

# Enterprise Vault™ インストール/設定

12.3

# Enterprise Vault™: インストールと設定

最終更新日: 2018-03-09。

## 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、ベリタス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](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](mailto:CustomerCare@veritas.com)

日本

[CustomerCare\\_Japan@veritas.com](mailto: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](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](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](mailto: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 .....	17
	このガイドの使い方 .....	17
	本書について .....	17
	Enterprise Vault についての詳しい情報の入手先 .....	18
	Enterprise Vault トレーニングモジュール .....	20
第 1 部	Enterprise Vault の必要条件 .....	21
第 2 章	Enterprise Vault ハードウェアの必要条件 .....	22
	Enterprise Vault サーバーのハードウェアの必要条件 .....	22
	仮想サーバーでの Enterprise Vault の実行 .....	23
	初期アーカイブ用の追加の処理量 .....	23
	SQL Server のハードウェアの必要条件 .....	23
	Enterprise Vault のネットワークの必要条件 .....	25
	Enterprise Vault のストレージの必要条件について .....	25
	ボルトストアのストレージ .....	26
	Enterprise Vault インデックスのストレージ .....	28
	SQL データベースのストレージの必要条件 .....	29
	Enterprise Vault キャッシュフォルダのストレージの必要条件 .....	32
	一時ファイルのローカルストレージの必要条件 .....	32
	TEMP フォルダのセキュリティ要件 .....	33
	TEMP フォルダへの追加のユーザーとグループアクセス権の付与 .....	33
第 3 章	Enterprise Vault の必要なソフトウェアとその設定 .....	35
	Enterprise Vault の必須ソフトウェアとその設定について .....	35
	Enterprise Vault サーバーの有効なコンピュータ名について .....	36
	Enterprise Vault Deployment Scanner について .....	36
	Enterprise Vault の基本的なソフトウェアの必要条件 .....	36
	Enterprise Vault に必要なオペレーティングシステムのコンポーネント .....	36
	SQL Server ソフトウェア .....	40
	SQLXML .....	41

インデックスサーバーにおける Net.Tcp ポート共有 .....	41
Enterprise Vault サーバーのベストプラクティス設定 .....	41
メッセージキューのクリーンアップ間隔: MessageCleanupInterval .....	41
メッセージキューのメッセージ格納限度: MachineQuota .....	42
便宜的ロックの無効化: OplocksDisabled .....	42
ループバックチェックの無効化: DisableLoopbackCheck .....	42
厳密な名前チェックの無効化: DisableStrictNameChecking .....	43
Outlook の添付ファイルと受信者の最大数: AttachmentMax and RecipientMax .....	43
TCP/IP 最大ポート数および TCP 時間待機の遅延 .....	44
Enterprise Vault サーバーのインストール前の作業 .....	45
ボルトサービスアカウントの作成 .....	46
SQL ログインアカウントの作成 .....	48
SQL データベースでの権限と役割の割り当てについて .....	49
必要な SQL Server ロールと権限の Active Directory グループへの割り当て .....	51
Enterprise Vault SQL データベースのロックダウン .....	51
Enterprise Vault の DNS エイリアスの作成 .....	51
Windows ファイアウォールの無効化または再設定 .....	52
データ場所の確保 .....	52
ユーザーアカウント制御 (UAC) について .....	53

## 第 4 章      Operations Manager の追加必要条件 ..... 54

Operations Manager の追加必要条件について .....	54
Operations Manager をインストールする場所とタイミング .....	54
Operations Manager に追加で必要なソフトウェア .....	55
Operations Manager のインストール前の追加タスク .....	55

## 第 5 章      分類の追加必要条件 ..... 56

分類の前提条件 .....	56
役割ベースの管理 (RBA) と分類機能 .....	57

## 第 6 章      Enterprise Vault Reporting の追加必要条件 ..... 58

Enterprise Vault Reporting の必要条件について .....	58
Enterprise Vault Reporting をインストールする場所と時期 .....	58
Enterprise Vault Reporting の前提条件 .....	59
監視または監査の有効化が必要な Enterprise Vault のレポート .....	59
Enterprise Vault Reporting のインストールの準備 .....	60

<b>第 7 章</b>	<b>Exchange Server アーカイブの追加必要条件</b>	62
	Exchange Server のアーカイブについて	62
	Exchange Server アーカイブのインストール前のタスク	62
	Enterprise Vault サーバーへの Outlook のインストール	63
	Enterprise Vault システムメールボックスの作成	64
	Windows Serverドメインコントローラに対する NSPI 接続の制限を削 除する	65
	Enterprise Vault サーバーでのユーザープロファイルの作成	65
	ボルトサービスアカウントのメールボックスの作成	66
	ボルトサービスアカウントの Exchange スロットルポリシーの設定	66
	ボルトサービスアカウントへのシステムメールボックスの[送信者]権限 の付与	68
	ボルトサービスアカウントへの Exchange Server 権限の割り当て	69
	Exchange Server アーカイブでの Enterprise Vault クライアントアクセス	72
	Enterprise Vault Outlook アドインの要件	72
	Mac OS X 用 Enterprise Vault クライアントの必要条件	73
	Enterprise Vault Office Mail App の必要条件	74
	OWA の必要条件	74
	カスタマイズされたショートカット	75
	アーカイブへのブラウザベースのアクセス	76
	RPC over HTTP の必要条件	76
	Enterprise Vault への Outlook Anywhere アクセスの要件	76
<b>第 8 章</b>	<b>Domino サーバーアーカイブの追加必要条件</b>	77
	すべての Enterprise Vault サーバーの Domino サーバーアーカイブの必 要条件	77
	Domino メールボックスアーカイブの要件	78
	Enterprise Vault Domino Gateway の必須ソフトウェア	78
	対象の Domino メールサーバーの必須ソフトウェア	79
	Notes クライアントの Enterprise Vault 拡張機能の要件	79
	Domino メールボックスアーカイブのインストール前の作業	79
	Enterprise Vault Domino Gateway の登録	80
	Domino メールボックスアーカイブ用のユーザー ID について	85
	対象の各 Domino メールサーバーに対するサーバー文書の設定	87
	Enterprise Vault Domino Gateway のインストールと設定	88
	Domino ジャーナルアーカイブの必要条件	90
	Domino ジャーナルデータベースからの Enterprise Vault アーカイブ の必要条件	90

	Domino のドメイン、サーバーおよびジャーナルの場所への Enterprise Vault のアクセスの設定 .....	91
	Domino メーリングリストグループ .....	92
	Domino ジャーナルアーカイブのクライアントアクセス .....	92
<b>第 9 章</b>	<b>ファイルシステムアーカイブ (FSA) の追加必要条件</b> .....	<b>93</b>
	FSA の要件について .....	93
	FSA での Enterprise Vault サーバーの必要条件 .....	93
	FSA ショートカットについて .....	94
	プレースホルダショートカットの必要条件 .....	95
	FSA エージェントについて .....	95
	FSA 用のファイルサーバーの準備 .....	96
	FSA でのクライアントの必要条件 .....	97
<b>第 10 章</b>	<b>SharePoint サーバーアーカイブの追加必要条件</b> .....	<b>98</b>
	SharePoint Server アーカイブの Enterprise Vault サーバーの必要条件について .....	98
	SharePoint Server の必要条件 .....	98
	SharePoint セキュリティ証明書について .....	100
<b>第 11 章</b>	<b>Skype for Business アーカイブの追加必要条件</b> .....	<b>101</b>
	Skype for Business アーカイブの必要条件について .....	101
	Skype for Business アーカイブの前提条件 .....	101
	ロールベースの管理 (RBA) と Skype for Business アーカイブ .....	102
	Skype for Business から対話をエクスポートするために必要な権限の割り当て .....	103
<b>第 12 章</b>	<b>SMTP アーカイブの追加必要条件</b> .....	<b>104</b>
	Enterprise Vault SMTP サーバーの追加要件 .....	104
<b>第 13 章</b>	<b>Enterprise Vault 検索の追加必要条件</b> .....	<b>106</b>
	Enterprise Vault による検索のサーバー必要条件 .....	106
	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 .....	107
	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 .....	108

第 14 章	スタンドアロンの Enterprise Vault 管理コンソールの追加必要条件 .....	110
	スタンドアロンの Enterprise Vault 管理コンソールの必要条件について .....	110
第 15 章	アーカイブディスカバリ検索サービスの追加必要条件 .....	112
	アーカイブディスカバリ検索サービスの追加の必要条件について .....	112
	アーカイブディスカバリ検索サービスに必要な追加のソフトウェア .....	113
	アーカイブディスカバリ検索サービスの SSL の設定 .....	113
	アーカイブディスカバリ検索サービスを監視するための Operations Manager の使用 .....	114
第 2 部	Enterprise Vault のインストール .....	115
第 16 章	ライセンスとライセンスキー .....	116
	Enterprise Vault ライセンスの概要 .....	116
	Enterprise Vault のライセンスキーの取得 .....	117
	Enterprise Vault ライセンスキーファイルのインストール .....	118
	Enterprise Vault ライセンスの置換と追加ライセンスのインストール .....	118
第 17 章	Enterprise Vault のインストール .....	119
	Enterprise Vault のインストールについて .....	119
	Enterprise Vault のインストール (ウィザード) .....	122
	Enterprise Vault のインストール (コマンドライン) .....	123
第 18 章	Enterprise Vault の修復、修正、アンインストール .....	127
	Enterprise Vault の修復、修正、アンインストールについて .....	127
	Enterprise Vault の修正 .....	127
	Enterprise Vault の修復 .....	128
	Enterprise Vault のアンインストール .....	130
第 3 部	Enterprise Vault の設定 .....	132
第 19 章	Enterprise Vault の設定について .....	133
	Enterprise Vault の設定について .....	133



第 20 章	Enterprise Vault 設定ウィザードの実行 .....	135
	Enterprise Vault 設定ウィザードを実行するタイミング .....	135
	Enterprise Vault 設定ウィザードの機能 .....	135
	Enterprise Vault 設定ウィザードの実行 .....	136
	Enterprise Vault 監視データベースの設定のトラブルシューティング .....	140
	デフォルトの SSL 設定の問題に関するトラブルシューティング .....	140
第 21 章	Enterprise Vault Web Access コンポーネントのセキュリティ保護 .....	142
	Enterprise Vault Web Access コンポーネントのデフォルトのセキュリティ .....	142
	Enterprise Vault Web Access コンポーネント用のポートまたはプロトコルのカスタマイズ .....	144
	Enterprise Vault Web Access コンポーネントの認証のカスタマイズ .....	145
	クライアントコンピュータでの Web Access コンポーネントのセキュリティのカスタマイズ .....	146
	プロキシバイパス一覧を使うための Internet Explorer の設定 .....	147
	Enterprise Vault Web Access コンポーネントを信頼するための Web ブラウザの設定 .....	148
	USGCB 準拠コンピュータへの Enterprise Vault サーバーの詳細の公開 .....	149
	Enterprise Vault Web Access コンピュータへのリモートアクセスの有効化 .....	150
第 22 章	Enterprise Vault 開始ウィザードの実行 .....	152
	Enterprise Vault 開始ウィザードの機能 .....	152
	Enterprise Vault 開始ウィザードの実行準備 .....	153
	Enterprise Vault 開始ウィザードの実行 .....	153
	Enterprise Vault 開始ウィザードのエクスプレスモードとカスタムモードについて .....	154
	Enterprise Vault 開始ウィザードでのインデックス設定について .....	154
	Enterprise Vault 開始ウィザードでのストレージ設定について .....	155
	Enterprise Vault 開始ウィザードでのポリシー定義について .....	158
	Enterprise Vault 開始ウィザードでの Exchange 対象設定について .....	158
	Enterprise Vault 開始ウィザードでの Domino 対象設定について ...	
	1 5 9	
	Enterprise Vault 開始ウィザードでのファイル対象設定について .....	161
	Enterprise Vault 開始ウィザードの計画 .....	161



	Enterprise Vault の単一インスタンスストレージの適切な共有設定の開発	198
	.....	198
	ボルトストアグループの作成	200
	ボルトストアの作成について	201
	Enterprise Vault のセーフコピーについて	201
	ボルトストアの作成	204
	ボルトストアパーティションの作成	205
	ボルトストアパーティションの初期状態	206
	コレクションと移行について	208
	標準のボルトストアパーティションの作成	209
	スマートパーティションの設定	211
	ローカルパスを使った NTFS パーティションのパーティションネットワーク共有	212
	ボルトストアグループに対する共有の設定	213
第 27 章	インデックスの場所の追加	215
	Enterprise Vault のインデックスの場所について	215
	Enterprise Vault のインデックスの場所の作成	215
第 28 章	インデックスサーバーグループの設定	217
	インデックスサーバーグループについて	217
	インデックスサーバーグループを作成する必要がありますか?	218
	複数の Enterprise Vault サーバーがありますか?	219
	ジャーナルアーカイブまたはファイルシステムアーカイブを使用しますか	
	または使う計画はありますか?	219
	Compliance Accelerator または Discovery Accelerator を使います	
	かまたは使う計画はありますか?	220
	サーバーのロードは既存の Enterprise Vault サーバーに均等に分散	
	されていますか?	220
	Enterprise Vault サーバーあたりおよそ 5,000 以上のメールボックス	
	のアーカイブがありますか?	221
	インデックスサーバーグループの作成	221
	インデックスサーバーグループにインデックスサーバーを追加	223
	インデックスサーバーグループからのインデックスサーバーの削除	224
	インデックスサーバーグループへのボルトストアの割り当て	225
	インデックスサーバーグループからのボルトストアの割り当て解除	226
	ボルトストアを別のインデックス付けに割り当てる	226
第 29 章	サイトのデフォルト設定のレビュー	229
	Enterprise Vault サイトのデフォルト設定のレビュー	229
	Enterprise Vault サイトのアーカイブスケジュールの設定	231

	Web Access アプリケーションの設定について .....	231
<b>第 30 章</b>	<b>Enterprise Vault 検索の設定 .....</b>	<b>233</b>
	Enterprise Vault による検索について .....	233
	Enterprise Vault Search ポリシーの定義 .....	234
	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 .....	236
	Enterprise Vault による検索用のプロビジョニンググループの設定 .....	237
	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 .....	238
	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 .....	239
	Enterprise Vault Search に対するユーザーのブラウザの構成 .....	240
	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 .....	241
	Forefront TMG とそれに類似する環境で使う Enterprise Vault 検索の設 定 .....	242
	Enterprise Vault 検索モバイル版の設定 .....	242
	Enterprise Vault 検索モバイル版のインストール前作業の実行 .....	243
	Enterprise Vault 検索モバイル版のインストール .....	243
	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 .....	245
	Enterprise Vault 検索モバイル版のインストールの確認 .....	246
<b>第 31 章</b>	<b>メタデータストアの管理 .....</b>	<b>247</b>
	メタデータストアについて .....	247
	メタデータストアの PowerShell コマンドレットについて .....	248
	高速参照とメタデータストアのインデックスについて .....	248
<b>第 5 部</b>	<b>VCS による Enterprise Vault のクラスタ 化 .....</b>	<b>249</b>
<b>第 32 章</b>	<b>VCS によるクラスタ化の概要 .....</b>	<b>250</b>
	サポートされる VCS 設定とソフトウェア .....	250
	Enterprise Vault と VCS GenericService エージェントについて .....	251
	VCS クラスタでの一般的な Enterprise Vault 構成 .....	251
	VCS 環境にコンポーネントをインストールして設定する順序 .....	252

第 33 章	Storage Foundation HA for Windows のインストールと設定 .....	254
	Enterprise Vault を使った Storage Foundation HA for Windows のインストールと設定 .....	254
	Storage Foundation HA 環境でのディスクグループとボリュームの管理 .....	256
第 34 章	Enterprise Vault の VCS サービスグループの設定 .....	258
	Enterprise Vault の VCS サービスグループの設定について .....	258
	Enterprise Vault の VCS サービスグループを設定するための準備 .....	259
	Enterprise Vault の VCS サービスグループの作成 .....	260
	既存の VCS サービスグループの修正 .....	262
	VCS サービスグループの削除 .....	263
第 35 章	Enterprise Vault 設定ウィザードの実行 .....	264
	Enterprise Vault 設定ウィザードの実行の準備 .....	264
	アクティブ/パッシブ VCS 構成での Enterprise Vault の設定 .....	264
	Enterprise Vault の初回インストールでの VCS クラスタサポートの追加 .....	265
	既存の Enterprise Vault インストール済み環境の VCS クラスタへのアップグレード .....	267
	既存のクラスタ化された Enterprise Vault サーバーへの SMTP アーカイブの追加 .....	271
	VCS N+1 構成での Enterprise Vault の設定について .....	271
	VCS N+1 クラスタ内での 2 つの Enterprise Vault サーバーノードと 1 つのスペアノードの設定 .....	272
	VCS クラスタの 3 つのノードのいずれかで実行するように 2 台の Enterprise Vault サーバーを構成する .....	274
	VCS クラスタ内の同じノードでの 2 台の Enterprise Vault サーバーの無効化 .....	275
第 36 章	Enterprise Vault での SFW HA-VVR のディザスタリカバリソリューションの実装 .....	277
	Enterprise Vault を使った SFW HA-VVR のインストールと設定について .....	277
	SFW HA-VVR のインストールと設定の手順の概要 .....	278
	プライマリサイトの VCS クラスタの設定 .....	279
	セカンダリサイトの VCS クラスタの設定 .....	280
	レプリケートするための VVR コンポーネントの追加 .....	280

	広域リカバリのために GCO コンポーネントを追加する .....	281
<b>第 37 章</b>	<b>VCS によるクラスタ化のトラブルシューティング .....</b>	<b>282</b>
	VCS ログ記録 .....	282
	Enterprise Vault Cluster Setup Wizard のエラーメッセージ .....	283
	Enterprise Vault 仮想サーバーのクラスタ化されたメッセージキューの表示 .....	284
<b>第 6 部</b>	<b>Windows Server フェールオーバークラス タリングでの Enterprise Vault のクラス タ化 .....</b>	<b>285</b>
<b>第 38 章</b>	<b>Windows Server フェールオーバークラスタリング でのクラスタ化の概要 .....</b>	<b>286</b>
	Windows Server フェールオーバークラスタでの Enterprise Vault のクラ スタ化について .....	286
	サポートされる Windows Server フェールオーバークラスタの構成 .....	287
	Windows Server フェールオーバークラスタリングでの Enterprise Vault のクラスタ化に必要なソフトウェアと制限 .....	287
	Windows Server フェールオーバークラスタでの共通の Enterprise Vault の設定 .....	288
	Windows Server フェールオーバークラスタの Enterprise Vault サービス の制御 .....	289
	Windows Server フェールオーバークラスタのクラスタサービスと Enterprise Vault サービスリソースについて .....	290
	Windows Server フェールオーバークラスタのフェールオーバー時の 動作 .....	290
<b>第 39 章</b>	<b>Windows Server フェールオーバークラスタリング でのクラスタ化の準備 .....</b>	<b>292</b>
	Windows Server フェールオーバークラスタリングでの Enterprise Vault のクラスタ化の準備 .....	292
	Windows Server フェールオーバークラスタの共有ディスクとボリュームの 設定 .....	293
	Enterprise Vault クラスタサービスを Windows Server フェールオーバー クラスタに対して設定する .....	294

<b>第 40 章</b>	<b>Windows Server フェールオーバークラスタでの Enterprise Vault の設定</b> .....	297
	Windows Server フェールオーバークラスタの Enterprise Vault の設定について .....	297
	Windows Server フェールオーバークラスタをサポートする新しい Enterprise Vault インストール済み環境を設定する方法 .....	298
	Windows Server フェールオーバークラスタリングをサポートする新しい Enterprise Vault サーバーの設定 .....	299
	Windows Server フェールオーバークラスタ内のフェールオーバーノードの設定 .....	303
	Enterprise Vault 監視データベースの設定のトラブルシューティング .....	304
	各種 Windows Server フェールオーバークラスタリングモードでの Enterprise Vault のインストール例 .....	304
	既存の Enterprise Vault インストール済み環境の Windows Server フェールオーバークラスタへの変換 .....	309
	既存の Enterprise Vault サーバーの Windows Server フェールオーバークラスタリングをサポートするサーバーへの変換 .....	310
	既存の Enterprise Vault クラスタの修正 .....	315
	既存の Windows Server フェールオーバークラスタへのノードの追加 .....	315
	Enterprise Vault クラスタサーバー用として既存の Windows Server フェールオーバークラスタに共有ストレージを追加する .....	316
	既存のクラスタ化された Enterprise Vault サーバーへの Enterprise Vault SMTP アーカイブの追加 .....	317
<b>第 41 章</b>	<b>Windows Server フェールオーバークラスタリングによるクラスタ化のトラブルシューティング</b> .....	318
	概要 .....	318
	Enterprise Vault イベントメッセージとフェールオーバークラスタのログ .....	319
	フェールオーバークラスタ環境で Enterprise Vault を設定するときのリソースの所有権と依存関係 .....	319
	フェールオーバークラスタノードのレジストリレプリケーション .....	319
	Enterprise Vault クラスタサーバーのクラスタ化されたメッセージキューの表示 .....	320
	Windows Server フェールオーバークラスタリング環境での Enterprise Vault サービスの起動と停止 .....	320
	Windows Server クラスタの潜在的なフェールオーバーの問題 .....	321

付録 A	Enterprise Vault サーバーを自動的に準備する	
	.....	322
	Enterprise Vault サーバーの自動準備について .....	322
	[マイシステムの準備]オプションによる Windows 機能の有効化 .....	322
	[マイシステムの準備]オプションの実行 .....	324



# 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。

- [このガイドの使い方](#)
- [本書について](#)
- [Enterprise Vault についての詳しい情報の入手先](#)

## このガイドの使い方

Enterprise Vault の新規インストールを実行する場合は、このガイドに従って操作してください。

Enterprise Vault の既存のインストール済み環境をアップグレードするには、『アップグレード』を参照してください。

Enterprise Vault Reporting のみをインストールする場合は、『レポート』を参照してください。

## 本書について

このガイドは、Enterprise Vault のインストールと設定に関する詳細情報を提供します。Enterprise Vault をインストールする前に、さまざまなコンポーネントについて理解できるように、『導入/計画』ガイドを参照してください。

Enterprise Vault をインストールし、設定するには、次の製品の管理方法を知る必要があります。

- Microsoft Windows Server
- Microsoft SQL Server
- Microsoft Message Queue Server
- Microsoft Internet Information Services (IIS)

■ 使用しているアーカイブストレージのハードウェアとソフトウェア

Enterprise Vault を Domino Server とともに使う場合は、Domino Server と Notes クライアントの管理知識も必要です。

Enterprise Vault を Exchange Server とともに使う場合は、Exchange Server と Outlook の管理知識も必要です。

Enterprise Vault を Windows SharePoint Services と SharePoint Portal Server とともに使う場合は、これらの製品の管理知識が必要です。

Enterprise Vault Reporting を使う場合は、Microsoft SQL Server Reporting Services の管理知識が必要です。

# 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"><li>■ 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。</li><li>■ 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。</li></ul>
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。

マニュアル	コメント
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。
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。

マニュアル	コメント
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。

# Enterprise Vault の必要条件

- 第2章 Enterprise Vault ハードウェアの必要条件
- 第3章 Enterprise Vault の必要なソフトウェアとその設定
- 第4章 Operations Manager の追加必要条件
- 第5章 分類の追加必要条件
- 第6章 Enterprise Vault Reporting の追加必要条件
- 第7章 Exchange Server アーカイブの追加必要条件
- 第8章 Domino サーバーアーカイブの追加必要条件
- 第9章 ファイルシステムアーカイブ (FSA) の追加必要条件
- 第10章 SharePoint サーバーアーカイブの追加必要条件
- 第11章 Skype for Business アーカイブの追加必要条件
- 第12章 SMTP アーカイブの追加必要条件
- 第13章 Enterprise Vault 検索の追加必要条件
- 第14章 スタンドアロンの Enterprise Vault 管理コンソールの追加必要条件
- 第15章 アーカイブディスカバリ検索サービスの追加必要条件

# Enterprise Vault ハードウェアの必要条件

この章では以下の項目について説明しています。

- [Enterprise Vault サーバーのハードウェアの必要条件](#)
- [SQL Server のハードウェアの必要条件](#)
- [Enterprise Vault のネットワークの必要条件](#)
- [Enterprise Vault のストレージの必要条件について](#)

## Enterprise Vault サーバーのハードウェアの必要条件

Enterprise Vault をインストールするコンピュータは、ドメインのメンバーである必要があります。

[表 2-1](#) に、Enterprise Vault 実働システムの推奨される最小仕様を示します。

**表 2-1** Enterprise Vault サーバーの最小仕様および推奨仕様

項目	推奨される最小仕様
プロセッサコアの数	最小: 4 推奨: 8 コアの合計数は物理 CPU とそのコアの任意の組み合わせとすることができます。
CPU の性能	2 GHz
メモリ	最小: 8 GB 推奨: 16 GB

項目	推奨される最小仕様
ディスク容量	1 GB <b>メモ:</b> Enterprise Vault は空きディスク領域が 1 GB 未満のパーティションにはインストールできません。

より小さな Enterprise Vault 環境では、Enterprise Vault のすべてのコアサービスを同じサーバーにインストールできます。ただし、より大きな環境では、ストレージサービスやインデックスサービスなどの個々のサービスを、専用の Enterprise Vault サーバーに配備することを検討できます。

Enterprise Vault サービスの配布について詳しくは、『導入/計画』ガイドを参照してください。

## 仮想サーバーでの Enterprise Vault の実行

仮想サーバーでは Enterprise Vault を実行できます。Enterprise Vault でサポートされる仮想化技術について詳しくは、Enterprise Vault [Compatibility Charts](#) を参照してください。

仮想 Enterprise Vault サーバーがインデックスサービスをホストする場合は、8 個のプロセッサコアをサポートする仮想マシンを使うことを推奨します。仮想マシンがこの数のプロセッサコアをサポートしない場合は、インデックスサービスのみをホストする専用の仮想サーバーを配備することを推奨します。

仮想サーバーでの Enterprise Vault のパフォーマンスについて詳しくは、『Enterprise Vault Performance Guide』(<https://www.veritas.com/docs/100000918>) を参照してください。

仮想サーバーへの Enterprise Vault の配備について詳しくは、Enterprise Vault のベストプラクティスに関する記事 (<https://www.veritas.com/docs/100038065>) を参照してください。

## 初期アーカイブ用の追加の処理量

大量のデータのバックログを短時間でアーカイブする場合は、最初に Enterprise Vault をインストールするときに、初期アーカイブを実行するために追加の Enterprise Vault サーバーを設定すると便利です。アーカイブが安定した状態に達したら、追加の Enterprise Vault サーバーを他の目的に使うように再配備できます。

## SQL Server のハードウェアの必要条件

Enterprise Vault では、次のように多くの SQL データベースが必要です。

- Enterprise Vault ディレクトリデータベースには、Enterprise Vault サイトの設定情報が保存されます。
- 各ボルトストアにはボルトストアデータベースがあり、このデータベースには、ボルトストアの設定情報とそのアーカイブに格納されているアイテムの詳細情報が保存されています。
- 各ボルトストアグループにはフィンガープリントデータベースがあり、このデータベースには、Enterprise Vault の単一インスタンスストレージ用に作成されている単一インスタンスストレージパーツに関連するフィンガープリントとその他の情報が保存されます。
- 監視データベースには、Enterprise Vault サイトの監視情報が保存されます。
- FSA レポートを設定すると、Enterprise Vault によって FSA レポート用データベースが作成され、FSA レポートデータが保存されます。必要であれば、拡張性を高めるために追加の FSA レポート用データベースを設定するか、または情報を分離できます。

これらのデータベースを管理する SQL Server は、通常、Enterprise Vault サーバーとは異なるコンピュータ上に配置します。

通常、SQL Server コンピュータの仕様は、Enterprise Vault サーバーの仕様に匹敵している必要があります。SQL Server が使えるメモリの量は、Windows と SQL Server のバージョンによって異なります。

表 2-2 に、実働 SQL Server の推奨する最小仕様を示します。サイズ変更のガイドラインについて詳しくは、ベリタスのサポート Web サイトで『Enterprise Vault SQL のベストプラクティスガイド』を参照してください。

[https://www.veritas.com/support/ja\\_JP/article.100012617](https://www.veritas.com/support/ja_JP/article.100012617)

表 2-2 SQL Server の最小仕様および推奨仕様

項目	推奨される最小仕様
プロセッサコアの数	最小: 4 推奨: 8 コアの合計数は物理 CPU とそのコアの任意の組み合わせとすることができます。
CPU の性能	2 GHz
メモリ	最小: 8 GB 推奨: 16 GB

Enterprise Vault サーバーごとに、個別の SQL Server を配置する必要はありません。原則として、1 つの SQL Server で最大 8 台の Enterprise Vault サーバーを管理できます。



## Enterprise Vault のネットワークの必要条件

Enterprise Vault は、大量のネットワークトラフィックを生成することがあります。最低限、接続が 100 Mbps スイッチドイーサネット LAN で予想される応答時間をサポートする環境を推奨します。

さまざまな条件における各種コンポーネント間で予想されるネットワークトラフィックのガイドラインについては、『Enterprise Vault Performance Guide』(<https://www.veritas.com/docs/100000918>) を参照してください。

Enterprise Vault の単一インスタンスストレージとの共有を設定すると、Enterprise Vault を使って、関連する接続全体でネットワーク遅延が許容可能であるかどうかの判断に役立つ接続性テストを行うことができます。

p.192 の「Enterprise Vault の単一インスタンスストレージについて」を参照してください。

## Enterprise Vault のストレージの必要条件について

Enterprise Vault の次のコンポーネントにはストレージが必要です。

- アーカイブ済みアイテムを保存するボルトストア。
- インデックス。
- 次の SQL Server データベース。
  - Enterprise Vault ディレクトリデータベース
  - ボルトストアデータベース
  - ボルトストアグループのフィンガープリントデータベース
  - 監視データベース
  - 1 つ以上の FSA レポート用データベース (FSA レポートが設定されている場合)
- Enterprise Vault が一時ファイルのために使うサーバーキャッシュ。
- 復元するアイテムの詳細を入れるために Enterprise Vault が使うショッピングバスケット。

さらに、Enterprise Vault サーバー上に小規模のローカルストレージが必要です。

このセクションでは、Enterprise Vault のストレージの必要条件に対する基本的なガイドを説明します。

すべてのサポート対象ストレージデバイスとソフトウェアについて詳しくは、Enterprise Vault [Compatibility Charts](#) を参照してください。

## ボルトストアのストレージ

Enterprise Vault Storage Service コンピュータはボルトストアのストレージにアクセスする必要があります。Enterprise Vault は、ボルトストアにさまざまなストレージを使い、他社製ソフトウェアとハードウェア製品によって提供される各種ストレージソリューションで動作するように設計されています。多くのストレージソリューションでは、高いパフォーマンスのアーカイブと取り込みが提供されます。次のような種類に分類できます。

- ローカルストレージ
- NTFS (NTFS ボリューム、またはネットワーク上に NTFS ボリュームとして表示されるネットワーク共有)
- SAN
- NAS
- CAS (Centera)
- Enterprise Vault ストレージストリーマ API をサポートするストレージデバイス

WORM (Write Once Read Many) 機能は一部のデバイスでサポートされます。

Enterprise Vault ストレージストリーマ API をサポートするストレージデバイスでボルトストアパーティションを作成することを計画する場合、適切なストレージデバイスソフトウェアが Enterprise Vault ストレージサーバーにインストールされていることを確認してください。ボルトストアグループのパーティションを管理するすべての Enterprise Vault ストレージサーバーにストレージデバイスソフトウェアをインストールします。

ストレージデバイスの速度は Enterprise Vault のパフォーマンスを決定づける最も重要な要因の 1 つです。

## WORM ストレージデバイスの準備

このセクションの情報は、SnapLock を使う NetApp ONTAP デバイス用です。他の WORM デバイスを使ってボルトストアパーティションを保存する場合は、可能であれば、同じような方法で設定することを推奨します。

必要なコマンドについて詳しくは、ストレージシステムの API のマニュアルを参照してください。

ボルトストアパーティションに対して使用できる WORM デバイスのリストについては、Enterprise Vault [Compatibility Charts](#) を参照してください。

NetApp デバイスでは、デフォルトの保持期間と、デバイスに格納するアイテムの最大保持期間を設定できます。Enterprise Vault の保持期間が[永続的]に設定されているアイテムをロックしたままにするには、ストレージデバイスで次の設定を明示的に行う必要があります。

- デフォルトの保持期間を無限に設定します。

- 最大保持期間を無限に設定します。

このいずれかが設定されていない場合、または無限以外の値に設定されている場合は、デバイスで設定したデフォルトの保持期間か最大保持期間の終了後、ユーザーまたは他社製アプリケーションがアイテムを削除できる可能性があります。

---

**メモ:** Enterprise Vault によってアイテムが期限切れになったり、削除されることはありません。

---

## ボルトストアに必要なストレージ容量

アイテムのアーカイブでは、まずアイテムが圧縮されてから、そのアイテムにメタデータが追加されます。原則として、アイテムは元のサイズの半分に圧縮され、およそ **5KB** のメタデータが構成されます。アイテムが共有されている場合は、メタデータのみが追加されます。

必要なストレージ容量の見積もりでは、次の原則が適用されます。

- アーカイブするアイテムの合計サイズを取得し、半分にします。
- 電子メールアイテムの場合、受信者の平均数で割ります。
- **5 KB** にアイテムの合計数を掛けて追加します。

圧縮率は大幅に変動することがあります。**Office** 文書は大きく圧縮される傾向があります。**ZIP** や **JPG** ファイルなどのその他の文書は、すでに圧縮されているためそれ以上圧縮できません。このため、必要なストレージ容量は常に多めに見積もる必要があります。

前の原則は、ほとんどの種類のアーカイブに適用されますが、ファイルシステムアーカイブ (**FSA**) では注意が必要です。たとえば、**ZIP** ファイルや **JPG** ファイルをアーカイブしても、領域は節約されません。

電子メールアーカイブの場合、メールボックス数、メッセージの数とサイズの増加も考慮する必要があります。これらの追加要因のため、確実な方法として、アーカイブに使われる領域が **Exchange Server** または **Domino** サーバーによってアイテムの格納に使われる領域と等しいと想定してストレージを見積もります。

## セカンダリストレージへのアーカイブ済みデータの移行

Enterprise Vault を使用してアーカイブしたデータをセカンダリストレージシステムに移行できます。Enterprise Vault を使用すると、ボルトストアパーティションから、Amazon Simple Storage Service、Microsoft Azure Blob Storage、Google Cloud Storage などのクラウドのセカンダリストレージの場所にファイルを移行できます。

『[Compatibility Charts](#)』には、Enterprise Vault がサポートするセカンダリストレージソフトウェアの最新の情報が記載されています。

---

**注意:** 応答が遅いセカンダリストレージを使う場合は、このストレージにアクセスする Enterprise Vault の操作の一部に時間がかかります。たとえば、テープやクラウドはともに非常に遅くなることのあるストレージです。

---

## Enterprise Vault インデックスのストレージ

Enterprise Vault Indexing Service をホストするコンピュータは、インデックス用に十分な容量のあるストレージにアクセスする必要があります。

また、各インデックスサービスは、インデックス付けの設定とレポートデータ用のディスク領域を必要とします。この領域は、インデックスサービスプロパティの[インデックスメタデータの場所]を使用して設定されます。Enterprise Vault をクラスタにインストールした場合は、インデックスメタデータフォルダ `Enterprise Vault installation folder\EVIndexing\data\metadata` を共有ドライブに移動する必要があります。また、インデックスサービスプロパティの[インデックスメタデータの場所]を更新する必要があります。

インデックスはローカルストレージ、SAN、NAS に配置できます。高速のインデックス付けが必要な場合、または多数のアーカイブ間の検索を行う場合は、NAS デバイスは適していないことがあります。

ソリューションの一部として、光ディスクなどの低速のストレージメディアを使うファイルシステムは、インデックスに適していません。

インデックスが NetApp デバイスや他の NAS システムに格納されている場合、インデックスを含むボリュームでは、便宜的ロックを無効にする必要があります。詳しくは Veritas Enterprise サポート Web サイトで次の記事を参照してください。

<https://www.veritas.com/docs/100017354>

ウイルス対策ソフトウェアによってデータが変更される可能性があるため、ウイルスチェックアプリケーションではインデックスの場所を除外しておくことが重要です。詳しくは Veritas Enterprise サポート Web サイトで次の記事を参照してください。

<https://www.veritas.com/docs/100017720>

表 2-3 に、インデックスの予測サイズを計算する方法を示します。

表 2-3 元のデータのサイズと比較したインデックスサイズ

インデックスの種類	元のデータのサイズに対するインデックスサイズの割合
簡略	4%
完全	12%

アーカイブするデータの種類もインデックスサイズに影響します。大量のテキストファイルや HTML ファイルをアーカイブした場合は、大きいサイズのインデックスが生成されます。

イメージファイルなどの多数のバイナリファイルをアーカイブした場合は、内容はインデックス付けされないため、小さいサイズのインデックスが生成されます。

インデックスファイルは共有できません。

## SQL データベースのストレージの必要条件

次の SQL データベースにはストレージ領域が必要です。

- Enterprise Vault ディレクトリデータベース
- ボルトストアデータベース
- ボルトストアグループのフィンガープリントデータベース
- 監視データベース
- 1 つ以上の FSA レポート用データベース (FSA レポートが設定されている場合)
- 監査データベース

### Enterprise Vault ディレクトリデータベースに必要なストレージ

ディレクトリデータベースの初期ストレージの必要条件は、データデバイスに 10 MB、トランザクションログデバイスに 25 MB で、合計 35 MB の初期ディスク領域が必要となります。

一時的な増加とトランザクションログに対応するため、ディレクトリデータベースに 5 GB の容量を用意することを推奨します。

### ボルトストアデータベースに必要なストレージ

各ボルトストアデータベースの初期ストレージの必要条件は、データデバイスに 100 MB、トランザクションログデバイスに 80 MB で、各ボルトストアデータベースに合計 180 MB の初期ディスク領域が必要となります。

データの追加に伴ってデータベースデバイスを拡張できる領域があることを確認します。トランザクションログは、バックアップと保守計画に応じて、適切なサイズに制限する必要があります。

各ボルトストアデータベースの基本的なサイジングガイドとして、アーカイブするアイテムごとに 250 バイトと、静的データ、トランザクションログ、一時的なデータの変動用に 5 GB を加えます。

Dell EMC Centera デバイスでボルトストアパーティションを設定し、パーティションでのコレクションを有効にした場合、関連付けされたボルトストアデータベースに保存セットテーブル用の追加の SQL インデックスが作成される場合があります。該当するボルトストアデータベースをホストする SQL Server でこのインデックスに必要な領域は、保存セットテーブルの 1 行あたり約 27 バイトです。

## フィンガープリントデータベースに必要なストレージ

ボルトストアグループのフィンガープリントデータベースには、グループのボルトストアにアーカイブされている各 SIS パーツに関するフィンガープリント、ストレージの場所、共有境界情報がアーカイブされます。

フィンガープリントデータベースの初期のストレージ必要条件是 **212 MB** で、その内訳は次のとおりです。

- プライマリファイルグループ用に **100 MB**
- **32** 個の非プライマリファイルグループごとに **1 MB**
- トランザクションログデバイス用に **80 MB**

非プライマリファイルグループには、SIS パーツのフィンガープリントと、SIS パーツに関するその他の情報が保存されます。Enterprise Vault の単一インスタンスストレージを使ってアイテムを共有する場合、非プライマリファイルグループのサイズが非常に急速に増大することがあります。データが追加されて大きくなるため、非プライマリファイルグループ用に十分な空き領域があることを確認してください。

新規ボルトストアグループウィザードには、フィンガープリントデータベースの初期設定を行うための次のオプションが表示されます。

- Enterprise Vault が 1 つのデバイス上のプライマリファイルグループとすべての非プライマリファイルグループを検索する場合のデフォルト基本設定。
- **32** 個の非プライマリ SQL ファイルグループに個別の場所を指定できる詳細設定オプション。

アーカイブと取り込みの許容されるパフォーマンスを確保するために、ボルトストアグループ内の共有の量に対してフィンガープリントデータベースを適切に設定することが重要です。

最適なパフォーマンスを得るには、次の手順を実行します。

- 詳細設定オプションを使って、SQL Server に可能な限り多くの場所を (最大 **32** 個) を指定します。
- 場所ごとにデバイスを 1 つずつ使います。同じデバイスに複数の場所を指定した場合、パフォーマンス上のメリットが得られません。

---

**メモ:** フィンガープリントデータベースの設定後の場所の追加または変更は、SQL Server の管理タスクです。

---

トランザクションログは、バックアップと保守計画に応じて、適切なサイズに制限してください。

## 監視データベースに必要なストレージ

監視データベースの初期ストレージの必要条件は、データデバイスに 100 MB、トランザクションログデバイスに 80 MB で、合計 180 MB の初期ディスク領域が必要となります。

監視データの追加に伴ってデータベースを拡張できる領域があることを確認します。

## FSA レポート用データベースに必要なストレージ

FSA レポートを設定すると、Enterprise Vault によって FSA レポート用データベースが作成されます。このデータベースには、Enterprise Vault ファイルコレクションサービスによって収集されたデータが格納されます。このデータは、FSA レポートのデータ分析レポートに使われます。

たとえば拡張性を高めるために追加の FSA レポート用データベースを作成するか、またはレポートデータを分離することがあります。

各 FSA レポート用データベースの初期ストレージの必要条件は、データデバイスに 100 MB、トランザクションログデバイスに 80 MB です。初期ディスク領域には合計 180 MB が必要です。

レポートデータが追加されて大きくなるため、各 FSA レポート用データベースに十分な空き領域があることを確認してください。

FSA レポート用データベースの履歴テーブルを調整するためのバッチファイルが提供されています。バッチファイルは、最新の情報と傾向に関する情報を保持しています。

『レポート』の FSA レポート用データベースの保守に関する説明を参照してください。

## 監査データベースに必要なストレージ

監査データベースは、監査を有効にするまで作成されません。デフォルトでは、監査は無効になっています。

監査データベースの初期ストレージの必要条件は、データベースに 100 MB、トランザクションログに 80 MB です。

個々の Enterprise Vault サーバーに対して監査を有効にできます。サイトの複数の Enterprise Vault サーバーに対する監査イベントを 1 つの監査データベースに書き込むことができます。

必要な容量は、ログに記録するイベントの数と種類、必要な詳細のレベルによって異なります。

『監査』ガイドに監査の設定方法が説明されています。

トランザクションログは、バックアップと保守計画に応じて、適切なサイズに制限してください。監査データベースのロールオーバー方法について詳しくは、次の Veritas のサポート文書を参照してください。

<https://www.veritas.com/docs/100016653>

## Enterprise Vault キャッシュフォルダのストレージの必要条件

キャッシュから、Enterprise Vault が使う一時ファイルの領域が提供されます。この Enterprise Vault サーバーで次のいずれかが設定されている場合は、キャッシュの場所を指定する必要があります。

- インデックスサービス
- PST 移行
- Celerra/VNX ファイルサーバーを対象にアーカイブするファイルシステム
- パススルー呼び戻しを設定する場合は、NetApp ファイルサーバーを対象にアーカイブするファイルシステム
- [ボルトキャッシュ]
- 分類

次のいずれかの機能が Enterprise Vault サーバーで設定されている場合、キャッシュの場所を指定する必要があります。管理コンソールから Enterprise Vault サーバーのコンピュータプロパティの[キャッシュ]タブでキャッシュの場所を設定します。

キャッシュの場所を設定するときは、次の点に注意します。

- 最適なパフォーマンスを確保するためには、ローカルに接続された高速ストレージでキャッシュフォルダを作成します。
- ボルトサービスアカウントには、キャッシュフォルダへの読み取りアクセス権と書き込みアクセス権が必要です。
- キャッシュの主な用途は、ボルトキャッシュクライアントに一時ストレージを提供することです。ボルトキャッシュを使う Enterprise Vault クライアントが少ない場合、最低 20 GB の空き容量のある場所で十分です。ボルトキャッシュを使うクライアントが多い場合は、もっと空き容量の多い場所を指定します。
- ウイルス対策ソフトウェアはキャッシュ内のデータを変更する可能性があるので、ウイルスチェックからキャッシュの場所を除外することが重要です。
- Veritas Cluster Server または Windows Server フェールオーバークラスターリングで Enterprise Vault をクラスタ化した場合、キャッシュの場所はクラスタリソースになります。

## 一時ファイルのローカルストレージの必要条件

一時ファイル用に小規模のローカルストレージが必要です。たとえば、ローカルの一時領域は、大きいファイルを処理する際にストレージサービスによって使われます。MSMQ ファイルと Windows システムファイル用にもローカルストレージが必要です。

TEMP システム変数をドライブ C 以外のドライブに再割り当てすることを推奨します。



低速のローカルディスクは、Enterprise Vault のパフォーマンスに深刻な影響を与えることがあります。MSMQ ファイル用に個別のディスクを割り当ててを推奨します。RAID 5 ではなく RAID 1+0 を使うなど、最高の速度を得られるようにディスクを設定する必要があります。

## TEMP フォルダのセキュリティ要件

重要な Enterprise Vault データが含まれている場合がある TEMP フォルダへの無断アクセスから保護するために、Admin サービスは起動時にフォルダへのアクセスを確認し、その後も定期的に確認します。Admin サービスは無断アクセス権限を検出すると、イベントログにエラーを書き込み、すぐに終了します。

TEMP フォルダへのアクセスは、次のいずれかの方法で承認された SID を使用して付与される必要があります。

- SID は、ローカル Administrators グループ、ローカル Backup Operators グループ、Domain Admins グループ、ローカルシステム、System Operators グループのいずれかを識別します。
- SID は TempFolderExceptions レジストリ値でリストに登録されているアカウントの 1 つを識別します。  
p.33 の「TEMP フォルダへの追加のユーザーとグループアクセス権の付与」を参照してください。
- アクセスは Creator Owner SID を使用して与えられます。TEMP フォルダの現在の所有者には前述の条件の下でのアクセス権が付与されます。
- この SID はユーザーを識別し、Admin サービスを実行しているユーザーの SID と同じです。

Enterprise Vault Admin サービスはフォルダの随意アクセス制御リスト (DACL) を調べます。DACL がない場合、検査は失敗し、サービスはすぐに終了します。DACL がある場合は、管理サービスは各アクセス制御エントリ (ACE) の SID をチェックし、正しく承認されていない SID を使用して TEMP フォルダへのアクセスが付与されている場合はすぐにサービスを終了します。

Enterprise Vault TEMP フォルダの要件について詳しくは、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/support/ja\\_JP/article.100014060](https://www.veritas.com/support/ja_JP/article.100014060)

## TEMP フォルダへの追加のユーザーとグループアクセス権の付与

権限のあるアカウントをリストアップするレジストリエントリを設定することで、TEMP フォルダにアクセスできる追加ユーザーとグループを指定できます。

### TEMP フォルダへの追加のユーザーとグループアクセス権を付与するには

- 1 レジストリエディタを開きます。
- 2 次のサブキーを参照します。

```
HKEY_LOCAL_MACHINE
¥SOFTWARE
¥Wow6432Node
¥KVS
```

- 3 「TempFolderExceptions」という名前の文字列エントリを作成し、権限のあるアカウントをセミコロンで区切られたリストに登録する値をそれに与えます。次に例を示します。

```
MyDomain¥JohnDoe;builtin¥JohnDoe
```

ローカルユーザーとグループを識別する builtin の使用に注目してください。

# Enterprise Vault の必要なソフトウェアとその設定

この章では以下の項目について説明しています。

- [Enterprise Vault](#) の必須ソフトウェアとその設定について
- [Enterprise Vault](#) サーバーの有効なコンピュータ名について
- [Enterprise Vault Deployment Scanner](#) について
- [Enterprise Vault](#) の基本的なソフトウェアの必要条件
- [Enterprise Vault](#) サーバーのベストプラクティス設定
- [Enterprise Vault](#) サーバーのインストール前の作業

## Enterprise Vault の必須ソフトウェアとその設定について

この章では、以下のことについて説明します。

- [Enterprise Vault](#) のコアコンポーネントのソフトウェアの必要条件。
- [Enterprise Vault](#) をインストールする前に実行する必要がある作業

「[Enterprise Vault Compatibility Charts](#)」には、必要なソフトウェアのサポート対象バージョンの詳細が示されています。

[Enterprise Vault](#) のその他の省略可能なコンポーネントとさまざまな種類のアーカイブには、追加要件があります。後の章で説明するように、計画しているインストールに対する追加の必要条件の情報もレビューします。

[Enterprise Vault](#) をクラスタ環境にインストールする場合にも必要条件があります。

# Enterprise Vault サーバーの有効なコンピュータ名について

コンピュータ名に Unicode 文字が含まれている Enterprise Vault サーバーは、適切に動作しない可能性があります。Enterprise Vault サーバーのコンピュータ名には ASCII 文字のみ含めることを強く推奨します。

## Enterprise Vault Deployment Scanner について

Enterprise Vault をインストールする前に、Enterprise Vault Deployment Scanner を使って不足している必要条件を見つけることができます。サーバーのインストールの準備が完了したら、Deployment Scanner を実行してすべての必要条件が正しくインストールされているかどうかを確認することを推奨します。Enterprise Vault インストーラを起動する場合、インストールが開始する前に Deployment Scanner を実行するオプションが選択できます。

Enterprise Vault Deployment Scanner は、Enterprise Vault メディアで提供される別のウィザードです。ツールを実行すると、ツールを実行したフォルダに Reports フォルダが作成され、その Reports フォルダにレポートファイルが作成されます。

Deployment Scanner と付属マニュアルは、Enterprise Vault メディアの Veritas Enterprise Vault¥Deployment Scanner フォルダにあります。

## Enterprise Vault の基本的なソフトウェアの必要条件

このセクションでは、Enterprise Vault コアサービスのオペレーティングシステムとソフトウェアの必要条件について説明します。

異なる種類のアーカイブには、追加の必要条件がある場合があります。

必要に応じて、Enterprise Vault 管理コンソールを別のコンピュータにインストールできます。

p.110 の「[スタンドアロンの Enterprise Vault 管理コンソールの必要条件について](#)」を参照してください。

## Enterprise Vault に必要なオペレーティングシステムのコンポーネント

Enterprise Vault では Windows サーバーのバージョンが各 Enterprise Vault サーバーにインストールされる必要があります。Windows Server のすべてのバージョンがサポートされているわけではなく、バージョンによっては特定の Service Pack やホットフィックスが必要です。

サポート対象バージョンについて詳しくは、Enterprise Vault [Compatibility Charts](#) を参照してください。

次のオプションと機能を指定して Windows をインストールします：

- NTFS ファイルシステム。
- Microsoft メッセージキュー (MSMQ) サービス。  
p.37 の「[MSMQ のインストール](#)」を参照してください。
- IIS (Internet Information Services) 7.5 以降。  
p.38 の「[IIS \(Internet Information Services\)](#)」を参照してください。
- .NET Framework 3.5 SP1、.NET Framework 4.5.2
- PowerShell 3.0 以降。  
p.39 の「[PowerShell](#)」を参照してください。
- Internet Explorer 9 以降。
- MSXML。  
p.39 の「[MSXML](#)」を参照してください。
- Windows TIFF IFilter  
p.39 の「[Windows IFilter](#)」を参照してください。

## MSMQ のインストール

Enterprise Vault のタスクは、MSMQ を使ってストレージサービスと通信します。ネットワーク内の複数のコンピュータに Enterprise Vault サービスをインストールする場合、各コンピュータで MSMQ を設定する必要があります。

MSMQ をインストールするときには次の点に注意してください。

- Active Directory 統合は無効にする必要があります。
- システムドライブ以外のドライブに MSMQ のストレージフォルダを配置することを推奨します。

### MSMQ をインストールするには

- 1 サーバーマネージャを開きます。
- 2 [クイックスタート] ペインの [ロールと機能の追加] をクリックします。
- 3 ウィザードが開いたら、[インストールの種類] 画面の [ロールベースまたは機能ベースのインストール] を選択し、[機能の選択] ページが表示されるまで [次へ] をクリックします。
- 4 [メッセージキュー] を選択します。Enterprise Vault に必要な MSMQ 機能は [メッセージキューサーバー] のみです。
- 5 [次へ] をクリックし、その後はウィザードの指示に従ってください。

## IIS (Internet Information Services)

各 Enterprise Vault サーバーには IIS 7.5 以降が必要です。

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。設定ウィザードは Enterprise Vault Web アプリケーションの適切なアプリケーションプールを自動的に作成して、正しい分離設定とアカウント設定を行います。

Enterprise Vault がアプリケーションプール用に設定したアカウントを使用することをお勧めします。たとえば、EnterpriseVaultAppPool が事前定義済みのローカルシステムアカウントで実行されない場合、EnterpriseVault Web アプリケーションでショッピングバスケットが正しく作成されません。

Enterprise Vault 12.3 以降の新規インストールでは、Enterprise Vault は Enterprise Vault Web アプリケーションへの接続に必要なプロトコルとして HTTPS を自動的に設定します。Enterprise Vault の新規インストール時にデフォルトの Web サイトで SSL をまだ設定していない場合は、Enterprise Vault 設定ウィザードが次の処理を行います。

- 自己署名証明書を作成してインストールします。
- ポート 443 に HTTPS バインドを追加し、自己署名証明書を割り当てます。
- すべての Enterprise Vault 仮想ディレクトリで SSL を有効にします。

自己署名証明書は一時的なものとなし、できるだけ早く信頼できる認証局から取得した証明書に交換することが重要です。自己署名証明書は、Enterprise Vault サーバーでは信頼されません。これにより、Enterprise Vault Outlook アドイン、Enterprise Vault 検索、および Veritas Information Classifier の機能の一部がリモートコンピュータから接続するクライアントで動作しなくなる場合があります。

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、IIS の Enterprise Vault 仮想ディレクトリの設定は変更されません。ただし、Enterprise Vault への Web 接続のセキュリティを確保するために、Enterprise Vault 仮想ディレクトリで SSL を手動で設定し、有効にすることをお勧めします。

p.144 の「[Enterprise Vault Web Access コンポーネント用のポートまたはプロトコルのカスタマイズ](#)」を参照してください。

### Enterprise Vault の IIS に関する要件

IIS に関連する役割サービスの最小セットがあります。これらの役割サービスがあることを確認する最も簡単な方法は、Enterprise Vault Install Launcher 内の[マイシステムの準備]オプションを使うことです。このオプションを使うと、Enterprise Vault サーバーに必要なすべての Windows の機能と役割が自動的にインストールされます。

[マイシステムの準備]を使わない場合は、機能と役割を手動で追加できます。

p.322 の「[Enterprise Vault サーバーの自動準備について](#)」を参照してください。

---

**メモ:** Windows Server Update Services ロールは Enterprise Vault と互換性がないのでインストールしないでください。

---

## PowerShell

PowerShell は、システム管理者向けに設計された Windows コマンドラインシェルです。各 Enterprise Vault サーバーに Windows PowerShell 3.0 以降が必要です。PowerShell を使うときのヘルプについて詳しくは、Microsoft の PowerShell マニュアルを参照してください。

Enterprise Vault PowerShell モジュールにサーバーグラフィックシェル機能もインストールする必要があります。サーバーマネージャで[役割と機能の追加]を使ってこの機能をインストールします。この機能をまだインストールしていない場合は、サーバーマネージャで[機能] > [ユーザーインターフェースとインフラ]の順に移動して[サーバーグラフィックシェル]を選択します。

PowerShell には、*cmdlets* というネイティブバイナリコマンドが用意されています。一部の Enterprise Vault 管理タスクは、PowerShell スナップインに用意されている追加の *cmdlets* を使って管理します。これらの Enterprise Vault *cmdlets* を使うには、PowerShell をインストールする必要があります。

### PowerShell を実行して Enterprise Vault スナップインをロードする方法

- ◆ [アプリ]画面で[Enterprise Vault]>[管理シェル]を選択します。

Enterprise Vault PowerShell スナップインは 32 ビット版であり、64 ビット版のサーバー上でも 32 ビット版の PowerShell で実行する必要があります。[管理シェル]ショートカットでは、32 ビット版の PowerShell が自動的に実行されます。ただし、Enterprise Vault *cmdlet* をバックアップスクリプトなどの外部スクリプトから直接実行する場合は、必ず 32 ビット版の PowerShell を呼び出す必要があります。

## MSXML

すべての Enterprise Vault サーバーコンピュータには MSXML が必要です。MSXML は、Internet Explorer とともに自動的にインストールされます。

Enterprise Vault サービスコンポーネントのインストール時に MSXML 6.0 が存在しない場合、Enterprise Vault インストーラによってインストールされ、確認は求められません。

## Windows IFilter

ストレージサービスは、必要であればアイテムを HTML またはテキストに変換し、この変換された内容がアイテムのインデックス付けに使われます。Enterprise Vault ストレージサービスは、Oracle® Corporation の Outside In® Technology コンテンツ変換を使ってほとんどのファイルの種類を変換します。Enterprise Vault は Windows TIFF IFilter を使って、イメージのファイルの種類的光学式文字認識 (OCR) 変換を提供します。

Windows TIFF IFilter は、Enterprise Vault インストーラによって自動的に有効化される (すでに有効でない場合) オプションの Windows 機能です。必要な場合は、追加の 64-bit IFilters をインストールして、コンテンツの変換機能を拡張できます。たとえば、IFilters を追加して、デフォルトのコンテンツコンバータによってサポートされていないファイルの種類のコンテンツ変換を提供できます。追加する IFilters は、ストレージサービスをホストする各 Enterprise Vault サーバーにインストールする必要があります。

OCR と IFilter のコンテンツの変換は、アーカイブ内のファイルと zip、tar、pst ファイルなどのコンテンツファイルに適用されます。

コンテンツの変換の設定は、Enterprise Vault 管理コンソールの詳細サイト設定を使って変更できます。[IFilter 変換のファイルの種類] 設定では、追加した IFilters を使って変換するファイルの種類を設定できます。[コンテンツの変換] サイト設定については、『管理者ガイド』で説明されています。

## SQL Server ソフトウェア

Enterprise Vault では、次のバージョンの SQL Server をサポートします。

- SQL Server 2012 x64 Edition (Enterprise、Business Intelligence、および Standard)
- SQL Server 2014 x64 Edition (Enterprise、Business Intelligence、および Standard)
- SQL Server 2016 x64 Edition (Enterprise、および Standard)
- SQL Server 2017 x64 Edition (Enterprise、および Standard)

SQL Server のサポート対象バージョンと必要なサービスパックの最新情報については、Enterprise Vault [Compatibility Charts](#) を参照してください。

次の点に注意してください。

- Windows 認証モードと混在モード認証の両方がサポートされています。
- のインストールでは大文字と小文字の区別がサポートされていないため、SQL インストールは大文字と小文字を区別しないで実行する必要があります。
- Enterprise Vault では、マスターとすべての Enterprise Vault データベースにわたって SQL の照合が一樣に行われる必要があります。照合に一貫性がないと Enterprise Vault をインストールできなくなるため、照合が一樣に行われることを開始前に確認する必要があります。

Deployment Scanner は、SQL Server が Enterprise Vault のすべての必要条件を満たしていることを確認するためにチェックを実行します。



## SQLXML

Enterprise Vault サービスコンポーネントをインストールするコンピュータには **SQLXML 4.0 SP1** が必要です。

Enterprise Vault サービスコンポーネントをインストールするときに **SQLXML 4.0 SP1** が存在しない場合は、Enterprise Vault インストーラが自動的にインストールします。確認は求められません。

## インデックスサーバーにおける Net.Tcp ポート共有

Enterprise Vault のインデックス付けには、Windows の **Net.Tcp** ポート共有サービスを使用します。**Net.Tcp** ポート共有サービスのスタートアップの種類が「**Disabled**」に設定されている場合、インデックスサービスはスタートアップの種類を「**Manual**」に自動的に変更してサービスを開始します。

## Enterprise Vault サーバーのベストプラクティス設定

Enterprise Vault のベストプラクティス設定は、Enterprise Vault サーバーで最善のパフォーマンスが得られるようにします。設定にはエラーを防止するものや、パフォーマンスを向上させるものがあります。

インストール中に、これらのベストプラクティス設定を自動的に指定するオプションがあります。これらの設定を手動で変更する必要はありません。

## メッセージキューのクリーンアップ間隔: MessageCleanupInterval

名前	MessageCleanupInterval
場所	HKEY_LOCAL_MACHINE <div>¥Software</div> <div>¥Microsoft</div> <div>¥MSMQ</div> <div>¥Parameters</div>
種類	DWORD
ベストプラクティス設定	1800000 (ミリ秒 = 30 分)
説明	MessageCleanupInterval は、Microsoft Message Queuing (MSMQ) が古いメッセージファイルを削除する間隔を制御します。MSMQ のデフォルトである 6 時間は Enterprise Vault に対しては長すぎます。古いメッセージファイルが蓄積されると、最終的にアーカイブサービスが停止する可能性があります。

## メッセージキューのメッセージ格納限度: MachineQuota

名前	MachineQuota
場所	HKEY_LOCAL_MACHINE <div>¥Software</div> <div>¥Microsoft</div> <div>¥MSMQ</div> <div>¥Parameters</div> <div>¥MachineCache</div>
種類	DWORD
ベストプラクティス設定	8388608 (KB = 8 GB)
説明	Microsoft Message Queuing (MSMQ) メッセージ用に許容されるデフォルトのディスククォータは、Enterprise Vault アーカイブタスクには十分ではありません。すべての領域が使われている場合、Enterprise Vault アーカイブタスクはアイテムをアーカイブすることができません。

## 便宜的ロックの無効化: OplocksDisabled

名前	OplocksDisabled
場所	HKEY_LOCAL_MACHINE <div>¥System</div> <div>¥CurrentControlSet</div> <div>¥Services</div> <div>¥MRXSmb</div> <div>¥Parameters</div>
種類	DWORD
ベストプラクティス設定	(16 進数) 01
説明	便宜的ロックにより、インデックスの破損を含む 32 ビットインデックスの問題が発生する可能性があります。

## ループバックチェックの無効化: DisableLoopbackCheck

名前	DisableLoopbackCheck
----	----------------------

場所	HKEY_LOCAL_MACHINE ¥System ¥CurrentControlSet ¥Control ¥Lsa
種類	DWORD
ベストプラクティス設定	00000001 (10 進数)
説明	DisableLoopbackCheck が設定されていない場合は、管理コンソールでアクセス拒否エラーが発生する可能性があり、設定内容によっては Enterprise Vault サービスを開始できないことがあります。

## 厳密な名前チェックの無効化: DisableStrictNameChecking

名前	DisableStrictNameChecking
場所	HKEY_LOCAL_MACHINE ¥System ¥CurrentControlSet ¥Services ¥LanmanServer ¥Parameters
種類	DWORD
ベストプラクティス設定	00000001 (10 進数)
説明	Enterprise Vault は DNS エイリアスを使います。クライアントコンピュータがエイリアス名を使って Windows サーバーへ接続すると、エラーメッセージが出されることがあります。この問題は、クライアントが DNS ゾーンで作成された CNAME エイリアスを使って接続しようとしたときに生じる可能性があります。サーバーはエイリアスに対する応答準備をしていないため、その名前への接続を受け入れません。厳密な名前チェックを無効にすると、この問題が解決されます。

## Outlook の添付ファイルと受信者の最大数: AttachmentMax and RecipientMax

名前	AttachmentMax RecipientMax
----	-------------------------------

場所	HKEY_CURRENT_USER ¥Software ¥Microsoft ¥Office ¥version ¥Outlook ¥Options ¥Mail
種類	DWORD
ベストプラクティス設定	AttachmentMax: (16 進数) FFFFFFFF  RecipientMax: (16 進数) FFFFFFFF
説明	<p>Outlook が Enterprise Vault Storage Service コンピュータで実行されている場合、Microsoft Outlook の問題によってエラーが発生することがあります。</p> <p>この問題は、アーカイブ済みアイテムが次のいずれかに該当する場合に発生します。</p> <ul style="list-style-type: none"> <li>■ [宛先]、[CC]、[BCC]のいずれかのフィールドの受信者が 2048 以上。</li> <li>■ 添付ファイルが 2048 以上である。</li> </ul> <p>この問題によるエラーは、Enterprise Vault がアーカイブ済みアイテムを呼び戻すときに常に発生する可能性があります。たとえば、インデックスを再構築するときなどです。</p> <p>この問題を解決するには、RecipientMax と AttachmentMax レジストリエントリの値を FFFFFFFF (16 進数) に設定します。</p>

## TCP/IP 最大ポート数および TCP 時間待機の遅延

名前	MaxUserPort  TcpTimedWaitDelay
場所	HKEY_LOCAL_MACHINE ¥System ¥CurrentControlSet ¥Services ¥Tcpip ¥Parameters
種類	DWORD

ベストプラクティス設定	MaxUserPort: (16 進数) fffe TcpTimedWaitDelay: (16 進数) 78
説明	<p>TCP/IP クライアント接続に一時的に使われるポートのデフォルトの数は、Enterprise Vault アーカイブに対して不十分な場合があります。ポートが少なすぎる場合、一部のアイテムはサーバーからアーカイブされず、Enterprise Vault にエラーメッセージが表示されることがあります。</p> <p>詳しくは Microsoft 社の次の記事を参照してください。  <a href="http://msdn.microsoft.com/library/aa560610.aspx">http://msdn.microsoft.com/library/aa560610.aspx</a></p>

# Enterprise Vault サーバーのインストール前の作業

実装するアーカイブの種類にかかわらず、このセクションで説明する作業を実行する必要があります。

表 3-1 Enterprise Vault サーバーのインストール前の作業

手順	作業	詳細の参照先セクション
手順 1	ボルトサービスアカウントを作成します。	p.46 の「 <a href="#">ボルトサービスアカウントの作成</a> 」を参照してください。
手順 2	SQL ログインアカウントを作成します。	p.48 の「 <a href="#">SQL ログインアカウントの作成</a> 」を参照してください。
手順 3	SQL データベースで必要な権限とロールを割り当てます。	p.49 の「 <a href="#">SQL データベースでの権限と役割の割り当てについて</a> 」を参照してください。
手順 4	Enterprise Vault の DNS エイリアスを作成します。	p.51 の「 <a href="#">Enterprise Vault の DNS エイリアスの作成</a> 」を参照してください。
手順 5	Windows ファイアウォールを無効にするか、再設定します。	p.52 の「 <a href="#">Windows ファイアウォールの無効化または再設定</a> 」を参照してください。
手順 6	Enterprise Vault インデックスおよびボルトストアパーティションファイルの格納場所を安全な場所にします。	p.52 の「 <a href="#">データ場所の確保</a> 」を参照してください。
手順 7	ユーザーアカウント制御 (UAC) についての情報を読み取ります。	p.53 の「 <a href="#">ユーザーアカウント制御 (UAC) について</a> 」を参照してください。

## ボルトサービスアカウントの作成

ボルトサービスアカウントは、Enterprise Vault プロセスが Windows サーバーオペレーティングシステムにアクセスするために使います。このアカウントは、Enterprise Vault ディレクトリ内のすべての Enterprise Vault コンピュータにより共有されます。複数の Enterprise Vault サイトを管理している場合は、複数の Enterprise Vault サイトに対して同じボルトサービスアカウントを使えます。

ボルトサービスアカウントは、各 Enterprise Vault コンピュータのローカル Administrators グループのメンバーである必要があります。このアカウントは、Enterprise Vault ディレクトリ内のすべてのサーバーのローカル Administrators グループメンバーである、ドメインベースの Windows セキュリティアカウントである必要があります。このアカウントのパスワードを空白にすることはできません。同じ Enterprise Vault ディレクトリに複数の Enterprise Vault サイトを作成する場合は、すべてのサイトに同じボルトサービスアカウントを使う必要があります。

このアカウントをドメイン管理者にしないでください。必要な権限を明示的に割り当てることを推奨します。このセクションでは、このアカウントに設定する必要がある基本的な権限について説明します。アーカイブの種類によっては、ボルトサービスアカウントに追加の権限が必要です。追加の権限の詳細については、実装するアーカイブの種類のセクションを参照してください。

Enterprise Vault コンピュータと同じドメインにアカウントを作成できる場合は、そのように作成してください。ボルトサービスアカウントと Enterprise Vault コンピュータをそれぞれ別のドメインに含める必要がある場合は、Enterprise Vault コンピュータのドメインが信頼できるドメインにこのアカウントを作成してください。

Microsoft メッセージキューのセキュリティで、Administrators グループに Enterprise Vault のキューへのアクセス権が付与されていることを確認してください。

Enterprise Vault のインストール時および Enterprise Vault 設定ウィザードの実行時は、ボルトサービスアカウントでログインする必要があります。

設定ウィザードの一部のページでは SQL Server データベースファイルのための場所を指定する必要があります。SQL Server コンピュータの観点からパスを入力することによって場所を明示的に指定できます。ウィザードはまた場所を選択するために SQL Server コンピュータを参照することを可能にする参照ボタンを提供しています。ただし、フォルダの参照は、ボルトサービスアカウントが SQL Server コンピュータの管理共有にアクセスできる場合にのみ利用可能です。管理コンソールのいくつかのウィザードが類似の参照ボタンを提供していることに注意してください。それらの参照ボタンを使うためには、管理コンソールを実行するために使うアカウントも SQL Server の管理共有にアクセスする必要があります。

SQL システム管理者 (sysadmin) ロールをボルトサービスアカウントに割り当てない場合は、Enterprise Vault 設定ウィザードを初めて実行する前にいくつかの追加手順を実行する必要があります。

p.49 の「SQL データベースでの権限と役割の割り当てについて」を参照してください。

設定中に、ボルトサービスアカウントの名前とパスワードを入力するように要求されます。Enterprise Vault により、アカウントに対して次の拡張ユーザー権限が自動的に付与されます。

- サービスとしてログオン
- プログラムのデバッグ
- プロセスレベルトークンの置き換え

Active Directory のレプリケーションの完了を待つ必要がある場合があります。レプリケーションが完了するまではアカウントを使えません。

#### ボルトサービスアカウントを作成する方法

- 1 ドメインコントローラで、[Active Directory ユーザーとコンピュータ]を開きます。
- 2 [Active Directory ユーザーとコンピュータ]の左側のペインで、[ドメイン]コンテナをダブルクリックします。
- 3 [ユーザー]コンテナをダブルクリックします。
- 4 操作メニューで[新規作成]をクリックし、[ユーザー]をクリックします。[新しいオブジェクト - ユーザー]画面が表示されます。
- 5 [新しいオブジェクト - ユーザー]画面に情報を入力し、[次へ]をクリックします。次に表示される画面で、パスワードの入力を要求されます。
- 6 パスワードを入力し、確認します。パスワードは必ず設定してください。ボルトサービスアカウントのパスワードを空白にすることはできません。

---

**メモ:** ボルトサービスアカウントのパスワードを以前変更し、Enterprise Vault アドオンをインストールしている場合、アドオンのボルトサービスアカウントのユーザーアカウントログイン資格情報を変更する必要がある場合もあります。詳しくはアドオンに付属のマニュアルを参照してください。

---

- 7 [パスワードを無期限にする]にチェックマークを付けます。
- 8 以下に示す他のチェックボックスはすべてはずします。
  - [ユーザーは次回ログオン時にパスワード変更が必要]
  - [ユーザーはパスワードを変更できない]
  - [アカウントは無効]
- 9 [次へ]をクリックして概要画面を表示します。
- 10 [完了]をクリックすると、新しいユーザーが作成されます。

新しいボルトサービスアカウントをローカルの **Administrators** グループに追加する方法

- 1 管理者として Enterprise Vault コンピュータにログオンします。
- 2 [コントロール パネル]で[管理ツール]を開き、[コンピュータの管理]コンソールを起動します。
- 3 [システム ツール]を展開し、[ローカル ユーザーとグループ]を展開します。
- 4 [グループ]を選択し、右側のペインで[Administrators]グループをダブルクリックします。
- 5 [追加]を使ってボルトサービスアカウントをこのグループに追加します。
- 6 [OK]をクリックします。
- 7 Enterprise Vault をインストールしたコンピュータごとにこれらの手順を繰り返します。

## SQL ログインアカウントの作成

ボルトサービスアカウントには、SQL Server に、必要な権限を持つ SQL ログインアカウントが必要です。次の手順では、このログインアカウントを作成する方法について説明します。

---

**メモ:** ボルトサービスアカウントを **Active Directory** グループのメンバーにしている場合、次の手順に従って、ボルトサービスアカウントではなくこのグループに対して SQL ログインアカウントを作成することもできます。ただし、このグループの SQL ログインアカウントには、ボルトサービスアカウントに対するログインアカウントでは必要ない追加のロールと権限が必要です。

p.51 の「[必要な SQL Server ロールと権限の Active Directory グループへの割り当て](#)」を参照してください。

---

SQL ログインアカウントを作成するには

- 1 SQL Server Management Studio を起動します。
- 2 Object Explorer で、[セキュリティ] > [ログイン]と選択します。
- 3 [ログイン]を右クリックし、[新しいログイン]を選択します。
- 4 **domain\username** としてボルトサービスアカウントを入力するか、[検索]をクリックしてアカウントを検索します。[検索]ダイアログボックスで、[場所]フィールドに正しいドメインが入力されていることを確認します。
- 5 [Windows 認証]を選択します。
- 6 [ページを選択]ペインの[サーバーロール]をクリックします。
- 7 dbcreator の横にチェックマークを付けます。



- 8 [OK]をクリックします。
- 9 ツールバーで、[新しいクエリ]をクリックします。
- 10 次のスクリプトを入力します。

```
use Master
GRANT VIEW SERVER STATE TO "domain¥vsa_account"
GRANT ALTER ANY LOGIN TO "domain¥vsa_account"
GRANT VIEW ANY DEFINITION TO "domain¥vsa_account"
GO
```

**domain¥vsa\_account** はボルトサービスアカウントのドメインと名前です。

- 11 [実行]をクリックします。
- 12 次のようにして、ボルトサービスアカウントに **dbcreator** ロールが設定されていることを確認します。
  - Object Explorer で、[セキュリティ] > [サーバーロール]を選択します。
  - 右側のペインで、**dbcreator** ロールをダブルクリックします。
  - ボルトサービスアカウントが所属リストにあることに注意してください。
- 13 次のようにして、ボルトサービスアカウントに適切な権限が設定されていることを確認します。
  - Object Explorer の最上位 SQL Server オブジェクトを右クリックして、[プロパティ]を選択します。
  - [権限]ページを選択します。
  - [ログインまたはロール]でボルトサービスアカウントを選択し、[有効]をクリックします。権限リストに[VIEW SERVER STATE]、[ALTER ANY LOGIN]、[VIEW ANY DEFINITION]が含まれていることを確認します。

## SQL データベースでの権限と役割の割り当てについて

SQL システム管理者 (**sysadmin**) ロールをボルトサービスアカウントに割り当てない場合は、Enterprise Vault 設定ウィザードを初めて実行する前に次の追加手順を実行する必要があります。

- ボルトサービスアカウントを **msdb** システムデータベースに追加します。
- ボルトサービスアカウントに **msdb** テーブル **sysjobs**、**sysjobschedules**、**sysjobsteps**、**sysjobsteps** の選択権限を付与します。
- ボルトサービスアカウントにデータベースロール **SQLAgentUserRole** を割り当てます。

これらの手順を実行しない場合は次の問題が発生します。

- Enterprise Vault は監視データベースからの履歴レコードのページに失敗し、これらのデータベースレコードは増大し続けます。
- 完了時に Enterprise Vault 設定ウィザードはエラーをイベントログに、カテゴリ「Monitoring Configuration Utility」、Event ID 41123 として記録します。次のようにエラーの説明が開始されて、Purge Job SQL スクリプトファイルの内容が表示されます。

Monitoring Configuration Utility reported error: SQL Error at: --

これらの追加手順を実行しないで Enterprise Vault 設定ウィザードを実行する場合は、Veritas サポート Web サイトの次の記事を参照してください。

<https://www.veritas.com/docs/100021414>

## SQL データベースの権限とロールの割り当て

msdb のシステムデータベースにボルトサービスアカウントを追加し、アカウントに必要なアクセス許可を付与し、アカウントに SQLAgentUserRole データベースのロールを割り当ててください。

### msdb システムデータベースにボルトサービスアカウントを追加する方法

- 1 SQL Server コンピュータで、SQL Server Management Studio を起動します。
- 2 目的の SQL Server を選択します。
- 3 [データベース]、[システム データベース]、[msdb]、[セキュリティ]、[ユーザー] の順に参照します。
- 4 [ユーザー] を右クリックし、[新しいユーザー] をクリックします。
- 5 [ユーザー名] フィールドに、新しいユーザー名を入力します。
- 6 [ログイン名] フィールドに、**domain¥user\_name** という形式でボルトサービスアカウントのドメインとユーザー名を入力します。
- 7 [OK] をクリックします。

### ボルトサービスアカウントに権限を付与する方法

- 1 作成した新しいユーザーを右クリックして、[プロパティ] をクリックします。
- 2 [セキュリティ保護可能なリソース] ページを選択します。
- 3 セキュリティ保護可能なリソースの一覧に次の msdb テーブルを追加し、これらのテーブルの選択権限をボルトサービスアカウントに付与します。
  - sysjobs
  - sysjobschedules
  - sysjobservers
  - sysjobsteps

ボルトサービスアカウントにデータベースロール **SQLAgentUserRole** を割り当てる方法

- 1 [データベース]、[システム データベース]、[msdb]、[セキュリティ]、[ロール]、[データベース ロール]の順に参照します。
- 2 [SQLAgentUserRole]を右クリックして、[プロパティ]をクリックします。
- 3 [全般] ページで [追加] をクリックして、作成したボルトサービスアカウントを選択します。

## 必要な SQL Server ロールと権限の Active Directory グループへの割り当て

必要な SQL Server ロールと権限は、直接ボルトサービスアカウントに割り当てるのではなく、ボルトサービスアカウントが属する **Active Directory** グループに割り当てられます。これを選択する場合、次のセクションに記載されるロールと権限を **Active Directory** グループに割り当てる必要があります。

- p.48 の「[SQL ログインアカウントの作成](#)」を参照してください。
- p.49 の「[SQL データベースでの権限と役割の割り当てについて](#)」を参照してください。

さらに、次の内容を **Active Directory** グループに割り当てる必要があります。

- sysadmin サーバーロール。
- msdb システムデータベースの実行権限。

## Enterprise Vault SQL データベースのロックダウン

デフォルトでは、ボルトサービスのアカウントが **Enterprise Vault SQL** データベースのすべてを所有します。これは、ボルトサービスのアカウントでデータベース内のすべてのオブジェクトにフルにアクセスができることを意味します。

**Enterprise Vault** のデータベースは、ボルトサービスアカウントのこれらのデータベースに対する所有権を無効にできる一連のロールを含み、**Enterprise Vault** の実行に必要な最小限の権限のみ割り当てます。詳しくは **Veritas サポート Web サイト** の次の記事を参照してください。

[https://www.veritas.com/support/ja\\_JP/article.100038151](https://www.veritas.com/support/ja_JP/article.100038151)

## Enterprise Vault の DNS エイリアスの作成

各 **Enterprise Vault** サーバーコンピュータに **DNS** エイリアスを作成することを推奨します。**Enterprise Vault** 設定ウィザードを実行すると、非修飾エイリアス (**evserver1** など) を入力するように要求されます。サイト内の最初のコンピュータに **Enterprise Vault** が設定されると、**Enterprise Vault** はそのコンピュータに対して入力された **DNS** エイリア

スを使って自動的にボルトサイトエイリアスを作成します。ボルトサイトエイリアスは、Enterprise Vault ソフトウェアで Enterprise Vault サイトを参照するために使われます。

DNS エイリアスに特殊文字は使用できません。RFC-1034 で定義されているように、a から z、A から Z、0 から 9、ハイフン (-)、ピリオド (.) のみが許可されます。最後の文字はハイフンやピリオドにはできません。

非修飾 DNS エイリアスを使うと、今後 Enterprise Vault サービスを実行するコンピュータを変更する場合に、柔軟に対応することができます。

## Windows ファイアウォールの無効化または再設定

Windows ファイアウォールは、Windows Server 2012 以降ではデフォルトで有効になっています。これにより、分散 COM (DCOM) は機能できなくなります。Enterprise Vault では DCOM が必要なため、Windows ファイアウォールを無効にするか、Windows ファイアウォールを適切に設定する必要があります。Enterprise Vault は DCOM 用に動的な TCP/IP ポートを必要とします。

TCP/IP の動的ポート範囲を設定する方法のガイドラインについては、次の記事を参照してください。

<http://support.microsoft.com/kb/929851>

Enterprise Vault が働くように Windows ファイアウォールで特定のポートを開く必要もあります。これらのポートについては、『Veritas Enterprise Vault™ 管理者ガイド』の「Enterprise Vault プログラムのファイアウォールの設定」を参照してください。

## データ場所の確保

Enterprise Vault データ用に使用される場所を確保することは重要です。権限があるアカウントのみが、インデックスとボルトストアパーティションに使用されるネットワーク共有およびフォルダへのアクセスを許されます。通常、これらの場所では、セキュリティ ACL を使ってアクセス制御を実装します。

Enterprise Vault データにネットワーク共有を使用する場合、ボルトサービスアカウントが、そのリモートサーバー上のネットワーク共有にフルアクセスできることを確認する必要があります。ネットワーク共有で Enterprise Vault データ場所へのアクセスを管理するために推奨される方法は、この目的でドメインセキュリティグループを作成することです。このアプローチにより、もしボルトサービスアカウントを変更したとしても、新しい許可をすべてのサブフォルダとファイルに反映させる必要が回避できます。

#### データ場所を確保する方法

- 1 インデックス場所およびボルトストアパーティションフォルダに使用する計画のあるネットワーク共有およびフォルダ上の **ACL** をチェックします。  
  
ボルトサービスアカウントとローカル管理者以外のアカウントは、これらの場所の保有や継承、アクセスはできません。
- 2 グループを使用してネットワーク共有へのアクセスを管理する場合、**Active Directory (EVDataAccess など)** にドメインセキュリティグループを作成します。
- 3 ボルトサービスアカウントを新しいグループに追加します。
- 4 その新しいグループに対して、インデックス場所およびボルトストアパーティションに使用する計画のあるネットワーク共有およびフォルダへのフルアクセスを認可します。

## ユーザーアカウント制御 (UAC) について

Veritas はストレージの場所としてマップしたドライブを使うことを推奨しません。マップされたドライブを使用すると、**Windows** のユーザーアカウント制御 (**UAC**) により、ストレージの場所に **Enterprise Vault** がアクセスできなくなる可能性があります。マップされたドライブの代わりに、**UNC** パスの使用が推奨されます。

# Operations Manager の追加必要条件

この章では以下の項目について説明しています。

- [Operations Manager の追加必要条件について](#)
- [Operations Manager をインストールする場所とタイミング](#)
- [Operations Manager に追加で必要なソフトウェア](#)
- [Operations Manager のインストール前の追加タスク](#)

## Operations Manager の追加必要条件について

Enterprise Vault Operations Manager は個別にインストール可能なコンポーネントです。これは、Internet Explorer がインストールされているコンピュータから Enterprise Vault をリモート監視できるようにする Web アプリケーションです。

## Operations Manager をインストールする場所とタイミング

Operations Manager を使って Enterprise Vault サイトの Enterprise Vault サーバーを監視するには、そのサイトの少なくとも 1 台の Enterprise Vault サーバーに Operations Manager をインストールする必要があります。

Operations Manager には、同一コンピュータに Enterprise Vault サービスが必要です。Enterprise Vault サービスコンポーネントのインストールと同時または後で、Operations Manager コンポーネントをインストールできます。Operations Manager を設定する前に、Enterprise Vault の設定ウィザードを実行して Enterprise Vault サービスを設定する必要があります。

## Operations Manager に追加で必要なソフトウェア

Operations Manager をインストールするコンピュータには、Enterprise Vault に必要なコアソフトウェアとその設定だけでなく、次のソフトウェアが必要です。

- IIS (Internet Information Services) はロックダウンされていない必要があります。

p.35 の「[Enterprise Vault の必須ソフトウェアとその設定について](#)」を参照してください。

## Operations Manager のインストール前の追加タスク

Operations Manager が Enterprise Vault データベースにアクセスするときに使えるように、「MonitoringUser」などの名前で Active Directory ドメインに Windows ユーザーアカウントを作成します。この監視ユーザーアカウントには Exchange メールボックスは必要ありません。アカウントは Windows の Administrators グループのメンバーである必要もありません。

監視ユーザーアカウントを作成する場合は、次のことに注意してください。

- [パスワードを無期限にする] オプションにチェックマークを付けます。
- 残りのチェックボックス ([ユーザーは次回ログオン時にパスワード変更が必要]、[ユーザーはパスワードを変更できない]、[アカウントは無効]) はチェックマークをはずしたままにします。

# 分類の追加必要条件

この章では以下の項目について説明しています。

- 分類の前提条件
- 役割ベースの管理(RBA)と分類機能

## 分類の前提条件

Microsoft ファイル分類インフラストラクチャ (FCI) を使用した分類を実装するには、サイト内の全 Enterprise Vault ストレージサーバーで、次のものがすべて必要です。

- Windows Server 2012 または 2012 R2。  
パフォーマンスの理由から、Windows Server 2012 オリジナルリリースではなく、Windows Server 2012 R2 をすべての Enterprise Vault サーバーで実行することを強く推奨します。
- File Server Resource Manager サービスと関連のツール機能 (fsrm.msc)。  
これらのコンポーネントを使用すると、Windows FCI を管理できます。そのため、分類ルールとプロパティの作成と編集を行うことができます。  
Enterprise Vault Install Launcher では、「マイシステムの準備」機能により File Server Resource Manager サービスとツールが自動的に有効化されます。
- Microsoft Data Classification Toolkit。  
Enterprise Vault サイト全体で分類プロパティとルールを配備するには、このツールキットと連携させることができる Enterprise Vault PowerShell cmdlet を使うことができます。Microsoft 社の Web サイトの次のページからダウンロードできます。  
<https://msdn.microsoft.com/library/hh204743.aspx>

Veritas Information Classifie を使用した分類では、Enterprise Vault をインストールする際に、必要なコンポーネントがすべてインストールされます。

Microsoft FCI または Veritas Information Classifier を使用して分類を管理するには、Enterprise Vault の保持機能のライセンスも必要です。保持機能のライセンスをインス



トールする必要がある場合、または既存のライセンスが期限切れになった場合、分類はテストモードで動作します。

## 役割ベースの管理(RBA)と分類機能

Enterprise Vault 分類機能を管理するには、Vault Administration Console の次の RBA ロールが 1 つ以上必要です。

- Domino 管理者
- Exchange 管理者
- 拡張コンテンツプロバイダの管理者
- ファイルサーバー管理者
- NSF 管理者
- メイン管理者
- PST 管理者
- SharePoint 管理者
- SMTP 管理者

RBA について詳しくは、『Veritas Enterprise Vault 管理者ガイド』を参照してください。

# Enterprise Vault Reporting の追加必要条件

この章では以下の項目について説明しています。

- [Enterprise Vault Reporting](#) の必要条件について
- [Enterprise Vault Reporting](#) をインストールする場所と時期
- [Enterprise Vault Reporting](#) の前提条件
- 監視または監査の有効化が必要な [Enterprise Vault](#) のレポート
- [Enterprise Vault Reporting](#) のインストールの準備

## Enterprise Vault Reporting の必要条件について

Enterprise Vault Reporting 機能は、レポートのしくみとして Microsoft SQL Server Reporting Services を使うことで、Enterprise Vault サーバーにエンタープライズレベルのレポート機能を提供します。管理者は、レポートサービスのレポートマネージャ Web アプリケーションを使って、レポートの内容を管理し、レポートを表示します。

Enterprise Vault FSA レポートを使う場合は、FSA レポートが必要です。

Enterprise Vault Reporting について詳しくは『レポート』を参照してください。

## Enterprise Vault Reporting をインストールする場所 と時期

通常、Enterprise Vault Reporting コンポーネントは、Microsoft SQL Server Reporting Services を実行するサーバー上に他の Enterprise Vault コンポーネントがなくてもイン

ストールできます。ただし、必要な前提条件が満たされている場合は、Reporting コンポーネントを Enterprise Vault サーバーのインストールに含めることができます。

Enterprise Vault Reporting コンポーネントはいつでもインストールできます。ただし、Enterprise Vault サービスがインストールされているサイトの少なくとも 1 台のコンピュータで Enterprise Vault 設定ウィザードを正常に実行するまでは、レポート設定ユーティリティを実行しないでください。

## Enterprise Vault Reporting の前提条件

Enterprise Vault Reporting は、次の前提条件を満たすコンピュータにインストールできます。

- Microsoft .NET Framework 3.5 SP1
- 次のいずれかのバージョンの Microsoft SQL Server Reporting Services が使用可能であること。
  - Microsoft SQL Server 2012 Reporting Services
  - Microsoft SQL Server 2014 Reporting Services
  - Microsoft SQL Server 2016 Reporting Services
  - Microsoft SQL Server 2017 Reporting Services
- Enterprise Vault データベースをホストするコンピュータ (1 つまたは複数) へのネットワーク接続がされていること

FSA Reporting を設定する場合は、FSA Reporting 用データベースをホストする SQL Server コンピュータに次のソフトウェアをインストールする必要があります。

- Microsoft SQLXML 4.0 SP1
- Microsoft MSXML 6.0

## 監視または監査の有効化が必要な Enterprise Vault のレポート

いくつかの Enterprise Vault Reporting のレポートは、ソースデータに対する Enterprise Vault 監視機能または Enterprise Vault 監査機能を使用しています。

次のレポートは、Enterprise Vault 監視機能を有効にすることが必要です。

- Enterprise Vault サーバーの 24 時間の健全性の状態
- Enterprise Vault サーバーの 7 日間の健全性の状態
- Exchange Server ジャーナルメールボックスアーカイブの健全性

- Exchange Server ジャーナルメールボックスアーカイブの傾向
- Domino サーバージャーナルメールボックスアーカイブの健全性
- Domino サーバージャーナルメールボックスアーカイブの傾向

次のレポートは、Enterprise Vault 監査機能を有効にすることが必要です。

- アーカイブ済みアイテムのアクセス
- アーカイブ済みアイテムのアクセス傾向

これらのレポートを使う場合は、必要に応じて Enterprise Vault の監視または監査を設定してください。

---

**メモ:** 監視と監査は、Enterprise Vault Reporting のインストールと設定の前または後のどちらでも設定できます。この影響を受けるレポートには、関連するデータが監視データベースまたは監査データベースに保存されるまで、情報が保存されません。

---

Enterprise Vault 設定ウィザードによる監視を有効にすることができます。

Operations Manager コンポーネントをインストールした場合は、Enterprise Vault Operations Manager Web アプリケーションによる監視を有効にすることもできます。

『管理者ガイド』の Enterprise Vault Operations Manager による監視に関する章の監視パラメータの設定に関するセクションを参照してください。

監査を設定するには、監査を有効にしてから、情報を収集する Enterprise Vault サーバーで監査を設定する必要があります。

『管理者ガイド』の監査に関する説明を参照してください。

## Enterprise Vault Reporting のインストールの準備

Enterprise Vault Reporting コンポーネントをインストールする前に、次の手順を実行する必要があります。

### Enterprise Vault Reporting のインストールを準備する方法

- 1 Enterprise Vault Reporting が Enterprise Vault データベースへのアクセス時に使えるように、「ReportingUser」などの名前と Active Directory ドメインに Windows ユーザーアカウントを作成します。このレポートのユーザーアカウントにはメールボックスは必要ありません。また、アカウントは Windows の Administrators グループのメンバーである必要もありません。

レポートのユーザーアカウントを作成する場合は、次の手順を実行します。

- [パスワードを無期限にする]オプションにチェックマークを付けます。

- 残りのチェックボックス([ユーザーは次回ログオン時にパスワード変更が必要]、[ユーザーはパスワードを変更できない]、[アカウントは無効])はチェックマークをはずしたままにします。
- 2 **Microsoft SQL Server Reporting Services** サーバーでボルトサービスアカウントに「コンテンツマネージャ」ロールを付与します。ユーザーアカウントへの **Microsoft SQL Server Reporting Services** のロールの割り当て方法については、Microsoft 社のマニュアルを参照してください。
  - 3 ボルトサービスアカウントを **Microsoft SQL Server Reporting Services** サーバーコンピュータの **Local Administrators** グループに追加します。

# Exchange Server アーカイブの追加必要条件

この章では以下の項目について説明しています。

- [Exchange Server のアーカイブについて](#)
- [Exchange Server アーカイブのインストール前のタスク](#)
- [Exchange Server アーカイブでの Enterprise Vault クライアントアクセス](#)
- [RPC over HTTP の必要条件](#)

## Exchange Server のアーカイブについて

次の対象 Exchange Server 上のメールボックスとパブリックフォルダからアイテムをアーカイブできます。

- Exchange Server 2010 SP1 とそれ以降
- Exchange Server 2013
- Exchange Server 2016

## Exchange Server アーカイブのインストール前のタスク

このセクションでは、Exchange Server のすべてのバージョンからのアーカイブをサポートするために完了する必要があるインストール前の作業について説明します。

- 「[Enterprise Vault サーバーへの Outlook のインストール](#)」
- 「[Enterprise Vault システムメールボックスの作成](#)」

- 「Windows Server ドメインコントローラに対する NSPI 接続の制限を削除する」
- 「Enterprise Vault サーバーでのユーザープロファイルの作成」
- 「ボルトサービスアカウントのメールボックスの作成」
- 「ボルトサービスアカウントの Exchange スロットルポリシーの設定」
- 「ボルトサービスアカウントへのシステムメールボックスの[送信者]権限の付与」
- 「ボルトサービスアカウントへの Exchange Server 権限の割り当て」

## 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 7-1 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。 <a href="https://www.veritas.com/docs/100040583">https://www.veritas.com/docs/100040583</a> 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。

## Enterprise Vault システムメールボックスの作成

Enterprise Vault システムメールボックスは、Exchange Server への接続時に、Exchange メールボックスタスク、Exchange ジャーナルタスク、Exchange パブリックフォルダタスクによって使われるメールボックスです。

Enterprise Vault でアーカイブする各 Exchange Server にシステムメールボックスを作成する必要があります。

---

**メモ:** Exchange 環境でデータベース可用性グループ (DAG) を使う場合、DAG に渡ってレプリケートされるデータベースにそれぞれの Enterprise Vault システムメールボックスを作成してください。

---

次の必要条件にも注意してください。



- このメールボックスは、**Enterprise Vault** のタスクが専用に使うメールボックスであり、他の目的には使えません。
- アドレステー一覧でメールボックスを非表示にしないでください。
- **Enterprise Vault** システムメールボックスが関連付けされているアカウントを無効にしないでください。

Exchange Server アーカイブタスクの作成時に、**Enterprise Vault** によってこのメールボックスの名前の入力が必要になります。

**Enterprise Vault** システムメールボックスを作成すると、メールボックスが利用可能になるまでにしばらく時間がかかることがあります。**Exchange Server** アーカイブタスクを追加する前に、メールボックスが利用可能になっている必要があります。

## Windows Server ドメインコントローラに対する NSPI 接続の制限を削除する

Windows Server ドメインコントローラは、NSPI 接続をユーザーあたり 50 個の同時接続に制限します。**Enterprise Vault** の **Exchange** アーカイブタスクのエラーを防ぐためにこの制限を解除する必要があります。

**Windows Server** ドメインコントローラの同時 **NSPI** 接続の制限を解除するには

- 1 **Windows Server** のドメインコントローラで、次のレジストリキーの下に「**NSPI max sessions per user**」という新しいレジストリ **DWORD** 値を作成します。

```
HKEY_LOCAL_MACHINE
¥System
  ¥CurrentControlSet
    ¥Services
      ¥NTDS
        ¥Parameters
```

- 2 「**NSPI max sessions per user**」を **0xffffffff** に設定します。

これは「**NSPI max sessions per user**」を最大値に設定します。これにより、各ユーザーの同時 **NSPI** 接続の制限を削除します。制限について詳しくは、**Microsoft** ナレッジベースの次の記事を参照してください。

<https://support.microsoft.com/kb/949469>

## Enterprise Vault サーバーでのユーザープロファイルの作成

**Enterprise Vault** をインストールする前に、次を行う必要があります。

- ボルトサービスアカウントを使って **Enterprise Vault** サーバーにログインし、**Windows** ユーザープロファイルを作成します。

他の任意のサービスアカウントで **Exchange** アーカイブタスクを実行する場合、各サービスアカウントに対してこの処理を完了する必要があります。

## ボルトサービスアカウントのメールボックスの作成

---

**メモ:** このセクションではボルトサービスアカウントの設定について説明します。ボルトサービスアカウント以外のサービスアカウントで **Exchange** アーカイブタスクを実行すると、その情報が他のアカウントに適用されます。

---

**Exchange Server** アーカイブのインストール前のタスク時に、**PowerShell** スクリプトを実行してボルトサービスアカウントの **Exchange** スロットルポリシーを設定する必要があります。

スロットルポリシーのスクリプトを実行するには、まずボルトサービスアカウントでメールボックスを作成する必要があります。

クロスフォレスト環境で **Exchange** を実行する場合は、リソースフォレストにボルトサービスアカウントのリンクメールボックスが必要です。

たとえば、**Exchange** が「**Resources**」というリソースフォレストに存在し、ユーザーアカウントが「**Users**」というユーザーフォレストに存在する場合があります。この場合、ボルトサービスアカウントは「**Users**」フォレストにあり、このフォレストはリンクされたメールボックスを「**Resources**」フォレストに持っているようにする必要があります。

このようなクロスフォレスト環境で、リンクされたメールボックスを所有している無効なユーザーアカウントに対して **PowerShell** スクリプトを実行します。

## ボルトサービスアカウントの Exchange スロットルポリシーの設定

---

**メモ:** 次の手順は、ボルトサービスアカウントの設定について説明します。ボルトサービスアカウント以外のサービスアカウントで **Exchange** アーカイブタスクを実行する場合は、その手順を他のアカウントに対して実行します。

---

**Exchange** には、サーバーに対して開くユーザーアカウントの接続数を 20 以下に制限するデフォルトのスロットルポリシーがあります。ボルトサービスアカウントのこの制限により、このアカウントで実行される **Enterprise Vault** タスクが失敗することがあります。

ボルトサービスアカウントから制限を解除する必要があります。**Enterprise Vault** は **SetEVThrottlingPolicy.ps1** と呼ばれる **PowerShell** スクリプトを備えています。このスクリプトを使って新しいポリシーを作成し、作成したポリシーをボルトサービスアカウントに割り当てて制限を解除します。

このスクリプトの次の必要条件に注意してください。

- Exchange 2010 と Exchange 2013 以降の両方からアーカイブする場合は、Exchange 2013 以降のサーバー上の Exchange 管理シェルのスクリプトを実行する必要があります。
- 使用環境に Exchange 2010 と Exchange 2013 の以降の両方が存在する場合、スクリプトは Exchange 2010 サーバーを自動的に設定してから、以降のサーバーを設定します。スクリプトには、Exchange のバージョンごとに Exchange スロットルポリシーを個別に設定するためのオプションが含まれています。このオプションを使う場合は、Exchange 2010 スロットルポリシーを最初に設定する必要があります。

PowerShell スクリプトを実行しないで、スロットルポリシーを手動で設定する場合は、ベリタスサポート Web サイトの次に記事に方法が記載されています。

Exchange 2010 の場合: <https://www.veritas.com/docs/100006018>

Exchange 2013 以降の場合: <https://www.veritas.com/docs/100012182>

### PowerShell スクリプトを実行して Exchange スロットルポリシーを設定する方法

- 1 次の管理ロールが割り当てられているアカウントを使って Exchange Server にログインします。

- メール受信者
- 受信者ポリシー

デフォルトでは、「組織管理」ロールグループのメンバーにはこれらのロールが割り当てられます。

- 2 SetEVThrottlingPolicy.ps1 スクリプトを Enterprise Vault メディアの Veritas Enterprise Vault¥PowerShell Scripts フォルダから Exchange サーバーにコピーします。

- 3 Exchange Server で、Exchange 管理シェルの開きます。

- 4 2007 またはそれ以前の Exchange から既存のボルトサービスアカウントのメールボックスを移動したら、次のコマンドを使ってメールボックスを更新します。

```
Set-Mailbox mailbox_name -ApplyMandatoryProperties
```

それぞれの内容は次のとおりです。

**mailbox\_name** はボルトサービスアカウントのメールボックスの名前です。

**mailbox\_name** にスペースが含まれる場合は引用符 (") で囲みます。

- 5 SetEVThrottlingPolicy.ps1 を実行します。構文は次のとおりです。

```
.¥SetEVThrottlingPolicy.ps1 -user domain¥user_name [-server  
exchange_mailbox_server] [-version exchange_version]  
[-DomainController domain_controller_name]
```

パラメータについて次に説明します。

<code>-user</code>	<p>ボルトサービスアカウントとそれが属するドメインを指定します。  <code>user_name</code> にスペースが含まれる場合は、  <code>domain¥user_name</code> の文字列全体を引用符 (") で囲みます。</p> <p>クロスフォレスト環境で Exchange を実行する場合は、ボルトサービスアカウントのリンクされたメールボックスを所有する無効なユーザーアカウントに対してスクリプトを実行します。</p> <p>p.66 の「ボルトサービスアカウントのメールボックスの作成」を参照してください。</p>
<code>-server</code>	<p>Exchange メールボックスサーバーの名前を指定します。メールボックスサーバー以外のコンピュータでスクリプトを実行する場合は、Exchange メールボックスサーバーを指定する必要があります。</p>
<code>-version</code>	<p>スロットルポリシーを設定する Exchange Server のバージョンを指定します (2010 または 2013AndLater)。</p>
<code>-DomainController</code>	<p>ボルトサービスアカウントがメンバーとなっているドメインにあるドメインコントローラの名前を指定します。</p> <p>このパラメータはオプションです。ただし、クロスフォレスト環境では、リソースフォレスト内のボルトサービスアカウントのリンクされたメールボックスに対してスクリプトが実行されるように、リソースドメインを指定する必要があります。</p>

- 6 スクリプトが完了すると、Exchange 管理シェルは終了します。
  - 7 これらの変更をすぐに強制的に反映する場合は、サービスが存在する各 Exchange サーバーの Microsoft Exchange RPC クライアントアクセスサービスを再起動します。
- サービスを再起動しなければ、デフォルトでは変更の反映に最大で 2 時間かかります。

## ボルトサービスアカウントへのシステムメールボックスの[送信者]権限の付与

ボルトサービスアカウントには、各 Exchange メールボックスサーバーの Enterprise Vault システムメールボックスの[送信者]権限が必要です。各アカウントにこの権限を手動で設定できます。次の手順を使います。

### ボルトサービスアカウントにシステムメールボックスの[送信者]権限を付与する方法

- 1 「Active Directory 権限」管理ロールが割り当てられているアカウントを使って Exchange Server にログインします。

デフォルトでは、「組織管理」役割グループのメンバーにこの役割が割り当てられます。

- 2 Exchange 管理シェルの開きます。

- 3 次のコマンドを実行します。

```
Add-ADPermission -Identity mailbox_name -User domain¥user_name  
-AccessRights ExtendedRight -ExtendedRights "send as"
```

それぞれの内容は次のとおりです。

- **mailbox\_name** は Enterprise Vault システムメールボックスです。**mailbox\_name** にスペースが含まれる場合は引用符 (") で囲みます。
- **domain** はボルトサービスアカウントが属する Active Directory ドメインです。
- **user\_name** はボルトサービスアカウントです。**user\_name** にスペースが含まれる場合は引用符 (") で囲みます。

## ボルトサービスアカウントへの Exchange Server 権限の割り当て

Enterprise Vault は、ボルトサービスアカウントに必要な権限を割り当てる PowerShell スクリプトを含みます。

ボルトサービスアカウントに **Exchange Server** 権限を割り当てるには

- 1 次の管理ロールが割り当てられているアカウントを使って Exchange Server にログインします。

- Active Directory 権限
- Exchange Server
- Organization Configuration

デフォルトでは、「組織管理」ロールグループのメンバーにはこれらのロールが割り当てられます。

- 2 SetEVExchangePermissions.ps1 というスクリプトを Enterprise Vault メディアの ¥Veritas Enterprise Vault¥PowerShell Scripts フォルダから Exchange サーバーにコピーします。

- 3 Exchange Server で、Exchange 管理シェルの開きます。

#### 4 SetEVEExchangePermissions.ps1 を実行します。

このスクリプトの構文は次のとおりです。

```
.¥SetEVEExchangePermissions.ps1 -User domain¥user_name [-Server  
exchange_server] [-Action <String>] [-Level <String>] [-Verbose  
<Boolean>]
```

パラメータは次のとおりです。

-User (必須)	<b>domain¥user_name</b> は、ボルトサービスアカウントおよびそれが属しているドメインです。 <b>user_name</b> にスペースが含まれる場合は、 <b>domain¥user_name</b> の文字列全体を引用符 (") で囲みます。
-Server	<b>exchange_server</b> は、Exchange Server の名前です。デフォルトは、スクリプトが実行されている Exchange Server です。
-Action	権限を追加するか (Add)、または削除します (Remove)。デフォルト値は Add です。
-Level	メールボックスタスクとプロビジョニングタスクに必要な権限を適用するか (All)、またはプロビジョニングタスクに必要な読み取り専用権限を適用します (Provisioning)。デフォルト値は All です。  Action パラメータが Remove に設定されている場合、このパラメータは無視されます。
-Verbose	すべてのスクリプト出力を表示するか (\$True)、または最小限の情報を表示します (\$False)。デフォルト値は \$False です。

#### 5 これらの変更をすぐに強制的に反映する場合は、各 Exchange メールボックスサーバーの Microsoft Exchange Information Store サービスを再起動します。

## ボルトサービスアカウントに割り当てる Microsoft Exchange 権限

表 7-2 は SetEVEExchangePermissions.ps1 がボルトサービスアカウントに割り当てる権限をリストします。

表 7-2 ボルトサービスアカウントに割り当てられる権限

パス	オブジェクト	権限
CN=Configuration, CN=Services, CN=Microsoft Exchange, CN=Organization, CN=Administrative Groups, CN=AdminGroup	CN=Databases と子孫のオブジェクト。	読み取り インフォメーション ストアの管理 インフォメーション ストアでの名前付きプロパティの作成 受信者 インフォメーション ストアの状態の表示
	CN=Servers と子孫のオブジェクト。  SetEVEExchangePermissions.ps1 は Exchange Server 2007 以前が環境に存在すればこれらの権限を割り当てます。	読み取り インフォメーション ストアの管理 インフォメーション ストアでの名前付きプロパティの作成 受信者 インフォメーション ストアの状態の表示
CN=Configuration, CN=Services, CN=Microsoft Exchange	CN=Organization。	読み取り
CN=Configuration, CN=Services, CN=Microsoft Exchange, CN=Organization	CN=ELC Folders Container と子孫のオブジェクト。	読み取り
	CN=Global Settings と子孫のオブジェクト。	読み取り
	CN=Transport Settings。	読み取り
CN=Configuration, CN=Services, CN=Microsoft Exchange, CN=Organization, CN=Transport Settings	CN=Rules。	読み取り
CN=Configuration, CN=Services, CN=Microsoft Exchange, CN=Organization, CN=Transport Settings, CN=Rules	CN=Journaling と子孫のオブジェクト。	読み取り
	CN=JournalingVersioned と子孫のオブジェクト。	読み取り

# Exchange Server アーカイブでの Enterprise Vault クライアントアクセス

ユーザーは、さまざまなクライアントへのアクセス方法を使ってアーカイブ内のアイテムにアクセスして管理できます。次のような方法があります。

- Enterprise Vault Outlook アドイン
- Mac OS X 用 Enterprise Vault クライアント
- Enterprise Vault Office Mail App (OWA 2013 以降と Outlook 2013 以降用)
- OWA クライアント (OWA 2010 用)
- Enterprise Vault のカスタマイズされたショートカット

## Enterprise Vault Outlook アドインの要件

Enterprise Vault Outlook アドインにより、ユーザーは次のアクティビティを含む Outlook のさまざまなアクティビティを実行できます。

- Enterprise Vault アーカイブに手動でアイテムを保存する。
- アーカイブ済みアイテムの表示、コピー、および削除。
- アーカイブに格納されているアイテムの検索。

Outlook クライアント内からアーカイブにアイテムを送信する前に、Outlook アドインをコンピュータにインストールしておく必要があります。Enterprise Vault サーバーの設定後に、Outlook アドインをユーザーのコンピュータにインストールしてください。

ユーザーのコンピュータには次のものがあります。

- Windows の次のいずれかのバージョン。
  - Windows 7
  - Windows 8
  - Windows 10
- Internet Explorer 9 以降 (Java スクリプトを有効にする)  
使わない場合でも必ずインストールしてください。
- TCP/IP プロトコル。
- Outlook 2010 以降のメールクライアント。  
電子メールクライアントをインストールする前に、Internet Explorer をインストールしてください。



- Microsoft Visual C++ 2013 (x86) と (x64) の再頒布可能パッケージ。コンピュータにこれらのパッケージが存在しない場合は、Enterprise Vault Outlook アドインインストーラが自動的にインストールします。
- ボルトキャッシュを有効にする場合は、ユーザーのコンピュータに Background Intelligent Transfer Service (BITS) 2.0 以降をインストールして有効にする必要があります。このサービスは Microsoft Windows の更新で使用され、Windows のすべての新しいバージョンに含まれています。必要に応じて、Microsoft の Web サイトからダウンロードできます。
- ボルトキャッシュを有効にする予定で、レジストリエントリ PstDisableGrow を設定してユーザーのコンピュータで PST ファイルの拡張を無効にしている場合は、Microsoft から適切な Outlook の Hotfix を入手してインストールする必要があります。Hotfix が Microsoft Update の一部としてすでにインストールされている場合があることに注意してください。  
『Exchange Server アーカイブの設定』ガイドの説明に従って、ユーザーのコンピュータで、PSTDisableGrowAllowAuthenticcodeOverrides レジストリも設定する必要があります。
- Windows Search プラグインを有効にする場合は、デスクトップコンピュータで Windows Search 4.x 以降が利用可能である必要があります。

## Mac OS X 用 Enterprise Vault クライアントの必要条件

Mac OS X 用の Enterprise Vault クライアントは、Enterprise Vault の機能を Microsoft Outlook for Mac 2011 または 2016 のユーザーに提供します。ユーザーはアイテムをアーカイブ、復元、削除したり、アーカイブ内のアイテムの検索を実行したりすることができます。

Mac OS X 用 Enterprise Vault クライアントは、次の必要条件を満たすコンピュータにインストールできます。

- Mac OS X バージョン 10.9 (Mavericks) 以降
- Outlook for Mac の次のいずれかのバージョン:
  - Outlook for Mac 2011 バージョン 14.0.0 以降
  - Outlook for Mac 2016 バージョン 15.8.1 以降
- Safari バージョン 7.0 以降

サポートされている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。

Mac OS X 用の Enterprise Vault クライアントは、次の認証タイプと、これらの組み合わせをサポートします。

- 基本認証

- ダイジェスト認証
- Windows 認証
- 基本認証 + ASP.NET 偽装
- 基本認証 + ダイジェスト認証
- 基本認証 + Windows 認証

---

メモ: それぞれの場合で、匿名認証も有効になっている必要があります。

---

## Enterprise Vault Office Mail App の必要条件

Enterprise Vault Office Mail App は、OWA 2013 以降のユーザーに Enterprise Vault 機能を提供します。また、Outlook アドインの代替として、または Outlook アドインに加えて、Office Mail App を Outlook 2013 以降のユーザーに対して有効にできます。

Office Mail App の必要条件は次のとおりです。

- Internet Explorer 9 以降がユーザーのコンピュータにインストールされている必要があります。サポート対象ブラウザの最新情報については、Enterprise Vault [Compatibility Charts](#) を参照してください。
- Exchange Server 2013 搭載のタブレットや電話で Office Mail App が正しく働くようにするには、Exchange Server 2013 の累積更新プログラム 3 をインストールする必要があります (<https://support.microsoft.com/kb/2892464> を参照)。累積更新プログラム 3 をインストールしないと、Office Mail App でアーカイブ済みアイテムの復元や削除ができません。

Office Mail App の設定および必要な追加設定について、詳しくは『Exchange Server アーカイブの設定』を参照してください。

## OWA の必要条件

Enterprise Vault サーバーで Exchange Server アーカイブを設定した後に Enterprise Vault への OWA アクセスを設定できます。Enterprise Vault への OWA アクセスの設定手順では、Exchange Server で OWA が設定済みであることを前提としています。

OWA 2010 クライアントから Enterprise Vault へのアクセスを可能にするには、Exchange Server 2010 CAS コンピュータに Enterprise Vault OWA 2010 Extensions が必要です。

p.75 の「[Enterprise Vault OWA Extensions の必要条件](#)」を参照してください。

以降の OWA クライアントには Enterprise Vault OWA Extensions は不要です。OWA 2013 以降のクライアントでは、Enterprise Vault Office Mail App が代わりに Enterprise Vault 機能を提供します。

p.74 の「[Enterprise Vault Office Mail App の必要条件](#)」を参照してください。

## Enterprise Vault OWA Extensions の必要条件

Enterprise Vault OWA Extensions をインストールするすべての Exchange Server は Exchange Server サービスパックと Hotfix レベルを同じにしてください。

Enterprise Vault OWA Extensions を Exchange Server にインストールする場合は、必ず、すべての Exchange Server に同じ Enterprise Vault リリースバージョンの Extensions をインストールしてください。

OWA クライアントから、Enterprise Vault にアクセスするには次の条件が必要です。

- Enterprise Vault OWA 2010 Extensions には Exchange Server 2010 SP1 以降が必要です。Exchange CAS コンピュータに Enterprise Vault OWA 2010 Extensions をインストールします。
- Web サーバー (IIS) に次のロールサービスがインストールされている必要があります。
  - IIS 管理スクリプトおよびツール
  - IP およびドメインの制限  
[機能の委任]のオプション[アドレスおよびドメインの制限]を[読み取り/書き込み]に設定する必要もあります。このオプションを見つけるには、インターネットインフォメーションサービス (IIS) マネージャを開いて、ナビゲーションペインのサーバーオブジェクトをクリックします。[機能の委任]を開き、オプションの一覧に[アドレスおよびドメインの制限]が表示されていることを確認します。
- Exchange Servers には MSXML が必要です。MSXML は、Internet Explorer 7.0 以降とともに自動的にインストールされます。

## カスタマイズされたショートカット

デスクトップコンピュータに Enterprise Vault クライアントをインストールしない場合は、[Exchange メールボックスポリシー]で Enterprise Vault のカスタマイズされたショートカットを設定できます。これらのショートカットにより、ユーザーはアーカイブ済みアイテムの HTML バージョンを表示できます。さらに、ユーザーはブラウザウィンドウに Enterprise Vault の参照と検索の機能を開いてアーカイブ済みアイテムにアクセスして管理できます。

Windows コンピュータでは、Internet Explorer 9 以降を各ユーザーのコンピュータにインストールして Java スクリプトを有効にする必要があります。

Mac コンピュータでは、Safari ブラウザと Outlook for Mac 電子メールクライアントがサポートされています。サポート対象バージョンについて詳しくは、Enterprise Vault [Compatibility Charts](#) を参照してください。

## アーカイブへのブラウザベースのアクセス

ユーザーは、デスクトップコンピュータに Enterprise Vault Outlook アドインをインストールせずにアーカイブの内容にアクセスできます。Web ブラウザで Enterprise Vault 検索機能を開いてアーカイブにアクセスすることもできます。

Web 接続で HTTPS を使用するために Enterprise Vault を設定する場合、Enterprise Vault 検索 URL は次の形式になります。

`https://web_server_name/EnterpriseVault/search/`

## RPC over HTTP の必要条件

このセクションでは、Outlook Anywhere ユーザーの RPC over HTTP アクセスをサポートするための必要条件を示します。

## Enterprise Vault への Outlook Anywhere アクセスの要件

Exchange Server 2010 の環境では、RPC over HTTP モードの Outlook を Outlook Anywhere と呼びます。Outlook Anywhere クライアントから Enterprise Vault の要求をサポートするには、Enterprise Vault Extensions は Exchange CAS コンピュータに必要ではありません。ただし、Enterprise Vault サーバーに RPC over HTTP アクセスを設定する必要があります。

ユーザーのコンピュータ上の Outlook は、RPC over HTTP を使うように設定するする必要があります。ユーザーのコンピュータには、Enterprise Vault Outlook アドインをインストールする必要があります。手順については、『Exchange サーバーアーカイブの設定』ガイドを参照してください。

# Domino サーバーアーカイブの追加必要条件

この章では以下の項目について説明しています。

- すべての [Enterprise Vault サーバーの Domino サーバーアーカイブの必要条件](#)
- [Domino メールボックスアーカイブの要件](#)
- [Domino ジャーナルアーカイブの必要条件](#)

## すべての Enterprise Vault サーバーの Domino サーバーアーカイブの必要条件

すべての Domino アーカイブにおいて、すべての Enterprise Vault サーバーに Notes クライアントをインストールする必要があります。

---

**メモ:** Enterprise Vault Domino Gateway には、Enterprise Vault サーバーとは異なる必要条件があります。

p.78 の「[Enterprise Vault Domino Gateway の必須ソフトウェア](#)」を参照してください。

---

次の手順に従って、すべての Enterprise Vault サーバーに Notes クライアントをインストールします。

- Notes 8.5.3 以降のクライアントソフトウェアをインストールします。最新のサポート対象ソフトウェアバージョンについて詳しくは、Enterprise Vault [Compatibility Charts](#) を参照してください。
- 「マルチユーザーインストール」オプションを使って Notes クライアントをインストールした場合は、Enterprise Vault サービスが使う Windows アカウントとしてログオンします。これは通常、ボルトサービスアカウントです。

- Notes クライアントを起動し、設定ウィザードを完了してください。Domino のアーカイブに使う ID ファイルを使用してください。  
p.85 の「[Domino メールボックスアーカイブ用のユーザー ID 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の要件

Domino メールボックスアーカイブの場合、次の項目を設定する必要があります。

- 1 つ以上の Enterprise Vault Domino Gateway。  
Enterprise Vault Domino Gateway は、Enterprise Vault 設定によってカスタマイズされる Domino サーバーです。Enterprise Vault Domino Gateway は、Notes クライアントと Enterprise Vault 間のインターフェースを提供します。アーカイブデータに対するすべての主要な処理 (オープン、復元、削除、検索) は Enterprise Vault Domino Gateway によって行われます。
- 1 つ以上の Enterprise Vault サーバー。必要に応じて、Enterprise Vault Domino Gateway を使って Enterprise Vault のサービスとタスクを実行できます。
- 対象の Domino メールサーバー。
- Notes と Domino Web Access の Enterprise Vault クライアント拡張機能。

リモートコンピュータに Enterprise Vault 管理コンソールをインストールする場合は、Domino ユーザーアーカイブを管理するためにそのコンピュータに Notes 8.5.3 以降もインストールする必要があります。

最新のサポート対象ソフトウェアバージョンについて詳しくは、Enterprise Vault [Compatibility Charts](#) を参照してください。

## Enterprise Vault Domino Gateway の必須ソフトウェア

Enterprise Vault Domino Gateway は、Enterprise Vault 12.3 と次のいずれかを実行している Windows サーバーである必要があります。

- Domino サーバー (64 ビットバージョン) と Notes Client の両方のバージョン 8.5.3 以降のサービスパック
- Domino サーバー (64 ビットバージョン) と Notes Client の両方のバージョン 9.0.0 以降のサービスパック

標準の Domino メールテンプレートを Enterprise Vault Domino Gateway 上に配置することをお勧めします。これらのテンプレートは Enterprise Vault `EVinstall.nsf` インストーラで必要になります。

すべてのサポート対象ソフトウェアのバージョンと必要なホットフィックスについて詳しくは、Enterprise Vault [Compatibility Charts](#) を参照してください。

各 Enterprise Vault Domino Gateway には少なくとも 1 つの Domino メッセージサーバーのライセンスが必要です。

## 対象の Domino メールサーバーの必須ソフトウェア

アーカイブ対象の Domino メールサーバーでは、Domino Server 8.0.0 以降を実行している必要があります。

最新のサポート対象ソフトウェアバージョンについて詳しくは、Enterprise Vault [Compatibility Charts](#) を参照してください。

## Notes クライアントの Enterprise Vault 拡張機能の要件

Notes または Domino Web Access (DWA) クライアントからアーカイブ済みアイテムへのクライアントアクセスは、Notes と DWA メールテンプレートへの変更を介して提供されます。ユーザーのワークステーションにアプリケーションをインストールする必要はありません。更新されたメールテンプレートを、組織全体の対象 Domino メールサーバーと DWA サーバーにインストールします。

Notes クライアントで Enterprise Vault の機能を利用可能にするには、そのワークステーションに Notes Client 8.0.0 以降をインストールしている必要があります。

最新のサポート対象ソフトウェアバージョンについて詳しくは、Enterprise Vault [Compatibility Charts](#) を参照してください。

Notes または DWA のメールクライアント内で Enterprise Vault による検索の使用を有効にするには、そのワークステーションに Internet Explorer 9 以降をインストールして Notes のデフォルトの Web ブラウザに設定する必要があります。ユーザーのシングルサインオンを Enterprise Vault Domino Gateway で設定する必要もあります。

p.82 の「[Enterprise Vault Domino Gateway でのシングルサインオンの設定](#)」を参照してください。

## Domino メールボックスアーカイブのインストール前の作業

すでに、次のものが作成済みです。

- ボルトサービスアカウント
- ボルトサービスアカウントの SQL ログインアカウント
- Enterprise Vault サーバーとサイトの DNS エイリアス

p.45 の「[Enterprise Vault サーバーのインストール前の作業](#)」を参照してください。

次の作業を実行して、Enterprise Vault Domino Gateway コンピュータに Domino サーバーと Notes をセットアップする必要があります。次の手順は、コンピュータに Enterprise Vault をインストールする前に完了しておく必要があります。これにより、Enterprise Vault のインストールプログラムでは、インストール対象が Domino サーバーであり、エクステン

ションマネージャファイルとその他のデータベースファイルをインストールしようとしていることが検出されます。

- IBM Domino Administrator クライアントを使って、次の処理を行います。
  - Enterprise Vault Domino Gateway コンピュータで実行する Domino サーバーを登録し、Domino Directory にこのサーバーを設定します。  
p.80 の「Enterprise Vault Domino Gateway の登録」を参照してください。
  - Domino メールボックスアーカイブのユーザー ID を指定または作成します。  
p.85 の「Domino メールボックスアーカイブ用のユーザー ID について」を参照してください。
  - Enterprise Vault がアーカイブする Domino メールサーバーのサーバー文書を設定します。  
p.87 の「対象の各 Domino メールサーバーに対するサーバー文書の設定」を参照してください。
- Enterprise Vault Domino Gateway をホストするコンピュータで、次の手順を実行します。
  - Domino サーバーバイナリをインストールして Domino サーバーを設定します。  
p.88 の「Enterprise Vault Domino Gateway のインストールと設定」を参照してください。
  - Notes クライアントバイナリと Hotfix をインストールしてクライアントを設定します。  
Domino のアーカイブに使う ID ファイルを使用してください。  
p.77 の「すべての Enterprise Vault サーバーの Domino サーバーアーカイブの必要条件」を参照してください。

これらの作業が完了したら、Enterprise Vault をインストールして初期設定を行うことができます。

p.122 の「Enterprise Vault のインストール(ウィザード)」を参照してください。

その後、Domino メールボックスアーカイブの設定を完了できます。手順については、『Domino サーバーアーカイブの設定』ガイドを参照してください。

## Enterprise Vault Domino Gateway の登録

アーカイブ対象の Domino ドメインごとに、少なくとも 1 つの Enterprise Vault Domino Gateway が必要です。実働環境では、Enterprise Vault Domino Gateway を一般的なメールサーバーとして使うことはできません。

Enterprise Vault Domino Gateway は、Domino パーティションサーバーとして使うことができます。

このセクションの説明に従い、IBM Domino Administrator クライアントを使って Enterprise Vault Domino Gateway を登録し、サーバー文書を設定します。Domino ドメイン内で



複数の Enterprise Vault Domino Gateway コンピュータを使う場合は、各 Enterprise Vault Domino Gateway に対して次のタスクを実行します。

- Enterprise Vault Domino Gateway で HTTP 用のインターネットポートを設定します。
- サーバーセキュリティを設定します。
- Enterprise Vault Domino Gateway でシングルサインオンを設定します。
- オプションで、Enterprise Vault Domino Gateway サーバーを Domino サーバークラスタに追加します。
- オプションで、Enterprise Vault Domino Gateway サーバーとの Web 接続のエイリアス URL を設定します。

## Enterprise Vault Domino Gateway でのインターネットポートの設定

Enterprise Vault では、Enterprise Vault Domino Gateway で HTTP タスクを設定する必要があります。IIS と Domino サーバーの HTTP タスクはどちらもポート 80 を使うため、Domino サーバーが使うポートを変更する必要があります。

### Enterprise Vault Domino Gateway でインターネットポートを設定する方法

- 1 IBM Domino Administrator クライアントで、Enterprise Vault Domino Gateway のサーバー文書を開きます。
- 2 [ポート]タブを選択し、サブ文書の[インターネットポート]タブを選択します。
- 3 [Web]タブで、TCP/IP 番号を 80 以外の数字 (8080 など) に設定します。

## Enterprise Vault Domino Gateway のサーバーのセキュリティ設定

IBM Domino Administrator クライアントを使って、サーバー文書を設定します。Domino ドメイン内で複数の Enterprise Vault Domino Gateway コンピュータを使う場合は、各 Enterprise Vault Domino Gateway に対して次の手順を実行します。

### Enterprise Vault Domino Gateway のサーバーのセキュリティを設定する方法

- 1 サーバー文書の[セキュリティ]ページを開きます。
- 2 [可能なプログラムの制限]セクションでは、[エージェントまたは XPages を呼び出すユーザーとして実行するエージェントを署名]フィールドでメールテンプレートに表示される署名するユーザーを確認してください。
- 3 下方向にスクロールして[サーバーアクセス]を表示します。
- 4 Enterprise Vault Domino Gateway メールテンプレートを作成するユーザーを[マスターテンプレートの作成]に追加します。

- 5 対象の Domino メールサーバーを[信頼できるサーバー]に追加します。
- 6 [保存して閉じる]をクリックします。
- 7 Enterprise Vault Domino Gateway ごとに手順 1 から手順 6 を繰り返します。

## Enterprise Vault Domino Gateway でのシングルサインオンの設定

アーカイブ検索機能の認証を有効にするには、Enterprise Vault Domino Gateway でシングルサインオンを設定する必要があります。

次の手順では、インターネットサイトの文書を使っていないことを想定しています。インターネットサイトの文書を使っている場合は、Domino の文書に記載されている手順を実行します。

Web 設定を使ったシングルサインオンの設定方法について詳しくは次の IBM の記事を参照してください。

<https://publib.boulder.ibm.com/infocenter/iseres/v5r4/topic/rzatz/51/sec/secssdom.htm>

### Enterprise Vault Domino Gateway でシングルサインオンを設定する方法

- 1 Domino Administrator クライアントで、[設定]タブに移動し、[サーバー] > [すべてのサーバー文書]ビューの順に選択します。Enterprise Vault Domino Gateway のサーバー文書を選択します (開かないでください)。
- 2 [Web]をクリックし、ドロップダウンボックスで[Web SSO 設定の作成]を選択します。
  - [設定名]フィールドで、デフォルト名を EVLtpaToken に変更します。
  - [DNS ドメイン]フィールドに、対象の Domino サーバーの DNS ドメインを入力します。
  - [Domino サーバー名]フィールドに、すべての Enterprise Vault Domino Gateway を追加します。DWA ユーザーに対してもシングルサインオンを設定する場合は、対象の Domino メールサーバーも追加する必要があります。
  - [キー]をクリックし、ドロップダウンメニューで[Domino SSO キーの作成]を選択します。[OK]をクリックします。
  - Web SSO 設定を保存して閉じます。
- 3 Enterprise Vault Domino Gateway のサーバー文書が選択されている場合は、[サーバーの編集]をクリックします。
  - [インターネットプロトコル]タブをクリックし、[Domino Web Engine]サブタブをクリックします。
  - [セッション認証]フィールドを[複数サーバー (SSO)]に変更し、[OK]をクリックします。

- [Web SSO 設定]フィールドで[EVLtpaToken]を選択します。
- サーバー文書を保存して閉じます。

## Enterprise Vault Domino Gateway サーバーのクラスタ化

Domino Server アーカイブ環境では、Veritas Cluster Server (VCS) または Windows Server フェールオーバークラスタリングなどを使って Enterprise Vault サービスをクラスタ化できます。IBM Domino サーバークラスタを使って Enterprise Vault Domino Gateway サーバーをクラスタ化します。

IBM Domino Administrator クライアントを使ってすべての Enterprise Vault Domino Gateway サーバーを同じ Domino クラスタに追加します。

## Enterprise Vault Domino Gateway サーバーとの Web 接続のエイリアス URL の設定

デフォルトでは、Enterprise Vault Domino Gateway サーバーの完全修飾インターネットホスト名が iNotes でのメールファイル拡張操作、および iNotes クライアントと iNotes での Enterprise Vault Search 操作のベース URL として使われます。完全修飾インターネットホスト名は [図 8-1](#) に示されるように、サーバー文書の[基本]サブドキュメントに設定されます。

図 8-1 ベース URL のデフォルト値

The screenshot shows the Domino Administrator client window titled 'DOMINO Domain - JPdomino/domino'. The 'サーバー: JPdomino/domino' tab is active. The '基本' (Basic) subdocument is selected in the left pane. The main pane displays the configuration for the server. The '完全なインターネットホスト名' (Fully Qualified Internet Host Name) field is highlighted with a green box and contains the value 'JPdomino.ev.com'. Other fields include 'サーバー名' (JPdomino/domino), 'サーバータイトル' (JPdomino), 'ドメイン名' (domino), 'クラスタ名' (empty), and '最大式実行時間' (120 秒).

基本	
サーバー名:	『JPdomino/domino』
サーバータイトル:	『JPdomino』
ドメイン名:	『domino』
完全なインターネットホスト名:	『JPdomino.ev.com』
クラスタ名:	
「サーバー - インターネットサイト」の文書からインターネット設定を読み込む:	『無効』
最大式実行時間:	『120』秒

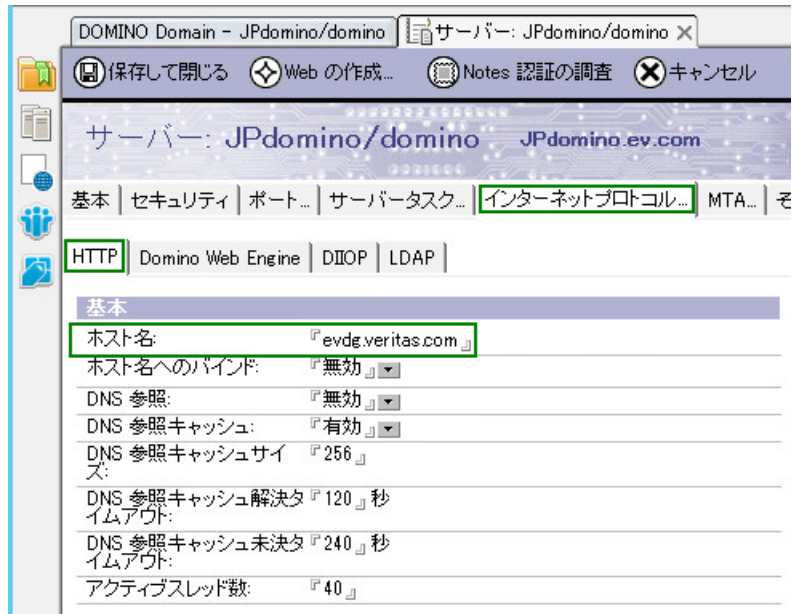
オプションで、完全修飾ホスト名ではなく、ベース URL として使うエイリアス値を設定できます。このセクションの手順で、エイリアス値の設定方法を説明します。

## Enterprise Vault Domino Gateway サーバーとの Web 接続のエイリアス URL の設定

- 1 DNS で、利用可能な状態にする Enterprise Vault Domino Gateway サーバーそれぞれに対してエイリアスを作成します。DNS のこのエイリアスアドレスはベース URL のエイリアス値を設定するのに使われます。
- 2 IBM Domino Administrator クライアントで、Enterprise Vault Domino Gateway サーバーの 1 つのサーバー文書を開きます。
- 3 [インターネットプロトコル]タブを選択します。
- 4 [HTTP]サブドキュメントの[ホスト名]フィールドで、このサーバーに対して以前作成した DNS エイリアスを入力します。図 8-2 はこのフィールドの値の例を示します。  
  
[ホスト名]フィールドに値がある場合、クライアントはその値をこの Enterprise Vault Domino Gateway サーバーとの Web 接続のベース URL として使います。このフィールドが空白の場合、クライアントは完全修飾インターネットホスト名をベース URL として使います。
- 5 Enterprise Vault Domino Gateway サーバーを再起動します。
- 6 Enterprise Vault Domino Gateway サーバーごとに手順 2 から手順 5 を繰り返します。

クラスターでは、Enterprise Vault Domino Gateway サーバーごとに各手順を繰り返します。

図 8-2 ベース URL のエイリアス値



## Domino メールボックスアーカイブ用のユーザー ID について

Domino のプロビジョニングタスクとメールボックスアーカイブタスクでは、次の処理を行うために、ユーザーのメールデータベースへのアクセスが必要です。

- 非表示ビューの追加
- 非表示の Enterprise Vault プロファイル文書の追加または更新
- メールアイテムのショートカットへの変更

Domino セキュリティモデルに準拠するには、認証されたユーザーが Notes ID ファイルを使って Domino メールデータベースにアクセスする必要があります。対象の Domino メールサーバーのサーバー文書を設定する場合、この ID には、少なくともアーカイブ対象のメールファイルに対する編集者のアクセス権、文書の削除権限、共有フォルダビューの作成権限を付与します。

p.86 の「すべての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限の付与」を参照してください。

この ID は、後で Domino メールボックスアーカイブを設定するときに、Enterprise Vault 管理コンソールで指定します。ID の (パスワードを含む) 詳細は暗号化され、Enterprise Vault ディレクトリデータベースに格納されます。

アクセス権が適切なレベルであれば、どのユーザー ID ファイルも使えますが、汎用ユーザーアカウントを作成し、必要なアクセス権限をユーザーに付与することを推奨します。

## Domino アーカイブユーザーの作成

汎用ユーザーアカウントを作成するには、Domino Administrator クライアントのユーザー登録ツールを使います。ユーザー文書には Domino ドメイン名が含まれる必要があるため、ユーザーは Notes メールユーザーである必要があります。ユーザーには、わかりやすい総称 (Enterprise Vault Domino Archiving など) を付けることを推奨します。

ユーザーがアドレス一覧の最後にだけ表示されるように、特殊文字「&」を付けて姓に接頭辞を付けることができます。たとえば、Enterprise Vault Domino &Archiving/organization のようにします。

---

**メモ:** ユーザーの ID ファイルをコピーして、Domino アーカイブタスクを実行するすべての Enterprise Vault サーバーの Notes データフォルダに保存します。Enterprise Vault Domino Gateway の Notes データフォルダ (たとえば C:\Program Files\IBM\Notes\data) にも ID ファイルをコピーする必要があります。

---

## すべての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限の付与

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]アクセス権限が最低限必要です。

---

**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、アイテムが未読であるかどうかを判別するために、Domino で管理者のアクセス権限を必要とするためです。

---

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。

すべてのメールファイルに対して Domino アーカイブユーザーのアクセス権限を付与する方法

- 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で、[ユーザーの種類]の設定を[読者]、[投稿者]の設定を[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のアクセス権限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[フルアクセスアドミニストレーション]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。

## 対象の各 Domino メールサーバーに対するサーバー文書の設定

対象の各 **Domino** メールサーバーに対してサーバー文書を設定する場合は、次の操作を実行する必要があります。

- 対象の各 **Domino** メールサーバーのサーバー文書に、**Enterprise Vault Domino Gateway** を信頼済みサーバーとして追加する必要があります。
- また、**Enterprise Vault** クライアントテンプレートへの署名に使う署名 ID に、次の権限が付与されている必要があります。
  - 呼び出したユーザーとして実行するエージェントまたは **XPage** を署名
  - マスターテンプレートの作成
- **Domino** アーカイブユーザーに、対象のユーザーメールファイルへのアクセス権が付与されている必要があります。
- 任意で、**DWA** ユーザーに対してシングルサインオンを有効にできます。  
 シングルサインオンの主な必要条件は、ユーザーが **Enterprise Vault** の検索機能を使えることです。ただし、シングルサインオンが設定されていない場合、**DWA** ユーザーは、アーカイブ済みアイテムを開くときに詳細な認証情報を再入力する必要があります。

ります。これを避けるために、ユーザーに Enterprise Vault の検索機能へのアクセス権を付与する予定がない場合にも、DWA サーバーにシングルサインオンを設定できます。

p.82 の「Enterprise Vault Domino Gateway でのシングルサインオンの設定」を参照してください。

#### 対象の各 Domino メールサーバーに対してサーバー文書を設定する方法

- 1 サーバー文書の[セキュリティ]ページを開きます。
- 2 [可能なプログラムの制限]セクションでは、メールテンプレートに署名するユーザーが次のフィールドに表示されていることを確認します。
  - 呼び出したユーザーとして実行するエージェントまたは XPage を署名
- 3 下方向にスクロールして[サーバーアクセス]を表示し、ドメイン内のすべての Enterprise Vault Domino Gateway を信頼済みサーバーとして追加します。
- 4 Enterprise Vault メールテンプレートを作成するユーザーを[マスターテンプレートの作成]に追加します。
- 5 [保存して閉じる]をクリックします。
- 6 対象の Enterprise Vault Domino メールサーバーごとに前述の手順を繰り返します。

## Enterprise Vault Domino Gateway のインストールと設定

各 Enterprise Vault Domino Gateway コンピュータに Domino サーバーバイナリをインストールします。インストール時には、[Messaging Server]オプションを選択する必要があります。

適切な Domino Hotfix を Enterprise Vault Domino Gateway にインストールする必要があります。

p.78 の「Enterprise Vault Domino Gateway の必須ソフトウェア」を参照してください。

ボルトサービスアカウントを Enterprise Vault Domino Gateway のローカル管理者にする必要があります。

Enterprise Vault Domino Gateway の Domino サーバーは、ボルトサービスアカウントで実行する必要があります。Domino サーバーをサービスとして実行することを推奨します。ただし、システムアカウント以外のアカウントでサービスを実行した場合はサーバーコンソールが表示されないことに注意してください。これは Microsoft Windows の制限です。コンソールを表示するには、リモートから接続できます。

Domino メールボックスアーカイブの設定時にサーバーコンソールをローカルで表示するには、次のように、Domino サーバーをアプリケーションとして実行することができます。

- ボルトサービスアカウントを使って Enterprise Vault Domino Gateway コンピュータにログオンします。



- **Domino Server** サービスが実行中の場合は、**Windows** サービスコンソールでこれを停止します。
- **Domino Server** サービスを無効にします。
- **Domino Server** を起動し(デスクトップアイコンをダブルクリックするか、*Domino program directory*\nserver.exe を実行します)、サーバーを通常のアプリケーションとして起動するオプションを選択します。**Domino** サーバーの設定が開始されます。

**Domino** サーバーの設定では、次の操作を行います。

- **Enterprise Vault Domino Gateway** に **Domino** サーバーを登録したときに作成した **Domino** サーバー ID を入力します。
- **[Internet Services]** ページで **[Web ブラウザ (HTTP Services)]** オプションを選択し、**HTTP** サーバータスクを追加します。
- 最適なパフォーマンスを得るため、**[カスタマイズ]** ボタンを使って、最小限必要なサーバータスク以外のタスクをすべて削除します。**Enterprise Vault Domino Gateway** に最小限必要な **Domino** サーバーのサービスは、次のとおりです。
  - **Indexer (Update)**
  - **Administration process (AdminP)**
  - **Domino web server (HTTP)**

---

**メモ:** 実環境では、**Enterprise Vault Domino Gateway** の **Domino** サーバーは、ボルトサービスアカウントで動作するサービスとして起動します。

---

**Enterprise Vault** でユーザーメールファイルのアーカイブを設定し、その後アーカイブポリシーの変更時にユーザーメールファイルを更新できるように、**Domino** ディレクトリは **Enterprise Vault Domino Gateway** に頻繁にレプリケートされます。

DWA ユーザーが、アーカイブされた署名済み MIME アイテムまたは暗号化済み MIME アイテムを開くことができるようにするには、**Enterprise Vault Domino Gateway** への **SSL** 接続が必要です。**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を設定するとき、**Enterprise Vault** は、**Enterprise Vault Web** アプリケーションの接続用にポート **443** に **HTTPS** を自動的に設定します。**SSL** がデフォルト **Web** サイトで設定されていない場合、**Enterprise Vault** は自己署名証明書を作成してインストールし、**HTTPS** バインドにこの証明書を使用します。

p.38 の「**IIS (Internet Information Services)**」を参照してください。

**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、**IIS** の **Enterprise Vault** 仮想ディレクトリの既存の設定は変更されません。**SSL** がデフォルト **Web** サイトで設定されていない場合、手動で設定する必要があります。

p.144 の「[Enterprise Vault Web Access](#) コンポーネント用のポートまたはプロトコルのカスタマイズ」を参照してください。

## Domino ジャーナルアーカイブの必要条件

このセクションでは、Domino ジャーナルアーカイブの最小必要条件について説明します。最新のサポート対象ソフトウェアバージョンについては、[Enterprise Vault Compatibility Charts](#) を参照してください。

### Domino ジャーナルデータベースからの Enterprise Vault アーカイブの必要条件

Enterprise Vault は、対象 Domino サーバーのデータディレクトリにある任意のサブフォルダからアーカイブを行います。各サブフォルダはアーカイブ前に構成しておく必要がありますが、フォルダ構造の下位レベルではなく、データディレクトリ直下のサブフォルダである必要があります。直下のサブフォルダでない場合は、Domino ジャーナルタスクはアーカイブするデータベースの検索に失敗します。

Enterprise Vault は、デフォルトで、サブフォルダにあるすべての Domino ジャーナルデータベースからアーカイブを行い、STDMailJournaling テンプレートを使います。レジストリ値を使うと、他のテンプレートをかうように指定できます。手順については、『Domino サーバーアーカイブの設定』ガイドを参照してください。

Enterprise Vault の通常の設定では、アーカイブ済みアイテムが格納されているボルトストアをバックアップするまで、もとのアイテムを保持します。バックアップを完了すると、Enterprise Vault はもとのアイテムを削除します。Domino データベース管理機能は、この Enterprise Vault の処理に影響を与えないようにする必要があります。これは、何らかの理由でアイテムがアーカイブされなかった場合に、そのアイテムが失われる可能性があるため、バージおよび圧縮機能を使えないためです（バージおよび圧縮機能については、サーバー設定文書のジャーナリングに関するセクションを参照）。

このため、サーバー設定についてのマニュアルのジャーナリングに関するセクションで説明されているように、Domino ジャーナルデータベースは、次のデータベース管理機能のいずれか 1 つに設定される必要があります。

- [定期的なロールオーバー]または[サイズロールオーバー]。ロールオーバーデータベースがアーカイブされるためには、初期データベースと同じディレクトリにある必要があります。
- なし。この方法を選択した場合、データベースは大きくなり続けます。そのため、ジャーナルディレクトリを毎晩圧縮することを推奨します。

ジャーナルデータベースがサーバーのデータディレクトリのサブフォルダ内に配置されるように、Domino ジャーナルを設定します。Domino ジャーナルが設定済みの場合、ジャーナルデータベースを移動し、サーバー設定文書を更新することが必要になる場合があります。

## クラスタ化された Domino ジャーナルデータベースからの Enterprise Vault アーカイブのサポート

Enterprise Vault は、Domino アプリケーションクラスタを使ってクラスタ化された Domino サーバー上の Domino ジャーナルデータベースからアーカイブを行うことができます。

クラスタ化されたジャーナルデータベースをサポートするには、次の必要条件を満たす必要があります。

- クラスタ内の各 Domino サーバーがローカルデータベースへのジャーナルを独立して行う必要があります。
- メールジャーナルデータベースがクラスタ内の他の Domino サーバーにレプリケートされないように設定されている必要があります。これは、クラスタレプリケーションとスケジュールされたレプリケーションの両方ともです。
- Enterprise Vault がクラスタ内の各サーバー上の Domino ジャーナルデータベースからアーカイブするように設定されている必要があります。

## Domino のドメイン、サーバーおよびジャーナルの場所への Enterprise Vault のアクセスの設定

アーカイブする Domino ジャーナルの場所を Enterprise Vault に設定する場合、少なくとも 1 つの Notes ID ファイルを指定する必要があります。Enterprise Vault は、ドメイン、サーバー、ジャーナルという 3 つのレベルの場所にアクセスする必要があります。それぞれのレベルに対して異なる ID ファイルを使ったり、簡潔にするために単一の ID ファイルを使ったりできます。

次のアクセスレベルがあります。

- Domino ドメインへのアクセス。このレベルへのアクセスは、Notes メールが有効に設定され、そのアカウントがサーバーと同じドメイン内にあるユーザーの ID ファイルによって指定されます。このアカウントは、Domino Directory に対する読み取りアクセスの権限を持っている必要があります。
- Domino サーバーへのアクセス。このレベルへのアクセスは、Domino サーバーとそのディレクトリに対するアクセス権限を持つユーザーの ID ファイルによって指定されます。  
デフォルトでは、Enterprise Vault はドメインにアクセスする場合と同じ ID ファイルを使います。
- Domino ジャーナルの場所へのアクセス。このレベルへのアクセスは、ジャーナルデータベースに対して、[編集者]、[設計者]、[管理者]のアクセス権限を持つユーザーの ID ファイルによって指定され、[文書の削除]権限も持っています。データベースが暗号化されている場合、この ID ファイルはデータベースの暗号化に使ったファイルである必要があります。

デフォルトでは、Enterprise Vault はサーバーにアクセスする場合と同じ ID ファイルを使います。サーバーアクセス用のファイルを指定しない場合、Enterprise Vault はドメインにアクセスする場合と同じ ID ファイルを使います。

#### Enterprise Vault へのアクセスを設定する方法

- ◆ ユーザーの ID ファイルをコピーして、Domino ジャーナルタスクを実行するすべての Enterprise Vault サーバーの Notes データフォルダ (たとえば C:\Program Files\IBM\Notes\data) に保存します。

## Domino メーリングリストグループ

Enterprise Vault Compliance Accelerator を使う場合に Domino メーリングリストグループの拡張を確実に行うために、Domino メーリングリストグループを設定する際にはメールアドレスフィールドを明示的に設定してください。

## Domino ジャーナルアーカイブのクライアントアクセス

クライアントユーザーは、Enterprise Vault のブラウザベースの検索機能を使って Domino サーバーのジャーナルアーカイブにアクセスできます。

# ファイルシステムアーカイブ (FSA) の追加必要条件

この章では以下の項目について説明しています。

- [FSA の要件について](#)
- [FSA での Enterprise Vault サーバーの必要条件](#)
- [FSA ショートカットについて](#)
- [FSA エージェントについて](#)
- [FSA 用のファイルサーバーの準備](#)
- [FSA でのクライアントの必要条件](#)

## FSA の要件について

必要な製品のすべてのサポート対象バージョンについて詳しくは、「Enterprise Vault [Compatibility Charts](#)」を参照してください。この文書には、Enterprise Vault が FSA をサポートする対象のプラットフォーム、オペレーティングシステム、プロトコルの詳細情報も示されています。アーカイブ済みアイテムのクライアントアクセス (アーカイブ済みアイテムのインターネットショートカットとプレースホルダショートカットを開くなど) がサポートされているオペレーティングシステムの一覧も示されています。

## FSA での Enterprise Vault サーバーの必要条件

FSA をホストする Enterprise Vault サーバーには Enterprise Vault ストレージサービスが必要です。

FSA をホストする Enterprise Vault サーバーコンピュータには、Internet Explorer 9 以降が必要です。

FSA を実装し、Exchange Server アーカイブを実装しない場合は、Enterprise Vault サーバーに Outlook をインストールする必要はありません。ただし、Enterprise Vault が Enterprise Vault 7.0 の前にアーカイブしたファイルにアクセスする場合は Enterprise Vault サーバーに Outlook が必要になります。

FSA が .MSG ファイルをアーカイブする場合は、ファイルサーバーからアーカイブする Enterprise Vault サーバーに Outlook がインストールされていなければ、これらのファイルの Enterprise Vault インデックス処理が制限されることにも注意してください。たとえば、Enterprise Vault は Outlook メッセージの内容はインデックス付けできますが、メッセージの件名または添付ファイルはインデックス付けできません。完全なインデックス付けの機能が必要な場合は、Enterprise Vault サーバーに Outlook をインストールしてください。

ファイルサーバーから Outlook .MSG ファイルをアーカイブし、Outlook が Enterprise Vault サーバーにない場合、Enterprise Vault は Enterprise Vault イベントログに警告メッセージを生成します。これらの警告メッセージを受信する必要がない場合は、レジストリ値を設定することによってそれらを防ぐことができます。このメッセージを防ぐためには、値が 0 の WarnForMissingOutlook という DWORD レジストリ値を Enterprise Vault サーバーの次のレジストリキーに追加してください。

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

## FSA ショートカットについて

Enterprise Vault は、必要に応じて、ファイルのアーカイブ時に、次のいずれかの種類のショートカットをもとの場所に残すことができます。

- プレースホルダのショートカット。これは、元のファイルとまったく同じように見えますが、開くと Enterprise Vault がアーカイブ済みファイルをフェッチする特殊なファイルです。このショートカットを作成するにはプレースホルダサービスを設定する必要があります。
- インターネット (URL) ショートカット。これは、アーカイブ済みファイルへのハイパーリンクを含む .url テキストファイルです。このショートカットを作成するためにプレースホルダサービスは必要ありません。

Enterprise Vault は一部のレガシーファイルのプレースホルダを作成できません。特に、以前 HPFS (OS/2) ファイルシステムに格納していたために拡張属性が設定されているファイルには、この処理を行うことができません。

インターネットショートカットとプレースホルダショートカットを開くなど、アーカイブ済みアイテムのクライアントアクセスがユーザーのオペレーティングシステムでサポートされていることを Enterprise Vault [Compatibility Charts](#) で確認してください。

## プレースホルダショートカットの必要条件

Enterprise Vault では、次の種類のファイルシステムでプレースホルダショートカットの作成がサポートされています。

- NTFS

FSA エージェントを、Enterprise Vault プレースホルダサービスを提供する各 Windows ファイルサーバーにインストールする必要があります。

p.95 の「[FSA エージェントについて](#)」を参照してください。

プレースホルダショートカットを必要とする各ディスクは NTFS デバイスである必要があります。ネットワーク上に表示される非 NTFS デバイスを NTFS デバイスとして使わないでください。

Enterprise Vault サーバーは、ファイルのアーカイブなど、ファイルシステムへのアクセス時に CIFS を使います。

- NetApp Filer.

FSA エージェントは不要です。Enterprise Vault サーバーはプレースホルダサービスに同等の処理を実行し、CIFS を使って NetApp Filer にアクセスします。

- Dell EMC Celerra/VNX。

FSA エージェントは不要です。Enterprise Vault サーバーはプレースホルダサービスに同等の処理を実行し、CIFS を使って Dell EMC Celerra/VNX ファイルシステムにアクセスします。

FSA をインストールして設定する前に、アーカイブ対象のファイルシステムがサポートされていることを確認してください。

『Enterprise Vault [Compatibility Charts](#)』を参照してください。

## FSA エージェントについて

Windows ファイルサーバーの場合、次のいずれかをする場合は FSA エージェントをターゲットのファイルサーバーにインストールする必要があります。

- プレースホルダショートカットを使います。
- FSA レポート用のデータを収集します。

Windows ファイルサーバーがクラスタにグループ化されている環境では、各クラスターノードに FSA エージェントをインストールする必要があります。

FSA エージェントをインストールするための必要条件と指示は『ファイルシステムアーカイブ (FSA) の設定』に記載されています。

Windows 以外のファイルサーバーでは、FSA レポートを実装する際に FSA エージェントを使います。FSA レポートデータを収集するように FSA レポートのプロキシサーバーを設定する必要があります。Enterprise Vault サーバーではない FSA レポートのプロキシサーバーを設定する場合、プロキシサーバーに FSA エージェントをインストールする必要があります。

---

メモ: NetApp C-Mode Filer で FSA レポートを使うには、Enterprise Vault 11.0.1 以降の FSA エージェントをインストールする必要があります。

---

## FSA 用のファイルサーバーの準備

ボルトサービスアカウントまたは適切な管理者ロールに属するアカウントで Enterprise Vault のファイルサーバーを設定して管理できます。FSA の管理を可能にする事前定義済みの管理者ロールはファイルサーバー管理者とメイン管理者です。

詳しくは『管理者ガイド』の「管理者のセキュリティの管理」を参照してください。

使うアカウントには管理コンソールを実行するコンピュータに対するローカル管理者権限がなければなりません。

Windows ファイルサーバーでは、アカウントは次の必要条件も満たす必要があります。

- 次の処理を実行するためには、アカウントがファイルサーバー上でローカル Administrators グループのメンバーである必要があります。
  - ボルト管理コンソールまたは手動により FSA エージェントをインストールする場合。
  - ファイルサーバークラスタのためのリソースを設定または再設定する場合。このアカウントは、ファイルサーバークラスタノードのそれぞれにおいて、ローカル Administrators グループのメンバーである必要があります。
- このアカウントには、対象のボリュームとして設定されているすべての共有で、フルコントロールの権限を持っている必要があります。また、このアカウントは、その共有のマップ先のフォルダに対して NTFS の読み取り権限を持っている必要があります。
- 対象としてフォルダを選択するときに管理コンソールを参照したい場合は、アカウントには対象フォルダに対する参照権限を持っている必要があります。権限がない場合には、フォルダーパスを入力して指定する必要があります。

Windows ファイルサーバーがターゲットで、ファイルサーバーでローカル管理者グループのメンバーとしてボルトサービスアカウントを追加しない場合には、このアカウントは一組の最小限の権限と特権を持つ、組み込みローカル Print Operators グループのメンバーとして実行できます。FSA Agent をインストールすると、インストーラがこのアカウントに対しこの一連の最小要件を設定します。



『ファイルシステムのアーカイブの設定』の「FSA のボルトサービスアカウントに必要な権利について」を参照してください。

**NetApp** ファイルサーバーのアーカイブを設定する前に、ファイルサーバーの必須の管理者権限を設定する必要があります。

**NetApp** ファイルサーバーまたは **Dell EMC Celerra/VNX** デバイスの準備方法について詳しくは『ファイルシステムアーカイブ (FSA) の設定』を参照してください。

## FSA でのクライアントの必要条件

アーカイブ済みアイテムに対して、FSA で利用可能なクライアントアクセスは次のとおりです。

- アイテムの元の場所にショートカットが作成されている場合、ユーザーはファイルサーバー上のショートカットをダブルクリックしてアーカイブ済みアイテムにアクセスできます。
- ショートカットを作成していない場合は、**Enterprise Vault** による検索機能を使って、アーカイブにあるアーカイブ済みアイテムにアクセスできます (**Java** スクリプト対応の **Internet Explorer 9** 以降が必要)。

# SharePoint サーバーアーカイブの追加必要条件

この章では以下の項目について説明しています。

- [SharePoint Server アーカイブの Enterprise Vault サーバーの必要条件について](#)
- [SharePoint Server の必要条件](#)

## SharePoint Server アーカイブの Enterprise Vault サーバーの必要条件について

Enterprise Vault ストレージサービスをホストするサーバーには Internet Explorer 9 以降が必要です。

SharePoint Server アーカイブを実装し、Exchange Server アーカイブを実装しない場合は、Enterprise Vault サーバーに Outlook をインストールする必要はありません。ただし、Enterprise Vault が Enterprise Vault 7.0 の前にアーカイブしたファイルにアクセスする場合は Enterprise Vault サーバーに Outlook が必要になります。

## SharePoint Server の必要条件

SharePoint Server に必要なソフトウェアと設定は次のとおりです。

- Enterprise Vault がサポートしている Microsoft SharePoint のバージョンを使う必要があります。  
詳しくは、「Enterprise Vault [Compatibility Charts](#)」を参照してください。
- ボルトサービスアカウントに SharePoint Server コンピュータのローカル管理者権限があることを確認してください。

- Enterprise Vault SharePoint タスクを実行するアカウント(通常、ボルトサービスアカウント)には、対象サイトコレクションとその内容に対するフルアクセスが付与されている必要があります。
- SharePoint サーバーで Windows Server 2008 (Service Pack 1 以降)を実行している必要があります。Windows Server 2008 Service Pack 1 がインストールされている場合は、IIS 用の以下の必須 Hotfix もインストールする必要があります。

<http://support.microsoft.com/kb/949516>

次の点に注意してください。

- Microsoft が Windows Vista 用に提供している Hotfix は、Windows Server 2008 に使う Hotfix です。
- デフォルトでは、Microsoft 社の Web ページは、使っているコンピュータのオペレーティングシステムと一致する Hotfix のダウンロードを示します。ダウンロードページで、Hotfix の正しいバージョンを選択できるようにすべてのプラットフォームと言語の Hotfix を示すオプションを選択します。
- サーバーファームにインストールする場合、すべてのフロントエンド Web サーバーに Enterprise Vault 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 SharePoint コンポーネントには Enterprise Vault SharePoint HttpModule が必要です。Enterprise Vault SharePoint コンポーネントのインストールを選択すると、Enterprise Vault セットアッププログラムによって自動的に Enterprise Vault HttpModule がインストールされます。
- DCOM ポート (135) が対象の SharePoint システムで開いている必要があります。
- Enterprise Vault および SharePoint が異なるコンピュータで実行されている場合は、Backup Exec を Enterprise Vault Microsoft SharePoint Components と同じコンピュータにインストールしないことを推奨します。
- SharePoint ターゲットを追加するときには、URL にホスト名を含める必要があります。
- アーカイブ対象として SharePoint 2013 以降の Web アプリケーションを追加するには、Web アプリケーションで次のように認証を設定していることを確認する必要があります。
  - 統合 Windows 認証が有効になります。
  - 対象の Web アプリケーション内のすべてのゾーンでの信頼できる識別情報およびフォームベース認証が無効になります。

アーカイブ対象として SharePoint 2010 の Web アプリケーションを追加するには、Web アプリケーションでクラシックモード認証が有効になっていることを確認する必要があります。

---

**メモ:** 認証設定は、Web アプリケーションを追加するためだけでなく、そのコンテンツをアーカイブするためにも必要です。対象を追加した後でこれらの設定を変更すると、アーカイブが停止します。

---

- SharePoint 2013 以降のサイトが認証を要求する場合、Windows のトークンサービス (C2WTS) への要求を設定して実行する必要があります。

C2WTS を設定方法の詳細については、次の記事を参照してください。

<http://support.microsoft.com/kb/2722087>

必要な製品のすべてのサポート対象バージョンについて詳しくは、「Enterprise Vault Compatibility Charts」を参照してください。

## SharePoint セキュリティ証明書について

SharePoint 仮想サーバーまたは Web アプリケーションが使う証明書は、SharePoint の URL と同じ名前である必要があります。たとえば、SharePoint の URL が `https://sharepoint` の場合は、証明書要求を発行するときに使う証明書の名前は `sharepoint` である必要があります。

この名前が一致しない場合、管理コンソールで SharePoint サイトを設定しようとする際に、Enterprise Vault がそのサイトの有効性を確認できなくなります。

# Skype for Business アーカイブの追加必要条件

この章では以下の項目について説明しています。

- [Skype for Business アーカイブの必要条件について](#)
- [Skype for Business アーカイブの前提条件](#)
- [ロールベースの管理 \(RBA\) と Skype for Business アーカイブ](#)
- [Skype for Business から対話をエクスポートするために必要な権限の割り当て](#)

## Skype for Business アーカイブの必要条件について

Skype for Business Server 2015 と Lync Server 2013 の対話をアーカイブできます。現在、他のバージョンはサポートされません。

Skype for Business Server は、SQL Server データベースまたは Exchange Server メールボックスに対話をアーカイブできます。ただし、Enterprise Vault では SQL Server データベースへのアーカイブのみをサポートしています。

Enterprise Vault、Skype for Business Server または Lync Server と、サーバーのオペレーティングシステムの言語バージョンはすべて同じである必要があります。

## Skype for Business アーカイブの前提条件

Skype for Business アーカイブを実装するには、次の操作を完了する必要があります。

- Skype for Business Server または Lync Server を Enterprise Vault に対する個別のサーバーにインストールします。Skype for Business Server または Lync Server を Enterprise Vault サーバーにインストールした場合、Skype for Business アーカイブが期待どおりに機能しないことがあります。この構成はサポートされません。

- 対話を SQL Server データベースにアーカイブするように、Skype for Business または Lync Server を設定します。詳しくは、Skype for Business または Lync Server のマニュアルを参照してください。

Enterprise Vault で Skype for Business ターゲットを有効にした場合、Enterprise Vault は、Enterprise Vault サーバー上で対話を SQL データベースから SMTP 保存フォルダにエクスポートします。SQL データベースでの対話の保存を避けるためには、Enterprise Vault Skype for Business アーカイブの設定を完了してから、SQL データベースへのアーカイブを有効にします。

---

**メモ:** Enterprise Vault が Skype for Business SQL データベースからデータを正常にエクスポートすると、このデータベースにはパージ用のマークが付けられます。Skype for Business サーバーがデータをパージすると、データは Enterprise Vault にのみ存在するため、Skype for Business から再度エクスポートできなくなります。

---

- Enterprise Vault サーバーに Skype for Business Server 2015 管理ツールまたは Lync Server 2013 管理ツールをインストールします。

---

**メモ:** 管理ツールのバージョンは、Skype for Business または Lync Server のバージョンと一致する必要があります。

Enterprise Vault をインストールした後に管理ツールをインストールする場合は、Enterprise Vault サーバー上のタスク制御サービスを再起動してください。

---

- Skype for Business アーカイブのライセンスをインストールします。  
 有効なライセンスをインストールしないと Enterprise Vault は、設定した Skype for Business ターゲットから対話をアーカイブできません。

これらの手順が完了したら、Enterprise Vault の設定を完了して Skype for Business の対話のアーカイブを開始する方法について、『Skype for Business アーカイブの設定』を参照してください。

## ロールベースの管理 (RBA) と Skype for Business アーカイブ

Skype for Business アーカイブを管理するには、SMTP 管理タスクを実行できる RBA ロールが必要です。デフォルトでは、次のロールがこの権限を持っています。

- メッセージ管理者
- メイン管理者
- SMTP 管理者

デフォルトでは、SMTP アーカイブタスクは、必要な権限がすでに割り当てられているボルトサービスアカウントで動作します。異なるアカウントを使用する場合は、SMTP 管理者とタスクアプリケーションのロールが必要です。Enterprise Vault 12.2 以降を使っているユーザーには、これらのロールが自動的に割り当てられます。ただし、以前のバージョンの Enterprise Vault で特定のユーザーアカウントで実行されるように SMTP アーカイブタスクが設定されている場合は、これらのロールをユーザーアカウントに手動で割り当てる必要があります。これらのロールは Add-EVRBARoleMember cmdlet で割り当てることができます。詳しくは、『PowerShell Cmdlet』ガイドを参照してください。

ロールベースの管理について詳しくは、『管理者ガイド』を参照してください。

## Skype for Business から対話をエクスポートするために必要な権限の割り当て

Skype for Business ターゲットを設定するときに、Enterprise Vault が Skype for Business サーバーにアクセスするために使用するユーザーアカウントを指定します。これは、デフォルトでは SMTP アーカイブタスクに割り当てられているアカウントですが、別のアカウントを指定することもできます。選択するアカウントに必要な権限は次のとおりです。

- Skype for Business ターゲットを処理するサーバーのローカル管理者グループのメンバーシップ
- Skype for Business ターゲットを処理するサーバーの「サービスとしてログオンする」権限
- Skype for Business ターゲットを処理するサーバーの SMTP 保存フォルダへのフルアクセス権限
- domain\RTCComponentUniversalServices と domain\RTCUniversalReadOnlyAdmins の Skype for Business Active Directory グループのメンバーシップ

Enterprise Vault は、Active Directory グループのメンバーシップとは別に、これらすべての権限を自動的に割り当てることができます。グループにユーザーを手動で追加する必要があります。

---

**メモ:** ユーザーアカウントに権限を付与したら、該当のサーバーでタスクコントローラサービスを再起動します。

---

後でターゲットを修正して特定のアカウントを使わなくなった場合には、一部の権限を削除するように求められます。Active Directory グループからユーザーを削除する場合は手動で行う必要があります。

# SMTP アーカイブの追加必要条件

この章では以下の項目について説明しています。

- [Enterprise Vault SMTP サーバーの追加要件](#)

## Enterprise Vault SMTP サーバーの追加要件

Enterprise Vault SMTP サーバーの必要なソフトウェアと設定は次のとおりです。

- SMTP アーカイブを実行する各 Enterprise Vault サーバーに Enterprise Vault SMTP アーカイブコンポーネントをインストールする必要があります。  
SMTP に必要なポートが各 Enterprise Vault SMTP サーバーで開いていることを確認します。
- SMTP アーカイブを実行する各 Enterprise Vault サーバーに SMTP アーカイブライセンス (EVSMTPArchiving) をインストールする必要があります。SMTP メールボックスジャーナルを実装する場合は、Enterprise Vault SMTP サーバーに EVSMTPArchiving ライセンスと EVArchive ライセンスの両方をインストールする必要があります。有効なライセンスがインストールされていない場合、Enterprise Vault は SMTP ターゲットのデータをアーカイブできません。
- 管理コンソールを利用して SMTP アーカイブを管理する管理者には Enterprise Vault SMTP 管理者ロールを与える必要があります。このロールは Enterprise Vault メッセージ管理者ロールと Enterprise Vault メイン管理者ロールに含まれます。
- SSL を使って SMTP 接続を保全する場合は、SSL 証明書を取得し、MTA が接続する Enterprise Vault サーバーを認証する必要があります。1 つの証明書を使って複数のサーバーを認証することも、それぞれのサーバーに別の証明書を使うこともできます。  
『SMTP アーカイブの設定』ガイドを参照してください。



- SMTP 保存フォルダのために、Enterprise Vault SMTP サーバーにローカルディスク領域が必要です。SMTP サービスはメッセージを受け取り、このフォルダに EML ファイルとして置きます。SMTP アーカイブタスクはメッセージを処理し、SMTP ターゲットアドレスを含むメッセージをアーカイブします。SMTP アーカイブタスクを作成するとき、SMTP 保存フォルダを指定します。保存フォルダの場所は、SMTP アーカイブタスクのプロパティに表示されます。

Vault Service アカウントには、SMTP 保存フォルダへの完全アクセス権を与える必要があります。セキュリティのために、他のアカウントにはこのフォルダへのアクセス権を与えないでください。

ウイルススキャンソフトウェアにはこのフォルダを除外させます。Enterprise Vault にメッセージを送信する MTA でメッセージのウイルススキャンを実行してください。

- Enterprise Vault にジャーナルレポート (P1 メッセージ) を正しく処理させるには、次の記事に記載されている形式にメッセージが準拠する必要があります。

<http://technet.microsoft.com/library/bb331962.aspx>

SMTP アーカイブでは現在、Domino サーバーがジャーナルするメッセージのジャーナルレポート情報が処理されないことに注意してください。

- SMTP アーカイブを実装し、Exchange Server アーカイブを実装しない場合、Enterprise Vault SMTP サーバーに Outlook をインストールする必要はありません。ただし、たとえば、Discovery Accelerator の PST へのエクスポート機能を使用して、MAPI 形式でアーカイブ済みのアイテムをエクスポートすることを計画している場合、Enterprise Vault サーバー上に Outlook が必要です。アーカイブ済みアイテムを管理するストレージサービスが別の Enterprise Vault サーバー上でホストされている場合、そのサーバーに Outlook がインストールされている必要があります。

『Enterprise Vault [Compatibility Charts](#)』に、前提条件となるソフトウェアのサポート対象バージョンの詳細が含まれています。

# Enterprise Vault 検索の追加必要条件

この章では以下の項目について説明しています。

- [Enterprise Vault](#) による検索のサーバー必要条件
- [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

## 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 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がある最小セットの役割サービスの一覧です。

HTTP 共通機能	<div>■ 静的コンテンツ</div> <div>■ ディレクトリの参照</div> <div>■ HTTP エラー</div> <div>■ HTTP リダイレクト</div>
アプリケーション開発	<div>■ ASP.NET</div> <div>■ ISAPI 拡張</div> <div>■ ISAPI フィルタ</div>
健全性と診断	<div>■ HTTP ログ</div> <div>■ ロギングツール</div>
セキュリティ	<div>■ 要求のフィルタリング</div>

- |         |               |
|---------|---------------|
| パフォーマンス | ■ 静的なコンテンツの圧縮 |
| 管理ツール   | ■ 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>

# スタンドアロンの Enterprise Vault 管理コンソールの追加必要条件

この章では以下の項目について説明しています。

- スタンドアロンの [Enterprise Vault 管理コンソールの必要条件について](#)

## スタンドアロンの Enterprise Vault 管理コンソールの必要条件について

Enterprise Vault 管理コンソールを次の必要なソフトウェアがインストールされている別のコンピュータに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 7  
詳しくは「[Windows 7 でのスタンドアロンの管理コンソール](#)」を参照してください。
  - Windows 8
  - Windows 8.1
  - Windows 10
  - Windows Server 2012
  - Windows Server 2016
- .NET Framework 3.5 SP1、.NET Framework 4.5.2
- Windows PowerShell 3.0 以降

Exchange Server をアーカイブするように Enterprise Vault を設定する場合は、リモート管理コンソールのコンピュータに Microsoft Outlook の次のいずれかのバージョンも必要です。

- Outlook 2010
- Outlook 2013
- Outlook 2016

Domino サーバーをアーカイブするように Enterprise Vault を設定する場合は、リモート管理コンソールコンピュータに IBM Notes クライアントが必要です。

## Windows 7 でのスタンドアロンの管理コンソール

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が必要とします。インストール後と管理コンソールの使用前に、次の手順を実行します。

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

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/en-us/library/vstudio/ff361644\(v=vs.100\).aspx](https://msdn.microsoft.com/en-us/library/vstudio/ff361644(v=vs.100).aspx).

# アーカイブディスカバリ検索サービスの追加必要条件

この章では以下の項目について説明しています。

- [アーカイブディスカバリ検索サービスの追加の必要条件について](#)
- [アーカイブディスカバリ検索サービスに必要な追加のソフトウェア](#)
- [アーカイブディスカバリ検索サービスの SSL の設定](#)
- [アーカイブディスカバリ検索サービスを監視するための Operations Manager の使用](#)

## アーカイブディスカバリ検索サービスの追加の必要条件について

アーカイブディスカバリ検索サービスは、Enterprise Vault インストール内の複数のボルトストアとアーカイブを通じてディスカバリタイプの検索を実行する検索クライアントアプリケーションを Veritas パートナーが開発できるシンプルな Web サービス API を提供します。

検索を実行するには、このサービスのライセンスが必要です。

次の点に注意してください。

- アーカイブディスカバリ検索サービスは、大量のアーカイブを対象とする同時検索に最適化されています。少量のアーカイブに対する大量の同時検索を目的に設計されてはいません。
- Enterprise Vault ビルディングブロック環境ではこのサービスの使用はサポートされていません。ただし、VCS (Veritas Cluster Server) と Windows Server フェールオーバークラスタ (WSFC) 環境の両方でサービスを使用できます。



## アーカイブディスカバリ検索サービスに必要な追加のソフトウェア

アーカイブディスカバリ検索サービスを使って Enterprise Vault インストール環境内のアーカイブ全体を検索するには、そのサイトにある 1 つ以上の Enterprise Vault サーバーにアーカイブディスカバリ検索サービスをインストールする必要があります。

また、Windows Communication Foundation (WCF) のアクティブ化機能が Enterprise Vault サーバーで有効になっていることを確認する必要があります。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。

### WCF アクティブ化機能を手動でインストールする方法

- 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]ウィザードが表示されます。
- 2 [機能を選択]ページが表示されるまで[次へ]をクリックします。
- 3 まだインストールされていない場合は、次の機能をすべてインストールします。

.NET Framework 3.5 の .NET Framework 3.5  
 機能 HTTP アクティブ化

非 HTTP アクティブ化

.NET Framework 4.5 の .NET Framework 4.5  
 機能

[WCF サービス]>[ HTTP アクティブ化]

[WCF サービス]> [名前付きパイプのアクティブ化]

[WCF サービス]>[TCP のアクティブ化]

## アーカイブディスカバリ検索サービスの SSL の設定

Vault 管理コンソールで、ウィザードに従ってアーカイブディスカバリ検索サービスの処理を設定できます。この設定ウィザードのページで要求エンドポイントを設定して、クライアントアプリケーションでこの検索要求を送信できます。このエンドポイントは、Microsoft IIS (インターネットインフォメーションサービス) でホストされる Web アプリケーションです。

セキュリティ上の理由により、SSL (Secure Sockets Layer) を使用してエンドポイントへのすべての接続を暗号化する必要があります。新規インストールを設定するとき、Enterprise Vault は、Enterprise Vault Web Access コンポーネントへの接続に HTTPS を自動的に

に設定します。デフォルトの Web サイトで SSL をまだ設定していない場合は、Enterprise Vault の設定ウィザードで自己署名証明書を作成してインストールします。自己署名証明書は一時的なものとして考え、信頼できる認証局から取得した証明書と、できるだけ早く交換することが重要です。次の手順では、実装方法について説明します。

信頼できる認証局からの証明書を取得およびインストールするには

- 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、次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。

- 要求エンドポイントをホストするサーバー。たとえば、Server1 と Server1.domain.com などが挙げられます。
- Vault Site エイリアス (Enterprise Vault サイトの DNS エイリアス)。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。

- 2 アーカイブディスカバリ検索サービスをインストールしている 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新しい証明書にリンクします。

これら 2 つの手順を実行する方法について詳しくは、IIS のマニュアルを参照してください。

## アーカイブディスカバリ検索サービスを監視するための Operations Manager の使用

Enterprise Vault Operations Manager を使用してアーカイブディスカバリ検索サービスの活動を監視します。まだ Operations Manager が設定されていない場合は、アーカイブディスカバリ検索サービスを設定する前に設定するのが最適です。

p.54 の「[Operations Manager をインストールする場所とタイミング](#)」を参照してください。

# Enterprise Vault のインストール

- [第16章 ライセンスとライセンスキー](#)
- [第17章 Enterprise Vault のインストール](#)
- [第18章 Enterprise Vault の修復、修正、アンインストール](#)

# ライセンスとライセンスキー

この章では以下の項目について説明しています。

- [Enterprise Vault ライセンスの概要](#)
- [Enterprise Vault のライセンスキーの取得](#)
- [Enterprise Vault ライセンスキーファイルのインストール](#)
- [Enterprise Vault ライセンスの置換と追加ライセンスのインストール](#)

## Enterprise Vault ライセンスの概要

Enterprise Vault では、Enterprise Licensing System (ELS) が使われます。関連付けられている Enterprise Vault サービスを実行するには、実装する Enterprise Vault 機能を対象とするライセンスキーファイルをインストールする必要があります。

次の種類の Enterprise Vault ライセンスを利用できます。

- 製品ライセンス。このライセンスは、製品の基本ライセンスと追加機能ライセンスで構成されます。ライセンスファイルをインストールする場合、Enterprise Vault の機能は、購入した機能のライセンスによって異なります。  
通常、製品ライセンスには有効期限がありません。
- 試用ライセンス。この 30 日間のライセンスでは、Enterprise Vault のすべての機能が利用可能です。ただし、機能にはキーによって定義された有効期限があります。ライセンスの有効期限が切れても、ソフトウェアは制限された読み取り専用モードで引き続き動作するので、アーカイブ済みアイテムの表示と取り込みができます。ただし、アイテムをアーカイブすることはできません。Enterprise Vault タスクは開始されず、個人用フォルダ (PST) ファイルの内容を Enterprise Vault に移行できません。
- 一時ライセンス。一時ライセンスは、10 から 90 日の期間利用できます。ライセンスの有効期限が切れても、ソフトウェアは制限された読み取り専用モードで引き続き動作するので、アーカイブ済みアイテムの表示と取り込みができます。ただし、

アイテムをアーカイブすることはできません。Enterprise Vault タスクは開始されず、個人用フォルダ (PST) ファイルの内容を Enterprise Vault に移行できません。

既存の Enterprise Vault 環境では、Enterprise Vault の「コンテンツプロバイダのライセンスおよび使用状況の概略」レポートを使ってライセンスを調整できます。このレポートについて詳しくは、『レポート』を参照してください。

## Enterprise Vault のライセンスキーの取得

Enterprise Vault ライセンスの購入方法の詳細については、次のアドレスの Veritas 社の Web サイトにある Veritas Enterprise Vault ライセンス情報を参照してください。

<https://www.veritas.com/licensing/process>

ライセンスが必要な Enterprise Vault の機能は次のとおりです。

- アーカイブディスカバリ検索サービス
- Compliance Accelerator
- カスタムフィルタとカスタムプロパティ
- Discovery Accelerator
- Domino サーバージャーナールアーカイブ
- Domino サーバメールボックスアーカイブ
- Enterprise Vault コアサービス
- Exchange Server ジャーナールアーカイブ
- Exchange Server メールボックスアーカイブ
- Exchange Server パブリックフォルダのアーカイブ
- ファイルシステムアーカイブ (FSA)
- IMAP クライアントアクセス
- Enterprise Vault コレクションファイルの移行
- PST ファイルの移行
- NSF 移行ウィザード
- Policy Manager (EVPM)
- 保持
- SharePoint Server アーカイブ
- Skype for Business アーカイブ
- SMTP アーカイブ
- ボルトキャッシュ

ライセンスを購入して、ライセンス証明、Voucher、アップグレードのお知らせを受け取ったら、次のアドレスにある Veritas Licensing Portal にアクセスして、ライセンスキーファイルの登録と生成を行う必要があります。

<https://www.veritas.com/licensing/process/activate>

Veritas Licensing Portal アカウントを作成するには、ライセンス文書または通知に記載されているシリアル番号が必要です。

ライセンスキーファイルを生成したら、デジタル署名済みの圧縮 ELS ライセンスファイルをダウンロードします。ELS ライセンスファイルには重複のない名前と拡張子 .slf が付いています。各ライセンスファイルには、複数の Enterprise Vault 機能のライセンスキーを含めることができます。

# Enterprise Vault ライセンスキーファイルのインストール

このファイルを、各 Enterprise Vault サーバーコンピュータの一時的な場所に保存します。

Enterprise Vault インストールウィザードにより、ELS ライセンスファイルの場所を入力するように求められ、Enterprise Vault の最上位フォルダ (たとえば、C:\Program Files (x86)\Enterprise Vault) にファイルがコピーされます。Enterprise Vault Admin Service が開始されると、ライセンスがインストールされ、イベントログにライセンス情報レポートメッセージが書き込まれます。

ELS ライセンスファイルがなくても Enterprise Vault のインストールは続行できますが、新しい ELS ライセンスを取得してインストールするまで、Enterprise Vault は制限された読み取り専用モードで実行されます。

## Enterprise Vault ライセンスの置換と追加ライセンスのインストール

Enterprise Vault の「コンテンツプロバイダのライセンスおよび使用状況の概略」レポートを使ってライセンスを調整できます。このレポートについて詳しくは、『レポート』ガイドを参照してください。

Enterprise Vault がすでにインストールされている状態で、追加のライセンスファイルをインストールしたり、既存のライセンスファイルを置換したりする場合は、このセクションで説明する手順に従います。

### ライセンスの置換または追加ライセンスのインストールを実行する方法

- 1 新しい .slf ライセンスファイルを Enterprise Vault フォルダ (C:\Program Files (x86)\Enterprise Vault など) に格納します。
- 2 Enterprise Vault の管理サービスを再起動してライセンスをインストールします。管理サービスによって、ライセンス情報のレポートメッセージがイベントログに書き込まれます。
- 3 Enterprise Vault が複数のサーバーで配備されている場合は、各 Enterprise Vault サーバーでこの手順を繰り返す必要があります。

# Enterprise Vault のインストール

この章では以下の項目について説明しています。

- [Enterprise Vault のインストールについて](#)
- [Enterprise Vault のインストール\(ウィザード\)](#)
- [Enterprise Vault のインストール\(コマンドライン\)](#)

## Enterprise Vault のインストールについて

Enterprise Vault をインストールする前に、次の操作を実行してください。

- Enterprise Vault をインストールするコンピュータの名前に **Unicode** 文字が含まれていると Enterprise Vault が適切に動作しなくなることがあるため、**Unicode** 文字が含まれていないことを確認します。コンピュータ名には **ASCII** 文字のみ含めることを強く推奨します。
- Enterprise Vault をインストールするすべてのコンピュータに、最新の **Windows** アップデートをインストールします。**Windows** アップデートが Enterprise Vault のインストール中に開始すると、インストールが失敗する場合があります。
- 計画したインストールのすべての前提条件が満たされていることを確認します。**Enterprise Vault** をインストールするコンピュータで、**Deployment Scanner** を実行します。  
p.36 の「[Enterprise Vault Deployment Scanner について](#)」を参照してください。

Enterprise Vault には、ウィザードベースのインストーラとコマンドラインインストーラが用意されています。これらのインストーラでは、次の操作を実行できます。

- Enterprise Vault のインストール
- 既存の Enterprise Vault インストールの修復

- 既存のインストールへの Enterprise Vault コンポーネントの追加
- Enterprise Vault のアンインストール

## 自動的にインストールされるソフトウェア

Enterprise Vault インストーラを実行すると、必要に応じて次のソフトウェアが自動的にインストールされます。

- Microsoft .NET Framework 3.5 SP1 (Windows 機能)
- Microsoft .NET Framework 4.5.2 完全
- Microsoft Visual C++ 2008 SP1 再頒布可能 MFC セキュリティ更新プログラム KB2538243 (x64)
- Microsoft Visual C++ 2008 SP1 再頒布可能 MFC セキュリティ更新プログラム KB2538243 (x86)
- Microsoft Visual C++ 2010 SP1 再頒布可能パッケージ (x64)
- Microsoft Visual C++ 2010 SP1 再頒布可能パッケージ (x86)
- Microsoft Visual C++ 2013 再頒布可能パッケージ (x64)
- Microsoft Visual C++ 2013 再頒布可能パッケージ (x86)
- Microsoft Visual C++ 2017 再頒布可能パッケージ (x64)
- Microsoft Visual C++ 2017 再頒布可能パッケージ (x86)
- SQLXML 4.0 SP1 (x64)

## Enterprise Vault サーバーのコア機能

インストールでは、次のコア Enterprise Vault サーバー機能をインストールできます。

- Enterprise Vault サービスすべてのコア Enterprise Vault サービス。インストールの完了後、Enterprise Vault サービスを使う前にこれらのサービスを設定する必要があります。これらのサービスの設定は Enterprise Vault 設定ウィザードの実行時に行われます。  
p.133 の「[Enterprise Vault の設定について](#)」を参照してください。
- 管理コンソール Enterprise Vault 管理コンソール。管理コンソールは、Microsoft 管理コンソール (MMC) のスナップインです。管理コンソールにより、Enterprise Vault を管理できるようになります。この機能をインストールすると、Enterprise Vault 設定ウィザード、PST 移行ウィザード、NSF 移行ウィザードもインストールされます。  
リモートシステムにスタンドアロンの管理コンソールをインストールする場合は、この機能のみを選択します。
- 検索アクセスコンポーネントこの機能では、ユーザーはモバイルデバイスでアーカイブのアイテムを検索したり、開いたりすることができます。



## その他の機能

必要な数の機能をインストールできます。インストーラでは、機能をインストールする前に前提条件が満たされているかが常に確認されます。

追加の機能を次に示します。

- [アーカイブディスカバリ検索サービス]。このサービスは、Enterprise Vault インストール先のすべてのアーカイブをサードパーティのクライアントアプリケーションで作成して実行する方法を提供します。このサービスは、これらのアプリケーションが検索の状態をチェックし、結果を取得し、検索をキャンセル、再送信、および閉じるための方法も提供します。アーカイブディスカバリ検索サービスは、任意の Enterprise Vault サーバーにインストールできます。

p.112 の「[アーカイブディスカバリ検索サービスの追加の必要条件について](#)」を参照してください。

- Enterprise Vault Lotus Domino Gateway この機能は、Notes と Enterprise Vault 間のインターフェースを提供します。アーカイブデータに対するすべての主要な処理（オープン、復元、削除、検索）は Enterprise Vault Domino Gateway によって行われます。

- SMTP アーカイブコンポーネント。SMTP アーカイブを実行する各 Enterprise Vault サーバーに Enterprise Vault SMTP アーカイブコンポーネントをインストールします。  
p.104 の「[Enterprise Vault SMTP サーバーの追加要件](#)」を参照してください。

- Microsoft SharePoint コンポーネント。これらのコンポーネントは、通常は Enterprise Vault サーバー以外のコンピュータにインストールします。  
p.98 の「[SharePoint Server の必要条件](#)」を参照してください。

- Operations Manager。この機能は、Internet Explorer がインストールされているコンピュータから Enterprise Vault サーバーをリモート監視できるようにする Web アプリケーションです。

任意のサイトの Enterprise Vault サーバーを監視する場合は、そのサイトに少なくとも 1 つの Enterprise Vault に Enterprise Vault Operations Manager をインストールする必要があります。

- Enterprise Vault Reporting。この機能は、レポートの仕組みとして Microsoft SQL Server Reporting Services を使うことで、Enterprise Vault サーバーにエンタープライズレベルのレポート機能を提供します。管理者は、レポートサービスのレポートマネージャ Web アプリケーションを使って、レポートの内容を管理し、レポートを表示します。

FSA Reporting を使う場合は、Enterprise Vault Reporting が必要です。

Enterprise Vault Reporting は、Microsoft SQL Server のレポートサービスを必要とします (SSRS)。

Enterprise Vault Reporting は Enterprise Vault サーバーにインストールできますが、通常は SSRS を実行している別のサーバーにインストールします。Enterprise

Vault Reporting のインストールと設定について詳しくは『レポート』ガイドを参照してください。

## Enterprise Vault のインストール (ウィザード)

ウィザードインストールを使うと、インストールオプションを双方向で選択できます。

### Enterprise Vault をインストールするには

- 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 Install Launcher の右ペインで、Enterprise Vault の下にある[View ReadMeFirst]をクリックします。インストールを続行する前に、ReadMeFirst の内容を確認します。
- 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、[Installation on first server in new site]をクリックします。
- 8 [Install]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 このコンピュータに必要な Enterprise Vault 機能をインストールします。
- 10 Domino がインストールされている場合、インストールによって、利用可能な Domino パーティションが一覧表示されます。インストールにより、選択した各パーティションに Enterprise Vault Domino Gateway ソフトウェアがインストールされます。
- 11 設定ではコンピュータを自動的にスキャンし、Enterprise Vault の前提条件を満たし、レポートを生成するかどうかを判断します。コンピュータが必要条件の一部しか満たしていない場合は、ウィザードで検索結果のレポートを表示するオプションを選択できます。
- 12 設定では、Enterprise Vault のベストプラクティス設定を使うようにコンピュータが設定されていることを確認します。
- 13 インストールの終了時に、コンピュータを再起動するように指示されることがあります。インストールは、コンピュータを再起動した後も続きます。インストールが完了したことを通知する確認メッセージが表示されます。

# Enterprise Vault のインストール(コマンドライン)

コマンドラインインストールでは次を実行できます。

- Enterprise Vault のサイレントインストールの実行。
- 事前にポピュレートされたデフォルト値を使ったインストールウィザードの実行。
- 既存のインストールの修復、変更または削除。

## 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へログインします。
- 2 Enterprise Vault メディアをロードします。
- 3 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
```

- 4 必要なパラメータを使って `setup (x64).exe` を実行します。パラメータについて詳しくは、下記を参照してください。

## 構文

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

サイレントインストールの場合:

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

## パラメータ

`/s` 省略可能。サイレントインストール。`/wait` および `/clone_wait` パラメータと一緒に使用する必要があります。

デフォルトのオプションを使って Enterprise Vault をインストールします。他のコマンドオプションを使って、デフォルト値を上書きできます。

このパラメータを省略すると、インストールウィザードが起動します。他のコマンドオプションを使って、ウィザードのデフォルト値を上書きできます。デフォルト値を上書きすることにより、異なるオプションを選択することなくクリックでウィザードを操作できます。

`/wait` サイレントインストールに `/s` パラメータを使用する場合は必須です。

`/clone_wait` サイレントインストールに `/s` パラメータを使用する場合は必須です。

/v 必須。コマンドオプションを導入します。完全なオプションの文字列を囲む二重引用符を使います。個々のオプションについては、二重引用符の後にバックスラッシュを使って、スペースまたはバックラッシュを含むオプションを区切ります。次に例を示します。

```
LOGFILE=%"C:¥EV.log¥"
```

```
LOGFILE=%"C:¥My Logs¥EV.log¥"
```

## [オプション]

複数のオプションを区切るには、垂直線(|)を使います。次に例を示します。

```
/v"COMPONENTS=VAULT|SMTP"
```

使うことのできるオプションを次に示します。

BESTPRACTICE	<p>ベストプラクティス設定を使うかどうかを制御します。設定可能な値は次のとおりです。</p> <p>BESTPRACTICE=0。ベストプラクティス設定を使わない場合</p> <p>BESTPRACTICE=1 (デフォルト)。ベストプラクティス設定を使う場合</p> <p>p.41 の「<a href="#">Enterprise Vault サーバーのベストプラクティス設定</a>」を参照してください。</p>
DOMINOPARTITIONS	<p>Enterprise Vault Domino Gateway ソフトウェアのインストール先の Domino パーティションを指定します。</p> <p>複数のパーティションを区切るには、垂直線を使います。例: Domino パーティション 1 と 2 にインストールする方法:</p> <pre>DOMINOPARTITIONS=1 2</pre>
ENABLEFEATURES	<p>インストーラで Enterprise Vault サーバーが必要とするすべての Windows の機能とロールを自動的にインストールするかどうかを制御します。設定可能な値は次のとおりです。</p> <p>ENABLEFEATURES=0 (デフォルト)。インストーラは Windows の機能とロールをインストールしません。</p> <p>ENABLEFEATURES=1。インストーラは必要な Windows の機能とロールをすべてインストールします。</p> <p>p.322 の「<a href="#">[マイシステムの準備]オプションによる Windows 機能の有効化</a>」を参照してください。</p>
INSTALLDIR	<p>インストール先のフォルダ。デフォルトフォルダは C:¥Program Files (x86)¥Enterprise Vault です。</p>
LOGFILE	<p>インストールログファイルのパス。デフォルトパスは %temp%¥EVInstall.log です。</p>

## COMPONENTS

これはインストールを行うときに必須のオプションです。コンポーネントは次のいずれかです。

- ADSS。アーカイブディスカバリ検索サービスをインストールします。
- DOMINO。Domino アーカイブと VAULT コンポーネントをインストールします。
- EVCOMMONITORINGWEBAPP。Enterprise Vault Operations Manager Web アプリケーションと VAULT コンポーネントをインストールします。
- EVOMREPORTING。Enterprise Vault Reporting をインストールします。
- EVSEARCH。Enterprise Vault Search をインストールします。VAULT を指定すると、このオプションも自動的にインストールされます。
- SHAREPOINT。SharePoint アーカイブをインストールします。
- SMTP。SMTP アーカイブと VAULT コンポーネントをインストールします。
- VAC。管理コンソールをインストールします。VAULT を指定するときにこのオプションも自動的にインストールされます。
- VAULT。すべての Enterprise Vault サーバーコンポーネント、EVSEARCH、VAC をインストールします。

p.119 の「Enterprise Vault のインストールについて」を参照してください。

## デフォルトオプション

任意のデフォルトオプションを上書きできます。/s パラメータを省略する場合は、インストールウィザード内でオプションを上書きできます。

デフォルトオプションは次のとおりです。

- インストール場所: C:\Program Files (x86)\Enterprise Vault
- Domino パーティション: パーティションなし
- ベストプラクティス設定: ベストプラクティス設定を使う
- インストールログの場所: %temp%\EVInstall.log

## 例のコマンド

- デフォルトオプションを使って VAULT コンポーネントをインストールする場合:  
start /wait "" "setup (x64).exe" /s /clone\_wait  
/v"COMPONENTS=VAULT"
- デフォルトオプションを使うが、D:\Logs\EVinstall.log のインストールログファイルを使ってインストールウィザードを起動する場合:  
"setup (x64).exe" /v"LOGFILE=%D:\Logs\EVinstall.log%"

- フォルダ D:¥myVault に **VAULT** コンポーネントをインストールする場合:  
`"setup (x64).exe" /v"INSTALLDIR=¥"D:¥myVault¥" COMPONENTS=VAULT"`
- デフォルトオプションを使うが、D:¥Logs¥EVinstall.log のインストールログファイルを使って **VAULT** コンポーネントをインストールする場合:  
`start /wait "" "setup (x64).exe" /s /clone_wait  
/v"LOGFILE=¥"D:¥Logs¥EVinstall.log¥" COMPONENTS=VAULT"`

# Enterprise Vault の修復、修正、アンインストール

この章では以下の項目について説明しています。

- [Enterprise Vault の修復、修正、アンインストールについて](#)
- [Enterprise Vault の修正](#)
- [Enterprise Vault の修復](#)
- [Enterprise Vault のアンインストール](#)

## Enterprise Vault の修復、修正、アンインストールについて

Enterprise Vault には、ウィザードベースのインストーラとコマンドラインインストーラが用意されています。これらのインストーラでは、次の操作を実行できます。

- Enterprise Vault のインストール
- 既存の Enterprise Vault インストールの修復
- 既存のインストールへの Enterprise Vault 機能の追加
- Enterprise Vault のアンインストール

## Enterprise Vault の修正

必要に応じて Enterprise Vault に新しい機能を追加することができます。この操作は、次の 2 つの方法で実行できます。

- Enterprise Vault インストールウィザードを使う。Enterprise Vault をインストールしたときと同じ方法でウィザードを実行します。  
p.122 の「Enterprise Vault のインストール(ウィザード)」を参照してください。
- コマンドラインから行う。コマンドラインオプションは、Enterprise Vault をインストールするのに使ったものと同じです。  
p.123 の「Enterprise Vault のインストール(コマンドライン)」を参照してください。

インストールした Enterprise Vault 機能を個別にアンインストールできないことに注意してください。

## Enterprise Vault の修復

ウィザードまたはコマンドラインを使って Enterprise Vault を修復できます。

### [プログラムと機能]からの修復

[プログラムと機能]から Enterprise Vault を修復する方法

- 1 Windows の[コントロールパネル]を開き、[プログラム]で[プログラムのアンインストール]をクリックします。
- 2 [プログラムと機能]で、Veritas Enterprise Vault を右クリックし、ショートカットメニューの[変更]をクリックします。
- 3 InstallShield ウィザードで、[修復]を選択し、[次へ]をクリックします。
- 4 ウィザードに従ってインストールを修復します。

### SMTP がインストールされていない場合のコマンドラインからの修復

SMTP がインストールされていない場合にコマンドラインからサイレントで Enterprise Vault を修復する方法

- 1 Enterprise Vault メディアをロードします。
- 2 管理者権限でコマンドプロンプトウィンドウを開きます。



- 3 コマンドプロンプトウィンドウで、Enterprise Vault メディア上の次のフォルダに変更します。

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

- 4 次のコマンドを入力します。

```
"setup (x64).exe" /s /v"REINSTALL=ALL"
```

ログファイルのデフォルトの場所は次のとおりです。

```
%temp%¥EVInstall.log
```

次の例のように、任意でログファイルの場所を指定できます。

```
"setup (x64).exe" /v"REINSTALL=ALL  
LOGFILE=¥"C:¥logs¥EVreinstall.log¥"
```

## SMTP がインストールされている場合のコマンドラインからの修復

SMTP コンポーネントがインストールされている場合は、SMTP を修復するかどうかを指定する必要があります。

---

**メモ:** SMTP を修復することを選択するときに Enterprise Vault SMTP サービスが実行中である場合は、インストールでは修復前にそのサービスが停止され、修復後に再起動されます。SMTP サービスは再起動されるまで利用できません。

---

### SMTP がインストールされている場合にコマンドラインからサイレントで Enterprise Vault を修復する方法

- 1 Enterprise Vault メディアをロードします。
- 2 管理者権限でコマンドプロンプトウィンドウを開きます。
- 3 コマンドプロンプトウィンドウで、Enterprise Vault メディア上の次のフォルダに変更します。

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

- 4 次のように、適切なコマンドを入力します。

- SMTP 以外のすべてのコンポーネントを修復するには、次を入力します。このオプションは Enterprise Vault SMTP サービスを停止しません。

```
"setup (x64).exe" /s /v"REINSTALL=ALL SMTPSERVICE=0"
```

- すべてのコンポーネントと SMTP を修復するには、次を入力します。このオプションは、SMTP サービスが実行中である場合はそのサービスを停止して再起動します。

```
"setup (x64).exe" /s /v"REINSTALL=ALL SMTPSERVICE=1"
```

ログファイルのデフォルトの場所は次のとおりです。

```
%temp%\%EVInstall.log
```

次の例のように、任意でログファイルの場所を指定できます。

```
"setup (x64).exe" /v"REINSTALL=ALL SMTPSERVICE=1  
LOGFILE=%"C:\logs\%EVreinstall.log%"
```

## Enterprise Vault のアンインストール

続行する前に、次の点に注意してください。

- Enterprise Vault をアンインストールする前に、『Veritas Enterprise Vault™ バックアップと回復』ガイドで説明しているように Enterprise Vault システムデータベースのバックアップを作成します。
- アンインストーラは、インストール後に作成または変更したファイルを削除しません。たとえば、アンインストーラは Enterprise Vault の Reports フォルダからレポートファイルを削除しません。
- Enterprise Vault サービスに関連付けされているデータがある場合、Enterprise Vault 管理コンソールを使ってこのサービスを削除することはできません。
- アンインストーラは、Enterprise Vault のインストール処理の一部として自動的にインストールされている次のソフトウェアコンポーネントを削除しません。
  - Microsoft Visual C++ 再頒布可能パッケージ
  - SQLXML 4.0 SP1

### ウィザードを使った Enterprise Vault のアンインストール

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

- 1 Windows の[コントロールパネル]を開き、[プログラム]で[プログラムのアンインストール]をクリックします。
- 2 プログラムの一覧から Enterprise Vault を選択して[アンインストール]をクリックします。

ウィザードで、Enterprise Vault とそのすべての機能をシステムから削除するかどうかを確認するメッセージが表示されます。

- 3 [はい]をクリックします。

アンインストーラによって実行中の Enterprise Vault サービスが停止されます。その後、すべての Enterprise Vault サービスと Enterprise Vault ソフトウェアがシステムから削除されます。アンインストーラによってデータが削除されることはありません。

Enterprise Vault を再インストールする必要がある場合は、Enterprise Vault のデータを手動で削除します。

## コマンドラインを使った Enterprise Vault のアンインストール

コマンドラインを使って Enterprise Vault をサイレントにアンインストールする方法

- 1 管理者権限でコマンドプロンプトウィンドウを開きます。
- 2 コマンドプロンプトウィンドウで、Enterprise Vault メディア上の次のフォルダに変更します。
- 3 次のコマンドを入力します。

```
"setup (x64).exe" /s /uninst
```

次の例のように、任意でログファイルの場所を指定できます。

```
"setup (x64).exe" /s /uninst  
/V"LOGFILE=%"C:¥logs¥EVuninstall.log¥"
```

アンインストーラによって実行中の Enterprise Vault サービスが停止されます。その後、すべての Enterprise Vault サービスと Enterprise Vault ソフトウェアがシステムから削除されます。アンインストーラによってデータが削除されることはありません。Enterprise Vault を再インストールする必要がある場合は、Enterprise Vault のデータを手動で削除します。

# Enterprise Vault の設定

- 第19章 Enterprise Vault の設定について
- 第20章 Enterprise Vault 設定ウィザードの実行
- 第21章 Enterprise Vault Web Access コンポーネントのセキュリティ保護
- 第22章 Enterprise Vault 開始ウィザードの実行
- 第23章 Enterprise Vault Operations Manager の設定
- 第24章 アーカイブディスカバリ検索サービスの設定

# Enterprise Vault の設定について

この章では以下の項目について説明しています。

- [Enterprise Vault の設定について](#)

## Enterprise Vault の設定について

インストールした Enterprise Vault コンポーネントによっては、Enterprise Vault インストールプログラムの終了時に、1 つ以上の設定プログラムを実行する必要がある場合があります。

以前のバージョンの Enterprise Vault からアップグレードした場合は、新バージョンの Enterprise Vault のアップグレード手順に従ってください。

Enterprise Vault を新規にインストールする場合は、次の手順を実行します。

- Enterprise Vault サービスコンポーネントをインストールした場合は、他の設定プログラムを実行する前に Enterprise Vault 設定ウィザードを実行します。  
p.135 の「[Enterprise Vault 設定ウィザードを実行するタイミング](#)」を参照してください。
- Enterprise Vault Web アプリケーションのセキュリティを確認します。  
p.142 の「[Enterprise Vault Web Access コンポーネントのデフォルトのセキュリティ](#)」を参照してください。
- Enterprise Vault Operations Manager コンポーネントをインストールした場合は、Enterprise Vault Operations Manager を設定します。  
p.169 の「[Enterprise Vault Operations Manager 設定ユーティリティを実行するタイミング](#)」を参照してください。
- アーカイブディスカバリ検索サービスをインストールしている場合は、その設定ウィザードが実行されます。

p.174 の「[アーカイブディスカバリ検索サービスの設定ウィザードの実行](#)」を参照してください。

- **Enterprise Vault Reporting** コンポーネントをインストールした場合は、**Enterprise Vault Reporting** を設定します。  
詳しくは『レポート』の **Enterprise Vault Reporting** の設定に関する章を参照してください。
- 管理コンソールコンポーネントのみをインストールした場合は、設定プログラムを実行する必要はありません。
- **Exchange、Domino、SharePoint、SMTP** などの特定のアーカイブ実装用のコンポーネントをインストールした場合は、それらのコンポーネントの個別の設定手順の実行が必要となる可能性があります。このガイドの関連セクションを参照してください。

# Enterprise Vault 設定ウィザードの実行

この章では以下の項目について説明しています。

- [Enterprise Vault 設定ウィザードを実行するタイミング](#)
- [Enterprise Vault 設定ウィザードの機能](#)
- [Enterprise Vault 設定ウィザードの実行](#)
- [Enterprise Vault 監視データベースの設定のトラブルシューティング](#)
- [デフォルトの SSL 設定の問題に関するトラブルシューティング](#)

## Enterprise Vault 設定ウィザードを実行するタイミング

Enterprise Vault 設定ウィザードは、インストール直後(コンピュータの再起動を要求された場合は再起動の後)か、**Web Access** コンポーネント用のインストール後の作業を実行した後に実行します。

次の点に注意してください。

- インストールの完了後すぐに設定ウィザードを実行する場合は、ユーザーが **Enterprise Vault** を使う前に、いくつかの追加作業を行う必要があります。  
p.133 の「[Enterprise Vault の設定について](#)」を参照してください。
- 設定が完了する前に、設定ウィザードを終了した場合は、再度設定ウィザードを実行して、ディレクトリデータベースを削除できます。設定ウィザードが正常に完了すると、同じコンピュータで再度設定ウィザードを実行することはできません。

## Enterprise Vault 設定ウィザードの機能

設定ウィザードによって、次のことが可能になります。

- Enterprise Vault ディレクトリデータベースに対して使用する SQL Server の選択
- Enterprise Vault ディレクトリデータベースの作成
- Enterprise Vault 監視データベースの作成
- Enterprise Vault サイトの作成
- サイトへのコンピュータの追加
- コンピュータで実行する Enterprise Vault サービスの選択
- Enterprise Vault データに使用するストレージ領域の選択

サービスの追加、データのストレージ領域の割り当てなど、一部のタスクは Enterprise Vault 管理コンソールを使用しても実行できます。ただし、次のタスクは、設定ウィザードを使用して実行する必要があります。

- 新しい Enterprise Vault ディレクトリの作成
- 新しい Enterprise Vault サイトの作成
- 新しい Enterprise Vault サーバーの追加

まだ設定されていない場合、設定ウィザードは IIS のデフォルト Web サイトに SSL を設定します。必要な場合、ウィザードは自己署名証明書を作成してインストールし、ポート 443 の HTTPS バインドを追加します。設定後、SSL はすべての Enterprise Vault 仮想ディレクトリで有効になります。

## Enterprise Vault 設定ウィザードの実行

---

**メモ:** これらの手順は、非クラスタ環境に適用されます。Veritas Cluster Server または Windows Server フェールオーバークラスタリング環境で Enterprise Vault を設定する場合は、代わりに、このマニュアル内のクラスタ化に関する適切なセクションを参照してください。

---

コンピュータの再起動後、またはインストールプログラムの完了後に、設定ウィザードを起動できます。

サイト内の最初の Enterprise Vault サーバーで設定ウィザードを実行するには、次の手順に従います。その後、他のコンピュータで設定ウィザードを使って Enterprise Vault を設定するときは、ヘルプで不明な手順を確認してください。

設定ウィザードを実行する前に、必要な SQL Server の権限と役割がボルトサービスアカウントに割り当て済みであることを確認してください。

p.49 の「SQL データベースでの権限と役割の割り当てについて」を参照してください。



設定ウィザードの実行中に Enterprise Vault 監視データベースの設定に関するエラーが表示された場合は、設定ウィザードを完了し、監視データベースのトラブルシューティング情報を参照してください。

p.140 の「Enterprise Vault 監視データベースの設定のトラブルシューティング」を参照してください。

## Enterprise Vault 設定ウィザードを実行する方法

- 1 [アプリ]画面で[Enterprise Vault]>[設定]を選択します。

設定ウィザードが起動します。最初の画面で、新しい Enterprise Vault ディレクトリデータベースを作成するかどうかを確認するメッセージが表示されます。

- 2 [はい]をクリックし、[次へ]をクリックします。

Enterprise Vault で、管理コンソールにデフォルト設定をポピュレートする場合に使う言語を選択するように求められます。

- 3 必要な言語を選択し、[次へ]をクリックします。

使用する Enterprise Vault サービスで使うアカウントの詳細を入力するように求められます。

- 4 以前に作成したボルトサービスアカウントの詳細を入力します。

p.46 の「ボルトサービスアカウントの作成」を参照してください。

アカウントを指定するときは、`domain_name¥username` の形式を使う必要があります。代わりに、ボルトサービスアカウントを参照することもできます。

ボルトサービスアカウントのパスワードを入力し、確認します。

- 5 [次へ]をクリックします。

使っているアカウントにボルトサービスアカウントのパスワードの有効性を確認する十分な権限がない場合は、警告メッセージが表示されます。[はい]をクリックして続行します。

ボルトサービスアカウントがローカル Administrators グループに追加されたことを伝えるメッセージが表示されます。[OK]をクリックしてメッセージを閉じます。

次に、アカウントに拡張ユーザー権限 ([サービスとしてログオン]、[プログラムのデバッグ]、[プロセスレベルトークンの置き換え]) が与えられることを通知するメッセージが表示されます。[OK]をクリックしてメッセージを閉じます。

設定ウィザードによってディレクトリサービスが作成され、次の画面でディレクトリデータベースに使う SQL Server の場所を入力するよう要求されます。

- 6 使用する SQL Server の場所を入力します。または、[参照]をクリックし、SQL Server を参照します。必要に応じて、SQL Server インスタンスを指定できます。

**7** [次へ]をクリックします。

ウィザードに、ディレクトリデータベースファイルとトランザクションログのデフォルトの場所が表示されます。

**8** 必要に応じて、場所を変更します。

**SQL Server** がリモートコンピュータ上にあることを指定した場合は、データファイルとトランザクションログファイルのパスがそのリモートコンピュータで有効である必要があります。

**9** [次へ]をクリックします。

ウィザードによって、ディレクトリデータベースが作成されます。次の画面で、監視データベースに使う **SQL Server** の場所を入力するよう要求されます。

**10** 使用する **SQL Server** の場所を入力します。必要に応じて、**SQL Server** インスタンスを指定できます。

**11** [次へ]をクリックします。

次の画面に、監視データベースファイルとトランザクションログ用の **SQL Server** のデフォルトの場所が表示されます。

**12** 必要に応じて、場所を変更します。

**SQL Server** がリモートコンピュータ上にあることを指定した場合は、データファイルとトランザクションログファイルのパスがそのリモートコンピュータで有効である必要があります。

ファイルシステムのルート上 (c:、c:\ など) にあるパスは指定しないでください。

**13** [次へ]をクリックします。

ウィザードによって、監視データベースが作成されます。

次の画面で新しい **Enterprise Vault** サイトの詳細を入力するよう要求されます。

**14** 新しい **Enterprise Vault** サイトの名前と説明を入力します。

**15** [次へ]をクリックします。

次の画面で、現在のコンピュータの **DNS** エイリアスを入力するよう要求されます。

入力する値は、このコンピュータの非修飾 **DNS** エイリアス (evserver1 など) である必要があります。完全修飾 **DNS** 名 (evserver1.mycompany.local など) は許可されません。

これがサイトに追加される最初のコンピュータである場合は、入力した **DNS** エイリアスはボルトサイトエイリアスとして自動的に使われます。

p.51 の「[Enterprise Vault の DNS エイリアスの作成](#)」を参照してください。

**16** 現在のコンピュータの **DNS** エイリアスを入力し、[次へ]をクリックします。

- 17 [次へ]をクリックして、Enterprise Vault サイトにコンピュータを追加します。

情報画面に、コンピュータにインストールされているソフトウェアの一覧が表示されます。この一覧に基づいて、コンピュータに追加する Enterprise Vault サービスが自動的に選択されます。
- 18 [次へ]をクリックします。一覧に、コンピュータに追加されるサービスが表示されます。
- 19 サービスの一覧を確認します。必要に応じて、次のようにサービスの追加または削除を実行できます。
  - サービスを削除するには、サービスをクリックして選択し、[削除]をクリックします。
  - サービスを追加するには、[追加]をクリックして、必要なサービスを選択します。
- 20 [次へ]をクリックします。情報ページに、ウィザードで作成されるサービスの一覧が表示されます。
- 21 [次へ]をクリックして、サービスを作成します。
- 22 ウィザードの最後の画面には、次のオプションが表示されます。
  - [Enterprise Vault 開始ウィザードを実行]。できるだけ迅速にアーカイブを設定するには、このオプションを選択します。このウィザードには、柔軟性を最大限に高めるために、エクスプレスオプションとカスタムオプションの両方が用意されています。
  - [Enterprise Vault 管理コンソールを実行]。すでに管理コンソールを熟知していて、アーカイブの設定も熟知している場合は、このオプションを選択します。
  - [何もしないでこのウィザードを閉じる]。設定ウィザードを終了するには、このオプションを選択します。この後で、デスクトップのショートカットをクリックして Enterprise Vault 開始ウィザードまたは管理コンソールを起動できます。
- 23 設定ウィザードを終了する場合は、[完了]をクリックします。

---

**メモ:** 設定ウィザードをコンピュータで正しく実行できるのは 1 回限りであることに注意してください。Enterprise Vault を正しく設定した後に、設定ウィザードを終了すると、再度このウィザードを実行することはできなくなります。Enterprise Vault Operations Manager や Enterprise Vault Reporting に関連するコンポーネント以外の Enterprise Vault コンポーネントの追加設定や管理を行うには、管理コンソールを使う必要があります。

IIS の Enterprise Vault Web アプリケーションを保護するために構成で自己署名証明書が使用されている場合、この証明書をできるだけ早く信頼できる認証局からの証明書に交換します。

---

## Enterprise Vault 監視データベースの設定のトラブルシューティング

設定ウィザードの実行中に、Enterprise Vault 監視データベースの設定が失敗したことを示すエラーが表示されたら、設定ウィザードを完了し、監視設定ユーティリティを実行して、監視データベースと監視エージェントを手動で設定します。

実行方法については、次の Veritas サポート Web サイトのテクニカルノートを参照してください。

<https://www.veritas.com/docs/100018087>

このテクニカルノートでは、監視エージェントに関する問題のトラブルシューティング方法についても説明しています。

## デフォルトの SSL 設定の問題に関するトラブルシューティング

Enterprise Vault 設定ウィザードで自己署名証明書を作成できない場合、または IIS で証明書と HTTPS バインドを設定できない場合、Enterprise Vault イベントログにエラーが報告されます。次に例を示します。

```
Failed to create HTTPS binding in IIS.  
Reason: Could not create self-signed certificate "Enterprise Vault"  
  
in IIS on this server.  
...
```

証明書と HTTPS バインドを作成し、Enterprise Vault 仮想ディレクトリで SSL を有効にするため、Enterprise Vault 設定ウィザードによってユーティリティ `HTTPSBindingAndCertificateProvider.exe` が起動されます。イベントログでエラーが報告される場合、次の処理を実行できます。

- `HTTPSBindingAndCertificateProvider.exe` によって作成されるログファイルで例外を検索します。ログファイルのパスは次のとおりです。  
`<%Temp%> ¥EVHTTPSBindingConfiguration.log`
- 一時的なエラーの場合は、次の手順の説明に従って、手動でユーティリティを再実行します。

### HTTPSBindingAndCertificateProvider.exe を手動で実行する方法

- 1 コマンドプロンプトウィンドウを開き、Enterprise Vault インストール先フォルダに移動します。これは通常、`C:¥Program Files (x86)¥Enterprise Vault` です。
- 2 次のコマンドラインを入力します。

```
HTTPSBindingAndCertificateProvider createcertificateandbinding  
EVServerAliasenableSSLFlagSSLport
```

ここでは、次のとおりです。

**EVServerAlias** は、Enterprise Vault サーバーに設定した完全修飾 DNS エイリアス、つまり、完全修飾のボルトサイトのエイリアスです。

**enableSSLFlag** は、Enterprise Vault 仮想ディレクトリで SSL を有効または無効にする数値フラグです。SSL を有効にする場合は **1** を、無効にする場合は **0** (ゼロ) を入力します。

**SSLport** パラメータはオプションです。デフォルトでは、ポート **443** が SSL バインドに使用されます。このパラメータを使用すると、別のポートを指定できます。

コマンドラインの例を次に示します。

```
HTTPSBindingAndCertificateProvider createcertificateandbinding  
test.domain.com 1
```

このコマンド例は、IIS で以下を行います。

- DNS エイリアスが `test.domain.com` の Enterprise Vault サーバーの自己署名証明書を作成します。この証明書は「Enterprise Vault」と呼ばれ、IIS の個人用証明書ストアに格納されます。
- デフォルトの Web サイトでは、HTTPS バインドが存在しない場合、ポート **443** でこのバインドを作成します。
- すべての Enterprise Vault 仮想ディレクトリで SSL を有効にします。

- 3 コマンド `HTTPSBindingAndCertificateProvider` が正常に完了したら、Enterprise Vault 管理コンソールで **Web Access** アプリケーションのポートとプロトコルを変更します。

これを行うには、Enterprise Vault 管理コンソールでサイトプロパティを開き、[全般] タブをクリックします。

- 4 [SSL ポートで HTTPS を使用]を選択します。HTTPS ポート **443** を使用していない場合、`HTTPSBindingAndCertificateProvider` コマンドラインで指定したポートに SSL ポート番号を変更します。
- 5 [OK]をクリックしてプロパティウィンドウを閉じます。変更は次のアーカイブ実行時に有効になります。

# Enterprise Vault Web Access コンポーネントのセキュリティ保護

この章では以下の項目について説明しています。

- [Enterprise Vault Web Access](#) コンポーネントのデフォルトのセキュリティ
- [Enterprise Vault Web Access](#) コンポーネント用のポートまたはプロトコルのカスタマイズ
- [Enterprise Vault Web Access](#) コンポーネントの認証のカスタマイズ
- クライアントコンピュータでの [Web Access](#) コンポーネントのセキュリティのカスタマイズ

## Enterprise Vault Web Access コンポーネントのデフォルトのセキュリティ

Enterprise Vault Web Access コンポーネントは 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。デフォルトの Web サイトで有効な証明書がない場合は、設定ウィザードで自己署名証明書を作成してインストールします。設定により、この証明書を HTTPS バインドに割り当てます。

デフォルトの Web サイトに有効な証明書を使用したポート 443 の HTTPS バインドがすでにある場合、Enterprise Vault 設定ウィザードでは、Enterprise Vault 仮想ディレクトリの SSL の有効化のみ行います。

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。自己署名証明書は、Enterprise Vault サーバーでは信頼されません。これにより、クライアントがリモートコンピュータから接続する場合、Enterprise Vault Outlook アドイン、Enterprise Vault 検索、Veritas Information Classifier の一部の機能が動作しなくなることがあります。

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。ただし、Enterprise Vault への Web 接続のセキュリティを確保するために、Enterprise Vault 仮想ディレクトリで SSL を手動で設定し、有効にすることをお勧めします。

Enterprise Vault Web Access コンポーネントにアクセスするために使われるポートまたはプロトコルを変更することができます。

p.144 の「[Enterprise Vault Web Access コンポーネント用のポートまたはプロトコルのカスタマイズ](#)」を参照してください。

---

**警告:** HTTP を使用する場合、Enterprise Vault クライアントと Enterprise Vault Web Access コンポーネント間の通信は暗号化が解除されるため、ネットワークの遮断に対して脆弱です。

---

基本認証と統合 Windows 認証の両方が自動的に設定されます。

自動的に設定される認証は、ログインするユーザーに対して次のような影響があります。

- 統合 Windows 認証に対応したブラウザ (Internet Explorer など) を使ってログインするユーザーは、ドメイン名とユーザー名を別々に指定する必要があります。

ユーザー名: *username*

パスワード: *password*

ドメイン: *domain*

このドメインにはデフォルト値を設定できません。

Internet Explorer のブラウザ設定を適切にカスタマイズしている場合は、ログオンが自動的に実行されるため、ログオン情報を手動で入力する必要はありません。Internet Explorer では、ユーザーが現在ログオンしているアカウントの情報が自動的に使われます。

p.146 の「[クライアントコンピュータでの Web Access コンポーネントのセキュリティのカスタマイズ](#)」を参照してください。

- 統合 Windows 認証に対応していないブラウザを使って Web Access コンポーネントにログインするユーザーは、ユーザー名の入力ボックスにドメイン名とユーザー名の両方を指定する必要があります。

ユーザー名: *domain ¥ username*

パスワード: *password*

デフォルトのドメインを設定できます。

p.145 の「Enterprise Vault Web Access コンポーネントの認証のカスタマイズ」を参照してください。

## Enterprise Vault Web Access コンポーネント用のポートまたはプロトコルのカスタマイズ

Enterprise Vault Web Access コンポーネントにアクセスするために使われるポートまたはプロトコルを変更することができます。プロトコルを変更する場合、IIS のデフォルト Web サイトの設定を変更する必要があります。

アイテムをアーカイブした後でポートを変更した場合、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[メールボックスを同期]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。

Enterprise Vault で Web Access のポートまたはプロトコルを変更する前に、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。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、FSAReporting 仮想ディレクトリなど、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注意してください。

p.144 の「証明書要求を作成し、IIS で SSL を実装する方法」を参照してください。

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

Enterprise Vault サイトで FSA レポートを使う場合、追加手順を実行する必要があります。そうしないと、管理コンソールで FSA レポートの状態がオフとして表示されます。サイトの各 Enterprise Vault サーバーと各ファイルサーバーで、次の手順を実行してください。

p.145 の「ポートまたはプロトコル変更後の FSA レポートに関する追加手順」を参照してください。

### 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。
- 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。

#### ポートまたはプロトコル変更後の FSA レポートに関する追加手順

- 1 FSA レポートユーザーとしてログオンします。FSA レポートユーザーとは、FSA レポート設定ウィザードを実行したときに、FSA レポートで使われるように指定した Windows ユーザーアカウントです。
- 2 Internet Explorer を開き、[ツール] > [インターネットオプション] の順にクリックします。
- 3 SSL ポートを使う場合は、[詳細設定] タブをクリックし、[セキュリティ] の [サーバー証明書の取り消しを確認する] にチェックマークが付いていないことを確認します。
- 4 [セキュリティ] タブをクリックし、[イントラネット] ゾーンを選択します。[レベルのカスタマイズ] をクリックして、[セキュリティの設定] を表示します。[ユーザー認証] の [ユーザー名とパスワードを入力してログオンする] にチェックマークが付いていないことを確認します。
- 5 サイトの各 Enterprise Vault サーバーと各ファイルサーバーで、1 から 4 までの手順を繰り返します。

## Enterprise Vault Web Access コンポーネントの認証のカスタマイズ

Web Access コンポーネントの標準セキュリティでは、Web Access コンポーネントにログインするたびに、ドメイン名、ユーザー名、パスワードを入力する必要があります。

IIS と Enterprise Vault では、基本認証にデフォルトのドメインを使えます。この場合、デフォルトのドメインのユーザーは Web Access コンポーネントを起動するときにドメイン名を指定する必要がありません。他のドメインのユーザーは、ドメイン名を指定する必要があります。

基本認証でデフォルトのドメインを使うように IIS を設定することができます。この設定方法は、インストールしている IIS のバージョンによって異なります。

p.146 の「[IIS 7 でのデフォルトのドメインの設定方法](#)」を参照してください。

デフォルトのドメインを使用するには、Web Access コンポーネントに対してデフォルトのドメインを定義する必要があります。

p.146 の「[Web Access コンポーネントのデフォルトのドメインを定義する方法](#)」を参照してください。

### IIS 7 でのデフォルトのドメインの設定方法

- 1 IIS (Internet Information Services) マネージャを起動します。
- 2 Enterprise Vault Web Access がインストールされているコンピュータのサイトコンテナを展開します。
- 3 [EnterpriseVault] フォルダをクリックします。
- 4 右側にある[IIS]領域の[認証]をダブルクリックします。
- 5 [匿名認証]が無効になっていて、[基本認証]が有効になっていることを確認します。
- 6 デフォルトのドメインを設定するには、次の手順を実行します。
  - [基本認証]を右クリックし、[編集]をクリックします。
  - Web Access コンポーネントを使うユーザーアカウントの大半が含まれるドメインの名前を入力します。
  - [OK]をクリックします。

### Web Access コンポーネントのデフォルトのドメインを定義する方法

- 1 テキストエディタを使って、次の行を含む WebApp.ini という初期設定ファイルを作成します。

```
Domain=DomainName
```

*DomainName* は IIS で基本認証用に指定したドメインの名前です。このファイルでは大文字と小文字が区別されます。

たとえば **myDomain** というドメインを使う場合は、次のように記述します。

```
Domain=myDomain
```

- 2 Enterprise Vault プログラムフォルダにこのファイルを保存します。たとえば、このフォルダは Web Access コンポーネントを実行するコンピュータの C:\Program Files (x86)\Enterprise Vault になります。

## クライアントコンピュータでの Web Access コンポーネントのセキュリティのカスタマイズ

ユーザーのコンピュータで、ログオン画面を表示せずに、ユーザーが Web Access コンポーネントに自動的にログオンするように Internet Explorer を設定できます。この場合

は、Web Access コンピュータを信頼するように Internet Explorer を設定する必要があります。

この信頼関係を設定するには、統合 Windows 認証を使う必要があります。

Internet Explorer が自動的にログオンするように設定するには、各クライアントコンピュータで Internet Explorer のインターネットオプションの修正が必要な場合があります。この設定は Windows レジストリに保存されます。したがって、この設定を保存しておき、多数のクライアントコンピュータに適用できます。

Internet Explorer のセキュリティを設定する方法は多数ありますが、状況によっては一部の方法が適切でないことがあります。ここでは次の方法について説明します。

- プロキシバイパス一覧を使う方法
- Web Access コンピュータに明示的に名前を付ける方法

ブラウザのセキュリティを設定する方法については、Internet Explorer ヘルプを参照してください。

USGCB (United States Government Configuration Baseline) に準拠する Windows コンピュータでは、Internet Explorer でローカルイントラネットゾーンの設定を変更できません。ただし、関連する USGCB グループポリシーオブジェクトを修正することによって Enterprise Vault サーバーの詳細をユーザーのコンピュータに公開できます。ユーザーは、認証を毎回要求されることなく、Enterprise Vault の処理を実行できます。

p.149 の「[USGCB 準拠コンピュータへの Enterprise Vault サーバーの詳細の公開](#)」を参照してください。

## プロキシバイパス一覧を使うための Internet Explorer の設定

プロキシバイパス一覧を使うには、プロキシサーバーを使う必要がある点に注意してください。

プロキシバイパス一覧を使うように Internet Explorer を設定する方法

- 1 Internet Explorer で、[ツール]メニューの[インターネットオプション]をクリックします。
- 2 [セキュリティ]タブをクリックし、[イントラネット]ゾーンをクリックします。
- 3 [サイト]をクリックし、[プロキシサーバーを使用しないサイトをすべて含める]にチェックマークを付けます。
- 4 [OK]をクリックします。
- 5 [レベルのカスタマイズ]をクリックします。
- 6 [ログオン]の下にある[イントラネットゾーンでのみ自動的にログオンする]をクリックします。
- 7 [OK]をクリックします。

- 8 [接続]タブをクリックし、[LAN の設定]をクリックします。
- 9 プロキシサーバーを使っていることを確認します。
- 10 [自動構成]のいずれかのチェックボックスにチェックマークが付いている場合は、Web Access コンピュータが自動構成の例外の一覧に含まれていることを確認してください。
- 11 [自動構成]のどのチェックボックスにもチェックマークが付いていない場合は、[LAN にプロキシ サーバーを使用する]にチェックマークを付けて[詳細設定]をクリックします。Web Access コンピュータを含む既存のエントリが存在しない場合は、[例外]一覧にそのコンピュータを指定します。

## Enterprise Vault Web Access コンポーネントを信頼するための Web ブラウザの設定

Enterprise Vault Web Access コンポーネントを信頼するようにユーザーの Web ブラウザを設定すると、アーカイブの検索やアーカイブ済みアイテムの表示、復元を行うためにログオンする必要がなくなります。例として、次の手順では Internet Explorer を適切に設定する方法について説明します。

のローカルイントラネットゾーンに Web Access コンピュータが自動的に追加されるようにユーザーのデスクトップを設定することもできます。これを設定するには、Exchange デスクトップポリシーの拡張 Outlook 設定を使います。詳しくは『管理者ガイド』を参照してください。

### Enterprise Vault Web Access コンポーネントを信頼するための Internet Explorer の設定方法

- 1 Internet Explorer で、[ツール]メニューの[インターネット オプション]をクリックします。
- 2 [セキュリティ]タブをクリックし、[イントラネット]ゾーンをクリックします。
- 3 [レベルのカスタマイズ]をクリックします。
- 4 [ログオン]の下にある[イントラネットゾーンでのみ自動的にログオンする]をクリックし、[OK]をクリックします。
- 5 [サイト]をクリックし、[詳細設定]をクリックします。
- 6 [次の Web サイトをゾーンに追加する]フィールドに Web Access コンピュータの完全修飾ドメイン名を入力して、[追加]をクリックします。たとえば、vault.company.com と入力します。
- 7 [次の Web サイトをゾーンに追加する]フィールドに、DNS ドメインを含めずに Web Access コンピュータのコンピュータ名を入力し、[追加]をクリックします。
- 8 [OK]をクリックします。

## USGCB 準拠コンピュータへの Enterprise Vault サーバーの詳細の公開

従来は FDCC (連邦政府共通デスクトップ基準) と呼ばれていた USGCB (米国政府共通設定基準) は、米国政府機関のネットワークに接続されている汎用ミニコンピュータに対する推奨セキュリティ設定の一覧です。USGCB のグループポリシーオブジェクトの設定 (GPO) を Windows コンピュータに適用している場合、ユーザーは Internet Explore のローカルなイントラネットゾーン設定を変更できません。そのため、ユーザーは Enterprise Vault にアクセスするたびに認証信用証明を入力する必要があります。たとえば、ユーザーがアイテムをアーカイブまたは取得するときに信用証明を要求されます。

このセクションでは、Enterprise Vault サーバーの詳細を USGCB Internet Explorer GPO に追加する方法を説明します。GPO を更新すると、Enterprise Vault サーバーの詳細がユーザーのコンピュータのローカルイントラネットゾーンに追加されます。GPO の設定はユーザー設定よりも優先されるため、Enterprise Vault サーバーの詳細が正しいことを確認する必要があります。

### USGCB 準拠のコンピュータに Enterprise Vault サーバーの詳細を公開する方法

- 1 管理者アカウントと GPO を修正して公開する権限を使ってドメインコントローラコンピュータにログオンします。
- 2 Group Policy Object Editor を開きます。
- 3 Internet Explorer の設定を Windows コンピュータに適用する USGCB GPO を選択します。
- 4 Group Policy Object Editor で、次のセクションにナビゲートします。  
 [コンピュータの構成] > [管理用テンプレート] > [Windows コンポーネント] > [Internet Explorer] > [インターネットコントロールパネル] > [セキュリティページ]
- 5 [サイトとゾーンの割り当て一覧] を右クリックし、[プロパティ] を選択します。
- 6 選択されていない場合は [有効] を選択し、[表示] をクリックして必要なゾーン割り当てを入力します。
- 7 [追加] をクリックします。

- 8 [追加するアイテムの名前を入力してください]フィールドに、Enterprise Vault サーバーの名前を入力します。

[追加するアイテムの値を入力してください]フィールドに 1 を入力します。

これで、サーバー名とイントラネットゾーンがマッピングされます。

同様に、すべての Enterprise Vault サーバー名を一覧に追加し、それらをイントラネットゾーンにマッピングします。この一覧にはすべての Enterprise Vault サーバーのエイリアスを含めてください。名前が SRV1 でエイリアスが EVSERVER1 の Enterprise Vault サーバーの場合、サイトとゾーンの割り当て一覧に次のように追加します。

```
Value Name: evserver1.mycorp.local
Value: 1
Value Name: srv1
Value: 1
```

- 9 Enterprise Vault サーバー名の一覧への追加が終了したら、[OK]をクリックします。
- 10 [サイトとゾーンの割り当て一覧]の[プロパティ]ページで、[適用]をクリックします。
- 11 ポリシーを次回更新するときに GPO への変更が Windows コンピュータに適用されます。
- 12 ユーザーのコンピュータの 1 つで、Enterprise Vault サーバー名がローカルイントラネットサイトに追加されていることを確認できます。
- 標準ユーザーとしてコンピュータにログオンします。
  - Internet Explorer を開きます。
  - [ツール]、[インターネットオプション]、[セキュリティ]、[ローカルイントラネット]、[サイト]、[詳細設定]の順にクリックします。
  - Enterprise Vault サーバー名が Web サイトに一覧表示されます。

## Enterprise Vault Web Access コンピュータへのリモートアクセスの有効化

場合によっては、Enterprise Vault Web Access コンポーネントのユーザーに対し、IIS コンピュータへのアクセス権を付与するときに、ドメインアカウントデータベースではなくローカル IIS コンピュータアカウントデータベースを使う必要があります。

---

**メモ:** IIS コンピュータがドメインコントローラの場合は、ローカルアカウントデータベースではなく、ドメインアカウントデータベースが使われます。IIS コンピュータがドメインコントローラの場合にこの手順を行うには、ドメインアカウントデータベースのセキュリティアクセスを変更する必要があります。この変更内容は IIS コンピュータだけでなく、ドメイン内のすべてのコンピュータに反映されます。ドメイン全体に変更を反映しない場合は、必ずドメインコントローラ以外で IIS を実行するようにしてください。

---

### Enterprise Vault Web Access コンピュータへのリモートアクセスを有効にする方法

- 1 [ローカルセキュリティポリシー]の管理ツールを起動します。
- 2 [ローカルセキュリティポリシー]ウィンドウで、[ローカルポリシー]コンテナを展開します。
- 3 [ユーザー権限の割り当て]をクリックします。
- 4 次の手順を一覧表示された順序で実行して、基本認証アクセスを設定します。
  - 右側のペインの[ローカルログオンを許可する]を右クリックし、ショートカットメニューの[プロパティ]をクリックします。
  - [ローカルセキュリティ設定]一覧に **Users** グループが表示されていることを確認します。
- 5 次の手順を一覧表示された順序で実行して、統合 Windows 認証アクセスを設定します。
  - [ローカルセキュリティポリシー]ウィンドウの左側のペインの[ユーザー権限の割り当て]を選択した状態で、右側のペインの[ネットワーク経由でコンピュータへアクセス]を右クリックし、ショートカットメニューの[プロパティ]をクリックします。
  - [ローカルセキュリティ設定]一覧に **Users** グループが表示されていることを確認します。

**Users** グループを追加しない場合は、下に示す方法を参照してください。

デフォルトでは、**Users** グループに **Domain Users** が含まれています。**Users** グループに **Domain Users** が含まれていない場合、または一部の **Web Access** ユーザーが別のドメインに所属している場合は、次のいずれかの操作を行います。

- **Web Access** ユーザーを **Users** グループに追加します。
- **Web Access** ユーザーを他のグループに追加し、そのグループにアクセス権を付与します。
- 各 **Web Access** ユーザーのアカウントにアクセス権を付与します。

Enterprise Vault Web Access コンポーネントの設定が完了しました。これで、IIS と同じドメインに所属するユーザーは、このアプリケーションを使えます。

# Enterprise Vault 開始ウィザードの実行

この章では以下の項目について説明しています。

- [Enterprise Vault 開始ウィザードの機能](#)
- [Enterprise Vault 開始ウィザードの実行準備](#)
- [Enterprise Vault 開始ウィザードの実行](#)
- [Enterprise Vault 開始ウィザードのエクスプレスモードとカスタムモードについて](#)
- [Enterprise Vault 開始ウィザードの計画](#)

## Enterprise Vault 開始ウィザードの機能

Enterprise Vault 開始ウィザードを使うと、できるだけ迅速にアーカイブを設定できます。

ウィザードは、必要に応じて次のことを行う場合に役立ちます。

- Exchange Server、Domino、ファイルシステムアーカイブのアーカイブポリシーの作成
- ストレージの場所の設定
- インデックス処理の設定
- 保持カテゴリの作成

ウィザードのセクションは、次のエクスプレスモードまたはカスタムモードのどちらかを選択して実行できます。

- エクスプレスモードでは、ウィザードからの質問が少なくなります。代わりに、多くの項目にデフォルト設定が適用されます。必要に応じて、後で管理コンソールを使って設定を変更することができます。



- カスタムモードでは、デフォルト設定を柔軟に変更できます。

---

**メモ:** エクスプレスモードでは、開始ウィザードにより、ローカルディスクを指定するように要求されます。ウィザードでは、そのディスクをすべてのストレージに使うように Enterprise Vault を設定します。リモートストレージまたは別のローカルストレージ設定を設定する場合は、ストレージ設定用にカスタムモードを選択する必要があります。

---

## Enterprise Vault 開始ウィザードの実行準備

開始ウィザードは、Enterprise Vault ライセンスキーを確認して、表示するオプションを決定します。開始ウィザードを実行する前に、ライセンスキーのインストールを完了している必要があります。

p.116 の「[Enterprise Vault ライセンスの概要](#)」を参照してください。

Enterprise Vault Deployment Scanner を実行して、Enterprise Vault の設定が正しいかどうかを示すレポートを作成することができます。

Enterprise Vault メディアの Documentation フォルダにある Deployment Scanner のガイドを参照してください。

### Enterprise Vault 開始ウィザードから Deployment Scanner を実行する方法

- ◆ 「開始する前の確認事項」ページで[Deployment Scanner の実行]をクリックします。

## Enterprise Vault 開始ウィザードの実行

Enterprise Vault の新規インストールの一環として、設定ウィザードを完了した直後に開始ウィザードを実行できます。

開始ウィザードは、完了前に終了しても再度実行することができます。開始ウィザードが正常に完了した場合、同じコンピュータで再度開始ウィザードを実行できますが、すべてのオプションが利用できない場合があります。サイトの他のコンピュータでも開始ウィザードを実行できます。

### Enterprise Vault 開始ウィザードを実行する方法

- ◆ 次のいずれかの操作を行います。
  - 設定ウィザードの最後のページで[Enterprise Vault 開始ウィザードを実行]を選択します。
  - [アプリ]画面で[Enterprise Vault]>[開始ウィザード]を選択します。

## Enterprise Vault 開始ウィザードのエクспレスモードとカスタムモードについて

開始ウィザードでは、エクспレスモードまたはカスタムモードを選択して次の各項目を行うことができます。

- インデックス設定
- ストレージ設定
- ポリシー定義
- Exchange 対象設定
- Domino 対象設定
- ファイルサーバー対象設定

エクспレスモードでは、ウィザードからの質問が少なくなります。代わりに、Enterprise Vault をできるだけ迅速に設定できるように、ウィザードではデフォルト設定が適用されます。必要に応じて、後で管理コンソールを使って設定を変更することができます。

カスタムモードでは、必要なすべての変更を実行できますが、すべてのオプションを設定するのに長い時間がかかることがあります。デフォルトのオプションを受け入れてから、管理コンソールで変更することもできます。

開始ウィザードのエクспレスモードのオプションを一覧表示した計画シートが用意されています。このシートに独自の必要条件を記録し、後で管理コンソールを使って必要な変更を加えることができます。

p.161 の「Enterprise Vault 開始ウィザードの計画」を参照してください。

## Enterprise Vault 開始ウィザードでのインデックス設定について

エクспレスモードではローカルストレージサービスを使用するため、Enterprise Vault 開始ウィザードがインデックス処理サービスを自動的に設定します。開始ウィザードは、インデックスサーバーグループを作成しませんし、既存のインデックスサーバーグループに現在のサーバーを追加することはありません。

現在のサーバーをインデックスサーバーグループに追加する場合、カスタムモードを[インデックス設定]に対して選択します。カスタムモードにより、インデックスサーバーグループを作成でき、サーバーをインデックスサーバーグループに追加できます。

### エクспレスモードでの自動インデックス設定

このセクションでは、インデックス設定にエクспレスモードを選択したときに、Enterprise Vault 開始ウィザードによって自動的に設定される設定について説明します。

表 22-1 に、ウィザードのエクспレスモードで作成されるボルトストアグループの設定を示します。

**表 22-1**                      エクспレスモードでのインデックス処理の設定

アイテム	説明
インデックスレベル	[完全]。アーカイブ済みアイテムのメタデータと内容をインデックス付けします。
プレビューの長さ	[128 文字]。
添付ファイルのプレビューの作成	[無効]。Enterprise Vault は添付ファイルのプレビューを作成しません。これらのプレビューは Enterprise Vault のこのリリースでは表示できません。
インデックスサブタスクの削除のタイミング	[7 日]。Enterprise Vault はタスクが完了してからこの期間が経過するインデックス処理サブタスクを削除します。タスクのすべてのサブタスクが削除されると、タスク自体が削除されます。
管理コンソールにおけるインデックスサーバーの場所	管理コンソールでは、[グループ化されていないサーバー]コンテナ内の[インデックス処理]の下に新しいインデックスサーバーが表示されます。

## Enterprise Vault 開始ウィザードでのストレージ設定について

エクспレスモードでは、Enterprise Vault 開始ウィザードにより、すべてのストレージがサーバー上にローカルに設定されます。

p.190 の「[Enterprise Vault アーカイブ用のストレージの設定について](#)」を参照してください。

ウィザードで、次の設定が行われます。

- ボルトストアグループ
- ボルトストア
- ボルトストアパーティション
- Enterprise Vault サーバーのキャッシュ
- インデックス
- ショッピングバスケット (ショッピングサービスが存在する場合)

次のいずれかを行う場合は、ストレージ設定の[カスタム]オプションを選択してください。

- リモートストレージの設定。

- 設定プログラムで指定したボルトストアとは異なるボルトストアに対する、別の SQL Server の使用。
- ボルトストアグループのフィンガープリントデータベースの構造の設定。

サイトの最初のサーバーにオープンボルトストアパーティションを作成する場合は、そのサイトの後続のサーバーで Enterprise Vault 開始ウィザードを実行するときに、オプションでストレージ設定が表示されることがあります。ただし、インデックスサービスを実行する Enterprise Vault サーバーそれぞれで、Enterprise Vault サーバーキャッシュを設定する必要があります。同様に、ショッピングサービスを実行するサーバーそれぞれで、ショッピングバスケット領域を設定する必要があります。

ボルトストアパーティションが他のサーバーで設定されているときは、Enterprise Vault のサーバーキャッシュやショッピングの場所を次のいずれかの方法で設定できます。

- [インデックス設定]と[エクспレス]モードを選択します。これにより、Enterprise Vault のサーバーキャッシュとショッピングの場所の両方を設定できます。
- [ストレージ設定]と[カスタム]モードをクリックします。これにより、サーバーキャッシュの場所を設定できます。

## エクспレスモードで指定する必要があるストレージ設定情報

エクспレスストレージ設定では、Enterprise Vault データを格納するために使うボリュームを指定する必要があります。この情報は、Enterprise Vault によって次のストレージの場所が作成されるときに使われます。

- キャッシュの場所: <volume>%EVStorage%Cache
- インデックスの場所: <volume>%EVStorage%Index
- ショッピングサービスのファイルがある場所: <volume>%EVStorage%Cache%Shopping

---

**メモ:** ウイルス対策ソフトウェアによってデータが変更される可能性があるため、ウイルスチェックアプリケーションではキャッシュおよびインデックスの場所を除外しておくことが重要です。

---

## エクспレスモードでの自動ストレージ設定

このセクションでは、ストレージ設定にエクспレスモードを選択したときに、Enterprise Vault 開始ウィザードによって自動的に設定される設定について説明します。

表 22-2 に、ウィザードのエクспレスモードで作成されるボルトストアグループの設定を示します。

表 22-2 エクспレスモードでのボルトストアグループの設定

項目	説明
名前	「Express Vault Store Group」。名前がすでに存在する場合は、名前が一意になるように番号が付加されます。たとえば、「Express Vault Store Group_1」などの名前に変更されます。
説明	ボルトストアグループ名と同じ。
フィンガープリントデータベース用 SQL Server 名	Enterprise Vault ディレクトリデータベースの設定プログラムで指定したものと同一 SQL Server。
フィンガープリントデータベース用ファイルグループのフォルダ	Enterprise Vault ディレクトリコンピュータのデフォルトのデータベースフォルダ。
フィンガープリントデータベース用ログフォルダ	Enterprise Vault ディレクトリコンピュータのデフォルトのログフォルダ。

表 22-3 に、ウィザードのエクспレスモードで作成されるボルトストアの設定を示します。

表 22-3 エクспレスモードでのボルトストアの設定

アイテム	説明
名前	「Express Vault Store」。名前がすでに存在する場合は、名前が一意になるように番号が付加されます。たとえば、「Express Vault Store_1」などの名前に変更されます。
説明	ボルトストア名と同じ。
SQL Server	Enterprise Vault ディレクトリデータベースの設定プログラムで指定したものと同一 SQL Server。
共有	「ボルトストア内で共有する」に設定します。
セーフコピー	[元のアイテムの削除]が有効です。  デフォルト動作は[はい、元の場所に保持します]に設定されています。  ジャーナルアーカイブに対しては[いいえ、アーカイブ後すぐに削除します]に設定されています。
アーカイブ使用量の限度	[サイトの設定を使用]に設定されます。

表 22-4 に、ウィザードのエクспレスモードで作成されるボルトストアパーティションの設定を示します。

表 22-4                    エクспレスモードでのボルトストアパーティションの設定

項目	説明
名前	「Express Vault Store Ptn1」。名前がすでに存在する場合は、名前が一意になるように番号が付加されます。たとえば、「Express Vault Ptn2」などの名前に変更されます。
説明	[ボルトストア <code>[Vault_store_name]</code> のパーティション]。
状態	[オープン]。
デバイスの種類	NTFS ボリューム。
データ重複排除	宛先デバイスはデータ重複排除を実行しません。
データ圧縮	宛先デバイスはデータ圧縮を実行しません。
パーティションロールオーバー	無効。
アーカイブが保全されたかどうかの確認方法	[アーカイブ属性を使用]。
コレクションファイルを使用	無効。
ファイルを移行	無効。

## Enterprise Vault 開始ウィザードでのポリシー定義について

ポリシーでは、アーカイブされる文書とアーカイブの方法を定義します。

Enterprise Vault では、ポリシーは自動的に作成されます。開始ウィザードでは、デフォルトの Enterprise Vault ポリシーを使います。エクспレスモードとカスタムモードのデフォルトポリシーは同じです。

後で必要に応じて、管理コンソールを使ってすべてのポリシー設定を変更できます。

## Enterprise Vault 開始ウィザードでの Exchange 対象設定について

Exchange Server 対象を設定することを選択した場合、開始ウィザードはネットワークで Exchange Server のインスタンスを検索します。その後、アーカイブを設定する Exchange Server コンピュータを選択できます。

選択した Exchange Server について、次の指定を行う必要があります。

- メールボックスアーカイブまたはジャーナルアーカイブ、あるいはその両方を設定するかどうかを指定します。

- メールボックスアーカイブを設定することを選択した場合は、Enterprise Vault でログオンに使用可能なサーバーにシステムメールボックスを指定する必要があります。
- ジャーナルアーカイブを設定することを選択した場合は、アーカイブするジャーナルメールボックスを指定し、各メールボックスに使用するジャーナルアーカイブを指定する必要があります。必要に応じて、ウィザードを使って新しいアーカイブを作成できます。

表 22-5 に、ウィザードのエクспレスモードで作成される Exchange プロビジョニンググループの設定を示します。

表 22-5                      エクспレスモードでの Exchange プロビジョニンググループの設定

項目	説明
プロビジョニンググループ名	「エクспレスプロビジョニンググループ」。 [ストレージ設定]を選択した場合、プロビジョニンググループはウィザードが作成する新規ボルトストアを使います。 [ストレージ設定]を選択しなかった場合、ウィザードは既存のボルトストアを使います。
プロビジョニンググループ対象	「Exchange Server 組織全体」
デスクトップポリシー	「デフォルトの Exchange デスクトップポリシー」
メールボックスポリシー	「デフォルトの Exchange メールボックスポリシー」
PST 移行ポリシー	「デフォルトの Exchange PST 移行ポリシー」
デフォルトの保持カテゴリ	「デフォルトの保持カテゴリ」

## Enterprise Vault 開始ウィザードでの Domino 対象設定について

Domino 対象を設定することを選択した場合、開始ウィザードはネットワークで Domino サーバーを検索します。その後、アーカイブを設定する Domino サーバーを選択できます。各 Domino サーバーに対して、メールボックスアーカイブまたはジャーナルアーカイブ、あるいはその両方を設定するかどうかを指定できます。開始ウィザードによって、アーカイブが適切に設定されます。

エクспレス Domino 設定を行うには、次の情報を指定する必要があります。

- ID ファイル名。Enterprise Vault は、ID ファイルを必要とするすべての Enterprise Vault 操作で ID ファイルをデフォルトの ID ファイルとして使用します。ウィザードでは、Notes データフォルダ (たとえば C:\Program Files\IBM\Notes\data) にある Domino ID ファイルが一覧に表示されます。

使う予定の ID ファイルは、ウィザードで選択できるようにデータフォルダに配置してください。

- ID ファイルのパスワード。ID ファイルのパスワードです。
- メールボックスアーカイブを設定する Domino サーバーの名前。
- ジャーナルアーカイブを設定する Domino サーバーの名前。
- Domino の対象からのアーカイブ時に使う保持カテゴリ。

表 22-6 に、ウィザードのエクспレスモードで作成される Domino プロビジョニンググループの設定を示します。

表 22-6                      エクспレスモードでの Domino プロビジョニンググループの設定

アイテム	説明
プロビジョニンググループ名	「エクспレスプロビジョニンググループ」。名前がすでに存在する場合は、名前が一意になるように番号が付加されます。たとえば、「エクспレスプロビジョニンググループ_1」などの名前に変更されます。
ボルトストア	[ストレージ設定]を選択した場合、プロビジョニンググループはウィザードが作成する新規ボルトストアを使います。[ストレージ設定]を選択しなかった場合、ウィザードは既存のボルトストアを選択します。
プロビジョニンググループ対象	'組織単位'
デスクトップポリシー	[デフォルトの Domino デスクトップポリシー]。このポリシーが利用できない場合、ウィザードはアルファベット順で利用可能な最初のポリシーを選択します。
メールボックスポリシー	「デフォルトの Lotus Domino メールボックスポリシー」。このポリシーが利用できない場合、ウィザードはアルファベット順で利用可能な最初のポリシーを選択します。
デフォルトの保持カテゴリ	「デフォルトの保持カテゴリ」



**表 22-7**                      エクスプレスモードでのボルトストアの設定

アイテム	説明
名前	ウィザードの現在の実行で作成されたボルトストア (存在する場合)。ウィザードでボルトストアが作成されなかった場合は、オープンパーティションのある最初のボルトストアが使われます。
説明	ボルトストア名に対する説明と同じ説明。
SQL Server	Enterprise Vault ディレクトリデータベースの設定プログラムで指定したものと同じ <b>SQL Server</b> 。
共有	「ボルトストア内で共有する」に設定します。
セーフコピー	[元のアイテムの削除]が有効です。  デフォルト動作は[はい、元の場所に保持します]に設定されています。  ジャーナルアーカイブに対しては[いいえ、アーカイブ後すぐに削除します]に設定されています。
アーカイブ使用量の限度	「サイトの設定を使用」に設定します。

## Enterprise Vault 開始ウィザードでのファイル対象設定について

開始ウィザードを使うと、指定したファイルサーバーに対するアーカイブを設定できます。

必要に応じて、Enterprise Vault FSA エージェントを各 Windows ファイルサーバーにインストールできます。プレースホルダショートカットが必要な場合、または FSA レポート用のデータを取得する必要がある場合は、FSA エージェントをインストールする必要があります。

## Enterprise Vault 開始ウィザードの計画

このセクションでは、エクスプレスモードで開始ウィザードを実行したときに自動的に行われる選択について説明します。エクスプレスモードの場合、開始ウィザードによる質問は多くはありません。代わりに、できるだけ多くのデフォルト設定が適用されます。必要に応じて、後で管理コンソールを使って設定を変更することができます。

[表 22-8](#) に、ウィザードのエクスプレスモードで作成するインデックス処理の設定を示します。

表 22-8 エクスプレスモードでのインデックス処理の設定

項目	ウィザードの値	管理コンソールで利用可能な値	ユーザーの選択
インデックスレベル	完全	[簡略]または[完全]	
プレビューの長さ	128 文字	128 または 1000。	
添付ファイルのプレビューの作成	無効	[無効]または[有効]	
インデックスサブタスクの削除のタイミング	7 日後	必要に応じて編集してください。	

表 22-9 に、ウィザードのエクスプレスモードで作成されるボルトストアグループの設定を示します。

表 22-9 エクスプレスモードでのボルトストアグループの設定

項目	ウィザードの値	管理コンソールで利用可能な値	ユーザーの選択
名前	「Express Vault Store Group」。名前がすでに存在する場合は、名前が一意になるように番号が付加されます。たとえば、「Express Vault Store Group_1」などの名前に変更されます。	必要に応じて編集してください。	
説明	ボルトストアグループ名と同じ。	必要に応じて編集してください。	
フィンガープリントデータベース用 SQL Server	Enterprise Vault ディレクトリデータベースの設定プログラムで指定したのと同じ SQL Server。	変更できません。	
フィンガープリントデータベース用ファイルグループのフォルダ	Enterprise Vault ディレクトリコンピュータのデフォルトのデータベースフォルダ。	変更できません。	

項目	ウィザードの値	管理コンソールで利用可能な値	ユーザーの選択
フィンガープリントデータベース用ログフォルダ	Enterprise Vault ディレクトリコンピュータのデフォルトのログフォルダ。	変更できません。	

表 22-10 に、ウィザードのエクスプレスモードで作成されるボルトストアの設定を示します。

**表 22-10** エクスプレスモードでのボルトストアの設定

項目	ウィザードの値	管理コンソールで利用可能な値	ユーザーの選択
名前	「Express Vault Store」。名前がすでに存在する場合は、名前が一意になるように番号が付加されます。たとえば、「Express Vault Store_1」などの名前に変更されます。	必要に応じて編集してください。	
説明	ボルトストア名と同じ。	必要に応じて編集してください。	
SQL Server	Enterprise Vault ディレクトリデータベースの設定プログラムで指定したのと同じ SQL Server。	別の SQL Server に変更できます。	
共有	[ボルトストア内で共有する]。	[共有しない]、[ボルトストア内で共有する]、[グループ内で共有する]。	

項目	ウィザードの値	管理コンソールで利用可能な値	ユーザーの選択
セーフコピー	<p>セーフコピーの場所と削除を制御します。</p> <p>[元のアイテムの削除]は有効です。</p> <p>[デフォルトの動作]は[はい、元の場所に保持します]に設定されます。</p> <p>[ジャーナルアーカイブ用]は[いいえ、アーカイブ後すぐに削除します]に設定されます。</p>	<p>[元のアイテムの削除]は有効と無効を切り替えることができます。</p> <p>[デフォルトの動作]には次の設定があります。</p> <ul style="list-style-type: none"> <li>■ いいえ、アーカイブ後すぐに削除します</li> <li>■ はい、元の場所に保持します</li> <li>■ はい、ストレージキューに保持します</li> </ul> <p>[ジャーナルアーカイブ用]には次の設定があります。</p> <ul style="list-style-type: none"> <li>■ いいえ、アーカイブ後すぐに削除します</li> <li>■ はい、元の場所に保持します</li> <li>■ はい、ストレージキューに保持します</li> </ul>	
アーカイブ使用量の限度	[サイトの設定を使用]。	[無効]、[有効]、[サイトの設定を使用]。	

表 22-11 に、ウィザードのエクспレスモードで作成されるボルトストアパーティションの設定を示します。

表 22-11 エクスプレスモードでのボルトストアパーティションの設定

項目	ウィザードの値	管理コンソールで利用可能な値	ユーザーの選択
名前	「Express Vault Store Ptn1」。名前がすでに存在する場合は、名前が一意になるように番号が付加されます。たとえば、「Express Vault Ptn2」などの名前に変更されます。	必要に応じて編集してください。	
説明	[ボルトストア [Vault_store_name] のパーティション]。	必要に応じて編集してください。	
状態	[オープン]。	[クローズ]、[オープン]、[準備完了]。	
デバイスの種類	NTFS ボリューム。	変更できません。	
データ重複排除	宛先デバイスはデータ重複排除を実行しません。	[デバイスはデータの重複排除を実行する]、 [宛先デバイスはデータ重複排除を実行しない]	
データ圧縮	宛先デバイスはデータ圧縮を実行しません。	[デバイスはデータの圧縮を実行する]、[宛先デバイスはデータ圧縮を実行しない]	
パーティションロールオーバー	無効。	[無効]、[容量に基づいて有効化]、[時刻に基づいて有効化]、[時刻または容量に基づいて有効化]。	
アーカイブが保全されたかどうかの確認方法	[アーカイブ属性を使用]。	[アーカイブ属性を使用]、[トリガファイルを確認]。	
コレクションファイルを使用	無効。	[コレクションファイルを使用]、[コレクションファイルを使用しない]	
ファイルを移行	無効。	[有効]、[無効]。	

表 22-12 に、ウィザードのエキスプレスモードで作成される Exchange プロビジョニンググループの設定を示します。

表 22-12 エクスプレスモードでの Exchange プロビジョニンググループの設定

項目	ウィザードの値	管理コンソールで利用可能な値	ユーザーの選択
プロビジョニンググループ名	「エキスプレスプロビジョニンググループ」。 [ストレージ設定]を選択した場合、プロビジョニンググループはウィザードが作成する新規ボルトストアを使います。 [ストレージ設定]を選択しなかった場合、ウィザードは既存のボルトストアを使います。	必要に応じて編集してください。	
プロビジョニンググループ対象	「Exchange 組織全体」	[Windows グループ]、 [Windows ユーザー]、 [配布グループ]、 [組織単位]、 [LDAP クエリー]、 [Exchange 組織全体]。	
デスクトップポリシー	「デフォルトの Exchange デスクトップポリシー」	必要に応じて編集してください。	
メールボックスポリシー	「デフォルトの Exchange メールボックスポリシー」	必要に応じて編集してください。	
PST 移行ポリシー	「デフォルトの Exchange PST 移行ポリシー」	必要に応じて編集してください。	
デフォルトの保持カテゴリ	「デフォルトの保持カテゴリ」	必要に応じて編集してください。	

表 22-13 に、ウィザードのエキスプレスモードで作成される Domino プロビジョニンググループの設定を示します。

表 22-13 エクスプレスモードでの Domino プロビジョニンググループの設定

項目	ウィザードの値	管理コンソールで利用可能な値	ユーザーの選択
プロビジョニンググループ名	「エクスプレスプロビジョニンググループ」。名前がすでに存在する場合は、名前が一意になるように番号が付加されます。たとえば、「エクスプレスプロビジョニンググループ_1」などの名前に変更されます。	必要に応じて編集してください。	
ボルトストア	[ストレージ設定]を選択した場合、プロビジョニンググループはウィザードが作成する新規ボルトストアを使います。[ストレージ設定]を選択しなかった場合、ウィザードは既存のボルトストアを選択します。	必要に応じて編集してください。	
プロビジョニンググループ対象	「組織単位」	[ディレクトリグループ]、[メールボックス]、[組織単位]、[社内階層]。	
デスクトップポリシー	「デフォルトの Domino デスクトップポリシー」。このポリシーが利用できない場合、ウィザードはアルファベット順で利用可能な最初のポリシーを選択します。	必要に応じて編集してください。	
メールボックスポリシー	「デフォルトの Lotus Domino メールボックスポリシー」。このポリシーが利用できない場合、ウィザードはアルファベット順で利用可能な最初のポリシーを選択します。	必要に応じて編集してください。	

項目	ウィザードの値	管理コンソールで利用可能な値	ユーザーの選択
デフォルトの保持カテゴリ	「デフォルトの保持カテゴリ」	必要に応じて編集してください。	



# Enterprise Vault Operations Manager の設定

この章では以下の項目について説明しています。

- [Enterprise Vault Operations Manager 設定ユーティリティを実行するタイミング](#)
- [Enterprise Vault Operations Manager 設定ユーティリティの実行](#)
- [Enterprise Vault Operations Manager へのアクセス](#)
- [Enterprise Vault Operations Manager のトラブルシューティング](#)

## Enterprise Vault Operations Manager 設定ユーティリティを実行するタイミング

Enterprise Vault Operations Manager 設定ユーティリティは、Operations Manager をサーバーにインストールした後に実行します。ただし、先に Enterprise Vault 設定ウィザードを使ってサーバーを正常に設定する必要があります。

設定が何らかの理由で失敗して設定を繰り返す必要がある場合は、Operations Manager 設定ユーティリティを再実行できます。

また、監視対象のユーザーアカウントの詳細を変更する必要がある場合も、ユーティリティを再実行できます。この場合は、Operations Manager がインストールされているすべてのサーバーでユーティリティを再実行してください。

---

**メモ:** Operations Manager が設定されているサーバーの FIPS 対応アルゴリズムの Windows ポリシー設定を有効または無効にした場合は、Operations Manager の設定ユーティリティを再実行する必要があります。

---

## Enterprise Vault Operations Manager 設定ユーティリティの実行

Operations Manager の初回設定を行ったり、設定を更新する (たとえば、監視対象のユーザーアカウントの詳細を変更する) には、Operations Manager 設定ユーティリティを実行します。

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

- 1 ボルトサービスアカウントでログインします。
- 2 Operations Manager 設定ユーティリティを起動します。
- 3 Operations Manager を実行する作成済みの監視対象のユーザーアカウントの詳細を入力します。  
  
監視対象のユーザーアカウントの Active Directory ドメイン、ユーザー名、パスワードを入力します。
- 4 [設定]をクリックしてユーティリティを実行します。  
  
ユーティリティによって必要な権限がアカウントに付与され、ユーザーが Enterprise Vault ディレクトリデータベースに監視対象ユーザーとして追加されます。
- 5 ユーティリティが完了したら、表示されたダイアログボックスで[OK]をクリックしてユーティリティを終了します。

---

**メモ:** このユーティリティを実行して監視対象のユーザーアカウントの詳細を更新した場合は、Operations Manager がインストールされているその他のすべての Enterprise Vault サーバーでこのユーティリティを再実行してください。

---

正常に設定されたことを確認するため、Operations Manager にアクセスできるかどうかを試してください。

## Enterprise Vault Operations Manager へのアクセス

Enterprise Vault サイト内の 1 台以上の Enterprise Vault サーバーに Enterprise Vault Operations Manager Web Application がインストールされている場合は、そのアプリケーションを使ってサイトの Enterprise Vault サーバーを監視できます。

Operations Manager を設定したら、アクセスして設定が正しいことを確認します。

## Enterprise Vault Operations Manager にアクセスする方法

- 1 Internet Explorer で、URL を次の形式で入力します。

`https://host_ipaddress/MonitoringWebApp/default.aspx`

Enterprise Vault 12.3 以降の新規インストールで使用するプロトコルは、デフォルトで HTTPS です。Enterprise Vault を 12.3 より前のバージョンからアップグレードした場合、使用されるプロトコルは、IIS での Enterprise Vault 仮想ディレクトリの設定方法に応じて決まります。

`host_ipaddress` は Enterprise Vault Operations Manager Web アプリケーション機能がインストールされている Enterprise Vault サーバーのホストコンピュータの IP アドレスです。

代わりに、Operations Manager がインストールされているコンピュータからアクセスする場合は、`localhost` を指定できます。この場合、この後の手順は必要ありません。

`https://localhost/MonitoringWebApp/default.aspx`

- 2 [ <IP アドレス> に接続 ] ダイアログボックスで、ホストコンピュータのドメイン内のアカウントのユーザー名とパスワードを入力します (`domain¥account` の形式を使います)。次に [OK] をクリックします。

---

**メモ:** Operations Manager にアクセスするために、ボルトサービスアカウント以外のユーザーに適切な役割を割り当てる必要があります。ユーザーは、Operations Manager のタブとテーブルのうち、割り当てられた役割で利用可能なもののみを表示できます。

詳しくは『管理者ガイド』の「役割ベースの管理」を参照してください。

---

ユーザー信用証明が有効であれば、Operations Manager にサイトの [概略] ページが表示されます。

# Enterprise Vault Operations Manager のトラブルシューティング

Enterprise Vault Operations Manager にアクセスしようとしたときにエラーページが表示された場合は、以下の操作を実行してから、再度アプリケーションにアクセスします。

- すべてのインストール前の手順を実行したことを確認します。  
p.54 の「[Operations Manager の追加必要条件について](#)」を参照してください。
- IIS がロックダウンされていないことを確認します。
- IIS のデフォルトの Web サイトで、統合 Windows 認証が有効になっていることを確認してから、IIS を再起動します。

問題が解決しない場合は、次の Veritas サポート Web サイトのテクニカルノートを参照してください。

<https://www.veritas.com/docs/100018176>

このテクニカルノートには、Operations Manager のインストールと使用に関する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。

# アーカイブディスカバリ検索サービスの設定

この章では以下の項目について説明しています。

- [開始する前の確認事項](#)
- [アーカイブディスカバリ検索サービスの設定ウィザードの実行](#)
- [アーカイブディスカバリ検索サービスの要求エンドポイントの手動設定](#)
- [アーカイブディスカバリ検索サービスの結果エンドポイントの手動設定](#)

## 開始する前の確認事項

アーカイブディスカバリ検索サービスを使用すると、Enterprise Vault インストール内のすべてのアーカイブの検索をサードパーティのクライアントアプリケーションで作成して実行できます。

先に進む前に、以下のことを確認します。

- アーカイブディスカバリ検索サービスを使用する場合のすべての前提条件を満たしている  
p.112 の「[アーカイブディスカバリ検索サービスの追加の必要条件について](#)」を参照してください。  
これは、IIS で SSL を設定する上で特に重要です。また、Windows Communication Foundation (WCF) のアクティブ化機能が Enterprise Vault サーバーで有効になっていることを確認する必要があります。
- サイトの少なくとも 1 台の Enterprise Vault サーバーにアーカイブディスカバリ検索サービスをインストールしている  
p.119 の「[Enterprise Vault のインストールについて](#)」を参照してください。

# アーカイブディスカバリ検索サービスの設定ウィザードの実行

アーカイブディスカバリ検索サービスの設定ウィザードを実行して、サービスの初期設定を行うか、既存の設定を更新できます。ウィザードでは次の操作を実行できます。

- 検索メタデータ情報をアーカイブする **SQL Server** のデータベースを作成します。この情報は **Enterprise Vault** サイト、インデックスサービス、ボルトストア、ボルト、検索を行うインデックスボリューム、その検索の詳細を含んでいます。また、インデックスボリュームのヒット数や検索結果の場所など、検索結果の情報も含んでいます。
- 検索結果を **XML** 形式で格納するフォルダを **Enterprise Vault** インデックスサーバーごとに指定します。  
検索結果には、重要な情報が含まれることがあります。最適なセキュリティのために、ボルトサービスアカウントのみがアクセスできるフォルダを指定することを推奨します。
- クライアント検索アプリケーションが検索要求を送信できる要求エンドポイントを設定します。
- **SQL Server** コンピュータから別の **SQL Server** コンピュータにアーカイブディスカバリ検索サービスのデータベースを移動すると、変更が加えられたことが **Enterprise Vault** ディレクトリデータベースに通知されます。

---

**メモ:** 移動先コンピュータの **SQL Server** は、アーカイブディスカバリ検索サービスのデータベースを作成した **SQL Server** より新しいバージョンである必要があります。たとえば、**SQL Server 2012** を実行しているコンピュータに、**SQL Server 2014** のデータベースを移動することはできません。

ボルトサービスアカウントには、移動先 **SQL Server** コンピュータの **dbcreator** の役割を設定する必要があります。

---

## アーカイブディスカバリ検索サービスの設定ウィザードを実行する方法

- 1 ボルトサービスアカウントとして、アーカイブディスカバリ検索サービスコンポーネントをインストールした **Enterprise Vault** サーバーにログオンします。
- 2 次のいずれかの操作を行います。
  - **Vault Administration Console** の左ペインで、[アーカイブディスカバリ検索サービス]を右クリックし、[設定]をクリックします。
  - **Windows** エクスプローラで **Enterprise Vault** プログラムフォルダ (C:\¥Program Files (x86)\¥Enterprise Vault など) にナビゲートして、**DSSConfiguration.exe** をダブルクリックします。

アーカイブディスカバリ検索サービスの設定ウィザードが開始されます。

- 3 ウィザードの最初のページが表示されたら、[次へ]をクリックして次のページに進みます。
- 4 実行する操作を選択して、画面に表示される指示に従います。  
  
ウィザードで利用できるオンラインヘルプで、各手順を完了する方法を確認できます。
- 5 要求エンドポイントの設定後、選択した Enterprise Vault サーバー上で Enterprise Vault 管理者サービスを再起動します。

## アーカイブディスカバリ検索サービスの要求エンドポイントの手動設定

アーカイブディスカバリ検索サービスの設定ウィザードでエンドポイントにデフォルトポート番号を使用するように選択すると、要求エンドポイントを自動的に設定できます。自動設定を行いたくない場合は、エンドポイントを手動で設定する必要があります。

### アーカイブディスカバリ検索サービスの要求エンドポイントを手動で設定する方法

- 1 IIS (Internet Information Services) マネージャを起動します。
- 2 要求エンドポイントのアプリケーションプールを作成するためには、次の手順を実行します。
  - IIS マネージャの左側のペインでサーバーノードを展開し、[アプリケーションプール]をクリックします。
  - [アプリケーションプール]ページの右側にある[処理]ペインで[アプリケーションプールの追加]をクリックします。
  - [アプリケーションプールの追加]ダイアログボックスで次の項目を設定し、[OK]をクリックします。

Name	EVDSSRequestAppPool
[.NET CLR バージョン]	.NET CLR Version v4.0. <i>nnnnn</i>
[マネージパイプラインモード]	統合
[アプリケーションプールを直ち 選択されている に開始する]	

- 3 IIS マネージャの左側のペインでサーバーノードを展開し、[サイト]ノードを展開します。
- 4 [Default Web Site]ノードを右クリックし、[アプリケーションの追加]をクリックします。

- 5 [アプリケーションの追加]ダイアログボックスで次の項目を設定し、[OK]をクリックします。

[エイリアス]	DSSRequestEndPoint
[アプリケーションプール]	EVDSSRequestAppPool
[物理パス]	DSS_installation_folder¥RequestEndPoint次に例を示します。  C:¥Program Files (x86)¥Enterprise Vault¥RequestEndPoint

- 6 IIS マネージャの左側のペインで[DSSRequestEndPoint]ノードを右クリックし、[機能/コンテンツ ビューに切り替え]をクリックします。
- 7 [機能ビュー]ペインで[認証]をダブルクリックします。
- 8 [認証]ページで、[匿名認証]を除くすべての認証モードが無効になっていることを確認します。[匿名認証]は有効にする必要があります。
- 9 [機能ビュー]ペインで[SSL 設定]をダブルクリックします。
- 10 [SSL 設定]ペインで、[SSL が必要]を選択して[クライアント証明書]を[同意]に設定します。
- 11 コンテンツビューに切り替えて、DSSRequestEndPoint ノードを表示します。
- 12 [/DSSRequestEndPoint コンテンツ]ページで RequestService.svc を右クリックし、[参照]をクリックします。
- 13 エラーが発生しないこと、およびサービスを正常に起動できることを確認します。

## アーカイブディスカバリ検索サービスの結果エンドポイントの手動設定

要求エンドポイントを手動で設定できるのと同様に、結果エンドポイントも手動で設定できます。

### アーカイブディスカバリ検索サービスの結果エンドポイントを手動で設定する方法

- 1 IIS (Internet Information Services) マネージャを起動します。
- 2 要求エンドポイントのアプリケーションプールを作成するためには、次の手順を実行します。
  - IIS マネージャの左側のペインでサーバーノードを展開し、[アプリケーションプール]をクリックします。



- [アプリケーションプール] ページの右側にある[処理] ペインで[アプリケーションプールの追加] をクリックします。
- [アプリケーションプールの追加] ダイアログボックスで次の項目を設定し、[OK] をクリックします。

Name	EVDSSResultAppPool
[.NET CLR バージョン]	.NET CLR Version v4.0. <i>nnnnn</i>
[マネージパイプライン モード]	統合
[アプリケーションプールを直ち に開始する]	選択されている

- 3 IIS マネージャの左側のペインでサーバーノードを展開し、[サイト] ノードを展開します。
- 4 [Default Web Site] ノードを右クリックし、[アプリケーションの追加] をクリックします。
- 5 [アプリケーションの追加] ダイアログボックスで次の項目を設定し、[OK] をクリックします。

[エイリアス]	DSSResultEndPoint
[アプリケーションプール]	EVDSSResultAppPool
[物理パス]	<i>DSS_installation_folder</i> ¥ResultEndpoint次に例を示します。  C:¥Program Files (x86)¥Enterprise Vault¥ResultEndpoint

- 6 IIS マネージャの左側のペインで[DSSResultEndPoint] ノードを右クリックし、[機能/コンテンツ ビューに切り替え] をクリックします。
- 7 [機能ビュー] ペインで[認証] をダブルクリックします。
- 8 [認証] ページで、[Windows 認証] を除くすべての認証モードが無効になっていることを確認します。[Windows 認証] は有効にする必要があります。
- 9 [機能ビュー] ペインで[SSL 設定] をダブルクリックします。
- 10 [SSL 設定] ペインで、[SSL が必要] を選択して[クライアント証明書] を[同意] に設定します。
- 11 [コンテンツビュー] に切り替えて、DSSResultEndPoint ノードを表示します。

- 12 [/DSSResultEndPoint コンテンツ] ページで `ResultService.svc` を右クリックし、  
[参照] をクリックします。
- 13 エラーが発生しないこと、およびサービスを正常に起動できることを確認します。

# Enterprise Vault の初期設定

- [第25章 Enterprise Vault の初期設定](#)
- [第26章 ストレージの設定](#)
- [第27章 インデックスの場所の追加](#)
- [第28章 インデックスサーバーグループの設定](#)
- [第29章 サイトのデフォルト設定のレビュー](#)
- [第30章 Enterprise Vault 検索の設定](#)
- [第31章 メタデータストアの管理](#)

# Enterprise Vault の初期設定

この章では以下の項目について説明しています。

- [ライセンスキー](#)
- [Enterprise Vault 管理コンソールの使用](#)
- [管理コンソールを使った Enterprise Vault コアサービスの追加](#)
- [Enterprise Vault 保持カテゴリの作成](#)
- [Enterprise Vault が制限されている場合やインターネットに接続していない場合のパフォーマンスの問題](#)

## ライセンスキー

設定ウィザードの最後に、Enterprise Vault サービスを起動するかどうかを尋ねられます。これらのサービスは、適切なライセンスキーをインストールするまで起動されません。

## Enterprise Vault 管理コンソールの使用

Enterprise Vault 管理コンソールは、Microsoft Management Console (MMC) のスナップインです。MMC では、管理ツールすべてに同じようなルックアンドフィールを持たせるための共通のフレームワークが提供されます。特定の管理者が必要とする的確な機能が含まれるように、MMC のスナップインをカスタマイズできます。

管理コンソールを使うと、Enterprise Vault サイト、サービス、アーカイブタスク、ポリシー、対象を管理できます。

複数のユーザーが同時に別々の管理コンソールを使って Enterprise Vault を変更する場合、あるユーザーによって変更された内容が必ずしも他のコンソールにも表示されるわ

けではありません。Enterprise Vault を管理する場合は、複数のコンソールを同時に使わないことを推奨します。複数のコンソールを使う場合は、変更を行う前に F5 キーを押して管理コンソールの表示を更新します。

## Enterprise Vault 管理コンソールの起動

管理コンソールを初めて使う場合には、ボルトサービスアカウントとしてログインします。他の管理者に役割を割り当て、管理コンソールを使って必要な Enterprise Vault 管理タスクを実行できるようにします。

### Enterprise Vault 管理コンソールを起動する方法

- 1 [アプリ]画面で[Enterprise Vault]>[管理コンソール]を選択します。
- 2 [接続]ダイアログボックスで、ディレクトリサービスを実行している Enterprise Vault サイトの任意のサーバー名または IP アドレスを入力します。IPv4 または IPv6 形式で IP アドレスを入力できます。

初めて管理コンソールを開く際、このリリースでの新機能を説明するダイアログボックスが表示されます。また、Enterprise Vault の機能強化を行うための招待状が表示される場合もあります。この機能は Veritas の品質を改善する上で役立ちます。

管理コンソールの左側のペインには、Enterprise Vault サイトを構成するコンポーネントの階層が表示されます。右側のペインには、階層で選択した内容が表示されます。

### ヘルプを表示する方法

- ◆ 次のいずれかの操作を行います。
  - Enterprise Vault のオンラインヘルプにアクセスするには、[ヘルプ]、[Enterprise Vault のヘルプ]をクリックします。このヘルプには Enterprise Vault のマニュアルが含まれています。
  - MMC の詳細を参照するには、MMC ウィンドウで、[ヘルプ]、[トピックの検索]をクリックします。MMC のヘルプが表示されます。

### 画面を更新する方法

- ◆ F5 キーを押すと、いつでも強制的に画面を更新できます。

## Enterprise Vault 管理コンソールの管理ロールについて

Enterprise Vault は、アクセス管理者の制御に使うことができる次のメカニズムを管理コンソールに提供します。

- 役割ベースの管理。多くの管理タスクでは、ボルトサービスアカウントに関連付けられたすべての権限が必要なわけではありません。役割ベースの管理では、個々の Enterprise Vault 管理者に、自分の管理タスクを実行するのに必要な権限のみを付与できます。

ユーザーは、担当範囲に一致する役割を個人またはグループに割り当てて、その役割に含まれるタスクを実行できます。権限は個々の管理者ではなく役割に関連付けられているため、各管理者の権限を編集せずに役割の権限を制御できます。

- 管理者権限。管理コンソールツリーの次のコンテナに対して、アクセス権を付与または拒否できます。
  - ファイルサーバー
  - Exchange Server
  - SharePoint 仮想サーバー
  - Enterprise Vault サーバー

役割の割り当て、管理者権限の使用、またはその両方によりアクセスを制御できます。

Enterprise Vault の初回インストール時には、ボルトサービスアカウントでのみ管理コンソールにアクセスできます。役割の割り当てによって管理者が実行できるタスクを制限することも、管理者権限を使って管理者に対して特定の管理コンソールコンテナの管理を制限することでアクセス制限を強化することもできます。

役割ベースの管理の設定手順については、『管理者ガイド』を参照してください。

## 管理コンソールを使った Enterprise Vault コアサービスの追加

管理コンソールを使って、次の Enterprise Vault コアサービスを追加します。

- インデックスサービス
- ストレージサービス
- ショッピングサービス
- タスク制御サービス

サービスの作成時に、ボルトサービスアカウントのパスワードの入力を求めるメッセージが表示されることがあります。

インデックスの保存場所が、ボルトサービスアカウントが書き込みアクセス権を持つアクセス可能なデバイス上にあることを確認します。

**Exchange** メールボックスアーカイブタスクまたはファイルシステムアーカイブタスクなどのアーカイブタスクを追加すると、これらのタスクはタスク制御サービスの制御下で実行されます。タスク制御サービスを停止すると、このサービスの制御下で実行されているタスクもすべて停止されます。

これらの各サービスは、同じ手順で追加できます。

### 管理コンソールを使って Enterprise Vault コアサービスを追加する方法

- 1 左側のペインで、[Enterprise Vault サーバー]コンテナが表示されるまで Enterprise Vault サイト階層を展開します。
- 2 [Enterprise Vault サーバー]コンテナを展開します。
- 3 サービスを追加するコンピュータを展開します。
- 4 [サービス]を右クリックし、ショートカットメニューの[新規作成]、[サービス]の順にクリックします。  
[サービスの追加]ダイアログボックスが表示され、追加できるサービスが一覧表示されます。
- 5 追加するサービスをクリックします。
- 6 [追加]をクリックします。

## Enterprise Vault 保持カテゴリの作成

計画時に、Enterprise Vault で事前に定義されている保持カテゴリより多くの保持カテゴリが必要であると判断することがあります。その場合は、独自の保持カテゴリを作成する必要があります。代わりに、必要に応じて事前定義済みの保持カテゴリを編集することもできます。

Exchange 管理フォルダからアーカイブするように Enterprise Vault を設定すると、管理フォルダの保持カテゴリに管理対象コンテンツの設定を自動的に同期できます。Enterprise Vault は、管理フォルダの保持カテゴリを自動的に作成します。詳しくは『管理者ガイド』を参照してください。

### 新しい保持カテゴリを作成する方法

- 1 管理コンソールの左ペインで、[ポリシー]が表示されるまでボルトサイト階層を展開します。
- 2 [ポリシー]、[保存と分類]の順に展開します。
- 3 [カテゴリ]を右クリックし、ショートカットメニューで[新規]、[保持カテゴリ]の順に選択します。  
新規保持カテゴリウィザードが起動します。
- 4 ウィザードに従って操作します。

## Enterprise Vault 保持カテゴリのプロパティについて

アイテムがアーカイブされるときに Enterprise Vault 保持カテゴリを割り当てることによって、格納されているアイテムを分類できます。このカテゴリ分類によって、カテゴリ別に検索できるため、アイテムの取り込みが簡単になります。保持カテゴリは、アイテムを保持する最小の期間も決定します。

Exchange Server のアーカイブでは、ユーザーはアーカイブ時にアイテムが適切な保持カテゴリで格納されるように、メールボックスフォルダまたはアイテムの保持カテゴリを選択できます。

後で保持カテゴリを修正すると、変更は過去にさかのぼって適用されます。たとえば、保持期間が 5 年の「Customer Accounts」保持カテゴリがあり、その保持期間を 10 年に変更した場合、「Customer Accounts」保持カテゴリによってすでにアーカイブされているアイテムは、10 年以上保持されます。

Enterprise Vault では、自動的に期限切れのアイテムを削除できます。詳しくは『管理者ガイド』を参照してください。

次の点に注意してください。

- 保持カテゴリを削除することはできません。必要に応じて名前を変更したり、ユーザーに対して非表示にすることはできます。
- 保持フォルダや分類機能など、Enterprise Vault の特定の機能は、アーカイブ済みアイテムの保持カテゴリを更新し、カテゴリがユーザーによって変更されないようにすることができます。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。

保持カテゴリには次のプロパティがあります。

名前	必要に応じて保持カテゴリ名を修正できます。新しい名前がすぐに使用されます。
説明	(必須) これは保持カテゴリの説明です。ユーザーにわかりやすい説明を入力します。
このカテゴリをユーザーに非表示	<p>新しいアイテムのアーカイブ時にユーザーがこのカテゴリを使えないようにする場合に、チェックマークを付けます。すでにアーカイブされているアイテムを検索する場合は該当のカテゴリを利用できます。</p> <p>Enterprise Vault では、サイトのデフォルトの保持カテゴリを非表示にできません。サイトのデフォルトの保持カテゴリを非表示にすると、Enterprise Vault によって自動的に別の保持カテゴリが選択され、サイトのデフォルトになります。</p>
この保持カテゴリをロック	意図しない変更を回避するには、このオプションにチェックマークを付けて、すべての保持カテゴリ設定をロックします。
管理用のメモ	メモ用。必要に応じてこのテキストを編集します。このテキストは Enterprise Vault 管理者のみが表示できます。



## 保持

Enterprise Vault が保持カテゴリを割り当てたアイテムを保持する期間を選択します。オプションは次のとおりです。

- 期間。アイテムを保持する最小期間を指定する場合に選択します。メールメッセージの場合は、メッセージが受信されてからの期間です。文書の場合は、文書の最終更新日以降の期間です。
- 固定有効期限。アイテムを期限切れにする期日を指定する場合に選択します。次の点に注意してください。
  - 固定の有効期限を指定した保持カテゴリの詳細を Microsoft Outlook で正しく表示するには、12.2 以降のバージョンの Enterprise Vault Outlook アドインが必要です。
  - WORM またはストリーマストレージデバイスにアーカイブすると、Enterprise Vault はアクセス日 (有効期限を表す) として固定の有効期限に関連アイテムに適用します。同様に、Enterprise Vault から Centera の保持期間を設定している Centera デバイスにアーカイブする場合、Enterprise Vault で Centera クリップへ適用される保持期間は固定の有効期限に基づきます。
- アイテムを無期限で保持。アイテムを無期限で保持する場合に選択します。

このカテゴリ内の期限切れアイテムの削除を禁止

保持カテゴリ中のアイテムの保持期限が切れる際にアイテムを自動削除しない場合はこのオプションを選択します。

この設定は、アーカイブに格納されているアイテムにのみ影響します。アーカイブ対象サーバーに存在しているアイテムには影響しません。

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

ユーザーがこの保持カテゴリの項目を削除することを防ぐには、このオプションを選択します。

この設定は、アーカイブに格納されているアイテムにのみ影響します。アーカイブ対象サーバーに存在しているアイテムには影響しません。

## 保持計画について

保持計画では、他の多数の設定に保持カテゴリを関連付けて、それらのすべてを 1 つ以上のアーカイブに適用できます。保持計画で適用できる追加設定には次の内容が含まれます。

- 分類ポリシー
- 1 つ以上の保持フォルダ
- 期限切れアイテムの破棄条件

保持計画をアーカイブに適用すると、アーカイブ内のアイテムの保持期間をより高度に制御できます。特に、保持計画では **Enterprise Vault** でアイテムをアーカイブするときに自動的に指定されたのとは異なる保持期間を指定することによって、アーカイブ済みアイテムを破棄できます。たとえば、**Enterprise Vault** で最初に割り当てられた保持カテゴリではなく、保持計画に関連付けられた保持カテゴリに従って、影響を受けるアイテムが **Enterprise Vault** によって期限切れになるように保持計画を構成できます。

## 分類ポリシーについて

保持計画で分類ポリシーを設定することを選択する場合、保持計画を割り当てるアーカイブに対して、分類ポリシーで次について決めます。

- **Enterprise Vault** がインデックスを付けてアーカイブすると同時にアイテムを分類するかどうか。Enterprise Vault によって分類タグが適用されると、**Compliance Accelerator** や **Discovery Accelerator** などのアプリケーションのユーザーは分類タグを使って、検索やレビューを実行するときにアイテムをフィルタ処理できます。
- ユーザーが手動でアイテムを削除する、または **Enterprise Vault** が自動的にそれらを期限切れにするときに、アイテムを分類するかどうか。

分類機能について詳しくは、『分類』ガイドを参照してください。

## 保持フォルダについて

---

**メモ:** ここに記載されている保持フォルダは、**Enterprise Vault** マニュアルの他の場所に記載されている **Domino** とファイルシステムアーカイブの保持フォルダとは異なります。**Domino** とファイルシステムアーカイブの保持フォルダは、**Enterprise Vault** がアイテムをアーカイブするアーカイブ元に作成しますが、ここに記載されている保持フォルダはアーカイブ自体の中に作成します。

このリリースでは、**Exchange** アーカイブとインターネットメールアーカイブ内にのみ、この 2 番目の種類の保持フォルダを作成できます。

---

保持フォルダ機能を使用すると、ユーザーのアーカイブ内のアーカイブ済みアイテムの保持と有効期限をフォルダレベルで管理できます。この機能を使用すると、これらのアーカイブに単一の保持フォルダまたはフォルダの階層を作成できます。各保持フォルダに設定された属性によって、**Enterprise Vault** がこのフォルダ内のアイテムに適用する保持および有効期限設定が決まります。たとえば、保持期間が 1 年の保持カテゴリをアイテムに適用するフォルダを作成して、**Enterprise Vault** がこれらのアイテムに以前に適用した保持カテゴリを上書きできます。さらに、保持フォルダのサブフォルダが保持フォルダの保持および有効期限設定を継承するのか、それとも独自の設定を持つのかを選択できます。

保持フォルダに対して定義する保持および有効期限設定は、関連する保持計画やサイトレベルなど、別の場所の **Enterprise Vault** で定義する設定を上書きします。

ユーザーは仮想ボルト、Enterprise Vault 検索、IMAP などの機能を使って、保持フォルダにアクセスしたり、保持フォルダとの間でアイテムを移動したりできます。

## 保持計画の作成

保持計画に割り当てる保持カテゴリや分類ポリシーを定義した後のみ、保持計画を作成することを推奨します。

保持計画を作成して 1 つ以上のアーカイブを適用した後に、保持計画を修正することができます。また、それらのアーカイブと計画の関連付けを解除したり、別の計画を割り当てたりすることもできます。

### 保持計画の作成方法

- 1 Enterprise Vault 管理コンソールの左ペインで、[ポリシー]が表示されるまでツリー表示を展開します。
- 2 [ポリシー]コンテナ、[保持と分類]コンテナの順に展開します。
- 3 [計画]を右クリックして、[新規]をポイントして[保持計画]をクリックします。  
[新しい保持計画]ウィザードが表示されます。
- 4 ウィザードのページの手順に従って次のように入力します。
  - 新しい保持計画の名前。名前は一意である必要があり、最大 40 個の英数字記号とスペース文字を含めることができます。
  - 計画の説明。説明は、最大 127 個の英数字、スペース、または特殊文字を含めることができます。
  - 保持計画と関連付ける保持カテゴリ。適当な保持カテゴリが存在しない場合は、ウィザードで作成するためのオプションが表示されます。
  - 必要に応じて、Enterprise Vault で保持計画で処理するアイテムを分類する分類機能を使用できるようにするかどうかを指定します。アイテムを分類することを選択する場合、必要な分類ポリシーを選択する必要もあります。
  - 必要に応じて、計画が適用されるアーカイブに保持フォルダを作成するかどうかを指定します。
  - 影響を受けるアイテムに割り当てる有効期限設定。

## Enterprise Vault が制限されている場合やインターネットに接続していない場合のパフォーマンスの問題

Enterprise Vault のファイルはデジタル署名されます。デフォルトでは、これらのファイルがアクセスされると、Windows はオンラインでファイルのデジタル証明書が失効している

かどうかを検査します。Enterprise Vault がインターネットに接続していない場合や接続速度が遅い場合は、次のタイミングで遅延が起きる可能性があります。

- Enterprise Vault をインストールするとき
- 管理コンソールを起動するとき
- ユーザーが Web ブラウザを使ってアーカイブを参照し、検索するとき

これらの遅延が発生した場合には、Windows による失効したデジタル証明書の検査を停止できます。これは、プロセス単位または特定のユーザーアカウントの下で動作するすべてのプロセスで実行できます。

## 個々のプロセスで証明書の失効確認をオフにする

Enterprise Vault サーバーが将来インターネットにアクセスする場合には、下で作成する設定ファイルを削除することにより証明書の失効確認を元に戻せます。

個々のプロセスで証明書の失効確認をオフにするには

- 1 Windows ノートパッドなどのプレーンテキストエディタを使って、次の行を含む設定ファイルを作成します。

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <runtime>
    <generatePublisherEvidence enabled="false"/>
  </runtime>
</configuration>
```

`generatePublisherEvidence` 要素について詳しくは、Microsoft 社の Web サイトの次の記事を参照してください。

<http://msdn.microsoft.com/library/bb629393.aspx>

- 2 次の 1 つ以上の操作をします。

- Enterprise Vault インストーラでの自己インストールルーチンによる検査をオフにするには、設定ファイルを `InstallUtil.exe.config` という名前で `InstallUtil.exe` (通常は `%windir%\Microsoft.NET\Framework\v4.n.n.n`) と同じフォルダに保存する
- Enterprise Vault インストーラでの自己登録ルーチンによる検査をオフにするには、設定ファイルを `RegAsm.exe.config` という名前で `RegAsm.exe` (通常は `%windir%\Microsoft.NET\Framework\v4.n.n.n`) と同じフォルダに保存する
- Enterprise Vault システムステータス MMC スナップインによる検査をオフにするには、設定ファイルを `mmc.exe.config` という名前で、`mmc.exe` と同じフォルダ (通常は `%windir%\SysWOW64` と `%windir%\system32`) に保存します。

- サーバー上のすべての Web アプリケーションによる検査をオフにするには、設定ファイルを w3wp.exe.config の名前と w3wp.exe と同じフォルダ (通常は %windir%\SysWOW64\inetsrv と %windir%\system32\inetsrv) に保存します。

## 特定のユーザーアカウントの下で動作するすべてのプロセスに対する証明書の失効確認をオフにする

この方法を使う場合には、Enterprise Vault サービスを実行するすべてのアカウントの Enterprise Vault サーバーごとに設定を変更する必要があります。

特定のユーザーアカウントの下で動作するすべてのプロセスに対する証明書の失効確認をオフにするには

- 1 Enterprise Vault サーバーで Enterprise Vault サービスを実行するアカウントとして、そのサーバーにログインします。このアカウントは、通常、ボルトサービスアカウントです。
- 2 Windows の [コントロールパネル] の [インターネットオプション] をダブルクリックします。
- 3 [インターネットのプロパティ] ダイアログボックスで [詳細設定] タブを選択します。
- 4 [セキュリティ] セクションで、[発行元証明書の取り消しを確認する] のチェックマークをはずします。
- 5 [OK] をクリックします。

# ストレージの設定

この章では以下の項目について説明しています。

- [Enterprise Vault アーカイブ用のストレージの設定について](#)
- [Enterprise Vault の単一インスタンスストレージについて](#)
- [Enterprise Vault の単一インスタンスストレージの適切な共有設定の開発](#)
- ボルトストアグループの作成
- ボルトストアの作成について
- ボルトストアパーティションの作成
- ボルトストアグループに対する共有の設定

## Enterprise Vault アーカイブ用のストレージの設定について

アーカイブ用にストレージを設定する前に、Enterprise Vault の最適化された単一インスタンスストレージを使うかどうかを検討してください。単一インスタンスストレージを使うとアーカイブ済みアイテムの共通のパーツを共有することで、ストレージの必要条件を大幅に減らすことができます。ただし、Enterprise Vault サーバーとパーティションをホストするストレージデバイスとの間のネットワークトラフィックが増加する場合があります。

単一インスタンスストレージを使う場合、必要条件を満たし、ネットワーク接続速度との互換性のある共有設定を決定する必要があります。

- p.192 の「[Enterprise Vault の単一インスタンスストレージについて](#)」を参照してください。
- p.198 の「[Enterprise Vault の単一インスタンスストレージの適切な共有設定の開発](#)」を参照してください。

新しいボルトストアグループは、デフォルトで Enterprise Vault の単一インスタンスストレージを使うように設定されます。

Enterprise Vault でアーカイブを作成できるようにするには、ボルトストアと少なくとも 1 つのボルトストアパーティションを含むボルトストアグループを作成する必要があります。

- ボルトストアグループは、ボルトストアのコンテナです。これは Enterprise Vault の単一インスタンスストレージの共有アイテムの外部境界を定義します。

p.200 の「[ボルトストアグループの作成](#)」を参照してください。

- ボルトストアは、Enterprise Vault Storage Service によるアイテムのアーカイブ先となる論理エンティティです。各ボルトストアには、独自のボルトストアデータベースがあります。ボルトストアデータベースには、ボルトストアのアーカイブと各アーカイブに格納されているすべてのアイテムに関する情報が保存されます。

p.201 の「[ボルトストアの作成について](#)」を参照してください。

- ボルトストアパーティションは、Enterprise Vault がアーカイブ済みデータを格納する物理的な場所です。各ボルトストアには、少なくとも 1 つのパーティションを含める必要があります。パーティションは、さまざまな物理ディスクや各種のストレージメディアに配置することができます。ボルトストアのデータが大きくなった場合、さらにパーティションを作成して容量を追加できます。特定の基準が満たされたときに、アーカイブが 1 つのパーティションから別のパーティションにロールオーバーするようにパーティションを設定できます。

p.205 の「[ボルトストアパーティションの作成](#)」を参照してください。

Enterprise Vault の分類機能を使用する場合は、「スマート」パーティションと呼ばれる特別な種類のパーティションにアイテムをアーカイブすることもできます。これらのパーティションは、以下の点を除き、標準のボルトストアパーティションと同じです。

- スマートパーティションには、選択した分類エンジン (Veritas Information Classifier または Microsoft ファイル分類インフラストラクチャ) で定義した 1 つ以上の分類タグを関連付けることができます。選択したタグを分類エンジンが割り当てたアイテムのみが、スマートパーティションにアーカイブされます。
- 複数のスマートパーティションをアーカイブ用に同時に開くことができます。これは、標準のボルトストアパーティションには当てはまりません。標準のボルトストアパーティションでは、各ボルトストアで開くことができるパーティションは 1 つに限られます。
- 特定の基準が満たされると、Enterprise Vault が次の使用可能なパーティションに自動的にロールオーバーするように、標準のボルトストアパーティションを設定できます。このロールオーバー機能は、スマートパーティションでは利用できません。

ボルトストアグループに Enterprise Vault の単一インスタンスストレージを設定するには、そのグループで共有を設定ウィザードを実行する必要があります。

p.213 の「[ボルトストアグループに対する共有の設定](#)」を参照してください。

# Enterprise Vault の単一インスタンスストレージについて

Enterprise Vault の最適化された単一インスタンスストレージを使うと、アーカイブ済みアイテムに必要なストレージ領域を大幅に削減できます。Enterprise Vault はメッセージの添付ファイルやドキュメントの内容というようなアイテムの共有可能なパーツ (SIS パーツ) を識別します。各 SIS パーツは共有境界内に個別に 1 回のみ格納されます。共有境界は、ボルトストアグループにある 1 つ以上のボルトストアを含むことができます。Enterprise Vault は、対象ボルトストアの共有境界にすでに格納した SIS パーツを識別するとき、SIS パーツを再度アーカイブする代わりに、格納済みの SIS パーツを参照します。

Enterprise Vault は、SIS パーツに最小サイズのしきい値を適用します。Enterprise Vault はサイズしきい値によって、想定されるストレージ節約量と、SIS パーツの作成、アーカイブ、取り込みに必要なリソースとのバランスをとることができます。

Enterprise Vault の単一インスタンスストレージは、次の複数の方法でストレージ領域を節約できます。

- Enterprise Vault は、共有境界内のすべてのボルトストア間で SIS パーツを共有します。たとえば、ジャーナルとメールボックスアーカイブに個別のボルトストアを使う場合、Enterprise Vault は、ボルトストア間で SIS パーツを共有できます。
- 同じ添付ファイルのある多数のメッセージを複数の受信者に個別に送信する場合、Enterprise Vault は、添付ファイルを 1 回のみ共有境界内に格納します。
- Enterprise Vault は SIS パーツを、ファイル名からではなく、内容から識別します。2 つのメッセージに、同じ添付ファイルが添付されている場合、これらのファイル名が異なっても、Enterprise Vault は添付ファイルを共有できます。
- Enterprise Vault は、ファイルサーバーにファイルとしても格納される Exchange メッセージの添付ファイルなど、種類が異なるアーカイブから発生する同一の SIS パーツを共有できます。

新しいボルトストアは、単一インスタンスストレージをデフォルトで使い、その中でアーカイブされたアイテムの SIS パーツのみを共有します。必要に応じて、ボルトストアグループで共有を設定ウィザードを実行して、ボルトストア間の共有を拡張したり、Enterprise Vault の単一インスタンスストレージを無効にすることができます。

次の点に注意してください。

- Dell EMC Centera デバイス上のパーティション。アイテムが、Dell EMC Centera デバイス上でホストされているパーティションに格納されている場合、Enterprise Vault の単一インスタンスストレージは実行されません。Enterprise Vault には、Centera デバイスの共有機能を利用するために、個別のデバイスレベル共有オプションが用意されています。

p.197 の「[Centera のデバイスレベル共有について](#)」を参照してください。



- **スマートパーティション。**Enterprise Vault は、同じスマートパーティション内のアイテム間で SIS パーツを共有しますが、スマートパーティションとその他のパーティション間では SIS パーツを共有しません。  
たとえば、2 人の従業員が、添付ファイルを含む同じ電子メールを受信するとします。コンプライアンス上の理由から、Enterprise Vault では 1 人の従業員の電子メールがスマートパーティションにアーカイブされ、もう 1 人の従業員の電子メールが標準のボルトストアパーティションにアーカイブされます。電子メールとその添付ファイルが最初に標準パーティションにアーカイブされると、その後電子メールがスマートパーティションにアーカイブされるとき、通常添付ファイルは再度アーカイブされません。これは、スマートパーティション上のデータが完全には適合しなくなることを意味します。ただし、この場合 Enterprise Vault では電子メールと添付ファイルの両方が再度アーカイブされます。

## 共有レベルと共有境界について

ボルトストアグループの共有を設定するときは、グループの各ボルトストアに共有レベルを設定します。グループの単一インスタンスストレージ共有の境界は、共有レベルによって決まります。

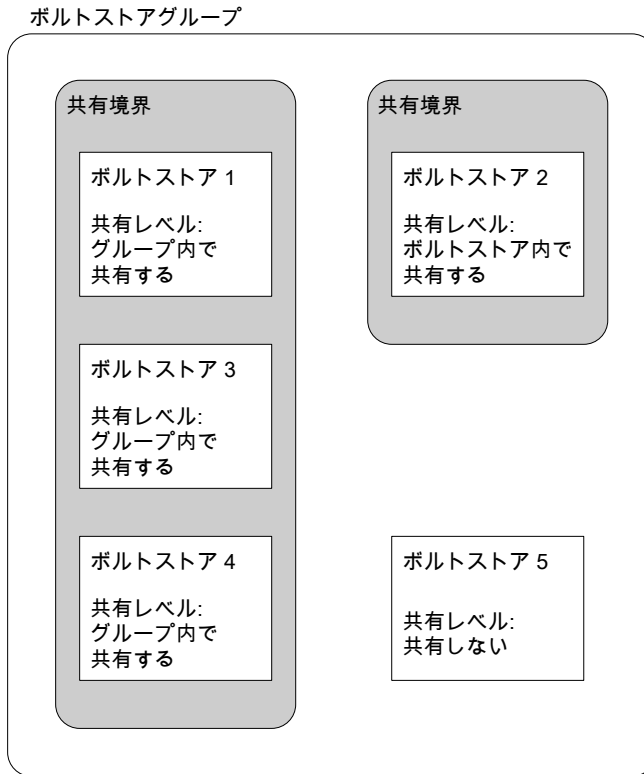
表 26-1                      ボルトストアの共有レベル

ボルトストアの共有レベル	共有に対する影響
グループ内で共有する	ボルトストアは、この共有レベルを持つボルトストアグループのその他すべてのボルトストアと SIS パーツを共有します。
ボルトストア内で共有する	ボルトストアは自己の内部でのみ SIS パーツを共有します。
共有しない	Enterprise Vault は、このボルトストアに対して単一インスタンスストレージを実行しません。

ボルトストアグループには、1 つ以上の共有境界を含めることができます。各共有境界には、Enterprise Vault の単一インスタンスストレージの結果として発生する SIS パーツを共有する 1 つ以上のボルトストアが含まれます。

図 26-1 に、次の 5 つのボルトストアを含むボルトストアグループの例を示します。

図 26-1 ボルトストアグループの共有境界



- ボルトストア 1、3、4 にはすべて、共有レベルとして[グループ内で共有する]が設定されています。これらのボルトストアは同じ共有境界内にあります。**Enterprise Vault** は、これら 3 つのボルトストアにアーカイブするアイテム用にこれらのボルトストア全体で **SIS** パーツを共有します。
- ボルトストア 2 の共有レベルは[ボルトストア内で共有する]であるため、ボルトストア 2 は独自の共有境界を所有しています。**Enterprise Vault** は、このボルトストアにアーカイブするアイテム用にボルトストア内で **SIS** パーツを共有します。
- ボルトストア 5 の共有レベルは[共有しない]です。このボルトストアは、どの共有境界にも含まれません。**Enterprise Vault** はこのボルトストアにアーカイブするアイテムに対して **Enterprise Vault** の単一インスタンスストレージを実行しません。

各ボルトストアには、複数のボルトストアを含む共有境界を 1 つのみ含めることができます。たとえば、図 26-1 では、既存のボルトストアではなく、相互に **SIS** パーツを共有する 2 つの新しいボルトストアは設定できません。代わりに、別のボルトストアグループに新しいボルトストアを作成できます。

Enterprise Vault は、新しいボルトストアに[ボルトストア内で共有する]という共有レベルを割り当てます。

ボルトストアの共有レベルを変更するには、そのボルトストアのためにパーティションを作成した後で、そのボルトストアグループで共有を設定ウィザードを実行する必要があります。

## Enterprise Vault の単一インスタンスストレージの動作

Enterprise Vault は、次の条件の両方が当てはまる場合、単一インスタンスストレージを使用してアイテムをアーカイブします。

- 対象ボルトストアの共有レベルが[ボルトストア内で共有する]または[グループ内で共有する]である
- 現在のオープンパーティションが **Centera** デバイスでホストされていない

Enterprise Vault は、次のように、単一インスタンスストレージのためにアイテムをアーカイブします。

- サイズの大きなメッセージ添付ファイルなど、共有に適したアイテムのパーツを識別します。これらのパーツは **SIS** パーツと呼ばれます。Enterprise Vault は、**SIS** パーツの最小サイズのしきい値を使用して、想定されるストレージ節約量と、**SIS** パーツの作成、アーカイブ、取り込みに必要なリソースとのバランスをとります。
- 各 **SIS** パーツに対してデジタルフィンガープリントを生成します。フィンガープリントとは、**SIS** パーツの内容によって決定される暗号化されたハッシュベースの識別子です。
- 各 **SIS** パーツについて、Enterprise Vault はボルトストアグループのフィンガープリントデータベースにアクセスして、フィンガープリントが同じ **SIS** パーツがボルトストアの共有境界内にすでに格納されているかどうかを判断します。フィンガープリントが同じ **SIS** パーツは、同一の **SIS** パーツです。
  - 同一の **SIS** パーツが共有境界内にすでに格納されていない場合、Enterprise Vault はその **SIS** パーツを格納し、その **SIS** パーツのフィンガープリント情報をフィンガープリントデータベースに保存します。
  - 同一の **SIS** パーツが共有境界内にすでに格納されている場合、Enterprise Vault は格納済みの **SIS** パーツを参照します。**SIS** パーツを再度格納することはありません。
- アイテムの残りの部分 (アイテムから **SIS** パーツを除いた部分) を未処理の保存セットファイルとして格納します。未処理の保存セットファイルは、アイテムに関する Enterprise Vault メタデータおよびそれに関する一意の情報 (ドキュメントまたは添付ファイルの場合はファイル名、メッセージの場合は追跡のためのフラグなど) を保持します。

Enterprise Vault は、アーカイブ済みアイテムのリストア要求を受け取ると、そのアイテムの未処理の保存セットファイルおよび SIS パーツファイルから、そのアイテムを再構成します。

アイテムの対象ボルトストアの共有レベルが[共有しない]であるか、対象パーティションが Centera デバイスでホストされている場合、Enterprise Vault は単一インスタンスストレージを使用しません。アイテムを Enterprise Vault メタデータと合わせて単一の保存セットファイルとしてをアーカイブします。

## フィンガープリントデータベースについて

ボルトストアグループのフィンガープリントデータベースには、ボルトストアグループに格納されている各 SIS パーツに関する情報が保存されます。この情報には、SIS パーツのデジタルフィンガープリント、SIS パーツが格納されるパーティションの名前、SIS パーツが共有されている共有境界などがあります。

ボルトストアグループを作成すると、Enterprise Vault ではそのボルトストアグループに対するフィンガープリントデータベースが作成されます。

---

**メモ:** フィンガープリントデータベースの設定後の場所の追加または変更は、SQL Server の管理タスクです。詳しくは、Microsoft SQL Server のマニュアルを参照してください。

---

新規ボルトストアグループウィザードには、フィンガープリントデータベースの SQL ファイルグループの設定用に次のオプションがあります。

- Enterprise Vault が 1 つのデバイス上のプライマリファイルグループとすべての非プライマリファイルグループを検索する場合の基本設定。
- 32 個の非プライマリファイルグループに追加の場所を設定するオプション。非プライマリファイルグループには、アーカイブ済みアイテムのフィンガープリント情報が格納されるため、単一インスタンスストレージを使うと、サイズがすぐに増大する可能性があります。最適なパフォーマンスを得るには、非プライマリファイルグループを複数の場所に分散させる必要があります。

最適なパフォーマンスを得るには、次の手順を実行します。

- 非プライマリファイルグループに追加の場所を設定するオプションを選択します。
- SQL Server の非プライマリファイルグループに対して、最大 32 個まで、可能な限り多くの場所を指定します。
- 場所ごとにデバイスを 1 つずつ指定します。同じデバイスに複数の場所を指定した場合、パフォーマンス上のメリットが得られません。

## SIS パーツの削除

各ボルトストアグループのフィンガープリントデータベースには、グループのボルトストアに存在する各 SIS パーツへの参照数が記録されます。

ユーザーがアーカイブ済みアイテムを削除すると、SIS パーツへの参照の数が減少します。アイテムを削除するときに、SIS パーツへの参照数が 0 になる場合、Enterprise Vault ではグループのボルトストアに SIS パーツへの参照が含まれるかどうか確認されます。参照が残っていない場合、SIS パーツが削除されます。参照が残る場合、SIS パーツは保持され、Enterprise Vault イベントログにエラーが生成されます。

---

**メモ:** コレクションを使う場合は、非参照 SIS パーツが CAB ファイルに一定期間残った後で削除されることがあります。

p.208 の「[コレクションと移行について](#)」を参照してください。

---

## Enterprise Vault の単一インスタンスストレージの要件

Enterprise Vault の単一インスタンスストレージには、システムに関する次の追加要件があります。

- フィンガープリントデータベース用のストレージ領域。Enterprise Vault の単一インスタンスストレージを使うと、フィンガープリントデータベースが非常に急速に大きくなることがあります。アーカイブと取り込みの許容されるパフォーマンスを確保するために、ボルトストアグループ内の共有の量に対してフィンガープリントデータベースを適切に設定することが重要です。

p.200 の「[ボルトストアグループの作成](#)」を参照してください。

- ネットワーク接続要件。Enterprise Vault サーバーは、Enterprise Vault の単一インスタンスストレージを使用したアイテムの格納または取り込み時に次のコンピュータと通信します。
  - ボルトストアの共有境界内にあるボルトストアのボルトストアパーティションをホストするコンピュータ。
  - ボルトストアグループのフィンガープリントデータベースをホストするコンピュータ。これらの接続のネットワーク接続速度は、格納と取り込みにかかる時間を許容範囲に抑えることができる十分な速さであることが必要です。

p.198 の「[Enterprise Vault の単一インスタンスストレージの適切な共有設定の開発](#)」を参照してください。

## Centera のデバイスレベル共有について

必要に応じて、Centera のデバイスレベル共有を活用するように Centera デバイスのパーティションを設定できます。Enterprise Vault は Centera デバイスが保存セットの共有可能なパーツを共有できるように、それらを別のデータ BLOB として格納します。

[新規パーティション]ウィザードには、パーティションを作成して **Centera** デバイスを指定するときにデバイスレベル共有を有効化するオプションが含まれています。

p.205 の「[ボルトストアパーティションの作成](#)」を参照してください。

デバイスレベル共有は、パーティションのプロパティの[全般]タブからも有効化できます。

**Centera** のためのパーティションは **Enterprise Vault** の単一インスタンスストレージの共有に加わりません。ボルトストアに共有のために設定される **Centera** 用パーティションを作成する場合、このパーティションは、**Enterprise Vault** の単一インスタンスストレージの共有では無視されます。

## Enterprise Vault ストレージストリーマ API をサポートするストレージデバイスのパーティション共有について

**Enterprise Vault** ストレージストリーマ API をサポートするストレージデバイスにボルトストアパーティションを作成できます。パーティション用の **Enterprise Vault** ストレージサービスをホストする **Enterprise Vault** サーバーに適切なストレージデバイスソフトウェアをインストールする必要があります。

ボルトストアグループ内での共有をサポートするには、同じボルトストアグループのパーティションを管理する各 **Enterprise Vault** ストレージサーバーにもストレージデバイスソフトウェアをインストールする必要があります。

## Enterprise Vault の単一インスタンスストレージの適切な共有設定の開発

**Enterprise Vault** の単一インスタンスストレージを使う場合、組織のデータ共有に関する必要条件を満たし、ネットワーク接続速度に対して適切な共有設定を作成する必要があります。

アーカイブを開始する前に、必要な共有設定の種類を検討します。変更可能な内容には制限があります。

- ボルトストアの共有レベルは変更できますが、変更は過去にさかのぼっては適用されません。たとえば、ボルトストアの共有レベルを[グループ内で共有する]から[ボルトストア内で共有する]に変更する場合、ボルトストアグループ内ですでに共有されているアイテムはボルトストアグループ内で共有されたままになります。
- 次の条件に該当しないものがある場合、ボルトストアを別のボルトストアグループに移動できません。
  - 以前に **Enterprise Vault 8.0** にアップグレードしました。
  - **Enterprise Vault** で **Enterprise Vault 8.0** にアップグレードされたボルトストアか、またはデフォルトのアップグレードグループ内で作成したボルトストアです。

- ボルトストアの共有レベルは「共有しない」で、変更したことはありません。

単一インスタンスストレージを設定する方法を決定するときには、以下のことを考慮してください。

- 組織の一部を「チャイニーズウォール」とも呼ばれる情報障壁で分離する必要があることがあります。たとえば、データセンターでは、利益相反を避けるために、投資、小売、合併買収の各グループ間で情報を分離することを、法律または企業方針によって要求される場合があります。  
情報を分離する必要がある組織グループごとに個別のボルトストアグループを作成する必要がある場合があります。

- 格納と取り込みにかかる時間を許容範囲内に抑えるために、適切なコンピュータ間に十分なネットワーク接続を確保する必要があります。最低限、単一インスタンスストレージを、**100 Mbps** スイッチドイーサネット LAN で予想される応答時間をサポートする環境に制限することを推奨します。  
ストレージサービスによってボルトストアが管理されている Enterprise Vault サーバーは、次のコンピュータとの間に十分な接続性を確保する必要があります。

- ボルトストアの共有境界内にあるボルトストアのボルトストアパーティションをホストするコンピュータ。

- ボルトストアグループのフィンガープリントデータベースをホストするコンピュータ。  
これらのコンピュータ間の接続速度が低下すると、Enterprise Vault が共有アイテムをアーカイブしたり、取り込んだりする時間が長くなります。  
組織が複数の広範囲の地域に分散している場合、地域ごとに個別のボルトストアグループを作成することが適切である場合があります。フィンガープリントデータベースは必ずローカルに配置してください。

Enterprise Vault では、接続性テストを実行してサンプルネットワーク接続で接続速度を推測することができます。新しいボルトストアグループまたはパーティションを作成するとき、または共有を設定するときには、該当するウィザードで、接続性テストの実行を求めるメッセージが表示されます。接続性テストは、許容レベルのパフォーマンスで共有設定を作成するのに役に立つことがあります。接続性テストでは、パフォーマンスを評価するために、ping 要求を数回実行して平均応答時間を測定します。環境で ping を無効にしている場合は、他のツールを使ってパフォーマンスが許容範囲内であるかどうかを判断してください。応答時間が 1 ミリ秒以下になるように設定することを推奨します。

テスト結果によって接続性が良好でないことが示された場合、接続速度が向上するように、共有境界の変更またはコンピュータの場所の変更を検討してください。パフォーマンスが低下しても構わない場合は、接続性テストの結果が良好でなくても許容することを選択できます。

- ボルトストアグループを作成するときは、計画された共有の必要条件を満たすように、フィンガープリントデータベースを適切に設定します。

p.200 の「[ボルトストアグループの作成](#)」を参照してください。

# ボルトストアグループの作成

ボルトストアは、ボルトストアグループ内でグループ化されます。**Enterprise Vault** 単一インスタンスストレージを使う場合、ボルトストアグループは、SIS パーツの共有のための外部境界として機能します。

ボルトストアグループとボルトストアの作成を開始する前に、どの種類の共有設定が組織の構造とネットワーク接続速度と互換性があるかを検討してください。

p.198 の「**Enterprise Vault** の単一インスタンスストレージの適切な共有設定の開発」を参照してください。

次のように、新規ボルトストアグループウィザードを使ってボルトストアグループを作成できます。

## ボルトストアグループを作成する方法

- 1 管理コンソールの左ペインで、[ボルトストアグループ]が表示されるまで、**Enterprise Vault** サイトの階層を展開します。
- 2 [ボルトストアグループ]を右クリックして、[新規作成]、[ボルトストアグループ]をクリックします。

新規ボルトストアグループウィザードが起動します。

- 3 ウィザードに従って操作します。次の情報を指定する必要があります。

- ボルトストアグループの名前。
- グループのフィンガープリントデータベースをホストおよび管理する **SQL** サーバー。
- フィンガープリントデータベースの **SQL** ファイルグループの場所。

新規ボルトストアグループウィザードには、ファイルグループを設定するための次のオプションが表示されます。

- **Enterprise Vault** が 1 つのデバイス上のプライマリファイルグループとすべての非プライマリファイルグループを検索するための基本設定。
- 32 個の非プライマリファイルグループに追加の場所を設定するオプション。単一インスタンスストレージを使うと、非プライマリファイルグループのサイズが急速に大きくなることがあります。最適なパフォーマンスを得るために、非プライマリファイルグループを複数の場所に分散します。

最適なパフォーマンスを得るには、次の手順を実行します。

- オプション[非プライマリファイルグループ用の追加の場所を設定する]を選択します。
- **SQL Server** の非プライマリファイルグループに対して可能な限り多くの場所 (最大 32 個) を指定します。



- 場所ごとにデバイスを 1 つずつ指定します。同じデバイスに複数の場所を指定した場合、パフォーマンス上のメリットが得られません。

---

**メモ:** フィンガープリントデータベースの設定後の場所の追加または変更は、SQL Server の管理タスクです。詳しくは、Microsoft SQL Server のマニュアルを参照してください。

---

ボルトストアグループが作成されたら、新規ボルトストアウィザードでボルトストアを作成する手順を実行します。

p.201 の「[ボルトストアの作成について](#)」を参照してください。

## ボルトストアの作成について

ボルトストアを作成するときは、ボルトストアを管理する Enterprise Vault Storage Service と、SQL ボルトストアデータベースの場所を指定する必要があります。

ボルトストアデータベースには、ボルトストアのアーカイブと各アーカイブに格納されているすべてのアイテムに関する情報が保存されます。たとえば、アーカイブ済みアイテムをバックアップした場合、このバックアップはボルトストアデータベースに保存されている情報に反映されます。

## Enterprise Vault のセーフコピーについて

アーカイブ済みアイテムが、アーカイブ先のボルトストアパーティションがバックアップされるまで保持されるように、Enterprise Vault を設定することができます。アーカイブから削除までの期間、元のアイテムは Enterprise Vault によってセーフコピーとして扱われます。ボルトストアパーティションがバックアップされたら、Enterprise Vault はセーフコピーを削除できます。

セーフコピーの削除は、ストレージサービスが起動されたとき、またはボルトストアのバックアップモードがクリアされたときに実行されます。また、Enterprise Vault は、ショートカットとプレースホルダを作成するように設定されている場合は、この時点で作成します。

## Enterprise Vault セーフコピーを削除するタイミングの選択

Enterprise Vault がセーフコピーを管理する方法を制御するために、各ボルトストアの作成時に次の設定のいずれかを選択する必要があります。

- [いいえ、アーカイブ後すぐに削除します]。すべてのセーフコピーはアイテムをアーカイブした直後に削除されます。
- [はい、元の場所に保持します]。Enterprise Vault はアーカイブ済みアイテムを含むパーティションのバックアップが作成されるまで元のアイテムを保持します。

- [はい、ストレージキューに保持します]。Enterprise Vault はアーカイブ済みアイテムを含むパーティションのバックアップが作成されるまでストレージキューにセーフコピーを保持します。

すべてのボルトストアにデフォルト設定を指定することが可能で、ジャーナルボルトストアに異なる設定を指定するオプションがあります。

## Enterprise Vault がセーフコピーを削除する前にパーティションのバックアップを作成していることを確認する

セーフコピーを保存する場合には、Enterprise Vault はセーフコピーを削除する前にパーティションのバックアップを作成していることを確認する必要があります。

Enterprise Vault は、次のいずれかに基づいて各パーティションのバックアップを作成していることを確認します。

- パーティション上のファイルのアーカイブ属性。バックアップ後にバックアップソフトウェアによってアーカイブ属性がリセットされた場合にのみ、パーティションがバックアップされたかどうかをアーカイブ属性で判断できます。
- トリガファイルのしくみ。バックアップソフトウェアによってバックアップ対象のファイルのアーカイブ属性がリセットされない場合は、このしくみを使う必要があります。

パーティションを作成するときに、各パーティションに対して使う方法を選択する必要があります。

## パーティションがバックアップされたかどうかのアーカイブ属性による判断

[アーカイブ属性を使用] オプションを使うには、ボルトストアパーティションのファイルが保護された後で、バックアップソフトウェアでそれらのファイルのアーカイブ属性をリセットする必要があります。バックアップソフトウェアによってアーカイブ属性がリセットされない場合は、トリガファイルのしくみを使う必要があります。

Enterprise Vault によってボルトストアパーティションにファイルが作成されると、ファイルのアーカイブ属性が設定されます。Enterprise Vault では、アーカイブ属性がクリアされるまで、ファイルはバックアップされていないと見なされ、対応するセーフコピーは削除されません。ただし、バックアップソフトウェアでアーカイブ属性がクリアされると、Enterprise Vault ではファイルがバックアップされたと見なされるため、セーフコピーを自由に削除できます。必要に応じて、セーフコピーの削除と同時にアーカイブ済みアイテムへのショートカットが作成されます。

---

**メモ:** 一部の WORM デバイスはアーカイブ属性の変更を許可していません。これらのデバイスは、[アーカイブ属性を使用] オプションと互換性がありません。

---

## トリガファイルメカニズムを使ってパーティションのバックアップを作成するかどうかを決める

一部のバックアップソフトウェアは、バックアップ後にファイルのアーカイブビットを消去します。この属性は、各ファイルのプロパティの[ファイルをアーカイブ可能にする]オプションに表示されます。

ただし、一部のバックアップソフトウェアと、データを保全する他の方法ではアーカイブビットは消去されません。この場合は、トリガファイルメカニズムを使って各パーティションのデータが安全であることを示す必要があります。

次の場合は、トリガファイルメカニズムを使う必要があります。

- データを保全するためにパーティションのスナップショットを作成する。
- アーカイブビットを消去しないバックアップソフトウェアを使う。
- 完全バックアップを作成した場合にのみアーカイブビットを消去する差分バックアップを作成する。

---

**メモ:** バックアップが正常に完了しないと、バックアップスクリプトでトリガファイルは作成されません。

---

[トリガファイルを確認]オプションでは、IgnoreArchiveBitTrigger.txt というトリガファイルを調べてボルトストアパーティションのファイルが 保全されているかどうかを判断します。各バックアップで、バックアップソフトウェアまたはスクリプトはバックアップを作成したことを示すために、パーティションのルートに新しく作成された IgnoreArchiveBitTrigger.txt を保存する必要があります。

たとえば、「Sales」というボルトストアがあり、E:¥EVStorage にパーティションを保存している場合は E:¥EVStorage¥Sales Ptn1 というパーティションフォルダがあります。この場合には、バックアップソフトウェアまたはスクリプトはパーティションのバックアップを作成したことを示すために、E:¥EVStorage¥Sales Ptn1 に IgnoreArchiveBitTrigger.txt を保存する必要があります。

---

**メモ:** バックアップスクリプトは、パーティションのバックアップを作成するときに新しい IgnoreArchiveBitTrigger.txt ファイルを作成する必要があります。ファイルの作成日がバックアップ日と異なる別のファイルの名前を変更するだけでは十分ではありません。

---

たとえば、新しいファイルを作成するバックアップスクリプトで次のコマンドを使うことができます。

```
echo "Enterprise Vault trigger file" > "E:¥EVStorage¥Sales  
Ptn1¥IgnoreArchiveBitTrigger.txt"
```

**Enterprise Vault** は `IgnoreArchiveBitTrigger.txt` を見つけると、`IgnoreArchiveBitTrigger.txt` を作成する前に作成したすべてのパーティションの保存セットファイルをバックアップであると見なします。**Enterprise Vault** は必要に応じて自由に、安全な保存セットファイルと対応するセーフコピーを削除してショートカットを作成します。

**Enterprise Vault** で `IgnoreArchiveBitTrigger.txt` が見つからない場合はパーティションのバックアップは作成されていないと見なされ、セーフコピーは削除されません。

**Enterprise Vault** はセーフコピーの削除を完了すると、ファイルが処理されたことや、パーティションの関連ファイルが安全であることを示す `.old` 拡張子が付いた `IgnoreArchiveBitTrigger.txt` の名前を変更します。

次のバックアップで、バックアップソフトウェアは新しい `IgnoreArchiveBitTrigger.txt` を作成します。

**Enterprise Vault** は、ストレージサービスを開始するときバックアップモードをボルトストアから消去するときにトリガファイルのパーティションを調べます。パーティションのスキャン間隔を設定すると、**Enterprise Vault** は設定したボルトで決定した間隔でパーティションを調べます。

**Centera** パーティションのトリガファイルメカニズムを使うことはできませんが、**Enterprise Vault** が **Centera API** をクエリーしてパーティションが複製されたかどうかを判断します。**Enterprise Vault** は、ストレージサービスを開始するときバックアップモードをボルトストアから消去するときに **Centera** パーティションを調べます。

**Centera** パーティションのスキャン間隔を設定すると、**Enterprise Vault** は設定したボルトで決定した間隔でパーティションを調べます。

## ボルトストアの作成

新規ボルトストアウィザードを使ってボルトストアを作成できます。

### ボルトストアを作成する方法

- 1 新規ボルトストアグループウィザードを使ってボルトストアグループを作成した場合、新規ボルトストアウィザードが自動的に起動します。手順 5 に進みます。
- 2 管理コンソールの左ペインで、[ボルトストアグループ]が表示されるまで、**Enterprise Vault** サイトの階層を展開します。
- 3 [ボルトストアグループ]コンテナを展開して、既存のボルトストアグループを表示します。
- 4 ボルトストアを作成するボルトストアグループを右クリックして、[新規作成] > [ボルトストア]の順に選択します。

新規ボルトストアウィザードが起動します。

- 5 新規ボルトストアウィザードで、ボルトストアを作成する手順を実行します。

次の情報を指定する必要があります。

- ボルトストアで使うストレージサービスをホストするコンピュータの名前。ウィザードでこの情報が必要になるのは、**Enterprise Vault** サイトにストレージサービスをホストする複数のコンピュータが含まれている場合のみです。
- ボルトストアの名前。名前には、英字、数字、スペースを含めることができます。
- ボルトストアデータベースを作成して管理する **SQL** サーバーと、データベースファイルの場所。
- セーフコピーの場所。**Enterprise Vault** は、セーフコピーを元の場所またはストレージキューに保存できます。ストレージキューの場所を選択すると、**Enterprise Vault** はアーカイブの直後に元のアイテムを削除できます。元の場所のストレージ領域はすぐに回復されます。
- アイテムのセーフコピーを削除するタイミングと、パーティションのバックアップを作成したことを **Enterprise Vault** が確認する方法。  
p.201 の「[Enterprise Vault のセーフコピーについて](#)」を参照してください。

---

**メモ:** **Enterprise Vault** は、新しいボルトストアに[ボルトストア内で共有する]という共有レベルを割り当てます。このルール例外は、以前 **Enterprise Vault 8.0** にアップグレードしたときに **Enterprise Vault** が作成したデフォルトのアップグレードグループに適用されます。デフォルトのアップグレードグループの共有を設定していない場合は、**Enterprise Vault** が[共有しない]という共有レベルをそのグループの新しいボルトストアに割り当てます。

ボルトストアの共有レベルを変更するには、そのボルトストアのためにパーティションを作成した後で、そのボルトストアグループで共有を設定ウィザードを実行する必要があります。

---

ボルトストアが作成されたら、新規パーティションウィザードでボルトストアのパーティションを作成する手順を実行します。

p.205 の「[ボルトストアパーティションの作成](#)」を参照してください。

## ボルトストアパーティションの作成

---

**メモ:** **Enterprise Vault** の分類機能を使用する場合、標準のボルトストアパーティションに加えて、またはその代わりに「スマート」パーティションを作成できます。

p.211 の「[スマートパーティションの設定](#)」を参照してください。

以下に示す点を除き、スマートパーティションは標準のボルトストアパーティションとほぼ同じです。

---

ボルトストアパーティションは、さまざまな物理ディスクや各種のストレージメディアに配置することができます。たとえば、パーティションをローカル NTFS ボリューム、NetApp Filer、Dell EMC Centera デバイス、ストリーマストレージデバイス上に作成できます。サポート対象デバイスの詳細な一覧については、Enterprise Vault [Compatibility Charts](#) を参照してください。

パーティションの場所を決めるときに、既存のパーティションの場所、または既存のパーティションに関連付けされたフォルダを含む場所は選択しないでください。ネットワーク共有またはマウントポイントを使う場合は、パーティションフォルダが重複しないように特に注意してください。フォルダが複数のパーティションに関連付けされていると、データが失われる可能性があります。

---

**メモ:** ボルトストアパーティションにディスククォータと File Server Resource Manager のクォータを使うことは推奨しません。

---

Enterprise Vault では、パーティションのルートパスは空であると想定されます。ルートパスを使って、Enterprise Vault によって作成されたもの以外のファイルまたはフォルダを保持しないでください。

WORM ストレージデバイスにアイテムを無期限に格納する場合は、デバイスの保持設定が正しく行われていることを確認します。

p.26 の「[WORM ストレージデバイスの準備](#)」を参照してください。

Enterprise Vault ストレージストリーマ API をサポートするストレージデバイスでボルトストアパーティションを作成することを計画する場合、適切なストレージデバイスソフトウェアが Enterprise Vault ストレージサーバーにインストールされていることを確認してください。ボルトストアグループのパーティションを管理するすべての Enterprise Vault ストレージサーバーにストレージデバイスソフトウェアをインストールします。

## ボルトストアパーティションの初期状態

ボルトストアのデータが大きくなった場合、さらにパーティションを作成して容量を追加できます。各ボルトストアには、1 つのオープン標準パーティションのみを含めることができ、Enterprise Vault は、パーティションがオープンしている間に、このパーティションにデータをアーカイブします。

---

**メモ:** この制限は、スマートパーティションには適用されません。複数のスマートパーティションをアーカイブ用に同時に開くことができます。

---

ボルトストアのオープンパーティションを管理する方法には次の 2 つがあります。

- ボルトストアのオープンパーティションは手動で変更できます。たとえば、オープンパーティションをホストするディスクが許容量に達したら、そのパーティションを終了して別のディスクでパーティションを開くことができます。

- 自動パーティションロールオーバー機能を使うと、特定の基準を満たしている場合にパーティションから別のパーティションにアーカイブをロールオーバーするようにパーティションを設定できます。たとえば、オープンパーティションをホストするディスクの空き領域が **5%** のみになったときにパーティションをロールオーバーするように設定できます。設定した日にパーティションをロールオーバーするように設定することもできます。詳しくは『管理者ガイド』を参照してください。

これらの機能の両方をサポートするために、パーティションの作成時に次の初期状態のいずれかを選択できます。

- [クローズ]を選択すると、クローズパーティションを作成できます。既存のオープンパーティションがある場合、このオプションを選択しても影響はありません。プロパティを編集して、新しいパーティションをいつでもオープンできます。  
p.207 の「[Enterprise Vault のクローズパーティションについて](#)」を参照してください。
- [オープン]を選択すると、オープンパーティションを作成できます。各ボルトストアには 1 つのオープンパーティションのみを含めることができます。ボルトストアに既存のオープンパーティションがある場合、そのパーティションは自動的にクローズされ、アイテムはこの新しいパーティションにアーカイブされます。
- [準備完了]を選択して、パーティションロールオーバーで利用可能な新しいパーティションを作成します。

---

**メモ:** このオプションは、スマートパーティションには使用できません。

---

## Enterprise Vault のクローズパーティションについて

パーティションを閉じると、Enterprise Vault は新しい情報を書き込むのを停止します。Enterprise Vault は、その後もクローズパーティションにあるアイテムを修正します。

---

**メモ:** クローズパーティションのサイズは増やすことができます。バックアップを作成する必要もあります。

---

Enterprise Vault は次の場合にクローズパーティションを修正します。

- 削除。Enterprise Vault はアーカイブからアイテムが削除された場合にパーティションを修正します。
- ストレージの期限切れ。Enterprise Vault は保持期間が切れるとアーカイブからアイテムを削除します。
- コレクション。Enterprise Vault コレクションソフトウェアをクローズパーティションで実行し続けます。  
コレクション処理はアーカイブ済みアイテムを表示するときに作成した一時ファイルを削除するので、クローズパーティションでコレクションを実行する必要があります。

- アイテムが保留中。保留状態のアイテムはパーティションを閉じる前にクローズパーティションに書き込まれます。

クローズパーティションを修正する可能性がある場合は、クローズパーティションのバックアップを定期的に行うことを推奨します。

クローズパーティションを修正しない場合は、定期的バックアップを実行する必要はありません。パーティションの最終的なバックアップを実行してバックアップルーチンからパーティションを削除できます。

## コレクションと移行について

ボルトストアパーティションを **Centera** 以外の非 **WORM** デバイスに保存する場合はパーティションに保存したファイルのコレクションと移行を設定したり、コレクションと移行のスケジュールを設定できます。

コレクションには、複数の小さいファイルを大きいコレクションファイル（.cab ファイル）に収集することも含まれます。コレクションはバックアップ時の重要な機能強化になる場合があります。コレクションは重複排除の消失の原因になるため、重複排除を実行するデバイスでは推奨しません。

移行では、長期ストレージデバイスにコレクションファイルを移動します。たとえば、古いコレクションを安く遅いストレージに移行すると合理的です。

コレクションファイルを使うことを選択した場合、コレクション基準を設定し、オプションで、コレクションファイルをセカンダリストレージに移行する方法とタイミングに関する詳細を指定できます。これらのオプションの設定については、管理コンソールヘルプを参照してください。

---

**メモ:** コレクションを使うと、非参照アイテムが削除する前にしばらくの間 .cab ファイルに残ることがあります。非参照アイテムの比率が一定のレベルに達すると、**Enterprise Vault** は .cab ファイルを圧縮して非参照アイテムを削除します。

---

他のストレージデバイスはデータファイルを移行できるように **Enterprise Vault** と統合されます。サポート対象デバイスは、**Enterprise Vault Compatibility Charts** に記載されています。

## Dell EMC Centera デバイス上でのコレクション

**Centera** デバイスでは、次のように、コレクションでの処理が異なります。

- **Centera** コレクションクリップが **CAB** ファイルの代わりに使用されます。
- 保存セットは、スケジュールに従って収集されるのではなく、アーカイブ後すぐに収集されます。



- コレクションの **Centera Clip** とそれに含まれる保存セットは、**Centera Clip** 内の保存セットへの参照がなくならない限り削除されません。

**Centera** デバイス上のボルトストアパーティションでのコレクションが有効になっている場合に最適なアーカイブパフォーマンスを確保するために、関連付けされたボルトストアデータベースの保存セットテーブルに追加インデックス **IX\_Collection\_Saveset\_Partition** を作成できます。このインデックスがない場合は、次の条件が満たされていれば、ストレージサービスの起動時に **Enterprise Vault** が自動的に作成します。

- 少なくとも 1 つの **Centera** ボルトストアパーティションが開いていてコレクションに対して有効になっていること。
- 保存セットテーブルのレコードの数が 1,000,000 以下であること。

該当するボルトストアデータベースをホストする **SQL Server** でこのインデックスに必要な領域は、保存セットテーブルの 1 行あたり約 27 バイトです。

## 標準のボルトストアパーティションの作成

次のように、新規パーティションウィザードを使って標準のボルトストアパーティションを作成できます。

**Enterprise Vault** 単一インスタンスストレージを使う環境では、ネットワーク接続速度は、共有をサポートするのに十分な速度である必要があります。ボルトストアで単一インスタンスストレージを使う場合は、新規パーティションウィザードにメッセージが表示されたときに接続性テストを実行してください。接続性テストは、接続速度が共有に対して十分であるかどうかを判断するのに役立ちます。

p.198 の「[Enterprise Vault の単一インスタンスストレージの適切な共有設定の開発](#)」を参照してください。

---

**メモ:** ボルトストアパーティションにディスククォータと **File Server Resource Manager** のクォータを使うことは推奨しません。

---

### 標準のボルトストアパーティションを作成する方法

- 1 新規ボルトストアウィザードを使ってボルトストアを作成した場合、新規パーティションウィザードが自動的に起動します。手順 7 に進みます。
- 2 管理コンソールの左ペインで、[ボルトストアグループ]が表示されるまで、**Enterprise Vault** サイトの階層を展開します。
- 3 [ボルトストアグループ]コンテナを展開して、既存のボルトストアグループを表示します。
- 4 パーティションを作成するボルトストアを含むボルトストアグループを展開します。
- 5 パーティションを作成するボルトストアを展開します。

- 6 [パーティション]コンテナを右クリックし、[新規]、[パーティション]の順にクリックします。

新規パーティションウィザードが起動します。

- 7 新規パーティションウィザードで、パーティションを作成する手順を実行します。

次の情報を指定する必要があります。

- パーティション名と説明。
- 新しいパーティションをクローズ、オープン、準備完了のどれで作成するか。含めることのできるオープンパーティションは1つのみです。オープンパーティションを作成すると、既存のすべてのオープンパーティションがクローズされます。
- パーティションを作成するデバイスの種類。ドロップダウンリストから、目的の種類のストレージデバイスを選択します。入力が必要な追加情報は、選択するデバイスの種類によって異なります。オプションについて詳しくは、ウィザードページの管理コンソールのヘルプを参照してください。
- デバイス上の新しいパーティションの場所。場所は **UNC** パスまたはドライブ文字で始まるパスとして入力できます。ネットワーク上の場所には、マップ済みネットワークドライブパスではなく、**UNC** 絶対パスを入力します。

---

**メモ:** 既存のパーティションの場所、または既存のパーティションに関連付けされたフォルダを含む場所は指定しないでください。ネットワーク共有またはマウントポイントを使う場合は、パーティションフォルダが重複しないように特に注意してください。フォルダが複数のパーティションに関連付けされていると、データが失われる可能性があります。

ストレージサービスは、2 つのパーティションで同じパスが共有されていることを検出した場合、起動しません。

**Enterprise Vault** では、パーティションのルートパスは空であると想定されます。ルートパスを使って、**Enterprise Vault** によって作成されたもの以外のファイルまたはフォルダを保持しないでください。

---

ストレージの種類を **[NTFS ボリューム]** として指定し、H:\... などのローカルパスを場所として指定すると、ストレージサービスによってパーティション用のネットワーク共有が作成されます。リモート **Enterprise Vault** サーバーのストレージサービスは、パーティションのデータにアクセスする必要がある場合にパーティションネットワーク共有を使います。

p.212 の「**ローカルパスを使った NTFS パーティションのパーティションネットワーク共有**」を参照してください。

¥¥server¥H\$¥¥partitionlocation などの管理共有が含まれた **UNC** パスを指定した場合は、管理共有を常に有効にする必要があります。サーバーの管理

共有を無効にすると、Enterprise Vault からパーティションにアクセスできません。

- ストレージデバイスで使われるストレージ設定。Enterprise Vault は、この情報を使ってデータストレージを最適化します。詳しくは、ウィザードページの管理コンソールのヘルプを参照してください。  
 ストレージ設定は、パーティションのプロパティの[ボリューム]タブで後から変更できます (ストレージモードを除く)。  
 デバイスのストレージの設定を後日変更する場合は、新しい動作を反映するためにパーティションのプロパティの[ボリューム]タブの関連ストレージの設定を更新する必要があります。
- Centera デバイス上のパーティションの場合、デバイスレベル共有を有効にするかどうか。
- このパーティションの機能を有効にすることを選択する場合は、パーティションロールオーバー条件。  
 Centera デバイスに準備完了パーティションを作成できますが、Centera によってホストされているパーティションから前方ロールオーバーを有効にすることはできません。
- セキュリティ ACL を使うかどうか。このオプションは Centera デバイスには適用されません。通常は、パーティション内のフォルダにあるセキュリティ ACL を使ってボルトストアパーティションを作成します。ただし、一部の光デバイスでは Enterprise Vault による ACL の追加を許可していません。  
 p.52 の「[データ場所の確保](#)」を参照してください。
- アーカイブが保全されたかどうか。
- ファイルコレクションソフトウェアを使うかどうか。コレクションファイルを使うことを選択した場合、コレクション基準を設定し、オプションで、コレクションファイルをセカンダリストレージに移行する方法とタイミングに関する詳細を指定できます。

## スマートパーティションの設定

スマートパーティションを設定する手順は、標準のボルトストアパーティションの設定手順とほぼ同じです。唯一の大きな違いは、スマートパーティションを設定するときに、スマートパーティションに関連付ける分類タグを 1 つ以上選択する必要があります。

### スマートパーティションを設定する方法

- 1 管理コンソールの左ペインで、[ボルトストアグループ]コンテナが表示されるまで、Enterprise Vault サイトの階層を展開します。
- 2 [ボルトストアグループ]コンテナを展開して、既存のボルトストアグループを表示します。

- 3 スマートパーティションを設定するボルトストアを含むボルトストアグループを展開します。
- 4 スマートパーティションを設定するボルトストアを展開します。
- 5 [スマートパーティション]コンテナを右クリックし、[新規作成]、[スマートパーティション]の順にクリックします。  
新規スマートパーティションウィザードが起動します。
- 6 画面に表示される指示に従います。以下の情報を指定する必要があります。
  - スマートパーティションの名前と説明
  - スマートパーティションの初期状態をオープンまたはクローズのどちらに設定するか
  - スマートパーティションと関連付ける分類タグ
  - パーティションを作成するストレージデバイスの種類
  - ストレージデバイス上の新しいパーティションの場所
  - ストレージデバイスで使用するストレージの設定
  - Dell EMC Centera デバイス上のパーティションの場合、デバイスレベル共有を有効にするかどうか
  - パーティションフォルダに、セキュリティ ACL を使用するスマートパーティションを作成するかどうか
  - スマートパーティションでバックアップを作成しているデータを確認する方法
  - ファイル収集ソフトウェアを使用して、大きい収集ファイルに多数の小さいファイルをまとめるかどうか

## ローカルパスを使った NTFS パーティションのパーティションネットワーク共有

ストレージの種類を[NTFS ボリューム]に指定し、ローカルパス(たとえば c:\¥... または H:\¥... で始まるパス)を指定している場合は、ストレージサービスでパーティションのネットワーク共有を作成します。リモート Enterprise Vault サーバーのストレージサービスは、パーティションのデータにアクセスする必要がある場合にパーティションネットワーク共有を使います。

---

**メモ:** UNC パスでパーティションの場所を指定すると Enterprise Vault はパーティションネットワーク共有を作成しません。

---

パーティションネットワーク共有を使うメリットは、ストレージサービスを開始するたびにローカルパーティションのネットワーク共有が検証されることです。共有の検証に失敗すると、ストレージサービスは新しいパーティションネットワーク共有を作成します。

パーティションネットワーク共有は次の形式の UNC パスでアクセスできます。

```
¥¥server¥EVPartitionnumber$
```

*server* は、パーティションがある Enterprise Vault サーバーです。*number* は重複のない 16 進数です。

ストレージサービスは、ボルトストアの共有レベルに関係なくパーティションネットワーク共有を作成します。ストレージサービスは、フルアクセス権があるボルトサービスアカウントにのみアクセス権を付与します。

ストレージサービスで初めてパーティションネットワーク共有を作成できなかった場合や検証に失敗してパーティションネットワーク共有を作成できなかった場合には、ストレージサービスは起動しません。Enterprise Vault はイベントログに次の説明とともにエラーを記録します。

```
The verification of a Partition Network Share failed.
```

Enterprise Vault がパーティションのルートパスにアクセスできない原因は、次のいずれかである可能性があります。

- ドライブがオフライン
- ディスクが壊れている
- コンピュータ名が変更されている
- クラスタ環境で共有ドライブを正しく設定していない

このエラーイベントが表示されたら、Windows エクスプローラを使ってローカル NTFS パーティションのローカルパスにアクセスできるかどうかを調べます。

## ボルトストアグループに対する共有の設定

ボルトストアグループにあるボルトストアの共有レベルを変更するには、そのボルトストアグループで共有を設定ウィザードを実行する必要があります。

---

**メモ:** 共有を設定ウィザードはいつでも再実行できますが、ボルトストアの共有レベルに対する変更は過去にさかのぼっては適用されません。

---

p.198 の「Enterprise Vault の単一インスタンスストレージの適切な共有設定の開発」を参照してください。

## ボルトストアグループに共有を設定する方法

- 1 管理コンソールの左ペインで、[ボルトストアグループ]が表示されるまで、**Enterprise Vault** サイトの階層を展開します。
- 2 [ボルトストアグループ]コンテナを展開して、既存のボルトストアグループを表示します。
- 3 共有を設定するボルトストアグループを右クリックし、ショートカットメニューの[プロパティ]をクリックします。
- 4 [共有]タブをクリックします。  
[共有]タブには、ボルトストアグループのボルトストアとその現在の共有レベルが一覧表示されます。
- 5 [共有を設定]をクリックします。  
共有を設定ウィザードが起動します。
- 6 デフォルトのアップグレードグループの特殊な場合として、グループのフィンガープリントデータベースがまだ存在していない場合、**Enterprise Vault** によってグループのフィンガープリントデータベースを設定できます。
- 7 共有を設定ウィザードを使うと、手順を追って、ボルトストアグループのボルトストアの共有レベルを設定できます。

1 つ以上のボルトストアの共有レベルを[ボルトストア内で共有する]または[グループ内で共有する]に変更した場合、ウィザードでは、変更を行う前に接続性テストを実行するように求めるメッセージが表示されます。接続性テストは、ネットワークの接続性が、選択した共有設定をサポートするのに十分であるかどうかを判断するのに役立ちます。

ウィザードでは、最後のページの[完了]をクリックするまで変更は行われません。

接続性テストの結果が良好ではなかった場合、次のいずれかを実行できます。

- [戻る]をクリックし、ボルトストアの共有レベルを変更し、接続性テストを再実行します。
- [キャンセル]をクリックして変更を破棄します。

接続性テストについて詳しくは、管理コンソールのヘルプの共有を設定ウィザードの項を参照してください。

# インデックスの場所の追加

この章では以下の項目について説明しています。

- Enterprise Vault のインデックスの場所について
- Enterprise Vault のインデックスの場所の作成

## Enterprise Vault のインデックスの場所について

Enterprise Vault によって、アーカイブごとにインデックスが自動的に作成されます。インデックスのサイズは、インデックス付けされたデータの量と、選択するインデックス付けのレベルによって異なります。[完全]インデックスは、元のデータによって使われる領域のおよそ 12% を必要とします。インデックスを格納するには、Enterprise Vault が使うインデックスの場所を 1 つ以上作成する必要があります。

Enterprise Vault のインデックスの設定および管理方法とベストプラクティスについて詳しくは、Veritas サポートサイトの次の記事を参照してください。

<https://www.veritas.com/docs/100037905>

次の点に注意してください。

- 開始ウィザードを実行した場合は、すでにインデックスの場所がいくつか作成されています。必要に応じて、さらにインデックスの場所を作成できます。
- ウイルス対策ソフトウェアによってデータが変更される可能性があるため、ウイルスチェックアプリケーションではインデックスの場所を除外しておくことが重要です。

## Enterprise Vault のインデックスの場所の作成

ローカル Administrators グループには、インデックスの場所に使うフォルダとその中のファイルへのフルアクセス権が必要です。ポリシーで別の方法を指示していない限り、これらのファイルとフォルダは誰からもアクセスできないようにする必要があります。

p.52 の「データ場所の確保」を参照してください。

### インデックスの場所を作成する方法

- 1 管理コンソールの左ペインで、Enterprise Vault サイト階層を展開して[Enterprise Vault サーバー]コンテナを表示します。
- 2 Enterprise Vault[サーバー]コンテナを展開します。
- 3 インデックスの場所を追加するインデックスサービスを実行するサーバーを展開します。
- 4 [サービス]をクリックします。
- 5 右ペインで[インデックスサービス]を右クリックし、ショートカットメニューで[プロパティ]をクリックします。
- 6 [インデックスの場所]タブをクリックします。
- 7 [追加]をクリックします。ボルトサービスアカウントのパスワードの入力を求めるメッセージが表示された場合は入力します。
- 8 [フォルダの選択]ダイアログボックスで、インデックスの格納場所として使用するフォルダを選択します。

場所の選択または作成にヘルプが必要な場合は、[ヘルプ]をクリックします。

新しいインデックスの場所を作成すると、Enterprise Vault によって、選択したフォルダ内に 8 つの新しいサブフォルダが作成されます。これらのサブフォルダには、index1、index2 などのように名前が付けられます。Enterprise Vault では、これらのサブフォルダを使ってインデックスを格納します。



# インデックスサーバーグループの設定

この章では以下の項目について説明しています。

- [インデックスサーバーグループについて](#)
- [インデックスサーバーグループを作成する必要がありますか？](#)
- [インデックスサーバーグループの作成](#)
- [インデックスサーバーグループにインデックスサーバーを追加](#)
- [インデックスサーバーグループからのインデックスサーバーの削除](#)
- [インデックスサーバーグループへのボルトストアの割り当て](#)
- [インデックスサーバーグループからのボルトストアの割り当て解除](#)
- [ボルトストアを別のインデックス付けに割り当てる](#)

## インデックスサーバーグループについて

インデックスサーバーは **Enterprise Vault** インデックスサービスがインストールされた **Enterprise Vault** サーバーです。インデックスサーバーはインデックスサーバーグループのメンバーに指定することも、グループ解除することもできます。

インデックスサーバーグループのインデックスサーバーでは次の操作を行います。

- インデックスサーバーグループと関連付けされたボルトストアをインデックス付けします。
- クエリーの検索に応答します。

インデックスサーバーグループはグループの異なるサーバーに新しいインデックスボリュームを割り当てます。ジャーナルアーカイブに属するインデックスボリュームを、グループの異なるサーバーに割り当てます。

デフォルトでは、**Enterprise Vault** はメールボックスアーカイブをホストするストレージサービスのあるインデックスサーバーグループのサーバーに、メールボックスのインデックスボリュームを割り当てようとしています。メールボックスがインデックスサーバーグループのインデックスサーバーでホストされていない場合、インデックスサーバーグループ内の任意のインデックスサーバーが使用される可能性があります。

- 別のサーバーにストレージサービスとインデックスサービスを配置する場合、これらのサービス間の通信はネットワークトラフィックで増加します。

---

**メモ:** ネットワークが追加の要求に対処できない場合は、インデックスサーバーグループでの利点はありません。

---

- インデックスサーバーグループは、**Enterprise Vault** の大規模環境または分散環境にインデックスサービスを提供します。分散環境では、**Enterprise Vault** サーバーがストレージサービスをホストすることもあれば、インデックスサービスをホストすることもあります。

『[Enterprise Vault Indexing](#)』ホワイトペーパーおよび『導入/計画』ガイドの「[Enterprise Vault indexing](#)」を参照してください。

## インデックスサーバーグループを作成する必要がありますか？

**表 28-1** はインデックスサーバーグループに利点があるかどうかを判断するさまざまな考慮事項をリストします。

**表 28-1**                      インデックスサーバーグループの考慮事項

Enterprise Vault の環境	詳細
複数の Enterprise Vault サーバーがありますか？	p.219 の「 <a href="#">複数の Enterprise Vault サーバーがありますか？</a> 」を参照してください。
ジャーナルアーカイブまたはファイルシステムアーカイブを使いますかまたは使う計画はありますか？	p.219 の「 <a href="#">ジャーナルアーカイブまたはファイルシステムアーカイブを使いますかまたは使う計画はありますか？</a> 」を参照してください。
Compliance Accelerator または Discovery Accelerator を使いますかまたは使う計画はありますか？	p.220 の「 <a href="#">Compliance Accelerator または Discovery Accelerator を使いますかまたは使う計画はありますか？</a> 」を参照してください。

Enterprise Vault の環境	詳細
現在 Enterprise Vault を使う場合は、サーバーの負荷の分散は不揃いですか？	p.220 の「サーバーのロードは既存の Enterprise Vault サーバーに均等に分散されていますか？」を参照してください。
Enterprise Vault サーバーあたりおよそ 5,000 以上のメールボックスのアーカイブがありますか？	p.221 の「Enterprise Vault サーバーあたりおよそ 5,000 以上のメールボックスのアーカイブがありますか？」を参照してください。

すべての質問またはほとんどの質問に「いいえ」と答えた場合は、ご使用の環境でインデックスサーバーグループを使うことが効果的であるとはいえない可能性があります。

## 複数の Enterprise Vault サーバーがありますか？

受け入れ可能なパフォーマンスがある単一の Enterprise Vault サーバーがある場合は、インデックスサーバーグループでの利点はありません。他のサーバーを追加する場合は、インデックスサーバーグループでの利点があります。

複数の Enterprise Vault サーバーがある場合、1 つ以上のインデックスサーバーグループにインデックスサービスを用いるサーバーをグループ化できます。

利点は十分に利用されていないサーバーかインデックス付け要求またはアーカイブ要求に対処できない他のサーバーかどうかによって異なります。

たとえば、サーバーが 3 つあり、1 つが Exchange ジャーナルアーカイブ専用で、2 つがメールボックスアーカイブ専用であると仮定します。この場合、インデックスサーバーグループにすべてのサーバーを配置すると有利です。グループ化により、3 つのすべてのサーバー間でジャーナルアーカイブインデックスボリュームを分散できます。この分散の効力は Discovery Accelerator アプリケーションの検索パフォーマンスを高めることです。

## ジャーナルアーカイブまたはファイルシステムアーカイブを使いますかまたは使う計画はありますか？

ジャーナルアーカイブまたは FSA のアーカイブを使う場合、次のどちらかまたは両方の操作を実行すると有利です。

- インデックス付け負荷を分散するためにインデックスサーバーグループにインデックスサービスを用いたサーバーをグループ化します。
- ジャーナルアーカイブと FSA のアーカイブを含むボルトストアのインデックス付け専用のインデックスサーバーグループに新しいサーバーを追加します。

この設定はサーバー間の大きいインデックスボリュームを分散するので検索パフォーマンスも向上させます。

## Compliance Accelerator または Discovery Accelerator を使いますか または使う計画はありますか？

Compliance Accelerator または Discovery Accelerator を使う場合は、次の操作を実行すると効果的です。

- 検索負荷を分散するためにインデックスサーバーグループにインデックスサービスを用いたサーバーをグループ化します。
- アーカイブがアーカイブの種類によって分割されるようにボルトストアを整理します。たとえば、ジャーナルアーカイブの特定のボルトストアを使います。それからインデックスサーバーグループに特定のアーカイブの種類を含むボルトストアを割り当てることができます。
- Compliance Accelerator または Discovery Accelerator が検索するそれらのアーカイブを含むボルトストアのインデックス付け専用のインデックスサーバーグループに新しいサーバーを追加します。

この設定は別のサーバー間の大きいインデックスボリュームを分散します。検索パフォーマンスは現在複数のサーバーにクエリーの並列実行があるので向上します。

## サーバーのロードは既存の Enterprise Vault サーバーに均等に分散されていますか？

Enterprise Vault サーバーは、アーカイブタスクとインデックス付けタスクの両方とストレージサービスがすべてリソースを共有しているため、過負荷が生じます。メモリと CPU 容量が不足しているサーバーもありますが、十分に利用されていないサーバーもあります。

次の操作を実行すると有利です。

- 一部またはすべてのボルトストアのインデックス付けと検索専用のインデックスサーバーグループに新しいサーバーを追加します。
- アーカイブが種類によって分割されるようにボルトストアを整理します。たとえば、ジャーナルアーカイブの特定のボルトストアを使います。それからインデックスサーバーグループに特定のアーカイブの種類を含むボルトストアを割り当てることができます。

この変更には次の利点があります。

- インデックス付け CPU とメモリの必要条件はインデックスサーバー間で共有します。
- インデックス付け負荷はアーカイブタスクとストレージタスクを実行するサーバーから削除されます。
- 別のサーバーに専用のリソースがあるのでインデックス付けと検索のパフォーマンスが向上します。

## Enterprise Vault サーバーあたりおよそ 5,000 以上のメールボックスのアーカイブがありますか？

インデックス付けおよび検索は多数のメールボックスのアーカイブを備えている Enterprise Vault サーバーに負荷を生じることがあります。

メールボックスのアーカイブを含むそれらのボルトストアのインデックス付け専用のインデックスサーバーグループに新しいサーバーを追加すると有利です。

この設定はインデックスサーバーグループのサーバー間で新しいメールボックスのアーカイブと関連付けされたそれらのインデックスボリュームを分散します。この分散により、別のサーバーで多数のアーカイブの同時クエリーを処理できます。

Enterprise Vault サーバーは大量のインデックスボリュームを検索することによって負荷が生じます。ユーザーが多くの検索のタイムアウトを見つけた場合は、インデックスグループが探索時間を短縮することができます。他の問題が不十分な検索パフォーマンスの原因である場合は、インデックスサーバーグループがパフォーマンスを向上させることはままありません。たとえば、インデックスサーバーグループは IIS に負荷が生じた場合パフォーマンスを向上できません。

メールボックスのアーカイブを含むボルトストアのインデックス付けおよび検索専用のインデックスサーバーグループに新しいサーバーを追加することができます。

この変更には次の利点があります。

- インデックスボリュームが複数のサーバー間で分散されるのでインデックス付けパフォーマンスが向上しました。
- 多くのアーカイブへの同時クエリーが複数のサーバー間で分散されるので検索パフォーマンスが向上しました。

## インデックスサーバーグループの作成

最初のインデックスサーバーグループを作成する前に、Enterprise Vault サイトに対するインデックスサーバーグループのメリットがあるかどうかを確認します。

p.217 の「[インデックスサーバーグループについて](#)」を参照してください。

p.218 の「[インデックスサーバーグループを作成する必要がありますか?](#)」を参照してください。

インデックスサーバーグループを作成するには

- 1 管理コンソールで、Enterprise Vault コンテナを展開します。
- 2 [ディレクトリ]コンテナを展開します。
- 3 Enterprise Vault サイトを展開します。
- 4 [インデックス]コンテナを展開します。

- 5 [インデックスサーバーグループ]を右クリックし、ショートカットメニューを[新規作成]、[インデックスサーバーグループ]の順にクリックします。

新規インデックスサーバーグループウィザードが起動します。サイトに 1 つのみインデックスサーバーがある場合、インデックスサーバーグループのメリットがないことを説明するメッセージが表示されます。それでもインデックスサーバーグループを作成する場合には、[続行]をクリックします。

- 6 ウィザード概要ページでは、インデックスサーバーグループに関する情報についての文書が参照できます。

『導入/計画』の「インデックスサーバーグループについて」のセクションを参照してください。

[次へ]をクリックして、[名前と説明]ページに移動します。

- 7 インデックスサーバーグループに[名前]と省略可能なオプションとして[説明]を入力します。この[名前]と[説明]はいつでも変更できます。

[次へ]をクリック

- 8 新しいインデックスサーバーグループに追加するインデックスサーバーを選択します。ここで、インデックスサーバーを追加するための必要条件はありません。必要に応じて、後でインデックスサーバーを追加することもできます。

[次へ]をクリックします。

- 9 新しいインデックスサーバーグループへのインデックスサーバーの追加を選択した場合、その新しいインデックスサーバーグループにボルトストアを関連付ける選択ができるようになります。

インデックスサーバーグループにインデックスサーバーを追加するとき、その関連するボルトストアは、自動的に含まれません。Enterprise Vault では、自らインデックスサーバーグループに関連付けるまで、それらのボルトストアをインデックスしません。それらのボルトストアが新しいインデックスサーバーグループによってインデックスされることを望む場合、[新しいインデックスサーバーグループに追加するように選択したサーバーによって現在インデックス付けされているすべてのボルトストア]を選択します。

[次へ]をクリックします。

- 10 [次へ]をクリックします。ページに、入力した詳細情報が表示されます。

- 11 [インデックスサーバーグループの作成]をクリックしてください。ウィザードは新しいインデックスサーバーグループを作成し、概要ページを表示します。

- 12 [閉じる]をクリックしてウィザードを終了します。

新しいインデックスサーバーグループにインデックスサーバーを追加しなかった場合は、インデックスサーバーグループのプロパティを編集してインデックスサーバーを追加できます。

p.223 の「[インデックスサーバーグループにインデックスサーバーを追加](#)」を参照してください。

## インデックスサーバーグループにインデックスサーバーを追加

インデックスサーバーは、インデックスサーバーグループにいつでも追加できます。インデックスサーバーグループのメンバーとしてデータがインデックス処理されると、そのインデックスサーバーをインデックスサーバーグループから削除することはできません。

---

**メモ:** インデックスサーバーグループにインデックスサーバーを追加するとき、その関連するボルトストアは、自動的に含まれません。インデックスサーバーグループのプロパティにある[ボルトストア]タブを使用して、それらのボルトストアをそのインデックスサーバーグループに関連付けます。

---

### インデックスサーバーをインデックスサーバーグループに追加するには

- 1 管理コンソールで、Enterprise Vault コンテナを展開します。
- 2 [ディレクトリ]コンテナを展開します。
- 3 Enterprise Vault サイトを展開します。
- 4 [インデックス]コンテナを展開します。
- 5 [インデックスサーバーグループ]を展開します。
- 6 インデックスサーバーを追加するグループを右クリックし、[プロパティ]をクリックします。
- 7 インデックスサーバーグループのプロパティで、[インデックスサーバー]タブをクリックします。一覧に、グループにすでにあるインデックスサーバーが表示されます。
- 8 [追加]をクリックします。一覧に、インデックスサーバーグループに追加できるインデックスサーバーが表示されます。
- 9 インデックスサーバーグループに追加するインデックスサーバーをクリックします。

ネットワークパフォーマンスを調べるために接続性テストを実行できます。テストはネットワークがインデックスサーバーグループ内の受け入れ可能なパフォーマンスを提供するかどうかを判断するのに役立ちます。このテストは、インデックスサーバーとインデックスサーバーグループに関連付けされたボルトストア間の ping 要求に対する応答時間を判断します。

接続テストを実行するには、以下の操作を行います。

- [接続性テスト]をクリックします。ダイアログボックスを展開して[接続性テスト]セクションを表示します。

- [テストを実行]をクリックします。  
テストは実行に数秒かかることがあります。リストは結果の概略を表示します。詳細を参照するには、[レポート]をクリックします。
- 10 追加したいインデックスサーバーを選択したら、[OK]をクリックします。続行するかどうかを確認するメッセージが表示されます。インデックスサーバーグループのメンバーとしてデータがインデックス処理されると、そのインデックスサーバーをインデックスサーバーグループから削除することはできません。[はい]をクリックして続行します。

また、インデックスサーバーをインデックスサーバーグループから削除することもできます。

p.224 の「[インデックスサーバーグループからのインデックスサーバーの削除](#)」を参照してください。

## インデックスサーバーグループからのインデックスサーバーの削除

インデックスサーバーグループからインデックスサーバーを削除するには、次の制限があります。

- インデックスサーバーグループのメンバーとしてデータがインデックス処理されると、そのインデックスサーバーをインデックスサーバーグループから削除することはできません。
- 未完了のインデックスタスクと関連付けられたインデックスサーバーを削除することはできません。

### インデックスサーバーグループからインデックスサーバーを削除する方法

- 1 管理コンソールで、Enterprise Vault コンテナを展開します。
- 2 [ディレクトリ]コンテナを展開します。
- 3 Enterprise Vault サイトを展開します。
- 4 [インデックス]コンテナを展開します。
- 5 [インデックスサーバーグループ]を展開します。
- 6 インデックスサーバーを削除するグループを右クリックし、[プロパティ]をクリックします。
- 7 インデックスサーバーグループのプロパティで、[インデックスサーバー]タブをクリックします。一覧に、グループにすでにあるインデックスサーバーが表示されます。
- 8 インデックスサーバーグループから削除するインデックスサーバーをクリックします。
- 9 [削除]をクリックします。  
確認メッセージに対して[はい]をクリックします。



# インデックスサーバーグループへのボルトストアの割り当て

インデックスサーバーグループにインデックスサーバーを追加するとき、その関連するボルトストアは、自動的に含まれません。Enterprise Vault では、自らインデックスサーバーまたはインデックスサーバーグループに割り当てるまで、それらのボルトストアをインデックスしません。

## インデックスサーバーグループにボルトストアを追加する方法

- 1 管理コンソールで、Enterprise Vault コンテナを展開します。
- 2 [ディレクトリ]コンテナを展開します。
- 3 Enterprise Vault サイトを展開します。
- 4 [インデックス]コンテナを展開します。
- 5 [インデックスサーバーグループ]を展開します。
- 6 インデックスサーバーを追加するグループを右クリックし、[プロパティ]をクリックします。
- 7 インデックスサーバーグループのプロパティで、[ボルトストア]タブをクリックします。リストはインデックスサーバーグループに割り当て済みであるボルトストアを示します。
- 8 [追加]をクリックします。次のように、インデックスサーバーグループに追加できるボルトストアが一覧表示されます。
  - Enterprise Vault のボルトストアは、インデックスしません。インデックスサーバーグループに追加されているインデックスサーバーに関連付けられたボルトストアが存在する可能性があります。
  - インデックスサーバーグループにないインデックスサーバーによって現在インデックスされているボルトストア。
- 9 インデックスサーバーグループと関連付けるボルトストアを選択します。
- 10 ネットワークパフォーマンスを調べるために接続性テストを実行できます。テストはネットワークがインデックスサーバーグループ内の受け入れ可能なパフォーマンスを提供するかどうかを判断するのに役立ちます。このテストは、ボルトストアとインデックスサーバーグループ内のインデックスサーバー間の ping 要求に対する応答時間を判断します。

接続テストを実行するには、以下の操作を行います。

- [接続性テスト]をクリックします。ダイアログボックスを展開して[接続性テスト]セクションを表示します。
- [テストを実行]をクリックします。

テストは実行に数秒かかることがあります。リストは結果の概略を表示します。詳細を参照するには、[レポート]をクリックします。

11 追加したいインデックスサーバーを選択したら、[OK]をクリックします。

また、インデックスサーバーグループからボルトストアを割り当て解除することもできます。

p.226 の「[インデックスサーバーグループからのボルトストアの割り当て解除](#)」を参照してください。

## インデックスサーバーグループからのボルトストアの割り当て解除

インデックスサーバーグループからボルトストアを割り当て解除するには、次の制限があります。

- インデックスサーバーグループのメンバーによってボルトストアのデータがインデックス処理されると、そのボルトストアをインデックスサーバーグループから割り当て解除することはできません。
- 未完了のインデックスタスクと関連付けられたボルトストアを割り当て解除することはできません。

### インデックスサーバーグループからボルトストアを割り当て解除する方法

- 1 管理コンソールで、Enterprise Vault コンテナを展開します。
- 2 [ディレクトリ]コンテナを展開します。
- 3 Enterprise Vault サイトを展開します。
- 4 [インデックス]コンテナを展開します。
- 5 [インデックスサーバーグループ]を展開します。
- 6 インデックスサーバーを追加するグループを右クリックし、[プロパティ]をクリックします。
- 7 インデックスサーバーグループのプロパティで、[ボルトストア]タブをクリックします。リストはインデックスサーバーグループに割り当て済みであるボルトストアを示します。
- 8 インデックスサーバーグループから割り当て解除するボルトストアをクリックします。
- 9 [削除]をクリックします。
- 10 [はい]をクリックします。

## ボルトストアを別のインデックス付けに割り当てる

次のように、ボルトストアを別のインデックス付けに再割り当てすることができます。

- まだインデックスサーバーグループに割り当てられていないボルトストアをインデックスサーバーグループに再割り当てすることができます。
- ボルトストアをあるインデックスサーバーグループから別のインデックスサーバーグループに再割り当てすることができますが、現在のインデックスサーバーグループが、そのボルトストアにおいてまだ何もインデックスしていない場合に限りです。

### ボルトストアを別のインデックス付けに割り当てる方法

- 1 管理コンソールで、Enterprise Vault コンテナを展開します。
  - 2 [ディレクトリ]コンテナを展開します。
  - 3 Enterprise Vault サイトを展開します。
  - 4 [ボルトストアグループ]コンテナを展開します。
  - 5 修正したいボルトストアを含むボルトストアグループを展開します。
  - 6 別のインデックス付けに割り当てたいボルトストアを右クリックして、[プロパティ]をクリックします。
  - 7 ボルトストアのプロパティにおいて[インデックス付け]タブをクリックします。  
 インデックス付けのセクションは、ボルトストアが現在、単一のインデックスサーバーによってインデックスされているか、インデックスサーバーグループによってインデックスされているか、またはインデックスされていないか、を示します。
  - 8 [変更]をクリックします。  
 リストは、ボルトストアを割り当て可能なインデックスサーバーグループを示します。
  - 9 ボルトストアを割り当てたいインデックスサーバーグループをクリックします。
  - 10 ネットワークパフォーマンスを調べるために接続性テストを実行できます。テストはネットワークがインデックスサーバーグループ内の受け入れ可能なパフォーマンスを提供するかどうかを判断するのに役立ちます。このテストは、ボルトストアとインデックスサーバーグループ内のインデックスサーバー間の ping 要求に対する応答時間を判断します。  
 接続テストを実行するには、以下の操作を行います。
    - [接続性テスト]をクリックします。ダイアログボックスを展開して[接続性テスト]セクションを表示します。
    - [テストを実行]をクリックします。  
 テストは実行に数秒かかることがあります。リストは結果の概略を表示します。詳細を参照するには、[レポート]をクリックします。
  - 11 新しいインデックスサーバーグループを選択している場合、[OK]をクリックします。
  - 12 [OK]をクリックしてボルトストアのプロパティを閉じます。
- また、インデックスサーバーグループからボルトストアを割り当て解除することもできます。

p.226 の「[インデックスサーバーグループからのボルトストアの割り当て解除](#)」を参照してください。

# サイトのデフォルト設定のレビュー

この章では以下の項目について説明しています。

- [Enterprise Vault サイトのデフォルト設定のレビュー](#)

## Enterprise Vault サイトのデフォルト設定のレビュー

Enterprise Vault サイトのプロパティに設定されているデフォルト設定を確認します。

サイトのプロパティには次の設定が含まれます。これらの一部は、下位レベルで上書きできます。たとえば、タスクプロパティでスケジュールを設定することによって、特定のタスクのサイトアーカイブスケジュールを上書きできます。

表 29-1                      サイトプロパティ

タブ	設定
全般	<ul style="list-style-type: none"><li>■ ボルトサイトエイリアスと説明。</li><li>■ <b>Web Access</b> アプリケーションで使うプロトコルとポート。</li><li>■ <b>Web Access</b> アプリケーションのユーザーのシステムメッセージ (必要な場合)。</li><li>■ <b>PST</b> 保留領域詳細のサイトプロパティ設定は <b>Exchange Server</b> アーカイブにのみ適用されます。</li><li>■ 管理者用のメモ (必要な場合)。</li></ul>

タブ	設定
アーカイブの設定	<ul style="list-style-type: none"> <li>■ デフォルトの保持カテゴリ。</li> <li>■ 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がある処理を実行したときに更新を許可するかどうか。</li> <li>■ アーカイブ内のアイテムの削除をユーザーに許可するかどうか。</li> <li>■ ユーザーが削除したアイテムを回復できるかどうか。</li> <li>■ 削除済みアイテムが回復に利用可能である期間。</li> </ul>
ストレージの有効期限	<ul style="list-style-type: none"> <li>■ ストレージの有効期限機能を実行するためのスケジュール。この設定に従って、割り当てられた保持期間よりも古いすべてのアイテムがアーカイブから削除されます。</li> <li>■ 有効期限の計算をアイテムの変更日、またはアーカイブ日から開始するか設定。</li> </ul>
サイトスケジュール	<ul style="list-style-type: none"> <li>■ 自動バックグラウンドアーカイブを実行するためのスケジュール。</li> </ul>
アーカイブの使用限度	<ul style="list-style-type: none"> <li>■ 必要に応じて、アーカイブサイズの限度を設定できます。</li> </ul>
インデックス	<ul style="list-style-type: none"> <li>■ インデックスレベル: [簡略]または[完全]。</li> <li>■ Disclaimer など、インデックス付けすべきではない電子メールの内容。</li> <li>■ インデックスサブタスクが削除されるまでの保留期間。</li> </ul>
詳細	<ul style="list-style-type: none"> <li>■ Enterprise Vault サイト内での Enterprise Vault のインデックス付け動作の調整に使える詳細設定。 <b>メモ:</b> テクニカルサポートプロバイダの指示がない限り、[インデックス]設定は変更しないでください。</li> </ul>
監視	<ul style="list-style-type: none"> <li>■ Enterprise Vault を監視するためのパフォーマンスカウンタ。</li> </ul>

### Enterprise Vault サイトのデフォルト設定をレビューする方法

- 1 管理コンソールで、Enterprise Vault サイトが表示されるまで、左側のペインの内容を展開します。
- 2 Enterprise Vault サイトを右クリックし、ショートカットメニューの[プロパティ]をクリックします。  
  
代わりに、サイトを選択し、ツールバーの[サイトプロパティを確認]ボタンをクリックすることもできます。
- 3 詳しい情報を参照するには、[サイトプロパティ]タブの[ヘルプ] をクリックします。

## Enterprise Vault サイトのアーカブスケジュールの設定

各アーカブタスクやサービスは、定義したスケジュールに従って実行されます。各タスクに利用できるスケジュールは次のとおりです。

- デフォルトのスケジュール。これはサイトプロパティで設定します。このスケジュールは Enterprise Vault サイトのすべてのアーカブタスクに適用されます。
- タスク固有のスケジュール。これはプロパティを編集して設定します。タスクに固有の設定を行う場合はこのスケジュールを編集して、サイトプロパティの設定を上書きします。

### Enterprise Vault サイトのアーカブスケジュールの設定方法

- 1 管理コンソールの左ペインで、サイトの階層を Enterprise Vault サイト名が表示されるまで展開します。
- 2 サイト名を右クリックして、[プロパティ]をクリックします。
- 3 [サイトスケジュール]タブをクリックします。
- 4 必要に応じてスケジュールを修正します。[サイトスケジュール]タブの使い方について詳しくはヘルプを参照してください。

スケジュールのある時間帯は青く、ない時間帯には白で表されます。

## Web Access アプリケーションの設定について

管理コンソールのサイトプロパティの[全般]ページで、Enterprise Vault Web Access アプリケーションにアクセスするためのプロトコルとポートを設定できます。

Web Access アプリケーションのデフォルトの URL は /EnterpriseVault に設定されています。これは、IIS の Web Access アプリケーション用の仮想ディレクトリの名前です。クライアントが Web Access アプリケーションに接続してアーカブにアクセスすると、Enterprise Vault は完全な URL を動的に作成します。

新規インストールでは、Web Access アプリケーションにはデフォルトでポート 443 経由の HTTPS を使用してアクセスします。Web Access アプリケーションの完全な URL は次のとおりです。

`https://FQDN/EnterpriseVault`

FQDN は、ユーザーのアーカブのためのストレージサービスをホストする Enterprise Vault サーバーの完全修飾ドメイン名です。

IIS コンピュータで別のポートまたはプロトコルが必要な場合は、[TCP ポートを使用]オプションまたは[SSL ポートで HTTPS を使用]オプションを使って必要な値を設定できます。

---

**メモ:** アイテムのアーカイブ後に、**Web Access** アプリケーションにアクセスするために使われるプロトコルまたはポートを変更した場合、既存のショートカットは動作しなくなります。

---

p.144 の「[Enterprise Vault Web Access コンポーネント用のポートまたはプロトコルのカスタマイズ](#)」を参照してください。



# Enterprise Vault 検索の設定

この章では以下の項目について説明しています。

- [Enterprise Vault による検索について](#)
- [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 による検索について

Enterprise Vault による検索を使うと、Enterprise Vault クライアントユーザーは自分のアーカイブを参照して、検索アクセスを行うことができます。

Enterprise Vault による検索のモバイル版では、ユーザーは Android、iOS、または Windows Mobile のスマートフォンから保有するアーカイブにアクセス可能になります。

表 30-1 [Enterprise Vault による検索]の設定手順

手順	Action	説明
手順 1	1 つ以上の検索ポリシーを定義して、ユーザーが利用できるようにする[Enterprise Vault による検索]の範囲を指定します。	p.234 の「Enterprise Vault Search ポリシーの定義」を参照してください。
手順 2	1 つ以上の検索プロビジョニンググループを設定して、検索ポリシーを割り当てる対象となるユーザーまたはユーザーグループを特定します。	p.237 の「Enterprise Vault による検索用のプロビジョニンググループの設定」を参照してください。
手順 3	1 つ以上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し、必要な検索ポリシーをプロビジョニンググループのターゲットに適用します。	p.239 の「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」を参照してください。
手順 4	Enterprise Vault による検索用のユーザーのブラウザを設定します。	p.240 の「Enterprise Vault Search に対するユーザーのブラウザの構成」を参照してください。
手順 5	Enterprise Vault による検索のモバイル版の設定。	p.242 の「Enterprise Vault 検索モバイル版の設定」を参照してください。

続行する前に、Enterprise Vault サーバーが[Enterprise Vault による検索]の必要条件を満たしていることを確認することが重要です。

p.106 の「Enterprise Vault による検索のサーバー必要条件」を参照してください。

## 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.236 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す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](http://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イ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探索します。

```
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.107 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。

p.144 の「[Enterprise Vault Web Access コンポーネント用のポートまたはプロトコルのカスタマイズ](#)」を参照してください。

## 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ができることを確認します。

- 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。

# メタデータストアの管理

この章では以下の項目について説明しています。

- [メタデータストアについて](#)
- [メタデータストアの PowerShell コマンドレットについて](#)
- [高速参照とメタデータストアのインデックスについて](#)

## メタデータストアについて

メタデータストアは、Enterprise Vault アーカイブから抽出したさまざまなインデックス属性を含んでいます。メタデータストアを使うと、さまざまな Enterprise Vault クライアントアプリケーションのインデックスメタデータにすばやくアクセスできます。Enterprise Vault は、必要に応じてメタデータストアを自動的に作成します。

アーカイブのメタデータストアは、関連付けられたボルトストアデータベースで保持されます。メタデータストアは、このデータベースのサイズを増やします。サイズについて詳しくは、次の URL で『Enterprise Vault SQL のベストプラクティスガイド』を参照してください。

[https://www.veritas.com/support/ja\\_JP/article.100012617](https://www.veritas.com/support/ja_JP/article.100012617)

管理コンソールの[サイトプロパティ]にある[アーカイブの設定]タブで、高速参照を自動的に有効にするアーカイブの種類を制御できます。既存のアーカイブの高速参照を有効にすることもできます。Enterprise Vault は、IMAP を使ってアクセスするアーカイブのメタデータストアを常に作成します。『IMAP のセットアップ』ガイドを参照してください。

Enterprise Vault は、アーカイブのメタデータストアを作成して Enterprise Vault による検索の高速参照を提供することができます。Enterprise Vault による検索に対してユーザーを有効にすると、Enterprise Vault はこれらのユーザーが検索を使った後に、関連付けられたメタデータストアのみを作成します。

p.233 の「[Enterprise Vault による検索について](#)」を参照してください。

Enterprise Vault による検索を使う前に一部のユーザーのメタデータストアを作成する場合は、New-EVMDSBuildTask PowerShell cmdlet を使うことができます。

## メタデータストアの PowerShell コマンドレットについて

Enterprise Vault では、アーカイブのメタデータストアの管理に役立つ次の PowerShell コマンドレットを使うことができます。

- New-EVMDSBuildTask。このコマンドレットは、アーカイブのメタデータストアを構築または再構築するインデックス付けタスクを作成します。コマンドレットは、Enterprise Vault 検索を使う前に一部のユーザーのメタデータストアを作成する場合に最も役立ちます。

このコマンドレットは自動的にアーカイブの高速参照を有効にするので、管理コンソールで高速参照を設定する必要はありません。

CSV ファイルをインポートして、処理するアーカイブを指定できます。

New-EVMDSBuildTask コマンドレットのヘルプを参照してください。

Get-MDSStatus から New-EVMDSBuildTask に出力をパイプして、複数のアーカイブを処理することもできます。例については、New-EVMDSBuildTask コマンドレットのヘルプを参照してください。

- Get-EVMDSStatus。このコマンドレットは、アーカイブメタデータストアの現在の状態を取得します。アーカイブのメタデータストアで見つからないアイテムの数を判断することもできます。

[無効]、[ビルドの保留]、[ビルド中]、[準備完了]、[ビルドに失敗しました]のいずれかの状態が示されます。

CSV ファイルをインポートして、状態を取得するアーカイブを指定できます。例については、Get-EVMDSStatus コマンドレットのヘルプを参照してください。

## 高速参照とメタデータストアのインデックスについて

アーカイブの高速参照が有効な場合には、Enterprise Vault はそのアーカイブのメタデータストアを作成します。メタデータストアは、そのアーカイブのボルトストアデータベースの最適化インデックスです。Enterprise Vault 検索でこのインデックスを使って、ユーザーがアーカイブを参照するときにアーカイブの内容に応答するビューを表示します。

Enterprise Vault 検索はメタデータストアがなくても働きますが、ストアがあるほうが応答がよくなります。

アーカイブのメタデータストアは、EVMDSBuildTask タスクで作成されます。

EVMDSBuildTask タスクを監視し、管理するには、管理コンソールの[インデックスタスクの監視]オプションを使います。「Metadata Store」でタスクビューをフィルタ処理すると、メタデータストアタスクのみを表示できます。



# VCS による Enterprise Vault のクラスタ化

- [第32章 VCS によるクラスタ化の概要](#)
- [第33章 Storage Foundation HA for Windows のインストールと設定](#)
- [第34章 Enterprise Vault の VCS サービスグループの設定](#)
- [第35章 Enterprise Vault 設定ウィザードの実行](#)
- [第36章 Enterprise Vault での SFW HA-VVR のディザスタリカバリソリューションの実装](#)
- [第37章 VCS によるクラスタ化のトラブルシューティング](#)

# VCS によるクラスタ化の概要

この章では以下の項目について説明しています。

- サポートされる VCS 設定とソフトウェア
- Enterprise Vault と VCS GenericService エージェントについて
- VCS クラスタでの一般的な Enterprise Vault 構成
- VCS 環境にコンポーネントをインストールして設定する順序

## サポートされる VCS 設定とソフトウェア

---

**メモ:** このマニュアルでは終始、VCS と SFW HA (*Storage Foundation HA for Windows*) という用語を使っています。ただし、バージョン 7.0 のクラスタソフトウェアでは、これらの用語の代わりにそれぞれ *Veritas InfoScale Availability* と *Veritas InfoScale Enterprise* という用語を使っています。

---

アクティブ/パッシブ構成と N+1 構成はどちらもサポートされていますが、アクティブ/アクティブ構成はサポートされていません。

アクティブ/パッシブ構成は、各 Enterprise Vault サーバーに専用のスペアサーバーを用意して、プライマリサーバーの停止時に備えて待機させておく構成です。N+1 構成は、各 Enterprise Vault サーバーに 1 台のコンピュータを用意して、いずれかのアクティブサーバーのフェールオーバーに備えて 1 台以上のスペアサーバーを待機させておく構成です。

次のソフトウェアがインストールされている必要があります。

- サポート対象バージョンの VCS

- Enterprise Vault
- サポート対象バージョンの Windows Server

ソフトウェアのサポート対象バージョンについて詳しくは、Enterprise Vault [Compatibility Charts](#) を参照してください。

計画しているクラスタ内のサーバーには、Compliance Accelerator も Discovery Accelerator もインストールしないでください。これらの製品はクラスタ内ではサポートされません。ただし、クラスタ化されていない Compliance Accelerator または Discovery Accelerator はクラスタ化された Enterprise Vault 仮想サーバーを参照できます。

## Enterprise Vault とVCS GenericService エージェントについて

VCS GenericService エージェントは次の Enterprise Vault のサービスをオンラインにして、それらの状態を監視した後、オフラインに戻します。

- 管理サービス
- ディレクトリサービス
- インデックスサービス
- ショッピングサービス
- ストレージサービス
- タスク制御サービス
- SMTP サービス (Enterprise Vault サーバーに Enterprise Vault SMTP アーカイブコンポーネントをインストールして設定している場合のみ)

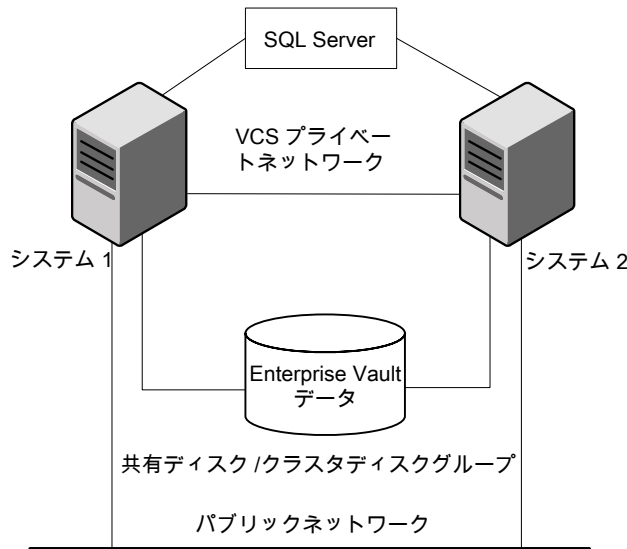
リソースの種類の定義、属性の定義、設定例など、GenericService エージェントについて詳しくは『Cluster Server 付属エージェントリファレンスガイド』を参照してください。

GenericService エージェントは、設定したサービスが実行されない場合にアプリケーションエラーを検出します。エラーが検出されると、Enterprise Vault サービスグループは、サービスグループのシステム一覧で次に利用可能なシステムにフェールオーバーし、サービスはその新しいシステム上で起動されます。これにより、Enterprise Vault が管理、アーカイブしているデータの可用性を維持できます。

## VCS クラスタでの一般的な Enterprise Vault 構成

図 32-1 は、一般的な構成を示しています。

図 32-1 アクティブ/パッシブフェールオーバー構成



この例では、Enterprise Vault サービスデータ用のボリュームが、共有ストレージのクラスタディスクグループに設定されています。Enterprise Vault 仮想サーバーはアクティブノード (システム 1) に設定されています。システム 1 でエラーが発生した場合、システム 2 がアクティブノードとなり、Enterprise Vault 仮想サーバーはシステム 2 でオンラインになります。

## VCS 環境にコンポーネントをインストールして設定する順序

VCS 環境にさまざまなコンポーネントをインストールして設定する順序は重要です。

### VCS 環境にコンポーネントをインストールして設定する方法

- 1 各クラスタノードで、Enterprise Vault サーバーコンポーネントとすべての必要な VCS コンポーネントをインストールします。

Enterprise Vault SMTP サービスを一般的なサービスとして含める場合は、Enterprise Vault サーバーコンポーネントと Enterprise Vault SMTP アーカイブ コンポーネントを各クラスタ ノードにインストールする必要があります。

- 2 Storage Foundation HA for Windows のインストールと設定を完了します。

インストール処理の一部として、Enterprise Vault Cluster Setup Wizard をインストールします。

- 3 ディスクグループとボリュームを設定します。
- 4 Enterprise Vault Cluster Setup Wizard を実行して、Enterprise Vault サービスグループを設定します。
- 5 クラスタのノードが正しくフェールオーバーすることをテストします。
- 6 Enterprise Vault 設定ウィザードを実行して、プライマリ Enterprise Vault クラスタノードを設定します。
- 7 必要に応じて、Enterprise Vault 開始ウィザードを実行して Enterprise Vault を設定します。
- 8 フェールオーバー Enterprise Vault クラスタノードを設定します。
- 9 クラスタのノードが引き続き正しくフェールオーバーすることをテストします。

# Storage Foundation HA for Windows のインストールと設定

この章では以下の項目について説明しています。

- [Enterprise Vault を使った Storage Foundation HA for Windows のインストールと設定](#)
- [Storage Foundation HA 環境でのディスクグループとボリュームの管理](#)

## Enterprise Vault を使った Storage Foundation HA for Windows のインストールと設定

注記されている場合を除き、このセクションで説明している手順の実行方法について詳しくは、Storage Foundation and High Availability Solutions の『Solutions ガイド』に記載されています。

**Enterprise Vault を使って Storage Foundation HA for Windows をインストールおよび設定する方法**

- 1 クラスタの一部となる各ノードに、SFW HA (Storage Foundation HA for Windows) 6.1 または 7.0 のすべての必須コンポーネントをインストールします。

このプロセスには、次のいくつかの段階があります。各ノードに対して、次の操作を行う必要があります。

- 製品のインストールの必要条件、ディスク領域の必要条件、SFW HA の必要条件をレビューします。
- ネットワークとストレージを設定します。

- SFW HA をインストールします。この処理の一部として、Enterprise Vault Cluster Setup Wizard をインストールするよう注意します。
- 2 VCS 設定ウィザードを実行して、クラスタを設定します。
  - 3 最初のノードからディスクグループとボリュームを設定します。Veritas Enterprise Administrator や同等の機能を持つディスク管理ソフトウェアを使用すると、この作業を行うことができます。  
共有ボリュームを作成して、次のデータを格納する必要があります。
    - インデックスサービスデータ
    - Enterprise Vault ストレージキュー
    - ショッピングサービスデータ
    - ボルトストアパーティション
    - PST 保存フォルダ
    - SMTP 保存フォルダ (Enterprise Vault SMTP アーカイブコンポーネントがインストールされている場合にのみ必要)
    - Enterprise Vault サーバーキャッシュ
    - Centera ステージング領域
    - レジストリレプリケーションデータ

パフォーマンス上の理由により、適切な場所に共有データを保存することを推奨します。一部のデータには個別のディスクが必要です。

詳しくは、<https://www.veritas.com/docs/100000918> で「Enterprise Vault Performance Guide」を参照してください。

p.256 の「[Storage Foundation HA 環境でのディスクグループとボリュームの管理](#)」を参照してください。
  - 4 Enterprise Vault サービスグループを設定するシステムにボリュームをマウントします。
  - 5 Enterprise Vault Cluster Setup Wizard を実行して、Enterprise Vault サービスグループを設定します。  
p.258 の「[Enterprise Vault の VCS サービスグループの設定について](#)」を参照してください。
  - 6 クラスタのノードが正しくフェールオーバーすることをテストします。
  - 7 クラスタのすべてのシステムに Enterprise Vault をインストールします。

- 8 Enterprise Vault 設定ウィザードを実行して、Enterprise Vault サービスとリソースを作成します。
- 9 クラスタ設定を確認し、フェールオーバー機能をテストします。

## Storage Foundation HA 環境でのディスクグループとボリュームの管理

このセクションでは、次の操作の実行方法について説明します。

- 動的ディスクグループのインポート
- 共有ボリュームのマウント
- ボリュームのマウント解除とディスクグループのデポート

SFW HA 環境を設定する場合は、次の点に注意する必要があります。

- Enterprise Vault サービスリソースグループを設定するシステムにボリュームをマウントする必要があります。
- ディスクグループを最初に作成すると、それを作成したノードにインポートされます。
- ディスクグループは 1 つのノードに 1 回のみインポートできます。
- 別のノードにディスクグループを移動するには、グループのボリュームのマウントを解除し、現在のノードからグループをデポートして、それを新しいノードにインポートし、ボリュームのマウントを解除します。

### 動的ディスクグループをインポートする方法

- 1 Veritas Enterprise Administrator を起動します。
- 2 ツリービューで動的ディスクグループのディスク名または動的ディスクグループ名を右クリックして、コンテキストメニューの[ダイナミックディスクグループのインポート]をクリックします。
- 3 画面に表示される指示に従います。

### ボリュームをマウントする方法

- 1 まだ動的ディスクグループをインポートしていない場合は、Veritas Enterprise Administrator を開いて、動的ディスクグループをインポートします。
- 2 ボリュームを右クリックして、[ファイルシステム]、[ドライブ名の英字とパスの変更]の順にクリックします。
- 3 [ドライブ文字およびパス]ダイアログボックスで、[追加]をクリックします。



- 4 ボリュームにドライブ文字を割り当てるか、フォルダとしてマウントするかによって、次のいずれかのオプションを選択します。

ドライブ文字を割り当てるには [ドライブ文字を割り当てる]をクリックし、必要な文字を選択します。

ボリュームをフォルダとしてマウントする方法 [空の NTFS フォルダにマウントする]をクリックし、[参照]をクリックして、共有ディスク上の空のフォルダを見つけます。

- 5 [OK]をクリックします。

#### ボリュームのマウントを解除し、動的ディスクグループをデポートする方法

- 1 Veritas Enterprise Administrator でボリュームを右クリックして、[ファイルシステム]、[ドライブ名の英字とパスの変更]の順にクリックします。
- 2 [ドライブ文字およびパス]ダイアログボックスで、[削除]をクリックします。
- 3 [OK]をクリックします。
- 4 ディスクを右クリックし、[ダイナミックグループのデポート]をクリックします。
- 5 [はい]をクリックして、ディスクグループをデポートすることを確定します。

# Enterprise Vault の VCS サービスグループの設定

この章では以下の項目について説明しています。

- Enterprise Vault の VCS サービスグループの設定について
- Enterprise Vault の VCS サービスグループを設定するための準備
- Enterprise Vault の VCS サービスグループの作成
- 既存の VCS サービスグループの修正
- VCS サービスグループの削除

## Enterprise Vault の VCS サービスグループの設定について

VCS では、サービスグループは仮想サーバーを表します。各サービスグループには一連のリソースが格納され、グループがクラスタ内の別のノードにフェールオーバーするときに、それらのリソースをオンラインまたはオフラインにすることができます。これらのリソースの組み合わせを調整して、完全な Enterprise Vault サーバーを作成できます。

次のリソースが含まれます。

- GenericService リソース
- IP アドレス
- コンピュータ名 (Lanman リソース)
- Microsoft Message Queue (MSMQ リソース)
- ディスクストレージ (MountV と DiskGroup リソース)
- NIC

クラスタで Enterprise Vault を設定する前に、Enterprise Vault サーバーを表すサービスグループを設定する必要があります。VCS では、Enterprise Vault クラスタ設定ウィザードを始めとする複数の方法でサービスグループを設定できます。Cluster Manager (Java コンソールまたは Web コンソール) あるいはコマンドラインも使えます。

Enterprise Vault のクラスタグループが Enterprise Vault に関連するリソースのみを含むようにすることを推奨します。

## Enterprise Vault の VCS サービスグループを設定するための準備

Enterprise Vault サービスグループを設定する前に、次の手順を実行します。

- DNS サーバーの設定を確認します。静的 DNS エントリで、仮想サーバー名 (Enterprise Vault サーバー名と同じになる) と仮想 IP アドレスがマップされていることを確認する必要があります。  
Enterprise Vault Cluster Setup Wizard では、複数の IP アドレスまたはコンピュータ名 (Lanman) リソースを含むサービスグループはサポートされないことに注意してください。
- クラスタ内のすべてのシステムで、Veritas Command Server サービスが実行されていることを確認します。
- Enterprise Vault Cluster Setup Wizard を実行するシステムで、High Availability Daemon (HAD) が実行されていることを確認します。
- クラスタ管理者権限を持っていることを確認します。ウィザードを実行するノードのローカル管理者でもある必要があります。
- 各ノードに Microsoft メッセージキュー (MSMQ) がローカルインストールされていることを確認します。
- 作成した共有ボリュームをマウントして、以下のデータを格納します。
  - インデックスサービスデータ
  - ショッピングサービスデータ
  - ボルトストアパーティション
  - PST 保存フォルダ
  - SMTP 保存フォルダ
  - Centera ステージング領域

クラスタ内の他のノードからボリュームをマウント解除します。

# Enterprise Vault の VCS サービスグループの作成

Storage Foundation HA for Windows のインストール処理の一部として、Enterprise Vault Cluster Setup Wizard のインストールが完了しています。このウィザードを使って、Enterprise Vault の VCS サービスグループを作成することができます。

## Enterprise Vault の VCS サービスグループを作成する方法

- 1 Enterprise Vault Cluster Setup Wizard を起動します。
- 2 [Welcome] ページの情報をレビューして、[次へ] をクリックし、[Wizard Options] ページを表示します。
- 3 [Create service group] をクリックし、[次へ] をクリックして、[Service Group Configuration] ページを表示します。
- 4 [Service Group Name] フィールドで、EVGRP1 などのグループの名前を入力します。
- 5 サービスグループを設定するシステムの [Systems in Priority Order] フィールドに移動します。  
  
[Systems in Priority Order] フィールドのシステムの優先度を変更する場合は、システムをクリックし、上矢印または下矢印ボタンをクリックします。
- 6 [次へ] をクリックして、設定の有効性を確認し、[Virtual Server Configuration] ページを表示します。
- 7 各フィールドで、次の手順を一覧表示された順序で実行します。
  - [Virtual Server Name] フィールドに、静的 DNS エントリの設定時に仮想 IP アドレスにマップしたサーバー名を入力します。
  - [Virtual IP address] フィールドに、仮想サーバーにマップしたアドレスを入力します。これは、現在のコンピュータと同じサブネットにあり、ネットワークで現在使われていないアドレスである必要があります。
  - 仮想 IP アドレスが属するサブネットのサブネットマスクを入力します。
  - クラスタのシステムごとに、パブリックネットワークアダプタ名を選択します。TCP/IP 対応のプライベートネットワークアダプタを含む、システム上のすべての TCP/IP 対応のアダプタがウィザードに一覧表示されます。プライベートネットワークに割り当てられているアダプタではなく、パブリックネットワークに割り当てるアダプタを選択してください。
  - [Advanced] をクリックして、Lanman リソースの詳細を指定します。仮想サーバーの組織単位の識別名を選択する必要があります。デフォルトでは、Lanman リソースは、デフォルトコンテナの [Computers] に仮想サーバーを追加します。

VCS Helper サービスのユーザーアカウントは、指定したコンテナに対して、コンピュータアカウントを作成し、更新するための適切な権限を持っている必要があります。

- 8 [Virtual Server Configuration] ページで、[次へ] をクリックし、[MSMQ and RegRep Directory Details] ページを表示します。

このページでは、仮想名を使ってアクセスできるように、MSMQ リソースを仮想化できます。このリソースにより、フェールオーバー後もキューの状態が維持されます。

- 9 各フィールドで次のように入力します。

- [MSMQ Directory] フィールドに、必要なディレクトリのパスを入力します。
- [Replication Directory] フィールドに、レジストリレプリケーションディレクトリのパスを入力します。レプリケーションデータには、レプリケートするレジストリキーの一覧が含まれます。

MSMQ とレプリケーションディレクトリは別々のボリューム上に設定することを推奨します。ボリュームは、共有ディスク上に設定した場合にのみ選択できます。

- 10 [次へ] をクリックして、[Storage Location Details] ページを表示します。

このページで、Enterprise Vault サービス用に設定するボリュームを選択できます。

ウィザードの前ページで、MSMQ とレジストリレプリケーションのストレージの場所を指定するときに選択したボリュームは選択できません。

- 11 [Available Volumes] フィールドで、サービスを設定した各ボリュームを選択してから、右矢印ボタンをクリックして、[Selected Volumes] フィールドに移動します。次の項目を設定したボリュームを選択する必要があります。

- インデックスサービスデータ
- ショッピングサービスデータ
- ボルトストアパーティション
- PST 保存フォルダ
- SMTP 保存フォルダ
- Centera ステージング領域

- 12 [次へ] をクリックして、[Service Group Summary] ページを表示します。

- 13 設定をレビューします。何らかの理由で属性名を修正する場合は、次の手順を一覧表示された順序で実行します。

- リソースをクリックし、修正する属性をクリックします。
- 表の行の最後にある [Edit] アイコンをクリックします。
- [Edit Attribute] ダイアログボックスに、属性値を入力します。

- [OK]をクリックします。
- リソースと属性ごとに手順を繰り返します。

**14** [次へ]をクリックして、[Completion]ページを表示します。

**15** [Bring the service group online]をクリックし、[完了]をクリックします。

サービスグループの追加が完了したら、ノード間のフェールオーバーが正常に行われることを確認してください。

# 既存の VCS サービスグループの修正

表 34-1 に、サービスグループで修正できるアイテムを一覧表示します。

**表 34-1**                      修正可能なサービスグループのアイテム

項目	メモ
システム一覧	クラスタのノードを追加、削除できます。ノードを削除する場合、そのノードがアクティブでないことを確認します。
ボリューム	ボリュームを追加、削除できます。Enterprise Vault サービスが設定されているボリュームを削除すると、サービスの高可用性が失われ、監視されなくなります。
仮想 IP	サービスグループがオフラインの場合に、仮想 IP アドレスを変更できます。仮想サーバー名は変更できません。この名前は、サービスグループの作成時に修正します。

Enterprise Vault Cluster Setup Wizard、Cluster Manager (Java コンソールと Web コンソール)、コマンドラインなどの複数の方法で Enterprise Vault サービスグループを修正できます。次の手順では、Enterprise Vault Cluster Setup Wizard を使ってサービスグループを修正する方法について説明します。

続行する前に、次の点に注意してください。

- サービスグループがオンラインであるノードからウィザードを実行する必要があります。ウィザードを使って、設定にリソースを追加または削除できます。
- リソースの属性を変更するには、サービスグループを部分的にオフラインにする必要があります。ただし、サービスグループの MountV と VMDg リソースは、ウィザードを実行するノードでオンラインにし、他のすべてのノードでオフラインにする必要があります。作成したすべてのボリュームをマウントし、ストレージサービスデータ (ボルトストア)、レジストリレプリケーション情報、ショッピングサービスデータ、SMTP 保存フォルダ、インデックスデータ、MSMQ データを格納します。
- システム一覧またはボリュームを修正する場合は、サービスグループをオンラインにする必要があります。

- 運用中の Enterprise Vault サーバーが含まれる既存の VCS サービスグループは修正しないでください。

#### 既存の VCS サービスグループを修正する方法

- 1 Enterprise Vault Cluster Setup Wizard を起動します。
- 2 [Welcome] ページの情報をレビューして、[次へ] をクリックし、[Wizard Options] ページを表示します。
- 3 [Modify service group] をクリックし、[次へ] をクリックします。
- 4 指示に従って、サービスグループを修正します。

オンラインサービスグループにシステムを追加すると、ローカル属性を持つすべてのリソースがしばらくの間 UNKNOWN の状態になることがあります。グループに新しいノードを追加したら、このノードで Enterprise Vault 設定ウィザードを実行し、Enterprise Vault サービスを設定します。

## VCS サービスグループの削除

以下の手順に従って、Enterprise Vault Cluster Setup Wizard を使ってサービスグループを削除します。

#### VCS サービスグループを削除する方法

- 1 Enterprise Vault Cluster Setup Wizard を起動します。
- 2 [Welcome] ページの情報をレビューして、[次へ] をクリックし、[Wizard Options] ページを表示します。
- 3 [Delete service group] をクリックし、[次へ] をクリックします。
- 4 [Service Group Summary] ページで [次へ] をクリックします。
- 5 ウィザードで、サービスグループの削除を確認するメッセージが表示されたら、[Yes] をクリックします。
- 6 [完了] をクリックします。

# Enterprise Vault 設定ウィザードの実行

この章では以下の項目について説明しています。

- [Enterprise Vault 設定ウィザードの実行の準備](#)
- [アクティブ/パッシブ VCS 構成での Enterprise Vault の設定](#)
- [VCS N+1 構成での Enterprise Vault の設定について](#)

## Enterprise Vault 設定ウィザードの実行の準備

Enterprise Vault 設定ウィザードには、VCS クラスタで Enterprise Vault を設定するためのオプションがあります。

Enterprise Vault 設定ウィザードを実行する前に、次のことを確認します。

- クラスタ内の最初のノードに Enterprise Vault サービスグループが存在し、オンラインである。  
p.258 の「[Enterprise Vault の VCS サービスグループの設定について](#)」を参照してください。
- SFW HA 6.1 または 7.0 がインストールされている

## アクティブ/パッシブ VCS 構成での Enterprise Vault の設定

このセクションでは、Enterprise Vault の初回インストールでのクラスタサポートの設定方法と、既存の標準 Enterprise Vault インストール済み環境をクラスタ環境にアップグレードする方法について説明します。



## Enterprise Vault の初回インストールでの VCS クラスタサポートの追加

クラスタの各ノードで Enterprise Vault 設定ウィザードを実行する必要があります。最初のノードでは、[クラスタをサポートする Enterprise Vault サーバーを新規作成]オプションにチェックマークを付けます。各追加ノードでは、[既存のクラスタ化されたサーバーのフェールオーバーノードとしてこのノードを追加]オプションにチェックマークを付けます。

Enterprise Vault SMTP サービスを一般的なサービスリソースとして追加する場合は、Enterprise Vault SMTP アーカイブコンポーネントを Enterprise Vault サーバーとともにクラスタのすべてのノードにインストールする必要があります。

### クラスタをサポートする Enterprise Vault サーバーを新規作成する方法

- 1 Enterprise Vault 設定ウィザードを開始します。
- 2 [クラスタをサポートする Enterprise Vault サーバーを新規作成]にチェックマークを付け、[次へ]をクリックします。
- 3 画面に表示される指示に従います。  
ウィザードの実行中には、次の点に注意してください。
  - コンピュータの DNS エイリアスの入力を求められたら、仮想サーバー名を指す非修飾 DNS エイリアスを入力します。
  - インデックスサービスとショッピングサービスのストレージの場所をレビューするように求められたら、その指示に従ってレビューしてください。
  - ウィザードでデータの場所を選択するよう求めるメッセージが表示されたら、クラスタの共有ドライブ上にあるサーバーのキャッシュの場所を指定します。
- 4 [完了]ページで、[すべてのリソースをオンラインにする]のチェックマークがはずれているのを確認し、[完了]をクリックします。
- 5 以下のステップに従って、パスをクラスタ内の共有ドライブにあるインデックスメタデータフォルダに設定します。インデックスメタデータフォルダは、Enterprise Vault によりインデックス設定データとレポートデータが格納されるフォルダです。
  - Cluster Manager コンソールを使って Enterprise Vault のディレクトリサービスと管理サービスをオンラインにします。
  - Enterprise Vault 管理コンソールの左ペインで、[Enterprise Vaultサーバー]、[EVServer.domain.local]、[サービス]の順に参照します。
  - 右ペインで[Enterprise Vault Indexing Service]を右クリックし、[プロパティ]をクリックします。
  - [サービスのプロパティ]ダイアログボックスの[全般]タブで、[インデックスメタデータの場所]のパスを、クラスタ内の共有ドライブのパス(v:\¥indexmetadata など)に設定します。
  - [OK]をクリックして変更内容を保存します。

- Cluster Manager コンソールを使って、Enterprise Vault インデックスサービスをオンラインにします。
- 6 最初のノードでサーバーを設定したら、フェールオーバーノードとして設定する各追加ノードからウィザードを実行します。

Enterprise Vault プログラムフォルダのパスは、クラスタ内のすべてのノードで同じである必要があります。たとえば、C:\Program Files (x86)\Enterprise Vault となります。ノードによってパスが異なると、フェールオーバー時に問題が発生する可能性があります。

#### 既存のクラスタサーバーにフェールオーバーノードを追加する方法

- 1 Enterprise Vault サービスグループがクラスタ内の別のノードでオンラインであることを確認します。設定するノードでサービスグループをオンラインにしないでください。設定するノードは、そのリソース用の利用可能なフェールオーバーノードである必要があります。
- 2 Enterprise Vault SMTP サービスを一般的なサービスリソースとしてサービスグループに加える場合は、必ず Enterprise Vault SMTP アーカイブコンポーネントを Enterprise Vault サーバーとともにフェールオーバーノードにインストールします。
- 3 Enterprise Vault 設定ウィザードを開始します。
- 4 [既存のクラスタ化されたサーバーのフェールオーバーノードとしてこのノードを追加]をクリックし、[次へ]をクリックします。
- 5 画面に表示される指示に従います。  
ノードを追加するサービスグループの名前を入力するように求められたら、最初のノードとして選択したサービスグループの名前を選択します。
- 6 概略ページで、情報をレビューし、[次へ]をクリックします。  
新しいノードに Enterprise Vault サービスグループが作成されることが通知されます。
- 7 [完了]ページで、[完了]をクリックしてウィザードを終了します。
- 8 フェールオーバーノードでリソースをオンラインにできることを確認します。これを確認するには、Cluster Explorer で、コンテキストメニューの[切換え]をクリックします。

#### 監視データベースの設定のトラブルシューティング

Enterprise Vault 設定ウィザードの実行中に、Enterprise Vault 監視データベースの設定が失敗したことを示すエラーが表示された場合は、設定ウィザードを完了し、監視設定ユーティリティを実行して、監視データベースと監視エージェントを手動で設定します。

実行方法については、次の Enterprise Vault サポート Web サイトから Veritas テクニカルノートを参照してください。

<https://www.veritas.com/docs/100018087>

このテクニカルノートでは、監視エージェントに関する問題のトラブルシューティング方法についても説明しています。

## 既存の Enterprise Vault インストール済み環境の VCS クラスタへのアップグレード

クラスタ化されていない単独のサーバーに Enterprise Vault をインストール済みの場合、この環境をフェールオーバークラスタに変換できます。クラスタに変換するには、既存の Enterprise Vault インストール済み環境が次の条件を満たす必要があります。

- Enterprise Vault はクラスタの一部としてではなく、非クラスタ構成で構成しておく必要があります。
- Enterprise Vault サーバーは、標準的なアドレスレコードではなく、DNS エイリアスを使って構成する必要があります。
- Enterprise Vault サーバーではインデックスサービス、ショッピングサービス、タスク制御サービス、ストレージサービスがすべて有効になっている必要があります。
- Enterprise Vault SMTP アーカイブが必要な場合は、Enterprise Vault SMTP アーカイブコンポーネントもサービスグループのすべてのノードにインストールする必要があります。
- 計画しているクラスタ内のサーバーには、Compliance Accelerator も Discovery Accelerator もインストールしないでください。これらの製品はクラスタ内ではサポートされません。ただし、クラスタ化されていない Compliance Accelerator または Discovery Accelerator はクラスタ化された Enterprise Vault 仮想サーバーを参照できます。

### 既存の Enterprise Vault インストール済み環境を VCS クラスタにアップグレードする方法

- 1 設定内容が Enterprise Vault サービスグループの必要条件を満たすことを確認します。  

p.259 の「[Enterprise Vault の VCS サービスグループを設定するための準備](#)」を参照してください。
- 2 Enterprise Vault Cluster Setup Wizard を実行して、Enterprise Vault サービスグループを作成し、構成するサーバーをそのグループに追加します。
- 3 次のすべてが高可用性共有ストレージデバイス上にあることを確認します。
  - インデックスサービスデータ
  - ショッピングサービスデータ
  - ボルトストアパーティション
  - PST 保存フォルダ

- SMTP 保存フォルダ
- Centera ステージング領域

高可用性共有ストレージデバイス上にない場合は、Enterprise Vault ディレクトリデータベースの場所を修正し、関連付けされたデータを新しい場所に移動します。

p.268 の「高可用性の場所への Enterprise Vault データの移動」を参照してください。

- 4 Enterprise Vault クラスタ変換ウィザードを起動します。
- 5 概要情報を読み、[次へ]をクリックします。
- 6 次のページが表示されたら、[すべての場所が高可用性の共有ストレージである]を選択して、[次へ]をクリックします。
- 7 Enterprise Vault MSMQ キュー内にあるメッセージが検出されたら、クラスタ化された MSMQ キューにそのメッセージを移行せずに変換を続行するかどうかを選択します。  
  
キューが消去されるまで待つから、クラスタ変換ウィザードを再実行します。キュー内に残ったメッセージは、新しいクラスタでは無視されます。キューの消去処理時間を短縮するには、タスク制御サービスを停止し、ファイルシステムアーカイブでアーカイブが実行されていないことを確認します。
- 8 各 Enterprise Vault サービスのクラスタリソースを作成するサービスグループを選択するように求められたら、前に作成したグループを選択します。
- 9 [次へ]をクリックしてクラスタリソースを作成してから、ウィザードで実行された処理の一覧をレビューします。
- 10 [完了]をクリックしてウィザードを終了します。
- 11 MMC (Microsoft Management Console) の DNS スナップインを使って、コンピュータ名エイリアスを、ローカル名ではなく仮想サーバー名を指すように変更します。
- 12 Veritas Cluster Manager を使って、クラスタのリソースをオンラインにします。

## 高可用性の場所への Enterprise Vault データの移動

高可用性の場所にデータを移動する手順の概略は、次のとおりです。

- インデックスサービス、ショッピングサービス、ストレージサービス、タスク制御サービスを停止します。
- Enterprise Vault ディレクトリデータベースとデータファイルのバックアップコピーを作成します。
- Enterprise Vault ディレクトリに対して、Vault 管理コンソールを使うか SQL クエリーを実行して、以下に説明するようにデータを移動します。

IndexRootPathEntry  
[IndexRootPath]

- この場所の内容を高可用性の場所に移動します。
- 新しい場所を指すように、SQL を使ってデータベースを更新します。

現在の場所を表示する SQL は、次のとおりです。

```
SELECT *
FROM IndexRootPathEntry
WHERE (IndexRootPathEntryId = '<ID FROM
LOG FILE>')
```

場所を更新する SQL は、次のとおりです。

```
UPDATE IndexRootPathEntry
SET IndexRootPath = '<THE NEW LOCATION>'
WHERE (IndexRootPathEntryId = '<ID FROM
LOG FILE>')
```

PartitionEntry [AccountName]

- プールエントリの認可ファイル (.pea) を高可用性の場所に移動します。
- Vault 管理コンソールを使って Centera パーティションのプロパティを表示し、[接続] タブの [プールエントリの認可ファイルの場所] フィールドを、新しい場所を指すように編集します。

PartitionEntry  
[PartitionRootPath]

- この場所の内容を高可用性の場所に移動します。
- 新しい場所を指すように、SQL を使ってデータベースを更新します。

現在の場所を表示する SQL は、次のとおりです。

```
SELECT *
FROM PartitionEntry
WHERE (PartitionEntryId = '<ID FROM LOG
FILE>')
```

場所を更新する SQL は、次のとおりです。

```
UPDATE PartitionEntry
SET PartitionRootPath = '<THE NEW
LOCATION>'
WHERE (PartitionEntryId = '<ID FROM LOG
FILE>')
```

PartitionEntryが場所  
[SecondaryLocation]

- セカンダリストレージファイルを高可用性の場所に移動します。
- 新しい場所を指すように、SQL を使ってデータベースを更新します。

現在の場所を表示する SQL は、次のとおりです。

```
SELECT *
FROM PartitionEntry
INNER JOIN Locations ON
PartitionEntry.SecondaryLocation =
Locations.LocationIdentity
WHERE (PartitionEntry.PartitionEntryId =
'<ID FROM LOG FILE>')
```

場所を更新する SQL は、次のとおりです。

```
UPDATE Locations
SET Location = '<NEW LOCATION>'
WHERE LocationIdentity =
(SELECT SecondaryLocation FROM PartitionEntry
WHERE PartitionEntryId = '<ID FROM LOG
FILE>')
```

PartitionEntry  
[StagingRootPath]

- この場所の内容を高可用性の場所に移動します。
- 新しい場所を指すように、SQL を使ってデータベースを更新します。

現在の場所を表示する SQL は、次のとおりです。

```
SELECT *
FROM PartitionEntry
WHERE (PartitionEntryId = '<ID FROM LOG
FILE>')
```

場所を更新する SQL は、次のとおりです。

```
UPDATE PartitionEntry
SET StagingRootPath = '<THE NEW LOCATION>'
WHERE (PartitionEntryId = '<ID FROM LOG
FILE>')
```

PSTMigratorTask  
[MigrationDirectory]

- 1 この場所の内容を高可用性の場所に移動します。
- 2 Vault 管理コンソールを使って、PST 移行タスクのプロパティを表示し、一時ファイルのフォルダを更新します。

- |  |   |
|--|---|
| ShoppingServiceEntry<br>[ShoppingRootPath] | <ul style="list-style-type: none"> <li>■ この場所の内容を高可用性の場所に移動します。</li> <li>■ Vault 管理コンソールを使って、ショッピングサービスの場所を新しい高可用性の場所に編集します。</li> </ul>                             |
| SiteEntry<br>[PSTHoldingDirectory]         | <ul style="list-style-type: none"> <li>■ この場所の内容を高可用性の場所に移動します。</li> <li>■ Vault 管理コンソールを使って、サイトのプロパティを表示し、PST 保存フォルダのプロパティを、新しい場所を指すように更新します。</li> </ul>           |
| SmtpArchivingTask<br>[HoldingFolder]       | <ul style="list-style-type: none"> <li>■ この場所の内容を高可用性の場所に移動します。</li> <li>■ Vault 管理コンソールを使って、SMTP アーカイブタスクのプロパティを表示し、SMTP 保存フォルダのプロパティを新しい場所を指すように更新します。</li> </ul> |

## 既存のクラスタ化された Enterprise Vault サーバーへの SMTP アーカイブの追加

Enterprise Vault SMTP アーカイブ機能を既存の Enterprise Vault クラスタに追加することがあります。

既存のクラスタ Enterprise Vault サーバーに SMTP アーカイブを追加するには

- 1 Enterprise Vault クラスタのすべてのノードに Enterprise Vault サーバーと SMTP アーカイブコンポーネントをインストールします。
- 2 クラスタ化された Enterprise Vault サーバーで新しい SMTP アーカイブタスクを作成します。Enterprise Vault は SMTP アーカイブタスクを作成する前に、アーカイブノードとその他のノードでの Enterprise Vault SMTP サービスの存在を検出し、SMTP サービスを一般的なサービスリソースとして設定します。
- 3 Enterprise Vault は一部のクラスタノードで SMTP アーカイブコンポーネントを検出しない場合、影響を受けるノードの一覧と、SMTP アーカイブコンポーネントをインストールするための警告を表示します。SMTP アーカイブタスクの作成を続行し、リストされたノードに SMTP アーカイブコンポーネントを後でインストールすることができます。クラスタのすべてのノードにコンポーネントをインストールしないと、Enterprise Vault はコンポーネントがインストールされていないノードにフェールオーバーできません。

## VCS N+1 構成での Enterprise Vault の設定について

アクティブ/パッシブクラスタの設定の安価な代替策として、VCS N+1 構成で Enterprise Vault を設定できます。そのため、クラスタには任意の数の Enterprise Vault サーバーと、単一のスペアノードが含まれます。

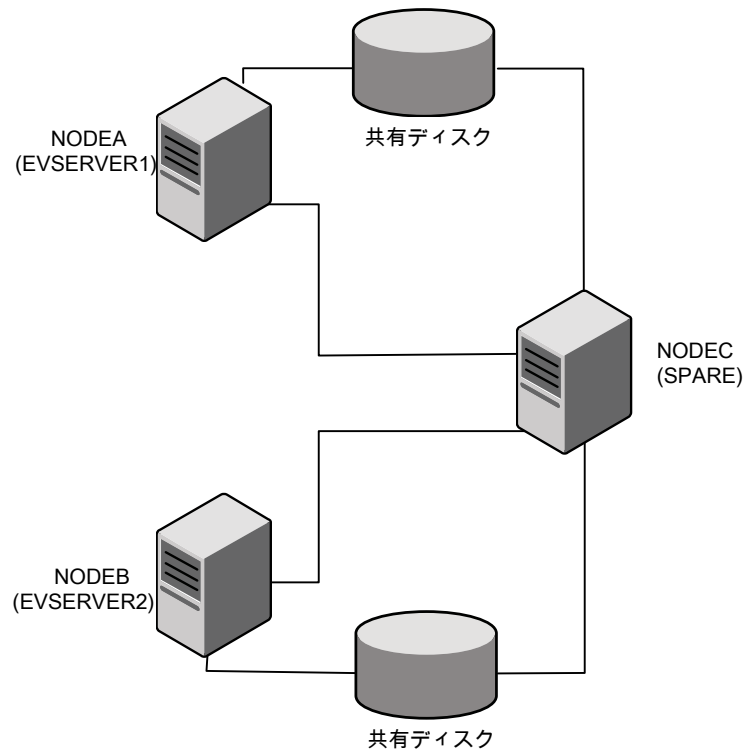
N+1 構成には 2 つの基本的な種類があります。たとえば、2 台の Enterprise Vault サーバーが含まれるクラスタでは、次の構成の種類を選択できます。

- クラスタ化された Enterprise Vault サーバーが 2 つのノードで実行され、共有スペアノードが存在します。
- 2 台の Enterprise Vault サーバーが、クラスタ内の 3 つのノードのいずれかで実行するように構成されます。

## VCS N+1 クラスタ内での 2 つの Enterprise Vault サーバーノードと 1 つのスペアノードの設定

図 35-1 に、Enterprise Vault サーバーが実行されている 2 つのノードと、スペアノードが存在する構成を示します。利用可能なノードの数に応じて、クラスタには多くの Enterprise Vault サーバーが含まれる可能性があることに注意してください。

図 35-1 2 つの Enterprise Vault サーバーノードと 1 つのスペアノードを含む 3 ノードの VCS クラスタ





EVSERVER1 のサービスグループが NODEA と NODEC で実行され、EVSERVER2 のサービスグループが NODEB と NODEC で実行されるように構成します。EVSERVER1 と EVSERVER2 はサービスグループの仮想コンピュータ名です。

### VCS N+1 クラスタ内で 2 つの Enterprise Vault サーバーノードと 1 つのスペアノードを設定する方法

- 1 Enterprise Vault サービスグループを設定するシステムにボリュームをマウントします。  
  
p.256 の「[Storage Foundation HA 環境でのディスクグループとボリュームの管理](#)」を参照してください。
- 2 NODEA または NODEC のいずれかで、Enterprise Vault Cluster Setup Wizard を実行し、これらの 2 つのノードに対して EVSERVER1 というサービスグループを作成します。
- 3 NODEB または NODEC のいずれかで、Enterprise Vault Cluster Setup Wizard を実行し、これらの 2 つのノードに対して EVSERVER2 というサービスグループを作成します。
- 4 初めて Enterprise Vault をインストールするか、既存のインストールをアップグレードするかに応じて、NODEA と NODEB で次の処理を行います。

#### ノード 新規インストール

#### アップグレードインストール

NODEA	Enterprise Vault 設定ウィザードを実行します。新しい Enterprise Vault サーバーを EVSERVER1 のクラスタグループに設定する場合に選択します。	クラスタ変換ウィザードを実行します。EVSERVER1 サービスグループにサービスリソースを作成する場合に選択します。
NODEB	Enterprise Vault 設定ウィザードを実行します。新しい Enterprise Vault サーバーを EVSERVER2 のクラスタグループに設定する場合に選択します。	クラスタ変換ウィザードを実行します。EVSERVER2 サービスグループにサービスリソースを作成する場合に選択します。

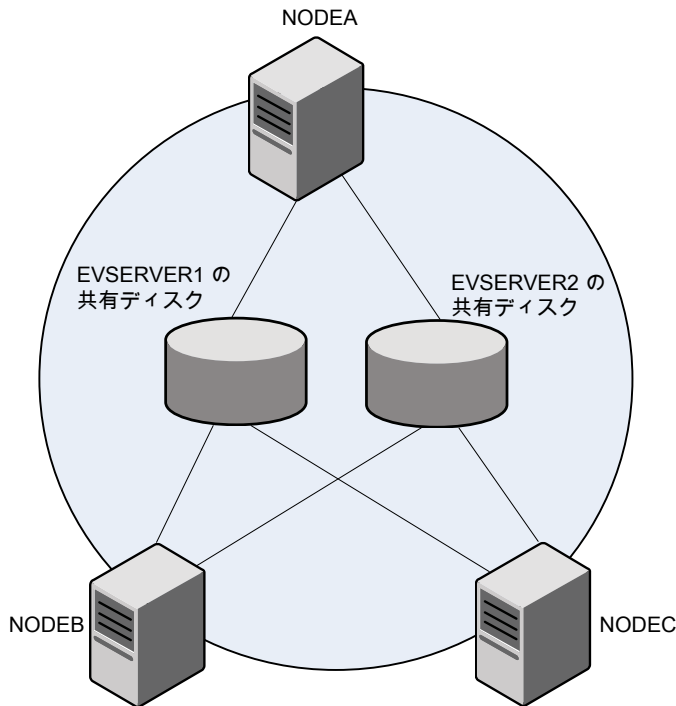
- 5 NODEC で Enterprise Vault 設定ウィザードを実行して、既存のクラスタサーバーのフェールオーバーノードとしてこのノードを追加するように選択します。いずれかのサービスグループを選択します。

NODEA と NODEB でサービスグループをオンラインにすると、Cluster Explorer で GenericService リソースに問題があると誤って表示されることがあります (左側のペインのアイコンに疑問符が付けられます)。これは、VCS によって、各リソースが 2 つのノードで同時にオンラインになっていると見なされるためです。この状況は無視してもかまいません。

## VCS クラスターの 3 つのノードのいずれかで実行するように 2 台の Enterprise Vault サーバーを構成する

図 35-2 に、VCS クラスターの 3 つのノードのいずれかで実行するように 2 台の Enterprise Vault サーバーを構成する方法を図で示します。この設定は、NODEB が失敗した場合に NODEC にサーバーを移動するという利点があります。NODEB をオンラインに戻して EVSERVER1 と EVSERVER2 のフェールオーバーサーバーとして機能するようにできます。

図 35-2 2 台の Enterprise Vault サーバーを備えた 3 つのノードの VCS クラスタ



## VCS クラスタの 3 つのノードのいずれかで実行するように 2 台の Enterprise Vault サーバーを構成する方法

- 1 Enterprise Vault サービスグループを設定するシステムにボリュームをマウントします。  
  
p.256 の「[Storage Foundation HA 環境でのディスクグループとボリュームの管理](#)」を参照してください。
- 2 [Enterprise Vault クラスタセットアップ]ウィザードで NODEA、NODEB、NODEC のノードを含む EVSERVER1 のサービスグループを作成します。
- 3 [Enterprise Vault クラスタセットアップ]ウィザードで NODEA、NODEB、NODEC のノードを含む EVSERVER2 のサービスグループを作成します。
- 4 初めて Enterprise Vault をインストールするか、既存のインストールをアップグレードするかに応じて、NODEA と NODEB で次の処理を行います。

### ノード 新規インストール

### アップグレードインストール

NODEA	Enterprise Vault 設定ウィザードを実行します。新しい Enterprise Vault サーバーを EVSERVER1 のクラスタグループに設定する場合に選択します。	クラスタ変換ウィザードを実行します。EVSERVER1 サービスグループにサービスリソースを作成する場合に選択します。
NODEB	Enterprise Vault 設定ウィザードを実行します。新しい Enterprise Vault サーバーを EVSERVER2 のクラスタグループに設定する場合に選択します。	クラスタ変換ウィザードを実行します。EVSERVER2 サービスグループにサービスリソースを作成する場合に選択します。

- 5 NODEC で Enterprise Vault 設定ウィザードを実行して、既存のクラスタサーバーのフェールオーバーノードとしてこのノードを追加するように選択します。いずれかのサービスグループを選択します。

このオプションとオプション 1 の設定の相違点は、サービスグループを作成するときにノードのサブセットではなくすべてのノードを選択する必要があることのみです。

システムに複数のスペアサーバー (N+2、N+3、N+4 など) が必要な場合は似たような方法を実行できます。その都度、各 Enterprise Vault サーバーにノードを設定してスペアノードをフェールオーバーノードとして追加する必要があります。

## VCS クラスタ内の同じノードでの 2 台の Enterprise Vault サーバーの無効化

アクティブ/アクティブクラスタ構成内の同じノード上で複数の Enterprise Vault サービスグループを実行することはできません。N+x 構成でクラスタを設定する場合、すべてのノードに Limit 属性と Prerequisites 属性を設定することでこの問題を回避できます。

これらの手順について詳しくは『Cluster Server Administrator's Guide』を参照してください。

### VCS クラスタ内の同じノードで 2 台の Enterprise Vault サーバーを無効化する方法

- 1 Veritas Cluster Manager を使って、クラスタにログオンします。
- 2 Cluster Monitor パネルの任意の場所をクリックして、Cluster Explorer を開きます。
- 3 クラスタの各ノードで、次の手順を一覧表示された順序で実行します。
  - 左側の設定ツリーで、属性を編集するノードをクリックします。
  - [表示]パネルで、[プロパティ]タブをクリックします。
  - [すべての属性を表示]をクリックして、属性ビューダイアログボックスを開きます。
  - Limit 属性を検索します。
  - 行の右側にある[編集]アイコンをクリックします。
  - [属性の編集]ダイアログボックスで、EnterpriseVault というキーを追加して、値に 1 を指定します。
  - [OK]をクリックしてダイアログボックスを閉じ、属性ビューダイアログボックスに戻ります。
  - 各 Enterprise Vault サービスグループの Prerequisites 属性について、手順を繰り返します。

値が 1 に指定された EnterpriseVault というキーが Limit 属性と Prerequisites 属性の両方に存在する場合は、2 台の Enterprise Vault サーバーを同じノードで実行できません。

# Enterprise Vault での SFW HA-VVR のディザスタリカバリソリューションの実装

この章では以下の項目について説明しています。

- Enterprise Vault を使った SFW HA-VVR のインストールと設定について
- SFW HA-VVR のインストールと設定の手順の概要
- プライマリサイトの VCS クラスタの設定
- セカンダリサイトの VCS クラスタの設定
- レプリケートするための VVR コンポーネントの追加
- 広域リカバリのために GCO コンポーネントを追加する

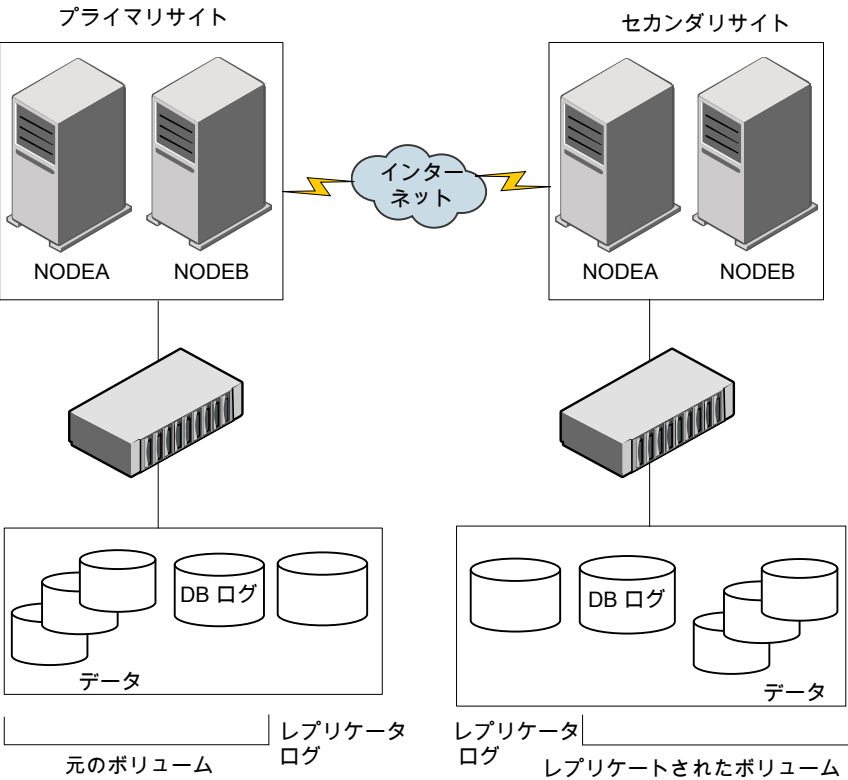
## Enterprise Vault を使った SFW HA-VVR のインストールと設定について

Enterprise Vault を使った SFW HA-VVR のインストールと設定の手順は、Storage Foundation and High Availability Solutions の『Solutions ガイド』に記載されている手順とほぼ同様です。

このシナリオでは、プライマリサイトに送信元ホストが存在し、セカンダリホストに送信先ホストが存在します。アプリケーションデータはプライマリサイトに格納され、Veritas Volume Replicator (VVR) を使ってセカンダリサイトにレプリケートされます。通常の操作では、プライマリサイトがデータとサービスを提供します。プライマリサイトで災害が発生してデータが破損した場合は、データにアクセスできるように、セカンダリホストがプライマリホストの役割を引き継ぎます。アプリケーションはセカンダリホストで再起動できます。

図 36-1 に、SFW HA-VVR の設定を示します。

図 36-1 SFW HA-VVR の設定



この例では、アプリケーションのサイトごとに 1 つのディスクグループがあります。各サイトに VVR レプリケーターログが必要であることに注意してください。ディスクグループが複数ある場合は、それぞれに追加のレプリケーターログが必要です。

## SFW HA-VVR のインストールと設定の手順の概要

表 36-1 に、SFW HA-VVR のインストールと設定に必要な作業を示します。

表 36-1 SFW HA-VVR のインストールと設定

手順	作業	詳細の参照先セクション
手順 1	プライマリサイトの VCS クラスタを設定します。	p.279 の「 <a href="#">プライマリサイトの VCS クラスタの設定</a> 」を参照してください。

手順	作業	詳細の参照先セクション
手順 2	セカンダリサイトの VCS クラスタを設定します。	p.280 の「セカンダリサイトの VCS クラスタの設定」を参照してください。
手順 3	レプリケーション用の VVR コンポーネントを追加します。	p.280 の「レプリケートするための VVR コンポーネントの追加」を参照してください。
手順 4	広範囲のリカバリ用にグローバルクラスタオプション (GCO) コンポーネントを追加します。	p.281 の「広域リカバリのために GCO コンポーネントを追加する」を参照してください。

## プライマリサイトの VCS クラスタの設定

プライマリサイトのクラスタを設定するには、次の手順を完了します。注記されている場合を除き、これらの手順の実行方法について詳しくは、**Storage Foundation and High Availability Solutions** の『**Solutions ガイド**』を参照してください。

### プライマリサイトの VCS クラスタを設定する方法

- 1 プライマリサイトのクラスタの一部となる各ノードに、**SFW HA 6.1** または **7.0** をインストールします。  
このプロセスには、次のいくつかの段階があります。
  - 製品のインストールの必要条件、ディスク領域の必要条件、**SFW HA** の必要条件をレビューします。
  - **Windows** をインストールし、ネットワークオプションを設定します。
  - プライマリサイトに **SFW HA** をインストールします。インストール中に **VVR** と **GCO** オプションを選択します。
  - **VVR Security Service** 設定ウィザードを使って、**Veritas Volume Replicator Security Service (VxSAS)** を設定します。
- 2 **VCS** 設定ウィザードを実行して、クラスタを設定します。
- 3 **Enterprise Vault** をインストールします。
- 4 ディスクグループとボリュームを設定します。共有ボリュームを作成して、次のデータを格納する必要があります。
  - インデックスサービスデータ
  - ショッピングサービスデータ
  - ボルトストアパーティション
  - PST 保存フォルダ
  - SMTP 保存フォルダ

■ Centera ステージング領域

また、MSMQとレジストリレプリケーションデータを格納する個別のボリュームも作成することを推奨します。

- 5 プライマリサイトで VCS サービスグループを設定します。

p.258 の「[Enterprise Vault の VCS サービスグループの設定について](#)」を参照してください。

- 6 クラスタ設定を確認し、フェールオーバー機能をテストします。

## セカンダリサイトの VCS クラスタの設定

セカンダリサイトのクラスタの設定手順は、プライマリサイトの設定手順に似ています。注記されている場合を除き、これらの手順の実行方法について詳しくは、**Storage Foundation and High Availability Solutions** の『**Solutions ガイド**』を参照してください。

### セカンダリサイトの VCS クラスタを設定する方法

- 1 セカンダリサイトの並列環境を作成します。
- 2 VCS 設定ウィザードを実行して、クラスタを設定します。
- 3 Enterprise Vault をインストールします。
- 4 セカンダリサイトのディスクグループとボリュームを設定します。

セカンダリサイトのディスクグループとボリュームの設定は、プライマリサイトと同じである必要があります。ディスク、ディスクグループ、ボリュームは、同じサイズ、同じ名前、同じ種類である必要があります。

- 5 セカンダリサイトの VCS サービスグループを設定します。プライマリサイトで指定したのと同じサービスグループ名を指定するように注意します。
- 6 クラスタ設定を確認し、フェールオーバー機能をテストします。

## レプリケートするための VVR コンポーネントの追加

このセクションでは、VVR コンポーネントのレプリケートの設定について説明します。これらの手順の実行方法について詳しくは、**Storage Foundation and High Availability Solutions** の『**Solutions ガイド**』を参照してください。



レプリケートするために VVR コンポーネントを追加するには

- 1 各サイトでレプリケータログボリュームを作成する
- 2 プライマリサイトとセカンダリサイトのホストで VVR の RDS (replicated data set) を設定する [Setup Replicated Data Set] ウィザードで、両方のサイトにレプリケートする RDS を設定できます。
- 3 VVR RVG サービスグループを作成する  
アプリケーションサービスグループが存在するシステムで [Volume Replicator Agent Configuration] ウィザードを実行する必要があります。

## 広域リカバリのために GCO コンポーネントを追加する

広域ディザスタリカバリのためにグローバルクラスタ化を管理するにはグローバルクラスタオプション (GCO) コンポーネントが必要です。以下の手順の実行方法について詳しくは、Storage Foundation and High Availability Solutions の『Solutions ガイド』を参照してください。

広域リカバリのために GCO コンポーネントを追加するには

- 1 環境がグローバルクラスタ操作の必要条件を満たしていることを確認する
- 2 リモートクラスタを追加してクラスタをリンクする
- 3 ローカルサービスグループをグローバルグループに変換する
- 4 追加のグローバルクラスタ管理タスクを実行する

# VCS によるクラスタ化のトラブルシューティング

この章では以下の項目について説明しています。

- [VCS ログ記録](#)
- [Enterprise Vault Cluster Setup Wizard のエラーメッセージ](#)
- [Enterprise Vault 仮想サーバーのクラスタ化されたメッセージキューの表示](#)

## VCS ログ記録

VCS はエンジンログとエージェントログという 2 つのエラーメッセージログを生成します。ログファイルの名前には文字が追加されます。A は最初のログファイル、B は 2 番目、C は 3 番目のようになります (例: agent\_A.txt)。

エージェントログは %VCS\_HOME%\log 内にあります (通常は c:\Program Files\Veritas\cluster server\log)。エージェントログメッセージの形式は、次のとおりです。

**Timestamp Mnemonic Severity Message\_ID Message\_Text**

それぞれの内容は次のとおりです。

<b>Timestamp</b>	メッセージがログに記録された日時を示します。
<b>Mnemonic</b>	製品を識別します (VCS など)。
<b>Severity</b>	エラーの重要度を示します (CRITICAL、ERROR、WARNING、NOTICE、または INFO)。CRITICAL メッセージの重要度が最大で、INFO メッセージの重要度が最小です。
<b>Message_ID</b>	エラーメッセージの一意の数値 ID です。接頭辞 V-16 は VCS を示します。

**Message\_Text** VCS で生成されたメッセージです。

たとえば、一般的なエージェントログメッセージは次のようになります。

```
2006/01/24 11:04:17 VCS ERROR V-16-10051-6026 GenericService:
CLSEV1-EnterpriseVaultAdminService:monitor:
The LanmanResName attribute has not been configured.
```

## Enterprise Vault Cluster Setup Wizard のエラーメッセージ

表 37-1 に、Enterprise Vault Cluster Setup wizard を実行した場合に表示される可能性のあるいくつかのメッセージについて説明します。

表 37-1 Enterprise Vault Cluster Setup Wizard のエラーメッセージ

メッセージ	説明
Access Denied.You must have Administrator privileges to run the wizard.	ローカル管理者のグループのメンバーであるユーザーのみがこのウィザードを実行できます。
VCS not running on the local machine.Either the service has not been started or it is in a stale state.	VCS サービスが起動していて、ローカルコンピュータ上で実行されていることを確認します。
MSMQ is not configured properly.	ウィザードは MSMQ がすべてのノードにインストールされ、設定されていることを確認します。このエラーメッセージは、MSMQ が特定のノードにインストールされていないか、設定が異なる場合に 표시됩니다。  問題を解決するには、Enterprise Vault Cluster Setup Wizard を続行する前に、MSMQ がインストールされ、設定されていることを確認します。
The required resource type MSMQ is not installed on this system.	ウィザードは MSMQ リソースの種類がシステムにインストールされていることを確認します。このリソースの種類は VCS によってインストールされます。

# Enterprise Vault 仮想サーバーのクラスタ化されたメッセージキューの表示

クラスタ化された Enterprise Vault インストールでは、デフォルトにより、Computer Management スナップインに Enterprise Vault メッセージキューが表示されません。その代わりに、スナップインはローカルコンピュータのキューのみを表示します。

## Enterprise Vault 仮想サーバーのクラスタ化されたメッセージキューを表示する方法

- 1 キューを表示するノード上で Enterprise Vault 仮想サーバーがオンラインになっていることを確認します。
- 2 管理者権限でコマンドプロンプトウィンドウを開きます。
- 3 コマンドプロンプトウィンドウで、Enterprise Vault のインストール先フォルダ (C:\Program Files (x86)\Enterprise Vault など) に移動します。
- 4 次のコマンドを入力します。

```
ClusterCompMgmt
```

- 5 Computer Management スナップインで、[サービスとアプリケーション] を展開し、[メッセージキュー] を展開します。Enterprise Vault メッセージキューは、[専用キュー] の下に一覧表示されます。

# Windows Server フェール オーバークラスタリングでの Enterprise Vault のクラスタ 化

- [第38章 Windows Server フェールオーバークラスタリングでのクラスタ化の概要](#)
- [第39章 Windows Server フェールオーバークラスタリングでのクラスタ化の準備](#)
- [第40章 Windows Server フェールオーバークラスタでの Enterprise Vault の設定](#)
- [第41章 Windows Server フェールオーバークラスタリングによるクラスタ化のトラブルシューティング](#)

# Windows Server フェールオーバークラスターリングでのクラスタ化の概要

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ーリングでの Enterprise Vault のクラスタ化について](#)
- [サポートされる Windows Server フェールオーバークラスターの構成](#)
- [Windows Server フェールオーバークラスターリングでの Enterprise Vault のクラスタ化に必要なソフトウェアと制限](#)
- [Windows Server フェールオーバークラスターリングでの共通の Enterprise Vault の設定](#)
- [Windows Server フェールオーバークラスターリングでの Enterprise Vault サービスの制御](#)

## Windows Server フェールオーバークラスターリングでの Enterprise Vault のクラスタ化について

Enterprise Vault を Windows Server フェールオーバークラスターリングでクラスタ化すると、Enterprise Vault で高可用性ソリューションを実現できます。Microsoft Exchange と SQL サーバーがクラスタ化されている環境で Enterprise Vault を設定する場合、サービスレベルの内容、回復時間、回復ポイント目標を満たすように Enterprise Vault をクラスタ化すると便利です。

Enterprise Vault クラスタサーバーを作成し、クラスター内の物理ノード間でフェールオーバーを可能にすることによって、高可用性が実現されます。クラスターサーバー上で実行される Enterprise Vault サービスは、仮想 IP アドレス、仮想コンピュータ名、仮想 Microsoft メッセージキュー、高可用性を備えた共有ディスクを使って動作します。エラーが発生し

た場合は、クラスタソフトウェアによって、クラスタサーバーのリソースがクラスタ内の別の物理ノードに移動されます。

フェールオーバークラスタで Enterprise Vault をクラスタ化するには、Windows Server フェールオーバークラスタの使用経験が必要です。詳しくは、Microsoft 社のマニュアルを参照してください。

## サポートされる Windows Server フェールオーバークラスタの構成

Enterprise Vault クラスタは次のノードで構成されます。

- 1 つ以上のプライマリノード。通常はそれぞれが Enterprise Vault クラスタサーバーをホストします。
- 1 つ以上のフェールオーバーノード。プライマリノードでエラーが発生した場合に Enterprise Vault クラスタサーバーのホストとしての役割を引き継ぐために待機します。

Enterprise Vault では、「アクティブ/アクティブ」クラスタ構成は許可されていません。つまり、クラスタノード上で実行できる Enterprise Vault クラスタサーバーは、常に 1 台のみです。この制限に対応したすべての操作モードで Enterprise Vault を設定できます。次に例を示します。

- アクティブ/パッシブフェールオーバーペア: プライマリノードに専用のフェールオーバーノードが存在する構成。
- N+1 (ホットスタンバイサーバー): 複数のプライマリノードが 1 台のフェールオーバーノードを共有する構成。一度に 1 台のノードエラーにのみ対応できます。
- N+M:N 台のプライマリノードと M 台のフェールオーバーノードでホットスタンバイの概念を拡張した構成。一度に M 台のノードエラーにのみ対応できます。
- N+M 多対多構成: N+M に類似しているが、フェールオーバー後、元のノードにフェールバックする必要がありません。元のノードが再度利用可能になると、そのノードはフェールオーバーノードとして動作します。

## Windows Server フェールオーバークラスタリングでの Enterprise Vault のクラスタ化に必要なソフトウェアと制限

プライマリノードとフェールオーバーノードのそれぞれにサポート対象のバージョンの Windows Server をインストールする必要があります。

各ノードで同じ Windows のバージョンが実行されている必要があります。

クラスターが Enterprise Vault SMTP アーカイブをサポートする必要がある場合は、クラスターの各ノードに Enterprise Vault SMTP アーカイブコンポーネントをインストールする必要があります。

クラスタ化のサポート対象バージョンについて詳しくは、「Enterprise Vault [Compatibility Charts](#)」を参照してください。

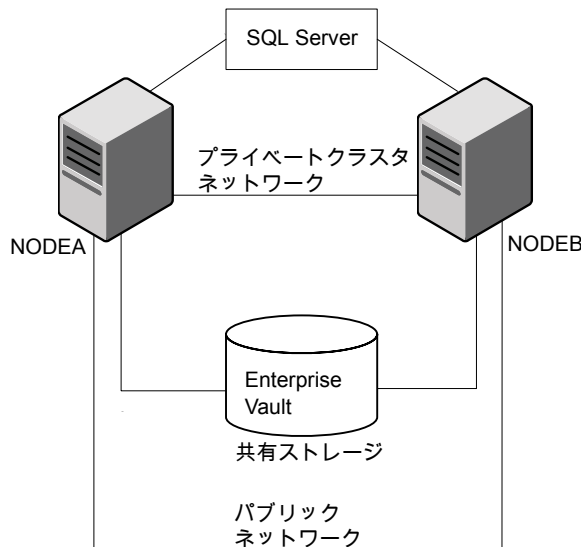
次の制限に注意してください：

- 計画しているクラスター内のサーバーには、**Compliance Accelerator** も **Discovery Accelerator** もインストールしないでください。これらの製品はクラスター内ではサポートされません。ただし、クラスター化されていない **Compliance Accelerator** または **Discovery Accelerator** は Enterprise Vault クラスターサーバーを参照できます。
- Enterprise Vault 設定ウィザードは、複数のクライアントアクセスポイントリソースまたは IP アドレスリソースが含まれるクラスターサービスをサポートしていません。
- Enterprise Vault のクラスターが Enterprise Vault に関連するリソースのみを含むようにすることを推奨します。

## Windows Server フェールオーバークラスターでの共通の Enterprise Vault の設定

図 38-1 は、一般的な構成を示しています。

図 38-1 アクティブ/パッシブフェールオーバーペア構成の Enterprise Vault





この例では、次のようになっています。

- NODEA と NODEB はフェールオーバークラスタにある 2 つの Enterprise Vault ノードです。NODEA はプライマリノードです。NODEB はフェールオーバーノードです。
- SQL サーバーと Microsoft Exchange もこのクラスタに設定されている場合があります。これらは Enterprise Vault に影響しません。
- Enterprise Vault サービスデータ用のボリュームが、共有ストレージに設定されています。
- Enterprise Vault クラスタサーバーはプライマリノード (NODEA) に設定されています。NODEA でエラーが発生した場合、クラスタサーバーのリソースが NODEB にフェールオーバーし、クラスタサーバーは NODEB でオンラインになります。

## Windows Server フェールオーバークラスタの Enterprise Vault サービスの制御

Enterprise Vault をクラスタをサポートするサーバー、または既存のクラスタサーバーのフェールオーバーノードのどちらに設定するかにかかわらず、設定ウィザードにより次の一連の Enterprise Vault サービスがノードにインストールされます。

- ディレクトリサービス
- インデックスサービス
- ショッピングサービス
- ストレージサービス
- タスク制御サービス

管理サービスは Enterprise Vault のインストール時にすでにインストールされています。Enterprise Vault SMTP アーカイブコンポーネントをインストールした場合は Enterprise Vault SMTP サービスも存在します。

クラスタのすべてのノードで共通設定を有効にするには、この一連のサービスを各ノードにインストールする必要があります。クラスタ構成では Enterprise Vault サービスを削除できません。

設定ウィザードにより、Enterprise Vault サービスは手動で起動するように設定されるため、クラスタソフトウェアはこれらのサービスを必要に応じて起動、停止できるようになります。

---

**メモ:** クラスタ構成では、管理コンソールまたは EVService ユーティリティを使ってサービスの起動や停止を行うことはできません。Windows のコントロールパネルのサービスアプレットを使ってサービスを停止すると、クラスタソフトウェアはシステムエラーが発生したものと判断し、サービスを再起動するか、フェールオーバーを開始します。Enterprise Vault サービスの起動や停止を安全に行うには、フェールオーバークラスタマネージャーだけを使用してください。

---

p.320 の「[Windows Server フェールオーバークラスターリング環境での Enterprise Vault サービスの起動と停止](#)」を参照してください。

## Windows Server フェールオーバークラスターのクラスタサービスと Enterprise Vault サービスリソースについて

Enterprise Vault サーバーをクラスタをサポートするサーバーとして設定する前に、Enterprise Vault クラスタサーバーとなるクラスタサービスを作成する必要があります。Enterprise Vault 設定ウィザードにより、次の Enterprise Vault サービスリソースがクラスタサービスに追加され、アクティブノードで追加したリソースの Enterprise Vault サービスの制御と監視を行えるようになります。

- 管理サービスリソース
- ディレクトリサービスリソース
- インデックスサービスリソース
- ショッピングサービスリソース
- ストレージサービスリソース
- タスク制御サービスリソース
- SMTP サービスリソース (SMTP アーカイブコンポーネントをノードにインストールしている場合のみ)

設定ウィザードにより、さらに別のリソース (Enterprise Vault Server Instance リソース) がクラスタサービスに追加されます。クラスタサービス内の他のすべての Enterprise Vault リソースは、このリソースに直接的または間接的に依存するように設定されます。これは、すでに Enterprise Vault を実行しているノードへのフェールオーバーを回避して、アクティブ/アクティブ操作モードにならないようにするためです。

## Windows Server フェールオーバークラスターのフェールオーバー時の動作

アクティブノードでエラーが発生すると、Enterprise Vault クラスタサーバーは、クラスタサービスの優先ノード一覧で次に利用可能なノードへのフェールオーバーを試行します。この場合、すべてのリソースにそのノードが所有者候補として設定されている必要があります。フェールオーバーノードで Enterprise Vault クラスタサーバーが実行されてい

い場合は、サーバーインスタンスリソースが最初にフェールオーバーします。その後、他のリソースが依存関係の順番に従ってフェールオーバーします。リソースによって Enterprise Vault サービスがフェールオーバーノードで起動されるため、Enterprise Vault が管理、アーカイブしているデータの可用性を維持できます。

# Windows Server フェールオーバークラスタリングでのクラスタ化の準備

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リングでの Enterprise Vault のクラスタ化の準備](#)
- [Windows Server フェールオーバークラスタの共有ディスクとボリュームの設定](#)
- [Enterprise Vault クラスタサービスを Windows Server フェールオーバークラスタに対して設定する](#)

## Windows Server フェールオーバークラスタリングでの Enterprise Vault のクラスタ化の準備

次の手順では、フェールオーバークラスタで新規または既存の Enterprise Vault インストール済み環境をクラスタ化する前に必要な準備の概要を示します。詳しくは、Microsoft 社のマニュアルを参照してください。

**Windows Server フェールオーバークラスタリングで Enterprise Vault のクラスタ化を準備する方法**

- 1 クラスタの操作モードを決定します。次の項目を決定します。
  - プライマリノードの数 (各ノードは Enterprise Vault クラスタサーバーの通常のホスト)
  - フェールオーバーノードの数

- 各クラスタサーバーの優先所有者となるノード
- 2 設定内容が必要条件を満たすことを確認します。  
p.287 の「[Windows Server フェールオーバークラスタリングでの Enterprise Vault のクラスタ化に必要なソフトウェアと制限](#)」を参照してください。
- 3 クラスタの共有ディスクとボリュームを設定します。  
p.293 の「[Windows Server フェールオーバークラスタの共有ディスクとボリュームの設定](#)」を参照してください。
- 4 フェールオーバークラスタマネージャーを使ってクラスタを作成し、プライマリノードとフェールオーバーノードを追加します。
- 5 各 Enterprise Vault クラスタサーバーに、必要なリソースが含まれるクラスタサービスを設定します。  
p.294 の「[Enterprise Vault クラスタサービスを Windows Server フェールオーバークラスタに対して設定する](#)」を参照してください。

## Windows Server フェールオーバークラスタの共有ディスクとボリュームの設定

クラスタに共有ストレージとボリュームを設定して、共有データを使えるようにする必要があります。各 Enterprise Vault クラスタサーバーには、次のデータを格納するためのボリュームが 1 つ以上必要です。

- MSMQ データ
- Enterprise Vault ストレージキュー
- インデックスサービスデータ
- ストレージサービスデータ (ボルトストアパーティション)
- ショッピングサービスデータ
- PST 保存フォルダ
- SMTP 保存フォルダ
- Centera ステージング領域

MSMQ データ、Enterprise Vault ストレージキュー、インデックスサービスデータ、ストレージサービスデータ、SMTP 保存フォルダに個別のストレージデバイスリソースを設定することを推奨します。これらのデータを同じドライブに配置すると、パフォーマンスが低下する場合があります。ただし、MSMQ データと Enterprise Vault ストレージキューは同じストレージデバイスリソースに置くことができます。これは MSMQ とストレージキューのパフォーマンスが類似しているためです。

パフォーマンス上の理由により、適切な場所に共有データを保存することを推奨します。一部のデータには個別のディスクが必要です。

詳しくは、<https://www.veritas.com/docs/100000918> で「Enterprise Vault Performance Guide」を参照してください。

たとえば、2 つの Enterprise Vault クラスタサーバー EVSERVER1 と EVSERVER2 を設定する場合、クラスタの共有ストレージを次のように割り当てることができます。

クラスタ	<ul style="list-style-type: none"> <li>■ ボリューム H: クォーラムデータ</li> </ul>
EVServer1	<ul style="list-style-type: none"> <li>■ ボリューム I: MSMQ データ</li> <li>■ ボリューム J: インデックスサービスデータ</li> <li>■ ボリューム K: ボルトストアデータ</li> <li>■ ボリューム L: PST 保存フォルダ、ショッピングサービスデータ、Centera ステージング領域</li> <li>■ ボリューム M: Enterprise Vault ストレージキュー</li> <li>■ ボリューム N: SMTP 保存フォルダ</li> </ul>
EVServer2	<ul style="list-style-type: none"> <li>■ ボリューム I: MSMQ データ</li> <li>■ ボリューム J: インデックスサービスデータ</li> <li>■ ボリューム K: ボルトストアデータ</li> <li>■ ボリューム L: PST 保存フォルダ、ショッピングサービスデータ、Centera ステージング領域</li> <li>■ ボリューム M: Enterprise Vault ストレージキュー</li> <li>■ ボリューム N: SMTP 保存フォルダ</li> </ul>

共有ディスクとボリュームの設定時には次の点に注意してください。

- 1 つのサーバーが同時に接続できるストレージデバイスは 1 つだけであるため、各ストレージデバイスの異なるクラスタサービスに対して個別にストレージを設定する必要があります。
- 必要なノードがフェールオーバー時にクラスタ化されたディスクリソースにアクセスできるように共有ディスクとボリュームを設定します。たとえば、2+1 構成では、クォーラムデータボリュームと、クラスタサーバーで使われているすべてのボリュームに対するアクセス権限がフェールオーバーノードに必要です。

## Enterprise Vault クラスタサービスを Windows Server フェールオーバークラスタに対して設定する

クラスタをサポートするクラスタサーバーごとにクラスタサービスを作成して設定する必要があります。たとえば、N+M クラスタでは N 個のクラスタサービスが必要です。Enterprise

Vault のクラスタが Enterprise Vault に関連するリソースのみを含むようにすることを推奨します。

**メモ:** Enterprise Vault 設定ウィザードは、複数のクライアントアクセスポイントリソースまたは IP アドレスリソースが含まれるクラスタサービスをサポートしていません。

表 39-1 Enterprise Vault クラスタサービスに必要なリソース

リソースの種類	依存関係	パラメータ	Comment
ストレージデバイスまたはボリュームマネージャ ディスクグループ	なし	必要なディスクボリュームを指定します。	この仮想サーバーで使うように設定した各ボリュームに対して 1 つのディスクリソースを設定します。
クライアントアクセスポイント	IP アドレスリソース	<ul style="list-style-type: none"><li>■ クラスタサービス名をクライアントアクセスポイントとして使います。</li><li>■ [DNS 登録の成功を必要とする]を選択することを推奨します。</li><li>■ [Kerberos 認証を有効にする]を選択します。これはメッセージキューリソースの場合に必須です。</li></ul>	クライアントアクセスポイントリソースを 1 つ設定します。
メッセージキュー	<ul style="list-style-type: none"><li>■ クラスタサーバーの MSMQ データのストレージデバイスリソース</li><li>■ クライアントアクセスポイントリソース</li></ul>	なし	1 つのメッセージキューリソースを設定します。

Enterprise Vault クラスタサービスを Windows Server フェールオーバークラスタに対して設定する方法

- 1 Windows のフェールオーバークラスタマネージャを起動します。
- 2 フェールオーバークラスタマネージャの左ペインで、[役割]を右クリックし、[役割の構成]をクリックします。

- 3 [高可用性ウィザード]の[役割の選択]ページで、[その他のサーバー]を選択して[次へ]をクリックします。
- 4 [高可用性ウィザード]の[クライアントアクセスポイント]ページで、クラスタネットワーク名および IP アドレスを入力し、[次へ]をクリックします。
- 5 [高可用性ウィザード]の[記憶域の選択]ページで、以前に設定したクラスタディスクを選択します。

p.293 の「[Windows Server フェールオーバークラスタの共有ディスクとボリュームの設定](#)」を参照してください。

- 6 必要なリソースをクラスタサービスに追加します。注記されている場合を除き、表に一覧表示されているリソースの種類ごとに 1 つのリソースを追加します。リソース名は次の形式で設定することを推奨します。

#### **`service_name-resource_type`**

たとえば、EV1 という名前のクラスタサービスにストレージデバイスリソースを追加する場合は、リソースに **EV1-StorageDevice** という名前を設定します。その後、Enterprise Vault 設定ウィザードにより、Enterprise Vault サービスリソースがこの名前の形式でクラスタサービスに追加されます。

選択したクラスタ操作モードに従って、必要なノードを各リソースの所有者候補として指定します。

- 7 [確認]ページで、[次へ]をクリックします。ウィザードは自動的に設定を完了します。
- 8 [概略]ページで、[完了]をクリックします。
- 9 フェールオーバークラスタマネージャで、作成したクラスタを右クリックし[リソースの追加]、[その他のリソース]、[メッセージキュー]の順にクリックします。
- 10 新しいリソースを右クリックし、[プロパティ]をクリックします。
- 11 [新規メッセージキューのプロパティ]ウィンドウで、[依存関係]タブをクリックします。
- 12 MSMQ ディスクとクライアントアクセスポイントをリソースのリストに追加し、[OK]をクリックします。
- 13 これでサービスは設定されました。クラスタがノード間でエラーなくフェールオーバーを実行できることを確認します。



# Windows Server フェールオーバークラスタでの Enterprise Vault の設定

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 Enterprise Vault の設定について](#)
- [Windows Server フェールオーバークラスタをサポートする新しい Enterprise Vault インストール済み環境を設定する方法](#)
- [既存の Enterprise Vault インストール済み環境の Windows Server フェールオーバークラスタへの変換](#)
- [既存の Enterprise Vault クラスタの修正](#)

## Windows Server フェールオーバークラスタの Enterprise Vault の設定について

この章では、次の内容について説明します。

- [クラスタをサポートする新しい Enterprise Vault インストール済み環境を設定する方法](#)
- [既存の Enterprise Vault インストール済み環境をクラスタに変換する方法](#)
- [既存の Enterprise Vault クラスタを修正して、別の Enterprise Vault クラスタサーバーまたはフェールオーバーノードを追加する方法、または共有ストレージを追加する方法](#)

先に進む前に、クラスタ化の準備を行う必要があります。

p.292 の「[Windows Server フェールオーバークラスタリングでの Enterprise Vault のクラスタ化の準備](#)」を参照してください。

# Windows Server フェールオーバークラスタをサポートする新しい Enterprise Vault インストール済み環境を設定する方法

このセクションでは、最初の Enterprise Vault インストール済み環境をクラスタとして設定する方法について説明します。

---

**メモ:** Enterprise Vault 設定ウィザードの実行中に Enterprise Vault 監視データベースの設定に関するエラーが表示された場合は、ウィザードを完了し、「[Enterprise Vault 監視データベースの設定のトラブルシューティング](#)」を参照してください。

---

## Windows Server フェールオーバークラスタをサポートする新しい Enterprise Vault インストール済み環境を設定する方法

- 1 Enterprise Vault を実行するすべてのノード (プライマリノードとフェールオーバーノードの両方) に Enterprise Vault をインストールします。ただし、この段階ではどのノードでも Enterprise Vault 設定ウィザードは実行しません。

クラスタに Enterprise Vault SMTP アーカイブが必要な場合は、SMTP アーカイブコンポーネントも各ノードにインストールする必要があります。

---

**注意:** すべてのノード上で Enterprise Vault のインストールフォルダは同じである必要があります。たとえば、プライマリノード上で Enterprise Vault を C:\Program Files (x86)\Enterprise Vault フォルダにインストールした場合は、フェールオーバーノード上でも C:\Program Files (x86)\Enterprise Vault にインストールする必要があります。このようにしないと、フェールオーバーノード上で Enterprise Vault を設定する際に問題が発生する場合があります。

---

- 2 クラスタサーバーとして使う Enterprise Vault サーバーを設定します。  
p.299 の「[Windows Server フェールオーバークラスタリングをサポートする新しい Enterprise Vault サーバーの設定](#)」を参照してください。
- 3 フェールオーバーノードとして使うノードで Enterprise Vault を設定します。  
p.303 の「[Windows Server フェールオーバークラスタ内のフェールオーバーノードの設定](#)」を参照してください。
- 4 クラスタをテストして、フェールオーバーが計画どおりに動作することを確認します。

## Windows Server フェールオーバークラスタリングをサポートする新しい Enterprise Vault サーバーの設定

新しくインストールされた Enterprise Vault サーバーで次のいずれかの手順を実行し、クラスタをサポートする Enterprise Vault サーバーとして設定します。次のどちらを実行するかによって、適切な手順を選択します。

- Enterprise Vault サーバーに Enterprise Vault ディレクトリを作成します。最初に設定する Enterprise Vault サーバーではこの処理が必須です。このディレクトリが Enterprise Vault サイトのコンテナとなり、サイトで Enterprise Vault サーバーの共通設定を定義します。各 Enterprise Vault サーバーは 1 つのサイトにのみ属する必要があります。設定処理により、新しいディレクトリに新しいサイトが作成され、Enterprise Vault サーバーがそのサイトに追加されます。また、指定した SQL サーバーにディレクトリデータベースも作成されます。
- 別の Enterprise Vault サーバーの Enterprise Vault ディレクトリに参加します。Enterprise Vault サーバーをディレクトリの既存の Enterprise Vault サイトに追加したり、ディレクトリに新しいサイトを作成してそのサイトに Enterprise Vault サーバーを追加したりすることができます。

新しい Enterprise Vault ディレクトリを作成する場合は、この手順に従ってください。既存のディレクトリがない場合は、この手順を使う必要があります。

### 新しいディレクトリでサーバーを設定する方法

- 1 フェールオーバークラスタマネージャを使って、以前に準備した適切なクラスタサービスが Enterprise Vault サーバーノードでオンラインになっていることを確認します。
- 2 サーバーノードで Enterprise Vault 設定ウィザードを起動します。
- 3 [クラスタをサポートする Enterprise Vault サーバーを新規作成]にチェックマークを付け、[次へ]をクリックします。
- 4 現在このノードでオンラインになっているクラスタサービスがウィザードに一覧表示されます。準備済みのクラスタサービスを選択して、[次へ]をクリックします。
- 5 ウィザードの次のページで、新しいボルトディレクトリを作成するか、既存のボルトディレクトリを使うかを選択できます。このコンピュータに新しいボルトディレクトリを作成するには[はい]を選択します。これで新しい Enterprise Vault サイトが作成されます。[次へ]をクリックします。
- 6 Enterprise Vault で、管理コンソールにデフォルト設定をポピュレートする場合に使う言語を選択します。次に、[次へ]をクリックします。

- 7 このウィザードで、ボルトサービスアカウントの詳細の入力が求められます。このアカウントは、Enterprise Vault のインストール前の作業で作成したアカウントです。**domain\_name¥username** の形式とします。別の方法として、[...] ボタンを使ってアカウントを参照することもできます。

パスワードの詳細を入力して[次へ]をクリックします。

ボルトサービスアカウントにコンピュータのユーザー権限が付与されたことを示すメッセージや、ディレクトリサービスの作成に関するメッセージがいくつか表示されます。

- 8 メッセージが表示されたら、Enterprise Vault ディレクトリデータベースで使う SQL Server の場所を入力し、[次へ]をクリックします。
- 9 Enterprise Vault ディレクトリデータベースとトランザクションログの場所を入力するように求められます。パフォーマンス上の理由から、これらを別々のディスクに配置することを推奨します。デフォルトの場所が表示されている場合は、その場所が不正であれば変更します。リモートコンピュータの SQL サーバーを指定した場合、パスはそのコンピュータで有効なパス (¥¥DC¥C\$¥Program Files¥Microsoft SQL Server¥MSSQL¥Data など) である必要があります。

次に、[次へ]をクリックします。

- 10 メッセージが表示されたら、Enterprise Vault 監視データベースで使う SQL Server の場所を入力します。この Enterprise Vault サーバーの設定が完了したらすぐに監視を開始するには、[すぐに監視を開始]を選択したままにします。次に、[次へ]をクリックします。
- 11 Enterprise Vault 監視データベースとトランザクションログの場所を入力するように求めるメッセージが表示されます。パフォーマンス上の理由から、これらを別々のディスクに配置することを推奨します。デフォルトの場所が表示されている場合は、その場所が不正であれば変更します。リモートコンピュータの SQL サーバーを指定した場合、パスはそのコンピュータで有効なパスである必要があります。

次に、[次へ]をクリックします。

- 12 新しいボルトサイトの名前と説明の入力が求められます。

ボルトサイトのエイリアスが自動的に作成されます。これは、ステップ 4 で選択したクラスタサービスのクライアントアクセスポイントです。

- 13 [次へ]をクリックして続行します。

- 14 選択した Enterprise Vault サイトと Enterprise Vault ディレクトリコンピュータが確認のため表示されます。現在設定しているコンピュータの[コンピュータエイリアス]を指定するように求められます。

ステップ 4 で選択した Enterprise Vault クラスタサービスのクライアントアクセスポイントを入力し、[次へ]をクリックして Enterprise Vault ディレクトリを更新します。

- 15 DNS エイリアスを使わないことを確認するメッセージが表示されます。ウィザードページで、再度[はい]をクリックし、[次へ]をクリックします。

- 16 このコンピュータに追加される Enterprise Vault サービスが一覧表示されます。[次へ]をクリックして、サービスを追加します。
- 17 追加した Enterprise Vault サービスがウィザードに表示されます。クラスタ構成では、サービスを追加または削除できないことに注意してください。[次へ]をクリックして続行します。
- 18 ウィザードには、追加したサービスの概要が表示されます。[次へ]をクリックして続行します。
- 19 設定ウィザードに、各 Enterprise Vault サービスにクラスタリソースを作成する必要があることが示されます。
- 20 ウィザードの最後のページに、ウィザードで実行した処理とその結果の一覧が表示されます。[Enterprise Vault 管理コンソールを実行]を選択し、[完了]をクリックしてウィザードを終了します。

---

**メモ:** 開始ウィザードを実行するオプションを選択しないでください。

---

- 21 以下のステップに従って、パスをクラスタ内の共有ドライブにあるインデックスメタデータフォルダに設定します。インデックスメタデータフォルダは、Enterprise Vault によりインデックス設定データとレポートデータが格納されるフォルダです。
  - Enterprise Vault ディレクトリサービスと管理サービスをオンラインにします。
  - Enterprise Vault 管理コンソールの左ペインで、[Enterprise Vaultサーバー]、[EVServer.domain.local]、[サービス]の順に参照します。
  - 右ペインで[Enterprise Vault Indexing Service]を右クリックし、[プロパティ]をクリックします。
  - [サービスプロパティ]ダイアログボックスの[全般]タブで、[インデックスメタデータの場所] のパスをクラスタ内の共有ドライブのパスに設定します。
  - [OK] をクリックして変更内容を保存し、インデックスサービスを起動します。

既存のディレクトリに参加する場合は、この手順に従ってください。既存のディレクトリがクラスタ内になくてもかまいません。

#### サーバーを設定し、既存のディレクトリに参加する方法

- 1 フェールオーバークラスタマネージャを使って、以前に準備した適切なクラスタサービスが Enterprise Vault サーバーノードでオンラインになっていることを確認します。
- 2 Enterprise Vault サーバーノード上の &ProductNameShort 設定ウィザードを起動します。
- 3 [クラスタをサポートする Enterprise Vault サーバーを新規作成]にチェックマークを付け、[次へ]をクリックします。

- 4 現在このノードでオンラインになっているクラスタサービスがウィザードに一覧表示されます。準備済みのクラスタサービスを選択して、[次へ]をクリックします。
- 5 ウィザードの次のページで[いいえ]を選択して別の Enterprise Vault サーバーの Enterprise Vault ディレクトリに参加するように選択し、リモート Enterprise Vault サーバーの DNS エイリアスを指定します。  
[次へ]をクリックして続行します。
- 6 ウィザードの次のページで次のいずれかの操作を実行します。
  - リモート Enterprise Vault ディレクトリで新しいボルトサイトを作成するように選択します。
  - [次へ]をクリックして手順 7 から続行します。
  - または、リモート Enterprise Vault ディレクトリの既存のボルトサイトに参加するように選択し、表示される一覧からボルトサイトを選択します。
  - [次へ]をクリックして手順 10 から続行します。
- 7 新しいボルトサイトの名前と説明の入力が求められます。
- 8 最初の Enterprise Vault サーバーがサイトに追加されると自動的に作成されるボルトサイトエイリアスは、手順 6 で指定したリモート Enterprise Vault サーバーの DNS エイリアスになります。
- 9 [次へ]をクリックして続行します。
- 10 選択した Enterprise Vault サイトと Enterprise Vault ディレクトリコンピュータが確認のため表示されます。現在設定しているコンピュータの [DNS エイリアス] を指定するように求められます。
- 11 Enterprise Vault クラスタサービスのクライアントアクセスポイントを入力します。
- 12 [次へ]をクリックして、Enterprise Vault ディレクトリを更新します。
- 13 このコンピュータに追加される Enterprise Vault サービスが一覧表示されます。[次へ]をクリックして、サービスを追加します。
- 14 新たに追加された Enterprise Vault サービスが一覧表示されるので、サービスのプロパティを確認することができます。クラスタ構成では、サービスを追加または削除できないことに注意してください。[次へ]をクリックして続行します。
- 15 インデックスサービスとショッピングサービスのストレージの場所が表示されます。デフォルトでは、選択したクラスタサービス内の最初のディスクリソースにこれらの場所が設定されています。場所が適切な場合は、[次へ]をクリックします。異なるストレージの場所を指定する場合は、[戻る]をクリックして、サービスのプロパティを編集します。ストレージの場所を、E:\Shopping などのローカルの場所に修正しようとする、警告が表示されます。
- 16 設定ウィザードに、各 Enterprise Vault サービスにクラスタリソースを作成する必要があることが示されます。

- 17 ウィザードの最後のページに、ウィザードで実行した処理とその結果の一覧が表示されます。[完了]をクリックしてウィザードを終了します。
- 18 以下のステップに従って、パスをクラスタ内の共有ドライブにあるインデックスメタデータフォルダに設定します。インデックスメタデータフォルダは、Enterprise Vault によりインデックス設定データとレポートデータが格納されるフォルダです。
  - Enterprise Vault ディレクトリサービスと管理サービスをオンラインにします。
  - Enterprise Vault 管理コンソールの左ペインで、[Enterprise Vaultサーバー]、[EVServer.domain.local]、[サービス]の順に参照します。
  - 右ペインで[Enterprise Vault Indexing Service]を右クリックし、[プロパティ]をクリックします。
  - [サービスプロパティ]ダイアログボックスの[全般]タブで、[インデックスメタデータの場所] のパスをクラスタ内の共有ドライブのパスに設定します。
  - [OK] をクリックして変更内容を保存し、インデックスサービスを起動します。

## Windows Server フェールオーバークラスタ内のフェールオーバーノードの設定

フェールオーバーノードとして使うノードで次の手順を実行します。

### Windows Server フェールオーバークラスタ内のフェールオーバーノードを設定する方法

- 1 Enterprise Vault クラスタサービスがクラスタ内の別のノードでオンラインであることを確認します。設定するノードでクラスタサービスをオンラインにしないでください。設定するノードは、そのリソース用の利用可能なフェールオーバーノードである必要があります。

- 2 クラスタリソースグループで SMTP サービスを設定する場合は、フェールオーバーノードに Enterprise Vault SMTP アーカイブコンポーネントをインストールしている必要があります。

- 3 ノードで Enterprise Vault 設定ウィザードを実行します。

- 4 [既存のクラスタ化されたサーバーのフェールオーバーノードとしてこのノードを追加]をクリックしてから、[次へ]をクリックします。

- 5 ノードをフェールオーバーノードとして追加する Enterprise Vault クラスタサービス名の指定を求めるメッセージが表示されます。

このノードにフェールオーバーするように設定されている Enterprise Vault クラスタサービスを選択し、[次へ]をクリックします。

- 6 ウィザードの次のページで、ボルトサービスアカウントのパスワードを入力し、[次へ]をクリックします。

- 7 ウィザードの次のページに、ウィザードの以降の処理が一覧表示されます。続行する場合は[次へ]をクリックし、[OK]をクリックして処理を確定します。
- 8 ウィザードの最後のページに、ウィザードで実行した処理とその結果の一覧が表示されます。[完了]をクリックしてウィザードを終了します。

## Enterprise Vault 監視データベースの設定のトラブルシューティング

Enterprise Vault 設定ウィザードの実行中に、Enterprise Vault 監視データベースの設定が失敗したことを示すエラーが表示されたら、設定ウィザードを完了し、監視設定ユーティリティを実行して、監視データベースと監視エージェントを手動で設定します。

実行方法については、次の Enterprise Vault サポート Web サイトから Veritas テクニカルノートを参照してください。

<https://www.veritas.com/docs/100018087>

このテクニカルノートでは、監視エージェントに関する問題のトラブルシューティング方法についても説明しています。

## 各種 Windows Server フェールオーバークラスタリングモードでの Enterprise Vault のインストール例

以下の例は、各種クラスタ操作モードで Enterprise Vault の最初のインストール済み環境を設定する方法を示しています。

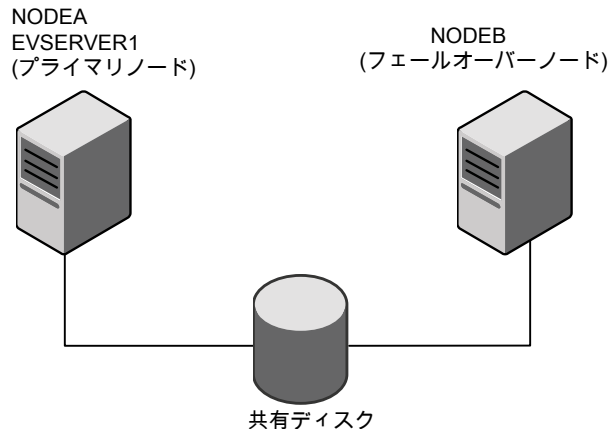
### アクティブ/パッシブフェールオーバー構成の Enterprise Vault のクラスタ化

この例では、「アクティブ/パッシブ」フェールオーバーペアの新しい Enterprise Vault インストール済み環境の設定について説明します。

図 40-1 に、Enterprise Vault クラスタサーバー EVSERVER1 を実行しているプライマリノード NODEA と、専用のフェールオーバーノード NODEB で構成される単一のフェールオーバーペアを示します。



図 40-1 フェールオーバーペアの設定



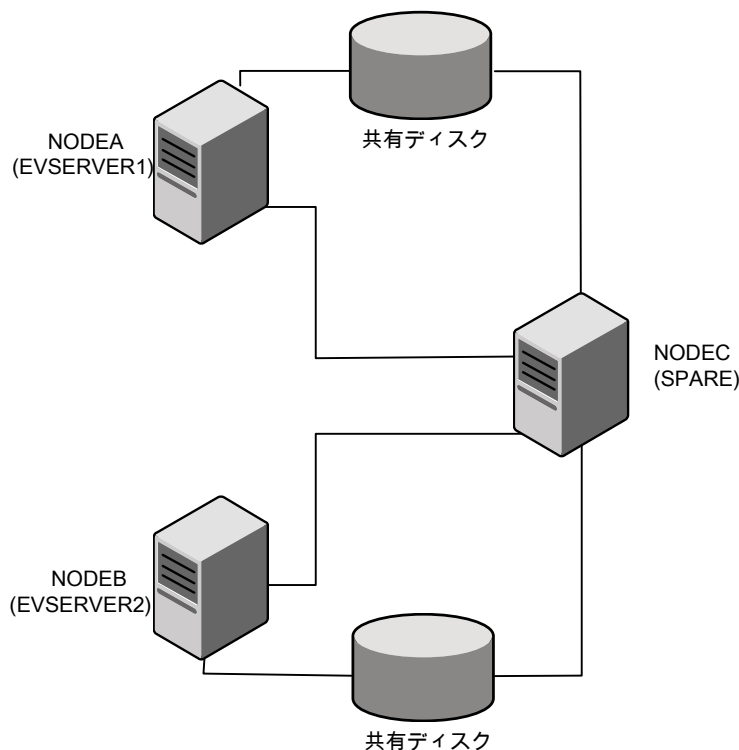
#### アクティブ/パッシブフェールオーバー構成の Enterprise Vault をクラスタ化する方法

- 1 次の手順を実行して、Enterprise Vault のクラスタ化の準備をします。
  - プライマリサーバーのノード (NODEA) を作成します。
  - フェールオーバーサーバーのノード (NODEB) を作成します。
  - クラスタサーバーのクラスタサービス EVSERVER1 を作成し、優先所有者を NODEA、NODEB の順に設定します。
  - 必要なリソースをクラスタサービスに追加し、NODEA と NODEB がこのリソースの所有者候補に設定されていることを確認します。
  - クラスタサーバーの DNS エントリを作成します。
- 2 Enterprise Vault を NODEA と NODEB にインストールします。ただし、Enterprise Vault 設定ウィザードは実行しません。
- 3 NODEA で Enterprise Vault 設定ウィザードを実行して、クラスタをサポートする新しい Enterprise Vault サーバーを設定するように選択します。Enterprise Vault サービスリソースを作成するクラスタサービスとして EVSERVER1 を選択します。ポルトサイトのエイリアスが自動的に作成されます。
- 4 NODEB で Enterprise Vault 設定ウィザードを実行して、既存のクラスタサーバーのフェールオーバーノードを設定するように選択します。このノードをフェールオーバーノードとして追加するクラスタサービスに EVSERVER1 を選択します。
- 5 NODEA から NODEB へのフェールオーバーをテストします。

## 「多対多」をサポートしない 2+1 構成の Enterprise Vault のクラスタ化

図 40-2 に、Enterprise Vault サーバーを実行している 2 つのノードと、1 つのスペアノードが存在する構成を示します。

図 40-2 「多対多」をサポートしない 2+1 構成



NODEA または NODEB でエラーが発生すると、そのノードで実行中の Enterprise Vault 仮想サーバーは NODEC にフェールオーバーできます。これは「多対多」構成ではないため、ノードでエラーが発生した場合は、ノードの回復後にリソースを戻して高可用性を回復する必要があります。

### 「多対多」をサポートしない 2+1 構成の Enterprise Vault をクラスタ化する方法

- 1 次の手順で、クラスタ化の準備をします。
  - クラスタに 3 つのノード (NODEA、NODEB、NODEC) を追加します。
  - 2 つのクラスタサービス (EVSERVER1、EVSERVER2) を作成し、必要なリソースを各サービスに追加します。

- ノードが次に示す順序で優先所有者になるように、サービスとリソースを設定します。

EVSERVER1      NODEA、NODEC

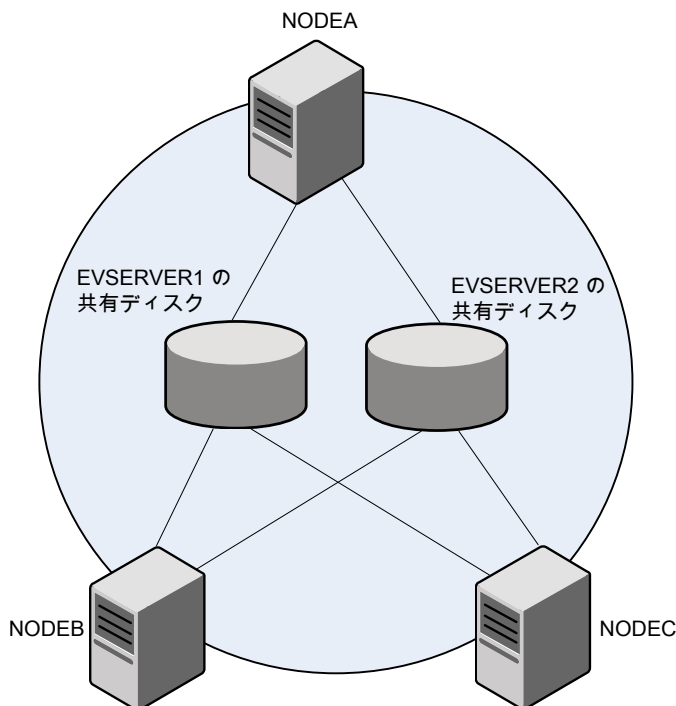
EVSERVER2      NODEB、NODEC

- クラスタサーバー EVSERVER1 と EVSERVER2 の DNS エントリを作成します。
- 2 Enterprise Vault を NODEA、NODEB、NODEC にインストールします。ただし、Enterprise Vault 設定ウィザードは実行しません。
  - 3 NODEA で Enterprise Vault 設定ウィザードを実行して、クラスタをサポートする新しい Enterprise Vault サーバーを設定するように選択します。Enterprise Vault サービスリソースを作成するクラスタサービスとして EVSERVER1 を選択します。ボルトサイトエイリアスは、クラスタサーバーエイリアスから自動的に作成されます。
  - 4 NODEB で Enterprise Vault 設定ウィザードを実行して、クラスタをサポートする新しい Enterprise Vault サーバーを設定するように選択します。Enterprise Vault サービスリソースを作成するクラスタサービスとして EVSERVER2 を選択します。ボルトサイトエイリアスは、クラスタサーバーエイリアスから自動的に作成されます。
  - 5 NODEC で Enterprise Vault 設定ウィザードを実行して、既存のクラスタサーバーのフェールオーバーノードを設定するように選択します。クラスタサービスとして EVSERVER1 か EVSERVER2 を選択します。このノードは EVSERVER1 と EVSERVER2 両方のフェールオーバーノードとして設定されます。
  - 6 クラスタをテストして、NODEA でエラーが発生した場合に EVSERVER1 のリソースが NODEC に正常にフェールオーバーすることを確認します。その後、EVSERVER1 のリソースを NODEA に戻し、NODEB でエラーが発生した場合に EVSERVER2 のリソースが NODEC に正常にフェールオーバーすることを確認します。

## 2+1「多対多」構成での Enterprise Vault のクラスタ化

2+1 構成の 2 つ目のオプションとして、Enterprise Vault クラスタサーバー EVSERVER1 と EVSERVER2 を 3 つのどのノードでも実行できるように設定する方法があります。この方法では、NODEA でエラーが発生して EVSERVER1 が NODEC にフェールオーバーした場合、NODEA をオンラインに戻して EVSERVER1 と EVSERVER2 のフェールオーバーノードとして使えます。

図 40-3 2+1「多対多」構成



設定処理を拡張して、任意の数のプライマリノードとフェールオーバーノードを使う **N+M** 構成を実現できます。**Windows Server** フェールオーバークラスタでサポートされているクラスターノードを合計 8 つまで使えます。

## 2+1「多対多」構成で Enterprise Vault をクラスタ化する方法

1 次の手順で、クラスタ化の準備をします。

- クラスタに 3 つのノード (NODEA、NODEB、NODEC) を追加します。
- 2 つのクラスタサービス (EVSERVER1、EVSERVER2) を作成し、必要なリソースを各サービスに追加します。
- ノードが次に示す順序で優先所有者になるように、サービスとリソースを設定します。

EVSERVER1      NODEA、NODEC、NODEB

EVSERVER2      NODEB、NODEC、NODEA

- 2 「多対多」をサポートしない 2+1 構成の手順 2 から手順 5 を実行します。  
p.306 の「[「多対多」をサポートしない 2+1 構成の Enterprise Vault のクラスタ化](#)」を参照してください。
- 3 クラスタをテストして、アクティブノードでエラーが発生した場合にクラスタサーバーが適切なノードにフェールオーバーすることを確認します。
- 4 たとえば、手順 1 に示したとおりにクラスタサービスの優先所有者を設定した場合は、次のことを確認します。
  - NODEA でエラーが発生した場合に EVSERVER1 が NODEC に正常にフェールオーバーすることを確認します。
  - その後、NODEA をスペアノードとしてオンラインに戻し、NODEB でエラーが発生した場合に EVSERVER2 が NODEA にフェールオーバーすることを確認します。

## 既存の Enterprise Vault インストール済み環境の Windows Server フェールオーバークラスタへの変換

クラスタ化されていない単独のサーバーに Enterprise Vault をインストール済みの場合、この環境をフェールオーバークラスタに変換できます。クラスタに変換するには、既存の Enterprise Vault インストール済み環境が次の条件を満たす必要があります。

- Enterprise Vault はクラスタの一部としてではなく、非クラスタ構成で構成しておく必要があります。
- Enterprise Vault は完全修飾ノード名ではなく DNS エイリアスで構成する必要があります。
- Enterprise Vault サーバーではインデックスサービス、ショッピングサービス、タスク制御サービス、ストレージサービスがすべて有効になっている必要があります。
- Enterprise Vault SMTP アーカイブが必要な場合は、Enterprise Vault サーバーに SMTP アーカイブコンポーネントをインストールしておく必要があります。
- 計画しているクラスタ内のサーバーには、Compliance Accelerator も Discovery Accelerator もインストールしないでください。これらの製品はクラスタ内ではサポートされません。ただし、クラスタ化されていない Compliance Accelerator または Discovery Accelerator は Enterprise Vault クラスタサーバーを参照できます。

既存の Enterprise Vault インストール済み環境は前述のいずれかの操作モードでクラスタ化できます。次の点に注意してください。

- 必要に応じて、新規と既存の Enterprise Vault サーバーを組み合わせてクラスタサーバーとして設定できます。
- フェールオーバーノードとして使うノードでは、Enterprise Vault の新規インストールを実行する必要があります。

### 既存の Enterprise Vault インストール済み環境を Windows Server フェールオーバークラスタに変換する方法

- 1 クラスタ化の準備を行います。  
[p.292 の「Windows Server フェールオーバークラスタリングでの Enterprise Vault のクラスタ化の準備」](#)を参照してください。
- 2 Enterprise Vault をフェールオーバーノードにインストールします。また、必要に応じて、既存のインストール済み環境に追加するプライマリノードにもインストールします。この段階では、どのノードでも Enterprise Vault 設定ウィザードは実行しないでください。Enterprise Vault のインストール方法については、このガイドのセクション I と II を参照してください。
- 3 既存の Enterprise Vault サーバーを、クラスタをサポートするサーバーに変換します。  
[p.310 の「既存の Enterprise Vault サーバーの Windows Server フェールオーバークラスタリングをサポートするサーバーへの変換」](#)を参照してください。
- 4 新しい Enterprise Vault サーバーを追加する場合は、新しい Enterprise Vault サーバーを、クラスタをサポートするサーバーとして設定します。  
[p.299 の「Windows Server フェールオーバークラスタリングをサポートする新しい Enterprise Vault サーバーの設定」](#)を参照してください。
- 5 フェールオーバーノードの Enterprise Vault を設定します。  
[p.303 の「Windows Server フェールオーバークラスタ内のフェールオーバーノードの設定」](#)を参照してください。
- 6 クラスタをテストして、フェールオーバーが計画どおりに動作することを確認します。

## 既存の Enterprise Vault サーバーの Windows Server フェールオーバークラスタリングをサポートするサーバーへの変換

このセクションでは、既存の Enterprise Vault サーバーをクラスタをサポートするサーバーに変換する方法と、高可用性の場所へのデータの移動について説明します。

### 既存の Enterprise Vault サーバーを Windows Server フェールオーバークラスタリングをサポートするサーバーに変換する方法

- 1 次のすべてが高可用性共有ストレージデバイス上にあることを確認します。
  - インデックスサービスデータ

- ショッピングサービスデータ
- ボルトストアパーティション
- PST 保存フォルダ
- SMTP 保存フォルダ \*
- Centera ステージング領域

\* SMTP 保存フォルダは Enterprise Vault クラスタで Enterprise Vault SMTP サービスを設定している場合にのみ必要です。

アイテムが高可用性共有ストレージデバイス上にない場合は、Enterprise Vault ディレクトリデータベースの場所を修正し、関連付けされたデータを新しい場所に移動します。

p.312 の「高可用性の場所への Enterprise Vault データの移動」を参照してください。

- 2 フェールオーバークラスタマネージャを使って、以前に準備した適切なクラスタサービスが Enterprise Vault サーバーノードでオンラインになっていることを確認します。
- 3 Windows で、Enterprise Vault クラスタ変換ウィザードを起動します。
- 4 ウィザードの最初のページが表示されたら、[次へ]をクリックして続行します。
- 5 このウィザードでは、いくつかの事項をチェックしてクラスタに変換するインストール済み環境が適切か判断します。チェック後、ウィザードの完了時に、現在物理ノードを指している DNS エイリアスまたはホストファイルのエントリを更新して、クラスタサーバー名を指すようにする必要があることを示す警告メッセージが表示されます。
- 6 その後、Enterprise Vault サービスとパーティションの現在のファイルの場所が一覧表示されます。設定を続行する前に、これらのすべての場所が高可用性の共有ストレージであることを確認する必要があります。チェックボックスにチェックマークを付けて高可用性を確認してから[次へ]をクリックして続行するか、[キャンセル]をクリックしてウィザードを終了し、必要なデータを高可用性の場所に移動してからウィザードを再実行します。
- 7 Enterprise Vault MSMQ キューにメッセージがあることが検出されると、各キューの名前とキューにあるメッセージ数を示すページが表示されます。権限の制約のため、これらのメッセージはクラスタメッセージキューに移動できません。ウィザードを中止して、Enterprise Vault によってメッセージキューが消去されるまで非クラスタ環境でサービスを実行することを推奨します。消去後にクラスタ変換ウィザードを再実行できます。この処理を行わずに設定を続行すると、メッセージはノード固有のキューに残り、処理されません。キューを消去せずに続行する場合は、[クラスタへの変換処理の設定を続行]にチェックマークを付けて[次へ]をクリックします。
- 8 現在このノードでオンラインになっているクラスタサービスがウィザードに一覧表示されます。必要なクラスタサービスを選択し、[次へ]をクリックします。

- 9 ウィザードによって必要なリソースが作成され、Enterprise Vault サービスを手動で起動できるように更新されます。また、ディレクトリデータベースのテーブルが更新され、コンピュータエントリテーブルのローカルコンピュータ名とメッセージキュー名が削除されます。ウィザードの最後のページに、ウィザードで実行した処理とその結果の一覧が表示されます。[完了]をクリックしてウィザードを終了します。
- 10 ローカルノード名ではなくクラスタサーバー名を指すように手動で DNS エイリアスを更新します (まだ設定していない場合)。
- 11 フェールオーバークラスタマネージャを使って、クラスタサーバーのリソースをオンラインにします。

## 高可用性の場所への Enterprise Vault データの移動

高可用性の場所に Enterprise Vault データを移動する手順の概略は、次のとおりです。

- インデックスサービス、ショッピングサービス、ストレージサービス、タスク制御サービスを停止します。
- Enterprise Vault ディレクトリデータベースとデータファイルのバックアップコピーを作成します。
- Enterprise Vault ディレクトリに対して、Enterprise Vault 管理コンソールを使うか SQL クエリーを実行して、以下に説明するようにデータを移動します。

IndexRootPathEntry  
 [IndexRootPath]

- この場所の内容を高可用性の場所に移動します。
- 新しい場所を指すように、SQL を使ってデータベースを更新します。

現在の場所を表示する SQL は、次のとおりです。

```
SELECT *
FROM IndexRootPathEntry
WHERE (IndexRootPathEntryId = '<ID FROM
LOG FILE>')
```

場所を更新する SQL は、次のとおりです。

```
UPDATE IndexRootPathEntry
SET IndexRootPath = '<THE NEW LOCATION>'
WHERE (IndexRootPathEntryId = '<ID FROM
LOG FILE>')
```



- PartitionEntry [AccountName] ■ プールエントリの認可ファイル (.pea) を高可用性の場所に移動します。
- Enterprise Vault 管理コンソールを使って Centera パーティションのプロパティを表示し、その後[接続]タブの [プールエントリの認可ファイルの場所] フィールドを、新しい場所を指すように編集します。

- PartitionEntry [PartitionRootPath] ■ この場所の内容を高可用性の場所に移動します。
- 新しい場所を指すように、SQL を使ってデータベースを更新します。

現在の場所を表示する SQL は、次のとおりです。

```
SELECT *
FROM PartitionEntry
WHERE (PartitionEntryId = '<ID FROM LOG
FILE>')
```

場所を更新する SQL は、次のとおりです。

```
UPDATE PartitionEntry
SET PartitionRootPath = '<THE NEW
LOCATION>'
WHERE (PartitionEntryId = '<ID FROM LOG
FILE>')
```

PartitionEntry/Locations  
 [SecondaryLocation]

- セカンダリストレージファイルを高可用性の場所に移動します。
- 新しい場所を指すように、SQL を使ってデータベースを更新します。

現在の場所を表示する SQL は、次のとおりです。

```
SELECT *
FROM PartitionEntry
INNER JOIN Locations ON
PartitionEntry.SecondaryLocation =
Locations.LocationIdentity
WHERE (PartitionEntry.PartitionEntryId =
'<ID FROM LOG FILE>')
```

場所を更新する SQL は、次のとおりです。

```
UPDATE Locations
SET Location = '<NEW LOCATION>'
WHERE LocationIdentity =
(SELECT SecondaryLocation FROM
PartitionEntry
WHERE PartitionEntryId = '<ID FROM LOG
FILE>')
```

PartitionEntry  
 [StagingRootPath]

- この場所の内容を高可用性の場所に移動します。
- 新しい場所を指すように、SQL を使ってデータベースを更新します。

現在の場所を表示する SQL は、次のとおりです。

```
SELECT *
FROM PartitionEntry
WHERE (PartitionEntryId = '<ID FROM LOG
FILE>')
```

場所を更新する SQL は、次のとおりです。

```
UPDATE PartitionEntry
SET StagingRootPath = '<THE NEW LOCATION>'
WHERE (PartitionEntryId = '<ID FROM LOG
FILE>')
```

PSTMigratorTask  
 [MigrationDirectory]

- この場所の内容を高可用性の場所に移動します。
- Enterprise Vault 管理コンソールを使って PST 移行タスクのプロパティを表示し、一時ファイルフォルダを更新します。

- |  |   |
|--|---|
| ShoppingServiceEntry<br>[ShoppingRootPath] | <ul style="list-style-type: none"> <li>■ この場所の内容を高可用性の場所に移動します。</li> <li>■ Enterprise Vault 管理コンソールを使ってショッピングサービスの場所を編集し、新しい高可用性の場所を設定します。</li> </ul>               |
| SiteEntry<br>[PSTHoldingDirectory]         | <ul style="list-style-type: none"> <li>■ この場所の内容を高可用性の場所に移動します。</li> <li>■ Enterprise Vault 管理コンソールを使ってサイトプロパティを表示し、新しい場所を指すように PST 保管フォルダのプロパティを更新します。</li> </ul>  |
| SmtptArchivingTask<br>[HoldingFolder]      | <ul style="list-style-type: none"> <li>■ この場所の内容を高可用性の場所に移動します。</li> <li>■ Vault 管理コンソールを使って、SMTP アーカイブタスクのプロパティを表示し、SMTP 保存フォルダのプロパティを新しい場所を指すように更新します。</li> </ul> |

## 既存の Enterprise Vault クラスタの修正

このセクションでは、既存の Enterprise Vault クラスタを修正して次の処理を行う方法について説明します。

- 新しい Enterprise Vault クラスタサーバーのホストまたはフェールオーバーノードとなるノードを追加します。
- クラスタサーバーの共有ストレージを追加します。
- 既存のクラスタに SMTP サービスを追加します。

## 既存の Windows Server フェールオーバークラスタへのノードの追加

ノードを既存の Enterprise Vault クラスタに追加して、新しい Enterprise Vault クラスタサーバーのホストまたはフェールオーバーノードとして使うと便利です。

### ノードを既存の Windows Server フェールオーバークラスタに追加する方法

- 1 新しいノードの必要なディスクボリュームを共有します。
- 2 フェールオーバークラスタマネージャーを使って、クラスタにノードを追加します。
- 3 新しい Enterprise Vault クラスタサーバーを追加する場合は、新しいクラスタサービスを準備して必要なリソースを追加します。

p.294 の「[Enterprise Vault クラスタサービスを Windows Server フェールオーバークラスタに対して設定する](#)」を参照してください。

- 4 新しいノードを、このノード上で実行されるクラスタサービスのすべてのリソースの所有者候補として設定します。

- 5 新しいノードを、このノード上で実行されるクラスタサービスの優先所有者一覧の適切な位置に追加します。
- 6 Enterprise Vault をノードにインストールします。
- 7 Enterprise Vault 設定ウィザードを実行し、必要に応じて、[クラスタをサポートする Enterprise Vault サーバーを新規作成]または[既存のクラスタ化されたサーバーのフェールオーバーノードとしてこのノードを追加]を選択します。
- 8 修正したクラスタをテストして、新しいノードでフェールオーバーが計画どおりに動作することを確認します。

## Enterprise Vault クラスタサーバー用として既存の Windows Server オーバークラスタに共有ストレージを追加する

Enterprise Vault クラスタサーバーのストレージを増やすには、共有ストレージを既存の Enterprise Vault クラスタに追加すると便利です。

### Enterprise Vault クラスタサーバー用として既存の Windows Server フェールオーバークラスタに共有ストレージを追加する方法

- 1 追加の共有ディスクとボリュームを設定し、このディスクとボリュームへのアクセスが必要なノードのボリュームを共有します。
- 2 新しいストレージを使うクラスタサーバーに対して次の設定を行います。
  - 新しいボリュームごとに、クラスタサービスにストレージデバイスリソースを追加します。

---

**メモ:** ストレージデバイスのリソースが Enterprise Vault サーバーインスタンスのリソースに依存するようにすることは重要です。これにより、2 台の Enterprise Vault クラスタサーバーがサポート外の「アクティブ/アクティブ」の構成で同じクラスタ化されたノードで実行されることを防ぎます。

Enterprise Vault サーバーインスタンスのリソースはディスクストレージに依存しません。このリソースは、クラスタグループ内で構成されるディスクのデータを格納しません。

---

- 管理サービスリソースのプロパティを変更して、新しい各ストレージデバイスに依存関係を追加します。
- 3 クラスタ操作モードに従って、必要なノードを新しいストレージデバイスリソースの所有者候補として指定します。
  - 4 修正したクラスタをテストして、Enterprise Vault クラスタサーバーがフェールオーバーの前後で新しい共有ストレージに正常にアクセスできることを確認します。

## 既存のクラスタ化された Enterprise Vault サーバーへの Enterprise Vault SMTP アーカイブの追加

Enterprise Vault SMTP アーカイブ機能を既存の Enterprise Vault クラスタに追加することがあります。

既存のクラスタ Enterprise Vault サーバーに SMTP アーカイブを追加するには

- 1 Enterprise Vault クラスタのすべてのノードに Enterprise Vault サーバーと SMTP アーカイブコンポーネントをインストールします。
- 2 クラスタ化された Enterprise Vault サーバーで新しい SMTP アーカイブタスクを作成します。Enterprise Vault は SMTP アーカイブタスクを作成する前に、アーカイブノードとその他のノードでの Enterprise Vault SMTP サービスの存在を検出し、SMTP サービスを一般的なサービスリソースとして設定します。
- 3 Enterprise Vault は一部のクラスタノードで SMTP アーカイブコンポーネントを検出しない場合、影響を受けるノードの一覧と、SMTP アーカイブコンポーネントをインストールするための警告を表示します。SMTP アーカイブタスクの作成を続行し、リストされたノードに SMTP アーカイブコンポーネントを後でインストールすることができます。クラスタのすべてのノードにコンポーネントをインストールしないと、Enterprise Vault はコンポーネントがインストールされていないノードにフェールオーバーできません。

# Windows Server フェールオーバークラスタリングによるクラスタ化のトラブルシューティング

この章では以下の項目について説明しています。

- 概要
- Enterprise Vault イベントメッセージとフェールオーバークラスタのログ
- フェールオーバークラスタ環境で Enterprise Vault を設定するときのリソースの所有権と依存関係
- フェールオーバークラスタノードのレジストリレプリケーション
- Enterprise Vault クラスタサーバーのクラスタ化されたメッセージキューの表示
- Windows Server フェールオーバークラスタリング環境での Enterprise Vault サービスの起動と停止
- Windows Server クラスタの潜在的なフェールオーバーの問題

## 概要

この章では、Windows Server フェールオーバークラスタの Enterprise Vault に関する問題のトラブルシューティングについて説明します。

## Enterprise Vault イベントメッセージとフェールオーバークラスターのログ

クラスタ化に固有の Enterprise Vault のイベントメッセージはありませんが、Enterprise Vault は標準のアプリケーションログと Enterprise Vault イベントログへのメッセージの書き込みを継続的に実行します。エラーについてはこれらのログを確認してください。

フェールオーバークラスターリソースがオンラインにならない場合は、イベントログと、クラスターのログが記録されたテキストファイル (通常は C: \&#165;WINDOWS \&#165;Cluster \&#165;cluster.log) を確認してください。

Enterprise Vault 関連の処理を確認するには、「Enterprise Vault」を検索します。

## フェールオーバークラスター環境で Enterprise Vault を設定するときのリソースの所有権と依存関係

Enterprise Vault をクラスターで設定するときに問題が発生しないようにするには、リソースの所有権を正しく設定する必要があります。設定ウィザードを実行しているノードが内部のすべてのリソースで所有者候補として一覧表示されている場合にのみ、そのクラスターサービスが選択肢として一覧表示されます。

フェールオーバー処理が計画どおりに実行されるようにするためにも、リソースの所有権と依存関係を正しく設定する必要があります。

p.295 の [表 39-1](#) を参照してください。

Enterprise Vault 設定ウィザードは、Enterprise Vault サービスリソースとサーバーインスタンスリソースをクラスターサービスに追加するときにこれらのリソースの依存関係を設定します。

共有ディスクを既存のクラスターに追加する場合は、ディスクのリソースと依存関係が正しく設定されていることを確認する必要があります。

p.316 の「[Enterprise Vault クラスターサーバー用として既存の Windows Server オーバークラスターに共有ストレージを追加する](#)」を参照してください。

## フェールオーバークラスターノードのレジストリレプリケーション

クラスターサーバーの設定時に、設定ウィザードによって管理サービスリソースにレジストリチェックポイントが設定されます。これにより、クラスターノードで必要なレジストリレプリケーションが行われるようになります。

Enterprise Vault クラスタサーバーに関連するレジストリエントリに問題があると考えられる場合は、チェックポイントが正しく設定されていることを確認します。Windows コマンドラインユーティリティ `cluster` を使って次のコマンドを入力します。

```
cluster resource EnterpriseVaultAdminService /check
```

`EnterpriseVaultAdminService` は管理サービスリソースの名前 (EVSERVER1-EnterpriseVaultAdminService など) です。

## Enterprise Vault クラスタサーバーのクラスタ化されたメッセージキューの表示

クラスタ化された Enterprise Vault インストールでは、デフォルトにより、Computer Management スナップインに Enterprise Vault メッセージキューが表示されません。その代わりに、スナップインはローカルコンピュータのキューのみを表示します。

### Enterprise Vault クラスタサーバーのクラスタ化されたメッセージキューを表示する方法

- 1 キューを表示するノード上で Enterprise Vault クラスタサーバーがオンラインになっていることを確認します。
- 2 管理者権限でコマンドプロンプトウィンドウを開きます。
- 3 コマンドプロンプトウィンドウで、Enterprise Vault のインストール先フォルダ (C:\Program Files (x86)\Enterprise Vault など) に移動します。
- 4 次のコマンドを入力します。

```
ClusterCompMgmt
```

- 5 Computer Management スナップインで、[サービスとアプリケーション] を展開し、[メッセージキュー] を展開します。Enterprise Vault メッセージキューは、[専用キュー] の下に一覧表示されます。

## Windows Server フェールオーバークラスターリング環境での Enterprise Vault サービスの起動と停止

クラスタ環境では、クラスタソフトウェアを使って Enterprise Vault サービスを制御する必要があります。このため、Enterprise Vault 設定ウィザードによって、これらのサービスは手動で起動するように設定されます。自動的に起動されるように設定を変更しないでください。

クラスタソフトウェアによる制御の範囲外でサービスが起動または停止されると、クラスタソフトウェアはこれをシステム状態の変更によるものと判断します。たとえば、サービスが停



止した場合、クラスタソフトウェアはエラーが発生したと判断して、サービスの再起動またはフェールオーバーの開始を試行します。

**Enterprise Vault** サービスの起動または停止は、クラスタソフトウェアから次のいずれかの方法で行う必要があります。

- フェールオーバークラスタマネージャを使って、関連するサービスリソースをオンラインまたはオフラインにします。
- **Windows** コマンドラインユーティリティ `cluster` を使います。このコマンドの構文を確認するには、コマンドプロンプトウィンドウを開いて次のように入力します。

```
cluster /?
```

詳しくは、**Microsoft** 社の **Web** サイトにて、次の記事を参照してください。

[https://technet.microsoft.com/en-us/library/cc732694\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc732694(v=ws.11).aspx)

これ以外の方法でサービスが起動または停止されないように、クラスタ構成の **Enterprise Vault** は次のように設定されます。

- サービスの起動と停止に使う **Enterprise Vault** 管理コンソールのボタンは利用できません。
- **EVService** ユーティリティを使ってサービスを起動または停止できません。ただし、タスクは **EVService** を使って引き続き制御できます。
- **Windows** のコントロールパネルのサービスアプレットを使った **Enterprise Vault** サービスの起動は **Enterprise Vault** によって遮断され、イベントメッセージがログに記録されます。ただし、**Windows** のコントロールパネルのサービスアプレットを使った **Enterprise Vault** サービスの停止は **Enterprise Vault** によって遮断されないため、このような操作を実行しないように注意する必要があります。

## Windows Server クラスタの潜在的なフェールオーバーの問題

**Windows Server** クラスタでのアクティブなノードの未計画なシャットダウン中に、**Enterprise Vault** サーバーインスタンスのリソースが最初の試行でパッシブノードに正常にフェールオーバーできない可能性があります。ただし、これは最終的にクラスタに対して構成されたタイムアウトと再起動のポリシー設定に従って発生するはずです。**Enterprise Vault** サーバーインスタンスのリソースがオフサインの期間は、**Enterprise Vault** リソースグループ全体もオフラインになります。

この問題を解決するには、**Enterprise Vault** サーバーインスタンスのリソースのプロパティのダイアログボックスを開き、[詳細なポリシー] タブで、[このリソースを別のリソースモニターで実行する]を選択します。

# Enterprise Vault サーバー を自動的に準備する

この付録では以下の項目について説明しています。

- [Enterprise Vault サーバーの自動準備について](#)
- [\[マイシステムの準備\]オプションによる Windows 機能の有効化](#)
- [\[マイシステムの準備\]オプションの実行](#)

## Enterprise Vault サーバーの自動準備について

Enterprise Vault Install Launcher の[\[マイシステムの準備\]](#)オプションは、どの Windows 機能が有効かを自動的に確認し、必要に応じて他の機能を追加します。

## [マイシステムの準備]オプションによる Windows 機能の有効化

Enterprise Vault Install Launcher の[\[マイシステムの準備\]](#)オプションにより、Enterprise Vault サーバーが必要とするすべての Windows 機能がインストールされます。[表 A-1](#) は、これらの機能の一覧です。

表 A-1 [マイシステムの準備]オプションによる Windows 機能の有効化

パス	機能
¥	.NET Framework 4.5 の機能
¥	Windows TIFF IFilter

パス	機能
¥.NET Framework 3.5 の機能	.NET Framework 3.5
	HTTP アクティブ化
	非 HTTP アクティブ化
¥.NET Framework 4.5 Features¥WCF Services	名前付きパイプのアクティブ化
	TCP のアクティブ化
¥Application Server¥Windows Process Activation Service Support¥	名前付きパイプのアクティブ化
	TCP のアクティブ化
¥File Services	File Server Resource Manager
¥Message Queuing¥Message Queuing Services	メッセージキューサーバー
¥Web サーバー (IIS)	Web サーバー
¥Web Server (IIS)¥Web Server¥Common HTTP Features	既定のドキュメント
	ディレクトリの参照
	HTTP エラー
	HTTP リダイレクト
	静的コンテンツ
¥Web Server (IIS)¥Web Server¥Health and Diagnostics	HTTP ログ
	ロギングツール
	要求の監視
	追跡
¥Web Server (IIS)¥Web Server¥Performance	静的なコンテンツの圧縮
¥Web Server (IIS)¥Web Server¥Security	基本認証
	IP およびドメインの制限
	要求のフィルタリング
	URL 承認
	Windows 認証

パス	機能
¥Web Server (IIS)¥Web Server¥Application Development	.NET Extensibility 3.5
	ISAPI 拡張
	ISAPI フィルタ
	ASP
	ASP.NET 3.5
	ASP.NET 4.5
	CGI
¥Web Server (IIS)¥Web Server¥Management Tools	IIS 管理コンソール
	IIS 管理スクリプトおよびツール
	管理サービス

## [マイシステムの準備]オプションの実行

[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。

[Install Launcher]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。