Veritas™ Cluster Server リリースノート

Linux

6.0.1

Symantec

Veritas™ Cluster Server 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

Veritas Cluster Server 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 Linux 対応の Veritas Cluster Server（VCS）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。VCS 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、VCS の製品マニュアルに記載の情報に優先します。

これは『Veritas Cluster Server 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

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 について

シマンテック社の Veritas™ Cluster Server (VCS) では、物理環境と仮想環境で動作するミッションクリティカルなアプリケーションに対し、高可用性 (HA) とディザスタリカバリ (DR) がもたらされます。VCS によって、アプリケーション、インフラストラクチャ、またはサイトにエラーが発生した際にも、継続的なアプリケーションの可用性が保証されます。

VCS エージェントについて

VCS 付属エージェントは、クラスタのキーリソースを管理します。付属エージェントの実装と設定は、プラットフォームごとに異なります。

付属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。

Veritas High Availability Agent Pack により、各種のアプリケーション、データベース、サードパーティ製のストレージソリューションに高可用性を提供するエージェントにアクセスできます。Agent Pack は Symantec™ Operations Readiness Tools (SORT) から入手できます。SORT について詳しくは、https://sort.symantec.com/home を参照してください。開発中のエージェントと、シマンテック社のコンサルティングサービスから入手できるエージェントについては、この製品の購入先にお問い合わせください。

VCS では、カスタムエージェントの作成が可能なフレームワークが提供されます。Veritas High Availability Agent Pack、付属エージェント、エンタープライズエージェントがニーズに合っていないときに、エージェントを作成してください。

カスタムエージェントの作成について詳しくは『Veritas Cluster Server エージェント開発者ガイド』を参照してください。また、シマンテック社のコンサルティングサービスを通して、カスタムエージェントもご要望いただけます。

Symantec Operations Readiness Tools について

SORT (Symantec Operations Readiness Tools) は、最も時間のかかる管理タスクの一部を自動化して単純化する Web サイトです。SORT により、データセンターをさらに効率的に管理し、シマンテック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	■ 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。 ■ シマンテック製品をインストールまたはアップグレードする準備ができているかどうかを判断するためにシステムを分析する。 ■ 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。 ■ 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。
リスクの管理	■ 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。 ■ システムと環境におけるリスクを識別して軽減する。 ■ 何百ものシマンテックエラーコードの説明と解決策を表示する。
効率の向上	■ 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。 ■ インストール済みのシマンテック製品とライセンスキーを一覧表示する。 ■ 環境をチューニングして最適化する。

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.symantec.com

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 Veritas Cluster Server 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 `installvcs` 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、`installvcs<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/installvcs601 -configure
```

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。

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。

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。

VCS 6.0.1 で導入された属性

次のセクションでは VCS 6.0.1 で導入された属性について説明します。

KVMGuest エージェントの属性:

- RHEVMInfo: RHEV 環境の情報を指定します。この属性は 5 つのキーを含んでいます。
  - Enabled: 仮想化環境を指定します
  - URL: REST API 通信用の RHEV-M URL
  - User: REST API 通信用の RHEV-M ユーザー
  - Password: RHEV-M ユーザーの暗号化されたパスワード
  - Cluster: VCS ホストが属する RHEV クラスタ
- ResyncVMCfg: ResyncVMCfg 属性は havmconfigsync ユーティリティによって設定されます。この属性が設定されると、エージェントは SyncDir 属性を使って仮想マシン構成(すでに存在する場合)を再定義します。SyncDir 属性が設定されない場合は、GuestConfigFilePath 属性が使われます。

サービスグループ属性

- UserAssoc: この属性は任意の目的に使うことができます。

クラスタレベルの属性

- FipsMode: FIPS モードがクラスタに有効であるかどうかを示します。値は、システムのブローカーのモードに依存します。

VCS の仮想化サポートに関連する変更

サポート対象の Linux 仮想化技術の変更

Veritas Storage Foundation and High Availability(SFHA)Solutions 6.0.1 製品は、Linux 環境の以下の仮想化技術をサポートします。

- Red Hat Enterprise Linux(RHEL)用のカーネルベースの仮想マシン(KVM)技術
- SUSE Linux Enterprise Server(SLES)用のカーネルベースの仮想マシン(KVM)技術

SFHA Solutions 製品は、KVM ゲスト仮想マシンに以下の機能を提供します

- ストレージの可視性
- ストレージ管理
- 高可用性
- クラスタのフェールオーバー
- レプリケーションのサポート

表 1-1　ゲストとホストで KVM 技術に対して SFHA Solutions でサポートされる設定

目標	推奨される SFHA Solutions 製品設定	KVM 技術
KVM ゲスト仮想マシンのストレージ可視性	KVM ゲスト仮想マシンの DMP（Dynamic Multi-Pathing）	RHEL SLES
KVM ホストのストレージ可視性	KVM ホストでの DMP	RHEL SLES
KVM ゲスト仮想マシンのストレージ管理機能とレプリケーションサポート	KVM ゲスト仮想マシンの Storage Foundation（SF）	RHEL SLES
KVMホストの高度なストレージ管理機能とレプリケーションサポート	KVM ホストの Storage Foundation Cluster File System（SFCFSHA）	RHEL SLES
KVMホストとゲスト仮想マシンのエンドツーエンドのストレージ可視性	KVM ホストとゲスト仮想マシンの DMP	RHEL SLES
KVM ゲスト仮想マシンのストレージ管理機能とレプリケーションサポート、および KVM ホストのストレージ可視性	KVM ホストの DMP と KVM ゲスト仮想マシンの SF	RHEL SLES
KVM ゲスト仮想マシンのアプリケーション監視と可用性	KVM ゲスト仮想マシンの Symantec ApplicationHA	RHEL
KVMホストの仮想マシン監視とフェールオーバー	KVM ホストの Veritas Cluster Server（VCS）	RHEL SLES
KVM ゲスト仮想マシンのアプリケーションフェールオーバー	KVM ゲスト仮想マシンの VCS	RHEL SLES

目標	推奨される SFHA Solutions 製品設定	KVM 技術
アプリケーション可用性と仮想マシン可用性	KVM ゲスト仮想マシンの Symantec Application HA と KVM ホストの VCS	RHEL
KVM ゲスト仮想マシンと物理ホスト間のアプリケーションフェールオーバー	KVM ゲスト仮想マシンと KVM 物理ホストマシン内の VCS	RHEL SLES

VCS は、以下の Linux 仮想化環境に対して仮想から仮想（ゲスト内）へのクラスタ化をサポートします。

- RHEV（Red Hat Enterprise Virtualization）
- Microsoft Hyper-V
- OVM（Oracle Virtual Machine）

VMware のサポートについては、『Veritas Storage Foundation in a VMware ESX Environment』を参照してください。

実装の詳細:

『Veritas Storage Foundation™ and High Availability Solutions Virtualization Guide for Linux』を参照してください。

RHEV（Red Hat Enterprise Virtualization）環境で動作する仮想マシンを管理する KVMGuest エージェント

KVMGuest エージェントは、仮想マシンをオンライン化またはオフライン化し、RHEV 環境で監視します。

KVMGuest エージェントは、RHEV-M（Red Hat Enterprise Virtualization - Manager）との通信と仮想マシンの管理に REST API を使用します。このエージェントを使って、RHEV 環境の仮想マシンを高可用にしたり、監視したりできます。

このエージェントは Red Hat Enterprise Virtualization 3.0 をサポートします。詳しくは、『Veritas Cluster Server 付属エージェントリファレンスガイド』と『Veritas Storage Foundation and High Availability Solutions 仮想化ガイド Linux』を参照してください。

クラスタノード間で仮想マシンの設定を同期するユーティリティ

`havmconfigsync` ユーティリティは、クラスタノード間で仮想マシンの設定を同期する機能を提供します。

havmconfigsync ユーティリティを使って、1 つのオンラインノードからクラスタの他のノードにかけて仮想マシンの設定を同期することができます。これを行うには、クラスタのノードのいずれかで havmconfigsync <vm_name> を実行して、仮想マシン名をパラメータとして渡します。これにより仮想マシンがオンラインであるノードが検出され、共有ストレージに実行中の仮想マシンの設定が保存されます。

共有ストレージの場所は SyncDir/GuestConfigPath 属性に指定されたファイルによって識別されます。

指定されるファイルのパスが、共有ストレージ（パラレルまたはフェールオーバー）にあることを確認します。

このユーティリティは新しい設定に更新する前にオリジナルの設定ファイルのバックアップを保存します。

クラスタの他のノードでは、フェールオーバーまたはスイッチングの間に、既存の設定を削除してから共有ストレージに保存された新しい設定を使って VM を定義することにより、オンライン操作で KVMGuest の設定を再定義します。

VCS 付属エージェントの変更点

この項では VCS の付属エージェントに関する変更点について説明します。

詳しくは、『Veritas Cluster Server 管理者ガイド』と『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。

新しい付属エージェント

VFRJob エージェント: Veritas File Replication Job（VFRJob）エージェントは、ソースシステム上で VFR Job の可用性を高めます。クラスタファイルシステムまたは非クラスタファイルシステムのレプリケーションのスケジュールは、VFR Job が行います。VFRJob 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。

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。

Mount エージェントの拡張

Mount エージェントを拡張すると、同じブロックデバイスからの複数の bind タイプのマウントが可能になります。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。

Application エージェントの拡張

Application エージェントは次のように拡張されました

- StartProgram を使って、ProPCV 機能を使用できます。StartProgram 属性は、アプリケーションエージェントの IMFRegList に追加されます。
  詳しくは、『付属エージェントリファレンスガイド』と『Veritas Cluster Server 管理者ガイド』を参照してください。

KVMGuest エージェントが SLES KVM 環境で動作する仮想マシンを管理する

KVMGuest エージェントは、仮想マシンをオンライン化またはオフライン化し、SLES KVM 環境で監視します。KVMGuest エージェントは virsh コマンドを使って仮想マシンを管理します。

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。

IMF に関する変更

このリリースには、IMF（Intelligent Monitoring Framework）への次の変更が含まれています。

Open IMF アーキテクチャ

Open IMF アーキテクチャは、ユーザースペースで起きるイベントについての通知の取得を有効にすることにより、IMF 機能を拡張します。このアーキテクチャは IMFD（IMF Daemon）を使って USNP（User Space Notification Provider）から通知を収集し、AMF ドライバに渡します。AMF ドライバは、それらの通知を適切なエージェントに順次渡します。IMFD は、Open IMF を必要とするエージェントにより、AMF への最初の登録時に開始されます。

Open IMF アーキテクチャには次の利点があります

- IMF は同じ VCS リソースの下の異なるタイプのイベントをグループ化できる、カーネル領域イベントとユーザー領域イベントのための中央通知プロバイダです。
- ユーザー領域からのみ取得できる通知を活用することで、より多くのエージェントを IMF 対応にすることができます。
- エージェントは USNP と対話せずに IMF からの通知を取得できます。

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

VCS 6.0.1 の新しい IMF 対応エージェント

次のエージェントは VCS 6.0.1 で IMF 対応です

- DiskGroup エージェント

VCS エンジンに関する変更

より多くの依存関係タイプをサポートする拡張 -propagate 機能

-propagate オプションは、依存関係ツリーにグローバルまたはリモートの依存関係が含まれている場合に使うことができます。次の依存関係タイプは、オンライン伝播オプションとオフライン伝播オプションの両方でサポートされます

- online global soft
- online global firm
- online remote soft
- online remote firm

FIPS モードでクラスタセキュリティを提供する VCS

VCS は FIPS を使用してクラスタを保護するためのオプションを提供します。このオプションにより、クラスタとの通信は FIPS 承認済みのアルゴリズムを使って暗号化されます。FIPS コンプライアンスは次のガイディングファクタとともに導入されます

- FIPS コンプライアンスは VCS 6.0.1 とともに利用できる設定可能なオプションです。既存の VCS の配備が VCS 6.0 以前のバージョンから 6.0.1 にアップグレードされるときに、FIPS コンプライアンスは自動的に有効になりません。
- FIPS モードを有効にするには、クラスタが新しく、セキュリティ条件が設定されずに構成されていることを確認する必要があります。すでにセキュアなクラスタで FIPS モードを設定するには、『Veritas Cluster Server 管理者ガイド』の「クラスタのセキュアモードの有効化と無効化」の手順を参照してください。

- VCS 6.0.1 は、GCO または CP サーバーベースのクラスタの FIPS をサポートしません。

VCS がサポートするファイルレプリケーションのフェールオーバー

ファイルレプリケーションのフェールオーバーは、VCS と新しい VFRJob エージェントの使用により高可用性を実現しています。VFRJob エージェントは、VFR ジョブのスケジューリングの開始および停止と、VFR ジョブのステータスの監視を行います。新しい VFRJob エージェントは、ソースシステム上でレプリケーションジョブを高可用化するのに使われます。VFRJob タイプリソースはフェールオーバーリソースで、VFRJob の HA（High Availability）を提供します。これは、ファイルシステムがマウントされるときのリソースシステムの VFR ジョブと、ファイルシステムがレプリケートされているターゲットシステムの VFR ジョブを監視します。ターゲットシステムは同じクラスタ内にある場合もありますが、クラスタの外にある場合もあります。

ファイルシステムもホストするシステムの場合、ファイルシステムのレプリケーションの実行は失敗し、これに依存するファイルシステムはクラスタ内の別のシステムにフェールオーバーするとともに、VFRJob リソースもまたそのシステムにフェールオーバーします。したがって、VFRJob エージェントは VFR ジョブを高可用化します。ソースシステムの VFRJob は、vxfstaskd デーモンです。デーモンはスケジューラであり、ソースシステム上で RUNNING 状態である必要があります。ファイルシステムがフェールオーバーすることがあるターゲットシステムでは、vxfsrepld デーモンを実行する必要があります。

postonline トリガと postoffline トリガは手動アップグレード後に有効にする

VCS versions 5.x から 6.0 以降への手動アップグレードを実行した場合、preonline トリガと postoffline トリガを有効にする必要があります。必要に応じて、サービスグループの TriggersEnabled 属性を設定してトリガを有効にできます。

PreOnline、TriggersEnabled、ContainerInfo にグローバルな（クラスタ全体で使用される）値が設定される

サービスグループの属性である PreOnline、TriggersEnabled、ContainerInfo には、グローバルな（クラスタ全体で使用される）値が設定されます。値はシステムごとにローカライズできます。

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。

VCS のシステム必要条件

この項では、VCS のシステム必要条件を説明します。

次の情報は、VCS クラスタに適用されます。SF Oracle RAC のインストールには適用されません。

VCS では、クラスタ内のすべてのノードが同じプロセッサアーキテクチャを使用し、同じバージョンのオペレーティングシステムを実行していることが必須です。ただし、ノード間で特定の RHEL または OEL バージョンの更新レベルが異なっていたり、特定の SLES バージョンのサービスパックレベルが異なっていてもかまいません。

メモ: VCS をインストールするシステムはターゲットシステムと同じ Linux の配布を実行する必要があります。

---

p.15 の「ハードウェア互換性リスト」を参照してください。

p.15 の「サポート対象の Linux オペレーティングシステム 」を参照してください。

ハードウェア互換性リスト

このソフトウェアがサポートしているハードウェアは、互換性リストとして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

Veritas Cluster Server のインストールまたはアップグレードを行う前に、最新の互換性リストを参照して、ご使用になるハードウェアとソフトウェアのサポート状態を確認ください。

サポート対象の Linux 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 1-2 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 1-2 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	カーネルバージョン	チップセット
Red Hat Enterprise Linux 6	アップデート2、3	2.6.32-220.el6 2.6.32-279.el6	64 ビット x86、EMT*/Opteron 4.1 の 64 ビットのみ
Red Hat Enterprise Linux 5	アップデート5、6、7、8	2.6.18-194.el5 2.6.18-238.el5 2.6.18-274.el5 2.6.18-308.el5	64 ビット x86、EMT*/Opteron 4.1 の 64 ビットのみ
SUSE Linux Enterprise 11	SP1、SP2	2.6.32.12-0.7.1 3.0.13-0.27.1	64 ビット x86、EMT*/Opteron 4.1 の 64 ビットのみ
SUSE Linux Enterprise 10	SP4	2.6.16.60-0.85.1	64 ビット x86、EMT*/Opteron 4.1 の 64 ビットのみ
Oracle Linux 6	**6.2、6.3	2.6.32-220.el6 2.6.32-279.el6	64 ビット x86、EMT*/Opteron
Oracle Linux 5	**アップデート 5、6、7、8	2.6.18-194.el5 2.6.18-238.el5 2.6.18-274.el5 2.6.18-308.el5	64 ビット x86、EMT*/Opteron

* 拡張メモリテクノロジ

** RHEL 互換モードのみ。

メモ: 64 ビットオペレーティングシステムのみサポートされます。

ご使用のシステムが、より古いバージョンの Red Hat Enterprise Linux、SUSE Linux Enterprise Server または Oracle Linux を実行している場合は、Veritas ソフトウェアをインストールする前にそれらをアップグレードしてください。オペレーティングシステムのアップグレードと再インストールについて詳しくは、Red Hat、SUSE、または Oracle のマニュアルを参照してください。

シマンテック社では、Oracle、Red Hat、および SUSE で配布されたカーネルバイナリのみをサポートします。

シマンテック社製品は、前述のカーネルとパッチの後続リリース適用後でも動作します。ただし、その場合は、オペレーティングシステムがカーネルの ABI（アプリケーションバイナリインターフェース）互換を維持していることが条件です。

VCS に必要な Linux RPM

VCS をインストールまたはアップグレードするシステムで、次のオペレーティングシステム固有の RPM をインストールしてください。VCS は、次の RPM が ABI との互換性を維持する前提で、次の RPM のすべてのアップデートをサポートします。

表 1-3 に、各 Linux オペレーティングシステムで VCS が必要とする RPM の一覧を示します。

表 1-3　必要な RPM

オペレーティングシステム	必要な RPM
RHEL 5	glibc-2.5-58.i686.rpm glibc-2.5-58.x86_64.rpm ksh-20100202-1.el5_5.1.x86_64.rpm libgcc-4.1.2-50.el5.i386.rpm libstdc++-4.1.2-50.el5.i386.rpm perl-5.8.8-32.el5_5.2.x86_64.rpm
RHEL 6	glibc-2.12-1.25.el6.i686.rpm glibc-2.12-1.25.el6.x86_64.rpm ksh-20100621-6.el6.x86_64.rpm libgcc-4.4.5-6.el6.i686.rpm libstdc++-4.4.5-6.el6.i686.rpm mksh-39-5.el6.x86_64.rpm perl-5.10.1-119.el6.x86_64.rpm
SLES 10	glibc-2.4-31.81.11.x86_64.rpm glibc-32bit-2.4-31.81.11.x86_64.rpm ksh-93t-13.17.19.x86_64.rpm libgcc-4.1.2_20070115-0.32.53.x86_64.rpm libstdc++-4.1.2_20070115-0.32.53.x86_64.rpm

オペレーティングシステム	必要な RPM
SLES 11	glibc-2.11.1-0.17.4.x86_64.rpm glibc-32bit-2.11.1-0.17.4.x86_64.rpm ksh-93t-9.9.8.x86_64.rpm libgcc43-32bit-4.3.4_20091019-0.7.35.x86_64.rpm libstdc++43-32bit-4.3.4_20091019-0.7.35.x86_64.rpm

サポート対象の Linux 仮想化技術

Veritas Cluster Server は Linux 環境での次の仮想化技術をサポートします。

- RHEL（Red Hat Enterprise Linux）および SLES（SUSE Linux Enterprise Server）向けの KVM（カーネルベースの仮想マシン）技術
- RHEV（Red Hat Enterprise Virtualization）
- OVM（Oracle Virtual Machine）
- Microsoft Hyper-V

表 1-4 Red Hat システム必要条件

サポート対象アーキテクチャ	■ Intel 64 ■ AMD64
最小のシステム必要条件	■ 6 GB の空きディスク領域 ■ 2 GB の RAM
推奨のシステム必要条件	■ 6 GB + ゲストごとにゲストオペレーティングシステムによって推奨される必要なディスク領域。ほとんどのオペレーティングシステムでは、6 GB よりも多いディスク領域が推奨されます。 ■ 各仮想化 CPU とホストに対してプロセッサコアまたはハイパースレッドを 1 つずつ ■ 2 GB の RAM + 仮想化ゲストに対する追加の RAM
Red Hat のマニュアル（詳細参照用）	http://www.redhat.com/virtualization/rhev/server/library/

表 1-5 SUSE システムの必要条件

サポート対象アーキテクチャ	■ Intel 64 ■ AMD64
最小のシステム必要条件	■ 6 GB の空きディスク領域 ■ 2 GB の RAM

推奨のシステム必要条件	■ 6 GB + ゲストごとにゲストオペレーティングシステムによって推奨される必要なディスク領域。ほとんどのオペレーティングシステムでは、6 GB よりも多いディスク領域が推奨されます。 ■ 各仮想化 CPU とホストに対してプロセッサコアまたはハイパースレッドを 1 つずつ ■ 2 GB の RAM + 仮想化ゲストに対する追加の RAM

詳しくは SUSE のマニュアルを参照してください。 http://www.suse.com/documentation/sles11/book_kvm/?page=/documentation/sles11/book_kvm/data/book_kvm.html

表 1-6 KVM でサポートされる RHEL（Red Hat Enterprise Linux）構成向けの VCS システムの必要条件

VCS バージョン	6.0.1
ホストのサポート対象 OS バージョン	RHEL 6 Update 1、Update 2、Update 3
VM ゲストのサポート対象 OS	RHEL 5 Update 4、Update5、Update 6、Update 7、Update 8 RHEL 6 Update 1、Update 2、Update 3
ハードウェアの必要条件	完全な仮想化が有効にされている CPU

表 1-7 KVM でサポートされる SLES（SUSE Linux Enterprise Server）構成向けの VCS システムの必要条件

VCS バージョン	6.0.1
ホストのサポート対象 OS バージョン	SLES 11 SP2 x86_64
VM ゲストのサポート対象 OS	SLES 11 SP2
ハードウェアの必要条件	完全な仮想化が有効にされている CPU

次の表に、Red Hat Enterprise 仮想化環境でゲスト内部 VCS（Veritas Cluster Server）を実行するために必要なソフトウェアの一覧を示します。

表 1-8 KVM でサポートされる RHEV（Red Hat Enterprise Virtualization）構成向けの VCS システムの必要条件

VCS バージョン	6.0.1
物理ホストのサポート対象 OS バージョン	Red Hat Enterprise Linux 6.2、Red Hat Enterprise Virtualization - Hypervisor v3.0

VM ゲストのサポート対象 OS	RHEL 5 Update 5、Update 6、Update 7、Update 8 RHEL 6 Update 1、Update 2
ハードウェアの必要条件	完全な仮想化が有効にされている CPU

次の表に、Microsoft Hyper-V 仮想化環境で VCS（Veritas Cluster Server）をゲスト内部で実行するために必要なソフトウェアの一覧を示します。

表 1-9 Microsoft Hyper-V 設定の VCS システムの必要条件

VCS バージョン	6.0.1
ホストのサポート対象 OS バージョン	Microsoft Windows 2008 R2 Datacenter Edition
仮想マシンのサポート対象 OS バージョン	RHEL 5 Update 5、Update 6、Update 7 SLES 10SP4 SLES 11SP1
ハードウェアの必要条件	完全な仮想化が有効にされている CPU

メモ: Microsoft Hyper V 環境のゲスト仮想マシンから到達できるように SCSI アダプタを通して接続されるストレージディスクのパススルーのために、Microsoft 社の Linux Integration Components をインストールする必要があります。次の場所から Linux Integration Components をダウンロードできます。

バージョン 3.2 の場合:

http://www.microsoft.com/en-us/download/details.aspx?id=28188

バージョン 2.1 の場合:

http://www.microsoft.com/en-us/download/details.aspx?id=24247

次の表に、Oracle Virtual Machine 仮想化環境で VCS（Veritas Cluster Server）をゲスト内部で実行するために必要なソフトウェアの一覧を示します。

表 1-10 Oracle VM（Oracle Virtual Machine）構成向けの VCS システムの必要条件

VCS バージョン	6.0.1
物理ホストのサポート対象 OS バージョン	Oracle VM サーバー v3.0

VM ゲストのサポート対象 OS	RHEL 5 Update 5、Update 6、Update 7 OEL 5 Update 5、Update 6、Update 7 RHEL 6 Update 1、Update 2 OEL 6 Update 1、Update 2
ハードウェアの必要条件	完全な仮想化が有効にされている CPU

VCS のサポート対象のソフトウェア

VCS は次の Volume Manager とファイルシステムをサポートします

- LVM2、RAW ディスク、VxVM における ext2、ext3、reiserfs、NFS、bind。
- LVM2 および RAW ディスクにおける ext4 と xfs

VCS は Veritas Storage Foundation の次のバージョンをサポートします。

Veritas Storage Foundation: Veritas Volume Manager（VxVM）と Veritas File System（VxFS）

- Storage Foundation 6.0.1
  - VxVM 6.0.1 と VxFS 6.0.1
- Storage Foundation 6.0
  - VxVM 6.0 と VxFS 6.0

メモ: VCS は、製品のアップグレードを促進するために、前バージョンの Storage Foundation と次バージョンの Storage Foundation をサポートします。

サポートされるエンタープライズエージェント

エージェントがサポートするエンタープライズアプリケーションとソフトウェアのためのエージェントを 表 1-11 に一覧で示します。

表 1-11 エンタープライズアプリケーションのための VCS エージェントでサポートされるソフトウェア

エージェント	アプリケーション	アプリケーションのバージョン	Linuxのバージョン
DB2	DB2 Enterprise Server Edition	9.1, 9.5, 9.7	RHEL5、OEL5、SLES10
		9.5、9.7	SLES11
		9.7	RHEL6、OLE6
Oracle	Oracle	10gR2、11gR1、11gR2	RHEL5、RHEL6 SLES10、SLES 11、 OEL5、OEL6
Sybase	Sybase Adaptive Server Enterprise	12.5.x、15.x	RHEL5、RHEL6 SLES10、SLES11、 OEL5、OEL6

メモ: RHEL6 と OEL6 では、Oracle データベースバージョン 11gR2（11.2.0.3）がサポートされます。

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

エージェントがサポートする VCS アプリケーションエージェントとソフトウェアのリストについては、シマンテック社の Web サイト（Veritas Cluster Server Agents Support Matrix）を参照してください。

サポート対象外

VCS 製品のこのリリースでは、次の機能がサポートされません。

サポートされなくなったエージェントとコンポーネント

次の項目は VCS のサポート対象外になりました。

- CP サーバーの設定に使用された `configure_cps.pl` スクリプトは、現在は推奨されておらず、サポートされていません。

非推奨属性

非推奨の DiskGroup エージェント属性は次のとおりです

- DiskGroupType

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。

LLT、GAB、I/O フェンシングの解決済みの問題

表 1-12 に、LLT、GAB、I/O フェンシングに関する解決済みの問題を示します。

表 1-12 LLT、GAB、I/O フェンシングの解決済みの問題

インシデント	説明
2708619	scsi3_disk_policy 属性を dmp に設定すると、Veritas フェンシングモジュール (VxFEN)を有効化できません。VxFEN のソースコードは、パーティションやスライスではなく完全なディスク名を含んでいる dmp デバイスパスを取得するように更新されています。
2845244	vxfen 起動スクリプトで `grep: can't open /etc/vxfen.d/data/cp_uid_db` エラーが発生します。 このエラーは、存在しない可能性のあるファイルを vxfen 起動スクリプトが読み込もうとするために発生します。このエラーは通常、インストール後に初めて vxfen を起動するときに発生します。
2554167	`/etc/lltab` ファイルで peerinact 値を 0 に設定すると、多数のログメッセージによってシステムログファイルがいっぱいになります。

付属エージェントの解決した問題

表 1-13 は、付属エージェントに関する解決した問題の一覧です。

表 1-13 付属エージェントの解決した問題

インシデント	説明
2850904	ストレージの接続が失われるか、VxDMP 以下のすべてのパスが無効化され、PanicSystemOnDGLoss が 0 に設定されている場合、Volume リソースの同時性違反とデータ破損が起きることがあります。
2794175	Mount エージェントのファイアドリルはフェールオーバーシナリオを正確に示しません。

インシデント	説明
2728802	「httpdDir」属性の指定した場所に「httpd」バイナリまたは「ab」バイナリが存在しない場合、Apache エージェントは詳細監視を実行できません。または HTTP サーバーを起動できません。
2850905	VxFS または NFS 以外のファイルシステムタイプでは、Mount リソースの IMF 登録はブロックする必要があります。
2850916	BlockDevice 属性または MountPoint 属性の値の末尾にスラッシュあると、Mount リソースは IMF に登録されません。
2822920	最上位レベルのドメイン（TLD）の名前が 4 文字を超えている場合、DNSAgent は UNKNOWN 状態に移行します。
2679251	VCS を強制的に停止した後（hastop -local -force）に Disk Reservation リソースを構成すると、システムパニックを引き起こすことがあります。
2800021	RHEL 5 のコマンドパスの不一致に起因して clean エントリポイントは失敗します。
2846389	VCS 6.0.1 より前のリリースでは、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数より 1 少ない数に設定されていました。コーディネーションポイントの過半数に障害が発生した場合、ネットワークを分割したシナリオではクラスタ全体でパニックが発生しました。このため、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よりも小さい値に設定しなければなりませんでした。VCS 6.0.1 以降、CoordPoint エージェントの FaultTolerance 属性はコーディネーションポイントの過半数未満に設定されます。

VCS エンジンの解決した問題

表 1-14 は、VCS エンジンに関する解決した問題の一覧です。

表 1-14 VCS エンジンの解決した問題

インシデント	説明
2832754	システム名が重複するクラスタ間でグローバルクラスタオプション（GCO）が設定されている場合、「-clear」、「-flush」、「-state」のオプションを指定して `hagrp` コマンドラインユーティリティを実行すると、正しくない出力が表示されます。
2741299	ファイル記述子（FD）で EBADF が生じると、CmdSlave は条件を満たせないループから抜け出すことができなくなります。CmdSlave 処理は FD で再試行を継続し、最終的にはコアダンプを出力します。

インシデント	説明
2647049	タイムゾーンが変更されても、VCSログはログのタイムラインを更新しません。このため、タイムゾーンがシステムで更新されても、VCSは引き続き古いタイミングでメッセージを出力します。
2850906	グループが自動的に有効にされると、リソースがオンラインであってもエンジンは Start 属性をクリアします。
2692173	-nopreオプションを選択すると、エンジンはリモートの親がオンラインであるかどうかを確認しません。
2684818	main.cf で SystemList 属性より前に次の属性が指定されていると、HAD 起動時に値は拒否されます。 ■ PreOnline ■ ContainerInfo ■ TriggersEnabled ■ SystemZones
2696056	haclus -status <cluster> コマンドを実行すると、エンジンでメモリリークが発生します。
2746802	フェールオーバーグループがプローブされると、VCSエンジンはMigrateQと TargetCount をクリアします。
2746816	gab_heartbeat_alarm_handler 関数とgabsim_heartbeat_alarm_handler 関数で使われる syslog 呼び出しは、async-signal-safe ではありません。

インストール関連の解決された問題

表 1-15 インストール関連の解決された問題

インシデント	説明
2622987	ホストが管理サーバーに報告していなくても、6.0 へのアップグレード前に sfmh-discovery が実行されていると、アップグレード後に sfmh-discovery を起動できない可能性があります。

エンタープライズエージェントの解決した問題

表 1-16 は、エンタープライズエージェントに関する解決した問題の一覧です。

表 1-16 エンタープライズエージェントの解決した問題

インシデント	説明
1985093	プロセスの強制終了時またはマシンの再ブート時にプロセスが自動的に再起動するように、ohasd プロセスのエントリが init スクリプトに含まれていることを確認してください。
2831044	Sybase エージェントスクリプトのエントリポイントは、大規模なプロセスコマンドラインを処理する必要があります。

エージェントフレームワークで解決した問題

表 1-17 は、エージェントフレームワークに関する解決した問題の一覧です。

表 1-17 エージェントフレームワークで解決した問題

インシデント	説明
2660011	ManageFaults 属性の値がサービスグループレベルで NONE に設定されている場合でも、リソースが FAULTED 状態に移行します。このリソースが Critical リソースであると、サービスグループにエラーが生じます。

Veritas Cluster Server: 6.0 RP1 で解決した問題

このセクションでは、Veritas Cluster Server 6.0 RP1 で解決したインシデントについて説明します。

表 1-18 Veritas Cluster Server 6.0 RP1 で解決した問題

修正済みの問題	説明
2684822	main.cf の SystemList の前に PreOnline のような純粋なローカル属性が指定されていると、HAD の開始時に拒否されます。
2653668	ノードがパニック状態に戻ると、HAD コアが SIGABRT でダンプされます
2644483	VCS ERROR V-16-25-50036 親サービスグループがオフラインになる前に子サービスグループがオンライン（回復）になります。メッセージはエラーメッセージとしてログに記録されます
2635211	AMF は spinlock を保持した状態で VxFS API を呼び出します。クラスタノードは異なるサービスグループのオンライン操作、オフライン操作、スイッチング操作の間にランダムにパニック状態になることがあります。
2616497	親が 1 つ以上のノードで障害発生状態にある場合、障害の伝播は起きません。

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。

LVMLogicalVolume リソースを含む VCS サービスグループのフェールオーバーでのクライアント上の無効な NFS ファイルハンドル（2016627）

LVMボリュームグループのVCSサービスグループはフェールオーバー後に自動的にオンラインになります。しかし、無効な NFS ファイルハンドルのエラーにより、クライアントアプリケーションで障害や割り込みが発生することがあります。

回避策: サービスグループフェールオーバーでのクライアント上の無効な NFS ファイルハンドルを回避するには、Share リソースの Options 属性に「fsid=」を指定します。

ストレージが無効なときに NFS クラスタ I/O が失敗する [2555662]

NFS クラスタからの I/O は共有ディスクまたは共有ストレージに保存されます。NFS クラスタに接続された共有ディスクまたは共有ストレージが無効なとき、NFS クライアントからの I/O は失敗し、I/O エラーが起きます。

回避策: アプリケーションが終了（失敗/停止）した場合は、アプリケーションを再起動します。

VCS のインストールとアップグレードに関する問題

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
```

手動のアップグレードでソフトリンクが削除される問題

VRTSvlic RPM の手動のアップグレード(5.1 から 6.0)を実行中に、以前のインストール時に作成された一部のソフトリンクが削除されます。その結果、指定したパスに vxkeyless バイナリが見つかりません。

これを避けるには、--nopreun オプションを使用します。

例: `rpm -Uvh --nopreun VRTSvlic-3.02.61.003-0.x86_64.rpm`

VRTSvlic RPMの手動アップグレードでキーレス製品レベルが失われる [2737124]

VRTSvlic RPM を手動でアップグレードすると、vxkeyless を使って設定した製品レベルが失われることがあります。vxkeyless display コマンドの出力は正しく表示されません。これを防ぐには、VRTSvlic RPM の手動アップグレード中に次の手順を実行します。

1. キーレスライセンス付与の対象としてノードで設定されている製品のリストを書き留めます。

   ```
   # vxkeyless display
   ```

2. 製品レベルを NONE に設定します。

   ```
   # vxkeyless set NONE
   ```

3. VRTSvlic RPMをアップグレードします。

   ```
   # rpm -Uvh --nopreun VRTSvlic-3.02.61.003-0.x86_64.rpm
   ```

4. 手順 1 で書き留めた製品のリストを復元します。

   ```
   # vxkeyless set product[|,product]
   ```

VCS スタックを VCS 5.1 より前のバージョンからアップグレードしているときは、MultiNICA IPv4RouteOptions 属性の再設定が必要（2003864）

5.1SP1 の MultiNICA エージェントは現在、デフォルトで `ip` コマンドを使います。経路の設定に関する `ip` コマンドと `ifconfig` コマンドの動作の違いために、MultiNICA は、新しいアクティブなデバイスのために経路をフラッシュして戻します。MultiNICA リソースの設定で `ifconfig` コマンドを使う予定がない場合は（下の表を参照）、MultiNICA リソースの定義で IPv4RouteOptions 属性を設定する必要があります。

メモ: RouteOptions 値が `route` コマンドで使われるのに対して、IPv4RouteOptions 値は `ip route` コマンドで使われます。これらの 2 つの属性に設定される値は、対応するコマンドによって大幅に異なります。

表 1-19 属性を設定するかどうかと、アップグレード中に実行する必要のある処理

オプション	RouteOptions または IPv4AddrOptions、あるいはその両方	IPv4RouteOptions	コメント	アップグレード中に実行する必要のある処理
設定済み	設定が必要な場合と必要でない場合がある	設定が必要な場合と必要でない場合がある	この場合は、`ifconfig` コマンドが使われます。RouteOptions が設定されている場合、この属性値は `route` コマンドを使って経路を追加または削除するために使われます。 Options 属性が設定されているため、IPv4RouteOptions 値は無視されます。	IPv4RouteOptions を設定する必要はない。

オプション	RouteOptions または IPv4AddrOptions、あるいはその両方	IPv4RouteOptions	コメント	アップグレード中に実行する必要のある処理
未設定	設定が必要な場合と必要でない場合がある	設定する必要がある	この場合は、ipコマンドが使われます。ip route コマンドを使って経路を追加または削除するには、IPv4RouteOptions を設定して使う必要があります。Options 属性が設定されていないため、RouteOptions 値は無視されます。	IPv4RouteOptions を設定し、デフォルトゲートウェイの IP を設定します。この属性の値は通常、次のようになります。 IPv4RouteOptions = “default via *gateway_ip*” 例: IPv4RouteOptions = “default via 192.168.1.1”

VRTSvlic のアップグレード後にキーレスライセンスが残る問題 [2141446]

5.1 からより新しいバージョンの VCS へのアップグレード後に、キーレスライセンスがシステムに残っていることがあります。その結果、VOM サーバーが設定されていない場合に、定期的な事前通知がログに記録される可能性があります。

これは、VCS の 5.1SP1 以降のバージョンへアップグレードする前にキーレスライセンスを使用している場合に起こります。アップグレード後に実際のキーをインストールし、`vxkeyless set NONE` を実行します。この場合、キーレスライセンスが完全に削除されず、2 カ月後に警告メッセージがログに記録される可能性があります (VOM サーバーが設定されていない場合)。製品の機能への影響はありません。

この問題を解決するには、次の手順を実行します。

1. キーレスライセンス付与の対象としてノードで設定されている製品のリストを書き留めます。リストを表示するには、`vxkeyless display` を実行します。
2. 次のコマンドを使って製品レベルを *NONE* に設定します。

   ```
   # vxkeyless set NONE
   ```

3. システムに残っているキーレスライセンスを見つけて削除します。このためには、`/etc/vx/licenses/lic` に格納されている各キーについて、次の手順を実行します。

   ■ 次のコマンドを使って、キーの VXKEYLESS 機能が有効かどうかを確認します。

```
# vxlicrep -k <license_key> | grep VXKEYLESS
```

- VXKEYLESS 機能が有効になっている場合にのみキーを削除します。

メモ: 検索を実行するとき、拡張子 .vxlic を検索文字列に含めないでください。

4. 次のコマンドを使って、以前の製品リストを復元します。

```
# vxkeyless set product1[|,product]
```

VRTSvcsag RPM のインストール時の SELinux のエラー

RHEL 5 SELinux が有効なマシンへの VRTSvcsag RPM のインストール時に、次の SELinux のエラーが表示されることがあります。

```
/usr/sbin/semodule: Failed on /opt/VRTSvcs/bin/selinux/vcsag.pp!
```

このエラーは、SELinux パッケージの不適切なインストールのために発生します。その結果、SELinux コマンドが正しく機能しないことがあります。

回避策: SELinux パッケージを再インストールし、init または fixfiles メソッドのいずれかでファイルシステムのラベルを付け直してください。

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。

アンインストーラがスクリプトをすべては削除しない（2696033）

VCS の削除後、RC の一部のスクリプトが /etc/rc*.d/ フォルダに残ります。これは RHEL6 とアップデートの chkconfig rpm の問題が原因です。/etc/rc*.d/ フォルダから VxVM パッケージを削除した後で、スクリプトを手動で削除できます。

回避策:

chkconfig-1.3.49.3-1 chkconfig rpm を RedHat のポータルからインストールしてください。次のリンクを参照してください。

http://grokbase.com/t/centos/centos/117pfhe4zz/centos-6-0-chkconfig-strange-behavior

http://rhn.redhat.com/errata/RHBA-2012-0415.html

Web インストーラにクラスタからノードを削除するオプションがない

Web インストーラで、クラスタからノードを削除するためのオプションが提供されません。

回避策: クラスタから手動でノードを削除してください。Web インストーラまたは CPI から使用できる、ノードを削除するためのオプションはありません。

ブラウザがまだ開いている場合、最初のセッション後に、同じ URL に対する認証が Web インストーラで求められない [2509330]

VCS のインストールまたは設定のいずれかの後、Web インストーラのウィンドウを閉じ、同じブラウザに別のウィンドウが開いている場合、後続のセッションでの認証を要求するメッセージが Web インストーラで表示されません。Web インストーラから段階的にログアウトするためのオプションがないので、ブラウザが Web インストーラに使われている限り、インストーラのセッションはシステムで開いたままになります。

ただし、これは URL 固有の問題であり、後続の操作を実行するために同じ URL を使うときにのみ発生します。そのため、この目的で別の URL を使えば、ブラウザは Web インストーラにアクセスするたびに、毎回認証のためのメッセージを表示します。

回避策: Web インストーラへのアクセスのために、別の URL を使うことができます。

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）

VCS 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。

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。

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。

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。

VCS 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）

VCS 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。

VCS の操作上の問題

SLES10 上のミラーボリュームに対して、LVMLogicalVolume の online エントリポイントが応答を停止し、タイムアウトする [2077294]

LVMLogicalVolume は、lvchange コマンドを使って論理ボリュームをアクティブにします。ミラーボリュームの場合、lvchange コマンドがスクリプトを介して呼び出されると、そのコマンド自体が応答を停止します。これにより、online エントリポイントがタイムアウトし、LVMLogicalVolume リソースの online エントリポイントが応答を停止します。これは SLES10 に関する問題です。

LVM SG の移行が、状態が無効になっているすべてのパスで失敗する [2081430]

ディスクへのすべてのパスを無効にした場合、LVM2 vg コマンドは応答を停止し、ディスクへの少なくとも 1 つのパスが復元されるまで待機します。LVMVolumeGroup エージェントは LVM2 コマンドを使っているため、この動作により LVMVolumeGroup エージェントの online エントリポイントと offline エントリポイントがタイムアウトし、clean EP が無期限にわたって応答を停止します。このため、サービスグループは別のノードにフェールオーバーできません。

回避策: 少なくとも 1 つのパスを復元する必要があります。

ネーティブ LVMVG を VCS の制御外でインポートしてアクティブにすると、SG が PARTIAL 状態になります。

VCS を起動する前に LVM ボリュームグループをインポートしてアクティブにすると、LVMLogicalVolume リソースはオンラインになりますが、LVMVolumeGroup がオフラインのままになります。これにより、サービスグループが PARTIAL 状態に置かれます。

回避策: VCS を起動する前に VCS LVMVolumeGroup リソースを手動でオフラインにするか、またはこのリソースを非アクティブにしてボリュームグループをエクスポートする必要があります。

TCP トラフィックを遮断するようファイアウォールが設定されたシステムでは、一部の VCS コンポーネントが動作しない

ファイアウォールがインストールされたシステムで VCS をインストールおよび設定した場合、次の問題が起きることがあります。

- GCO（グローバルクラスタオプション）を使ってディザスタリカバリを設定した場合、リモートクラスタ（セタンダリサイトのクラスタ）の状態は「initing」と表示されます。

- CP サーバーを使うようにフェンシングを設定した場合、フェンシングクライアントは CP サーバーへの登録に失敗します。
- サーバー間の信頼関係の設定は失敗します。

回避策:

- 必要なポートとサービスがファイアウォールによって遮断されないことを確認してください。VCS によって使われるポートとサービスの一覧については、『Veritas Cluster Server インストールガイド』を参照してください。
- VCS によって必要な TCP ポートが遮断されないようにファイアウォールポリシーを設定してください。必要な設定については、それぞれのファイアウォールまたは OS のベンダー文書を参照してください。

DiskGroup リソースを使ったサービスグループの切り替えが、UseFence の SCSI3 への設定と powerpath 環境の設定との予約競合の原因になる [2749136]

UseFence が SCSI3 に設定され、powerpath 環境が設定されると、DiskGroup リソースを使ったサービスグループの切り替えにより syslog に次のメッセージが表示される場合があります。

```
reservation conflict
```

これは VCS の問題ではありません。UseFence が SCSI3 に設定されると、ディスクグループは予約通りにインポートされます。このメッセージはディスクの解放中および予約中に記録されます。

回避策: 次の URL で入手可能な TechNote を参照してください。
http://www.symantec.com/business/support/index?page=content&id=TECH171786.

VCS エンジンに関する問題

CPU 使用率が非常に高いと、HAD による GAB へのハートビートの送信が失敗する場合がある [1744854]

CPU 使用率が 100% に非常に近いと、HAD による GAB へのハートビートの送信が失敗する場合があります。

hacf -cmdtocf コマンドで破損した main.cf ファイルが生成される [1919951]

`-dest` オプションを指定して `hacf -cmdtocf` コマンドを実行すると、types ファイルから include 文が削除されます。

回避策: hacf -cmdtocf コマンドを使って生成された main.cf ファイルに、include 文を追加します。

TriggerPath の先頭または末尾に複数のスラッシュがあると、トリガが実行されない [2368061]

TriggerPath 属性で指定するパスの先頭または末尾に、複数の「¥」文字を含めることはできません。

回避策: パスの先頭または末尾から、余分な「¥」文字を削除してください。

EngineRestarted に誤った値があるノードで、サービスグループが自動起動しない [2653688]

HAD が hashadow プロセスで再起動されるときに、すべてのサービスグループがプローブされるまでの間、EngineRestarted 属性の値が一時的に 1 に設定されます。すべてのサービスグループがプローブされると、値はリセットされます。別のノードの HAD がほぼ同時に開始された場合、EngineRestarted 属性の値がリセットされない可能性があります。そのため、サービスグループは、EngineRestarted 属性の値の不一致により、新しいノードで自動起動されません。

回避策: EngineRestarted が 1 に設定されたノードで VCS を再起動してください。

最上位のリソースが無効になると、グループがオンラインにならない [2486476]

親との依存関係がない最上位のリソースが無効になり、その後で他のリソースがオンラインにならない場合、次のメッセージが表示されます。

```
VCS NOTICE V-16-1-50036 There are no enabled
 resources in the group cvm to online
```

回避策: 無効になった最上位のリソースの子リソースをオンラインにしてください。

NFS リソースが再起動されたときに、予想外にオフラインになりエラーが報告される [2490331]

エージェントプロセスが HAD によって複数回再起動され、エージェントプロセスのうちの 1 つのみが有効で、残りのプロセスは外部で終了または停止されずに中止された場合、VCS はリソース操作を実行しません。エージェントプロセスが実行中の場合でも HAD はそれを認識せず、そのためどのようなリソース操作も実行しません。

回避策: エージェントプロセスを終了してください。

子グループがオンラインのノードで、親グループがオンラインにならない [2489053]

これは、親グループの AutostartList に、子グループがオンラインであるノードエントリが含まれていない場合に起こります。

回避策: システム名を指定することで親グループをオンラインにし、その後で `hargp -online [parent group] -any` コマンドを使って親グループをオンラインにしてください。

VCS が LEAVING 状態にあるときに、temp 属性を修正できない [2407850]

ローカルノードが LEAVING 状態にある場合、temp 属性を修正するための `ha` コマンドが拒否されます。

回避策: 別のノードからコマンドを実行するか、設定の読み取り書き込みを有効にしてください。

セキュリティ保護された WAC とセキュリティ保護されていない WAC が接続されている場合、engine_A.log は 5 秒間隔でログを受信する [2653695]

GCO 内の 2 つ WAC は、常にセキュアモードまたは非セキュアモードのどちらかで開始される必要があります。セキュリティ保護された WAC 接続とセキュリティ保護されていない WAC 接続があると、ログメッセージが engine_A.log ファイルに送信されます。

回避策: WAC が GCO 内の両方のクラスタでセキュアモードまたは非セキュアモードのどちらかで実行中であることを確認してください。

Oracle グループはセカンダリクラスタでファイアドリルグループがオンラインになっている場合にはオンラインにならない [2653695]

ローカルクラスタで並列グローバルサービスグループの障害が発生し、ローカルクラスタ内にフェールオーバーターゲットが見つからなかった場合、リモートクラスタへのサービスグループのフェールオーバーが試みられます。しかし、リモートクラスタでサービスグループのファイアドリルがオンラインになっている場合には、オフラインローカルの依存関係に対する違反となるので、グローバルサービスグループはリモートクラスタにフェールオーバーすることができません。

回避策: リモートクラスタのファイアドリルサービスグループをオフラインにして、サービスグループをオンラインにしてください。

フラッシュ操作と強制的なフラッシュ操作後に、サービスグループがオンラインにならないことがある [2616779]

オフライン操作が正常に行われなかったサービスグループでフラッシュ操作と強制的なフラッシュ操作が実行された後に、サービスグループがオンラインになることに失敗する場合があります。

回避策: オフライン操作が正常に行われなかった場合、通常のフラッシュ操作の代わりに、force flush コマンドを使ってください。通常のフラッシュ操作がすでに実行されている場合、-any オプションを使ってサービスグループを開始します。

TargetCount が高いと hagrp -online -sys コマンドでサービスグループがオンラインにならない [2871892]

サービスグループのオフラインを開始してからオフラインを終了する前に強制的なフラッシュを開始すると、先に開始されたサービスグループのオフラインは障害と見なされます。リソースのスタートビットがすでにクリアされていると、サービスグループは OFFLINE|FAULTED 状態に移動しますが、TargetCount は高いまま残ります。

回避策: 回避策はありません。

プライマリおよびセカンダリクラスタのエラーが 2 回連続して発生すると、自動フェールオーバーが発生しない [2858187]

GCO に Steward が設定されていない 3 つのクラスタ（clus1、clus2、clus3）がある場合、clus1 が clus2 への接続を失うと、clus2 の状態を確認するために clus3 に照会が送信されます。次のいずれかの条件がパーシストされます

1. clus2 がダウンしていることが確認されると、clus2 は FAULTED としてマーク付けされます。
2. clus3 に照会を送信できない場合は、ネットワークの切断が発生したと判断され、clus2 はUNKNOWN としてマーク付けされます。

2 番目の場合、ClusterFailoverPolicy が Auto に設定されても自動フェールオーバーは発生しません。グローバルサービスグループを手動でフェールオーバーする必要があります。

回避策: 上で説明された条件が適用されるクラスタから地理的に独立している場所で Steward を設定してください。

GCO クラスタが INIT の状態のままになる [2848006]

GCO クラスタは、GCO を設定した後、次の理由により INIT の状態のままになります

- クラスタがセキュアな場合、2 つのクラスタ間の信頼関係が正しく設定されていない。
- WACポート（14155）を有効にするようにファイアウォールが正しく設定されていない。

回避策: 上の 2 つの条件が解決されていることを確認してください。2 つのクラスタ間の信頼関係の設定について詳しくは、『Veritas Cluster Server 管理者ガイド』を参照してください。

クラスタがセキュアな場合、ha コマンドが root 以外のユーザーに対して失敗することがある [2847998]

最初にホームディレクトリなしで root 以外のユーザーを使い、次に同じユーザーにホームディレクトリを作成した場合、ha コマンドは動作しません。

回避策

1. /var/VRTSat/profile/<user_name> を削除します。
2. /home/user_name/.VRTSat を削除します。
3. 同じ root 以外のユーザーが所有する /var/VRTSat_lhc/<cred_file> ファイルを削除します。
4. 同じ root 以外のユーザーで ha コマンドを実行します(これは通ります)。

ClusterAddress の変更中に古い ClusterAddress がノードに設定されたままになる [2858188]

ClusterService グループがオンラインのときに gcoconfig を実行して ClusterAddress を変更する場合は、古い ClusterAddress がノードに設定されたままになります。

回避策: 手動でノードから古い ClusterAddress の設定を解除するか、gcoconfig を実行する前に次のコマンドを実行して ClusterService グループをオフラインにします。

```
hagrp -offline -force ClusterService -any
```

または

```
hagrp -offline -force ClusterService -sys <sys_name>
```

付属エージェントに関する問題

I/O パスの障害発生時に LVM 論理ボリュームが自動アクティブ化される [2140342]

I/O パスの障害発生時に LVM 論理ボリュームが自動アクティブ化されます。これにより、VCS エージェントは「同時性違反」エラーを報告し、リソースグループを一時的にオフラインまたはオンラインにします。これはネーティブ LVM の動作に原因があります。

回避策: この問題を回避するには、LVM タグ付けオプションを有効にします。

KVMGuest の monitor エントリポイントは、破損したゲスト、または OS にインストールされた内部ゲストがない場合でもリソースを ONLINE と報告する [2394235]

VCS KVMGuest の monitor エントリポイントは、ゲスト内部のオペレーティングシステムが破損しているか、ゲストにオペレーティングシステムがインストールされていない場合でも、リソースの状態を ONLINE として報告します。VCS KVMGuest エージェントは、ゲストの状態を判断するために `virsh` ユーティリティを使います。ゲストが開始されるとき、`virsh` ユーティリティは実行中のゲストの状態を実行中として報告します。この実行状態に基づいて、VCS KVMGuest エージェントの monitor エントリポイントは、ONLINE としてリソースの状態を報告します。

オペレーティングシステムがゲスト中にインストールされていないか、インストールされているオペレーティングシステムが壊れた場合でも、`virsh` ユーティリティはまだゲストを実行中として報告します。そのため、VCS もリソースの状態を ONLINE として報告します。Red Hat KVM がゲスト中のオペレーティングシステムの状態を提供しないので、VCS はオペレーティングシステムの状態に基づいてゲストの状態を検出できません。

回避策: この既知の問題の回避策はありません。

監視されている仮想マシンの移行中に発生する同時性違反 [2755936]

VCS サービスグループが仮想マシンを監視する KVMGuest リソースを 2 つ以上持ち、仮想マシンの 1 つが別のホストに移行した場合は、複数のノードでサービスグループレベルの同時性違反が発生し、サービスグループの状態が PARTIAL になります。

回避策: サービスグループの 1 つの KVMGuest リソースだけを設定してください。

SLES11 上で reiserfs ファイルシステムを使用した場合、LVM の論理ボリュームが動かないことがある [2120133]

LVM の論理ボリュームは、論理ボリュームを含んでいるサービスグループがクラスタノードの間で連続的に切り替えられた場合、SLES11 上で reiserfs ファイルシステムを使用すると動作しなくなることがあります。

この問題は次の場合に発生します。

- reiserfs ファイルシステムを使用している LVM 論理ボリュームを使用したサービスグループの連続的な切り替え時。
- SLES11 上で reiserfs ファイルシステムを使用した場合のみ。
- SLES11 上のデバイスマッパーの動作が原因。

ただし、問題は一貫していません。デバイスマッパーは、論理ボリュームを処理している間に停止し、論理ボリュームのハングアップを引き起こします。このような場合、LVM2 コ

マンドは論理ボリュームの消去にも失敗します。LVM2 コマンドがハングアップした論理ボリュームをアクティブ解除できないため、VCS はこの状況に対処できません。

解決策: この状況で論理ボリュームが動かなくなったシステムを再起動する必要があります。

KVMGuest リソースが手動で開始されたときに、フェールオーバーターゲットノードでオンラインになる [2394048]

VCS KVMGuest リソースは、VM ゲストが手動で開始されたときに、そのリソースがプライマリノードでオンラインであっても、フェールオーバーターゲットノードでオンラインになります。

Red Hat KVM（カーネルベースの仮想マシン）では、同じゲストイメージを使って複数のノードでゲストを開始できます。ゲストイメージはクラスタファイルシステムに存在しています。ゲストイメージがクラスタファイルシステムに格納されている場合、すべてのクラスタノードで同時に利用可能になります。

ゲストイメージを使ってクラスタファイルシステムでゲストを開始することで、VCS の KVMGuest リソースが特定のノードでゲストをオンラインにしたときに、同じゲストを他のノードで手動で開始しても、Red Hat KVM ではこの実行が防止されません。ただし、この特定のゲストが VCS 制御下にあるため、リソースがパラレルサービスグループ設定にない限り、リソースが複数のノードで同時に ONLINE になることを VCS が許可しません。VCS は、この同時性違反を検出し、2 番目のノードのゲストを停止します。

メモ: この問題は、CVM RAW ボリュームでも発生します。

回避策: VCS では回避策は必要ありません。VCS の同時性違反の機構によって、このシナリオは適切に処理されます。

Application エージェントは、envfile が設定されシェルが csh の状態で、ユーザーを root として処理できない [2490296]

Application エージェントは、envfile が設定されシェルが csh の状態のとき、ユーザーを root として処理できません。Application エージェントは、root ユーザーに対して `Start`/`Stop`/`Monitor`/`Clean` の各プログラムを実行するために、`system` コマンドを使います。これにより、`Start`/`Stop`/`Monitor`/`Clean` の各プログラムは `sh` シェルで実行されるため、root ユーザーに csh シェルがあり、EnvFile がそれに応じて記述されているときに、エラーが発生します。

回避策: root ユーザーのシェルとして `csh` を設定しないでください。代わりに、root のシェルとして `sh` を使います。

単一のサービスグループに多数のリソースを設定した場合、DiskReservation エージェントが clean を呼び出すことがある [2336391]

単一のサービスグループに多数の DiskReservation リソース（400 個を超えるリソース）を設定し、サービスグループをオフラインにしようとすると、DiskReservation エージェントが clean を呼び出すことがあります。

単一のサービスグループ設定に 400 個を超える DiskReservation リソースがあり、同数の Mount リソースがあると、このサービスグループをオフラインにすることで、DiskReservation エージェントで clean エントリポイントの呼び出しが発生することがあります。この問題は、150 個程度のリソースを設定した場合には発生しません。

回避策: 回避策はありません。

設定された MountPoint パスにスペースが含まれている場合、Mount リソースに対する IMF 登録に失敗する [2442598]

Mount リソースの設定された MountPoint パスにスペースが含まれている場合、Mount エージェントはリソースを正しくオンラインにできますが、ONLINE 監視のための IMF 登録に失敗します。これは、AMF ドライバが、パス内のスペースをサポートしていないために発生します。先頭と末尾のスペースはエージェントによって処理され、IMF 監視はこうしたリソースに対して実行できます。

回避策: シマンテック社では、パス内にスペースがあるリソースに対する IMF 監視をオフにすることをお勧めします。リソースに対する IMF 監視の無効化に関する情報は、『Veritas Cluster Server 管理者ガイド』を参照してください。

ボリュームが VCS の外部でマウント解除された場合、DiskGroup エージェントはリソースをオフラインにできない

`umount -l` コマンドを使ってボリュームが VCS の外部でマウント解除された場合、DiskGroup エージェントはリソースをオフラインにできません。

サービスグループには DiskGroup、Volume、Mount の各リソースが含まれ、このサービスグループはオンラインです。ボリュームは、VxFSMountLock が有効化された Mount リソースによってマウントされています。`umount -l` システムコマンドを使ってボリュームを手動でマウント解除しようとすると、マウントポイントがなくなりますが、ファイルシステムのロックがそのまま残ります。ボリュームはマウントがロックされているために停止できず、したがってディスクグループをインポートできません。これが原因で、ディスクグループリソースが UNABLE から OFFLINE 状態になります。また、再度ファイルシステムのマウントを試行すると、マウントはすでにロックされているために失敗します。この問題は、Linux のファイルシステムの動作が原因で起こります。

回避策: マウントロックが有効化されているときは、VxFS ファイルシステムをマウント解除するために `umount -l` コマンドを使わないでください。代わりに、まず

/opt/VRTS/bin/fsadmコマンドを使ってマウントポイントをロック解除し、次にファイルシステムをマウント解除してください。

ネットワークケーブルが抜かれた場合、RemoteGroup エージェントがフェールオーバーしない [2588807]

ネットワークケーブルが抜かれた場合、ControlMode が OnOff に設定されたの RemoteGroup リソースは、クラスタの別のノードにフェールオーバーしないことがあります。RemoteGroup リソースがリモートクラスタに接続できない場合、このリソースの状態は UNKNOWN になります。

回避策:

- リモートクラスタに接続し、RemoteGroupリソースをオフラインにすることを試してください。
- リモートクラスタに接続できず、ローカルサービスグループを停止したい場合、RemoteGroup リソースの ControlMode オプションを MonitorOnly に変更します。その後、RemoteGroup リソースをオフラインにすることを試します。リソースがオフラインになった後は、リソースの ControlMode オプションを OnOff に変更します。

CVM 環境の FireDrill の VVR セットアップが CFSMount エラーで失敗することがある [2564411]

Java コンソールまたは hagrp -online コマンドによって FireDrill サービスグループをオンラインにしようとすると、CFSMount リソースが FAULTED 状態になることがあります。

回避策: fsck コマンドを実行してください。エンジンログからこれらのコマンドを見つけることができます。

CoordPoint エージェントがエラー状態のままになる [2852872]

CoordPoint エージェントが、rfsmが再生中の状態になることを検出するために、エラー状態のままになります。

回避策: HAD の停止後、フェンシングを再設定してください。

RVGsnapshot エージェントが、vxvset を使って作成されたボリュームセットと連携して動作しない [2553505]

RVGsnapshot エージェントが、vxvsetを使って作成されたボリュームセットと連携して動作しません。これは、VVR 環境の FireDrill の間に発生します。

回避策: 回避策はありません。

VCS が Monitor プログラムを検出しない場合、engine_A.log にメッセージが記録されない [2563080]

サービスグループがオンラインで KVM ゲストの Monitor プログラムを VCS が検出できない場合、engine_A.log にメッセージは記録されません。

回避策: リソース状態が不明な場合も、エージェントログログファイルのメッセージを参照してください。

NFS に対する IPv6 サポートがない [2022174]

IPv6 は NFS に対してサポートされません。

回避策: 回避策はありません。

VCS 6.0 への完全アップグレード後、アップグレード前にエージェントがオンラインだった場合、エージェントはオンラインになることに失敗する [2618482]

NFSRestart、DNS、LogicalVolumeGroup の各タイプのリソースは、VCS 6.0 への完全アップグレード前にオンラインだった場合、アップグレード後自動的にはオンラインになりません。

回避策: アップグレード前にオンラインだったリソースは、アップグレード後に手動でオンラインにしてください。

RHEV-Mドメインが「内部」である場合、KVMGuestエージェントが通信しない（2738491）

KVMGuest エージェントは REST API を使って Red Hat Enterprise Virtualization Managerと通信します。RHEV-Mの設定時に設定されるデフォルトドメインは、ローカルドメインの internal です。REST API は内部ドメインを使って RHEV-M と通信しません。

回避策: `rhevm -manage -domains` コマンドを使って有効なドメインを追加してください。Red Hat は、このコマンドを使って REST API 通信に有効なドメインを追加するための手順を提供します。詳しくは、Red Hat Enterprise Virtualization のマニュアルを参照してください。

共有ストレージの設定ファイルへのアクセスが失われると SambaShare エージェントの clean エントリポイントが破損する [2858183]

Samba サーバーの設定ファイルが共有ストレージにあり、共有ストレージへのアクセスが失われると、SambaShare エージェントの clean エントリポイントが破損します。

回避策: 回避策はありません。

ケーブルが引き抜かれた、または IP が設定解除された場合に SambaShare エージェントがリソースのオフライン化に失敗する [2848020]

IP が設定解除されるか、またはケーブルが引き抜かれるシナリオの場合、エージェントは SambasShare リソースのオフライン化に失敗します。

回避策: 回避策はありません。

KVMGuest が「non-responding」状態にある仮想マシンのためにリソースの状態を OFFLINE に戻す [2848003]

仮想マシンが「non-responding」状態になると、KVMGuest エージェントはリソースの状態を OFFLINE に戻します。この状況は、ストレージドメインが「inactive」状態にあり、データセンターが「down」状態のときに発生します。

回避策: RHEV-M のストレージドメインをアクティブ化し、データセンターが「up」状態にあることを確認してください。

KVMGuest エージェントが VM の一時停止状態を認識しないことによって KVMGuest リソースに障害が発生する [2796538]

SUSE KVM 環境では、仮想マシンが保存されると、その状態が一時停止に変更され、その後に終了します。一時停止状態が続くのは非常に短い時間のため、タイミングの問題により、KVMGuest エージェントがこの状態を見落とす場合があります。次にリソースの状態が INTENTIONAL OFFLINE の代わりに OFFLINE に戻りますが、これが原因で KVMGuest リソースに障害が発生し、フェールオーバーされます。

これは SUSE KVM の制限事項のためで、このようなイベントに対して別々の状態を提供しません。

回避策: 回避策はありません。

ホストが保守モードになると発生する同時性違反 [2735283]

仮想マシンを実行している Red Hat Enterprise Virtualization ホストが保守状態になると、RHEV によって仮想マシンの移行が開始されます。VCS は、「migrating」などの仮想マシンの状態に応じて移行を検出します。移行が進行中であっても、タイミングの問題により RHEV Manager が仮想マシンの状態を「up」であると送信する場合があります。この状態が原因で、リソースが移行先のノードで ONLINE とマーク付けされ、同時性違反が発生する場合があります。

回避策: 回避策はありません。

KVM ゲストですべてのパスが無効のとき、論理ボリュームリソースがストレージの接続消失を検出しない [2871891]

KVM 環境では、すべてのストレージのパスが無効の場合、LVMLogicalVolume および LVMVolumeGroup リソースはストレージの接続消失を検出しません。これは、ストレージのパスが無効であっても、ネーティブ LVM コマンドが成功を返し、これにより VCS がリソースの状態を ONLINE とレポートするため、SG のフェールオーバーが開始されないことが原因です。VCS によって監視されるアプリケーションがこのボリュームに対して読み取り/書き込み I/O を行っている場合は、障害を検出し、サービスグループのフェールオーバーを開始できます。

回避策: 回避策はありません。

再起動後、VM がオンラインで表示された直後にリソースが ONLINE で表示されない [2735917]

VM の再起動中、VM が実行を開始した直後ではリソースは ONLINE になりません。VM の状態が「Reboot in Progress」のとき、INTENTIONAL OFFLINE がレポートされますが、VM の UP 後は、次の監視が 300 秒後にスケジュールされているとリソースはそれを直ちに検出できません。

回避策: OfflineMonitorInterval を減らし、適切な値に設定してください。

VCS データベースエージェントに関する問題

診断監視が VCS agent for Oracle と連携して機能しない [2101432]

Oracle 社が提供する診断用 API の非互換性が原因で、Oracle エージェントでの診断監視が Oracle agent for VCS で機能しません。

回避策: MonitorOption 属性を 0 に設定して、診断監視を無効にします。

VCS agent for Oracle に対して計画的オフラインが機能しない [1805719]

診断監視に関する問題が原因で、意図的なオフラインが VCS agent for Oracle に対して機能しません。

SLES11 プラットフォーム上の Oracle エージェントに対する診断監視なし [1919203]

Oracle エージェントは、SLES11 プラットフォーム上の診断監視をサポートしていません。

ASMInstAgent が ASM ディスクグループの ASM インスタンスに対して pfile/spfile を持つことをサポートしない

ASMInstAgent は、ASM ディスクグループの ASM インスタンスに対して pfile/spfile を持つことをサポートしません。

回避策:

デフォルトの $GRID_HOME/dbs ディレクトリに pfile/spfile のコピーを入れておき、ASM インスタンスの起動中にこれが選択されるようにします。

VCS agent for ASM: 診断監視が ASMInst エージェントでサポートされない

ASMInst エージェントは診断監視をサポートしません。

回避策: MonitorOption 属性を 0 に設定します。

特定の Oracle エラーに指定された NOFAILOVER アクション

Oracle 用 Veritas High Availability エージェントでは、詳細監視時に検出された Oracle エラーの処理が改善されています。このエージェントは、Oracle エラーとそれに対するアクションの一覧で構成された参照ファイル oraerror.dat を使います。

アクションについて、詳しくは『Veritas Cluster Server Agent for Oracle インストールおよび設定ガイド』を参照してください。

現在、この参照ファイルでは、次の Oracle エラーが起きた場合の対応策として NOFAILOVER アクションが指定されています。

```
ORA-00061, ORA-02726, ORA-6108, ORA-06114
```

NOFAILOVER の場合、エージェントはリソースの状態を OFFLINE に設定し、サービスグループをフリーズします。エージェントを停止し、oraerror.dat ファイルを編集して、NOFAILOVER アクションを環境に応じた適切なアクションに変更することもできます。エージェントを再起動すると、変更が有効になります。

エージェントフレームワークに関する問題

過負荷下でエージェントがハートビートに失敗することがある [2073018]

過負荷下でエージェントが VCS エンジンとのハートビートに失敗することがあります。

この問題は、エージェントがタスクを実行するための十分な CPU を獲得できず、エージェントのハートビートが AgentReplyTimeout 属性に設定されている時間を超えた場合に発生することがあります。そのため、VCS エンジンはエージェントを停止し、再起動します。VCS エンジンはエージェントを停止し、再起動すると、ログを生成します。

回避策:システムの負荷が高くなっている可能性があることに気付いた場合、次の回避策を実行できます。

- AgentReplyTimeout 属性の値を大きな値に設定します。
- AgentClass 属性と AgentPriority 属性を使用して、エージェントのスケジュールクラスとスケジュール優先度を高くして、エージェントの CPU 不足を回避します。

エージェントフレームワークが依存属性の前後のスペースを処理できない(2027896)

エージェントフレームワークでは、依存リソースのターゲットリソース属性名にスペースを使用できません。

回避策: 依存リソースのターゲットリソース属性名の先頭と末尾にスペースを入れないでください。

エージェントフレームワークはサービススレッドがエントリポイント内でハングアップした場合に検出しない [1442255]

まれに、エージェントフレームワークはすべてのサービススレッドが C エントリポイント内でハングアップした場合に検出しません。この場合、それらを正常に取り消さないことがあります。

回避策: エージェントのサービススレッドがハングアップした場合、kill 信号を送信して、エージェントを再起動します。コマンド `kill -9 hung agent's pid` を実行します。`haagent -stop` コマンドはこの状況で機能しません。

リソースをオンラインとオフラインにする間の IMF 関連のエラーメッセージ [2553917]

AMF に登録されたリソースに対し、`hagrp -offline` または `hagrp -online` を明示的に、または一括処理で実行してリソースをそれぞれオフラインまたはオンラインにする場合、どちらのときにも IMF でエラーメッセージが表示されます。

表示されるエラーは想定される動作であり、IMF 機能にまったく影響しません。

回避策: 回避策はありません。

グローバルクラスタに関する問題

グローバルクラスタ環境のセキュリティ保護されたサイトで、エンジンログファイルが著しく多くのログメッセージを受け取る[1919933]

1 つのサイトで WAC プロセスがセキュアモードで動作し、別のサイトがセキュアモードを使用していない場合、セキュリティ保護されたサイトのエンジンログファイルは 5 秒ごとにログを取得します。

回避策: グローバルクラスタの 2 つの WAC のプロセスは、セキュアモードか非セキュアモードのいずれかで常に起動される必要があります。セキュリティ保護された WAC 接続と、セキュリティ保護されていない WAC 接続により、エンジンログファイルが上のメッセージでいっぱいになります。

ファイアドリルサービスグループがセカンダリサイトでオフラインになる前にアプリケーショングループがプライマリサイトでオンライン化を試みる（2107386）

ファイアドリルサービスグループがオフライン化を試みる間に、アプリケーションサービスグループがプライマリサイトでオンラインになると、アプリケーショングループで障害が発生します。

回避策: アプリケーションサービスグループがプライマリサイトでオンラインになる前に、ファイアドリルサービスグループがセカンダリサイトで完全にオフラインになるようにします。

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。

LLT は結合された NIC が起動するときに検出しないことがある（2604437）

LLT が結合された NIC で設定されていて、その結合された NIC が `ifconfig` コマンドで停止されたとき、LLT は対応するリンクをダウンとマークします。結合された NIC が `ifconfig` コマンドで再び起動されたとき、LLT はこの変更を検出せず、リンクをアップとマークしません。

回避策: すべてのポートを閉じ、LLT を再起動し、ポートを再び開いてください。

LLT 接続は NIC 上で vlan を設定したときには構成できない（2484856）

LLT リンクを設定するのにすでに使用された NIC 上では、vlan を設定するときに LLT 接続は構成されません。

回避策: 後で vlan を設定する場合は、LLT を設定するときに `lltab` ファイルに NIC の MAC アドレスを指定しないでください。すでに指定済みの NIC の MAC アドレスがある場合は、その MAC アドレスを `lltab` ファイルから削除し、ファイルを更新してから LLT を再起動します。

LLT ポートの統計で recvbytes よりも大きい recvcnt が示されることがある（1907228）

パケットを受信するたびに、LLT は次の変数を増分します

- recvcnt（パケットごとに 1 ずつ増加）
- recvbytes（すべてのパケットのパケットサイズのみ増加）

これらの変数は両方とも整数です。一定のトラフィックでは、recvbytes はすぐに MAX_INT に達してロールオーバーします。これにより recvbytes の値が recvcnt の値よりも小さくなることがあります。

これは LLT の機能に影響しません。

LLT は大きいクラスタ設定のノードに正しくないポートレベル接続を宣言することがある（1810217）

ポートがクラスタのノードで頻繁に登録、登録解除されると、LLT はポートレベルの接続が別のピアノードに存在すると宣言することがあります。これはポートがピアノードに登録されていなくても、一部の極端なケースで発生します。

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 クライアントを初期化解除する間、「gabdebug -R GabTestDriver」のコマンドはログに refcount 値 2 を記録する（2536373）

`-nodeinit` オプションで gtx ポートを登録解除した後、`gabconfig -C` コマンドは refcount として 1 を表示します。しかし GAB クライアントを初期化解除するために強制

的な deinit オプション（gabdebug -R GabTestDriver）を実行すると、次のようなメッセージがログに記録されます。

```
GAB INFO V-15-1-20239
Client GabTestDriver with refcount 2 forcibly deinited on user request
```

refcount 値は内部的に 1ずつ増やされます。しかし、refcount 値は 2 と表示されます。これは、gabconfig -C コマンドの出力と矛盾しています。

回避策: この問題に対する回避策はありません。

再設定時にパニックが発生する（2590413）

クラスタの再設定の際、GAB のブロードキャストプロトコルと、シーケンス要求パスとの間で、競合状態が発生します。この条件は非常に狭いウィンドウ期間で発生するものですが、生じると、GAB のマスターでパニックが発生します。

回避策: この問題に対する回避策はありません。

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。

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、『Veritas Cluster Server 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。

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 RPM 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、VCS 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
```

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、『Veritas Cluster Server 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。

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。

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。

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。

セキュアな CP サーバーは IP アドレスとして 127.0.0.1 を使用するローカルホストとは接続しない（2554981）

cpsadmコマンドは、IP アドレスとして 127.0.0.1 を使用するローカルホストでは、セキュアな CP サーバーに接続しません。

回避策: CP サーバーで設定され、ローカルノードと関連付けられているいずれかの仮想 IP を使用して、セキュアな CP サーバーに接続してください。

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。

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。

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。

クラスタ内の一部のノードに対し、フェンシングが RFSM 状態を繰り返しとして示すことがある（2555191）

キャンパスクラスタ環境で、コーディネーションポイントクライアントに基づくフェンシングが、クラスタ内の一部のノードに対して RFSM 状態を繰り返しとして示すことがあります。

回避策:

RFSM 状態を繰り返しとして示すノードのフェンシングを再起動します。

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。

6.0.1 での Veritas Cluster Server Agents for Veritas Volume Replicator の既知の問題

6.0.1 リリースの Veritas Cluster Server Agents for Veritas Volume Replicator の新しい既知の問題は次のとおりです。

fdsetup は、「-」などの文字を含んだディスク名を正しく解析できない（1949294）

fdsetup は、「-」などの文字を含んだディスク名を正しく解析できません。

RVGLogowner および RVGPrimary エージェントのサンプル main.cf ファイルで無効なエントリが発生する [2872047]

RVGLogowner エージェントおよび RVGPrimary エージェントのサンプル main.cf ファイルで無効なエントリが発生します。

無効なエントリは CFSQlogckd リソースを含む RVGLogowner エージェントの main.cf.seattle ファイルと main.cf.london ファイルにあります。ただし、CFSQlogckd は VCS 5.0 以降はサポートされていません。

RVGPrimary エージェントでは、無効なエントリはファイル main.cf.seattle と main.cf.london にあり、DetailMonitor 属性を含んでいます。

回避策

1 cvm グループの RVGLogowner エージェントの main.cf.seattle の場合:

- 次の行を削除します。

```
CFSQlogckd qlogckd (
             Critical = 0
              )

cvm_clus requires cvm_vxconfigd
        qlogckd requires cvm_clus
        vxfsckd requires qlogckd

        // resource dependency tree
        //
        //      group cvm
        //      {
        //      CFSfsckd vxfsckd
        //          {
        //          CFSQlogckd qlogckd
        //              {
        //              CVMCluster cvm_clus
        //                  {
        //                  CVMVxconfigd cvm_vxconfigd
        //                  }
        //              }
        //          }
        //      }
```

- 上の行を次に置き換えます。

```
cvm_clus requires cvm_vxconfigd
        vxfsckd requires cvm_clus
```

```
// resource dependency tree
//
//      group cvm
//      {
//      CFSfsckd vxfsckd
//          {
//           CVMCluster cvm_clus
//              {
//               CVMVxconfigd cvm_vxconfigd
//              }
//          }
//      }
```

2 cvm グループの RVGLogowner エージェントの main.cf.london の場合:

- 次の行を削除します

```
CFSQlogckd qlogckd (
             Critical = 0
              )

cvm_clus requires cvm_vxconfigd
        qlogckd requires cvm_clus
        vxfsckd requires qlogckd

        // resource dependency tree
        //
        //      group cvm
        //      {
        //      CFSfsckd vxfsckd
        //          {
        //          CFSQlogckd qlogckd
        //              {
        //              CVMCluster cvm_clus
        //                  {
        //                  CVMVxconfigd cvm_vxconfigd
        //                  }
        //              }
        //          }
        //      }
```

- 上の行を次に置き換えます。

```
cvm_clus requires cvm_vxconfigd
        vxfsckd requires cvm_clus

        // resource dependency tree
        //
        //      group cvm
        //      {
        //      CFSfsckd vxfsckd
        //          {
        //           CVMCluster cvm_clus
        //              {
        //               CVMVxconfigd cvm_vxconfigd
        //              }
        //          }
        //      }
```

3 cvm グループの RVGPrimary エージェントの main.cf.seattle の場合:

- グループ ORAGrp で、Oracle リソースデータベースの場合、`DetailMonitor = 1` の行を削除します

4 cvm グループの RVGPrimary エージェントの main.cf.london の場合:

- グループ ORAGrp で、Oracle リソースデータベースの場合、`DetailMonitor = 1` の行を削除します

IMF（Intelligent Monitoring Framework）に関する問題

Firedrill セットアップ作成中の登録エラー [2564350]

`Firedrill setup` ユーティリティを使って Firedrill セットアップを作成している間、VCS で次のエラーが発生します。

```
AMF amfregister ERROR V-292-2-167
Cannot register mount offline event
```

Firedrill 操作中に、VCS はエンジンログに IMF 登録エラーと関連するエラーメッセージを記録することがあります。これは、ファイアドリルサービスグループに、IMF を介して同じ MountPoint を監視する 2 番目の CFSMount リソースがあるために起こります。同じ MountPoint のオンラインまたはオフラインのイベントを両方のリソースが登録しようとするために、結果的に 1 つの登録に失敗します。

回避策: 回避策はありません。

haimfconfig コマンドを使っているときに、Perl エラーが発生する

haimfconfig コマンドを使っているときに、Perl エラーが発生します。

```
Perl errors seen while using haimfconfig command
```

このエラーは、型固有の設定ファイルのために main.cf で指定されている絶対パスが原因です。現在、haimfconfig では main.cf の型固有の設定ファイルのための絶対パスをサポートしていません。

回避策: 実際のパスを実際のファイル名に置き換え、ファイルを絶対パスの場所から /etc/VRTSvcs/conf/config ディレクトリにコピーしてください。

たとえば、OracleTypes.cf が main.cf にインクルードされる場合、次のようになります。

```
include "/etc/VRTSagents/ha/conf/Oracle/OracleTypes.cf"
```

これは main.cf で次のように置換する必要があります。

```
include "OracleTypes.cf"
```

別の名前を使用してディスクグループをインポートすると、IMF は登録されたディスクグループについて通知を行わない（2730774）

ディスクグループリソースが AMF に登録されている場合、そのディスクグループを別の名前でインポートすると、AMF は名前が変更されたディスクグループを認識しないため、DiskGroup エージェントに通知しません。このため、DiskGroup エージェントは引き続き、該当するディスクグループリソースをオフラインとしてレポートします。

回避策: ディスクグループをインポートするときは、ディスクグループの名前が AMF に登録されている名前と一致するようにします。

linkamf のダイレクト実行で構文エラーが表示される [2858163]

ダイレクト実行されると、Bash は Perl を解釈できません。

回避策: 次のように linkamf を実行します。

```
# /opt/VRTSperl/bin/perl /opt/VRTSamf/imf/linkamf <destination-directory>
```

再ブートサイクル中にエラーメッセージが表示される [2847950]

再ブートサイクル中に、エンジンログに次のメッセージが記録される場合があります。

```
AMF libvxamf ERROR V-292-2-149 Cannot unregister event: no rid -1 found
AMF libvxamf ERROR V-292-2-306 Unable to unregister all events (errno:405)
```

これは IMF の機能に影響しません。

回避策: 回避策はありません。

同時性違反回避のために ProPCV が処理の ONLINE 化を防ぐときに表示されるエラーメッセージに I18N サポートがない [2848011]

次のメッセージは同時性違反回避のために ProPCV が処理の ONLINE 化を防ぐときに表示されます。メッセージは英語で表示され、I18N サポートはありません。

```
Concurrency Violation detected by VCS AMF.
Process <process-details> will be prevented from startup.
```

回避策: 回避策はありません。

システムのシャットダウン中に表示されるエラーメッセージ [2804673]

システムのシャットダウン中に、syslog に次のメッセージが表示される場合があります。

```
Stopping AMF...
AMF amfconfig ERROR V-292-2-405 AMF_UNCONFIG failed, return value = -1
```

システムはシャットダウンを続けます。

回避策: 回避策はありません。

getnotification が AMF によってクリーニングされたグループへのアクセスを要求するとシステムにパニックが発生する [2848009]

AMF は、外部または内部アクティビティが原因で障害が発生したエージェントの処理中に、そのエージェントによって監視されるグループをクリーニングします。同時に、エージェントの通知が実行中で、getnotification スレッドがすでに削除されたグループへのアクセスを要求すると、システムにパニックが発生します。

回避策: 回避策はありません。

プロセステーブルスキャン中に libvxamf ライブラリに対するエラー条件が発生する [2848007]

プロセステーブルスキャン中に libvxamf ライブラリに対するエラー条件が発生する場合があります。その結果、AMF によるプロセスのオフライン登録が失敗します。ほとんどの場合、この登録は、このリソースの次の監視サイクルの間にエージェントによって再び試行され、成功します。このリソースに対して従来の監視が続行されるので、致命的な障害にはなりません。

回避策: 回避策はありません。

AMF が、VCS エラーコードまたはログなしで、コンソールに StartProgram の名前を複数回表示する [2872064]

VCS AMF は、処理が開始されるのを防ぐ際に、コンソールと syslog にメッセージを表示します。メッセージには開始が妨げられた処理のシグネチャが含まれています。場合によっては、このシグネチャは PS 出力で表示されるシグネチャと一致しないことがあります。たとえば、実行が妨げられたシェルスクリプトの名前は 2 回印刷されます。

回避策: 回避策はありません。

imfd デーモンを終了すると vxnotify 処理が孤立する [2728787]

`kill -9` コマンドを使って imfd デーモンを終了すると、imfd によって作成された `vxnotify` 処理が自動的に終了せず、孤立します。ただし、`amfconfig -D` コマンドを使って `imfd` デーモンを停止すると、対応する `vxnotify` 処理は終了します。

回避策: 適切なコマンド(この場合 `amfconfig -D` コマンド)を使ってデーモンを段階的に停止するか、Session-ID を使ってデーモンを終了します。Session-ID はデーモンの -PID(ネガティブ PID)です。

次に例を示します。

```
# kill -9 27824
```

デーモンを段階的に停止すると、デーモンによって生成されたすべての子プロセスが停止します。ただし、`kill -9 pid` を使ったデーモンの終了は推奨のオプションではありません。これを使って停止した場合は、デーモンの他の子プロセスを手動で強制終了する必要があります。

amfconfig が set および reset コマンドと同時に動作する場合、コアダンプが発生する [2871890]

ノードで `amfconfig -S -R` を実行するとき、コマンドの正しい使用法が表示される代わりにコマンドコアダンプが発生します。ただし、このコアダンプはそのノードの AMF 機能に影響しません。代わりに正しいコマンド構文を使う必要があります。

回避策: 正しいコマンドを使ってください。

```
# amfconfig -S <options>
# amfconfig -R <options>
```

Cluster Manager(Java コンソール)に関連する問題

このセクションでは、Cluster Manager(Java コンソール)に関連する問題について説明します。

テンプレートを読み込んでいる間 Cluster Manager(Java コンソール)がエラーを表示することがある(1433844)

[ツール(Tools)]>[テンプレート(Templates)]メニューから Cluster Manager のテンプレートビューにアクセスできます。VCS クラスタセットアップで Storage Foundation を設定してある場合、Cluster Manager がテンプレートを読み込むときに次のエラーが起きることがあります。

```
VCS ERROR V-16-10-65 Could not load :-
/etc/VRTSvcs/Templates/DB2udbGroup.tf
```

回避策: このエラーは無視してください。

Cluster Manager の一部の機能がファイアウォールセットアップで動作しない [1392406]

Cluster Manager と VCS クラスタ間でファイアウォール構成を使用した特定の環境では、Cluster Manager が次のエラーメッセージで失敗します。

```
V-16-10-13 Could not create CmdClient. Command Server
may not be running on this system.
```

回避策: すべてのクラスタノードで 14150 番のポート開いてください。

仮想化に関する問題

リソースが ONLINE|STATE UNKNOWN 状態でスタックするとホストが再ブートに失敗する [2738864]

Red Hat Enterprise Virtualization 環境では、仮想マシンを監視する KVMGuest リソースが ONLINE のときにホストの再ブートが実行されると、ホストの再ブートは失敗します。これは、VCS が仮想マシンをシャットダウンする前に VDSM が停止することにより発生します。この場合、仮想マシンの状態は ONLINE|STATE UNKNOWN のままになります。そのため VCS での停止が失敗し、結果的にホストの再ブートも失敗します。

回避策: ホストの再ブートを開始する前にサービスグループを他のノードに切り替えてください。

ストレージのドメインが非アクティブのときに VM が PAUSED 状態になる [2747163]

実行中の仮想マシンによって関連付けられるストレージドメインが非アクティブになると、仮想マシンが paused 状態になることがあります。

回避策: 仮想マシンを実行する場合はストレージドメインが常にアクティブであることを確認してください。

他のホストのスワップ領域が不十分なため KVMGuest リソースの切り替えが失敗する [2753936]

仮想マシンは、ホストに利用可能な十分なスワップ領域がない場合、ホストで開始されません。

回避策: 各ホストに仮想マシンを開始するための利用可能な十分なスワップ領域があることを確認してください。

SLES 11SP2 に導入されたポリシーが SUSE KVM 環境の VM の段階的な終了をブロックすることがある [2792889]

SUSE KVM 環境では、SLES11 SP2 内部で実行される仮想マシンが、SLES 11SP2 に導入された一部のポリシーが原因で仮想マシンの段階的な終了の要求をブロックすることがあります。SUSE では、仮想マシンに対して `polkit-gnome-authorization` でポリシーをオフにすることを推奨します。

回避策: このような要求をブロックするポリシーがすべてオフになっていることを確認してください。

SUSE KVM 環境で `libvirtd` の負荷が終了することがある [2824952]

SUSE KVM環境では、`libvirtd` 処理が終了し、`/etc/init.d/libvirtd status` コマンドが表示されることがあります。

```
#/etc/init.d/libvirtd  status
Checking status of libvirtd                    dead
```

これは、`libvirtd` 処理での高い負荷が原因である場合があります。

回避策: `libvirtd` 処理を再起動してから実行してください。

```
# service libvirtd stop
# service libvirtd start
```

VM の監視対象が未定義の場合、KVMGuest リソースのオフラインまたは切り替えが失敗することがある [2796817]

SUSE KVM 環境では、実行中の仮想マシンが `virsh undefine` コマンドを使って定義されていない場合、その VM を監視する KVMGuest リソースのオフラインまたは切り替えの試行が失敗します。これは、エージェントが KVM ハイパーバイザからの情報を取得できないためです。

回避策: 特定のノードの VM を未定義にするには、最初に KVMGuest リソースを含むサービスグループを別のノードに切り替え、次に最初のノードの VM を未定義にします。

VCS がタイミングの問題により通常の監視サイクルの間に移行イベントを検出することがある [2827227]

仮想化環境では、VCS が VCS の外部で開始された仮想マシンの移行を検出し、それに応じて状態を変更します。ただし、タイミングの問題により VCS が移行イベントを見落とし、通常の監視サイクルの間に移行を検出する場合があります。たとえば、OfflineMonitorInterval を 300 秒に設定した場合、VCS が仮想マシンが移行したノードの ONLINE をレポートするのに最大 5 分かかります。

回避策: 利用できる回避策はありません。

VM が動作していないにもかかわらずメモリ使用量が高い [2734970]

VM が動作していない（停止している）にもかかわらずメモリ使用量が高くなります。これは RHEV の動作が原因です。

回避策: 回避策はありません。

スワップの割合が不十分なためリソースが VM を ONLINE にするのに失敗するとリソースの障害が発生する [2827214]

仮想化環境では、CPU、メモリ、またはディスクなどの必須の仮想化リソースが使用できないために VCS が仮想マシンの開始を失敗すると、リソースは FAULTED 状態になります。

回避策: 必須の仮想化リソースが仮想化環境で常に利用可能であることを確認してください。

ネーティブ LVM ボリュームのゲスト VM の移行により、libvirtd プロセスが突然終了することがある（2582716）

ゲスト VM イメージがネーティブ LVM ボリュームにあるときに、管理者が開始したゲストの移行により、`libvirtd` プロセスが突然終了することがあります。

回避策: `libvird` プロセスを手動で開始してください。

仮想マシンはストレージのドメインが非アクティブであり、データセンターが停止している場合に「応答なし」の状態を返すことがある（2747177）

Red Hat Enterprise 仮想化環境では、ストレージドメインが非アクティブな状態にあり、データセンターが停止状態にある場合、仮想マシンが「応答なし」の状態を返し、KVMGuest リソースがオフライン状態になることがあります。

回避策: この問題を解決するには、次を実行してください。

1 RHEV-M のストレージドメインをアクティブにします。

2 データセンターが稼働状態にあること確認します。

KVM ゲストイメージが CVM-CFS に存在していると、RHEL 6.1 でゲスト仮想マシンが失敗する場合がある [2659944]

KVM ゲストイメージファイルが CVM-CFS に存在していると、そのゲスト仮想マシンの移行は RHEL 6.1 で「Permission Denied」エラーとともに失敗する場合があります。これによりゲスト仮想マシンはソースノードと宛先ノード両方、および関連付けられた VCS KVMGuest で「shut-off」状態になります。

回避策: ゲストイメージファイルに 777 権限があることを確認してください。

KVM 仮想化ゲストを開始するか KVMGuest リソースの online が開始された後システムがパニックになる [2337626]

システムは、KVM ゲストが開始されるか、KVMGuest リソースの online が開始されるとパニックになります。この問題はまれにしか発生しません。

この問題は、libvirtd プロセスのファイル記述子のリークが原因で発生します。libvirtd プロセスのファイル記述子の最大のファイルオープン限度は 1024 です。KVM ゲストが開始されるとき、1024 を超えるファイル記述子がオープンされることがあります。そのため、最大のファイルオープン限度を超えた場合、KVM ゲストを開始するか、新しいファイルをオープンしようとすると、システムがパニックになります。VCS は、libvirtd プロセスのファイル記述子のリークを疑うため、この動作を制御できません。

回避策: この問題の確実な解決策はありません。ただし、libvirtd プロセスによってオープンされているファイルの数を、`/proc/<pid of libvirtd>/fd/` で確認できます。ファイル数が 1000 を超えている場合は、次のコマンドで libvirtd を再起動してください。

```
/etc/init.d/libvirtd restart
```

ソフトウェアの制限事項

このセクションでは、このリリースのソフトウェアの制限事項について説明します。

コンポーネントまたは製品に関連するソフトウェアの制限事項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.76 の「マニュアル」を参照してください。

VCS のインストールとアップグレードに関する制限事項

リモートシステムからインストーラを使う場合は、リモートシステムのオペレーティングシステムとアーキテクチャが、ターゲットシステムと同じである必要がある [589334]

リモートシステムからインストーラを使用する場合は、リモートシステムのオペレーティングシステムとアーキテクチャが、VCSをインストールしようとしているターゲットシステムと同じである必要があります。

付属エージェントに関する制限事項

ホストが切断された場合にネットワークサービスを使用したプログラムが応答を停止することがある

ホストがネットワークから切断された場合、ネットワークサービスを使用したプログラム（たとえば、NIS、NFS、RPC または TCP ソケットのリモートホスト接続）が応答を停止することがあります。この種のプログラムをエージェントのエントリポイントとして使用した場合、ネットワークの切断によってエントリポイントが応答を停止してタイムアウトになる可能性があります。

たとえば、NIS マップをクライアントとして使うように設定されたホストでは、ネットワークから切断されると、`ps -ef` などの基本的なコマンドがハングアップする可能性があります。

ユーザーはローカルに作成することをお勧めします。ローカルユーザーを反映するには、次のように設定します。

/etc/nsswitch.conf

Volume エージェントの clean によりボリュームのリソースが停止する可能性がある

FaultOnMonitorTimeouts 属性が、監視のタイムアウト後、Volume エージェントの clean エントリポイントを呼び出すと、`vxvol -f stop` コマンドが実行されます。このコマンドは、まだマウントされているボリュームも含め、すべてのボリュームを強制的に停止します。

PidFiles を使用してアプリケーションリソースを監視する際に誤った同時性違反が発生する

アプリケーションによって作成される PID ファイルには、Application エージェントによって監視されるプロセスの PID が含まれます。これらのファイルは、アプリケーションを実行しているノードがクラッシュした後も存在する場合があります。ノードの再起動時、PID ファイルにリストされている PID が、ノードで実行されている他のプロセスに割り当てられる場合があります。

そのため、Application エージェントが PidFiles 属性のみを使用してリソースを監視している場合は、実行中のプロセスを検出して、誤って同時性違反と見なされることがあります。その結果、VCS の制御下にない一部のプロセスが停止される場合があります。

Mount エージェントの制限事項

Mount エージェントには次の制限があります

- Mount エージェントはブロックデバイスをシステムの唯一のマウントポイントにマウントします。ブロックデバイスがマウントされた後、エージェントは別のデバイスを同じマウントポイントにマウントできません。
- Mount エージェントは次のものをサポートしません。
  - SLES 11SP1、SLES 11SP2 上の ext4 ファイルシステム
  - VxVM で設定された ext4 ファイルシステム
  - VxVM で設定された xfs ファイルシステム

Share エージェントの制限事項

Share エージェントが正しく監視するには、/var/lib/nfs/etab ファイルがシステムの再ブート時に消去されることを確認します。Share エージェントのクライアントは、一体化したフェールオーバーを確実にするために完全修飾ホスト名を指定する必要があります。

DiskReservation エージェントのドライバの必要条件

VRTSvcsdr パッケージには scsiutil ユーティリティが付属しています。DiskReservation エージェントは scsiutil ユーティリティによってサポートされるドライバのみをサポートします。

VCS の StartVolumes 属性の値に関係なくディスクグループ内のボリュームが自動的に起動する

ディスクグループがインポートされるときに、ディスクグループ内のボリュームは、VCS での StartVolumes 属性の値にかかわらず、自動的に起動します。この動作は、Veritas Volume Manager のシステムレベル属性 `autostartvolumes` の値が On に設定されている場合に発生します。

回避策: ディスクグループのインポート後にディスクグループ内のボリュームを自動的に起動させたくない場合は、システムレベルで AutoStartVolumes 属性を OFF に設定します。

Application エージェントの制限事項

- ProPCV は、MonitorProcesses で設定されるスクリプトベースの処理の実行を防止しません。

IMF に関する制限事項

- Linux で、「bind」ファイルシステムタイプに対する IMF 登録はサポートされません。
- SLES11 SP1 と RHEL6.1 の場合:
  - BlockDevice を複数の MountPoint にマウント可能なリソースに対しては、IMF を有効にしないでください。
  - FSType 属性の値が nfs の場合、「nfs」ファイルシステムタイプに対する IMF 登録はサポートされません。

エージェントディレクトリのベース名はエージェントのタイプ名である必要がある(エージェントは IMF サポート取得にアウトオブザボックスの imf_init IMF エントリポイントを使う)[2858160]

アウトオブザボックスの imf_init IMF エントリポイントを使ってエージェントの IMF サポートを取得するには、エージェントディレクトリのベース名がタイプ名である必要があります。AgentFile が Script51Agent などのアウトオブザボックスエージェントの 1 つに設定される場合、そのエージェントは IMF サポートを取得しません。

回避策:

1 エージェントディレクトリで次のシンボリックリンクを作成してください(たとえば /opt/VRTSagents/ha/bin/WebSphereMQ6 ディレクトリ)。

```
# cd /opt/VRTSagents/ha/bin/<ResourceType>
# ln -s /opt/VRTSvcs/bin/Script51Agent <ResourceType>Agent
```

2 VCS_HOME の値に基き、AgentFile 属性を次のコマンドを実行して更新してください。

- VCS_HOME が /opt/VRTSvcs の場合:

```
# hatype -modify <ResourceType> AgentFile
/opt/VRTSvcs/bin/<ResourceType>/<ResourceType>Agent
```

- VCS_HOME が /opt/VRTSagents/ha の場合:

```
# hatype -modify <ResourceType> AgentFile
/opt/VRTSagents/ha/bin/<ResourceType>/<ResourceType>Agent
```

VCS データベースエージェントに関する制限事項

DB2 RestartLimit の値

依存関係のない複数の DB2 リソースがすべて同時に起動したときには、互いに干渉し合ったり、競合したりする傾向があります。これは、DB2 に関する既知の問題です。

DB2 エージェントの RestartLimit のデフォルト値は 3 です。この値を大きくすると、DB2 リソースの再起動範囲が広がります（リソースのオンライン化が失敗した後）。これにより、DB2 リソースがすべて同時に起動する確率が低くなります。[1231311]

VCS agent for Oracle の計画的オフライン機能の制限事項

計画的オフライン後に、Oracle リソースで障害が発生しません。

VCS agent for Oracle の計画的オフライン機能では、診断監視を有効にする必要があります。エージェントは Oracle の診断 API を使用して、データベースの状態を検出します。API がデータベースの正常終了を戻すと、エージェントはリソースの状態を INTENTIONAL OFFLINE とマーク付けします。後で Oracle エージェントのオンライン機能が成功しない場合、エージェントはリソースを FAULTED とマーク付けしません。エージェントが各監視サイクルの間に API からデータベースの状態を正常終了として受け取るため、状態は INTENTIONAL OFFLINE のままになります。[1805719]

Quorum_dev が設定されていないと Sybase エージェントが qrmutil に基づいたチェックを実行しない（2724848）

Sybase Cluster Edition の Quorum_dev 属性を設定しない場合、Sybase エージェントは qrmutil ベースの検査を実行しません。この設定のエラーは望ましくない結果を引き起こす可能性があります。たとえば、qrmutil がエラーによる停止状態を返した場合、エージェントはシステムをパニック状態にしません。このとき、Quorum_dev 属性が設定されていないため、Sybase のエージェントは qrmutil ベースの検査を実行しません。

したがって、Sybase Cluster Edition では Quorum_Dev attribute の設定は必須です。

Security-Enhanced Linux は SLES 配布でサポートされない

VCS は、SLES10 および SLES11 上では Security-Enhanced Linux（SELinux）をサポートしません。[1056433]

クラスタ内のシステムは同じシステムロケール設定が必要

VCS は、異なるシステムロケールを持つシステムのクラスタ化には対応していません。クラスタ内のすべてのシステムは、同一のロケールに設定する必要があります。

ディスクグループの VxVM サイトがキャンパスクラスタ内のノードをファイアドリルで再ブートした後も切断されたままである

DiskGroupSnap リソースをオンラインにしたときに、DiskGroupSnap エージェントが定義されたターゲットのディスクグループからサイトを切断します。DiskGroupSnap エージェントは VCS action エントリポイントを起動して、VxVM コマンドを実行し、サイトを切断します。ここで使うコマンドは、ディスクグループがインポートされるノード上、すなわちプライマリサイトで実行する必要があります。

ファイアドリルサービスグループまたはディスクグループがオンラインになっているノードをシャットダウンしようとした場合、ノードは LEAVING 状態に変わります。VCS エンジンはノード上のすべてのサービスグループをオフラインにすることを試み、すべての action エントリポイントの要求を拒否します。このため、DiskGroupSnap エージェントはアクションを起動し、ファイアドリルサイトをターゲットのディスクグループに再接続できません。エージェントは、ノードが leaving 状態になっていることを示すメッセージを記録し、ロックファイルを削除します。エージェントの監視機能からは、リソースがオフライン状態にあることが示されます。ノードの再起動後もディスクグループサイトが切断状態になっています。[1272012]

回避策:

ノードをシャットダウンする前、またはローカルに VCS 停止する前に、`hagrp -offline` コマンドを使ってファイアドリルサービスグループをオフラインにする必要があります。

ノードが再起動した場合は、プライマリサイトでインポートされたディスクグループにファイアドリルサイトを手動で再接続する必要があります。

セカンダリノードがクラッシュまたは再起動した場合は、次のコマンドを使って、プライマリサイトでインポートされたターゲットディスクグループにファイアドリルサイトを手動で再接続する必要があります: `/opt/VRTSvcs/bin/hares -action $targetres joindg -actionargs $fdsitename $is_fenced -sys $targetsys`

DiskGroupSnap エージェントに関する制限事項

DiskGroupSnap エージェントには次の制限があります。

- DiskGroupSnap エージェントは階層化ボリュームをサポートしません。[1368385]
- DiskGroupSnap リソースに対して Bronze 設定を使用する場合は、次の場合にセカンダリサイトでデータの一貫性が失われる可能性があります。[1391445]
  - ファイアドリルサービスグループがオンラインになった後で、ファイアドリルを実行中にプライマリサイトで災害が発生した場合。
  - ファイアドリルサービスグループがオフラインになった後で、セカンダリサイトのディスクが同期されているときにプライマリサイトで災害が発生した場合。

  シマンテック社では DiskGroupSnap リソースに対しては Gold 設定を使用することを推奨します。

パニック後にシステムが再ブートする

VCS カーネルモジュールがシステムパニックを発行する場合、システムの再ブートが必要です。[293447]サポート対象 Linux カーネルでは自動的に（CPU）処理を停止しません。Linux の「panic」カーネルパラメータを 0 以外の値に設定し、強制的にシステムを再ブートします。/etc/sysctl.conf ファイルの最後に次の 2 行を追加します。

```
# force a reboot after 60 seconds
  kernel.panic = 60
```

RHEV-M のホストと実際のホストが一致する必要がある [2827219]

RHEV-M のホストは、特定のホストのホスト名コマンドの名前と同じ名前に設定する必要があります。これは必須であり、これによって RHEV Manager がホスト名によってホストを検索できるようになります。

Cluster Manager（Java コンソール）の制限事項

この項では、Cluster Manager（Java コンソール）の制限事項について説明します。

Cluster Manager（Java コンソール）バージョン 5.1 以前のバージョンは、VCS 6.0 セキュアクラスタを管理できない

VCS 5.1 よりも前のバージョンの Cluster Manager（Java コンソール）は、VCS 6.0 セキュアクラスタの管理には使えません。Cluster Manager は最新バージョンのものを使うことをお勧めします。

Cluster Manager のアップグレード方法については、『Veritas Cluster Server インストールガイド』を参照してください。

ホストのファイルに IPv6 エントリがある場合、Cluster Manager が機能しない

/etc/hosts ファイルに IPv6 エントリが含まれている場合、VCS Cluster Manager は、VCS エンジンへの接続に失敗します。

回避策: /etc/hosts ファイルから IPv6 エントリを削除します。

VCS Simulator では I/O フェンシングをサポートしていない

Simulator を実行するとき、UseFence 属性がデフォルトの「None」に設定されていることを確認してください。

KDE デスクトップの使用

Cluster Manager（Java コンソール）の一部のメニューとダイアログボックスは、KDE デスクトップでは、正しいサイズではなく、整列されずに表示されることがあります。KDE デスクトップでコンソールの機能が動作し、正しく表示するには、Sawfish ウィンドウマネージャを使います。Sawfish ウィンドウマネージャを明示的に選択する必要があります。これは KDE デスクトップでデフォルトウィンドウマネージャとして表示が想定される場合でも該当します。

Cluster Manager（Java コンソール）からのサポートの制限

VCS 6.0 で導入された機能が、Java コンソールで予想どおりに動作しないことがあります。ただし、シミュレータの CLI オプションでは、すべての VCS 6.0 機能がサポートされます。すべての新機能はすでに Veritas Operations Manager（VOM）でサポートされているため、VOM を使うことをお勧めします。ただし、Java コンソールでは、VCS 6.0 より前のリリースの機能を予想どおりに使用し続けることができます。

セキュアクラスタに接続するために必要なポートの変更 [2615068]

セキュアクラスタに接続するためには、デフォルトポートは 2821 から 14149 に変更する必要があります。[ログイン]ダイアログボックスの[拡張設定]を選択し、セキュアクラスタログインを IP: 2821 から IP: 14149 に変更します。

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。

VxFEN が RACER ノードの再選をアクティブ化する場合の優先フェンシングの制限事項

優先フェンシング機能は、より小さいサブクラスタを遅延させることで、より重みが大きいかより大きなサブクラスタを優先します。この小さなサブクラスタの遅延は、より大きなサブクラスタの初期 RACER ノードが競争を完了できる場合のみ有効です。何らかの原因で初期 RACER ノードが競争を完了できず、VxFEN ドライバがレーサー再選アルゴリズムをアクティブ化した場合、小さいサブクラスタの遅延はレーサーの再選のために要する時間で相殺され、より重みが小さいかより小さなサブクラスタが競争に勝つ可能性があります。この制限事項は好ましくありませんが、容認できます。

I/O フェンシングが設定されたクラスタでのシステムの停止

I/O フェンシング機能は、クラスタ相互接続の障害、つまり、「スプリットブレイン」によって引き起こされるデータ破損を防ぎます。相互接続障害がもたらす可能性のある問題と I/O フェンシングが提供する保護については、『Veritas Cluster Server 管理者ガイド』を参照してください。

SCSI-3 ベースのフェンシングを使用したクラスタでは、データディスクとコーディネータディスクの両方に SCSI-3 PR キーを配置することにより、I/O フェンシングがデータ保護を実装します。CP サーバーベースのフェンシングを使用したクラスタでは、データディスクに SCSI-3 PR のキーを配置し、CP サーバーに類似の登録を配置することによって、I/O フェンシングがデータ保護を実装します。VCS 管理者は、I/O フェンシングによって保護されるクラスタを利用する場合に必要になるいくつかの操作上の変更点を知っておく必要があります。特定のシャットダウン手順によりコーディネーションポイントとデータディスクからキーを確実に削除し、その後のクラスタの起動における潜在的な問題を防ぐことができます。

shutdown コマンドではなく、reboot コマンドを使うと、シャットダウンスクリプトがバイパスされ、コーディネーションポイントとデータディスクにキーが残る可能性があります。再起動とその後の起動イベントの順序によっては、クラスタがスプリットブレイン状態の可能性について警告し、起動に失敗する場合があります。

回避策: 一度に 1 つのノードで shutdown -r コマンドを使い、各ノードでシャットダウンが完了するのを待ちます。

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 RPM 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 RPM 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。

グローバルクラスタに関する制限事項

- グローバルクラスタに設定するクラスタアドレスは、名前解決が可能な仮想 IP のみを設定できます。
  グローバルクラスタの設定時に、仮想 IP をハートビートに使う場合は、その仮想 IP アドレスは、DNS に登録する必要があります。
- グローバルクラスタ設定で、クラスタの合計数は 4 を超えることができません。
- Symm ハートビートエージェントを設定した場合は、すべてのホストが停止しているときでもクラスタの障害発生は宣言されません。
  Symm エージェントは、2 つの Symmetrix アレイ間のリンクを監視するために使われます。クラスタのすべてのホストが停止しているが、ローカルストレージとリモートストレージの間のレプリケーションリンクを Symm エージェントが確認できる場合、エージェントはハートビートを ALIVE と報告します。このため、DR サイトはプライマリサイトの障害発生を宣言しません。

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 1-20 は Veritas Cluster Server に関するマニュアルのリストです。

表 1-20 Veritas Cluster Server のマニュアル

マニュアル名	ファイル名
Veritas Cluster Server インストールガイド	vcs_install_601_lin.pdf
Veritas Cluster Server リリースノート	vcs_notes_601_lin.pdf
Veritas Cluster Server 管理者ガイド	vcs_admin_601_lin.pdf
Veritas Cluster Server 付属エージェントリファレンスガイド	vcs_bundled_agents_601_lin.pdf
Veritas Cluster Server エージェント開発者ガイド (このマニュアルはオンラインでのみ提供されます)	vcs_agent_dev_601_unix.pdf
Veritas Cluster Server Agent for DB2 インストールおよび設定ガイド	vcs_db2_agent_601_lin.pdf
Veritas Cluster Server Agent for Oracle インストールおよび設定ガイド	vcs_oracle_agent_601_lin.pdf
Veritas Cluster Server Agent for Sybase インストールおよび設定ガイド	vcs_sybase_agent_601_lin.pdf

表 1-21 は、Veritas Storage Foundation and High Availability Solutions 製品のマニュアルのリストです。

表 1-21 Veritas Storage Foundation and High Availability Solutions 製品のマニュアル

マニュアル名	ファイル名
Veritas Storage Foundation and High Availability Solutions ソリューションガイド	sfhas_solutions_601_lin.pdf
Veritas Storage Foundation and High Availability Solutions 仮想化ガイド	sfhas_virtualization_601_lin.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。

マニュアルページは、セクション 1、1M、3N、4、4M に分かれており、man（1）設定ファイル /etc/man.config を編集してこれらのページを表示します。

man(1) 設定ファイルを編集するには

1 man コマンドでマニュアルページにアクセスしている場合は、ユーザーのシェルで LC_ALL を「C」に設定し、ページが正しく表示されるようにします。

```
export LC_ALL=C
```

詳しくは、Red Hat Linux のサポート Web サイトのインシデント 82099 を参照してください。

2 /etc/man.config に次の行を追加します。

```
MANPATH /opt/VRTS/man
```

別の man パスもこの設定ファイルに指定されています。

3 新しいセクション番号を追加します。特定の行を変更します。

```
MANSECT         1:8:2:3:4:5:6:7:9:tcl:n:l:p:o
```

目的

```
MANSECT         1:8:2:3:4:5:6:7:9:tcl:n:l:p:o:3n:1m
```