Symantec™ Cluster Server 版本说明

AIX

6.1

Symantec

Symantec™ 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：6.1

文档版本：6.1 Rev 0

法律声明

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征和功能的特定查询。技术支持小组还负责创建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 提供的支持服务包括以下内容：

- 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
- 电话和/或基于 Web 的支持，提供快速响应及最新信息
- 升级保障，提供软件升级
- 全球支持，提供区域性工作时间或全天候两种购买选项
- 超级支持服务，包括帐户管理服务

有关 Symantec 支持服务的信息，请通过以下 URL 访问我们的网站：

www.symantec.com/business/support/index.jsp

所有支持服务都将根据您的支持协议和当时有效的企业技术支持策略来提供。

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

介质中提供有 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 页上提供了文档版本信息。最新产品文档可从 Symantec 网站获得。

https://sort.symantec.com/documents

我们十分重视您对产品文档的反馈。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

有关最新的 HOWTO 文章、文档更新的信息，或者要询问有关产品文档的问题，请访问 Symantec Connect 中的 Storage and Clustering Documentation 论坛。

https://www-secure.symantec.com/connect/storage-management/forums/storage-and-clustering-documentation

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，包括发布论坛帖子、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

Symantec 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 AIX 的 Symantec Cluster Server (VCS) 版本 6.1 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。

本文档是《Symantec Cluster Server 版本说明》的“文档版本：6.1 Rev 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：

`/docs/product_name`

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：

- 《Symantec Storage Foundation 版本说明》(6.1)

关于 Symantec Cluster Server

由 Symantec 出品的 Symantec 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，请参见《Symantec Cluster Server Bundled Agents 参考指南》。

通过 Symantec 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) 获取。™ Operations Readiness Tools (SORT)。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 Symantec 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《Symantec Cluster Server Agent 开发指南》。还可以通过 Symantec 咨询服务请求自定义代理。

关于编译自定义代理

必须使用 IBM XL C/C++ for AIX Compiler 8.0 版编译使用 C++ 开发的自定义代理。要与框架库进行运行时链接，请使用 -brtl 标志。

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 产品以及生成安装和升级自定义报告的准备。 ■ 按产品或平台，并按需要安装的顺序列出修补程序。显示并下载最新修补程序或历史修补程序。 ■ 按供应商、平台或 Storage Foundation and High Availability (SFHA) 版本显示阵列支持库 (ASL) 详细信息。ASL 使连接到基于 SFHA 的服务器的阵列更易于管理。 ■ 根据代理类型、应用程序和平台列出 VCS 和 ApplicationHA 代理、文档和下载。
识别风险并获取特定于服务器的建议	■ 分析服务器中是否存在潜在环境风险。生成风险评估自定义报告，其中包含有关系统可用性、存储利用率、性能和最佳做法的特定建议。 ■ 显示数千个 Symantec 错误代码的说明和解决方案。

提高效率

- 获取有关对修补程序、阵列特定模块 (ASL/APM/DDI/DDL)、文档、产品版本、硬件兼容性列表 (HCL) 和 VCS/ApplicationHA 代理所做更改的自动电子邮件通知。
- 从生产环境中快速收集已安装的 Symantec 产品和许可证密钥信息。生成许可证/部署自定义报告，其中包括产品名称、版本和平台、服务器层、Symantec 性能值单位 (SPVU) 以及服务使用期结束日期。
- 列出并下载 Symantec 产品文档，其中包括产品指南、手册页、兼容性列表和支持文章。
- 在单个页面上访问指向重要资源的链接，其中包括 Symantec 产品支持、SymConnect 论坛、客户服务、Symantec 培训和教育、Symantec FileConnect、授权门户和 my.symantec.com。此页面还包括指向主要供应商支持站点的链接。
- 使用 iOS 设备的一部分 SORT 功能。从以下位置下载应用程序：
  https://sort.symantec.com/mobile

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/TECH211540
- 有关此版本可用的最新修补程序，请转到：
  https://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/TECH211575
  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。

6.1 中引入的更改

本节列出了 Symantec Cluster Server 6.1 的更改。

VCS 6.1 中引入的属性

下节介绍 VCS 6.1 中引入的属性。

NFS 代理属性

Protocol	指定用于运行 nfsd 后台驻留程序的协议。代理使用此属性确保 NFS 后台驻留程序使用指定的协议运行。

AIX 上的 LPAR 代理属性

ProfileFile	指定指向 LPAR 配置文件的路径。
RemoveProfileOnOffline	可以在使 LPAR 资源脱机或将来 LPAR 资源发送故障，无法实施 LPAR 迁移时，从物理资源服务器删除 LPAR 配置文件。

NotifierMngr 代理属性

MessageExpiryInterval	指定消息的过期期限（以秒为单位）。如果引擎在 MessageExpiryInterval 以内没有向通知程序发送消息，则会将消息从引擎的消息队列中删除。

DiskGroup 代理属性

ClearClone	导入磁盘组的磁盘时，从中清除 clone 和 udid_mismatch 标志，并根据需要更新 UDID。

用于启用目标系统动态选择的新属性

统计信息	指示是否启用统计数据收集，以及是否可以将 FaultOverPolicy 设置为 BiggestAvailable。为 CPU、内存和交换等系统资源收集统计数据。
MeterWeight	代表为集群属性的 HostMeters 键指定的权重，以便在多个系统满足服务组属性的负载要求时确定适用于该服务组的目标系统。
HostAvailableMeters	列出可用于测量系统资源的计量器。不能在 main.cf 中配置此属性。

HostMeters	指示当前在集群中计量的参数（CPU、Mem 或 Swap）。
MeterControl	指示为 HostMeters 中指定的键计量和预测系统属性 AvailableCapacity 的时间间隔。
HostAvailableForecast	指示根据过去计量的 AvailableCapacity 而为集群中的系统预测的可用容量。
MeterRecord	用作带有预定义键的内部系统属性。仅当集群属性 Statistics 设置为 Enabled 时才会更新此属性。
ReservedCapacity	指示当 FailOverPolicy 设置为 BiggestAvailable 时在系统上为即将进入联机状态的服务组保留的容量。此属性包含 HostMeters 中指定的所有键（例如 CPU、Mem 和 Swap）。这些键的值按照集群属性 MeterUnit 中指定的相应单位进行设置。
CapacityReserved	指示是否保留容量以用于使服务组联机或故障转移。仅当服务组属性 FailOverPolicy 设置为 BiggestAvailable 时才会保留容量。
UnSteadyCount	代表用于未决的联机或脱机操作的资源总数目。它是本地属性。
MemThresholdLevel	根据生成日志的级别确定内存利用率的阈值。

有关更多信息，请参考 *Symantec Cluster Server 管理指南*。

与安装和升级相关的更改

在 6.1 中，产品安装程序的更改如下。

支持跨平台安装

您可以使用基于脚本的安装程序或基于 Web 的安装程序在运行任何所支持平台的目标系统上安装 VCS，即使源系统和目标系统运行在不同平台上也可以进行安装。

自动下载安装程序修补程序

如果您运行的是 6.1 产品安装程序，而您的系统可以访问 Internet，则安装程序自动导入任何所需的安装程序修补程序，并开始使用

如果您的系统无法访问 Internet，您仍然可以使用 Symantec Operations Readiness Tools 修补程序查找工具下载安装程序修补程序。

自动下载安装程序修补程序需要安装程序进行出站网络调用。如果您知道系统具有防火墙，或者不希望安装程序进行出站网络调用，则可以通过使用非 Internet 修补程序中心 (-noipc) 选项运行安装程序禁止外部网络尝试。例如：

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

支持使用 Deployment Server 集中安装

利用 Deployment Server，可以在一个中央位置存储多个版本映像，并将这些映像部署到任何受支持平台的系统中。自 5.1 版本起，可以加载 Symantec 产品的产品二进制文件并将其存储在一个中央存储库中。

可以使用 Deployment Server 来执行以下任务：

- 版本检查
- 版本映像管理
- 安装或升级系统
- 更新元数据和首选项

改进的修补和更新进程

您现在可以直接通过安装程序下载产品维护版本以及公共修补程序版本。如果您使用带有 -version 选项的 installer 命令，安装程序将列出可用的 GA 版本、维护版本以及修补程序版本。如果您可以访问 Internet，则可以按照安装程序提示将可用的修补程序以及修复程序下载到您的本地系统。

下载修补程序和修复程序需要安装程序进行出站网络调用。如果您知道系统具有防火墙，或者不希望安装程序进行出站网络调用，则可以通过使用非 Internet 修补程序中心 (-noipc) 选项运行安装程序禁止外部网络尝试。使用 -noipc 选项时，安装程序不会尝试连接 Symantec Operations Readiness Tools (SORT) 网站。例如：

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

支持同时安装或升级基础版本、维护修补程序和修补程序

从版本 6.1 开始，Symantec 提供了一种可轻松地使用“安装捆绑”直接一步将系统安装或升级到基础、维护或修补程序级别的方法。“安装捆绑”可以将安装程序合并在一起，方便客户执行一次操作即可直接安装或升级到维护或修补程序级别。“安装捆绑”过程包括从 GA 版本执行安装程序，指针将指向更高的维护或修补程序版本。安装程序将同时安装这两个版本，就像它们处于同一版本映像中一样。各种脚本、文件集和修补程序组件合并在一起，多个版本同时安装，就像它们是一个安装实体一样。

有五种可能的集成方法。必须从最高级别脚本实施所有执行。

- 基础 + 维护
- 基础 + 修补程序
- 维护 + 修补程序
- 基础 + 维护 + 修补程序
- 基础或维护 + 多个修补程序

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《Symantec Cluster Server 管理指南》和《Symantec Cluster Server Bundled Agents 参考指南》。

Apache HTTP 服务器代理对 IMF 的支持

Apache HTTP 服务器代理可识别 IMF，并且使用 AMF 内核驱动程序进行 IMF 通知。该代理还可以针对 Apache 资源执行详细的监视。您可以使用 LevelTwoMonitorFreq 属性调节详细监视的频率。SecondLevelMonitor 属性已废弃。

如果配置了 MonitorProgram 属性，则 Application 代理中支持二级监视

如果除 MonitorProgram 外，使用 MonitorProcesses、PidFiles 或同时使用两者配置了 Application 资源，您可以配置 Application 资源以作为二级监视运行 MonitorProgram。要启用二级监视，请将 LevelTwoMonitorFreq 属性设置为一个大于 0 的值。Application 资源 LevelTwoMonitorFreq 属性的默认值为 1（一）。

即使与 MonitorProcess 或 PidFiles 或两者一起配置了 MonitorProgram，更改之后，Applicatoin 代理可以利用 AMF 进行即时通知。

改进后的 Proxy 代理日志可以提供更多详细信息

现在，Proxy 代理日志消息可以提供更多的详细信息，例如，代理转为未知或故障状态的原因。当 Proxy 资源联机或脱机时，还会记录调试消息。

Apache 代理会在进程停止时使资源脱机 [2978005]

现在，Apache 代理已进行如下修改：当 Apache 进程作为脱机入口点的一部分停止时，资源立即变为脱机。

NFS 代理增强功能

NFS 代理支持在指定协议下运行 nfsd 后台驻留程序。

Mount 代理的新代理函数

Mount 代理支持 attr_changed 函数。将 VxFSMountLock 属性值从 1 或 2 更改为 0 时，此函数将解锁装入。

LPAR 代理增强功能

AIX 的 LPAR 代理已得到增强，添加了以下功能：

支持通过 VCS 迁移 LPAR 资源

将新迁移入口点添加到 LPAR 代理，以通过 VCS 执行 LPAR 的实时迁移。

添加对使用 LPAR 实时迁移的 LPAR 配置文件管理支持

LPAR 代理得到增强，在 LPAR 实时迁移以外还支持 LPAR 故障转移。当 LPAR 资源从物理源服务器实时迁移到物理目标服务器时，迁移过程会删除物理源服务器上的 LPAR 配置文件。如果目标物理服务器上的已迁移 LPAR 故障或者如果 LPAR 服务组需要从目标服务器切换回来，则 LPAR 无法在物理源服务器上联机，因为 LPAR 配置文件配置不可用。为了便于将 LPAR 故障转移回物理源服务器，必须首先创建 LPAR 配置文件配置。LPAR 代理得到增强，可在将 LPAR 资源联机时读取在 ProfileFile 属性中配置的 LPAR 配置文件，并且在故障转移物理服务器上创建 LPAR。同样，LPAR 代理得到增强，可根据 RemoveProfileOnOffline 属性值在将 LPAR 脱机时删除 LPAR 配置。

对 VCS 引擎的更改

OpenVCSCommunicationPort 属性决定了是否允许使用外部通信端口

OpenVCSCommunicationPort 属性决定了 VCS 的外部通信端口是否打开以进行通信。

如果 VCS 的外部通信端口未打开，则适用以下限制：

- 不能使用 Java 控制台管理 VCS。
- 通过 `hawparsetup` 命令设置的 RemoteGroup 资源和用户无法访问 VCS。

目标系统的动态选择

有了目标系统的动态选择，VCS 能做出将应用程序故障转移到最大可用系统的动态决策。 VCS 监视系统在 CPU、内存和交换等方面的可用容量，从而选择最具可用

性的系统。有关目标系统的动态选择的更多信息，请参见《Symantec Cluster Server 管理指南》。

需要修改以实现目标系统的动态选择的属性

若要在 VCS 中实现目标系统的动态选择，请修改下列属性：

- HostUtilization：指示主机上资源的使用率百分比，这些百分比由 HostMonitor 代理来计算。
- FailOverPolicy：控制 VCS 如何计算故障转移的目标系统。此服务组属性中新增了策略值 BiggestAvailable。

  BiggestAvailable：VCS 根据 SystemList 中所有系统的预测可用容量选择系统。具有最高预测的可用容量的系统会被选中。只有启用了集群属性 Statistics，并且定义服务组属性 Load 的 CPU、Memory 或 Swap（以 MeterUnit 属性中指定的绝对单位衡量）时，才能设置此策略。
- Load：这是由系统容量和服务组负载构成的 FailOverPolicy 属性值。
- HostMonitor：包含 HostMonitor 代理监视的主机资源列表。
- AvailableCapacity：指示系统的可用容量。
- Capacity：代表系统的总容量。

注意：AvailableCapacity、Capacity、Load 和 DynamicLoad 属性具有多维值

对 VCS 代理框架的更改

VCS 代理框架引入了以下更改。

服务组的实时迁移

VCS 目前支持具有资源的服务组的实时迁移功能，以监视虚拟机。迁移服务组的进程同时涉及将服务组在最小停机时间内从源系统移动到目标系统。针对此过程为代理开发人员引入了命名为“migrate”的新入口点。此入口点可以用于 Script60Agent。可以使用新属性（MigrateTimeout、MigrateWaitLimit 和 SupportedOperations）控制迁移入口点的行为。

有关更多信息，请参见《Symantec Cluster Server 管理指南》、《Symantec Cluster Server Bundled Agents 参考指南》、《Symantec Cluster Server Agent 开发指南》以及《Symantec Storage Foundation and High Availability Solutions 虚拟化指南》。

对 Oracle 代理的更改

本节介绍了对 Symantec Cluster Server Agent for Oracle 所做的更改。

VCS agent for Oracle 使用 Oracle 运行状况检查 API 来确定 Oracle 实例的有意脱机行为

Symantec Cluster Server agent for Oracle 使用 Oracle 运行状况检查 API 来确定节点上的 Oracle 实例是正常关闭还是被中止。当 Oracle 实例正常关闭以脱离 VCS 的控制时，代理会将此操作确认为有意脱机。

从 VCS 6.1 版本起，不再提供预构建的运行状况检查二进制文件。您需要运行 `build_oraapi.sh` 脚本，以根据 Oracle 版本构建 Oracle 运行状况检查二进制文件。

有关更多信息，请参考《Symantec Cluster Server Agent for Oracle 安装和配置指南》。

对 LLT、GAB 和 I/O 防护的更改

本节涵盖 LLT、GAB 和 I/O 防护的新增功能和增强功能。

在单节点集群上禁用 LLT、GAB 和 I/O 防护

如果只要管理节点的应用程序并使用 VCS 的应用程序重新启动功能，请在单节点 Symantec Cluster Server (VCS) 集群上禁用 LLT、GAB 和 I/O 防护内核模块。

请注意，禁用这些内核模块意味着您将无法使应用程序在多个节点之间高度可用。但是，如果将来您决定将集群扩展到多个节点，还可以启用这些模块并使应用程序高度可用。

有关更多信息，请参考《Symantec Cluster Server 管理指南》。

对 LLT 的更改

在 6.1 中，Symantec Cluster Server 包括对 LLT 的以下更改：

LLT 命令更改

此版本中引入了以下命令更改。

`lltconfig` 中的更新：

- 引入了新选项 `lltconfig -l`。添加新链接时，可以使用 `-l` 选项指定该链接为低优先级链接。

对 I/O 防护的更改

在 6.1 中，Symantec Cluster Server (VCS) 包括对 I/O 防护的以下更改：

在配置 I/O 防护的同时设置协调点的顺序

可以在安装程序中使用 `-fencing` 选项来设置协调点的顺序。

确定协调点（协调磁盘或协调点服务器）在网络分裂期间参与争用的顺序。在安装程序中设置的协调点顺序会更新到 /etc/vxfenmode 文件。I/O 防护会根据 vxfenmode 文件中列出的顺序联系协调点。

因此，该顺序必须基于 I/O 防护联系协调点进行成员仲裁的可能性。

有关更多信息，请参见《Symantec Cluster Server 安装指南》。

使用安装程序刷新现有协调点上的键或注册

可以在安装程序中使用 `-fencing` 选项来刷新现有协调点上的注册。

由于阵列意外重新启动、键损坏或某些其他原因，现有协调点上可能会发生注册丢失。如果协调点丢失集群节点的注册，则集群在出现网络分裂时可能会发生混乱。当 CoordPoint 代理向 VCS 通知任何现有协调点上发生注册丢失时，必须刷新协调点上的注册。

当集群联机而且集群上没有发生应用程序停机时，您也可以在协调点上执行计划的注册刷新操作。

有关更多信息，请参见《Symantec Cluster Server 安装指南》。

在单节点 VCS 集群上配置 CP 服务器时，CPI 自动安装 CP 服务器专用许可证

当您在单节点 VCS 集群上配置 CP 服务器时，安装程序自动安装 CP 服务器专用许可证。此外，还确保 Veritas Operations Manager (VOM) 将单一节点协调点服务器上的许可证标识为特定于 CP 服务器的许可证，而非 VCS 许可证。

有关更多信息，请参见《Symantec Cluster Server 安装指南》。

基于站点的首选防护策略

防护驱动程序在协调点争夺期间优先选择具有较高站点优先级的节点。VCS 使用站点级别的属性 Preference 来确定节点权重。

有关更多信息，请参见《Symantec Cluster Server 管理指南》。

对 CP 服务器与应用程序客户端集群节点之间 HTTPS 通信的支持

CP 服务器与其应用程序客户端集群节点可通过 HTTPS 这个行业标准协议实现安全通信。在 6.1 之前的版本中，CP 服务器与其客户端之间的通信通过进程间消息传送 (IPM) 协议来完成，该协议是 Symantec 专属协议。通过基于 IPM 的通信实现的安全通信使用 Symantec 产品验证服务 (AT) 在 CP 服务器与客户端节点之间建立安全通信。推出使用 HTTPS 的安全通信后，CP 服务器功能可向后兼容之前版本。为了在 6.1 之前的版本上支持客户端节点，除了基于 HTTP 的通信之外，CP 服务器还支持基于 IPM 的通信。不过，从 6.1 开始，客户端节点仅支持基于 HTTPS 的通信。

有关更多信息，请参考《Symantec Cluster Server 安装指南》和《Symantec Cluster Server 管理指南》。

/etc/vxfenmode 文件中的安全属性已过时

从 VCS 6.1 开始，协调点 (CP) 客户端将使用 HTTPS 协议与 CP 服务器进行通信。因此，/etc/vxfenmode 中的 security 参数将被废弃，即使将该参数设置为 1 或 0 也无济于事。

需要运行 6.1 版的 CP 服务器才能将应用集群滚动升级到 6.1 版

在 6.1 版上运行的应用集群和 CP 服务器通过 HTTPS 协议进行通信。因此，将集群升级到 6.1 之后，使用 CP 服务器作为防护协调点的应用集群将无法再访问 6.1 版之前的 CP 服务器。要确保顺利升级，应用集群必须使用运行 6.1 版的 CP 服务器，否则必须将运行较早版本的 CP 服务器升级到 6.1 版。请注意，运行 6.1 版的 CP 服务器仍然可以使用 6.1 版之前的应用集群。

在 vxfentsthdw 实用程序中引入的磁盘大小检查和用于覆盖错误的选项

vxfentsthdw 实用程序已增强，可检查磁盘大小兼容性，并且为更好地进行错误评估引入了新的错误消息。该实用程序还提供了覆盖选项 (-o)，可覆盖与大小相关的错误并继续测试。

vxfenswap 实用程序中 hacli 的新命令

引入了新选项 -p 以指定 vxfenswap 实用程序可用来与集群中的其他节点进行通信的协议值。该协议支持的值可以是 ssh、rsh 或 hacli。

更改校园集群

多站点管理

您可以通过配置 SiteAware 集群级别属性来创建站点，以将其用于校园集群中的初始故障转移决策。您可以定义站点并将系统添加到已定义的站点。一个系统只能从属于一个站点。站点定义在 VCS、Veritas Operations Manager 和 VxVM 间是一致的。您可以定义站点依赖项，以将相连的应用程序限制为在同一站点中进行故障转移。

如果为集群配置站点，服务组会在选择其他站点中的某个主机前，尝试停留在自己的站点内。例如，在一个具有两个站点（站点 A 和站点 B）的校园集群中，您可以在由 Web、应用程序和数据库构成的三层应用基础架构中定义一个服务组间的站点依赖关系，以将故障转移限制在同一站点内。

您必须使用 Veritas Operations Manager 6.0 来定义站点和依赖关系以及配置集群的站点。

有关更多信息，请参考*Symantec Cluster Server 管理指南*。

与产品名称品牌相关的更改

从 6.1 版开始，Storage Foundation and High Availability Solutions 产品名称将更名。

表 1-1 列出了更名后的 Storage Foundation and High Availability Solutions 产品。

表 1-1 更名后的 Storage Foundation and High Availability Solutions 产品

旧产品名称	使用 Symantec 品牌的新产品名称
Veritas Storage Foundation	Symantec Storage Foundation
Veritas Dynamic Multi-Pathing	Symantec Dynamic Multi-Pathing
Veritas Replicator 选件	Symantec Replicator 选件
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 软件开发工具包	Symantec File System 软件开发工具包

Symantec 更名不适用于以下情况：

- 产品的首字母缩略词
- 命令名称
- 错误消息
- 警报消息
- 模块和组件
- 功能名称

- Veritas Operations Manager 产品品牌

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 支持这样的环境：集群中的少数节点承载在使用 VIOS 向操作系统提供存储和网络连接的 LPAR 上。集群中的其余节点承载在直接向操作系统提供存储和网络连接的物理系统上。不过，只有当存储通过 LPAR 中的 NPIV 可用时，SCSI3 I/O 防护才在此环境中受到支持。如果 NPIV 在 LPAR 中不可用，则非 SCSI3 防护不受支持。

VCS 要求集群中的所有节点使用相同的处理器体系结构且集群中的所有节点必须运行相同的 VCS 版本。集群中的每个节点可以运行不同版本的操作系统，但操作系统应受集群中的 VCS 版本支持。

请参见第 21 页的“硬件兼容列表”。

请参见第 21 页的“支持的 AIX 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/TECH211575

安装或升级 Symantec 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 AIX 操作系统

本节列出了此版本 Symantec 产品所支持的操作系统。要获得最新的更新，请访问“Symantec Operations Readiness Tools Installation and Upgrade (Symantec Operations Readiness Tools 安装和升级)”页面：https://sort.symantec.com/land/install_and_upgrade。

表 1-2 显示了此版本支持的操作系统。

表 1-2 支持的操作系统

操作系统	级别	芯片组
AIX 7.1	TL0、TL1 或 TL2	Power 5、Power 6 或 Power 7
AIX 6.1	TL6、TL7 或 TL8	Power 5、Power 6 或 Power 7

VCS 支持的软件

VCS 支持下列卷管理器和文件系统：

- Logical Volume Manager (LVM)
- LVM 上的 Journaled File System (JFS) 和 Enhanced Journaled File System (JFS2)

VCS 支持下列 Symantec Storage Foundation 版本：

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

- Storage Foundation 6.1
  - 具有 VxFS 6.1 的 VxVM 6.1
- Storage Foundation 6.0.1
  - 具有 VxFS 6.0.1 的 VxVM 6.0.1

注意：VCS 支持 Storage Foundation 的早期版本以及以后的版本，以便于产品升级。

有关支持的 Enterprise Agent 的数据库版本，请参考支持表，网址为：http://www.symantec.com/business/support/index?page=content&id=DOC4039。

受支持的 Enterprise Agent

请参考以下链接获取每个代理支持的 Enterprise Agent 支持表：

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

有关更多详细信息，请参见 Oracle、DB2 和 Sybase 的 Symantec Cluster Server 代理指南。

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 Symantec 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：

不再支持的代理和组件

VCS 不再支持下列代理和组件：

- 过去用来配置 CP 服务器的 configure_cps.pl 脚本现已废弃，不再受支持。
- 由于将始终通过 HTTPS 与 CP 服务器进行通信，安全参数已废弃。因此，在 `/etc/vxfenmode` 中启用或禁用此参数不会产生任何影响。

已废弃的属性

下表列出了在此版本中废弃的属性。

表 1-3 在此版本中废弃的属性

属性名	代理类型
SecondLevelMonitor	Apache **注意：** SecondLevelMonitor 属性在 VCS 6.1 中已废弃。可以改用 Apache 资源类型级别的 LevelTwoMonitorFreq 属性
DetailMonitor	Oracle、Sybase **注意：** 如果在早期版本中启用了详细信息监视，请在将 VCS 手动升级到 6.1 时，将 LevelTwoMonitorFreq 属性的值设置为 DetailMonitor 属性的值。

已解决的问题

本节介绍此版本中已修复的事件。

已解决的 LLT、GAB 和 I/O 防护问题

表 1-4 列出了已解决的 LLT、GAB 和 I/O 防护方面的问题。

表 1-4 已解决的 LLT、GAB 和 I/O 防护问题

事件	说明
2619600	在已为数据磁盘启用 SCSI-3 防护的 SFHA 或 SFCFSHA 节点上执行实时分区移动性 (LPM) 之后，设备或磁盘上的 I/O 因出现保留冲突而失败。
2869763	运行 `addnode -responsefile` 命令时，如果集群正使用 LLT over UDP，则新节点上生成的 `/etc/llttab` 文件不正确。因此，此过程将会失败，且您无法使用 CPI 响应文件将节点添加到集群。

事件	说明
2991093	当 HAD 终止时，首选防护节点权重不会重置为默认值。尽管该节点上缺少高可用性，但在网络分裂情况下仍优先防护该节点。
2995937	vxfen 使用的首选防护节点权重的默认值为 1（一）。但是，当 HAD 在没有任何服务组的情况下启动，或者如果 HAD 已停止或终止，则节点权重将重置为 0（零）。由于当 HAD 终止时，vxfen 将首选防护权重重置为其默认值，因此停止 HAD 和终止 HAD 将显示不同的首选防护权重。
2110148	安装程序无法拆分在一个或多个 CP 服务器中注册的集群。
2802682	重新安装堆栈之后，如果使用现有配置文件，则基于服务器的防护可能无法启动。
2858190	如果系统中没有安装 VRTSvxfen 文件集，则 vxfentsthdw 实用程序正常运行所需的特定脚本文件不可用。因此，如果系统中没有安装 VRTSvxfen 文件集，则无法从安装介质中运行实用程序。
3101262	GAB 队列过载，导致 I/O 传送期间面临内存压力。
3218714	GAB 不记录有关更改可调参数值的消息。
2858076	更改模块参数 `gab_conn_wait` 不起作用。

已解决的安装相关问题

表 1-5 已解决的安装相关问题

事件	说明
2873102	安装、配置或卸载 VCS 时，安装程序将提示您有选择性地将安装日志上传到 Symantec 网站。如果安装程序遇到连接问题，则可能出现错误。
2737124	如果手动升级 `VRTSvlic` 文件集，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。
2141446	从 VCS 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 Veritas Operations Manager Server，会重复记录提示。

已解决的 VCS 引擎问题

表 1-6 列出了已解决的 VCS 引擎问题。

表 1-6 已解决的 VCS 引擎问题

事件	说明
2858188	如果您尝试使用 gcoconfig 重新配置已配置的 Global Cluster Option (GCO)，则在重新配置全局集群选项时，该命令不会更改现有 GCO IP。
2941155	在 GCO 环境中声明集群故障时，Symantec Cluster Server (VCS) 在故障集群上不将组标记为脱机。
2954319	在负载较重的系统上，记录程序线程经常从 GAB 选取 SIGABRT。记录程序线程以低优先级运行且不能进行计划。因此 SIGABRT 未处理且 GAB 使计算机发生混乱。
2736627	如果在系统上禁用 IPv6，则远程集群状态保持 INIT 状态且 Icmp 心跳状态保持 UNKNOWN。
3042450	在子服务组发生故障时，冻结并配置为 online local hard 依赖关系的父服务组将处于脱机状态。
3079893	在某服务组联机后，如果该服务组中的资源发生故障以及如果该服务组的 OnlineRetryLimit 和 OnlineRetryInterval 设置为非零值，则 Symantec Cluster Server 不重新尝试将该服务组联机。
3090710	高可用性后台驻留程序 (HAD) 启动并在 VxFEN 驱动程序配置完成前停止。
3207663	用户触发“hauser -addpriv”命令为组设置用户权限并提供不带短划线的任何字符串，而不是“-group”选项时，不会看到语法错误且将设置不正确的权限。
3112608	在服务组切换失败后，资源将无法联机。

已解决的捆绑代理问题

表 1-7 列出了已解决的捆绑代理问题。

表 1-7 已解决的捆绑代理问题

事件	说明
2989861	为 havmconfigsync 命令显示不正确的命令用法。
2952387	需要修改 LPAR 代理，以便 VCS 在切换过程中使用实时迁移。
2962270	Apache 代理要求联机监视 IMF 支持。
2954312	如果从 HMC 查看到的 DLPAR 主机名与 DLPAR 名称不相同，则 MemCPUAllocator 代理将无法向 DLPAR 提供 CPU 或内存。

事件	说明
2964772	如果 NFSRestart 资源脱机，则 NFSRestart 代理可能会意外停止本地容器中的 NFS 进程。
2523171	如果已为服务组设置 ContainerInfo 属性，且“Enabled”键已设置为 1（一）以外的某个值，则运行 `hawparsetup.pl` 会将“Enabled”键的值重写为 1。因此，`hawparsetup.pl` 不检查是否已设置“ContainerInfo”属性中的“Enabled”键。
3315273	如果在资源中配置的卷组具有的磁盘超过 128 个，则 LVMVG 资源无法联机。
3028760	联机或脱机操作期间，NFSRestart 资源无法启动 NFS 进程，例如 `statd` 和 `lockd`。

已解决的 AMF 相关问题

表 1-8 已解决的 AMF 问题

事件	说明
2937673	amfstat、组取消注册和事件通知上下文中出现争用条件，从而导致 AMF 驱动程序出现混乱。
2848009	AMF 向代理通知某些事件时，如果该代理退出，AMF 有时会导致节点出现混乱。
2703641	如果 amf 监视的某些事件在安装或卸载 VRTSamf 修补程序后仍保持已注册状态，则会安装或卸载该修补程序。
3030087	`amfconfig -Uo` 命令必须停止 IMFD 以及 AMF 在内部启动或设置的其他功能。
2954309	强制从 AMF 停止脚本取消配置 AMF 会删除代理可能存在的对 AMF 的依赖关系。
3191098	卸载 VXFS 文件系统时，AMF 驱动程序导致计算机出现混乱。受 AMF 驱动程序的影响，函数有时会不停调用自身，从而导致堆栈损坏和混乱情况。
3090229	vxconfigd 后台驻留程序无响应时，用于磁盘组通知的 libusnp_vxnotify.so 库会进入无限循环。这会导致 AMF 进入不一致状态，使得 AMF 驱动程序进而导致节点发生混乱。
3145047	受到 AMF 与 VXFS 交互的方式的影响，即使没有任何装入处于联机状态，AMF 仍会访问 VXFS 驱动程序，而不会真正保留模块引用。因此，尽管 AMF 正在访问 VXFS，仍可以将其卸载。

事件	说明
3133181	由于 AMF 驱动程序发生运行错误，IMFD 向 AMF 发出的 ioctl 调用有时会在 AMF 内停滞。此时 IMFD 进程无法退出，直至此 ioctl 调用返回到用户空间。
3018778	使用 `haimfconfig` 命令时显示 Perl 错误。
3259682	如果 `vxconfigd` 挂起，则尝试从 `vxconfigd` 获取磁盘组状态的 imfd 注册线程也会挂起。因此，等待 IMFD 的 `amfregister` 命令会停滞。
3279336	如果 AMF 尚未配置，但仍在向 AMF 注册磁盘组资源，则这两种上下文都可能会进入挂起状态。
3177476	如果向 AMF 联机注册的进程在触发后撤消注册，计算机会发生混乱。

已解决的 Enterprise Agent 问题

表 1-9 列出了已解决的 Enterprise Agent 问题。

表 1-9 已解决的 Enterprise Agent 问题

事件	说明
1938138	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。
3088915	即使 Oracle 进程正在容器内部运行，VCS 仍将报告在容器内部中配置为 OFFLINE 的 Oracle 资源的状态。
2847994	ASMDG 代理按用户命令所指示发现设备（任何一个卷）繁忙时，ASMDG 代理将延迟脱机入口点的退出。对于在 ASMDG 代理的 DiskGroup 属性中提到的每个磁盘组，代理将运行 SQL 命令并获取该代理使用的卷列表。
3240209	在 Oracle 联机操作期间，由于模式匹配不正确，因此 Oracle 代理不必要地尝试备份数据库。
1805719	因为健康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。

已解决的操作问题

表 1-10 列出了已解决的 Enterprise Agent 问题。

表 1-10 已解决的操作问题

事件	说明
3210553	如果修改了系统标记但却未选择复制数据集群 (RDC) 设置中的防护选项，则伸展站点向导无法修改标记。

已知问题

本节介绍了本版本中的已知问题。

与安装和升级 VCS 相关的问题

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 [2574731]

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
```

resstatechange 触发器发出错误警告

重新启动资源时，可能会遇到下列警告：

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

解决方法：在未来版本中，重新启动资源时，不会调用 resstatechange 触发器。相反，如果设置 TriggerResRestart 属性，则将调用 resrestart 触发器。最新版本中提供了 resrestart 触发器。有关详细信息，请参考 VCS 文档。

在备用磁盘上升级到 6.1 之后，VRTSsfcpi 文件集 仍会保留 (2811749)

在 AIX 上，如果运行命令 `alt_disk_scenario` 执行磁盘克隆，并从 6.0 或更高版本升级到 6.1，则较旧版本的 VRTSsfcpi 文件集 将会保留。

解决方法：完成升级后，有选择性地卸载较旧版本的 VRTSsfcpi60 文件集。保留较旧版本不会造成任何危害。

无法从备用磁盘通过手动执行 Live Upgrade 来卸载 VRTSvcsea 软件包

说明：在手动执行 Live Upgrade 过程（从 5.1x 升级至 5.1SP1）中，所有软件包均被复制到备用根磁盘中。但是，无法从备用磁盘卸载 VRTSvcsea 软件包以将其升级至 5.1SP1。

解决方法：不是删除 VRTSvcsea 软件包，而是必须应用修补程序将此软件包升级至 5.1SP1 版本。

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。

滚动升级期间，引擎日志中显示 Perl 消息 [2627360]

在配置了 MultiNICA 资源的情况下从 VCS 5.1SP1 滚动升级到 6.0 时，如果在系统上升级了 VRTSperl 文件集而未升级 VRTSvcsag 文件集，则可能会显示与 Perl 代码相关的消息。该消息与以下消息类似：

```
Using a hash as a reference is deprecated at MultiNICA.pm line 108.
```

解决方法：完成到 VCS 6.0 的滚动升级。

停止 Web 安装程序导致出现错误消息称设备正忙 (2633924)

如果您启动 Web 安装程序，然后执行一项操作（如预先检查、配置或卸载），您可能会收到错误消息称设备正忙。

解决方法：执行以下操作之一：

- 终止 start.pl 进程。

- 再次启动 Web 安装程序。在第一个网页中，您会看到会话仍然处于活动状态。接管此会话并结束它，或者直接终止它。

如果已配置非共享的（已分离）WPAR，在安装、升级或卸载任何 Symantec 产品时，无法相应地在 WPAR 中安装、升级或卸载文件集 (3313690)

在 AIX 上，如果已配置非共享的（已分离）工作负载分区 (WPAR)，通过 Symantec 产品安装程序对任何 Symantec 产品执行安装、升级或卸载任务时，无法相应地在 WPAR 中安装、升级或卸载文件集。

解决方法：此问题没有解决方法。

如果已配置共享的（系统）WPAR，在安装、升级或卸载任何 Symantec 产品时，无法相应地在 WPAR 中同步文件集 (3313690)

在 AIX 上，如果已配置共享的（系统）工作负载分区 (WPAR)，通过 Symantec 产品安装程序对任何 Symantec 产品执行安装、升级或卸载任务时，无法相应地安装、升级或卸载文件集。

解决方法：在安装、升级或卸载任务后，执行以下命令以在全局系统中同步 WPAR：

```
# /usr/sbin/syncwpar -A
```

由于 CP 服务器处于安全模式，从 6.0 之前的版本滚动升级 VCS 将失败 [3262900]

如果 CP 服务器配置为以安全模式运行，不支持将 VCS 从低于 6.0 的版本滚动升级到 6.1。由于 `vxcpserv` 进程与共享身份验证不兼容，因此 CP 服务器服务组无法在执行滚动升级的第 1 阶段后联机。

解决方法：使用完全升级或分阶段升级，而不使用滚动升级。

VCS 的操作问题

使用 sqlplus 连接到不受 VCS 控制的数据库所用的时间太长而无法响应

拔下公共网络电缆之后，使用 sqlplus 连接到不受 VCS 控制的数据库花费的时间超过 10 分钟而无法响应。[704069]

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《Symantec 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。

禁用存储时 NFS 集群 I/O 出现故障 [2555662]

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。

如果在联机迁移设置处于 partial 状态时系统重新启动，则恢复和回滚到原始配置可能不会成功 (2611423)

在从 LVM 联机迁移到 VxVM 卷期间，如果在迁移设置处于 partial 状态时系统重新启动，即 start 操作尚未成功完成，则 recover 和 abort 操作可能无法恢复和回滚配置。

解决方法： 这需要根据状态手动干预以进行清理，从而还原原始配置。

CP 服务器不允许在其运行时添加和删除 HTTPS 虚拟 IP 或端口 [3322154]

当 CP 服务器正在运行时，不支持添加和删除 HTTPS 虚拟 IP 或端口。但是，您可以添加或删除 IPM 虚拟 IP 或端口。

解决方法：没有解决方法。 如果您想为 HTTPS 添加新的虚拟 IP，您必须遵循生成 CP 服务器 (server.crt) 的 HTTPS 证书的整个手册过程，如《Symantec Cluster Server 安装指南》中所述。

CP 服务器不支持通过 HTTPS 协议进行 IPv6 通信 [3209475]

使用 HTTPS 协议时，CP 服务器不支持进行 IPv6 通信。这意味着在 VCS 6.1 中，侦听 HTTPS 的 CP 服务器只能使用 IPv4。因此，VCS 6.1 防护客户端也只能使用 IPv4。

解决方法：没有解决方法。

CP 服务器在多节点集群上从 6.0 升级到 6.1 后，如果使用默认数据库路径，CP 服务器服务组无法联机 [3326639]

如果在启用安全性的情况下进行升级之前，在多节点集群上配置了 CP 服务器，则在 CP 服务器升级后必须重新配置 CP 服务器。如果重用旧凭据和旧数据库路径，则 CP 服务器服务组不会联机。由于 6.0 版和 6.1 版中 CP 服务器的默认数据库路径不同，因此重用旧凭据和默认数据库路径会导致 CP 服务器服务组无法联机。

解决方法：如果在启用安全性的情况下配置 CP 服务器多节点集群，并且在 CP 服务器升级后重新配置 CP 服务器时要重用旧凭据（如数据库路径），则请在升级前后使用相同的数据库路径。

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 [1744854]

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

hacf -cmdtocf 命令生成一个断开的 main.cf 文件 [1919951]

将 `hacf -cmdtocf` 命令与 `-dest` 选项一起使用会从类型文件删除 include 语句。

解决方法：在使用 `hacf -cmdtocf` 命令生成的 main.cf 文件中添加 include 语句。

在执行 CPU 绑定时 VCS 无法验证处理器 ID [2441022]

如果在尝试将 HAD 绑定到远程系统上的处理器时指定了无效的处理器编号，HAD 不会绑定到任何 CPU。不过，此命令不会显示任何错误来指示指定的 CPU 不存在。具体的错误会记录到绑定操作失败的节点上，各个值将恢复为默认值。

解决方法：Symantec 建议您在本地系统上修改 CPUBinding。

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 [2653688]

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]

如果没有任何父依赖关系的顶层资源处于禁用状态，则其他资源将不联机，且显示下面的消息：

```
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 [2490331]

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：终止代理进程。

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

全局服务组中的两个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：确保在全局服务组中的两个集群中，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 [2653695]

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。

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。

提升的 TargetCount 禁止使用 `hagrp -online -sys` 命令将服务组联机 [2871892]

启动服务组脱机、且在脱机完成之前，如果启动强制刷新，则早期启动的服务组的脱机将视为故障。由于资源的起始位已清除，因此服务组将转为OFFLINE|FAULTED状态，但 TargetCount 仍会增大。

解决方法：没有解决方法。

使用 `vcsencrypt` 或 `vcsdecrypt` 时系统有时会显示错误消息 [2850899]

如果在系统中没有配置随机数生成器的情况下运行 vcsencrypt 或 vcsdecrypt，则系统有时会显示以下错误消息：

```
VCS ERROR V-16-1-10351 Could not set FIPS mode
```

解决方法：确保系统中已定义随机数生成器，使加密能够正确运行。通常，随机数生成器所需的文件为 /dev/random 和 /dev/urandom。

在两个连续主集群和辅助集群失败的情况下，自动故障转移无法进行 [2858187]

如果尚未在 GCO 中配置含 steward 的三个集群（clus1、clus2、clus3），且 clus1 与 clus2 断开连接，则 clus1 会将查询发送至 clus3，检查 clus2 的状态，了解以下条件之一是否仍然存在：

1. 如果能够确认 clus2 已关闭，则将 clus2 标记为 FAULTED。
2. 如果无法将查询发送至 clus3，则将假定网络已断开，且将 clus2 标记为 UNKNOWN

在第二种情况下，即使 ClusterFailoverPolicy 已设置为 Auto，自动故障转移也不会发生。您必须手动对全局服务组进行故障转移。

解决方法：从发生上述情况的集群内的不同地理位置中配置 steward。

GCO 集群保持 INIT 状态 [2848006]

配置 GCO 之后，GCO 集群仍保持 INIT 状态，其原因如下：

- 两个集群之间没有建立适当的信任关系（如果集群安全）。
- 没有将防火墙正确配置为允许 WAC 端口 (14155)。

解决方法：确保已纠正以上两种情况。有关在两个集群之间建立信任关系的信息，请参考《Symantec Cluster Server 管理指南》。

如果集群是安全的，则非 root 用户的 `ha` 命令可能会失败 [2847998]

如果先使用没有主目录的非 root 用户，然后为同一个用户创建主目录，则 `ha` 命令无法运行。

解决方法

1 删除 /var/VRTSat/profile/<user_name>，

2 删除 /home/user_name/.VRTSat。

3 删除同一个非 root 用户所拥有的 /var/VRTSat_lhc/<cred_file> 文件。

4 使用同一个非 root 用户运行 `ha` 命令（此步骤将会成功）。

在安全的 FIPS 模式集群上执行每个 `ha` 命令需要较长时间 [2847997]

对于非 root 用户来说，在 FIPS 安全模式集群中，与在没有 FIPS 的安全模式集群相比，`ha` 命令所需的时间要多 2-3 秒。这些额外所需的时间供加密模块可用于 FIPS 模式之前执行 FIPS 自检。

解决方法：没有解决方法。

对任何标量属性运行 -delete -keys 都会导致核心转储 [3065357]

对任何标量属性运行 -delete -keys 并不是一项有效的操作，请勿使用。不过，任何无意或有意使用此命令都可能导致引擎发生核心转储。

解决方法：没有解决方法。

在定义了 Load 和 Capacity 的情况下启用 Cluster Statistics 时，VCS 进入 admin_wait 状态 [3199210]

如果出现以下情况，则 VCS 会在本地启动时进入 admin_wait 状态：

1. Statistics 属性值设置为默认值 Enabled。
2. Group Load 和 System Capacity 值在 main.cf 中的 Units 中定义。

解决方法：

1. 在集群中的所有节点上停止 VCS。
2. 执行以下任一步骤：
   - 在集群中的一个节点上编辑 main.cf，并将 Statistics 属性设置为 Disabled 或 MeterHostOnly。
   - 从 main.cf 中删除 Group Load 和 System Capacity 值。
3. 在节点上运行 hacf -verify，以验证配置是否有效。
4. 在节点上启动 VCS，然后在集群中的其余节点上启动 VCS。

如果未将 VCS 设置为自动启动，并且在启动 VCS 前 utmp 文件为空，代理将报告错误状态[3326504]

如果在重新启动后未将 VCS 配置为自动启动，并且在使用 hastart 命令手动启动 VCS 前已清空 utmp 文件，某些代理可能会报告错误状态。

utmp 文件（不同操作系统中文件名可能会有所不同）用于维护为特定计算机完成的重新启动记录。hastart 命令使用的检查引导实用程序使用由 OS 提供的函数，而 OS 使用 utmp 文件查找是否已重新启动系统，以便在代理启动前删除各种代理的临时文件。如果 OS 函数未返回正确值，高可用性后台驻留程序 (HAD) 将启动，但未删除失效的代理文件。这可能会导致某些代理报告错误状态。

解决方法：如果用户希望删除 utmp 文件，则仅当 VCS 已运行时执行此操作，或客户应在启动 VCS 前手动删除 /var/VRTSvcs/lock/volatile/ 中的临时文件。

与捆绑代理相关的问题

NFS 服务器关闭后 VCS 资源可能会超时 [2129617]

如果服务器 NFS 装入的文件系统和 NFS 服务器关闭或无法访问，VCS 资源可能会超时。只有 AIX 平台会出现此行为。

解决方法：必须卸载 NFS 装入的文件系统使集群恢复正常。

使用 IPv6 协议时 MultiNICB 资源可能会表现出意外行为 [2535952]

使用 IPv6 协议时，请将 LinkTestRatio 属性设置为 0。如果将此属性设置为其他值，MultiNICB 资源可能会表现出意外行为。

解决方法：将 LinkTestRatio 属性设置为 0。

Application 代理无法处理用户为 root、设置了 envfile 且 shell 为 csh 的情况 [2490296]

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。

使 LPAR 资源脱机可能会失败 [2418615]

使 LPAR 资源脱机可能会失败，并在 engine_A.log 文件中记录下面的消息。

```
<Date Time> VCS WARNING V-16-10011-22003 <system_name>
LPAR:<system_name>:offline:Command failed to run on MC
<hmc_name> with error HSCL0DB4 An Operating System
Shutdown can not be performed because the operating system image
running does not support remote execution of this task from the HMC.
This may be due to problem in communication with
MC <hmc_name>
```

这是因为 HMC 和管理 LPAR 之间的 RMC 失败。由于 LPAR 在脱机状态下无法正常关闭，因此 LPAR 会在 clean 调用过程中强行关闭，因此它会显示为已出故障。

解决方法：如果要将 RSCT 后台驻留程序重复用于 LPAR 和 HMC，请参考《Symantec Storage Foundation™ and High Availability Solutions 虚拟化指南》。

LPAR 代理可能无法显示正确的 LPAR 状态 [2425990]

虚拟 I/O 服务器 (VIOS) 重新启动时，LPAR 代理可能无法获得这种资源的正确状态。在这种情况下，LPAR 代理可能无法显示 LPAR 的正确状态。

解决方法：重新启动管理 LPAR 和依赖于该 VIOS 的所有受管 LPAR。

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。

CoordPoint 代理一直处于故障状态 [2852872]

CoordPoint 代理一直处于故障状态，是因为它检测到 `rfsm` 处于重放状态。

解决方法：HAD 停止之后，重新配置防护。

在容器中运行的应用程序不支持防止并发冲突 (PCV) [2536037]

对于在容器中运行的应用程序，VCS 将使用一项类似的功能，就像没有向 IMF 注册该资源一样。因此，没有用来使资源脱机的 IMF 控制机制。 当同一资源在多个节点上联机时，代理会检测到这种情况并将此报告给引擎。引擎使用脱机监视程序使资源脱机。因此，即使在经过一段滞后时间后才检测到同一资源同时在多个节点上联机，VCS 也会使该资源脱机。

对于在 AIX 上的 WPAR 内运行的应用程序，PCV 不起作用。

解决方法：没有解决方法。

VCS 不监视已经存在的 WPAR 内的应用程序 [2494532]

如果在安装 VCS 时系统中已存在 WPAR，并且需要使用 VCS 监视此 WPAR 或此 WPAR 内运行的应用程序，则 VCS 不会监视在此 WPAR 内运行的应用程序。这是因为 VCS 软件包/文件在此 WPAR 内不可见。

解决方法：对此 WPAR 运行 `syncwpar` 命令。这会使 VCS 软件包/文件在此 WPAR 内可见，随后 VCS 便可以监视在此 WPAR 内运行的应用程序。

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 和 DNS 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。

指示 HMC 用户和 HMC 名称错误的错误消息未反映正确的问题

指示 HMC 用户和 HMC 名称错误的 errorsd 未反映正确的问题。如果您在 LPAR 资源的 engine_A.log 中看到如下错误，这表明 HMC 用户不正确：

```
Permission denied, please try again
Permission denied, please try again
```

如果您在 LPAR 资源的 engine_A.log 中看到如下错误，这表明 HMC 名称不正确：

```
ssh: abc: Hostname and service name
not provided or found.
```

您必须查看 applicationha_utils.log 文件确认这一名称。

所有配置的 VIOS 关闭时，LPAR 代理可能会转储核心 [2850898]

如果使用的是虚拟输入输出服务器 (VIOS)，则在 VIOS 重新启动/重新引导/崩溃后，LPAR 需要重新启动。如果在 VIOS 重新引导后管理 LPAR 未重新启动，则 LPAR 代理可能会转储核心。

解决方法：重新启动依赖已重新引导的 VIOS 的管理 LPAR。

NFS 客户端报告因网络裂脑而导致的 I/O 错误 [3257399]

在发生网络裂脑后，失败的节点可能会出现一段比较混乱的时间。因此，当该故障节点上的某些资源（如 IP 资源）仍处于联机状态时，故障转移节点上的服务组可能无法联机。此外，还会禁用该故障节点上的磁盘组，但相同节点上的 IP 资源可继续处于联机状态。

解决方法：在服务组中的每个系统上，使用保留为包含 DiskGroup 资源的服务组配置 preonline 触发器：

1 将 preonline_ipc 触发器从 /opt/VRTSvcs/bin/sample_triggers/VRTSvcs 复制到 /opt/VRTSvcs/bin/triggers/preonline/，并将其命名为 T0preonline_ipc：

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

2 为该服务组启用 preonline 触发器。

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

可识别 WPAR 的代理无法在非共享 WPAR 中运行 [3313698]

非共享 WPAR 具有可写的 WPAR 本地文件系统：/usr 文件系统和 /opt 文件系统。通用产品安装程序在全局环境的 /opt/VRTSvcs 中安装 VCS 软件包，并在 /usr/lib 中安装库。由于 VCS 软件包无法与非共享 WPAR 上的 /usr 和 /opt 的本地副本同步，因此 VCS 软件包对非共享 WPAR 不可用。如果没有 VCS 软件包，配置为监视非共享 WPAR 中的应用程序的代理无法运行。

解决方法：没有解决方法。

可识别 WPAR 代理无法记录安全集群中的消息 [3343222]

可识别 WPAR 代理无法记录安全集群中的消息。

解决方法：在每个集群节点上执行下列步骤：

1 如果 WPAR 资源不存在，则请运行 hawparsetup 实用程序：

```
# /opt/VRTSvcs/bin/hawparsetup.pl <service_group> <resource>
 <WPAR> <password> <systems>
```

2 要查找 FQDN 格式的域名，请运行：

```
# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/vssat
 listpd -t ab|grep -w vcs_lzs | awk {'print $NF'}
```

上述命令将提供完全限定域名。

例如：vcs_lzs@81a4f374-1dd2-11b2- 80a4-163d778711bd

3 如果步骤 2 中提及的命令输出提供了域名，请转至步骤 5，或使用以下命令生成 FQDN 格式的域名：

```
# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/vssat
 createpd -t ab -d vcs_lzs
```

4 查找 FQDN 格式的域名

```
# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/vssat
 listpd -t ab|grep -w vcs_lzs | awk {'print $NF'}
```

5 使用以下命令（其中提及了 FQDN）中的上述域名。

```
# /opt/VRTS/bin/hauser -add
 w_<wpar_resource_name>_<clustername>@FQDN
#  /opt/VRTS/bin/hauser  -addpriv
 w_<wpar_resource_name>_<clustername>@FQDN
 Administrator -group <service_group>
# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/vssat
 showprpl --pdrtype ab --domain vcs_lzs
--prplname w_<wpar_resource_name>_<clustername>
#   echo $?
```

如果返回代码为非零值，则运行以下命令，

```
# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/vssat
 addprpl -t ab -d vcs_lzs -p w_<wpar_resource_name>_<clustername>
 -s <password> -q service
# clogin <wpar_name> "VCS_HOST=<host_name>; export VCS_HOST;
 VCS_DOMAIN=<FQDN>; export VCS_DOMAIN; VCS_DOMAINTYPE=vx; export
 VCS_DOMAINTYPE; /opt/VRTSvcs/bin/halogin
 w_<wpar_resource_name>_<clustername>  <password>""
```

如果系统已加载，则代理会停滞或需要一些时间来处理命令 [3323253]

如果代理运行所在的系统已加载，则代理可能会停滞或需要较长时间来处理命令。

解决方法：使用以下命令将代理的 NumThreads 值设置为 1：

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

从存储阵列分离或重新挂接一个或多个协调磁盘后，CoordPoint 代理出现故障 (3317123)

从存储阵列分离或重新挂接协调磁盘后，CoordPoint 代理可能会出现故障，因为它读取 I/O 防护内核模块中存储的旧值。

解决方法：运行 `vxfenswap` 实用程序，刷新基于服务器的 I/O 防护和基于磁盘的 I/O 防护的协调点上的注册键。即使注册键未丢失，您也必须运行 `vxfenswap` 实用程序，刷新 I/O 防护内核模块中存储的协调点信息。

有关刷新基于服务器和基于磁盘的 I/O 防护的协调点上的注册键的详细信息，请参考《Symantec Cluster Server 管理指南》。

Mount 资源不支持在 MountPoint 和 BlockDevice 属性值中使用空格 [3335304]

Mount 资源无法处理配置的 MountPoint 或 BlockDevice 属性值中间的空格。

解决方法：没有解决方法。

与 VCS 数据库代理相关的问题

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

Symantec 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《Symantec 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。

如果 sybase 服务器名称在配置文件末尾提供，则 IMF 注册将失败 [2365173]

AMF 驱动程序支持长度不超过 80 个字符的参数。为使 AMF 能够检测到 Sybase 进程的开头，Sybase 服务器名称必须出现在参数的前 80 个字符内。

解决方法：必须让服务器名称 -sSYBASE_SERVER 在配置文件中居于第一行：`ASE-15_0/install/RUN_SYBASE_SERVER`。

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 (2027896)

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 [1442255]

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。

使用多个资源时在节点上发现对 VCS 命令的响应发生延迟，且系统的 CPU 使用率或 swap 使用率高 [3208239]

如果在 VCS 节点上配置大量要监视的资源，并且 CPU 使用率接近 100% 或 swap 使用率非常高，则 VCS 对命令的响应可能会延迟数分钟。

其中一些命令如下所述：

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

当相关 VCS 代理没有足够的 CPU 带宽来处理命令时，便会出现延迟。代理也可能忙于处理大量暂停的内部命令（如定期监视每个资源）。

解决方法：更改面临此问题的某些 VCS 代理类型属性的值，并在系统恢复正常 CPU 负载后还原原始属性值。

1 备份属性的原始值，如 IMF 属性的 MonitorInterval、OfflineMonitorInterval 和 MonitorFreq。

2 如果代理不支持智能监视框架 (IMF)，则增大 MonitorInterval 和 OfflineMonitorInterval 属性的值。

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

其中，<TypeName> 是发生延迟时所用代理的名称，<value> 是适用于您环境的所有数值。

3 如果代理支持 IMF，则增大 IMF 的 MonitorFreq 属性值。

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

其中，<value> 是适用于您环境的所有数值。

4 等待几分钟，确保 VCS 已执行所有暂停命令，然后执行任何新的 VCS 命令。

5 如果延迟仍然存在，请适当地重复步骤 2 或 3。

6 如果 CPU 使用率恢复正常限值，则将属性变更恢复为备份值，以避免检测资源故障时出现延迟。

CFSMount 代理可能无法与 VCS 引擎进行心跳通信，并且在具有高内存负载的系统上的引擎日志中记录错误消息 [3060779]

在具有高内存负载的系统上，CFSMount 代理可能无法与 VCS 引擎进行心跳通信，导致引擎日志中出现 V-16-1-53030 错误消息。

VCS 引擎必须从 CFSMount 代理处接收定期心跳，以确保 CFSMount 代理在系统上正常运行。心跳由 AgentReplyTimeout 属性决定。由于高 CPU 使用率或内存工作负载（例如，swap 使用率高于 85%），代理可能无法获得足够的 CPU 周期来进行安排。这将导致与 VCS 引擎的心跳通信丢失，因此 VCS 引擎将终止代理并启动新代理。可以通过引擎日志中的以下错误消息进行识别：

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

解决方法：增大 AgentReplyTimeout 值并查看 CFSMount 代理是否变稳定。如果此解决方法无法解决该问题，则尝试以下解决方法。通过运行以下命令，为 CFSMount 代理将属性 NumThreads 的值设置为 1：

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

在运行上述命令之后，如果 CFSMount 代理仍持续终止，请将此问题报告给 Symantec 支持团队。

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 [1919933]

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。

已知的 LLT 问题

本节介绍此版本中已知的 LLT 相关问题。

LLT 可能无法与虚拟环境中对等节点上的 LLT 进行连接 (2343451/2376822)

在从 5.0 MP3 或更早版本升级到版本 6.0 后，LLT 可能无法与 AIX 虚拟环境中对等节点上的 LLT 进行连接。

这是 IBM VIOS 的已知问题。 请在 VIOS 服务器上安装 APAR IV00776。 如果没有此修补程序，VIOS 将无法处理新的 LLT 数据包头，因此会丢弃数据包。

解决方法：禁用 SEA 适配器的 largesend 属性。使用以下命令检查每个 VIOS 上的 SEA 适配器（在该适配器上根据 LLT 映射配置虚拟链接）的属性：

```
# lsattr -El SEA
```

如果 largesend 设置为 1，请使用以下命令将其设置为 0：

```
# chdev -l SEA -a largesend=0
```

LLT 端口统计数据有时显示 recvcnt 大于 recvbytes (1907228)

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。

停止 LLT 服务后且正在卸载 LLT 时，节点可能出现混乱 [3333290]

LLT 使用 AIX 操作系统的 `xmfree()` 函数来释放网络消息。此函数将堆作为参数。堆是在 AIX 中分配内存之前创建的。在少数情况下，LLT 卸载期间，当 LLT 使用 `xmfree()` 函数释放消息时，LLT 可能会销毁此堆。此问题会导致 LLT 使节点发生混乱。

没有解决方法。您可以重新启动节点并恢复正常操作。

已知的 GAB 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。

解决方法：此问题没有解决方法。

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用条件。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。

解决方法：此问题没有解决方法。

已知的 I/O 防护问题

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《Symantec 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@sys1,
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：尝试在应用集群上启动 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 或更高版本后，cpsadm 命令失败 (2846727)

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 文件集，`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过程。

解决此问题

1 将 `cpsadm` 重命名为 `cpsadmbin`：

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

2 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 "$@"
```

3 将新文件的权限更改为 775：

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

通用产品安装程序无法在 5.1SP1 版本的客户端系统和 6.0 版本或更高版本的服务器之间建立信任关系 [3226290]

该问题是由 VCS 5.1SP1 版本不支持信任存储的单独目录所引起的。但是，VCS 6.0 版本及更高版本支持信任存储的单独目录。因此，由于对信任存储的支持不匹配，您无法在客户端系统和服务器之间建立信任关系。

解决方法：使用 `cpsat` 或 `vcsat` 命令在协调点服务器和客户端系统之间手动建立信任关系，以便服务器和客户端系统能够在安全模式下通信。

CP 服务器中的主机名和用户名区分大小写 (2846392)

CP 服务器中的主机名和用户名区分大小写。防护用来与 CP 服务器通信的主机名和用户名大小写必须与 CP 服务器数据库中显示的相同，否则防护将无法启动。

解决方法：确保 CP 服务器中的主机名和用户名使用相同的大小写。

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：使用通过 CP 服务器配置并在本地节点上探查到的任意虚拟 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：此问题没有解决方法。

CoordPoint 代理未报告将新磁盘添加到协调器磁盘组的情况 [2727672]

即使协调器磁盘组的构成情况由于在协调器磁盘组中添加了新的磁盘而发生更改，CoordPoint 代理的 LevelTwo 监视也不会报告故障

解决方法：此问题没有解决方法。

对于集群中的某些节点，防护可能会将 RFSM 状态显示为重放 (2555191)

校园集群环境中基于协调点客户端的防护可能会针对该集群中的某些节点将 RFSM 状态显示为重放。

解决方法：

在将 RFSM 状态显示为重放的节点上，重新启动防护。

CP 服务器进程 vxcpserv 仅与在该 CP 服务器进程启动时可用的 VIP 上的客户端节点进行通信 (3156922)

配置 CP 服务器时，CPSSG 服务组将配置为用来管理 vxcpserv 进程（CP 服务器进程）及其依赖项（仲裁资源）。CP 服务器由进程代理管理，其相关虚拟 IP 地址 (VIP) 则由仲裁资源管理。仲裁资源仅在各 VIP 之间获得仲裁时才联机。

VCS 使 CPSSG 组联机时，vxcpserv 进程仅在仲裁资源联机之前所启动的 VIP 上进行监听。对于即便在仲裁资源联机之后启动的 VIP，vxcpserv 不会进行监听。因此，CP 服务器进程仅为在 CP 服务器进程启动时可用的 VIP 上的客户端节点提供服务。

请注意，可通过发出带有平台特定标志的 netstat 命令来获得 vxcpserv 进程所监听的 VIP 的列表。

解决方法：使用下列命令重新启动在 vxcpserv 资源下配置的 CP 服务器

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

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

其中，<system> 指 CPSSG 组处于联机状态的节点。

如果您运行带有 hacli 选项的 vxfenswap 实用程序，该实用程序会从 /etc/vxfemode 文件中删除注释行 (3318449)

vxfenswap 实用程序使用 RSH、SSH 或 hacli 协议与集群中的对等节点进行通信。当您使用 vxfenswap 替换基于磁盘的防护中的协调磁盘时，vxfenswap 从 /etc/vxfenmode（本地节点）复制到 /etc/vxfenmode（远程节点）。

通过 hacli 选项，实用程序可以从远程文件 /etc/vxfenmode 中删除注释行，但在本地文件 /etc/vxfenmode 中保留注释。

解决方法：将注释从本地文件 /etc/vxfenmode 手动复制到远程节点。

仅当为基于 HTTPS 的通信配置 CP 服务器时，engine_A.log 显示一条误导性消息 (3321101)

当您仅为基于 HTTPS 的通信（而非基于 IPM 的通信）配置 CP 服务器时，engine_A.log 文件显示以下消息。

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

解决方法：忽略该消息。

vxfentsthdw 实用程序可能无法在安装有部分 SFHA 堆栈的系统上运行 [3333914]

如果已通过正确配置的 SF 和 VxVM 完整安装 SFHA 堆栈和 VCS，则 vxfentsthdw 实用程序可以运行。如果没有安装完整 SFHA 堆栈和 VCS，它也可以运行。但是，不支持在已安装和配置 SF 但未安装 VCS 的位置进行部分安装。该实用程序将显示 -g 或 -c 选项的错误。

解决方法：安装 VRTSvxfen 软件包，然后从安装介质或 /opt/VRTSvcs/vxfen/bin/ 位置运行实用程序。

如果在联机服务组中将 SysDownPolicy 设置为 AutoDisableNoOffline，防护配置将失败 [3335137]

如果将一个或多个联机服务组中的 SysDownPolicy 配置为 AutoDisableNoOffline，防护配置（如基于服务器的防护、基于磁盘的防护和禁用模式防护）将失败。由于服务组已配置为 `SysDownPolicy = { AutoDisableNoOffline }`，因此停止 VCS 失败，从而导致防护配置失败。

解决方法：配置防护之后和停止 VCS 之前，必须手动使配置为 `SysDownPolicy = { AutoDisableNoOffline }` 的服务组脱机。

当客户端节点由于节点混乱等原因发生故障时，重新启动节点后 I/O 防护在该客户端节点上不生效 (3341322)

当发生以下其中一种情况时，会出现此问题：

- 针对 HTTPS 通信配置的任一 CP 服务器发生故障。
- 针对 HTTPS 通信配置的任一 CP 服务器中的 CP 服务器服务组发生故障。
- 针对 HTTPS 通信配置的任一 CP 服务器中的任一 VIP 发生故障。

重新启动客户端节点时，将在该节点上启动防护配置。防护后台驻留程序 vxfend 会调用节点上的一些防护脚本。其中每个脚本都有 120 秒的超时值。如果这些脚本中的任何一个脚本发生故障，则该节点上的防护配置将失败。

其中一些脚本使用 `cpsadm` 命令与 CP 服务器进行通信。当节点启动时，`cpsadm` 命令将尝试使用 VIP 连接到 CP 服务器（超时值为 60 秒）。因此，如果在单个脚本中运行的多个 `cpsadm` 命令超过超时值，则总超时值将超过 120 秒，这将导致其中一个脚本超时。因此，I/O 防护在该客户端节点上不生效。

请注意，该问题不会发生在 CP 服务器和客户端集群之间的基于 IPM 的通信中。

解决方法：修复 CP 服务器。

&product_version 中的 Symantec Cluster Server Agents for Volume Replicator 已知问题

以下是 6.1 版本中新增的其他 Symantec Cluster Server Agents for Volume Replicator 已知问题。

RVGLogowner 代理的示例 main.cf 文件中存在失效条目 [2872047]

RVGLogowner 代理的示例 main.cf 文件中存在失效条目。RVGLogowner 代理的 main.cf.seattle 文件中存在失效条目，其中包括 CFSQlogckd 资源。但是，从 VCS 5.0 起不支持 CFSQlogckd。

解决方法：在 cvm 组中删除下列两行：

```
CFSQlogckd qlogckd (
             Critical = 0
            )
```

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。

如果使用其他名称导入某个注册的磁盘组，IMF 不会提供有关该磁盘组的通知 (2730774)

如果将某个磁盘组资源注册到 AMF，然后使用其他名称导入该磁盘组，则 AMF 无法识别重命名的磁盘组，所以不会向 DiskGroup 代理提供通知。因此，DiskGroup 代理会一直将该磁盘组资源报告为脱机。

解决方法：确保在导入某个磁盘组时，该磁盘组名称与注册到 AMF 的磁盘组相匹配。

直接执行 `linkamf` 时显示语法错误 [2858163]

直接执行时，Bash 无法解释 Perl。

解决方法：请按如下所示运行 `linkamf`：

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

重新启动周期过程中显示错误消息 [2847950]

在某些重新启动周期过程中，引擎日志中将记录下列消息：

```
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)
```

这不会对 IMF 的功能产生任何影响。

解决方法：没有解决方法。

当 ProPCV 阻止进程变为 ONLINE 状态以防止出现没有 I18N 支持的并发冲突时，将显示错误消息 [2848011]

当 ProPCV 阻止进程变为 ONLINE 状态以防止出现并发冲突时，将显示以下消息。消息将以英语显示，且没有 I18N 支持。

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

解决方法：没有解决方法。

libvxamf 库在执行进程表扫描时遇到错误情况 [2848007]

有时，在执行进程表扫描时，libvxamf 库会遇到错误情况。其结果是，向 AMF 的脱机注册进程将会失败。大多数情况下，当代理在此资源的下一个监视周期内再次尝试时，此注册将成功。由于此资源的传统监视将会继续，因此这并非灾难性故障。

解决方法：没有解决方法。

AMF 在控制台上多次显示不含 VCS 错误代码或日志的 StartProgram 名称 [2872064]

VCS AMF 阻止进程启动时，将在控制台和 Syslog 中显示一条消息。该消息包含已阻止启动的进程的签名。在某些情况下，此签名可能与 PS 输出中可见的签名不匹配。例如，阻止执行的 Shell 脚本的名称将输出两次。

解决方法：没有解决方法。

禁用 Apache 代理时，VCS 引擎会因为取消 Reaper 显示错误 [3043533]

当 `haimfconfig` 脚本用于禁用一个或多个代理的 IMF 时，VCS 引擎将在引擎日志中记录以下消息：

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

这是预期行为，不是问题。

解决方法：没有解决方法。

终止 imfd 后台驻留程序将孤立 vxnotify 进程 [2728787]

如果使用 kill -9 命令终止 imfd 后台驻留程序，则 imfd 创建的 vxnotify 进程不会自动退出，但会孤立。但是，如果使用 amfconfig -D 命令停止 imfd 后台驻留程序，则对应的 vxnotify 进程将会终止。

解决方法：停止任何后台驻留程序的正确方式是使用适当的命令（在这种情况下为 amfconfig -D 命令）将它正常停止，或使用会话 ID 来终止后台驻留程序。会话 ID 是后台驻留程序的 -PID（负 PID）。

例如：

```
# kill -9 -27824
```

正常停止后台驻留程序时，将停止该后台驻留程序生成的所有子进程。但是，使用 kill -9 *pid* 终止后台驻留程序并非停止后台驻留程序的建议选项，随后您必须手动终止后台驻留程序的其他子进程。

在已配置代理目录和代理文件的情况下，代理无法变为可识别 IMF 的代理 [2858160]

如果已为代理配置代理目录和代理文件，则该代理无法变为可识别 IMF 的代理。

解决方法：没有解决方法。

如果接收到将已撤消注册的资源撤消注册的请求，AMF 可能导致该系统混乱 [3333913]

如果 AMF 遇到任何内部错误，它将撤消注册无法支持的所有资源。在此类事件期间，如果任何代理调用了此类资源之一的撤消注册，AMF 可能导致该计算机混乱。

解决方法：没有解决方法。

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。

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。

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 66 页的“文档”。

与安装和升级 VCS 相关的限制

不支持使用本机操作系统工具来升级安全集群

此版本不支持使用本机操作系统工具（例如备用磁盘安装 (ADI) 和 Network Install Manager Alternate Disk Migration (NIMADM)）来升级安全集群。

关于在 Symantec Storage Foundation and High Availability 集群中升级到 6.1 的限制

Symantec Storage Foundation (SF) 6.1 要求 AIX 操作系统版本为 6.1 TL6 或更高版本。要将 SF 从 5.0 MP3 RP5 之前的版本升级到 6.1，必须先将 SF 升级到 5.0 MP3 RP5 版本。如果升级到 5.0 MP3 RP5 要求中间操作系统升级，则操作系统的级别不能超过 6.1 TL1。在升级到 5.0 MP3 RP5 之后，必须将操作系统升级到 AIX 6.1 TL6，这是 6.1 版本的最低要求。您必须将 SF 升级到 5.0 MP3 RP5，否则，如果 Symantec Storage Foundation and High Availability 集群中的节点上运行的是 AIX 6.1 TL2（或更高版本）与 SF 5.0 MP3 RP5 之前的版本，则删除该节点可能发生系统混乱或崩溃。删除该节点会造成文件系统线程退出。 混乱是 AIX 6.1 TL2 引入的检查所致，该检查会在内核线程调用退出时验证 lockcount 值。

有关详细信息，请参见以下技术说明：

http://www.symantec.com/docs/TECH67985

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/netsvc.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 文件中包含应用程序代理监视的进程的 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，如果应用程序代理仅使用 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。

不管 VCS [2162929] 中的 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。

针对目录联机事件向 IMF 注册了 WPAR 代理

目录联机事件用于监视 WPAR 根目录。 如果 WPAR 根目录的父目录已删除或已移至其他位置，则 AMF 不会向 WPAR 代理提供通知。 在 WPAR 监视程序的下一周期中，它会检测到这种变化并报告资源的状态为脱机。

应用程序代理的限制

- ProPCV 无法阻止执行在 MonitorProcesses 下配置的基于脚本的进程。

当使用 DSM 站点来标记站点边界时，校园集群防火练习不起作用 [3073907]

校园集群 FireDrill 代理当前使用 SystemZones 属性来确定站点边界。因此，校园集群 FireDrill 在启用 DSM 的环境中不受支持。

解决方法：禁用 DSM 并在应用程序服务组上配置 SystemZones 属性来执行防火练习。

不支持管理 LPAR 的实时分区移动性 (LPM)

不支持管理 LPAR 的实时分区移动性 (LPM)。

与 VCS 引擎相关的限制

当多个组出现故障时，负载无法进行整合和优化 [3074299]

当多个组同时出现故障并进行故障转移时，不整合和优化负载，无法选择目标系统。

解决方法：没有解决方法。

首选防护忽略预测的可用容量 [3077242]

VCS 中的首选防护在做防护决策时不考虑预测的可用容量。防护决策基于所配置的系统权重。

解决方法：没有解决方法。

当设置了 BiggestAvailable 策略时，SystemZone 或站点内发生故障转移 [3083757]

当配置了 BiggestAvailable 故障转移策略时，SytemZone 或站点内始终都会发生故障转移。故障转移的目标系统始终基于 SystemZone 内的最大可用系统进行选择。

解决方法：没有解决方法。

在 BiggestAvailable 和 Priority 同属一组的组中，Priority 组的负载被忽略 [3074314]

当同一集群中存在同时以 BiggestAvailable 和 Priority 作为故障转移策略的组时，不考虑 Priority 组的负载。

解决方法：没有解决方法。

与 IMF 相关的限制

- 如果某个进程使用 IMF 为脱机监视注册，则在进程和相关参数的字符超过 70 的情况下，IMF 不会检测正在执行的进程。对于 ProPCV，如果进程和相关参数的长度超过 70 个字符，IMF 可能无法阻止进程进入联机状态。此限制会影响 Application 和 Process 代理。有关详细信息，请参考《Symantec Cluster Server Bundled Agents 参考指南》。[2768558]

与 VCS 数据库代理相关的限制

DB2 RestartLimit 值 [1234959]

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。

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。

DiskGroupSnap 代理的限制 [1919329]

DiskGroupSnap 代理具有以下限制：

- DiskGroupSnap 代理不支持分层卷。
- 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：
  - 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。

使用 VIO 服务器和客户端分区虚拟化共享存储

在 Advanced POWER™ Virtualization (APV) 环境中，AIX 使用 VIO 服务器监视和管理虚拟化客户端分区的 I/O 路径。在非常高的级别上，VIO 服务器为分区提供对处于物理计算机外部的存储的访问。VIO 服务器将物理硬件封装到称为虚拟 SCSI 适配器（服务器适配器）的虚拟适配器中。在客户端上，可以创建映射到服务器适配器并允许分区连接到外部存储的虚拟适配器（客户端适配器）。

VIO 服务器为跨分区共享有限网络资源提供相似的机制。请参考随系统提供的手册以帮助设置分区，并配置和使用各种组件（如 VIO 服务器和 HMC），这些组件是 IBM 的 APV 环境的不可分割的组成部分。

将 VIO 服务器与 VCS 结合使用所需的最低修补程序级别是：版本 2.1.3.10-FP-23 及更高版本。

支持的存储

请参考 IBM 数据表：

http://www14.software.ibm.com/webapp/set2/sas/f/vios/home.html

磁盘限制

将 VCS 与 VIO 服务器及其客户端分区一起使用时，需要确保未对共享存储设置任何保留。这允许不同系统上的客户端分区能够访问和使用同一共享存储。

- 如果共享存储受 MPIO 控制，请将磁盘的 reserve_policy 属性设置为 no_reserve。
- 如果共享存储不受 MPIO 控制，请在阵列文档中查找一个用于设置磁盘的相似属性。

对 EMC 磁盘的内部测试显示，此字段映射为 EMC 磁盘的 reserve_lock 属性。这种情况下，将其设置为 no 会获得相同结果。

从不同 Central Electronics Complex (CEC) 模块上的客户端分区访问相同的 LUN

本节简要概述如何设置共享存储，以便可从不同 CEC 模块上的客户端分区看到它。

VIO 服务器和客户端分区已设置并准备就绪后，请确保在客户端分区上安装了正确级别的操作系统，并已将物理适配器映射到客户端分区以提供对外部共享存储的访问。

要创建可共享的磁盘组，需要确保不同的分区使用同一组磁盘。确保磁盘（从多个分区看到的）相同的一种好方法是使用磁盘序列号，因为磁盘序列号是唯一的。

除非另有说明，否则请在 VIO 服务器上运行以下命令（在非 root 用户模式下）。

获取感兴趣的磁盘的序列号：

```
$ lsdev -dev hdisk20 -vpd
 hdisk20
 U787A.001.DNZ06TT-P1-C6-T1-W500507630308037C-
 L401 0401A00000000  IBM FC 2107

 Manufacturer.............IBM
 Machine Type and Model......2107900
 Serial Number..............7548111101A
 EC Level...................131
 Device Specific.(Z0).......10
 Device Specific.(Z1).......0100
 …
```

确保另一个 VIO 服务器返回同一序列号。此操作确保您查看的是同一实际物理磁盘。

列出虚拟 SCSI 适配器。

```
$ lsdev -virtual | grep vhost
 vhost0  Available  Virtual SCSI Server Adapter
 vhost1  Available  Virtual SCSI Server Adapter
```

注意：通常，vhost0 是内部磁盘的适配器。在上面的示例中，vhost1 将 SCSI 适配器映射到外部共享存储。

将 hdisk20（在该示例中）映射到 SCSI 适配器之前，请更改磁盘的保留策略。

```
$ chdev -dev hdisk20 -attr reserve_policy=no_reserve
hdisk20 changed
```

要使 hdisk20（在该示例中）对客户端分区可用，请将它映射到适合的虚拟 SCSI 适配器。

如果现在要打印 hdisk20 的保留策略，输出将如下所示：

```
$ lsdev -dev hdisk20 attr reserve_policy
 value
 no_reserve
```

接下来创建一个虚拟设备以将 hdisk20 映射到 vhost1。

```
$ mkvdev -vdev hdisk20 -vadapter vhost1 -dev mp1_hdisk5
 mp1_hdisk5 Available
```

最后，在客户端分区上运行 cfgmgr 命令，使此磁盘可通过客户端 SCSI 适配器看到。

可以使用此磁盘（hdisk20 物理磁盘，在客户端分区上称为 mp1_hdisk5）创建磁盘组、共享卷，并最终创建共享文件系统。

在客户端上执行关于服务组、资源、资源属性等的常规 VCS 操作。

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《Symantec 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。

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。

操作系统不区分 IPv4 和 IPv6 数据包计数

在双堆栈配置中，当使用数据包计数且 IPv6 网络已禁用时，NIC 代理可能不检测出现故障的 NIC。由于 IPv6 网络关闭时其数据包计数仍在增加，因此该代理可能不检测故障。之所以数据包计数增加，是因为操作系统不区分 IPv4 和 IPv6 网络的数据包计数。代理因此推断 NIC 处于启动状态。如果为 IPv4 和 IPv6 资源使用同一 NIC 设备，请将 PingOptimize 设置为 0 并为 IPv6 或 IPv4 NIC 资源的 NetworkHosts 属性指定一个值。 [1061253]

在 WPAR 内运行的某个服务组在其网络连接断开时可能不会进行故障转移

对于 WPAR 配置，如果 WPAR root 在 NFS 上，则 WPAR 服务组在 NFS 连接断开时可能不会进行故障转移。此问题是由于 AIX 操作系统限制引起的。[1637430]

与 LLT 相关的限制

本节讲述了与 LLT 相关的软件限制。

VCS 尝试形成集群时，LLT over IPv6 UDP 无法检测到其他节点 (1907223)

LLT over IPv6 需要本地链接作用域多播以在 VCS 尝试形成集群时发现其他节点。如果在您的环境中多播网络连接不适宜或不可用，请使用对等节点的地址消除对多播通信的需求。

解决方法：在 /etc/lltab 文件中为每个本地链接添加 set-addr 条目。添加该条目以指定在相应的对等链接上可用的对等节点的地址。例如，将下列行添加到 lltab 文件中来为节点指定 set-addr 条目。在此示例中，节点的 IPv6 地址是 fe80::21a:64ff:fe92:1d70。

```
set-addr 1 link1 fe80::21a:64ff:fe92:1d70
set-arp 0
```

系统重新启动后 LLT 没有自动启动 (2058752)

重新启动系统后，如果未完成终端设置过程，则 LLT 不会自动启动，也不会记录任何错误消息。可以使用 `/etc/init.d/llt.rc` 命令手动启动 LLT。

如果重新安装系统，则系统重新启动时会在系统控制台上显示一条设置终端设置的消息（如果尚未设置）。直到完成终端设置过程之后，LLT 才会启动。

解决方法：解决 LLT 启动问题

1 重新启动系统后，使用任意可用方法（例如，从 HMC）打开系统控制台。

2 在控制台上，转到终端设置菜单，然后设置所选择的终端。

3 选择“**Task Completed (已完成任务)**”菜单选项。

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。

对于使用原始磁盘的协调器磁盘使用 RDAC 驱动程序和 FAStT 阵列时的限制

对于已连接存储的多径处理，AIX 将 RDAC 驱动程序用于 RDAC 阵列。因为它是主动/被动阵列，所以只有当前主动路径会显示给客户端。I/O 防护驱动程序 vxfen 只能使用单个主动路径，并且不会事先知道阵列上的协调器磁盘的被动路径。如果单个主动路径发生故障，则集群中的所有节点都会失去对协调器磁盘的访问。

协调器磁盘的路径丢失不会被发现，直到发生重新启动、裂脑或导致集群成员集更改的任何其他原因才注意到。在这些情况下集群将无法形成，而且所有节点会发生混乱以防止数据损坏。不会发生数据丢失。

解决方法：使用 DMP 并将协调器磁盘的路径指定为 DMP 路径而不是原始磁盘，以避开此限制。

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《Symantec 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 文件集以后，将不再在内存中加载 DMP 模块。在卸载 VRTSvxvm 文件集的系统上，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。

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。

文档

软件介质上的 `/docs/product_name` 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。

请确保您使用的是文档的最新版本。每个指南的第 2 页上提供了文档版本信息。每个文档的标题页上提供了出版日期。从 Symantec 网站可以获取最新的产品文档。

http://sort.symantec.com/documents

文档集

Storage Foundation and High Availability Solutions 产品系列中的每个产品均包括版本说明、安装指南和其他文档，如管理指南和代理指南。大多数情况下，您可能也需要参考关于产品组件的文档。

SFHA Solutions 文档介绍应用于此产品系列的功能和解决方案。无论使用哪个 SFHA Solutions 产品，这些文档都具参考价值。

Symantec Cluster Server 文档

表 1-11 列出了有关 Symantec Cluster Server 的文档。

表 1-11 Symantec Cluster Server 文档

书名	文件名	说明
《Symantec Cluster Server 版本说明》	vcs_notes_61_aix.pdf	提供版本信息，如产品的系统要求、更改、已解决事件、已知问题和限制。
《Symantec Cluster Server 安装指南》	vcs_install_61_aix.pdf	提供安装此产品所需的信息。
《Symantec Cluster Server 管理指南》	vcs_admin_61_aix.pdf	提供管理此产品所需的信息。
《Symantec Cluster Server Bundled Agents 参考指南》	vcs_bundled_agents_61_aix.pdf	提供有关捆绑代理、其资源和属性以及其他相关信息的信息。

书名	文件名	说明
《Symantec Cluster Server Agent 开发指南》 （仅可联机获得此文档。）	vcs_agent_dev_61_unix.pdf	提供有关多种 Symantec 代理和开发自定义代理过程的信息。
《Symantec Cluster Server Agent for DB2 安装和配置指南》	vcs_db2_agent_61_aix.pdf	提供安装和配置 DB2 代理的说明。
《Symantec Cluster Server Agent for Oracle 安装和配置指南》	vcs_oracle_agent_61_aix.pdf	提供安装和配置 Oracle 代理的说明。
《Symantec Cluster Server Agent for Sybase 安装和配置指南》	vcs_sybase_agent_61_aix.pdf	提供安装和配置 Sybase 代理的说明。

Symantec Storage Foundation and High Availability Solutions 产品文档

表 1-12 列出了 Symantec Storage Foundation and High Availability Solutions 产品的文档。

表 1-12 Symantec Storage Foundation and High Availability Solutions 产品文档

文档标题	文件名	说明
Symantec Storage Foundation and High Availability Solutions—What's new in this release（《Symantec Storage Foundation and High Availability Solutions—此版本的新增功能》） （可联机获得此文档。）	sfhas_whats_new_61_unix.pdf	提供有关此版本的新功能和增强功能的信息。
《Symantec Storage Foundation and High Availability Solutions 快速入门指南》	getting_started.pdf	提供有关使用 Veritas 基于脚本的安装程序安装 Symantec 产品的高级概述。本指南对新用户和想要快速复习的老用户很有用。
《Symantec Storage Foundation and High Availability Solutions 解决方案指南》	sfhas_solutions_61_aix.pdf	提供有关如何单独使用或配合使用 SFHA Solutions 产品组件和功能以便提高存储和应用程序的性能和恢复能力并简化管理的信息。
《Symantec Storage Foundation and High Availability Solutions 虚拟化指南》 （可联机获得此文档。）	sfhas_virtualization_61_aix.pdf	提供有关 Symantec Storage Foundation and High Availability 对虚拟化技术的支持的信息。在运行 SFHA 产品的系统上安装虚拟化软件之前，请先通读本文档。

文档标题	文件名	说明
《Symantec Storage Foundation and High Availability Solutions 灾难恢复操作指南》 （可联机获得此文档。）	sfhas_dr_impl_61_aix.pdf	提供有关配置校园集群、全局集群和复制数据集群 (RDC)，以便使用 Storage Foundation and High Availability Solutions 产品进行灾难恢复和故障转移的信息。
《Symantec Storage Foundation and High Availability Solutions 故障排除指南》	sfhas_tshoot_61_aix.pdf	提供有关使用 Symantec Storage Foundation and High Availability Solutions 时可能会遇到的常见问题和针对这些问题的可能解决方案的信息。

Symantec ApplicationHA 文档

表 1-13 列出了有关 Symantec ApplicationHA 的文档。

表 1-13 Symantec ApplicationHA 文档

文档标题	文件名	说明
《Symantec ApplicationHA 版本说明》	applicationha_notes_61_lpar_aix.pdf	介绍新功能以及软件和系统要求。本文档还包含发布时已知的限制和问题列表。
《Symantec ApplicationHA 安装指南》	applicationha_install_61_lpar_aix.pdf	介绍安装和配置 Symantec ApplicationHA 的步骤。本文档也提供一些最常见的故障排除步骤。
《Symantec ApplicationHA 安装使用指南》	applicationha_users_61_lpar_aix. pdf	提供有关配置和管理逻辑分区 (LPAR) 虚拟化环境中的 Symantec ApplicationHA 的信息。本文档也提供一些最常见的故障排除步骤。
Symantec ApplicationHA Agent for Oracle Configuration Guide （《Symantec ApplicationHA Agent for Oracle 配置指南》）	applicationha_oracle_agent_61_lpar_aix.pdf	介绍如何为 Oracle 配置应用程序监视。
Symantec ApplicationHA Generic Agent Configuration Guide （《Symantec ApplicationHA Generic Agent 配置指南》）	applicationha_gen_agent_61_lpar_aix.pdf	介绍如何为通用应用程序配置应用程序监视。
Symantec ApplicationHA Agent for DB2 Configuration Guide （《Symantec ApplicationHA Agent for DB2 配置指南》）	applicationha_db2_agent_61_lpar_aix.pdf	介绍如何为 DB2 配置应用程序监视。

文档标题	文件名	说明
Symantec ApplicationHA Agent for Apache HTTP Server Configuration Guide（《Symantec ApplicationHA Agent for Apache HTTP Server 配置指南》）	applicationha_apache_agent_61_lpar_aix.pdf	介绍如何为 Apache HTTP Server 配置应用程序监视。

Veritas Operations Manager (VOM) 是管理工具，可用于管理 Symantec Storage Foundation and High Availability Solutions 产品。如果您使用 VOM，请参考位于以下位置的 VOM 产品文档：

https://sort.symantec.com/documents

手册页

Symantec 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 Symantec 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。

Symantec 网站上联机提供了 HTML 格式的最新手册页：

https://sort.symantec.com/documents