Veritas Storage Foundation™ and High Availability Solutions インストールおよびアップグレードガイド

Windows 2000, Windows Server 2003

5.0

11353462

symantec™

Veritas Storage Foundation and HA Solutions インストールおよびアップグレードガイド

Storage Foundation 5.0 for Windows HA

Symantec Corporation
www.symantec.com
Printed in Singapore

サードパーティ（第三者）製ソフトウェアの権利に関する通知

本製品には、特定のサードパーティ製ソフトウェアが配布、組み込み、または同梱されている場合があります。また、本製品のインストールおよび使用にともない、サードパーティ製ソフトウェアの使用を推奨する場合があります。同サードパーティ製ソフトウェアのライセンスは、著作権の保有者により別途付与されます。サードパーティのソフトウェアの使用に必要なライセンスおよび著作権に関する情報については、本製品リリースノートのサードパーティに関する章を参照してください。

ライセンスと登録

Storage Foundation for Windows および Storage Foundation HA for Windows はライセンスが必要な製品です。ライセンスのインストールについては、『Veritas Storage Foundation and High Availability Solutions インストールおよびアップグレードガイド Windows 2000, Windows Server 2003』を参照してください。

テクニカルサポート

製品のサポートを受けるには、http://entsupport.symantec.com ページへアクセスし「Phone Support」または「E-mail Support」をクリックします。このページから TechNote、Software Alerts、ソフトウェアのダウンロード、ハードウェア互換性リスト、VERITAS Email Notifications サービスなどにアクセスすることもできます。「Knowledge Base Search」機能を使用し、製品ドキュメントのリリースなどの製品情報へアクセスすることができます。

目次

1

インストール

この項では、Veritas Storage Foundation for Windows 5.0 と Veritas Storage Foundation High Availability for Windows 5.0 のインストールに使用する手順について説明します。

1

SFW と SFW HA のプリインストールと計画

この章で扱う内容は次のとおりです。

前提条件

次の前提条件を確認してください。

- 製品のリリースノートを確認します。
- 必要条件を確認します。
  3 ページの「前提条件」を参照してください。
- 実行中のすべてのアプリケーションを終了します。

- VVR の場合は、VVR のサポート機能を備えた SFW を実行するシステムが 2 つ以上必要です。1 つはプライマリとして、他方はセカンダリとして機能し、これらの間はネットワークで接続する必要があります。どちらのシステムも DHCP をサポートしません。VVR レプリケーションの設定に DHCP 対応の IP を使うことはできません。DHCP IP は別のホストに再割り当てされる場合があるので、DHCP IP は失われます。

必要条件

インストールする前に、システムの製品のインストール必要条件を確認します。最小限の必要条件とシマンテック社が推奨する必要条件は異なる場合があります。

必要なディスク領域

ソフトウェアが正しく機能するには、すべての種類のインストールにさらに 50 MB 以上のディスク領域が必要になります。非システムドライブに製品をインストールする場合は、システムドライブと非システムドライブの両方にディスク領域が必要です。

表 1-1 に、SFW と SFW HA に必要なディスク領域を示します。

表 1-1　　必要なディスク領域

インストールの種類	システムドライブへのインストール	非システムドライブへのインストール
SFW + 全オプション + クライアントコンポーネント	1240 MB	非システム領域 : 1240 MB システム領域 : 265 MB
SFW + 全オプション	980 MB	非システム領域 : 980 MB システム領域 : 225 MB
クライアントコンポーネント	420 MB	非システム領域 : 420 MB システム領域 : 80 MB
SFW HA + 全オプション + クライアントコンポーネント	1675 MB	非システム領域 : 1675 MB システム領域 : 345 MB
SFW HA + 全オプション	1230 MB	非システム領域 : 1230 MB システム領域 : 285 MB
クライアントコンポーネント	630 MB	非システム領域 : 630 MB システム領域 : 115 MB
言語パッケージ	325 MB	非システム領域 : 325 MB システム領域 : 90 MB

オペレーティングシステム必要条件

SFW と SFW HA には、特定の Windows オペレーティングシステム専用のクライアントコンポーネントとサーバーコンポーネントがあります。

サーバー用の SFW と SFW HA ソフトウェア

SFW または SFW HA サーバーソフトウェアをインストールするには、サーバーで次のいずれかのオペレーティングシステムを実行している必要があります。

- Windows 2000 Server、Advanced Server または Datacenter Server（すべて Service Pack 4 と Update Rollup1 が必須）
- Windows Server 2003（32 ビット）: Standard Edition、Enterprise Edition、または Datacenter Edition（すべてのエディションで SP 1 が必須）
- Windows Server 2003 R2（32 ビット）: Standard Edition、Enterprise Edition、または Datacenter Edition
- Windows Server 2003（32 ビット）: Web Edition: SFW を完全サポートし、SFW HA のファイル共有のみサポート（SP 1 が必須）
- Windows Server 2003 for 64 ビット Itanium（IA64）: Enterprise Edition、または Datacenter Edition（すべてのエディションで SP 1 が必須）
- Windows Server 2003 x64 Editions（AMD 64 または Intel EM64T）: Standard x64 Edition、Enterprise x64 Edition、または Datacenter x64 Edition
- Windows Server 2003 x64 Editions（AMD 64 または Intel EM64T）: Standard x64 R2 Edition、Enterprise x64 R2 Edition、または Datacenter x64 R2 Edition

クライアント用 SFW と SFW HA ソフトウェア

SFW または SFW HA クライアントソフトウェアをインストールするには、クライアントで次のいずれかのオペレーティングシステムを実行している必要があります。

- Windows 2000 Server、Advanced Server または Datacenter Server（すべて Service Pack 4 と Update Rollup1 が必須）
- Windows Server 2003（32 ビット）: Standard Edition、Enterprise Edition、または Datacenter Edition（すべてのエディションで SP 1 が必須）
- Windows Server 2003 R2（32 ビット）: Standard Edition、Enterprise Edition、または Datacenter Edition
- Windows Server 2003 for 64 ビット Itanium（IA64）: Enterprise Edition、または Datacenter Edition（すべてのエディションで SP 1 が必須）

- Windows Server 2003 for Intel Xeon（EM64T）または AMD Opteron: Standard x64 Edition、Enterprise x64 Edition、または Datacenter x64 Edition
- Windows Server 2003 x64 Editions（AMD64 または Intel EM64T）: Standard x64 R2 Edition、Enterprise x64 R2 Edition、または Datacenter x64 R2 Edition
- Windows XP Professional（SP 2 が必須）
- Windows 2000 Professional（SP 4 が必須）

一般的な必要条件

SFW または SFW HA ソフトウェアをインストールする前に、設定が次の条件を満たしていることを確認し、次のサイトにある SFW 5.0 のハードウェア互換性リストを参照してサポートされるハードウェアを確認してください。

http://entsupport.symantec.com

メモリ

1 GB の RAM が必須

システムプロセッサ

プロセッサの必要条件は次のとおりです。

32 ビット

- 800 メガヘルツ（MHz）Pentium III 互換プロセッサ以上
- 1 GHz 以上のプロセッサを推奨

x64

- 1 GHz AMD Opteron、AMD Athlon 64、Intel EM64T をサポートする Intel Xeon、EM64T をサポートする Intel Pentium IV プロセッサ以上

IA64

- 1 GHz Itanium プロセッサ以上
- 1 GHz デュアルコア Intel Itanium 2 プロセッサ以上

ディスプレイ

ディスプレイの必要条件は次のとおりです。

- 最小限の解像度 : 800 x 600 ピクセル
- 推奨解像度 : 1024 x 768 ピクセル以上
- VCS Cluster Manager（Java コンソールと Web コンソール）には、8 ビット（256 色）のディスプレイと、2D 画像を表示できるグラフィックカードが必要です。

ストレージデバイスの互換性

Veritas DMP（Dynamic Multi-pathing）またはクラスタ化（SFW HA または MSCS）を使用しない場合、SFW は Microsoft Windows Server Catalog のすべての製品をサポートします。

Veritas DMP とクラスタ化を設定する場合は、ハードウェア互換性リスト（http://entsupport.symantec.com）を参照し、SFW で動作が確認されているハードウェアを確認してください。

リモートシステム

各リモートコンピュータに対するネットワークアクセスおよび管理者権限が必要です。VVR オプションを使用する SFW HA と SFW では、DHCP はサポートされていません。サポートされているのは、固定 IP アドレスだけです。

Veritas Volume Replicator の固定 IP アドレス

VVR では、レプリケーションに固定 IP が必要です。DHCP（Dynamic Host Configuration Protocol）で割り当てられていない IP アドレスが、システムに 1 つ以上設定されていることを確認してください。

SFW の単一インスタンス

1 つのシステムで一度に実行できる Veritas Storage Foundation 5.0 for Windows のインスタンスは 1 つのみです。

ドライバ署名オプション

Windows Server 2003 が稼働するシステムにインストールする場合は、ソフトウェア認証に関する警告メッセージを無視するように Windows のドライバ署名オプションを設定する必要があります。

Veritas Cluster Server クラスタ管理コンソール

Veritas クラスタ管理コンソールは、次のブラウザでサポートされます。

- Microsoft Internet Explorer 6.0 SP2 以降
- Firefox 1.5 以降

Veritas Cluster Management には Macromedia Flash Plugin v8.0 が必要です。

ファイアウォールおよびアンチスパイウェア

SFW または SFW HA をインストールする前に、スパイウェアの監視と除去ソフトウェアを無効化します。また、ローカルクライアントを検出できるように、ファイアウォールも無効化します。

Veritas Storage Foundation for Windows（SFW）の必要条件

サポートされるソフトウェアの必要条件

Veritas Storage Foundation 5.0 for Windows（SFW）

システム必要条件

SFW でのシステムの必要条件は次のとおりです。

- SCSI、ファイバーチャネル、iSCSI ホストバスアダプタ（HBA）または iSCSI イニシエータでサポートされる NIC（共有ストレージへのアクセス用）。
- 各システムに 1 GB の RAM

アクセス権の必要条件

インストールするすべてのノードについて、Local Administrators グループのメンバーである必要があります。

追加必要条件

次の必要条件も満たす必要があります。

- 全製品およびサードパーティ製アプリケーションのインストールメディア
- 全製品およびサードパーティ製アプリケーションのライセンス

Veritas Storage Foundation High Availability for Windows（SFW HA）の必要条件

SFW HA をインストールする前に、設定が次の条件を満たしていることを確認し、http://entsupport.symantec.com にある SFW 5.0 のハードウェア互換性リストを参照してサポートされるハードウェアを確認してください。

ディザスタリカバリ設定の場合、グローバルクラスタオプションを選択し、オプションで Veritas Volume Replicator を選択します。

サポートされるソフトウェア

この項では、サポートされているソフトウェアを示します。

Veritas Storage Foundation HA 5.0 for Windows（SFW HA）

システム必要条件

システムは次の必要条件を満たしている必要があります。

- クラスタ内のノード間で移行するアプリケーションをサポートするための共有ディスク。キャンパスクラスタには、ミラーリング用に複数のアレイが必要です。ディザスタリカバリ設定には、各サイトに 1 つのアレイが必要です。
- SCSI、ファイバーチャネル、iSCSI ホストバスアダプタ（HBA）または iSCSI イニシエータでサポートされる NIC（共有ストレージへのアクセス用）。
- 2 枚の NIC: パブリックとプライベート共有用に 1 枚と、プライベートネットワーク専用に 1 枚。シマンテック社は、3 枚の NIC の使用をお勧めします。
  11 ページの「最善策」を参照してください。
- 各システムに 1 GB の RAM。
- すべてのサーバーで同じオペレーティングシステム、サービスパックレベル、システムアーキテクチャを実行する必要があります。

ネットワーク必要条件

この項では、次のネットワーク必要条件を示します。

- SFW HA を、Windows 2000 または Windows Server 2003 ドメインのサーバーにインストールします。
- Windows Server 2003 SP1 を実行しているシステムの Windows ファイアウォールを無効化します。

- 目的別に固定 IP アドレスが必要です。
  - 各アプリケーションの仮想サーバーのサイトで利用可能な 1 つの固定 IP アドレス
  - クラスタ内の各物理ノードに対して 1 つの IP アドレス
  - 通知、クラスタ管理コンソール（Web コンソール）、またはグローバルクラスタオプション（VVR のみ）などのオプションを設定する場合は、クラスタごとに 1 つの固定 IP アドレスを使用します。すべてのオプションに同じ IP アドレスを使用できます。
  - VVR のみの場合、クラスタ内で実行される各アプリケーションインスタンスのサイトごとに、1 つ以上の固定 IP アドレスが必要です。
- 各ノードに対して名前解決を設定します。
- DNS サービスが使用可能であることを確認します。AD 統合 DNS または BIND 8.2 以上がサポートされます。
  逆引き参照ゾーンが DNS に存在していることを確認します。逆引き参照ゾーンの作成方法については、アプリケーションのマニュアルを参照してください。
- Lanman エージェントでは DDNS を使用して仮想名を IP アドレスにマップするため、DNS 清掃は VCS に設定されている仮想サーバーに影響を与えます。清掃を使用している場合は、Lanman エージェントの DNSRefreshInterval 属性を設定する必要があります。これにより、Lanman エージェントが、DNS サーバー上のリソースコードを更新できるようになります。
  『Veritas 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。

権限の必要条件

この項では、権限の必要条件を示します。

- ドメインユーザーである必要があります。
- インストールするすべてのノードについて、Local Administrators グループのメンバーである必要があります。
- すべてのノードに対応する Active Directory オブジェクトに対する書き込みアクセス許可が必要です。
- VCS Helper サービス用の新しいユーザーアカウントを作成する場合は、Domain Administrator 権限を持つか、Account Operators グループに属する必要があります。VCS Helper サービス用に既存のユーザーアカウントコンテキストを使用する場合は、そのユーザーアカウントのパスワードを知っている必要があります。

追加必要条件

次の追加必要条件を確認してください。

- 全製品およびサードパーティ製アプリケーションのインストールメディア
- 全製品およびサードパーティ製アプリケーションのライセンス
- すべてのシステムの同じパスに、オペレーティングシステムをインストールする必要があります。たとえば、あるノードで Windows 2003 を C:¥WINDOWS にインストールする場合、その他すべてのノードでも C:¥WINDOWS にインストールする必要があります。すべてのノードで同じドライブ文字が使用可能で、インストールに十分な領域がシステムドライブにあることを確認します。

最善策

次のタスクを実行することをお勧めします。

- Microsoft Exchange Server と Microsoft SQL Server を、同じクラスタ内で別々のフェールオーバーノードに設定します。
- ネットワークアダプタが 3 枚（プライベートネットワーク専用に 2 枚の NIC と、パブリックネットワーク用に 1 枚の NIC）装備されいることを確認します。
  2 枚の NIC のみを使う場合、1 つの NIC の優先度を低くし、その優先度の低い NIC をパブリックとプライベート通信に使用します。
- 単一点障害を防ぐため、それぞれのハブまたはスイッチを介して各プライベート NIC をルーティングします。
- DNS サーバーの［動的更新］オプションが［セキュリティ保護のみ］に設定されていることを確認してください。

ライセンス

SFW と SFW HA のライセンスは、特定のサーバーで使われている Microsoft Windows 2000 Server または Windows Server 2003 オペレーティングシステムに基づいています。Symantec 製品を実行しているシステムごとにライセンスが必要です。

メモ：リリース 4.3 以前の SFW と SFW HA のライセンスキーは、リリース 5.0 の SFW と SFW HA ではサポートされません。

評価ライセンスキー

評価ライセンスキーは製品に組み込まれています。このキーを使用するには、インストーラのライセンスキー入力画面で［次へ］をクリックします。このライセンスキーは限定された評価期間のみ有効です。

Storage Foundation for Windows Basic（SFW Basic）

Storage Foundation Basic for Windows（SFW Basic）は、特にエッジ層の作業負荷のために設計されたフリーテクノロジです。これは、費用のかからない SFW ライセンスで、DMP オプションが含まれます。各物理サーバーには SFW Basic ライセンスが必須で、特定の限定事項が適用されます。

17 ページの「SFW Basic」を参照してください。

仮想サーバーのライセンスポリシー

すべてのオプションとエージェントを含む Veritas Storage Foundation and High Availability Solutions の各製品には、物理サーバーでの使用または仮想コンピュータ内での使用に関係なく、個別のライセンスが必要です。ライセンスを保持するソフトウェアの各ライセンスには、特定のサーバーで同時に実行可能なインスタンス数が指定されています。

表 1-2 に、Storage Foundation for Windows（SFW）の各エディションと、適用される追加のライセンス条項を示します。

表 1-2　　SFW ライセンス条項

Microsoft オペレーティングシステムエディション	SFW ライセンス条項
■ Server Edition ■ Standard Edition ■ Web Edition	ライセンスを保持するソフトウェアをインストールする各仮想サーバーまたは物理サーバーごとに、そのソフトウェアの個別のライセンスが必要です。
■ Advanced Edition ■ Enterprise Edition	各ライセンスに対して、1 つの物理サーバー上でライセンスを保持するソフトウェアのインスタンスを 1 つ実行できます。また、物理サーバー上に存在する仮想サーバーでは、ライセンスを保持するソフトウェアのインスタンスを最大 4 つまで同時に実行できます。
Datacenter Edition	各ライセンスに対して、1 つの物理サーバー上または物理サーバーに存在する無制限の仮想サーバー上で、ライセンスを保持するソフトウェアのインスタンスを 1 つ実行できます。

クライアントライセンス

SFW と SFW HA のクライアントコンポーネントをインストールする場合、ライセンスは不要です。

ライセンスの管理

インストーラを使用すると、特定のライセンスを追加および削除することができます。オプションのライセンスを追加してもオプションがインストールされるわけではありません。オプションをインストールするには追加 / 削除機能を使用します。複数システムのライセンスキーサポートインストール

メモ : リリース 4.3 以前の SFW と SFW HA のライセンスキーは、リリース 5.0 の SFW と SFW HA ではサポートされません。提供されるデフォルトの評価ライセンスキーを使えます。このライセンスキーは限定された評価期間のみ有効です。永久ライセンスキーを取得するには製品を購入する必要があります。

Symantec License Inventory Manager

Symantec License Inventory Manager は、ネットワークで使用されているすべての Symantec ソフトウェア製品とライセンスを明確に識別可能な企業の資産管理追跡ツールです。Symantec License Inventory Manager は個別に利用できます。Symantec License Inventory Manager ライセンスとメディアキットを注文するには、シマンテック社の販売担当者にお問い合わせください。

123 ページの「Symantec License Inventory Agent の設定」を参照してください。

Vxlicrep

Vxlicrep は、システムで使用中のライセンスに関するレポートを生成するコマンドラインツールです。

Vxlicrep を使用してライセンスレポートを表示するには

コマンドプロンプトを開きます。

オプションを指定せずに vxlicrep を入力すると、デフォルトのレポートが生成されます。

次のオプションの 1 つを使用して、必要な種類のレポートを作成することもできます。

-g　デフォルトレポート

-s　短縮レポート

-e　拡張 / 詳細レポート

-h　このコマンドのヘルプの表示

vxlicrep に -e オプションを指定して出力した詳細レポートを次に示します。

```
VERITAS License Manager vxlicrep utility version 3.00.007
Copyright (C) VERITAS Software Corp 2002. All Rights reserved.

Creating a report on all VERITAS products installed on this system

------------------**********----------

  License Key                = NGCE-PBXW-I3IR-8UXL-S9GO-ERU7-H6P
  Product Name               = Storage Foundation for Windows
  License Type               = DEMO
  OEM ID                     = 4095
  Demo End Date              = 2007年3月18日 0:00:00
                             (57.4 days from now).
  Editions Product           = YES

Features :=
  OS Level                   = Windows
  License OS Platform        = Windows Datacenter
  Version                    = 5.0
  Edition Type               = Windows

  Storage Foundation         = Storage Foundation Standard
  VxCache Option             = Enabled
  DMP Option                 = Enabled
  FlashSnap Option           = Enabled
  VVR Option                 = Enabled
  VCS Option                 = Enabled
  Mode#VERITAS Cluster Server = VCS
  VCS App Agents#VERITAS Cluster Server = Enabled
  VCS HWREP Agents#VERITAS Cluster Server = Enabled
  Global Cluster Option#VERITAS Cluster Server = Enabled


------------------**********----------

  License Key                = P4E7-ZOCX-GBI8-W4O4-ORVE-PPU9-P
  Product Name               = VERITAS Cluster Server
  License Type               = DEMO
  OEM ID                     = 4095
  Demo End Date              = 2007年3月18日 0:00:00
                             (57.4 days from now).
  Point Product              = YES

Features :=
  Platform                   = Unused
  Version                    = Unused
  Tier                       = Unused
  Reserved                   = 0

  Mode                       = VCS
  Global Cluster Option      = Enabled
```

SFW と SFW HA のライセンスパッケージ

次のライセンスパッケージは、SFW または SFW HA で使用可能です。一覧表示されているオプションの一部は、ライセンスを個別に購入する必要があります。表 1-3 に、SFW と SFW HA で利用可能なエージェントとオプションを一覧表示します。

表 1-3 SFW と SFW HA のオプションとエージェントパッケージ

製品ライセンス	含まれるオプションとエージェント	個別に利用可能なオプションとエージェント
SFW 5.0		オプション： ■ FlashSnap オプション ■ DMP（Dynamic Multi-Pathing）オプション ■ MSCS のクラスタオプション ■ Volume Replicator オプション
SFW Enterprise 5.0	■ FlashSnap オプション ■ DMP（Dynamic Multi-Pathing）オプション ■ MSCS のクラスタオプション	■ Volume Replicator オプション
SFW HA 5.0	■ Application Agent: Veritas Cluster Server Application Agent for Microsoft Exchange Database Agents: ■ Veritas Cluster Server Database Agent for Microsoft SQL ■ Veritas Cluster Server Database Agent for Oracle	■ FlashSnap オプション ■ DMP（Dynamic Multi-Pathing）オプション ■ Volume Replicator オプション
SFW Enterprise HA 5.0	オプション： ■ FlashSnap オプション ■ DMP（Dynamic Multi-Pathing）オプション エージェント（エージェントのフルネームについては SFW HA 5.0 を参照）： ■ Application Agent ■ Database Agents	■ Volume Replicator オプション

表 1-3 SFW と SFW HA のオプションとエージェントパッケージ (続き)

製品ライセンス	含まれるオプションとエージェント	個別に利用可能なオプションとエージェント
SFW HA/DR 5.0	オプション : ■ グローバルクラスタオプション エージェント（エージェントのフルネームについては SFW HA 5.0 を参照）: ■ Application Agent ■ Database Agents Hardware Replication Agents: ■ Veritas Cluster Server Hardware Replication Agent for EMC Symmetrix Remote Data Facility（SRDF）。 ■ Veritas Cluster Server Hardware Replication Agent for Hitachi TrueCopy。 ■ Veritas Cluster Server Hardware Replication Agent for IBM Peer-to-Peer Remote Copy（PPRC）。 ■ Veritas Cluster Server Hardware Replication Agent for EMC Mirrorview。 ■ Veritas Cluster Server Hardware Replication Agent for IBM Metro Mirror	■ FlashSnap オプション ■ DMP（Dynamic Multi-Pathing）オプション ■ Volume Replicator オプション
SFW Enterprise HA/DR 5.0	オプション : ■ グローバルクラスタオプション ■ FlashSnap オプション ■ DMP（Dynamic Multi-Pathing）オプション エージェント（エージェントのフルネームについては SFW HA 5.0 を参照）: ■ Application Agent ■ Database Agents ■ Hardware Replication Agent（エージェントのリストについては SFW HA/DR 5.0 を参照）	■ Volume Replicator オプション

SFW Basic

このリリースは SFW Basic としても使用可能です。SFW Basic の機能は SFW と同じで、Veritas DMP（Dynamic Multi-pathing）オプションが含まれます。ただし、SFW Basic には次の制限があります。

- 同じ物理サーバー上に存在する必要がある 4 つのダイナミックボリュームまたは 4 つのファイルシステム。1 台の物理サーバー上に存在するすべての仮想サーバーのボリュームの合計とファイルシステムの合計は、それぞれ 4 つ以内でなければなりません。
- 2 つの物理プロセッサ
  - 物理 CPU 1 つを 1 つのプロセッサとして数えます。
  - 「n」個のコアを持つ 1 つのプロセッサは、1 つのプロセッサとして数えます。

SFW Basic は、SFW 5.0 または SFW HA 5.0 にアップグレードできます。

SFW Basic は特定のライセンスキーを使って利用できます。

設定チェッカーの使用

設定チェッカーウィザードは、SFW HA をインストールする前や、Microsoft Exchange または SQL Server 環境でディザスタリカバリを実行する前に、設定を確認できるツールです。このウィザードには次のいずれかの方法でアクセスできます。

- Symantec 製品インストーラ CD-ROM
- Solutions Configuration Center
- コマンドラインから、次のコマンドを実行する。`C:¥Program Files¥Common Files¥Veritas Shared¥VPI¥{5.0.0.xx}¥setup install_mode=9 solution=1`

設定チェッカーウィザードを実行する目的は次のとおりです。

- Veritas Storage Foundations and High Availability Solutions ソフトウェア（SFW または SFW HA）をインストールする前に設定を確認して、既存の設定が関連するすべてのソフトウェアとハードウェアの必要条件を満たすようにする。
- 高可用性（HA）環境の場合、SFW HA ソフトウェアをインストールした後、ディザスタリカバリを設定する前に、設定を確認する。

ウィザードのチェックが完了すると、概略レポートが HTML ファイルとして次の場所に自動的に保存されます。

<ConfigChecker インストールディレクトリ *>*
¥Reports¥*<TimeStamp>*¥report.htm

レポートには、選択されたシステムで実行されたチェックの合計数のうち、成功した数と失敗した数が表示され、システムで実行されたすべてのチェックをまとめたレポートが出力されます。インストール前チェックを実行する場合は複数のシステムを選択できますが、ディザスタリカバリを設定する場合は 1 つのシステムしか選択できないことに注意してください。

インストール前チェック

SFW HA をインストールする前にを実行すると、次のチェックが実行されます。

- SFW または SFW HA が存在するかどうか
- ソフトウェアとハードウェアの互換性
- オペレーティングシステムのバージョン、サービスパック、Hotfix
- 利用可能なディスク領域
- 合計物理メモリ
- Symantec 製品の使用するネットワークポートが利用可能かどうか
- Active Directory
- ネットワーク設定

設定チェッカーウィザードの実行

1. 次のいずれかの方法で設定チェッカーウィザードを起動します。
   - インストールメディアから、［Tools］、［vpi］の順に選択し、［LaunchConfigChecker.bat］をダブルクリックします。
   - デスクトップの［Solutions Configuration Center］アイコン をダブルクリックし、画面の右側にあるメニューで［設定チェッカー］をクリックします。
   - コマンドラインプロンプトで、次のコマンドを入力します。
     C:¥Program Files¥Common Files¥Veritas Shared¥VPI¥*{5.0.0.xx}*¥setup install_mode=9 solution=1
2. ［ようこそ］画面上の情報を読み、［次へ］をクリックします。
3. ［Computer Selection］画面で、チェックするすべてのノードを選択します。ノードを選択すると、そのノードの説明が画面の右側に表示されます。説明には、コンピュータ名、オペレーティングシステム、インストール済みのシマンテック社製品の一覧が含まれます。

4 一覧にノードが表示されない場合は、そのノードを含んでいるはずのドメインを右クリックします。[コンピュータの追加]ダイアログボックスが表示されます。ドメインとコンピュータ名を入力して、[OK]をクリックします。

5 これで、ノードが該当するドメインの下に表示されます。リストから 1 つ以上のノードを選択し、[次へ]をクリックすると、[アカウント情報]ダイアログボックスが開きます。選択したコンピュータのユーザー名とパスワードを入力し、[OK]をクリックします。
セキュアクラスタのノードを選択する場合は、Windows のドメインアカウント情報を使ってログインします。ユーザー名の前に必ず「<ドメイン名>¥」を入力します。

6 [オプションの選択]画面で、[SFW プレインストールチェック]または[SFW HA Install Check]のいずれかを選択します。デフォルトでは、SFW または SFW HA プレインストールチェックの下のすべてのオプションが選択されます。チェックを実行したくないオプションについては、そのオプションをクリックしてチェックマークをオフにします。オプションの選択が終了したら、[次へ]をクリックします。

7 [検証]画面が表示され、設定チェッカーによるチェックが開始されます。チェックが完了したら、[次へ]をクリックします。

8 [概略]画面に完了したチェックが一覧表示されます。緑色のチェックマークは、チェックは正常に終了したことを意味します。赤い X 印は、チェックが失敗したことを意味します。
たとえば、オプション[利用可能なディスク領域のチェック]が失敗した場合、そのオプションをクリックして選択すると、[説明]ペインに失敗の理由が示されます。

9 [保存]をクリックして概略を HTML ファイルとして保存するか、[印刷]をクリックして概略を印刷します。

10 [完了]をクリックして、ウィザードを閉じます。一部またはすべてのオプションのチェックが失敗した場合は、設定を修正（メモリやディスク領域の増加、ドライバの更新など）してウィザードを再度実行できます。

インストール後のチェック

SFW または SFW HA をインストールした後に設定チェッカーウィザードを実行すると、次のチェックを実行できます。

- 汎用チェック
  システムチェックを実行し、互換性のあるソフトウェアとハードウェアかどうか、合計物理メモリ、利用可能なメモリ、OS のバージョン、ドライバ署名ポリシーの設定、Active Directory の有無、DNS が利用可能かどうか、ドメインコントローラが利用可能かどうか、グローバルカテゴリが利用可能かどうか、VM ボリュームの状態、ポートが利用可能かどうかを確認します。
- SFW HA チェック
  使用中のドライブ文字、利用可能な NIC カード、Active Directory の有無、クラスタ間での Windows サービスの一貫性、クラスタ間でのシステム環境変数の一貫性、ライセンスファイルの一貫性、クラスタ間での VCS サービスグループの一貫性、クラスタ間での VCS リソースタイプの一貫性を確認します。
- Exchange のディザスタリカバリチェック
  SFW HA を Microsoft Exchange 環境で設定している場合、設定チェッカーは、互換性のあるバージョンの Exchange とサービスパックの確認、クラスタ間での Exchange サービスグループの一貫性の確認を行います。
- SQL Server のディザスタリカバリチェック
  SFW HA を Microsoft SQL Server 環境で設定している場合、設定チェッカーは、互換性のあるバージョンの SQL Server とサービスパックの確認、クラスタ間での SQL Server サービスグループの一貫性の確認を行います。

設定チェッカーウィザードの実行

1. 次のいずれかの方法で設定チェッカーウィザードを起動します。
   - インストールメディアから、[Tools]、[vpi] の順に選択し、[LaunchConfigChecker.bat] をダブルクリックします。
   - デスクトップの［Solutions Configuration Center］アイコン をダブルクリックし、画面の右側にあるメニューで［設定チェッカー］をクリックします。
   - コマンドラインプロンプトで、次のコマンドを入力します。
     ```
     C:¥Program Files¥Common Files¥Veritas Shared¥
     VPI¥{5.0.0.xx}¥setup install_mode=9 solution=1
     ```
2. ［ようこそ］画面上の情報を読み、［次へ］をクリックします。
3. ［Computer Selection］画面で、チェックするノードを選択します。ノードを選択すると、そのノードの説明が画面の右側に表示されます。説明には、コンピュータ名、オペレーティングシステム、インストール済みのシマンテック社製品の一覧が含まれます。

4 一覧にノードが表示されない場合は、そのノードを含んでいるはずのドメインを右クリックします。[コンピュータの追加] ダイアログボックスが表示されます。ドメインとコンピュータ名を入力して、[OK] をクリックします。

5 これで、ノードが該当するドメインの下に表示されます。リストからノードを選択し、[次へ] をクリックすると、[アカウント情報] ダイアログボックスが開きます。選択したコンピュータのユーザー名とパスワードを入力し、[OK] をクリックします。
セキュアクラスタのノードを選択する場合は、Windows のドメインアカウント情報を使ってログインします。ユーザー名の前に必ず「<ドメイン名>¥」を入力します。

6 [オプションの選択] 画面で、実行するチェックを 1 つ以上選択します。デフォルトでは、最適なチェックに対するすべてのオプションが選択されます。実行したくないオプションについては、そのオプションをクリックしてチェックマークをオフにします。オプションの選択が終了したら、[次へ] をクリックします。

7 [検証] 画面が表示され、設定チェッカーによるチェックが開始されます。チェックが完了したら、[次へ] をクリックします。

8 [概略] 画面に完了したチェックが一覧表示されます。緑色のチェックマークは、チェックは正常に終了したことを意味します。赤い X 印は、チェックが失敗したことを意味します。
たとえば、オプション [利用可能なメモリのチェック] が失敗した場合、そのオプションをクリックして選択すると、[説明] ペインに失敗の理由が示されます。

9 [保存] をクリックして概略を HTML ファイルとして保存するか、[印刷] をクリックして概略を印刷します。

10 [完了] をクリックして、ウィザードを閉じます。一部またはすべてのオプションのチェックが失敗した場合は、設定を修正（メモリやディスク領域の増加、ドライバの更新など）してウィザードを再度実行できます。

SFW HA のインストール計画

SFW HA のインストール中に、インストーラは Veritas Storage Foundation for Windows と Veritas Cluster Server を自動的にインストールします。その他の該当するオプションは、インストール時に選択できます。また、インストール処理中に、2 つ以上のシステムで同時にインストールすることも選択できます。初期インストールが終了した後で、VCS 設定ウィザードを実行して VCS クラスタの設定を行います。VCS 設定ウィザードでは、セキュリティオプション、クラスタ管理コンソール、通知、グローバルクラスタ広域接続リソースなど、オプションの VCS 機能を設定できます。

環境によっては、Symantec Product Authentication Service やクラスタ管理コンソールをクラスタ外部のシステムに設定することもできます。

次の情報を参照して、環境の設定方法を決定してください。

- Symantec Product Authentication Service について
- Veritas クラスタ管理コンソールについて
- 通知について
- グローバルクラスタについて

Symantec Product Authentication Service について

Symantec Product Authentication Service を使用すると、セキュリティ管理者は認証を設定し、シマンテック社のアプリケーションでシングルサインオンサービスを利用できるようになります。この場合、ユーザーは 1 つのシマンテック社のアプリケーションに 1 回ログオンすれば、他のアプリケーションは 1 回目のログオンで取得した信用情報を使用できます。

Symantec Product Authentication Service は、クラスタをセキュアモードに設定する機能を提供します。Symantec Product Authentication Service は、認証と SSL にデジタル証明書を使用し、パブリックネットワーク上での通信を暗号化することで、クラスタノードとクライアント（Java コンソールなどを含む）間の通信の安全を確保します。

クラスタをセキュアモードに設定するため、SFW HA では、ユーザーの環境内のシステムをルートブローカーとして指定し、クラスタ内のすべてのノードを認証ブローカーとして指定して設定を行う必要があります。

- ルートブローカー
  ルートブローカーは、メインの登録局および認証局として機能します。ルートブローカーは自己署名の証明書を持ち、他のブローカーを認証することができます。

- 認証ブローカー
  認証ブローカーは中間的な登録および認証局として機能します。認証ブローカーは、ルートによって署名された証明書を持っています。クラスタの各ノードは、認証ブローカーとして機能します。

『Symantec Product Authentication Service Quick Start Guide』には、ユーザーの環境でルートブローカーを設定するためのベストプラクティスとオプションが説明されています。

Veritas クラスタ管理コンソールについて

Veritas クラスタ管理コンソールは、1 つの Web コンソールからクラスタの監視と管理を行える高可用性管理ソリューションです。

クラスタ管理コンソールを設定して、単一クラスタまたは複数クラスタ、またはその両方を管理できます。

- クラスタ管理コンソールを使用して複数クラスタを管理する場合は、スタンドアロンの管理サーバーを設定する必要があります。
- クラスタ管理コンソールを使って単一クラスタを管理する場合は、VCS 設定ウィザードで、クラスタ管理コンソール（別名 Web コンソール）を設定するオプションを選択します。クラスタ管理コンソールの設定は、初期クラスタの設定時にも、後からでも実行できます。

操作モード	設定の説明
ローカルでの 1 つのクラスタの管理（単一クラスタモード）	クラスタ管理コンソールは、クラスタ内の各ノードにインストールされます。またクラスタ管理コンソールを、VCS 設定ウィザードを使用して ClusterService サービスグループの一部として設定し、Web コンソールを設定できます。クラスタ管理コンソールは、堅ろうなクラスタ管理機能を提供し、サポートされる Web ブラウザであればどのシステムからでも実行できます。

操作モード	設定の説明
集中型で総合的なエンタープライズ規模による複数クラスタの管理（マルチクラスタモード）	クラスタ管理コンソールの 1 つのインスタンスを、スタンドアロンサーバーのすべてのクラスタの外部にインストールします。コンソールを使用すると、コマンドを視覚的に、また直感的にマルチクラスタ管理エンジン（管理サーバー）に入力できます。管理サーバーは、そのコマンドを基に監視や管理処理を開始します。管理サーバーはデータベースを使用して、クラスタ設定、クラスタの状態、イベント、イベントポリシー、レポートジョブ、レポート出力などを格納します。 管理サーバーとクラスタノードがファイアウォールで区切られている場合、クラスタコネクタと呼ばれるコンポーネントを各クラスタノードにインストールします。クラスタコネクタを使うと、ファイアウォールを経由してクラスタと通信できます。またクラスタコネクタは、クラスタデータのバッファを提供します。コンソールがオフラインになった後でオンラインに戻った時に、オフラインの期間に収集されたデータをクラスタコネクタバッファから取得できます。 『Veritas Cluster Management Console 実装ガイド』を参照してください。

操作モードの設定が異なる場合、モード間で 1 つのクラスタ管理コンソールインストールを切り替えることはできません。また、同じシステム上でもモードの互換性はありません。そのため、1 つのシステムで両方の操作モードを実行することはできません。ただし、複数のモードは同じマルチクラスタ環境内で共存させることができます。たとえば、VCS クラスタノードで単一クラスタモードのインストール、管理サーバーホストでマルチクラスタモードのインストールを共存させることができます。企業内の複数の IT 管理者が異なる範囲を担当する場合、このような配備が最適です。

通知について

イベント通知を、SMTP 電子メール通知または SNMP トラップを使用して送信するように、SFW HA を設定できます。

通知処理は、VCS 設定ウィザードを使用して初期クラスタの設定時、または後で設定できます。

『Veritas Cluster Server 管理者ガイド』を参照してください。

グローバルクラスタについて

グローバルクラスタは、互いにリンクする 2 つ以上のローカルクラスタで構成されます。グローバルクラスタを使用すると、災害が発生したときに地理的に分散しているクラスタ間でアプリケーションをフェールオーバーできます。

グローバルクラスタは、Solutions Configuration Center にあるディザスタリカバリ設定ウィザード、またはグローバルグループ設定ウィザードを使用して設定できます。2 つの処理ともに、クラスタ間通信用の Wide Area Connector リソースが必要です。このリソースは、ディザスタリカバリ設定ウィザードの途中に自動で設定することも、VCS 設定ウィザードを使用してオプションで設定することもできます。

ディザスタリカバリ設定ウィザードについては、ソリューションガイドに掲載されています。グローバルグループ設定ウィザードと VCS 設定ウィザードについては、『Veritas Cluster Server 管理者ガイド』で説明されています。

『Veritas Storage Foundation and High Availability Solutions HA and Disaster Recovery ソリューションガイド Microsoft Exchange』、『Veritas Storage Foundation and High Availability Solutions HA and Disaster Recovery ソリューションガイド Microsoft SQL』、または『Veritas Storage Foundation and High Availability Solutions ソリューションガイド』を参照してください。

または

『Veritas Cluster Server 管理者ガイド』を参照してください。

MSCS を使用する SFW のインストール計画

SFW で MSCS クラスタをセットアップする場合の推奨事項は次のとおりです。

- MSCS がすでに設定されている必要があります。これにより、SFW では、Volume Manager ディスクグループなどの MSCS リソースと、その他の様々な共有リソースのインストールが可能になります。
- SFW をインストールするときには MSCS クラスタがアクティブ状態で稼働している必要があるため、MSCS クラスタ内のシステムへのインストールには、プッシュインストールは行わないことをお勧めします。
- SFW のインストールには再ブートが必要であり、再起動を行うとクラスタのアクティブなノードがフェールオーバーするため、ローリングインストールを使います。
- 最初にクラスタの非アクティブノードに SFW をインストールした後、MSCS の［グループの移動］コマンドを使ってアクティブなノードを移動します。次に、クラスタの残りのノードに SFW をインストールします。『Veritas Storage Foundation 管理者ガイド』を参照してください。

VVR のインストール計画

次の環境で、Windows 2000 と Windows Server 2003（32 ビット）が稼働するサーバー間でのレプリケーションがサポートされます。

- スタンドアロンサーバー（クラスタなし）で、VVR オプションを使う Storage Foundation for Windows
- VVR オプションとグローバルクラスタオプション（GCO）を使う Storage Foundation for Windows HA
- VVR オプションと MSCS オプションを使う Storage Foundation for Windows

RDC（Replicated Data Cluster）設定では、Windows 2000 と Windows Server 2003（32 ビット）が稼働するサーバー間でのレプリケーションはサポートされません。

2

SFW または SFW HA のインストール

この章で扱う内容は次のとおりです。

SFW または SFW HA のインストールについて

この章では、Veritas Storage Foundation 5.0 for Windows（SFW）または Veritas Storage Foundation High Availability 5.0 for Windows（SFW HA）のインストールについて説明します。また、ライセンス、機能の追加、アンインストールについても説明します。

インストーラを使用したインストール

インストーラを使用して、Veritas Storage Foundation for Windows または Veritas Storage Foundation HA for Windows のソフトウェアをインストールします。SFW HA のインストールには、Veritas Storage Foundation for Windows と Veritas Cluster Server が含まれます。その他の該当するオプションは、インストール時に選択できます。この項の手順は、サーバーのインストールに基づいています。

Windows のドライバ署名オプションの設定

選択するインストールのオプションによっては、一部の Symantec ドライバが署名されない場合があります。Windows Server 2003 が稼働するシステムにインストールする場合は、Windows のドライバ署名オプションを設定し、インストールできるようにする必要があります。

表 2-1 に、無署名ドライバのオプションをインストールする場合の、ローカルまたはリモートシステムでのインストーラの動作を示します。

表 2-1　　無署名ドライバを使用したときのインストール動作

ドライバ署名設定	ローカルシステムでのインストール動作	リモートシステムでのインストール動作
無視	常時許可	常時許可
警告	警告メッセージ。ユーザーの手動操作が必要です。	インストールは続行されます。インストールを完了させるには、リモートシステムにローカルにログオンしてダイアログボックスに応答する必要があります。
ブロック	禁止	禁止

ローカルシステムでは、ドライバ署名オプションを［無視］または［警告］のいずれかに設定します。リモートシステムでは、ユーザーの手動操作なしにインストールを進められるようオプションを［無視］に設定します。

各システムでドライバ署名オプションを変更するには

1. システムにローカルにログオンします。
2. ［コントロールパネル］を開き、［システム］をクリックします。
3. ［ハードウェア］タブをクリックし、［ドライバの署名］をクリックします。
4. ［ドライバ署名オプション］ダイアログボックスで現在の設定を確認し、［無視］または表からインストールを続行できる別のオプションを選択します。

5 ［OK］をクリックします。

6 コンピュータごとに同じ手順を繰り返します。
ドライバ署名オプションを変更しないと、検証中にそのコンピュータでインストールが失敗します。インストールを完了したら、ドライバ署名オプションをもとの状態に戻します。

Storage Foundation HA for Windows のインストール

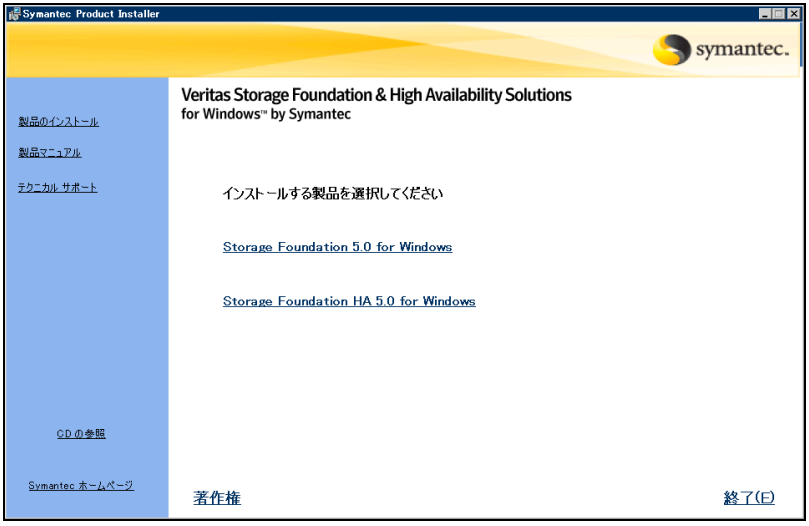
Veritas Storage Foundation HA for Windows をインストールします。

製品をインストールするには

1 自動実行機能でインストールを開始するか、Setup.exe をダブルクリックします。

2 インストール用の言語を選択し、［OK］をクリックします。SFW 製品の選択画面が表示されます。

3 ［Storage Foundation HA 5.0 for Windows.］をクリックします。



このページには、次のリンクも示されます。

製品のインストール　このリンクをクリックすると、この［製品のインストール］画面に戻ります。

関連マニュアル　このリンクをクリックすると、スタートガイドおよびリリースノートのリンクを表示できます。

テクニカルサポート	このリンクをクリックすると、シマンテック社テクニカルサポートに関する情報が表示されます。
CD の参照	このリンクをクリックすると、CD の内容を参照できます。
Symantec ホーム	このリンクをクリックすると、次のサイトに移動します。 http://www.symantec.com

4 次のいずれかの操作をします。
- ［標準 / カスタム］をクリックして、インストールを開始します。
- クライアントコンポーネントのみをインストールするには、［管理コンソール］リンクをクリックします。

5 ［ようこそ］ダイアログボックスの説明に目を通してから、［次へ］をクリックします。

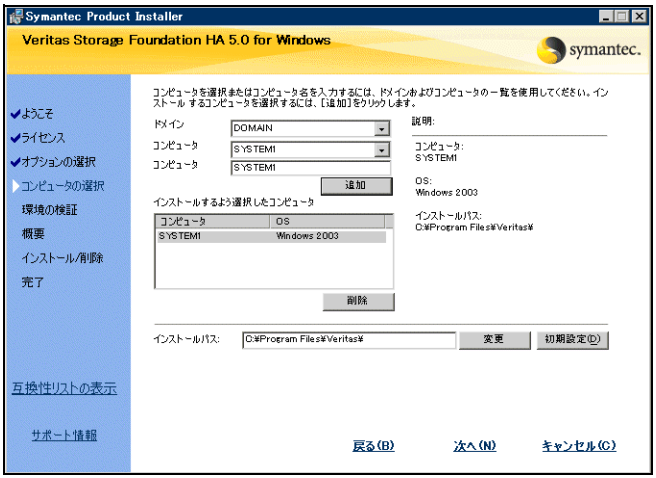
6 表示ウィンドウのスクロール矢印を使用して使用許諾契約を読みます。契約条項に同意する場合は、［使用許諾契約書に同意します。］ラジオボタンを選択して、［次へ］をクリックします。

7 機能のライセンスキーを追加する前に、製品のライセンスキーを入力します。一番上のフィールドにライセンスキーを入力し、［追加］をクリックします。
ライセンスキーを持っていない場合は、［次へ］をクリックしてデフォルトの評価ライセンスキーを使用します。このライセンスキーは限定された評価期間のみ有効です。

8 追加するライセンスキーに対して同じ手順を繰り返します。［次へ］をクリックします。
- ライセンスキーを削除するには、削除するキーをクリックし、［削除］をクリックします。
- ライセンスキーの詳細を表示するには、キーをクリックします。

9 適切な SFW または SFW HA 製品オプションを選択し、［次へ］をクリックします。

10 インストールするドメインとコンピュータを選択し、［次へ］をクリックします。



ドメイン
: リストからドメインを選択します。

ドメインとネットワークのサイズ、速度、状況によっては、ドメインとコンピュータのリスト作成に時間がかかる場合があります。

コンピュータ
: インストール用のコンピュータを追加するには、［コンピュータ］リストから選択するか、コンピュータ名を［コンピュータ］フィールドに入力します。次に、［追加］をクリックします。

追加したコンピュータを削除するには、［インストールするよう選択したコンピュータ］フィールドで該当するコンピュータ名をクリックし、［削除］をクリックします。

コンピュータ名をクリックすると、詳細が表示されます。

インストールパス	オプションでインストールパスを変更します。 ■ パスを変更するには、［インストールするよう選択したコンピュータ］フィールドでコンピュータを選択し、新しいパスを入力して、［変更］をクリックします。 ■ デフォルトのパスをリストアするには、コンピュータを選択し、［デフォルト］をクリックします。 デフォルトパスは次のとおりです。 C:¥Program Files¥Veritas 64 ビットインストールでのデフォルトパスは次のとおりです。 C:¥Program Files (x86)¥Veritas

11 インストールプログラムを実行しているコンピュータとドメインコントローラが別々のサブネットに存在する場合は、インストーラでターゲットコンピュータを検出できないことがあります。この場合は、インストーラにエラーメッセージが表示された後で、検出されなかったコンピュータのホスト名または IP アドレスを手動で入力します。

12 選択したコンピュータが必要条件を満たしているかどうかが確認され、結果が表示されます。情報を確認し、［次へ］をクリックします。
検証でコンピュータに問題が見つかった場合は、その問題を解決し、再度評価を実行します。リスト内で該当するコンピュータをクリックすると、そのコンピュータの問題についての情報を表示できます。［環境の再検証］をクリックすると、システムの検証処理を再開できます。

13 複数のパスを使用していて DMP ASL または特定の DSM を選択した場合は、Veritas DMP の警告が表示されます。Veritas DMP 警告が表示された場合は、次の手順に従います。

- DMP ASL のインストールの場合 - データの破損を防ぐために、マルチパスストレージのパスを 1 つだけ残してすべて切断していることを確認します。
- DMP DSM のインストールの場合 - DMP DSM 機能のインストールの所要時間は、インストール時に接続されている物理パスの数によって異なります。この機能のインストール時間を短縮するには、インストール時に接続する物理パスを 1 つだけにします。インストール後は、システムを再ブートする前に、追加の物理パスを再接続します。

14 ［OK］をクリックします。

15 情報を確認し、［インストール］をクリックします。必要に応じて［戻る］をクリックして、変更を行います。

16 ［インストールの状態］画面に、状態メッセージおよびインストールの進行状況が表示されます。
インストールに失敗した場合は、［次へ］をクリックしてレポートを表示し、失敗した理由を確認します。インストールを修復するか、アンインストールしてインストールしなおす必要があります。

17 インストールが完了したら、概略画面を確認し、［次へ］をクリックします。

18 リモートノードでインストールしている場合は、［再ブート］をクリックします。ローカルノードは、この時点では再ブートできません。また、障害が発生したノードはデフォルトでチェックボックスがオフになります。再ブートするリモートノードの横にあるチェックボックスをオンにします。

19 ノードで再ブートが正常に完了すると、［再起動の状態］画面でノードが［オンライン］になり、［次へ］ボタンが使用できるようになります。［次へ］をクリックします。

20 ログファイルを確認し、［完了］をクリックします。

21 ［はい］をクリックして、ローカルノードを再ブートします。

ドライバ署名オプションをリセットするには

インストール手順を完了したら、各コンピュータのドライバ署名オプションをリセットします。

ドライバ署名オプションをリセットするには

1 コントロールパネルを開き、［システム］をクリックします。

2 ［ハードウェア］タブをクリックし、［ドライバの署名］をクリックします。

3 ［ドライバ署名オプション］ダイアログボックスで、オプションを［警告］または［ブロック］にリセットします。

4 ［OK］をクリックします。

5 コンピュータごとに同じ手順を繰り返します。

コマンドラインによるインストール

SFW と SFW HA ソフトウェアでは、コマンドプロンプトで Setup.exe コマンドを入力して、コマンドラインを使ってサイレントインストールを実行できます。サイレントインストールで 1 回にインストールできるのは、1 台のコンピュータだけです。

この項の最後に、SFW クライアントと SFW サーバーのローカルインストールや、SFW サーバーのリモートインストールを示すコマンド例を示します。

38 ページの「サイレントインストールの例 : SFW クライアント」を参照してください。

38 ページの「サイレントインストールの例 : SFW サーバー」を参照してください。

38 ページの「サイレントインストールの例 : SFW サーバー のリモートインストール」を参照してください。

コマンドウィンドウからインストールを開始するには

1. スタートメニューで［ファイル名を指定して実行］を選択して、コマンドウィンドウを開きます。
2. ［名前］フィールドに「cmd」と入力し、［OK］をクリックします。
3. コマンドウィンドウから、製品 CD のルートディレクトリに移動します。
4. 次のコマンド構文を使って、SFW をインストールします。

```
Setup.exe /s INSTALL_MODE=InstallMode [SOLUTION=Solution]
[LICENSEKEY="LicenseKey"] [OPTIONS="a,b,c,..."]
[INSTALLDIR="InstallDirPath"] [NODE=SysA]
[REBOOT=RebootMode]
```

引数の最大長は 2,048 です。構文では大文字と小文字は区別されません。

Setup.exe のパラメータ

表 2-2 に、パラメータで指定できる値を示します。

表 2-2 Setup.exe のパラメータ

パラメータ	使用方法
/s	サイレントモードを設定します。サイレントモードに設定されていない場合は、インストーラ GUI を再起動します。
INSTALL_MODE	インストールまたはアンインストールを指定します。 ***1*** = インストール ***5*** = アンインストール 例 : **INSTALL_MODE=1**

表 2-2 Setup.exe のパラメータ (続き)

パラメータ	使用方法
SOLUTION	インストールの種類を設定します。 ***1*** = SFW サーバー ***2*** = SFW HA サーバー ***3*** = SFW クライアント ***4*** = SFW HA クライアント ***5*** = 言語パッケージ ***6*** = VCS Server（VCS Agent for NetApp SnapMirror インストール） ***7*** = VCS Client（VCS Agent for NetApp SnapMirror インストール） 例 : **SOLUTION=*1*** **メモ :** サーバーコンポーネントと、それに対応するクライアントコンポーネントをインストールするには、setup.exe /s コマンドを 2 回続けて実行します。1 回目は SOLUTION パラメータにサーバーコンポーネントを設定し、2 回目は対応するクライアントコンポーネントを設定します。スクリプトを使用してサーバーとクライアントをインストールする場合は、まずクライアントをインストールしてからサーバーをインストールして、サーバーのインストール後にスクリプトがシステムを再ブートできるようにすることをお勧めします。
LICENSEKEY	インストールのためのライセンスキーを設定します。複数のキーを入力する場合は、カンマで区切ります。ただし、カンマの前後にスペースを入れないでください。 ライセンスキーは二重引用符（"）で囲む必要があります。 *LicenseKey* にデフォルトの設定はありません。 例 : **LICENSEKEY="*123-234-123-234-345,321-543-765-789-321*"**
OPTIONS	インストールの種類に対する目的のオプション（ある場合）を設定します。オプションのリストは、二重引用符（"）で囲む必要があります。 **メモ :** デフォルトの設定はありません。表 2-3 を参照して、利用可能なオプションの完全な一覧と説明を確認してください。 **メモ :** MPIO の DSM（Device Specific Module）および DMP の ASL（Array Support Library）は、同じサーバーに同時に共存することはできません。 例 : **OPTIONS="*MSCS,VVR*"**

表 2-2 Setup.exe のパラメータ (続き)

パラメータ	使用方法
INSTALLDIR	インストールディレクトリのデフォルト以外のパスを設定する場合のみ使用します。パスは二重引用符（"）で囲む必要があります。 パスを指定しないときに使用するデフォルトの設定は、SystemDrive:¥Program Files¥Veritas です。 例 : **INSTALLDIR="*C:¥InstallationDirectory*"**
NODE	ノード名を設定します。一度に指定できるノードは 1 つだけです。 ノードの指定がない場合のデフォルト設定は、ローカルノードです。 例 : **Node=*SysA***
REBOOT	インストール完了時におけるシステムの自動再ブートを設定します。 ***0*** = 再ブートしない ***1*** = 再ブートする デフォルトの設定は、システムを再ブートしない 0 です。 例 : **REBOOT=*1*** **メモ :** サーバーコンポーネントに対する SFW ドライバを確実に正しくインストールには、インストールの完了時にシステムを再ブートします。クライアントコンポーネントのインストールの完了時には、システムを再ブートする必要はありません。

オプションは使用する製品と環境によって異なります。表 2-3 に、利用可能なオプションを示します。

表 2-3 利用可能オプション

オプション	説明	SFW	SFW HA
VVR	Volume Replicator（VVR）は、ディザスタリカバリ用に、複数サイトでデータをレプリケートします。	✔	✔
FlashSnap	FlashSnap を使用すると、ボリュームの永続的な分割ミラースナップショットを作成、保守できます。	✔	✔
VxCache	VxCache は、システムメモリの一部を使用し、I/O 処理効率を向上させます。	✔	✔
MSCS	MSCS のクラスタオプション	✔	

表 2-3　利用可能オプション (続き)

オプション	説明	SFW	SFW HA
DMP	DMP の Array Support Library（ASL）	✔（32 ビットのみ）	✔（32 ビットのみ）
vemcsymm	EMC Symmetrix/DMX DSM（Windows Server 2003 のみ）	✔	✔
vemcclar	EMC Clariion DSM（Windows Server 2003 のみ）	✔	✔
vhdsaa	Hitachi TagmaStore/HP XP DSM（Windows Server 2003 のみ）	✔	✔
vhdsap	Hitachi 95xx-AMS-WM DSM（Windows Server 2003 のみ）	✔	✔
vhpeva	HP EVA-MSA DSM（Windows Server 2003 のみ）	✔	✔
vibmaads	IBM DS8000/ESS DSM（Windows Server 2003 のみ）	✔	✔
vibmap	IBM DS6000 DSM（Windows Server 2003 のみ）	✔	✔
vengap	IBM DS4000/Sun 6000 DSM（Windows Server 2003 のみ）	✔	✔
vnetapp	NETAPP DSM（Windows Server 2003 のみ）	✔	✔
GCO	グローバルクラスタオプション（GCO）により、クラスタをリンクして広域フェールオーバーとディザスタリカバリを実現できます。		✔
SQL	Database Agent for Microsoft SQL Server		✔
Oracle	Database Agent for Oracle		✔（32 ビットのみ）
SRDF	Hardware Replication Agent for EMC SRDF		✔
TRUECOPY	Hardware Replication Agent for Hitachi TrueCopy		✔
EXCHANGE	Enterprise Agent for Microsoft Exchange		✔（32 ビットのみ）

表 2-3　利用可能オプション (続き)

オプション	説明	SFW	SFW HA
MIRRORVIEW	Hardware Replication Agent for EMC MirrorView		✔
MetroMirror	Hardware Replication Agent for MetroMirror		✔
PPRC	Hardware Replication Agent for IBM PPRC		✔

サイレントインストールの例 : SFW クライアント

このサンプルコマンドでは、SFW クライアントをインストールします。インストールのパスは C:¥InstallationDirectory で、インストールの終了時にシステムは再ブートされません。

```
Setup.exe /s INSTALL_MODE=1 SOLUTION=3
    INSTALLDIR="C:¥InstallationDirectory" REBOOT=0
```

サイレントインストールの例 : SFW サーバー

このサンプルコマンドでは、123-234-123-234-345 というライセンスキーとともに、MSCS と VVR の各オプションとライセンスキーを指定して、SFW サーバーをインストールします。インストールのパスは C:¥InstallationDirectory で、インストールの終了時にシステムは再ブートされます。

```
Setup.exe /s INSTALL_MODE=1 SOLUTION=1
    LICENSEKEY="123-234-123-234-345,321-543-765-789-321,
    321-543-765-789-789" OPTIONS="MSCS,VVR"
    INSTALLDIR="C:¥InstallationDirectory" REBOOT=1
```

サイレントインストールの例 : SFW サーバー のリモートインストール

このサンプルコマンドでは、123-234-123-234-345 というライセンスキーとともに、MSCS と VVR の各オプションとライセンスキーを指定して、SFW サーバーをインストールします。インストールのパスは C:¥InstallationDirectory で、インストールするノードは SysA です。インストールの終了時にシステムは再ブートされます。

```
Setup.exe /s INSTALL_MODE=1 SOLUTION=1
    LICENSEKEY="23-234-123-234-345,321-543-765-789-321,
    321-543-765-789-789" OPTIONS="MSCS,VVR"
    INSTALLDIR="C:¥InstallationDirectory" NODE=SysA REBOOT=1
```

次に実行可能なタスク

SFW HA クラスタの設定

SFW HA のインストールが終了した後で、VCS 設定ウィザードを実行して VCS クラスタの設定を行います。詳しくは、22 ページの「SFW HA のインストール計画」を参照してください。

クラスタの設定とオプションの VCS 機能については、次のマニュアルを参照してください。

- Veritas Cluster Server 管理者ガイド
- Veritas Storage Foundation and High Availability Solutions HA and Disaster Recovery ソリューションガイド Microsoft Exchange
- Veritas Storage Foundation and High Availability Solutions HA and Disaster Recovery ソリューションガイド Microsoft SQL
- Veritas Storage Foundation and High Availability Solutions ソリューションガイド

SFW を使用する iSCSI SAN の設定

iSCSI のイニシエータノードでは、SFW を使用して、iSCSI のターゲットポータルの定義、iSCSI ターゲットへのログインとログアウト、ターゲットポータルグループ設定の表示を行えます。また SFW を使用して、Microsoft iSNS サーバーの iSNS オブジェクトの接続と管理を行えます。サーバーの iSCSI イニシエータを Microsoft iSCSI Software Target に接続している場合は、イニシエータにアクセス可能な一連の LUN を表示できます。

前提条件

SFW を使用する iSCSI SAN を設定する場合、次の前提条件と、各製品に付属のマニュアルに掲載されている必要条件を考慮する必要があります。

- Microsoft iSCSI イニシエータ 2.02 以上。
- iSCSI HBA または専用の NIC カード。
- Windows Storage Server R2 と VDS 1.1 アップデート。
- Microsoft VDS iSCSI ハードウェアプロバイダ
  (Microsoft iSCSI Software Target に接続する場合)。

iSCSI SAN の設定

iSCSI SAN を設定するには、ターゲットポータルの設定、iSCSI ターゲットと iSCSI イニシエータの設定、ストレージの設定、アクセス権の割り当て、iSNS サーバーへの登録が必要です。

iSCSI ターゲットとストレージは、ストレージデバイス製造元の指示に従って設定する必要があります。

iSCSI イニシエータを設定するには、iSCSI イニシエータソフトウェアを各サーバーにインストールし、イニシエータが iSCSI ターゲットに接続できるようにしておく必要があります。省略可能なオプションとして、iSNS サーバーソフトウェアをサーバーにインストールし、ネットワーク上の iSCSI ターゲットを自動検出できるようにしておく必要もあります。

アクセス権を割り当てるには

1. VEA GUI のツリービューで、iSCSI ノードをクリックします。iSNS サーバーはイニシエータとターゲットを自動検出するので、iSCSI ノードを展開するとネットワークで利用可能なすべてのイニシエータとターゲットが表示されます。
2. イニシエータで利用可能にするターゲットにログインします。
   - ターゲットを選択し、そのコンテキストメニューから［ログイン］を選択します。
   - 設定するオプションのログイン設定があればそれらをすべてオンにします。利用可能なログイン設定には、ログインの永続的な復元を可能にする設定や、マルチパスログインを可能にする設定があります。
   - CHAP や IPsec などのセキュリティを設定するには、［拡張設定］をオンにしてセキュリティ設定ダイアログにアクセスします。

セキュリティ設定がストレージデバイスの設定と互換性があることを確認します。

SFW iSCSI の遅延起動の使用

SFW と SFW HA は通常、システムの起動中に、動的（非クラスタ）ディスクグループをインポートします。ただし、起動時に、Microsoft iSCSI Software Initiator で管理されたストレージデバイスを検出またはインポートすることはできません。SFW と SFW HA で、管理されたこのストレージを検出してインポートする時間を確保できるようにするには、Veritas DG Delayed Import Service（VxDgDI）を設定して、`vxdg latestart` コマンドを使う必要があります。

vxdg latestart

vxdg の遅延起動コマンドは、コマンドラインに次の形式で入力します。

`vxdg -g`***`DynamicDiskGroupName`*** `latestart on|off`

ここで、***DynamicDiskGroupName*** は、Microsoft iSCSI Software Initiator で管理されたダイナミックディスクグループの名前です。

`vxdg latestart` コマンドに `on` を指定すると、`-g`***DynamicDiskGroupName*** に指定されているダイナミックディスクグループが、システム起動後に Veritas DG Delayed Import Service（VxDgDI）によってインポートされるようになります。VxDgDI がストレージを制御するサービスに依存するように設定すると、VxDgDI はダイナミックディスクグループをインポートできるようになります。これにより、ストレージが使用可能になるのに必要な時間を確保することができます。VxDgDI サービスによってインポートされたストレージを使用するアプリケーションも VxDgDI に依存するように設定する必要があります。これにより、ストレージが使用可能になったときにアプリケーションは処理を開始することができます。

たとえば、iSCSI ストレージは、システム起動時には使用できないため、システムの起動後にインポートする必要があります。VxDgDI が iSCSI サービスに依存するように設定すると、システム起動後に iSCSI サービスの準備が完了したときに、ダイナミックディスクグループがインポートされます。iSCSI ストレージを使用し、VxDgDI サービスに依存するように設定されているアプリケーションは、その後処理を開始します。

ダイナミックディスクグループが同じホスト上にある限り、再ブートしても `vxdg latestart` は有効な状態のままになります。ダイナミックディスクグループをデポートして別のホストにインポートすると、`vxdg latestart` は無効になるため、新しいホストで再有効化する必要があります。クラスタ環境では、ディスクグループはクラスタアプリケーションによってインポートされるため、vxdg latestart を有効化する必要はありません。

`vxdg latestart` を使用するには

1. Windows の［サービス］ダイアログボックスで、Veritas DG Delayed Import Service のスタートアップの種類を［手動］から［自動］に変更します。
2. Windows レジストリを編集して、VxDgDI がストレージを制御するサービスに依存するように設定します（Windows 2003 では、regedit を使ってサービスを設定します。Windows 2000 では、regedt32 を使ってサービスを設定します）。

   Windows 2003 で、VxDgDI が Microsoft iSCSI イニシエータサービス（MSiSCSI）に依存するように設定するための手順を次に示します。

   - レジストリエディタ（regedit）を開いて、Windows レジストリを編集します。

- 次のレジストリキーを選択します。
  HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥VxDgDI
- DependOnService 値を右クリックし、［修正］を選択します。
  DependOnService 値が存在しない場合は、この値を作成します。レジストリエディタの右ペインの何も表示されていない部分を右クリックしてコンテキストメニューを表示し、［新規］、［複数行文字列値］の順に選択し、新しい値の名前に「DependOnService」と指定します。
  DependOnService 値を右クリックし、［修正］を選択します。
- ［文字列の編集］ダイアログで、［値のデータ］ペインの一番下の新しい行に「MSiSCSI」と入力します。
- ［OK］をクリックして、レジストリエディタを閉じます。
- システムを再ブートして変更を適用します。
- 手順 4 で示しているように、さらにレジストリを編集する必要がある場合は、システムを再ブートしないでください。
- レジストリにこれ以上変更を行う必要がない場合は、この時点でシステムを再ブートします。

3 コマンドラインに vxdg latestart コマンドを入力します。
例：
vxdg -gDynDskGrp2 latestart on
ダイナミックディスクグループ DynDskGrp2 をシステム起動後にインポートできるようになります。

4 VxDgDI サービスによってインポートされたストレージを使用するアプリケーションは、Veritas DG Delayed Import Service の起動処理が完了した後に、対象ストレージを使用できるようになります。ただし、Microsoft Exchange などの Windows サービスとして起動するアプリケーションが対象ストレージを使用できるようにするには、Windows のレジストリエディタを使用して、それらのアプリケーションが Veritas DG Delayed Import Service に依存するように設定する必要があります（Windows 2003 では、regedit を使ってサービスを設定します。Windows 2000 では、regedt32 を使ってサービスを設定します）。
Windows 2003 で、Microsoft Exchange のサービス（Microsoft Exchange Information Store サービス）が VxDgDI に依存するように設定する手順を次に示します。

- レジストリエディタ（regedit）を開いて、Windows レジストリを編集します。
- 次のレジストリキーを選択します。
  HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥MSExchangeIS

- DependOnService 値を右クリックし、［修正］を選択します。
  DependOnService 値が存在しない場合は、この値を作成します。レジストリエディタの右ペインの何も表示されていない部分を右クリックしてコンテキストメニューを表示し、［新規］、［複数行文字列値］の順に選択し、新しい値の名前に「DependOnService」と指定します。
  DependOnService 値を右クリックし、［修正］を選択します。
- ［文字列の編集］ダイアログで、［値のデータ］ペインの一番下の新しい行に「VxDgDI」と入力します。
- ［OK］をクリックして、レジストリエディタを閉じます。
- システムを再ブートして変更を適用します。

SFW または SFW HA の更新

インストーラを使うと、インストールされている SFW と SFW HA のクライアントコンポーネントとサーバーコンポーネントを更新できます。

SFW と SFW HA を更新するには

1. Windows のコントロールパネルを開き、［プログラムの追加と削除］を選択します。
2. ［Veritas Storage Foundation with High Availability 5.0 for Windows（Server）Components］を選択し、［変更］をクリックします。
3. ［Symantec Product Installer］画面が表示されます。［LiveUpdate］を選択します。［次へ］をクリックします。
4. ［LiveUpdate］画面が表示されます。利用可能な更新があるかどうかを自動で確認する場合は［オン（自動的に更新を確認）］を選択し、利用可能な更新があるかどうかを手動で確認する場合は［オフ（手動で更新を確認）］を選択します。
5. LiveUpdate モードを選択します。［オン（自動的に更新を確認）］を選択した場合は、［高速］または［対話式］を選択できます。［高速］では、更新は自動的にダウンロードされインストールされます。［対話式］では、利用可能な更新のリストが表示されるので、コンピュータにダウンロードしてインストールする更新を選択します。
6. ［［完了］をクリックした後に、最新の更新を確認します］を選択します。［完了］をクリックします。

機能の追加または削除

インストーラを使用すると、機能を追加または削除することができます。機能を追加または削除できるのは、ローカルシステムのみです。

機能を追加または削除するには

1. Windows のコントロールパネルを開き、［プログラムの追加と削除］を選択します。
2. ［Veritas Storage Foundation with High Availability 5.0 for Windows（Server）Components］を選択し、［変更］をクリックします。
3. ［Symantec Product Installer］画面が表示されます。［追加または削除］を選択します。［次へ］をクリックします。
4. ［サーバーコンポーネント］画面が表示されます。ツリーナビゲーション構造の中にある、追加または削除するコンポーネントのオプションチェックボックスをそれぞれオンまたはオフにします。

オプションのライセンスキーを追加するには、次の手順に従います。

1. オプションを右クリックし、［ライセンスを追加］を選択します。
2. 表示されたポップアップウィンドウで、オプションのライセンスキーを入力し、［OK］をクリックします。
3. チェックボックスをオンにして、オプションを追加します。［次へ］をクリックします。

検証と概略

1. ［検証］画面が表示されます。選択したオプションが必要条件を満たしているかどうかが確認され、結果が表示されます。情報を確認し、［次へ］をクリックします。
   検証でシステムに問題が見つかった場合は、システムのリスト内で該当するシステムをクリックして、そのシステムの問題についての情報を表示できます。問題を解決し、［環境の再検証］をクリックして、検証処理を再開します。
2. ［概略］画面が表示されます。情報を確認し、［更新］をクリックして、製品の更新を開始します。
3. ［更新の状態］画面が開き、状態メッセージおよび更新の進行状況が表示されます。
4. 完了したら、概略情報を確認し、［次へ］をクリックします。
5. ［完了］画面で、［完了］をクリックします。

6 メッセージボックスで［はい］をクリックして、システムを再ブートします。

インストールの修復

インストーラでは、SFW と SFW HA のクライアントとサーバーコンポーネントの既存のインストールを修復できます。修復は、ローカルシステムでのみ実行できます。

インストールを修復するには

1 Windows のコントロールパネルを開き、［プログラムの追加と削除］を選択します。

2 ［Veritas Storage Foundation with High Availability 5.0 for Windows（Server）Components］を選択し、［変更］をクリックします。

3 ［Symantec Product Installer］画面が表示されます。［修復］を選択します。［次へ］をクリックします。

4 ［検証］画面が表示されます。システムが必要条件を満たしているかどうかが確認され、結果が表示されます。情報を確認し、［次へ］をクリックします。
検証でシステムに問題が見つかった場合は、システムのリスト内で該当するシステムをクリックして、そのシステムの問題についての情報を表示できます。問題を解決し、［環境の再検証］をクリックして、検証処理を再開します。

5 ［概略］画面が表示されます。情報を確認し、［修復］をクリックして、修復プロセスを開始します。

6 ［修復の状態］画面が表示されます。状態メッセージと修復の進行状況が表示されます。
修復に失敗した場合は、［次へ］をクリックしてレポートを表示し、失敗した理由を確認します。ソフトウェアをアンインストールしてインストールしなおす必要があります。

7 完了したら、概略情報を確認し、［次へ］をクリックします。

8 ［完了］画面で、［完了］をクリックします。

9 メッセージボックスで［はい］をクリックして、システムを再ブートします。

ライセンスの管理

インストーラを使うと、SFW と SFW HA のクライアントコンポーネントとサーバーコンポーネントのインストールの、オプション用のライセンスキーを追加または削除できます。

ライセンスキーを追加または削除するには

1. Windows のコントロールパネルを開き、［プログラムの追加と削除］を選択します。
2. ［Veritas Storage Foundation with High Availability 5.0 for Windows（Server）Components］を選択し、［変更］をクリックします。
3. ［Symantec Product Installer］画面が表示されます。［ライセンス管理］を選択します。［次へ］をクリックします。
4. ライセンスキーの画面が表示されます。追加するライセンスキーを入力し、［更新］をクリックします。ライセンスキーを削除する場合は、［ライセンス］フィールドからライセンスキーを選択し、［削除］をクリックします。

インストーラを使ったアンインストール

リモートコンピュータからソフトウェアをアンインストールするには、アンインストールするローカルコンピュータに SFW または SFW HA がインストールされている必要があります。

次の手順は、Windows 2000 システムから SFW サーバーコンポーネントとクライアントコンポーネントをアンインストールする場合に適用されます。クライアントコンポーネントおよび高可用性サーバーのアンインストール手順もほぼ同じです。SFW HA のアンインストールの場合は、アンインストールする前にクラスタの設定を解除する必要があります。

インストーラを使用してアンインストールするには

1. Windows のコントロールパネルで、［プログラムの追加と削除］を選択します。
2. ［Veritas Storage Foundation 5.0 for Windows（Server Components）］をクリックします。
3. ［削除］をクリックします。
4. ［次へ］をクリックします。
5. ［クライアントのコンポーネント］画面で、チェックボックスをオンにして、サーバーコンポーネントとともにクライアントコンポーネントをアンインストールします。［次へ］をクリックします。

6 ［ドメイン］および［コンピュータ］ドロップダウンメニューからアンインストールするシステムを選択し、［追加］をクリックします。［コンピュータ］フィールドにコンピュータ名を入力して追加することもできます。他のシステムからのアンインストールを繰り返します。
［アンインストールするよう選択したコンピュータ］リストからシステムを削除するには、システムをクリックし、［削除］をクリックします。

7 ［次へ］をクリックします。

8 ［検証］画面で、選択したシステムが必要条件を満たしているかどうかが確認され、結果が表示されます。情報を確認し、［次へ］をクリックします。
検証でシステムに問題が見つかった場合は、システムのリスト内で該当するシステムをクリックして、そのシステムの問題についての情報を表示できます。問題を解決し、［環境の再検証］をクリックして、検証処理を再開します。

9 ［概略］画面が表示され、アンインストール先に選択した設定とシステムが表示されます。［アンインストール］をクリックします。

10 ［アンインストールの状態］画面に、状態メッセージおよびインストールの進行状況が表示されます。
アンインストールが失敗した場合は、状態画面にアンインストールが失敗したことが表示されます。［次へ］をクリックして、レポートを確認し、エラーの原因を解決してから、そのコンピュータでこの手順を再度実行します。

11 完了したら、概略情報を確認し、［次へ］をクリックします。

12 リモートノードを再ブートします。ローカルノードは、この時点では再ブートできません。
- 再ブートするリモートノードの横にあるチェックボックスをオンにします。
- ［再ブート］をクリックします。
- ノードで再ブートが正常に完了すると、［再起動の状態］画面でノードが［オンライン］になり、［次へ］ボタンが使用できるようになります。［次へ］をクリックします。
- リモートノードが再ブートされたら、［次へ］をクリックします。

13 ［完了］画面で、ログファイルを確認し、［完了］をクリックします。

14 ［はい］をクリックして、ローカルシステムを再ブートします。

コマンドラインによるアンインストール

SFW ソフトウェアをサイレントアンインストールするには、コマンドプロンプトから Setup.exe コマンドを使います。

この項の終わりには、クライアントコンポーネントのアンインストール方法を示す 2 つのコマンドの使用例が記載されています。

50 ページの「Setup.exe の例 : SFW クライアントコンポーネントのアンインストール」を参照してください。50 ページの「Setup.exe の例 : SFW サーバーコンポーネントのアンインストール」を参照してください。

コマンドプロンプトからアンインストールを開始するには

1. スタートメニューで［ファイル名を指定して実行］を選択して、コマンドウィンドウを開きます。
2. ［名前］フィールドに「cmd」と入力し、［OK］をクリックします。
3. コマンドウィンドウから、製品 CD のルートディレクトリに移動します。
4. 次のコマンド構文を使って、SFW をサイレントアンインストールします。

   Setup.exe /s INSTALL_MODE=*InstallMode* **[SOLUTION=***Solution***] [REBOOT=***RebootMode***] [NODE=***SysA***]**

パラメータで指定できる値は、次のとおりです。

表 2-4　製品アンインストール用のパラメータ

パラメータ	使用方法
/s	サイレントモードを設定します。
INSTALL_MODE	インストールまたはアンインストールを指定します。 ***1*** = インストール ***5*** = アンインストール デフォルトの設定は、インストールを示す ***1*** です。このパラメータを、アンインストールを示す ***5*** に設定します。 例 : **INSTALL_MODE=*5***

表 2-4 製品アンインストール用のパラメータ

パラメータ	使用方法
SOLUTION	アンインストールの種類を設定します。 ***1*** = SFW サーバー ***2*** = SFW HA サーバー ***3*** = SFW クライアント ***4*** = SFW HA クライアント ***5*** = 言語パッケージ ***6*** = VCS サーバー（VCS Agent for NetApp SnapMirror インストール） ***7*** = VCS クライアント（VCS Agent for NetApp SnapMirror インストール） デフォルトの設定は、SFW サーバー を示す ***1*** です。 例 : **SOLUTION=*1*** **メモ :** サーバーコンポーネントと、それに対応するクライアントコンポーネントをアンインストールするには、`setup.exe /s` コマンドを 2 回実行します。1 回目は SOLUTION パラメータにサーバーコンポーネントを設定し、2 回目は対応するクライアントコンポーネントを設定します。
REBOOT	インストール完了時におけるシステムの自動再ブートを設定します。 ***0*** = 再ブートしない ***1*** = 再ブートする デフォルトの設定は、システムを再ブートしない ***0*** です。 例 : **REBOOT=*1***
NODE	ノード名を設定します。一度に指定できるノードは 1 つだけです。 ノードの指定がない場合のデフォルト設定は、ローカルノードです。 例 : **Node=*SysA*** **メモ :** サーバーコンポーネントに対する SFW ドライバを確実に正しくインストールするには、インストールの完了時にシステムを再ブートします。クライアントコンポーネントのインストールの完了時には、システムを再ブートする必要はありません。

Setup.exe の例 : SFW クライアントコンポーネントのアンインストール

このサンプルコマンドでは、SFW サーバーコンポーネントを完全にアンインストールします。アンインストールの終了時にシステムは再ブートされます。

```
Setup.exe /s INSTALL_MODE=5 SOLUTION=1 REBOOT=1
```

Setup.exe の例 : SFW サーバーコンポーネントのアンインストール

このサンプルコマンドでは、SFW サーバーコンポーネントを完全にアンインストールします。アンインストールの終了時にシステムは再ブートされます。

```
Setup.exe /s INSTALL_MODE=5 SOLUTION=1 REBOOT=1
```

Veritas Dynamic Multi-pathing（DMP）のインストールとアンインストール

この項では、次のトピックについて説明します。

手順について詳しくは、『Veritas Storage Foundation 管理者ガイド』を参照してください。

概要

Veritas Dynamic Multi-pathing（DMP）オプションは、サーバーとストレージアレイの間の複数のパスをサポートすることによって、耐障害性を付加します。Veritas Dynamic Multi-pathing（DMP）は次のいずれかの方法で実装されます。

- DMP ASL（Array Support Library）、または
- DMP DSM（Device Specific Module）

メモ : DMP ASL と DMP DSM は異なる製品であり、同じコンピュータで実行することはできません。

DMP ASL または DMP DSM の選択

DMP ASL と DMP DSM は環境に応じて選択します。どちらを実装する場合も、事前にオペレーティングシステムのバージョンや、個々のアレイに対するサポートなどの要因を検討する必要があります。シマンテック社テクニカルサポートの Web サイト（http://entsupport.symantec.com）で、ハードウェア互換性リストを参照し、SFW または SFW HA で動作が確認されているハードウェアを確認してください。

DMP DSM

DMP DSM は、Microsoft Windows Server 2003 MPIO（Multipath Input/Output）ソリューションと連動する DMP 手順です。DMP DSM では次がサポートされます。

- Windows Server 2003
- Windows Storport ドライバ
- Microsoft iSCSI イニシエータ
- Dynamic Least Queue Depth ロードバランシング
- クラスタ化によるアクティブ / アクティブ DMP

DMP ASL

DMP ASL は、以前の SFW リリースで使われていた DMP 手順です。DMP ASL では次がサポートされます。

- Windows 2000 および Windows Server 2003
- Windows ミニポートドライバ
- SCSI ポートドライバ
- 負荷分散ポリシー
- 32 ビットオペレーティングシステムのみ

必要条件

次の前提条件を確認してください。

- ホストに SAN スイッチへの各パス用の HBA ポートがあることを確認します。
- ホストに、ホストバスアダプタポートごとに 1 つの SCSI ケーブルまたはファイバーケーブルがあることを確認します。
- iSCSI の場合は、各ホストバスアダプタポートに一意の SCSI ID を割り当てます。

- パスを 1 つだけ接続します。

警告 : SFW のインストール後に、ケーブルの接続順を変更しないでください。たとえば、ホストバスアダプタ A がアレイのポート A に接続されており、ホストバスアダプタ B がアレイのポート B に接続されている場合は、アレイのポートを（A を B に、B を A に）交換して接続しないでください。

DMP DSM（Device Specific Module）のインストールとアンインストール

この項では次のトピックについて説明します。

DMP の Device Specific Module（DSM）の設定

あらゆる設定に DMP DSM を追加する一般的な手順は次のとおりです。

- 新しいホストアダプタハードウェアを設置します。
- アレイストレージに接続するパスを 1 つだけにして、インストール時間を短縮します。
- SFW または SFW HA のインストールプロセス内で DMP DSM を選択して、ソフトウェアをインストールします。

『Veritas Storage Foundation 管理者ガイド』を参照してください。

メモ : DMP DSM は DMP ASL と共存できないため、DMP ASL をアンインストールしてから DMP DSM をインストールする必要があります。

DMP DSM に適切なハードウェアドライバをインストールすることは大変重要です。ハードウェアドライバの詳細については、ハードウェアのマニュアルを参照してください。

新しいスタンドアロンサーバーへの DMP DSM（Device Specific Module）のインストール

次の手順に従って、DMP DSM を新しいスタンドアロンサーバーにインストールします。

新しいスタンドアロンサーバーに DMP DSM をインストールするには

1. 必要なハードウェアと適切なドライバをインストールします。
2. アレイのパスを 1 つだけコンピュータに接続します。
3. インストール時に、［オプションの選択］画面で［Dynamic Multi-pathing］の下の［DSM（Device Specific Module）］を選択します。
4. ウィザードを完了し、指示に従って再ブートします。
5. 追加のパスを物理的に再接続します。

クラスタへの SFW HA と DMP DSM（Device Specific Module）の初めてのインストール

クラスタ環境の DMP DSM では、アクティブ / アクティブまたはアクティブ / パッシブの負荷分散設定を使用できます。DMP DSM では、SCSI-2 用に予約されているディスクの負荷分散はアクティブ / パッシブに自動的に設定されます。クラスタ環境のアクティブ / アクティブ負荷分散では、アレイは SCSI-3 Persistent Group Reservations（SCSI-3 PGR）を有効化する必要があります。SCSI-3 PGR は、Windows Server 2003 でのみ利用可能であり、デフォルトでは無効になっています。DMP DSM と SCSI-3 PGR の有効化と無効化について詳しくは、『Veritas Storage Foundation 管理者ガイド』と、http://entsupport.symantec.com にある SFW 5.0 のハードウェア互換性リスト（HCL）を参照してください。

メモ : Veritas Storage Foundation & High Availability Solutions 5.0 for Windows 製品のハードウェア互換性リスト（HCL）は、シマンテック社テクニカルサポートの Web サイトにあります。HCL には、各サポート対象のアレイを使用してテストされた HBA、ファームウェア、スイッチなどの情報が記載されています。DMP ASL または DMP DSM を使用する前に、HCL を参照して詳細を確認してください。

警告 : これらの手順に従わないと、ディスク署名の不整合が発生し、SFW HA または別のアプリケーションが失敗する原因になります。

SFW HA と DMP DSM をクラスタに初めてインストールするには

1. インストールの実行前に、アレイのパスを 1 つだけコンピュータに接続します。
2. SFW HA と DMP DSM とを、クラスタのすべてのノードに同時にインストールします。インストール時に適切な機能を選択します。
3. インストール後に再ブートします。
4. 追加のパスを物理的に再接続します。
5. 再ブート後は、様々な VCS ウィザードを実行して、VCS クラスタの設定を行います。VCS クラスタの作成と設定について詳しくは、『Veritas Storage Foundation 管理者ガイド』を参照してください。

クラスタへの SFW MSCS と DMP DSM（Device Specific Module）の初めてのインストール

クラスタで MSCS と DMP DSM（Device Specific Module）を同時にサポートするには、次の手順を実行する必要があります。

警告 : これらの手順に従わないと、ディスク署名の不整合が発生し、MSCS または別のアプリケーションが失敗する原因になります。

クラスタに MSCS と DMP DSM を初めてインストールするには

1. MSCS クラスタを作成します。
2. インストールの実行前に、アレイのパスを 1 つだけコンピュータに接続します。
3. SFW と DMP DSM を同時にインストールします。インストール時に適切な機能を選択します。
4. インストール後に再ブートします。
5. 追加のパスを物理的に再接続します。
6. MSCS クラスタのセットアップと設定を行います。

既存のスタンドアロンサーバーへの DMP DSM（Device Specific Module）の追加

次の手順に従い、既存のサーバーに DMP DSM を追加します。

既存のサーバーに DMP DSM を追加するには

1. 追加ハードウェアと適切なドライバをインストールします。
2. アレイのパスを 1 つだけコンピュータに接続します。
3. Windows のコントロールパネルを開き、［プログラムの追加と削除］を選択します。
4. ［プログラムの変更と削除］を選択します。
5. ［SFW サーバーコンポーネント］エントリを選択し、［変更］をクリックします。
6. インストーラ画面が表示されます。［追加または削除］を選択します。［次へ］をクリックします。
7. ［オプションの選択］画面が表示されます。［Dynamic Multi-pathing］の下の［DMP DSM（Device Specific Module）］を選択します。
8. オプションのライセンスキーを追加するには、次の手順に従います。
   - 画面の一番右にある［ライセンスを追加］リンクをクリックします。
   - ［ライセンスを追加］リンクは、オプションのライセンスがない場合にのみ表示されます。
   - 表示されたポップアップウィンドウで、オプションのライセンスキーを入力し、［OK］をクリックします。
   - チェックボックスをオンにしてオプションを追加し、［次へ］をクリックします。
9. システムを再ブートします。
10. 追加の物理パスを再接続します。
11. 追加パスが存在していることを確認します。
    - Veritas Enterprise Administrator コンソールを開きます。
    - ［システム］フィールドで、［ディスク］ツリーを展開します。
    - 任意の外部ディスクをクリックします。
    - コンソールの上部で、［DMP］タブをクリックします。
    - パスが存在していることを確認します。

既存の SFW HA または SFW MSCS クラスタへの DMP DSM の追加

ローリングアップグレードを実行して、SFW または SFW HA と、DMP DSM を各ノードに別々にインストールすることをお勧めします。

既存の SFW HA または MSCS クラスタに DMP DSM を追加するには

1. リソースを別のノードに移動するか、リソースをオフラインにします。
2. 追加ハードウェアと適切なドライバをインストールします。
3. アレイのパスを 1 つだけコンピュータに接続します。
4. Windows のコントロールパネルを開き、［プログラムの追加と削除］を選択します。
5. ［プログラムの変更と削除］を選択します。
6. ［SFW HA Server Components］エントリを選択し、［変更］をクリックします。
7. インストーラ画面が表示されます。［追加または削除］を選択します。［次へ］をクリックします。
8. ［オプションの選択］画面が表示されます。［Dynamic Multi-pathing］の下の［DMP DSM（Device Specific Module）］を選択します。
   オプションのライセンスキーを追加するには、次の手順に従います。
   - 画面の一番右にある［ライセンスを追加］リンクをクリックします。
   - ［ライセンスを追加］リンクは、オプションのライセンスがない場合にのみ表示されます。
   - 表示されたポップアップウィンドウで、オプションのライセンスキーを入力し、［OK］をクリックします。
   - チェックボックスをオンにして、オプションを追加します。

   ［次へ］をクリックします。
9. 追加の物理パスを再接続します。
10. システムを再ブートします。
11. 追加パスが存在していることを確認します。
    - Veritas Enterprise Administrator コンソールを開きます。
    - ［システム］フィールドで、［ディスク］ツリーを展開します。
    - 任意の外部ディスクをクリックします。
    - コンソールの上部で、［DMP］タブをクリックします。
    - パスが存在していることを確認します。

DMP DSM のアンインストール

DMP DSM をアンインストールするには、インストーラの［追加または削除］機能を使います。

44 ページの「機能の追加または削除」を参照してください。

DMP の Array Support Library（ASL）のインストールとアンインストール

この項では次のトピックについて説明します。

システムにすでに DMP ASL（Array Support Library）が存在し、SFW または SFW HA にアップグレードする場合は、次を参照してください。

69 ページの「SFW 5.0 にアップグレードする前に」を参照してください。
95 ページの「SFW HA 5.0 にアップグレードする前に」を参照してください。

DMP の Array Support Library（ASL）の設定

DMP の ASL（Array Support Library）とともに SFW または SFW HA をインストールする前に、ディスクアレイへに接続されているパスを 1 つだけにします。DMP の ASL（Array Support Library）をインストールしたら、アレイを DMP ASL の制御下に置き、追加のパスを接続します。ディスクアレイを有効化し（DMP ASL の制御下に置く）、パスを接続する手順については、後で説明します。

メモ : DMP ASL と DMP DSM は共存できません。既存の DMP DSM をアンインストールしてから DMP ASL をインストールしてください。

警告 : セカンダリデータパスを共有ストレージに接続する前に、アレイが DMP ASL の制御下にあることを確認してください。セカンダリパスが接続された状態で DMP ASL の制御下にないストレージを使用すると、予測不可能なオペレーティングシステムの動作を招き、データが破損する可能性があります。

ハードウェアについては、ハードウェアのマニュアルを参照してください

DMP ASL の機能や、DMP ASL を新しいクラスタまたは既存のクラスタに追加する手順について詳しくは、『Veritas Storage Foundation 5.0 管理者ガイド』を参照してください。

DMP ASL を追加する対象がどのような設定でも、一般的な手順は同じです。

手順は次のとおりです。

- 新しいホストアダプタハードウェアをインストールしますが、アレイストレージに接続するパスは必ず 1 つだけにします。
- SFW または SFW HA のインストールプロセス内で DMP ASL を選択して、ソフトウェアをインストールします。
- 設定プロセスの最後に、インストールの設定が終了したら、アレイを DMP ASL の制御下に置き、追加パスを接続します。

新しいスタンドアロンサーバーへの DMP ASL のインストール

インストールの実行前に、各ノードに接続されているアレイのパスは 1 つだけになっていることを確認します。

メモ : DMP ASL を実行できるのは、32 ビットオペレーティングシステムのみです。

新しいスタンドアロンサーバーに DMP ASL をインストールするには

1. 必要なハードウェアと適切なドライバをインストールします。
   57 ページの「DMP の Array Support Library（ASL）の設定」を参照してください。
2. インストール前に、アレイのパスを 1 つだけコンピュータに接続します。
3. インストール時に、［オプションの選択］ページで［Dynamic Multi-pathing］の下の［DMP ASL］を選択します。
4. インストールを完了し、コンピュータを再ブートします。
5. ディスクアレイストレージを DMP ASL の制御下に置き、コンピュータからの追加パスを接続します。再スキャンし、追加パスが表示されていることを確認します。
   このタスクについて詳しくは、前の項に掲載されています。

59 ページの「DMP ASL のインストール後のディスクアレイストレージの有効化」を参照してください。

DMP ASL のインストール後のディスクアレイストレージの有効化

この項では、アレイストレージを DMP ASL の制御下に置き（アレイの有効化）、追加パスを接続します。

DMP ASL のインストール後にディスクアレイを有効化するには

1. スタートメニューで［プログラム］、［Symantec］、［Veritas Storage Foundation］、［Veritas Enterprise Administrator］の順に選択して、Veritas Enterprise Administrator を開きます。
2. ツリービューの［ディスク］フォルダで、ストレージアレイのディスクを選択します。
3. 右ペインで、そのディスクの［パス］タブをクリックします。［パス］タブにパスが 1 つ表示されます。
4. パスを右クリックし、パスのコンテキストメニューから［アレイ設定］を選択します。
5. ［アレイ設定］ウィンドウで、［DMP を無効にする］のチェックマークをはずします。
6. 適切なケーブルを使って、サーバーの追加パスをスイッチに接続し、スイッチの設定をすべて行います。
7. 再スキャンを実行します。
8. 追加パスが表示されることを確認します。
   - Veritas Enterprise Administrator コンソールを開きます。
   - ［システム］フィールドで、［ディスク］ツリーを展開します。
   - 任意の外部ディスクをクリックします。
   - コンソールの上部で、DMP の［パス］タブをクリックします。
   - パスが存在していることを確認します。

クラスタへの SFW HA と DMP ASL の初めてのインストール

クラスタで SFW HA と DMP ASL を同時にサポートするには、次の手順に従う必要があります。これらの手順に従わないと、ディスク署名の不整合が発生し、SFW HA または別のアプリケーションが失敗する原因になります。

インストールの実行前に、各ノードに接続されているアレイのパスは 1 つだけになっていることを確認します。

メモ : DMP ASL を実行できるのは、32 ビットオペレーティングシステムのみです。

SFW HA と DMP ASL をクラスタに初めてインストールするには

1. 必要なハードウェアをインストールします。
2. インストール前に、アレイのパスを 1 つだけコンピュータに接続します。
3. Storage Foundation HA 5.0 for Windows をクラスタのすべてのノードにインストールします。
4. ［オプションの選択］ページで、［Dynamic Multi-pathing］の下の［DMP ASL］を選択します。
5. インストールを完了し、必要に応じて再ブートします。
6. Veritas Enterprise Administrator で、ディスクアレイストレージを DMP ASL の制御下に置きます。
   - ツリービューの［ディスク］フォルダで、ストレージアレイのディスクを選択します。
   - 右ペインで、そのディスクの［パス］タブをクリックします。［パス］タブにパスが 1 つ表示されます。
   - パスを右クリックし、パスのコンテキストメニューから［アレイ設定］を選択します。
   - ［アレイ設定］ウィンドウで、［DMP を無効にする］のチェックマークをはずします。
7. 適切なケーブルを使って、サーバーの追加パスをスイッチに接続し、スイッチの設定をすべて行います。
8. 再スキャンを実行します。
9. 追加パスが表示されることを確認します。
   - Veritas Enterprise Administrator コンソールを開きます。
   - ［システム］フィールドで、［ディスク］ツリーを展開します。
   - 任意の外部ディスクをクリックします。
   - コンソールの上部で、DMP の［パス］タブをクリックします。
   - 2 つのパスが存在していることを確認します。
10. VEA および VCS のウィザードを使用して、VCS クラスタの設定を行います。

クラスタへの MSCS と DMP ASL の初めてのインストール

クラスタで SFW MSCS と DMP ASL を同時にサポートするには、次の手順に従う必要があります。これらの手順に従わないと、ディスク署名の不整合が発生し、MSCS または別のアプリケーションが失敗する原因になります。

インストールの実行前に、各ノードに接続されているアレイのパスは 1 つだけになっていることを確認します。

メモ : DMP ASL を実行できるのは、32 ビットオペレーティングシステムのみです。

クラスタに SFW と MSCS を初めてインストールするには

1. MSCS クラスタを作成します。
2. Storage Foundation 5.0 for Windows をインストールします。
3. ［オプションの選択］ページで、［DMP ASL］オプションと［MSCS］オプションを選択します。
4. ウィザードを完了し、必要に応じて再ブートします。
5. Veritas Enterprise Administrator で、ディスクアレイストレージを DMP ASL の制御下に置きます。
   - ツリービューの［ディスク］フォルダで、ストレージアレイのディスクを選択します。
   - 右ペインで、そのディスクの［パス］タブをクリックします。［パス］タブにパスが 1 つ表示されます。
   - パスを右クリックし、パスのコンテキストメニューから［アレイ設定］を選択します。
   - ［アレイ設定］ウィンドウで、［DMP を無効にする］のチェックマークをはずします。
6. 適切なケーブルを使って、サーバーの追加パスをスイッチに接続し、スイッチの設定をすべて行います。
7. 再スキャンを実行します。
8. 追加パスが表示されることを確認します。
   - Veritas Enterprise Administrator コンソールを開きます。
   - ［システム］フィールドで、［ディスク］ツリーを展開します。
   - 任意の外部ディスクをクリックします。
   - コンソールの上部で、DMP の［パス］タブをクリックします。
   - パスが存在していることを確認します。
9. MSCS クラスタ環境を設定および設定します。

既存のスタンドアロンサーバーへの DMP ASL の追加

次の手順に従い、既存のスタンドアロンサーバーに DMP ASL を追加します。

既存のスタンドアロンサーバーに DMP ASL を追加するには

1. 追加ハードウェアをインストールし、ディスクアレイにホストアダプタパスが 1 つしか接続されていないことを確認します。
2. Windows のコントロールパネルを開き、［プログラムの追加と削除］を選択します。
3. ［プログラムの変更と削除］を選択します。
4. ［SFW サーバーコンポーネント］エントリを選択し、［変更］をクリックします。
5. インストーラ画面が表示されます。［追加または削除］を選択します。［次へ］をクリックします。
6. ［オプションの選択］画面が表示されます。［Dynamic Multi-pathing］の下の［DMP Array Support Libraries (ASLs)］を選択します。
   オプションのライセンスキーを追加するには、次の手順に従います。
   - 画面の一番右にある［ライセンスを追加］リンクをクリックします。
   - ［ライセンスを追加］リンクは、オプションのライセンスがない場合にのみ表示されます。
   - 表示されたポップアップウィンドウで、オプションのライセンスキーを入力し、［OK］をクリックします。
   - チェックボックスをオンにして、オプションを追加します。

   ［次へ］をクリックします。
7. ウィザードを完了し、必要に応じて再ブートします。
8. Veritas Enterprise Administrator で、ディスクアレイストレージを DMP ASL の制御下に置きます。
   - ツリービューの［ディスク］フォルダで、ストレージアレイのディスクを選択します。
   - 右ペインで、そのディスクの［パス］タブをクリックします。ディスクに対する DMP ASL 制御が有効化されていないため、［パス］タブには 1 つのパスのみ表示されます。
   - パスを右クリックし、パスのコンテキストメニューから［アレイ設定］を選択します。
   - ［アレイ設定］ウィンドウで、［DMP を無効にする］のチェックマークをはずします。
9. サーバーからのパスを接続します。
10. 再スキャンを実行します。

11 追加パスが表示されることを確認します。

- Veritas Enterprise Administrator コンソールを開きます。
- ［システム］フィールドで、［ディスク］ツリーを展開します。
- 任意の外部ディスクをクリックします。
- コンソールの上部で、DMP の［パス］タブをクリックします。
- パスが存在していることを確認します。

59 ページの「DMP ASL のインストール後のディスクアレイストレージの有効化」を参照してください。

既存の SFW HA または SFW MSCS クラスタへの DMP ASL の追加

各ノードに別々に DMP ASL のローリングインストールを行うことをお勧めします。

メモ : DMP ASL を実行できるのは、32 ビットオペレーティングシステムのみです。

既存の SFW HA または MSCS クラスタに DMP ASL を追加するには

1 リソースを別のノードに移動するか、リソースをオフラインにします。

2 追加ハードウェアをインストールし、ディスクアレイにホストアダプタパスが 1 つしか接続されていないことを確認します。

3 Windows のコントロールパネルを開き、［プログラムの追加と削除］を選択します。

4 ［プログラムの変更と削除］を選択します。

5 ［SFW HA Server Components］エントリを選択し、［変更］をクリックします。

6 インストーラ画面が表示されます。［追加または削除］を選択します。［次へ］をクリックします。

7 ［オプションの選択］画面が表示されます。［Dynamic Multi-pathing］の下の［DMP Array Support Libraries (ASLs)］を選択します。
オプションのライセンスキーを追加するには、次の手順に従います。

- 画面の一番右にある［ライセンスを追加］リンクをクリックします。
- ［ライセンスを追加］リンクは、オプションのライセンスがない場合にのみ表示されます。
- 表示されたポップアップウィンドウで、オプションのライセンスキーを入力し、［OK］をクリックします。

- チェックボックスをオンにしてオプションを追加し、［次へ］をクリックします。

8 ウィザードを完了し、必要に応じて再ブートします。

9 Veritas Enterprise Administrator で、ディスクアレイストレージを DMP ASL の制御下に置きます。

- ツリービューの［ディスク］フォルダで、ストレージアレイのディスクを選択します。
- 右ペインで、そのディスクの［パス］タブをクリックします。ディスクに対する DMP ASL 制御が有効化されていないため、［パス］タブには 1 つのパスのみ表示されます。
- パスを右クリックし、パスのコンテキストメニューから［アレイ設定］を選択します。
- ［アレイ設定］ウィンドウで、［DMP を無効にする］のチェックマークをはずします。

10 適切なケーブルを使って、サーバーの追加パスをスイッチまたはアレイに接続し、スイッチまたはアレイに必要な設定をすべて行います。

11 再スキャンを実行します。

12 パスが存在していることを確認します。

- Veritas Enterprise Administrator コンソールを開きます。
- ［システム］フィールドで、［ディスク］ツリーを展開します。
- 任意の外部ディスクをクリックします。
- コンソールの上部で、DMP の［パス］タブをクリックします。
- パスが存在していることを確認します。

13 他のノードについても上記の手順を繰り返します。

DMP ASL のアンインストール

DMP ASL をアンインストールするか、DMP ASL とともに SFW または SFW HA をアンインストールする場合、アレイストレージへのプライマリパスだけを残して、すべて切断してからアンインストールすることが重要です。アップグレードする場合も、パスはプライマリパスだけに限定する必要があります。

警告 : アップグレードまたはアンインストールの前に DMP ASL をシングルパスにしないと、データが破損する可能性があります。

DMP ASL の制御下のパスをシングルパスにするには

1. SFW または SFW HA で、各マルチパスアレイに対する DMP ASL 制御を無効にします（[DMP を無効にする] チェックボックスをオンにします）。
2. 各マルチパスアレイからプライマリパスだけを残して、すべて物理的に取り外します。
3. 再スキャンを実行します。

DMP ASL をアンインストールするには、インストーラの［追加または削除］機能を使用します。

44 ページの「機能の追加または削除」を参照してください。

SFW または SFW HA をインストールする方法について詳しくは、46 ページの「インストーラを使ったアンインストール」を参照してください。

2

アップグレード

この項では、次の各章で Veritas Storage Foundation for Windows 5.0 または Veritas Storage Foundation High Availability for Windows 5.0 へのアップグレードに使用する手順を説明します。

3

SFW 5.0 へのアップグレード

この章では、Veritas Storage Foundation 5.0 for Windows（SFW 5.0）へのアップグレードについて説明します。この章で扱う内容は次のとおりです。

SFW 5.0 にアップグレードする前に

アップグレードする前に、システムが最小限の製品バージョンを満たしていることを確認する必要があります。アップグレードの準備を行う必要もあります。

警告 : SFW 4.x Rule Manager を使用して作成したルールは自動的にアップグレードされず、SFW 5.0 では機能しません。詳しくは http://entsupport.symantec.com/docs/285845 を参照してください。

サポートされる最小限の製品バージョンの確認

SFW 5.0 にアップグレードするには、既にシステムにバージョン 4.1 以降の SFW がインストールされている必要があります。以前にインストールされた SFW のバージョンは、最小限の製品バージョンを満たす必要があります。アップグレード前に、インストーラは、最小限の製品バージョンを満たしているかどうか確認します。

インストーラが必要とする最小限のレベルを現在のインストールが満たしていない場合は、手動で適切な製品アップグレードを行って必要な最小限の製品レベルを満たしてから、インストーラを使用することをお勧めします。製品の中間バージョンは、シマンテック社テクニカルサポートの Web サイト http://entsupport.symantec.com で入手できます。ライセンスの取得については、ご購入先にお問い合わせください。以前のバージョンをアンインストールしてから新しい製品をインストールする方法もあります。

アップグレードの準備

製品をアップグレードするには、次の手順を実行する必要があります。

- すべてのデータを安全な場所にバックアップする。
- システム状態をバックアップする。
- ソフトウェアをアップグレードするためのハードウェア必要条件を確認する。
- アップグレードしたソフトウェアをサポートするために、Microsoft Active Directory を更新する必要があるかどうかを確認する。たとえば、Microsoft Exchange 2000 を Exchange 2003 にアップグレードする場合は、Active Directory を更新する必要があります。
- 各製品のアップグレード後にシステムをテストする（特に、最小限の必要なバージョンにするために製品アップグレードを適用した後）。差分アップグレードにより、トラブルシューティングが容易になります。

アップグレードに関する追加情報

この項では、SFW と MSCS を使用したアップグレードに関する次の情報を説明します。

- アップグレードの際、選択したシステムの検証中にメッセージが表示される場合があります。これらの情報メッセージはエラーを示すものではありません。エラーが発生した場合は、システムの状態によって問題が確認できます。
- このアップグレードを実行するには、クラスタの非アクティブなノードに SFW 5.0 をインストールし、次に、MSCS の［Move Group］コマンドを使ってアクティブなノードを移動して、クラスタの残りのノードに SFW をインストールするローリングアップグレード手順を使用します。

日本語版パッケージアップグレード情報

日本語言語パッケージをアップグレードするには、次のタスクを実行します。

- これから説明する手順に従い、英語版ディスクを使用して SFW 5.0 に完全にアップグレードします。
- 日本語版ディスクを使用して、SFW 5.0 の日本語バージョンにアップグレードします。

以前の 4.x バージョンからのアップグレード

SFW 4.1、4.2、4.3、4.3 MP1 から SFW 5.0 にアップグレードする場合は、次のタスクを順番に行います。

VVR または DMP がすでにインストールされ、設定されている場合、SFW 5.0 へのアップグレードの前後に次の手順を実行する必要があります。

- 72 ページの「アップグレードのための VVR 環境の準備」
- 73 ページの「アップグレード環境に DMP を追加する準備」または
73 ページの「アップグレードのための既存の DMP 環境の準備」
- 74 ページの「アップグレード環境に DMP DSM を追加する準備」
- 74 ページの「SFW 5.0 へのアップグレード」
- 81 ページの「アップグレード後の VVR の再有効化」
- 83 ページの「アップグレード後の DMP の再有効化」
- 83 ページの「ダイナミックディスクグループのアップグレード」

アップグレードのための VVR 環境の準備

VVR を使用してプライマリサイトからセカンダリサイトへデータのレプリケーションを行う場合は、次の手順に従って RVG（Replicated Volume Group）を停止し、レプリケーションリンク（RLINK）を切断します。

プライマリサイトを準備するには

1. VVR によりサイト間のデータのレプリケーションを行うアプリケーションを停止します。
2. スタートメニューで［ファイル名を指定して実行］を選択して、コマンドウィンドウを開きます。［名前］フィールドに「cmd」と入力し、［OK］をクリックします。
3. プライマリサイトで **vxprint -IVP** コマンドを実行します。`Diskgroup` は *`diskgroup_name`* です。
4. アップグレードの実行中にアプリケーションがボリュームにアクセスしたり、ボリュームを変更したりすることを防ぐために、RVG を停止します。Veritas Enterprise Administrator コンソールで、RVG を右クリックし、表示されるメニューから［データアクセスを無効化］オプションを選択します。
5. プライマリサイトで次のコマンドを実行して、レプリケータログのデータがセカンダリサイトに書き込まれたことを確認します。
   `vxrlink [-g`*`diskgroup_name`*`] status `*`rlink_to_secondary`
   次の手順に進む前に、RLINK が最新の状態であることを確認します。
6. VVR によってセカンダリサイトへのデータのレプリケーションが実行されないように RLINK を切断します。Veritas Enterprise Administrator コンソールで、セカンダリ RVG を右クリックし、［レプリケーションを停止］オプションを選択して、VVR によるセカンダリサイトへのレプリケーションを停止します。
7. RVG からのレプリケータログの関連付けを解除します。Veritas Enterprise Administrator コンソールで、［レプリケータログ］を右クリックし、表示されるメニューから［レプリケータログの関連付けを解除］オプションを選択します。

セカンダリサイトを準備するには

1. タスクバーのスタートメニューで［ファイル名を指定して実行］をクリックして、コマンドウィンドウを開きます。［名前］フィールドに［cmd］と入力し、［OK］をクリックします。
2. **vxprint -IVP** コマンドを実行して、RLINK 名および RVG 名を検索します。`Diskgroup` は *`diskgroup_name`* です。

3 アップグレードの実行中にアプリケーションがボリュームにアクセスしたり、ボリュームを変更したりすることを防ぐために、RVG を停止します。Veritas Enterprise Administrator コンソールで、RVG を右クリックし、表示されるメニューから［データアクセスを無効化］オプションを選択します。

4 RVG からのレプリケータログの関連付けを解除します。Veritas Enterprise Administrator コンソールで、［レプリケータログ］を右クリックし、表示されるメニューから［レプリケータログの関連付けを解除］オプションを選択します。

アップグレード環境に DMP を追加する準備

既存の環境に DMP が含まれておらず、SFW 5.0 にアップグレードする際に追加する場合は、ホストアダプタハードウェアを追加してからアップグレードしてください。SFW にアップグレードして DMP をインストールする前に、新しいホストアダプタからのパスをアレイストレージに接続しないでください。インストーラの実行中に［オプション］画面で［DMP］オプションを選択します。

シマンテック社テクニカルサポートの Web サイト（http://entsupport.symantec.com）で、ハードウェア互換性リストを参照し、SFW で動作が確認されているハードウェアを確認してください。

メモ : DMP ASL と DMP DSM は共存できません。DMP DSM をアンインストールしてから DMP ASL をインストールしてください。

警告 : SFW 5.0 にアップグレードした後、共有ストレージの追加データパスを接続する前に DMP の制御下にアレイを配置します。セカンダリパスが接続された状態で DMP の制御下にないストレージを使用すると、予測不可能なオペレーティングシステムの動作を招き、データが破損する可能性があります。

アップグレードのための既存の DMP 環境の準備

システムに以前から DMP がインストールされている場合は、アレイストレージのプライマリパスだけを残してすべて切断してから、ソフトウェアのアップグレードまたは古いバージョンの Volume Manager のアンインストールを行います。詳しくは次のマニュアルを参照してください。

- 50 ページの「Veritas Dynamic Multi-pathing（DMP）のインストールとアンインストール」
- 『Veritas Storage Foundation and High Availability Solutions 5.0 ソリューションガイド』

アップグレード環境に DMP DSM を追加する準備

既存の環境に DMP DSM が含まれておらず、SFW 5.0 にアップグレードする際に追加する場合は、ホストアダプタハードウェアを追加してからアップグレードしてください。アップグレードのためにインストーラを実行するときに、［オプション］画面で［DMP DSM］オプションを選択します。インストールする前に、マルチパスストレージのパスを 1 つだけ残してすべて切断して、インストール時間を短縮します。

シマンテック社テクニカルサポートの Web サイト（http://entsupport.symantec.com）で、ハードウェア互換性リストを参照し、SFW で動作が確認されているハードウェアを確認してください。

メモ : DMP DSM と DMP ASL は共存できません。DMP ASL をアンインストールしてから DMP DSM をインストールしてください。

SFW 5.0 へのアップグレード

インストーラでは Volume Manager 4.x、SFW 4.1、4.2、4.3 のインストールオプションを SFW 5.0 にアップグレードできます。

ドライバ署名オプションの変更

選択するインストールのオプションによっては、一部のシマンテック社ドライバが署名されない場合があります。Windows Server 2003 が稼働するシステムにインストールする場合は、Windows のドライバ署名オプションを設定し、インストールできるようにする必要があります。

表 3-1 に、無署名ドライバのオプションをインストールする場合の、ローカルまたはリモートシステムでのインストーラの動作を示します。

表 3-1　　無署名ドライバを使用したときのインストール動作

ドライバ署名設定	ローカルシステムでのインストール動作	リモートシステムでのインストール動作
無視	常時許可	常時許可
警告	警告メッセージ。ユーザーの手動操作が必要です。	インストールは続行されます。インストールを完了させるには、リモートシステムにローカルにログオンしてダイアログボックスに応答する必要があります。
ブロック	禁止	禁止

ローカルシステムでは、ドライバ署名オプションを［無視］または［警告］のいずれかに設定します。リモートシステムでは、ユーザーの手動操作なしにインストールを進められるようオプションを［無視］に設定します。

各システムでドライバ署名オプションを変更するには

1. システムにローカルにログオンします。
2. ［コントロールパネル］を開き、［システム］をクリックします。
3. ［ハードウェア］タブをクリックし、［ドライバの署名］をクリックします。
4. ［ドライバ署名オプション］ダイアログボックスで現在の設定を確認し、［無視］または表からインストールを続行できる別のオプションを選択します。
5. ［OK］をクリックします。
6. コンピュータごとに同じ手順を繰り返します。
   ドライバ署名オプションを変更しないと、検証中にそのコンピュータでインストールが失敗します。インストールを完了したら、ドライバ署名オプションをもとの状態に戻します。

ソフトウェアのアップグレード

インストーラを使ってソフトウェアをアップグレードします。

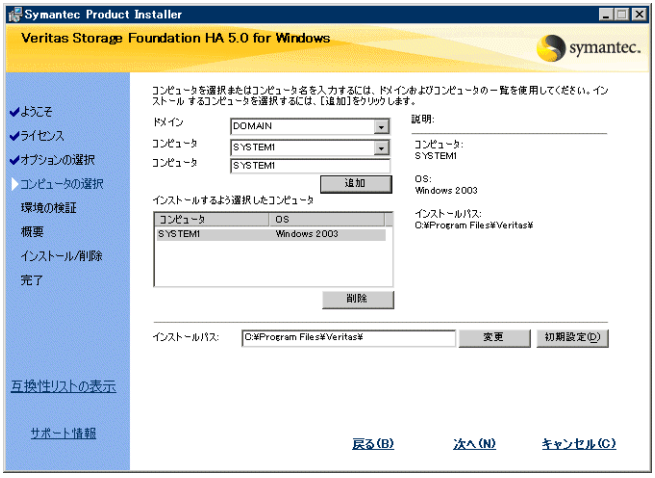
SFW 5.0 にアップグレードするには

1. 自動実行機能でインストールを開始するか、Setup.exe をダブルクリックします。
2. インストール用のデフォルトの言語を選択し、［OK］をクリックします。
3. ［Storage Foundation 5.0 for Windows］をクリックします。
4. ［標準 / カスタム］リンクをクリックします。インストーラがファイルのコピーを開始します。
5. ［ようこそ］画面を確認し、［次へ］をクリックします。
6. 使用許諾契約に目を通します。契約条項に同意する場合は、［使用許諾契約書に同意します。］ラジオボタンを選択して、［次へ］をクリックします。
7. アップグレードまたはインストールするシマンテック社製品オプションそれぞれにライセンスキーを入力します。
   - 一番上のフィールドにライセンスキーを入力します。
   - キーを追加するには、［追加］をクリックします。キーを削除するには、削除するキーをクリックし、［削除］をクリックします。
   - インストールするシマンテック社製品および機能ごとに、初めの 2 つの箇条書きされた手順を繰り返します。キーをクリックして、詳細を確認します。

■ ［次へ］をクリックします。

8 該当するチェックボックスをオンまたはオフにして、インストールするオプションを選択します。現在インストールされているすべてのオプションをアップグレード対象に選択する必要があります。［次へ］をクリックします。画面の下部に、インストールに必要なディスク領域の合計が表示されます。オプションを追加または削除すると、ディスク領域の合計が増減します。

9 アップグレードするドメインとコンピュータを選択し、［次へ］をクリックします。



ドメイン　リストからドメインを選択します。

ドメインとネットワークのサイズ、速度、状況によっては、ドメインとコンピュータのリスト作成に時間がかかる場合があります。

コンピュータ　インストール用のコンピュータを追加するには、［コンピュータ］リストから選択するか、コンピュータ名を［コンピュータ］フィールドに入力します。次に、［追加］をクリックします。

追加したコンピュータを削除するには、［インストールするよう選択したコンピュータ］フィールドで該当するコンピュータ名をクリックし、［削除］をクリックします。

コンピュータ名をクリックすると、詳細が表示されます。

インストールパス	オプションでインストールパスを変更します。 ■ パスを変更するには、［インストールするよう選択したコンピュータ］フィールドでコンピュータを選択し、新しいパスを入力して、［変更］をクリックします。 ■ デフォルトのパスをリストアするには、コンピュータを選択し、［デフォルト］をクリックします。 デフォルトパスは次のとおりです。 C:¥Program Files¥Veritas 64 ビットインストールでのデフォルトパスは次のとおりです。 C:¥Program Files (x86)¥Veritas

10 選択したコンピュータが必要条件を満たしているかどうかが確認され、結果が表示されます。情報を確認し、［次へ］をクリックします。ノードの［インストールの種類］が［アップグレード］として一覧表示されていることに注意してください。エラーが発生した場合は、［詳細］ボックスで説明されている問題を解決し、［環境の再検証］をクリックして、［次へ］をクリックします。

11 Veritas Dynamic Multi-pathing の警告のときは、次のいずれかの処理を行います（該当する場合）。

- DMP ASL のインストールの場合 - データの破損を防ぐために、マルチパスストレージのパスを 1 つだけ残してすべて切断していることを確認します。
- DMP DSM のインストールの場合 - DMP DSM 機能のインストールの所要時間は、インストール時に接続されている物理パスの数によって異なります。この機能のインストール時間を短縮するには、インストール時に接続する物理パスを 1 つだけにします。インストール後は、システムを再ブートする前に、追加の物理パスを再接続します。

［OK］をクリックします。

12 アップグレード前の概略情報を確認し、［インストール］をクリックします。必要に応じて［戻る］をクリックして、必要な変更を行います。

13 すべてのコンピュータでインストールが成功すると、手順 14 で説明する概略ページに自動的に進みます。
インストールに失敗した場合は、［次へ］をクリックしてレポートを表示し、失敗した理由を確認します。インストールを修復するか、アンインストールしてインストールしなおす必要があります。セキュリティのアラートによって、シマンテック社ドライバのソフトウェアを受け入れるかどうかを確認するメッセージが表示されたら、［はい］をクリックします。

14 アップグレードの概要レポートが表示されます。画面を確認し、［次へ］をクリックします。

15 リモートコンピュータを再ブートします。ローカルコンピュータは、この時点では再ブートできません。また、障害が発生したコンピュータはデフォルトでチェックボックスがオフになります。次の手順を順番に実行します。

- アップグレードしたリモートコンピュータを選択します。
- ［再ブート］をクリックします。
- ［次へ］をクリックします。

16 ［完了］をクリックします。

17 ［はい］をクリックして、ローカルコンピュータを再ブートします。

- Volume Replicator（VVR）オプションをアップグレードまたはインストールした場合は、再ブート後に Veritas Volume Replicator Security Service（VxSAS）用のウィザード起動すれば、すべてのコンピュータのセキュリティサービスを設定できます。
  78 ページの「VxSAS サービスの設定（VVR のみ）」を参照してください。
  VVR のこの必要なサービスについて詳しくは『Veritas Storage Foundation 5.0 Veritas Volume Replicator Option 管理者ガイド』を参照してください。
- アップグレード後は、ドライバ署名オプションをもとの状態にリセットします。リセットしないと、システムのセキュリティが損なわれる可能性があります。アップグレードを続ける場合は、アップグレードが完了してからオプションをリセットしてください。
  91 ページの「ドライバ署名オプションをリセットするには」を参照してください。

VxSAS サービスの設定（VVR のみ）

次の手順を実行して、VVR に VxSAS サービスを設定します。

この手順には次の前提条件があります。

- このウィザードを起動するには、サーバーに管理者権限でログオンする必要があります。
- 指定するアカウントには、指定したすべてのホストでの管理者権限と、サービスとしてログオンする権限が必要です。
- 空白のパスワードは指定しないでください。Windows Server 2003 環境では、サービスとしてログオンする権限に対し、空白のパスワードを持つアカウントはサポートされていません。
- VxSAS サービスを設定する必要のあるホストにローカルホストからアクセスできることを確認します。

メモ : SFW または SFW HA をインストールした後、VxSAS ウィザードは自動的には起動しません。VVR Security Service の設定を行うには、このウィザードを手動で起動する必要があります。この必要なサービスの詳細については、『Veritas Storage Foundation Volume Replicator Option 管理者ガイド』を参照してください。

VxSAS サービスを設定するには

1 ウィザードを起動するには、スタートメニューで［すべてのプログラム］、［Symantec］、［Veritas Storage Foundation］、［設定ウィザード］、［VVR Security Service 設定ウィザード］の順に選択するか、必要なマシンのコマンドプロンプトから `vxsascfg.exe` を実行します。
［ようこそ］ページが表示されます。このページには、VxSAS サービスを設定するときに役立つ重要な情報が表示されます。［ようこそ］ページに表示された情報を読み、［次へ］をクリックします。

2 アカウント情報ウィザードのページで次のように入力します。

アカウント名（domain¥account）	［アカウント名］フィールドに管理アカウント名を入力します。
パスワード	パスワードを［パスワード］フィールドで指定します。

RDS の一部にする予定の 1 つのホストに対して、すでに VxSAS サービスを設定している場合は、別のホストで VxSAS サービスを設定するときにも、必ず同じユーザー名とパスワードを指定してください。
必要な情報を入力して、［**次へ**］をクリックします。

3 ドメインの選択ウィザードのページから、設定するホストが所属する必要なドメインを選択します。

ドメインの選択	［利用可能なドメイン］ペインに、Windows のネットワークコンピュータに存在するすべてのドメインが表示されます。 ダブルクリックするか、矢印ボタンを使用して［利用可能なドメイン］ペインから［選択したドメイン］ペインに適切な名前を移動して、必要なドメインを選択します。
ドメインの追加	必要なドメイン名が表示されていない場合は、［ドメインの追加］オプションを使用してそのドメイン名を追加します。オプションを指定するとダイアログが表示され、ドメイン名を指定できます。［追加］をクリックして、名前を［選択したドメイン］リストに追加します。

ドメインを指定してから、［次へ］をクリックします。

4 ［ホストの選択］ページから必要なホストを選択します。

ホストの選択	［利用可能なホスト］ペインに、指定したドメイン内に存在するホストが表示されます。 ダブルクリックするか、矢印ボタンを使用して［利用可能なホスト］リストから［選択したホスト］リストに適切な名前を移動して、必要なホストを選択します。複数のホストを選択するには、Shift キーと上下矢印キーを使用します。
ホストの追加	必要なホスト名が表示されていない場合は、［ホストの追加］を使用してそのホスト名を追加します。［ホストの追加］ダイアログの［ホスト名］フィールドで、必要なホスト名または IP を指定します。［追加］をクリックして、名前を［選択したホスト］リストに追加します。

ホスト名を選択すると、［設定］ボタンが有効になります。［設定］ボタンをクリックして、VxSAS サービスの設定を開始します。

5 設定が完了すると、［設定結果］ページが表示されます。操作が正常に終了した場合は、［状態］カラムに、操作が正常に終了したことを示す適切なメッセージが表示されます。
操作が正常に終了しなかった場合は、ページには状態が失敗と表示され、アカウントの更新が失敗した理由について、該当する詳細情報が表示されます。また、その失敗の考えられる原因と、その失敗に対処する推奨方法も表示されます。
入力した情報を変更する場合は、［戻る］をクリックします。

6 ［完了］をクリックして、ウィザードを終了します。

ドライバ署名オプションのリセット

インストール手順を完了したら、各コンピュータのドライバ署名オプションをリセットします。

ドライバ署名オプションをリセットするには

1 コントロールパネルを開き、［システム］をクリックします。

2 ［ハードウェア］タブをクリックし、［ドライバの署名］をクリックします。

3 ［ドライバ署名オプション］ダイアログボックスで、オプションを［警告］または［ブロック］にリセットします。

4 ［OK］をクリックします。

5 コンピュータごとに同じ手順を繰り返します。

アップグレード後の VVR の再有効化

環境をアップグレードした後に、VVR でプライマリサイトからセカンダリサイトへデータのレプリケーションを行う場合

レプリケーションを開始するには、次の手順に従います。

- VVR とクラスタ（VCS または MSCS）が含まれるサイトでは、クラスタ環境で VVR を再有効化する手順を完了する必要があります。
「アップグレード後の、クラスタ環境での VVR の再有効化」を参照してください。
- クラスタ（VCS または MSCS）のないサイトでは、「クラスタのない環境での VVR の再有効化」を参照してください。

アップグレード後の、クラスタ環境での VVR の再有効化

アップグレードを実行した後に、クラスタで VVR を再度有効にします。

VCS Java コンソールから、更新されたオブジェクトを有効にするには

1. プライマリサイトで、RVG サービスグループをオンラインにします。VCS Java コンソールで、RVG サービスグループを右クリックし、［オンライン］メニューオプションを選択します。
2. セカンダリサイトで、RVG サービスグループをオンラインにします。VCS Java コンソールで、RVG サービスグループを右クリックし、［オンライン］メニューオプションを選択します。
3. プライマリサイトで、アプリケーションサービスグループをオンラインにします。VCS Java コンソールで、アプリケーションサービスグループを右クリックし、［オンライン］メニューオプションを選択します。
4. サービスグループをオンラインにしてもアプリケーションが起動しない場合は、必要なタスクを実行してアプリケーションを起動します。このタスクには、環境のオプションに応じて、データベースのマウントやアプリケーションの手動起動などが含まれる場合があります。

コマンドラインから、更新されたオブジェクトを有効にするには

1. タスクバーのスタートメニューで［ファイル名を指定して実行］をクリックして、コマンドウィンドウを開きます。［名前］フィールドに「cmd」と入力し、［OK］をクリックします。
2. プライマリサイトで、hagrp コマンドを実行して RVG サービスグループをオンラインにします。

```
hagrp -online group_name -sys system_name
```

3 セカンダリサイトで、hagrp コマンドを実行して RVG サービスグループをオンラインにします。
hagrp -online group_name -sys system_name

4 プライマリサイトで、hagrp コマンドを実行してアプリケーションサービスグループをオンラインにします。
hagrp -online group_name -sys system_name

5 サービスグループをオンラインにしてもアプリケーションが起動しない場合は、必要なタスクを実行してアプリケーションを起動します。このタスクには、環境のオプションに応じて、データベースのマウントやアプリケーションの手動起動などが含まれる場合があります。

クラスタのない環境での VVR の再有効化

VEA から、更新されたオブジェクトを有効にするには

1 プライマリ RVG を選択して右クリックし、メニューから［データアクセスの有効化］オプションを選択します。

2 セカンダリ RVG を選択して右クリックし、メニューから［データアクセスの有効化］オプションを選択します。

3 必要に応じて必要なタスクを実行し、アプリケーションを起動します。このタスクには、環境のオプションに応じて、データベースのマウントやアプリケーションの手動起動などが含まれる場合があります。

コマンドラインから、更新されたオブジェクトを有効にするには

1 タスクバーのスタートメニューで［ファイル名を指定して実行］をクリックして、コマンドウィンドウを開きます。［名前］フィールドに「cmd」と入力し、［OK］をクリックします。

2 セカンダリサイトで、vxrvg コマンドを使い、RVG 下のボリュームへのアクセスを有効にします。
vxrvg -g *diskgroup* **start rvg_name**

3 プライマリサイトで、vxrvg コマンドを使い、RVG 下のボリュームへのアクセスを有効にします。
vxrvg -g *diskgroup* **start rvg_name**

4 必要に応じて必要なタスクを実行し、アプリケーションを起動します。このタスクには、環境のオプションに応じて、データベースのマウントやアプリケーションの手動起動などが含まれる場合があります。

アップグレード後の DMP の再有効化

DMP をインストールし、設定プロセスの最後でストレージアレイが DMP の下に含まれるまでは、ストレージの 2 番目のパス（SAN に接続された各サーバー上の 2 番目のホストバスアダプタ）を接続しないでください。DMP 制御なしにストレージのパスが 2 つ存在すると、データが破損する可能性があります。

警告 : アップグレードする前に、データをバックアップしてください。

各デュアルパスアレイに対する DMP 保護をリストアするには

Veritas Enterprise Administrator で、マルチパス構成にするアレイを DMP の管理下に置きます。

1. ツリービューの［ディスク］フォルダで、ストレージアレイのディスクを選択します。
2. 右ペインで、そのディスクの［パス］タブをクリックします。ディスクはまだ DMP の制御下にはないため、［パス］タブには 1 つのパスのみ表示されます。
3. パスを右クリックし、［アレイ設定］を選択します。
4. ［アレイ設定］ウィンドウで、［DMP を無効にする］のチェックマークをはずします。
5. インストール前に取り外したパスをすべて物理的に接続し直します。
6. ディスクを再スキャンします。

ダイナミックディスクグループのアップグレード

以前のインストールに Volume Manager 4.x が含まれる場合、最新のプログラムの機能を使用できるようにディスクグループの種類をアップグレードしてください。

『Veritas Storage Foundation 5.0 管理者ガイド』を参照してください。

メモ : ディスクグループを SFW 5.0 にアップグレードする場合、それ以前のバージョンの Volume Manager またはディスクの管理を実行中の別のサーバーにそのディスクグループをインポートすることはできません。ディスクグループをアップグレードした後、そのグループを以前のバージョンに戻すことはできません。

ダイナミックディスクグループバージョンをアップグレードするには

1 ツリービューでアップグレードするディスクグループを右クリックし、［ダイナミックディスクグループバージョンのアップグレード］を選択します。

2 ［はい］をクリックしてダイナミックディスクグループをアップグレードします。

以前のバージョンの Volume Manager for Windows 2000 または Volume Manager for Windows NT では、Volume Manager 3.0 の制限である 18 文字を超えるダイナミックディスクグループ名を付けることができました。このようなディスクグループのダイナミックグループバージョンをアップグレードする場合は、名前を短縮する必要があります。また、ディスクグループのボリュームが長い名前を持つ場合も、18 文字より短い名前を付ける必要があります。

MSCS 環境でのアップグレード

MSCS 環境では、VM 4.x、SFW 4.1 から SFW 5.0 にアップグレードすることができます。この項の説明は、これらのアップグレードのすべてに適用できます。

VM 4.x からのアップグレード、または Microsoft Cluster Server（MSCS）を使用した SFW 4.1 から SFW へのアップグレードを行う場合は、再ブートが必要です。アクティブなクラスタノードを再ブートすると、そのノードがフェールオーバーします。これを防ぐには、ローリングインストールを使用します。ローリングインストールでは、非アクティブなクラスタノードで最初にアップグレードしてから、アクティブなクラスタノードをセカンドノードに切り替えて、最初のノードをアップグレードします。

既存の設定で、DMP がインストールされ、設定されている場合、SFW 5.0 へのアップグレードの前後に追加手順を実行する必要があります。

既存の設定で、VVR がインストールされ、設定されている場合、SFW 5.0 にアップグレードするための追加手順はありません。

DMP およびオペレーティングシステムのアップグレード手順はオプションであるため、使用環境に適用されない場合もあります。

この項では、クラスタ内の 2 つのノードを Node A と Node B とします。最初は、Node A は非アクティブなクラスタノードで、Node B はアクティブなクラスタノードです。次のアップグレード手順が完了すると、Node A はアクティブなクラスタノードになります。Cluster Administrator コンソールを使用して、アップグレードが完了した後で Node B をアクティブなクラスタノードにすることができます。

MSCS の設定で VM 4.x、SFW 4.1 から SFW 4.3 MP1 の各バージョンから SFW 5.0 にアップグレードするには

1. Node A について、DMP がインストールされている場合は、86 ページの「Node B でのアップグレードのための既存の DMP 環境の準備（Node B がアクティブ）」に記載されたアップグレード開始前の手順に従います。
2. Node A について、SFW 5.0 にアップグレードします。
   87 ページの「Node A での SFW 5.0 へのアップグレード（Node B がアクティブ）」を参照してください。
3. Node A について、DMP がインストールされている場合は、91 ページの「Node A でのアップグレード後の DMP 再有効化（Node B がアクティブ）」に記載されたアップグレード完了後の手順に従います。
4. アクティブなノードを移動します。
   92 ページの「Node A のアクティブ化」を参照してください。
5. Node B について、DMP がインストールされている場合は、92 ページの「Node B でのアップグレードのための既存の DMP 環境の準備（Node A がアクティブ）」に記載されたアップグレード開始前の手順に従います。
6. Node B について、SFW 5.0 にアップグレードします。
   92 ページの「Node B での SFW 5.0 のアップグレード（Node A がアクティブ）」を参照してください。
7. DMP がインストールされている場合、93 ページの「Node B でのアップグレード後の DMP 再有効化（Node A がアクティブ）」に記載されたアップグレード完了後の手順に従います。
8. ダイナミックディスクグループをアップグレードする場合は、93 ページの「ダイナミックディスクグループのアップグレード（Node A がアクティブ）」を参照してください。

Node B でのアップグレードのための既存の DMP 環境の準備（Node B がアクティブ）

このプロセスの前に、クラスタのアクティブなノードが Node B であることを確認します。

警告 : アップグレードまたはアンインストールの前に、アレイに対する DMP 制御下のパスをシングルパスにしないと、データが破損する可能性があります。

DMP 下のパスをシングルパスにするには

1. VEA コンソールを開きます。
2. 各マルチパスアレイからパスを 1 つだけ残して、すべて物理的に取り外します。
3. 無効化するアレイの［アレイ設定］画面を表示します。
4. ツリービューの［ディスク］フォルダで、ストレージアレイのディスクを選択します。
5. 右ペインで、そのディスクの［パス］タブをクリックします。
6. パスを右クリックし、表示されたパスのコンテキストメニューから［アレイ設定］を選択します。
7. ［アレイ設定］ウィンドウで、［DMP を無効にする］のチェックマークを付けます。
8. ［OK］をクリックします。これにより、アレイに対する DMP 制御が無効化されます。
9. VEA のメニューバーで［アクション］、［再スキャン］の順に選択します。Veritas Storage Foundation for Windows によりアレイが再スキャンされ、表示が更新されます。

アレイに対する DMP 制御を無効化すると、［パス］タブに表示されるパスの状態は更新されません。このため、アレイを無効化した後にパスで障害が発生しても、［パス］タブには［正常］と表示される場合があります。

Node A での SFW 5.0 へのアップグレード（Node B がアクティブ）

アップグレードを開始する前に、次のタスクを行います。

- クラスタのアクティブなノードが Node B であることを確認します。
- 警告メッセージを無視するように Windows のドライバ署名オプションを設定します。

ドライバ署名オプションの変更

選択するインストールのオプションによっては、一部のシマンテック社ドライバが署名されない場合があります。Windows Server 2003 が稼働するシステムにインストールする場合は、Windows のドライバ署名オプションを設定し、インストールできるようにする必要があります。

表 3-1 に、無署名ドライバのオプションをインストールする場合の、ローカルまたはリモートシステムでのインストーラの動作を示します。

表 3-2　　無署名ドライバを使用したときのインストール動作

ドライバ署名設定	ローカルシステムでのインストール動作	リモートシステムでのインストール動作
無視	常時許可	常時許可
警告	警告メッセージ。ユーザーの手動操作が必要です。	インストールは続行されます。インストールを完了させるには、リモートシステムにローカルにログオンしてダイアログボックスに応答する必要があります。
ブロック	禁止	禁止

ローカルシステムでは、ドライバ署名オプションを［無視］または［警告］のいずれかに設定します。リモートシステムでは、ユーザーの手動操作なしにインストールを進められるようオプションを［無視］に設定します。

各システムでドライバ署名オプションを変更するには

1. システムにローカルにログオンします。
2. ［コントロールパネル］を開き、［システム］をクリックします。
3. ［ハードウェア］タブをクリックし、［ドライバの署名］をクリックします。
4. ［ドライバ署名オプション］ダイアログボックスで現在の設定を確認し、［無視］または表からインストールを続行できる別のオプションを選択します。
5. ［OK］をクリックします。

6 コンピュータごとに同じ手順を繰り返します。
ドライバ署名オプションを変更しないと、検証中にそのコンピュータでインストールが失敗します。インストールを完了したら、ドライバ署名オプションをもとの状態に戻します。

ソフトウェアのインストール

インストーラを使ってソフトウェアをインストールします。

Node A で SFW 5.0 をインストールするには

1 CD のルートディレクトリに移動して、Setup.exe をダブルクリックします。

2 ［Storage Foundation 5.0 for Windows］をクリックします。

3 ［標準 / カスタム］をクリックして、サーバーコンポーネントとオプションのクライアントコンポーネントをアップグレードします。

4 ［ようこそ］ページで、［次へ］をクリックします。

5 使用許諾契約書に同意する場合は、［次へ］をクリックします。

6 ライセンスキーを入力し、［追加］をクリックします。ライセンスキーのリストからキーを削除するには、削除するキーをクリックして、［削除］をクリックします。

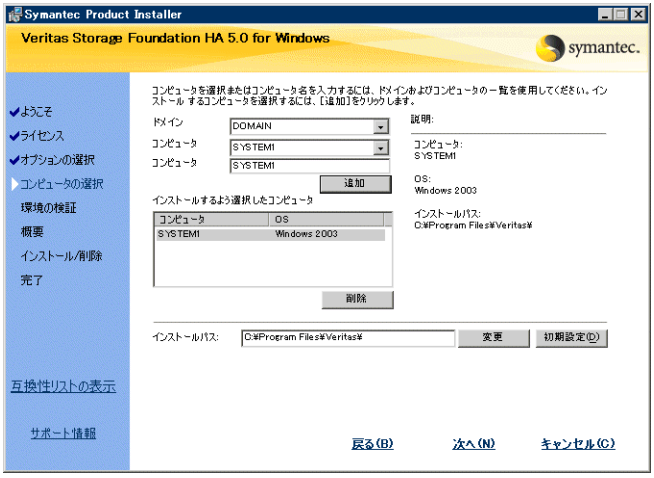
7 アップグレードする製品ごとにシマンテックライセンスを取得していることを確認します。キーのリストからキーを選択して、指定したライセンスの詳細を表示します。

8 ［次へ］をクリックします。

9 MSCS オプションと他の適切なオプション（DMP など）を選択します。［次へ］をクリックします。

10 クライアントコンポーネントをインストールするオプションを選択し、［次へ］をクリックします。

11 アップグレードするドメインとコンピュータを選択し、［次へ］をクリックします。



ドメイン
: リストからドメインを選択します。

ドメインとネットワークのサイズ、速度、状況によっては、ドメインとコンピュータのリスト作成に時間がかかる場合があります。

コンピュータ
: インストール用のコンピュータを追加するには、［コンピュータ］リストから選択するか、コンピュータ名を［コンピュータ］フィールドに入力します。次に、［追加］をクリックします。

追加したコンピュータを削除するには、［インストールするよう選択したコンピュータ］フィールドで該当するコンピュータ名をクリックし、［削除］をクリックします。

コンピュータ名をクリックすると、詳細が表示されます。

インストールパス	オプションでインストールパスを変更します。 ■ パスを変更するには、［インストールするよう選択したコンピュータ］フィールドでコンピュータを選択し、新しいパスを入力して、［変更］をクリックします。 ■ デフォルトのパスをリストアするには、コンピュータを選択し、［デフォルト］をクリックします。 デフォルトパスは次のとおりです。 C:¥Program Files¥Veritas 64 ビットインストールでのデフォルトパスは次のとおりです。 C:¥Program Files (x86)¥Veritas

12 インストール用のシステムが検証された後、［次へ］をクリックします。
エラーが発生した場合は、［詳細］ボックスで説明されている問題を解決し、［環境の再検証］をクリックして、［次へ］をクリックします。

13 ダイナミッククォーラム用の調停時間の設定が最適になるように［OK］をクリックします。
最小時間および最大時間の設定により、MSCS でクォーラムの調停に使用できる時間を定義します。クォーラムの調停は、クラスタの制御ノードがアクティブではなくなり、クラスタの他のノードがクォーラムリソースとクラスタの制御を獲得しようとする場合に行われるプロセスです。

14 概略情報を確認し、［インストール］をクリックします。必要に応じて［戻る］をクリックして、必要な変更を行います。

15 進行状況インジケータは、インストールの状況を示します。セキュリティのアラートによって、シマンテック社ドライバのソフトウェアを受け入れるかどうかを確認するメッセージが表示されたら、［はい］をクリックします。
システムでインストールが正常に終了すると、［インストールレポート］画面が表示されます。
いずれかのシステムでインストールが正常に終了しなかった場合は、状態画面にインストールが失敗したことが表示されます。［次へ］をクリックして、インストールレポートを表示します。

16 レポートを確認して、［次へ］をクリックします。

17 ［完了］をクリックします。

18 ローカルノードを再ブートします。
アップグレード後は、ドライバ署名オプションをもとの状態にリセットします。リセットしないと、システムのセキュリティが損なわれる可能性があります。アップグレードを続ける場合は、アップグレードが完了してからオプションをリセットしてください。

ドライバ署名オプションをリセットするには

インストール手順を完了したら、各コンピュータのドライバ署名オプションをリセットします。

ドライバ署名オプションをリセットするには

1 コントロールパネルを開き、[システム] をクリックします。

2 [ハードウェア] タブをクリックし、[ドライバの署名] をクリックします。

3 [ドライバ署名オプション] ダイアログボックスで、オプションを [警告] または [ブロック] にリセットします。

4 [OK] をクリックします。

5 コンピュータごとに同じ手順を繰り返します。

Node A でのアップグレード後の DMP 再有効化（Node B がアクティブ）

このタスクの前に、クラスタのアクティブなノードが Node B にあることを確認します。

警告 : アップグレードする前に、データをバックアップしてください。

DMP をインストールし、設定プロセスの最後でストレージアレイが DMP の下に含まれるまでは、ストレージの 2 番目のパス（SAN に接続された各サーバー上の 2 番目のホストバスアダプタ）を接続しないでください。DMP 制御なしにストレージのパスが 2 つ存在すると、データが破損する可能性があります。

各デュアルパスアレイに対する DMP（Dynamic Multi-pathing）保護をリストアするには

1 ストレージアレイのツリービューの [アレイ設定] 画面で、[ディスク] フォルダのストレージアレイからディスクを選択します。

2 右ペインで、そのディスクの [パス] タブをクリックします。ディスクはまだ DMP の制御下にはないため、[パス] タブには 1 つのパスのみ表示されます。

3 パスを右クリックし、[アレイ設定] を選択します。

4 [アレイ設定] ウィンドウで、[DMP を無効にする] のチェックマークをはずします。

5 インストール前に取り外したパスをすべて物理的に接続し直します。

6 ディスクを再スキャンします。
50 ページの「Veritas Dynamic Multi-pathing（DMP）のインストールとアンインストール」を参照してください。

『Veritas Storage Foundation and High Availability Solutions 5.0 ソリューションガイド』を参照してください。

DMP のレジストリ設定を再度適用するには（Windows Server 2003 にアップグレードする場合）

既に次に保存しておいた VM 4.x、SFW 4.1 DMP のレジストリ設定を再度適用します。

```
HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥VXD
MPEMC
¥Tunable
```

Node A のアクティブ化

次の手順に従って Node A をアクティブなノードにします。

Node A をアクティブなノードにするには

1. Cluster Administrator コンソールから［Cluster Group］に移動します。
2. ［Cluster Group］を右クリックし、［グループの移動］をクリックします。この手順により、リソースは移動し、リソースの所有権は Node A になります。

Node B でのアップグレードのための既存の DMP 環境の準備（Node A がアクティブ）

このタスクの前に、クラスタのアクティブなノードが Node A であることを確認します。

Node B に対して既存の DMP 環境を準備するには、86 ページの「Node B でのアップグレードのための既存の DMP 環境の準備（Node B がアクティブ）」にある Node A 用のガイドラインを参照してください。

Node B での SFW 5.0 のアップグレード（Node A がアクティブ）

このタスクの前に、クラスタのアクティブなノードが Node A であることを確認します。

Node B で SFW 5.0 をアップグレードするには、87 ページの「Node A での SFW 5.0 へのアップグレード（Node B がアクティブ）」にある Node A 用のガイドラインを参照してください。

Node B でのアップグレード後の DMP 再有効化（Node A がアクティブ）

このタスクの前に、クラスタのアクティブなノードが Node A であることを確認します。

Node B でのアップグレード後に DMP を再有効化するには、91 ページの「Node A でのアップグレード後の DMP 再有効化（Node B がアクティブ）」にある Node A 用のガイドラインを参照してください。

ダイナミックディスクグループのアップグレード（Node A がアクティブ）

このタスクの前に、クラスタのアクティブなノードが Node A であることを確認します。

以前のインストールに Volume Manager 4.x 以降が含まれる場合、最新のプログラムの機能を使用できるようにディスクグループの種類をアップグレードしてください。この手順はアクティブなノードで実行する必要があります。

『Veritas Storage Foundation 5.0 管理者ガイド』を参照してください。

メモ : ディスクグループを SFW にアップグレードする場合、それ以前のバージョンの Volume Manager またはディスクの管理を実行中の別のサーバーにそのディスクグループをインポートすることはできません。ディスクグループをアップグレードした後、そのグループを以前のバージョンに戻すことはできません。

ダイナミックディスクグループバージョンをアップグレードするには

1. アクティブなノードの SFW 5.0 のツリービューで、アップグレードするディスクグループを右クリックし、［ダイナミックディスクグループバージョンのアップグレード］を選択します。
2. ［はい］をクリックしてダイナミックディスクグループをアップグレードします。
   以前のバージョンの Volume Manager for Windows 2000 または Volume Manager for Windows NT では、Volume Manager 3.0 の制限である 18 文字を超えるダイナミックディスクグループ名を付けることができました。このようなディスクグループのダイナミックグループバージョンをアップグレードする場合は、名前を短縮する必要があります。また、ディスクグループのボリュームが長い名前を持つ場合も、18 文字より短い名前を付ける必要があります。

4

SFW HA 5.0 へのアップグレード

この章では、以前のバージョンの Veritas 製品から Veritas Storage Foundation HA 5.0 for Windows（SFW HA 5.0）へのアップグレードについて説明します。

この章では、次のトピックについて説明します。

SFW HA 5.0 にアップグレードする前に

アップグレードする前に、システムが最小限の製品バージョンを満たしていることを確認する必要があります。アップグレードの準備を行う必要もあります。

警告 : SFW 4.x Rule Manager を使用して作成したルールは自動的にアップグレードされず、SFW 5.0 では機能しません。詳しくは http://entsupport.symantec.com/docs/285845 を参照してください。

Microsoft Exchange、Microsoft SQL Server、Oracle 環境での SFW HA のアップグレードについて詳しくは、シマンテック社テクニカルサポートの Web サイトを参照してください。

Microsoft Exchange 環境での SFW HA のアップグレードについての追加情報は、http://entsupport.symantec.com/docs/286178 を参照してください。

Microsoft SQL Server 環境での SFW HA のアップグレードについての追加情報は、http://entsupport.symantec.com/docs/286179 を参照してください。

Oracle 環境での SFW HA のアップグレードについての追加情報は、http://entsupport.symantec.com/docs/286182 を参照してください。

サポートされる最小限の製品バージョンの確認

SFW HA 5.0 にアップグレードするには、既にシステムにバージョン 4.1 以降の SFW または SFW HA をインストールしている必要があります。以前にインストールされた製品は、最小限の製品バージョンを満たす必要があります。アップグレード前に、インストーラによって、最小限の製品バージョンを満たしているかどうかが確認されます。

インストーラが必要とする最小限のレベルを現在のインストールが満たしていない場合は、手動で適切な製品アップグレードを行って必要なレベルを満たしてから、インストーラを使用することをお勧めします。製品の中間バージョンは、シマンテック社のサポート Web サイトからダウンロードできます。ライセンスの取得については、ご購入先にお問い合わせください。以前のバージョンをアンインストールしてから新しい製品をインストールする方法もあります。

アップグレードの準備

製品をアップグレードするには、次のタスクを行ってください。

- すべてのデータを安全な場所にバックアップする。
- システム状態をバックアップする。
- ソフトウェアをアップグレードするためのハードウェア必要条件を確認する。
- アップグレードしたソフトウェアをサポートするために、Microsoft Active Directory を更新する必要があるかどうかを確認する。たとえば、Microsoft Exchange 2000 を Exchange 2003 にアップグレードする場合は、Active Directory を更新する必要があります。
- 各製品のアップグレード後にシステムをテストする（特に、最小限の必要なバージョンにするために製品アップグレードを適用した後）。差分アップグレードにより、トラブルシューティングが容易になります。

VCS の場合のアップグレードに関する追加情報

インストーラは、設定のアップグレード中に次のタスクを実行します。

- VCS 4.x の設定での属性の種類と名前を、SFW HA 5.0 の設定と互換性のあるものに置き換えます。たとえば、Exchange の Application Agent 属性 E2kService は ExchService にアップグレードされます。
- VCS 4.x の設定のデフォルト属性値を、VCS 5.0 の設定のデフォルト属性値にマップします。
- SFW HA 5.0 で不要になった属性を削除します。たとえば、AgentDebug 属性が削除されます。

- ユーザーパスワードを更新します。SFW HA 5.0 では異なる暗号化機構が使用されているため、パスワードは解読されて、VCS 5.0 の暗号化機構を使用して再暗号化されます。

日本語版パッケージアップグレード情報

前のバージョンの日本語言語パッケージをアップグレードするには、次のタスクが必要です。

- これから説明する手順に従い、英語版ディスクを使用して SFW HA 5.0 に完全にアップグレードします。
- 日本語版ディスクを使用して、SFW HA 5.0 の日本語バージョンにアップグレードします。

以前の 4.x バージョンからのアップグレード

この項では、SFW 4.1、4.2 または SFW HA 4.1、4.2、4.3、4.3 MP1 からのアップグレードについて説明します。VVR または DMP がすでにインストールされ、設定されている場合、SFW 5.0 へのアップグレードの前後に追加手順を実行する必要があります。

次の VVR と DMP のアップグレード手順はオプションであるため、使用環境に適用されない場合もあります。

- 98 ページの「アップグレードのための VVR 環境の準備」
- 99 ページの「アップグレード環境に DMP を追加する準備」または 99 ページの「アップグレードのための既存の DMP 環境の準備」
- 100 ページの「アップグレード環境に DMP DSM を追加する準備」
- 101 ページの「SFW HA 5.0 へのアップグレードの準備」
- 102 ページの「SFW HA 5.0 へのアップグレード」
- 109 ページの「VCS アップグレード後のオプションのタスク」
- 112 ページの「アップグレード後の VVR の再有効化」
- 115 ページの「アップグレード後の DMP の再有効化」
- 116 ページの「ダイナミックディスクグループのアップグレード」

アップグレードのための VVR 環境の準備

VVR を使用してプライマリサイトからセカンダリサイトへデータのレプリケーションを行う場合は、次の手順に従って RVG（Replicated Volume Group）を停止し、レプリケーションリンク（RLINK）を切断します。

プライマリサイトを準備するには

1. Cluster Manager を使用して、VVR によりサイト間のデータのレプリケーションを行うアプリケーションをオフラインにします。
2. タスクバーのスタートメニューで［ファイル名を指定して実行］をクリックして、コマンドウィンドウを開きます。［名前］フィールドに「cmd」と入力し、［OK］をクリックします。
3. プライマリサイトで vxprint -lVP コマンドを実行します。`Diskgroup` は *`diskgroup_name`* です。
4. プライマリサイトで次のコマンドを実行して、レプリケータログのデータがセカンダリサイトに書き込まれたことを確認します。
   **`vxrlink [-g`*`diskgroup`*`] status `*`rlink_to_secondary`*
   次の手順に進む前に、RLINK が最新の状態であることを確認します。
5. Cluster Manager を使用して、VVR レプリケーションサービスグループ内の VvrRvg リソースをオフラインにします。
6. VVR によってセカンダリサイトへのデータのレプリケーションが実行されないように RLINK を切断します。Veritas Enterprise Administrator コンソールで、セカンダリ RVG を右クリックし、［レプリケーションを停止］オプションを選択して、VVR によるセカンダリサイトへのレプリケーションを停止します。
7. RVG からのレプリケータログの関連付けを解除します。Veritas Enterprise Administrator コンソールで、［レプリケータログ］を右クリックし、表示されるメニューから［レプリケータログの関連付けを解除］オプションを選択します。

セカンダリサイトを準備するには

1. Cluster Manager を使用して、VVR レプリケーションサービスグループ内の VvrRvg リソースをオフラインにします。
2. タスクバーのスタートメニューで［ファイル名を指定して実行］をクリックして、コマンドウィンドウを開きます。［名前］フィールドに「cmd」と入力し、［OK］をクリックします。
3. セカンダリサイトで vxprint -lVP コマンドを実行します。`Diskgroup` は *`diskgroup_name`* です。

4 RVG からのレプリケータログの関連付けを解除します。Veritas Enterprise Administrator コンソールで、［レプリケータログ］を右クリックし、表示されるメニューから［レプリケータログの関連付けを解除］オプションを選択します。

アップグレード環境に DMP を追加する準備

既存の環境に DMP が含まれておらず、SFW HA 5.0 にアップグレードする際に追加する場合は、ホストアダプタハードウェアを追加してから SFW HA 5.0 ソフトウェアをアップグレードしてください。SFW HA にアップグレードして DMP をインストールする前に、新しいホストアダプタからのパスをアレイストレージに接続しないでください。インストーラの実行中に［オプション］画面で［DMP］オプションを選択します。

シマンテック社テクニカルサポートの Web サイト（http://entsupport.symantec.com）で、ハードウェア互換性リストを参照し、SFW HA で動作が確認されているハードウェアを確認してください。

メモ : DMP ASL と DMP DSM は共存できません。DMP ASL をアンインストールしてから DMP DSM をインストールしてください。

警告 : SFW HA 5.0 へのアップグレードが完了した後、共有ストレージの追加データパスを接続する前に DMP の制御下にアレイを配置してください。セカンダリパスが接続された状態で DMP の制御下にないストレージを使用すると、予測不可能なオペレーティングシステムの動作を招き、データが破損する可能性があります。

アップグレードのための既存の DMP 環境の準備

システムに以前から DMP がインストールされている場合は、アレイストレージのプライマリパスだけを残してすべて切断してから、ソフトウェアのアップグレードまたは古いバージョンの Volume Manager のアンインストールを行います。

マルチパスアレイからプライマリパスだけを残して、すべて物理的に取り外します。VEA コンソールを使って各マルチパスアレイに対する DMP 制御を無効にし、環境を再スキャンします。

警告 : アップグレードまたはアンインストールの前に DMP パスをシングルパスにしないと、データが破損する可能性があります。

DMP 下のパスをシングルパスにするには

1 VEA コンソールを開きます。

2 無効化するアレイの［アレイ設定］画面を表示します。

3 ツリービューの［ディスク］フォルダで、ストレージアレイのディスクを選択します。

4 右ペインで、そのディスクの［パス］タブをクリックします。

5 パスを右クリックし、表示されたパスのコンテキストメニューから［アレイ設定］を選択します。

6 ［アレイ設定］ウィンドウで、［DMP を無効にする］のチェックマークを付けます。

7 ［OK］をクリックします。これにより、アレイに対する DMP 制御が無効化されます。

8 アレイの無効化が VEA により許可されない場合は、プライマリパスがアレイとの間に残された唯一の接続であることを確認してください。

9 VEA のメニューバーで［アクション］、［再スキャン］の順に選択します。アレイが再スキャンされ、表示が更新されます。

DDI パッケージのアンインストール

クラスタ環境のノードから DDI パッケージをアンインストールする前に、クラスタリソースを別のノードに移動する必要があります。

1 DMP DSM が管理する各アレイには、パスが 1 つだけ接続されていることを確認します。

2 Windows の［プログラムの追加と削除］を開き、DDI をアンインストールします。DMP DSM エントリのシマンテックサポートを選択し、［削除］をクリックしてアンインストールを開始します。

3 アンインストールプロセスが完了したら、システムを再ブートします。

アップグレード環境に DMP DSM を追加する準備

既存の環境に DMP DSM が含まれておらず、SFW 5.0 へのアップグレード後にマルチパスを追加する場合は、ホストアダプタハードウェアを追加してからアップグレードしてください。アップグレードのためにインストーラを実行するときに、［オプション］画面で適切な DMP DSM を選択します。インストールする前に、マルチパスストレージのパスを 1 つだけ残してすべて切断して、インストール時間を短縮します。

互換性のあるハードウェアのリストについては、
http://entsupport.symantec.com にあるハードウェア互換性リストを参照してください。

メモ : DMP DSM と DMP ASL は共存できません。DMP ASL をアンインストールしてから DMP DSM をインストールしてください。

SFW HA 5.0 へのアップグレードの準備

アップグレードプロセスを開始する前に、VCS Java コンソールを使用して、VCS 設定を保存して閉じます。この操作により、最新の設定がディスクに保存され、設定の状態が読み取り専用モードに変更されます。また、アップグレードプロセスを開始する前に、VCS を停止することも必要です。VVR プライマリクラスタとセカンダリクラスタの両方で、次の手順を実行します。

設定を保存して閉じるには

VCS Java コンソールで、Cluster Explorer ツールバーの［設定を保存して閉じます］をクリックします。

コマンドプロンプトで、次のコマンドを入力します。

```
C:¥> haconf -dump -makero
```

サービスグループをオフラインにするには

コマンドプロンプトで、次のコマンドを入力します。

```
C:¥> hagrp -offline group_name -sys system_name
```

ここで、*group_name* はサービスグループの名前、*system_name* はグループがオンラインになっているノード名です。

オンラインになっているすべてのサービスグループについて、このコマンドを繰り返します。

VCS サービスを停止するには

1. すべてのクラスタノードで HAD を停止します。次のコマンドを入力します。

   ```
   C:¥> hastop -all -force
   ```

2. すべてのクラスタノードで Veritas VCSComm Startup サービスを停止します。次のコマンドを入力します。

   ```
   C:¥> net stop vcscomm
   ```

3. すべてのクラスタノードで GAB と LLT を停止します。次のコマンドを入力します。

   ```
   C:¥> net stop gab
   C:¥> net stop llt
   ```

SFW HA 5.0 へのアップグレード

インストーラは自動的に Volume Manager 4.x、SFW 4.1 または 4.2、SFW HA 4.1、4.2、4.3 を SFW HA 5.0 にアップグレードします。クラスタに VCS Enterprise Agents とオプションがインストールされている場合は、SFW HA 5.0 にアップグレードするときに同じ Enterprise Agents とオプションを選択してください。アップグレードしたクラスタに Enterprise Agents およびオプションを含めない場合は、次に進む前にクラスタから Enterprise Agents をアンインストールします。

SFW HA のアップグレードは、Windows 2000 または Windows Server 2003 ドメインのサーバーで実行する必要があります。Windows NT 4.0 ドメインはサポートされていません。

ドライバ署名オプションの変更

選択するインストールのオプションによっては、一部のシマンテック社ドライバが署名されない場合があります。Windows Server 2003 が稼働するシステムにインストールする場合は、Windows のドライバ署名オプションを設定し、インストールできるようにする必要があります。

表 4-1 に、無署名ドライバのオプションをインストールする場合の、ローカルまたはリモートシステムでのインストーラの動作を示します。

表 4-1　　無署名ドライバを使用したときのインストール動作

ドライバ署名設定	ローカルシステムでのインストール動作	リモートシステムでのインストール動作
無視	常時許可	常時許可
警告	警告メッセージ。ユーザーの手動操作が必要です。	インストールは続行されます。インストールを完了させるには、リモートシステムにローカルにログオンしてダイアログボックスに応答する必要があります。
ブロック	禁止	禁止

ローカルシステムでは、ドライバ署名オプションを［無視］または［警告］のいずれかに設定します。リモートシステムでは、ユーザーの手動操作なしにインストールを進められるようオプションを［無視］に設定します。

各システムでドライバ署名オプションを変更するには

1　システムにローカルにログオンします。

2　［コントロールパネル］を開き、［システム］をクリックします。

3 ［ハードウェア］タブをクリックし、［ドライバの署名］をクリックします。

4 ［ドライバ署名オプション］ダイアログボックスで現在の設定を確認し、［無視］または表からインストールを続行できる別のオプションを選択します。

5 ［OK］をクリックします。

6 コンピュータごとに同じ手順を繰り返します。
ドライバ署名オプションを変更しないと、検証中にそのコンピュータでインストールが失敗します。インストールを完了したら、ドライバ署名オプションをもとの状態に戻します。

ソフトウェアのアップグレード

インストーラを使ってソフトウェアをアップグレードします。

インストーラを使用して製品をアップグレードするには

1 自動実行機能でインストールを開始するか、Setup.exe をダブルクリックします。

2 インストール用のデフォルトの言語を選択し、［OK］をクリックします。シマンテック社製品の選択画面が表示されます。

3 ［Storage Foundation HA 5.0 for Windows］をクリックします。

4 ［標準 / カスタム］をクリックして、インストールを開始します。［管理コンソール］リンクをクリックすると、クライアントコンポーネントのみをインストールできます。

5 ［ようこそ］ダイアログボックスの説明に目を通してから、［次へ］をクリックします。

6 使用許諾契約書に同意する場合は、［次へ］をクリックします。

7 一番上のフィールドに、アップグレードまたはインストールするシマンテック社製品オプションそれぞれのライセンスキーを入力します。

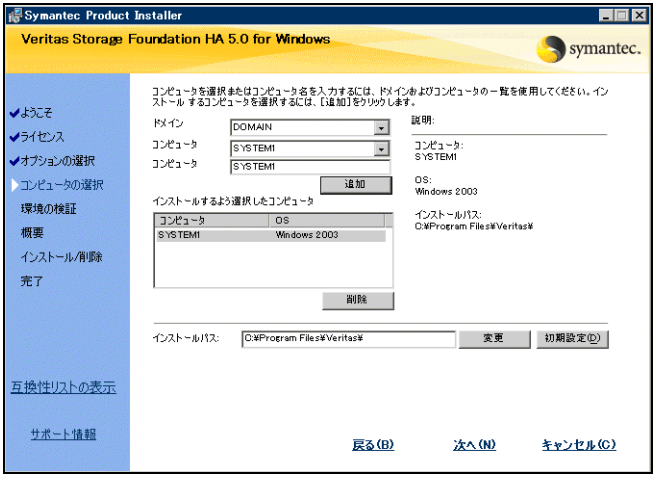
8 キーを追加するには、［追加］をクリックします。
キーを削除するには、削除するキーをクリックし、［削除］をクリックします。

9 インストールするシマンテック社製品および機能ごとに、手順 7 と手順 8 を繰り返します。キーをクリックして、詳細を確認します。

10 ［次へ］をクリックします。

11 適切な Storage Foundation HA オプションを選択し、［次へ］をクリックします。ノードに以前の VCS エージェントとオプションがインストールされている場合は、アップグレードするときに同じエージェントとオプションを選択してください。アップグレードしたクラスタにエージェントとオプションを含めない場合は、処理を進める前にクラスタからそれらをアンインストールします。

12 インストールするドメインとコンピュータを選択し、［次へ］をクリックします。



ドメイン	リストからドメインを選択します。 ドメインとネットワークのサイズ、速度、状況によっては、ドメインとコンピュータのリスト作成に時間がかかる場合があります。
コンピュータ	インストール用のコンピュータを追加するには、[コンピュータ] リストから選択するか、コンピュータ名を [コンピュータ] フィールドに入力します。次に、[追加] をクリックします。 追加したコンピュータを削除するには、[インストールするよう選択したコンピュータ] フィールドで該当するコンピュータ名をクリックし、[削除] をクリックします。 コンピュータ名をクリックすると、詳細が表示されます。
インストールパス	オプションでインストールパスを変更します。 ■ パスを変更するには、[インストールするよう選択したコンピュータ] フィールドでコンピュータを選択し、新しいパスを入力して、[変更] をクリックします。 ■ デフォルトのパスをリストアするには、コンピュータを選択し、[デフォルト] をクリックします。 デフォルトパスは次のとおりです。 C:¥Program Files¥Veritas 64 ビットインストールでのデフォルトパスは次のとおりです。 C:¥Program Files (x86)¥Veritas

13 選択したコンピュータが必要条件を満たしているかどうかが確認され、結果が表示されます。情報を確認し、[次へ] をクリックします。ノードの [インストールの種類] が [アップグレード] として一覧表示されていることに注意してください。エラーが発生した場合は、[詳細] ボックスで説明されている問題を解決し、[環境の再検証] をクリックして、[次へ] をクリックします。

14 Veritas Dynamic Multi-pathing の警告のときは、次のいずれかの処理を行います（該当する場合）。

■ DMP ASL のインストールの場合 - データの破損を防ぐために、マルチパスストレージのパスを 1 つだけ残してすべて切断していることを確認します。

- DMP DSM のインストールの場合 - DMP DSM 機能のインストールの所要時間は、インストール時に接続されている物理パスの数によって異なります。この機能のインストール時間を短縮するには、インストール時に接続する物理パスを 1 つだけにします。インストール後は、システムを再ブートする前に、追加の物理パスを再接続します。

［OK］をクリックします。

15 アップグレード前の概略情報を確認します。必要に応じて［戻る］をクリックして、変更を行います。［インストール］をクリックします。

16 すべてのノードでインストールが成功すると、概略ページに自動的に進みます。
インストールが完了したことが進行状況インジケータに示されたら、［次へ］をクリックして、概略ページに進み、失敗したインストールの詳細を確認します。セキュリティのアラートによって、シマンテック社ドライバのソフトウェアを受け入れるかどうかを確認するメッセージが表示されたら、［はい］をクリックします。

17 インストールレポートを確認し、必要に応じて対処して、［次へ］をクリックします。

18 リモートコンピュータを再ブートします。ローカルコンピュータは、この時点では再ブートできません。また、障害が発生したコンピュータはデフォルトでチェックボックスがオフになります。アップグレードしたリモートコンピュータを選択し、［再ブート］をクリックします。
リモートコンピュータがオンラインに戻るまで待ちます。［次へ］をクリックします。

19 ［完了］をクリックします。

20 ［はい］をクリックして、ローカルノードを再ブートします。

- Volume Replicator（VVR）オプションをアップグレードまたはインストールした場合は、再ブート後に Veritas Volume Replicator Security Service（VxSAS）用のウィザード起動すれば、すべてのノードのセキュリティサービスを設定できます。
107 ページの「VxSAS サービスの設定（VVR のみ）」を参照してください。
- リモート Windows Server 2003 システムのドライバ署名オプションを変更していない場合は、VxSAS の設定を行う必要があります。
107 ページの「VxSAS サービスの設定（VVR のみ）」を参照してください。

VxSAS サービスの設定（VVR のみ）

次の手順を実行して、VVR に VxSAS サービスを設定します。

この手順には次の前提条件があります。

- このウィザードを起動するには、サーバーに管理者権限でログオンする必要があります。
- 指定するアカウントには、指定したすべてのホストでの管理者権限と、サービスとしてログオンする権限が必要です。
- 空白のパスワードは指定しないでください。Windows Server 2003 環境では、サービスとしてログオンする権限に対し、空白のパスワードを持つアカウントはサポートされていません。
- VxSAS サービスを設定する必要のあるホストにローカルホストからアクセスできることを確認します。

メモ : SFW または SFW HA をインストールした後、VxSAS ウィザードは自動的には起動しません。VVR Security Service の設定を行うには、このウィザードを手動で起動する必要があります。この必要なサービスについて詳しくは『Veritas Storage Foundation Volume Replicator Option 管理者ガイド』を参照してください。

VxSAS サービスを設定するには

1. ウィザードを起動するには、スタートメニューで［すべてのプログラム］、［Symantec］、［Veritas Storage Foundation］、［設定ウィザード］、［VVR Security Service 設定ウィザード］の順に選択するか、必要なマシンのコマンドプロンプトから `vxsascfg.exe` を実行します。
   ［ようこそ］ページが表示されます。このページには、VxSAS サービスを設定するときに役立つ重要な情報が表示されます。［ようこそ］ページに表示された情報を読み、［次へ］をクリックします。
2. アカウント情報ウィザードのページで次のように入力します。

アカウント名（domain¥account）	［アカウント名］フィールドに管理アカウント名を入力します。
パスワード	パスワードを［パスワード］フィールドで指定します。

   RDS の一部にする予定の 1 つのホストに対して、すでに VxSAS サービスを設定している場合は、別のホストで VxSAS サービスを設定するときにも、必ず同じユーザー名とパスワードを指定してください。
   必要な情報を入力して、［**次へ**］をクリックします。

3 ドメインの選択ウィザードのページから、設定するホストが所属する必要なドメインを選択します。

ドメインの選択	［利用可能なドメイン］ペインに、Windows のネットワークコンピュータに存在するすべてのドメインが表示されます。 ダブルクリックするか、矢印ボタンを使用して［利用可能なドメイン］ペインから［選択したドメイン］ペインに適切な名前を移動して、必要なドメインを選択します。
ドメインの追加	必要なドメイン名が表示されていない場合は、［ドメインの追加］オプションを使用してそのドメイン名を追加します。オプションを指定するとダイアログが表示され、ドメイン名を指定できます。［追加］をクリックして、名前を［選択したドメイン］リストに追加します。

ドメインを指定してから、［次へ］をクリックします。

4 ［ホストの選択］ページから必要なホストを選択します。

ホストの選択	［利用可能なホスト］ペインに、指定したドメイン内に存在するホストが表示されます。 ダブルクリックするか、矢印ボタンを使用して［利用可能なホスト］リストから［選択したホスト］リストに適切な名前を移動して、必要なホストを選択します。複数のホストを選択するには、Shift キーと上下矢印キーを使用します。
ホストの追加	必要なホスト名が表示されていない場合は、［ホストの追加］を使用してそのホスト名を追加します。［ホストの追加］ダイアログの［ホスト名］フィールドで、必要なホスト名または IP を指定します。［追加］をクリックして、名前を［選択したホスト］リストに追加します。

ホスト名を選択すると、［設定］ボタンが有効になります。［設定］ボタンをクリックして、VxSAS サービスの設定を開始します。

5 設定が完了すると、［設定結果］ページが表示されます。操作が正常に終了した場合は、［状態］カラムに、操作が正常に終了したことを示す適切なメッセージが表示されます。
操作が正常に終了しなかった場合は、ページには状態が失敗と表示され、アカウントの更新が失敗した理由について、該当する詳細情報が表示されます。また、その失敗の考えられる原因と、その失敗に対処する推奨方法も表示されます。
入力した情報を変更する場合は、［戻る］をクリックします。

6 ［完了］をクリックして、ウィザードを終了します。

ドライバ署名オプションのリセット

インストール手順を完了したら、各コンピュータのドライバ署名オプションをリセットします。

ドライバ署名オプションをリセットするには

1 コントロールパネルを開き、［システム］をクリックします。

2 ［ハードウェア］タブをクリックし、［ドライバの署名］をクリックします。

3 ［ドライバ署名オプション］ダイアログボックスで、オプションを［警告］または［ブロック］にリセットします。

4 ［OK］をクリックします。

5 コンピュータごとに同じ手順を繰り返します。

VCS アップグレード後のオプションのタスク

次のタスクは、クラスタ設定によってはオプションです。

アップグレードしたクラスタへのカスタムリソースの組み込み

VCS 設定ウィザードでは、カスタムリソースはアップグレードされません。以前の設定内のサービスグループにカスタムリソースが含まれていても、ウィザードでは、アップグレードしたクラスタにそのサービスグループは組み込まれません。

カスタムリソースが含まれているサービスグループを、アップグレードしたクラスタに組み込むには

1 カスタムエージェント用のエージェントバイナリが *%VCS_HOME%*¥bin に格納されていることを確認します。ここで、変数 *%VCS_HOME%* は VCS のインストールディレクトリであり、通常は C:¥Program Files¥Veritas¥cluster server です。

2 クラスタ内のすべてのノードで VCS エンジン（HAD）を停止します。コマンドプロンプトで、次のコマンドを入力します。
C:¥> **hastop -all -force**

3 SFW HA 5.0 ソフトウェアのインストール時に、以前の設定ファイルがバックアップ場所にコピーされます。バックアップされた types.cf と main.cf ファイルは、C:¥Documents and Settings¥All Users¥Application Data¥Veritas¥cluster server¥vpibackup に保存されます。

4 バックアップされた types.cf からカスタムリソースのリソースタイプ定義をコピーし、それを VCS 5.0 クラスタの types.cf ファイルに追加します。

5 バックアップされた main.cf からカスタムリソースが含まれているサービスグループ設定をコピーし、それを VCS 5.0 クラスタの main.cf ファイルに追加します。

6 カスタムリソースタイプ用のリソースが VCS 5.0 の付属エージェント用のリソースに依存している場合は、VCS 付属エージェントのリソース定義を更新して新しい属性を追加するか、または廃止された属性を削除する必要があります。
新しい属性と廃止された属性について詳しくは『Veritas Storage Foundation and High Availability Solutions 5.0 リリースノート』を参照してください。
属性値とその説明について詳しくは『Veritas Cluster Server 5.0 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。

7 設定を確認します。次のコマンドを入力します。
C:¥> **hacf -verify** *config_directory*
変数 *config_directory* は、main.cf と types.cf が格納されているディレクトリのパスを示します。

8 設定を変更したノードで、VCS エンジン（HAD）を起動します。コマンドプロンプトで、次のコマンドを入力します。
```
C:¥> hastart
```

9 その他のすべてのクラスタノードで、VCS エンジン（HAD）を起動します。

ClusterService グループへの GCO リソースの追加

VCS 5.0 には、広域ディザスタリカバリのために一連の VCS クラスタが連携して動作できるようにするグローバルクラスタオプションが用意されています。『Veritas Cluster Server 5.0 管理者ガイド』を参照してください。

グローバルクラスタ内でのセキュアな通信の確立

グローバルクラスタは、デフォルトでは非セキュアモードで作成されます。ローカルクラスタがセキュアモードで実行されている場合、グローバルクラスタを非セキュアモードで実行し続けることも、クラスタ間のセキュアな通信を確立するように選択することも可能です。

グローバルクラスタ内でセキュアな通信を確立するには、次の前提条件を満たしている必要があります。

- グローバルクラスタ内のクラスタは、セキュアモードで実行されている必要があります。
- ドメイン管理者権限が必要です。

グローバルクラスタにセキュアな通信を追加するには、次の情報が必要です。

- グローバル設定での各クラスタのアクティブホスト名または IP アドレス。
- 設定内での各クラスタの管理者のユーザー名とパスワード。
- ローカルクラスタが同じルートブローカーを指していない場合、各ルートブローカーのホスト名とポートアドレス。

セキュアな通信を追加するには、次のタスクを実行します。

- ClusterService グループの ClusterService-Proc（wac）リソースを、グローバル環境のクラスタ上でオフラインにします。
- -secure オプションを各ノードの StartProgram 属性に追加します。
- ローカルクラスタが同じルートブローカーを指していない場合は、ルートブローカー間に信頼関係を確立します。
- グローバルクラスタのクラスタ上で ClusterService-Proc（wac）リソースをオンラインにします。

ClusterService-Proc（wac）リソースをすべてのクラスタ上でオフラインにするには

1. Cluster Monitor で、グローバルクラスタ内のクラスタにログオンします。
2. Cluster Explorer 設定ツリーの［サービスグループ］タブで［ClusterService］グループと［プロセス］エージェントを展開します。
3. ［ClusterService-Proc］リソースを右クリックし、［オフライン］をクリックして、メニューから適切なシステムをクリックします。
4. グローバルクラスタの追加クラスタそれぞれで、手順 1 から手順 3 を繰り返します。

-secure オプションを StartProgram リソースに追加するには

1. Cluster Explorer 設定ツリーの［サービスグループ］タブで、［ClusterService］グループの［プロセス］タイプの下にある［ClusterService-Proc］リソースを右クリックします。
2. ［ビュー］をクリックしてから［プロパティ］ビューをクリックします。
3. ［編集］アイコンをクリックし、StartProgram 属性を編集します。
4. ［属性の編集］ダイアログボックスで、実行可能なスカラー値のパスに -secure スイッチを追加します。例：
   `C:¥Program Files¥Veritas¥Cluster Server¥bin¥wac.exe -secure`
5. クラスタ内の各システムで手順 4 を繰り返します。
6. ［OK］をクリックして［属性の編集］ダイアログボックスを閉じます。
7. ツールバーの［設定を保存して閉じます］アイコンをクリックします。

8 グローバルクラスタ内の各クラスタで手順 1 から手順 7 を繰り返します。

1 つ以上のルートブローカーがある場合に、ルートブローカー間に信頼関係を確立するには

- ローカルクラスタが同じルートブローカーを指していない場合にのみ、ルートブローカー間に信頼関係を確立する必要があります。
  各クラスタのルートブローカーにログオンし、グローバルクラスタ内の他のルートブローカーへの信頼関係を設定します。コマンドの完全な構文は次のとおりです。
  vssat setuptrust --broker *<host:port>* --securitylevel <low|medium|high> [--hashfile *<filename>* | --hash *<root hash in hex>*]
  たとえば、RB1 を指す Cluster1 と RB2 を指す Cluster2 で構成されているグローバルクラスタ内で低セキュリティレベルの信頼関係を確立するには
  RB1 から次を入力します。
  vssat setuptrust --broker RB2:14141 --securitylevel low
  RB2 から次を入力します。
  vssat setuptrust --broker RB1:14141 --securitylevel low

すべてのクラスタ上で ClusterService-Proc（wac）リソースをオンラインにするには

1 Cluster Explorer 設定ツリーの［サービスグループ］タブで［ClusterService］グループと［プロセス］エージェントを展開します。

2 ［ClusterService-Proc］リソースを右クリックし、［オンライン］をクリックして、メニューから適切なシステムをクリックします。

3 グローバルクラスタの追加クラスタそれぞれで、手順 1 と手順 2 を繰り返します。

アップグレード後の VVR の再有効化

VVR を使ってプライマリサイトからセカンダリサイトへデータのレプリケーションが行われる環境をアップグレードした後、次の手順に従ってレプリケーションを開始します。

- VVR とクラスタ（VCS または MSCS）が含まれるサイトでは、クラスタを準備する前に、「アップグレード後の、クラスタ環境での VVR の再有効化」に記載された手順を完了します。
- クラスタ（VCS または MSCS）のないサイトでは、「クラスタのない環境での VVR の再有効化」に進みます。

アップグレード後の、クラスタ環境での VVR の再有効化

VCS Java コンソールから、更新されたオブジェクトを有効にするには

1. プライマリサイトで、RVG サービスグループをオンラインにします。VCS Java コンソールで、RVG サービスグループを右クリックし、[オンライン] メニューオプションを選択します。
2. セカンダリサイトで、RVG サービスグループをオンラインにします。VCS Java コンソールで、RVG サービスグループを右クリックし、[オンライン] メニューオプションを選択します。
3. プライマリサイトで、アプリケーションサービスグループをオンラインにします。VCS Java コンソールで、アプリケーションサービスグループを右クリックし、[オンライン] メニューオプションを選択します。
4. サービスグループをオンラインにしてもアプリケーションが起動しない場合は、必要なタスクを実行してアプリケーションを起動します。このタスクには、環境のオプションに応じて、データベースのマウントやアプリケーションの手動起動などが含まれる場合があります。

コマンドラインから、更新されたオブジェクトを有効にするには

1. タスクバーのスタートメニューで [ファイル名を指定して実行] をクリックして、コマンドウィンドウを開きます。[名前] フィールドに「cmd」と入力し、[OK] をクリックします。
2. プライマリサイトで、hagrp コマンドを実行して RVG サービスグループをオンラインにします。
   hagrp -online group_name -sys system_name
3. セカンダリサイトで、hagrp コマンドを実行して RVG サービスグループをオンラインにします。
   hagrp -online group_name -sys system_name
4. プライマリサイトで、hagrp コマンドを実行してアプリケーションサービスグループをオンラインにします。
   hagrp -online group_name -sys system_name
5. サービスグループをオンラインにしてもアプリケーションが起動しない場合は、必要なタスクを実行してアプリケーションを起動します。このタスクには、環境のオプションに応じて、データベースのマウントやアプリケーションの手動起動などが含まれる場合があります。

クラスタのない環境での VVR の再有効化

VEA から、更新されたオブジェクトを有効にするには

1. プライマリ RVG を選択して右クリックし、メニューから［データアクセスの有効化］オプションを選択します。
2. セカンダリ RVG を選択して右クリックし、メニューから［データアクセスの有効化］オプションを選択します。
3. 必要に応じて必要なタスクを実行し、アプリケーションを起動します。このタスクには、環境のオプションに応じて、データベースのマウントやアプリケーションの手動起動などが含まれる場合があります。

コマンドラインから、更新されたオブジェクトを有効にするには

1. タスクバーのスタートメニューで［ファイル名を指定して実行］をクリックして、コマンドウィンドウを開きます。［名前］フィールドに「cmd」と入力し、［OK］をクリックします。
2. セカンダリサイトで、vxrvg コマンドを使い、RVG 下のボリュームへのアクセスを有効にします。
   vxrvg -g *diskgroup* **start rvg_name**
3. プライマリサイトで、vxrvg コマンドを使い、RVG 下のボリュームへのアクセスを有効にします。
   vxrvg -g *diskgroup* **start rvg_name**
   必要に応じて必要なタスクを実行し、アプリケーションを起動します。このタスクには、環境のオプションに応じて、データベースのマウントやアプリケーションの手動起動などが含まれる場合があります。

アップグレード後の DMP DSM パスの再接続

SFW HA のアップグレードが完了したら、DMP DSM アレイへのすべてのパスを再接続します。

アップグレード後の DMP の再有効化

DMP をインストールし、設定プロセスの最後でストレージアレイが DMP の下に含まれるまでは、ストレージの 2 番目のパス（SAN に接続された各サーバー上の 2 番目のホストバスアダプタ）を接続しないでください。DMP 制御なしにストレージのパスが 2 つ存在すると、データが破損する可能性があります。

警告 : 手順を進める前に、データをバックアップしてください。

アップグレード後に DMP を再有効化するには

最初のサーバーの SFW HA で、DMP を起動してストレージアレイのディスクを DMP の制御下に追加します。ストレージアレイを DMP の制御下に追加するには、次の手順を実行します。

1. Veritas Enterprise Administrator で、次の手順に従いストレージアレイの［アレイ設定］画面を表示します。
   - ツリービューの［ディスク］フォルダで、ストレージアレイのディスクを選択します。
   - 右ペインで、そのディスクの［パス］タブをクリックします。ディスクはまだ DMP の制御下にはないため、［パス］タブには 1 つのパスのみ表示されます。
   - パスを右クリックし、［アレイ設定］を選択します。
2. ［アレイ設定］ウィンドウで、［DMP を無効にする］のチェックマークをはずします。
3. 適切なケーブルを使用して、サーバーの 2 番目のパスを 2 番目のスイッチに接続します。
   - ストレージアレイの 2 番目の HBA と 2 番目のコントローラ経由でパスを接続します。
   - スイッチの設定が必要であれば、それを行います。
4. ディスクを再スキャンし、2 つのパスが DMP GUI の［パス］タブに表示されることを確認します。ストレージアレイの［アレイ設定］ダイアログにアクセスし、アレイの負荷分散設定がアクティブ / パッシブに設定されていることを確認します。クラスタディスクではアクティブ / パッシブに設定されている必要があります。
5. 追加のノードに対してこの手順を繰り返します。

ダイナミックディスクグループのアップグレード

以前のインストールに Volume Manager 4.x が含まれる場合、最新のプログラムの機能を使用できるようにディスクグループの種類をアップグレードしてください。

『Veritas Storage Foundation 5.0 管理者ガイド』を参照してください。

メモ : ディスクグループを SFW HA 5.0 にアップグレードする場合、それ以前のバージョンの Volume Manager またはディスクの管理を実行中の別のサーバーにそのディスクグループをインポートすることはできません。ディスクグループをアップグレードした後、そのグループを以前のバージョンに戻すことはできません。

ダイナミックディスクグループバージョンをアップグレードするには

1. ツリービューでアップグレードするディスクグループを右クリックし、［ダイナミックディスクグループバージョンのアップグレード］を選択します。
2. ［はい］をクリックしてダイナミックディスクグループをアップグレードします。

5

Microsoft Service Pack のアップグレード

この章で扱う内容は次のとおりです。

VCS 環境での Microsoft Exchange 2003 SP2 の設定

この項では、すでにインストールされている Microsoft Exchange 2003 に Exchange 2003 SP2 を適用する場合に、VCS 環境で Microsoft Exchange 2003 SP2 を設定する方法を説明します。

Microsoft Exchange 2003 SP2 へのアップグレード

この項では、VCS クラスタでの Microsoft Exchange のインストールのアップグレードについて説明します。

前提条件

Microsoft Exchange 2003 SP2 にアップグレードする前提条件は次のとおりです。

- ExchService タイプのすべてのリソースの DetailMonitor 属性がゼロに設定されていることを確認します。
- サービスパックをインストールする前に、クラスタが非セキュアモードで実行されるように設定されていることを確認します。

次の手順に従って、Exchange サービスグループに組み込まれているノードで、Exchange 2003 のインストールをアップグレードします。Exchange サービスグループに組み込まれているすべてのノードが、Microsoft Exchange と同じバージョンおよび同じサービスパックレベルであることを確認してください。

Microsoft Exchange 2003 SP2 にアップグレードするには

Exchange データベースがフェールオーバーノードにマウントされていないことを確認します。

1. Exchange のインストールをアップグレードする Exchange サービスグループをオンラインにします。
2. Exchange のインストールをアップグレードするノードで HAD を停止します。コマンドプロンプトで、次のコマンドを入力します。
   ```
   C:¥> hastop -local -force
   ```
3. サービスグループがオンラインになっているノードに、Microsoft Exchange 2003 SP2 をインストールします。Internet Information Services（IIS）6.0 のホットフィックスをインストールするよう求められた場合は、Microsoft サポート技術情報 831464 を参照してください。
4. ノードで HAD を起動します。コマンドプロンプトで、次のコマンドを入力します。
   ```
   C:¥> hastart
   ```
5. Exchange サービスグループに組み込まれている残りのすべてのノードで、手順 1 から手順 4 を繰り返します。
6. Exchange をアップグレードするすべてのシステムで、ExchConfig レジストリ情報を更新します。コマンドラインからローカルシステムのレジストリを更新するには、次のように入力します。
   ```
   Setup.exe /UpdateExchVersion
   ```
   2 つ以上のシステムのレジストリを更新するには、次のように入力します。
   ```
   Setup.exe /UpdateExchVersion system_name1 system_name2
   ...
   ```

VCS 環境での Microsoft SQL 2000 Service Pack 4 の設定

この項では、Microsoft SQL 2000 Server Service Pack 4 を、Veritas Storage Foundation HA for Windows 5.0 が稼働するコンピュータにインストールするのに必要な手順を説明します。

Microsoft SQL 2000 Service Pack 4 を実働サーバーに適用する前に次の点を検討します。

- システムとユーザーデータベースの最新のバックアップがあることを確認します。
- この手順には、サーバー停止時間が必要です。

メモ : この手順では、最新の MSSQL データファイルディレクトリをバックアップしたフラットファイルが共有ディスクに格納されていること（この例では、S:¥MSSQL$SQL2000.SP3A）、現在の SQL ディレクトリには、この例では同じドライブ文字の S:¥MSSQL$SQL2000 というディレクトリであることを前提としています。異なる名前のディレクトリを使っている場合は、必要に応じてお使いのディレクトリ名に置き換えてください。

Microsoft SQL 2000 Server Service Pack 4 をインストールするには

1. Veritas Cluster Manager コンソールで、SQL Server サービスグループを右クリックし、すべてのノードで［オフライン］を選択します。
2. SQL Server サービスグループをオフラインにしたノードで、SQL データベースが格納されている共有ドライブの MountV リソースをオンラインにします（例 : S:¥MSSQL$SQL2000）。
3. 共有ディスクに、最新の MSSQL データファイルディレクトリ（S:¥MSSQL$SQL2000）のコピーを作成して名前を変更します（例 : S:¥MSSQL$2000.SP3A）。
4. Veritas Cluster Manager コンソールで、オンラインになっている SQL Server サービスグループを右クリックし、［フリーズ］、［永続的］の順に選択します。
5. Microsoft が提供する手順を使って、Microsoft SQL 2000 Service Pack 4 をアクティブなノード（SQL Server サービスグループがオンラインになっているノード）にインストールします。
6. このサービスグループに 2 つ以上のインスタンスを含める場合、追加の各 SQL インスタンスで手順 5 を繰り返します。
7. Veritas Cluster Manager コンソールで、まだオンラインになっている SQL Server サービスグループを右クリックし、［アンフリーズ］を選択します。

8 Veritas Cluster Manager コンソールで、SQL Server サービスグループを右クリックし、オンラインであったノードで［オフライン］を選択します。

9 ディザスタリカバリ環境では、レプリケーションサービスグループを、このクラスタ内の他のノード（追加のノードまたはフェールオーバーノード）のいずれかに切り替えます。

10 フェールオーバーノードで、SQL データベースが格納されている共有ドライブの MountV リソースをオンラインにします（例：S:¥MSSQL$SQL2000）。

11 共有ディスクで、S:¥MSSQL$SQL2000 ディレクトリの名前を S:¥MSSQL$SQL2000.SP4 に変更します。すでに、S:¥MSSQL$SQL2000.SP4 が共有ディスク内にある場合は、そのディレクトリを削除してから S:¥MSSQL$SQL2000 ディレクトリの名前を変更します。

12 共有ディスクで、S:¥MSSQL$SQL2000.SP3A ディレクトリの名前を S:¥MSSQL$SQL2000 に変更します。このクラスタ内で更新する追加のノードがある場合は、ディレクトリの名前を変更するのではなく、S:¥MSSQL$SQL2000.SP3A ディレクトリを S:¥MSSQL$SQL2000 にコピーします。

13 Veritas Cluster Manager コンソールで、オンラインになっている SQL Server サービスグループを右クリックし、［フリーズ］、［永続的］の順に選択します。

14 Microsoft が提供する手順を使って、Microsoft SQL 2000 Service Pack 4 をアクティブなノード（SQL Server サービスグループがオンラインになっているノード）にインストールします。

15 このサービスグループに 2 つ以上のインスタンスを含める場合、追加の各 SQL インスタンスで手順 14 を繰り返します。

16 Veritas Cluster Manager コンソールで、まだオンラインになっている SQL Server サービスグループを右クリックし、［アンフリーズ］を選択します。

17 Veritas Cluster Manager コンソールで、SQL Server サービスグループを右クリックし、オンラインであったノードで［オフライン］を選択します。

18 3 つ以上の SQL 2000 ノードを使っている場合、追加の各ノードで手順 9 から手順 17 を繰り返します。

19 ディザスタリカバリ環境の場合、セカンダリサイトでこの手順を繰り返します。

20 すべてのノードで Microsoft SQL 2000 Server Service Pack 4 のインストールが完了したら、インスタンスへのユーザー接続性をテストします。

21 SQL Server サービスグループをオンラインにし、ノード間でフェールオーバーさせて、そのサービスグループをテストします。テストが完了するとアップグレードは完了です。

22 SQL Server サービスグループが 2 つ以上ある場合は、各 SQL Server サービスグループでこの手順全体を繰り返します。

VCS 環境での Microsoft SQL 2005 Service Pack 1 の設定

この項では、Microsoft SQL 2005 Server Service Pack 1 を、Veritas Storage Foundation HA for Windows 5.0 が稼働するコンピュータにインストールするのに必要な手順を説明します。

Microsoft SQL 2005 Server Service Pack 1 を実働サーバーに適用する前に次の点を検討します。

- システムとユーザーデータベースの最新のバックアップがあることを確認します。
- この手順には、サーバー停止時間が必要です。

メモ : この手順では、最新の MSSQL データファイルディレクトリをバックアップしたフラットファイルが共有ディスクに格納されていること（この例では、S:¥Microsoft SQL Server）、現在の SQL ディレクトリには、この例では同じドライブ文字の S:¥MSSQL$SQL2000 というディレクトリが使われていることを前提とします。異なる名前のディレクトリを使っている場合は、必要に応じてお使いのディレクトリ名に置き換えてください。

Microsoft SQL 2005 Server Service Pack 1 をインストールするには

1 Veritas Cluster Manager コンソールで、SQL Server サービスグループを右クリックし、すべてのノードで［オフライン］を選択します。

2 SQL Server サービスグループをオフラインにしたノードで、SQL データベースが格納されている共有ドライブの SQL 2005 リソースをオンラインにします。

3 Veritas Cluster Manager コンソールで、オンラインになっている SQL Server サービスグループを右クリックし、［フリーズ］、［永続的］の順に選択します。

4 Microsoft SQL 2005 Service Pack 1 のインストール先のノードで、VVR RVG サービスグループがオンラインになっていることを確認します。Microsoft 社が提供する手順を使って、Microsoft SQL 2005 Service Pack 1 をアクティブなノード（SQL Server サービスグループがオンラインになっているノード）にインストールします。

『Veritas Storage Foundation and High Availability Solutions HA and Disaster Recovery ソリューションガイド Microsoft SQL』を参照してください。

5 このサービスグループに 2 つ以上のインスタンスを含める場合、追加の各 SQL インスタンスで手順 5 を繰り返します。

6 Veritas Cluster Manager コンソールで、まだオンラインになっている SQL Server サービスグループを右クリックし、［アンフリーズ］を選択します。

7 Veritas Cluster Manager コンソールで、SQL Server サービスグループを右クリックし、オンラインであったノードで［オフライン］を選択します。

8 フェールオーバーノードで、SQL データベースが格納されている共有ドライブの SQL 2005 リソースをオンラインにします。

9 Veritas Cluster Manager コンソールで、オンラインになっている SQL Server サービスグループを右クリックし、［フリーズ］、［永続的］の順に選択します。

10 Microsoft SQL Server 2005 Service Pack 1 のセットアップ手順を実行して、Microsoft SQL 2005 Service Pack 1 をアクティブなノード（SQL Server サービスグループがオンラインになっているノード）にインストールします。

11 このサービスグループに 2 つ以上のインスタンスを含める場合、追加の各 SQL インスタンスで手順 14 を繰り返します。

12 Veritas Cluster Manager コンソールで、まだオンラインになっている SQL Server サービスグループを右クリックし、［アンフリーズ］を選択します。

13 Veritas Cluster Manager コンソールで、SQL Server サービスグループを右クリックし、オンラインであったノードで［オフライン］を選択します。

14 オプションで、各サービスグループの再ブートとオンライン化を行い、各ノードでデータベースが接続されていることを確認します。

15 3 つ以上の SQL 2005 ノードを使っている場合、追加の各ノードで手順 9 から手順 17 を繰り返します。

16 ディザスタリカバリ環境の場合、セカンダリサイトでこの手順を繰り返します。

17 すべてのノードで Microsoft SQL 2005 Server Service Pack 1 のインストールが完了したら、インスタンスへのユーザー接続性をテストします。

18 SQL Server サービスグループをオンラインにし、ノード間でフェールオーバーさせて、そのサービスグループをテストします。テストが完了するとアップグレードは完了です。

19 SQL Server サービスグループが 2 つ以上ある場合は、各 SQL Server サービスグループでこの手順全体を繰り返します。

A

Symantec License Inventory Agent の設定

この付録では、次のトピックについて説明します。

Symantec License Inventory Manager について

Symantec License Inventory Manager（ライセンスインベントリマネージャ）は、企業の資産管理追跡ツールです。ネットワーク上の Symantec Information Availability 製品の目録を作成し、これらの製品の配置に関する重要な情報を統合整理します。この情報を使って次のことが行えます。

- 企業で使われているすべてのシマンテック社のソフトウェア製品とライセンスを明確にできます。
- ライセンスのセルフコンプライアンスをより容易に行えます。
- 企業の使用許諾契約の配置状況を把握できます。
- ライセンスコンプライアンス管理するオーバーヘッドを削減できます。
- 配置されたライセンスを基に、サポート契約と保守契約を更新できます。
- シマンテック社のソフトウェアの使用をより詳細に制御できます。
- 実際のソフトウェア使用状況を基に、部門への配賦を管理できます。
- より柔軟なライセンス交付モデルと価格設定モデルを使えます。

- 詳細な配置データを利用して、購入ソフトウェアに対する投資利益率（ROI）を分析できます。

このライセンスインベントリマネージャは、サーバー階層、アクセスポイント階層、エージェント階層で構成される 3 階層システムです。サーバー階層は Symantec License Inventory Server です。この階層で、エージェントやアクセスポイントから収集した情報の統合整理と格納を行います。

アクセスポイント階層はオプションです。この階層には Symantec License Inventory Access Point が含まれ、エージェントとサーバー間の統合整理層として機能します。

エージェント階層には Symantec License Inventory Agent が含まれます。この階層はネットワーク内の個々のホストに配置されます。各エージェントは、エージェントのホストにインストールされているサポート対象のシマンテック製品の製品情報を収集します。次にエージェントは収集した情報をアクセスポイントまたはサーバーに送信します。

Symantec License Inventory Agent がインストールされている場合

Symantec License Inventory Manager は個別に利用できます。Symantec License Inventory Manager ライセンスとメディアキットを注文するには、シマンテック社の販売担当者にお問い合わせください。

インストールメディアには、Symantec License Inventory Manager のオンラインマニュアルが収録されています。販売担当者に連絡して、マニュアルの印刷コピーも注文できます。注文できるマニュアルは次のとおりです。

- 『Symantec License Inventory Manager Installation and Configuration Guide』
- 『Symantec License Inventory Manager Administrator's Guide』
- 『Symantec License Inventory Manager User's Guide』

インストールメディアにはオンラインマニュアルが収録されており、この付録で説明されているすべてのトピックの詳細が掲載されています。

この製品に関する更新、パッチ、ソフトウェアの問題の最新情報については、次のサイトにあるリリースノートをお読みください。

http://entsupport.symantec.com

シマンテック製品のインストーラを使って、シマンテック製品のインストールされているホストにエージェントをインストールまたはアップグレードします。エージェントは次のフォルダにインストールされています。

```
C:¥Program Files¥Symantec¥License Inventory Manager¥Agent
```

エージェントはデフォルト設定でインストールされており、稼働中のシステムへの影響を最小限にします。この最小限の設定では、データとインターフェースの安全を確保するためにエージェントとリモート通信を行うことはできません。

サーバーとアクセスポイントがインストールされている場合

サーバーとアクセスポイントは自動的にインストールされません。Symantec License Inventory Manager を使う場合は、サーバーとアクセスポイント（オプション）を手動でインストールする必要があります。サーバーとアクセスポイントをインストールすると、エージェントは情報を収集できるようになり、ユーザーはインベントリレポートを作成できます。

サーバーとアクセスポイントは、Symantec License Inventory Manager インストールディスクからインストールできます。

エージェントを使用してできること

エージェントをインストールした後、ユーザーはエージェントを使ってエージェントがインストールされているシステムのシマンテック製品を追跡できます。エージェントを使わないように選択した場合は、エージェントを削除できます。

ただし、エージェントを使うには、エージェントとそのサーバーまたはアクセスポイントとの間でリモート通信ができるように、手動でエージェントを設定する必要があります。エージェントの詳細な再設定手順については、『Symantec License Inventory Manager 4.2 リリースノート』に説明されています。このマニュアルは、次の URL からダウンロードできます。

http://entsupport.symantec.com/docs/2856021

エージェントを削除する方法

Symantec License Inventory Manager を使用しない場合は、［プログラムの追加と削除］を使ってエージェントを削除できます。エージェントは［プログラムの追加と削除］に Symantec License Inventory Agent プログラムとして表示されています。

後で、Symantec License Inventory Manager インストールディスクを使ってエージェントを再インストールすることもできます。このディスクは、Symantec License Inventory Manager キットで利用できます。

索引