

Veritas™ Cluster Server リリースノート

Solaris

6.0.1

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

Copyright © 2012 Symantec Corporation. All rights reserved.

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

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

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

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

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](#)
- [コンポーネント製品のリリースノート](#)
- [Veritas Cluster Server について](#)
- [Symantec Operations Readiness Tools について](#)
- [重要なリリース情報](#)
- [6.0.1 で導入された変更点](#)
- [VCS のシステム必要条件](#)
- [サポート対象外](#)
- [修正済みの問題](#)
- [既知の問題](#)
- [ソフトウェアの制限事項](#)
- [マニュアル](#)

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 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、クラスター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。

カスタムエージェントのコンパイルについて

C++ で開発されたカスタムエージェントは、Oracle Solaris Studio を使ってコンパイルする必要があります。libvcsagfw.so in usr/lib のレイアウトは次のとおりです。

```
/usr/lib/libvcsagfw.so --> . /libvcsagfw.so.2
```

古いコンパイラでコンパイルされたカスタムエージェントを使うと、VCS 6.0.1 でそのエージェントが機能しない場合があります。カスタムエージェントでスクリプトを使う場合は、ScriptAgent へのリンクを継続します。VCS 5.0 以降用に作成されたエージェントでは、Script50Agent を使います。

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 | <ul style="list-style-type: none">■ 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 | <ul style="list-style-type: none">■ 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 | <ul style="list-style-type: none">■ 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ンングプロセス

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ン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
```

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。

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。

MultiNICB エージェントの属性:

- **IPMPDevice:** IPMP インターフェース名を保存します。Solaris 11 で IPMP モードの MultiNICB リソースを設定するには、この属性の値を、MultiNICB 制御下のインターフェースのために作成された IPMP インターフェースの有効な名前を設定します。同時に、MultiNICB の UseMpathd 属性が 1 に設定されていることを確認してください。この属性は Oracle Solaris 11 にのみ適用されます。

IPMultiNICB エージェントの属性:

- **DeleteRouteOptions:** インターフェースの設定解除時にルートを削除する文字列。RouteOptions 属性および DeleteRouteOptions 属性が設定されているときは、ルートの追加に RouteOptions 属性が使われ、ルートの削除に DeleteRouteOptions 属性が使われます。RouteOptions 属性が設定されていないときは、DeleteRouteOptions 属性は無視されます。

LDom エージェント属性

- **ResyncVMCfgr:** ResyncVMCfgr 属性は havmconfigsnc 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 CFgFile 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。

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、システムのプロ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

Solaris での仮想化のサポート

次の新しい仮想化機能が Solaris に導入されました

- **Oracle Solaris 11** では、VCS は ZFS ファイルシステムでのブーンルート作成のみをサポートします。

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

havmconfsync 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。

havmconfsync 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 `havmconfsync <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 `CFGFile` 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 を再定義することにより、オンライン操作で `LDom` の設定を再定義します。

メモ: havmconfsync ユーティリティは Solaris x86 ではサポートされません。

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。

solaris10 ブランドゾーンに追加されたサポート

Oracle Solaris では、Solaris 11 システムの solaris10 ブランドゾーンのサポートが追加されました。Zone エージェントは、Solaris 11 システムの solaris10 ブランドゾーンのサポート用に更新されます。

ネットワークルートの追加および削除のための属性の分割

新しい属性 `DeleteRouteOptions` が `IPMultiNICB` リソース設定に導入されました。これにより、リソースがオフラインのときに異なるコマンドを使ってネットワークルートを削除できます。`RouteOptions` 属性および `DeleteRouteOptions` 属性が設定されているときは、ルートの追加に `RouteOptions` 属性が使われ、ルートの削除に `DeleteRouteOptions` 属性が使われます。ただし、`RouteOptions` 属性が設定されていないときは、`DeleteRouteOptions` 属性は無視されます。

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。

Share エージェントに関する変更

Solaris 11 では、VCS 6.0.1 は、Share エージェントを設定するために、再ブート後もノードに少なくとも 1 つの共有ディレクトリがある必要があります。

Solaris 11 では、次のコマンドを使って、再ブート後もディレクトリを共有します。

```
#share /xyz
```

Apache エージェントの必要条件の変更

Solaris 11 のプラットフォームでは、VCS Apache エージェントは必要条件として次のパッケージを必要とします。

```
pkg:/compatibility/ucb
```

上記のパッケージがない場合、次のエラーが表示されます。

```
Can't exec "/usr/ucb/ps": No such file or
directory at /opt/VRTSvcs/bin/Apache/Proc.pm line 699.
Use of uninitialized value $sErrorString in scalar chomp
at /opt/VRTSvcs/bin/Apache/Proc.pm line 720.
```

NFS エージェントの変更

Solaris 11 では、NFS リソースの `UseSMF` 属性を 0 に設定すると、サポートされません。

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。

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。

Solaris 11 では IPMultiNICB と MultiNICB は IPMP モードでの設定が必要

VCS 6.0.1 では、IPMP モードは MultiNICB エージェントの設定が唯一サポートされているモードであるため、Solaris 11 システムの IPMultiNICB と MultiNICB のリソースは次に示す順序で設定する必要があります。

1. MultiNICB の制御下にあるインターフェースのための IPMP インターフェースを手動で作成します。詳しくは、『Oracle Solaris Administration: Network interfaces and Network Virtualization Guide』を参照してください。
2. MultiNICB リソースの `IPMPDevice` 属性に IPMP インターフェース名を指定します。
3. MultiNICB リソースの `UseMpathd` 属性と `ConfigCheck` 属性をそれぞれ `1` と `0` に設定します。

4. IPMP インターフェースと対応する基本インターフェースが正しく設定され、それらが起動していることを確認してから MultiNICB リソースを有効にしてください。

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 IMF Daemon (IMFD) 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 リソースの下で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。

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/llttab 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。

たとえば、クラスタ内のノードで Solaris を実行している場合は、すべてのノードで Solaris SPARC または Solaris x64 を実行する必要があります。

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、クラスタ内のすべてのノードが同じ VCS バージョンを実行していることが必須です。オペレーティングシステムがクラスタ内の VCS バージョンでサポートされている場合に限り、クラスタ内の各ノードで別バージョンのオペレーティングシステムを実行できます。

p.14 の「ハードウェア互換性リスト」を参照してください。

p.14 の「サポート対象の Solaris 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 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

オペレーティングシステム	レベル	チップセット
Solaris 11	SRU1 以降	x86

VCS のサポート対象のソフトウェア

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)

Oracle Solaris 11

- Storage Foundation 6.0.1
 - VxVM 6.0.1 と VxFS 6.0.1
- Storage Foundation 6.0PR1
 - VxVM 6.0PR1 と VxFS 6.0PR1

Oracle Solaris 10

- 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。

サポート対象の Oracle VM Server for SPARC

サポート対象の Oracle VM Server for SPARC のバージョンは OVM 2.0、OVM 2.1、OVM 2.2 です。

Oracle VM Server for SPARC のサポートされる OS のバージョンについては、『Oracle VM server for SPARC リリースノート』を参照してください。

ゲストドメインで実行される Oracle Solaris OS のバージョンは、プライマリドメインで実行される Oracle Solaris OS のバージョンに依存しません。したがって、プライマリドメインで Oracle Solaris 10 OS が実行中でも、ゲストドメインで Oracle Solaris 11 OS を実行できます。同様に、プライマリドメインで Oracle Solaris 11 OS が実行中でも、ゲストドメインで Oracle Solaris 10 OS を実行できます。

プライマリドメインで Oracle Solaris 10 OS を実行する場合と Oracle Solaris 11 OS を実行する場合の違いは、各 OS の機能だけです。

サポート対象の CP サーバー向け Solaris オペレーティングシステム

表 1-2 サポート対象の CP サーバー向け Solaris OS のバージョン

オペレーティングシステム	レベル	チップセット
Solaris 10	アップデート 8、9、10	SPARC
Solaris 10	アップデート 8、9、10	x64
Solaris 11	SRU1 以降	SPARC
Solaris 11	SRU1 以降	x64

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 1-3](#) に一覧で示します。

表 1-3 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	Solaris のバージョン
DB2	DB2 Enterprise Server Edition	9.1, 9.5, 9.7	SPARC: Solaris 10 x64: Solaris 10
Oracle	Oracle	10gR2、 11gR1、 11gR2	SPARC: Solaris 10 x64: Solaris 10
		11.2.0.3	SPARC: Solaris 11 x64: Solaris 11
Sybase	Sybase Adaptive Server Enterprise	12.5.x、15.x	SPARC: Solaris 10 x64: Solaris 10

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。
- AlternateIO は Solaris 11 プラットフォームでは使用できません。
- VCS 6.0.1 は NFS サーバーでホストされる UFS ファイルシステムを使用した NFS マウントをサポートしません。

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 1-4 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 1-4 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
2845244	<p><code>vxfen</code> 起動スクリプトで <code>grep: can't open /etc/vxfen.d/data/cp_uid_db</code> エラーが発生します。</p> <p>このエラーは、存在しない可能性のあるファイルを <code>vxfen</code> 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 <code>vxfen</code> を起動するときに発生します。</p>
2554167	<p><code>/etc/llttab</code> ファイルで <code>peerinact</code> 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。</p>

インシデント	説明
2699308	Vxfenswap は、LANG が「C」以外の値に設定されると失敗します。vxfenswap ユーティリティは、内部で tr コマンドを使います。LANG 環境変数が C 以外の値に設定されていると、vxfenswap ユーティリティの不適切な動作が生じることがあります。
2726341	Solaris 11 で、vxfen 起動スクリプトはフェンシングの正しい状態を報告しません。
2850926	フェンシングはデバイス /dev/vxfen のオープンに失敗しましたというエラーメッセージをログして起動する可能性があります。この問題は、フェンシングの起動スクリプトがまだメモリにロード中のドライバにアクセスを試みると発生します。ただし、フェンシングは、エラーメッセージに関係なくシームレスに起動します。
2699291	ログは、vxfen サービスが無効になると、mv コマンドに関連するエラーを報告します。
2762660	VRTSllt パッケージのインストール後スクリプトは、SMF サービス system/llt を無効にするように試みながら、エラーを報告します。
2762660	VRTSvxfen パッケージのインストール後スクリプトは、SMF サービス system/vxfen を無効にするように試みながら、エラーを報告します。

付属エージェントの解決した問題

表 1-5 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 1-5 付属エージェントの解決した問題

インシデント	説明
2509227	MultiNICB エージェントは、LinkTestRatio 属性を 1 に設定し、IgnoreLinkStatus 属性を 0 (ゼロ) に設定することで、リンクベースの検出とプローブベースの検出を実行するように設定できます。ただし、これらの値を設定すると、エージェントはリソース状態の識別のための ICMP 要求の送信に失敗することがあります。その結果、エージェントは誤ったリソース状態を報告し、プローブベースの検出が失敗することがあります。
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。
2730451	Oracle Solaris 11 システムで、Solaris ブランドの共有 IP ゾーンで IP リソースを設定すると、IP リソースがオンラインになりません。

インシデント	説明
2850923	Zpool が破損しているために <code>-f</code> オプションと <code>-F</code> オプション を使用しても正常にインポートできない場合は、Zpool エージェントは ONLINE を報告します。Zpool の健全性が低下し、ファイルシステムは I/O エラーを報告します。
2639181	Mount エージェントの <code>clean</code> エントリポイントは、停止後、 <code>nfs</code> タイプのリソースをマウント解除できません。
2850924	<code>zfs list</code> コマンドが Zpool エージェントで失敗すると、エラー処理が示されます。
2850925	<code>pkg verify</code> コマンドはエラーメッセージを表示します。
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。
2728802	「 <code>httpdDir</code> 」属性の指定した場所に「 <code>httpd</code> 」バイナリまたは「 <code>ab</code> 」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。
2703707	Apache リソース監視を実行したときにゾーンがまだブート中であると、失効したクレデンシャルが理由となって警告メッセージが表示されます。これらのメッセージは無視して問題ありません。
2509227	リソース状態のプロンプベースの検出を実行するように MultiNICB エージェントを設定できないことがあります。
2680428	Solaris ゾーンの IPMultiNICB リソースを設定すると、エージェントはオプションを使用できません。
2730979	IPMP モードでは、インターフェースを無効にする <code>if_mpadm</code> コマンドが失敗すると、IPMultiNICB エージェントはリソースを FAULTED 状態として報告することがあります。
2714464	属性値にスペースのみを指定すると、関連する VCS エージェントに問題が生じることがあります。
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があると、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。

インシデント	説明
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。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 1-6 は、VCS エンジンに関する解決した問題の一覧です。

表 1-6 VCS エンジンの解決した問題

インシデント	説明
2879413	2 つの CmdServer インスタンスが 1 つのノードで実行されていることがあります。1 つは IPv4 のインスタンスで、もう 1 つは IPv6 です。
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 hagrpd 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。
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。 <ul style="list-style-type: none"> ■ PreOnline ■ ContainerInfo ■ TriggersEnabled ■ SystemZones
2696056	haclus -status <cluster> コマンドを実行すると、エンジンでメモリーークが発生します。

インシデント	説明
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 1-7 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 1-8 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 1-8 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。
2850920	CCSMH 5.2 または 5.1 をアンインストールするために /opt/VRTS/messages が見つからない場合でも、VRTSvcsea パッケージのアンインストールが失敗しません。

エージェントフレームワークで解決した問題

表 1-9 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 1-9 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
1786742	hares -action の出力が、設定済みのロケールの言語ではなく英語のテキストで表示されます。
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。

AMF に関連する解決した問題

表 1-10 AMF の解決した問題

インシデント	説明
2632569	AMF モジュールが停止した後も、アクセス時に自動的にロードされます。

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 1-11 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。
2680435	RunInContainer は 0 に設定されるため、IPMultiNICB エージェントはローカルゾーンの Options 属性を伝送しません。
2662766	Mount エージェントの clean エントリポイントは nfs タイプのファイルシステムのアンマウントを失敗します。
2653668	高可用性デーモン (HAD) プロセスは予想外に終了します。
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。
2632576	SMF の AMF が無効でも AMF ドライバのロードを停止できません

修正済みの問題	説明
2616497	複数の階層の障害は処理されません。

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。

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

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。

```
# hagr -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  
# hagr -unfreeze service_group -persistent  
# haconf -dump -makero
```

VRTSvlic パッケージ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 パッケージ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 パッケージ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 パッケージをアップグレードします。

```
# pkgrm VRTSvlic
```

この手順で依存関係が報告されることがありますが、この依存関係は安全に上書きできます。

```
# pkgadd -d VRTSvlic.pkg
```

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]
```

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]
```

VCS のアップグレードまたはアンインストール時にモジュールのアンロードが失敗することがある

VCS をアップグレードまたはアンインストールするとき、一部のモジュールのアンロードに失敗し、次のようなエラーメッセージが表示されることがあります。

```
fdd failed to stop on node_name  
vxfs failed to stop on node_name
```

この問題は、サブクラスタ内のどれか 1 つまたはすべてのノードで起きる可能性があります。

回避策: アップグレードまたはアンインストールの完了後、インストーラが提示する手順に従って問題を解決してください。

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。その代わりに、**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。

ローカルゾーンの Solaris システムに VRTSvlic パッケージをインストールすると、エラーメッセージが表示される [2555312]

installed 状態のローカルゾーンがある Solaris システムに VRTSvlic パッケージのインストールを試みると、システムで次のエラーメッセージが表示されます。

```
cp: cannot create /a/sbin/vxlicinst: Read-only file system
cp: cannot create /a/sbin/vxlicrep: Read-only file system
cp: cannot create /a/sbin/vxlictest: Read-only file system
```

回避策: Solaris システムでは、VRTSvlic パッケージをインストールする前に、すべての非グローバルゾーンが開始されており、**running** 状態であることを確認してください。

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。

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させ

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。

VCS Zone ユーザーは、VCS 6.0 へのアップグレード後に追加する必要がある

Zone リソースを含む設定を次のリリースから VCS 6.0 にアップグレードする場合はこれに該当します。

- Zone エージェントの DeleteVCSZoneUser 属性が 1 に設定されている VCS 5.1SP1RP1 以降の VCS リリース
- VCS 5.1SP1 以前の VCS リリース

次の問題が発生することがあります。

Zone エージェントの `offline` または `clean` のエントリポイントによって VCS Zone ユーザーが設定から削除されます。VCS 6.0 へのアップグレード後、VCS Zone ユーザーを設定に追加する必要があります。VCS Zone ユーザーは、アップグレード後に新しい構文で `hazonesetup` ユーティリティを実行することで追加できます。Solaris の `hazonesetup` ユーティリティについて詳しくは、『Veritas Storage Foundation and High Availability Solutions 仮想化ガイド』を参照してください。Solaris について詳しくは、『Veritas Storage Foundation and High Availability Solutions 仮想化ガイド』を参照してください。

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。

VCS 5.1 から 6.0.1 へのアップグレード中にクラスタが STALE_ADMIN_WAIT 状態になる [2850921]

VCS 5.1 から VCS 6.0.1 への手動アップグレードの実行中、`main.cf` に `DB2udbTypes.cf` のエントリがあると、クラスタは `STALE_ADMIN_WAIT` 状態になります。

VCS 5.1 の VRTSvcsea パッケージをインストールする

と、`/etc/VRTSagents/ha/conf/Db2udb/Db2udbTypes.cf` をポイントする `/etc/VRTSvcscs/conf/config` ディレクトリ内に `Db2udbTypes.cf` ファイルのシンボリックリンクが作成されます。手動アップグレード時には、VCS 5.1 の VRTSvcsea パッケージは削除され、続いて `/etc/VRTSvcscs/conf/config` ディレクトリ内のファイル `Db2udbTypes.cf` のシンボリックリンクが削除されます。VCS 6.0.1 の VRTSvcsea の完全なインストールの後、`/etc/VRTSvcscs/conf/config` 内のファイル `Db2udbTypes.cf` が欠落するため、クラスタが **STALE ADMIN WAIT** 状態になります。

回避策: 手動アップグレードの後、HAD を開始する前に、`Db2udbTypes.cf` を手動で `/etc/VRTSagents/ha/conf/Db2udb` ディレクトリから `/etc/VRTSvcscs/conf/config` ディレクトリにコピーしてください。

非グローバルゾーンが installed 状態でゾーンルートがノードにマウントされていない場合、CPI を使用した VCS インストールに失敗する(2731178)

Solaris 10 では、CPI がインストールまたはアンインストール中に installed 状態のゾーンを起動しようとします。ゾーンルートの基になるストレージについて、ノードへのインポートとマウントを行っていない場合、この起動は失敗し、インストールまたはアンインストールが失敗します。

回避策: インストールまたはアンインストールを行うために CPI を起動するときは、非グローバルゾーンが **running** 状態または **configured** 状態になっているようにします。

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

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。

SMFをサポートするためにVCSをアップグレードするときに、古い legacy_run サービスが現れる [2431741]

Solaris 10 システムに VCS 5.0MPx がインストールされている場合、VCS は、開始するサービスの管理のために RC スクリプトを使います。VCS のために SMF をサポートする任意のバージョンに VCS をアップグレードする場合、SMF サービスに加え、これらの RC スクリプトに対して古い legacy_run サービスが表示されます。

回避策: これらのレガシーサービスを削除するには、次の 2 つの方法があります。

- `svccfg -s smf/legacy_run` を使って `svccfg` コンソールを開き、レガシーサービスを削除します。

次に例を示します。

```
svccfg -s smf/legacy_run
svc:/smf/legacy_run> listpg *
rc2_d_S7011t    framework    NONPERSISTENT
rc2_d_S92gab    framework    NONPERSISTENT
svc:/smf/legacy_run> delpg rc2_d_S7011t
svc:/smf/legacy_run> delpg rc2_d_S92gab
svc:/smf/legacy_run> exit
```

- システムを再起動します。

AlternateIO リソースがある VCS クラスタノードで `hastop -all` コマンドを実行し、StorageSG にサービスグループがあると、ノードが LEAVING 状態のままになることがある

AlternateIO リソースが設定された VCS クラスタノードで、StorageSG 属性に Zpool、VxVM、または CVMVolDG の各リソースがあるサービスグループが含まれると、「`hastop -local`」または「`hastop -all`」コマンドによってノードが「LEAVING」状態のままになることがあります。

この問題は、代替の I/O ドメインのシナリオにおいて、LDom リソースが含まれるサービスグループと、論理ドメインにエクスポートされるストレージリソースが含まれるサービスグループの間に依存関係がないことが原因で発生します。このシナリオでは、VCS はリソースを使う論理ドメインを停止する前に、ストレージサービスグループを停止するように試みることがあります。

回避策: `hastop -local` コマンドまたは `hastop -all` コマンドを発行する前に、LDom サービスグループを停止してください。

システムメッセージの中の文字が失われる [2334245]

特定のコマンドに応じ、特に長いシステムメッセージが表示される場合、メッセージ中の文字が失われることがあります。

回避策: 回避策はありません。

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。

engine_A.log ファイルにホスト名が見つからない (1736295)

GUI は `engine_A.log` ファイルを読み込みません。GUI は `engine_A.ldf` ファイルを読み取り、そのメッセージ ID を取得し、次に適切なロケール (日本語または英語) の `bmc` ファイルのメッセージをクエリーします。`bmc` ファイルにシステム名が存在しないため、それらは失われているものとして読み込まれます。

hacf -cmdtofcf 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 -cmdtofcf 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 -cmdtofcf 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。

uuidconfig.pl -clus -display -use_llthost コマンドの実行時に文字破損が発生する [2350517]

パスワードなしの ssh または rsh が設定されていない場合、英語以外のロケールの uuidconfig.pl コマンドを使用すると、パスワードの入力を促すメッセージを表す英語以外の文字列の代わりに、文字化けした文字が表示されることがあります。

回避策: 回避策はありません。

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。

障害回復のシナリオで、フェールオーバーの際に、セカンダリサイトの Oracle サービスグループで障害が発生する [2653704]

Oracle サービスグループは、プライマリサイトで災害が発生したとき、DR サイトでオンラインになることができません。このことは、サービスグループの `AutoFailover` 属性が 1 に設定されていて、DR サイトの対応する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、発生します。ファイアドリルサービスグループは、DR サイト上でオンラインのままになっている可能性があります。

回避策: Oracle (または任意のデータベース)リソースを含んでいるサービスグループで障害が発生した場合、DR サイトでファイアドリルがオンラインになっている間の自動 DR フェールオーバーが試行された後で、ファイアドリルサービスグループを手動でオフラインにしてください。それから、DR サイトの Oracle サービスグループをオンラインにすることを試みてください。

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 `hagrps -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>
```

Solaris 11 では、VRTSvcs パッケージがパッケージ検証のエラーメッセージを表示することがある [2858192]

Solaris 11 では、VRTSvcs パッケージはパッケージ検証のエラーメッセージを表示することがあります。これは、VCS 設定ファイルの一部が製品設定の一部として修正されるためです。このエラーは無視してかまいません。

回避策: 回避策はありません。

VCS SMF サービスを無効にするとサービスが保守状態になる [2848005]

CmdServer プロセスが停止すると、VCS SMF サービスを無効にした場合、サービスが保守状態になります。

回避策: サービスの保守状態を解消するには、次を実行します。

```
# svcadm clear system/vcs
```

セキュリティ有効モードのクラスタでセキュリティを無効にすると、VCS サービスが起動しない (2724844)

スクリプトベースのインストーラを使用して VCS クラスタの状態をセキュリティ有効モードからセキュリティ無効モードに変更すると、VCS の SMF サービスは保守状態に入ります。

回避策: 次の手順を実行します

- 1 VCS の SMF サービス状態をクリアします。

```
# svcadm clear system/vcs
```

- 2 SMF サービスを有効にします。

```
# svcadm enable system/vcs
```

システムログの起動時の信頼性に関する障害メッセージ [2721512]

セキュリティが有効になった状態でクラスタを設定すると、シマンテックの認証に関するメッセージがシステムメッセージログに記録されることがあります。これらのメッセージは、機能に何の影響もなく、無視してかまいません。

回避策: 回避策はありません。

付属エージェントに関する問題

ゾーン内で実行するエントリポイントが完全に取り消されない [1179694]

エントリポイントを取り消すと、zlogin プロセスのみが取り消されます。ゾーン内で実行するスクリプトのエントリポイントは zlogin コマンドを使って **fork** されます。しかし、zlogin コマンドは Solaris ゾーンのコンテキストで実行する sh コマンドを **fork** します。このシェルプロセスおよびそのファミリーは zlogin プロセスのグループ ID を継承せず、代わりに新しいグループ ID を取得します。そのため、エージェントフレームワークがシェルプロセスの子または孫を追跡することは困難であり、このことが zlogin プロセスのみの取り消しにつながります。

回避策: Oracle は、ローカルゾーンのエントリポイントスクリプトを実行するために開始された zlogin プロセスのすべての子を強制終了する API またはしくみを提供する必要があります。

Linux NFS でエクスポートされたディレクトリを Solaris の Mount エージェントでマウントできない

Solaris の Mount エージェントはマウントディレクトリをマウントします。この時点で、Linux NFS でエクスポートされたディレクトリをマウントしようとすると、マウントに失敗して次のエラーが表示されます。

```
nfs mount: mount: <MountPoint>: Not owner
```

これは、システムの NFS のデフォルトバージョンが Solaris と Linux で一致しないことが原因です。

この問題は、Mount リソースの MountOpt 属性の値を vers=3 に設定することによって回避できます。

例

```
root@north $ mount -F nfs south:/test /logo/
nfs mount: mount: /logo: Not owner
root@north $
Mount nfsmount (
```

```
MountPoint = "/logo"  
BlockDevice = "south:/test"  
FSType = nfs  
MountOpt = "vers=3"  
)
```

ノードからのすべてのストレージパスが無効な場合に zpool コマンドがループに陥る

Solaris Zpool エージェントは、zpool コマンドを実行して zpool のインポートとエクスポートを行います。ストレージへのすべてのパスが無効な場合、zpool コマンドは応答しません。それどころか、zpool export コマンドがループに陥り、zpool をエクスポートしようとして、この状態は、ストレージパスが復元され、zpool が消去されるまで続きます。その結果、Zpool エージェントのオフライン化とクリーンプロシージャが失敗し、サービスグループは他のノードにフェールオーバーできません。

回避策: ストレージパスを復元し、保留中のすべてのコマンドが正常に実行されるように zpool clear コマンドを実行する必要があります。これにより、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るようになります。

グローバルゾーンからファイルシステムと共にゾーンの停止が試行された場合、ゾーンが停止状態のままになる [2326105]

ファイルシステムをマウント解除せずにゾーンが停止された場合、そのゾーンは停止状態に移行し、zoneadm コマンドで停止されません。

回避策: ファイルシステムをグローバルゾーンから手動でマウント解除した後で、ゾーンを停止してください。VxFS の場合、グローバルゾーンからのファイルシステムのマウント解除には、次のコマンドを使います。

VxFSMountLock が 1 のときにマウント解除するには、次のコマンドを使います。

```
umount -o mntunlock=VCS <zone root path>/<Mount Point>
```

VxFSMountLock が 1 のときに強制的にマウント解除するには、次のコマンドを使います。

```
# umount -f -o mntunlock=VCS <zone root path>/<Mount Point>
```

VxFSMountLock が 0 のときにマウント解除するには、次のコマンドを使います。

```
# umount <zone root path>/<Mount Point>
```

VxFSMountLock が 0 のときに強制的にマウント解除するには、次のコマンドを使います。

```
# umount -f <zone root path>/<Mount Point>
```

ゾーンを停止するには、次のコマンドを使います。

```
# zoneadm -z <zone_name> halt
```

Process エージェントと ProcessOnOnly エージェントは複数の空白が含まれる属性値を拒否する [2303513]

Process エージェントと ProcessOnOnly エージェントは、複数の空白で区切られている引数の属性値を受け入れません。引数属性は、プロセスの引数のセットを指定します。スクリプトがプロセスを制御する場合は、そのスクリプトが引数として渡されます。複数の引数を区切るには、単一の空白を使用する必要があります。引数の間に複数のスペースを挿入したり、属性の先頭や末尾にスペースを挿入したりすることはできません。この属性は 80 文字以内にする必要があります。

回避策: 引数の属性値を区切る場合には、単一の空白のみを使用してください。引数の属性値の間の複数の空白や、後続の空白文字は避けてください。

ストレージの接続が失われた場合、zpool コマンドがハングアップし、再ブートまでメモリに残る [2368017]

zpool の FailMode 属性が continue または wait に設定され、下位のストレージが利用可能でなければ、zpool コマンドはハングアップし、次の再ブートまでメモリに残ります。

これは、ディスクへのストレージの接続性が失われ、zpool コマンドがハングアップし、停止や強制終了できない場合に起こります。monitor エントリポイントによって実行された zpool コマンドはメモリに残ります。

回避策: この問題に対する推奨される回避策はありません。

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。

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、バ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、バ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。

zoneadm が同時に呼び出されると、ゾーンのリソースのオフラインに失敗することがある [2353541]

ゾーン EP のオフラインには、ゾーンをオフラインにするために zoneadm コマンドが使われます。そのため、zoneadm が複数のゾーンに対して同時に呼び出されると、コマンドが失敗することがあります。これは、Oracle バグ 6757506 によるもので、このバグが原因で、zoneadm コマンドの複数のインスタンス間で競合状態が発生し、次のメッセージが表示されます。

```
zoneadm: failed to get zone name: Invalid argument
```

回避策: 回避策はありません。

hazonesetup スクリプトを使っている間に変わったパスワードが、すべてのゾーンには適用されない [2332349]

複数のゾーンに対して同じユーザー名を使う場合、1 つのゾーンのパスワードを更新しても、他のゾーンのパスワードが更新されません。

回避策: 複数のゾーンのために使われる VCS ユーザーのパスワードを更新するときに、すべてのゾーンのパスワードを更新してください。

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 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。

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。

コンテナで実行されるアプリケーションに対し、同時性違反(PCV)の防止がサポートされない [2536037]

コンテナで実行されるアプリケーションに対し、そのリソースが **IMF** に登録されていない場合、**VCS** は類似の機能を使います。そのため、このときリソースをオフラインにするための **IMF** 制御がありません。同じリソースが複数のノードでオンラインになると、エージェントは検出してエンジンに報告します。エンジンはリソースをオフラインにするためにオフライン監視を使います。そのため、同じリソースが複数のノードで同時にオンラインになることを検出する前にタイムラグが生じた場合でも、**VCS** はリソースをオフラインにします。

PCV は、**Solaris** のローカルゾーン内部で実行中のアプリケーションに対して機能しません

回避策: 回避策はありません。

Netmask の値が 16 進の IPMultiNIC の場合、Monitor プログラムはリソースを UNKNOWN に変更しない [2754172]

IPMultiNIC タイプのリソースの場合、**Netmask** 属性の値が 16 進形式で指定されていると、**Monitor** プログラムはリソースの状態を **UNKNOWN** に変更しません。

NetMask 属性の値が 16 進形式で指定されているときに、**Monitor** はリソースの状態を遷移しません。そのため、コード関連エラーがログに記録されることがあります。

回避策: 回避策はありません。

共有リソースが予想外にオフラインになることが原因で、サービスグループがフェールオーバーする [1939398]

NFSRestart リソースがオフラインになり、**UseSMF** 属性が 1 に設定されていると、共有リソースが予想外にオフラインになり、フェールオーバーが起きます。

NFSRestart リソースがオフラインになるときに、**NFS** デーモンは停止します。**UseSMF** 属性が 1 に設定されていると、エクスポートされたファイルシステムは利用不能になり、そのために共有リソースは予想外にオフラインになります。

回避策: 共有リソースの `ToleranceLimit` の値に、1 を超える値を設定してください。

Mount エージェントでループバックマウントのすべてのシナリオがサポートされない

VCS 制御下のマウントポイントの場合、マウントポイントに対してループバックマウントを作成できます。たとえば、マウントポイント `/mntpt` が `/a` にループバックマウントとしてマウントされ、`/a` が `/b` にループバックマウントとしてマウントされると、マウントリソースのオフラインとオンラインに失敗します。

回避策: マウントポイント `/mntpt` を `/b` にループバックマウントとしてマウントしてください。

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、LDom、Project 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。

無効な Netmask の値によってコードエラーが表示されることがある [2583313]

IP リソース属性に無効な `Netmask` の値を指定した場合、リソースをオンラインにしようとするときに、次のようなコードエラーが表示されることがあります。

```
=====  
Illegal hexadecimal digit 'x' ignored at  
/opt/VRTSperl/lib/site_perl/5.12.2/Net/Netmask.pm line 78.  
ifconfig: <Netmask_value>: bad address  
=====
```

回避策: 有効な `Netmask` の値を指定したことを確認してください。

ForceAttach 属性が有効な ZFS に設定されるゾーンルートがブートエラーを引き起こす (2695415)

Solaris 11 システムでは、`-F` オプションでゾーンを接続すると、ZFS にゾーンルートが設定されている場合、ゾーンのブートエラーが発生することがあります。

回避策: `Zone` リソースの `ForceAttach` 属性を 1 から 0 に変更してください。この設定に加え、`DetachZonePath` のデフォルト値を 1 のままにすることをお勧めします。

ゾーンが過渡状態にあるとき Apache リソースにエラーメッセージが表示される [2703707]

ゾーンの開始時に Apache リソースがプローブされると、次のエラーメッセージがログに記録されます。

```
Argument "VCS ERROR V-16-1-10600 Cannot connect to VCS engine¥n"
isn't numeric in numeric ge (>=) at /opt/VRTSvcs/bin/Apache/Apache.pm
line 452.
VCS ERROR V-16-1-10600 Cannot connect to VCS engine
LogInt(halog call failed):TAG:E:20314 <Apache::ArgsValid> SecondLevel
MonitorTimeout must be less than MonitorTimeout.
```

回避策:このメッセージは無視してもかまいません。ゾーンが完全に開始されると、halog コマンドは失敗することなく、Apache エージェントの監視が正常に実行されます。

ゾーンがシャットダウンしているときの監視で、NICリソースがオフラインであると間違って報告される(2683680)

NIC リソースが Exclusive IP ゾーンに設定されている場合は、ゾーンが機能していれば NIC リソースはゾーン内で監視されます。ゾーンがシャットダウンしているときに NIC 監視プログラムが呼び出されると、監視プログラムは NIC リソースがオフラインであると間違って報告することがあります。これは、ネットワークサービスの一部がオフラインでありながらゾーンが完全に終了していない場合に起こります。この報告はゼロ以外の値に ToleranceLimit 値を上書きして設定することで回避できます。

回避策: NIC リソースが Exclusive IP ゾーンに設定されているときは、ToleranceLimit 属性を 0 以外の値に設定することをお勧めします。

ToleranceLimit 値は次のように計算します。

ゾーンの完全なシャットダウンに要する時間は、NIC リソースの MonitorInterval 値 + (MonitorInterval 値 x ToleranceLimit 値) と等しいかまたはそれ以下である必要があります。

たとえば、ゾーンがシャットダウンするのに 90 秒かかり、NIC エージェントの MonitorInterval が 60 秒(デフォルト値)に設定されている場合は、ToleranceLimit 値を 1 に設定します。

ノードまたはゾーンの再起動時に Apache PidFile を含むディレクトリが削除されると、Apache リソースがオンラインにならない (2680661)

Apache HTTP サーバーが PidFile を作成するディレクトリは、ノードまたはゾーンの再起動時に削除されることがあります。通常、PidFile は /var/run/apache2/httpd.pid に

置かれます。ゾーンが再ブートするとき、`/var/run/apache2` ディレクトリが削除され、これが原因で HTTP サーバーの起動が失敗することがあります。

回避策: Apache HTTP サーバーが `PidFile` をアクセス可能な場所に書き込むようにしてください。Apache HTTP の設定ファイルで `PidFile` の場所を更新できます (例: `/etc/apache2/httpd.conf`)。

LDom 設定ファイルとホスト OVM バージョンの非互換性が原因で LDom リソースのオンライン化に失敗することがある (2814991)

OVM のバージョンがホストによって異なるクラスタで LDom を実行している場合、OVM のバージョンが異なるホストに LDom 設定ファイルをインポートすると、そのホストで生成される LDom 設定ファイルにエラーメッセージが表示されることがあります。この場合、LDom リソースのオンライン化にも失敗します。

たとえば、あるクラスタに OVM のバージョンが 2.2 であるノードと OVM のバージョンが 2.1 であるノードがあり、そこで LDom を実行している場合、OVM 2.2 を使うホストで生成される XML 設定を OVM 2.1 を使うホストにインポートすると、エラーが表示されることがあります。このため、LDom リソースのオンライン化に失敗します。

次のエラーメッセージが表示されます。

```
ldm add-domain failed with error Failed to add device
/ldom1/ldom1 as ld1_disk1@primary-vds0 because this device
is already exported on LDom primary. Volume ld1_disk1
already exists in vds primary-vds0.
```

回避策: `CfgFile` 属性を指定している場合、生成される XML 設定と、ノード上にインストールされている OVM バージョンに互換性があることを確認します。

指定された IP アドレスが `allowed-address` プロパティに指定されている値に一致しない場合、IP または IPMultiNICB リソースのオンライン化に失敗することがある (2729505)

IP または IPMultiNICB リソースをゾーンで実行するように設定しているとき、そのリソースに指定されている IP アドレスが `allowed-address` プロパティに指定されている値と一致しないと、IP リソースのオンライン化に失敗することがあります。この動作は、Solaris 11 プラットフォームでのみ確認されています。

回避策: IP アドレスをゾーン設定の `allowed-address` プロパティに追加していることを確認します。

PidFiles 属性が指定されたコンテナで実行されるアプリケーションリソースが VCS 6.0 以降へのアップグレード時に offline を返す [2850927]

PidFiles 属性を使用して構成されたコンテナで実行されるように設定されているアプリケーションリソースが、VCS 6.0 以降のバージョンへのアップグレード後、状態を **offline** として返します。

VCSを以前のバージョンから6.0以降にアップグレードする場合、アプリケーションリソースが PidFiles に設定されている監視方法を使ってコンテナで実行されるように設定されていると、アップグレードを実行することで、リソースの状態は **offline** と返されます。これは、アプリケーションエージェントに導入された変更に起因します。リソースがコンテナで実行されるように設定されていて、リソースの監視用に PidFiles が設定されていると、この属性の期待値はゾーンルートに対する PID ファイルの相対パス名になります。

VCS 6.0 より前のリリースでは、この属性の期待値はゾーンルートを含む PID ファイルのパス名でした。

たとえば、コンテナで実行するように VCS 5.0MP3 に設定されているアプリケーションリソースには、次のような設定があります。

```
Application apptest (
  User = root
  StartProgram = "/ApplicationTest/app_test_start"
  StopProgram = "/ApplicationTest/app_test_stop"
  PidFiles = {
    "/zones/testzone/root/var/tmp/apptest.pid" }
  ContainerName = testzone
)
```

一方、VCS 6.0 以降のリリースでは、同じリソースに次のような設定があります。

```
Application apptest (
  User = root
  StartProgram = "/ApplicationTest/app_test_start"
  StopProgram = "/ApplicationTest/app_test_stop"
  PidFiles = {
    "/var/tmp/apptest.pid" }
)
```

メモ: コンテナ情報は、サービスグループレベルで設定されています。

回避策: 2 番目の例に示すように、PidFiles のパス名をゾーンルートに対する相対パス名に変更します。

```
# hares -modify apptest PidFiles /var/tmp/apptest.pid
```

NFS サーバーの / ファイルシステムのマウントがサポートされていない [2847999]

Mount エージェントは、NFS ファイルシステム用の NFS サーバーの / ファイルシステムでの BlockDevice 属性をサポートしません。

回避策: 回避策はありません。

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 SambaShare 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。

Solaris 11 では、グループがオフラインのとき、またはフェールオーバー中に NIC リソースに障害が発生することがある [2754172]

NIC リソースに排他的な IP ゾーンが設定されると、グループがオフラインのとき、またはフェールオーバー中に NIC リソースに障害が発生することがあります。この問題は Solaris 11 でゾーンのシャットダウンに時間がかかると発生します。このウィンドウの表示中に NIC 監視が呼び出されると、NIC エージェントはこれを障害と見なします。

回避策: 排他的な IP ゾーンのために設定された場合は、NIC リソースの ToleranceLimit を増やしてください。

shutdown コマンドを使ってサーバーが停止されると NFS クライアントがエラーレポートを返す [2872741]

Solaris 11 では、NFS 共有サービスグループを持つ VCS クラスタノードが shutdown コマンドを使って停止されると、NFS クライアントが「Stale NFS file handle」エラーをレポートする場合があります。シャットダウン中に、SMF サービス svc:/network/shares は仮想

IP を停止する前にすべての共有パスの共有を解除します。したがって、このパスにアクセスしている NFS クライアントは無効なファイルハンドルのエラーを取得します。

回避策: VCS クラスタノードをシャットダウンする前に、`svc:/network/shares SMF` サービスを無効にして、シャットダウン中に VCS が共有パスの共有解除のみを制御するようにしてください。

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。

ASMIInstAgent 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

ASMIInstAgent 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 ASMIInst エージェントでサポートされない

ASMIInst 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。

OHASD にアプリケーションリソースとして設定されているオフラインリソースを監視する ASMInstance リソースが VCS ログにエラーメッセージを記録する [2846945]

Oracle High Availability Services デーモン (OHASD) が VCS で監視対象のアプリケーションリソースとして設定されている場合、このリソースがフェールオーバーノードでオフラインになっていると、オフラインを監視する ASMInstance リソースが、VCS ログに次のエラーメッセージを記録します。

```
ASMInst:asminst:monitor:Cluster Synchronization Service  
process is not running.
```

回避策: 独立したパラレルサービスグループのアプリケーションを設定し、リソースがオンラインになるようにします。

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。

Live Upgrade に関する問題

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

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

回避策: `vxlufinish` コマンドを実行します。システムを再ブートする前に、`/altroot.5.10/etc/vfstab` ディレクトリ内にある、CFS としてマウントされる共有ディスクのすべてのボリュームのエントリを手動で削除してください。

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

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

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

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

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

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

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

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

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

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

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

回避策: Oracle パッチ 113280-10、121430-72、またはそれ以降をインストールしてから、vxlustart を実行します。

日本語ロケールの VCS に関する問題

この項では日本語ロケールの VCS 6.0.1 に関する問題について説明します。

hares -action コマンドが英語で出力を表示する [1786742]

hares -action コマンドが英語で出力を表示します。

文字破損の問題

文字破損は、インストーラがフランスロケールの HIASCII オプションを使って実行される場合に発生します。[1539754, 1539747]

回避策: 回避策はありません。

ゾーン内のメッセージがローカライズされていない

ロケールが Solaris ゾーンに対して正しく設定されません。そのため、ゾーン内でローカライズされたメッセージを表示できないことがあります。

回避策: 回避策はありません。

hamsg を使って表示されるローカライズされた文字があるシステムメッセージが、正しく表示されないことがある

hamsg を使ってシステムメッセージを表示する場合、メッセージに英語とローカライズされた文字の組合せがあると、メッセージが正しく表示されないことがあります。[2405416]

回避策: 回避策はありません。ただし、VCS ログファイルで英語のメッセージを表示できます。

スタンドアロンユーティリティの出力が英語で表示される [2848012]

次のユーティリティの出力は英語で表示されます

- -haping
- -hamultinib
- -haipswitch

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。

プライマリおよび第 1 セカンダリクラスタにパニックが発生すると第 2 セカンダリクラスタがプライマリのロールをテイクオーバーできない [2858187]

GCO に Steward なしで 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。

- 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。
- 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。この場合、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。これが発生した場合、ユーザーは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:

上の 3 つの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。

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 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場合があります。

これは LLT の機能に影響しません。

デバイスの絶対パスが `llttab` 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、`llttab` 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、`llttab` ファイルで `/dev/net/net:1` ではなく `/dev/net/net1` をお使いください。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/llttab` 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 deinitied 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。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。

再ブート後、GAB SMF サービスの起動に失敗することがある (2724565)

SFRAC 環境では、add_drv を呼び出すときの GAB と LMX の競合が原因で GAB を起
動できないことがあります。

回避策: 次のコマンドを使用して、GAB SMF サービスおよび他の依存するサービスを手
動で起動します。

```
# svcadm enable gab  
# svcadm enable vxfen  
# svcadm enable vcs
```

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。

vxfen サービスのタイムアウト問題による Solaris 10 ノードの再ブートの遅延 (1897449)

shutdown -i6 -g0 -y コマンドを使ってノードを再ブートすると、次のエラーメッセージが表示されることがあります。

```
svc:/system/vxfen:default:Method or service exit
timed out. Killing contract 142
svc:/system/vxfen:default:Method "/lib/svc/method/vxfen stop"
failed due to signal Kill.
```

このエラーは、VCS が I/O フェンシングの停止を試みるときに vxfen クライアントが引き続きアクティブになっていることが原因で発生します。その結果、vxfen stop サービスがタイムアウトになり、システムの再ブートを遅らせます。

回避策: 次の手順を実行して、この vxfen stop サービスのタイムアウトエラーが起きないようにします。

vxfen stop サービスのタイムアウトエラーが起きないようにするには

- 1 VCS を停止します。クラスタ内の任意のノードで、次のコマンドを実行します。

```
# hastop -all
```

- 2 システムを再ブートします。

```
# shutdown -i6 -g0 -y
```

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。

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 `vxfsend` 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。

vxfsnwap 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)

vxfsnwap 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 vxfsnconfig -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) vxfsnwap 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。vxfsnwap 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) vxfsnwap 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: vxfsnwap 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 vxfsnconfig 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。vxfsnadm -d コマンドは次のエラーを表示します。

```
VXFEN vxfsnadm 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 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、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 -1` 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:

`cpstat` または `vcstat` 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 状態を繰り返すとして示すことがある (2555191)

キャンバスクラスタ環境で、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 状態を繰り返すとして示すことがあります。

回避策:

RFSM 状態を繰り返すとして示すノードのフェンシングを再起動します。

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。

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。

ゾーンが準備完了状態または停止状態にあるときに、IMF はゾーンをエラーにしない [2290883]

ゾーンが準備完了状態または停止状態にあるときに、IMF はゾーンをエラーにしません。

ゾーンが準備完了状態または停止状態にあるかどうかを、IMF は検出しません。Ready 状態では、実行中のゾーン内で動作しているサービスはありません。

回避策: ゾーンをオフラインにしてから、再起動してください。

ゾーンが保守状態に入るときに、IMF がゾーンの状態を検出し ない [2535733]

IMF は状態の変更を検出しません。ただし、次のサイクルでは、Zone 監視によって状態の変更が検出されます。

回避策: 回避策はありません。

エンジンログが、AMF とのマウントオフライン登録の数に比例した メッセージでいっぱいになる [2619778]

特定のエラー条件において、AMF に登録されるすべてのマウントオフラインイベントが同時に通知されます。これにより、登録されるマウントオフラインイベントごとに、次のメッセージがエンジンログに出力されます。

```
<Date> <Time> VCS INFO V-16-2-13717  
(vcsnode001) Output of the completed operation  
(imf_getnotification)
```

```
=====  
Cannot continue monitoring event  
Got notification for group: cfsmount221
```

```
=====
```

これはこのエラー条件での予想どおりの動作です。メッセージを別にすれば、VCS ソリューションの機能には影響がありません。

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。

同時性違反の出力のプロアクティブな防止に国際化サポートを利用できない [2848011]

次の ProPCV メッセージに国際化サポートは利用できません。

```
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。

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。

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。

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。

Java GUI を使用する Solaris 11 で、セキュア VCS クラスタにログインできない (2718955)

VCS Java GUI を使用する Solaris 11 システムで展開されるセキュアクラスタへの接続は、VCS 6.0PR1 ではサポートされません。Java GUI を使おうとすると、システムに次のエラーが表示されます。

```
Incorrect username/password
```

回避策: 回避策はありません。

仮想化に関する問題

solaris10 ブランドゾーンの Solaris 11 システムに表示されるロケールメッセージ

Solaris 11 システムで `zlogin` コマンドを実行すると、システムは次のエラーメッセージをログに記録します。

```
Could not set locale correctly.
```

Solaris 11 のデフォルトロケールは `en_US.UTF-8` で、Solaris 10 のデフォルトロケールは `C` です。Solaris 10 ブランドゾーンでは、`en_US.UTF-8` はデフォルトではゾーン内にインストールされていません。したがって、エラーメッセージはログに記録されます。

回避策: このメッセージが表示されても機能に問題はないので無視してもかまいません。このメッセージを避けるには、solaris10 ブランドゾーンに `en_US.UTF-8` ロケールをインストールしてください。

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.74 の「[マニュアル](#)」を参照してください。

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 の制御下でない一部のプロセスが停止される場合があります。

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。

LDom リソースのオンライン化の失敗 [2517350]

ブートディスクが、仮想ディスクマルチパスグループ (mpgroup) の一部であるゲストドメイン内で設定され、仮想ディスクへのプライマリパスが使用できない場合、LDom リソースのオンライン化に失敗します。

これは、ゲストドメインをブートするときに、仮想ディスクマルチパスグループの一部である仮想ディスク用に存在する他のデバイスパスの再試行を許可しない、Oracle VM サーバーの制限事項が原因です。

回避策: なし。

Directory Online イベントに対して IMF に登録される Zone エージェント

Directory Online イベントは、ゾーンルートディレクトリを監視します。ゾーンルートディレクトリの親ディレクトリが削除されたり別の場所に移動されたりした場合でも、AMF は Zone エージェントに通知を提供しません。この変更は Zone の monitor の次のサイクルで検出され、OFFLINE としてリソースの状態が報告されます。

LDom リソースは、プライマリドメインが適切な手順を経てシャットダウンされたときに、clean エントリポイントを呼び出す

LDom エージェントは、プライマリドメインが停止したときに、ゲストドメインを停止するようにゲストドメインの障害ポリシーを設定します。そのため、プライマリドメインがシャットダウンされると、ゲストドメインは停止します。さらに、プライマリドメインがシャットダウンされると、ldmd デーモンが突然停止し、LDom 設定が読み取れなくなります。これらの操作は、VCS の制御下になく、VCS は clean エントリポイントを呼び出すことがあります。

回避策: 回避策はありません。

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。

インターフェースオブジェクト名は、Solaris 11 のゲストドメインの VCS ネットワーク再設定スクリプトの net<x>/v4static と一致する必要がある [2840193]

Solaris 11 のゲストドメインが DR 用に設定され、インターフェースオブジェクト名が net<x>/v4static パターンと一致していないと、ゲストドメイン内で実行される VCS ゲストネットワーク再設定スクリプト (VRTSvcsnr) が新しいインターフェースオブジェクトを追加し、既存のエントリはそのまま残ります。

Share エージェントの制限事項 (2717636)

Share リソースが VCS でシステムディレクトリ (例: /usr) または起動時にマウントされる Oracle Solaris 11 を共有するように設定されている場合、パニックまたは停止後にノード上で VCS が開始されると、VCS 共有リソースはオンラインでそれを検出します。このとき、共有リソースがフェールオーバーサービスグループの一部である場合は同時性違反になり、グループがクラスタの別のノードにフェールオーバーすることがあります。その後、VCS は Share リソースを終了させます。これは共有コマンドの動作が原因か、または

Oracle Solaris 11 で、共有コマンドと共有されるディレクトリが再ブート後もシステムに永続的に残ることが原因です。

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` の値に基づき、`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。

混在スタック環境の 5.0MP3 からのグローバルクラスタのアップグレードを実行すると、エンジンがハングアップする [1820327]

(IPv4 と IPv6 が使用中である) 混在スタック VCS 環境を 5.0MP3 から 5.1SP1 にアップグレードしようとする、HAD がハングアップすることがあります。

回避策: 5.0MP3 からのアップグレードを実行するときは、システムで IPv6 アドレスが plumb されていないことを確認します。

ゾーンルートが VxFS 共有ストレージにある場合、VCS インストーラを使って VCS をインストールまたはアップグレードする [1215671]

ゾーンルートが Veritas File System (VxFS) にある場合は、VCS インストーラプログラムを使って VCS をインストールまたはアップグレードする必要があります。

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。

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。

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。

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、より重みが大いかに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、より重みがいかに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な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 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。

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。
- ゾーンルートのレプリケーションについて、**Zone Disaster Recovery** の **Veritas Volume Replicator** の設定はサポートされていません。**Oracle Solaris 11** は **ZFS** ファイルシステムのゾーンルートのみをサポートします。
- **VCS 6.0.1** では、**Solaris 10** バージョンと **Solaris 11** バージョンで動作するシステム間のクラスタのような混合ノードのクラスタの設定はサポートされていません。手動設定、または **CPI** 設定のいずれもサポートされていません。

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 1-12 は Veritas Cluster Server に関するマニュアルのリストです。

表 1-12 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_sol.pdf
Veritas Cluster Server リリースノート	vcs_notes_601_sol.pdf
Veritas Cluster Server 管理者ガイド	vcs_admin_601_sol.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_sol.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 アプリケーションノート: Dynamic Reconfiguration for Oracle Servers	vcs_dynamic_reconfig_601_sol.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_sol.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_sol.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_sol.pdf

表 1-13 は、Veritas Storage Foundation and High Availability Solutions 製品のマニュアルのリストです。

表 1-13 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_sol.pdf
Veritas Storage Foundation and High Availability Solutions 仮想化ガイド	sfhas_virtualization_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。

