Storage Foundation7.0 設定およびアップグレードガイド- Linux

9 月 2015

VERITAS™

Storage Foundation 設定およびアップグレードガイド

この本で説明されているソフトウェアは使用許諾契約の下で提供され、同意条項に従う場合にのみ使うことができます。

製品のバージョン: 7.0

マニュアルバージョン: 7.0 Rev 1

法的通知と登録商標

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

テクニカルサポート

シマンテック社のテクニカルサポートは、サポートセンターを世界規模で運営しています。テクニカルサポートの主な役割は、製品の特徴や機能に関する問い合わせに対応することです。テクニカルサポートグループは、オンラインのナレッジベースも作成しています。テクニカルサポートグループは、社内の他の部門と連携して、適時ユーザーの質問に答えます。たとえば、テクニカルサポートグループは製品技術部門およびシマンテックセキュリティレスポンスと協力して、アラートサービスやウイルス定義の更新を提供します。

シマンテック社が提供しているサポートには次のものが含まれます。

- 組織の大きさに合わせて適切な量のサービスを選択可能な、さまざまなサポートオプション
- 迅速な対応と最新情報を提供する、電話および Web によるサポート
- ソフトウェアアップグレードを配布するアップグレード保証
- 地域別の業務時間帯、または 24 時間 365 日利用できるグローバルなサポート
- アカウント管理サービスを含むプレミアムサービス製品

シマンテック社のサポート提供については、次の URL で当社の Web サイトを参照できます。

www.symantec.com/business/support/index?page=home&locale=ja_JP

すべてのサポートサービスは、サポート契約と現在のエンタープライズテクニカルサポートポリシーに応じて提供されます。

テクニカルサポートへのお問い合わせ

現在のサポート契約にご加入いただいているお客様は、以下の URL からテクニカルサポート情報にアクセスできます。

http://www.symantec.com/ja/jp/support/contact_techsupp_static.jsp

テクニカルサポートにお問い合わせになる前に、製品のマニュアルに記載されているシステムの必要条件が満たされていることをご確認ください。また、問題を再現する必要がある場合は、問題が発生したコンピュータからお問い合わせください。

テクニカルサポートに連絡するときは、以下の情報をご用意ください。

- 製品のリリースレベル
- ハードウェアに関する情報
- 使用可能なメモリ、ディスク容量、および NIC 情報
- オペレーティングシステム
- バージョンとパッチレベル

- ネットワークトポロジー
- ルーター、ゲートウェイ、および IP アドレス情報
- 問題についての詳細情報
  - エラーメッセージおよびログファイル
  - シマンテック社に連絡する前に行ったトラブルシューティング
  - 最近行ったソフトウェア設定の変更やネットワークの変更

ライセンスと登録

シマンテック製品に登録またはライセンスキーが必要な場合は、次の URL にあるテクニカルサポートの Web ページにアクセスしてください。

www.symantec.com/business/support/index?page=home&locale=ja_JP

カスタマサービス

カスタマサービス情報は、次の URL で入手できます。

www.symantec.com/business/support/index?page=home&locale=ja_JP

カスタマサービスは、次のような種類の技術関連以外のお問い合わせにご利用いただけます。

- 製品ライセンスまたはシリアル化に関する質問
- 住所または名前の変更などの製品登録の更新
- 一般的な製品情報（機能、使用できる言語、地域の販売店）
- 製品の更新とアップグレードに関する最新情報
- アップグレード保証とサポート契約に関する情報
- シマンテック社の購入プログラムに関する情報
- シマンテック社のテクニカルサポートオプションに関する相談
- 技術関連以外の購入前の質問
- CD-ROM またはマニュアル関連の問題

サポート契約のリソース

現在のサポート契約についてシマンテック社にお問い合わせになる場合は、次に示すお住まいの地域のサポート契約管理チームにお問い合わせください。

アジア太平洋地域および日本	customercare_apj@symantec.com
ヨーロッパ、中東、およびアフリカ	semea@symantec.com
北米および中南米	supportsolutions@symantec.com

マニュアル

製品マニュアルは PDF 形式でメディアに含まれています。マニュアルの最新版を使用していることを確認してください。マニュアルのバージョンは各ガイドの 2 ページ目に記載されています。最新の製品マニュアルはシマンテック社の Web サイトで入手できます。

https://sort.symantec.com/documents

製品マニュアルに関するご意見、ご感想をお待ちしています。改善点のご提案、誤記や記載漏れなどをお送りください。タイトル、マニュアルのバージョン（2 ページ目に記載されています）、報告する内容が含まれる章タイトルと項タイトルも記載してください。次の宛先にお送りください。

doc_feedback@symantec.com

最新の HOWTO 技術情報、マニュアルの更新、製品のマニュアルに関する質問については、Symantec Connect のストレージとクラスタのマニュアルのフォーラムを参照してください。

https://www-secure.symantec.com/connect/storage-management/forums/storage-and-clustering-documentation

Symantec Connect について

Symantec Connect はシマンテック社の企業のお客様向けのピアツーピアの技術コミュニティサイトです。参加者はフォーラムへの投稿、記事、ビデオ、ダウンロード、ブログの作成や意見の提案などによって、他の製品ユーザーと連絡を取ったり情報を共有したりできます。また、シマンテック社の製品チームやテクニカルサポートと対話できます。内容はコミュニティによって評価され、メンバーは貢献に対する報酬ポイントを受け取ります。

http://www.symantec.com/connect/storage-management

目次

1

Storage Foundation の概要および設定

1

Storage Foundation の概要

この章では以下の項目について説明しています。

Storage Foundation について

Storage Foundation には各種の機能レベルを持つ VxFS（Veritas File System）と VxVM（Veritas Volume Manager）があります。

Veritas File System はアプリケーションに容易な管理と高速リカバリ機能を提供する高性能のジャーナルファイルシステムです。Veritas File System は拡張性のあるパフォーマンス、連続的な可用性、増加された I/O スループットと構造整合性を提供します。

Veritas Volume Manager はディスクストレージの物理的な制限事項を削除します。データ可用性を妨げることなくオンラインでストレージ I/O パフォーマンスを設定し、共有し、管理し、最適化できます。Veritas Volume Manager は使いやすい、オンラインストレージの管理ツールを提供して、ダウンタイムを削減します。

VxFS と VxVM は、すべての Veritas InfoScale 製品の一部です。VxFS と VxVM を個々のコンポーネントとしてインストールしたり、更新したりしないでください。

Storage Foundation Basic はすべての Storage Foundation Standard 機能をサポートしますが、配備とテクニカルサポートに制限があります。

Veritas Replicator Option について

Veritas Replicator Option は任意で追加できる機能で、個別にライセンスが必要となります。

File Replicator により、IP ネットワークを介したファイルレベルでのレプリケーションを実行できます。File Replicator は、Veritas File System によって提供されるデータ複製を利用して、ネットワークリソースへのレプリケーションによる影響を軽減します。

Volume Replicator は、連続的なデータ可用性とディザスタリカバリを提供するために、すべての標準 IP ネットワークを通してリモートの場所にデータをレプリケートします。

Volume Replicator は、Storage Foundation、Storage Foundation and High Availability、Storage Foundation Cluster File System、Storage Foundation for Oracle RAC、および Storage Foundation for SybaseCE と利用可能です。

このオプションをインストールする前に、製品のリリースノートを参照してください。

このオプションをインストールするには、この製品のインストールガイドの指示に従います。

Veritas InfoScale Operations Manager について

Veritas InfoScale Operations Manager には、Veritas InfoScale 製品の集中型管理コンソールが用意されています。Veritas InfoScale Operations Manager を使って、ストレージリソースを監視、視覚化、管理したり、レポートを生成したりすることができます。

Veritas InfoScale Operations Manager を使って Storage Foundation と Cluster Server の環境を管理することをお勧めします。

Veritas InfoScale Operations Manager は http://go.symantec.com/vom からダウンロードできます。

インストール、アップグレード、設定の手順について詳しくは、Veritas InfoScale Operations Manager のマニュアルを参照してください。

Veritas Enterprise Administrator（VEA）のコンソールは Veritas InfoScale 製品に含まれなくなりました。VEA の使用を続けたい場合は、http://www.symantec.com/operations-manager/support からソフトウェアバージョンをダウンロードできます。Storage Foundation Management Server は非推奨です。

Symantec Operations Readiness Tools について

SORT（Symantec Operations Readiness Tools）は、最も時間のかかる管理タスクの一部を自動化して単純化する Web サイトです。データセンターのリスクを特定して操作効率を改善するのに役立ち、データセンターのアーキテクチャとスケールにまつわる複雑性を管理できるようになります。

表 1-1 は、それらを達成するのに役立つ 3 つの主なデータセンタータスクと SORT ツールのリストです。

表 1-1　データセンタータスクと SORT ツール

タスク	SORT ツール
インストールとアップグレードの準備	■ インストールとアップグレードのチェックリスト メモリ、ディスク容量、アーキテクチャを含むシステムの必要条件を表示します。 ■ インストールとアップグレードのカスタムレポート Veritas InfoScale 製品をインストールまたはアップグレードする準備ができているかどうかを判断するためにレポートを作成します。 ■ アレイ固有のモジュールファインダー UNIX サーバー用最新 ASL（Array Support Libraries）と APM（Array Policy Modules）、Wndows サーバー用 DDI（Device Driver Installers）とデバイス検出層（DDL）を一覧表示します。 ■ 高可用性エージェントの表 アプリケーション、データベース、レプリケーション、シマンテック社のパートナーのためにエージェントを検索してダウンロードします。
リスクの特定およびサーバー固有の推奨事項の取得	■ パッチの通知 パッチの更新についての自動電子メールの通知を受信します。（サインインが必須です。） ■ リスク評価のチェックリスト Veritas InfoScale 製品およびプラットフォームに基づく設定の推奨事項を表示します。 ■ リスク評価のカスタムレポート システムを分析し、システム可用性、ストレージの使用、パフォーマンス、ベストプラクティスについての推奨事項を提供するレポートを作成します。 ■ エラーコードの説明とソリューション 何千ものエラーコードの詳細情報を表示します。

タスク	SORT ツール
効率の向上	■ パッチファインダー Veritas InfoScale エンタープライズ製品用のパッチを一覧表示し、ダウンロードします。 ■ ライセンスと配備のカスタムレポート インストールされた Veritas InfoScale 製品およびライセンスキーを一覧表示するカスタムレポートを作成します。製品、プラットフォーム、サーバー層、システムによってライセンスを表示します。 ■ Symantec Performance Value Unit (SPVU) Calculator 価格設定の測定移行に役立つ計算機を使います。 ■ マニュアル マニュアルページ、製品ガイド、サポート技術情報を含む Veritas InfoScale 製品のマニュアルを一覧表示してダウンロードします。 ■ 関連リンク 単一ページに Veritas InfoScale 製品サポート、フォーラム、カスタマーサービス、ベンダー情報へのリンクを表示します。

SORT は追加料金なしで入手できます。

SORT にアクセスするには、次に移動してください。

https://sort.symantec.com

2

Storage Foundation の設定

この章では以下の項目について説明しています。

インストーラを使った Storage Foundation の設定

最小限の設定が必要ですが、インストーラを使って Storage Foundation を設定できます。

Storage Foundation を設定するには

1. /opt/VRTS/install/ インストールディレクトリに移動します。
2. configure オプションを指定してインストーラコマンドを実行します。

```
# ./installer -configure
```

または /opt/VRTS/install/installer コマンドを実行して、設定オプションを選択します。

```
Task Menu:
C) Configure a Product Component
U) Uninstall a Product
L) License a Product
S) Start a Product
D) View Product Descriptions
X) Stop a Product
O) Perform a Post-Installation Check
?) Help

Enter a Task: [C,U,L,S,D,X,O,?] C
```

SF の手動設定

SF 内で、さまざまな製品を手動で設定できます。

Veritas Volume Manager の設定

Veritas Volume Manager を設定するには、次の手順を使います。製品インストーラを使って VxVM をインストールおよび設定した場合は、この項の手順を完了する必要はありません。

インストール後における VxVM ディスクグループとボリュームの設定について詳しくは、『Storage Foundation 管理者ガイド』の「Veritas Volume Manager の設定」を参照してください。

Veritas File System の設定

Veritas File System をインストールした後、mkfs コマンドを使って、ディスクスライスまたは Veritas Volume Manager ボリュームにファイルシステムを作成できます。このファイルシステムを使う前に、mount コマンドを使ってファイルシステムをマウントする必要があります。umount コマンドを使って、ファイルシステムを後でマウント解除できます。次の

ファイルにファイルシステム用のエントリを追加すれば、システムブート時にファイルシステムを自動的にマウントできます。

```
/etc/fstab
```

固有コマンドについては、Storage Foundation のマニュアルとオンラインマニュアルページで説明しています。

詳しくは、『Storage Foundation 管理者ガイド』を参照してください。

ファイルシステムモジュールのロードとアンロード

vxfs ファイルシステムモジュールは、VxFS ファイルシステムへの最初の参照で自動的にロードされます。これは、ユーザーが VxFS ファイルシステムをマウントしようとすると実行されます。

場合によっては、手動でファイルシステムモジュールをロードする方が効率的です。たとえば、サイズの大きいクラスシステムには、複数のディスクチェーンを接続したデュアルインターフェース I/O カードを多数搭載できます。このようなシステムが再ブートされると、デバイス調査処理にかかる時間が長くなるため、再ブートを実行するのではなく、modprobe コマンドを使って vxfs モジュールをロードします。

```
# modprobe vxfs ; modprobe vxportal ; modprobe fdd
```

insmod コマンドを使って vxfs モジュールをロードしないでください。insmod は、モジュール設定ファイル /etc/modprobe.conf を調べないからです。

モジュールが正常にロードされたかどうかを判断するには、次に示すように lsmod コマンドを使います。

```
# lsmod | grep vxportal
vxportal               2952           0
vxfs                   3427960        0    fdd vxportal
# lsmod | grep fdd
fdd                    67212          0    (unused)
vxfs                   3427960        0    [fdd vxportal]
# lsmod | grep vxfs
vxfs                   3427960        0    [fdd vxportal]
```

出力の最初のフィールドはモジュール名です。モジュールをアンロードするには、次のように入力します。

```
# rmmod fdd
# rmmod vxportal
# rmmod vxfs
```

マウントされた VxFS ファイルシステムがある場合、rmmod コマンドは失敗します。VxFS ファイルシステムがマウントされているかどうかを判断するには、次のように入力します。

```
# df -T | grep vxfs
```

SFDB の設定

デフォルトでは、vxdbd デーモンが設定されていない SFDB ツールは無効になっています。/opt/VRTS/bin/sfae_config status コマンドを使用して、SFDB ツールが有効になっているか無効になっているかを確認できます。

SFDB ツールを有効にするには

1. root としてログインします。
2. 次のコマンドを実行して、vxdbd デーモンを設定し、起動します。この手順を実行した後、システムの再起動時にデーモンが開始されるように、システムスタートアップにエントリが作成されています。

   ```
   #/opt/VRTS/bin/sfae_config enable
   ```

SFDB ツールを無効にするには

1. root としてログインします。
2. 次のコマンドを実行します。

   ```
   #/opt/VRTS/bin/sfae_config disable
   ```

2

Storage Foundation のアップグレード

3

Storage Foundation のアップグレード計画

この章では以下の項目について説明しています。

- アップグレードについて
- サポートされているアップグレードパス
- SF のアップグレードの準備
- インストールバンドルを使ったフルリリース(ベース、メンテナンス、ローリングパッチ)と個々のパッチの同時インストールまたは同時アップグレード

アップグレードについて

このリリースでは 6.0 以降バージョンからのアップグレードをサポートします。既存のインストールが 60 より前のバージョンである場合、まずバージョン 6.0 にアップグレードしてから、このマニュアルで既に説明した手順に従って製品をアップグレードする必要があります。

インストーラは、次のタイプのアップグレードをサポートします。

- 完全アップグレード
- 応答ファイルを使った自動アップグレード

表 3-1 では、アップグレード後の製品のマッピングが記述されています。

表 3-1　アップグレード後の Veritas InfoScale 製品のマッピング

製品(6.2.x 以前)	製品(7.0)	コンポーネント(7.0)
SF Basic	サポートされるアップグレードはありません	適用不可能

製品（6.2.x 以前）	製品（7.0）	コンポーネント（7.0）
SF	Veritas InfoScale Storage	SF
DMP	Veritas InfoScale Foundation	SF

アップグレード中に、インストールプログラムにより次のタスクが実行されます。

1. アップグレード前に製品を停止します。
2. インストールされたパッケージをアップグレードし、追加のパッケージをインストールします。

   現在のインストールで永続ライセンスキーを使用している場合、7.0 に更新するように促すメッセージが表示されます。更新しないことを選択した場合、古いライセンスの使用は継続できますが、製品の機能が対応するコンポーネントに限定されます。たとえば、既存の SFCFSHA のインストールの永続ライセンスを更新しないことを選択した場合、アップグレード後にインストーラによって SFCFSHA コンポーネントが有効になります。Veritas InfoScale Enterprise 製品の他のコンポーネントの機能は利用できなくなります。インストールでキーレスライセンスが使用される場合、インストーラで全機能を備えた新製品に対する新しいキーが登録されます。
3. 既存の設定をリストアします。

   たとえば、設定に SF のインストールが含まれる場合、インストーラで設定が SF にアップグレードされ、復元されます。設定に複数のコンポーネントが含まれる場合、インストーラでコンポーネントの設定がアップグレードされ、復元されます。
4. 設定されたコンポーネントを開始します。

メモ: ルートディスクがカプセル化されている場合、ルートディスクをカプセル解除する必要はありません。アップグレード後にシステムを再ブートします。

サポートされているアップグレードパス

サポートされないオペレーティングシステムバージョンをお使いの場合、まずサポートされるバージョンのオペレーティングシステムにアップグレードします。また、オペレーティングシステムのメジャーバージョン間のアップグレードはサポートされません。たとえば、RHEL 6 から RHEL 7 へのアップグレードなどです。オペレーティングシステムのメジャーバージョン間の移行を計画している場合は、製品を再インストールする必要があります。サポートされているオペレーティングシステムバージョンについては、『Veritas InfoScale リリースノート』を参照してください。

表 3-2 に、RHEL または Oracle Linux 上でサポートされるアップグレードパスの一覧を示します。

表 **3-2** RHEL および Oracle Linux のサポート対象のアップグレードパス

アップグレード元の製品バージョン	現在の **OS** バージョン	アップグレード先の **OS** バージョン	製品バージョンに	コンポーネントに
6.0 と 6.0 RP1	RHEL 6 Update 1、2 Oracle Linux 6 Update 1	RHEL 6 Update 4、5、6 Oracle Linux 6 Update 4、5、6	Veritas InfoScale Storage 7.0	SF
6.0.1	RHEL 6 Update 1、2、3 Oracle Linux 6 Update 1、2、3	RHEL 6 Update 4、5、6 Oracle Linux 6 Update 4、5、6	Veritas InfoScale Storage 7.0	SF
6.0.2	RHEL 6 Update 1、2 Oracle Linux 6 Update 1、2	RHEL 6 Update 4、5、6 Oracle Linux 6 Update 4、5、6	Veritas InfoScale Storage 7.0	SF
6.0.3	RHEL 6 Update 1、2、3、4、5 Oracle Linux 6 Update 1、2、3、4、5	RHEL 6 Update 4、5、6 Oracle Linux 6 Update 4、5、6	Veritas InfoScale Storage 7.0	SF
6.0.5	RHEL 6 Update 1、2、3、4、5、6 Oracle Linux 6 Update 1、2、3、4、5、6	RHEL 6 Update 4、5、6 Oracle Linux 6 Update 4、5、6	Veritas InfoScale Storage 7.0	SF
6.1	RHEL 6 Update 3、4、5 Oracle Linux 6 Update 3、4、5	RHEL 6 Update 4、5、6 Oracle Linux 6 Update 4、5、6	Veritas InfoScale Storage 7.0	SF
6.1.1、6.2	RHEL 6 Update 3、4、5、6 Oracle Linux 6 Update 3、4、5	RHEL 6 Update 4、5、6 Oracle Linux 6 Update 4、5、6	Veritas InfoScale Storage 7.0	SF

アップグレード元の製品バージョン	現在の OS バージョン	アップグレード先の OS バージョン	製品バージョンに	コンポーネントに
6.2	RHEL 7 Oracle Linux 7	RHEL 7、Update 1 Oracle Linux 7 、Update 1	Veritas InfoScale Storage 7.0	SF
6.2.1	RHEL 6 Update 4、5、6 Oracle Linux 6 Update 4、5、6	RHEL 6 Update 4、5、6 Oracle Linux 6 Update 4、5、6	Veritas InfoScale Storage 7.0	SF
6.2.1	RHEL 7、Update 1 Oracle Linux 7 、Update 1	RHEL 7、Update 1 Oracle Linux 7 、Update 1	Veritas InfoScale Storage 7.0	SF

表 3-3 は、SLES のアップグレードでサポートされるアップグレードパスの一覧を示しています。

表 3-3 SLES でのサポートされるアップグレードパス

アップグレード元の製品バージョン	現在の OS バージョン	アップグレード先の OS バージョン	製品バージョンに	コンポーネントに
6.0 と 6.0 RP1	SLES 11 SP1	SLES 11 SP3	Veritas InfoScale Storage 7.0	SF
6.0.1、6.0.2、6.0.3	SLES 11 SP1 SLES 11 SP2	SLES 11 SP3	Veritas InfoScale Storage 7.0	SF
6.0.4	SLES 11 SP2 SLES 11 SP3	SLES 11 SP3	Veritas InfoScale Storage 7.0	SF
6.0.5	SLES 11 SP1 SLES 11 SP2 SLES 11 SP3	SLES 11 SP3	Veritas InfoScale Storage 7.0	SF
6.1、6.1.1、6.2、6.2.1	SLES 11 SP2 SLES 11 SP3	SLES 11 SP3	Veritas InfoScale Storage 7.0	SF

アップグレード元の製品バージョン	現在の OS バージョン	アップグレード先の OS バージョン	製品バージョンに	コンポーネントに
6.2.1	SLES 12	SLES 12	Veritas InfoScale Storage 7.0	SF

SF のアップグレードの準備

アップグレードする前に、システムとストレージを準備する必要があります。次の手順を確認してから、適切なタスクを実行してください。

アップグレードの準備

アップグレードを実行する前に次のタスクを完了してください。

- システムのアップグレードに関する最新情報については、『Veritas InfoScale 7.0 リリースノート』を確認ください。
- 詳しいことは、シマンテック社テクニカルサポート Web サイトで確認してください。
  http://www.symantec.com/techsupp/
- アップグレードを実行する管理者は、root アクセス権限を持ち、オペレーティングシステムの管理について十分に理解している必要があります。
- すべてのユーザーがログアウトしていて、すべての主要なユーザーアプリケーションが適切に停止されていることを確認します。
- アップグレードするシステムに有効なバックアップがあることを確認します。
  p.24 の「バックアップの作成」を参照してください。
- アップグレードするために十分なファイルシステム領域があることを確認します。RPMs をコピーする場所を特定します。たとえば、ルートファイルシステムに十分な領域がある場合は `/packages/Veritas`、`/var` ファイルシステムに十分な領域がある場合は `/var/tmp/packages` にします。

  `/tmp` にはファイルを置かないでください。システムの再起動時に削除されます。

  また、アップグレードスクリプトを実行するまでアクセスできないファイルシステムには、ファイルを保存しないでください。

  アップグレードスクリプトへの変更が必要なければ、シマンテック社から提供されたディスクを使ってアップグレードすることもできます。

  `/usr/local` が最初にスライスとして作成されていた場合は、変更が必要です。
- `/etc/init.d/` 内の起動スクリプトを編集し、ファイルシステムが存在しないと異常終了することがわかっているアプリケーションのコマンドまたはプロセスをコメントアウトします。

- 現在のオペレーティングシステムが製品のバージョン 7.0 をサポートすることを確認してください。オペレーティングシステムがこの製品をサポートしない場合は、段階的アップグレードを計画してください。
- アップグレードと、Veritas InfoScale 製品を使うアプリケーションのために、十分な停止時間とダウンタイムをスケジュール設定します。設定によっては、停止が数時間になる場合があります。
- rootdg 内にスワップパーティションがない場合は、/etc/fstab からコメントアウトする必要があります。可能ならば、ルートディスク上にある以外のスワップパーティションは、/etc/fstab からコメントアウトされ、アップグレード中にマウントされないようにする必要があります。rootdg 内にアクティブなスワップパーティションがない場合は、upgrade_start は失敗します。
- アップグレード前にファイルシステムが正常にマウント解除されていることを確認します。
- アレイをアップグレードします(必要な場合)。
p.28 の「アレイサポートのアップグレード」を参照してください。
- 情報をミラー化ディスクに確実に保存するために、システムをシャットダウンし、ミラー化ディスクを物理的に削除します。ディスクを物理的に削除することで、フェールバックポイントがわかります。
- ルートディスクがカプセル化されているかどうかを確認します。
p.25 の「ルートディスクがカプセル化されているかどうかの確認」を参照してください。
- ネーティブスタックの DMP サポートが無効になっていることを確認します(dmp_native_support=off)。ネーティブスタックの DMP サポートが有効になっていると(dmp_native_support=on)、インストーラによりそのことが検出され、システムを再起動するように求められることがあります。

バックアップの作成

アップグレードの前に、関連するシステム情報を保存します。

バックアップを作成するには

1. スーパーユーザーとしてログインします。
2. アップグレードする前に、保存する必要のあるすべてのデータのバックアップが作成されていることを確認します。
3. /boot/grub/menu.lst、/etc/grub.conf や /etc/lilo.conf、/etc/fstab などのファイルの情報をバックアップします。

4 インストーラは VxVM プライベートリージョンの設定ファイルの最近のバックアップが /etc/vx/cbr/bk に保存されていることを検証します。

保存されていない場合は、警告メッセージが表示されます。

警告: /etc/vx/cbr/bk ディレクトリをバックアップします。

5 fstab ファイルを fstab.orig にコピーします。

```
# cp /etc/fstab /etc/fstab.orig
```

6 vxlicrep、vxdisk list、vxprint -ht コマンドを実行し、出力を記録します。この情報を使って、アップグレード後にシステムを再設定します。

7 Veritas InfoScale Enterprise 7.0 ソフトウェアをインストールする場合、インストール手順で VCS 設定保持の詳細について、『Cluster Server 設定およびアップグレードガイド』に記載されているガイドラインに従ってください。

8 外部の quotas ファイルと quotas.grp ファイルをバックアップします。

6.0.3 からアップグレードする場合は、quotas.grp.64 ファイルと quotas.64 ファイルもバックアップする必要があります。

9 クォータがすべてのマウントされているファイルシステムでオフになっていることを確認します。

ルートディスクがカプセル化されているかどうかの確認

次のコマンドを実行して、システムのルートディスクが VxVM の制御下にあるかどうかを確認します。

```
# df -v /
```

/dev/vx/dsk/rootdg/rootvol がルート(/)ファイルシステムとしてマウントされていると表示された場合、ルートディスクは VxVM の制御下にあります。

ルートディスクがカプセル化されている場合は、該当するアップグレード手順に従ってください。

Volume Replicator のアップグレード前の計画

Volume Replicator(VVR)をインストールまたはアップグレードする前に:

- システムに VVR をインストールするための十分な空きディスク領域があることを確認します。

- root 権限があることを確認します。インストールとアップグレード手順を実行するには root 権限が必要です。
- VVR を使ったレプリケーションが設定されている場合は、アップグレードする前に、ディスクグループバージョンを少なくとも 110 にしておくことをお勧めします。
  次のコマンドを使ってディスクグループバージョンを確認できます。

  ```
  # vxdg list diskgroup
  ```

- VVR を使ったレプリケーションが設定されている場合、SRL ボリュームのサイズが 110 MB よりも大きいことを確認します。
  『Veritas InfoScale™ 7.0 Replication 管理者ガイド』を参照してください。
- VVR を使ったレプリケーションが設定されている場合は、すべてのホストで、すべてのプライマリ RLINK が最新であることを確認します。

  ```
  # /usr/sbin/vxrlink -g diskgroup status rlink_name
  ```

  メモ: プライマリ RLINK が最新になるまで処理を続行しないでください。

- VCS で VVR レプリケーションを管理している場合は、VVR と VCS エージェントをアップグレードするための準備手順に従います。

詳しくは、『Veritas InfoScale™ 7.0 Replication 管理者ガイド』を参照してください。

詳しくはマニュアルの『スタートガイド』を参照してください。

前の VVR バージョンからのアップグレードの計画

VVR を以前の VVR バージョンからアップグレードする場合、ホストを個別の時間にアップグレードすることによって、アプリケーション停止時間を減らして、VVR をアップグレードできます。プライマリがアップグレードされる間、アプリケーションはセカンダリに移行されるので、ダウンタイムを削減できます。プライマリをアップグレードすると、VVR のバージョンがセカンダリと異なるものになりますが、それでも複製は可能です。この機能により、両方のサイト上で VVR アップグレードが完了しなくても、高可用性を保つことができます。セカンダリホストは、RDS（Replicated Data Set）のプライマリホストより前にアップグレードすることをお勧めします。

Storage Foundation バージョンを渡ってレプリケートするための VVR サポートに関する情報が記載されている Veritas InfoScale™ 7.0 リリースノート を参照してください。

異なるバージョン間でレプリケートするのは、プライマリとセカンダリを同時にアップグレードすることの制限を取り除くためです。VVR は、アップグレードするシステムで RVG（Replicated Volume Group）のある既存の RDS をレプリケートし続けることができます。プライマリとセカンダリが異なるバージョンであるとき、VVR は `vradmin` コマンドでの設定の変更、または新しい RDS の作成をサポートしません。

TCP をネットワークプロトコルとして指定する場合は、プライマリおよびセカンダリの VVR バージョンによって、チェックサムが計算されるかどうかが決まります。表 3-4 に示すように、プライマリまたはセカンダリで 7.0 以前のバージョンの VVR が動作していて、TCP プロトコルを使う場合は、レプリケートするデータパケットごとにチェックサムが計算されます。プライマリとセカンダリで VVR 7.0 が動作している場合は、チェックサムは計算されません。代わりに TCP チェックサム機構が使われます。

表 3-4 VVR バージョンとチェックサム計算

7.0 以前の VVR（DG バージョン <= 140）	VVR 7.0（DG バージョン >= 150）	VVR がチェックサム TCP 接続を計算するかどうか
プライマリ	セカンダリ	はい
セカンダリ	プライマリ	はい
プライマリとセカンダリ		はい
	プライマリとセカンダリ	いいえ

メモ: VVR の異なるバージョン間で複製する場合、新しい機能に関連するコマンドを使用しないでください。前のバージョンは新しい機能をサポートしない場合があり、問題が起きる可能性があります。

RDS のすべてのホストを同時にアップグレードする必要がないのであれば、1 台のホストをアップグレードした後、バージョン間の複製を使用できます。その後、都合のよい時点で、RDS の他のホストをアップグレードできます。

メモ: クラスタを設定している場合、クラスタ内のすべてのノードを同時にアップグレードする必要があります。

接続プロトコルとして IPv6 を使うための VVR の計画とアップグレード

SF は IPv6 を接続プロトコルとして使うことをサポートします。

このリリースでは、VVR の次の設定をサポートしています。

- インターネットプロトコルとして IPv4 を使った IPv4 専用ノード間のレプリケーションを引き続きサポートする
- インターネットプロトコルとして IPv4 を使った IPv4 専用ノードと IPv4/IPv6 デュアルスタックノード間のレプリケーションをサポートする
- インターネットプロトコルとして IPv6 を使った IPv6 専用ノードと IPv4/IPv6 デュアルスタックノード間のレプリケーションをサポートする
- IPv6 専用ノード間のレプリケーションをサポートする

- IPv4/IPv6 デュアルスタックノードから、1 つ以上の IPv6 専用ノードおよび 1 つ以上の IPv4 専用ノードへのレプリケーションをサポートする
- ディスクグループを共有するクラスタ内のすべてのノードが IPv4 または IPv6 である場合にのみ、共有ディスクグループのレプリケーションをサポートする

アレイサポートのアップグレード

Veritas InfoScale 7.0 リリースには、単一のRPMである VRTSaslapm にすべてのアレイサポートが含まれます。アレイサポートRPMには、以前に VRTSvxvm RPMに含まれていたアレイサポートが含まれます。またアレイサポートRPMには、以前に外部アレイサポートライブラリ（ASL）とアレイポリシーモジュール（APM）としてパッケージ化されていたサポートも含まれます。

サポート対象アレイについて詳しくは、7.0 ハードウェア互換性リストを参照してください。

製品インストーラで Storage Foundation 製品をアップグレードする場合、インストーラが自動的にアレイサポートをアップグレードします。 手動手順で Storage Foundation 製品をアップグレードする場合は、以前にシステムにインストールした外部 ASL または APM をすべて削除してください。外部 ASL または APM が検出された場合、VRTSvxvm RPM のインストールはエラーになって終了します。

Veritas InfoScale 7.0 をインストールした後、シマンテック社は VRTSaslapm RPM への更新を通して、新しいディスクアレイのサポートを提供します。

アレイサポートについて詳しくは、『 Storage Foundation 管理者ガイド』を参照してください。

インストールバンドルを使ったフルリリース（ベース、メンテナンス、ローリングパッチ）と個々のパッチの同時インストールまたは同時アップグレード

バージョン 6.1 以降では、インストールバンドルを使ってシステムを 1 回の手順で直接、ベースレベル、メンテナンスレベル、パッチレベルで簡単にインストールまたはアップグレードできます。複数のパッチやパッケージをまとめてインストールまたはアップグレードすることもできます。インストールバンドルのインストーラには、1 度の実行でメンテナンスまたはパッチレベルに直接インストールまたはアップグレードできるようにマージする機能があります。各種のスクリプト、RPMs、パッチコンポーネントがマージされ、1 つの統合されたリリースのように複数のリリースが一緒にインストールされます。システムをメンテナンスレベルまたはパッチレベルにインストールまたはアップグレードするために 2 つ以上のインストールアクションを実行する必要はありません。

リリースは、次のカテゴリに分けられます。

表 3-5　リリースレベル

レベル	内容	フォームファクタ	適用先	リリースタイプ	ダウンロード場所
BASE	機能	RPMs	すべての製品	メジャー、マイナー、サービスパック（SP）、プラットフォームリリース（PR）	FileConnect
メンテナンス	修正、新機能	RPMs	すべての製品	MR（メンテナンスリリース）、RP（ローリングパッチ）	SORT（Symantec Operations Readiness Tools）
パッチ	修正	RPMs	単一製品	P パッチ、プライベートパッチ、パブリックパッチ	SORT、サポートサイト

Install Bundles を使用してインストールまたはアップグレードを行うとき

- Veritas InfoScale 製品を検出し、メンテナンスレベルの単一バージョンとして割り当てます。各システムには、適用される 1 つ以上のパッチがある場合もあります。
- ベースリリースは FileConnect からアクセス可能で、お客様のシリアル番号を必要とします。メンテナンスリリースとパッチリリースは、SORT から自動的にダウンロード可能です。
- 6.0.1 以降のバージョンから、自動インストーラを使ってパッチをインストールできるようになりました。
- アップグレードの競合を防止するために、パッチを検出することができます。パッチリリースは統合リリースとして提供されていません。これらは必要に応じてシマンテック社テクニカルサポートからのみ利用可能です。

`-base_path` と `-patch_path` オプションを使って、複数のリリースからインストールコードをインポートすることができます。異なるメディアパスから RPMs とパッチを見つけ、複数のリリースの RPM とパッチ定義をマージすることができます。これらのオプションを使用して、リリースコンポーネントごとに必要な操作を正しく実行するために新しいタスクおよびフェーズ機能を使用することができます。これらのオプションを使用して、定義済みフェーズで RPMs とパッチをインストールすることができます。これは、単一の開始または停止プロセスを実行し、単一の操作ですべてのレベルに対し前操作および後操作を実行する場合に役立ちます。

統合を行うには 4 つの方法があります。すべてのコマンドは、最上位のベースレベルまたはメンテナンスレベルのインストールスクリプトから実行する必要があります。

次に例を示します。

- 7.0 はベースバージョンです
- 7.0.1 はメンテナンスバージョンです
- 7.0.1.100 は 7.0.1 のパッチバージョンです
- 7.0.0.100 は 7.0 のパッチバージョンです

1. ベース + メンテナンス:

   この統合方法は、前のバージョンから 7.0.1 にインストールまたはアップグレードするときに使用することができます。

   次のコマンドを入力します。

   ```
   # installmr -base_path <path_to_base>
   ```

2. ベース + パッチ:

   この統合方法は、前のバージョンから 7.0.0.100 にインストールまたはアップグレードするときに使用することができます。

   次のコマンドを入力します。

   ```
   # installer -patch_path <path_to_patch>
   ```

3. メンテナンス + パッチ:

   この統合方法は、バージョン 7.0 から 7.0.1.100 にアップグレードするときに使用することができます。

   次のコマンドを入力します。

   ```
   # installmr -patch_path <path_to_patch>
   ```

4. ベース + メンテナンス + パッチ:

   この統合方法は、前のバージョンから 7.0.1.100 にインストールまたはアップグレードするときに使用することができます。

   次のコマンドを入力します。

   ```
   # installmr -base_path <path_to_base>
   -patch_path <path_to_patch>
   ```

メモ: 6.1 以降のリリースからは、*-patch_path <path_to_patch> -patch2_path <path_to_patch> ... -patch5_path <path_to_patch>* を使って最大 5 つのパッチを追加できます。

4

Storage Foundation のアップグレード

この章では以下の項目について説明しています。

以前のバージョンから 7.0 への Storage Foundation のアップグレード

以前のリリースの Storage Foundation を実行している場合は、この章で説明する手順に従って最新バージョンにアップグレードできます。

p.32 の「製品インストーラを使った Storage Foundation のアップグレード」を参照してください。

Storage Foundation 7.0 がすでにインストールされている状態でカーネルをアップグレードする必要がある場合は、カーネルのアップグレード手順を使います。

カーネルのアップグレードについては、『Storage Foundation 管理者ガイド』を参照してください。

製品インストーラを使った Storage Foundation のアップグレード

この手順を実行して、Storage Foundation（SF）にアップグレードします。

以前のバージョンから 7.0 に SF をアップグレードするには

1. スーパーユーザーとしてログインします。
2. 次のコマンドを使って、VxFS ファイルシステムまたはストレージチェックポイントがマウントされているかどうかを確認します。

   ```
   # df -k | grep vxfs
   ```

3. 次のコマンドを使って、すべての Storage Checkpoint とファイルシステムのマウントを解除します。

   ```
   # umount /checkpoint_name
   # umount /filesystem
   ```

4. すべてのファイルシステムが正常にマウント解除されたことを確認します。

   ```
   # echo "8192B.p S" | fsdb -t vxfs filesystem | grep clean
   flags 0 mod 0 clean clean_value
   ```

   clean_value の値が 0x5a の場合、ファイルシステムは正常にマウント解除されています。0x3c の場合、ファイルシステムは正常にマウント解除されていません。0x69 の場合、ファイルシステムが正常にマウント解除されたかどうかが不明です。正常にマウント解除されたかどうかが不明なファイルシステムでは、拡張処理が未完了です。

   次の手順を列挙されている順序で実行します。

   - ファイルシステムが正常にマウント解除されていない場合、そのファイルシステムに対して次のコマンドを実行します。

     ```
     # fsck -t vxfs filesystem
     # mount -t vxfs filesystem mountpoint
     # umount mountpoint
     ```

     これらのコマンドを実行すると、そのファイルシステム上で未完了であった拡張処理が完了し、ファイルシステムが正常にマウント解除されます。
     umount コマンドの実行が失敗して次のエラーが表示された場合、大きいサイズの RPM クローンを削除するための拡張処理が完了していない可能性があります。

     ```
     file system device busy
     ```

     次のメッセージがコンソールに表示された場合、拡張処理が未完了であると判断できます。

     ```
     Storage Checkpoint asynchronous operation on file_system
     file system still in progress.
     ```

- 拡張処理が未完了の場合、その拡張処理が完了するまで、そのファイルシステムをマウントしたままにしておく必要があります。RPM クローンのサイズがきわめて大きい場合、削除に数時間かかる可能性があります。
- この手順を再度実行し、ファイルシステムがマウント解除されたことを確認します。

5 キャッシュ領域がオンラインの場合は、VxVM RPM をアップグレードする前に、キャッシュ領域をオフラインにする必要があります。次のコマンドを使って、キャッシュ領域をオフラインにします。

```
# sfcache offline cachename
```

6 すべての VxVM ボリュームに対するアクティビティを停止します。たとえば、ボリュームにアクセスするデータベースなどのアプリケーションを停止し、ボリューム上に作成されたファイルシステムをマウント解除します。

7 各ディスクグループに対して次のコマンドを入力して、すべてのボリュームを停止します。

```
# vxvol -g diskgroup stopall
```

開かれたままになっているボリュームがないことを確認するには、次のコマンドを使います。

```
# vxprint -Aht -e v_open
```

8 /etc/fstab ファイルに定義された VxFS ファイルシステムのマウントポイントと VxVM ボリュームを記録します。フレッシュインストールが実行されたシステム上の /etc/fstab ファイルにこれらのエントリを再作成する必要があります。

9 必要なインストール前のチェックを実行します。

10 インストーラを起動するには、次の例のように CD-ROM 内の installer コマンドを実行します。

```
# cd /cdrom/cdrom0
# ./installer
```

11 アップグレードするには、G を入力して、Return キーを押します。

12 ソフトウェアがインストールされるシステム名（次の例では「host1」）を入力するよう求められます。システム名（1 つまたは複数）を入力し、Return キーを押します。

```
Enter the 64 bit <platform> system names separated
by spaces : [q, ?] host1host2
```

<プラットフォーム**>** は、RHEL6 のようなシステムが稼動するプラットフォームです。

既存の設定によっては、各種メッセージやプロンプトが表示される場合があります。プロンプトに適切に回答します。

システム検証段階では、ブートディスクがカプセル化されているかどうかとアップグレードのパスが確認されます。アップグレードがサポートされていない場合、ブートディスクをカプセル化を解除する必要があります。

13 エンドユーザー使用許諾契約の条件に同意するかどうかを尋ねられます。同意する場合は y を押して続行します。

14 インストーラが、アップグレードするいずれかのシステムにミラー化されカプセル化されたブートディスクがあるかどうかを検出します。ミラー化されたブートディスクがあるシステムでは、アップグレードを続行する前に、システムのブートディスクグループのバックアップを作成することができます。ブートディスクグループを分割してバックアップを作成する場合は、y を入力します。

15 バックアップブートディスクグループの名前を入力するようメッセージが表示されます。名前を入力するか、または Enter キーを押してデフォルトを受け入れます。

16 分割操作の開始を確認するメッセージが表示されます。y を押して続行します。

メモ: 分割操作には時間がかかることがあります。

---

17 製品プロセスを停止します。

```
Do you want to stop SF processes now? [y,n,q] (y) y
```

y を選択すると、インストーラはアップグレードを行う前に、製品のプロセスを停止し、いくつかの設定を更新します。

18 指定したRPMsの停止、アンインストール、再インストール、および起動が実行されます。

19 必要に応じて、**で記録した、各ノードの** /etc/fstab8 ファイルのマウントポイントを復元します。

20 すべてのボリュームを再起動するため、各ディスクグループに対して次のコマンドを実行します。

```
# vxvol -g diskgroup startall
```

21 すべてのノードで、すべての VxFS ファイルシステムとストレージチェックポイントを再マウントします。

```
# mount /filesystem
# mount /checkpoint_name
```

22 次のオプションの設定手順を実行できます。

- 現在、適切なライセンスがインストールされていない Storage Foundation 7.0 の機能を使う場合は、ライセンスを取得し、`vxlicinst` コマンドを実行してライセンスをシステムに追加します。
- VxFS ディスクレイアウトのバージョンと VxVM ディスクグループのバージョンをアップグレードするには、アップグレード手順を実行します。
  p.47 の「VxVM ディスクグループのバージョンのアップグレード」を参照してください。

23 この手順は、ミラー化されたルートディスクを分割してバックアップしたときにのみ実行します。ブートが正常に実行されたら、アップグレードを確認し、バックアップディスクグループを再結合します。アップグレードに失敗した場合は、バックアップディスクグループに戻してください。

p.45 の「現在のディスクグループへのバックアップブートディスクグループの再結合」を参照してください。

p.45 の「アップグレードに失敗した場合にバックアップブートディスクグループに戻す」を参照してください。

Volume Replicator のアップグレード

以前のバージョンの Volume Replicator（VVR）が設定されている場合、Storage Foundation 製品をアップグレードすると、製品インストーラが自動的に VVR をアップグレードします。

レプリケーションを中断せずにアップグレードするオプションが用意されています。

p.36 の「レプリケーションを中断しない VVR のアップグレード」を参照してください。

レプリケーションを中断しない VVR のアップグレード

ここでは、レプリケーションの進行中に、VVR を以前のバージョンから現在のバージョンにアップグレードするための手順を説明します。この手順では、RDS 内のすべてのホストを同時にアップグレードする必要はないことを前提としています。

また、複数のバージョン間でレプリケーションを設定する必要がある場合もあります。

p.26 の「前の VVR バージョンからのアップグレードの計画」を参照してください。

プライマリホストとセカンダリホストの両方に以前のバージョンの VVR がインストールされている場合、プライマリホストまたはセカンダリホストのいずれかでアップグレードを実行できます。セカンダリホストは、RDS 内のプライマリホストより前にアップグレードすることを推奨します。ここには、プライマリホストのアップグレードとセカンダリホストのアップグレードのための一連の手順が個別に含まれています。

メモ: クラスタを設定している場合、クラスタ内のすべてのノードを同時にアップグレードする必要があります。

セカンダリ上の VVR のアップグレード

次の手順に従って、セカンダリホストをアップグレードします。

セカンダリをアップグレードするには

1. 次のコマンドを使って、プライマリの一時停止を開始することによってセカンダリホストへのレプリケーションを停止します。

   ```
   # vradmin -g diskgroup pauserep local_rvgname sec_hostname
   ```

2. セカンダリ上の VVR 6.0 以降を VVR 7.0 にアップグレードします。

3. 次のいずれかを実行します。

   - ディスクグループを今すぐアップグレードします。次を入力します。

     ```
     # vxdg upgrade dgname
     ```

   - ディスクグループを後でアップグレードします。
     ディスクグループを後でアップグレードする場合、ディスクグループをアップグレードする前に、レプリケーションを必ず一時停止してください。また、レプリケーションを一時停止した後、プライマリおよびセカンダリのディスクグループをアップグレードします。

4. 次のコマンドを使って、プライマリからのレプリケーションを再開します。

   ```
   # vradmin -g diskgroup resumerep local_rvgname sec_hostname
   ```

プライマリ上での VVR のアップグレード

セカンダリをアップグレードした後、製品のインストーラを使ってプライマリをアップグレードします。

プライマリをアップグレードするには

1 次のコマンドを使ってプライマリの一時停止を開始することにより、プライマリホストへのレプリケーションを停止します。

```
# vradmin -g diskgroup pauserep local_rvgname
```

2 セカンダリ上の VVR 6.0 以降を VVR 7.0 にアップグレードします。

3 次のいずれかを実行します。

- ディスクグループを今すぐアップグレードします。次を入力します。

```
# vxdg upgrade dgname
```

- ディスクグループを後でアップグレードします。
ディスクグループを後でアップグレードする場合、ディスクグループをアップグレードする前に、レプリケーションを必ず一時停止してください。また、レプリケーションを一時停止した後、プライマリおよびセカンダリのディスクグループをアップグレードします。

4 次のコマンドを使って、プライマリからのレプリケーションを再開します。

```
# vradmin -g diskgroup resumerep local_rvgnamesec_hostname
```

p.26 の「前の VVR バージョンからのアップグレードの計画」を参照してください。

SFDB のアップグレード

SFDB ツールの 7.0 へのアップグレードがデフォルトで有効になっている場合、vxdbd デーモンが設定されていることを意味します。SFDB ツールが無効になっている場合、有効にすることができます。

SFDB ツールを有効にするには

1 root としてログインします。

2 次のコマンドを実行して、vxdbd デーモンを設定し、起動します。

```
# /opt/VRTS/bin/sfae_config enable
```

メモ: 認証設定を含む SFDB インストールを 7.0 にアップグレードすると、このコマンドはエラーにより失敗します。この問題を解決するには、SFDB 認証を再度設定してください。詳しくは、『Veritas InfoScale™ Storage and Availability Management for Oracle Databases』または『Veritas InfoScale™ DB2 データベース用ストレージと可用性管理』を参照してください。

5

応答ファイルを使用した SF 自動アップグレードの実行

この章では以下の項目について説明しています。

応答ファイルを使った SF のアップグレード

一般に、あるシステムで SF のアップグレードを実行した後にインストーラによって生成された応答ファイルは、他のシステムで SF をアップグレードするために使えます。

SF の自動アップグレードを実行するには

1. SF をアップグレードするシステムがアップグレード条件を満たしていることを確認します。
2. アップグレード前のタスクが完了していることを確認します。
3. SF をアップグレードするシステムに応答ファイルをコピーします。
4. 必要に応じて、応答ファイルの変数の値を編集します。
5. 製品ディスクをマウントし、インストールプログラムが含まれるフォルダに移動します。
6. 応答ファイルをコピーしたシステムからアップグレードを開始します。次に例を示します。

   ```
   # ./installer -responsefile /tmp/response_file
   ```

   ここで、/tmp/*response_file* は応答ファイルの絶対パス名です。

SF をアップグレードするための応答ファイルの変数

表 5-1 に、SF を設定するために定義できる応答ファイル変数の一覧を示します。

表 5-1 SF をアップグレードするための応答ファイルの変数

変数	説明
CFG{accepteula}	メディアの EULA.pdf ファイルに同意するかどうかを指定します。 リストまたはスカラー: スカラー オプションまたは必須: 必須
CFG{systems}	製品のインストールまたはアンインストールを行うシステムのリストです。 リストまたはスカラー: リスト オプションまたは必須: 必須
CFG{upgrade}	インストールされたすべての RPMs をアップグレードします。 リストまたはスカラー: リスト オプションまたは必須: 必須
CFG{keys}{keyless} CFG{keys}{license}	`CFG{keys}{keyless}` はシステムに登録されるキーレスキーのリストです。 `CFG{keys}{license}` はシステムに登録されるユーザー定義のキーのリストです。 リストまたはスカラー: リスト オプションまたは必須: 必須
CFG{opt}{keyfile}	すべてのリモートシステムとの通信に使う ssh キーファイルの場所を定義します。 リストまたはスカラー: スカラー オプションまたは必須: オプション
CFG{opt}{tmppath}	インストール中に必要な一時ファイルやRPMsを保管する作業ディレクトリの作成場所を定義します。デフォルトの場所は /var/tmp です。 リストまたはスカラー: スカラー オプションまたは必須: オプション

変数	説明
CFG{opt}{logpath}	ログファイルをコピーする場所を指定します。デフォルトの場所は /opt/VRTS/install/logs です。 リストまたはスカラー: スカラー オプションまたは必須: オプション
CFG{mirrordgname}{system}	ルート dg がカプセル化されていて、分割ミラーを選択している場合 システムのターゲットディスクグループ名を分割します。 リストまたはスカラー: スカラー オプションまたは必須: オプション
CFG{splitmirror}{system}	ルート dg がカプセル化されていて、分割ミラーを選択している場合 作成される分割ミラーバックアップディスクグループを必要とするシステムを指定します。 リストまたはスカラー: スカラー オプションまたは必須: オプション
CFG{opt}{disable_dmp_native_support}	1 に設定した場合は、ネーティブ LVM ボリュームグループと ZFS プールの Dynamic Multi-pathing サポートはアップグレード後に無効になります。アップグレード中にネーティブ LVM ボリュームグループと ZFS プールの Dynamic Multi-Pathing サポートを維持すると、システムに設定されたネーティブ LVM ボリュームグループと ZFS プールの数に応じて RPM のアップグレード時間が長くなります。 リストまたはスカラー: スカラー オプションまたは必須: オプション
CFG{opt}{patch_path}	複数のリリースを同時にインストールできるように、ベースレベルリリースまたはメンテナンスレベルリリースと統合するパッチレベルリリースのパスを定義します。 リストまたはスカラー: スカラー オプションまたは必須: オプション

変数	説明
CFG{opt}{patch2_path}	複数のリリースを同時にインストールできるように、ベースレベルリリースまたはメンテナンスレベルリリースと統合する 2 番目のパッチレベルリリースのパスを定義します。 リストまたはスカラー: スカラー オプションまたは必須: オプション
CFG{opt}{patch3_path}	複数のリリースを同時にインストールできるように、ベースレベルリリースまたはメンテナンスレベルリリースと統合する 3 番目のパッチレベルリリースのパスを定義します。 リストまたはスカラー: スカラー オプションまたは必須: オプション
CFG{opt}{patch4_path}	複数のリリースを同時にインストールできるように、ベースレベルリリースまたはメンテナンスレベルリリースと統合する 4 番目のパッチレベルリリースのパスを定義します。 リストまたはスカラー: スカラー オプションまたは必須: オプション
CFG{opt}{patch5_path}	複数のリリースを同時にインストールできるように、ベースレベルリリースまたはメンテナンスレベルリリースと統合する 5 番目のパッチレベルリリースのパスを定義します。 リストまたはスカラー: スカラー オプションまたは必須: オプション

SF アップグレードの応答ファイルサンプル

次の例は、Storage Foundation をキーレスライセンスキーでアップグレードするための応答ファイルを示しています。

```
our %CFG;

our %CFG;
$CFG{accepteula}=1;
$CFG{keys}{keyless}=[ qw(STORAGE) ];
$CFG{prod}="STORAGE70";
$CFG{opt}{upgrade}=1;
$CFG{systems}=[ qw(sys1) ];
1;
```

次の例は、Storage Foundation を永続ライセンスキーでアップグレードするための応答ファイルを示しています。

```
our %CFG;

$CFG{accepteula}=1;
$CFG{keys}{license}=[ qw(7.0SF_PermanentKey) ];
$CFG{opt}{noipc}=1;
$CFG{opt}{upgrade}=1;
$CFG{prod}="STORAGE70";
$CFG{systems}=[ qw(sys1) ];

1;
```

6

アップグレード後のタスクの実行

この章では以下の項目について説明しています。

オプションの設定手順

アップグレードが完了した後、追加の作業を実行する必要がある場合があります。

次のオプションの設定手順を実行できます。

- Volume Replicator（VVR）が設定されている場合は、次の手順をこの順番で実行します。
  - RLINK を再接続します。
  - SRL を関連付けます。

- ブートディスクのカプセル化とミラー化を行うには、『 Storage Foundation 管理者ガイド』の「ディスクの管理」の章に記載されている手順を実行します。
- VxFS ディスクレイアウトバージョンと VxVM ディスクグループのバージョンをアップグレードするには、アップグレード手順を実行します。
p.47 の「VxVM ディスクグループのバージョンのアップグレード」を参照してください。

現在のディスクグループへのバックアップブートディスクグループの再結合

アップグレード中、ミラー化されたブートディスクを分割した場合は、この手順を実行してバックアップブートディスクグループを再結合します。アップグレードが成功して再ブートしたら、ブートディスクグループを保持する必要はありません。

バックアップブートディスクグループを再結合するには

◆ *backup_bootdg* ディスクグループをブートディスクグループに再結合します。

```
# /etc/vx/bin/vxrootadm -Y join backup_bootdg
```

`-Y` オプションはサイレント操作を示します。*backup_bootdg* はアップグレード中に作成したバックアップブートディスクグループの名前です。

アップグレードに失敗した場合にバックアップブートディスクグループに戻す

この手順は、アップグレードが失敗し、そのアップグレード中にミラー化されたブートディスクを分割してバックアップした場合に実行します。アップグレードしたときに作成したバックアップに戻すことができます。

アップグレードに失敗した場合にバックアップブートディスクグループに戻すには

1 ブートディスクグループを確認するには、`vxprint` コマンドの出力で *rootvol* ボリュームを探します。

```
# vxprint
```

2 `vxdg` コマンドを使って、現在ブートを実行しているブートディスクグループを特定します。

```
# vxdg bootdg
```

3 バックアップブートディスクグループからオペレーティングシステムをブートします。

4 バックアップディスクグループに元のブートディスクグループを結合します。

```
# /etc/vx/bin/vxrootadm -Y join original_bootdg
```

-Y オプションはサイレント操作を示します。*original_bootdg* は不要になったブートディスクグループです。

自動アップグレードが失敗した場合の VVR のリカバリ

設定段階でアップグレードが失敗した場合、VVR アップグレードディレクトリを表示した後に設定を復元してからアップグレードを再試行する必要があります。設定を復元するには、アップグレードディレクトリ内のスクリプトを次の順番で実行します。

```
# restoresrl
# adddcm
# srlprot
# attrlink
# start.rvg
```

設定の復元後、現在の手順は再試行できます。

ディスクレイアウトバージョンのアップグレード

このリリースでは、ディスクレイアウトバージョンが 7、8、9、10 のファイルシステムのみ作成してマウントできます。ディスクレイアウトバージョン 6 は、以降のディスクレイアウトバージョンにアップグレードする目的にかぎり、ローカルマウントのみを実行できます。

メモ: 64 ビットのクォータを使う予定の場合、最新のディスクレイアウトバージョン 10 にアップグレードする必要があります。 それ以前のディスクレイアウトバージョンで 64 ビットのクォータを使うことはこのリリースでは推奨されません。

ディスクレイアウトバージョン 6 は非推奨であり、ディスクレイアウトバージョン 6 のある既存ファイルシステムはクラスタマウントできません。ディスクレイアウトバージョン 6 のあるクラスタファイルシステムをアップグレードするには、ファイルシステムをローカルマウントしてファイルシステムをアップグレードし、次に以降バージョンに vxupgrade ユーティリティを使ってファイルシステムをアップグレードします。

ディスクレイアウトバージョンをアップグレードするには

- ディスクレイアウトバージョン 6 からバージョン 10 にするには、このファイルシステムのディスクレイアウトを段階的にアップグレードする必要があります。次に例を示します。

```
# vxupgrade -n 7 /mnt
# vxupgrade -n 8 /mnt
# vxupgrade -n 9 /mnt
# vxupgrade -n 10 /mnt
```

vxupgrade(1M)マニュアルページを参照してください。

ディスクレイアウトバージョン 4 がある既存のファイルシステムは、vxfsconvert コマンドを使ってディスクレイアウトバージョン 7 以降にアップグレードする必要があります。

vxfsconvert(1M)マニュアルページを参照してください。

メモ: シマンテック社はこのリリースをアップグレードする前に、最もサポートが高いのディスクレイアウトバージョンに既存ファイルシステムをアップグレードすることを推奨します。一度ディスクレイアウトバージョンをアップグレードしたら、以前のバージョンにダウングレードすることはできません。

ファイルシステムのディスクレイアウトバージョンは、次のコマンドを使って確認できます。

```
# fstyp -v /dev/vx/dsk/dg1/vol1 | grep -i version
```

ディスクレイアウトバージョンについて詳しくは、『Storage Foundation 管理者ガイド』を参照してください。

VxVM ディスクグループのバージョンのアップグレード

Veritas Volume Manager の各ディスクグループには、バージョン番号が関連付けられています。VxVM の各リリースでは、それぞれ特定のディスクグループバージョンがサポートされます。VxVM では、該当するバージョンのディスクグループ上のタスクをインポートして実行することができます。一部の新しい機能とタスクは現在のディスクグループバージョンのディスクグループのみで動作します。タスクを実行したり機能を使ったりする前に、既存のディスクグループをアップグレードしてください。

7.0 の Veritas Volume Manager ディスクグループバージョンは、旧リリースの VxVM のものと異なります。VxVM の前のリリースからアップグレードする場合は、ディスクグループバージョンをアップグレードすることをお勧めします。

SF 7.0 にアップグレードした後で、ISP によって編成されるすべての既存のディスクグループをアップグレードする必要があります。バージョンのアップグレードなしで、設定のクエリー操作はうまく働き続けます。ただし、設定変更操作は正しく機能しません。

ISP ディスクグループについて詳しくは、『Storage Foundation 管理者ガイド』を参照してください。

ディスクグループのバージョンを確認するには、次のコマンドを使います。

```
# vxdg list diskgroup
```

ディスクグループを現在のディスクグループバージョンにアップグレードするには、次のコマンドを使います。

```
# vxdg upgrade diskgroup
```

ディスクグループのバージョンについて詳しくは、『Storage Foundation 管理者ガイド』を参照してください。

変数の更新

/etc/profile で、PATH 変数と MANPATH 変数を必要に応じて更新してください。

MANPATH に /opt/VRTS/man、PATH に /opt/VRTS/bin が含まれている可能性があります。

デフォルトディスクグループの設定

システム全体のデフォルトのディスクグループを作成しておくと便利です。デフォルトディスクグループの作成の主要な利点は VxVM コマンドでデフォルトディスクグループがデフォルトで使われることです。-g オプションを使う必要はありません。

システムで次のコマンドを実行すると、インストール後にデフォルトのディスクグループ名を設定できます。

```
# vxdctl defaultdg diskgroup
```

詳しくは、『Storage Foundation 管理者ガイド』を参照してください。

Storage Foundation のアップグレードの確認

『Veritas InfoScale インストールガイド』の「Verifying the Veritas InfoScale installation」の章を参照してください。

3

設定後のタスク

- 第7章 設定タスクの実行

7

設定タスクの実行

この章では以下の項目について説明しています。

クォータの切り替え

すべてのノードを 7.0 にアップグレードすると、グループとユーザーのクォータが無効にされていた場合は有効になります。

グループとユーザーのクォータを有効にするには

◆ クォータの切り替え:

```
# vxquotaon -av
```

ネーティブデバイスの DMP サポートの有効化

Dynamic Multi-Pathing（DMP）は SF のコンポーネントです。DMP は、DMP メタデバイス上の VxVM（Veritas Volume Manager）ボリュームと、それらのボリューム上の VxFS（Veritas File System）ファイルシステムをサポートします。

また、DMP は DMP デバイスのネーティブオペレーティングシステムのボリュームおよびファイルシステムに対するマルチパス機能も提供します。

ネーティブデバイスでの DMP の使用について詳しくは、『Dynamic Multi-Pathing 管理者ガイド』を参照してください。

初めて SF をインストールした後、次の手順に従ってネーティブデバイスの DMP サポートを有効にします。

SF をアップグレードする前からネーティブデバイスの DMP ネーティブサポートがシステムで有効になっている場合は、SF がアップグレードされるときに DMP ネーティブサポートは保持されます。

ネーティブデバイスの DMP サポートを有効化するには

- チューニングパラメータをオンにして DMP サポートを有効にする:

```
# vxdmpadm settune dmp_native_support=on
```

`dmp_native_support`パラメータには持続性があります。

SFDB ツールの認証の設定について

Storage Foundation for Databases（SFDB）ツールの認証を設定するには、次のタスクを実行します。

認証を必要とするための `vxdbd` デーモンの設定	p.51 の「SFDB ツール認証のための vxdbd の設定」を参照してください。
SFDB ツールに対して認証を使用しているクラスタへのノードの追加	

SFDB ツール認証のための vxdbd の設定

vxdbd を設定するには、root ユーザーとして次の手順を実行します

1. 認証サービスを設定する `sfae_auth_op` コマンドを実行します。

```
# /opt/VRTS/bin/sfae_auth_op -o setup
Setting up AT
Starting SFAE AT broker
Creating SFAE private domain
Backing up AT configuration
Creating principal for vxdbd
```

2. `vxdbd` デーモンを停止します。

```
# /opt/VRTS/bin/sfae_config disable
vxdbd has been disabled and the daemon has been stopped.
```

3 /etc/vx/vxdbed/admin.properties 設定ファイルの AUTHENTICATION キーを yes に設定して、認証を有効にします。

/etc/vx/vxdbed/admin.properties が存在しない場合、cp /opt/VRTSdbed/bin/admin.properties.example /etc/vx/vxdbed/admin.properties を使用します。

4 vxdbd デーモンを起動します。

```
# /opt/VRTS/bin/sfae_config enable
vxdbd has been enabled and the daemon has been started.
It will start automatically on reboot.
```

vxdbd デーモンは認証を必要とするように設定されました。

4

設定およびアップグレードの参照

- 付録 A. セキュアシェルまたはリモートシェルの通信用の設定

A

セキュアシェルまたはリモートシェルの通信用の設定

この付録では以下の項目について説明しています。

製品インストール前のセキュアシェルまたはリモートシェル通信モードの設定について

Veritas InfoScale ソフトウェアをリモートシステムからインストールしたり、システムをインストールして設定したりするには、ノード間で通信を確立する必要があります。インストーラが実行されるシステムには、rsh（リモートシェル）ユーティリティまたは ssh（セキュアシェル）ユーティリティを実行する権限が必要となります。インストーラは、Veritas InfoScale ソフトウェアをインストールするシステムでスーパーユーザー権限を使って実行する必要があります。

セキュアシェル（ssh）またはリモートシェル（rsh）を使って製品をリモートシステムにインストールできます。シマンテック社では、rsh よりも安全な ssh を使うことをお勧めします。

メモ: SELinux を有効にした RHEL5/OEL5 システム上にインストールするときは、RedHat の SELinux ポリシー制約のため、ssh のみがサポートされます。

様々な方法で ssh および rsh の接続を設定できます。

- UNIX シェルコマンドを使って手動で SSH と RSH の接続を設定できます。
- `installer -comsetup` コマンドを実行して SSH と RSH 接続を対話的に設定できます。
- パスワードユーティリティ `pwdutil.pl` を実行できます。

この項では、パスワードを使用せずに ssh の通信を設定する方法を説明します。この例では、インストールディレクトリのあるソースシステム（sys1）と、ターゲットシステム（sys2）の間に ssh を設定します。この手順は、ターゲットシステムが複数ある場合にも当てはまります。

メモ: 製品のインストーラではパスワード不要の通信を確立できます。

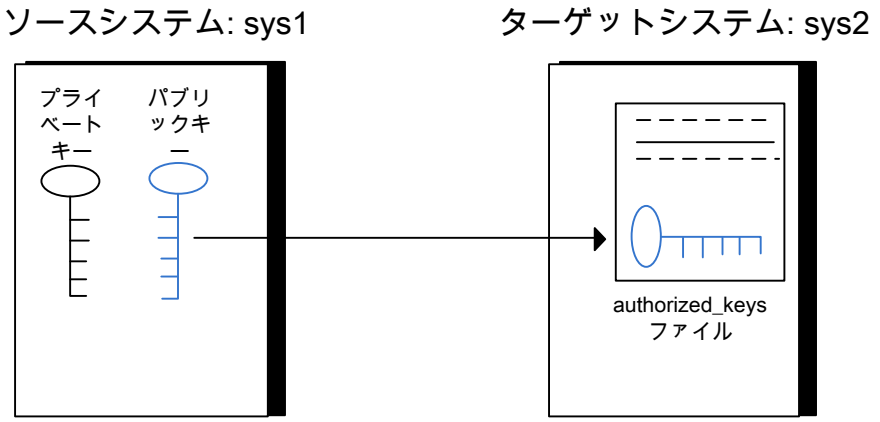
パスワードなし ssh の手動設定

ssh プログラムを使うことで、リモートシステムにログインしてコマンドを実行できます。ssh によって、安全でないネットワーク上の 2 つの信頼できないホスト間で、暗号化通信と認証処理を実現できます。

この手順では、最初に DSA キーペアを作成します。キーペアから、ソースシステムからの公開キーをターゲットシステム上の authorized_keys ファイルに追加します。

図 A-1 に、この手順を示します。

図 A-1　DSA キーペアを作成してターゲットシステムに追加する



ssh を有効にする前に、ssh のマニュアルとオンラインマニュアルページをお読みください。ssh の設定に関する問題が発生した場合は、オペレーティングシステムサポートプロバイダにお問い合わせください。

オンラインマニュアルやその他のリソースを利用するには、http://openssh.org にある OpenSSH の Web サイトにアクセスしてください。

DSA キーペアを作成するには

1　ソースシステム（sys1）で、root としてログインし、ルートディレクトリに移動します。

```
sys1 # cd /root
```

2　ソースシステムで DSA キーのペアを生成するには、次のコマンドを入力します。

```
sys1 # ssh-keygen -t dsa
```

以下に類似したシステム出力が表示されます。

```
Generating public/private dsa key pair.
Enter file in which to save the key (/root/.ssh/id_dsa):
```

3　Enter キーを押して、デフォルトの `/root/.ssh/id_dsa` ディレクトリを受け入れます。

4 パスフレーズの入力を求められたら、Enter キーを 2 回押します。

```
Enter passphrase (empty for no passphrase):
```

パスフレーズを入力しません。Enter キーを押します。

```
Enter same passphrase again:
```

Enter キーを再度押します。

5 次の行のような出力が表示されます。

```
Your identification has been saved in /root/.ssh/id_dsa.
Your public key has been saved in /root/.ssh/id_dsa.pub.
The key fingerprint is:
1f:00:e0:c2:9b:4e:29:b4:0b:6e:08:f8:50:de:48:d2 root@sys1
```

安全なファイル転送を使って、ソースシステムからの公開キーをターゲットシステムの authorized_keys ファイルに追加するには

1 ソースシステム（sys1）からターゲットシステム（sys2）上の一時ファイルに公開キーを移動します。

SFTP（Secure File Transfer Program）を使います。

この例では、ルートディレクトリ内のファイル名 id_dsa.pub が、公開キーの一時ファイルの名前です。

安全なファイル転送のために次のコマンドを使ってください。

```
sys1 # sftp sys2
```

このシステムで安全なファイル転送が初めて設定された場合、以下のような出力が表示されます。

```
Connecting to sys2 ...
The authenticity of host 'sys2 (10.182.00.00)'
can't be established. DSA key fingerprint is
fb:6f:9f:61:91:9d:44:6b:87:86:ef:68:a6:fd:88:7d.
Are you sure you want to continue connecting (yes/no)?
```

2 「yes」と入力します。

以下のような出力が表示されます。

```
Warning: Permanently added 'sys2,10.182.00.00'
(DSA) to the list of known hosts.
root@sys2 password:
```

3 sys2 の root パスワードを入力します。

4 sftp プロンプトで、次のコマンドを入力します。

```
sftp> put /root/.ssh/id_dsa.pub
```

次の出力が表示されます。

```
Uploading /root/.ssh/id_dsa.pub to /root/id_dsa.pub
```

5 SFTP セッションを終了するため、次のコマンドを入力します。

```
sftp> quit
```

6 ターゲットシステムの authorized_keys ファイルに id_dsa.pub キーを追加します。ターゲットシステム(この例では sys2)で ssh セッションを開始するには、sys1 で次のコマンドを入力します。

```
sys1 # ssh sys2
```

プロンプトで sys2 の root パスワードを入力します。

```
password:
```

sys2 で次のコマンドを入力します。

```
sys2 # cat /root/id_dsa.pub >> /root/.ssh/authorized_keys
sys2 # rm  /root/id_dsa.pub
```

7 ソースインストールシステム上で次のコマンドを実行します。ssh セッションが期限切れになるか終了した場合は、これらのコマンドを実行してセッションを更新することもできます。プライベートキーがシェル環境に追加され、root ユーザーがグローバルに使えるようになります。

```
sys1 # exec /usr/bin/ssh-agent $SHELL
sys1 # ssh-add

  Identity added: /root/.ssh/id_dsa
```

これはシェル固有の手順で、シェルがアクティブである間のみ使えます。セッション中にシェルを閉じた場合は、手順をもう一度実行する必要があります。

ターゲットシステムに接続できることを確認するには

1 ソースシステム（sys1）で次のコマンドを入力します。

```
sys1 # ssh -l root sys2 uname -a
```

sys2 は、ターゲットシステムの名前です。

2 このコマンドはソースシステム（sys1）からターゲットシステム（sys2）に実行され、パスフレーズやパスワードは要求されなくなります。

3 ターゲットシステムごとにこの手順を繰り返します。

installer -comsetup コマンドを使用した ssh および rsh 接続の設定

installer -comsetup コマンドを使用して対話形式で ssh および rsh の接続を設定できます。

次を入力します。

```
# ./installer -comsetup

Input the name of the systems to set up communication:
Enter the <platform> system names separated by spaces:
[q,?] sys2
Set up communication for the system sys2:

  Checking communication on sys2 ..................... Failed

CPI ERROR V-9-20-1303 ssh permission was denied on sys2. rsh
permission was denied on sys2. Either ssh or rsh is required
to be set up and ensure that it is working properly between the local
node and sys2 for communication

Either ssh or rsh needs to be set up between the local system and
sys2 for communication

Would you like the installer to setup ssh or rsh communication
automatically between the systems?
Superuser passwords for the systems will be asked. [y,n,q,?] (y) y

Enter the superuser password for system sys2:

     1)  Setup ssh between the systems
```

```
     2)  Setup rsh between the systems
     b)  Back to previous menu

Select the communication method [1-2,b,q,?] (1) 1

Setting up communication between systems. Please wait.
Re-verifying systems.

 Checking communication on sys2 ..................... Done

Successfully set up communication for the system sys2
```

pwdutil.pl ユーティリティを使用した ssh および rsh 接続の設定

pwdutil.pl パスワードユーティリティは、scripts ディレクトリの下にバンドルされています。ユーザーはこのユーティリティをスクリプトで実行して、ssh および rsh 接続を自動的に設定できます。

```
# ./pwdutil.pl -h
Usage:

Command syntax with simple format:

    pwdutil.pl check|configure|unconfigure ssh|rsh <hostname|IP addr>
    [<user>] [<password>] [<port>]

Command syntax with advanced format:

    pwdutil.pl [--action|-a 'check|configure|unconfigure']
               [--type|-t 'ssh|rsh']
               [--user|-u  '<user>']
               [--password|-p '<password>']
               [--port|-P '<port>']
               [--hostfile|-f '<hostfile>']
               [--keyfile|-k '<keyfile>']
               [-debug|-d]
               <host_URI>

    pwdutil.pl -h | -?
```

表 A-1 pwdutil.pl ユーティリティのオプション

オプション	使用法
--action|-a 'check|configure|unconfigure'	処理の種類を指定します。デフォルトは「検査」です。
--type|-t 'ssh|rsh'	接続の種類を指定します。フォルトは「ssh」です。
--user|-u '<user>'	ユーザー ID を指定します。デフォルトはローカルユーザー ID です。
--password|-p '<password>'	ユーザーのパスワードを指定します。デフォルトはユーザー ID です。
--port|-P '<port>'	ssh 接続のポート番号を指定します。デフォルトは 22 です。
--keyfile|-k '<keyfile>'	プライベートキーファイルを指定します。
--hostfile|-f '<hostfile>'	ホストをリストするファイルを指定します。
-debug	デバッグ情報を印刷します。
-h|-?	ヘルプメッセージを印刷します。
<host_URI>	次の形式で指定できます。 <hostname> <user>:<password>@<hostname> <user>:<password>@<hostname>: <port>

pwdutil.pl ユーティリティを使用して ssh または rsh を確認、設定、設定解除できます。次に例を示します。

- 1 ホストだけで ssh 接続を確認するには:

```
pwdutil.pl check ssh hostname
```

- 1 ホストだけで ssh を設定するには:

```
pwdutil.pl configure ssh hostname user password
```

- 1 ホストだけで rsh を設定解除するには:

```
pwdutil.pl unconfigure rsh hostname
```

- 同じユーザー ID とパスワードで複数のホストの ssh を設定するには:

```
pwdutil.pl -a configure -t ssh -u user -p password hostname1
hostname2 hostname3
```

- 異なるユーザー ID とパスワードで異なるホストの ssh または rsh を設定するには:

```
pwdutil.pl -a configure -t ssh user1:password1@hostname1
user2:password2@hostname2
```

- 1 つの設定ファイルで、複数のホストの ssh か rsh を確認または設定するには:

```
pwdutil.pl -a configure -t ssh --hostfile /tmp/sshrsh_hostfile
```

- ホスト設定ファイルの機密性を保持するために、サードパーティのユーティリティを使用して、ホストファイルをパスワードで暗号化および暗号解除することができます。次に例を示します。

```
### run openssl to encrypt the host file in base64 format
# openssl aes-256-cbc -a -salt -in /hostfile -out /hostfile.enc
enter aes-256-cbc encryption password: <password>
Verifying - enter aes-256-cbc encryption password: <password>

### remove the original plain text file
# rm /hostfile

### run openssl to decrypt the encrypted host file
# pwdutil.pl -a configure -t ssh `openssl aes-256-cbc -d -a
-in /hostfile.enc`
enter aes-256-cbc decryption password: <password>
```

- デフォルトの $HOME/.ssh ディレクトリにない ssh 認証キーを使うには、--keyfilfile オプションを使用して、ssh のキーを指定することができます。次に例を示します。

```
### create a directory to host the key pairs:
# mkdir /keystore

### generate private and public key pair under the directory:
# ssh-keygen -t rsa -f /keystore/id_rsa

### setup ssh connection with the new generated key pair under
the directory:
# pwdutil.pl -a configure -t ssh --keyfile /keystore/id_rsa
user:password@hostname
```

次のコマンドを使用して、設定ファイルの内容を参照できます。

```
# cat /tmp/sshrsh_hostfile
user1:password1@hostname1
user2:password2@hostname2
user3:password3@hostname3
user4:password4@hostname4

# all default: check ssh connection with local user
hostname5
The following exit values are returned:

0     Successful completion.
1     Command syntax error.
2     Ssh or rsh binaries do not exist.
3     Ssh or rsh service is down on the remote machine.
4     Ssh or rsh command execution is denied due to password is required.
5     Invalid password is provided.
255   Other unknown error.
```

ssh セッションの再起動

この手順が完了した後に、次のシナリオのいずれかで ssh を再起動できます。

- ターミナルセッションが閉じた後
- 新しいターミナルセッションが開いた後
- システムが再起動した後
- ssh を起動してから長い時間が経過し、ssh を更新する必要がある場合

ssh を再起動するには

1. ソースインストールシステム（sys1）で、秘密キーをシェル環境に追加します。

   ```
   sys1 # exec /usr/bin/ssh-agent $SHELL
   ```

2. root ユーザーがそのキーをグローバルに使えるようにします。

   ```
   sys1 # ssh-add
   ```

Linux の rsh の有効化

次の項では、リモートシェルを有効にする方法について説明します。

Veritas InfoScale 製品のインストールのためにセキュアシェル環境を設定することを推奨します。

p.55 の「パスワードなし ssh の手動設定」を参照してください。

リモートシェルの設定について詳しくは、オペレーティングシステムのマニュアルを参照してください。

rhel6/sles の rsh を有効にするには

1. rsh および rsh-server RPMs がインストールされていることを確認するには、次のコマンドを入力します。

   ```
   # rpm -qa | grep -i rsh
   ```

   /etc/securetty ファイルにまだ「rsh」行がない場合は、次のコマンドを入力して追加します。

   ```
   # echo "rsh" >> /etc/securetty
   ```

2. /etc/xinetd.d/rsh ファイル内の disable = no 行を修正します。

3. /etc/pam.d/rsh ファイル内で、auth タイプを required から sufficient に変更します。

   ```
   auth      sufficient
   ```

4. 「promiscuous」フラグを /etc/pam.d/rsh and /etc/pam.d/rlogin の項目「pam_rhosts_auth.so」の後に追加します。

5. rsh サーバーを有効にするには、次のコマンドを入力します。

   ```
   # chkconfig rsh on
   ```

6. .rhosts ファイルを修正します。.rhosts ファイルの各行には、各リモートシステムの完全修飾ドメイン名または IP アドレスが記述されています。このファイルには、ローカルシステムへのアクセス権を持っているユーザーの名前も記述されています。たとえば、ルートユーザーが sys1 に sys2 からリモートアクセスする必要がある場合は、sys2 のエントリを追加します。次のコマンドを入力して、sys1 の .rhosts ファイルに *companyname*.com を行います。

   ```
   # echo "sys2.companyname.com" >> $HOME/.rhosts
   ```

7. Veritas InfoScale 製品をインストールします。

rhel6/sles の rsh を無効にするには

1 /etc/securetty ファイル内の rsh エントリを削除します。

2 次のコマンドを入力することで rsh サーバーを無効にします。

```
# chkconfig rsh off
```

3 インストール手順を完了したら、セキュリティを確保するため、各ユーザーの $HOME ディレクトリから .rhosts ファイルを削除します。

```
# rm -f $HOME/.rhosts
```

rhel7 の rsh を有効にするには

◆ 次のコマンドを実行すると、rsh パスワードなし接続が有効になります。

```
# systemctl start rsh.socket
# systemctl start rlogin.socket
# systemctl enable rsh.socket
# systemctl enable rlogin.socket
# echo rsh >> /etc/securetty
# echo rlogin >> /etc/securetty
#echo "+ +" >> /root/.rhosts
```

rhel7 の rsh を無効にするには

◆ 次のコマンドを実行すると、rsh パスワードなし接続が無効になります。

```
# systemctl stop rsh.socket
# systemctl stop rlogin.socket
# systemctl disable rsh.socket
# systemctl disable rlogin.socket
```

索引