Symantec™ VirtualStore リリースノート

Solaris

6.0.1

Symantec

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: 6.0.1

マニュアルバージョン: 6.0.1 Rev 0

著作権について

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

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

このリリースノートには Solaris 対応の Symantec VirtualStore（SVS）バージョン 6.0.1 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: 6.0.1 Rev 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。最新の製品マニュアル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。

`/docs/product_name`

シマンテック社は、システムの `/opt/VRTS/docs` ディレクトリにファイルをコピーすることを推奨します。

このリリースには、次のコンポーネント製品のリリースノートが含まれます

- 『Veritas Storage Foundation リリースノート』(6.0.1)
- 『Veritas Cluster Server リリースノート』(6.0.1)
- 『Veritas Storage Foundation Cluster File System High Availability リリースノート』(6.0.1)

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。

https://sort.symantec.com/

- ハードウェア互換性リストには、サポート対象のハードウェアについての情報が含まれ、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。

6.0.1 で導入された変更点

この項では Symantec VirtualStore 6.0.1 の変更点の一覧を示します。

SFHA Solutions 製品の新しいバージョニングプロセス

シマンテック社は、ストレージ、可用性、バックアップ、アーカイブ、および企業セキュリティ製品などの当社の異なる製品の配備に関して、お客様に統一されたエクスペリエンスを提供するためにバージョニングプロセスの単純化を行いました。この変更によって、全製品に 3 桁のバージョンが付きます。この方法に従い、最新の SFHA Solutions リリースはバージョン 6.0.1 として利用可能です。

ソフトウェアメディア内のマニュアルの新しいディレクトリの場所

製品マニュアルの PDF ファイルは、ソフトウェアのメディア内の `/docs` ディレクトリに配置されるようになりました。`/docs` ディレクトリ内に各バンドル製品のサブディレクトリがあり、その製品固有のマニュアルがその中にあります。`sfha_solutions` ディレクトリに、すべての製品に適用されるマニュアルが含まれています。

インストールとアップグレードに関する変更

6.0.1 の製品インストーラには、次の変更点が含まれています。

ローカルにインストールされたインストールとアンインストールのスクリプトにリリースバージョンが含まれる

Veritas 製品を設定するためにローカルスクリプト(/opt/VRTS/install)を実行する場合、インストールされたスクリプトの名前にリリースバージョンが含まれるようになりました。

メモ: インストールメディアから Veritas 製品をインストールする場合は、引き続きリリースバージョンを含まない `installsvs` コマンドを実行してください。

インストールされたバイナリからスクリプトを実行するには、installsvs*<version>* コマンドを実行します。

<version> はピリオドやスペースを含まない現在のリリースバージョンです。

たとえば、製品の 6.0.1 バージョンを設定するには、次のコマンドを実行します。

```
# /opt/VRTS/install/installsvs601 -configure
```

ディスクグループの VxVM プライベートリージョンバックアップの事前点検(アップグレード実施前)

インストーラは、アップグレード実施前に、VxVM プライベートリージョン内にあるすべてのディスクグループの設定ファイルの最近のバックアップが /etc/vx/cbr/bk ディレクトリ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。

Solaris 11 自動インストーラのサポート

Oracle Solaris Automated Installer(AI)を使って、ネットワークの複数のクライアントシステムで Solaris 11 のオペレーティングシステムをインストールできます。AI は x86 と SPARC システム両方でハンズフリーインストール(手動操作のない自動インストール)を実行します。また、AI メディア(Oracle の Web サイトからダウンロード可能な、Oracle の提供するブート可能な AI のイメージ)を使用して、単一の SPARC または x86 プラットフォームに Oracle Solaris OS をインストールできます。いずれの場合も、インストールを完了するにはネットワーク上にパッケージのリポジトリへのアクセスが必要です。

コーディネーションポイントサーバー設定に関するインストーラのサポート

インストーラで -configcps オプションを使用して CP サーバーを設定できるようになりました。CP サーバーを設定するこの機能は、インストーラに組み込まれるようになりました。以前のバージョンでは、CP サーバーを設定するには configure_cps.pl スクリプトを使う必要がありました。

応答ファイルを生成して、CP サーバーを設定することもできます。インストーラで -responsefile '*/tmp/sample1.res*' オプションを使って CP サーバーを設定できるようになりました。

詳しくは、『Veritas Cluster Server インストールガイド』を参照してください。

チューニングファイルテンプレートのサポート

インストーラを使って、チューニングファイルテンプレートを作成できます。-tunables オプションを指定してインストーラを開始すると、サポート対象のすべてのチューニングパラメータのリスト、チューニングファイルテンプレートの場所が表示されます。

追加のインストール postcheck オプション

postcheck オプションが追加の検査を含むように拡張されました。

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。
- VM（Volume Manager）の検査。
- FS（ファイルシステム）の検査。
- CFS（Cluster File System）の検査。

Symantec VirtualStore に関する変更

6.0.1 の Symantec VirtualStore（SVS）には、次の変更点が含まれています。

Citrix XenDesktop

SymantecVirtualStore (SVS) 6.0.1 は、Citrix XenDesktop とともに使用する領域最適化済みの仮想マシンをすばやく作成できます。VirtualStore vCenter プラグインは、VMware vSphere、Citrix XenDesktop、VirtualStore 間の統合を提供し、仮想マシンの管理を容易にします。

Symantec VirtualStore 6.0.1 は、VMware vSphere 5.0 に対してテストする必要がある

Symatec VirtualStore (SVS) 6.0.1 はテスト済みであり、シマンテック社は、ファイルシステムおよび vSphere プラグインを含むすべての SVS の機能が VMware Vspere 5.0 と共に使われたときに正しく動作することを証明します。

LLT への変更

このリリースには、LLT への次の変更が含まれています。

/etc/lltab ファイルの peerinact の値の設定

シマンテック社は、peerinact の値を 0 に設定しないことを推奨します。peerinact の無限タイムアウト機能を設定するため、peerinact を大きい値に設定してください。サポート対象の値の範囲は 1 から 2147483647 までです。

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。

CoordPoint エージェントの拡張

CoordPoint エージェントは、VxVM 管理コマンドの不注意な実行によるコーディネータディスクグループからのディスクの削除や、ディスクの VxVM プライベートリージョンの破損など、コーディネータディスクグループの構成の変更を監視します。

エージェントは CoordPoint リソースの詳細な監視を実行し、障害を報告します。ユーザーはこのリリースで導入された LevelTwoMonitorFreq 属性を設定することで、詳細な監視の頻度を調整できます。たとえば、この属性に 5 を設定すると、エージェントは 5 番目の監視サイクルごとにコーディネータディスクグループの構成を監視します。

CoordPoint エージェントについて詳しくは、『Veritas Cluster Server 付属エージェントリファレンスガイド』を参照してください。

スクリプトベースのインストーラを使った CoordPoint エージェントの設定と、コーディネータディスクを監視するための CoordPoint エージェントの手動設定については、『Veritas Cluster Server インストールガイド』を参照してください。

クラスタがオンラインのときの I/O フェンシングコーディネータディスクまたはコーディネータディスクグループの置き換えについては、『Veritas Cluster Server 管理者ガイド』を参照してください。

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。

サポート対象の Solaris オペレーティングシステム

ここでは、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 1-1 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 1-1 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	x86
Solaris 11	SRU1 以降	SPARC
Solaris 11	SRU1 以降	x86

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）
- VMware vSphere 5.0（ESX 5.0 以降と vCenter Server 5.0 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

サポート対象の Citrix XenDesktop バージョン

- Citrix XenDesktop 5

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。

Symantec VirtualStore の修正済みの問題

このリリースで修正された Symantec VirtualStore の問題はありません。

Veritas File System の修正済みの問題

このセクションでは、このリリースの Veritas File System で修正されたインシデントについて説明します。

表 1-2 Veritas File System の修正済みの問題

インシデント	説明
2838471	お客様のユースケースをサポートするため、rstchown マウントオプションを追加する必要があります。
2764861	vxcompress による圧縮解除でクォータ制限が無視されます。
2753944	ファイル作成スレッドがハングすることがあります。
2735912	fsppadm enforce を使った階層再配置のパフォーマンスが、多数のファイルを移動するときに低下します。
2712392	VxFS でスレッドがハングします。
2709869	vx_free() で fiostat の解放を試みたときに、システムが redzone 違反でパニックします。
2684573	いくつかのチェックポイントが削除されると、VRTScavf パッケージに対する cfsumount(1M) コマンドのパフォーマンスが低下します。

インシデント	説明
2674639	- p オプションを指定して cp(1) コマンドを実行する場合、FCL（File Change Log）機能が有効になっているファイルシステムでは失敗することがあります。次のエラーメッセージが表示されます: cp:「file_name」の権限を設定中（setting permissions for 'file_name'）: 入出力エラー（Input/output error）cp:「file_name」の権限を保存中（preserving permissions for 'file_name'）: 使用可能なデータはありません（No data available）。
2670022	重複したファイル名がディレクトリ内にある場合があります。
2655788	CDS（cross-platform data sharing）を使用して、32,000 以上の nlink を持つファイルシステムを変換すると、vx_maxlink および maxlink_enable チューニングパラメータが更新されません。
2651922	VxFS ファイルシステム上での ls -l コマンドの実行速度が遅く、CPU 使用率が高くなります。
2600168	cp_vxfs コマンドの -p オプションは、Solaris では正しく動作しません。
2597347	1 つのデバイスレコードのみ破損しており、レプリカは破損していない場合、fsck はコアダンプを出力しないはずです。
2583197	パーティションディレクトリおよび Storage Checkpoints が存在するファイルシステムでディスクレイアウトバージョン 8 を 9 にアップグレードすると、読み取り専用ファイルシステムであるとのエラーメッセージが返されることがあります。
2566875	クォータ限度を超過する write(2) 操作が、ユーザーのクォータ限度に達する前に、EDQUOT エラー（ディスククオータ超過）で失敗します。
2559450	コマンド fsck_vxfs (1m) は、SEGV_ACCERR エラーでコアダンプを出力することがあります。
2536130	FCL が有効になっている場合、fscdsconv が特定のプラットフォーム間での FS 変換に失敗します。
2272072	VCS エンジンの HAD が応答しなかったため、GAB がボックスでパニックを発生させます。lobolt が折り返します。
2086902	Spinlock が vxfs の spinlock で長時間保持され、多くの競合が生じます。
1529708	vxrepquota の出力に形式の問題があります。

Veritas File System: 6.0 RP1 の修正済みの問題

ここでは、Veritas File System 6.0 RP1 で解決したインシデントについて説明します。

表 1-3 Veritas File System 6.0 RP1 の修正済みの問題

修正済みの問題	説明
2679361	I18N-level0 環境では、ネットワークカスタマイズの画面に NIC が表示されません。
2678096	カウント値が 0 のとき、fiostat コマンドによりコアダンプが出力されます。
2663750	cvm 耐性シナリオで完全なストレージの障害が発生した後、エンジンログにメッセージが出力されます。
2660761	クラスタをマウントしたファイルシステムで、SmartMove 機能の実行中にメモリ破損が検出されます。
2655786	共有エクステントは、レプリケーションプロセスでは共有としては転送されません。
2655754	スピンロックの割り込みレベルが正しくないため、デッドロックが発生し、その時点で、遅延した割り当てリストがロックされます。
2653845	-r と -R オプションを指定して fsckptadm(1M) コマンドを実行すると、相互排他的な 2 つのオプションが同時に実行されます。
2646936	ソースファイルシステムに共有エクステントが存在すると、レプリケーションプロセスによりコアダンプが出力されます。
2645441	ネーティブのファイルシステムが vxfs ディスクレイアウトバージョン 8 に移行されました(レイアウトバージョン 9 がデフォルトです)。
2645435	fsmap(1M) コマンドの実行中、エラーメッセージ UX:vxfs fsmap: ERROR: V-3-27313 が表示されました。
2645112	共有の圧縮済みエクステントにマッピングされた通常のファイルで書き込み操作を実行すると、破損が生じます。
2645109	vxfilesnap コマンドの実行が成功した場合で、filesnap 操作を行った後、短時間のうちにソースファイルが削除されると、対象ファイルが破損して、スーパーブロックの VX_FULLFSCK フラグが設定されることがまれにあります。
2645108	特定の場合には、最終割り当てエクステントとして共有エクステントを所有する通常のファイルに書き込みを行うと、EIO エラーが発生することがあります。
2630954	内部 CFS ストレス再構成テスト中に fsck(1M) コマンドが終了します。
2630754	Solaris x86 の 64 ビット vxfsutil.so が読み込まれません。

修正済みの問題	説明
2624459	DMAPI を使ってパーティションディレクトリのリストを作成すると、すべてのエントリが出力されません。
2613884	リカバリ後、メタデータの破損が検出されることがあります。
2609002	重複排除セッションが完了していません。
2600168	cp_vxfs コマンドの -p オプションは、Solaris では正しく動作しません。
2599590	fsadm(1M) コマンドを使って DLV5 ファイルシステムの拡張または縮小を行うと、システムパニックが引き起こされます。
2583197	ファイルシステムをバージョン 8 から 9 にアップグレードすると、パーティションディレクトリとクローンの表示に失敗します。
2563251	fsmigadm "commit/status" エラーメッセージはクリアする必要があります。
2552095	fsadm(1M) コマンドを使ってファイルシステムを再構成しているときにシステムがパニックを引き起こすことがあります。
2536130	破損したファイルシステムや VxFS 以外のファイルシステムの変換に fscdsconv(1M) コマンドを使うと、コアが生成されます。
2389318	小さいファイルシステムで遅延した割り当てを有効にするとファイルシステムが無効になることがあります。

インストールとアップグレードに関連した解決済みの問題

ここでは、インストールとアップグレードに関連していて、このリリースで解決されたインシデントについて記します。

表 1-4　インストールとアップグレードに関連した解決済みの問題

インシデント	説明
2627076	クロック同期問題があると不正確なサーバー名が表示されることがあります。
2526709	5.1SP1 から 6.0 にアップグレードした後、DMP-OSN のチューニングパラメータ値が永続化されません。
2424410	Sparc では、Solaris 9 から Solaris 10 Update 10 への Live Upgrade に失敗することがあります。
2088827	製品の移行時に、インストーラがディスク容量の使用を過大予想します。

インストールとアップグレード: 6.0 RP1 で解決した問題

6.0 RP1 ではインストールとアップグレードについて新しく解決したインシデントはありません。

既知の問題

ここでは、このリリースの既知の問題について説明します。

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 バッキング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す。

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 ウィザードの使用中、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す。

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 VCMDS
   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。

Solaris 11 SRU1 でシステムがハングアップすることがある

Solaris 11 SRU1 の実行中に、Oracle のバグのためにシステムがハングアップすることがあります。Oracle バグ ID は 7105131(deadman panic)です。

回避策: Solaris 11 の SRU1 を SRU2a に更新する必要があります。このバグは SRU2a(Oracle Solaris 11 SRU(Support Repository Updates)インデックス(ドキュメント ID 1372094.1))で修正されます

Veritas File System の既知の問題

この項では、Veritas File System（VxFS）のこのリリースでの既知の問題について説明します。

NFS 上で同じターゲット名で複数回 FileSnap を作成すると「ファイルが存在します」エラーが発生することがある（2353352）

「ファイルが存在します」エラーは、NFS クライアントのキャッシュ動作の結果として発生します。リンク操作が成功しているので、NFS クライアントは、`file2::snap:vxfs:` といった指定されたターゲット名でファイルが作成されていると仮定します。その結果、NFS クライアントはこの名前でファイルをキャッシュに保存します。

回避策:スナップショットが作成された後で、ターゲットファイルを削除します。これにより、NFS のクライアントに、強制的にキャッシュから名前を削除させます。次に例を示します。

```
# ln file1 file2::snap:vxfs:
# rm file2::snap:vxfs:
```

小さいファイルシステムで遅延した割り当てを有効にするとファイルシステムが無効になることがある（2389318）

小さいファイルシステム（約 100 MB）で遅延した割り当てを有効にすると、ファイルシステムが無効になることがあります。この場合、次のエラーメッセージが出て、システムコンソールログに表示されます。

```
mesg 001: V-2-1: vx_nospace - file_system file system full
(size block extent)
```

回避策: `vxtunefs` コマンドで、ファイルシステムの遅延した割り当てを無効にしてください。

遅延した割り当ては、マルチボリュームファイルシステムのボリュームの 1 つの使用率が 100% 近くになっていると、他のボリュームに空き容量があっても、自動的にオフになることがある（2438368）

遅延した割り当ては、マルチボリュームファイルシステムのボリュームの 1 つの使用率が 100% 近くになっていると、ファイルシステムの他のボリュームに空き容量があっても、自動的にオフになることがあります。

回避策:ボリュームに十分な空き容量ができれば、遅延した割り当ては自動的に再開します。

重複排除はエラー 110 で失敗することがある（2591473）

ある場合には、データ重複排除は次の例のようなメッセージを出して失敗します。

```
Saving    Status    Node            Type        Filesystem
-------------------------------------------------------------------------
00%       FAILED    node01          MANUAL      /data/fs1
        2011/10/26 01:38:58 End full scan with error
```

さらに、重複排除のログには次の例のようなエラーが記録されます。

```
2011/10/26 01:35:09 DEDUP_ERROR AddBlock failed. Error = 110
```

これらのエラーは、空き容量の少ない状態で重複排除処理が実行されたこと、そして完了するにはより多くの空き容量が必要であることを示しています。

回避策: ファイルシステムで、より多くの容量を空けてください。

vxresize はファイルシステムの縮小の際「ブロックが現在使用中」エラーで失敗する（2437138）

vxresize の縮小操作は、ファイルシステム上でアクティブな I/O が進行中で、縮小目標サイズがファイルシステムの現在の使用状況に近いときに失敗します。次の例のようなメッセージが表示されます。

```
UX:vxfs fsadm: ERROR: V-3-20343: cannot shrink /dev/vx/rdsk/dg1/vol1 -
blocks are currently in use.
VxVM vxresize ERROR V-5-1-7514 Problem running fsadm command for volume
vol1, in diskgroup dg1
```

回避策:I/O が停止した後で縮小操作を再実行してください。

システム起動時にコンソールで警告メッセージが表示されることがある（2354829）

システム起動時に、システムコンソールで次のメッセージが表示されることがあります。

```
WARNING: couldn't allocate SDT table for module vxfs
WARNING: couldn't allocate FBT table for module vxfs
Loading smf(5) service descriptions: 2/2
```

これらの警告は、SDT および FBT DTrace のプローブが、VxFS モジュールでは利用できないことを示しています。それでも VxFS のモジュールは正しくロードされており、動作します。Dtrace SDT/FBT には、サポートできるモジュールサイズの制限があります。VxFS のモジュールは Dtrace がサポートできるサイズを超えているので、SDT および FBT Dtrace のプローブは VxFS では動作しないことがあります。

回避策: この問題に対する回避策はありません。

LLT の既知の問題

ここでは、LLT 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。

デバイスの絶対パスが lltab ファイルで使われていない場合に LLT を設定できない（2858159）

（Oracle Solaris 11）仮想マシン上では、lltab のリンクに対応するデバイスの絶対パスを使ってください。たとえば、lltab ファイルで /dev/net/net:1 ではなく /dev/net/net1 を使ってください。そうしないと、LLT を設定できません。

UDP 上の LLT を使うクラスタへのノードの追加に CPI 応答ファイルを使えない（2869763）

`addnode -responsefile` コマンドを実行するときに、クラスタが UDP 上の LLT を使っていると、新しいノードで生成される `/etc/lltab` ファイルが正しくなりません。そのため、この手順は失敗し、CPI 応答ファイルを使ってクラスタにノードを追加できません。

回避策: ありません。

GAB の既知の問題

ここでは、GAB 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。

GAB は Oracle Solaris 11 の段階的アップグレード中に停止に失敗することがある（2858157）

Oracle Solaris 11 の段階的アップグレード中、GAB は停止に失敗することがあります。しかし、CPI は警告を表示し、スタックの停止を続行します。

回避策: インストーラがアップグレードを完了した後で、ノードを再ブートしてください。

gablogd で pfiles ファイルまたは truss ファイルを実行できない（2292294）

pfiles または truss が gablogd 上で実行されるときに、gablogd に信号が発行されます。gablogd は gab ioctl を呼び出し、イベントを待機中であるためにブロックされます。その結果、pfiles コマンドはハングアップします。

回避策: なし。

（Oracle Solaris 11）仮想マシン上で、GAB が開始に失敗し、終了した可能性があることを CPI（共通の製品インストーラ）が報告することがある（2879262）

GABの起動スクリプトは、起動のために予測よりも時間がかかることがあります。起動の遅延により、GAB がエラーになって終了したことを CPI が報告することがあります。

回避策: 手動で GAB とすべての依存するサービスを開始します。

I/O フェンシングの既知の問題

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 コマンドが VxFEN をオンラインとして表示する（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` コマンドを使用します。

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@sys1,
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どうかをチェックするようにクエリーします。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: アプリケーションクラスタで VxFEN を開始する前に、クラスタ名、UUID、ノード、権限などのクラスタ詳細が CP サーバーに追加されていることを確認します。

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: vxfenswap ユーティリティを SSH で（-n オプションなしで）使います。

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 を開始します。

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 アクションを使って、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ます。

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情報を手動で追加します。また、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、クラスタ情報を CP サーバーに追加します。

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 が設定されていなければ、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 が設定されていなければ、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 環境変数の値を 255 に設定します。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）

vxcpserv 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: この問題に対する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 スクリプトによって作成される NIC のリソースの名前が適切でない場合があります。たとえば、m 番目の VIP が n 番目の NIC にマップされ、m と n とが必ずしも同じでない場合です。この場合、CPSSG は問題なく動作し続けますが、configure_cps.pl を使って CPSSG を設定解除しようとすると、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うことができます。

- 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。

    ```
    # hagrp -online CPSSG -any
    ```

CP サーバーをセキュアモードで 6.0 以降にアップグレードした後に cpsadm コマンドが失敗する（2846727）

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。

この問題を解決するには

1 cpsadm という名前を cpsadmbin に変更します。

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

2 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 "$@"
```

3 新しいファイルの権限を 775 に変更します。

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

CoordPoint エージェントがコーディネータディスクグループへの新規ディスクの追加を報告しない [2727672]

コーディネータディスクグループに新しいディスクを追加したために、コーディネータディスクグループの構成要素に変更があった場合でも、CoordPoint エージェントの LevelTwo 監視は障害を報告しません。

回避策: この問題に対する回避策はありません。

コーディネーションポイントサーバーベースのフェンシングは、6.0.1 のコーディネーションポイントサーバーを使って 5.1SP1RP1 で設定されている場合に失敗することがある（2824472）

5.1SP1 インストーラ（CPI）は、5.1SP1 にトラストストアの個別のディレクトリがないために、5.1SP1 クライアントと 6.0 以降のサーバーの間で信頼関係を設定できません。信頼関係を設定できないと、5.1SP1 インストーラは、セキュアモードで 5.1SP1 クライアントが 6.0 以降の CPS と連動するように設定できません。

回避策:

cpsat または vcsat コマンドを使って CPS とクライアントとの間の信頼関係を手動で設定してください。これにより、CPS とクライアントはセキュアモードで正しく通信できます。

CoordPoint エージェントの FaultTolerance 属性の上限値はコーディネーションポイントの過半数を下回っている必要があります。（2846389）

CoordPoint エージェントの FaultTolerance 属性の上限値はコーディネーションポイントの過半数を下回っている必要があります。現在この値はコーディネーションポイント数未満です。

CP サーバーではホスト名とユーザー名の大文字と小文字が区別される（2846392）

CP サーバーのホスト名とユーザー名は、大文字と小文字が区別されます。CP サーバーと通信するためにフェンシングが使うホスト名とユーザー名は、大文字と小文字が CP サーバーデータベース内の文字と同じである必要があり、異なる場合はフェンシングを開始できません。

回避策: ホスト名とユーザー名に、CP サーバーと大文字と小文字が同じ文字を使うようにしてください。

VRTSvxfen パッケージがシステムにインストールされていない場合、インストールメディアから vxfentsthdw ユーティリティを直接実行できない（2858190）

VRTSvxfen パッケージがシステムにインストールされていない場合、vxfentsthdw ユーティリティが機能するために必要な特定のスクリプトファイルが使用可能になりません。そのため、システムに VRTSvxfen パッケージがインストールされていないと、このユーティリティをインストールメディアから実行できません。

回避策: VRTSvxfen パッケージをインストールしてから、インストールメディアまたは /opt/VRTSvcs/vxfen/bin/ からユーティリティを実行してください。

CP サーバーのユーザー名は大文字と小文字が区別されない必要がある（2846392）

CP サーバーのホスト名とユーザー名は、大文字と小文字の区別がないはずです。しかし、現在 CP サーバーは、ユーザー名とホスト名のどちらも大文字と小文字が区別されない状態をサポートしていません。CP クライアントは、ホスト名とユーザー名に大文字と小文字が異なる文字が使われている CP サーバーと通信できず、そのためにフェンシングを開始できません。

Oracle Solaris 11 への段階的アップグレードの最初のノードの再ブート後、Veritas Cluster Server が起動しないことがある（2852863）

VCS（Veritas Cluster Server）に依存するカーネルレベルのサービスのいずれかが起動しないと、VCS は起動しません。add_drv コマンドがシステムへのドライバの追加に失敗することが原因で、LLT、GAB、Vxfen の各モジュールも起動に失敗することがあります。Solaris 11 では、add_drv コマンドは、別の add_drv コマンドがシステムで同時に実行されると、実行できないことがあります。

回避策:

LLT、GAB、Vxfen の各モジュールの状態を確認します。3 つのサービスがすべてが SMF でオンラインであること確認します。その後で、VCS の開始を再試行します。

VRTSvxfen パッケージをインストールする前に vxfentsthdw ユーティリティが起動しない（2858190）

VRTSvxfen パッケージをインストールするまでは、vxfentsthdw ユーティリティを格納する /etc/vxfen.d/script/vxfen_scriptlib.sh のファイルが存在しません。この場合、このユーティリティは実行されません。

回避策:

VRTSvxfen パッケージをインストールすることに加え、インストール DVD から vxfentsthdw ユーティリティを直接実行してください。

共通の製品インストーラはリリースバージョン 5.1SP1 のクライアントシステムとリリースバージョン 6.0 以降のサーバーの間で信頼関係を設定できない（2824472）

この問題は、5.1SP1 リリースバージョンがトラストストアの個別のディレクトリをサポートしていないために発生します。しかし、リリースバージョン 6.0 以降はトラストストアの個別のディレクトリをサポートしています。このトラストストアのサポートの不一致が原因で、クライアントシステムとサーバーとの間の信頼関係を設定できません。

回避策: cpsat または vcsat コマンドを使ってコーディネーションポイントサーバーとクライアントシステムとの間の信頼関係を手動で設定してください。これにより、サーバーとクライアントシステムはセキュアモードで通信できます。

スタックの再インストール後、サーバーベースのフェンシングは開始に失敗することがある（2802682）

スタックの再インストール後、既存の設定ファイルを使う場合、サーバーベースのフェンシングは開始に失敗することがあります。

回避策:

スタックの再インストール後、スタックがアンインストールされるときにクライアントクラスタ情報が削除されるため、コーディネーションポイントサーバーのクライアントクラスタ情報を追加する必要があります。詳しくは、『Symantec VirtualStore インストールガイド』のサーバーベースの I/O フェンシングを手動で設定する方法の項を参照してください。または、手動で /etc/vxfenmode ファイルと main.cf ファイルを修正し、無効モードでフェンシングを開始してから、フェンシングを設定できます。

インストールの既知の問題

ここでは、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 SFCFSHA 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。

誤った resstatechange トリガの警告

リソースを再起動するときに、次の警告が表示されることがあります。

```
CPI WARNING V-9-40-4317 The installer has detected that resstatechange
trigger is configured by setting TriggerResStateChange attributes.
```

回避策:

将来のリリースでは、resstatechange トリガはリソースが再起動するときに呼び出されません。その代わり、resrestart トリガは TriggerResRestart 属性で設定した場合に呼び出されます。resrestart トリガは現在のリリースで利用可能です。詳しくは、VCS のマニュアルを参照してください。

dmp_native_support を有効にした場合の Solaris 10 での 6.0.1 への Live Upgrade が失敗する（2632422）

Solaris 10 での 6.0.1 への Live Upgrade の実行中、`dmp_native_support` が有効になっていると、`vxlustart` コマンドが失敗します。ネーティブデバイスの Veritas Dynamic Multi-Pathing（DMP）サポートでは、名前の付け方がエンクロージャに基づく名前付け（EBN）に設定されている必要があります。ネーティブデバイスのサポートが有効になっている場合、DMP 6.0.1 では、名前の付け方を EBN から変更することは許可されません。

DMP 5.1 Service Pack 1（5.1SP1）のバグが原因で、名前の付け方をオペレーティングシステムに基づく名前の付け方（OSN）に設定できることがあります。ただし、これはサポートされた設定ではありません。名前の付け方を OSN に設定すると、`vxlustart` コマンドが失敗します。

回避策: すべてのノードで `dmp_native_support` を無効にします。

Web インストーラを停止するとデバイスがビジー状態であるというエラーメッセージが表示される（2633924）

Web インストーラを起動すると、操作（プレチェック、設定、アンインストールなど）が実行され、デバイスがビジー状態であることを知らせるエラーメッセージが表示されることがあります。

回避策: 次のいずれかを実行します。

- start.pl プロセスを終了します。
- Web インストーラを再度起動します。最初の Web ページで、セッションがアクティブであることが確認できます。このセッションをテイクオーバーして終了させるか、または直接終了させます。

CommandCentral と Storage Foundation をインストールするときの誤ったアンインストールエラーメッセージ（2628165）

Veritas CommandCentral Management Server 製品を Solaris マシンにインストールし、次いでそのマシンに Storage Foundation ソフトウェアをインストールしようとすると、VRTSsfmh がアンインストールされることを示す次の誤ったメッセージが表示されることがあります。

```
CPI WARNING V-9-40-3866 The VRTSsfmh package on hostname will be
uninstalled.

Note that the system hostname is reporting to the following
management servers:

ccs://hostname
```

回避策: この誤ったメッセージは無視してください。

ブラウザが開いたままの場合、Web インストーラは最初のセッションの後で認証を要求しない（2509330）

SVS をインストールまたは設定し、Web インストーラを閉じた後でも、他のブラウザウィンドウが開いていた場合には、Web インストーラはその後のセッションで認証を要求しません。Web インストーラからログアウトするオプションはないので、システム上でブラウザが開いている限り、セッションは開いたままになります。

回避策: すべてのブラウザウィンドウを閉じて、ブラウザセッションを終了し、その後でもう一度ログインしてください。

Solaris 10 で JumpStart によって Flash アーカイブをインストールした場合、新しいシステムは再ブート時にメンテナンスモードに入ることがある（2379123）

Flash アーカイブをカプセル化ルートディスクのゴールデンホストで作成し、この Flash アーカイブを JumpStart で別のホストにインストールした場合、新しいシステムは、最初の再ブート時にメンテナンスモードに入ります。

この問題は、Flash アーカイブの事前定義済みルートディスクミラーのために発生します。アーカイブを、クローンシステム（異なるハードディスクドライブを持っている可能性がある）に適用すると、新しくクローンされたシステムは、再ブート時のルートディスクミラー化でスタックすることがあります。

回避策: カプセル化ルートディスクのないゴールデンホストで Flash アーカイブを作成してください。Flash アーカイブを作成する前に `vxunroot` を実行して、ミラー化されたルートディスクをクリーンアップしてください。

ルータビリティを有効にした状態で Veritas Storage Foundation 5.1 Service Pack 1 Rolling Patch 2 から 6.0.1 にアップグレードすると失敗する（2581313）

Solaris 10 で、カプセル化されたルートディスクを使用して、Veritas Storage Foundation（SF）5.1 Service Pack（SP）1 Rolling Patch（RP）2 から 6.0.1 にアップグレードしようとすると、失敗します。これは、Veritas Volume Manager（VxVM）のインストール後スクリプトが `initrd` デーモンを開始できないからです。

回避策: カプセル化ルートディスクを使用して 5.1 SP1 RP2 から 6.0.1 にアップグレードするには、アップグレードの前に、システムに nash ユーティリティを再インストールする必要があります。

カプセル化ルートディスクを使用して 5.1 SP1 RP2 から 6.0.1 にアップグレードするには

1. ルートディスクをカプセル化します。
2. nash ユーティリティを再インストールします。
3. SF 6.0.1 リリースにアップグレードします。

アップグレードの途中でインストーラを停止した後、アップグレードを再開すると、サービスグループがフリーズすることがある [2574731]

サービスグループは、製品のインストーラを使用してアップグレードを開始し、インストーラがいくつかのプロセスを停止した後でインストーラを停止し、それからアップグレードを再開すると、フリーズします。

回避策:アップグレードが完了した後で、サービスグループを手動でアンフリーズしてください。

サービスグループを手動でアンフリーズするには

1. フリーズしたサービスグループすべてをリストします。

```
# hagrp -list Frozen=1
```

2. フリーズしているサービスグループをすべてアンフリーズします。

```
# haconf -makerw
# hagrp -unfreeze service_group -persistent
# haconf -dump -makero
```

ロケール変更後、vxconfig デーモンを再起動する（2417547）

vxconfig デーモンを使用するノードのロケールを変更した場合、vxconfig デーモンを再起動する必要があります。vxconfigデーモンはブート時に開始します。ロケールを変更した場合、デーモンを再起動する必要があります。

回避策:『Veritas Storage Foundation Cluster File System High Availability 管理者ガイド』の「vxconfigd デーモンのリカバリ」を参照してください。

ターゲットシステムのルートディスクがカプセル化されている場合にはフラッシュアーカイブのインストールはサポートされない

シマンテック社は、マスターシステムのルートディスクがカプセル化されている場合、フラッシュアーカイブを使用した SVS インストールをサポートしません。

インストールを開始する前にターゲットシステムのルートディスクがカプセル化が解除されていることを確認してください。

設定なしで 5.0 MP3 をインストールしてから 6.0.1 にアップグレードすると、インストーラが続行できない（2016346）

製品を設定せずに 5.0 MP3 リリースをインストールした場合は、6.0.1 リリースにアップグレードできません。このアップグレードパスはサポートされません。

回避策: 5.0 MP3 をアンインストールし、次に 6.0.1 をインストールします。

Symantec VirtualStore HA のアップグレードまたはアンインストールでモジュールアンロードエラーが発生する場合がある（2159652）

Symantec VirtualStore HA をアップグレードまたはアンインストールするとき、一部のモジュールが次のメッセージと類似のエラーメッセージでアンロードに失敗する場合があります。

```
fdd を node_name で停止できませんでした
vxfs を node_name で停止できませんでした
```

問題はサブクラスタのいずれか 1 つまたはすべてのノードで発生することがあります。

回避策:アップグレードまたはアンインストールが完了した後、インストーラから提供される指示に従って問題を解決してください。

カプセル化ルートディスクを使用して 5.1SP1 から 6.0.1 にアップグレードする際に、デポートされたディスクグループでターゲットディスクグループ名が使用されていた場合には、ルートミラーの分割が失敗する（2280560）

カプセル化ルートディスクを使用して SVS 5.1 SP1 から SVS 6.0.1 へアップグレードする際に、分割操作のターゲットディスクグループ名が、既存のデポートされたディスクグループで使用されていた場合には、ルートミラーの分割が失敗します。

回避策:

分割操作のターゲットには、異なるディスクグループ名を指定してください。

1 つ以上の CP サーバーに登録されたクラスタをインストーラが分割できない（2110148）

サーバーベースのフェンシングを使うクラスタの分割は、現時点でサポートされていません。

クラスタを 2 分割し、インストーラを使って 2 つのクラスタで Symantec VirtualStore HA を再設定することは可能です。たとえば、クラスタ *clus1* を *clus1A* と *clus1B* に分割することができます。

ただし、インストーラを使って Symantec VirtualStore HA を再設定する場合は、*clus1* と同じクラスタ UUID が *clus1A* と *clus1B* の両方で設定されます。*clus1A* と *clus1B* の両方が I/O フェンシングのために同じ CP サーバーを使う場合、CP サーバーは最初に登録を試みたクラスタからの登録のみを許可します。次に登録を試みたクラスタからの登録は拒否します。したがってインストーラは、サーバーベースのフェンシングを使うクラスタの再設定中に障害を報告します。

回避策: この問題に対する回避策はありません。

マスターノードのカーネルのアップグレードの終了後、スレーブノードの cvm グループがオンラインにならない（2439439）

あるノードでカーネルのアップグレードが正常に終了した後では、別のノードの cvm グループはオンラインになりません。

回避策: ローリングアップグレードを実行する前に、クラスタが JEOPARDY 状態になっていないか確認してください。

SmartMove が有効で、ブレークオフスナップショットボリュームが再接続されると、Veritas File System モジュールのアンロードに失敗することがある（2851403）

SmartMove が有効であり、ブレークオフスナップショットボリュームが再接続された場合、Veritas File System モジュールの vxportal と vxfs はアンロードに失敗することがあり

ます。スナップショットの再接続によって、vxportal モジュールの参照数が増え、これが原因でモジュールのアンロードにエラーが発生します。

回避策:

vxportal モジュールをアンロードする前に、手動で Veritas Volume Manager モジュール（vxspec、vxio、vxdmp）をアンロードしてください。これにより、vxportal モジュールの参照数が減少します。

SVS のインストールの完了時に Perl モジュールのエラーが発生する（2879417）

SVS をインストール、設定、アンインストールするときに、インストーラはオプションとしてシマンテック社の Web サイトにインストールログをアップロードするためのメッセージを表示します。インストーラで接続の問題が発生した場合、次のようなエラーが表示されます。

状態を読み取れません(Status read failed):
<midia_path>/../perl/lib/5.14.2/Net/HTTP/Methods.pm **行** 269 **の接続はピアによってリセットされます**(Connection reset by peer at <midia_path>/../perl/lib/5.14.2/Net/HTTP/Methods.pm line 269)

回避策:

このエラーは無視してください。悪影響はありません。

ソフトウェアの制限事項

6.0.1 リリースの Veritas Storage Foundation Cluster File System High Availability（SFCFSHA）のソフトウェア制限事項は、次のとおりです。

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

マニュアルは、ソフトウェアメディアの `/docs/<製品名>` ディレクトリで PDF 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。

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 1-5 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 1-5 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	sfcfs_notes_601_sol.pdf
Veritas Storage Foundation Cluster File System High Availability インストールガイド	sfcfs_install_601_sol.pdf
Veritas Storage Foundation Cluster File System High Availability 管理者ガイド	sfcfs_admin_601_sol.pdf

表 1-6 は Symantec VirtualStore に関するマニュアルのリストです。

表 1-6 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_601_sol.pdf
Symantec VirtualStore インストール/設定ガイド	virtualstore_install_601_sol.pdf
Symantec VirtualStore Administrator's Guide	virtualstore_admin_601_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

メモ: GNOME PDF Viewer を使用してシマンテック社のマニュアルを参照することはできません。マニュアルを参照するには、Adobe Acrobat を使用してください。

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。