

Symantec™ VirtualStore リ リースノート

Solaris

6.0

Symantec™ VirtualStore リリースノート

このマニュアルで説明するソフトウェアは、使用許諾契約に基づいて提供され、その内容に同意する場合にのみ使用することができます。

製品バージョン: 6.0

マニュアルバージョン: 6.0.0

法的通知と登録商標

Copyright © 2010 copyright; Symantec Corporation. All rights reserved.

Symantec、Symantec ロゴ、Veritas、Veritas Storage Foundation、CommandCentral、NetBackup、Enterprise Vault、LiveUpdate は、Symantec Corporation 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。

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、Symantec Corporation 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限り、免責されるものとします。Symantec Corporation は、本書の供給、性能、使用に関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。

ライセンス対象ソフトウェアと関連書類は、FAR 12.212 の規定によって商用コンピュータソフトウェアとみなされ、場合に応じて、FAR 52.227-19「Commercial Computer Software - Restricted Rights」、DFARS 227.7202「Rights in Commercial Computer Software or Commercial Computer Software Documentation」、そ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。米国政府によるライセンス対象ソフトウェアと関連書類の使用、修正、複製のリリース、実演、表示または開示は、本使用許諾契約の条項に従ってのみ行われるものとします。

弊社製品に関して、当資料で明示的に禁止、あるいは否定されていない利用形態およびシステム構成などについて、これを包括的かつ暗黙的に保証するものではありません。また、弊社製品が稼動するシステムの整合性や処理性能に関しても、これを暗黙的に保証するものではありません。

これらの保証がない状態で、弊社製品の導入、稼動、展開した結果として直接的、あるいは間接的に発生した損害等についてこれが補償されることはありません。製品の導入、稼動、展開にあたっては、お客様の利用目的に合致することを事前に十分に検証および確認いただく前提で、計画および準備をお願いします。

Symantec VirtualStore リリースノート

この文書では以下の項目について説明しています。

- [このリリースノートについて](#)
- [コンポーネント製品のリリースノート](#)
- [Symantec VirtualStore について](#)
- [重要なリリース情報](#)
- [6.0 で導入された変更点](#)
- [システム必要条件](#)
- [修正済みの問題](#)
- [既知の問題](#)
- [ソフトウェアの制限事項](#)
- [マニュアルの誤記](#)
- [マニュアル](#)

このリリースノートについて

このリリースノートには Solaris 対応の SVS (Symantec VirtualStore) 6.0 に関する重要な情報が記載されています。SVS をインストールまたはアップグレードする前に、このリリースノートをすべてお読みください。

リリースノートに記載された情報は、SVS の製品マニュアルに記載の情報に優先します。

これは『Symantec VirtualStore リリースノート』の マニュアルバージョン: **6.0.0** です。始めに、このガイドの最新版を使っていることを確認してください。最新の製品ドキュメントはシマンテック社の Web サイトで利用可能です。

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

このリリースのアップデート、パッチ、既知の問題に関する最新情報については、Symantec テクニカルサポートの Web サイト上の次の TechNote を参照してください。

<http://www.symantec.com/docs/TECH141448>

コンポーネント製品のリリースノート

このリリースノートに加え、コンポーネント製品のリリースノートを確認してから製品をインストールしてください。

マニュアルはソフトウェアメディアの次の場所で、PDF 形式で利用可能です。

`/product_name/docs`

シマンテック社はファイルをシステムの `/opt/VRTS/docs` ディレクトリにコピーすることをお勧めします。

このリリースは、次のコンポーネント製品のリリースノートを含んでいます。

- Veritas Storage Foundation リリースノート (6.0)
- Veritas Cluster Server リリースノート (6.0)
- Veritas Storage Foundation Cluster File System High Availability リリースノート (6.0)

Symantec VirtualStore について

Veritas Storage Foundation Cluster File System High Availability (SFCFSHA) で動作する Symantec VirtualStore (SVS) は、仮想マシンを配備してホストするために最適化された、拡張性が高い、高可用性の NAS ソリューションとして役立ちます。

VirtualStore は、クラスタ全体の高可用性と線形スケーラビリティを提供する Cluster File System (CFS) をベースとして構築されています。

重要なリリース情報

- このリリースに関する重要な更新については、シマンテック社テクニカルサポート Web サイトの最新 TechNote を確認してください。

<http://www.symantec.com/docs/TECH164885>

- このリリースで利用可能な最新のパッチについては、次を参照してください。

<http://sort.symantec.com/>

- このハードウェア互換性リストにはサポートされているハードウェアの情報が記されており、定期的に更新されます。サポートされているハードウェアの最新情報については、次の URL を参照してください。

<http://www.symantec.com/docs/TECH170013>

Storage Foundation and High Availability Solutions をインストール、またはアップグレードする前に、最新の互換性リストをチェックして、ハードウェアとソフトウェアの互換性を確認してください。

6.0 で導入された変更点

この項では Symantec VirtualStore 6.0 の変更点の一覧を示します。

インストールとアップグレードに関する変更

6.0 の製品インストーラには、次の変更点が含まれています。

ブートディスクをアップグレード中にカプセル化し、ミラー化する場合のバックアップブートディスクグループの作成

5.1 SP (Service Pack) 1 またはそれ以降のリリースからアップグレードする場合、インストーラは、ミラー化されたブートディスクグループを分割してバックアップディスクグループを作成することができます。アップグレードが失敗した場合には、このバックアップを使うことができます。

メモ: Solaris x64 オペレーティングシステムで、5.1 SP1 リリースから 6.0 リリースにアップグレードする際に、ミラー化されたブートディスクグループをインストーラに分割させたい場合には、まず 5.1 SP1 RP (ローリングパッチ) 1 リリースにアップグレードする必要があります。ミラー化されたブートディスクグループを分割する必要がない場合には、5.1 SP1 リリースから 6.0 リリースに直接アップグレードできます。

Solaris 10 の Flash アーカイブを使用する製品配備のサポート

Storage Foundation and High Availability スイート製品および Solaris 10 オペレーティングシステムを、JumpStart と組み合わせてインストールする場合には、Flash アーカイブを使用できます。

詳しくは『インストールガイド』を参照してください。

インストーラは、重複する VCS クラスタ ID を検出し、自動的にクラスタ ID を生成できる

インストーラは重複した VCS クラスタ ID を検出し、未使用の 1 つを選択するようメッセージを表示するようになりました。また、インストール時に未使用の ID を生成することもできます。

インストーラは製品バージョンと Hotfix を調べることができる

既存の製品のバージョンについては、インストールの前後で `installer` コマンドを `-version` オプションとともに使って調べることができます。現在のバージョンの製品をインストールした後は、`/opt/VRTS/install` ディレクトリの `showversion` スクリプトを使ってバージョン情報を見つけることができます。

これらのコマンドを用いると、次の情報を確認できます。

- リリースされているすべての **Storage Foundation and High Availability Suite** 製品のインストール済みバージョン
- 必要であるのに見つからないパッケージまたはプラットフォームに適用されるパッチ
- インストールされた製品の SORT からの利用可能な更新 (パッチまたは Hotfix を含む)

製品に応じて、スクリプトは 4.0 以降のバージョンを識別できます。

インストーラの `postcheck` オプションの使用

インストーラの `postcheck` オプションを使えば、インストール関連の問題を診断し、トラブルシューティングに関する情報を得ることができます。

ローリングアップグレードの改良

ローリングアップグレード手順が合理化され簡易化されました。

チューニングパラメータの変更では応答ファイルの使用が可能

デフォルト以外の製品とシステムチューニングパラメータの設定には、チューニングパラメータのテンプレートファイルを使うことができます。このファイルを使うと、I/O ポリシーのようなチューニングパラメータの設定や、インストール中または後でのネイティブマルチパスの切り替えを行うことができます。

詳しくは『インストールガイド』を参照してください。

SVS (Symantec Virtual Store) インストーラの使用

スクリプトベースまたは Web ベースのインストーラを使用して、Symantec VirtualStore をインストール、設定、およびアンインストールできます。SVS は、SVS ライセンスを使って有効にできます。

パッケージの更新

このリリースでのパッケージに関する変更を次に示します。

- 製品インストーラスクリプト用の新しい VRTSsfcp60 パッケージ
VRTSsfcp60 パッケージがこのリリースで導入されました。VRTSsfcp60 パッケージは Veritas 製品のインストール、設定、アップグレードでインストーラが使用するインストーラスクリプトとライブラリを含んでいます。
- Solaris SPARC で製品データの重複を排除する新しい VRTSfsadv パッケージ
Solaris SPARC では、VRTSfsadv パッケージがこのリリースで導入されました。VRTSfsadv パッケージはデータの重複排除機能のライブラリを含んでいます。

詳しくは、『インストールガイド』を参照してください。

Symantec VirtualStore (SVS) に関する変更

Symantec VirtualStore 6.0 には、次の変更点が含まれています。

デフォルトのディスクレイアウトバージョンは 9

このリリースでは、ディスクレイアウトバージョン 9 がデフォルトのバージョンとなっており、次の機能のサポートを有効にします。

- ファイル圧縮
- データの重複排除

『管理者ガイド』を参照してください。

VMware View 統合の実現

これにより、FileSnap を使ってクローンを作成したコンピュータを、新しいデスクトッププールとして VMware View にインポートできます。

Symantec FileSnap を使って仮想マシンのクローンを作成する方法について詳しくは、『Symantec VirtualStore インストール/設定ガイド』を参照してください。

クラスタ化された NFS 環境での Oracle 向けの Direct NFS のサポート

クラスタ化 NFS からの NFS のサポートが追加されました。Symantec VirtualStore (SVS) を Oracle データベースのバックエンドストレージとして使うことができます。

Direct NFS (dNFS) は、TCP/IP を使用してアクセスできる NAS ストレージに配置された、より高速で拡張性に富んだ NFS ストレージへのアクセスを提供する、最適化された NFS クライアントです。

クラスタ化された NFS と Oracle データベース向けの VirtualStore ユーティリティを使用した Oracle の展開について詳しくは、『Symantec VirtualStore 管理者ガイド』を参照してください。

svsdbsnap (1M) マニュアルページを参照してください。

vCenter プラグインの拡張

これらの vCenter プラグインの拡張により、次のことが可能になります。

- VMware vSphere プラグインをホストするためのフェールオーバーの Web サービスをセットアップする。
- VMware vCenter サーバーにクラスタを登録する。
- VMware vCenter サーバーからクラスタを登録解除する。
- 特定の VMware vCenter サーバーへの登録を検証する。
- クラスタを登録する VMware vCenter サーバーのリストを表示する。

VirtualStore の設定について詳しくは、『Symantec VirtualStore インストール/設定ガイド』を参照してください。

svsvmwadm (1M) マニュアルページを参照してください。

クラスタ化 NFS クラスタへのノードの追加

cfsshare コマンドには、クラスタ化 NFS (CNFS) クラスタにノードを追加する機能があります。

『Veritas Storage Foundation Cluster File System High Availability 管理者ガイド』を参照してください。

cfsshare (1M) のマニュアルページを参照してください。

VirtualStore を使った iSCSI の管理

svsiscsiadm コマンドは、VirtualStore ファイルシステムに存在するファイルによってバックアップされる iSCSI LUN のエクスポートの管理を簡素化する機構を提供します。これ

によって、オペレーティングシステムとともに出荷される iSCSI ターゲットドライバの実装を活用できます。

『Symantec VirtualStore 管理者ガイド』を参照してください。

svsiscsiadm (1M) マニュアルページを参照してください。

VirtualStore のインストールと設定の拡張

VirtualStore のインストールと設定について、次の点が拡張されました。

- 標準インストールモード - 標準的なデフォルト設定で VirtualStore を自動的に設定します。
- カスタムインストールモード - VirtualStore 設定のカスタマイズをユーザーに促します。

『Symantec VirtualStore インストール/設定ガイド』を参照してください。

cfsshare コマンドの向上

cfsshare コマンドで次の点が向上されました。

- cfsshare マニュアルページに -D オプションが追加されました。-D オプションは、ファイルシステムによって使われるボリュームの I/O を詳細に監視するために使います。
- コマンドから返されるエラーメッセージの方が有用です。

cfsshare (1M) のマニュアルページを参照してください。

『Veritas Storage Foundation Cluster File System High Availability 管理者ガイド』を参照してください。

Network File System での FileSnap の作成

既存のファイルから拡張子「::snap:vxfs:」を持つ新しいファイルへのハードリンクを作成することによって、NFS (Network File System) 上で FileSnap を作成できます。

『管理者ガイド』を参照してください。

ファイル圧縮

ファイルは圧縮して、使用されるスペースを減らすことができます。ファイルのアクセシビリティは保持されます。圧縮は、アプリケーションに対しては透過的です。圧縮ファイルの見た目と操作性は、圧縮されていないファイルとほぼ同じです。圧縮ファイルは同じ名前を持ち、圧縮されていないファイルと同様に読み取りと書き込みができます。

『管理者ガイド』を参照してください。

ソースファイルシステムの NFS v3 上の VxFS ファイルシステムへの移行

NFS は、ネットワーク接続ストレージソリューションで最もよく使用されるファイルシステムの 1 つで、UNIX 環境で使用される標準ファイル共有機構の 1 つです。この機能は、ソースファイルシステムを、既存の NFS v3 ソリューション上の VxFS ファイルシステムに移行することを可能にします。

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

Solaris SPARC でのデータ重複排除

Solaris SPARC では、ファイルシステムにおいて、後処理として定期的な重複排除を実行できます。継続的なコストなしに重複したデータを除去できます。この機能にはエンタープライズライセンスが必要です。

『管理者ガイド』を参照してください。

セキュアモードでの SVS クラスタに関する変更

このリリースでは、セキュアクラスタのインストールと設定がかなり簡単になりました。この単純化されたセキュアクラスタ設定モデルを使用すれば、クラスタを簡単にセキュアクラスタに変換することができます。

新しいアーキテクチャは埋め込み VxAT に基づいています。これにより、セキュリティコンポーネントは SVS パッケージの一部としてインストールされます。ルートブローカーはもはや、新しいアーキテクチャの単一障害点ではありません。VRTSat の別個のパッケージへの依存関係はありません。SVS ホストにすでにログオンしているルート以外のユーザーが、パスワードを入力するように促されることはなくなりました。さらに、クラスタレベルユーザー機能が、セキュアクラスタのユーザー管理を単純化するために導入されました。

詳しくは『インストールガイド』および『管理者ガイド』を参照してください。

LLT への変更

このリリースには、LLT に関する次の新機能と変更が含まれています。

- LLT リンク障害のより高速な検出
LLT には、オペレーティングシステムのリンク停止の通知機能を使って LLT リンク障害をすぐに検出する機能があります。
- LLT は、VLAN のタグ付け (IEEE 802.1Q) をサポートするようになりました。
- lltconfig コマンドには、次の新しいオプションがあります。
 - -Q

このオプションを使ってリンクを「非表示」に設定できます。LLT は、リンク障害のより高速な検出を有効にする場合に、このタイプのリンクを必要とします。

- -j
LLTリンク障害検出レベルを設定するためにこのオプションを使うことができます。
- コマンドはまた新しいタイマーパラメータ `linkstable` を含んでいます。このパラメータは、高速リンク障害検出を有効にした場合に、LLT がローカルノードの任意のリンクのリンク停止イベントを処理する前に待つ時間を指定します。この `linkstable` は、ときどき障害になるリンクにより無駄にメンバーシップが変化することを防ぐことができます。
- -N
このオプションは、使用されているすべてのクラスタ ID をリスト表示します。
- -M
このオプションは、現在ロードされている LLT のモジュールのバージョン情報を表示します。

詳しくは、`lltconfig` のマニュアルページを参照してください。

`llttab` ファイルは次の変更を含んでいます。

- **hidden**
新しいキーワード **hidden** は、リンクが、高速リンク障害検出を有効にした場合に LLT が使う非表示のリンクであることを示します。
- **set-linkfaildetectlevel**
この新しいコマンドオプションを `/etc/llttab` ファイルで使用し、LLT リンク障害検出のレベルを設定することができます。
- リンク利用率の統計は、パフォーマンス関連の問題の根本原因を分析できるように拡張されました。
- ARP キャッシュの定期的な消去は無効になりました。

詳しくは、『Symantec VirtualStore インストール/設定ガイド』および『Symantec VirtualStore 管理者ガイド』を参照してください。

GAB への変更

この項では、このリリースでの GAB に関連する新機能と変更について説明します。

アプリケーションの可用性を確保するためのさらなる GAB と I/O フェンシングの統合

VxFEN モジュールが決定を実装する前のスプリットブレインの状況の場合に、GAB は、スプリットブレイン後の結合を解決しようと試みる場合があります。GAB は 1 つを除きすべての結合しているサブクラスタを削除します。この動作によりクラスタ全体が停止すること

があります。このシナリオを避けるため、GAB はフェンシングモジュールに優先順位を設定するようになりました。

本リリースの GAB と I/O フェンシングの統合によって、GAB がサブクラスタの結合を開始する前に I/O フェンシングモジュールの決定がまだ保留中の場合、GAB は `iofence` メッセージを遅らせます。GAB の待ち時間は、どの VxFEN が遅延値を計算して GAB に渡すかに基づき、VxFEN のチューニングパラメータ `panic_timeout_offst` の値によって変わります。

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

GAB はポートに加えて名前でもクライアントを認識できる

カーネルクライアントが GAB API を初期化するとき、クライアント名の文字列を定義できるようになりました。GAB は、クライアント名を登録することで、GAB ポートが登録される前でもクライアントを追跡できます。また、GAB は、LLT ポートを登録するとき、LLT にクライアント名の情報を渡します。`lltstat -p` コマンドも、使用中のポートの状態の詳細を表示するときに、GAB のクライアント名を表示します。

この機能は GAB カーネルクライアントにのみ適用できます。HAD のような、ユーザーサイトの GAB クライアントには適用できません。

gabconfig コマンドの新しい -C オプション

`gabconfig` のコマンドの `-C` オプションは、GAB に登録されている GAB クライアントの名前を一覧表示します。`-c` オプションを `-a` オプションとともに使用すると、ポートメンバーシップの詳細とともにクライアント名が一覧表示されます。

I/O フェンシングに関する変更

ここでは、I/O フェンシングに関するこのリリースでの新機能と変更点について説明します。

非 SCSI3 フェンシングのサポート

SCSI-3 PR をサポートしない環境では、非 SCSI-3 フェンシングが、設定可能な時間 (`loser_exit_delay`、デフォルトは 55) だけ勝者側を遅延させることによって適度なデータ保護を提供します。また、敗者側を速やかにパニック状態にするようにフェンシングコンポーネントが強化されました。これらの機能強化により、データ破損の可能性を大幅に低減することができます。

詳しくは、『Symantec VirtualStore インストール/設定ガイド』および『Symantec VirtualStore 管理者ガイド』を参照してください。

インストーラがオンラインクラスタでフェンシング設定間の移行をサポート

インストーラを使って、ディスクベースとサーバーベースのフェンシング設定の間で移行できるようになりました。また、同じインストーラオプションを使って、オンラインクラスタで任意の I/O フェンシング設定のコーディネーションポイントを置換できます。インストーラは `vx fenceswap` スクリプトを内部的に使用します。

また、これらの I/O フェンシングの再設定操作を実行するために、応答ファイルを使用することができます。

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

I/O フェンシングの競争の間の RACER ノード再選のサポート

ネットワーク分割の際、VxFEN モジュールは、サブクラスタの代わりにコーディネーションポイントを得るべく競争するために、各サブクラスタの最も低いノードを RACER ノードとして選びます。他の SPECTATOR ノードは、RACER ノードがフェンシングを行うのを待ちます。

以前のリリースでは、I/O フェンシングの競争は、次のとおり単一の RACER ノードに完全に依存していました。

- RACER ノードがコーディネーションポイントの大半に到達できなければ、RACER ノードの VxFEN のモジュールは `LOST_RACE` メッセージを送信し、`LOST_RACE` メッセージを受信したサブクラスタのすべてのノードもパニックになります。
- アービトレーションの間に RACER ノードがパニックになると、サブクラスタの SPECTATOR ノードは、RACER ノードが競争に負けたと見なし、SPECTATOR ノードもパニックになります。

新しい RACER ノード再選機能によって、VxFEN モジュールは、サブクラスタ内でノード ID が次に小さいノードを RACER ノードとして再選します。この機能により、コーディネーションポイントに対してサブクラスタが競争を続ける機会が最適化されます。

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

CP サーバーの複数の仮想 IP アドレスのサポート

CP サーバーにアクセスするために複数のネットワークパス (仮想 IP アドレス) を設定できるようになりました。CP サーバーは複数の仮想 IP アドレスで応答準備します。あるネットワークパスが障害になっても、CP サーバーは再起動を必要とせず、他の利用可能な仮想 IP アドレスの 1 つで応答準備し続けます。

詳しくは、『Symantec VirtualStore インストール/設定ガイド』および『Symantec VirtualStore 管理者ガイド』を参照してください。

CP サーバーの Quorum エージェントのサポート

複数の仮想 IP アドレスのサポートを使うと、Quorum エージェントを使用して、CP サーバーサービスグループのフェールオーバーポリシーを設定できるようになりました。Quorum リソースがオンラインのままになるためにオンラインであることが必要な IP リソースの最小数を指定できます。

詳しくは、『Symantec VirtualStore インストール/設定ガイド』および『Symantec VirtualStore 管理者ガイド』を参照してください。

GAB は、フェンシングが有効な状態で、一部のクラスタノードが利用不能なときに自動的にクラスタをシーディングできる

以前のリリースでは、クラスタ内の一部のノードが動作していない場合、既存のスプリットブレインのリスクを避けるため、GAB ポートは起動しません。そのような場合、コマンド `gabconfig -x` を使って手動で GAB ポートを起動し、GAB をシーディングできます。ただしクラスタの I/O フェンシングを有効していた場合には、I/O フェンシングはクラスタ内の既存のスプリットブレインを処理できます。

このリリースでは、I/O フェンシングのこの機能が拡張され、自動的に次のように GAB をシーディングできます。

- クラスタのいくつかのノードが起動していない場合、GAB ポート(ポート a)はクラスタのすべてのメンバーノードで起動します。
- コーディネーションポイントに、任意の非メンバーノードからのキーがなければ、I/O フェンシング(GAB ポート b)も起動します。

この新機能はデフォルトでは無効になっています。I/O フェンシングが有効モードで設定されているクラスタでは、GAB のこの自動シーディング機能を手動で有効にする必要があります。

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

引き続き、`gabconfig -x` コマンドを使って手動でクラスタをシーディングすることができます。

ノードを段階的に終了した場合、ピアノードでは I/O フェンシングの競争条件がトリガされない

以前のリリースでは、段階的にノードを終了すれば、その I/O フェンシングキーはコーディネーションポイントから消去されました。しかし、残っているサブクラスタの競争が、ノードの段階的な終了でデータディスクから登録を削除することを妨げました。この操作の間に、サブクラスタがコーディネーションポイントへアクセスできなくなると、RACER がコーディネーションポイントへの競争で敗れると、クラスタ全体がパニックに陥ることがありました。

このリリースでは、この動作は変わりました。ノードを段階的に終了させるとき、そのノードの CVM または他のクライアントは、VxFEN のモジュールが設定解除される前に停止します。それで、キーはデータディスクからすでにクリアされています。残っているサブクラスタが、段階的に終了しているノードのキーをコーディネーションポイントからクリアしようとして、キーをクリアすることができなくても、パニックが発生することはありません。

VxExplorer のトラブルシューティングアーカイブの収集の拡張

SORT (Symantec Operations Readiness Tools) データコレクタには VxExplorer のアーカイブを収集し、送信するための機能が含まれています。このアーカイブは、問題診断とトラブルシューティングのためにシマンテック社のテクニカルサポートに送付することができます。VxExplorer はカスタマのデータを収集しません。

従来の vxexplorer スクリプトは、異なる方式で動作するようになりました。スクリプトを実行すると、指定されたローカルホスト上の SORT データコレクタが -vxexplorer オプション付きで起動されます。

データコレクタを使用して VxExplorer のアーカイブを収集する方法については、次を参照してください。

www.symantec.com/docs/HOWTO32575

SFHA Solutions 6.0 のリリースでのライセンス供与の変更

Storage Foundation and High Availability Solutions 6.0 では、ライセンス供与が次のように変わります。

- Cluster File System のライセンスは廃止されます。CFS のカスタマは、Storage Foundation Cluster File System High Availability (SFCFS HA) 機能を使用する資格を与えられます。
- VVR オプションは Veritas Replicator オプションに名前が変更されます。このオプションは、VVR (ボリュームベースのレプリケーション) と、新しいファイルベースのレプリケーションのソリューションを含んでいます。
- VVR Enterprise ライセンスは廃止されます。この機能を使用するには、Storage Foundation Enterprise を使い、Veritas Replicator オプションを追加してください。VVR Enterprise のカスタマは、Storage Foundation Enterprise と Replicator オプションを使用する資格を与えられます。
- VCS のライセンスは、完全なクラスタ機能、および一部のスタート/ストップ機能を有効にします。
- Storage Foundation Enterprise CFS for Oracle RAC (Linux/x64) のカスタマは、Storage Foundation Enterprise for Oracle RAC (Linux/x64) を使用する資格を与えられます。

標準およびエンタープライズのライセンスには次の機能が含まれています。

- 圧縮機能は標準ライセンスで利用できます。
- **SmartTier** 機能は標準ライセンスで利用できるようになりました。
- 重複排除機能は **Solaris SPARC** のエンタープライズライセンスで利用できます。

次の製品は、このリリースには含まれています。

- **Dynamic Multi-Pathing**
- **VirtualStore**
- **Storage Foundation Basic**
- **Storage Foundation Standard**
- **Storage Foundation Enterprise**
- **Veritas Cluster Server**
- **Veritas Cluster Server HA/DR**
- **Storage Foundation Standard HA: Veritas Cluster Server および Storage Foundation Standard**
- **Storage Foundation Enterprise HA: Storage Foundation Enterprise および Veritas Cluster Server**
- **Storage Foundation Enterprise HA/DR**
- **Storage Foundation Enterprise Cluster File System HA**
- **Storage Foundation Enterprise Cluster File System HA/DR**
- **Storage Foundation Enterprise for Oracle RAC**
- **Storage Foundation Enterprise HA/DR for Oracle RAC**
- **Storage Foundation Enterprise for Sybase ASE CE**
- **Storage Foundation Enterprise HA/DR for Sybase CE**

HA: 高可用性

HA/DR: 高可用性と障害回復

Veritas Replicator オプションは、**Dynamic Multi-Pathing** と **Veritas Cluster Server** を除く **Storage Foundation and High Availability** のすべての製品に追加できます。

製品、機能、およびオプションは、オペレーティングシステムとプラットフォームによって異なる場合があることにご注意ください。サポート対象のプラットフォームについて詳しくは、製品のマニュアルを参照してください。

製品マニュアルに関する変更

Storage Foundation and High Availability Solutions 6.0 リリースには、製品マニュアルに関する次の変更点が含まれています。

表 1-1 は、このリリースで導入されたマニュアルのリストです。

表 1-1 新しいマニュアル

新しいマニュアル	注意
Veritas Storage Foundation インストールガイド	Veritas Storage Foundation のインストールとアップグレードに関する情報。
Veritas Storage Foundation 管理者ガイド	Veritas Storage Foundation の管理に関する情報。
Veritas Storage Foundation and High Availability リリースノート	Veritas Storage Foundation and High Availability ユーザー向けのリリース特定の情報。
Veritas Storage Foundation and High Availability Solutions ソリューションガイド	Veritas Storage Foundation and High Availability Solutions のソリューションと使用例。
Veritas Storage Foundation and High Availability Solutions トラブルシューティングガイド	Veritas Storage Foundation and High Availability Solutions のトラブルシューティング情報。
Symantec VirtualStore リリースノート	Symantec VirtualStore のリリース特定の情報。
Veritas Storage Foundation for Sybase ASE CE リリースノート	Veritas Storage Foundation for Sybase ASE CE のリリース特定の情報。
Veritas Storage Foundation for Sybase ASE CE インストールガイド	Veritas Storage Foundation for Sybase ASE CE のインストールに関する情報。
Veritas Storage Foundation for Sybase ASE CE 管理者ガイド	Veritas Storage Foundation for Sybase ASE CE の管理に関する情報。
Virtual Business Services-Availability ユーザーズガイド	Virtual Business Service に関する情報。このマニュアルはオンラインで参照できます。

表 1-2 は、このリリースで廃止されたマニュアルのリストです。

表 1-2 廃止されたマニュアル

廃止されたマニュアル	注意
Veritas File System 管理者ガイド	内容は、『Veritas Storage Foundation 管理者ガイド』と『Veritas Storage Foundation Cluster File System High Availability 管理者ガイド』に含まれています。
Veritas Volume Manager 管理者ガイド	内容は、『Veritas Storage Foundation 管理者ガイド』と『Veritas Storage Foundation Cluster File System High Availability 管理者ガイド』に含まれています。
Veritas Storage Foundation 拡張機能管理者ガイド	内容は、『Veritas Storage Foundation and High Availability Solutions ソリューションガイド』に含まれています。
Veritas Volume Manager トラブルシューティングガイド	内容は、『Veritas Storage Foundation and High Availability Solutions トラブルシューティングガイド』に含まれています。
Veritas Cluster Server Agents for Veritas Volume Replicator 設定ガイド	内容は、『Veritas Cluster Server 付属エージェントリファレンスガイド』に含まれています。
Veritas Volume Replicator 計画およびチューニングガイド	内容は、『Veritas Storage Foundation and High Availability Solutions のレプリケーションの管理者ガイド』に含まれています。
Veritas Volume Replicator Advisor ユーザーズガイド	内容は、『Veritas Storage Foundation and High Availability Solutions のレプリケーションの管理者ガイド』に含まれています。

表 1-3 は、バイナリにバンドルされなくなったマニュアルのリストです。これらのマニュアルはオンラインで参照できます。

表 1-3 オンラインのマニュアル

マニュアル
Veritas Cluster Server エージェント開発者ガイド
Veritas Cluster Server アプリケーションノート: Dynamic Reconfiguration of Oracle Sun Servers
Veritas File System プログラマーズリファレンスガイド

システム必要条件

ここでは、このリリースのシステムの必要条件について説明します。

サポート対象 Solaris オペレーティングシステム

この項は、このリリースの Veritas 製品のサポート対象オペレーティングシステムを一覧表示します。

表 1-4 では、このリリースのサポート対象のオペレーティングシステムを示しています。

表 1-4 サポート対象のオペレーティングシステム

オペレーティングシステム	レベル	チップセット
Solaris 10	アップデート 8、9、10	SPARC
Solaris 10	アップデート 8、9、10	x64

サポートされる VMware ソフトウェアバージョン

- VMware vSphere 4 (ESX 4.0 Update 1 以降と vCenter Server 4.0 Update 1 以降)
- VMware vSphere 4.1 (ESX 4.1 以降と vCenter Server 4.1 以降)

クローン作成時にゲストオペレーティングシステムカスタマイズでサポートされるゲストオペレーティングシステム

- Windows XP
- Windows Server 2003
- Windows 7
- Windows Server 2008
- Red Hat Enterprise Linux (RHEL 5)
- Red Hat Enterprise Linux (RHEL 6)
- SUSE Linux Enterprise Server (SLES 10)
- SUSE Linux Enterprise Server (SLES 11)

メモ: 一部のゲストオペレーティングシステムとバージョンのカスタマイズには、vCenter Server が十分新しいバージョンであることが必要となります。詳しくは『http://www.vmware.com/pdf/vsphere4/r40/vsp_compatibility_matrix.pdf』を参照してください。

クローン作成時の VMware View 統合でサポートされるゲストオペレーティングシステム

- Windows XP
- Windows 7

修正済みの問題

ここでは、このリリースで修正されたインシデントについて説明します。

製品に関連する修正済みのインシデントの完全な一覧については、対応するリリースノートを参照してください。

p.33 の「[マニュアル](#)」を参照してください。

Symantec VirtualStore の修正済みの問題

ここでは、このリリースの Symantec VirtualStore で修正されたインシデントについて説明します。

Symantec VirtualStore: 5.1 SP1 PR3 で修正された問題

ここでは、Symantec VirtualStore 5.1 SP1 PR3 で修正されたインシデントについて説明します。

表 1-5 VirtualStore の修正済みの問題

インシデント	説明
2316752	sysprep と VirtualStore に関する問題が修正されました。
2277467	Symantec Quick Clone Virtual Machine Wizard が完了しないという問題が修正されました。

既知の問題

このセクションでは、このリリースの既知の問題について説明します。

製品に関連する既知の問題の完全な一覧については、対応するリリースノートを参照してください。

p.33 の「[マニュアル](#)」を参照してください。

Symantec VirtualStore の問題

ファイルシステム上で利用可能な領域を超える LUN を作成すると `svsiscsiadm create lun` コマンドが失敗する (2567517)

ファイルシステム上で利用可能な総領域を超えるサイズの LUN を作成すると、`svsiscsiadm create lun` コマンドが失敗します。下位の `iscsitadm` コマンドは失敗し、次のエラーメッセージが表示されます。

```
iscsitadm: Error Requested size is too large for system
```

このエラーのレポートは、`/var/VRTSvcs/log/engine_A.log` ファイルに記録されます。

その後、同じターゲット上で LUN を作成しようとしても、LUN を作成するための呼び出しは再び失敗し、次のエラーメッセージが表示されます。

```
iscsitadm: Error Failed to create a symbolic link to the backing store
```

このエラーのレポートは、`/var/VRTSvcs/log/engine_A.log` ファイルに記録されます。

これにより、ターゲットは使用できなくなります。

回避策

この問題を解決するには

- 1 `svsiscsiadm create lun` コマンドが失敗した **TargetID** と **LunID** を書き留めます。失敗した **LunID** を見つけるには、前回、`svsiscsiadm list` コマンドを使って `svsiscsiadm create lun` コマンドを実行したときに失敗したターゲットの **LunID** を書き留めます。失敗した **LunID** を特定するには、前回 `svsiscsiadm list` コマンドの実行時に表示された **LunID** に 1 を足します。

- 2 **TargetID** の設定ディレクトリに移動します。

```
# cd /etc/iscsi/TargetID .
```

- 3 追加に失敗した LUN バックアップファイルのパスを参照するシンボリックリンクを削除します。次の **LunID** が、失敗した (1 を足した) **LunID** です。

```
# rm -f /etc/iscsi/TargetID/lun.($lunid + 1)
```

シンボリックリンクの削除後は、使用できなくなったターゲットで LUN を追加できるはずで

CFS コマンドは root 以外によって実行された場合にハングアップすることがある(2403263)

CFS コマンドは root 以外によって実行された場合にハングアップすることがあります。

回避策

この問題を解決するには

- ◆ root 以外のセッションでは、CFS コマンドを実行する前に、認証情報を保存する halogin コマンドを使用してください。

halogin コマンドを実行すると、VCS は暗号化されたログイン情報をユーザーのホームディレクトリに格納します。

VirtualStore クラスタの再ブート中に作成された VirtualStore マシンクローンが起動しないことがある(2164664)

SVS ノードの再ブート中にクローンを作成するときに、次のようなエラーメッセージが出力されることがあります。

```
clone vms could not start X server
```

回避策

ノードのクラッシュ中に作成されたすべてのクローンを削除し、クローン操作を再実行してください。

クローンを作成できないことがある(2348628)

クローンを作成できず、VMware の vApp テンプレートと OVF テンプレートを使用している場合は、vApp を無効にする必要があります。

回避策

vApp を無効にするには

- 1 VI クライアントで仮想マシンを右クリックし、[設定の編集(Edit Settings)]、[オプション(Options)]、[vApp オプション(vApp Options)]の順に選択します。
- 2 [無効化(Disable)]をクリックします。

仮想マシンに対して NDMP または NBU のインテリジェントバックアップが必要である(2378396)

NDMP クライアントまたは NBU クライアントを使って仮想マシンをバックアップする際に消費される領域は、仮想マシンのディスク領域が一部しか使われていない場合でも、仮想マシンのディスクサイズと同じになります。

仮想マシンディスク (VMDK) ファイルのサイズが 10 GB であり、ディスク領域が 1 GB しか使われていない場合、元の VMDK ファイルに未割り当てのディスク領域が 9 GB も含まれていますが、NDMP クライアントまたは NBU クライアントによって実行されるバックアップでは 10 GB のバックアップデータが生成されます。

回避策

領域効率の高いバックアップを作成するには、VMware 固有のバックアップアプリケーション (NetBackup for VMware など) を使います。

複数のインスタンスが開いていると Symantec Quick Clone Virtual Machine Wizard が期待どおりに動作しないことがある (2309702)

単一の vSphere クライアントからウィザードの複数のパラレルセッションを同時に起動した場合、期待どおりにウィザードが動作しないことがあります。

たとえば、次のような場合にこの問題が発生します。

- wingoldvm1 を右クリックしてウィザードを起動した。
- その直後に、slesgoldvm1 を右クリックしてウィザードを起動した。

この状況では、同じ vSphere クライアントからウィザードの 2 つのインスタンスが実行されているため、予期しない動作を招くことがあります。

回避策

この問題を解決するには

- ウィザードの両方のインスタンスを閉じます。
- ウィザードの 1 つの新しいインスタンスを再び開きます。

クローンの作成中に FileStore クラスタノード、ESX サーバー、vCenter サーバーが再ブートされた場合、Symantec Quick Clone Virtual Machine Wizard によって作成された仮想マシンが正しくブートしないことがある (2164664、2374229)

ウィザードを使ってクローンを作成しているときに、次のいずれかのサーバーがクラッシュしたり再ブートされたりすると、クローンが正しく作成されないことがあります。

- FileStore ノード
- クローンが作成される ESX ホスト
- vCenter サーバー

作成されたクローンとして vCenter インベントリに表示されても、クローンのゲスト OS はブートできないことがあります。

回避策

サーバーがクラッシュしたとき、またはサーバーが再ブートされたときに作成されたすべてのクローンを削除して、ウィザード操作を再試行します。

クローンを作成するのに不適切なクラスタを選択してもエラーメッセージが表示されない(2372713)

複数の FileStore クラスタが同じ Virtual Center で登録されている場合、ゴールデンイメージのクローンを作成するのに不適切なクラスタを選択しても、Symantec Quick Clone Virtual Machine Wizard によって警告メッセージは表示されません。この状況は、すべての FileStore クラスタが同じファイルシステムパス (/mnt など) をエクスポートしている場合に起こることがあります。ウィザードを使ってゴールデンイメージのディスク (vmdks) のクローン作成を行う際に、不適切なクラスタが選択されたことを通知する事前の警告の代わりに、ウィザードの最後のページでエラーが表示されます。表示されるエラーは次のようになります。

```
/mnt/goldvm/goldvm.vmdk no such file or directory...
```

回避策

この問題に対する回避策はありません。

キーレスライセンスを有効にしても、インストーラで「Registering SVS license」と表示される

キーレスライセンスを有効にしても、インストール時に次のメッセージを含む出力が表示されます。

```
Registering SVS license
```

回避策: このメッセージは無害なので無視してください。製品はライセンスキーなしで正常にインストールされます。

日本語環境でのクローン問題(2623471)

Guest OS Customization または VMware View の統合でクローンを作成できない可能性があります。FileSnap ウィザードの使用で、オプションが表示されないか、エラー状態になっていることが考えられます。

回避策

回避策には、英語ロケールで vCenter Server を一時的に実行することが関係していません。

この問題を解決するには

- 1 vCenter Server で、タスクマネージャまたは `services.msc` を使用して次のサービスを停止します。

```
VMware VCMSD  
VMware VirtualCenter Server  
VMware VirtualCenter Management Webservices  
VMware vCenter Update Manager Services
```

- 2 次の言語ディレクトリの名前 `ja` を、`ja-x` に変更します。

```
C:\Program Files\VMware\Infrastructure\VirtualCenter Server\ja  
C:\Program Files\VMware\Infrastructure\VirtualCenter Server\  
locale\ja  
C:\Program Files\VMware\Infrastructure\VirtualCenter Server\  
imgres\ja
```

- 3 手順 1 からサービスを再起動します。
- 4 FileSnap ウィザードを使用し、カスタマイズまたは View の統合で FileSnap クローンを作成します。
- 5 vCenter Server を日本語ロケールに切り替えるには、手順 1 ~ 3 を逆順に行います。

I/O フェンシングに関する問題

ここでは、I/Oフェンシングに関するこのリリースでの既知の問題について説明します。

I/O フェンシングが起動していないときに、svcs が VxFEN がオンラインであると表示する(2492874)

Solaris 10 SMF では、サービスの状態を、サービスの開始メソッドが返す終了コードに基づいて判断します。VxFEN の開始メソッドは、`vxfen-startup` をバックグラウンドで実行し、終了コード 0 を返します。そのため、`vxfen-startup` スクリプトが起動後にエラーで終了しても、そのことは SMF まで伝わりません。この動作のため、`svcs` コマンドは VxFEN の状態を間違って表示することがあります。

回避策: I/O フェンシングが動作しているかどうかを確認するには、`vxfenadm` コマンドを使用してください。

CP サーバーにクラスタの詳細が存在しない場合、VxFEN は既存のスプリットブレインについてのメッセージを出して、失敗する (2433060)

サーバーベースの I/O フェンシングを開始するとき、ノードがクラスタに参加せず、ログファイルに次のようなエラーメッセージを記録することがあります。

```
/var/VRTSvcs/log/vxfen/vxfen.log ファイル
```

```
VXFEN vxfenconfig ERROR V-11-2-1043  
Detected a preexisting split brain. Unable to join cluster.
```

```
/var/VRTSvcs/log/vxfen/vxfen.log ファイル
```

```
operation failed.  
CPS ERROR V-97-1400-446 Un-authorized user cpsclient@system01,  
domaintype vx; not allowing action
```

アプリケーションクラスタの `vxfend` デーモンは、コーディネーションポイントサーバー (CP サーバー) に対して、GAB のメンバーシップに属するクラスタメンバーが CP サーバーに登録されているかチェックするようこのクエリーを出します。アプリケーションクラスタが何らかの理由で CP サーバーに接触できなかった場合、フェンシングは CP サーバー上の登録を判断できず、予防的にすでにスプリットブレインが発生していると想定します。

回避策: アプリケーションの VxFEN を開始する前に、クラスタ名、UUID、ノード、権限といったクラスタ詳細が CP サーバーに追加されていること確認してください。

vxfenswap ユーティリティは RSH の制限事項によるコーディネーションポイントの検証エラーを検出しない (2531561)

`vxfenswap` ユーティリティは、コーディネーションポイントの検証のため、クラスタの各ノード上で RSH または SSH により `vxfenconfig -o modify` コマンドを実行します。RSH を使用して (`-n` オプションを付けて) `vxfenswap` コマンドを実行した場合、RSH はノードのコーディネーションポイントの検証エラーを検出しません。`vxfenswap` はこのポイントから、検証がすべてのノードで成功だったように続行します。しかし後の段階で、VxFEN ドライバへの新しいコーディネーションポイントのコミットを試みるときに失敗します。エラーの後には、全体の操作をロールバックし、ゼロ以外のエラーコードを返して正常に終了します。SSH を使用して (`-n` オプションなしで) `vxfenswap` を実行した場合には、SSH はコーディネーションポイントの検証エラーを正しく検出し、全体の操作をすぐにロールバックします。

回避策: SSH で (`-n` オプションなしで) `vxfenswap` ユーティリティを使用してください。

フェンシングが再ブート後にノードの 1 つで起動しない(2573599)

VxFEN の設定解除でカーネルでの処理が完了していないときに VxFEN の起動を試みた場合、/var/VRTSvcs/log/vxfen/vxfen.log ファイルに次のエラーが出されます。

```
VXFEN vxfenconfig ERROR V-11-2-1007 Vxfen already configured
```

ただし、gabconfig -a コマンドの出力にはポート **b** は表示されません。vxfenadm -d コマンドは次のエラーを表示します。

```
VXFEN vxfenadm ERROR V-11-2-1115 Local node is not a member of cluster!
```

回避策: しばらくしてから再び VxFEN を開始してください。

CP サーバーが利用不能な IP アドレスを繰り返しログに記録する(2530864)

コーディネーションポイントサーバー (CP サーバー) が、vxcps.conf ファイルに記されている、またはコマンドラインから動的に追加された、どの IP アドレスからも応答を受けなかった場合、CP サーバーは、障害を示すため、定期的な間隔でログにエラーを記録します。ログの記録は、IP アドレスが正常にバインドされるまで続きます。

```
CPS ERROR V-97-51-103 Could not create socket for host  
10.209.79.60 on port 14250
```

```
CPS ERROR V-97-1400-791 Coordination point server could not  
open listening port = [10.209.79.60]:14250  
Check if port is already in use.
```

回避策: cpsadm コマンドの rm_port アクションを使用して、問題となっている IP アドレスを、応答を待機している IP アドレスのリストから削除してください。

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

クラスタノードが CP サーバーに登録されていなくてもフェンシングポート **b** が数秒間可視になる(2415619)

クラスタノードが CP サーバーに登録されていない状態で、コーディネーションポイントサーバー (CP サーバー) の情報をクラスタノードの vxfenmode に設定し、フェンシングを開始すると、フェンシングポート **b** が数秒間可視になり、それから消えます。

回避策: この問題を解決するには、CP サーバーにクラスタノードとユーザーの情報を手動で追加してください。または、インストーラを使用することもできます。インストーラは設定時に、クラスタノードとユーザーの情報を CP サーバーに追加するからです。

cpsadm コマンドは LLT がアプリケーションクラスタで設定されていない場合には失敗する(2583685)

cpsadm コマンドは、cpsadm コマンドを実行するアプリケーションクラスタノードで LLT が設定されていない場合は、コーディネーションポイントサーバー (CP サーバー) と通信できません。次のようなエラーが表示されます。

```
# cpsadm -s 10.209.125.200 -a ping_cps
CPS ERROR V-97-1400-729 Please ensure a valid nodeid using
environment variable
CPS_NODEID
CPS ERROR V-97-1400-777 Client unable to communicate with CPS.
```

ただし、CP サーバー上で cpsadm コマンドを実行すれば、CP サーバーをホストしているノードで LLT が設定されていなくても、この問題は起こりません。CP サーバーノード上の cpsadm コマンドは、LLT が設定されていない場合は、常に LLT ノード ID が 0 であると想定します。

CP サーバーとアプリケーションクラスタ間のプロトコルに従えば、アプリケーションクラスタノード上で cpsadm を実行した場合、cpsadm はローカルノードの LLT ノード ID を CP サーバーに送信する必要があります。しかし、LLT が一時的に設定解除されていた場合、またはノードが LLT が設定されないシングルノード VCS 設定である場合には、cpsadm コマンドは LLT ノード ID を取得できません。そのような状況では、cpsadm コマンド失敗します。

回避策: CPS_NODEID 環境変数を 255 に設定してください。cpsadm コマンドは、LLT から LLT ノード ID を取得できなかった場合には、CPS_NODEID 変数を読み込んで、続行します。

サーバーベースのフェンシングはデフォルトポートが指定されていない場合に間違っ て起動する(2403453)

フェンシングをカスタマイズモードで設定した場合には、デフォルトのポートを指定しなくても、フェンシングは起動します。しかし、vxfenconfig -l コマンドではポート番号が出力されません。

回避策: 少なくとも 1 台の CP サーバーでカスタマイズされたフェンシングを使用する場合には、/etc/vxfenmode ファイル内に「port=<port_value>」の設定を残しておいてください。ポートのデフォルト値は 14250 です。

30 秒の間隔をカスタマイズできない(2551621)

vxcpsserv プロセスは、起動時に IP アドレスにバインドすることができなかった場合、30 秒間隔でその IP アドレスへのバインドを試みます。この間隔は設定可能ではありません。

回避策: 回避策はありません。

configure_cps.pl スクリプトで CPSSG を設定する際に NIC リソースが間違った名前で作成される(2585229)

configure_cps.pl スクリプトが作成する NIC リソースの名前は、たとえば、**m** 番目の VIP を **n** 番目の NIC にマップしていて、**m** と **n** とが必ずしも同じでない場合には、正しいものにはなりません。この場合、CPSSG は問題なく動作し続けますが、configure_cps.pl で CPSSG を設定解除しようとする、失敗します。

回避策: CPSSG を設定解除するためには、VCS の設定から CPSSG の設定を削除する必要があります。

CP サーバーの設定は、SFHA クラスタにホストされている CP サーバーのセキュアな信用証明の設定中に、失敗する(2621029)

configure_cps.pl ユーティリティを使う CP サーバーの設定は、SFHA クラスタでホストされている CP サーバーのセキュアな信用証明を設定しているときに、失敗します。次のエラーが出ることがあります。

```
Creating softlink to credential directory /etc/VRTScps/db/CPSERVER  
on node nodename.
```

```
Unable to connect to node nodename using /usr/bin/ssh.
```

```
Please configure ssh communication and retry. Exiting.
```

回避策: 次のオプションを使用することができます。

- configure_cps.pl ユーティリティを実行する前に、**root** ユーザーのデフォルトシェルを **KSH** または **bash** に変更します。
- クラスタの各ノードで configure_cps.pl ユーティリティを実行した後に、次の手順を実行します。
 - 手動で古い信用証明ディレクトリまたはソフトリンクを削除します。次に例を示します。

```
# rm -rf /var/VRTSvcs/vcsauth/data/CPSERVER
```

- 信用証明ディレクトリの共有場所への新しいソフトリンクを作成します。

```
# ln -s path_of_CP_server_credential_directory ¥  
/var/VRTSvcs/vcsauth/data/CPSERVER
```

- CPSSG サービスグループを起動します。

```
# hagrps -online CPSSG -any
```

CP サーバーをセキュアモードで 6.0 にアップグレードした後に cpsadm コマンドが失敗する(2478502)

cpsadm コマンドは、コーディネーションポイントサーバー (CP サーバー) をセキュアモードで 6.0 にアップグレードした後に失敗することがあります。古い VRTSat パッケージをシステムから削除していないと、cpsadm コマンドは、システムに存在するその古いセキュリティバイナリを読み込みます。インストーラが CP サーバーで cpsadm コマンドを実行し、SVS クラスタ (アプリケーションクラスタ) を追加またはアップグレードすると、インストーラも失敗します。

回避策: CP サーバーのすべてのノードで次の手順を実行します。

- cpsadm という名前を cpsadmbin に変更します。

```
# mv /opt/VRTScps/bin/cpsadm /opt/VRTScps/bin/cpsadmbin
```

- 次の内容で、ファイル /opt/VRTScps/bin/cpsadm を作成します。

```
#!/bin/sh
EAT_USE_LIBPATH="/opt/VRTScps/lib"
export EAT_USE_LIBPATH
/opt/VRTScps/bin/cpsadmbin "$@"
```

- 新しいファイルに次の権限を与えます。

```
# chmod 755 /opt/VRTScps/bin/cpsadm
```

インストールに関する問題

このセクションでは、インストール時とアップグレード時の既知の問題について説明します。

Solaris 10 Update 10 への Live Upgrade を実行した後、代替ブートの環境からのブートが失敗することがある(2370250)

設定に、クラスタ内の CFS としてマウントされている共有ディスクグループ内のボリュームが含まれている状況で、vxlustart コマンドを使用してサポート対象の Solaris バージョンから Solaris 10 Update 10 への Live Upgrade を実行した場合、代替ブート環境からのブートに失敗することがあります。

回避策:vxlufinish コマンドを実行します。システムを再ブートする前

に、/altroot.5.10/etc/vfstab ディレクトリ内にある、CFS としてマウントされる共有ディスクのすべてのボリュームのエントリを手動で削除してください。

Solaris 10 Update 10 への Live Upgrade はゾーンが存在する場合に失敗する(2521348)

ゾーンが存在する場合に vxlustart コマンドを使用して Solaris 10 Update 7 5.1SP1 から Solaris 10 Update 10 に SFCFSA Live Upgrade を実行すると、次のエラーメッセージを出して失敗します。

```
ERROR: Installation of the packages from this media of the media failed;
pfinstall returned these diagnostics:
Processing default locales
    - Specifying default locale (en_US.ISO8859-1)
Processing profile
ERROR: This slice can't be upgraded because of missing usr packages for
the following zones:
ERROR:     zone1
ERROR:     zone1
ERROR: This slice cannot be upgraded because of missing usr packages
for one or more zones.
The Solaris upgrade of the boot environment <dest.27152> failed.
```

これは Solaris の luupgrade コマンドを使用した場合に発生する既知の問題です。

回避策: この問題の可能な回避策があるかどうか、Oracle の情報を確認してください。

Sparc では Solaris 9 から Solaris 10 Update 10 への Live Upgrade に失敗することがある(2424410)

Sparc 上での Solaris 9 から Solaris 10 Update 10 への Live Upgrade は、次のエラーにより失敗することがあります。

```
Generating file list.
Copying data from PBE <source.24429> to ABE <dest.24429>.
99% of filenames transferredERROR: Data duplication process terminated
unexpectedly.
ERROR: The output is </tmp/lucreate.13165.29314/lucopy.errors.29314>.

29794 Killed
Fixing zonepaths in ABE.
Unmounting ABE <dest.24429>.
100% of filenames transferredReverting state of zones in PBE
<source.24429>.
ERROR: Unable to copy file systems from boot environment <source.24429>
to BE <dest.24429>.
ERROR: Unable to populate file systems on boot environment <dest.24429>.
```

```
Removing incomplete BE <dest.24429>.  
ERROR: Cannot make file systems for boot environment <dest.24429>.
```

これは Solaris の `lucreate` コマンドを使用した場合に発生する既知の問題です。

回避策: この問題の可能な回避策があるかどうか、Oracle の情報を確認してください。

ソフトウェアの制限事項

VMware vSphere Extension for VirtualStore の制限事項

このリリースの VMware vSphere Extension for VirtualStore で認識されているソフトウェアの制限事項は、次のとおりです。

ウィザードの更新に対して F5 キーの使用がサポートされていない (2362940)

ウィザードの更新に対して F5 キーの使用はサポートされていません。

回避策

新しいデータまたは更新されたデータを取得するには、ウィザードを再起動する必要があります (F5 キーは使わない)。

VMware スナップショットを含む仮想マシンをゴールデンイメージとして使うことができない (2514969)

VMware スナップショットが格納されている仮想マシン (またはテンプレート) は、FileSnap ウィザードでクローンを作成するためのゴールデンイメージとして使うことができません。このような仮想マシン (またはテンプレート) を使うには、最初にスナップショットを削除してから FileSnap ウィザードを使います。

I/O フェンシングに関する制限事項

この項では、I/O フェンシングに関するソフトウェアの制限事項について説明します。

VRTSvxvm をアンインストールすると、VxFEN が dmp のディスクポリシーと SCSI3 モードで設定された場合問題が生じる (2522069)

VxFEN を dmp のディスクポリシーと SCSI3 モードで設定した場合、コーディネータディスクの DMP ノードが、システム停止時またはフェンシングアービトレーションの間にアクセスされることがあります。VRTSvxvm パッケージをアンインストールした後では、DMP のモジュールはもはやメモリに読み込まれません。VRTSvxvm がパッケージアンインス

トールされたシステムでは、VxFEN がシステム停止時またはフェンシングアービトレーションの間に DMP デバイスにアクセスすると、システムパニックが発生します。

マニュアルの誤記

以下では、マニュアルバージョン:6.0.0 の製品マニュアルの補足や修正について説明します。これらの追加または修正は、シマンテック社のサポート Web サイトからダウンロードできる新しいバージョンの製品マニュアルや Symantec Operations Readiness Tools (SORT) では適用済みである場合があります。

そのコンポーネントまたは製品に関するマニュアルの誤記については、対応するリリースノートを参照してください。

p.33 の「[マニュアル](#)」を参照してください。

VirtualStore のマニュアルページ

次の誤記は、VirtualStore のマニュアルページに当てはまります。

svsvmwadm の -P および --vcport オプションがない

- P オプションと --vcport オプションが svsvmwadm のマニュアルページで見つかりません。次のオプションと説明があることになっています。

```
-P, --vcport      HTTPS port in the range 1-65535 (443 default)
                  configured in VMware vCenter Server
```

マニュアル

マニュアルはソフトウェアメディアの `/product_name/docs` ディレクトリで PDF の形式で利用可能です。追加マニュアルはオンラインで入手できます。

シマンテック社では、インストールガイドやリリースノートなどの適切な情報を、ユーザーのシステムの `/opt/VRTS/docs` ディレクトリにコピーして参照できるようにしておくことをお勧めします。

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。マニュアルの発行日付は、各マニュアルのタイトルページ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。

<http://sort.symantec.com/documents>

マニュアルセット

表 1-6 は Veritas Storage Foundation Cluster File System High Availability に関するマニュアルのリストです。

表 1-6 Veritas Storage Foundation Cluster File System High Availability のマニュアル

マニュアル名	ファイル名
Veritas Storage Foundation Cluster File System High Availability リリースノート	sfdfs_notes_60_sol.pdf
Veritas Storage Foundation Cluster File System High Availability インストールガイド	sfdfs_install_60_sol.pdf
Veritas Storage Foundation Cluster File System High Availability 管理者ガイド	sfdfs_admin_60_sol.pdf

表 1-7 は Symantec VirtualStore に関するマニュアルのリストです。

表 1-7 Symantec VirtualStore のマニュアル

マニュアル名	ファイル名
Symantec VirtualStore リリースノート	virtualstore_notes_60_sol.pdf
Symantec VirtualStore インストール/設定ガイド	virtualstore_install_60_sol.pdf
Symantec VirtualStore 管理者ガイド	virtualstore_admin_60_sol.pdf

VOM (Veritas Operations Manager) を使用して Veritas Storage Foundation and High Availability 製品を管理する場合は、次の Web サイトにある VOM 製品のマニュアルを参照してください。

<http://sort.symantec.com/documents>

マニュアルページ

Veritas Storage Foundation and High Availability Solutions 製品のマニュアルページは、`/opt/VRTS/man` ディレクトリにインストールされています。

`man(1)` コマンドで Veritas Storage Foundation マニュアルページを参照できるように、`MANPATH` 環境変数を設定します。

- Bourne シェルまたは Korn シェル (`sh` または `ksh`) の場合は、次のコマンドを入力します。

```
MANPATH=$MANPATH:/opt/VRTS/man  
export MANPATH
```

- C シェル (csh または tcsh) の場合は、次のコマンドを入力します。

```
setenv MANPATH ${MANPATH}:/opt/VRTS/man
```

man (1) のマニュアルページを参照してください。

