

# Storage Foundation 7.2 設定 およびアップグレードガイド- Linux

# Storage Foundation 設定/アップグレードガイド

最終更新: 2016-11-29

マニュアルのバージョン: 7.2 Rev 1

## 法的通知と登録商標

Copyright © 2016 Veritas Technologies LLC. All rights reserved.

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

この製品には、サードパーティへの著作権を示す必要のあるサードパーティのソフトウェアが含まれる場合があります（「サードパーティプログラム」）。一部のサードパーティプログラムは、オープンソースまたはフリーウェアのライセンスの下で利用できます。このソフトウェアに付属の使用許諾契約によって、このようなオープンソースまたはフリーウェアのライセンスでお客様が有することのできる権利または義務は変更されないものとします。この Veritas 製品に伴うサードパーティの法的通知と登録商標の文書、または以下を参照してください。

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

本書に記載の製品は、ライセンスに基づいて配布され、使用、コピー、配布、逆コンパイル、リバースエンジニアリングはそのライセンスによって制限されます。本書のいかなる部分も、Veritas Technologies LLC とそのライセンサーの書面による事前の許可なく、いかなる形式、方法であっても複製することはできません。

本書は「現状有姿のまま」提供され、商品性、特定目的への適合性、不侵害の黙示的な保証を含む、すべての明示的または黙示的な条件、表明、保証は、この免責が法的に無効であるとみなされないかぎり、免責されるものとします。VERITAS TECHNOLOGIES LLC は、本書の供給、性能、使用に関係する付随的または間接的損害に対して責任を負わないものとします。本書に記載の情報は、予告なく変更される場合があります。

ライセンスソフトウェアおよびマニュアルは、FAR 12.212 の規定によって商業用コンピュータソフトウェアと見なされ、Veritas 社によりオンプレミスで提供されるかホストされたサービスとして提供されるかに関わらず、FAR Section 52.227-19「Commercial Computer Software - Restricted Rights」および DFARS 227.7202「Commercial Computer Software and Commercial Computer Software Documentation」、その他の後継規制の規定により制限された権利の対象となります。使用許諾されたソフトウェアおよび文書の米国政府による修正、再生リリース、履行、表示または開示は、この契約の条件に従って行われます。

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

<http://www.veritas.com>

## テクニカルサポート

テクニカルサポートはグローバルにサポートセンターを管理しています。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。サポート内容およびテクニカルサポートの利用方法に関する情報については、次の **Web** サイトにアクセスしてください。

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

Veritas Account 情報は、次の URL で管理できます。

<https://my.veritas.com>

現在のサポート契約についてご不明な点がある場合は、次に示すお住まいの地域のサポート契約管理チームに電子メールでお問い合わせください。

世界中 (日本以外)

[CustomerCare@veritas.com](mailto:CustomerCare@veritas.com)

日本

[CustomerCare\\_Japan@veritas.com](mailto:CustomerCare_Japan@veritas.com)

## マニュアル

マニュアルが最新版であることを確認してください。各マニュアルの 2 ページ目には最新更新日が記載されています。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。最新のマニュアルはベリタスの **Web** サイトで入手できます。

<https://sort.veritas.com/documents>

## マニュアルに関するご意見やご感想

ご意見、ご感想をお待ちしています。マニュアルに対する改善点の提案や誤植や抜けについての報告をお願いします。送信の際は、マニュアルの題名とバージョン、章、セクションのタイトルを明記してください。次の宛先にお送りください。

[doc.feedback@veritas.com](mailto:doc.feedback@veritas.com)

また、ベリタスのコミュニティサイトで、マニュアル情報を確認したり質問したりできます。

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

## Veritas SORT (Services and Operations Readiness Tools)

Veritas SORT (Services and Operations Readiness Tools) は、時間のかかる特定の管理タスクを自動化および単純化するための情報とツールを提供する **Web** サイトです。製品に応じて、SORT はインストールとアップグレードの準備、データセンターのリスクの識別、効率性の改善に役立ちます。使用している製品に対して SORT が提供しているサービスおよびツールについては、次のデータシートを参照してください。

[https://sort.veritas.com/data/support/SORT\\_Data\\_Sheet.pdf](https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf)

<b>第 1 部</b>	<b>Storage Foundation の概要および設定</b>	<b>7</b>
<b>第 1 章</b>	<b>Storage Foundation の概要</b>	<b>8</b>
	Storage Foundation について	8
	Veritas Replicator Option について	9
	Veritas InfoScale Operations Manager について	9
	Veritas SORT (Services and Operations Readiness Tools) について	9
<b>第 2 章</b>	<b>Storage Foundation の設定</b>	<b>11</b>
	インストーラを使った Storage Foundation の設定	11
	SF の手動設定	12
	Veritas Volume Manager の設定	12
	Veritas File System の設定	12
	SFDB の設定	14
<b>第 2 部</b>	<b>Storage Foundation のアップグレード</b>	<b>15</b>
<b>第 3 章</b>	<b>Storage Foundation のアップグレード計画</b>	<b>16</b>
	アップグレードについて	16
	サポートされているアップグレードパス	17
	SF のアップグレードの準備	22
	アップグレードの準備	22
	バックアップの作成	23
	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	24
	Volume Replicator のアップグレード前の計画	24
	アレイサポートのアップグレード	27
	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	27

<b>第 4 章</b>	<b>Storage Foundation のアップグレード</b> .....	31
	以前のバージョンから 7.2 への Storage Foundation のアップグレード	
	.....	31
	製品インストーラを使った Storage Foundation のアップグレード ....	
	3 1	
	Volume Replicator のアップグレード .....	35
	レプリケーションを中断しない VVR のアップグレード .....	35
	SFDB のアップグレード .....	37
<b>第 5 章</b>	<b>応答ファイルを使用した SF 自動アップグレードの 実行</b> .....	38
	応答ファイルを使った SF のアップグレード .....	38
	SF をアップグレードするための応答ファイルの変数 .....	39
	SF アップグレードの応答ファイルサンプル .....	41
<b>第 6 章</b>	<b>アップグレード後のタスクの実行</b> .....	43
	オプションの設定手順 .....	43
	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	
	.....	44
	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 .....	44
	自動アップグレードが失敗した場合の VVR のリカバリ .....	45
	DAS ディスク名をリセットして FSS 環境のホスト名を含める .....	45
	ディスクレイアウトバージョンのアップグレード .....	45
	VxVM ディスクグループのバージョンのアップグレード .....	46
	変数の更新 .....	47
	デフォルトディスクグループの設定 .....	47
	Storage Foundation のアップグレードの確認 .....	48
<b>第 3 部</b>	<b>設定後のタスク</b> .....	49
<b>第 7 章</b>	<b>設定タスクの実行</b> .....	50
	クォータの切り替え .....	50
	ネイティブデバイスの DMP サポートの有効化 .....	50
	SFDB ツールの認証の設定について .....	51
	SFDB ツール認証のための vxdbd の設定 .....	51

第 4 部	設定およびアップグレードの参照 .....	53
付録 A	インストールスクリプト .....	54
	インストールスクリプトオプション .....	54
	postcheck オプションの使用について .....	59
付録 B	セキュアシェルまたはリモートシェルの通信用の設定 .....	62
	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 .....	62
	パスワードなし ssh の手動設定 .....	63
	installer -comsetup コマンドを使用した ssh および rsh 接続の設定 .....	67
	pwdutil.pl ユーティリティを使用した ssh および rsh 接続の設定 .....	68
	ssh セッションの再起動 .....	71
	Linux の rsh の有効化 .....	72
索引	.....	74

# 1

## Storage Foundation の概要 および設定

- [第1章 Storage Foundation の概要](#)
- [第2章 Storage Foundation の設定](#)

# 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](#)
- [Veritas InfoScale Operations Manager について](#)
- [Veritas SORT \(Services and Operations Readiness Tools\) について](#)

## 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 <https://sort.veritas.com/> 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、<https://www.veritas.com/product/storage-management/infoscale-operations-manager> 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。

## Veritas SORT (Services and Operations Readiness Tools) について

Veritas SORT (Services and 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。SORT により、データセンターをさらに効率的に管理し、Veritas 製品を最大限に活用できるようになります。

SORT によって実行できるようになる操作は、次のとおりです。

- |                          |   |
|--------------------------|---|
| 次のインストールまたはアップグレードのための準備 | <ul style="list-style-type: none"><li>■ 製品のインストールとアップグレードの必要条件(オペレーティングシステムバージョン、メモリ、ディスク容量、アーキテクチャを含む)を一覧表示する。</li><li>■ Veritas 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ないかどうかを判断するためにシステムを分析する。</li><li>■ 中央リポジトリから最新のパッチ、マニュアル、高可用性エージェントをダウンロードする。</li><li>■ ハードウェア、ソフトウェア、データベース、オペレーティングシステムの最新の互換性リストにアクセスする。</li></ul> |
| リスクの管理                   | <ul style="list-style-type: none"><li>■ 中央リポジトリにあるパッチ、アレイ固有のモジュール (ASL、APM、DDI、DDL)、高可用性エージェントの変更について自動電子メール通知を取得する。</li><li>■ システムと環境におけるリスクを識別して軽減する。</li><li>■ 何百もの Veritas エラーコードの説明と解決策を表示する。</li></ul>  |
| 効率の向上                    | <ul style="list-style-type: none"><li>■ 製品のバージョンとプラットフォームに基づいてパッチを検索してダウンロードする。</li><li>■ インストール済みの Veritas 製品とライセンスキーを一覧表示する。</li><li>■ 環境をチューニングして最適化する。</li></ul>  |

---

**メモ:** SORT の機能の一部はすべての製品で使用できません。SORT へは追加料金なしでアクセスできます。

---

SORT にアクセスするには、次に移動してください。

<https://sort.veritas.com>

# 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](#)
- [SF の手動設定](#)
- [SFDB の設定](#)

## 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き実行されます。

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、`rmmmod` 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

- [第3章 Storage Foundation のアップグレード計画](#)
- [第4章 Storage Foundation のアップグレード](#)
- [第5章 応答ファイルを使用した SF 自動アップグレードの実行](#)
- [第6章 アップグレード後のタスクの実行](#)

# 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 6.0.1 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 6.0.1 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 以降)	コンポーネント (7.0 以降)
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 以降)	コンポーネント (7.0 以降)
SF	Veritas InfoScale Storage	SF
SF	Veritas InfoScale Foundation	SF
SF	Veritas InfoScale Enterprise	SF

**メモ:** 7.0 以降では、既存の Veritas InfoScale 製品は同じ製品の新しいバージョンにアップグレードします。たとえば、Veritas InfoScale Enterprise 7.1 はアップグレードして Veritas InfoScale Enterprise 7.2 になります。

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恒久ライセンスキーを使用している場合は、ライセンスを 7.2 に更新することを促すメッセージが表示されます。更新を選択しない場合は引き続き古いライセンスを使用できますが、製品の機能が古いライセンスの対応コンポーネントに制限されます。たとえば、既存の SF のインストールの恒久ライセンスを更新しないことを選択した場合は、アップグレード後にインストーラによって SF 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
6.0.1	RHEL 6 Update 1、2、3  Oracle Linux 6 Update 1、2、3	RHEL 6 Update 6、7、8  RHEL 7 Update 1、2  Oracle Linux 6 Update 6、7、8  Oracle Linux 7 Update 1、2	Veritas InfoScale Storage 7.2	SF
6.0.2	RHEL 6 Update 1、2  Oracle Linux 6 Update 1、2	RHEL 6 Update 6、7、8  RHEL 7 Update 1、2  Oracle Linux 6 Update 6、7、8  Oracle Linux 7 Update 1、2	Veritas InfoScale Storage 7.2	SF
6.0.3	RHEL 6 Update 1、2、3、4、5  Oracle Linux 6 Update 1、2、3、4、5	RHEL 6 Update 6、7、8  RHEL 7 Update 1、2  Oracle Linux 6 Update 6、7、8  Oracle Linux 7 Update 1、2	Veritas InfoScale Storage 7.2	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
6.0.5	RHEL 6 Update 1、2、3、4、5、6、7、8 Oracle Linux 6 Update 1、2、3、4、5、6、7、8	RHEL 6 Update 6、7、8 RHEL 7 Update 1、2 Oracle Linux 6 Update 6、7、8 Oracle Linux 7 Update 1、2	Veritas InfoScale Storage 7.2	SF
6.1	RHEL 6 Update 3、4、5、6 Oracle Linux 6 Update 3、4、5	RHEL 6 Update 6、7、8 RHEL 7 Update 1、2 Oracle Linux 6 Update 6、7、8 Oracle Linux 7 Update 1、2	Veritas InfoScale Storage 7.2	SF
6.1.1	RHEL 6 Update 3、4、5、6、7 Oracle Linux 6 Update 3、4、5	RHEL 6 Update 6、7、8 RHEL 7 Update 1、2 Oracle Linux 6 Update 6、7、8 Oracle Linux 7 Update 1、2	Veritas InfoScale Storage 7.2	SF
6.2	RHEL 6 Update 3、4、5、6 Oracle Linux 6 Update 3、4、5 RHEL 7 Oracle Linux 7	RHEL 6 Update 6、7、8 RHEL 7 Update 1、2 Oracle Linux 6 Update 6、7、8 Oracle Linux 7 Update 1、2	Veritas InfoScale Storage 7.2	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	RHEL 6 Update 4、5、6、7 Oracle Linux 6 Update 4、5、6	RHEL 6 Update 6、7、8 RHEL 7 Update 1、2 Oracle Linux 6 Update 6、78 Oracle Linux 7 Update 1、2	Veritas InfoScale Storage 7.2	SF
6.2.1	RHEL 7、Update 1 Oracle Linux 7、Update 1	RHEL 6 Update 6、7、8 RHEL 7 Update 1、2 Oracle Linux 6 Update 6、7、8 Oracle Linux 7 Update 1、2	Veritas InfoScale Storage 7.2	SF
7.0、7.0.1	RHEL6 Update 4、5、6、7 RHEL 7、RHEL 7 Update 1 Oracle Linux 6 Update 4、5、6、7 Oracle Linux 7、Oracle Linux 7 Update 1	RHEL6 Update 4、5、6、7 RHEL 7、RHEL 7 Update 1、2 Oracle Linux 6 Update 4、5、6、7 Oracle Linux 7、Oracle Linux 7 Update 1、2	Veritas InfoScale Storage 7.2	SF
7.1	RHEL 6 Update 4、5、6、7、8 RHEL 7 GA Update 1、2 Oracle Linux 6 Update 4、5、6、7、8	RHEL 6 Update 4、5、6、7、8 RHEL 7 GA Update 1、2 Oracle Linux 6 Update 6、7、8 Oracle Linux 7 Update 1、2	Veritas InfoScale Storage 7.2	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
6.0.1、6.0.2、6.0.3	SLES 11 SP1 SLES 11 SP2	SLES11 SP3、 SP4	Veritas InfoScale Storage 7.2	SF
6.0.4	SLES 11 SP2 SLES 11 SP3	SLES11 SP3、 SP4	Veritas InfoScale Storage 7.2	SF
6.0.5	SLES 11 SP1 SLES 11 SP2 SLES 11 SP3 SLES 11 SP4	SLES11 SP3、 SP4	Veritas InfoScale Storage 7.2	SF
6.1、6.2	SLES 11 SP2 SLES 11 SP3	SLES11 SP3、 SP4	Veritas InfoScale Storage 7.2	SF
6.1.1	SLES 11 SP2、 SP3、SP4	SLES11 SP3、 SP4	Veritas InfoScale Storage 7.2	SF
6.2.1	SLES 11 SP2、 SP3、SP4 SLES 12 SP0、 SP1	SLES11 SP3、 SP4 SLES 12 SLES 12 SP1	Veritas InfoScale Storage 7.2	SF
7.0	SLES11 SP3、 SLES12	SLES11 SP3、 SLES12 SP0、 SP1	Veritas InfoScale Storage 7.2	SF
7.0.1	SLES11 SP3、 SP4 SLES 12 SP0、 SP1	SLES11 SP3、 SP4 SLES 12 SP0、 SP1	Veritas InfoScale Storage 7.2	SF
7.1	SLES11 SP3、 SP4 SLES 12 SP0、 SP1	SLES11 SP3、 SP4 SLES 12 SP0、 SP1	Veritas InfoScale Storage 7.2	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 7.2 リリースノート』を確認してください。
- 詳しいことは、ベリタステクニカルサポート Web サイトで確認してください。  
[https://www.veritas.com/support/en\\_US.html](https://www.veritas.com/support/en_US.html)
- 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.23 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。**RPM**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であれば、ベリタス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 **7.2** 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.27 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.24 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`)。ネイティブスタックの 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。
- CP サーバーベースのフェンシングを使うアプリケーションクラスタをバージョン 6.1 以降にアップグレードする場合は、まず CP サーバーシステムで VCS または SFHA をバージョン 6.1 以降にアップグレードすることを確認してください。7.0.1 以降から、CP サーバーではクライアントとの HTTPS ベースの通信のみがサポートされ、IPM ベースの通信はサポートされていません。IPM ベースの CP サーバーが設定されている CP サーバーをアップグレードする場合、CP サーバーを再設定する必要があります。  
CP サーバーシステムで VCS または SFHA をアップグレードする手順については、関連する設定およびアップグレードガイドを参照してください。

## 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 7.2 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。

```
# vxdbg list diskgroup
```

- VVR を使ったレプリケーションを設定している場合は、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™ 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™ レプリケーション管理者ガイド』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。

## 以前の 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™ 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 vradmim 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 7.2 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 7.2 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

7.2 以前の VVR (DG バージョン <= 140)	VVR 7.2 (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ます、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

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

- 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 7.2 リリースには、単一の RPM である `VRTSas1apm` 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は、7.2 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 7.2 をインストールした後、ベリタスは `VRTSas1apm` 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、RPM、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	RPM	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	RPM	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)	Veritas SORT (Services and Operations Readiness Tools)
パッチ	修正	RPM	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ベリタス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 RPM 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 RPM 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。

- 7.2 はベースバージョン
- 7.2.1 はメンテナンスバージョン
- 7.2.1.100 は 7.2.1 のパッチバージョン
- 7.2.0.100 は 7.2 のパッチバージョン

1. ベース + メンテナンス:

この統合方法は、7.2.1 をインストールするときや前のバージョンからアップグレードするとき使用できます。

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、7.2.0.100 をインストールするときや前のバージョンからアップグレードするとき使用できます。

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 7.2 から 7.2.1.100 にアップグレードするとき使用できます。

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、7.2.1.100 をインストールするときや前のバージョンからアップグレードするとき使用できます。

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 以降のリリースでは、`-patch_path <パッチのパス>` `-patch2_path <パッチのパス>` ... `-patch5_path <パッチのパス>` を使って最大 5 つのパッチを追加できます。

---

# 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 7.2 への Storage Foundation のアップグレード](#)
- [Volume Replicator のアップグレード](#)
- [SFDB のアップグレード](#)

## 以前のバージョンから 7.2 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.31 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 7.2 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 7.2 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不明です。正常にマウント解除されたかどうか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 クロウ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
```

開い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 インストール前に必要な確認を行います。

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, ?] host1 host2
```

<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 RPM 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/fstab 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 7.2 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.46 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.44 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.44 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.35 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.25 の「[以前の 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_rvgnam sec_hostname
```

- 2 セカンダリ上の VVR 6.0.1 以降を VVR 7.2 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 dname
```

- 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_rvgnam 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 6.0.1 以降を VVR 7.2 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 dgroupname
```

- 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
```

p.25 の「[以前の 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

7.2 へのアップグレード中に、SFDB ツールがデフォルトで有効になっている場合は vxdm デーモンが設定済みであ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、vxdm デーモンを設定し、起動します。

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

---

**メモ:** 認証設定で SFDB のインストールを 7.2 にアップグレードすると、エラーが起きてコマンドが失敗します。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。

---

# 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
- SF をアップグレードするための応答ファイルの変数
- SF アップグレードの応答ファイルサンプル

## 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 RPM 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 RPM 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}	<p>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。</p> <p>リストまたはスカラー: スカラー</p> <p>オプションまたは必須: オプション</p>
CFG{mirrordgname}{system}	<p>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</p> <p>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。</p> <p>リストまたはスカラー: スカラー</p> <p>オプションまたは必須: オプション</p>
CFG{splitmirror}{system}	<p>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</p> <p>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。</p> <p>リストまたはスカラー: スカラー</p> <p>オプションまたは必須: オプション</p>
CFG{opt}{disable_dmp_native_support}	<p>1 に設定した場合は、ネイティブ LVM ボリュームグループと ZFS プールの <b>Dynamic Multi-pathing</b> 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イティブ LVM ボリュームグループと ZFS プールの <b>Dynamic Multi-Pathing</b> サポートを維持すると、システムに設定されたネイティブ 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。</p> <p>リストまたはスカラー: スカラー</p> <p>オプションまたは必須: オプション</p>
CFG{opt}{patch_path}	<p>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。</p> <p>リストまたはスカラー: スカラー</p> <p>オプションまたは必須: オプション</p>



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{acceptula}=1;  
$CFG{keys}{keyless}=[ qw(STORAGE) ];  
$CFG{prod}="STORAGE72";  
$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(7.2SF_PermanentKey) ];
$CFG{opt}{noipc}=1;
$CFG{opt}{upgrade}=1;
$CFG{prod}="STORAGE72";
$CFG{systems}=[ qw(sys1) ];

1;
```

# 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
- 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
- 自動アップグレードが失敗した場合の VVR のリカバリ
- DAS ディスク名をリセットして FSS 環境のホスト名を含める
- ディスクレイアウトバージョンのアップグレード
- VxVM ディスクグループのバージョンのアップグレード
- 変数の更新
- デフォルトディスクグループの設定
- Storage Foundation のアップグレードの確認

## 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.46 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 `vxvg` 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。

```
# vxvg 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、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  
# adddcn  
# srlprot  
# attrlink  
# start.rvg
```

設定の復元後、現在の手順は再試行できます。

## DAS ディスク名をリセットして FSS 環境のホスト名を含める

7.1 より前のバージョンを使用している場合、FSS 環境の DAS ディスクの場合はホスト名が接頭辞として使用されるように VxVM ディスク名を再生成する必要があります。ホスト接頭辞を使用して、ディスクの元を一意に識別できます。たとえば、ホスト *sys1* 上のディスク *disk1* のデバイス名が *sys1\_disk1* と表示されます。

ディスク名を再生成するには、次のコマンドを実行します。

```
# vxddladm -c assign names
```

## 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、vxfscnvert 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。

vxfscnvert (1M) マニュアルページを参照してください。

---

**メモ:** ベリタス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/voll | grep -i version
```

ディスクレイアウトバージョンについては、『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。

**7.2 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 7.2 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動作し続けます。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う便利です。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「Veritas InfoScale インストール」の章を参照してください。



# 設定後のタスク

- [第7章 設定タスクの実行](#)

# 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](#)
- [ネイティブデバイスの DMP サポートの有効化](#)
- [SFDB ツールの認証の設定について](#)

## クォータの切り替え

すべてのノードを 7.2 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
```

## ネイティブデバイスの 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 デバイスのネイ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。

ネイ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イティブデバイスの 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イティブデバイスの DMP ネイ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 ネイティブサポートは保持されます。

ネイティブデバイスの 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:

```
# vxddmpadm 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 ツールの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 sfcae\_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. インストールスクリプト](#)
- [付録 B. セキュアシェルまたはリモートシェルの通信用の設定](#)

# インストールスクリプト

この付録では以下の項目について説明しています。

- [インストールスクリプトオプション](#)
- [postcheck オプションの使用について](#)

## インストールスクリプトオプション

表 A-1 に、インストールスクリプトのコマンドラインオプションを示します。通常、インストールまたはアップグレードを初めて実行する場合、オプションは必要はありません。インストールスクリプトオプションは、特に指定のないかぎり、すべての Veritas InfoScale 製品スクリプトで使えます。

表 A-1 使用可能なコマンドラインオプション

コマンドラインオプション	機能
-allpkgs	指定の製品に必要な RPM をすべて表示します。RPM は正しいインストール順序で列挙されます。出力を使って、コマンドライン経由のインストールスクリプトまたはネットワーク経由のインストールスクリプトを作成できます。
-comcleanup	-comcleanup オプションを指定すると、インストーラによってシステムに追加されたセキュアシェルまたはリモートシェルの設定が削除されます。このオプションは、シェルの自動設定を実行したインストールルーチンが突然終了した場合にのみ必要とされます。
-comsetup	-comsetup オプションは、システム間の ssh 通信または rsh 通信を設定するのに使われ、パスワードやパスフレーズの入力には要求されません。

コマンドラインオプション	機能
-configcps	-configcps オプションは、実行中のシステムまたはクラスタの CP サーバーの設定に使用します。
-configure	インストール後、製品を設定します。
-disable_dmp_native_support	アップグレード中に、ネイティブ LVM ボリュームグループと ZFS プールの <b>Dynamic Multi-Pathing</b> サポートを無効にします。アップグレード中にネイティブ LVM ボリュームグループと ZFS プールの <b>Dynamic Multi-Pathing</b> サポートを維持すると、システムに設定されたネイティブ 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。
-fencing	実行中のクラスタの I/O フェンシングを設定します。
-fips	-fips オプションは、実行中の VCS クラスタで fips モードのセキュリティの有効と無効を切り替えるために使用します。このオプションは、-security または -securityonnode オプションと一緒に使う必要があります。
-hostfile <i>full_path_to_file</i>	インストールするホスト名のリストを含むファイルの場所を指定します。
-install	製品をシステムにインストールするために使われます。
-online_upgrade	オンラインアップグレードを実行するために使われます。このオプションを使用すると、インストーラはクラスタ全体をアップグレードします。アップグレード処理中のアプリケーションのゼロダウンタイムもサポートされています。現在、このオプションは VCS および <b>ApplicationHA</b> のみをサポートしています。
-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。
-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。
-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。

コマンドラインオプション	機能
-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。
-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。
-keyfile ssh_key_file	セキュアシェル (SSH) インストール用のキーファイルを指定します。このオプションは、-I ssh_key_file をすべての SSH 呼び出しに渡します。
-kickstart dir_path	Linux RHEL Kickstart でのインストールのために Kickstart 設定ファイルを生成します。ファイルは、Kickstart インストールに使うことができる形式で、正しいインストール順序での必要な RPM のリストが含まれます。dir_path はファイルを作成するディレクトリのパスを示します。
-license	指定したシステムで製品ライセンスを登録または更新します。
-logpath log_path	インストーラログファイル、概略ファイル、応答ファイルの保存場所として、/opt/VRTS/install/logs 以外のディレクトリを指定します。
-noipc	パッチや最新のリリース情報を自動的に取得するためにインストーラが Veritas SORT (Services and Operations Readiness Tool) へのアウトバウンドネットワーク呼び出しを行わないようにします。
-nolic	ライセンスキーを入力せずに製品RPMをインストールできるようにします。このオプションを指定した場合、ライセンスがある機能の設定、起動、使用はできません。
-pkgtable	製品の RPM を正しいインストール順序でグループごとに表示します。
-postcheck	さまざまな HA およびファイルシステム関連プロセス、さまざまなポートの利用可能性、クラスタ関連サービスグループの利用可能性を検査します。



コマンドラインオプション	機能
-precheck	インストール前のチェックを実行し、システムがすべてのインストールの必要条件を満たしているかどうかを確認します。事前に確認を行ってから製品をインストールすることをお勧めします。
-prod	操作のために製品を指定します。
-component	操作するコンポーネントを指定します。
-redirect	進行バーを表示せずに、進行状況の詳細を表示します。
-require	インストーラパッチファイルを指定します。
-responsefile <i>response_file</i>	情報の入力を求めるメッセージを表示する代わりに、指定ファイルに格納されているシステム情報と設定情報を使って、インストールと設定を自動化します。 <i>response_file</i> は絶対パス名で指定する必要があります。以降のインストールで応答ファイルを使うには、そのファイルを編集する必要があります。ファイル内で変数フィールドを定義します。
-rsh	このオプションは、システム間の通信にデフォルトのSSHとSCPではなくRSHとRCPを使う場合に指定します。  <a href="#">p.62の「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」</a> を参照してください。
-security	-security オプションはセキュアモードと非セキュアモードとの間の操作で実行中のVCS クラスタを変換するために使います。
-securityonenode	-securityonenode オプションは、ノード別にセキュアクラスタノードを設定するために使います。
-securitytrust	-securitytrust オプションは、別のブローカーとの信頼関係を設定するために使います。
-serial	各システムでシリアルにインストールスクリプトでインストール、アンインストール、起動、停止処理を実行することを指定します。このオプションが指定されていない場合、これらの操作はすべてのシステムで同時に実行されます。

コマンドラインオプション	機能
-setrunables	製品をインストールして設定した後でチューニングパラメータを設定する場合に、このオプションを指定します。チューニングパラメータ値を有効にするには、製品のプロセスを再起動しなければならない場合があります。このオプションは <code>-runablesfile</code> オプションとともに使う必要があります。
-start	指定の製品のデーモンとプロセスを開始します。
-stop	指定の製品のデーモンとプロセスを停止します。
-timeout	<code>-timeout</code> オプションは、スクリプトがタイムアウトになる前に各コマンドの完了を待機する秒数を指定するために使用します。 <code>-timeout</code> オプションを設定すると、デフォルト値の <b>1200</b> 秒が上書きされます。 <code>-timeout</code> オプションを <b>0</b> に設定するとスクリプトのタイムアウトを防ぐことができます。 <code>-timeout</code> オプションは <code>-serial option</code> では機能しません。
-tmpdir <i>tmp_path</i>	<code>/var/tmp</code> 以外のディレクトリをインストールスクリプトの作業ディレクトリとして指定します。指定したディレクトリは初期ログの記録先になるほか、リモートシステムへの RPM のインストールに先立つパッケージのコピー先として使われます。
-runables	サポートされているすべてのチューニングパラメータを表示し、チューニング可能なファイルテンプレートを作成します。
-runables_file <i>runables_file</i>	チューニングパラメータファイルを指定する際にこのオプションを指定します。チューニングパラメータファイルにはチューニングパラメータが含まれている必要があります。
-uninstall	このオプションは、製品をシステムからアンインストールするために使われます。
-upgrade	製品の既存のバージョンがあり、それをアップグレードすることを指定します。

コマンドラインオプション	機能
-version	インストール済みの製品とそのバージョンをチェックして報告します。インストール済みのRPMと製品に適用可能なパッチ、および不足しているRPMとパッチを識別します。該当するインストール済みのRPMとパッチ、および不足しているRPMとパッチの件数を含む概略を表示します。インターネット接続が利用可能である場合は、インストール済みの製品にインストールしているパッチや利用可能な更新を一覧表示します。
-yumgroupxml	-yumgroupxml オプションは、yum グループ定義 XML ファイルを生成するために使われます。createrepo コマンドは、製品の RPM すべての自動インストールに対して yum グループを作成するために RedHat Linux のファイルを使用することができます。XML ファイルを格納するのに使用可能な場所は、絶対パスとして指定してください。-yumgroupxml オプションは Red Hat Linux でのみサポートされます。

## postcheck オプションの使用について

インストール後チェックを使うことで、インストールに関連する問題を判断し、トラブルシューティングに役立てることができます。

---

**メモ:** このコマンドオプションを使うと、ノードでダウンタイムが発生します。

---

postcheck オプションを使うと、次の VCS 関連の問題をトラブルシューティングするときに役立ちます。

- ハートビートリンクが存在しません。
- ハートビートリンクが通信できません。
- ハートビートリンクは結合または集約された NIC の一部を構成しています。
- 重複したクラスタ ID が存在します (LLT が検査時に実行されていない場合)。
- ノード間で VRTSllt pkg バージョンの整合性がとれていません。
- llt-linkinstall 値が正しくありません。
- /etc/llthosts 設定および /etc/llttab 設定が正しくありません。
- /etc/gabtab ファイルが正しくありません。
- GAB の linkinstall 値の中に、正しくない値が存在します。

- ノード間で **VRTSgab pkg** バージョンの整合性がとれていません。
- `main.cf` ファイルまたは `types.cf` ファイルが無効です。
- `/etc/VRTSvcs/conf/sysname` ファイルとホスト名の整合性がとれていません。
- クラスタ **UUID** が存在しません。
- `uuidconfig.pl` ファイルが見つかりません。
- ノード間で **VRTSvcs pkg** バージョンの整合性がとれていません。
- `/etc/vxfenmode` ファイルが見つからないか、または正しくありません。
- `/etc/vxfendg file` ファイルが無効です。
- **vxfen link-install** 値が正しくありません。
- **VRTSvxfen pkg** バージョンの整合性がとれていません。

postcheck オプションは次の **SFHA** または **SFCFSHA** の問題をトラブルシューティングするうえで役立ちます。

- `/etc/vx/reconfig.d/state.d/install-db` ファイルが削除されなかったため、**Volume Manager** を起動できません。
- `volboot` ファイルがロードされていないため、**Volume Manager** を起動できません。
- ライセンスが存在しないため、**Volume Manager** を起動できません。
- `main.cf` ファイルの **CVM** 設定が正しくないため、**Volume Manager** を起動できません。たとえば、**Autostartlist** 値がノードで見つかりません。
- `/etc/llthosts` ファイルでノード **ID** の整合性がとれていないため、**Cluster Volume Manager** をオンラインにすることができません。
- **Vxfen** が起動されていないため、**Cluster Volume Manager** をオンラインにすることができません。
- **gab** が設定されていないため、**Cluster Volume Manager** を起動できません。
- **CVM** プロトコルが一致しないため、**Cluster Volume Manager** をオンラインにすることができません。
- **Cluster Volume Manager** のグループ名が「`cvm`」から変更されたため、**CVM** がオフラインになります。

インストーラのインストール後チェックオプションを使用することで、次の検査を実行できます。

すべての製品に対する全般的な検査。

- すべての必須 **RPM** がインストールされている。
- 必須の **RPM** のバージョンが正しい。

- 必須の RPM の検証問題がない。

#### Volume Manager (VM) の検査。

- 動作していないデーモンの一覧表示 (vxattachd, vxconfigbackupd, vxesd, vxrelocd ...)。
- 状態が **online** または **online shared** ではないディスクの一覧表示 (vxdisk list)。
- 状態が **enabled** ではないディスクグループの一覧表示 (vxdg list)。
- 状態が **enabled** ではないボリュームの一覧表示 (vxprint -g <dgname>)。
- 状態が **Unstartable** であるボリュームの一覧表示 (vxinfo -g <dgname>)。
- /etc/fstab に設定されていないボリュームの一覧表示。

#### ファイルシステム (FS) の検査。

- ロードされていない VxFS カーネルモジュールの一覧表示 (vxfs/fdd/vxportal)。
- /etc/fstab ファイルにあるすべての VxFS ファイルシステムがマウントされているかどうか。
- /etc/fstab にあるすべての VxFS ファイルシステムがディスクレイアウト 6 以降を使用しているかどうか。
- マウントされているすべての VxFS ファイルシステムがディスクレイアウト 6 以降を使用しているかどうか。

#### Cluster File System の検査。

- FS と ODM が最新のプロトコルレベルで動作しているかどうか。
- マウントされているすべての CFS ファイルシステムが VCS によって管理されているかどうか。
- cvm サービスグループがオンラインであるかどうか。

# 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](#)
- [パスワードなし ssh の手動設定](#)
- [installer -comsetup コマンドを使用した ssh および rsh 接続の設定](#)
- [pwdutil.pl ユーティリティを使用した ssh および rsh 接続の設定](#)
- [ssh セッションの再起動](#)
- [Linux の rsh の有効化](#)

## 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。ベリタスでは、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。

---

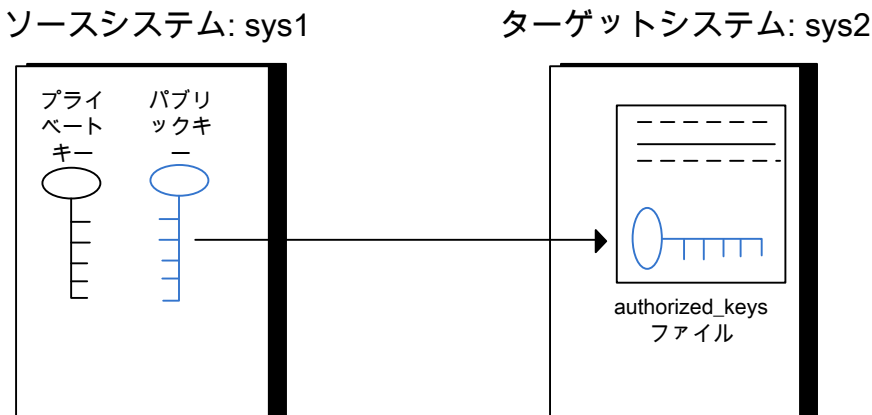
## パスワードなし ssh の手動設定

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 B-1 に、この手順を示します。

図 B-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://www.openssh.com/>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** のルート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** のルート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、パスワード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 B-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、設定解除できません。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、`--keyfile` 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.63 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 RPM 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
```

## S

- SFDB 認証
  - vxdbd の設定 51
- SFDB の認証 51

## U

- upgrade
  - 準備 22
  - バックアップの作成 23

## V

- VVR 4.1
  - からのアップグレードの計画 25
- VVR のアップグレード
  - 4.1 から 25
  - 計画 24
- VVR をアップグレードする計画 24

## あ

- アップグレード
  - アレイサポート 27
  - 応答ファイルを使う 38
- アップグレードに失敗 44
- アップグレードの準備 22
- アップグレード後
  - 検証 48
  - 変数の更新 47
- インストールスクリプトオプション 54
- インストールバンドル
  - 統合オプション 27
- インストール前 24
- 応答ファイル
  - アップグレード 38

## か

- 概要
  - Veritas InfoScale Operations Manager 9

## さ

- 再結合
  - バックアップブートディスクグループ 44
- 作成
  - バックアップ 23

## た

- ディスクグループ
  - rootdg 12
- 同時インストールまたはアップグレード 27

## は

- バックアップブートディスクグループ 44
  - 再結合 44

## ら

- ルートディスクグループ 12