Symantec™ Cluster Server リリースノート

Solaris

6.1

Symantec

Symantec™ 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。

製品のバージョン: 6.1

マニュアルバージョン: 6.1 Rev 0

法的通知と登録商標

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Symantec 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 Solaris 対応の Symantec Cluster Server（VCS）バージョン 6.1 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『Symantec Cluster Server リリースノート』の マニュアルバージョン: 6.1 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。

- Symantec Storage Foundation リリースノート（6.1）

Symantec Cluster Server について

シマンテック社の Symantec 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、『Symantec Cluster Server Bundled Agents リファレンスガイド』を参照してください。

Symantec 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、次を参照してください https://sort.symantec.com/home。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。Symantec 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『Symantec 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 6.1 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

- 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して、インストールとアップグレードのカスタムレポートを生成する。
- パッチを製品またはプラットフォームごとに、インストールする必要がある順番で一覧表示する。ごく最近のパッチまたは過去のパッチを表示してダウンロードする。
- ASL（Array Support Library）の詳細をベンダー、プラットフォーム、SFHA（Storage Foundation and High Availability）のバージョンごとに表示する。ASL により、SFHA ベースのサーバーに接続されているアレイの管理が簡単になります。
- エージェントのタイプ、アプリケーション、プラットフォームに基づいて、VCS と ApplicationHA のエージェント、マニュアル、ダウンロードを一覧表示する。

リスクの特定およびサーバー固有の推奨事項の取得	■ 潜在的な環境リスクに備えサーバーを分析する。システムの可用性、ストレージの使用状況、パフォーマンス、ベストプラクティスに関する特定の推奨事項を使ってリスク評価カスタムレポートを生成する。 ■ 何千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	■ パッチ、アレイ固有のモジュール（ASL、APM、DDI、DDL）、マニュアル、製品リリース、HCL（Hardware Compatibility List の略でハードウェア互換性リストの意味）、VCS/ApplicationHA 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。 ■ インストールされているシマンテック製品とライセンスキーの情報を運用環境からすばやく収集する。製品名、バージョン、プラットフォーム、サーバー層、SPVU（Symantec Performance Value Unit）、サポート終了期日を含む、ライセンスまたは配備のカスタムレポートを生成する。 ■ 製品ガイド、マニュアルページ、互換性リスト、サポート記事などのシマンテック製品文書を一覧表示してダウンロードする。 ■ シマンテック製品サポート、SymConnect フォーラム、カスタマケア、シマンテック社のトレーニングと教育、シマンテック社の FileConnect、ライセンシングポータル、my.symantec.com などの重要なリソースへのリンクに 1 つのページからアクセスする。このページには、主要ベンダーのサポートサイトへのリンクも含まれます。 ■ iOS デバイスから SORT 機能のサブセットを使う。次の Web サイトからアプリケーションをダウンロードする必要があります。 https://sort.symantec.com/mobile

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/TECH211540
- 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/

- このハードウェア互換性リストにはサポートされているハードウェアの情報が記されており、定期的に更新されます。サポートされているハードウェアの最新情報については、次の URL を参照してください。
  http://www.symantec.com/docs/TECH211575
  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。

6.1 で導入された変更点

この項では Symantec Cluster Server 6.1 の変更点の一覧を示します。

VCS 6.1 で導入された属性

次のセクションでは VCS 6.1 で導入された属性について説明します。

Solaris の LDom エージェントの属性

DomainFailurePolicy:

ゲストのドメインに対して、マスタードメインとマスタードメインの障害ポリシーのリストを指定します。

属性キー: マスタードメインの名前。

キーの値: ゲストドメイン上のマスタードメインによって実施される障害ポリシー。

この機能を使うには

- LDom リソース属性の DomainFailurePolicy をマスタードメインとその障害ポリシーに設定します。
- LDom サービスグループ属性の SysDownPolicy を AutoDisableNoOffline に設定します。

UserName:

別のホストからホスト上の論理ドメインを移行する権限があるユーザー名を指定します。

Password:

UserName 属性で指定したユーザーの暗号化パスワードを指定します。

ReregPGR

この属性を 1 に設定すると、`hagrp -migrate` コマンドを使った論理ドメインのライブ移行後に、LDom エージェントはその論理ドメイン内部で `vxdmpadm pgrrereg` コマンドを実行します。

NFS エージェントの属性

Protocol	nfsd デーモンを実行するプロトコルを指定します。エージェントはこの属性を使い、指定されたプロトコルを使用して NFS デーモンが動作していることを確認します。
MountdOptions	mountd デーモンのオプションを指定します。

NotifierMngr エージェント属性

DiskGroup エージェントの属性

ClearClone	ディスクグループのインポート時に「clone」と「udid_mismatch」フラグをディスクグループのディスクから消去します。また、必要な場合は UDID を更新します。

ターゲットシステムの動的な選択を有効にする新しい属性

Statistics	統計収集が有効であるかどうか、FaultOverPolicy を BiggestAvailable に設定可能であるかどうかを示します。統計は、CPU、メモリ、スワップなどのシステムリソースについて収集されます。
MeterWeight	複数のシステムがグループ属性の Load 要件に適合する場合に、サービスグループのターゲットシステムを判別するために指定されたクラスタ属性の HostMeters キーの重みを表します。
HostAvailableMeters	システムリソースの測定に使用可能なメーターを一覧表示します。この属性は main.cf で設定できません。
HostMeters	クラスタで現在測定されているパラメータ（CPU、Mem または Swap）を示します。
MeterControl	HostMeters で指定したキーに対するシステム属性 AvailableCapacity の測定と予測が完了するまでの間隔を示します。
HostAvailableForecast	過去に測定した AvailableCapacity に基づき予測されたクラスタのシステムの利用可能な容量を示します。

MeterRecord	事前定義されたキーを持つ内部システム属性として動作します。この属性は、クラスタ属性の Statistics を有効に設定した場合のみ更新されます。
ReservedCapacity	オンラインに切り替わろうとしている、FailOverPolicy を BiggestAvailable に設定しているサービスグループ用に予約済みのシステムの容量を示します。この属性は、CPU、Mem、Swap など HostMeters で指定したすべてのキーを持ちます。キーの値は、クラスタ属性の MeterUnit で指定した対応の単位で設定します。
CapacityReserved	サービスグループをオンラインに切り替えるか、フェールオーバーするための容量が予約されているかどうかを示します。サービスグループの属性の FailOverPolicy を BiggestAvailable に設定している場合のみ容量が予約されます。
UnSteadyCount	オンラインまたはオフライン操作が保留されているリソースの合計数を表します。これはローカライズされた属性です。
MemThresholdLevel	各種レベルのログが生成される基準となるメモリ利用率のしきい値を決定します。

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

インストールとアップグレードに関する変更

6.1 の製品インストーラには、次の変更点が含まれています。

異なるプラットフォーム間でのインストールのサポート

インストール元システムとインストール先システムが異なるプラットフォームで動作している場合でも、スクリプトベースのインストーラまたは Web ベースのインストーラを使って、サポート対象プラットフォームを実行するインストール先システムに VCS をインストールできます。

Solaris 11 Live Upgrade のサポート

Solaris 11 システムで Live Upgrade を使って製品と Solaris オペレーティングシステムのアップグレードを実行できます。Live Upgrade 処理では、ZFS ストレージアプリケーションがプライマリブートディスクに代替ブート環境を作成します。すべてのブート環境は現在のディスクに保存されます。したがって、代替ブートディスクは不要になりました。

インストーラのホットフィックスの自動ダウンロード

6.1 製品のインストーラを実行し、システムがインターネットにアクセスしている場合には、インストーラは必要なインストーラのホットフィックスを自動的にインポートして使用を開始します。

システムがインターネットにアクセスしていなくても、Symantec Operations Readiness Tools パッチ検索ツールを使ってインストーラのホットフィックスを手動でダウンロードできます。

インストーラのホットフィックスを自動でダウンロードするには、インストーラがアウトバウンドネットワーク呼び出しを行う必要があります。システムがファイアウォールの背後にある場合やインストーラがアウトバウンドネットワーク呼び出しを行わないようにする場合は、インターネットパッチセンター（-noipc）オプションを使わずにインストーラを実行して外部ネットワークの試行を無効にします。次に例を示します。

```
# ./installer -version -noipc system1 system2
```

配備サーバーを使用した集中型インストールのサポート

配備サーバーにより、複数のリリースイメージを中央の 1 つの場所に格納し、それらをサポート対象プラットフォームのシステムに配備することができます。バージョン 5.1 にさかのぼるシマンテック製品用の製品バイナリを中央リポジトリにロードし、格納することができます。

次のタスクを実行するために配備サーバーを使用することができます。

- バージョンチェック
- リリースイメージ管理
- システムのインストールまたはアップグレード
- メタデータおよび優先設定の更新

処理のパッチ修正と更新の向上

製品の保守リリースとパブリックホットフィックスリリースをインストーラから直接ダウンロードできるようになりました。-version オプションで installer コマンドを実行すると、インストーラには利用可能な GA リリース、保守リリース、ホットフィックスリリースの一覧が表示されます。インターネットにアクセスしている場合は、インストーラのプロンプトに従ってローカルシステムに利用可能なパッチとホットフィックスをダウンロードできます。

パッチとホットフィックスをダウンロードするには、インストーラがアウトバウンドネットワーク呼び出しを行う必要があります。システムがファイアウォールの背後にある場合やインストーラがアウトバウンドネットワーク呼び出しを行わないようにする場合は、インターネットパッチセンター（-noipc）オプションを使わずにインストーラを実行して外部ネットワークの試行を無効にします。-noipc オプションを使うと、インストーラは SORT（Symantec Operations Readiness Tools）Web サイトに接続しません。次に例を示します。

```
# ./installer -version -noipc system1 system2
```

ベースリリース、保守パッチ、ホットフィックスを同時にインストールまたはアップグレードするためのサポート

バージョン 6.1 から提供している Install Bundles は、お使いのシステムを 1 回の手順で簡単にベース、保守またはホットフィックスレベルにする、直接インストールまたはアップグレードを行うための方法です。Install Bundles はインストーラをマージする機能です。お客様は一度の実行で保守レベルまたはホットフィックスレベルに直接インストールまたはアップグレードすることができます。Install Bundles は、より上位の保守またはホットフィックスリリースへのポインタを持つ GA リリースからのインストーラの実行により構成されています。インストーラによりそれらの両方が同じリリースイメージで組み合わせられたようにインストールされます。さまざまなスクリプト、パッケージ およびパッチコンポーネントがマージされ、複数のリリースが 1 つのインストールエンティティであるかのようにまとめてインストールされます。

5 つの可能な統合方法があります。すべての実行は最高レベルのスクリプトから実行する必要があります。

- ベース + 保守
- ベース + ホットフィックス
- 保守 + ホットフィックス
- ベース + 保守 + ホットフィックス
- ベースまたは保守 + 複数のホットフィックス

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、『Symantec Cluster Server 管理者ガイド』と『Symantec Cluster Server Bundled Agents リファレンスガイド』を参照してください。

Apache HTTP サーバーエージェントの IMF サポート

Apache HTTP サーバーエージェントは、IMF 対応であり、IMF 通知に AMF カーネルドライバを使います。エージェントは Apache リソースの詳細な監視も実行します。ユーザーは LevelTwoMonitorFreq 属性で詳細な監視の頻度を調整できます。この SecondLevelMonitor 属性は非推奨です。

Mount エージェントを使った非グローバルゾーン内での直接マウントのサポート

非グローバルゾーン内に VxFS を直接マウントできます。非グローバルゾーン内に VxFS を直接マウントするには、リソースレベルで ContainerOpts 属性を無効にし、RunInContainer 属性の値を 1 に設定します。

MonitorProgram 属性を設定している場合にアプリケーションエージェントでレベル 2 の監視をサポートする

アプリケーションリソースに MonitorProgram、PidFiles、または MonitorProcesses と一緒に両方を設定している場合は、レベル 2 の監視として MonitorProgram を実行するようにアプリケーションリソースを設定できます。レベル 2 の監視を有効にするには、LevelTwoMonitorFreq 属性をゼロより大きい値に設定します。アプリケーションリソースの LevelTwoMonitorFreq 属性のデフォルト値は 1（1 回）です。

この値を変更すると、MonitorProgram を MonitorProcess または PidFiles と一緒に設定している場合でもこの両方と一緒に設定している場合でも、アプリケーションエージェントはインスタント通知に AMF を利用します。

詳細を提供するために改善されたプロキシエージェントログ

プロキシエージェントログメッセージでは、エージェントの状態が不明またはエラーになる理由などに関する詳細が提供されるようになりました。デバッグメッセージも、プロキシリソースがオンラインまたはオフラインになるときログに記録されます。

Apache エージェントは、プロセスの停止時にリソースがオフラインで取得する [2978005]

Apache エージェントは、Apache プロセスがオフラインエントリポイントの一部として停止すると、ただちにリソースをオフラインで取得するように修正されました。

NFS エージェントの拡張

NFS エージェントは、指定されたプロトコルでの nfsd デーモンの実行をサポートします。

Mount のエージェントの新しいエージェント機能

Mount エージェントは attr_changed 機能をサポートします。この機能は VxFSMountLock 属性の値を 1 または 2 のいずれかから 0 に変更すると、マウントをロック解除します。

LDom エージェントの拡張

Solaris 用 LDom エージェントは拡張され、次の機能が含まれています。

- VCS による LDom リソースの移行のサポート

VCS によるゲストドメイン移行を開始するために、新しい移行エントリポイントが LDom エージェントに追加されました。2 つの新しい属性 UserName および Password がゲストドメインの移行をサポートするために導入されました。

- VCS では、複数の I/O ドメイン環境で制御ドメイン再起動を持つ論理ドメインがサポートされています。
  ゲストドメインは、プライマリまたは代替 I/O ドメインからの I/O サービスが利用可能な場合は、制御ドメインが再起動または停止されても機能し続けます。この場合、Oracle VM for SPARC ゲストドメイン (LDom) が複数の I/O ドメイン (通常はプライマリドメインと代替 I/O ドメイン) からの I/O サービスに提供されます。
- Oracle VM Server for SPARC を設定するための新しいコマンド
  新しいコマンド `haldomsetup` は、VCS 管理下で Oracle VM Server for SPARC ゲストドメインを設定できるようにするために導入されました。詳しくは、『Symantec Cluster Server マニュアルページ』を参照してください。

p.8 の「VCS 6.1 で導入された属性」を参照してください。

MonitorCPU 属性のデフォルト値を 0（ゼロ）に変更した Solaris の LDom エージェント

MonitorCPU 属性が有効で、LDom に接続されているすべての仮想 CPU の使用率が 0 % または 100 % の場合は、リソースは失敗したと宣言されます。

MonitorCPU 属性のデフォルト値を 0 に設定すると、リソースのエラーを防ぐことができます。

VCS エンジンに関する変更

外部通信ポートを許可するかどうかを決定する OpenVCSCommunicationPort 属性

OpenVCSCommunicationPort 属性は、VCS の外部通信ポートを通信用に開くかどうかを決定します。

VCS の外部通信ポートが開かれていない場合、次の制限事項が適用されます。

- Java コンソールを使って VCS を管理できません。
- RemoteGroup リソースと `hazonesetup` コマンドで設定したユーザーが VCS にアクセスできません。

ターゲットシステムの動的選択

ターゲットシステムの動的選択では、VCS が利用可能な最大システムへのアプリケーションのフェールオーバーを動的に決定できます。VCS は CPU、メモリ、スワップからシステムの利用可能な容量を監視し、利用可能な最大システムを選択します。ターゲットシ

ステムの動的選択について詳しくは、『Symantec Cluster Server 管理者ガイド』を参照してください。

ターゲットシステムの動的選択を実装するために修正した属性

VCS にターゲットシステムの動的選択を実装するために、次の属性を修正しました。

- HostUtilization: HostMonitor エージェントが計算したホストのリソース使用率(%)を示します。
- FailOverPolicy: VCS がフェールオーバー先システムを判断する方法を制御します。このサービスグループ属性に新しいポリシー値 BiggestAvailable を追加しました。
  BiggestAvailable: VCS は SystemList のすべてのシステムに利用可能な予測量に基づいてシステムを選択します。利用可能な容量が最も多く予測されたシステムを選択します。このポリシーは、クラスタ属性 Statistics が有効で、MeterUnit 属性に指定したように絶対単位で CPU、メモリ、スワップにサービスグループ属性 Load を定義する場合にのみ設定できます。
- Load: これは、システム容量とサービスグループの負荷から成る FailOverPolicy 属性の値です。
- HostMonitor: HostMonitor エージェントが監視するホストリソースのリストを含めます。
- AvailableCapacity: システムの利用可能な容量を示します。
- Capacity: システムの合計容量を表します。

メモ: AvailableCapacity、Capacity、Load、DynamicLoad の属性には多次元値があります。

VCS エージェントフレームワークの変更点

VCS エージェントフレームワークは次のように変更されました。

サービスグループのライブ移行

VCS は、仮想マシンを監視するリソースがあるサービスグループにライブ移行機能を提供するようになりました。サービスグループの移行処理には同時に、最小停止時間で移行元システムから移行先システムにサービスグループを移動することも含まれます。エージェント開発者のために「migrate」という名前の新しいエントリポイントをこの処理に導入しました。このエントリポイントは Script60Agent で利用可能です。移行動作のエントリポイントは新しい属性(MigrateTimeout、MigrateWaitLimit、SupportedOperations)を使って制御できます。

詳しくは、『Symantec Cluster Server 管理者ガイド』、『Symantec Cluster Server Bundled Agents リファレンスガイド』、『Symantec Cluster Server Agent 開発者ガイ

ド』、『Symantec Storage Foundation and High Availability Solutions 仮想化ガイド』を参照してください。

Oracle エージェントの変更点

このセクションでは、Symantec Cluster Server agent for Oracle の変更点について説明します。

VCS agent for Oracle は、Oracle 診断 API を使って Oracle インスタンスの意図的なオフライン化を決定します。

Symantec Cluster Server agent for Oracle は、Oracle 診断 API を使って、ノード上の Oracle インスタンスが適切にシャットダウンしたか、中止されたかを判別します。Oracle インスタンスが VCS の制御外で適切にシャットダウンした場合、エージェントはその操作を意図的なオフライン化として認識します。

VCS 6.1 リリース以降では、事前に構築された診断バイナリは出荷されません。`build_oraapi.sh` スクリプトを実行して、Oracle バージョンに基づき Oracle 診断バイナリを構築する必要があります。

詳しくは、『Symantec Cluster Server Agent for Oracle インストール/設定ガイド」を参照してください。

Oracle 12c の従来の機能をサポートする

Oracle 12c の従来の機能のみをサポートするようになりました。Oracle 12c に導入された新機能（Oracle Pluggable Database など）は VCS 6.1 ではサポートされません。

LLT、GAB、I/O フェンシングへの変更

ここでは、LLT、GAB、I/O フェンシングに追加された新しい機能または拡張について説明します。

単一のノードクラスタでの LLT、GAB、I/O フェンシングの無効化

単一ノードでアプリケーションを管理し、VCS のアプリケーション再起動機能を使う場合のみ、その単一ノードの VCS（Symantec Cluster Server）クラスタで LLT、GAB、I/O フェンシングのカーネルモジュールを無効にします。

カーネルモジュールを無効にすると、複数のノード全体のアプリケーションに高可用性を提供できなくなることに注意してください。ただし、後でクラスタを複数のノードに拡張するときに、これらのモジュールを有効にし、アプリケーションを高可用にすることができます。

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

カーネルコンポーネントは、Solaris 10 上の非グローバルゾーン内にパッケージメタデータをインストールしない

VCS カーネルコンポーネント VRTSllt、VRTSgab、VRTSvxfen および VRTSamf パッケージは、Solaris 10 オペレーティングシステムの非グローバルゾーン内にパッケージメタデータをインストールしなくなりました。

LLT への変更

6.1 の Symantec Cluster Server には、次の LLT への変更点が含まれています。

LLT コマンドの変更

このリリースでは次のコマンドの変更が行われています。

`lltconfig` のアップデート:

- 新しいオプション `lltconfig -l` が追加されました。新しいリンクを追加するとき、`-l` オプションを使用してそのリンクが低優先度リンクであることを指定することができます。

新しい SMF サービスにより、Solaris 11 で LLT ドライバを追加または削除するときに競合状態が回避される（3273046）

Solaris 11 では、LLT ドライバの追加と削除を管理するために、2 つの新しい SMF サービス、「llt-postinstall」と「llt-preremove」が追加されました。これらの新しい SMF サービスが追加されたため、LLT ドライバは、パッケージのインストール中にのみ追加され、パッケージの削除時に削除されます。新しい SMF サービスによって、システム再始動時の LLT ドライバのインストールエラーが回避されます。

GAB への変更

6.1 の Symantec Cluster Server（VCS）には、次の GAB への変更点が含まれています。

誤ったフェールオーバーを防ぐ Adaptive GAB の調整

ノードで GAB が異なるロード状態に適応できるように（CPU 負荷ごとに）、VCS 環境変数 `VCS_GAB_TIMEOUT_SECS` と `VCS_GAB_PEAKLOAD_TIMEOUT_SECS` を設定できます。GAB は、オペレーティングシステムから取得した負荷平均数と HAD に設定した変数に基づいて負荷期間のタイムアウトの範囲を計算します。GAB はタイムアウト期間後に HAD を強制終了します。

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

新しい SMF サービスにより、Solaris 11 で GAB ドライバを追加または削除するときに競合状態が回避される

Solaris 11 では、GAB ドライバの追加と削除を管理するために、2 つの新しい SMF サービス、「gab-postinstall」と「gab-preremove」が追加されました。これらの新しい SMF サービスが追加されたため、GAB ドライバは、パッケージのインストール中にのみ追加され、パッケージの削除時に削除されます。新しい SMF サービスによって、システム再始動時の GAB ドライバのインストールエラーが回避されます。

I/O フェンシングに関する変更

6.1 の Symantec Cluster Server（VCS）には、次の I/O フェンシングへの変更点が含まれています。

I/O フェンシングの設定時にコーディネーションポイントの順序を設定する

インストーラで `-fencing` オプションを使うと、コーディネーションポイントの順序を設定できます。

ネットワークパーティション時にコーディネーションポイント（コーディネーションディスクまたはコーディネーションポイントサーバー）が競争に参加する順序を決定します。インストーラで設定したコーディネーションポイントの順序が /etc/vxfenmode ファイルに更新されます。I/O フェンシングは、vxfenmode ファイルにリストされる順序に基づきコーディネーションポイントにアプローチします。

したがって、I/O フェンシングがメンバーシップアービトレーションの目的でコーディネーションポイントに達する可能性に基づき順序を決定する必要があります。

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

インストールプログラムを使って既存コーディネーションポイントでキーまたは登録を更新する

インスーラで `-fencing` オプションを使って、既存のコーディネーションポイントの登録を更新できます。

既存のコーディネーションポイントの登録の損失は、偶発的なアレイの再起動、キーの破損、その他の原因により発生する場合があります。コーディネーションポイントがクラスタノードの登録を失うと、ネットワーク分割の発生時にクラスタでパニックが発生する場合があります。CoordPoint エージェントによって既存のコーディネーションポイントのいずれかの登録が損失したことが VCS に通知されるときに、コーディネーションポイントの登録を更新する必要があります。

クラスタがオンラインのときに、クラスタでのアプリケーションダウンタイムなしで、コーディネーションポイントの登録の計画更新を行うこともできます。

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

CPI は単一ノードの VCS クラスタで CP サーバーを設定し、CP サーバー固有のライセンスを自動的にインストールする

CP サーバーを単一ノードの VCS クラスタで設定すると、インストーラは CP サーバー固有のライセンスを自動的にインストールします。これはまた VOM（Veritas Operations Manager）が、シングルノードのコーディネーションポイント（CP）サーバーのライセンスを、VCS ライセンスとしてではなく、CP サーバー固有のライセンスとして識別できるようにします。

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

サイトベースの優先フェンシングポリシー

コーディネーションポイントの獲得時にフェンシングドライバは、優先度が高いサイトが存在するノードを優先します。VCS はサイトレベル属性の Preference を使ってノードの重みを判断します。

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

CP サーバーとアプリケーションクライアントクラスタノード間の HTTPS 通信をサポート

CP サーバーおよびアプリケーションクライアントクラスタノードは業界標準の HTTPS プロトコルを使用して安全に通信できます。リリース 6.1 以前は、CP サーバーとクライアント間の通信はシマンテック社の専有プロトコルである IPM（Inter Process Messaging）プロトコルを通して行われていました。安全な IPM ベースの通信では Symantec Product Authentication Services （AT）を使用して CP サーバーとクライアントノードの間で安全な通信を確立します。HTTPS を使用した安全な通信を行えますが、CP サーバー機能は以前のリリースとの下位互換性も保っています。リリース 6.1 以前のクライアントノードをサポートするため、CP サーバーは HTTP ベースの通信に加えて IPM ベースの通信もサポートします。ただし、6.1 以降のクライアントノードは HTTPS ベースの通信だけをサポートします。

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

非推奨になった `/etc/vxfenmode` ファイルの security 属性

VCS 6.1 から、Coordination Point（CP）クライアントは HTTPS プロトコルを使用して CP サーバーと通信するようになりました。したがって、`/etc/vxfenmode` の「security」パラメータは非推奨となり、1 または 0 に設定しても効果がありません。

リリースバージョン 6.1 へのアプリケーションクラスタのローリングアップグレードにリリースバージョン 6.1 を実行する CP サーバーが必要

リリースバージョン 6.1 で実行するアプリケーションクラスタと CP サーバーは HTTPS プロトコルを使って通信します。そのため、クラスタを 6.1 にアップグレードすると、フェンシングコーディネーションポイントとして CP サーバーを使うアプリケーションクラスタは、6.1 より前の CP サーバーにアクセスできなくなります。円滑にアップグレードするには、アプ

リケーションクラスタでリリースバージョン 6.1 を実行する CP サーバーを使うか、または以前のリリースバージョンを実行する CP サーバーを 6.1 にアップグレードする必要があります。リリースバージョン 6.1 を実行する CP サーバーは 6.1 より前のアプリケーションクラスタで働くことができます。

新しい SMF サービスにより、Solaris 11 で I/O フェンシングドライバを追加または削除するときに競合状態が回避される（3273046）

Solaris 11 では、I/O フェンシングドライバの追加と削除を管理するために、2 つの新しい SMF サービス、「vxfen-postinstall」と「vxfen-preremove」が追加されました。これらの新しい SMF サービスが追加されたため、I/O フェンシングドライバは、パッケージのインストール中にのみ追加され、パッケージの削除時に削除されます。新しい SMF サービスによって、システム再始動時の I/O フェンシングドライバのインストールエラーが回避されます。

vxfentsthdw ユーティリティに導入された、ディスクサイズを確認する機能とエラーを無効にするオプション

vxfentsthdw ユーティリティが拡張されて、ディスクのサイズの互換性を確認するようになりました。また、エラーをより適切に評価するための、新しいエラーメッセージも導入されました。このユーティリティでは、サイズ関連のエラーを無効にしてテストを続行するためのオプション（-o）も提供されます。

vxfenswap ユーティリティの hacli の新しいコマンド

vxfenswap ユーティリティがクラスタの他のノードとの通信に使うことができるプロトコル値を指定するために、新しいオプション -p が導入されました。プロトコルのサポート対象値は ssh、rsh、hacli です。

キャンパスクラスタの変更点

複数サイトの管理

SiteAware クラスタ属性を設定すると、キャンパスクラスタで最初のフェールオーバーの決定に使うサイトを作成できます。サイトを定義し、定義したサイトにシステムを追加できます。システムは 1 つのサイトにのみ属すことができます。サイト定義は、VCS、Veritas Operations Manager、VxVM 全体で同じです。同じサイト内部でフェールオーバーするには、接続したアプリケーションを制限するようにサイトの依存関係を定義します。

クラスタにサイトを設定した場合は、サービスグループは別のサイトのホストを選択するまでサイト内部にとどまろうとします。たとえば、2 つのサイト（サイト A とサイト B）があるキャンパスクラスタで、Web、アプリケーション、データベースから成る 3 層のアプリケーションインフラでサービスグループ間のサイトの依存関係を定義し、同じサイト内部のフェールオーバーを制限できます。

サイトと依存関係を定義し、クラスタにサイトを設定するには Veritas Operations Manager 6.0 が必要です。

詳しくは『』を参照してください。

製品名の商標関連の変更

6.1 リリース以降では、Storage Foundation と High Availability Solutions 製品名の商標を変更しました。

表 1-1 に、商標変更した Storage Foundation と High Availability Solutions の製品を示します。

表 1-1 商標変更した Storage Foundation と High Availability Solutions の製品

以前の製品名	シマンテック商標を使った新しい製品名
Veritas Storage Foundation	Symantec Storage Foundation
Veritas Dynamic Multi-Pathing	Symantec Dynamic Multi-Pathing
Veritas Replicator Option	Symantec Replicator Option
Veritas Volume Replicator	Symantec Volume Replicator
Veritas Storage Foundation Cluster File System HA	Symantec Storage Foundation Cluster File System HA
Veritas Storage Foundation for Oracle RAC	Symantec Storage Foundation for Oracle RAC
Veritas Storage Foundation HA	Symantec Storage Foundation HA
Veritas Cluster Server	Symantec Cluster Server
Veritas Disaster Recovery Advisor	Symantec Disaster Recovery Advisor
Veritas Storage Foundation and High Availability Solutions	Symantec Storage Foundation and High Availability Solutions
Veritas High Availability Agent Pack	Symantec High Availability Agent Pack
Veritas File System Software Development Kit	Symantec File System Software Development Kit

次の項目には Symantec への商標変更は適用されません。

- 製品の頭字語
- コマンド名

- エラーメッセージ
- アラートメッセージ
- モジュールとコンポーネント
- 機能名
- Veritas Operations Manager 製品の商標

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 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かぎり、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.22 の「ハードウェア互換性リスト」を参照してください。

p.22 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/TECH211575

Symantec 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

この項では、このリリースのシマンテック社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。現在のアップデートについては、「Symantec Operations Readiness

Tool のインストールとアップグレード」のページを参照してください。
https://sort.symantec.com/land/install_and_upgrade。

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	チップセット
Solaris 10	アップデート 9、10、11	SPARC
Solaris 11	Solaris 11.1 と SRU（Support Repository Updates）11.1.12.5.0 以前	SPARC

このリリース（バージョン 6.1）は、x86-64 アーキテクチャではサポートされていません。

このリリース（バージョン 6.1）は、Solaris 11 オペレーティングシステムの Solaris と Solaris 10のブランドゾーン、Solaris 10 オペレーティングシステムのネーティブブランドゾーンをサポートします。

VCS のサポート対象のソフトウェア

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

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

Oracle Solaris 11

- Storage Foundation 6.1
  - VxVM 6.1 と VxFS 6.1
- Storage Foundation 6.0.3
  - VxVM 6.0.3 と VxFS 6.0.3

Oracle Solaris 10

- Storage Foundation 6.1
  - VxVM 6.1 と VxFS 6.1
- Storage Foundation 6.0.3
  - VxVM 6.0.3 と VxFS 6.0.3

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。

エンタープライズエージェントのサポート対象のデータベースバージョンについては、次のサポート表を参照してください
http://www.symantec.com/business/support/index?page=content&id=DOC4039。

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、OVM 3.0 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 1-3　　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 9、10、11	SPARC
Solaris 11	Solaris 11.1 と SRU（Support Repository Updates）11.1.12.5.0 以前	SPARC

サポートされるエンタープライズエージェント

サポート対象の企業エージェントに対する各エージェントのサポート表について、次のリンクを参照してください。

Oracle	Support matrix for Oracle
DB2	Support matrix for DB2
Sybase	Support matrix for Sybase

詳細については、Symantec Cluster Server の Oracle、DB2、Sybase 用のエージェント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（ Symantec 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。
- CP サーバーとの通信に常に HTTPS を使うので「security」パラメータは非推奨になりました。そのため、/etc/vxfenmode でこのパラメータの有効と無効を切り替えても何の影響もありません。

非推奨属性

このリリースで非推奨の属性を次の表に示します。

表 1-4　　このリリースで非推奨の属性

属性名	エージェントのタイプ
SecondLevelMonitor	Apache **メモ:** SecondLevelMonitor 属性は VCS 6.1 では推奨されなくなりました。代わりに、Apache リソースのタイプのレベルで LevelTwoMonitorFreq 属性を使用できます。
DetailMonitor	Oracle、Sybase **メモ:** 以前のバージョンで詳細監視を有効にしていた VCS を 6.1 に手動でアップグレードした場合、DetailMonitor の値に LevelTwoMonitorFreq の値を設定します。

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 1-5 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 1-5　　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
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らない。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ない。
2991093	HAD の終了時に優先フェンシングノードの重みがデフォルト値にリセットされない。そのノードの高可用性が欠如しているにもかかわらず、ネットワーク分割のシナリオでフェンシングによりそのノードが優先される。
2995937	vxfen が使う優先フェンシングノードの重みのデフォルト値は 1。しかし、サービスグループなしで HAD が開始した場合や、HAD が停止または終了した場合に、ノードの重みが 0（ゼロ）にリセットされる。HAD の終了時に vxfen が優先フェンシングの重みをデフォルト値にリセットするため、HAD の停止時と HAD の強制終了時では異なる優先フェンシングの重みとなる。
3025931	システムの終了時に、GAB サービス停止スクリプトが正常に実行されなかった場合、次の GAB サービスの再ブートがロードに失敗するケースがまれにあります。GAB ドライバはシステムに追加されたままになりますが、モジュールはロードされません。このような場合、GAB ドライバに devlink エントリが作成されず、GAB の設定は失敗します。
2110148	1 つ以上の CP サーバーに登録されたクラスタをインストーラが分割できない。
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る。
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らない。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ない。
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。
3140359	`gabconfig -cx` と `gabconfig -x` 間の競合が原因でポートが起動しない。
3101262	GAB キューが、I/O 転送時のメモリ不足が原因で過負荷になっている。
3218714	GAB はチューニングパラメータの値の変更に関するメッセージをログに記録しない。
2858076	モジュールパラメータ `gab_conn_wait` を変更しても何の影響もない。

インストール関連の解決された問題

表 1-6 インストール関連の解決された問題

インシデント	説明
2873102	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、エラーが表示されることがあります。
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。
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。
2141446	VCS 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、Veritas Operations Manager Server 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ます。

VCS エンジンの解決した問題

表 1-7 は、VCS エンジンに関する解決した問題の一覧です。

表 1-7 VCS エンジンの解決した問題

インシデント	説明
2858188	すでに設定されたグローバルクラスタオプション（GCO）を gcoconfig を使って再設定しようとしても、グローバルクラスタオプションの再設定中はこのコマンドは既存の GCO IP を変更しません。
2941155	GCO 環境でクラスタ障害が宣言された場合、障害が発生したクラスタ上のグループに Symantec Cluster Server（VCS）がオフラインのマークを付けません。
2954319	負荷が高いシステムでは、ロガースレッドが GAB から頻繁に SIGABRT を取得します。ロガースレッドは低い優先度で実行するため、スケジュールされない場合があります。そのため、SIGABRT が処理されず、GAB がマシンにパニックを発生させます。
2736627	IPv6 がシステムで無効になっている場合は、リモートクラスタの状態が INIT のままになり、Icmp ハートビート状態は UNKNOWN のままになります。

インシデント	説明
2848005	CmdServer プロセスを終了した場合、または実行中の VCS クラスタ上で何らかの理由でこのプロセスが停止したため SMF コマンド（たとえば、svcadm disable <service>）で VCS を停止した場合は、CmdServer が停止できないため、VCS SMF サービスが保守状態になります。
3028644	SNMP 設定に何らかの問題がある場合は、Symantec Cluster Server の notifiler プロセスがコアをダンプします。
3042450	親サービスグループがフリーズされていて、online local hard 依存として設定されている場合、このサービスグループがエラーになると、その親サービスグループがオフラインになります。
3079893	Symantec Cluster Server は、サービスグループがオンラインになる間にそのサービスグループ内のリソースにエラーが発生し、そのサービスグループの OnlineRetryLimit と OnlineRetryInterval にゼロ以外の値が設定されている場合は、そのサービスグループをオンラインにするための再試行を実行しません。
3090710	VxFEN ドライバの設定が完了するまでに High Availability Daemon（HAD）が起動し、停止します。
3207663	ユーザーが「hauser -addpriv」コマンドを実行してグループにユーザー特権を設定し、「-group」オプションの代わりにダッシュ（-）を付けずに何らかの文字列を指定した場合は、構文エラーが確認されず、誤った特権が設定されます。
3112608	サービスグループの切り替えの失敗後、リソースはオンラインになれません。
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。
3318764	High Availability Daemon（HAD）実行中に、utmp ファイル（ファイル名が別のオペレーティングシステム（OS）と異なっている）の内容が空の場合に `hastart -version` コマンドを実行すると、checkboot ユーティリティがセグメンテーション違反でエラーとなり、一部のエージェントが失敗する場合があります。

付属エージェントの解決した問題

表 1-8 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 1-8 付属エージェントの解決した問題

インシデント	説明
2989861	`havmconfigsync` コマンドに、コマンドの使い方が誤っているというメッセージが表示されます。
2967536	監視エントリポイントが MonitorProgram 属性でテストコマンドを呼び出して実行可能ファイルかどうかを確認します。デフォルト以外のユーザーでアプリケーションが設定されている場合は、`su - <user> <cmd>` を使ってコマンドが実行されます。これは、コマンドを呼び出すのに `-c` フラグが必要なためであり、`csh` では機能しません。例: `su - <user> -c <cmd>`。
2962270	Apache エージェントにオンライン監視 IMF サポートが必要です。
2979745	MultiNICA でネットワーク接続性の損失を検知できません。
3033290	`engine_A.log` ファイルに不要な zoneadm メッセージがあります。
3005729	どんな場合でも、すでにオンラインとなっているリソースを LDom エージェントの online 機能で停止したり、バインド解除したりしないでください。リソースをオンラインにするための要件を満たしているかどうかをこの関数で確認する必要があります。
3153987	Oracle Solaris では、clean プログラムがゼロ以外の値を戻した場合でも、Application エージェントの clean エントリポイントが正常であると報告されます。
2964772	NFSRestart リソースがオフラインになると、NFSRestart エージェントがローカルコンテナの NFS プロセスを突然停止することがあります。
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。
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。
3039221	シェルに書き込まれた LDom エージェントのエントリポイントが Perl に変換されました。
3028760	オンラインまたはオフラインの操作時に NFSRestart リソースが `statd` や `lockd` などの NFS 処理を開始しません。

AMF に関連する解決した問題

表 1-9 AMF の解決した問題

インシデント	説明
2937673	amfstat のコンテキスト、グループの登録解除、イベント通知で競合状態が発生し、その結果 AMF ドライバでパニックが発生します。
2848009	AMF が一部のイベントについてエージェントに通知しているときにそのエージェントが終了すると、AMF によりノードでパニックが発生する場合があります。
2703641	VRTSamf patch のインストールまたはアンインストール後に amf によって監視される一部のイベントが登録されたままになっていると、VRTSamf patch がインストールまたはアンインストールされます。
3030087	`amfconfig -Uo` コマンドは、AMF によって内部的に開始または設定される IMFD とその他の関数を停止する必要があります。
2954309	AMF 停止スクリプトから AMF を強制的に設定解除し、AMF に対してエージェントが持つ可能性のあるすべての依存関係を削除します。
3090229	vxconfigd デーモンが応答しない場合、ディスクグループ通知で使われる libusnp_vxnotify.so ライブラリが永続的なループに陥ります。これにより、AMF ドライバによるノードのパニックが発生し、AMF が一貫性のない状態になります。
3145047	AMF が VXFS と相互作用する方法により、いずれのマウントがオンラインでない場合でも、AMF はモジュール参照を実際に保持することなしに VXFS ドライバにアクセスできます。したがって、AMF が VXFS にアクセスできる場合でも VXFS のアンロードが可能です。
3133181	AMF ドライバの動作エラーにより、IMFD により AMF に渡された ioctl が AMF 内で動けなくなる場合があります。IMFD の処理はこの ioctl が userspace に戻るまで終了できません。
3018778	`haimfconfig` コマンドを使っているときに Perl エラーが発生します。
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、エラーメッセージがエンジンログに出力されます。
3259682	`vxconfigd` がハングアップすると、`vxconfigd` からディスクグループの状態を取得する imfd の登録スレッドもハングアップします。したがって、IMFD を待機する `amfregister` コマンドが停止します。
3279336	AMF でディスクグループのリソースを登録している場合、AMF を設定解除すると、両方のコンテキストがハングアップ状態になることがあります。

インシデント	説明
3177476	すでにトリガした後で AMF へのプロセスオンライン登録を設定解除すると、コンピュータでパニックが発生します。
3274145	ファイルシステム自体をまだロードしていない場合は AMF をロードしないでください。
3322153	AMF でのイベントの登録と登録解除が競合する場合は、ソフトロックアップが発生し、コンピュータでパニックが起こります。

エンタープライズエージェントの解決した問題

表 1-10 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 1-10 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
1938138	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。
3088915	Oracle プロセスがコンテナ内で実行している場合でも、VCS がコンテナ内に設定された Oracle リソースの状態を OFFLINE として報告します。
2847994	ASMDG エージェントは、デバイス(ボリュームのいずれか)がビジーであることを検出すると、ユーザーコマンドで指示されたとおりにオフラインエントリポイントの終了を遅らせます。ASMDG エージェントの DiskGroup 属性に示された各ディスクグループに対して、エージェントが SQL コマンドを実行し、ディスクグループによって使われているボリュームのリストを取得します。
3240209	Oracle オンライン操作時に、誤ったパターン一致のため、Oracle エージェントがデータベースを不必要にバックアップしようとします。
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。

動作上の解決した問題

表 1-11 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 1-11 動作上の解決した問題

インシデント	説明
3210553	RDC(Replicated Data Cluster)の設定でフェンシングオプションを選択せずにシステムタグを修正した場合、ストレッチサイトのウィザードでタグの修正に失敗します。

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。

VCS のインストールとアップグレードに関する問題

Solaris 10 で JumpStart を使って製品をインストールした場合に、xprtld が起動しない（3325954）

JumpStart 方式を使ってオペレーティングシステムとシマンテック製品をインストールし、インストール後にマシンを再ブートして製品の設定と起動を行うと、xprtld プロセス以外のプロセスはすべて起動します。

回避策:

再ブートの後、次のコマンドを手動で実行して、xprtld を起動します。

```
# /opt/VRTSsfmh/adm/xprtldctrl start
```

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
```

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。

```
lt failed to stop on node_name
gab failed to stop on node_name
```

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

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

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なくなります。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。

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。

手動ライブアップグレードで VRTSvcsea パッケージを代替ディスクからアンインストールできない

説明: 5.1x から 5.1SP1 への手動ライブアップグレード手順では、すべてのパッケージが代替ルートディスクにコピーされます。ただし、VRTSvcsea パッケージを代替ディスクからアンインストールして、このパッケージを 5.1SP1 にアップグレードすることはできません。

回避策: VRTSvcsea パッケージを削除する代わりに、このパッケージを 5.1SP1 バージョンにアップグレードするためのパッチを適用する必要があります。

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。

VCS Zone ユーザーは、VCS 6.0 以降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 以降にアップグレードする場合がこれに該当します。

- 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、『Symantec 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、『Symantec 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。

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。

Solaris 11 で VRTSvcs をアンインストールするとログメッセージが表示される [2919986]

Solaris 11 OS で VRTSvcs パッケージをアンインストールすると次のメッセージが表示されます。

```
The following unexpected or editable files and directories were
salvaged while executing the requested package operation; they
have been moved to the displayed location in the image:

  var/VRTSvcs/log -> /var/pkg/lost+found/var/VRTSvcs/log-20111216T122049Z
  var/VRTSvcs/lock -> /var/pkg/lost+found/var/VRTSvcs/lock-20111216T122049Z
  var/VRTSvcs -> /var/pkg/lost+found/var/VRTSvcs-20111216T122049Z
```

```
  etc/VRTSvcs/conf/config
->/var/pkg/lost+found/etc/VRTSvcs/conf/config-20111216T122049Z
```

これは IPS パッケージの予期された動作であるため、このメッセージを無視しても安全です。上記のメッセージに記載されるファイルはパッケージの一部ではありません。その結果、アンインストールにより、これらのファイルは /var/pkg/lost+found ディレクトリに移動します。

VCS 5.1 から 6.1 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 6.1 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/VRTSvcs/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/VRTSvcs/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 6.1 の VRTSvcsea の完全なインストールの後、/etc/VRTSvcs/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/VRTSvcs/conf/config ディレクトリにコピーしてください。

CP サーバーのセキュアモードで 6.0 より前のバージョンからの VCS ローリングアップグレードに失敗する [3262900]

CP サーバーをセキュアモードで設定している場合は、6.0 より前のバージョンから 6.1 に VCS をローリングアップグレードできません。vxcpserv 処理が共有認証と互換性がないため、CP サーバーサービスグループはローリングアップグレードのフェーズ 1 を実行した後でオンラインにできません。

回避策: ローリングアップグレードではなくフルアップグレードや段階的アップグレードを実行します。

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（セカ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、『Symantec 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_S70llt    framework     NONPERSISTENT
rc2_d_S92gab    framework     NONPERSISTENT
svc:/smf/legacy_run> delpg rc2_d_S70llt
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。

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。

Solaris 10 update 8 または 9 から Solaris 10 update 10 または 11 に OS をアップグレードすると、Samba サーバー、SambaShare エージェント、NetBios エージェントをオンラインにできない [3321120]

Solaris 10 update 8 と update 9 では、Samba バイナリのデフォルトパスは `/usr/sfw/sbin/smbd`、デフォルトの Samba 設定ファイルの場所は `/etc/sfw/smb.conf` です。Solaris 10 update 10 と update 11 では、Samba バイナリのデフォルトパスは `/usr/sbin/smbd` に変更されました。デフォルトの Samba 設定ファイルの場所は `/etc/samba/smb.conf` です。したがって、Solaris 10 update 8 または update 9 から

Solaris 10 update 10 または update 11 に OS をアップグレードすると、Samba サーバー、SambaShare エージェント、NetBios エージェントはバイナリや設定ファイルを検索できません。

回避策: Solaris 10 update 8 または update 9 から Solaris 10 update 10 または update 11 に OS をアップグレードすると、Samba サーバーリソースの SambaTopDir と ConfFile の属性が正しい場所を適切に反映するように更新されます。

CP サーバーの実行中に CP サーバーが HTTPS 仮想 IP またはポートの追加や削除を許可しない [3322154]

CP サーバーは、CP サーバーの実行中に HTTPS 仮想 IP やポートを追加、削除することをサポートしません。ただし、IPM の仮想 IP やポートは追加も削除もできます。

回避策: 回避策はありません。HTTPS に新しい仮想 IP を追加する場合は、『Symantec Cluster Server インストールガイド』に記載されている CP サーバーの HTTPS 証明書（server.crt）を生成する手動の手順をすべて実行する必要があります。

CP サーバーが HTTPS プロトコルを使った IPv6 通信をサポートしない [3209475]

CP サーバーは、HTTPS プロトコルを使っている場合に IPv6 通信をサポートしません。VCS 6.1 では、HTTPS で応答準備する CP サーバーは IPv4 のみを使うことができます。そのため、VCS 6.1 フェンシングクライアントも IPv4 のみを使うことができます。

回避策: 回避策はありません。

VCS カーネルコンポーネントの SMF サービスを新しいブート環境にインストールすると保守状態になることがある [3331801]

VCS を新しいブート環境にインストールし、システムを新しいブート環境でブートすると、VCS カーネルコンポーネントの SMF サービス（LLT、GAB、I/O フェンシング）が保守状態のままでオンラインにならないことがあります。

回避策: SMF サービスの状態を消去し、オンラインにできなかったサービスと、依存関係にあるサービスを手動で有効にします。

複数ノードのクラスタで CP サーバーを 6.0 から 6.1 にアップグレードすると、CP サーバーサービスグループをデフォルトのデータベースパスでオンラインにできない [3326639]

セキュリティを有効にしてアップグレードする前に CP サーバーを複数ノードのクラスタに設定した場合は、CP サーバーをアップグレードしてから CP サーバーを再設定する必要があります。 古いデータベースパスで古いクレデンシャルを再利用すると、CP サーバーサービスグループはオンラインになりません。6.0 と 6.1 では CP サーバーのデフォルトのデータベースパスが異なるので、古いクレデンシャルとデフォルトのデータベース

パスを再利用すると CP サーバーサービスグループをオンラインにすることができません。

回避策: セキュリティを有効にして CP サーバーのマルチノードクラスタを設定した場合や、CP サーバーのアップグレード後にデータベースパスなどの古いクレデンシャルを CP サーバーの再設定で再利用する予定がある場合は、アップグレード前後で同じデータベースパスを使います。

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（1919953）

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 -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。

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、パスワードプロンプト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

グローバルサービスグループ内の 2 つの 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 がグローバルサービスグループ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 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、『Symantec 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)。

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。

スカラー属性に対して -delete -keys を実行するとコアダンプが発生する [3065357]

スカラー属性に対する -delete -keys の実行は有効な操作ではありません。使用しないでください。ただし、このコマンドを偶発的または意図的に使用すると、エンジンにコアダンプが発生する可能性があります。

回避策: 回避策はありません。

クラスタの Statistics が有効になっており、Load と Capacity が定義されていと VCS が admin_wait 状態になる[3199210]

ローカルで開始された VCS は、次の条件が揃うと admin_wait 状態になります。

1. Statistics 属性値がデフォルトの Enabled に設定されている。
2. Group Load および System Capacity の値の単位が `main.cf` で定義されている。

回避策:

1. クラスタ内のすべてのノードで VCS を停止します。
2. 次のいずれかの手順を実行します。
   - クラスタ内のいずれか 1 つのノードの `main.cf` を編集し Statistics 属性を Disabled または MeterHostOnly に設定する。
   - `main.cf` から Group Load および System Capacity の値を削除する。
3. このノードで `hacf -verify` を実行し、設定が有効であることを確認します。
4. このノードで VCS を起動し、その後でクラスタ内の残りのノードで起動します。

VCS を自動的に開始するように設定せず、VCS を開始する前に `utmp` ファイルが空になるとエージェントが誤った状態を報告する [3326504]

再ブート後に VCS を自動的に開始するように設定していない場合に hastart コマンドを実行して VCS を手動で開始する前に `utmp` ファイルを空にすると、一部のエージェントで誤った記述を報告することがあります。

`utmp` ファイル(ファイル名はオペレーティングシステムによって異なる)は、特定のコンピュータで完了した再起動レコードの保守に使用します。`hastart` コマンドが使用する checkboot ユーティリティは OS が提供する関数を使います。次に、`utmp` ファイルを使用して、さまざまなエージェントの一時ファイルを削除してエージェントを起動するために、システムを再起動したかどうかを確認します。OS の関数が正しい値を返さない場合は、古いエージェントファイルを削除せずに HAD (High Availability Daemon)を開始します。これにより、一部のエージェントが正しくない状態を報告する場合があります。

回避策: ユーザーが `utmp` ファイルを削除する場合は、VCS をすでに動作しているか、またはユーザーが VCS を開始する前に `/var/VRTSvcs/lock/volatile/` の一時ファイルを手動で削除する必要があるときにのみ実行してください。

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ます。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。

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スクリプトを使用している間変わるパスワードはすべてのゾーン[2332349]適用されません

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。

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。

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こります。

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、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。

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
```

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。

NFS クライアントでネットワークスプリットブレインによる I/O エラーが報告される [3257399]

ネットワークスプリットブレインが起きると、エラーが発生したノードがパニックになることがあります。 結果として、一部のリソース(IP リソースなど)がエラーが発生したノードでオンラインのままになっているためフェールオーバーノードのサービスグループがオンライン

になれない場合があります。エラーが発生しているノードのディスクグループも無効になる可能性がありますが、同じノードの IP リソースはオンラインのままになります。

回避策: サービスグループ内の各システムの予約された DiskGroup リソースを含むサービスグループに対し、preonline トリガを設定してください。

1 preonline_ipc トリガを /opt/VRTSvcs/bin/sample_triggers/VRTSvcs から /opt/VRTSvcs/bin/triggers/preonline/ に T0preonline_ipc としてコピーします。

```
# cp /opt/VRTSvcs/bin/sample_triggers/VRTSvcs/preonline_ipc
/opt/VRTSvcs/bin/triggers/preonline/T0preonline_ipc
```

2 サービスグループに対して preonline トリガを有効にします。

```
# hagrp -modify <group_name> TriggersEnabled
PREONLINE -sys <node_name>
```

システムが読み込まれた場合、エージェントが動かなくなるか、コマンドの処理に時間がかかる[3323253]

エージェントが動作しているシステムが読み込まれた場合、そのエージェントが動かなくなったり、コマンドの処理に時間がかかります。

回避策: 次のコマンドを使って、エージェントの NumThreads の値を「1」に設定します。

```
# hatype -modify <Agent> NumThreads 1
```

1 つ以上のコーディネーションディスクとストレージアレイとの接続を切断または再確立した後に、CoordPoint エージェントがエラーになる（3317123）

ストレージアレイとコーディネーションディスクとの接続を切断または再確立した後に、CoordPoint エージェントがエラーになることがあります。これは、エージェントが、I/O フェンシングカーネルモジュールに格納されている古い値を読み取るためです。

回避策: vxfenswap ユーティリティを実行して、サーバーベースの I/O フェンシングとディスクベースの I/O フェンシングの両方のコーディネーションポイントの登録キーを更新します。ただし、登録キーが失われない場合でも、vxfenswap ユーティリティを実行して、I/O フェンシングカーネルモジュールに格納されているコーディネーションポイント情報を更新する必要があります。

サーバーベースとディスクベースの I/O フェンシングのコーディネーションポイントの登録キーを更新する方法について詳しくは、『Symantec Cluster Server 管理者ガイド』を参照してください。

Mount リソースが MountPoint と BlockDevice の属性値のスペースをサポートしない [3335304]

Mount リソースは、設定済みの MountPoint や BlockDevice の属性値の中にあるスペースを扱いません。

回避策: 回避策はありません。

VCS データベースエージェントに関する問題

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 Symantec 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『Symantec Cluster Server Agent for Oracle インストール/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。

複数のリソースを含むノードで VCS コマンドへの遅延応答が発生し、システムの CPU 使用率またはスワップの使用状況が高くなる [3208239]

VCS ノードで監視するために大量のリソースを設定した場合に、CPU 使用率が 100% に近い、またはスワップの使用状況が非常に高い場合、コマンドへの VCS 応答に数分の遅延が発生することがあります。

一部のコマンドは次のように記述されます。

- `# hares -online`
- `# hares -offline`
- `# hagrp -online`
- `# hagrp -offline`
- `# hares -switch`

遅延は、関連する VCS エージェントがコマンドの処理に十分な CPU の帯域幅を取得できないために発生します。エージェントは、大量の保留中の内部コマンド（各リソースの定期的な監視など）を処理するためにビジー状態である場合もあります。

回避策: システムの CPU 負荷が通常に戻った後に、問題のある一部の VCS エージェントタイプ属性の値を変更して、元の属性値を復元します。

1 IMF 属性の MonitorInterval、OfflineMonitorInterval、MonitorFreq などの属性の元の値をバックアップします。

2 エージェントで IMF（Intelligent Monitoring Framework）がサポートされていない場合、MonitorInterval 属性と OfflineMonitorInterval 属性の値を増やします。

```
# haconf -makerw
# hatype -modify <TypeName> MonitorInterval <value>
# hatype -modify <TypeName> OfflineMonitorInterval <value>
# haconf -dump -makero
```

<TypeName> は遅延が発生しているエージェント名で、<value> は環境に適切な数値です。

3 エージェントで IMF がサポートされている場合、IMF の MonitorFreq 属性の値を増やします。

```
# haconf -makerw
# hatype -modify <TypeName> IMF -update MonitorFreq <value>
# haconf -dump -makero
```

<value> は、環境に適切な数値です。

4 数分待って VCS が保留中のコマンドをすべて実行したことを確認してから、新しい VCS コマンドを実行します。

5 遅延が解決されない場合、手順 2 または 3 を必要に応じて繰り返します。

6 CPU 使用率が通常の限度に戻ったら、リソースのエラー検出の遅延を避けるため、変更した属性をバックアップされている値に戻します。

CFSMount エージェントが VCS エンジンにハートビートを送信できないことがあり、システムのエンジンログにメモリの負荷が高いことを示すエラーメッセージが記録される [3060779]

メモリの負荷が高いシステムでは、CFSMount エージェントが VCS エンジンにハートビートを送信できないことがあり、エンジンログに V-16-1-53030 エラーメッセージが記録されます。

VCS エンジンは、システムでエージェントが正しく動作していること確認するために CFSMount エージェントから定期的にハートビートを受信する必要があります。ハートビートは AgentReplyTimeout 属性によって決まります。CPU 使用率やメモリ作業負荷が高い（たとえば、スワップ使用率が 85 %を超える）ことが原因で、エージェントがスケジュールに十分な CPU サイクルを確保できないことがあります。そのため、VCS エンジンがハートビートを受信できず、エージェントを切断して新しいエージェントを開始します。これは、エンジンログの次のエラーメッセージで確認できます。

```
V-16-1-53030 Termination request sent to CFSMount
agent process with pid %d
```

回避策: AgentReplyTimeout 値を大きくして CFSMount エージェントが安定したかどうかを確認します。それでも問題が解決しない場合は次の回避策を試します。次のコマンドを実行して CFSMount エージェントの NumThreads 属性値を 1 に設定します。

```
# hatype -modify CFSMount NumThreads 1
```

このコマンドを実行しても CFSMount エージェントが切断されたままの場合は、シマンテック社のサポートチームに報告してください。

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 SFCFSHA Live Upgrade を実行すると、次のエラーメッセージを出して失敗します。

```
ERROR: Installation of the packages from this media of the media failed;
pfinstall returned these diagnostics:
Processing default locales
        - Specifying default locale (en_US.ISO8859-1)
Processing profile
ERROR: This slice can't be upgraded because of missing usr packages for
the following zones:
ERROR:    zone1
ERROR:    zone1
ERROR: This slice cannot be upgraded because of missing usr packages for
```

```
one or more zones.
The Solaris upgrade of the boot environment <dest.27152> failed.
```

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

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

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 6.1 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を使用して表示される文字を各国化するシステムメッセージは正しく表示されないかもしれません

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
- -hamultinicb
- -haipswitch

回避策: 回避策はありません。

gcoconfig ウィザードで英語のエラーメッセージが表示される［3018221］

gcoconfig ウィザードが内部からコマンドを呼び出しているかどうかにかかわらず、コマンドのメッセージが英語で表示されます。

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 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。

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

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

Solaris 11 で高速リンクエラー検出がサポートされない（2954267）

高速リンクエラー検出は、Solaris 11 オペレーティングシステムではサポートされません。これは、Solaris 11 オペレーティングシステムでは、リンクエラーが発生した場合、LLT への通知呼び出しを提供できないためです。オペレーティングシステムのカーネルがリンクエラーについて LLT へ通知した場合、LLT は、通常のリンクエラー検出サイクルよりもはるかに早く、リンクエラーを検出できます。Solaris 11 では LLT へリンクエラーが通知されないため、通常の検出サイクルまで、エラーが検出されません。

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。

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、『Symantec 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 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 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
```

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［3226290］

この問題は、VCS 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。ただし、VCS 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、サーバーとクライアントシステムがセキュアモードで通信できるようにしてください。

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。

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。

CP サーバープロセスの vxcpserv が、CP サーバープロセスの起動時に利用可能であった VIP のクライアントノードとしか通信しない（3156922）

CP サーバーを構成する際、CPSSG サービスグループは vxcpserv プロセス（CP サーバープロセス）とその依存関係（クォーラムリソース）を管理するよう構成されます。CP サーバーはプロセスエージェントによって管理され、依存する仮想 IP アドレス（VIP）はクォーラムリソースによって管理されます。クォーラムリソースは VIP のクォーラムを達成したときだけオンラインになります。

VCS が CPSSG グループをオンラインにするとき、vxcpserv プロセスは、クォーラムリソースがオンラインになる前に起動した VIP のみに応答します。vxcpserv は、クォーラムリソースがオンラインになった後で起動したとしてもそれらの VIP に応答しません。したがって、CP サーバープロセスは CP サーバープロセスの起動時に利用可能であった VIP としか通信しません。

netstat コマンドをプラットフォーム固有のフラグと共に発行することにより vxcpserv プロセスに応答する VIP の一覧を取得することができます。

回避策: 次のコマンドを使用して vxcpserv リソースの下で構成された CP サーバーを再起動します

```
# hares -offline vxcpserv -sys <system >
```

```
# hares -online vxcpserv -sys <system >
```

ここで、<system> は GPSSG グループがオンラインであるノードを示しています。

vxfenswap ユーティリティを hacli オプションで実行すると、コメント行が /etc/vxfemode ファイルから削除される（3318449）

vxfenswap ユーティリティは、クラスタ内のピアノードとの通信に RSH、SSH、または hacli プロトコルを使います。ディスクベースのフェンシングでコーディネーションディスクを置換するのに vxfenswap を使うと、vxfenswap は /etc/vxfenmode（リモートノード）に /etc/vxfenmode（ローカルノード）をコピーします。

hacli オプションを指定すると、ユーティリティはリモートの /etc/vxfenmode ファイルからコメント行を削除しますが、ローカルの /etc/vxfenmode ファイルのコメントは維持します。

回避策: ローカルの /etc/vxfenmode からリモートノードにコメントを手動でコピーします。

HTTPS ベースの通信のみに CP サーバーを設定すると、engine_A.log で紛らわしいメッセージが表示される（3321101）

CP サーバーを HTTPS ベースの通信のみに設定し、IPM ベースの通信には設定しなかった場合、engine_A.log ファイルに次のメッセージが表示されます。

```
No VIP for IPM specified in /etc/vxcps.conf
```

回避策: このメッセージは無視してください。

vxfentsthdw ユーティリティが部分的な SFHA スタックを使ってインストールしたシステムで動作しないことがある [3333914]

vxfentsthdw ユーティリティは、適切に設定された SF と VxVM を使って SFHA スタックと VCS が完全にインストールされている場合に動作します。また、SFHA スタック全体と VCS がインストールされていない場合にも、動作します。しかし、SF はインストールされ、設定されているが、VCS はインストールされていないという、部分的インストールはサポートされません。このユーティリティでは、-g オプションまたは -c オプションでエラーが表示されます。

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。

オンラインサービスグループで SysDownPolicy が AutoDisableNoOffline に設定されている場合、フェンシングの設定が失敗する [3335137]

1 つ以上のオンラインサービスグループの SysDownPolicy を AutoDisableNoOffline に設定している場合は、サーバーベース、ディスクベース、無効モードなどのフェンシング設定が失敗します。サービスグループを `SysDownPolicy = { AutoDisableNoOffline }` と設定しているので、VCS を停止するとフェンシング設定に失敗します。

回避策: VCS を停止する前にフェンシングを設定した場合は、`SysDownPolicy = { AutoDisableNoOffline }` で、手動で設定したサービスグループをオフラインにする必要があります。

ノードのパニックなどが原因でクライアントノードが停止したときにノードを再起動すると、そのクライアントノードで I/O フェンシングが起動しない（3341322）

この問題は、次の状況に 1 つでも当てはまると起きます。

- HTTPS 通信を設定したいずれかの CP サーバーが停止する
- HTTPS 通信を設定したいずれかの CP サーバーの CP サーバーサービスグループが停止する
- HTTPS 通信を設定したいずれかの CP サーバーで VIP が停止する

クライアントノードを再起動すると、ノードでフェンシング設定を開始します。フェンシングデーモン vxfend は、ノードで一部のフェンシングスクリプトを呼び出します。これらのスクリプトそれぞれに 120 秒のタイムアウト値が設定されています。これらのスクリプトに失敗すると、そのノードのフェンシング設定は失敗します。

一部のスクリプトは `cpsadm` コマンドを使って CP サーバーと通信します。ノードを起動すると、`cpsadm` コマンドが、60 秒のタイムアウト値が設定された VIP を使って CPサーバーに接続します。したがって、単一スクリプト内部で実行する複数の `cpsadm` コマンドがタイムアウト値を超え、合計タイムアウト値が 120 秒を超えると、いずれかのスクリプトがタイムアウトします。そのため、I/O フェンシングはクライアントノードで起動しません。

CP サーバーとクライアントクラスタ間の IPM ベースの通信ではこの問題は起きません。

回避策: CP サーバーを修正します。

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。

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。

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。

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。

Apache エージェントが無効のとき、VCS エンジンが reaper のキャンセルに関するエラーを表示する[3043533]

1 つ以上のエージェントで haimfconfig スクリプトを使用して IMF を無効にすると、VCS エンジンがエンジンログに次のメッセージを記録します。

```
AMF imf_getnotification ERROR V-292-2-193
Notification(s) canceled for this reaper.
```

これは期待される動作であり問題ではありません。

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。

エージェントディレクトリとエージェントファイルを設定しているエージェントを IMF 対応にできない [2858160]

エージェントディレクトリとエージェントファイルを設定しているエージェントは IMF 対応にはできません。

回避策: 回避策はありません。

すでに登録解除されているリソースの登録解除要求を受信すると AMF がシステムをパニックにする [3333913]

AMF で内部エラーが起きた場合は、サポート対象外のすべてのリソースを登録解除します。このような事象で、エージェントがこのようなリソースのいずれかの登録解除を呼び出すと、AMF がコンピュータをパニックにすることがあります。

回避策: 回避策はありません。

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（2718943）

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。

ライブ移行に関する問題

ライブ移行に関する問題は、次のとおりです。

複数の IO サービスを含むゲストドメインのオペレーティングシステムは、ゲストが移行するとハングする [3127470]

ゲストドメインがプライマリドメインからではなく複数の IO ドメインの IO サービスから提供され、別のノードに移行されてソースノードに戻されると、ゲストドメイン内のオペレーティングシステムがハングします。

回避策: 物理システムのファームウェアが最新バージョンにアップグレードされていることを確認してください。

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.84 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 の制御下に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（2162929）

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。

キャンパスクラスタファイアドリルは、DSM サイトがサイト境界のマーク付けに使用される場合に機能しない [3073907]

キャンパスクラスタファイアドリルエージェントは現在、サイト境界の識別に SystemZones 属性を使用します。そのため、キャンパスクラスタファイアドリルは、DSM が有効な環境でサポートされていません。

回避策: DSM を無効にし、アプリケーションサービスグループで SystemZones 属性を設定して、ファイアドリルを実行します。

VCS エンジンに関する制限事項

複数のグループで障害が発生すると、負荷の統合と最適化が失敗する [3074299]

複数のグループで同時に障害が発生し、フェールオーバーすると、ターゲットシステムを選択するための負荷の統合と最適化は行われません。

回避策: 回避策はありません。

優先フェンシングが、予測される利用可能な処理能力を無視する [3077242]

VCS の優先フェンシングでは、フェンシングデシジョンに対して予測される利用可能な処理能力が考慮されません。フェンシングデシジョンは、設定されたシステムの重みに基づいています。

回避策: 回避策はありません。

BiggestAvailable ポリシーが設定されると、SystemZone またはサイト内でフェールオーバーが発生する [3083757]

BiggestAvailable フェールオーバーポリシーが設定されると、SytemZone またはサイト内で常にフェールオーバーが発生します。フェールオーバーのターゲットシステムは常に、SystemZone 内の最も大きい利用可能システムに基づいて選択されます。

回避策: 回避策はありません。

Priority グループの負荷が、同じグループ内の BiggestAvailable および Priority を含むグループで無視される [3074314]

同じクラスタにフェールオーバーポリシーとして BiggestAvailable と Priority を含むグループがある場合、Priority グループの負荷が考慮されません。

回避策: 回避策はありません。

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 [1234959]

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。

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と、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。

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 [1919329]

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。

- DiskGroupSnap リソースに対して Bronze 設定を使う場合は、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。
  - 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、『Symantec 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、『Symantec 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 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 6.1 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

Storage Foundation and High Availability Solutions 製品ラインの各製品には、リリースノート、インストールガイド、そして管理およびエージェントに関するガイドなどのその他のマニュアルが含まれています。またほとんどの場合、製品のコンポーネントに関するマニュアルを参照する必要があります。

SFHA Solutions マニュアルは製品ライン全体に適用される機能およびソリューションを説明しています。これらのマニュアルはどの SFHA Solutions 製品にも関係があります。

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。

Symantec Cluster Server のマニュアル

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

表 1-12 Symantec Cluster Server のマニュアル

マニュアル名	ファイル名	説明
Symantec Cluster Server リリースノート	vcs_notes_61_sol.pdf	製品のシステム必要条件、変更、修正されたインシデント、既知の問題、制限事項などのリリース情報を提供します。
Symantec Cluster Server インストールガイド	vcs_install_61_sol.pdf	製品をインストールするために必要な情報を提供します。
Symantec Cluster Server 管理者ガイド	vcs_admin_61_sol.pdf	製品を管理するために必要な情報を提供します。
Symantec Cluster Server Bundled Agents リファレンスガイド	vcs_bundled_agents_61_sol.pdf	付属エージェント、そのリソースおよび属性、その他の関連情報を提供します。
Symantec 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参照できます。)	vcs_agent_dev_61_unix.pdf	さまざまなシマンテック社のエージェントについての情報およびカスタムエージェントを開発するための手順を説明しています。
Symantec Cluster Server アプリケーションノート: Dynamic Reconfiguration for Oracle Servers (このマニュアルはオンラインでのみ参照できます。)	vcs_dynamic_reconfig_61_sol.pdf	Oracle サーバーの VCS クラスタシステムドメインに動的再設定操作を実行する方法について説明します。
Symantec Cluster Server Agent for DB2 インストールおよび設定ガイド	vcs_db2_agent_61_sol.pdf	DB2 エージェントをインストールし、設定するための情報を提供します。

マニュアル名	ファイル名	説明
Symantec Cluster Server Agent for Oracle インストールおよび設定ガイド	vcs_oracle_agent_61_sol.pdf	Oracle エージェントをインストールし、設定するための情報を提供します。
Symantec Cluster Server Agent for Sybase インストールおよび設定ガイド	vcs_sybase_agent_61_sol.pdf	Sybase エージェントをインストールし、設定するための情報を提供します。

Symantec Storage Foundation and High Availability Solutions 製品のマニュアル

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

表 1-13 Symantec 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	説明
Symantec Storage Foundation and High Availability Solutions - このリリースでの新機能 (このマニュアルはオンラインで参照できます。)	sfhas_whats_new_61_unix.pdf	このリリースの新しい機能および拡張についての情報を提供します。
Symantec Storage Foundation and High Availability Solutions スタートガイド	getting_started.pdf	Veritas スクリプトベースのインストーラを使った Symantec 製品のインストールに関する概要を提供します。このガイドは新しいユーザーや製品を再び使用するユーザーが手短に使い方を習得するのに便利です。
Symantec Storage Foundation and High Availability Solutions ソリューションガイド	sfhas_solutions_61_sol.pdf	SFHA Solutions 製品のコンポーネントや機能を別々に、および連携して使用することで、どのようにパフォーマンスと耐障害性が向上し、ストレージやアプリケーションの管理が容易になるかを説明します。
Symantec Storage Foundation and High Availability Solutions 仮想化ガイド (このマニュアルはオンラインで参照できます。)	sfhas_virtualization_61_sol.pdf	Symantec Storage Foundation and High Availability の仮想化テクノロジのサポートに関する情報を提供します。仮想化ソフトウェアを SFHA 製品を実行しているシステムにインストールする前にこのマニュアル全体を参照してください。

マニュアル名	ファイル名	説明
Symantec Storage Foundation and High Availability Solutions ディザスタリカバリ実装ガイド (このマニュアルはオンラインで参照できます。)	sfhas_dr_impl_61_sol.pdf	キャンパスクラスタ、グローバルクラスタ、Storage Foundation and High Availability Solutions 製品を使用したディザスタリカバリフェールオーバーの RDC(Replicated Data Cluster)に関する情報を提供します。
Symantec Storage Foundation and High Availability Solutions トラブルシューティングガイド	sfhas_tshoot_61_sol.pdf	Symantec Storage Foundation and High Availability を使用するときに発生する可能性のある一般的な問題を説明し、これらの問題の解決法を提供します。

Symantec ApplicationHA のマニュアル

表 1-14 は Symantec ApplicationHA に関するマニュアルのリストです。

表 1-14 Symantec ApplicationHA のマニュアル

マニュアル名	ファイル名	説明
Symantec ApplicationHA リリースノート	applicationha_notes_61_ldom_sol.pdf	新しい機能、ソフトウェアおよびシステムの必要条件を説明します。また、このマニュアルにはリリース時における制限事項と既知の問題の一覧が掲載されています。
Symantec ApplicationHA インストールガイド	applicationha_install_61_ldom_sol.pdf	Symantec Cluster Server をインストールし、設定する手順を説明します。いくつかの最も一般的なトラブルシューティング手順についても説明します。
Symantec ApplicationHA ユーザーズガイド	applicationha_users_61_ldom_sol.pdf	Oracle VM Server for SPARC (OVM) 仮想化環境で Symantec Cluster Server を設定し管理する方法について説明します。いくつかの最も一般的なトラブルシューティング手順についても説明します。
Symantec ApplicationHA Agent for Oracle 設定ガイド	applicationha_oracle_agent_61_ldom_sol.pdf	Oracle のアプリケーション監視を設定する方法について説明します。
Symantec ApplicationHA 汎用エージェント設定ガイド	applicationha_gen_agent_61_ldom_sol.pdf	汎用アプリケーションのアプリケーション監視を設定する方法について説明します。

マニュアル名	ファイル名	説明
Symantec Cluster Server Agent for Apache HTTP Server 設定ガイド	applicationha_apache_agent_61_ldom_sol.pdf	Apache HTTP Server のアプリケーション監視を設定する方法について説明します。

Veritas Operations Manager (VOM) は Symantec Storage Foundation and High Availability Solutions 製品を管理するために使用する管理ツールです。VOM を使用する場合は、次より VOM 製品マニュアルを参照してください。

https://sort.symantec.com/documents

マニュアルページ

Symantec 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 Symantec 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。

最新の HTML 形式のマニュアルページが、シマンテック社の Web サイトの次の URL からオンラインで参照できます。

https://sort.symantec.com/documents