Veritas™ Cluster Server 版本说明

Linux

6.0

Symantec

Veritas™ Cluster Server 版本说明

本手册所述软件是根据许可协议而提供，仅可按该协议的条款使用。

产品版本： 6.0

文档版本： 6.0.0

法律声明

Copyright © 2012 Symantec Corporation. © 2012 Symantec Corporation 版权所有。All rights reserved. 保留所有权利。

Symantec、Symantec 徽标、Veritas、Veritas Storage Foundation、CommandCentral、NetBackup、Enterprise Vault 和 LiveUpdate 是 Symantec Corporation 或其附属公司在美国和其他国家/地区的商标或注册商标。“Symantec”和“赛门铁克”是 Symantec Corporation 在中国的注册商标。其他名称可能为其各自所有者的商标，特此声明。

本文档中介绍的产品根据限制其使用、复制、分发和反编译/逆向工程的授权许可协议分发。未经 Symantec Corporation（赛门铁克公司）及其特许人（如果存在）事先书面授权，不得以任何方式任何形式复制本文档的任何部分。

本文档按“现状”提供，对于所有明示或暗示的条款、陈述和保证，包括任何适销性、针对特定用途的适用性或无侵害知识产权的暗示保证，均不提供任何担保，除非此类免责声明的范围在法律上视为无效。Symantec Corporation（赛门铁克公司）不对任何与提供、执行或使用本文档相关的伴随或后果性损害负责。本文档所含信息如有更改，恕不另行通知。

根据 FAR 12.212 中的定义，授权许可的软件和文档被视为“商业计算机软件”，受 FAR 第 52.227-19 节“Commercial Computer Software - Restricted Rights”（商业计算机软件受限权利）和 DFARS 第 227.7202 节“Rights in Commercial Computer Software or Commercial Computer Software Documentation”（商业计算机软件或商业计算机软件文档权利）中的适用规定，以及所有后续法规中规定的权利的制约。美国政府仅可根据本协议的条款对授权许可的软件和文档进行使用、修改、发布复制、执行、显示或披露。

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

技术支持

Symantec 技术支持具有全球性支持中心。技术支持的主要任务是响应有关产品特性和功能的特定查询。技术支持小组还负责编写我们的联机知识库文章。技术支持小组与 Symantec 内的其他职能部门相互协作，及时解答您的问题。例如，技术支持小组与产品工程和 Symantec 安全响应中心协作，提供警报服务和病毒定义更新服务。

Symantec 提供的维护服务包括：

- 一系列支持服务，使您能为任何规模的单位选择适用的支持服务
- 通过电话和 Web 支持快速响应并提供最新信息
- 升级保证可保证软件顺利升级
- 全天候提供全球支持
- 高级功能，包括“客户管理服务”

有关 Symantec 维护计划的更多信息，请访问我们的网站：

http://www.symantec.com/zh/cn/support/index.jsp

与技术支持联系

具有有效维护协议的客户可以通过以下网址访问技术支持信息：

http://www.symantec.com/zh/cn/support/index.jsp

在联系技术支持之前，请确保您的计算机符合产品文档中所列的系统要求。而且您应当坐在发生问题的计算机旁边，以便需要时重现问题。

联系技术支持时，请准备好以下信息：

- 产品版本信息
- 硬件信息
- 可用内存、磁盘空间和 NIC 网卡信息
- 操作系统
- 版本和补丁程序级别
- 网络结构
- 路由器、网关和 IP 地址信息
- 问题说明：
  - 错误消息和日志文件
  - 联系 Symantec 之前执行过的故障排除操作

- 最近所做的软件配置更改和网络更改

授权许可与产品注册

如果您的 Symantec 产品需要注册或许可证密钥，请访问我们的技术支持网页：

https://licensing.symantec.com/

客户服务

可从以下网站获得客户服务信息：

http://www.symantec.com/zh/cn/support/index.jsp

客户服务可帮助您解决一些非技术性问题，例如以下几类问题：

- 有关产品许可或序列号的问题
- 产品注册更新（例如，更改地址或名称）
- 一般产品信息（功能、可用的语言、当地经销商）
- 有关产品更新和升级的最新信息
- 有关升级保障和维护合同的信息
- Symantec 采购计划的相关信息
- 有关 Symantec 技术支持选项的建议
- 非技术性的售前问题
- 与光盘或手册相关的问题

维护协议资源

如果想就现有维护协议事宜联络 Symantec，请通过以下方式联络您所在地区的维护协议管理部门：

国家/地区	销售热线	电子邮件
中国大陆	800 810 8826	China-Sales@symantec.com
中国台湾	0080 1611 391	Taiwan-Sales@symantec.com
中国香港特别行政区	800 963 421	HongKong-Sales@symantec.com

文档

介质中提供了PDF格式的产品指南。请确保您使用的是文档的最新版本。每个指南的第 2 页提供了文档版本信息。从 Symantec 网站可以获取最新的产品文档。

https://sort.symantec.com/documents

您对产品文档的反馈对我们很重要。请发送改进建议和有关错误或疏漏的报告。请在您的报告中包括所报告的文本内容的文档标题和文档版本（位于第二页上）以及章节标题。请将反馈发送到：

doc_feedback@symantec.com

关于 Symantec Connect

Symantec Connect 是为 Symantec 企业客户提供的点对点技术社区网站。参与者可以与其他产品用户联络并共享信息，包括创建论坛帖子、文章、视频、下载、博客和提出建议，并可与 Symantec 产品团队和技术支持进行交流。内容会由社区进行评分，成员可凭其贡献获得奖励积分。

http://www.symantec.com/connect/storage-management

其他企业服务

Symantec 全面提供各种服务以使您能够充分利用您对 Symantec 产品的投资，并拓展您的知识、技能和全球视野，让您在管理企业安全风险方面占据主动。

现有下列企业服务：

安全托管服务	托管服务消除了管理和监控安全设备和事件的负担，确保能够对实际威胁快速响应。
咨询服务	Symantec 咨询服务由 Symantec 及其可信赖的合作伙伴提供现场专业技术指导。Symantec 咨询服务提供各种预先包装和可自定义的服务选项，其中包括评估、设计、实施、监控和管理功能。每种功能都注重于建立和维护您的 IT 资源的完整性和可用性。
教育服务	教育服务提供全面的技术培训、安全教育、安全认证和安全意识交流计划。

要访问有关企业服务的更多信息，请通过以下 URL 访问我们的网站：

http://www.symantec.com/zh/cn

Veritas Cluster Server 版本说明

本文档包含以下主题：

关于本文档

本文档提供有关适用于 Linux 的 Veritas Cluster Server (VCS) 版本 6.0 的重要信息。请在安装或升级 VCS 之前仔细阅读整个文档。

“版本说明”中的信息可取代 VCS 的产品文档中提供的信息。

本《Veritas Cluster Server 版本说明》是文档版本：6.0.0。开始之前，请确保使用的是本指南的最新版本。Symantec 网站上提供了最新的产品文档，网址为：

https://sort.symantec.com/documents

组件产品版本说明

除阅读本版本说明文档外，在安装产品前，还请查看组件产品的版本说明。

软件介质上的以下位置提供了 PDF 格式的产品指南：

/product_name/docs

Symantec 建议将这些文件复制到系统上的 /opt/VRTS/docs 目录中。

此版本包括下列组件产品的版本说明：

- 《Veritas Storage Foundation 版本说明 (6.0)》

关于 Veritas Cluster Server

由 Symantec 出品的 Veritas™ Cluster Server (VCS) 为在物理环境和虚拟环境中运行的任务关键型应用程序提供高可用性 (HA) 和灾难恢复 (DR)。VCS 可确保即使出现应用程序、基础架构或站点故障，应用程序也会持续可用。

关于 VCS 代理

VCS 捆绑代理管理集群的主要资源。捆绑代理的实现和配置因平台而异。

有关捆绑代理的更多信息，请参考《Veritas Cluster Server Bundled Agents 参考指南》。

通过 Veritas High Availability Agent Pack 可访问为各种应用程序、数据库和第三方存储解决方案提供高可用性的代理。Agent Pack 可通过 Symantec™ Operations Readiness Tools (SORT) 获取。有关 SORT 的更多信息，请参见 https://sort.symantec.com/home。有关正在开发的代理和可通过 Symantec 咨询服务获得的代理的信息，请与您的 Symantec 销售代表联系。

VCS 提供了允许创建自定义代理的框架。在 Veritas High Availability Agent Pack、捆绑代理或 Enterprise Agent 不能满足您需求的情况下，可创建代理。

有关创建自定义代理的更多信息，请参考《Veritas Cluster Server Agent 开发指南》。还可以通过 Symantec 咨询服务请求自定义代理。

关于 Symantec Operations Readiness Tools

Symantec Operations Readiness Tools (SORT) 是一个网站，可自动处理和简化某些最耗时的管理任务。SORT有助于您更高效地管理数据中心，并充分利用Symantec产品。

SORT 可以帮助您执行以下操作：

为下一次安装或升级做准备	■ 列出产品安装和升级要求，包括操作系统版本、内存、磁盘空间和体系结构。 ■ 分析系统以确定是否已做好安装或升级 Symantec 产品的准备。 ■ 从中央储存库下载最新的修补程序、文档和高可用性代理。 ■ 访问硬件、软件、数据库和操作系统的最新兼容性列表。
管理风险	■ 从中央储存库获取有关对修补程序、阵列特定模块 (ASL/APM/DDI/DDL) 和高可用性代理所做更改的自动电子邮件通知。 ■ 确定并降低系统和环境风险。 ■ 显示数百个 Symantec 错误代码的说明和解决方案。
提高效率	■ 根据产品版本和平台查找并下载修补程序。 ■ 列出已安装的 Symantec 产品和许可证密钥。 ■ 调整并优化您的环境。

注意：SORT 的某些功能并非对所有产品都可用。访问 SORT 不需要额外费用。

要访问 SORT，请转到：

https://sort.symantec.com

重要版本信息

- 有关此版本的重要更新，请查看Symantec技术支持网站上最新发布的新闻和技术说明：
  http://www.symantec.com/docs/TECH164885
- 有关此版本可用的最新修补程序，请转到：
  http://sort.symantec.com/

- 硬件兼容性列表中包含有关所支持硬件的信息，该列表会定期更新。有关所支持硬件的最新信息，请访问以下 URL：
  http://www.symantec.com/docs/TECH170013
  在安装或升级 Storage Foundation and High Availability Solutions 产品之前，请查看最新的兼容性列表，以确认硬件和软件的兼容性。

6.0 中引入的更改

本节列出了 Veritas Cluster Server 6.0 的更改。

与安装和升级相关的更改

在 6.0 中，产品安装程序的更改如下。

在 Linux 上支持使用 yum 进行产品安装

现在，您可以使用 yum 安装任何 Veritas 产品。Red Hat Enterprise Linux 5 和 6 支持 Yum 安装。

有关详细信息，请参见“安装指南”。

安装程序现在可以检测重复的 VCS 集群 ID，并可以自动生成集群 ID

安装程序现在可以检测重复的 VCS 集群 ID，并提示您选择未使用的 VCS 集群 ID。它还可以在安装期间生成未使用的 ID。

安装程序可以检查产品版本和修补程序

在安装之前或之后，您可以使用带有 `-version` 选项的 installer 命令检查现有产品的版本。安装当前版本的产品后，可以使用/opt/VRTS/install 目录中的 `showversion` 脚本查找版本信息。

通过这些命令可以查找以下信息：

- 所有已发行 Storage Foundation and High Availability Suite 产品的已安装版本
- 缺少的必备RPM或修补程序（因平台而异）
- SORT 提供的已安装产品的可用更新（包括修补程序）

该脚本可以识别 4.0 及更高的版本，视具体产品而定。

使用安装程序的 postcheck 选项

可以使用安装程序的 postcheck 选项来诊断安装相关问题并提供故障排除信息。

滚动升级方面的改进

滚动升级过程已得到简化。

软件包更新

下面列出了此版本中的软件包更改。

- 新增了用于产品安装程序脚本的 VRTSsfcpi60 RPM
  此版本中引入了 VRTSsfcpi60 RPM。VRTSsfcpi60 RPM包含安装程序用于安装、配置和升级 Veritas 产品的安装程序脚本和库。
- 新增了 VRTSvbs RPM
  VRTSvbs RPM通过虚拟业务服务配置在 Veritas Operations Manager 托管主机上实现了 VBS 命令行界面。
  有关详细信息，请参见 *Virtual Business Service–Availability User's Guide*（《虚拟业务服务可用性安装使用指南》）。
- VRTSvcsag RPM更改
  将 /etc/VRTSvcs/conf/types.cf 和各种示例配置与 VRTSvcsag RPM（而非 VRTSvcs RPM）打包在了一起。对于需要属性更改的捆绑代理，这可以简化修补程序安装。

有关详细信息，请参见“安装指南”。

支持 Linux 上基于内核的虚拟机 (KVM)

Storage Foundation and High Availability Solutions 提供了可增强基于内核的虚拟机 (KVM) 环境的配置。Storage Foundation and High Availability Solutions 6.0 产品已在 Red Hat Enterprise Linux (RHEL) 6.1 发行版中受支持。

Storage Foundation and High Availability Solutions 产品为 KVM 来宾虚拟机提供以下功能：

- 存储可见性
- 存储管理
- 高可用性
- 集群故障转移
- 复制支持

有关实施信息：

请参见《Veritas Storage Foundation™ and High Availability Solutions 虚拟化指南 - Linux》。

对 VCS 引擎的更改

支持在服务组依赖关系中包含多个子级

一个服务组可以与多个子服务组建立依赖关系。所有子依赖项都必须得到满足后，父服务组才能联机。在多子级配置中不支持的依赖关系类型为 online local hard 和 offline local。如果依赖关系树包含全局和/或远程依赖关系，则不能使用 -propagate 选项。

有关更多详细信息，请参考“管理指南”。

用于使服务组依赖关系中的多个服务组联机或脱机的单一命令行选项

如果服务组依赖关系中有父服务组，则可以使用单个命令使整个依赖关系树从下到上全部联机，而无需手动地使每个组联机。对于联机操作，此命令从依赖关系树中最下面的服务组开始使服务组联机。同样，如果服务组依赖关系中有子服务组，则可以使用单个命令使整个依赖关系树从上到下全部脱机，而无需手动地使每个组脱机。对于脱机操作，此命令从依赖关系树的顶端开始使服务组脱机。

可以分别使用下面的命令使服务组联机或（和）脱机：

- `hagrp -online -propagate <grp_name> -sys <sys_name>`
- `hagrp -offline -propagate <grp_name> -sys <sys_name>`

注意：如果依赖关系树包含全局和/或远程依赖关系，则不能使用 -propagate 选项。

将 -propagate 选项与 hagrp -online 搭配使用时，VCS 会自动使所有必需的子服务组联机。同样，将 -propagate 选项与 hagrp -offline 搭配使用时，VCS 会自动使所有必需的父组脱机。

能够向更广的受众发送通知

除了资源所有者、资源类型、服务组、系统或集群以外，您还可以将用户配置为与资源、资源类型、服务组、系统或集群有关的事件的相关通知收件人。

请使用以下属性配置通知收件人：

- ResourceRecipients
- TypeRecipients
- GroupRecipients
- SystemRecipients

- ClusterRecipients

注册的收件人会收到严重程度等于或大于相应属性中所指定程度的事件的相关通知。有关更多信息，请参见《Veritas Cluster Server 管理指南》。

能够指定在 VCS 集群的所有节点上通用的单个用户

您可以在不指定主机名的情况下向 VCS 配置中添加用户（例如 **admin**），并向其分配管理员权限。此管理用户可以使用特定于主机的凭据登录，并可以执行任意管理操作。

因此，您不需要在 VCS 配置中按以下形式多次添加同一 admin 用户：admin@host1、admin@host2，以此类推。此用户在添加后便可以从集群中的任意节点执行操作。

与 IMF 相关的更改

此版本包含对智能监视框架 (IMF) 进行的以下更改：

IMF 在默认情况下已启用，并且新增了对代理的支持

默认情况下，已经为可以利用 IMF 的所有代理启用了智能监视框架 (IMF) 功能。

在 VCS 6.0 中，以下代理可识别 IMF：

- DB2udb（仅提供 PRON IMF 支持）
- Sybase
- SybaseBk

通过自动化脚本为代理启用和禁用 IMF

VCS 提供了 `/opt/VRTSvcs/bin/haimfconfig` 脚本，当 VCS 处于运行状态或停止状态时，都可以使用此脚本为代理启用和禁用 IMF。您可以使用此脚本为所有可识别 IMF 的代理禁用 IMF，包括捆绑代理、Enterprise Agent 和自定义代理。您必须在集群中的每个节点上都运行一次此脚本。

注意：如果代理在当前节点上处于运行状态，则此自动化脚本会在与用户确认后重新启动此代理，以便启用 IMF。

使用 IMF 防止并发冲突 (PCV)

利用新增的基于 IMF 的主动 PCV 功能，VCS 可以主动防止同一 VCS 故障转移服务组在集群中的多个节点上联机。通常，VCS 会在此类并发冲突发生后检测到相应的冲突情况。此功能仅适用于应用程序资源，默认情况下处于禁用状态。

有关详细信息，请参考“管理指南”。

可实现在自定义代理中支持 AMF 的支持插件

基于脚本的自定义代理现在可以通过按照《Veritas Cluster Server Agent 开发指南》中所述的步骤操作来利用 IMF 功能。

增强了 amfstat 实用程序

amfstat 实用程序现已增强，可显示 AMF 驱动程序可支持的新事件类型。有关详细信息，请参考 amfstat 手册页。

与 VCS 触发器有关的更改

此版本包括与 VCS 触发器有关的以下更改：

- VCS 可以执行特定于服务组和/或资源的触发器脚本。因此，不需要将多个对象的触发器脚本合并成单个触发器脚本。
- 可以通过使用 TriggersEnabled 属性为每个系统启用 nofailover、postonline 和 postoffline 触发器。
- 可以执行一个触发器的多个脚本。必须使用 T<num> 命名方式将触发器脚本安装在触发器目录中。VCS 按 T<num> 顺序执行触发器脚本。
  例如：如果 preonline 目录包含 T00preonline、T01preonline、T02preonline 脚本，则会先执行 T00preonline 脚本，再执行 T01preonline，最后执行 T02preonline。
- 如果设置了 RestartLimit，代理将重新启动出故障的资源。每当代理重新启动资源时，如果 TriggerResRestart 属性设置为 1 或者在 TriggersEnabled 属性中指定了 RESRESTART，VCS 便会调用 resrestart 触发器。否则，VCS 将调用 resstatechange 触发器。有关更多信息，请参见《Veritas Cluster Server 管理指南》。

小心：将不再使用 resstatechange 来指示重新启动操作。在更高版本中，您只能使用 resrestart 触发器来指示重新启动资源。

新属性

以下几节介绍了 VCS 6.0、5.1SP1、VCS 5.1 和 VCS 5.0MP3 中引入的属性。

VCS 6.0 中引入的属性

DNS 代理的属性

- UseGSSAPI：如果配置的 DNS 服务器是 Windows DNS 服务器，请使用此属性。如果此属性设置为 1，那么代理会将 -g 选项与 `nsupdate` 命令一起使用。
- RefreshInterval：此属性表示一个以秒为单位的时间间隔，经过此时间间隔后，DNS 代理将尝试刷新 DNS 服务器上的资源记录 (RR)。
- CleanRRKeys：使用此属性可指示 online 代理函数在添加新记录之前先清理已配置之键的所有现有 DNS 记录。默认值 (0) 禁用此行为。

集群级别的属性

- EnableVMAutoDiscovery： 启用或禁用虚拟机自动发现。默认情况下，虚拟机自动发现处于禁用状态。
- SystemRebootAction：确定是否在系统重新启动时忽略已冻结的服务组。

服务组属性

- OnlineClearParent：当为服务组启用此属性并且服务组联机或被检测到联机时，VCS 会清除联机类型（例如本地联机、全局联机和远程联机）的所有父组的故障。
- ProPCV： 对于启用 ProPCV 的资源，指示是否主动防止服务组发生并发冲突。
- TriggerPath： 用于自定义触发器路径。
- TriggerResRestart： 确定在资源重新启动时是否调用 restart 触发器。
- TriggersEnabled： 确定是否在节点上启用特定触发器。

资源类型属性：

- AdvDbg： 允许激活高级调试。

Sybase 代理的属性：

- Quorum_dev：定额设备管理集群成员资格、存储集群配置数据，并包含在服务器实例和节点之间共享的信息。它必须是集群中的所有节点都可访问的磁盘。请指定完全限定的定额设备名称。注意：应仅为集群版本指定此属性。例如：/dev/vx/rdsk/Sybase_install_dg/quorum_vol。
- interfaces_File：指定 Sybase 实例的接口文件的位置。如果配置了此属性，则当连接到 isql 会话时使用 [-I interfaces file] 选项。如果没有配置此属性，则代理将不使用 -I 选项。
- ShutdownWaitLimit： 指定代理在发出 `shutdown with wait` 命令之后、在尝试发出 `kill -15 <data server-pid>` 命令（如果需要）之前等待 Sybase 实例停止的最大秒数。
- DelayAfterOnline：指定完成 Online 入口点之后、调用下一个监视周期之前经过的秒数。
- DelayAfterOffline：指定完成 Offline 入口点之后、调用下一个监视周期之前经过的秒数。

SybaseBk 代理的属性：

- interfaces_File： 指定 Sybase 实例的接口文件的位置。如果配置了此属性，则当连接到 isql 会话时会使用 [-I inerfaces file] 选项。如果没有配置此属性，则代理将不使用 -I 选项。

Oracle 代理的属性

- DBName：指定数据库名称。此属性仅对策略管理的数据库来说是必需的。必须将此属性的值设置为数据库名称。
- ManagedBy：指定数据库是由管理员管理的还是由策略管理的。此属性的默认值为 ADMIN。您不需要明确地设置其值。在由策略管理的 RAC 数据库中，必须将此属性设置为 **POLICY**。

DiskGroupSnap 代理的属性：

- FDType： 指定要用于防火练习的配置。此属性可以采用的值为 Bronze 和 Gold（默认值）。

VCS 5.1SP1 中引入的属性

Application 代理属性

- EnvFile：此属性指定在运行 `StartProgram`、`StopProgram`、`MonitorProgram` 或 `CleanProgram` 之前必须获取的环境文件。
- UseSUDash：此属性指定代理在运行 `StartProgram`、`StopProgram`、`MonitorProgram` 或 `CleanProgram` 时必须运行 `su - user -c <program>` 或 `su user -c <program>`。

RemoteGroup 代理属性

- ReturnIntOffline：此属性可以使用以下三个值之一。这些值不相互排斥，可相互结合使用。要使 ReturnIntOffline 属性有效，必须将 IntentionalOffline 属性设置为 1。
  - RemotePartial：当远程服务组处于 ONLINE|PARTIAL 状态时，使 RemoteGroup 资源返回 IntentionalOffline。
  - RemoteOffline：当远程服务组处于 OFFLINE 状态时，使 RemoteGroup 资源返回 IntentionalOffline。
  - RemoteFaulted：当远程服务组处于 OFFLINE|FAULTED 状态时，使 RemoteGroup 资源返回 IntentionalOffline。

DiskGroup 代理属性

- Reservation：确定是否要启用 SCSI-3 保留。有关详细信息，请参见“Bundled Agents 参考指南”。

必须确保磁盘与 SCSI-3 兼容，才能支持 SCSI-3 磁盘保留。因为所有磁盘都与 SCSI-3 不兼容，所以在此类磁盘组上执行保留命令会失败。Reservation 属性可帮助解决此类问题。Reservation 属性可以使用以下三个值之一：

- ClusterDefault：是否使用 SCSI-3 保留导入磁盘组，具体取决于集群级别 UseFence 属性。
- SCSI3：使用 SCSI-3 保留导入磁盘组。
- NONE：不使用 SCSI-3 保留导入磁盘组。代理将忽略集群级别 UseFence 属性。

注意：在执行非 SCSI-3 防护时必须为 DiskGroup 类型的所有资源将此属性设置为 NONE。

LVMVolumeGroup 代理属性

- EnableLVMTagging：如果将此属性的值设置为 1，此属性会启用 LVMTagging。而默认情况下，该属性的值为 0，因此 LVMTagging 是处于禁用状态。

NFSRestart 代理属性

- Lower：定义 NFSRestart 资源在服务组中的位置。Share 资源下的 NFSRestart 资源需要的值为 1。而资源依赖关系树顶部的 NFSRestart 资源拥有的 Lower 属性值为 0。

MultiNICA 代理属性

- Mii：如果将此属性设置为 1，代理将使用 ethtool 和 Mii 硬件寄存器确定网卡的运行状况。

NotifierSourceIP 代理属性

- NotifierSourceIP：：可让您指定通知程序发送数据包必须使用的接口。此属性为字符串/标量。您必须指定 DNS 可解析的 IP 地址或 `/etc/hosts` 文件中列出的 IP 地址。

SambaServer 代理属性

- PidFile：Samba 后台驻留程序 (smbd) Pid 文件的绝对路径。如果您使用的是带有非默认名称或路径的 Samba 配置文件，则此属性是强制属性。
- SocketAddress：Samba 后台驻留程序 (smbd) 侦听连接的 IPv4 地址。如果您要在某个节点上配置多个 SambaServer 资源，则此属性是强制属性。
- SambaTopDir：Samba 后台驻留程序和二进制文件的父级路径。

ASMInst 代理属性

- MonitorOption：启用或禁用运行状况检查监视。

NetBios 代理属性

- PidFile：Samba 后台驻留程序 (nmbd) PidFile 的绝对路径。如果您使用的是带有非默认名称或路径的 Samba 配置文件，则此属性是强制属性。

Sybase 代理属性

- Run_ServerFile：该属性指定 Sybase 实例的 RUN_SERVER 文件的位置。如果未指定此属性，将在启动 Sybase 服务器实例时访问此文件的默认位置。

集群级别属性

- AutoAddSystemToCSG：指示如果确认了 ClusterService 服务组，集群中新加入的系统是否包含在该服务组的 SystemList 中。值 1（默认值）表示新系统已添加到 ClusterService 的 SystemList 中。值 0 表示新系统未添加到 ClusterService 的 SystemList 中。
- CounterMissTolerance：如果 GlobalCounter 在 CounterInterval 的 CounterMissTolerance 间隔内没有更新，则 VCS 会根据上次更新 GlobalCounter 以来所经历的 CounterMissAction（即 CounterMissTolerance * CounterInterval）时间报告此问题，随后将执行 CounterMissAction。CounterMisstolerance 的默认值为 20。
- CounterMissAction：只要在 CounterInterval 的 CounterMissTolerance 间隔期间没有更新 GlobalCounter，就会执行 CounterMissAction 中提及的相关操作。
  CounterMissAction 的两个可能值为 LogOnly 和 Trigger。
  LogOnly 将消息记录在引擎日志和 SysLog 中。Trigger 调用能够默认执行收集 comms tar 文件操作的触发器。Trigger 的默认值为 LogOnly。
- PreferredFencingPolicy：用于确定网络分裂时未发生故障的子集群的 I/O 防护争夺策略。有效值为 Disabled、System 或 Group。
  Disabled：首选防护已禁用。防护驱动程序在协调点争夺期间优先选择具有最多节点的子集群。
  System：防护驱动程序在协调点争夺期间根据体系结构、CPU 数量或内存优先选择功能最强大的系统。VCS 使用系统级别的属性 FencingWeight 来计算节点权重。
  Group：防护驱动程序在协调点争夺期间优先选择具有较高优先级服务组的节点。VCS 使用组级别的属性 Priority 来确定节点权重。

资源类型属性

- IMF：确定可识别 IMF 的代理是否必须执行智能资源监视。
  它是一个具有以下三个键的关联属性：Mode、MonitorFreq 和 RegisterRetryLimit。
  - Mode：定义是否根据资源的状态执行 IMF 监视。Mode 的值可以是 0、1、2 或 3。默认值为 0。
  - MonitorFreq：指定代理调用 monitor 代理函数的频率。默认值为 1。

- RegisterRetryLimit：定义代理尝试注册资源的最大次数。默认值为 3。

- IMFRegList：包含属性列表。这些属性的值在 IMF 通知模块中注册。如果在 IMFRegList 属性中定义的属性发生更改，则会在 IMF 中取消注册资源（如果此资源已经注册）。如果没有定义 IMFRegList 且在 ArgList 中定义的任何属性发生更改，则从 IMF 取消注册资源。
- AlertOnMonitorTimeouts：指示在连续的监视失败多少次后 VCS 会向用户发送 SNMP 通知。

VCS 5.1 中引入的属性

VCS 5.1 中引入了下列新属性。有关更多信息，请参见《Veritas Cluster Server 管理指南》。

资源类型属性：

- CleanRetryLimit：将资源转至 ADMIN_WAIT 状态之前重试 Clean 函数的次数。
- EPClass：用于控制除了 online 入口点之外的代理函数（入口点）的调度等级。
- EPPriority：用于控制除了 online 入口点之外的代理函数（入口点）的调度优先级。
- FaultPropogation：指定当资源出现故障时 VCS 是否应该将故障向上传播到父资源并使整个服务组脱机。
- OnlineClass：用于控制 online 代理函数（入口点）的调度等级。
- OnlinePriority：用于控制 online 代理函数（入口点）的调度优先级。

集群级别属性：

- CID：CID 为集群提供了通用唯一标识。
- DeleteOnlineResource：定义是否可以删除联机资源。
- HostMonLogLvl：控制 HostMonitor 功能的行为。

VCS 5.0 MP3 中引入的属性

VCS 5.0MP3 中引入了以下属性。

资源类型属性：

- FaultPropagation：指定当资源出现故障时 VCS 是否应该将故障向上传播到父资源并使整个服务组脱机。
- AgentFile：代理二进制文件的完整名称和路径。当代理二进制文件未安装于其默认位置时使用。
- AgentDirectory：代理二进制文件和脚本所在目录的完整路径。当代理二进制文件未安装于其默认位置时使用。

集群级别属性：

- DeleteOnlineResource：定义是否可以删除联机资源。
- HostMonLogLvl：控制 HostMonitor 后台驻留程序的行为。在启动集群时配置此属性。您无法在正在运行的集群中修改此属性。
- EngineShutdown：提供对 hastop 命令更好的控制。
- BackupInterval：时间周期（分钟），每过一个周期，VCS 备份一次配置文件。
- OperatorGroups：拥有集群 Operator 权限的操作系统用户帐户组的列表。
- AdministratorGroups：拥有集群管理权限的操作系统用户帐户组的列表。
- Guests：拥有集群 Guest 权限的用户的列表。

系统级别属性：

- EngineVersion：指定 VCS 的主要版本、次要版本、维护修补程序版本以及局部修补程序版本。

服务组级别属性：

- TriggerResFault：定义 VCS 在资源出现故障时是否调用 resfault 触发器。
- AdministratorGroups：拥有服务组管理权限的操作系统用户帐户组的列表。
- OperatorGroups：拥有服务组 Operator 权限的操作系统用户帐户组的列表。
- Guests：拥有服务组 Guest 权限的用户的列表。

对 VCS 捆绑代理的更改

本节介绍了 VCS 的捆绑代理的变更。

有关详细信息，请参见《Veritas Cluster Server 管理指南》和《Veritas Cluster Server Bundled Agents 参考指南》。

对 Windows DNS 服务器的支持

DNS 代理现在支持在其配置中使用 Windows DNS 服务器。已为此功能向 DNS 代理配置中添加了 UseGSSAPI 这一新属性。

有关如何使用此属性的详细信息以及配置 DNS 代理以使用 Windows DNS 服务器的其他要求，请参见《Veritas Cluster Server Bundled Agents 参考指南》。

DNS 代理支持对 Windows DNS 服务器进行 DNS 清理

DNS 代理现在可以配置为向已配置的 Windows DNS 服务器发送定期刷新请求，以避免发生资源记录老化和清理。

发生角色更改后 RVGPrimary 代理开始从新的主节点复制到 RDS 中的其他辅助节点

成功迁移或接管辅助节点 RVG 后，RVGPrimary 代理会确保自动开始从新的主节点复制到 RDS 中存在的其他辅助节点（如果有）。

有关 RVGPrimary 代理在包含多个辅助节点的环境中如何工作的信息，请参考 *SF Replication Administrator's Guide*（“SF 复制管理指南”）。

NIC 代理对 ethtool 的支持

从 VCS 5.1 版本起，Linux NIC 和 MultiNICA 代理支持基于 ethtool 的设备状态监视。

使校园集群防火练习变得容易

通过引入 FDType 这一新属性，已使校园集群防火练习配置变得更为容易。您只需设置此属性即可控制防火练习风格，而不用为其他属性指定具体的值。

您需要安装 Global Cluster Option (GCO) 许可证才能在校园集群配置中运行防火练习。

DiskGroup 代理在行为方面的更改

下列更改影响到了 DiskGroup 代理：

- PanicSystemOnDGLoss 属性的类型从布尔型更改为整型。
  PanicSystemOnDGLoss 属性现在接受下列值：
  0：不停止系统
  1：如果任一磁盘组进入禁用状态或者磁盘组资源由于监视超时而出现故障，则停止系统。
  2：如果磁盘组进入禁用状态，则停止系统。
  3：如果磁盘组资源由于监视超时而出现故障，则停止系统。
- 如果 MonitorReservation 属性设置为 0、集群范围的属性 UseFence 的值设置为 SCSI3 并且发现磁盘组是在未进行 SCSI 保留的情况下导入的，则 monitor 代理函数会使包含 DiskGroup 资源的服务组脱机。

Application 代理的增强

Application 代理进行了以下增强：

- 对代理进行了增强，以支持对 StartProgram、StopProgram、MonitorProgram 和 CleanProgram 使用共享磁盘。
- 对代理进行了增强，使之理解 MonitorProgram 返回代码的 Unix 样式，即 0 (ONLINE) 和 1 (OFFLINE)。

Mount 代理的增强

Mount 代理现在支持 ext4 和 xfs 文件系统。

Apache 代理的增强

下面是对 Apache 代理的增强

- 对 httpDir 属性进行了增强，以便您可以指定二进制文件的完整路径（包括二进制文件名）。如果您仅指定目录名称，此代理将采用默认二进制文件名 httpd。
- 如果 httpDir 目录中的 Apache Benchmarking 二进制文件不使用此默认名称，则此代理会识别到备用的二进制文件名 ab2，并执行详细监视。
- 增强了 Apache 代理版本解析功能，使之适应 IBM HTTP Server 7.0。

首次捕获有关 VCS 代理入口点超时的失败数据

为调试入口点超时，引入了 AdvDbg 这一新属性。此属性有助于 VCS 捕获有关入口点超时的一些信息，如进程堆栈、进程树和核心。这有助于对入口点超时情况进行故障排除。

有关详细信息，请参见《Veritas Cluster Server Agent 开发指南》。

网络代理的更改

NetMask 属性是以下代理的必需属性：

- IP
- IPMultiNIC
- IPMultiNICA
- IPMultiNICB

对数据库代理的更改

对 DB2 代理的更改

- VCS Agent for DB2 现在支持在非 MPP 及 MPP 配置模式下以智能资源监视方式监视是否有处于 PRON 模式的联机 Db2 进程。
- 在 VCS 6.0 版本之前，如果从源节点到目标节点的分区移动性具有高速互联/交换机配置，那么在 db2nodes.cfg 配置文件中交换机名称条目不会得到更新。在 VCS 6.0 版本中，DB2 代理可确保在此配置文件中交换机名称得到正确更新。
- 增加了 IMF 对 DB2 代理的支持：DB2 代理现在利用 IMF 功能来即时检测资源状态变化。这可以大幅减少对资源状态的定期监视工作，从而也减少了此代理对 CPU 的占用。

有关详细信息，请参见“管理指南”。

对 Oracle 代理的更改

- VCS Agent for Oracle 新增了两个属性：DBName 和 ManagedBy。
- VCS Agent for Oracle 为 StartUpOpt 和 ShutDownOpt 属性增加了一些选项：
  - StartUpOpt 属性引入了 SRVCTLSTART_RO 作为附加的启动选项。
  - ShutDownOpt 属性引入了 SRVCTLSTOP_TRANSACT、SRVCTLSTOP_ABORT 和 SRVCTLSTOP_IMMEDIATE 作为附加的关闭选项。
- VCS Agent for Oracle 引入了对策略管理的数据库的支持。
- VCS Agent for Oracle ASM 实例引入了以下附加启动选项：
  - STARTUP_MOUNT
  - STARTUP_OPEN
  - SRVCTLSTART_MOUNT
  - SRVCTLSTART_OPEN
- VCS Agent for Oracle ASM 实例引入了以下附加关闭选项：
  - SRVCTLSTOP
- 对于 Oracle 11.2.0.2 版本，Oracle Agent for VCS 支持使用 `srvctl` 实用程序进行 Oracle 重新启动配置的启动和关闭选项。

对 Sybase 代理的更改

Veritas Cluster Server Agent for Sybase 包括以下新的或增强的功能：

- VCS Agent for Sybase 和 VCS Agent for SybaseBk 现在支持智能资源监视。
- 在 VCS 6.0 版本中，智能监视框架 (IMF) 默认情况下处于启用状态。可以使用 `haimfconfig` 脚本为 Sybase 和 SybaseBk 代理启用/禁用 IMF。Sybase 代理现在利用 IMF 功能来即时检测资源状态变化。这可以大幅减少对资源状态的定期监视工作，从而也减少了此代理对 CPU 的占用。
  有关详细信息，请参见“管理指南”以及“Agent for Sybase 安装和配置指南”。
- 除了支持 Sybase ASE Enterprise Edition 以外，Sybase 代理经过增强，还支持 Sybase ASE Cluster Edition。对于 Sybase ASE Cluster Edition，VCS Agent for Sybase 可以使 Sybase Adaptive Server 在 VCS 集群中具有高可用性。
- Sybase 代理引入了以下新属性：
  - Quorum_dev

- interfaces_File
- ShutdownWaitLimit（默认值 60）
- DelayAfterOnline（默认值 10）
- DelayAfterOffline（默认值 2）

- SybaseBk 代理引入了以下新属性：
  - interfaces_File
- 对于 Sybase 代理，ToleranceLimit 属性的默认值设置为 1（一）。
- DetailMonitor 属性在 VCS 6.0 中已废弃。可以改为使用 Sybase 代理的 LevelTwoMonitorFreq 属性。LevelTwoMonitorFreq 属性的默认值为 0（零）。
- $SYBASE 的长路径名限制问题已得到解决。
- 对于采用 VCS Cluster Manager（Java 控制台）的 VCS 6.0 版本，Sybase 代理和 SybaseBk 代理在默认情况下会对密码进行加密。Sybase 代理和 SybaseBk 代理既支持明文密码，也支持经过加密的密码。如果需要，可以使用命令行或通过编辑配置文件来为代理属性指定明文值。
- Sybase 代理在关闭所用的 Sybase 数据服务器期间采用新的 timeout 选项而非 shutdown with nowait。对于 Sybase ASE Enterprise Edition，12.5.4 版本以及 15.0.2 及以后的版本都支持 shutdown 命令的 timeout 选项。
  对于 Sybase ASE Cluster Edition，从 15.5 ESD #1 版本起，支持 shutdown 命令的 timeout 选项。

对以安全模式运行的 VCS 集群的更改

在此版本中，极大简化了安全集群的安装和配置体验。使用这个简化的安全集群配置模型，可以将集群轻松转换成安全集群。

新的体系结构基于嵌入式 VxAT，其中的安全组件作为 VCS 软件包的一部分安装。在新的体系结构中，根代理不再是单点故障。单独的 VRTSat 软件包没有依赖关系。现在，不再提示已登录 VCS 主机的非 root 用户输入密码。另外，引入了一个集群级用户功能，以简化安全集群中的用户管理。

有关详细信息，请参见“安装指南”和“管理指南”。

对 LLT 的更改

此版本包括以下新功能以及对 LLT 的更改：

- LLT 现在支持 VLAN 标记 (IEEE 802.1Q)。
- `lltconfig` 命令包括下列新选项：
  - -N

可以使用此选项列出所有已使用的集群 ID。

- -M
  可以使用此选项显示当前已加载的 LLT 模块版本信息。

有关更多信息，请参见 `lltconfig` 手册页。
有关更多信息，请参见 `llttab` 手册页。

- 增强了链路利用率统计数据，这些统计数据可用于分析性能相关问题的根本原因。
- 禁止定期刷新 ARP 缓存。
- 当 NIC 的 MAC 地址更改时，LLT 立即重新了解新的 MAC 地址，并且更新与更改有关的对等节点。

有关更多详细信息，请参见《Veritas Cluster Server 安装指南》和《Veritas Cluster Server 管理指南》。

对 GAB 的更改

本节介绍了与此版本中的 GAB 相关的新功能和更改。

提供更好的 GAB 和 I/O 防护集成以确保应用程序可用性

如果在 VxFEN 模块执行裂脑决定前发生裂脑情形，有时 GAB 会在裂脑发生后继续尝试解决加入问题。GAB将只留一个加入的子集群，将其余的全部删除。此行为可能会导致整个集群关闭。为避免这种情况发生，GAB 现在让防护模块优先。

对于此版本中的 GAB 和 I/O 防护集成，如果在 GAB 启动子集群加入前 I/O 防护模块仍未做出决定，GAB 会延迟发出 iofence 消息。GAB 等待时间取决于 VxFEN 可调参数 *panic_timeout_offst* 的值，VxFEN 将根据此值计算延迟值并将延迟值传递给 GAB。

有关更多详细信息，请参见《Veritas Cluster Server 管理指南》。

除了端口以外，GAB 现在可以通过名称来识别客户端

当内核客户端对GAB API进行初始化时，这些客户端现在可以定义客户端名称字符串。GAB 现在增加了客户端名称，有了此名称，即使在 GAB 端口注册前，GAB 也可以跟踪客户端。在注册 LLT 端口时，GAB 还会将客户端名称信息传递给 LLT。`lltstat -p` 命令在提供正在使用的端口的状态详细信息时，也会显示 GAB 客户端名称。

此功能仅适用于 GAB 内核客户端，不适用于用户领域 GAB 客户端（如 HAD）。

gabconfig 命令新增了 -C 选项

gabconfig 命令的 -C 选项列出了已向 GAB 注册的 GAB 客户端的名称。-C 选项在与 -a 选项搭配使用时，会将客户端名称与端口成员资格详细信息一同列出。

对 I/O 防护的更改

本节介绍了与此版本中的 I/O 防护相关的新功能和更改。

安装程序支持在联机集群中的不同防护配置间迁移

现在可以使用安装程序在基于磁盘的防护配置与基于服务器的防护配置之间进行迁移。还可以使用同一安装程序选项为联机集群中的任何 I/O 防护配置替换协调点。安装程序在内部使用 vxfenswap 脚本。

您也可以使用响应文件来执行这些 I/O 防护重新配置操作。

有关更多详细信息，请参见《Veritas Cluster Server 管理指南》。

支持在 I/O 防护争夺期间重新选择争夺者节点

发生网络分裂时，VxFEN模块会选择每个子集群中最低的节点作为争夺者节点来代表该子集群争夺协调点。其他旁观者节点将等待该争夺者节点执行防护。

在之前的版本中，I/O 防护争夺完全依靠单个争夺者节点，具体如下：

- 如果争夺者节点无法到达绝大多数协调点，则争夺者节点上的 VxFEN 模块会发送一条 LOST_RACE 消息，该子集群中的所有节点在收到此 LOST_RACE 消息后也会发生混乱。
- 如果争夺者节点在仲裁期间发生混乱，则该子集群中的旁观者节点将认为争夺者节点在争夺中失败，因而这些旁观者节点也会发生混乱。

借助新的争夺者节点重新选择功能，VxFEN 模块可以重新选择该子集群中 ID 最小的下一个节点作为争夺者节点。此功能使该子集群继续进行协调点争夺的机会得到优化。

有关更多详细信息，请参见《Veritas Cluster Server 管理指南》。

支持在 CP 服务器中使用多个虚拟 IP 地址

现在可以配置多个网络路径（虚拟 IP 地址）来访问一台 CP 服务器。CP 服务器在多个虚拟 IP 地址进行侦听。如果一个网络路径出故障，CP 服务器无需重新启动，继续在其他可用虚拟 IP 地址中的一个地址侦听即可。

有关更多详细信息，请参见《Veritas Cluster Server 安装指南》和《Veritas Cluster Server 管理指南》。

支持在 CP 服务器中使用 Quorum 代理

由于支持多个虚拟 IP 地址，因此现在可以使用 Quorum 代理来配置 CP 服务器的服务组故障转移策略。可以指定必须有至少多少项 IP 资源处于联机状态才可让 Quorum 资源保持联机。

有关更多详细信息，请参见《Veritas Cluster Server 安装指南》和《Veritas Cluster Server 管理指南》。

启用防护后，GAB 现在可以在某些集群节点不可用时自动对集群进行种子设定

在早期版本中，如果某些节点在集群中未启动并运行，则 GAB 端口不会激活，以免带来任何产生预先存在的裂脑的风险。在这种情况下，可以使用 `gabconfig -x` 命令手动对 GAB 进行种子设定，以激活 GAB 端口。不过，如果在集群中启用了 I/O 防护，则 I/O 防护可以处理集群中任何预先存在的裂脑情况。

在此版本中，I/O 防护已扩展此功能，以便能够自动按如下方式对 GAB 进行种子设定：

- 如果集群中有多个节点未启动，GAB 端口（端口 a）仍会在集群中的所有成员节点上启动。
- 如果协调点没有来自任何非成员节点的密钥，I/O 防护（GAB 端口 b）也会启动。

默认情况下此新功能处于禁用状态。在 I/O 防护配置为启用模式的集群中，必须手动启用 GAB 的此自动种子设定功能。

有关更多详细信息，请参见《Veritas Cluster Server 管理指南》。

您仍然可以使用 `gabconfig -x` 命令手动地对集群进行种子设定。

节点的正常关闭不再在对等节点上触发 I/O 防护争夺情况

在早期版本中，正常脱离的节点会从协调点清除其 I/O 防护键。但是，剩余的子集群与该正常脱离的节点争夺以从数据磁盘删除其注册。在此操作期间，如果该子集群失去对协调点的访问权，即争夺者失去对协调点的争夺，则整个集群可能发生混乱。

在此版本中，此行为已进行了更改。当节点正常脱离时，CVM 或该节点的其他客户端将先终止，然后再取消配置 VxFEN 模块。因此，数据磁盘中已经清除了其键。剩余的子集群尝试从协调点清除正常脱离的节点的键，但是如果不能清除这些键，并不会发生混乱。

与虚拟化支持有关的更改

本节列出此版本在虚拟化方面的更改。

Linux 上的新 KVMGuest 代理

KVMGuest 代理用于监视基于 Linux 内核的虚拟机（KVM 来宾）、使 KVM 来宾联机和脱机。KVMGuest 代理使用 virsh 命令。

您可以使用此代理使 KVM 来宾具有高可用性以及对其进行监视。此代理是作为虚拟化支持的一部分添加的。

虚拟化支持

可以在使用 Red Hat KVM（基于内核的虚拟机）创建的虚拟机或来宾内安装和运行 VCS。支持以下集群配置：

- 跨相同或不同物理主机上的多个 VM 来宾 (VM-VM) 的 VCS 集群 - 以提供应用程序可用性
- 跨多台物理机 (PM-PM) 且在 VM 来宾中不进行资源监视的 VCS 集群 - 以提供虚拟机可用性
- 跨多台物理机 (PM-PM) 且在 VM 来宾中进行资源监视的 VCS 集群 - 既提供虚拟机可用性、又提供应用程序可用性
- 跨物理机和 VM 来宾的 VCS 集群（在 KVM 和 Veritas Cluster Server 集群配置的基础上新增的一种配置）

下表显示了 KVM 支持的各种配置的系统要求。

表 1-1 KVM 支持的各种配置的系统要求

支持的主机操作系统版本	RHEL 6 Update 1
VM 来宾中支持的操作系统	RHEL 6 Update 1
硬件要求	支持完全虚拟化的 CPU

SFHA Solutions 6.0 版本中的授权许可更改

Storage Foundation and High Availability Solutions 6.0 引入了以下授权许可更改：

- 集群文件系统许可证已废弃。CFS 客户有权使用 Storage Foundation Cluster File System High Availability (SFCFS HA) 功能。
- VVR 选件重命名为 Veritas Replicator 选件。此选件包括 VVR（基于卷的复制）和基于文件的新复制解决方案。
- VVR Enterprise 许可证已废弃；您可以使用 Storage Foundation Enterprise 并添加 Veritas Replicator 选件来获取此功能。VVR Enterprise 客户有权使用带有 Replicator 选件的 Storage Foundation Enterprise。
- VCS 许可证启用完全集群功能以及有限的启动/停止功能。

- Storage Foundation Enterprise CFS for Oracle RAC (Linux/x64) 客户有权使用 Storage Foundation Enterprise for Oracle RAC (Linux/x64)。

Standard 和 Enterprise 许可证中包含以下功能：

- 压缩功能通过 Standard 许可证提供。
- SmartTier 功能现在通过 Standard 许可证提供。
- 重复数据删除功能通过 Enterprise 许可证提供。

此版本中包含以下产品：

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

HA：High Availability

HA/DR：High Availability and Disaster Recovery

Veritas Replicator 选件可添加到除 Dynamic Multi-Pathing 和 Veritas Cluster Server 以外的所有 Storage Foundation and High Availability 产品。

请注意，产品、功能和选件可能因操作系统和平台而异。有关支持的平台的信息，请参见产品文档。

用于收集 VxExplorer 故障排除存档的增强功能

Symantec Operations Readiness Tools (SORT) 数据收集器包含用于收集和提交 VxExplorer 存档的功能。您可以将此存档发送给 Symantec 技术支持以便诊断并排除故障。VxExplorer 不收集客户数据。

当前 `VxExplorer` 脚本的工作方式与其旧版有所不同。运行该脚本时，它会使用 `-vxexplorer` 选项在指定本地主机上启动 SORT 数据收集器。

要了解有关使用数据收集器收集 VxExplorer 存档的详细信息，请参见：

www.symantec.com/docs/HOWTO32575

与产品文档相关的更改

Storage Foundation and High Availability Solutions 6.0 版本包括对产品文档的以下更改。

表 1-2 列出了此版本中引入的文档。

表 1-2 新文档

新文档	说明
Veritas Storage Foundation 安装指南	Veritas Storage Foundation 的安装和升级信息。
Veritas Storage Foundation 管理指南	Veritas Storage Foundation 的管理信息。
Veritas Storage Foundation and High Availability 版本说明	供 Veritas Storage Foundation and High Availability 用户查阅的版本特定信息。
Veritas Storage Foundation and High Availability Solutions 解决方案指南	Veritas Storage Foundation and High Availability Solutions 的解决方案和用例。
Veritas Storage Foundation and High Availability Solutions 故障排除指南	Veritas Storage Foundation and High Availability Solutions 的故障排除信息。
Veritas Storage Foundation and High Availability Solutions 虚拟化指南	Veritas Storage Foundation and High Availability Solutions 的虚拟化相关信息。
Symantec VirtualStore 版本说明	Symantec VirtualStore 的版本特定信息。
Veritas Storage Foundation for Sybase ASE CE 版本说明	Veritas Storage Foundation for Sybase ASE CE 的版本特定信息。
Veritas Storage Foundation for Sybase ASE CE 安装指南	Veritas Storage Foundation for Sybase ASE CE 的安装信息。

新文档	说明
Veritas Storage Foundation for Sybase ASE CE 管理指南	Veritas Storage Foundation for Sybase ASE CE 的管理信息。
Virtual Business Services–Availability User's Guide（《虚拟业务服务可用性安装使用指南》）	有关虚拟业务服务的信息。可联机获得此文档。

表 1-3 列出了此版本中废弃的文档。

表 1-3 已废弃的文档

已废弃的文档	说明
Veritas File System 管理指南	这部分内容现在包含在《Veritas Storage Foundation 管理指南》和《Veritas Storage Foundation Cluster File System High Availability 管理指南》中。
Veritas Volume Manager 管理指南	这部分内容现在包含在《Veritas Storage Foundation 管理指南》和《Veritas Storage Foundation Cluster File System High Availability 管理指南》中。
Veritas Storage Foundation 高级功能管理指南	这部分内容现在包含在《Veritas Storage Foundation and High Availability Solutions 解决方案指南》中。
Veritas Volume Manager 故障排除指南	这部分内容现在包含在《Veritas Storage Foundation and High Availability Solutions 故障排除指南》中。
Veritas Cluster Server Agents for Veritas Volume Replicator 配置指南	这部分内容现在包含在《Veritas Cluster Server Bundled Agents 参考指南》中。
Veritas Volume Replicator 规划与优化指南	这部分内容现在包含在 *Veritas Storage Foundation and High Availability Solutions Replication Administrator's Guide*（《Veritas Storage Foundation and High Availability Solutions 复制管理指南》）中。
Veritas Volume Replicator Advisor 安装使用指南	这部分内容现在包含在 *Veritas Storage Foundation and High Availability Solutions Replication Administrator's Guide*（《Veritas Storage Foundation and High Availability Solutions 复制管理指南》）中。

表 1-4 列出了不再与二进制文件捆绑的文档。这些文档现在可通过联机方式获得。

表 1-4 联机文档

文档
Veritas Cluster Server Agent 开发指南
Veritas File System 程序员参考指南

VCS 5.1SP1PR2 中引入的更改

本节介绍 VCS 5.1SP1PR2 中引入的更改。

增加了对 Red Hat Enterprise Linux 6 的支持

在此版本中增加了对 Red Hat Enterprise Linux (RHEL6) 的支持。

与 NFSv4 导出相关的更改

在 RHEL6 之前，对于 NFSv4 导出，操作系统未分配导出到 NFS 客户端的伪文件系统的根目录。因此，需要将 fsid=0 选项放入其中一项 Share 资源中，以使 Share 路径成为根目录。对于 RHEL6，这不是必须执行的操作。默认情况下，/ 是导出到 NFS 客户端的伪文件系统的根目录。

VCS 5.1SP1PR3 中引入的更改

本节介绍 VCS 5.1SP1PR3 中引入的更改。

简化安装和配置

VirtualStore 安装程序已进行了简化，以便允许以典型模式进行安装。此外，已不再需要在所有 VirtualStore 节点上都安装 VMware PERL SDK。

VMware View 集成

克隆向导提供了用于自动将虚拟机克隆导入到 VMware View 池的选项。

能够在克隆后打开虚拟机电源

克隆向导提供了用于在创建虚拟机克隆后打开它们的电源的选项。

对多个 VirtualStore 集群的支持

不支持将多个 VirtualStore 插件（每个 VirtualStore 集群各一个）与单个 vCenter Server 一起使用。

支持向单个 vCenter Server 注册的多个 VirtualStore 集群。

VCS 系统要求

本节介绍 VCS 的系统要求。

以下信息适用于 VCS 集群。这些信息不适用于 SF Oracle RAC 安装。

VCS 要求集群中的所有节点使用相同的处理器体系结构并运行相同的操作系统版本。然而，对于特定的 RHEL 或 OEL 版本节点可以有不同的更新级别，对于特定的 SLES 版本可以有不同的服务包级别。

注意：安装 VCS 的系统必须与目标系统运行相同的 Linux 发行版。

请参见第 33 页的“硬件兼容列表”。

请参见第 33 页的“支持的 Linux 操作系统 ”。

硬件兼容列表

兼容性列表中包含有关所支持硬件的信息，该列表会定期更新。有关支持的硬件的最新信息，请访问以下 URL：

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

安装或升级 Veritas Cluster Server 前，请查看当前兼容性列表确认硬件和软件的兼容性。

支持的 Linux 操作系统

本节列出了此版本 Veritas 产品所支持的操作系统。

表 1-5 显示了此版本支持的操作系统。

表 1-5 支持的操作系统

操作系统	级别	内核版本	芯片组
Red Hat Enterprise Linux 6	6.1	2.6.32-131.0.15.el6	64 位 x86、EMT*/Opteron 4.1（仅 64 位）

操作系统	级别	内核版本	芯片组
Red Hat Enterprise Linux 5	Update 5、6、7	2.6.18-194.el5 2.6.18-238.el5 2.6.18-274.el5	64 位 x86，EMT*/Opteron 4.1（仅 64 位）
SUSE Linux Enterprise 11	SP1	2.6.32.12-0.7	64 位 x86，EMT*/Opteron 4.1（仅 64 位）
SUSE Linux Enterprise 10	SP4	2.6.16.60-0.85.1	64 位 x86，EMT*/Opteron 4.1（仅 64 位）
Oracle Enterprise Linux 6	**6.1	2.6.32-131.0.15.el6	64 位 x86，EMT*/Opteron
Oracle Enterprise Linux 5	**Update 5、6、7	2.6.18-194.el5 2.6.18-238.el5 2.6.18-274.el5	64 位 x86，EMT*/Opteron

* 扩展内存技术

** 仅 RHEL 兼容模式。

注意：仅支持 64 位操作系统。

如果系统运行的是 Red Hat Enterprise Linux、SUSE Linux Enterprise Server 或 Oracle Enterprise Linux 的旧版本，请先对其进行升级，然后再尝试安装 Veritas 软件。有关升级或重新安装系统的详细信息，请参见 Red Hat、SUSE 或 Oracle 文档。

Symantec 仅支持 Oracle、Red Hat 和 SUSE 分发的内核二进制文件。

如果操作系统保持内核应用程序二进制接口 (ABI) 兼容性，则 Symantec 产品可在使用以后发行的内核和修补程序的情况下运行。

VCS 所必需的 Linux RPM

确保已在要安装或升级 VCS 的系统上安装了特定于以下操作系统的 RPM。如果 RPM 保持了 ABI 兼容性，VCS 将支持对以下 RPM 执行的所有更新。

表 1-6 列出了 VCS 针对给定 Linux 操作系统所需的 RPM。

表 1-6 必需的 RPM

操作系统	必需的 RPM
RHEL 5	compat-libstdc++-33-3.2.3-61.x86_64.rpm glibc-2.5-49.i686.rpm glibc-2.5-49.x86_64.rpm ksh-20100202-1.el5.x86_64.rpm libgcc-4.1.2-48.el5.x86_64.rpm libgcc-4.1.2-48.el5.i386.rpm libstdc++-4.1.2-48.el5.i386.rpm pam-0.99.6.2-6.el5_4.1.x86_64.rpm
RHEL 6	compat-libstdc++-33-3.2.3-69.el6.x86_64.rpm compat-libstdc++-296-2.96-144.el6.i686.rpm glibc-2.12-1.7.el6.x86_64.rpm glibc-2.12-1.7.el6.i686.rpm ksh-20100621-2.el6.x86_64.rpm libgcc-4.4.4-13.el6.i686.rpm libgcc-4.4.4-13.el6.x86_64.rpm libstdc++-4.4.4-13.el6.x86_64.rpm pam-1.1.1-4.el6.x86_64.rpm
SLES 10	glibc-2.4-31.81.11.x86_64.rpm glibc-32bit-2.4-31.81.11.x86_64.rpm ksh-93t-13.17.19.x86_64.rpm libgcc-4.1.2_20070115-0.32.53.x86_64.rpm libstdc++-4.1.2_20070115-0.32.53.x86_64.rpm pam-0.99.6.3-28.23.15.x86_64.rpm

操作系统	必需的 RPM
SLES 11	glibc-2.11.1-0.17.4.x86_64.rpm glibc-32bit-2.11.1-0.17.4.x86_64.rpm ksh-93t-9.9.8.x86_64.rpm libgcc43-32bit-4.3.4_20091019-0.7.35.x86_64.rpm libgcc43-4.3.4_20091019-0.7.35.x86_64.rpm libstdc++33-3.3.3-11.9.x86_64.rpm libstdc++43-32bit-4.3.4_20091019-0.7.35.x86_64.rpm

VCS 支持的软件

VCS 支持下列卷管理器和文件系统：

- LVM2 上的 ext2、ext3、reiserfs、NFS 和 bind，原始磁盘以及 VxVM。
- LVM2 和原始磁盘上的 ext4 和 xfs
- Veritas Storage Foundation (SF)：Veritas Volume Manager (VxVM) 和 Veritas File System (VxFS)

  VCS 6.0 支持 SF 的下列版本：

  - SF 6.0
    - 具有 VxFS 6.0 的 VxVM 6.0
  - SF5.1SP1
    - 具有 VxFS 5.1SP1 的 VxVM 5.1SP1

注意：VCS 支持 SF 的早期版本以及以后的版本，以便于产品升级。

支持 VCS 代理

表 1-7 列出了各企业应用程序对应的代理以及这些代理所支持的软件。

表 1-7 各企业应用程序对应的 VCS 代理所支持的软件

代理	应用程序	应用程序版本	Linux 版本
DB2	DB2 Enterprise Server Edition	9.1、9.5、9.7	RHEL5、OLE5、SLES10
		9.5、9.7	SLES11
		9.7	RHEL6、OLE6
Oracle	Oracle	10gR2、11gR1、11gR2	RHEL 5、SLES10、SLES 11、OEL5
Sybase	Sybase Adaptive Server Enterprise	12.5.x、15.x	RHEL5、RHEL6 SLES10、SLES11、OEL5、OEL6

有关更多详细信息，请参见适用于此代理的《Veritas Cluster Server 安装指南》。

有关 VCS 应用程序代理及其所支持的软件的列表，请参见 Symantec 网站上的 Veritas Cluster Server Agents Support Matrix。

不再支持的功能

此版本的 VCS 产品不支持以下功能：

- 此版本中废弃了一些文档。
  请参见第 30 页的“与产品文档相关的更改”。

不再支持的代理和组件

VCS 不再支持下列代理和组件：

- 配置向导
- CampusCluster 代理
- SANVolume 代理
- VRTSWebApp
- Oracle 8.0.x、Oracle 8.1.x 和 Oracle 9i - 不受 Oracle 代理支持。
- VCS 文档软件包 (VRTSvcsdc)
  VCS 文档软件包 (VRTSvcsdc) 已被废弃。软件光盘的 *cluster_server/docs* 目录下包含采用可移植文档格式 (PDF) 的 VCS 文档。

Symantec 建议将相关文档从光盘复制到您的系统目录 /opt/VRTS/docs 下，以供参考。

- 《Veritas Cluster Server Agents for Veritas Volume Replicator 配置指南》已废弃，其内容已纳入到 *Veritas Storage Foundation and HIgh Availability Solutions Replication Administrator's Guide*（《Veritas Storage Foundation and HIgh Availability Solutions 复制管理指南》）和《Veritas Cluster Server Bundled Agents 参考指南》中。
- hahbsetup 工具。由于没有支持的功能需要此工具，因此已将其删除。
- VRTScutil RPM。已不再支持此 RPM。

已废弃的属性

已废弃的 Oracle 代理属性：

- AgentDebug
- DetailMonitor

已废弃的 Mount 代理属性：

- SecondLevelMonitor
- SecondLevelTimeout

已废弃的 Host Monitor 属性：

- CPUUsageMonitoring：此属性无法再用于禁用由 Host Monitor 代理执行的 CPU 利用率监视。

Sybase 代理属性：

- DetailMonitor

已解决的问题

本节介绍此版本中已修复的事件。

请参见相应的“版本说明”，以获取已修复的该产品相关事件的完整列表。

请参见第 83 页的“文档”。

已解决的 LLT、GAB 和 I/O 防护问题

表 1-8 列出了已解决的 LLT、GAB 和 I/O 防护问题。

表 1-8 已解决的 LLT、GAB 和 I/O 防护问题

事件	说明
2515932	[GAB] 如果已配置 GAB，则 gabconfig ioctl 行为更改为返回 EALREADY。
2495020	[防护] 如果您运行 `vxfenswap` 命令将防护模式从 scsi3 更改为“自定义”，则 vxfend 不会终止，并且在 vxfenswap 提示确认时选择回滚。
2442402	[LLT] 通过减少唤醒调用减少了 lltd 的 CPU 占用量。
2437022	[防护] 磁盘策略更改后，无法对同一磁盘组运行 `vxfenswap` 命令。
2426664	[防护] 当您运行 `vxfenswap` 命令从自定义模式迁移到 scsi3 模式时，vxfend 不终止。
2411652	[GAB] 在大小为 64KB 的 MAX 消息的 GAB 中，增加了消息排队之前的检查。
2386325	[防护] 防护配置失败，vxfenadm 为所有在 0x83 页中具有超过 96 个字节的 SCSI 查询数据的 LUN 输出相同的序列号。
2369742	[防护] 一旦 vxfenconfig -c 采用特定模式（假设是自定义模式）时返回了 EFAULT（“1036 Unable to configure...(1036 无法配置...)”），之后采用其他模式（假设是 scsi3）运行 vxfenconfig -c 时就会全都失败，并出现 EBADMSG 错误（“1050 Mismatched modes...(1050 模式不匹配...)”）。
2351011	[防护] vxfenswap 实用程序无法准确地检查在后台中其他节点上运行的 vxfenconfig 命令的退出状态。这会导致当 vxfenconfig 进程因故不能成功时 vxfenswap 实用程序表现为无限期地挂起。
2337916	[防护] 如果由于客户端正在注册而导致防护无法取消配置，则防护关闭脚本不会重试停止防护模块。
2311361	[防护] 如果防护正在运行且配置了 CoordPoint 资源，则引擎日志中每五分钟显示一次防护详细信息。
2253321	[防护] 如果在防护启动时任一协调点不可用，则防护无法启动。
2252470	[防护] 提供选项以迫使防护库使用各种 ID 类型通过标准查询或扩展查询来获取序列号。
2218448	[VxCPS] 如果在承载 CP 服务器的单节点集群中未安装或配置 LLT，则 cpsadm 命令失败。
2209664	[VxCPS] 即使在 single_cp=1 且需要在 vxfend_A.log 中设置警告消息的格式时，使用三个磁盘配置防护也会成功。
2209144	[VxCPS] 当使用 configure_cps.pl 脚本取消配置 CP 服务器时，出现语法错误。
2203070	[防护] 未能在 64 节点集群中配置防护，防护仅在前 33 个节点上有效。

事件	说明
2178126	[GAB] 如果 GAB 无法在内存不足的情况下（通常在置备不足的虚拟机设置中）以原子方式分配内存，则 GAB 无法启动。
2161816	[防护]对于大型集群而言，如果已配置基于系统的或基于组的首选防护策略，则在某些情况下，首选防护将不按预期方式工作。

2139883	[GAB] 在 RHEL5 更新 5 和更高版本中，会在控制台中重复看到类似如下的消息：
	`INFO: task gablogd:22812 blocked for more than 120 seconds.`
	`"echo 0 > /proc/sys/kernel/hung_task_timeout_secs" disables this message.`

2112742	[VxCPS] 在具有不同区域设置的节点上进行配置后，基于服务器的 I/O 防护无法启动。
2100896	[防护] 即使使用 vxfenswap 成功从基于服务器迁移到基于磁盘，也出现失败消息。
2085941	[VxCPS] 协调点服务器（CP 服务器）仅绑定到单个虚拟 IP 并在该 IP 上进行侦听。如果 CP 服务器无法建立与此虚拟 IP 的连接，则应用集群无法访问该 CP 服务器。因此，如果连接因 CP 服务器的虚拟 IP 所在的子网而失败，则您无法访问 CP 服务器，即使存在另一个子网，客户端可在该子网中通过一个不同的 IP 连接到 CP 服务器。
2076240	[VxCPS] 重新配置使用基于服务器的 I/O 防护（自定义防护模式）的应用集群时，安装程序不会在重新配置前从CP服务器中删除应用集群信息。因此，如果重新配置应用集群并选择使用相同的CP服务器在自定义模式下配置I/O防护，则重新配置应用集群的基于服务器的防护将失败。
1973713	[防护] CP 服务器代理的代理 XML 文件缺失。

捆绑代理中已解决的问题

表 1-9 列出了已解决的捆绑代理问题。

表 1-9 捆绑代理中已解决的问题

事件	说明
1923877	使用 `hanotify` 的代理在 vcs.mib 和 vcs_trapd 文件中应有对应的条目。
2212600	在 NFS 配置中使用 Phantom 资源时，Phantom 资源会擅自进入 FAULTED 状态。

事件	说明
1539927	删除目标资源后再重新添加它时，未正确填充依赖资源的 ArgListValues。
2255688	如果 DNS 服务器中已经存在资源记录，则 DNS 代理不应发送更新请求。
2255772	集群重新启动后，DNS 资源在 AutoStart 节点上应联机。
2593176	在出现序列裂脑情况时，DiskGroup 代理的 Online 入口点应从 vxdg import 命令中查找正确的返回代码。
2371672	由于仅支持 PRON 监视，因此对于 DB2 代理，请将 IMF 模式设置为 2。目前，此模式设置为 3。
2379649	Apache 代理无法支持非默认的二进制文件名称 (httpd2) 以及 httpd 二进制文件。
2489758	如果用户 Shell 为 csh 且配置了环境文件属性，则 Apache 代理无法使资源联机。
2514438	在 Apache 代理中增加对基准工具 ab2 及 ab 的支持。
2258553	手动导入且未受防护的磁盘组在 VCS 中依然处于联机状态，不执行任何操作，也不显示任何消息；即使集群配置为 UseFence = SCSI3 也是如此。
2423977	配置不存在的用户时，Application 代理将无法正常工作。
2415454	当 MonitorProgram 不存在时，Application 代理的 Monitor 入口点应报告 OFFLINE；而当它存在但不可执行时，则应报告 UNKNOWN。
2324342	在 GCO 环境中，DNS 资源的故障转移会造成 DNS 服务器中出现重复的资源记录。
2579773	在 RHEL6U1 和 SLES11SP1 风格中，Mount 代理不会装入 bind 文件系统。
2296386	IP 代理应设置有效的广播地址而非 0.0.0.0。
2318470	在未受 VCS 控制的情况下更改了在 IP 代理的界面上配置的网络掩码时，VCS 应显示一则警告消息。
2354244	由于 preonline_ipc 触发器失败，NFS 服务组无法进行故障转移。
2393939	更正 Apache 代理版本解析功能，使之适应 IBM HTTP Server 7.0。

事件	说明
2222781	在故障转移后 IP 代理无法发送正确的 ARP（属于 ARP REPLY 类型）。
2422980	在完成联机后，尽管进程看起来正在正确运行，但对 Process 资源进行监视的程序会出故障。
2406655	如果 Application 资源的监视类型为 PID 文件/MonitorProgram，则 Propcv action 入口会在引擎日志中显示错误消息。

VCS 引擎中已解决的问题

表 1-10 列出了已解决的 VCS 引擎问题。

表 1-10 VCS 引擎中已解决的问题

事件	说明
1948444	如果将集群地址属性修改为 NULL，则会显示无效的 IP 地址消息。
2085292	SFSYBASECE：针对 ASE 和 vxfend 依赖关系问题提供 resstatechange 脚本。
2173455	IState 的 hares -wait 命令不起作用。
2182462	VCS_GAB_TIMEOUT 仅限采用介于 30,000 ms 与 300,000 ms 之间的值。
2194478	覆盖资源级别的 ExternalStateChange 属性时，HAD 会转储核心。
2195609	当系统切换到模拟器的运行状态时，模拟器核心会转储。
2210718	如果非关键资源在组正在进入联机状态时出现故障，则 VCS 服务组将依然处于 STARTING|PARTIAL 状态。
2244182	当 main.cf 文件为空时，hacf -verify 命令将显示语法错误。
2252099	对于 VCS，并行的“非本地”父组不会自动启动。
2276242	如果在某些情况下并行 SG 的联机命令是使用 -any 标志执行的，则此命令将失败。
2285716	如果服务组中既有持久性资源处于 FAULTED 状态，也有非持久性资源处于此状态，则该服务组将无法重新启动。

事件	说明
2296173	在关闭或重新启动 SystemZone 中的节点时，故障转移策略不考虑 AutoFailover = 2 和 SystemZone。
2330981	向 SystemList 中添加节点或从中删除节点时，不应向服务组的 SystemList 中已经存在的节点上运行的代理发送有关资源的任何通知。
2345879	VCS 不应在计算出的防护权重值基础上加 1。
2398808	在 vcsenv 文件中未指定文件描述符的软限制。
2400234	对于混乱的节点，从集群中的其他节点查看时，其资源状态依然为 OFFLINE|UNABLE TO OFFLINE。
2406743	使用 hagrp -modify 命令向组中添加系统时，会报告持久性资源处于 OFFLINE（而非 FAULTED）状态。
2411865	如果系统中存在不响应的 NFS 装入，则代理的入口点可能会超时。
2416761	HAD 占用超过 99% 的 CPU 时间。多个 ha 命令在 pollsys() 中处于挂起状态。
2477302	在节点发生混乱时服务组未进行故障转移。
2479006	如果在 VCS 通过已出故障资源的路径（在组的 PathCount 仍为正数时）使资源脱机时，引擎收到第二条有关已脱机资源的脱机消息，则引擎核心将转储。
2482035	HAD 在 VxFEN 启动前停止。
2488867	当 VCS 使服务组或资源脱机或者将其故障转移到另一集群时，HAD 无法发送有关资源状态变化的确认消息。
2519988	无法从模拟器启动板使用 start cluster 启动任何集群。
2077414	ContainerInfo 属性的值在组级别的显示与在资源级别的显示不匹配。
2198335	使用 hares -display 命令显示 ResourceInfo 属性的值时存在的问题。
2204343	父服务组在与其之间存在 online local firm 依赖关系的子服务组具有 OnOnly 资源时不进行故障转移。
2216914	如果发生并发冲突且此时在一个节点上已使服务组脱机并对其进行了刷新，则 IntentOnline 属性会误设置为零。

事件	说明
2220677	当 VCSAPI_LOG_LEVEL 设置为非零值时，RemoteGroup 代理将崩溃。
2341239	具有组级管理员权限的用户无法对服务组执行操作。
2354935	`hacli -cmd` 命令会触发 HAD 核心转储。
2388052	对于 PreOnline 脚本的 whyonlining 参数，MANUAL 对应于手动联机；而 FAULT 则同时对应于故障转移和手动切换。不过，当手动切换服务组时，PreOnline 脚本的 whyonlining 参数将显示为 MANUAL。
2197899	在本地有依赖项的子服务组在其 systemlist 中始终应包含父服务组的 systemlist 中包含的所有系统。
2202616	有时，当节点重新启动时，即使服务组在其他位置处于联机状态，该服务组的 IntentOnline 属性也会设置为 2。这在以后会导致该服务组考虑 AutoStartList 属性。
2486414	在 GAB 处于禁用状态时，如果运行单个节点或独立的 VCS 集群，则会在日志中记录 GAB 错误。
2521535	针对无效键执行 `hares -modify -delete` 命令会以代码零返回。
2558997	当系统出故障时，在集群内的系统中 CurrentLimits 属性不会正确更新。
2292481	VRTSvcs 预卸载脚本检测到错误的 HAD 进程。
2434953	删除 VRTSvcs 软件包对 VRTSgab 软件包的依赖关系。
2527123	删除 liblltdb 库的静态链接。
2399895	如果两个或更多个父服务组在集群中的备用系统上处于联机状态，则对子服务组执行的 `hagrp -switch` 命令将失败。
2205747	VCS 服务的默认名称已从 vcs 更改为 vcs-app。
2329486	Preonline 触发器的 whyonlining 参数需设置为 SYSFAULT。

已解决的安装相关问题

表 1-11 已解决的安装相关问题

事件	说明
2061338	使大量进程资源联机时系统进入系统资源不足状态。
2494592	安装 VRTSvcs 软件包时，会覆盖 /opt/VRTSvcs/bin/vcsenv 文件。

已解决的 Enterprise Agent 问题

表 1-12 列出了已解决的 Enterprise Agent 问题。

表 1-12 已解决的 Enterprise Agent 问题

事件	说明
2124793	为 ASMInst 资源的 StartUpOpt 属性提供其他选项。
2202513	增加在关闭 Sybase 数据服务器期间对 Timeout 选项的支持。
2203201	VCS Cluster Manager（Java 控制台）不对 Sybase 和 SybaseBK 代理的密码进行加密。
2234530	在使 DB2 服务组联机后，DB2 代理无法向 IMF 注册用于进行 PRON 监视的 db2sysc 进程。
2271885	如果不设置 Listener 属性，则 Netlsnr 资源的 MonitorMethod 属性无法反映 IMF 值。
2336496	DB2 代理为特定分区更新 db2nodes.cfg 中的 switch-name，这是不正确的。应该为主机更新 switch-name。
2343816	增加对由策略管理的 Oracle 11gR2 数据库环境的支持。
2348684	增加 PRON 对以下 DB2 的支持：其 IMF 处于 MPP 模式和非 MPP 模式。
2392688	提供用于以只读模式为 Oracle 代理启动数据库的 SRVCTL READ ONLY 选项。
2403770	Sybase 代理脚本为 cat 命令设置的路径错误。
2407334	Sybase 代理的清除脚本选择进行删除的 IPC 对象类型不正确。
2480890	启用 Sybase 代理的 WaitForRecovery 属性后，恢复状态误显示为未知。

事件	说明
2554938	由于仅支持 PRON 监视，因此对于 DB2 代理，请将 IMF 模式设置为 2。目前，此模式设置为 3。
2367719	解决在启用了 selinux 时面临的 Oracle 代理中的虚拟防火练习问题。

已解决的 AMF 驱动程序相关问题

表 1-13 已解决的 AMF 内核问题

事件	说明
2507061	在 amfstat 输出中，将 argv0 标志的值从 AMF 驱动程序中复制出来时，此值会损坏。
2486501	当用户尝试向 AMF 驱动程序注册装入联机监视事件时，节点会发生混乱。
2392390	如果在未受 VCS 控制的情况下取消对 AMF 的配置，日志中会连续显示错误消息： “Failed to open [/dev/amf]: No such device (无法打开 [/dev/amf]: 没有找到此类设备)”
2386280	AMF：将模块版本从 1.0 更新到了 2.0
2323310	有时会允许基于进程的代理向 AMF 注册用于进行脱机监视的联机进程。
2301725	在极少数情况下，当系统调用进入 AMF 驱动程序与取消配置 AMF 驱动程序同时发生时，节点会发生混乱。
2255535	如果 Mount 代理使用 IMF 监视 VxFS 类型的装入，则只要 Mount 代理正在运行就无法卸载 AMF 驱动程序。
2238441	imf_register 入口点 (PRON) 误检测到 db2sysc 进程。
2213447	在特殊情况下取消对 Reaper 的注册时，`amfregister` 命令会返回不需要的消息。
2165304	在 imf_register 入口点中，每次注册后应刷新从 amfregister.xml 中读取的值。
2145014	如果在未受 VCS 控制的情况下用户从 AMF 取消注册某一事件，VCS 将不会从 AMF 收到有关该事件的任何状态变化通知。

Veritas Cluster Server：5.1 SP1 RP1 中已解决的问题

本节介绍了 5.1SP1RP1 版本的 Veritas Cluster Server 中已解决的事件。

表 1-14 Veritas Cluster Server 5.1 SP1 RP1 中已解决的问题

已解决的问题	说明
1949294	fdsetup 现在可以正确地分析包含诸如 - 之类的字符的磁盘名称。
1949303	fdsetup 不再允许使用不属于 RVG 的卷，这解决了可能导致 RVGSnapshot 代理失败的一种原因。
2011536	为 db2udb 代理增加了 IMF 支持。
2159991	解决了在日语版系统中配置 Veritas Storage Foundation for Oracle RAC 后 engine_A.log 文件中的消息所出现的一个问题。
2172181	解决了在日语版系统中配置 Veritas Storage Foundation for Oracle RAC 后 engine_A.log 文件中与 AMF 有关的 CAVF 代理消息所出现的一个问题。
2179652	db2udb 代理的监视脚本现在可以处理空属性值。
2184205	解决了 HAD 中的以下问题：如果父服务组与子服务组之间存在 online local firm 依赖关系，则父服务组不会进行故障转移。
2194473	如果覆盖静态属性时覆盖到资源级别，则 HAD 不再转储核心。
2205556	解决了 DNS 代理的脱机 EP 存在的以下问题：在多主记录的 OffDelRR=1 时，未删除所有 A/AAAA 记录。
2205563	现在 clean EP 在 OffDelRR=1 时可以正确地删除资源记录。
2205567	解决了以下问题：将属性设置为 master.vfd 会导致 DNS 代理无法查询 DNS 服务器。
2208675	现在会对 NIC/MultiNICA 监视程序中的广播 ping 进行返回值检查，这解决了可能导致在采用 Link 选项配置的 IPv6 中 MultiNic 资源进入 FAULTED 状态的一个原因。
2208901	解决了 RVGSnapshot 代理存在的一个问题。
2209337	解决了 VCSAPI 存在的以下问题：如果 VCSAPI 日志级别设置为非零值，RemoteGroup 代理便会崩溃。
2214539	解决了以下问题：重新启动节点有时会将组的 intentonline 设置为 2，即使该组在其他位置处于联机状态也是如此。这导致该组使用 autostartlist，并且不执行故障转移。
2217446	解决了导致 VRTSvcsag 安装失败的一个问题。
2218556	解决了 cpsadm 命令中的以下问题：如果在单节点集群中未安装或配置 LLT，该命令有时会失败。

已解决的问题	说明
2218561	解决了以下问题：MonitorTimeStats 会间歇性地误显示 303 秒。
2219955	解决了以下问题：即便在使用 VCS Steward 时也会发生裂脑情况。
2220749	解决了以下问题：Cluster Manager（Java 控制台）不对 Oracle 代理的 DBAPword 属性进行加密。
2241419	解决了以下问题：当根代理不是 VCS 节点时，halogin 在安全环境中无法工作。

Veritas Cluster Server：5.1 SP1 RP2 中已解决的问题

表 1-15 介绍了在 Veritas Cluster Server 5.1 SP1 RP2 中已解决的事件。

表 1-15 Veritas Cluster Server 5.1 SP1 RP2 中已解决的问题

已解决的问题	说明
2416842	_had 占用超过 99% 的 CPU 时间。多个 ha 命令在 pollsys() 中处于挂起状态
2411653	在 GAB 中添加了对最大消息大小的检查
2407755	Application 代理和 Netlsnr 代理失败
2407653	在强制卸载 AMF 模块的情况下，vxfs/ext3 的模块引用计数处理不当。
2406748	我们能够向 AMF 注册已经联机的进程来进行脱机监视。
2405780	当 Mii 设置为 0 时未通过电缆拔出测试
2405391	LLT：arp 确认数据包中应包含节点的节点名称。
2403851	AMF 状态显示模块已加载但未配置。
2403782	Sybase 代理脚本为 linux 上的 cat 命令设置的路径错误。
2403633	在组未完全脱机的情况下，也应允许更新 ContainerInfo 属性
2400485	一旦 vxfenconfig -c 采用模式 A 时返回了 EFAULT（“1036 Unable to configure... (1036 无法配置...)”），之后采用模式 B 运行 vxfenconfig -c 时就会全都失败，并出现 EBADMSG 错误（“1050 Mismatched modes... (1050 模式不匹配...)”）。
2400330	在 VCS 5.1SP1 中，whyonlining 的行为与所宣称的不符。

已解决的问题	说明
2399898	在 5.0MP3RP2 及更高版本中，如果有 2 个或更多个处于联机状态的父组位于备用节点上，则对子组运行 hagrp -switch 时失败。
2398807	VCS 应在 /opt/VRTSvcs/bin/vcsenv 中设置针对文件描述符的软限制。
2394176	vxfenswap 进程挂起，ps -ef 在一个节点上显示 vxfenconfig -o modify，但在其他节点上则不显示。vxfenswap -a cancel 终止停滞的操作。
2386326	无法配置防护，vxfenadm 为所有在 0x83 页中具有超过 96 个字节的 SCSI 查询数据的 LUN 输出相同的序列号
2382592	使用 hares -display 显示 SRDF 资源的 ResourceInfo 属性时存在问题
2382493	父服务组在与子服务组之间存在 online local firm 依赖关系的情况下不进行故障转移。
2382463	在 CPS 首选防护中的系统策略中到达边界条件 (10000) 时不增加 had 权重 (1)。
2382335	vxfentsthdw 无法在两个节点上选择相同的防护磁盘。
2381083	广播地址 0.0.0.0 是由 IP 代理设置的
2372483	SambaServerAgent 在 FileStore 5.7 中生成了核心转储。
2372072	hacf 的用户核心
2366201	对防护进行了增强，使之在绝大多数协调点都可用时启动。
2354932	hacli -cmd 在 5.1SP1RP1 系统中触发 had 核心转储
2330980	向 SystemList 中添加节点/从中删除节点时，不应向组的 SystemList 中已经存在的节点上运行的代理发送有关资源的任何通知。
2330045	当网络发生故障时，RemoteGroup 资源不脱机。
2330041	在将 SF 5.0MP3 RP2 升级到 SF5.1SP1 后，VCS 组依赖关系不将并行的父组联机。
2318334	Oracle 要求数据库的 $Oracle_home/lib 库位于 /usr/lib 之前，成为 LD_LIBRARY_PATH 中的第一个库。
2301731	因在系统关闭期间出现错误互斥而导致 amf_lock() 中出现混乱。
2287061	启用 amf 时，cfsmount 代理无法正常启动。向 AMF 驱动程序进行基本事件注册时失败。
2276622	无法使用 RamSan DMP 设备配置 SCSI-3 防护。

已解决的问题	说明
2271882	如果不在 Netlsnr 资源中设置 Listener 属性，则 MonitorMethod 属性无法反映 IMF 值。
2253441	未设置 NetMask 属性时，VCS 应设置正确的默认掩码
2528475	支持在 VCS5.x 的 preonline_ipc 中使用 IPMultiNIC/IPMultiNICB 类型。
2509515	使用 Options 属性和 B 类地址时，资源无法进入脱机状态。
2483964	在刚完成联机时，尽管进程看起来正在正确运行，但对 Process 资源进行监视的程序会出故障。
2483314	当有大量 Oracle 实例处于运行状态时，Oracle 代理核心会转储。（大约 50 个）
2483044	当在 check_failover 函数中针对 Resource.C 中的 gp->activecount()->gets32GL(nodename) == 0\" 进行断言时，采用 SIGSEGV 的 had 崩溃
2477372	LLT：通过减少唤醒调用减少了 lltd 的 CPU 占用量
2477296	在节点发生混乱时应用程序服务组未进行故障转移
2477280	出现并发冲突后系统重新启动时，应用程序资源未进行故障转移
2439772	当 Solaris 10 上的 SFHA5.1RP2 中发生网络中断后，WAC 资源脱机失败
2438261	无法执行从 scsi raw 到 scsi dmp 策略的联机迁移。
2426663	在 OCPR 上从自定义模式切换到 scsi3 模式时，vxfend 不会终止
2426572	使用 hagrp -modify 命令向组中添加系统时，会报告持久性资源处于 OFFLINE（而非 FAULTED）状态
2423990	配置不存在的用户时，Application 代理将无法正常工作。
2382559	联机迁移失败，并显示“I/O fencing does not appear to be configured on node (节点上似乎未配置 I/O 防护)”消息
2382460	即使在 single_cp=1 且需要在 vxfend_A.log 中设置警告消息的格式时，使用 3 个磁盘配置防护也会成功
2382452	使用 configure_cps.pl 脚本取消配置 CP 服务器时存在语法错误。
2367721	通过修改 owner.vfd 为虚拟防火练习启用 selinux permissive/enforcing。
2366701	关于在 VCS 属性中使用变量的查询

已解决的问题	说明
2366201	当绝大多数协调点都可用时，允许防护启动。
2364875	对捆绑代理进行增强，使其支持 RHEL 6 环境。
2330047	VCS Share 代理主机名比较区分大小写。
2511385	Sybase 的联机脚本在数据库恢复前将数据库标记为联机
2439695	即使用户选择不启用 VXFEN，也会加载 VXFEN 模块。
2426572	使用 hagrp -modify 命令向组中添加系统时，会报告持久性资源处于 OFFLINE（而非 FAULTED）状态
2411860	各种 VCS 服务组切换故障
2407755	Application 代理和 Netlsnr 代理失败
2405514	因在系统关闭期间出现错误互斥而导致 amf_lock() 中出现混乱。
2400330	在 VCS 5.1SP1 中，whyonlining 的行为与所宣称的不符
2382452	使用 configure_cps.pl 脚本取消配置 CP 服务器时存在语法错误
2372072	hacf 的用户核心
2296172	在关闭/重新启动 SystemZone 中的节点时，故障转移策略不考虑 AutoFailover = 2 和 SystemZone。
2393939	增强了 Apache 代理版本解析功能，使之适应 IBM HTTP Server 7.0。

5.1 SP1 PR2 版本中已解决的问题

本节介绍在 5.1SP1PR2 版本中已解决的事件。

表 1-16 在 5.1SP1PR2 版本中已解决的问题

事件	说明
2220674	如果 VCSAPI 日志级别设置为非零值，RemoteGroup 代理便会崩溃。
2187918	如果覆盖静态属性时覆盖到资源级别，则 HAD 会转储核心。
2211333	父服务组在与子服务组之间存在 online local firm 依赖关系的情况下不进行故障转移。

事件	说明
2198682	当防护是使用 3 个磁盘配置的时，即使 single_cp=1，也必须将警告消息记录到 vxfend_A.log 中。
2208017	ResourceInfo 显示限制在 20 个字符以内，当键值超过 20 个字符的限制时，不会将它们全部显示。因此，只会显示不超过 20 个字符限制的完整键值。

已知问题

本节介绍了本版本中的已知问题。

请参见相应的“版本说明”，以获取已知的该产品相关问题的完整列表。

请参见第 83 页的“文档”。

包含 LVMLogicalVolume 资源的 VCS 服务组发生故障转移后客户端上产生过期的 NFS 文件句柄

LVM 卷组的 VCS 服务组将在故障转移后自动联机。然而，客户端应用程序可能会失败或被过期的 NFS 文件句柄错误中断。

解决方法：若要避免服务组进行故障转移后客户端上产生过期的 NFS 文件句柄，请在 Share 资源的 Options 属性中指定 fsid=。

禁用存储时 NFS 集群 I/O 出现故障

NFS 集群中的 I/O 保存在共享磁盘或共享存储中。当禁用共享磁盘或共享存储与 NFS 集群的连接时，NFS 客户端的 I/O 会出现故障并且显示一个 I/O 错误。

解决方法：如果应用程序退出（出现故障/停止），请重新启动应用程序。

迁移本机 LVM 卷上的来宾 VM 可能导致 libvirtd 进程突然终止 [2582716]

在来宾 VM 映像位于本机 LVM 卷上时，由管理员启动的对该来宾的迁移可能导致 `libvirtd` 进程突然终止。

解决方法：手动启动 `libvirtd` 进程。

与安装相关的问题

本节介绍了安装和升级期间的已知问题。

在升级期间停止安装程序然后再恢复升级可能会冻结服务组 (2591399)

如果您在安装程序已停止一些进程后停止安装程序，然后再恢复升级，则服务组会因使用产品安装程序升级而冻结。

解决方法：在升级完成后，您必须手动取消冻结服务组。

手动取消冻结服务组

1 列出所有冻结的服务组

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

2 取消冻结所有冻结的服务组：

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

在手动升级过程中软链接被删除的问题

对 VRTSvlic RPM 执行手动升级（从 5.1 升级到 6.0）时，在先前安装中创建的一些软链接被删除。结果，在指定路径中找不到 `vxkeyless` 二进制文件。

为避免这种情况，请使用 `--nopreun` 选项。

例如：`rpm -Uvh --nopreun VRTSvlic-3.02.60.007-0.x86_64.rpm`

手动升级 VRTSvlic RPM时丢失无密钥产品级别 [2115662]

如果手动升级 `VRTSvlic` RPM，使用 `vxkeyless` 设置的产品级别可能会丢失。此时无法正确显示 `vxkeyless display` 命令的输出。若要避免此问题，请在手动升级 VRTSvlic RPM 时执行下列步骤。

1. 记下节点上配置为进行无密钥许可的产品清单。

   ```
   # vxkeyless display
   ```

2. 将产品级别设置为 NONE。

   ```
   # vxkeyless set NONE
   ```

3. 升级 VRTSvlic RPM。

```
# rpm -Uvh --nopreun VRTSvlic-3.02.60.007-0.x86_64.rpm
```

4. 还原步骤 1 中记下的产品清单。

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

当从 VCS 5.1 之前的版本升级 VCS 堆栈时，需要重新配置 MultiNICA IPv4RouteOptions 属性

默认情况下，5.1SP1 MultiNICA 代理现在使用 `ip` 命令。由于 `ip` 与 `ifconfig` 命令之间关于路由配置存在行为差异，MultiNICA 会刷新路由并为新的活动设备恢复路由。如果 MultiNICA 资源配置不打算利用 `ifconfig` 命令（请参见下表），则必须在 MultiNICA 资源定义中配置 IPv4RouteOptions 属性。

注意：RouteOptions 值由 `route` 命令使用，而 IPv4RouteOptions 值由 `ip route` 命令使用。为这两个属性配置的值是基本只与它们各自的命令相关。

表 1-17 是否配置属性，以及在升级期间需要执行的必要操作

Options	RouteOptions 和/或 IPv4AddrOptions	IPv4RouteOptions	注释	在升级期间需要执行的操作
已配置	可以或不可以配置	可以或不可以配置	这种情况下，会使用 `ifconfig` 命令。如果设置了 RouteOptions，则属性值用于使用命令 `route` 添加/删除路由。 配置 Options 属性时，会忽略 IPv4RouteOptions 值。	不需要配置 IPv4RouteOptions。

Options	RouteOptions 和/或 IPv4AddrOptions	IPv4RouteOptions	注释	在升级期间需要执行的操作
未配置	可以或不可以配置	必须配置	这种情况下，会使用 ip 命令。必须配置 IPv4RouteOptions 并使用 ip route 命令及该属性来添加/删除路由。 未配置 Options 属性时，会忽略 RouteOptions 值。	配置 IPv4RouteOptions 并设置默认网关的 IP。此属性的值通常如下所示：IPv4RouteOptions = "default via *gateway_ip*" 例如：IPv4RouteOptions = "default via 192.168.1.1"

升级 VRTSvlic 后存在的无密钥许可提示问题 [2141446]

从 5.1 升级到 VCS 更高版本后，一些无密钥许可证可能会遗留在系统中。因此，如果没有配置 VOM 服务器，可能会重复记录提示。

如果在升级到 VCS 的 5.1SP1 或更高版本之前使用的是无密钥许可证，则会发生此问题。升级后，可安装真正的密钥并运行 `vxkeyless set NONE`。在这种情况下，可能不会彻底删除无密钥的许可证，在两个月后将会看到记录的警告消息（如果没有配置 VOM 服务器）。这不会造成任何功能影响。

若要解决此问题，请执行以下步骤：

1. 记下节点上配置为进行无密钥许可的产品清单。运行 `vxkeyless display` 以显示列表。
2. 使用以下命令将产品级别设置为 *NONE*：

   ```
   # vxkeyless set NONE
   ```

3. 查找并删除遗留在系统中的无密钥许可证。要执行此操作，请对存储在 `/etc/vx/licenses/lic` 中的每个密钥执行以下步骤：

   - 使用以下命令，验证是否启用了密钥的 `VXKEYLESS` 功能：

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

   - 当且仅当启用了 `VXKEYLESS` 功能时，才删除该密钥。

   注意：执行搜索时，不要将 .vxlic 扩展名包括在搜索字符串中。

4. 使用以下命令还原以前的产品列表：

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

在安装 VRTSvcsag RPM 期间出现 SELinux 错误

在启用了 RHEL 5 SELinux 的计算机上安装 VRTSvcsag RPM 期间，您可能会观察到以下 SELinux 错误：

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

此错误是由于未正确安装 SELinux 软件包所致。因此，SELinux 命令可能无法正确运行。

解决方法：重新安装 SELinux 软件包，并通过 init 或 fixfiles 方法重新标记文件系统。

需要显式禁用安全 WAC 通信 [2392568]

如果您让 WAC 以安全方式通信（VCS 配置为安全模式）并且您禁用了 VCS 安全性，则禁用了 VCS 安全性的 WAC 将继续尝试以安全方式通信，且不会成功。因此，禁用 VCS 安全性后，需要显式禁用 WAC 安全性。

解决方法：没有解决方法。需要显式禁用安全 WAC 通信。

Web 安装程序没有用来从集群中删除节点的选项

Web 安装程序未提供用来从集群中删除节点的选项。

解决方法：手动从集群中删除节点。Web 安装程序或 CPI 中未提供用来删除节点的选项。

在第一个会话以后，如果浏览器仍处于打开状态，则 Web 安装程序不要求对同一 URL 再进行身份验证 [2509330]

如果您在安装或配置 VCS 后已经关闭了 Web 安装程序窗口，并打开了同一浏览器的其他窗口，则在后续会话中 Web 安装程序不再要求进行身份验证。由于没有用来从 Web 安装程序正常注销的选项，因此只要 Web 安装程序使用的浏览器在系统中处于打开状态，其会话便依然保持打开状态。

不过，此问题是特定于 URL 的，仅在您使用同一 URL 执行后续操作时才会观察到此问题。因此，如果您使用不同 URL 来实现您的目的，则每次您访问 Web 安装程序时浏览器都会提示进行身份验证。

解决方法：您可以使用不同的 URL 来访问 Web 安装程序。

如果在首个会话后浏览器仍打开，则Web安装程序不要求身份验证 (2509330)

如果在安装或配置VCS后关闭Web安装程序，并打开其他浏览器窗口，则Web安装程序在后续会话中不要求身份验证。由于没有用于注销Web安装程序的选项，因此只要系统上的浏览器处于打开状态，会话就会一直保持打开状态。

解决方法：确保所有浏览器窗口都已关闭以结束浏览器会话，然后重新登录。

在主节点上完成内核升级后，从属节点上的 cvm 组未联机 (2439439)

在一个节点上成功完成内核升级后，cvm 组未在另一个节点上联机。

解决方法：在执行滚动升级之前，确保集群未处于危险状态。

将 Veritas 产品升级到 6.0 时存在的 sfmh 发现问题 (2622987)

如果在升级到 6.0 前主机不向 VOM 报告，但 sfmh 发现正在运行，则在升级后 sfmh-discovery 可能无法启动。

解决方法：

如果主机不向 VOM 报告，请在升级到 6.0 前手动停止 sfmh-discovery。

如果存在锁同步问题，有时会显示不正确的服务器名称 (2627076)

使用基于 Web 的安装程序安装集群时，如果由于存在锁同步问题您选择将系统与 NTP 服务器同步，则您在消息中可能会看到 NTP 服务器名称，而非您的服务器名称。

解决方法：

忽略这些消息。此产品仍然安装在正确的服务器上。

VCS 的操作问题

对于 SLES10 上的镜像卷，LVMLogicalVolume online 入口点停止响应并超时 [2077294]

`LVMLogicalVolume` 使用 `lvchange` 命令激活逻辑卷。对于镜像卷，通过脚本调用 `lvchange` 命令时，该命令本身会停止响应。这会导致 online 入口点超时，且 `LVMLogicalVolume` 资源的 online 入口点停止响应。这是 SLES10 的一个问题。

在所有路径都已禁用的状态下，LVM SG 转移失败 [2081430]

如果已禁用了磁盘的所有路径，则 LVM2 vg 命令会停止响应，并等到至少还原一个磁盘路径为止。因为 LVMVolumeGroup 代理使用 LVM2 命令，此行为会导致 LVMVolumeGroup 代理的 online 入口点和 offline 入口点超时，并且 clean EP 会无限期停止响应。因此，该服务组无法故障转移到其他节点。

解决方法：您至少需要还原一个路径。

在 VCS 外部导入并激活本机 LVMVG 后服务组进入 PARTIAL 状态

如果在启动 VCS 前导入并激活 LVM 卷组，则尽管 LVMLogicalVolume 资源会联机，但 LVMVolumeGroup 仍保持脱机。这会导致服务组处于 PARTIAL 状态。

解决方法：必须手动使 VCS LVMVolumeGroup 资源脱机，或者在启动 VCS 前停用该资源并导出卷组。

在防火墙配置为阻止 TCP 通信的系统上，有些 VCS 组件无法工作

如果在安装了防火墙的系统上安装并配置 VCS，可能会出现以下问题：

- 如果使用 Global Cluster Option (GCO) 设置灾难恢复，则远程集群（位于辅助站点的集群）的状态将显示为 initing。
- 如果将防护配置为使用 CP 服务器，则防护客户端无法向 CP 服务器注册。
- 在服务器间建立信任关系时将失败。

解决方法：

- 确保必需的端口和服务未被防火墙阻止。有关 VCS 使用的端口和服务的列表，请参考《Veritas Cluster Server 安装指南》。
- 通过配置防火墙策略使 VCS 必需的 TCP 端口不会被阻止。有关所需的配置，请参考防火墙或操作系统供应商提供的相应文档。

与 VCS 引擎相关的问题

过高的 CPU 利用率可能导致 HAD 无法向 GAB 发送心跳

当 CPU 利用率非常接近 100% 时，HAD 可能无法向 GAB 发送心跳。[1818687]

代理框架可能会拒绝 hares -action 命令

当某个探查到的资源被禁用稍后又启用时，代理框架可能会拒绝 hares -action 命令，直到代理成功监视该资源。

当 triggerpath 中有多个前导或尾随斜杠时，触发器不会执行 [2368061]

在 TriggerPath 属性中指定的路径不得包含多个前导或尾随 \ 字符。

解决方法：从该路径中删除多余的前导或尾随 \ 字符。

在具有不正确 EngineRestarted 值的节点上服务组不会自动启动 [2397532]

通过 `hashadow` 进程重新启动 HAD 时，EngineRestarted 属性的值会暂时设置为 1，直到探查完所有服务组为止。所有服务组均探查完后，便会重置此值。如果另一节点上的 HAD 大致在同一时间启动，则它可能不会重置 EngineRestarted 属性的值。因此，由于 EngineRestarted 属性的值不匹配，服务组不会在新节点上自动启动。

解决方法：在 EngineRestarted 设置为 1 的节点上重新启动 VCS。

如果顶层资源处于禁用状态，则不会使组联机 [2486476]

如果没有任何依赖关系的顶层资源处于禁用状态，则其他资源将不会联机，并且会显示下面的消息：

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

解决方法：使处于禁用状态的最顶层资源的子资源联机。

在重新启动时 NFS 资源意外脱机并报告错误 [2490404]

VCS 不执行资源操作，因此，如果 HAD 多次重新启动一个代理进程，那么只有其中一个代理进程是有效的，其余进程都会中止，既不会退出也不会在外部停止。尽管此代理进程正在运行，但 HAD 无法识别到它，因而不会执行任何资源操作。

解决方法：强行停止此代理进程。

父组不会在子组处于联机状态的节点上联机 [2489053]

如果父组的 AutostartList 不包含子组处于联机状态的节点条目，便会发生这种情况。

解决方法：通过指定系统名称使父组联机，然后再使用 `hargp -online [parent group] -any` 命令使父组联机。

VCS 处于 LEAVING 状态时，无法修改临时属性 [2407850]

如果本地节点处于 LEAVING 状态，则用于修改临时属性的 `ha` 命令将遭到拒绝。

解决方法：从其他节点执行此命令，或者启用配置读/写。

如果既连接了安全 WAC 又连接了非安全 WAC，则 engine_A.log 每 5 秒钟会收到一次日志 [1539646]

GCO 中的两个 WAC 始终都必须以安全模式或非安全模式中的一种模式启动。如果既有安全 WAC 连接又有非安全 WAC 连接，则会导致向 engine_A.log 文件发送日志消息。

解决方法：以确保在 GCO 中的两个集群中，WAC 要么均以安全模式运行，要么均以非安全模式运行。

如果防火练习组在辅助集群中联机，则 Oracle 组无法联机 [2556835]

如果并行全局服务组在本地集群中出现故障，并且在本地集群中未找到故障转移目标，它会尝试将服务组故障转移到远程集群。但是，如果服务组的防火练习在远程集群中联机，则将违反 offline local 依赖关系，全局服务组将无法故障转移到远程集群。

解决方法：将防火练习服务组脱机，在远程集群中将该服务组联机。

POSTONLINE 和 POSTOFFLINE 触发器在默认情况下未启用 [2567387]

在 VCS 6.0 之前，POSTONLINE 和 POSTOFFLINE 触发器在默认情况下已启用，因此只要有服务组联机，这两个触发器便会执行。在 VCS 6.0 中，您必须在升级到 VCS 6.0 后显式启用 POSTONLINE 和 POSTOFFLINE 触发器。

另外，也可采用下面这种方法使这两个触发器在升级后执行：

1. 升级前，在 /etc/default/vcs 中设置 vcs_start = 0

   这样，在升级后 HAD 便不会启动。

2. 将现有 VCS 升级到 VCS 6.0。
3. 在 /etc/default/vcs 中设置 vcs_start = 1
4. 使用 `hastart` 在每个节点上启动 VCS。
5. 按如下方式在 main.cf 中为所需的组设置 TriggersEnabled：

   ```
   TriggersEnabled @<systemname>={POSTONLINE, POSTOFFLINE}
   ```

触发器行为示例：

```
group scriptfileonoff (
        SystemList = { vcssx235 = 0, vcssx236 = 1 }
```

```
AutoStartList = { vcssx235, vcssx236 }
TriggersEnabled @vcssx235 = { POSTONLINE }
)
MyFileOnOff MFileOnOff (
        PathName = "/tmp/mf1"
        )
MyFileOnOff MFileOnOff1 (
        PathName = "/tmp/mf2"
```

在一个节点上看到两个 CmdServer 实例正在运行 [2399292]

您可能看到一个节点上有两个CmdServer实例正在运行。其中一个实例使用IPv4，另一个使用 IPv6。

不过，这不会对功能有任何影响。

解决方法：没有解决方法。

服务组可能会在刷新和强制刷新操作之后无法联机 [2616779]

在脱机操作未成功的服务组上执行刷新和强制刷新操作之后，该服务组可能会无法联机。

解决方法：如果脱机操作未成功，则使用强制刷新命令而非常规刷新操作。如果已执行常规刷新操作，则使用 `-any` 选项启动该服务组。

与捆绑代理相关的问题

在 I/O 路径出现故障期间将自动激活 LVM 逻辑卷 [2140342]

在 I/O 路径出现故障期间自动激活了 LVM 逻辑卷。这样会导致 VCS 代理报告“并发冲突”错误，并使资源组临时脱机/联机。这是由本机 LVM 的行为导致的。

解决方法：启用“LVM Tagging (LVM 标记)”选项可避免此问题。

启动KVM虚拟化来宾或启动联机的KVMGuest资源后出现系统混乱 [2337626]

启动 KVM 来宾或启动联机的 KVMGuest 资源后，出现系统混乱。很少会观察到此问题。

观察到此问题是因为在libvirtd进程中出现文件描述符泄漏。libvirtd进程针对文件描述符的最大文件打开限制为1024个。您有时可能会观察到在KVM来宾启动时打开了超过 1024 个文件描述符。因此，如果超出了此最大文件打开限制，则任何尝试启动KVM来宾或打开新文件的行为都会导致系统发生混乱。VCS在怀疑libvirtd进程中出现文件描述符泄漏时，无法控制此行为。

解决方法：此问题无明确的解决方案；不过，您可以在 /proc/<libvirtd 的 PID>/fd/ 中检查 libvirtd 进程打开的文件数目。如果文件计数超过 1000，请使用下面的命令重新启动 libvirtd：

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

即使是已损坏的来宾或未安装操作系统的来宾，KVMGuest 的 monitor 入口点也会报告资源处于 ONLINE 状态 [2394235]

即使来宾操作系统已损坏甚至来宾内未安装操作系统，KVMGuest 的 monitor 入口点也会报告资源处于 ONLINE 状态。VCS KVMGuest 代理使用 virsh 实用程序来确定来宾的状态。来宾启动后，virsh 实用程序会报告这个正在运行的来宾处于正在运行状态。根据此正在运行状态，VCS KVMGuest 代理的 monitor 入口点报告该资源处在 ONLINE 状态。

如果来宾内未安装操作系统或者所安装的操作系统已损坏，那么 virsh 实用程序仍会报告该来宾处于正在运行状态。因此，VCS 也会报告该资源处在 ONLINE 状态。由于 RedHat KVM 不提供来宾操作系统的状态，因此 VCS 无法根据操作系统的状态检测来宾状态。

解决方法：此已知问题无解决方法。

LVM 逻辑卷在采用安装在 SLES11 上的 reiserfs 文件系统时可能会停滞 [2120133]

LVM 逻辑卷在采用安装在 SLES11 上的 reiserfs 文件系统时，如果持续不断地在集群节点之间切换包含该逻辑卷的服务组，则该逻辑卷可能会停滞。

在以下条件下可能会观察到此问题：

- 在持续不断地切换采用 reiserfs 文件系统的 LVM 逻辑卷所属的服务组期间。
- 仅在 SLES11 上且采用 reiserfs 文件系统时。
- 是由于 SLES11 上 device-mapper 的行为所致。

不过，此问题并不一致。有时 device-mapper 在处理逻辑卷时会出现停滞，从而导致逻辑卷挂起。在这种情况下，LVM2 命令也无法清除该逻辑卷。VCS 无法处理这种情况，因为 LVM2 命令无法停用挂起的逻辑卷。

解决方案：在这种情况下，必须重新启动出现逻辑卷停滞的系统。

手动启动 KVMGuest 资源时，该资源会在故障转移目标节点上联机 [2394048]

VCS KVMGuest 资源在手动启动该 VM 来宾时会在故障转移目标节点上联机，即使该资源在主节点上处于联机状态也是如此。

基于 Red Hat 内核的虚拟机 (KVM) 允许在多个节点上使用同一来宾映像启动来宾。此来宾映像位于集群文件系统中。如果此来宾映像存储在集群文件系统中，那么它会同时在所有集群节点上变为可用状态。

如果 VCS 的 KVMGuest 资源已通过使用集群文件系统中的来宾映像启动来宾使其在一个节点上联机，那么当您手动在其他节点上启动同一来宾时，Red Hat KVM 不会阻止您执行此操作。不过，由于此特定来宾受 VCS 控制，因此 VCS 不允许该资源同时在多个节点上处于 ONLINE 状态（除非它在并行服务组配置中）。VCS 可以检测到此并发冲突，并关闭第二个节点上的来宾。

注意：对于 CVM 原始卷，也观察到了此问题。

解决方法：在 VCS 中不需要任何解决方法。VCS 的并发冲突机制可以妥善处理这种情况。

Application 代理无法处理用户为 root、设置了 envfile 且 shell 为 csh 的情况 [2584285]

Application 代理无法处理用户为 root、设置了 envfile 且 shell 为 csh 的情况。Application 代理使用 `system` 命令为 root 用户执行 `Start`/`Stop`/`Monitor`/`Clean` 程序。这会在 `sh` shell 中执行 `Start`/`Stop`/`Monitor`/`Clean` 程序，正因为此，当 root 用户采用 csh shell 且相应地写入 EnvFile 时会出现错误。

解决方法：请勿设置 `csh` 作为 root 用户的 shell。请改用 `sh` 作为 root 的 shell。

如果您将 DiskReservation 代理的大量资源配置在单个服务组中，此代理可能会调用 clean [2336391]

如果您将大量 DiskReservation 资源（超过 400 项资源）配置在单个服务组中并尝试使该服务组脱机，DiskReservation 代理可能会调用 clean。

在包含超过 400 项 DiskReservation 资源及等量 Mount 资源的单一服务组配置中，服务组脱机可能会导致 DiskReservation 代理调用 clean 入口点。如果配置大约 150 项资源，则不会观察到此问题。

解决方法：没有解决方法。

如果所配置的 MountPoint 路径包含空格，则针对 Mount 资源进行的 IMF 注册将失败 [2442598]

如果为 Mount 资源配置的 MountPoint 在其路径中包含空格，则 Mount 代理可以正确地使该资源联机，但为进行 ONLINE 监视而进行的 IMF 注册将失败。这是因为 AMF 驱动程序不支持在路径中使用空格。此代理会处理前导空格和尾随空格，对于此类资源，可以进行 IMF 监视。

解决方法：对于路径中包含空格的资源，Symantec 建议禁用 IMF 监视。有关如何为资源禁用 IMF 监视的信息，请参考《Veritas Cluster Server 管理指南》。

如果卷是在 VCS 外部卸载的，DiskGroup 代理将无法使资源脱机

如果卷是使用 `umount -l` 命令在 VCS 外部卸载的，DiskGroup 代理将无法使资源脱机。

假设有一个服务组包含 DiskGroup、Volume 和 Mount 资源，且此服务组处于联机状态。Mount 资源在 VxFSMountLock 处于启用状态的条件下装入了卷。那么，尝试使用 `umount -l` 系统命令手动卸载此卷时会导致装入点消失；但文件系统锁依然保持原样。由于此卷的装入被锁定，因此无法停止此卷，进而也无法导入相应磁盘组。这会导致磁盘组资源进入 UNABLE to OFFLINE 状态。此外，任何尝试重新装入此文件系统的操作都将失败，因为其装入已经被锁定。此问题是由 Linux 上的文件系统行为所致。

解决方法：装入锁处于启用状态时，请勿使用 `umount -l` 命令卸载 VxFS 文件系统；而应先使用 `/opt/VRTS/bin/fsadm` 命令解锁装入点，然后再卸载文件系统。

在拔出网络电缆的情况下，RemoteGroup 代理不进行故障转移 [2588807]

在拔出网络电缆的情况下，ControlMode 设置为 OnOff 的 RemoteGroup 资源可能不会故障转移到集群中的其他节点。如果此 RemoteGroup 资源无法连接到远程集群，其状态会变为 UNKNOWN。

解决方法：

- 连接到远程集群并设法使此 RemoteGroup 资源脱机。
- 如果无法连接到远程集群并且您希望将本地服务组关闭，请将 RemoteGroup 资源的 ControlMode 选项更改为 MonitorOnly。然后设法使此 RemoteGroup 资源脱机。此资源脱机后，请将此资源的 ControlMode 选项更改为 OnOff。

服务组中的并发冲突 [2555306]

如果存储连接断开或 VxDMP 下的所有路径都已禁用且 PanicSystemOnDGLoss 设置为 0，那么 Volume 资源可能会发生并发冲突和数据损坏。

发生这种情况的条件如下：

- 在集群环境/配置中，如果集群范围的 UseFence 属性设置为 SCSI3 且服务组包含 PanicSystemOnDGLoss 属性设置为 0（零）的 Volume 资源和 DiskGroup 资源，则会发生这种情况。
- 如果存储连接已断开或 VxDMP 下的所有路径都已禁用，则 VCS 会对服务组执行故障转移。如果在服务组出故障的节点上恢复了存储连接且未手动逐出磁盘

组，那么，假如磁盘组在服务组故障转移期间未逐出，则该卷可能会启动。因此，卷资源的状态在两个节点上都会显示为联机，从而造成并发冲突。这可能会导致数据损坏。

解决方法：确保磁盘组在存储连接恢复后尽快逐出。

建议每当配置磁盘组资源时都要配置 Volume 资源，并根据需要将 PanicSystemOnDGLoss 属性设置为 1 或 2。

在 CVM 环境中使用 FireDrill 设置 VVR 可能失败并出现 CFSMount 错误 [2564411]

当您尝试通过 Java 控制台或 `hagrp -online` 命令使 FireDrill 服务组联机时，CFSMount 资源会进入故障状态。

解决方法：运行 `fsck` 命令。您可以在引擎日志中找到这些命令。

Coordpoint 代理一直处在故障状态 [2555191]

Coordpoint 代理一直处在故障状态，因为它检测到 `rfsm` 处于重放状态。

解决方法：清除此故障并重新配置防护。

RVGsnapshot 代理无法处理使用 vxvset 创建的卷集 [2553505]

RVGsnapshot 代理无法处理使用 `vxvset` 创建的卷集。在 VVR 环境中进行防火练习期间，会出现这种情况。

解决方法：没有解决方法。

如果 VCS 找不到监视程序，则 engine_A.log 中不存在日志消息 [2563080]

当 VCS 找不到符合以下条件的监视程序时，engine_A.log 中不会记录任何消息：其 KVM 来宾包含处于联机状态的服务组。

解决方法：如果资源状态未知，还可以参考代理日志文件中的消息。

NFS 不支持 IPv6 [2022174]

NFS 不支持 IPv6。

解决方法：没有解决方法。

部分代理如果在完全升级到 VCS 6.0 之前为联机状态，则在完全升级之后可能无法联机 [2618482]

NFSRestart、DNS 和 LogicalVolumeGroup 类型的资源如果在完全升级到 VCS 6.0 之前为联机状态，则在完全升级之后无法自动联机。

解决方法：如果这些资源之前为联机状态，则请在升级之后手动将其联机。

与 VCS 数据库代理相关的问题

运行状况检查监视对 VCS Agent for Oracle 不起作用 [2101570、1985055]

VCS 的 Oracle 代理中的运行状况检查监视不起作用，因为 Oracle 提供的运行状况检查 API 不兼容。

解决方案：通过将 MonitorOption 属性设置为 0（零）禁用运行状况检查监视。

有意脱机对 VCS Agent for Oracle 不起作用 [1805719]

因为运行状况检查监视会出现问题，所以有意脱机对 VCS Agent for Oracle 不起作用。

确保 ohasd 在 init 脚本中具有相应条目 [1985093]

确保 ohasd 进程在 init 脚本中具有相应条目，以便进程终止或计算机重新启动时可以自动重新启动该进程。

解决方法：重新启动 `ohasd` 进程。在 `/etc/inittab` 文件中添加 `ohasd process` 进程，以确保此进程被终止时或重新启动计算机时会自动重新启动此进程。

在 SLES11 平台上未对 Oracle 代理进行运行状况检查监视 [1938167]

Oracle 代理不支持在 SLES11 平台上进行运行状况检查监视。

ASMInstAgent 不支持在 ASM 磁盘组上放置 ASM 实例的 pfile/spfile

ASMInstAgent 不支持在 ASM 磁盘组上放置 ASM 实例的 pfile/spfile。

解决方法：

在默认的 $GRID_HOME/dbs 目录中放置 pfile/spfile 的副本，以确保在 ASM 实例启动过程中选取该副本。

VCS Agent for ASM：ASMInst 代理不支持健康状况检查监视

ASMInst 代理不支持健康状况检查监视。

解决方法：将 MonitorOption 属性设置为 0。

为某些 Oracle 错误指定 NOFAILOVER 操作

Veritas High Availability Agent for Oracle 增强了对在执行详细信息监视期间遇到的 Oracle 错误的处理功能。代理使用参考文件 oraerror.dat，该文件包括 Oracle 错误以及应采取的操作的列表。

有关这些操作的说明，请参见《Veritas Cluster Server Agent for Oracle 安装和配置指南》。

目前，在遇到以下 Oracle 错误时该参考文件会指定 NOFAILOVER 操作：

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

NOFAILOVER 操作是指代理将资源的状态设置为 OFFLINE 并冻结服务组。可以停止代理，编辑 oraerror.dat 文件，然后将 NOFAILOVER 操作更改为适合您环境的另一项操作。该更改在重新启动代理时生效。

在 ASMDG 资源脱机后 ASM 实例无法卸载 VxVM 卷

在 ASMInstance 资源属于某个单独并行服务组的配置中，即使在使 ASMDG 资源脱机之后 ASM 实例也无法卸载卷。因此，无法使 Volume 资源脱机。将 VxVM 卷用作 ASM 磁盘组时，会发生此问题。 [918022]

解决方法：将 ASMInstance 资源配置为配置有 ASMDG 资源的故障转移服务组的一部分。

与代理框架相关的问题

在负载繁重的情况下，代理可能无法进行心跳通信 [2073018]

在负载繁重的情况下，代理可能无法使用 VCS 引擎进行心跳通信。

当代理未获得足够的CPU来执行其任务时，以及代理心跳超过在AgentReplyTimeout属性中设置的时间时，可能会发生这种情况。VCS引擎将因此而停止并重新启动代理。VCS 引擎在停止并重新启动代理时，将生成一个日志。

解决方法：如果您注意到系统负载可能很繁重，则：

- 可将 AgentReplyTimeout 属性的值设置为一个较高的值
- 可使用 AgentClass 和 AgentPriority 属性增加代理的调度等级和调度优先级，以避免供代理使用的 CPU 不足。

代理框架无法处理依赖属性的前导空格和尾随空格

代理框架不允许依赖资源的目标资源属性名称中存在空格。

解决方法：请不要在依赖资源的目标资源属性名称中输入前导空格和尾随空格。

代理框架检测不到服务线程在入口点内是否挂起 [1511211]

在少数情况下，代理框架检测不到是否所有服务线程在 C 入口点内都已挂起。在这种情况下，它可能无法成功取消这些服务线程。

解决方法：如果代理的服务线程挂起，请发送终止信号以重新启动该代理。请使用以下命令：`kill -9 hung agent's pid`。`haagent -stop` 命令在此情况中不起作用。

使资源联机和脱机时出现与 IMF 有关的错误消息 [2553917]

对于向 AMF 注册的资源，如果显式地或通过某一收集进程运行 `hagrp -offline` 或 `hagrp -online` 来分别使资源脱机或联机，则在任一种情况下 IMF 都会显示错误消息。

所显示的错误是预期行为，不会以任何方式影响 IMF 功能。

解决方法：没有解决方法。

与全局集群相关的问题

全局集群环境中的安全站点上的引擎日志文件收到过多日志消息 [1539646]

当 WAC 进程以安全模式在某个站点上运行，而另一个站点没有使用安全模式时，安全站点上的引擎日志文件将每 5 秒钟接收一次日志。

解决方法：全局集群中的两个 WAC 进程必须始终在安全或非安全模式下启动。安全和非安全 WAC 连接会导致上述消息大量充斥引擎日志文件。

防火练习服务组在辅助站点上脱机之前，应用程序组尝试在主站点上联机 (2107386)

应用程序服务组在主站点上联机，而同时防火练习服务组尝试脱机，从而导致应用程序组发生故障。

解决方法：确保应用程序服务组在主站点上联机之前，防火练习服务组在辅助站点上完全脱机。

与 LLT 相关的问题

本节介绍此版本中已知的 LLT 相关问题。

LLT 可能无法检测绑定的 NIC 何时启动 (2604437)

如果 LLT 是通过绑定的 NIC 配置的，并且使用 `ifconfig` 命令关闭了该绑定的 NIC，则 LLT 会将相应的链接标记为断开。当使用 `ifconfig` 命令再次启动绑定的 NIC 时，LLT 无法检测到此更改并将该链接标记为已启动。

解决方法：关闭所有端口，重新启动 LLT，然后再次打开端口。

当在 NIC 上配置 vlan 时，无法构成 LLT 连接 (2484856)

当在已用来配置 LLT 链路的 NIC 上配置 vlan 时，无法构成 LLT 连接。

解决方法：如果希望稍后配置 vlan，则在配置 LLT 时不要在 `llttab` 文件中指定 NIC 的 MAC 地址。如果已指定 NIC 的 MAC 地址，请从 `llttab` 文件中删除 MAC 地址，在重新启动 LLT 之前更新该文件。

LLT 端口统计数据有时显示 recvcnt 大于 recvbytes (1788315)

随着每个数据包的接收，LLT 会增大下列变量：

- recvcnt（每增加一个数据包增加 1）
- recvbytes（按每个数据包的大小增加）

这两个变量均为整数。随着流量的恒定，recvbytes 会迅速达到或超过 MAX_INT。这可能会导致 recvbytes 值小于 recvcnt 值。

但这并不影响 LLT 功能。

在大型集群配置中 LLT 可能会误声明节点的端口级连接 (1809827)

当端口在集群的节点上频繁注册和取消注册时，LLT 可能声明端口级连接与另一个对等节点共存。这会在某些罕见情况下发生，即使对等节点上甚至未注册端口。

与 GAB 相关的问题

本节介绍此版本中已知的 GAB 相关问题。

当取消初始化 GAB 客户端时，gabdebug -R GabTestDriver 命令将 refcount 值记录为 2 (2536373)

在使用 -nodeinit 选项取消注册 gtx 端口后，gabconfig -C 命令将 refcount 显示为 1。但是，当运行强制性的 deinit 选项 (gabdebug -R GabTestDriver) 来取消初始化 GAB 客户端时，将记录类似如下的消息。

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

refcount 值在内部按 1 递增。但是，refcount 值显示作为 2，这与 gabconfig -C 命令输出冲突。

集群在重新配置期间发生混乱 (2590413)

当集群重新配置时，GAB广播协议在顺序请求路径中遇到争夺情况。这种情况会在极短的时间段中发生，最终导致 GAB 主节点混乱。

与 I/O 防护相关的问题

本节介绍此版本中已知的 I/O 防护相关问题。

CP 服务器反复记录不可用的 IP 地址 (2530864)

如果协调点服务器（CP 服务器）无法侦听 vxcps.conf 文件中提到的或使用命令行动态添加的任何 IP 地址，则 CP 服务器定期记录错误以指示该故障。记录将一直继续，直到成功绑定该 IP 地址。

```
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.
```

解决方法：使用 cpsadm 命令的 rm_port 操作，从侦听的 IP 地址中删除出现错误的 IP 地址。

有关更多详细信息，请参见《Veritas Cluster Server 管理指南》。

即使集群节点未向 CP 服务器注册，防护端口 b 也会出现几秒钟 (2415619)

如果您在集群节点的 vxfenmode 文件中提供协调点服务器（CP 服务器）信息，然后启动防护，则即使集群节点未在 CP 服务器上注册，防护端口 b 也会在出现几秒钟后消失。

解决方法：要解决此问题，请将集群节点信息和用户信息手动添加到 CP 服务器。或者，您可以使用安装程序，安装程序会在配置期间将集群节点信息和用户信息添加到 CP 服务器。

如果应用集群中未配置 LLT，则 cpsadm 命令失败 (2583685)

如果在运行 cpsadm 命令的应用集群节点上未配置 LLT，则 cpsadm 命令无法与协调点服务器（CP 服务器）通信。您会发现类似如下的错误：

```
# 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.
```

不过，如果您在 CP 服务器上运行 cpsadm 命令，则即使在承载 CP 服务器的节点上未配置 LLT，此问题也不会出现。如果未配置 LLT，则 CP 服务器节点上的 cpsadm 命令总是将 LLT 节点 ID 假设为 0。

根据 CP 服务器与应用集群之间的协议，当您在应用集群节点上运行 cpsadm 时，cpsadm 需要将本地节点的 LLT 节点 ID 发送到 CP 服务器。但是，如果临时取消配置 LLT，或者该节点是未配置 LLT 的单节点 VCS 配置，则 cpsadm 命令无法检索 LLT 节点 ID。在这种情况下，cpsadm 命令失败。

解决方法：将 CPS_NODEID 环境变量的值设置为 255。如果 cpsadm 命令无法从 LLT 获取 LLT 节点 ID，则该命令读取 CPS_NODEID 变量并且继续进行操作。

如果 CP 服务器中缺少集群详细信息，则 VxFEN 失败，并显示已存在裂脑消息 (2433060)

当您启动基于服务器的 I/O 防护时，节点可能不会加入集群，并在日志中显示类似如下的错误消息：

在 /var/VRTSvcs/log/vxfen/vxfen.log 文件中：

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

在 /var/VRTSvcs/log/vxfen/vxfen.log 文件中：

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

应用集群中的 vxfend 后台驻留程序查询协调点服务器（CP 服务器），以检查 GAB 成员集中显示的集群成员是否已向 CP 服务器注册。如果应用集群出于某种原因未

能与CP服务器联系，则防护无法确定CP服务器上的注册情况，因此保守地假设已存在裂脑。

解决方法：尝试在应用程序上启动 VxFEN 之前，请确保集群详细信息（例如集群名称、UUID、节点和权限）已添加到 CP 服务器。

由于 RSH 限制，vxfenswap 实用程序不检测协调点验证是否失败 (2531561)

vxfenswap 实用程序在每个集群节点上通过 RSH 或 SSH 运行 vxfenconfig -o modify命令，以执行协调点验证。如果您使用RSH（带有 -n选项）运行vxfenswap命令，则 RSH 不检测节点上的协调点验证是否失败。vxfenswap 继续从这点进行操作，如同所有节点上的验证已成功一样。但是，稍后当它尝试将新协调点提交到VxFEN驱动程序时，则会失败。失败之后，它回滚整个操作，彻底退出，并显示一个非零错误代码。如果您使用 SSH（不带 -n 选项）运行 vxfenswap，则 SSH 可以正确地检测协调点验证的失败并立即回滚整个操作。

解决方法：将 vxfenswap 实用程序与 SSH（不带 -n 选项）一同使用。

重新启动后防护在其中一个节点上不生效 (2573599)

如果 VxFEN 取消配置在内核中未完成其处理，而同时您又尝试启动 VxFEN，则可能会在 /var/VRTSvcs/log/vxfen/vxfen.log 文件中看到以下错误：

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

但是，gabconfig -a 命令的输出并不列出端口 b。vxfenadm -d 命令显示以下错误：

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

解决方法：过一段时间后再启动 VxFEN。

以安全模式将 CP 服务器升级到 6.0 后，cpsadm 命令失败 (2478502)

以安全模式将协调点服务器（CP服务器）升级到6.0后，cpsadm命令可能会失败。如果未从系统中删除旧的 VRTSat RPM，cpsadm 命令会加载系统中存在的旧安全库。当安装程序在 CP 服务器上运行 cpsadm 命令以添加或升级 VCS 集群（应用集群）时，安装程序也会失败。

解决方法：在 CP 服务器的所有节点上执行下列步骤：

- 将 cpsadm 重命名为 cpsadmbin。

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

- 创建一个包含以下内容的 /opt/VRTScps/bin/cpsadm 文件：

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

- 向此新文件提供以下权限：

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

如果未提及默认端口，则基于服务器的防护不会正确启动 (2403453)

如果您在自定义模式下配置防护并且未提供默认端口，则防护启动。但是，vxfenconfig -l 命令输出不列出端口号。

解决方法：当将自定义防护用于至少一个 CP 服务器时，请在 /etc/vxfenmode 文件中保留 port=<port_value> 设置。默认端口值为 14250。

安全 CP 服务器不与将 127.0.0.1 作为 IP 地址的 localhost 进行连接 (2554981)

cpsadm 命令不连接到将 127.0.0.1 作为 IP 地址的 localhost 上的安全 CP 服务器

解决方法：使用任何通过 CP 服务器配置并在本地节点上探查到的虚拟 IP 来连接安全 CP 服务器。

无法自定义 30 秒期限 (2551621)

如果 vxcpserv 进程在启动期间无法绑定到某 IP 地址，它会每间隔 30 秒尝试绑定到该 IP 地址。此间隔是不可配置的。

解决方法：没有解决方法。

当使用 configure_cps.pl 脚本配置 CPSSG 时，创建的 NIC 资源的名称不正确 (2585229)

举例来说，当第 m 个 VIP 映射到第 n 个 NIC 且每个 m 不等于 n 时，configure_cps.pl 脚本创建的 NIC 资源的名称不正确。在这种情况下，虽然 CPSSG 可以继续无问题地工作，但是当您使用 configure_cps.pl 取消配置 CPSSG 时，它将失败。

解决方法：要取消配置 CPSSG，必须从 VCS 配置中删除 CPSSG 配置。

6.0 中的 Veritas Cluster Server Agents for Veritas Volume Replicator 已知问题

以下是 6.0 版本中新增的其他 Veritas Cluster Server Agents for Veritas Volume Replicator 已知问题。

fdsetup 无法正确解析包含诸如 - 之类的字符的磁盘名称 (1949294)

fdsetup 无法正确解析包含诸如 - 之类的字符的磁盘名称。

与智能监视框架 (IMF) 有关的问题

创建防火练习设置时出现注册错误 [2564350]

使用 `Firedrill setup` 实用程序创建防火练习设置时，VCS 遇到下面的错误：

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

在防火练习操作期间，VCS 可能会在引擎日志中记录与 IMF 注册失败有关的错误消息。之所以出现这种错误，是因为在防火练习服务组中，还有另一项 CFSMount 资源正在通过 IMF 监视同一 MountPoint。这两项资源会尝试在同一 MountPoint 上注册联机/脱机事件，因此其中一项资源的注册将失败。

解决方法：没有解决方法。

使用 haimfconfig 命令时显示 Pearl 错误

使用 `haimfconfig` 命令时显示 Pearl 错误：

```
Pearl errors seen while using haimfconfig command
```

此错误发生的原因是在 main.cf 中为特定于类型的配置文件指定了绝对路径。目前，`haimfconfig` 不支持在 main.cf 中为特定于类型的配置文件指定绝对路径。

解决方法：用实际文件名取代实际路径，然后将该文件从其绝对位置复制到 `/etc/VRTSvcs/conf/config` 目录。

例如，如果 main.cf 中以如下方式包含 OracleTypes.cf：

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

那么应在 main.cf 中将上述内容替换成以下内容：

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

与 Cluster Manager（Java 控制台）相关的问题

此部分介绍了与 Cluster Manager（Java 控制台）相关的问题。

加载模板时 Cluster Manager（Java 控制台）可能会显示错误 (1433844)

在 Cluster Manager 中，可以从“Tools (工具)”>“Templates (模板)”菜单中访问“Template View (模板视图)”。如果在 VCS 集群设置中配置了 Storage Foundation，则 Cluster Manager 加载模板时可能会发生以下错误。

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

解决方法：忽略该错误。

某些 Cluster Manager 功能在防火墙设置中不起作用 [1392406]

在 Cluster Manager 和 VCS 集群之间存在防火墙配置的某些环境中，Cluster Manager 会失败，并显示以下错误消息：

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

解决方法：必须在所有集群节点上打开端口 14150。

VCS Cluster Manager（Java 控制台）不对 Sybase 和 SybaseBK 代理的密码进行加密 [2379510]

如果在 Sybase.xml 和 SybaseBk.xml 文件中将 `isvcsagencrypt` 标志设置为 True，则会对属性值进行加密。不过，Sybase 和 SybaseBk 代理的密码属性在 Sybase.xml 和 SybaseBk.xml 文件中未将 `isvcsagentcrypt` 标志设置为 True。

解决方法：已将 Sybase 和 SybaseBk 代理修改为默认情况下对密码进行加密。这样，如果使用 VCS Cluster Manager（Java 控制台）配置属性，便不需要对密码进行加密。

与虚拟业务服务 (VBS) 相关的问题

对包含共享服务组和不同控制器的虚拟业务服务的故障传播 [2407832]

对于包含共享服务组和不同控制器的某些配置，故障传播功能可能不起作用。

解决方法：没有解决方法。

如果参与服务组包含多个具有 LOCAL FIRM 依赖关系类型的子级，则虚拟业务服务无法启动 [2490098]

如果参与服务组包含多个具有 LOCAL FIRM 依赖关系类型的子级，则虚拟业务服务无法启动。之所以出现这种情况，是因为 Vertias Cluster Server (VCS) 不支持传播依赖关系。

解决方法：将依赖的 VCS 组移入不存在任何依赖关系的虚拟业务服务中。虚拟业务服务会识别 VCS 依赖关系并将它们视作 soft 型虚拟业务服务依赖关系。

软件限制

本节介绍了此版本的软件限制。

请参见相应的“版本说明”，以获取该组件或产品相关的软件限制的完整列表。

请参见第 83 页的“文档”。

与安装和升级 VCS 相关的限制

从远程系统使用安装程序时，远程系统和目标系统必须具有相同的操作系统和体系结构 [589334]

如果从远程系统使用安装程序，则该远程系统必须具有和要安装 VCS 的目标系统相同的操作系统和体系结构。

与 VCS 引擎相关的限制

VCS 删除使用 HostMonitor 对象名称的用户定义的 VCS 对象

如果已使用 HostMonitor 后台驻留程序的保留字在 main.cf 文件中定义了以下对象，则 VCS 将在 VCS 引擎启动时删除这些对象。[1293092]

- 定义为 VCShmg 的任何组及其所有资源。
- 定义为 HostMonitor 的任何资源类型以及此类资源类型的所有资源。
- 定义为 VCShm 的任何资源。

与捆绑代理相关的限制

如果主机断开连接，使用网络服务的程序可能会停止响应

如果主机从网络中断开，则使用网络服务（例如连接到远程主机的NIS、NFS、RPC或TCP套接字连接）的程序会停止响应。如果将此类程序用作代理入口点，则网络断开会导致入口点停止响应并且可能会超时。

例如，如果将主机配置为使用 NIS 映射作为客户端，则当网络断开时诸如 `ps -ef` 的基本命令可能会挂起。

Symantec 建议在本地创建用户。要反映本地用户，请配置：

/etc/nsswitch.conf

Volume 代理清除可能会强制停止 Volume 资源

当属性 FaultOnMonitorTimeouts 在监视超时后调用 Volume 代理的 clean 入口点时，也将发出 `vxvol -f stop` 命令。此命令强制停止所有卷，即使仍在装入这些卷。

使用 PidFiles 监视应用程序资源时发生假并发冲突

应用程序创建的 PID 文件中包含 Application 代理监视的进程的 PID。即使运行该应用程序的节点崩溃后，这些文件也可能继续存在。在重新启动节点时，操作系统可能会将 PID 文件中列出的 PID 分配给该节点上运行的其他进程。

因此，如果 Application 代理仅使用 PidFiles 属性监视资源，则该代理可能会发现进程正在运行并报告错误的并发冲突。这可能会导致停止不受 VCS 控制的某些进程。

Mount 代理的限制

Mount 代理存在以下限制：

- Mount 代理只在系统上的一个装入点装入块设备。装入块设备后，该代理无法在同一装入点装入其他设备。
- Mount 代理不支持：
  - SLES11SP1 上的 ext4 文件系统
  - 在 VxVM 上配置的 ext4 文件系统
  - 在 VxVM 上配置的 xfs 文件系统

Share 代理的限制

要确保 Share 代理正常提供监视功能，请确认在系统重新启动时清除了 /var/lib/nfs/etab 文件。必须以完全限定主机名指定 Share 代理中的客户端，以确保无缝故障转移。

DiskReservation 代理的驱动程序要求

VRTSvcsdr 软件包随附了 scsiutil 实用程序。DiskReservation 代理仅支持 scsiutil 实用程序所支持的那些驱动程序。

不管 VCS 中 StartVolumes 属性的值为何，磁盘组中的卷都将自动启动

不管 VCS 中 StartVolumes 属性的值为何，在导入磁盘组时，该磁盘组中的卷都将自动启动。如果 Veritas Volume Manager 中的系统级属性 `autostartvolumes` 的值设置为 On，便会观察到这种行为。

解决方法：在导入磁盘组后，如果您不希望磁盘组中的卷自动启动，请在系统级别上将 autostartvolumes 属性设置为 Off。

与 IMF 相关的限制

- 不支持 bind 文件系统类型在 Linux 上进行 IMF 注册。
- 对于 SLES11 SP1 和 RHEL6.1 的情况：
  - 不应为可在多个装入点上装入 BlockDevice 的资源启用 IMF。
  - 如果 FSType 属性值为 nfs，则不支持 nfs 文件系统类型的 IMF 注册。

与 VCS 数据库代理相关的限制

DB2 RestartLimit 值

当多个无依赖关系的 DB2 资源全部同时启动时，它们可能会相互干扰或相互竞争。这是 DB2 的已知问题。

DB2 代理 RestartLimit 的默认值为 3。这个较高的值使 DB2 资源并不集中重新启动（在资源联机失败后），从而降低了所有 DB2 资源同时启动的可能性。[1231311]

VCS agent for Oracle 有意脱机功能的局限

Oracle 资源在有意脱机后绝不会发生故障。

VCS agent for Oracle 的有意脱机功能要求您启用健康状况检查监视。该代理使用 Oracle 的健康状况检查 API 来查找数据库的状态。如果 API 返回的状态为数据库正

常关闭，则该代理会将资源状态标记为 INTENTIONAL OFFLINE。之后，即使 Oracle 代理的联机功能不起作用，该代理也不会将资源标记为 FAULTED。由于该代理在每个监视周期内从 API 收到的数据库状态都为正常关闭，因此状态一直保持为 INTENTIONAL OFFLINE。 [1805719]

与全局集群相关的限制

- 全局集群的集群地址需要已解析的虚拟 IP。
  如果虚拟 IP 用于心跳代理，则虚拟 IP 地址必须具有 DNS 条目。
- 全局集群配置中的集群总数不得超过 4 个。
- 在配置 Symm 心跳代理时，即使所有的主机都已关闭，也不可以声明集群出现故障。
  Symm 代理用于监视两个 Symmetrix 阵列之间的链接。当某个集群中所有的主机都已关闭但 Symm 代理能够查看本地存储和远程存储之间的复制链接时，此代理会将心跳报告为 ALIVE。因此，DR 站点不会声明主站点出现故障。

SLES 分发产品不支持安全性增强型 Linux

在 SLES10 和 SLES11 上，VCS 不支持安全性增强型 Linux (SELinux)。 [1056433]

集群中的系统必须具有相同的系统区域设置

VCS 不支持具有不同系统区域设置的系统组成集群。必须将集群中所有系统的区域设置设置为相同。

节点通过防火练习在校园集群中重新启动后，磁盘组的 VxVM 站点仍保持分离状态

使 DikGroupSnap 资源联机时，DiskGroupSnap 代理会从定义的目标磁盘组中分离站点。DiskGroupSnap 代理调用 VCS action 入口点以运行 VxVM 命令来分离站点。这些命令必须运行于导入磁盘组的节点（在主站点）。

如果尝试关闭防火练习服务组或磁盘组处于联机状态的节点，则该节点会进入 LEAVING 状态。VCS 引擎尝试使该节点上的所有服务组脱机并拒绝所有 action 入口点请求。因此，DiskGroupSnap 代理无法调用 Action 以将防火练习站点重新挂接到目标磁盘组。该代理将记录一条消息，即节点处于 LEAVING 状态，然后删除锁文件。代理的 monitor 函数声明资源脱机。重新启动节点后，磁盘组站点仍保持分离状态。 [1272012]

解决方法：

必须先使用 `hagrp -offline` 命令使防火练习服务组脱机，才能关闭节点或从本地停止 VCS。

如果节点已重新启动，则必须手动将防火练习站点重新挂接到在主站点上导入的磁盘组。

如果辅助节点已崩溃或重新启动，则必须手动将防火练习站点重新挂接到使用以下命令在主站点上导入的目标磁盘组：`/opt/VRTSvcs/bin/hares -action $targetres joindg -actionargs $fdsitename $is_fenced -sys $targetsys`。

DiskGroupSnap 代理的限制

DiskGroupSnap 代理具有以下限制：

- DiskGroupSnap 代理不支持分层卷。 [1368385]
- 如果为 DiskGroupSnap 资源使用 Bronze 配置，则在下列情况中会出现辅助站点的数据不一致：[1391445]
  - 防火练习服务组联机后，主站点在防火练习过程中发生灾难。
  - 防火练习服务组脱机后，当辅助站点的磁盘重新同步时主站点发生灾难。

  Symantec 建议为 DiskGroupSnap 资源使用 Gold 配置。

发生混乱后重新启动系统

如果 VCS 内核模块导致系统混乱，则需要重新启动系统 [293447]。支持的 Linux 内核不会自动停止 (CPU) 处理。将 Linux 的 panic 内核参数设置非零值可以强制重新启动系统。在 /etc/sysctl.conf 文件的末尾追加以下两行：

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

Cluster Manager（Java 控制台）限制

本节介绍 Cluster Manager（Java 控制台）的软件限制。

Cluster Manager（Java **控制台**）5.1 **版及更低版本无法管理** VCS 6.0 **安全集群**

低于 VCS 5.1 的版本中的 Cluster Manager（Java 控制台）无法用于管理 VCS 6.0 安全集群。Symantec 建议使用最新版本的 Cluster Manager。

有关升级 Cluster Manager 的说明，请参见《Veritas Cluster Server 安装指南》。

如果 hosts 文件中包含 IPv6 条目，则 Cluster Manager 不起作用

如果 /etc/hosts 文件中包含 IPv6 条目，则 VCS Cluster Manager 无法连接到 VCS 引擎。

解决方法：从 /etc/hosts 文件中删除 IPv6 条目。

VCS Simulator 不支持 I/O 防护

运行 Simulator 时，请确保将 UseFence 属性设置为默认值 None。

使用 KDE 桌面

Cluster Manager（Java 控制台）上的某些菜单和对话框在 KDE 桌面上可能显示为不对齐或大小不合适。要确保该控制台在KDE桌面上呈现正确的外观和功能，请使用 Sawfish 窗口管理器。您必须明确选择 Sawfish 窗口管理器，即使它会在 KDE 桌面上显示为默认的窗口管理器时也是如此。

Cluster Manager（Java 控制台）提供的有限支持

VCS 6.0 中引入的功能可能不按预期方式与 Java 控制台协同工作。不过，模拟器的 CLI 选项支持所有 VCS 6.0 功能。建议您使用 Veritas Operations Manager (VOM)，因为所有新增功能在 VOM 中都已经受到支持。不过，Java 控制台可以像以往一样按预期方式与 VCS 6.0 之前版本的功能协同工作。

连接到安全集群要求进行端口变更 [2615068]

要连接到安全集群，默认端口必须从 2821 更改为 14149。您必须选择“**Login (登录)**”对话框中的“**Advanced settings (高级设置)**”，然后将 **IP：2821** 更改为 **IP：14149** 以便进行安全集群登录。

与 I/O 防护相关的限制

本节介绍了与 I/O 防护相关的软件限制。

VxFEN 激活争夺者节点重新选择时在首选防护方面的限制

首选防护功能通过延迟较小的子集群来使权重更高、规模更大的子集群占得先机。这种延迟较小子集群的做法仅在较大子集群中的初始争夺者节点能够完成争夺时有效。如果由于某种原因初始争夺者节点无法完成争夺，并且 VxFEN 驱动程序激活了争夺者节点重新选择算法，则由于争夺者节点重新选择会耗用一定的时间，因此这种延迟较小子集群的做法所起到的作用将会被化为无形，这样，权重较低或者规模较小的子集群可能会在争夺中取胜。此限制尽管并不是想要的，但还是可以容忍的。

停止配置了 I/O 防护的集群中的系统

I/O 防护功能可防止由于发生故障的集群互联或“裂脑”而导致的数据损坏。有关出故障的互联可能导致的问题和 I/O 防护提供的保护的说明，请参见《Veritas Cluster Server 管理指南》。

在采用基于 SCSI-3 的防护的集群中，I/O 防护通过在数据磁盘和协调器磁盘上都放置 SCSI-3 PR 密钥来实现数据保护。在采用基于 CP 服务器的防护的集群中，I/O 防护通过在数据磁盘上放置 SCSI-3 PR 密钥并在 CP 服务器上放置类似注册项来实现数据保护。VCS 管理员必须注意在处理由 I/O 防护保护的集群时所需的几个操作更改。特定的关闭过程可确保从协调点和数据磁盘中删除密钥，从而防止后续集群启动可能出现问题。

使用 reboot 命令（而不是 shutdown 命令）可以绕过关闭脚本，并且可以保留协调点和数据磁盘上的密钥。集群可能会警告可能出现裂脑情况而无法启动，这取决于重新启动和后续启动事件的顺序。

解决方法：每次在一个节点上使用 shutdown -r 命令，并等待每个节点完成关闭操作。

如果使用 dmp 磁盘策略在 SCSI3 模式下配置了 VxFEN，则卸载 VRTSvxvm 会导致问题 (2522069)

如果使用 dmp 磁盘策略在 SCSI3 模式下配置了 VxFEN，则可以在系统关闭或防护仲裁期间访问协调器磁盘的 DMP 节点。卸载 VRTSvxvm RPM以后，将不再在内存中加载 DMP 模块。在卸载 VRTSvxvm RPM的系统上，如果 VxFEN 尝试在关闭或防护仲裁期间访问 DMP 设备，则系统发生混乱。

文档勘误表

以下几节介绍了产品文档（文档版本：6.0.0）的补充或更正。更新版本的产品文档（可以从 Symantec 支持网站下载）和 Symantec Operations Readiness Tools (SORT) 中可能包含这些补充或更正内容。

请参见相应的“版本说明”，以了解与该组件或产品相关的文档勘误表。

请参见第 83 页的“文档”。

请参见第 9 页的“关于 Symantec Operations Readiness Tools”。

Veritas Cluster Server Bundled Agents 参考指南

主题：“MultiNICA 代理”>“属性”

对 Device 属性的说明还需要提到以下内容：

Device 属性必须按系统进行本地化，并且必须具有不同的基础 IP 地址（具体解释见“IPMultiNIC 代理”的“示例配置：IPMultiNIC 和 MultiNICA”）。

Veritas Cluster Server 安装指南

“VCS 支持的软件”部分中的附注内容应为：VCS 支持 SF 的早期版本以及以后的版本，以便于产品升级。

文档

软件介质上的 /*product_name*/docs 目录中提供了 PDF 格式的产品指南。其他文档通过联机方式提供。

Symantec 建议将相关信息（例如，安装指南和版本说明）复制到系统的 /opt/VRTS/docs 目录中，以备参考。

请确保您使用的是文档的最新版本。每个指南的第 2 页提供了文档版本信息。从 Symantec 网站可以获取最新的产品文档。

http://sort.symantec.com/documents

文档集

表 1-18 列出了 Veritas Cluster Server 的文档。

表 1-18 Veritas Cluster Server 文档

书名	文件名
Veritas Cluster Server 安装指南	vcs_install_60_lin.pdf
Veritas Cluster Server 版本说明	vcs_notes_60_lin.pdf
Veritas Cluster Server 管理指南	vcs_admin_60_lin.pdf
Veritas Cluster Server Bundled Agents 参考指南	vcs_bundled_agents_60_lin.pdf
Veritas Cluster Server Agent 开发指南	vcs_agent_dev_60_unix.pdf
Veritas Cluster Server Agent for DB2 安装和配置指南	vcs_db2_agent_60_lin.pdf
Veritas Cluster Server Agent for Oracle 安装和配置指南	vcs_oracle_agent_60_lin.pdf
Veritas Cluster Server Agent for Sybase 安装和配置指南	vcs_sybase_agent_60_lin.pdf

表 1-19 列出了 Veritas Storage Foundation and High Availability Solutions 产品的文档。

表 1-19 Veritas Storage Foundation and High Availability Solutions 产品文档

文档标题	文件名
Veritas Storage Foundation and High Availability Solutions 解决方案指南	sfha_solutions_60_lin.pdf
Veritas Storage Foundation and High Availability Solutions 虚拟化指南	sfha_virtualization_60_lin.pdf

如果您使用 Veritas Operations Manager (VOM) 管理 Veritas Storage Foundation and High Availability 产品，请参考 VOM 产品文档，网址是：

http://sort.symantec.com/documents

手册页

Veritas Storage Foundation and High Availability Solutions 产品的手册页安装在 /opt/VRTS/man 目录中。

设置 MANPATH 环境变量，以便 man(1) 命令可以指向 Veritas Storage Foundation 手册页：

- 对于 Bourne 或 Korn shell（sh 或 ksh），请输入以下命令：

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

- 对于 C shell（csh 或 tcsh），请输入以下命令：

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

请参见 man(1) 手册页。

手册页分为 1、1M、3N、4 和 4M 部分。编辑 man(1) 配置文件 /etc/man.config 以查看这些页。

编辑 man(1) 配置文件

1 如果使用 man 命令访问手册页，请在 shell 中将 LC_ALL 设置为 C 以确保正确显示这些页。

```
export LC_ALL=C
```

有关更多信息，请参见 Red Hat Linux 支持网站上的问题 82099。

2 将以下行添加到 /etc/man.config 中：

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

其中的其他 man 路径是在配置文件指定的。

3 添加新的节编号。将以下行：

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

更改为

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

新增的虚拟业务服务 (VBS) 相关功能

虚拟业务服务 (VBS) 功能扩展了自 VOM 3.x 版本起提供的 VOM 业务实体 (BE) 功能。VOM BE 支持应用程序实体类型，今后在 VOM 4.1 和 SFHA 6.1 版本中将此类型称作“虚拟业务服务 (VBS)”。借助虚拟业务服务，用户可以定义和管理异构、集群间、多层的应用程序。每一层由一个服务组加以表示，可以在单独的VCS集群或 ApplicationHA 节点上配置此服务组。VBS 在 VCS HA/DR 和 ApplicationHA 基础上构建，旨在跨物理和虚拟环境提供业务服务可用性。可以选择将应用程序层（服务组）与可配置的依赖关系类型和故障操作关联起来。

VBS 中的有序启动/停止操作

VBS 允许通过单击一次或通过单个命令行界面有序启动/停止整个业务服务。如果应用程序承载在VMWare虚拟机上，则可以将虚拟机配置为在您启动或停止虚拟业务服务时自动启动或停止。

能够通过 CLI 执行 VBS 操作

您可以从任何参与层集群的任何节点使用 CLI 来操作虚拟业务服务。因此，在您配置 VBS 后，VOM CS 是可选的。

VBS 对 DR 的支持

VBS 提供了一套在 VCS DR 基础上构建的全面 DR 解决方案。这种 DR 支持的基础是 VBS 中具有一个或多个 GCO 服务组。

VBS 对强健故障管理的支持

VBS 通过一些可配置的操作提供了强健的故障管理功能，例如，在子服务组出现故障或进行恢复时停止、启动、重新启动服务组（应用程序层）便属于此类操作。在 VBS 内配置的服务组之间支持三种依赖关系类型（即 Soft、Firm、Restart）。

针对虚拟业务服务的安全访问控制

仅允许参与层中的 root 用户通过 CLI 在 VBS 上执行操作。通过 VOM 执行的操作支持基于角色的访问控制 (RBAC)。

对 VBS 上所执行的操作进行的审核跟踪

通过审核跟踪和日志可以轻松跟踪在 VBS 上执行的所有用户操作。