Veritas Access 安装指南

Linux

7.4

VERITAS

Veritas Access 安装指南

上次更新日期： 2018-05-28

文档版本：7.4 Rev 1

法律声明

Veritas Technologies LLC
500 E Middlefield Road
Mountain View, CA 94043

http://www.veritas.com

技术支持

技术支持具有全球性支持中心。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。有关我们的支持服务以及如何联系技术支持的信息，请访问我们的网站：

https://www.veritas.com/support

从以下 URL 您可以管理 Veritas 帐户信息：

https://my.veritas.com

如果您对现有支持协议有疑问，请通过以下方式联系您所在地区的支持协议管理部门：

全球（日本除外）	CustomerCare@veritas.com
日本	CustomerCare_Japan@veritas.com

文档

请确保您具有文档的最新版本。每个文档的第 2 页显示了上次更新日期。每个指南的第 2 页提供了文档版本信息。可在 Veritas 网站上找到最新的文档：

https://sort.veritas.com/documents

文档反馈

您的反馈对我们很重要。请对我们的文档提出改进意见、报告错误或遗漏。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以及章节标题。请将反馈发送到：

doc.feedback@veritas.com

您也可以在 Veritas 社区网站上查看文档信息或提出问题：

http://www.veritas.com/community/

Veritas Services and Operations Readiness Tools (SORT)

Veritas Services and Operations Readiness Tools (SORT) 是一个网站，提供的信息和统计可自动处理和简化某些耗时的管理任务。根据您的产品，SORT 会帮助您准备安装和升级、识别您数据中心的风险并提高操作效率。要了解 SORT 为您的产品提供了哪些服务和工具，请参见数据表：

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

目录

1

Veritas Access 简介

本章节包括下列主题：

- 关于 Veritas Access

关于 Veritas Access

Veritas Access 是一款软件定义的横向扩展网络连接存储 (NAS) 解决方案，专为商用硬件上的非结构化数据而设计。Veritas Access 支持弹性和多协议访问，并可根据策略将数据移入和移出公有云或私有云。

您可通过以下任一方式使用 Veritas Access。

表 1-1 用于使用 Veritas Access 的界面

界面	说明
GUI	提供了集中式控制板和 Quick Actions（具有多个用于管理存储的操作项）。 有关详细信息，请参见 GUI 和联机帮助。
RESTful API	可以通过脚本自动对 Veritas Access 群集运行存储管理命令。 有关详细信息，请参见 *Veritas Access RESTful API Guide*（《Veritas AccessRESTful API 指南》）。
命令行界面（CLI 或 CLISH）	整个群集的单一管理点。 有关详细信息，请参见手册页。

表 1-2 介绍了 Veritas Access 的功能。

表 1-2 Veritas Access 主要功能

功能	说明
多协议访问	Veritas Access 支持以下协议： ■ Amazon S3 ■ CIFS ■ FTP ■ iSCSI 目标 ■ NFS ■ Oracle Direct NFS ■ SMB 3 ■ 带有 S3 的 NFS
用于 Enterprise Vault 归档的 WORM 存储	可以将 Veritas Access 配置为要由 Enterprise Vault 归档的 WORM 主存储。 经过认证，Veritas Access 可以作为 Enterprise Vault 12.1 的 CIFS 主 WORM 存储。 有关详细信息，请参见《Veritas Access Enterprise Vault 解决方案指南》。
通过 NFS 的 WORM 支持	Veritas Access 可通过 NFS 支持 WORM。
为 Enterprise Vault 归档创建分区安全通知 (PSN) 文件	在远程站点上成功备份分区之后，会在源分区创建分区安全通知 (PSN) 文件。 有关详细信息，请参见《Veritas Access Enterprise Vault 解决方案指南》。
使用最大 IOPS 设置管理应用程序 I/O 工作量	MAXIOPS 限制确定文件系统下的存储每秒总共处理的最大 I/O 数。
灵活存储共享 (FSS)	为本地存储启用群集范围内的网络共享。
横向扩展文件系统	横向扩展文件系统提供了以下功能： ■ 这种文件系统可管理跨内部存储和云存储的单一命名空间，它将为大型数据集提供更出色的容错功能。 ■ 具有高可用性的 NFS 和 S3 共享。 如果需要将大容量的数据存储在单个命名空间中，请使用横向扩展文件系统（最大文件系统大小为 3PB）。 ■ 创建 CIFS 共享。 ■ 使用 FTP 实现横向扩展文件系统的文件共享。

功能	说明
云成为横向扩展文件系统的一层	Veritas Access 支持将云服务添加为横向扩展文件系统的存储层。您可以根据文件名模式以及上次访问和修改文件的时间，在各层之间移动数据。使用调度策略定期在各层之间移动数据。 Veritas Access 可根据自动化策略，将数据从内部层移至 Amazon S3、Amazon Glacier、Amazon Web Services (AWS)、GovCloud (US)、Azure、Google 云、Alibaba、Veritas Access S3、IBM Cloud Object Storage 和与 S3 兼容的任何存储提供商。此外，您还可以检索 Amazon Glacier 中的归档数据。
SmartIO	对于在 Veritas Access 文件系统上运行的应用程序，Veritas Access 支持在固态硬盘 (SSD) 上读取和写回缓存。
SmartTier	Veritas Access 内置的 SmartTier 功能可将数据移动到成本较低的存储中，从而降低存储成本。此外，Veritas Access 存储分层也有利于在不同的驱动器体系结构和内部部署环境之间移动数据。
快照	Veritas Access 支持通过快照从数据损坏中恢复。如果文件或整个文件系统已删除或已损坏，则可通过最新的未损坏快照进行替换。
重复数据删除	您可以在文件系统中定期运行后处理重复数据删除，此操作无需任何持续成本即可消除重复数据。
压缩	您可以在保留文件可访问性的情况下，对应用程序透明地执行压缩，以通过压缩文件来减少所用空间。压缩文件与未压缩文件的外观和操作行为几乎完全相同：压缩文件的名称不变，并且可以像未压缩文件一样读取和写入。
纠删码	对于 NFS 用例，使用 *EC log* 选项配置了纠删码。
IP 负载平衡	使用 IP 负载平衡，对于在主动-主动群集中运行的服务，可以让单个虚拟 IP 充当负载平衡器 IP 来将传入的请求分发到 Veritas Access 群集中的不同节点。
适用于 RHEL 7.x 的“Veritas Access 即 iSCSI 目标”	可以配置“Veritas Access 即 iSCSI 目标”，以便为块存储提供服务。在 Veritas Access 群集中，iSCSI 目标即服务以主动-主动模式托管。
NetBackup 集成	内置 NetBackup 客户端，用于将文件系统备份到 NetBackup 主服务器或媒体服务器。备份数据后，存储管理员可以从 Veritas Access 中删除不需要的数据，释放昂贵的主存储以保存更多数据。

功能	说明
OpenDedup 集成	与 OpenDedup 集成在一起，对数据进行重复数据删除并将其保存到内部或云存储中，以便长期保留数据。 有关详细信息，请参见《Veritas Access NetBackup 解决方案指南》。
OpenStack 插件	与 OpenStack 集成： ■ 通过 OpenStack Cinder 集成，OpenStack 可以使用 Veritas Access 托管的存储。 ■ 通过 OpenStack Manila 集成，您可以与 OpenStack Manila 上的虚拟机共享 Veritas Access 文件系统。
配额	支持设置文件系统配额、用户配额和硬配额。
复制	通过 IP 网络定期复制数据。 有关详细信息，请参见 `episodic(1)` 手册页。 通过 IP 网络同步复制数据 有关详细信息，请参见 `continuous(1)` 手册页。
支持 LDAP、NIS 和 AD	Veritas Access 使用轻型目录访问协议 (LDAP) 进行用户身份验证。
分区目录	由于支持分区目录，目录条目会重新分配到各种哈希目录中。这些哈希目录不会显示在用户或操作系统的命名空间视图中。每当执行新的创建、删除或查找操作时，此功能会查找相应的哈希目录，并在该目录中执行操作。这样就可以畅通无阻地访问父级目录索引节点及其他哈希目录，从而大幅提高文件系统的性能。 默认情况下，不会启用此功能。要启用此功能，请参见 `storage_fs`(1) 手册页。
独立的存储池	使您能够创建具有独立配置的隔离存储池。即使主存储池中的所有配置磁盘都发生故障，隔离存储池也可以防止其丢失相关元数据。
性能和优化	可对以下工作量执行基于工作量的优化： ■ 媒体服务器 - 流媒体代表新一代的富 Internet 内容。近年来，随着视频制作、压缩、缓存、流及其他内容传送技术的发展，音频和视频已经作为富媒体融入到互联网中。您可以使用 Veritas Access 存储富媒体、视频、影片、音频、音乐和照片。 ■ 虚拟机 支持 ■ 其他工作量

2

Veritas Access 授权许可

本章节包括下列主题：

关于 Veritas Access 产品授权许可

在此版本中，Veritas 引入了适用于 Veritas Access 的每核心 TB 授权许可模式。此版本也支持早期版本的每核心和每 TB 授权许可模式。

每核心 TB 授权许可模式基于每核心容量和期限。现在，您可以根据您的原始容量要求对 Veritas Access 进行授权许可。这是通过软件进行管理的。

根据容量与核心的比率，提供了三种类型的基于容量的许可证。每个许可证都有分配的存储容量，其范围为 2001 TB - 无限制。

- 高级
- 标准
- 基本

基于时间的许可证类别包括以下许可证：

- 永久：有效期无限制的许可证。
- 订购：在订购期限内有效的许可证，需要不时进行续订。通常情况下，订购期限可为 1 年、2 年或 3 年等。
- 试用软件：有效期为 60 天的许可证。

Veritas 会根据您在群集中的当前系统配置建议最适合您需求的层。新计量和建议的层基于容量利用率与核心的比率。容量利用率是指利用的原始容量，而核心是指群集中存在的物理核心数。GUI 中的 **Recommended Tier** 中也提供此信息。

表 2-1 授权许可方法

分层模式	每核心 TB 计量容量	容量层范围	基于时间的授权许可
高级	TB 与核心的比率 <= 4 TB/核心	2001 TB - 无限制	订购 - 1 年、2 年和 3 年 永久 - 对某个产品版本无限制 试用软件 - 60 天
标准	TB 与核心的比率 4 TB/核心 - 25 TB/核心	2001 TB - 无限制	订购 - 1 年、2 年和 3 年 永久 - 对某个产品版本无限制
基本	TB 与核心的比率 > 25 TB/核心	2001 TB - 无限制	订购 - 1 年、2 年和 3 年 永久 - 对某个产品版本无限制

您可以从 Access External Product 页面下载 Veritas Access 进行评估。

试用软件采用高级层授权许可模式，存储容量范围为 2001 TB - 无限制。您可以从试用软件升级到任何有效的每核心许可证。如果您有采用每核心或每 TB 授权许可的 Veritas Access 7.3.1，并升级到 Veritas Access 7.4，您可以继续使用 7.3.1 每核心许可证或 7.3.1 每 TB 许可证。

注意：

- 必须在安装产品期间提供有效的许可证。如果未提供有效的许可证，则会安装 60 天期限的试用软件许可证。
- 如果超出许可的存储容量，产品使用不会受到影响。但是，Veritas 建议，在此类情况下，您必须购买或续订许可证以增加容量。
- 如果您未能在到期日期之前购买或续订许可证，将提供 60 天的宽限期，且产品使用不受任何影响。
- 如果您未能在宽限期之后购买或续订许可证，则重新启动系统或重新启动服务（如 CIFS、S3、NFS 和 FTP）后，服务将无法启动。
- Veritas 保留通过审核确保授权和合规的权利。
- 如果在对此产品进行授权许可时遇到问题，请访问 Veritas 授权许可支持网站。https://www.veritas.com/licensing/process

表 2-2 Veritas Access 授权许可功能性强制措施

强制执行	操作
有效期内	无
宽限期内	持续性的消息（仅在 GUI 中）
宽限期后	重新启动节点之前，您可以停止 NFS、CIFS、FTP 和 S3 服务，但无法重新启动这些服务（即使尚未重新启动节点）。 重新启动节点之后，NFS、CIFS、FTP 和 S3 服务在重新启动的节点上不会联机。

如果使用 GUI 添加 Veritas Access 许可证：

- 如果许可证已过期，则在重新启动节点后，NFS、CIFS、FTP 和 S3 服务将在该节点上停止。如果此服务在群集中的任意位置运行，则其状态将显示为联机，即使此服务在此节点上处于脱机状态也是如此。分别检查每个节点上的警报，查看服务在本地处于联机还是脱机状态。
- 系统提供了用于启动、停止 NFS、CIFS 和 S3 服务及检查其状态的选项。您无法启动、停止 FTP 服务或检查其状态。
- 您只能提供本地系统中的许可证文件，GUI 不支持 `scp` 路径。

如果使用 CLISH 添加 Veritas Access 许可证：

- 如果许可证已过期，则在重新启动节点后，NFS、CIFS、FTP 和 S3 服务将在该节点上停止。可以使用 `support services show` 命令来显示此服务在每个节点上的状态。
- 系统提供了用于启动、停止 NFS、CIFS、FTP 和 S3 服务及检查其状态的选项。
- 您可以使用 `license add` 命令添加许可证。`license add` 命令还为 `scp` 路径提供支持。
- `license list` 和 `license list details` 命令提供群集中每个节点上安装的许可证的详细信息。

3

系统要求

本章节包括下列主题：

重要版本信息

在安装产品之前，请阅读《Veritas Access 版本说明》以了解最新信息。

硬件兼容性列表中包含所支持硬件的相关信息，该列表会定期更新。您可以使用硬件兼容性列表中认证和提及的任何商用硬件。

有关所支持硬件的最新信息，请参见位于以下位置的兼容性列表：

https://sort.veritas.com/documents/doc_details/isa/7.4/Linux/CompatibilityLists/

有关此版本的重要更新，请查看 Veritas 技术支持网站上最新发布的新闻和技术说明：

https://www.veritas.com/support/en_US/article.100042732

系统要求

表 3-1 列出了运行 Veritas Access 系统软件的每个节点的系统要求。

表 3-1 Veritas Access 系统要求

最低配置	建议配置
每个 Veritas Access 节点均使用基于 Intel 的 64 位服务器架构，且此架构与 RHEL 7 Update 3、RHEL 7 Update 4 或者 AMD64 和 Intel EMT 兼容。不支持 Itanium。	两个节点配备 2.0 GHz 或更高频率的双核或四核处理器，以实现最佳性能。
32 GB 具备纠错技术的内存 (ECC RAM)	建议值取决于预期工作量。
一个内部驱动器，大小为 RAM + 60 GB	双引导驱动器，每个驱动器的大小为 RAM + 60 GB 或更大容量。在基于FSS的环境中，建议使用其他内部驱动器 (SSD + HDD)。
四个 1 G 以太网接口（两个以太网接口用于公用网络，另外两个用于专用网络。）	建议使用四个 10 G 以太网接口（两个以太网接口用于公用网络，另外两个用于专用网络。）。
一个光纤通道主机总线适配器 (HBA)	如果您使用的是需要通过光纤通道协议映射的共享 LUN，建议使用两个光纤通道主机总线适配器(HBA)来实现高可用性 (HA)。如果环境中仅包含 DAS 或 iSCSI 磁盘，则 HBA 要求是可选的。
内部/外部 USB DVD-ROM DVD 驱动器	不适用
冗余电源	建议配备，但非必需。
SmartIO 缓存功能	如果要使用 SmartIO 缓存功能，建议使用基于 PCI 的 SSD 卡。
至少需要 1 台服务器	不适用

表 3-2 列出了运行 Veritas Access 系统软件的操作系统 (OS) 分区要求。

表 3-2 Veritas Access 的操作系统分区要求

分区	推荐大小（最小值）	详细信息
/opt	100 GB	用于存储 Veritas Access 软件、日志和核心转储。
/usr	3 GB	用于安装相关的操作系统 RPM。
swap	8 GB	用于在物理内存已满时交换空间。

分区	推荐大小（最小值）	详细信息
/	30 GB	用于操作系统。

注意：上述操作系统分区要求仅适用于 Veritas Access，操作系统特定的软件包需要额外空间，这需要根据要求进行计算和分配。

Linux 要求

Veritas Access 不支持 Veritas Access 在其上运行的操作系统。Veritas Access 的每个版本均有严格的操作系统版本要求。

Veritas Access 7.4 版本要求并支持以下 Red Hat Enterprise Linux (RHEL) 或 Oracle Linux (OL) 操作系统版本：

- Red Hat Enterprise Linux (RHEL)
  - RHEL 7 Update 3 和 4
- Oracle Linux（仅在 RHEL 兼容模式下）
  - OL 7 Update 3 和 4

在 Veritas Access 安装期间，必须满足最低操作系统要求。也可以请求提供 Veritas Access 7.4 的 Kickstart 文件，协助合作伙伴满足操作系统安装要求。无需从 Veritas 获得认证，即可安装包括安全漏洞修补程序在内的操作系统修补程序。但是，如果未得到 Veritas 的特别批准，不得对操作系统的内核 RPM 进行修补。

Red Hat Enterprise Linux (RHEL) 操作系统更新的认证可能需要新的 Veritas Access 次要版本。未经 Veritas 事先许可，不能安装 RHEL 操作系统更新。

Veritas Access 可以安装在运行以下操作系统的计算机上：

要求	版本	版本
Red Hat Enterprise Linux 版本	RHEL 7 Update 3	RHEL 7 Update 4
Oracle Linux	OL 7 Update 3	OL 7 Update 4
内核版本	3.10.0-514.el7	3.10.0-693.el7
必需的 RPM	请参见第 24 页的“RHEL 7.3 所需的操作系统 RPM”。 请参见第 18 页的“OL 7.3 所需的操作系统 RPM”。	请参见第 26 页的“RHEL 7.4 所需的操作系统 RPM”。 请参见第 21 页的“OL 7.4 所需的操作系统 RPM”。

操作系统 RPM 安装要求和操作系统修补

Veritas 已将安装 Veritas Access 之前所需的操作系统 RPM 分成四组：

类别 1

- 此组 RPM 是只能使用准确预定义的 RPM 版本安装的内核 RPM。
- RHEL 7.3 和 RHEL 7.4 所需的 RPM 版本不同。
- OL 7.3 和 OL 7.4 所需的 RPM 版本不同。
- 如果未得到 Veritas 的特别批准，不得修补此类别中的 RPM。
- 请参见第 18 页的“需要使用准确预定义的 RPM 版本安装的内核 RPM”。
- 请参见第 18 页的“需要使用预定义的确切 RPM 版本安装的 OL 内核 RPM”。

类别 2

- 此组 RPM 包括必须使用最低预定义的 RPM 版本安装的 OS 库和 OS 软件包。
- RHEL 7.3 和 RHEL 7.4 所需的 RPM 版本不同。
- OL 7.3 和 OL 7.4 所需的 RPM 版本不同。
- 可以使用 Red Hat 官方修补程序对此类别中的 RPM 进行修补。
- 对这些 RPM 的修补无需得到 Veritas 的批准或认证。
- 请参见第 18 页的“OL 7.3 所需的操作系统 RPM”。
- 请参见第 21 页的“OL 7.4 所需的操作系统 RPM”。
- 请参见第 24 页的“RHEL 7.3 所需的操作系统 RPM”。
- 请参见第 26 页的“RHEL 7.4 所需的操作系统 RPM”。

类别 3

- 此组 RPM 是类别 2 RPM 所需的依赖性 RPM，其安装由 Red Hat 强制执行。
- Veritas Access 不需要安装这些 RPM 的任何特定版本。
- 这些 RPM 的版本由 Red Hat 确定。
- 可以使用 Red Hat 官方修补程序对此类别中的 RPM 进行修补。
- 对这些 RPM 的修补无需得到 Veritas 的批准或认证。
- Veritas 不会将这些 RPM 记录为 Veritas Access 必需的 RPM。

类别 4

- 此组 RPM 是 Veritas Access ISO 中附带提供的第三方 RPM。
- 这些 RPM 不是操作系统 RPM。它包括 Samba、Ganesha 以及其他第三方产品。

- 如果未得到 Veritas 的特别批准，不得修补此类别中的 RPM。
- 由于它们包括在 Veritas Access ISO 中，因此 Veritas 将会安装这些 RPM。

需要使用准确预定义的 RPM 版本安装的内核 RPM

安装 Red Hat Enterprise Linux 操作系统之后，请安装以下 RPM，然后重新启动系统。使用指定的链接从 Red Hat 站点下载 RPM。这些链接需要 Red Hat 注册 ID（用户名和密码）。

RHEL 7 Update 3 内核软件包：

以下 RPM 包括在 **os_rpms** 目录下的 DVD 映像中，并使用 CPI 安装进行安装。

- kernel-debuginfo-3.10.0-514.el7.x86_64.rpm
- kernel-headers-3.10.0-514.el7.x86_64.rpm
- kernel-debuginfo-common-x86_64-3.10.0-514.el7.x86_64.rpm

RHEL 7 Update 4 内核软件包：

以下 RPM 包括在 **os_rpms** 目录下的 DVD 映像中，并使用 CPI 安装进行安装。

- kernel-headers-3.10.0-693.el7.x86_64.rpm

需要使用预定义的确切 RPM 版本安装的 OL 内核 RPM

OL 环境应当是下列仅包含 Red Hat 兼容内核的环境之一：

- OL 7.3
- OL 7.4

注意：对于 OL 7.x 操作系统，不支持 `uek` 内核。

示例：

```
[root@oel_01 ~]# cat /etc/redhat-release
Red Hat Enterprise Linux Server release 7.4 (Maipo)
[root@oel_01 ~]# cat /etc/oracle-release
Oracle Linux Server release 7.4
[root@oel_01 ~]# uname -r
3.10.0-693.el7.x86_64
```

OL 7.3 所需的操作系统 RPM

以下列表中指定的 RPM 版本号是这些操作系统 RPM 所需的最低版本号。

Required OS lib rpms for OL 7.3:

bc-1.06.95-13.el7.x86_64	coreutils-8.22-18.el7.x86_64
ed-1.9-4.el7.x86_64	findutils-4.5.11-5.el7.x86_64
glibc-2.17-157.el7.x86_64	libacl-2.2.51-12.el7.x86_64
libgcc-4.8.5-11.el7.x86_64	libstdc++-4.8.5-11.el7.x86_64
openssl-libs-1.0.2k-12.el7.x86_64	perl-Exporter-5.68-3.el7.noarch
perl-Socket-2.010-4.el7.x86_64	policycoreutils-2.5-8.el7.x86_64
python-2.7.5-48.el7.x86_64	python-libs-2.7.5-48.el7.x86_64
zlib-1.2.7-17.el7.x86_64	

Required OS packages for OL 7.3:

apr-devel 1.4.8-3	apr-util-devel 1.5.2-6
arptables 0.0.4-8	at 3.1.13-22
autogen-libopts 5.18-5	avahi-libs 0.6.31-17
bash 4.2.46-20	binutils 2.25.1-22
cairo 1.14.2-1	coreutils 8.22-18
cups-libs 1.6.3-26	ethtool 4.5-3
fuse 2.9.2-7	fuse-devel 2.9.2-7
fuse-libs 2.9.2-7	glibc-common 2.17.157
glibc-devel.x86_64 2.17.157	glibc-headers 2.17.157
glibc-utils 2.17.157	glibc.i686 2.17.157
glibc.x86_64 2.17.157	httpd 2.4.6-45
httpd-devel 2.4.6-45	httpd-manual 2.4.6-45
httpd-tools 2.4.6-45	infiniband-diags 1.6.5-3
initscripts 9.49.37-1	iproute 3.10.0-74
ipvsadm 1.27-7	iscsi-initiator-utils 6.2.0.873-35
jansson 2.10-1	kernel-debuginfo =3.10.0-514.el7

kernel-debuginfo-common-x86_64 =3.10.0-514.el7

kernel-headers =3.10.0-514.el7

kmod 20-9

krb5-devel 1.14.1-26

krb5-libs 1.14.1-26

krb5-workstation 1.15.1-8

ksh 20120801-26.el7

libibumad 1.3.10.2-1

libibverbs-utils 1.2.1-1

libjpeg-turbo 1.2.90-5

libpcap 1.5.3-8

libtirpc 0.2.4-0.8

libyaml 0.1.4-11

lshw B.02.17-12

lsof 4.87-4

lsscsi 0.27-4

memcached 1.4.15-10

mlocate 0.26-6

mod_ssl 2.4.6-45

mod_wsgi 3.4-12

net-snmp 5.7.2-24

net-snmp-utils 5.7.2-24

net-tools 2.0-0.17

nfs-utils 1.3.0-0.33

nmap-ncat 6.40-7

nscd 2.17-157

nss-pam-ldapd 0.8.13-8

ntp 4.2.6p5-25

ntpdate 4.2.6p5-25

openldap 2.4.40-13

openldap-clients 2.4.40-13

opensm 3.3.19-1

opensm-libs 1.0.2k-12.el7

openssl 1.0.2k-12.el7

openssl-devel 1.0.2k-12.el7

openssl-libs 1.0.2k-12.el7

pango 1.36.8-2

perl 5.16.3

perl-Convert-ASN1 0.26-4

perl-JSON 2.59-2

perl-LDAP 0.56-5

perl-Net-Telnet 3.03-19.el7

perl-XML-Parser 2.41-10

psmisc 22.20-11

python-backports 1.0-8
python-backports-ssl_match_hostname 3.4.0.2-4
python-chardet 2.2.1-1
python-memcached 1.59-1.noarch
python-paramiko 1.7.7.1-3
python-requests 2.6.0-1
python-setuptools 0.9.8-4
python-six 1.9.0-2
python-urllib3 1.10.2-2
PyYAML 3.10-11
rdma 7.3_4.7_rc2-5
rrdtool 1.4.8-9
rsh 0.17-76
sg3_utils 1.37-9
sg3_utils-libs 1.37-9
strace 4.8-11
sysstat 10.1.5-11
targetcli 2.1.fb41-3
telnet 0.17-60
traceroute 2.0.22-2
tzdata-java
unzip 6.0-16
vim-enhanced 7.4.160
vsftpd 3.0.2-21
wireshark 1.10.14-10
yp-tools 2.14-3
ypbind 1.37.1-7
zip 3.0-11

OL 7.4 所需的操作系统 RPM

以下列表中指定的 RPM 版本号是这些操作系统 RPM 所需的最低版本号。

Required OS packages for OL 7.4:
PyYAML 3.10-11
apr-devel 1.4.8-3
apr-util-devel 1.5.2-6
arptables 0.0.4-8
at 3.1.13-22
autogen-libopts 5.18-5
avahi-libs 0.6.31-17
bash 4.2.46-28
binutils 2.25.1-31
cairo 1.14.8-2

coreutils 8.22-18

cups-libs 1.6.3-29

ethtool 4.8-1

fuse 2.9.2-8

fuse-devel 2.9.2-8

fuse-libs 2.9.2-8

glibc-common 2.17.196

glibc-devel.x86_64 2.17.196

glibc-headers 2.17.196

glibc-utils 2.17.196

glibc.i686 2.17.196

glibc.x86_64 2.17.196

httpd 2.4.6-67

httpd-devel 2.4.6-67

httpd-manual 2.4.6-67

httpd-tools 2.4.6-67

infiniband-diags 1.6.7-1

initscripts 9.49.39-1

iproute 3.10.0-87

ipvsadm 1.27-7

iscsi-initiator-utils 6.2.0.874-4

jansson 2.10-1

kmod 20-15

krb5-devel 1.15.1-8

krb5-libs 1.15.1-8

krb5-workstation 1.15.1-8

libibumad 13-7

libibverbs-utils 13-7

libjpeg-turbo 1.2.90-5

libpcap 1.5.3-9

libtirpc 0.2.4-0.10

libyaml 0.1.4-11

lshw B.02.18-7

lsof 4.87-4

lsscsi 0.27-6

memcached 1.4.15-10

mlocate 0.26-6

mod_ssl 2.4.6-67

mod_wsgi 3.4-12

net-snmp 5.7.2-28

net-snmp-utils 5.7.2-28

net-tools 2.0-0.22

nfs-utils 1.3.0-0.48

nmap-ncat 6.40-7

nscd 2.17-196

nss-pam-ldapd 0.8.13-8

ntp 4.2.6p5-25

ntpdate 4.2.6p5-25

openldap 2.4.44-5

openldap-clients 2.4.44-5

opensm 3.3.19-1

opensm-libs 3.3.19-1

openssl 1.0.2k-12.el7

openssl-devel 1.0.2k-12.el7

openssl-libs 1.0.2k-12.el7

pango 1.40.4-1

perl 5.16.3

perl-Convert-ASN1 0.26-4

perl-JSON 2.59-2

perl-LDAP 0.56-5

perl-Net-Telnet 3.03-19.el7

perl-XML-Parser 2.41-10

psmisc 22.20-15

python-backports 1.0-8

python-backports-ssl_match_hostname 3.4.0.2-4

python-chardet 2.2.1-1

python-memcached 1.59-1.noarch

python-paramiko 1.7.7.1-3

python-requests 2.6.0-1

python-setuptools 0.9.8-7

python-six 1.9.0-2

python-urllib3 1.10.2-3

rrdtool 1.4.8-9

rsh 0.17-76

sg3_utils 1.37-12

sg3_utils-libs 1.37-12

strace 4.12-4

sysstat 10.1.5-12

targetcli 2.1.fb46-1

telnet 0.17-64

traceroute 2.0.22-2

tzdata-java

unzip 6.0-16

vim-enhanced 7.4.160

vsftpd 3.0.2-22

wireshark 1.10.14-14

yp-tools 2.14-5

ypbind 1.37.1-9

zip 3.0-11

RHEL 7.3 所需的操作系统 RPM

以下列表中指定的 RPM 版本号是此操作系统 RPM 所需的最低版本号。

Required OS lib rpms for RHEL 7.3:

bc-1.06.95-13.el7.x86_64	coreutils-8.22-18.el7.x86_64
ed-1.9-4.el7.x86_64	findutils-4.5.11-5.el7.x86_64
glibc-2.17-157.el7.x86_64	libacl-2.2.51-12.el7.x86_64
libgcc-4.8.5-11.el7.x86_64	libstdc++-4.8.5-11.el7.x86_64
openssl-libs-1.0.2k-12.el7.x86_64	perl-Exporter-5.68-3.el7.noarch
perl-Socket-2.010-4.el7.x86_64	policycoreutils-2.5-8.el7.x86_64
python-2.7.5-48.el7.x86_64	python-libs-2.7.5-48.el7.x86_64
zlib-1.2.7-17.el7.x86_64	

Required OS packages for RHEL 7.3:

apr-devel 1.4.8-3	apr-util-devel 1.5.2-6
arptables 0.0.4-8	at 3.1.13-22
autogen-libopts 5.18-5	avahi-libs 0.6.31-17
bash 4.2.46-20	binutils 2.25.1-22
cairo 1.14.2-1	coreutils 8.22-18
cups-libs 1.6.3-26	ethtool 4.5-3
fuse 2.9.2-7	fuse-devel 2.9.2-7
fuse-libs 2.9.2-7	glibc-common 2.17.157
glibc-devel.x86_64 2.17.157	glibc-headers 2.17.157
glibc-utils 2.17.157	glibc.i686 2.17.157
glibc.x86_64 2.17.157	httpd 2.4.6-45
httpd-devel 2.4.6-45	httpd-manual 2.4.6-45
httpd-tools 2.4.6-45	infiniband-diags 1.6.5-3

initscripts 9.49.37-1

iproute 3.10.0-74

ipvsadm 1.27-7

iscsi-initiator-utils 6.2.0.873-35

jansson 2.10-1

kernel-debuginfo =3.10.0-514.el7

kernel-debuginfo-common-x86_64 =3.10.0-514.el7

kernel-headers =3.10.0-514.el7

kmod 20-9

krb5-devel 1.14.1-26

krb5-libs 1.14.1-26

krb5-workstation 1.15.1-8

ksh 20120801-26.el7

libibumad 1.3.10.2-1

libibverbs-utils 1.2.1-1

libjpeg-turbo 1.2.90-5

libpcap 1.5.3-8

libtirpc 0.2.4-0.8

libyaml 0.1.4-11

lshw B.02.17-12

lsof 4.87-4

lsscsi 0.27-4

memcached 1.4.15-10

mlocate 0.26-6

mod_ssl 2.4.6-45

mod_wsgi 3.4-12

net-snmp 5.7.2-24

net-snmp-utils 5.7.2-24

net-tools 2.0-0.17

nfs-utils 1.3.0-0.33

nmap-ncat 6.40-7

nscd 2.17-157

nss-pam-ldapd 0.8.13-8

ntp 4.2.6p5-25

ntpdate 4.2.6p5-25

openldap 2.4.40-13

openldap-clients 2.4.40-13

opensm 3.3.19-1

opensm-libs 3.3.19-1

openssl 1.0.2k-12.el7

openssl-devel 1.0.2k-12.el7

openssl-libs 1.0.2k-12.el7

pango 1.36.8-2

perl 5.16.3

perl-Convert-ASN1 0.26-4

perl-JSON 2.59-2

perl-LDAP 0.56-5

perl-Net-Telnet 3.03-19.el7

perl-XML-Parser 2.41-10

psmisc 22.20-11

python-backports 1.0-8

python-backports-ssl_match_hostname 3.4.0.2-4

python-chardet 2.2.1-1

python-memcached 1.59-1.noarch

python-paramiko 1.7.7.1-3

python-requests 2.6.0-1

python-setuptools 0.9.8-4

python-six 1.9.0-2

python-urllib3 1.10.2-2

PyYAML 3.10-11

rdma 7.3_4.7_rc2-5

rrdtool 1.4.8-9

rsh 0.17-76

sg3_utils 1.37-9

sg3_utils-libs 1.37-9

strace 4.8-11

sysstat 10.1.5-11

targetcli 2.1.fb41-3

telnet 0.17-60

traceroute 2.0.22-2

tzdata-java

unzip 6.0-16

vim-enhanced 7.4.160

vsftpd 3.0.2-21

wireshark 1.10.14-10

yp-tools 2.14-3

ypbind 1.37.1-7

zip 3.0-11

RHEL 7.4 所需的操作系统 RPM

以下列表中指定的 RPM 版本号是此操作系统 RPM 所需的最低版本号。

Required OS lib rpms for RHEL 7.4:

bc-1.06.95-13.el7.x86_64	coreutils-8.22-18.el7.x86_64
ed-1.9-4.el7.x86_64	findutils-4.5.11-5.el7.x86_64
glibc-2.17-157.el7.x86_64	libacl-2.2.51-12.el7.x86_64
libgcc-4.8.5-11.el7.x86_64	libstdc++-4.8.5-11.el7.x86_64

```
openssl-libs-1.0.2k-12.el7.x86_64 perl-Exporter-5.68-3.el7.noarch
perl-Socket-2.010-4.el7.x86_64    policycoreutils-2.5-8.el7.x86_64
python-2.7.5-48.el7.x86_64        python-libs-2.7.5-48.el7.x86_64
zlib-1.2.7-17.el7.x86_64

Required OS packages for RHEL 7.4:
apr-devel 1.4.8-3                         apr-util-devel 1.5.2-6

arptables 0.0.4-8                         at 3.1.13-22

autogen-libopts 5.18-5                    avahi-libs 0.6.31-17

bash 4.2.46-28                            binutils 2.25.1-31

cairo 1.14.8-2                            coreutils 8.22-18

cups-libs 1.6.3-29                        ethtool 4.8-1

fuse 2.9.2-8                              fuse-devel 2.9.2-8

fuse-libs 2.9.2-8                         glibc-common 2.17.196

glibc-devel.x86_64 2.17.196               glibc-headers 2.17.196

glibc-utils 2.17.196                      glibc.i686 2.17.196

glibc.x86_64 2.17.196                     httpd 2.4.6-67

httpd-devel 2.4.6-67                      httpd-manual 2.4.6-67

httpd-tools 2.4.6-67                      infiniband-diags 1.6.7-1

initscripts 9.49.39-1                     iproute 3.10.0-87

ipvsadm 1.27-7                            iscsi-initiator-utils 6.2.0.874-4

jansson 2.10-1                            kmod 20-15

krb5-devel 1.15.1-8                       krb5-libs 1.15.1-8

krb5-workstation 1.15.1-8                 libibumad 13-7

libibverbs-utils 13-7                     libjpeg-turbo 1.2.90-5
```

libpcap 1.5.3-9

libtirpc 0.2.4-0.10

libyaml 0.1.4-11

lshw B.02.18-7

lsof 4.87-4

lsscsi 0.27-6

memcached 1.4.15-10

mlocate 0.26-6

mod_ssl 2.4.6-67

mod_wsgi 3.4-12

net-snmp 5.7.2-28

net-snmp-utils 5.7.2-28

net-tools 2.0-0.22

nfs-utils 1.3.0-0.48

nmap-ncat 6.40-7

nscd 2.17-196

nss-pam-ldapd 0.8.13-8

ntp 4.2.6p5-25

ntpdate 4.2.6p5-25

openldap 2.4.44-5

openldap-clients 2.4.44-5

opensm 3.3.19-1

opensm-libs 3.3.19-1

openssl 1.0.2k-12.el7

openssl-devel 1.0.2k-12.el7

openssl-libs 1.0.2k-12.el7

pango 1.40.4-1

perl 5.16.3

perl-Convert-ASN1 0.26-4

perl-JSON 2.59-2

perl-LDAP 0.56-5

perl-Net-Telnet 3.03-19.el7

perl-XML-Parser 2.41-10

psmisc 22.20-15

python-backports 1.0-8

python-backports-ssl_match_hostname 3.4.0.2-4

python-chardet 2.2.1-1

python-memcached 1.59-1.noarch

python-paramiko 1.7.7.1-3

python-requests 2.6.0-1

python-setuptools 0.9.8-7

python-six 1.9.0-2

python-urllib3 1.10.2-3

PyYAML 3.10-11

```
rrdtool 1.4.8-9                          rsh 0.17-76

sg3_utils 1.37-12                        sg3_utils-libs 1.37-12

strace 4.12-4                            sysstat 10.1.5-12

targetcli 2.1.fb46-1                     telnet 0.17-64

traceroute 2.0.22-2                      tzdata-java

unzip 6.0-16                             vim-enhanced 7.4.160

vsftpd 3.0.2-22                          wireshark 1.10.14-14

yp-tools 2.14-5                          ypbind 1.37.1-9

zip 3.0-11
```

在 VMware ESXi 环境中安装 Veritas Access 所需的软件要求

表 3-3 在 VMware ESXi 环境中安装 Veritas Access 所需的软件要求

项目	说明
操作系统 (OS)	Red Hat Enterprise Linux (RHEL) 7.3 和 7.4 Oracle Linux (OL) 7.3 和 7.4
VMware 环境	VMware ESXi 5.5、6.0（认证版本）
IP 地址	具有两个公用 NIC 的双节点群集需要 9 个 IP： ■ 4 个 IP 地址用于配置物理 IP。 ■ 4 个 IP 地址用于配置虚拟 IP。 ■ 1 个 IP 地址用于管理控制台。 ■ 1 个 IP 地址用于复制。

安装 Veritas Access 虚拟机所需的硬件要求

表 3-4 安装 Veritas Access 虚拟机所需的硬件要求

项目	说明
CPU	1 个 CPU – 64 位、双核或四核，2.0 GHz 或更高频率
RAM	■ 32 GB RAM（用于物理服务器） ■ 60 GB（或更多）RAM 内部可用的存储容量（用于引导磁盘）
网络接口卡 (NIC)	四个 NIC 卡 ■ 两个用于公用网络的 NIC 卡（最少） ■ 两个用于专用网络的 NIC 卡
光纤通道 HBA	如果要使用共享 LUN，则需要双端口光纤通道 HBA。如果环境中仅包含 DAS 磁盘，则 HBA 要求是可选的。

Management Server Web 浏览器支持

以下是 Veritas Access 支持的 Web 浏览器：

表 3-5

浏览器	版本	注释
Internet Explorer	■ IE 10 ■ IE 11	JavaScript：已启用 Cookie：已启用
Firefox	FireFox 4.x 及更高版本	JavaScript：已启用 Cookie：已启用
Google Chrome	Google Chrome 10 及更高版本	JavaScript：已启用 Cookie：已启用

受支持的 Web 浏览器的其他注意事项：

- 浏览器必须支持 JavaScript 1.2 或更高版本。
- 如果使用弹出窗口拦截程序（包括 Yahoo 工具栏或 Google 工具栏），请禁用此类程序，或将其配置为接受来自您连接的 Veritas Access 节点的弹出窗口。
- 对于 Windows Server 2003 上的 Internet Explorer 8.0，请从以下位置下载并安装修补程序：

http://support.microsoft.com/kb/938397/en-gb

- 如果无法使用 Internet Explorer 9.0 下载 gendeploy 脚本，请访问以下位置以解决此问题：
  http://support.microsoft.com/kb/2549423
- 对于 Internet Explorer，启用“高级”Internet 选项“多媒体”类别中的“在网页中播放动画”选项。
- 对于 Internet Explorer，当打开弹出窗口拦截程序时，请确保过滤级别设置为“中”或“低”。
- 对于 Internet Explorer，请确保该站点包括在受信任站点的列表之内。
- 如果无法将该站点添加到受信任站点的列表，则在“安全”设置中启用“二进制文件和脚本行为”选项。
- 必须安装版本 10 或更高版本的 Adobe Flash 插件。

支持的 NetBackup 版本

Veritas Access 支持 NetBackup 7.7.3 或更高版本。

支持的 OpenStack 版本

RHEL 7 操作系统和 OpenStack Kilo、Mitaka、Newton 或 Ocata 版本支持 OpenStack 驱动程序（Cinder 和 Manila）。

针对以下版本测试了 Cinder 和 Manila 驱动程序：

- DevStack 存储库中的 OpenStack Kilo、Mitaka、Newton 或 Ocata 版本
- OpenStack RDO

注意：Manila 驱动程序仅适用于内核 NFS，它不适用于 NFS-Ganesha。

支持的 Oracle 版本和主机操作系统

Veritas Access 可通过 Direct NFS 支持 Oracle 版本。Veritas Access Direct NFS 仅支持 NFS 协议版本 3。

Veritas Access 仅支持 Oracle 单实例。不支持 OracleRAC。

以下是 Veritas Access 支持的 Oracle 版本：

- Oracle 版本 11gR2（11.2.0.4 或更高版本）
- Oracle 12c (12.1.0.1)

以下是 Veritas Access 支持的 Oracle 主机操作系统（按重要性顺序）：

- Linux
- AIX
- Solaris
- HP-UX
- Oracle Linux

支持的 IP 版本 6 Internet 标准协议

表 3-6 介绍了 IP 版本 6 (IPv6) Internet 标准协议。

表 3-6 IPv6 Internet 标准协议

说明	示例格式
首选格式	ABCD:EF01:2345:6789:ABCD:EF01:2345:6789
压缩格式	FF01::101
混合格式	0:0:0:0:0:FFFF:129.144.52.38

网络和防火墙要求

表 3-7 显示了 Veritas Access 用于传输信息的默认端口。

表 3-7 默认的 Veritas Access 端口

端口	协议或服务	用途	被阻止后产生的影响
21	FTP	FTP 服务器侦听连接的端口。 **注意：**如果需要，用户可以配置其他端口。	FTP 功能被阻止。
22	SSH	安全访问 Veritas Access 服务器	无法访问 Veritas Access。
25	SMTP	发送 SMTP 邮件。	阻止从 Veritas Access 发送的 SMTP 邮件。

端口	协议或服务	用途	被阻止后产生的影响
53	DNS 查询	与 DNS 服务器通信	域名映射失败。
111	rpcbind	RPC portmapper 服务	RPC 服务失败。
123	NTP	与 NTP 服务器通信	整个群集的服务器时钟不同步。需要 NTP 的功能（如 DAR）不可用。
139	CIFS	CIFS 客户端与服务器通信	CIFS 客户端无法访问 Veritas Access 群集
161	SNMP	发送 SNMP 警报	无法广播 SNMP 警报。
445	CIFS	CIFS 客户端与服务器通信	CIFS 客户端无法访问 Veritas Access 群集。
514	syslog	记录程序消息	不会记录 syslog 消息。
756、757、755	statd	NFS statd 端口	NFS v3 协议无法正常运行。
2049	NFS	NFS 客户端与服务器通信	NFS 客户端无法访问 Veritas Access 群集。
3172、3173	ServerView	ServerView 端口	ServerView 无法运行。
4001	mountd	NFS 装入协议	NFS 客户端无法在 Veritas Access 群集中装入文件系统。
4045	lockd	处理锁定请求	文件锁定服务不可用。
5634	HTTPS	Management Server 连接	可能无法访问 Web GUI。
56987	复制	文件同步、Veritas Access 复制	Veritas Access 复制后台驻留程序被阻止。无法进行复制。

端口	协议或服务	用途	被阻止后产生的影响
8088	REST 服务器	REST 客户端与服务器通信	REST 客户端无法访问 Veritas Access 的 REST API。
8143	S3	Veritas Access S3 服务器的数据端口	用户将无法使用 Veritas Access 对象服务器。
8144	ObjectAccess 服务	Veritas Access S3 服务器的管理端口。	用户无法创建使用 ObjectAccess 服务所需的访问密钥或密钥。
11211	Memcached 端口	CLISH 框架	CLISH 无法正常运行，群集配置可能会损坏。
30000:40000	FTP	FTP 被动端口	FTP 被动模式失败。
14161	HTTPS	访问 Veritas Access GUI	用户无法访问 Veritas Access GUI

NetBackup 端口

NetBackup 使用 TCP/IP 连接在一个或多个 TCP/IP 端口之间进行通信。根据环境中的操作和配置类型，需要不同的端口来启用连接。NetBackup 对备份、还原和管理等操作具有不同的要求。

表 3-8 显示了 Veritas Access NetBackup 用来传输信息的一些最常见的 TCP 和 UDP 端口。有关详细信息，请参见《Veritas NetBackup 安全和加密指南》。

表 3-8 默认的 NetBackup TCP 和 UDP 端口

端口范围	协议
1556	TCP、UDP
13701-13702、13705-13706	TCP
13711、13713、13715-13717、13719	TCP
13720-13722	TCP、UDP
13723	TCP
13724	TCP、UDP

端口范围	协议
13782-13783	TCP、UDP
13785	TCP

OpenDedup 端口和禁用 iptable 规则

此用例特定于在 Veritas Access 上运行 OpenDedup。每次创建 SDFS 卷并将其装入 Veritas Access 时，它都会开始在特定端口上侦听。最初，它会从端口 6442 开始，并针对后续卷递增 + 1。

表 3-9 OpenDedup 端口

端口范围	协议或服务	用途	被阻止后产生的影响
从 6442 开始并针对后续卷递增 + 1	TCP	允许在 Veritas Access 和 OpenDedup 之间通信	Veritas Access 无法与 OpenDedup 通信

要允许与 Veritas Access 上运行的 OpenDedup 端口进行通信，请完全禁用 iptable 规则

1 使用 `df` 命令显示 SDFS 卷已装入以及它正在侦听哪个端口。

SDFS 卷已作为 LTR 脚本的一部分装入。

```
[root@ltrclust_02 ~]# df -h | tail -2
sdfs:/etc/sdfs/pool100-volume-cfg.xml:6442
11G     0   11G   0% /pool100
```

2 使用 `netstat` 命令验证端口是否已打开。

```
[root@ltrclust_02 ~]# netstat -tulpn | grep 6442
tcp        0      0 :::6442    :::*        LISTEN
3761/jsvc.exec
```

3 禁用 iptable 规则，以便允许在卷装入之后与 OpenDedup 端口通信，在卷卸载之后禁止与该端口通信。

使用以下命令可禁用 iptable 规则：

```
[root@ltrclust_02 ~]# iptables -F

[root@ltrclust_02 ~]# /etc/init.d/iptables stop

[root@ltrclust_02 ~]# iptables -L
```

使用 iptables -L 命令验证是否已禁用所有 iptable 规则。

应在所有 Veritas Access 群集节点上和装有 OpenDedup 的 NetBackup 介质服务器上运行 iptable 规则。

4 步骤 3 中禁用 iptable 规则的替代方法是，添加一个用来打开 OpenDedup 端口的 iptable 规则，以便同时使用现有的 iptable 规则。

示例：

```
[root@ltrclust_02 ~]# iptables -A INPUT -p tcp --dport 6442 -j ACCEPT
```

CIFS 协议和防火墙端口

为使 CIFS 服务在 Active Directory (AD) 域环境中正常运行，需要允许或打开以下协议和防火墙端口，以便 CIFS 服务器能够与 Active Directory 域控制器和 Windows/CIFS 客户端顺畅地通信。

必须在防火墙中允许使用 Internet 控制消息协议 (ICMP) 协议从 CIFS 服务器连接到域控制器。需要启用“允许传入回显请求”才能运行 CIFS 服务。

表 3-10 列出了其他 CIFS 端口和协议。

表 3-10 其他 CIFS 端口和协议

端口	协议	用途
53	TCP、UDP	DNS
88	TCP、UDP	Kerberos
139	TCP	DFSN、NetBIOS 会话服务、NetLog
445	TCP、UDP	SMB、CIFS、SMB2、DFSN、LSARPC、NbtSS、NetLogonR、SamR、SrvSvc
464	TCP、UDP	Kerberos 更改或设置密码

端口	协议	用途
3268	TCP	LDAP GC
4379	TCP	CIFS 中的 CTDB

表 3-11 列出了使用 SSL 的 LDAP 所需的端口。

表 3-11 使用 SSL 端口的 LDAP

端口	协议	用途
636	TCP	LDAP SSL
3269	TCP	LDAP GC SSL

最大配置限制

配置 Veritas Access 系统软件的最大配置限制如下所示：

表 3-12 最大配置限制

Veritas Access 系统软件	配置限制
文件系统大小	对于不支持云分层的非横向扩展文件系统，为 5 PB 对于支持云分层的横向扩展文件系统，为 3 PB
Veritas Access 节点数	20
支持的 LUN 数	理论上，最大磁盘数限制为操作系统所能够连接的磁盘数。不过，我们仅在数千磁盘这一量级上进行了测试。
支持的文件系统数	500
文件系统内的层数	2（主层和辅助层）

4

准备安装 Veritas Access

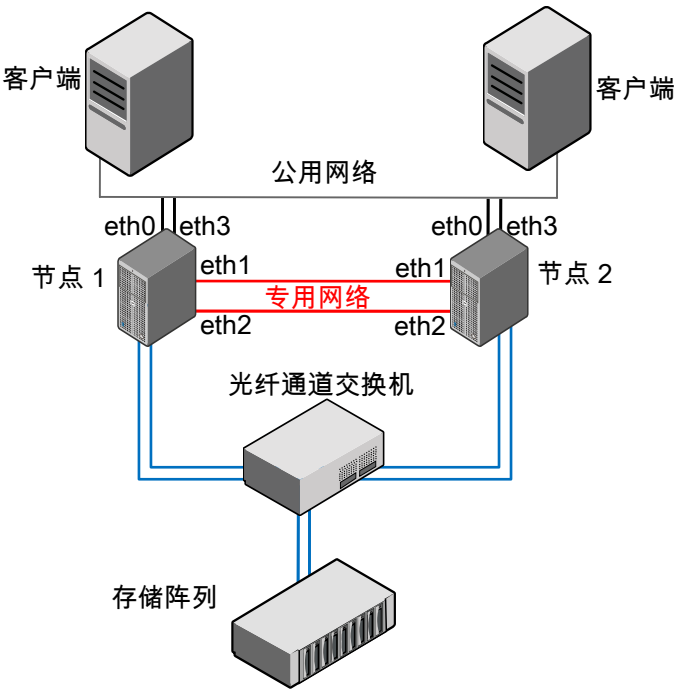
本章节包括下列主题：

安装过程概述

Veritas Access 群集是一组称为“节点”并相互连接在一起的服务器。这些节点共同构成一个统一实体，称为“群集”。

图 4-1 显示了一个 Veritas Access 群集的示例。

图 4-1 Veritas Access 群集示例概览



注意：图 4-1 中提及的 NIC 名称仅供示例使用。您需在安装期间确定各 NIC 的实际名称。

Veritas Access 软件安装概述介绍了以下几个步骤：

- 从网络管理员处收集网络信息。
- 连接网络硬件。
- 在每个节点上安装操作系统。
- 在节点上安装 Veritas Access。如果驱动节点是群集节点之一，则必须从该节点的控制台中启动安装程序。如果驱动节点不是群集的一部分，则可从驱动节点中运行安装程序，以便通过 ssh 连接安装和配置群集。
  从 Veritas Access 7.2 版本起，可从群集的任意节点中运行安装程序。
  请参见第 59 页的“在群集上安装和配置 Veritas Access 软件”。
  请参见第 56 页的“关于驱动节点”。
- 在节点上运行安装和配置以配置整个群集。安装时间可能因具体配置而异。

节点的硬件要求

下表总结了每个节点的硬件要求。

表 4-1 节点的硬件要求

项目	要求
网络接口卡 (NIC)	每个节点至少需要 4 个 NIC。 两个 NIC 连接到专用网络。 ■ 对于双节点群集，可在每个节点上交叉连接两个专用 NIC 或使用交换机。 ■ 如果群集中有两个以上节点，请确保配有专用交换机（或配有使用专用 VLAN 的公用交换机或专用交换机），且所有专用 NIC 均连接到该交换机。 将每个节点中的两个公用 NIC 连接到公用网络。每个公用 NIC 都必须可以访问该网关。
IP 地址	对于双节点群集，请确保具有 9 个可用的 IP 地址。 ■ 4 个 IP 地址用于配置物理 IP。 ■ 4 个 IP 地址用于配置虚拟 IP。 ■ 1 个 IP 地址用于配置 Operations Manager 控制台。 ■ 1 个 IP 地址用于复制（可选）。 请确保这 9 个 IP 地址与分配给目标群集节点以在安全外壳 (Secure Shell, ssh) 上安装 Veritas Access 的 IP 地址不同。

连接网络硬件

安装 Veritas Access 软件之前，必须通过为所有节点配置所需网络硬件并将以太网接口连接到专用网络和公用网络来组成群集。

要组成群集，请执行以下操作：

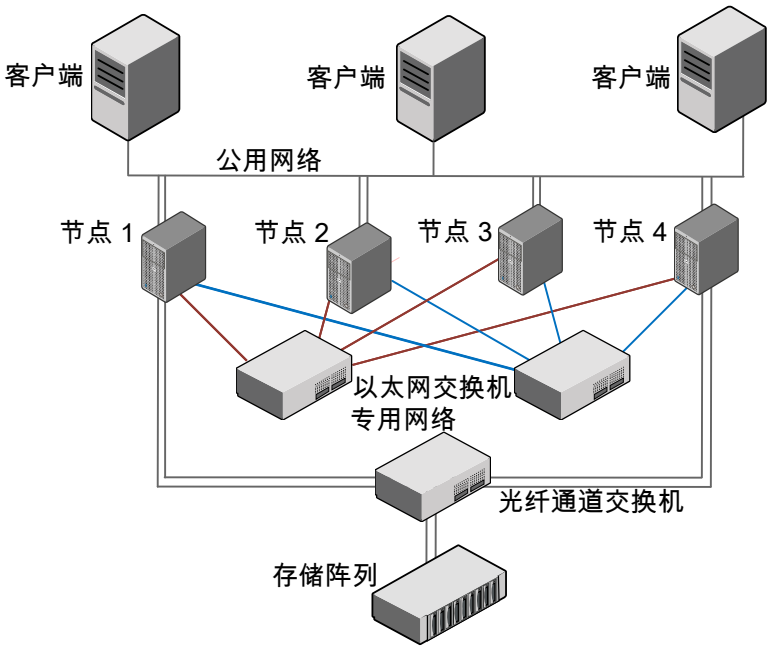
- 确定群集的首选位置。
- 确保每个节点至少具有两个冗余以太网接口（千兆以太网），以便连接到专用网络以实现群集内部控制。
- 确保每个节点至少额外具有两个以太网接口（千兆以太网），以便连接到公用网络。您可以使用主板上的嵌入式接口或附加的 (PCI) 网络适配器接口中的公用以太网接口。
- 要连接公用 NIC，请将以太网电缆的一端连接到节点背面的以太网接口。将以太网电缆的另一端连接到公司网络，以便它们能够访问网关。每个节点至少需要两个公用接口。

- 要连接专用 NIC，请使用按 NIC 名称排序的前两个可用 NIC。可用 NIC 是指未连接到公用网络或未从该节点中排除的 NIC。
  例如，如果 NIC 为 eth1、eth2、eth3 和 eth4，且所有 NIC 均未连接到公用网络或未被排除，则 eth1 和 eth2 将用作专用 NIC。
  将以太网电缆的一端连接到节点背面的以太网接口 1 和 2。对于双节点群集，将以太网电缆的另一端连接到第二个节点上的相应以太网接口。对于 2 个节点以上的群集，将以太网电缆的另一端连接到专用交换机或 VLAN。
- 请您的网络管理员提供安装 Veritas Access 时要使用的 IP 地址。所需的 IP 地址数取决于群集中的节点数和网络接口卡数。
  每个节点的每个公共接口至少需要一个 IP 地址。对于虚拟 IP 地址，如果在安装期间为每个 NIC 的虚拟 IP 地址数输入 0，则可以稍后在 CLISH 中配置虚拟 IP 地址。
  Veritas Access 支持 Internet 协议版本 4 (IPv4) 或 Internet 协议版本 6 (IPv6)，但二者不能混用。

物理 IP 地址	一个与特定以太网接口地址关联且无法自动故障转移的 IP 地址。
虚拟 IP 地址 (VIP)	一个与特定以太网接口关联的 IP 地址 (VIP)，可通过 Veritas Access 软件故障转移到其他节点上的其他接口。
控制台 IP 地址	一个用来与 Veritas Access 群集管理控制台进行通信的专用虚拟 IP 地址。此虚拟 IP 地址将分配给主节点。如果主节点发生故障，则 Veritas Access 软件会自动从群集中选择新的主节点，并将控制台 IP 地址故障转移到新的主节点中。

图 4-2 显示了一个 4 节点群集示意图。

图 4-2 专用网络配置：4 节点群集



注意：在同一个 IPv4 网络上，不能配置两个或更多 Veritas Access 专用网络。

关于获取 IP 地址

在 Veritas Access 安装过程中，可以为 1 至 20 个节点配置 IP 地址。默认值为两个节点。

注意：您可以配置 IPv4 地址或 IPv6 地址（具体取决于安装 Veritas Access 时使用的地址），但不能同时使用二者。请勿将以 172.16.X.X 开头的 IP 地址用作物理 IP 地址或虚拟 IP 地址，因为此 IP 地址范围供专用网络使用。

您需要从负责群集所在设备的网络管理员处获取物理 IP 地址、虚拟 IP 地址以及所选公用网络的网络掩码。所有（物理和虚拟）IP 地址必须属于同一个子网，并使用相同的网络掩码作为节点的访问 IP。

根据设计，安装程序不支持在安装期间使用本地主机 (127.0.0.1) IP 地址。

注意：网络掩码用于 IPv4 地址。前缀用于 IPv6 地址。IPv6 地址前缀的可接受范围是 0-128（整数）。

从网络管理员获取的信息用于配置以下内容：

- 物理 IP 地址
- 虚拟 IP 地址
- 控制台 IP 地址
- 复制 IP 地址（可选）
- 默认网关的 IP 地址
- 域名系统 (DNS) 服务器的 IP 地址
- DNS 域名
- 网络时间协议 (NTP) 服务器的 IP 地址（可选）
- Veritas NetBackup 的虚拟 IP 地址（可选）

关于计算 IP 地址要求

本节提供了如何计算双节点群集 IP 地址的示例。在此示例中，群集中的所有节点都具有相同的硬件配置。因此，群集中所有节点的网络接口卡 (NIC) 数量相同。

- 两个专用 NIC 和两个公用 NIC 应连接到相应的网络。
- 一个公用 IP 地址应分配到一个公用接口，以通过 SSH 进行安装。专用接口的 IP 地址不应位于相同网段中。
- 必须将公用 IP 地址写入到网络配置文件 `/etc/sysconfig/network-scripts/ifcfg-ethX` 以使其永久保存。

表 4-2 标准配置所需 IP 的示例计算

IP 的数量	项目
2	群集中的节点数
4	每个节点上的接口数
2	每个节点所需的专用接口数

选择每个节点上的两个专用接口后，剩余的所有接口都将用作公用接口。

计算每个节点的公用接口数

- 节点上的接口总数减去节点上所需的专用接口数，等于节点上剩余的公用接口数。

```
Total number of interfaces (4)
- Number of private interfaces (2)
= Number of public interfaces

4 - 2 = 2
```

计算群集的物理和虚拟 IP 地址

1. 群集安装所需的物理 IP 地址总数等于群集中的节点数乘以每个节点上的公用接口数：

```
Total number of nodes (2)
x Number of public interfaces per node (2)
= Total number of physical IP addresses

= 2 x 2 = 4
```

2. 群集中的节点数乘以每个节点上的公用接口数等于群集安装所需的虚拟 IP 地址总数：

```
Total number of nodes (2)
x Number of public interfaces per node (2)
= Total number of virtual IP addresses

= 2 x 2 = 4
```

3. Veritas Access Operations Manager 所需的 IP 地址数等于一 (1)。

计算群集的公用 IP 地址总数

- 群集的物理 IP 地址数加上群集的虚拟 IP 地址数，再加上 Operations Manager 的 IP 地址数，等于群集所需的公用 IP 地址总数。

```
Total number of physical IP addresses/cluster (4)
+ Total number of virtual IP addresses/cluster (4)
+ Number of IP addresses for the Management Console (1)
= Total number of public IP addresses required for the cluster

= 4 + 4 + 1 = 9
```

请求并指定 IP 地址

1 从网络管理员处请求需要的公用 IP 地址。

2 例如，如果网络管理员提供的 IP 地址介于 10.209.105.120 至 10.209.105.128 之间，可通过以下方式分配资源：

```
Start of Physical IP address: 10.209.105.120
Start of Virtual IP address: 10.209.105.124
Management Console IP:"10.209.105.128"
```

这为您提供了四个物理 IP 地址（10.209.105.120 到 10.209.105.123）、四个虚拟 IP 地址（10.209.105.124 到 10.209.105.127）和一个 Operations Manager 的 IP 地址 (10.209.105.128)。

10.209.105.120 和 10.209.105.121 分配给 pubeth0 和 pubeth1 作为第一个节点上的物理 IP 地址。

10.209.105.122 和 10.209.105.123 分配给 pubeth0 和 pubeth1 作为第二个节点上的物理 IP 地址。

10.209.105.124 到 10.209.105.127 分配给 pubeth0 和 pubeth1 作为两个节点上的虚拟 IP 地址。

减少安装时所需的 IP 地址数

可以通过不配置任何虚拟 IP 地址来减少安装时所需的 IP 地址数。在 Veritas Access 安装期间，为每个 NIC 的虚拟 IP 地址数输入 0。

安装时不需要虚拟 IP 地址。可以稍后在 CLISH 中使用 Network> ip addr add 命令配置虚拟 IP 地址。

有关添加 NIC 的详细信息，请参见 network(1) 手册页。

在安装时，每个节点的每个公共接口至少需要一个 IP 地址。

表 4-3 对于双节点群集（每个节点配有两个公用 NIC），安装时所需 IP 地址的配置示例

IP 地址数	项目
4	物理 IP 地址的数量。 四个 IP 地址包括原始物理 IP 地址。
1	一个 IP 地址用于管理控制台。

关于检查存储配置

警告：在完成安装操作系统之前，请勿连接光纤通道HBA。如果本地磁盘损坏，则连接光纤通道 HBA 时，会阻止在本地磁盘上安装操作系统。由于扫描磁盘，因此在本地磁盘上安装软件需要较长时间。

Veritas Access 支持灵活存储共享 (FSS)，它允许用户在 Veritas Access 设备上配置和管理直接连接的存储。

安装操作系统之后，请检查存储配置。如果不想使用FSS，请确保每个节点符合以下条件：

- 一个或两个连接到存储区域网络 (SAN) 交换机的光纤通道主机总线适配器 (HBA)。
  建议配备两个光纤通道HBA，最低需要一个。只有一个光纤通道HBA时，也可支持除高可用性以外的所有光纤通道操作。
- 一个内部引导磁盘。确保该磁盘在安装 Veritas Access 软件之前已配备就绪。

如果要使用 FSS，请确保每个节点的内部引导磁盘旁边至少额外连接两个本地磁盘。

5

在 VMware ESXi 中部署用于安装 Veritas Access 的虚拟机

本章节包括下列主题：

在 VMware ESXi 中设置网络

在开始之前，安装 ESXi 服务器。可以使用 vSphere Client，在 ESXi 主机上部署第一个虚拟机。

在 VMware ESXi 中设置网络

1 启动 vSphere Client 并键入主机的登录详细信息。

在 **IP address / Hostname** 文本框中，输入 **ESXi server IP/hostname**。

在 **User name** 文本框中，键入 **root**。

在 **Password** 文本框中，键入 ***my_esxi_password***。

2 设置 Veritas Access 的网络要求。

3 要设置公用网络虚拟交换机，请执行以下操作：

- 在 ESXi 主机的 **Configuration** 选项卡中，导航到 **Hardware > Networking**。
- 单击右上角的 **Add Networking**。

- 针对连接类型选择 **Virtual Machine**，然后单击 **Next**。
- 在 **Create a virtual switch** 部分下，选择与公用网络相连的 NIC。
- 输入适用于公用虚拟交换机的网络标签。
- 验证摘要，然后单击 **Finish** 来创建公用网络虚拟交换机。
- 重复上述步骤来创建多个公用网络交换机。

4 要设置专用网络虚拟交换机，请执行以下操作：

- 在 ESXi 主机的 **Configuration** 选项卡中，导航到 **Hardware > Networking**。
- 单击右上角的 **Add Networking**。
- 针对连接类型选择 **Virtual Machine**，然后单击 **Next**。
- 取消选择默认情况下选择用于创建虚拟交换机的 NIC。
- 输入适用于专用虚拟交换机的网络标签。
- 验证摘要，以查看物理适配器下是否未显示适配器，然后单击 **Finish** 来创建专用网络虚拟交换机。
- 重复上述步骤来创建第二个专用网络虚拟交换机。

为引导磁盘和 LUN 创建数据存储

为引导磁盘和 LUN 创建数据存储

1 为虚拟机的 vmdk 文件创建数据存储。

2
- 在 ESx 主机的 **Configuration** 选项卡中，导航到 **Hardware > Storage**。
- 单击右上角的 **Add Storage**。
- 针对存储类型选择 **Disk/LUN**，然后单击 **Next**。
- 选择要用于创建虚拟机 vmdk 文件的磁盘。
- 查看当前的磁盘布局，然后单击 **Next**。
- 输入您选择的数据存储名称，然后单击 **Next**。
- 选择专用于数据存储的磁盘空间。默认选项是使用完整列表。
- 查看详细信息，然后单击 **Finish**。

为 Veritas Access 安装创建虚拟机

为 Veritas Access 安装创建虚拟机

1 完成网络配置并定义数据存储后，创建虚拟机。

- 在最左侧框架中树结构的顶部，选择 **ESXi host IP/hostname**。
- 从文件菜单中，选择 **New Virtual Machine**，这将打开用于创建虚拟机的弹出窗口。
- 针对配置选择 **Custom**，然后单击 **Next**，以确定虚拟机的确切配置。
- 输入选择的虚拟机名称，然后单击 **Next**。
- 选择用来存储虚拟机 `vmdk` 文件的数据存储，然后单击 **Next**。
- 选择要使用的虚拟机版本，然后单击 **Next**。Veritas 建议使用版本 8。
- 针对来宾操作系统选择 **Linux**，针对版本选择 **Red Hat Enterprise Linux 6 or 7 (64-bit)**，然后单击 **Next**。

选择 CPU 数量。Veritas 建议使用八个核心：

- 两个虚拟套接字，每个虚拟套接字四个核心。
- 一个虚拟套接字，每个虚拟套接字八个核心。
- 基于工作量的任何更多数量的核心。
  选择内存配置。Veritas 建议 32 GB。
- 在网络配置中，建议选择四个 NIC。
  对于 NIC1，选择公用网络虚拟交换机并验证该适配器是否正确。
  对于 NIC2，选择公用网络虚拟交换机并验证该适配器是否正确。
  对于 NIC3，选择专用网络虚拟交换机 1 并验证该适配器是否正确。
  对于 NIC4，选择专用网络虚拟交换机 2 并验证该适配器是否正确。
- 针对 SCSI 控制器选择 **VMware Paravirtual**。
- 在磁盘配置页面中，选择 **Create a new virtual disk**，然后单击 **Next**。
- 选择引导磁盘大小。Veritas 建议 100 GB。
- 针对磁盘配置类型选择 **Thick Provision Eager Zeroed**。
- 针对数据存储选择 **Specify a data store or data store cluster**，然后单击 **Next**。
  在选择数据存储之后，单击 **Next**。
- 将 **Virtual device node** 设置为默认节点（对于引导磁盘，为 SCSI (0:0)），然后单击 **Next**。
- 查看虚拟机配置，然后单击 **Finish** 来创建虚拟机。

虚拟机创建任务完成。

2 选择虚拟机，然后单击 **Edit virtual machine settings** 以验证以下内容：

- 应该有四个网络适配器：两个用于公用网络，两个用于专用网络。
- 验证内存和 CPU 配置是否正确。

3 重复步骤 1 和步骤 2 以创建第二个虚拟机，从而形成双节点 Veritas Access 群集。

4 将 LUN/DAS 磁盘添加到虚拟机。

要添加本地 DAS 磁盘，请执行以下操作：

- 选择虚拟机，然后单击 **Edit virtual machine settings**。
- 单击 **Add** 按钮。
- 针对设备类型选择 **Hard Disk**，然后单击 **Next**。
- 在磁盘类型中选择 **Create a new virtual disk**，然后单击 **Next**。
- 选择 DAS 磁盘大小。Veritas 建议 100 GB。
- 针对磁盘配置类型选择 **Thick Provision Eager Zeroed**。
- 针对数据存储选择 **Specify a data store or data store cluster**，然后单击 **Next**。
- 对于第一个 SAS 磁盘，将 **Virtual device node** 设置为 SCSI (1:0)，然后单击 **Next**。

  在创建所有必需的 DAS 磁盘后，完成以下操作：

  - 选择用于 DAS 磁盘的 SCSI 控制器 1。
  - 将 SCSI 总线共享模式设置为 **Virtual**。
    需要使用此模式，以便在 VxVM 基于磁盘阵列的命名 (EBN) 模式下声明 DAS 磁盘，且仅当磁盘处于 EBN 模式下时，主机名才由 VxVM 添加前缀，使其与阵列中的共享 LUN 有所区分。
- 单击 **OK** 以创建 DAS 磁盘。
  重复此步骤可为其他 Veritas Access 节点创建 DAS 磁盘。

5 将共享磁盘映射到 LUN。仅支持在原始设备映射 (RDM) 模式下从阵列映射 LUN。

将共享 LUN 映射到第一个虚拟机：

- 选择第一个虚拟机，然后单击 **Edit virtual machine settings**。
- 单击 **Add** 按钮。
- 针对设备类型选择 **Hard Disk**，然后单击 **Next**。

- 选择要映射的 LUN，然后单击 **Next**。
- 选择用来存储 LUN 映射的数据存储，或者选择 **Store with virtual machine**。
- 针对兼容模式选择 **Physical**，以直接访问阵列 LUN 硬件。
- 对于共享磁盘，将 **Virtual device node** 设置为 SCSI (2:0)，然后单击 **Next**。
- 查看磁盘的映射，然后单击 **Finish** 以将阵列 LUN 磁盘映射到虚拟机。
  对于要映射的其他 LUN 重复此步骤，并将 **Virtual device node** 更新为下一个可用的 SCSI 控制器端口。

在映射所有必需的 LUN 之后，完成以下操作：

- 选择用于共享 LUN 的 SCSI 控制器 2。
- 将 SCSI 总线共享模式设置为 **Virtual**。
  需要使用此模式，以便在 VxVM 基于磁盘阵列的命名 (EBN) 模式下声明共享 LUN。这可使其与阵列中的共享 LUN 有所区分。
- 单击 **OK**，以便在 RDM 模式下完成 LUN 映射。

将共享 LUN 映射到第二个虚拟机：

- 选择第一个虚拟机，然后单击 **Edit virtual machine settings**。
- 单击 **Add** 按钮。
- 针对设备类型选择 **Hard Disk**，然后单击 **Next**。
- 在磁盘类型中选择 **Use an existing Virtual Disk**，然后单击 **Next**。
- 将共享磁盘映射到第一个虚拟机时，导航到存储共享磁盘的数据存储中相应的磁盘路径。
- 对于共享磁盘，将 **Virtual device node** 设置为 SCSI (2:0)，然后单击 **Next**。确保磁盘映射顺序与第一个虚拟机的映射顺序相同，且已针对相同的 SCSI 控制器完成映射，以实现共享磁盘配置。
- 查看磁盘的映射，然后单击 **Finish** 以将阵列 LUN 磁盘映射到虚拟机。
  对于已映射到其他虚拟机的所有共享 LUN 重复此步骤，并将 **Virtual device node** 更新为下一个可用的 SCSI 控制器端口。

在映射所有必需的 LUN 之后，完成以下操作：

- 选择用于共享 LUN 的 SCSI 控制器 2。
- 将 SCSI 总线共享模式设置为 **Virtual**。
  需要使用此模式，以便在 VxVM 基于磁盘阵列的命名 (EBN) 模式下声明共享 LUN。这可使其与阵列中的共享 LUN 有所区分。
- 单击 **OK**，以便在 RDM 模式下完成 LUN 映射。

虚拟机的网络和存储配置完成。

6 安装 Veritas Access 安装程序支持的 RHEL 7 Update 3 或 4（64 位）操作系统。

请参见第 57 页的“在目标 Veritas Access 群集上安装操作系统”。

注意：虚拟机可包含 DAS 磁盘和/或共享 LUN。对于纠删码文件系统，只能包含 DAS 磁盘。

6

安装和配置群集

本章节包括下列主题：

安装概述

您可以在群集中安装 Veritas Access。群集中可以添加 1 到 20 个节点。通过向群集添加单个节点或多个节点，可以使系统具备容错功能并根据需要进行扩展。

安装步骤摘要

Veritas Access 软件安装包括两个主要部分：

- 操作系统安装。
  Veritas Access 需要 Red Hat Enterprise Linux。
  请参见请参见第 14 页的“系统要求”。
- Veritas Access 软件安装。

表 6-1 简要概述了各个安装步骤，其中可通过交叉引用来查看有关每个任务的详细信息。

表 6-1 安装步骤摘要

任务	步骤	有关详细信息
任务 1：在群集的每个节点上安装操作系统。	包括以下步骤： ■ 对 USB 设备、硬盘控制器等执行系统自动发现。 ■ 选择安装设备。 ■ 设置时钟和时区。 ■ 为自动安装做好系统准备。 ■ 手动执行磁盘分区。 ■ 按最低要求自动安装软件包。 ■ 安装 Red Hat Enterprise Linux 内核更新。	请参见第 59 页的“在群集上安装和配置 Veritas Access 软件”。
任务 2：在群集上安装 Veritas Access 软件。	包括以下步骤： ■ 安装所需的 Red Hat Enterprise Linux 操作系统 RPM。如果配置了 yum，则安装程序可帮助在预检过程中安装所需的 RPM。 ■ 提取 Veritas Access tar 文件，然后运行安装程序。 ■ 输入网络配置信息（群集名称、IP 地址、DNS 信息等）。 ■ 验证节点上的安装情况。	请参见第 59 页的“在群集上安装和配置 Veritas Access 软件”。

安装之前

安装 Veritas Access 软件之前：

- 确保在安装过程中作为访问配置一部分的所有公用和专用接口的名称在要安装 Veritas Access 的所有 Veritas Access 群集节点中应相同。
- 如果在安装 Veritas Access 之前，系统具有网络接口绑定，则需要将绑定名称指定为 bond0、bond1、bond2 等，然后才能开始安装 Veritas Access。
- 在安装 Veritas Access 之前，如果系统具有配置了 VLAN 的网络接口，并且用户希望在 Veritas Access 节点中配置它，则配置了 VLAN 的接口名称必须遵循如下所示的命名格式：
  <interface_name>.<vlan_id>。例如，eth0.100 或 ens168.101。
- 请确保没有 DHCP 服务器在专用网络中运行。
- 在群集中所有节点的 BIOS 中禁用 USB 以太网接口。
- 请确保群集与公用连接之间至少有两个专用连接。公用连接接口必须可以访问网关。
- 将 DAS 或 SAN 存储连接到群集节点。如果您要配置防护功能以避免出现裂脑情况，请确保 SAN 磁盘与 SCSI3 兼容。
- 为群集中的每个节点分配一个公用 IP 地址。此 IP 地址由安装程序使用，配置后，它会重新用作其中一个公用接口的物理 IP 地址。
- 请确保分配的 IP 在重新启动后永久保留。要使 IP 永久保留，请在 `/etc/sysconfig/network-scripts/ifcfg-XX` 中进行以下更改：
  例如：

```
TYPE=Ethernet
HWADDR=00:50:56:3d:f1:3e
DEVICE=eth2
BOOTPROTO=none
IPADDR=10.200.56.214
NETMASK=255.255.252.0
NM_CONTROLLED=no
ONBOOT=yes
```

注意：请确保具有足够的公用 IP，可满足安装 Veritas Access 软件时的 IP 需求。

在群集的每个节点上安装操作系统

安装 Veritas Access 软件之前，必须先安装 Red Hat Enterprise Linux 操作系统和内核版本。以下步骤提供了相关说明和下载链接。

在群集的每个节点上安装 Red Hat Enterprise Linux 操作系统

1 满足与系统要求相关的前提条件。确保您拥有正确的 Red Hat Linux 操作系统版本和内核版本。

2 根据需要使用以下一项信息安装 Red Hat Enterprise Linux 操作系统：

- 请参考 *Red Hat Enterprise Linux 7 Install guide*（《Red Hat Enterprise Linux 7 安装指南》）中的 *Chapter 1. Obtaining Red Hat Enterprise Linux*（“第 1 章：获取 Red Hat Enterprise Linux”）：
  https://access.redhat.com/downloads/
  https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/pdf/installation_guide/Red_Hat_Enterprise_Linux-7-Installation_Guide-en-US.pdf

关于驱动节点

如果不打算从群集的节点控制台（节点的本地管理控制台）中安装 Veritas Access，则需要群集中另一个不是 Veritas Access 目标节点的服务器，以便在 Veritas Access 安装中使用。此服务器称为驱动节点。

运行 Veritas Access 安装脚本时，Veritas Access 安装程序将帮助在驱动节点和目标 Veritas Access 群集节点之间设置 ssh 连接。

驱动节点平台可以为：RHEL 7、SLES 11 SP2 或 SLES 11 SP3。

下表提供了有关在使用不同类型网络设备的情况下，是否支持从群集节点或驱动节点安装 Veritas Access 的信息。

网络设备类型	驱动节点	群集节点
普通网络设备	是	是
通过安装程序创建绑定设备，并在通过其启动安装的绑定中添加 NIC	是	否
在通过其启动安装的 NIC 以外的 NIC 上创建绑定设备	是	是
在通过其启动安装的 NIC 以外的 NIC 上，通过安装程序创建 VLAN	否	是

网络设备类型	驱动节点	群集节点
在通过其启动安装的NIC上，通过安装程序创建 VLAN	否	否
排除从其启动安装的 NIC	否	否
在通过其启动安装的 NIC 以外的 NIC 上，创建绑定和基于绑定设备的 VLAN	否	是
将绑定预配置为公用设备，并从其他 NIC 进行安装	是	是
通过安装程序创建绑定，并选择其作为专用连接	否	否
通过安装程序创建VLAN，并选择其作为专用连接	否	否
使用公用 NIC 和预先存在的公用绑定进行安装	是	是

在目标 Veritas Access 群集上安装操作系统

此安装过程中的第一个任务是在群集中的每个节点上安装 Red Hat Enterprise Linux 操作系统。

安装操作系统

1 插入 Red Hat Enterprise Linux 7.4 操作系统安装 DVD，并从该 DVD 引导服务器。

请参见第 16 页的“Linux 要求”。

您也可以使用外部 USB DVD-ROM。

2 选择 **Install Red Hat Enterprise Linux 7.4**。

3 在系统加载后，为 **language for installation** 选择 **English**，然后单击 **Continue**。

在安装程序显示安装摘要后，您可以自定义安装过程。

4 单击 **Date & Time**，从提供的映射中选择您的系统位置，然后单击 **Done** 应用配置。

5 为语言系统支持和键盘语言选择 **English** 语言。

6 要选择系统软件，请单击 **Software Selection**，然后从列表中选择基本安装环境。

7 为 **Compatibility Libraries Add-ons** 选择 **Minimal Install**，然后单击 **Done** 以对安装过程应用此更改。

8 选择磁盘，然后手动执行磁盘分区以配置系统分区。

请参见第 14 页的“系统要求”。

9 单击 **Network & Hostname**，并提供系统主机名以设置您的网络连接。

设置主机名后，将以太网设置为 On 以启动您的网络接口。单击 **Configure** 并提供适用于您的网络连接的静态网络设置。

10 编辑以太网接口设置后，单击 **Done**。

此时将显示默认安装程序窗口。

11 验证安装设置，然后单击 **Begin Installation** 开始系统安装。

12 在安装过程中，开始在您的硬盘上写入系统组件时，您需要提供 root 密码。单击 **Root Password** 输入密码，完成后单击 **Done**。

完成安装后，安装程序将显示成功安装的详细信息。

13 Red Hat Enterprise Linux 安装至此完成。您可以按照本节中所述的相同步骤在群集的其他节点上安装操作系统。

有关详细过程，请参见“Red Hat Enterprise Linux 文档”。

在目标 Veritas Access 群集上安装 Oracle Linux 操作系统

此安装过程中的第一个任务是在群集的每个节点上安装 Oracle Linux (OL) 操作系统。

安装 OL 操作系统

1 插入 OL 操作系统安装 DVD，从该 DVD 启动服务器，然后按 **Enter** 键。

请参见第 16 页的“Linux 要求”。

您也可以使用外部 USB DVD-ROM。

2 按 **Tab** 键将焦点移到 **Skip** 键，然后按 **Enter** 键继续。

3 在 **Welcome** 屏幕上，单击 **Next** 选项。

4 选择 **English** 作为语言，然后单击 **Next** 选项。

5 选择 **U.S. English** 作为键盘设置，然后单击 **Next** 选项。

6 选择 **Basic Storage Devices** 选项，然后单击 **Next** 选项。

7 输入完全限定的主机名，然后单击 **Configure Network** 选项。

8 突出显示相关的连接，然后单击 **Edit** 选项。

9 选中 **Connect automatically** 复选框。如果您未使用 DHCP，单击 **IPv4 Settings** 选项卡，将方法设置为 **Manual**，单击 **Add** 选项，然后输入相应的网络详细信息。当您对这些详细信息感到满意时，单击 **Apply** 和 **Close** 选项以返回到主机名屏幕，然后单击 **Forward** 选项。

10 通过单击地图上最接近的城市选择相应的时区。单击 **Next** 选项。

11 输入服务器的 root 密码，然后单击 **Next**。

12 选择所需的分区类型。如果要修改默认的分区布局，请选中 **Review and modify partitioning layout** 选项。单击 **Next** 选项。

13 OEL 安装程序列出了适合您磁盘大小的默认分区方案。根据需要对其进行修改，然后单击 **Next** 选项。单击 **Format** 和 **Write changes to disk** 选项。

14 通过单击 **Next** 选项接受引导加载程序设置。

15 选择 **Minimal Install** 和 **Oracle Linux Server** 选项，然后单击 **Next** 选项。

16 等待安装完成。

17 单击 **Reboot** 选项以完成安装。

18 Veritas Access 仅支持与 Red Hat Enterprise Linux 兼容的内核。在安装 OEL 之后，直接获取与 Red Hat Enterprise Linux 兼容的内核。

在目标群集节点上安装 Veritas Access

安装群集是一次性活动。您可以安装多达 20 个节点的群集。

继续执行操作之前，请注意以下事项：

- 如果未向群集分配足够的 IP 地址，则安装无法继续。

注意：不能混合 IPv4 和 IPv6 地址；新的 IP 地址必须与最初安装 Veritas Access 时使用的地址相同。

请参见第 42 页的“关于获取 IP 地址”。

安装双节点群集大约需要 40 分钟。根据具体配置和节点数的不同，安装时间可能会有所差异。

在群集上安装和配置 Veritas Access 软件

安装和配置群集

注意：安装期间，安装程序日志位于 `/var/tmp`。

1 输入以下任一命令以启动安装。

```
# ./installaccess node1_ip node2_ip
```

其中，*node1_ip* 和 *node2_ip* 是已分配给目标群集节点以通过 SSH 安装 Veritas Access 的公用物理 IP 地址。

这些是当前分配给节点以便进行安装通信的 IP 地址。

此示例用于安装两个节点。要安装另一个目标节点群集，请将 *node3_ip* 添加到此步骤中使用的命令行。

2 安装程序将检查操作系统的依赖性，并自动安装所需的操作系统 RPMs。如果操作系统 RPMs 的依赖性未排序，则需要提供 Redhat 订购管理器用户 ID 和密码。

3 安装程序将安装 Veritas Access RPMs。

4 选择授权许可方法。回答授权许可问题并按照提示操作。

```
1)  Enter a valid perpetual or subscription license key file
2)  Register with evaluation mode and complete system licensing
later

How would you like to license the systems? [1-2,q,?] (2)
```

5 安装程序将显示要在配置后打开的防火墙端口，并询问是否要打开它们：

```
Veritas Access needs to open the following ports:
111 Rpcbind (NFS)
11211 Memcached Port
123 NTP Service
139 CIFS Service
14161 GUI
161 SNMP Service
2049 NFS Service
21 FTP Port
22 SSH Service
25 SMTP Port
30000:40000 FTP Passive Port Range
3172,3173 Server View Ports
4001 Mountd (NFS)
4045 NLM (NFS)
4379 CTDB Port
445 CIFS TCP Service
514 Syslog Service
53 DNS Service
5634 VIOM
56987 Replication Service
756,757,755 Statd (NFS)
8088 REST Server
8143 Object Access Gateway
8144 Object Access Admin Gateway
Do you want to proceed? [y,n,q] (y)
```

6 安装程序要求提供以下信息来配置群集：

```
Enter the cluster name: [q,?]
Do you want to rename the hosts' name like vac_01, vac_02? [y,n,q,b,?] (n)
Enter the public IP starting address or : [b,q,?]
Enter the netmask for the public IP address: [b,q,?] (255.255.255.0)
Enter the number of VIPs per interface: [b,q,?] (0) 1
Enter the virtual IP starting address: [b,q,?]
Enter the default gateway IP address: [b,q,?]
Enter the DNS IP address: [b,q,?] (10.0.2.3)
Enter the DNS domain name: [b,q,?] (community.veritas.com)
Enter the console virtual IP address: [b,q,?]
Do you want to use the separate console port? [y,n,q,b,?] (n)
Enter the private IP starting address: [b,q,?] (172.16.0.3)
```

注意：群集名称应与 DNS 兼容。群集名称必须至少包含 3 个字符，最多包含 10 个字符。群集名称中允许使用以下字符：a-z、0-9、-、小写字母、数字和连字符。任何其他字符无效。此外，如果已选择单独的控制台端口，则第一个公用 NIC 会用作专用的控制台端口。

7 安装程序将询问您是否要配置网络时间协议 (NTP) 服务器。

```
Do you want to configure the Network Time Protocol(NTP) server
to
synchronize the system clocks? [y,n,q]  y
Enter the Network Time Protocol server: [q,?]
```

如果输入 **y**，则可以键入 NTP 服务器。如果输入 **n**，则不配置 NTP 服务器。

8 安装程序将要求确认输入的群集信息。

安装程序将检测网络设备、检查网络设备与网关的连接以及显示相关信息。

```
Checking network configuration ..................................... Done
Detecting network devices .......................................... Done
Checking network connection ........................................ Done

Detecting network devices completed successfully.

Common NICs on all systems:

NIC       Type       Properties     Public
=========================================
ens161    Physical   -              N
ens192    Physical   -              Y
ens193    Physical   -              Y
ens224    Physical   -              Y
ens256    Physical   -              N

For the 'Public' field of the NIC:
    Y: means the NIC can connect to the public gateway, and can be selected as
public NIC.
    N: means the NIC cannot connect to the public gateway, and can be selected
as private NIC.
    -: means the NIC was not tested if connect to the public gateway.
    blank: means this NIC is excluded or not selectable.
```

要配置 Veritas Access 网络，您需要排除未使用的 NIC，并至少包括一个公用 NIC 和一个专用 NIC。建议包括两个公用 NIC 和两个专用 NIC，并且所有系统上选定的专用 NIC 应互连。

如果确实要配置 NIC 绑定或排除 NIC，请输入 **y**。

如果不需要配置 NIC 绑定或排除 NIC，请输入 **n**。转到步骤 安装和配置群集 。

请参见第 73 页的“排除 NIC”。

请参见第 79 页的“创建 NIC 绑定”。

请参见第 91 页的“创建 VLAN 设备 ”。

9 您需要选择以下选项之一以进行安装：

- 手动选择 NIC
- 配置 NIC 绑定

- 通过安装程序配置 VLAN

```
Do you want to manually select NICs, or configure NIC bonding or VLAN tagging? [y,n,q]
 (n)
Enter n : If you want installer to do auto network configuration for the cluster
Enter y : If you want to select public and private NICs manually, configure NIC bonding

          or to create VLAN using installer.
```

安装程序将在群集的每个节点上执行公用和专用NIC检测测试，如果输入的物理或虚拟 IP 少于配置群集所需的 IP，则安装程序将要求您添加所需的 IP。

10 验证网络配置详细信息（例如新IP地址、主机名和其他详细信息）是否正确。

11 安装程序将提示您验证网络配置。

验证配置信息是否正确，例如新 IP 地址、主机名和其他详细信息。

```
Configuration checklist:

System         Public NIC Physical IP
============== ========== ==============
192.168.10.10 ens192     192.168.10.20
192.168.10.10 ens224     192.168.10.21
192.168.10.10 ens193     192.168.10.22
192.168.10.11 ens192     192.168.10.23
192.168.10.11 ens224     192.168.10.24
192.168.10.11 ens193     192.168.10.25

System         Private NIC
============== ============
192.168.10.10 ens161
192.168.10.10 ens256
192.168.10.11 ens161
192.168.10.11 ens256

Virtual IP
=============================================================================
192.168.10.30 192.168.10.31 192.168.10.32 192.168.10.33 ...(6 in total)

Console IP
==============
192.168.10.50

Gateway IP   DNS IP       Domain name
============ ============ ===================
192.168.10.1 192.168.10.2 vxindia.veritas.com

Is this information correct? [y,n,q,b,?] (y)
```

12 确认网络配置详细信息后，安装程序将重命名主机名（如果您已选择对其进行重命名）并为系统分配 IP。此外，安装程序还将检查低延迟传输 (LLT) 链路状态并自动选择它们。

注意：如果已选择 InfiniBand NIC 作为专用 NIC，则安装程序不会检查 LLT 链路状态。

13 安装程序将执行 Veritas Access 服务组配置。

14 安装程序将提示您是否要在安装期间配置 I/O 防护。

```
Do you want to configure I/O Fencing in enabled mode? [y,n,q,?]
(y)
```

如果不需要配置 I/O 防护，请输入 **n**。

要配置 I/O 防护，请输入 **y**。

请参见第 98 页的“配置 I/O 防护”。

15 安装程序将自动重新启动群集节点，从而为每个节点启用 Kdump 功能。

16 检查日志文件以确认安装和配置。日志位于 `/opt/VRTS/install/logs/`。

注意：安装后，使用先前分配的控制台 IP 地址连接到 Veritas Access，然后使用默认用户名 `master` 和默认密码 `master` 登录。

Veritas Access 图形用户界面

Veritas Access 具有图形用户界面 (GUI)，可为特定的 Veritas Access 群集提供控制板，并为共享、存储基础架构、报告和设置提供相关视图。GUI 允许管理员执行群集相关的任务并对结果进行监视。在此版本中，GUI 是 Veritas Access 的一部分。

成功完成 I/O 防护配置后，GUI 链接将显示在屏幕上。

```
Open the https://<console IP>:14161 URL
in your browser to start the Veritas Access GUI application.
```

关于管理 NIC、绑定和 VLAN 设备

输入 **y** 时，安装程序允许您执行以下操作：

```
Do you want to manually select NICs, or configure NIC bonding or VLAN tagging? [y,n,q]
 (n) y
```

- 选择公用 NIC
  请参见第 67 页的“选择公用 NIC”。
- 选择专用 NIC
  请参见第 70 页的“选择专用 NIC”。
- 排除 NIC
  请参见第 73 页的“排除 NIC”。

- 包括 NIC
  请参见第 76 页的“包括 NIC”。
- 创建新的 NIC 绑定以及将 NIC 添加到绑定
  请参见第 79 页的“创建 NIC 绑定”。
- 移除绑定
  请参见第 85 页的“移除 NIC 绑定”。
- 从绑定列表中移除 NIC
  请参见第 88 页的“从绑定列表中移除 NIC”。
- 在特定 NIC 上添加 VLAN 设备
  请参见第 91 页的“创建 VLAN 设备 ”。
- 在特定 NIC 上删除 VLAN 设备
  请参见第 94 页的“删除 VLAN 设备 ”。

注意：NIC 绑定和 NIC 排除配置选项既支持单个 NIC 绑定，也支持多个 NIC 绑定。

使用 NIC 排除功能时，可以排除第一个节点上的任何 NIC。但是，如果要排除其他节点上的任何 NIC，则可按节点选择要排除的 NIC。

请参见第 73 页的“排除 NIC”。

选择公用 NIC

在群集中安装 Veritas Access 时，您可能希望将特定网络设备配置为公用接口（即使它们无法访问网关）以及将特定网络设备配置为专用接口。

选择公用 NIC

1 在手动选择模式下，输入 **1** 以选择公用 NIC。

```
NIC selection/NIC bonding/NIC VLAN configuration

Common NICs on all systems:

NIC         Type       Properties       Public
=================================================
ens161      Physical   -                N
ens192      Physical   -                Y
ens193      Physical   -                Y
ens224      Physical   Slave of bond0
ens225      Physical   Slave of bond0
ens256      Physical   -                N
ens257      Physical   -
bond0       Virtual    Bond balance-rr  Y
ens192.100 Virtual    VLAN 100         -

     1)  Select public NICs
     2)  Select private NICs
     3)  Exclude NICs
     4)  Include NICs
     5)  Create a new bond
     6)  Add NICs to a bond
     7)  Remove bonds
     8)  Remove NICs from the bond list
     9)  Create VLAN device
    10)  Delete VLAN device
    11)  Save and continue

Select the NIC option to be configured in this cluster: [1-11,q]
 1
```

2 选择要选为公用 NIC 的 NIC。

```
Choose NICs as public

     1)  ens161
     2)  ens192
     3)  ens193
     4)  ens256
     5)  bond0
     6)  ens192.100
     7)  Unselect previous public NICs
     b)  Back to previous menu

Choose items, separated by spaces: [1-7,b,q] 2 4 5 6
NIC selection/NIC bonding/NIC VLAN configuration

Common NICs on all systems:

NIC         Type       Properties       Public
=====================================================
ens161      Physical   -                N
ens192      Physical   -                Y (Selected)
ens193      Physical   -                Y
ens224      Physical   Slave of bond0
ens225      Physical   Slave of bond0
ens256      Physical   -                Y (Selected)
ens257      Physical   -
bond0       Virtual    Bond balance-rr  Y (Selected)
ens192.100 Virtual     VLAN 100         Y (Selected)

     1)  Select public NICs
     2)  Select private NICs
     3)  Exclude NICs
     4)  Include NICs
     5)  Create a new bond
     6)  Add NICs to a bond
     7)  Remove bonds
     8)  Remove NICs from the bond list
     9)  Create VLAN device
    10)  Delete VLAN device
    11)  Save and continue
```

```
Select the NIC option to be configured in this cluster: [1-11,q]
```

注意：要开始配置群集，请在手动选择或配置公用和专用 NIC 后，输入 **11**，以选择 `Save and continue` 选项。

选择专用 NIC

在群集中安装 Veritas Access 时，您可能希望将特定网络设备配置为专用接口。

选择专用 NIC

1 在手动选择模式下，输入 **2** 以选择专用 NIC。

```
NIC selection/NIC bonding/NIC VLAN configuration

Common NICs on all systems:

NIC         Type        Properties        Public
=================================================
ens161      Physical    -                  N
ens192      Physical    -                  Y (Selected)
ens193      Physical    -                  Y (Selected)
ens224      Physical    Slave of bond0
ens225      Physical    Slave of bond0
ens256      Physical    -                  N
ens257      Physical    -
bond0       Virtual       Bond balance-rr  Y (Selected)
ens192.100 Virtual    VLAN 100          Y (Selected)

     1)  Select public NICs
     2)  Select private NICs
     3)  Exclude NICs
     4)  Include NICs
     5)  Create a new bond
     6)  Add NICs to a bond
     7)  Remove bonds
     8)  Remove NICs from the bond list
     9)  Create VLAN device
    10)  Delete VLAN device
    11)  Save and continue

Select the NIC option to be configured in this cluster: [1-11,q]
  2
```

2 选择要选为专用 NIC 的 NIC。

```
Choose NICs as private

     1)  ens161
     2)  ens192
     3)  ens193
     4)  ens256
     5)  Unselect previous private NICs
     b)  Back to previous menu

Choose items, separated by spaces: [1-5,b,q] 1 4

NIC selection/NIC bonding/NIC VLAN configuration

Common NICs on all systems:

NIC         Type       Properties       Public
=====================================================
ens161      Physical   -                N (Selected)
ens192      Physical   -                Y (Selected)
ens193      Physical   -                Y (Selected)
ens224      Physical   Slave of bond0
ens225      Physical   Slave of bond0
ens256      Physical   -                N (Selected)
ens257      Physical   -
bond0       Virtual    Bond balance-rr  Y (Selected)
ens192.100 Virtual    VLAN 100         Y (Selected)

     1)  Select public NICs
     2)  Select private NICs
     3)  Exclude NICs
     4)  Include NICs
     5)  Create a new bond
     6)  Add NICs to a bond
     7)  Remove bonds
     8)  Remove NICs from the bond list
     9)  Create VLAN device
    10)  Delete VLAN device
    11)  Save and continue

Select the NIC option to be configured in this cluster: [1-11,q]
```

注意：要开始配置群集，请在手动选择或配置公用和专用 NIC 后，输入 **11**，以选择 `Save and continue` 选项。

排除 NIC

在群集上安装 Veritas Access 时，您可能希望使用某些 NIC 实现其他存储目的。您可以排除不希望用于 Veritas Access 的 NIC。

注意：NIC 绑定/NIC 排除配置选项既支持单个 NIC 绑定，也支持多个 NIC 绑定。

排除 NIC

1 在手动选择模式下，输入 **3**。

```
NIC selection/NIC bonding/NIC VLAN configuration

Common NICs on all systems:

NIC         Type       Properties       Public
=================================================
ens161      Physical   -                N
ens192      Physical   -                Y
ens193      Physical   -                Y
ens224      Physical   Slave of bond0
ens225      Physical   Slave of bond0
ens256      Physical   -                N
ens257      Physical   -                Y
bond0       Virtual    Bond balance-rr  Y
ens192.100 Virtual    VLAN 100         -

     1)  Select public NICs
     2)  Select private NICs
     3)  Exclude NICs
     4)  Include NICs
     5)  Create a new bond
     6)  Add NICs to a bond
     7)  Remove bonds
     8)  Remove NICs from the bond list
     9)  Create VLAN device
    10)  Delete VLAN device
    11)  Save and continue

Select the NIC option to be configured in this cluster: [1-11,q]
 3
```

2 选择要排除的 NIC。

```
Choose NICs for exclusion

     1)  ens161
     2)  ens192
     3)  ens193
     4)  ens256
     5)  ens257
     6)  bond0
     7)  ens192.100
     b)  Back to previous menu

Choose items, separated by spaces: [1-7,b,q] 3 5

NIC selection/NIC bonding/NIC VLAN configuration

Common NICs on all systems:

NIC         Type        Properties        Public
=====================================================
ens161      Physical    -                 N
ens192      Physical    -                 Y
ens193      Physical    -
ens224      Physical    Slave of bond0
ens225      Physical    Slave of bond0
ens256      Physical    -                 N
ens257      Physical    -
bond0       Virtual     Bond balance-rr   Y
ens192.100 Virtual      VLAN 100          -

     1)  Select public NICs
     2)  Select private NICs
     3)  Exclude NICs
     4)  Include NICs
     5)  Create a new bond
     6)  Add NICs to a bond
     7)  Remove bonds
     8)  Remove NICs from the bond list
     9)  Create VLAN device
    10)  Delete VLAN device
    11)  Save and continue
```

```
Select the NIC option to be configured in this cluster: [1-11,q]
```

包括 NIC

在群集上安装 Veritas Access 时，您可能希望包括先前已排除的一个或多个 NIC。可以包括要用于 Veritas Access 的 NIC。

包括 NIC

1 在手动选择模式下，输入 **4**。

```
Common NICs on all systems:

NIC         Type       Properties       Public
=====================================================
ens161      Physical   -                N
ens192      Physical   -                Y
ens193      Physical   -
ens224      Physical   Slave of bond0
ens225      Physical   Slave of bond0
ens256      Physical   -                N
ens257      Physical   -
bond0       Virtual    Bond balance-rr  Y
ens192.100 Virtual    VLAN 100         -

     1)  Select public NICs
     2)  Select private NICs
     3)  Exclude NICs
     4)  Include NICs
     5)  Create a new bond
     6)  Add NICs to a bond
     7)  Remove bonds
     8)  Remove NICs from the bond list
     9)  Create VLAN device
    10)  Delete VLAN device
    11)  Save and continue

Select the NIC option to be configured in this cluster: [1-11,q]
 4
```

2 选择要包括的 NIC。

```
Choose NICs for inclusion

     1)  ens193
     2)  ens257
     b)  Back to previous menu

Choose items, separated by spaces: [1-2,b,q]  1


NIC selection/NIC bonding/NIC VLAN configuration

Common NICs on all systems:

NIC         Type       Properties       Public
=====================================================
ens161      Physical   -                N
ens192      Physical   -                Y
ens193      Physical   -                Y
ens224      Physical   Slave of bond0
ens225      Physical   Slave of bond0
ens256      Physical   -                N
ens257      Physical   -
bond0       Virtual    Bond balance-rr  Y
ens192.100 Virtual    VLAN 100         -

     1)  Select public NICs
     2)  Select private NICs
     3)  Exclude NICs
     4)  Include NICs
     5)  Create a new bond
     6)  Add NICs to a bond
     7)  Remove bonds
     8)  Remove NICs from the bond list
     9)  Create VLAN device
    10)  Delete VLAN device
    11)  Save and continue

Select the NIC option to be configured in this cluster: [1-11,q]
```

创建 NIC 绑定

管理员可在 Veritas Access 安装期间从给定的公用 NIC 接口列表创建绑定 NIC 接口。借助此功能，管理员可以节省大量用于安装和安装后绑定创建的物理 IP 地址。

- 无法绑定 InfiniBand NIC，因为它们的 PCI ID 都相同。

如果不希望创建绑定接口，请继续安装。

请参见第 42 页的“关于获取 IP 地址”。

请参见第 43 页的“关于计算 IP 地址要求”。

创建绑定

1 选择手动选择模式后，安装程序将提示您输入您的选择。输入 **5** 创建新绑定。

```
NIC selection/NIC bonding/NIC VLAN configuration

Common NICs on all systems:

NIC        Type       Properties       Public
=================================================
ens161     Physical   -                N
ens192     Physical   -                Y
ens193     Physical   -                Y
ens224     Physical   -                Y
ens225     Physical   -                Y
ens256     Physical   -                N
ens257     Physical   -                Y

     1)  Select public NICs
     2)  Select private NICs
     3)  Exclude NICs
     4)  Include NICs
     5)  Create a new bond
     6)  Add NICs to a bond
     7)  Remove bonds
     8)  Remove NICs from the bond list
     9)  Create VLAN device
    10)  Delete VLAN device
    11)  Save and continue

Select the NIC option to be configured in this cluster: [1-11,q]
 5
```

2 为新绑定选择绑定模式。

```
Configure the mode of the NIC bonding:

     1)  balance-rr
     2)  active-backup
     3)  balance-xor
     4)  broadcast
     5)  802.3ad
     6)  balance-tlb
     7)  balance-alb
     b)  Back to previous menu

Select the bonding mode: [1-7,b,q] 1

bond0 is created. Please add NICs to bond0 to enable it.

Press [Enter] to continue:
```

如果选择 **3** 或 **5**，则需要为绑定模式选择绑定选项：

```
1) layer2
2) layer3+4
3) default

Select the bonding option: [1-3,b,q] 1
```

安装程序将提示您选择要为群集配置的 NIC 选项。

3 输入 **6** 将 NIC 添加到绑定。

注意：需要在绑定中添加 NIC。

```
NIC selection/NIC bonding/NIC VLAN configuration

Common NICs on all systems:

NIC         Type        Properties        Public
=====================================================
ens161      Physical    -                 N
ens192      Physical    -                 Y
ens193      Physical    -                 Y
ens224      Physical    -                 Y
ens225      Physical    -                 Y
ens256      Physical    -                 N
ens257      Physical    -                 Y
bond0       Virtual     Bond balance-rr   -

     1)  Select public NICs
     2)  Select private NICs
     3)  Exclude NICs
     4)  Include NICs
     5)  Create a new bond
     6)  Add NICs to a bond
     7)  Remove bonds
     8)  Remove NICs from the bond list
     9)  Create VLAN device
    10)  Delete VLAN device
    11)  Save and continue

Select the NIC option to be configured in this cluster: [1-11,q]
 6
```

4 输入 **6** 选择要在绑定中添加的 NIC。

```
Choose NICs for bonding

     1)  ens161
     2)  ens192
     3)  ens193
     4)  ens224
     5)  ens225
     6)  ens256
     7)  ens257
     b)  Back to previous menu

Choose NICs, separated by spaces: [1-7,b,q,?] 4 5
```

5 选择要为其添加 NIC 的绑定名称

```
Choose a bond name to add NICs

     1)  bond0
     b)  Back to previous menu

Choose bonds, separated by spaces: [1-1,b,q] 1

Adding ens224 ens225 to bond0 was successful

Press [Enter] to continue:

NIC selection/NIC bonding/NIC VLAN configuration

Common NICs on all systems:

NIC        Type       Properties       Public
=====================================================
ens161     Physical   -                N
ens192     Physical   -                Y
ens193     Physical   -                Y
ens224     Physical   Slave of bond0
ens225     Physical   Slave of bond0
ens256     Physical   -                N
ens257     Physical   -                Y
bond0      Virtual    Bond balance-rr  Y

     1)  Select public NICs
     2)  Select private NICs
     3)  Exclude NICs
     4)  Include NICs
     5)  Create a new bond
     6)  Add NICs to a bond
     7)  Remove bonds
     8)  Remove NICs from the bond list
     9)  Create VLAN device
    10)  Delete VLAN device
    11)  Save and continue

Select the NIC option to be configured in this cluster: [1-11,q]
```

移除 NIC 绑定

管理员可以移除绑定。

移除 NIC 绑定

1 输入 **7** 将移除现有绑定。

```
Common NICs on all systems:

NIC        Type       Properties         Public
=========================================================
ens161     Physical   -                  N
ens192     Physical   -                  Y
ens193     Physical   Slave of bond1
ens224     Physical   Slave of bond0
ens225     Physical   Slave of bond0
ens256     Physical   -                  N
ens257     Physical   -                  Y
bond0      Virtual    Bond balance-rr    Y
bond1      Virtual    Bond active-backup Y

     1)  Select public NICs
     2)  Select private NICs
     3)  Exclude NICs
     4)  Include NICs
     5)  Create a new bond
     6)  Add NICs to a bond
     7)  Remove bonds
     8)  Remove NICs from the bond list
     9)  Create VLAN device
    10)  Delete VLAN device
    11)  Save and continue

Select the NIC option to be configured in this cluster: [1-11,q]
 7
```

2 选择要移除的绑定。

```
Choose bonds to be removed

     1)  bond0
     2)  bond1
     b)  Back to previous menu

Choose bonds, separated by spaces: [1-2,b,q] 2

Deleting NIC bonding bond1 succeeded

Press [Enter] to continue:
NIC selection/NIC bonding/NIC VLAN configuration

Common NICs on all systems:

NIC        Type       Properties       Public
=====================================================
ens161     Physical   -                N
ens192     Physical   -                Y
ens193     Physical   -                Y
ens224     Physical   Slave of bond0
ens225     Physical   Slave of bond0
ens256     Physical   -                N
ens257     Physical   -                Y
bond0      Virtual    Bond balance-rr  Y

     1)  Select public NICs
     2)  Select private NICs
     3)  Exclude NICs
     4)  Include NICs
     5)  Create a new bond
     6)  Add NICs to a bond
     7)  Remove bonds
     8)  Remove NICs from the bond list
     9)  Create VLAN device
    10)  Delete VLAN device
    11)  Save and continue

Select the NIC option to be configured in this cluster: [1-11,q]
```

从绑定列表中移除 NIC

安装期间，管理员可以在保存配置之前移除已绑定的从属 NIC。

从绑定列表中移除 NIC

1 在 Veritas Access 安装期间，安装程序将提示您输入自己的选择。输入 **8** 将从绑定列表中移除 NIC。

注意：NIC 绑定或 NIC 排除配置选项既支持单个 NIC/绑定，也支持多个 NIC/绑定。

```
NIC selection/NIC bonding/NIC VLAN configuration

Common NICs on all systems:

NIC        Type       Properties         Public
=======================================================
ens161     Physical   -                  N
ens192     Physical   Slave of bond1
ens193     Physical   Slave of bond1
ens224     Physical   Slave of bond0
ens225     Physical   Slave of bond0
ens256     Physical   -                  N
ens257     Physical   -                  Y
bond0      Virtual    Bond balance-rr    Y
bond1      Virtual    Bond active-backup Y

     1)  Select public NICs
     2)  Select private NICs
     3)  Exclude NICs
     4)  Include NICs
     5)  Create a new bond
     6)  Add NICs to a bond
     7)  Remove bonds
     8)  Remove NICs from the bond list
     9)  Create VLAN device
    10)  Delete VLAN device
    11)  Save and continue

Select the NIC option to be configured in this cluster: [1-11,q]
 8
```

2 选择要从 NIC 绑定中移除的 NIC。

```
Choose NICs to be deleted from the NIC bonding

     1)  ens192
     2)  ens193
     3)  ens224
     4)  ens225
     b)  Back to previous menu

Choose NICs, separated by spaces: [1-4,b,q,?] 1

Removing ens192 from bonding was successful

Press [Enter] to continue:
NIC selection/NIC bonding/NIC VLAN configuration

Common NICs on all systems:

NIC         Type        Properties          Public
=======================================================
ens161      Physical    -                   N
ens192      Physical    -                   Y
ens193      Physical    Slave of bond1
ens224      Physical    Slave of bond0
ens225      Physical    Slave of bond0
ens256      Physical    -                   N
ens257      Physical    -                   Y
bond0       Virtual     Bond balance-rr     Y
bond1       Virtual     Bond active-backup  Y

     1)  Select public NICs
     2)  Select private NICs
     3)  Exclude NICs
     4)  Include NICs
     5)  Create a new bond
     6)  Add NICs to a bond
     7)  Remove bonds
     8)  Remove NICs from the bond list
     9)  Create VLAN device
    10)  Delete VLAN device
    11)  Save and continue
```

```
Select the NIC option to be configured in this cluster: [1-11,q]
```

关于 VLAN 标记

当 VLAN（虚拟局域网）跨多个交换机时，VLAN 标记是必需的。通过 VLAN，可以在物理网络内部创建独立的逻辑网络。VLAN 标记是指在数据包头中插入 VLAN ID 以标识该数据包所属的 VLAN 的做法。

通过使用 VLAN 标记功能，您可以：

- 在安装期间创建 VLAN 设备
- 在指定的绑定接口上创建 VLAN 设备。

注意：需要先创建绑定接口。

请参见第 91 页的“创建 VLAN 设备 ”。
请参见第 94 页的“删除 VLAN 设备 ”。

创建 VLAN 设备

您可以为公用 NIC 接口或公用绑定创建 VLAN 设备。

请参见第 91 页的“关于 VLAN 标记”。

注意：如果您需要在配置 Veritas Access 网络时将 VLAN 接口用作公用 NIC，则必须在安装 Veritas Access 期间将在其中创建 VLAN 的 NIC 添加为公用 NIC。

例如，在安装 Veritas Access 时，如果 VLAN 为 `eth0.100`，则在配置访问网络期间应选择 `eth0.100` 和 `eth0` 作为公用 NIC。

创建 VLAN 设备

1 在手动选择模式下，输入 **9** 以创建 VLAN 设备。

```
NIC selection/NIC bonding/NIC VLAN configuration

Common NICs on all systems:

NIC        Type       Properties       Public
=================================================
ens161     Physical   -                N
ens192     Physical   -                Y
ens193     Physical   -                Y
ens224     Physical   Slave of bond0
ens225     Physical   Slave of bond0
ens256     Physical   -                N
ens257     Physical   -                Y
bond0      Virtual    Bond balance-rr  Y

     1)  Select public NICs
     2)  Select private NICs
     3)  Exclude NICs
     4)  Include NICs
     5)  Create a new bond
     6)  Add NICs to a bond
     7)  Remove bonds
     8)  Remove NICs from the bond list
     9)  Create VLAN device
    10)  Delete VLAN device
    11)  Save and continue

Select the NIC option to be configured in this cluster: [1-11,q]
 9
```

2 选择要在其中创建 VLAN 设备的 NIC。

3 输入设备的 VLAN ID。

```
Choose NICs to create VLAN device on:
     1)  ens161
     2)  ens192
     3)  ens193
     4)  ens256
     5)  ens257
     6)  bond0
     b)  Back to previous menu

Choose VLAN devices, separated by spaces: [1-6,b,q] 2

Enter the VLAN ID for the device (1-4094): [b,q,?] 100


NIC selection/NIC bonding/NIC VLAN configuration

Common NICs on all systems:

NIC         Type       Properties       Public
=====================================================
ens161      Physical   -                N
ens192      Physical   -                Y
ens193      Physical   -                Y
ens224      Physical   Slave of bond0
ens225      Physical   Slave of bond0
ens256      Physical   -                N
ens257      Physical   -                Y
bond0       Virtual    Bond balance-rr  Y
ens192.100 Virtual    VLAN 100         -

     1)  Select public NICs
     2)  Select private NICs
     3)  Exclude NICs
     4)  Include NICs
     5)  Create a new bond
     6)  Add NICs to a bond
     7)  Remove bonds
     8)  Remove NICs from the bond list
     9)  Create VLAN device
    10)  Delete VLAN device
    11)  Save and continue
```

```
Select the NIC option to be configured in this cluster: [1-11,q]
```

删除 VLAN 设备

您可以删除公用 NIC 接口或公用绑定的 VLAN 设备。

请参见第 91 页的“关于 VLAN 标记”。

删除 VLAN 设备

1 在手动选择模式下，输入 **10** 以删除 VLAN 设备。

```
Common NICs on all systems:

NIC         Type       Properties       Public
=====================================================
ens161      Physical   -                N
ens192      Physical   -                Y
ens193      Physical   -                Y
ens224      Physical   Slave of bond0
ens225      Physical   Slave of bond0
ens256      Physical   -                N
ens257      Physical   -                Y
bond0       Virtual    Bond balance-rr  Y
ens192.100 Virtual    VLAN 100         -

     1)  Select public NICs
     2)  Select private NICs
     3)  Exclude NICs
     4)  Include NICs
     5)  Create a new bond
     6)  Add NICs to a bond
     7)  Remove bonds
     8)  Remove NICs from the bond list
     9)  Create VLAN device
    10)  Delete VLAN device
    11)  Save and continue

Select the NIC option to be configured in this cluster: [1-11,q]
 10
```

2 选择要删除的 VLAN NIC。

```
Choose VLAN NICs to be deleted

     1)  ens192.100
     b)  Back to previous menu

Choose VLAN devices, separated by spaces: [1-1,b,q] 1

NIC selection/NIC bonding/NIC VLAN configuration

Common NICs on all systems:

NIC        Type       Properties       Public
=====================================================
ens161     Physical   -                N
ens192     Physical   -                Y
ens193     Physical   -                Y
ens224     Physical   Slave of bond0
ens225     Physical   Slave of bond0
ens256     Physical   -                N
ens257     Physical   -                Y
bond0      Virtual    Bond balance-rr  Y

     1)  Select public NICs
     2)  Select private NICs
     3)  Exclude NICs
     4)  Include NICs
     5)  Create a new bond
     6)  Add NICs to a bond
     7)  Remove bonds
     8)  Remove NICs from the bond list
     9)  Create VLAN device
    10)  Delete VLAN device
    11)  Save and continue

Select the NIC option to be configured in this cluster: [1-11,q]
```

VLAN 标记的限制

请注意使用 VLAN 标记的以下限制：

- 仅支持全新安装。对于使用 -updateparameter 选项的重新配置以及节点添加配置，不支持 VLAN 标记。
- 仅支持在绑定的 NIC 上创建 VLAN 设备。
- 仅支持在安装时创建一个 VLAN 设备。

更换以太网接口卡

在某些情况下，可能需要更换节点上的以太网接口卡。本节介绍更换此卡的步骤。

注意：此过程适用于更换现有的以太网接口卡。它不适用于添加以太网接口卡到群集。如果添加的以太网接口卡需要新的设备驱动程序，请先在节点上安装新的设备驱动程序，然后再安装以太网接口卡。

更换以太网接口卡

1 使用 Cluster> shutdown 命令关闭节点。

例如：

```
Cluster> shutdown access_03
Stopping Cluster processes on access_03.......done
Sent shutdown command to access_03
```

2 使用 Cluster> del 命令从群集中删除节点。

例如：

```
Cluster> del access_03
```

3 在节点上安装更换的以太网接口卡。

4 打开节点。

5 确保以太网接口卡处于活动和联机状态。

6 使用 Cluster> add 命令重新将节点添加到群集。

例如：

```
Cluster> add 172.16.113.118
```

有关本节中介绍的 Cluster> add 和 Upgrade> 命令的详细信息，请参见相关的手册页。

配置 I/O 防护

Veritas Access 支持两种防护模式：

- 基于磁盘的防护，适用于包含共享磁盘的群集
- 基于多数的防护，适用于包含本地 DAS 磁盘的群集

如果要同时使用共享磁盘 (SAN) 和本地磁盘，则必须使用基于多数的防护。Veritas 建议不要通过安装程序配置 I/O 防护。

1 在 Veritas Access 配置期间，启动产品之后，安装程序将询问您是否要配置防护：

```
Do you want to configure I/O Fencing in enabled mode? [y,n,q,?]
(y)
```

2 输入 **y** 以配置防护。

您可以选择以下防护模式之一：

- 如果群集不包含已初始化的共享磁盘，则需要配置基于多数的防护。

```
1. Majority Based Fencing
Select the fencing mechanism to be configured:[b](1)
```

- 如果已连接并初始化共享磁盘，则配置基于磁盘的 I/O 防护。系统会提示您选择防护类型。

```
1. Majority Based Fencing
2. Disk Based Fencing
Select the fencing mechanism to be configured:[b](2)
```

注意：您可以选择三个可用的 VxVM 磁盘，或将三个磁盘初始化为 VxVM 磁盘以形成防护磁盘组。必须不多不少选择三个磁盘。

3 安装程序将停止本产品，并在重新启动之前应用防护配置。

关于配置 Veritas NetBackup

如果使用 Veritas NetBackup，为了遵守 NetBackup 最终用户许可协议 (EULA)，您必须在将 NetBackup 配置为使用 Veritas Access 之前，购买并在外部 NetBackup 主服务器上输入有效的许可证密钥。有关在 NetBackup 主服务器上输入 NetBackup 许可证密钥的详细信息，请参见《Veritas NetBackup 安装指南》。

如果使用 NetBackup，请通过 `Backup> virtual-ip` 命令配置虚拟 IP 地址，使该地址不同于其余所有虚拟 IP 地址，例如控制台服务器 IP 地址和用于安装 Veritas Access 软件的物理 IP 地址。

关于在 Veritas Access 配置期间启用 kdump

在 Veritas Access 配置期间，Veritas Access 安装程序会尝试在群集节点上启用 kdump。为了满足 Veritas Access 软件要求，安装程序将使用以下选项来修改 `/etc/kdump.conf` 和 `/boot/grub/grub.conf` 文件：

- `/boot/grub/grub.conf`
  ```
  crashkernel = 512M-2G:64M, 2G-:256M
  ```

- `/etc/kdump.conf`
  ```
  path /opt/VRTSsnas/core/kernel/
  core_collector makedumpfile -c --message-level 1 -d 31
  ```

重新配置 Veritas Access 群集名称和网络

安装并配置 Veritas Access 之后，可以根据需要重新配置群集名称和网络。

重新配置群集之前，由于已禁止 root 用户访问权限，因此您必须为节点启用 *support* 用户。*support* 用户默认密码为 *veritas*。第一次登录后可以更改密码。

重新配置 Veritas Access 群集名称和网络

1 使用 *support* 用户名和密码登录到主机控制台。

2 确保所有服务组均处于脱机状态。输入以下命令：

/opt/VRTS/install/installaccess -updateparameter

3 输入系统的专用 IP。

172.16.0.3 172.16.0.4

注意： 只能输入系统的专用 IP。公用 IP 不应在此处使用。

4 输入群集名称和网络信息。

```
Enter the cluster name:
Enter the public IP starting address:
Enter the netmask for the public IP address:
Enter the number of VIPs per interface:
Enter the virtual IP starting address:
Enter the default gateway IP address:
Enter the DNS IP address:
Enter the DNS domain name:
Enter the console virtual IP address:
Do you want to use the separate console port? [y,n,q] (n):
Do you want to configure the Network Time Protocol(NTP) server
to
synchronize the system clocks? [y,n,q] (n) y:
Enter the Network Time Protocol server:
```

安装程序将确认输入的信息是否正确。配置已完成，群集上已配置新的群集和 IP。

安装程序将显示日志和摘要文件的位置。如果需要，请查看文件以确认配置状态。

注意： 群集名称只能包含字母、数字或下划线。群集名称必须以字母表的字母开头，最大长度为 15 个字符。此外，如果已选择单独的控制台端口，则第一个公用 NIC 会用作专用的控制台端口。

注意： 如果群集具有 DAS 磁盘，则将该群集名称限制为 10 个字符。

格式化 DAS 磁盘之后，请勿更改群集名称。

在 Veritas Access 群集上配置 KMS 服务器

您可以在 Veritas Access 群集上配置 KMS 服务器。

在 Veritas Access 群集上配置 KMS 服务器

1 获取 KMS 服务器的 SSL 公钥（采用 base64 格式）及其端口号。此密钥用于在 Veritas Access 群集和 KMS 服务器之间进行通信。

2 在 Veritas Access 群集上生成 SSL 自签名密钥对：

```
System> kms certificate generate
```

3 导入 KMS 服务器的公钥。

```
System> kms certificate import_server_cert
```

4 配置 KMS 服务器。提供在步骤 1 中获得的 SSL 公钥，输入如此处所示。

```
System> kms config server <server_ip><server_port>
```

其中，*server_ip* 是 KMS 服务器 IP

server_port 是 KMS 服务器端口号。

5 KMS 管理员现在使用其管理 GUI 设置信任证书，以允许在 KMS 服务器和 Veritas Access 群集之间进行通信。

有关详细信息，请参见 `system_kms` 手册页。

7

使用响应文件自动运行 Veritas Access 安装和配置

本章节包括下列主题：

关于响应文件

安装程序脚本在任何安装、配置、升级或卸载过程中均会生成响应文件。响应文件包含您在该过程中输入的配置信息。过程完成之后，安装脚本将显示响应文件的位置。

通过使用 `-responsefile` 选项调用安装脚本，可以将响应文件用于未来安装过程。响应文件会将参数传递给脚本，以便自动执行安装或卸载。

请参见第 142 页的“安装脚本选项”。

执行静默 Veritas Access 安装

静默安装和配置会使用您准备的响应文件，在不提示的情况下安装 Veritas Access 软件。如果要在大量节点上安装 Veritas Access 软件，此功能很有用。

在执行静默 Veritas Access 安装和配置之前，必须手动在两个节点之间配置安全 shell (ssh) 通信。

请参见第 144 页的“手动配置无密码安全外壳 (ssh)”。

您可以从 ISO 映像的根目录获取 Veritas Access 示例响应文件。

使用 Veritas Access 静默安装功能

- 输入以下命令：

```
# ./installaccess -responsefile access.responsefile
```

生成 access.response 示例文件

1 安装和配置 Veritas Access 软件且不出现任何错误。

2 从日志目录中获取 `access.response` 示例文件。

使用 access.response 示例文件

1 将 Veritas Access 示例响应文件重命名为 `access.responsefile`。

2 根据配置需要修改此文件，例如更改群集名称、IP 地址范围和其他参数。

安装时间可能因您的配置而异。

请参见第 59 页的“在群集上安装和配置 Veritas Access 软件”。

用于安装和配置 Veritas Access 的响应文件变量

表 7-1 列出了在安装和配置 Veritas Access 时可以定义的响应文件变量。

表 7-1 用于安装 Veritas Access 的响应文件变量

变量	说明
CFG{bondmode}{bond<n>}	定义 BOND 的绑定模式。 列表或标量：列表 可选或必需：可选
CFG{bondname}	BOND 的绑定名称列表。 列表或标量：列表 可选或必需：可选
CFG{config_majority_based_fencing}	启用多数防护。该值为 `1`。它不能与 I/O 防护变量“fencing_scsi3_disk_policy”、“fencing_newdg_disks”和“fencing_dgname”一起使用。 列表或标量：标量 可选或必需：对于基于多数的防护为必需

变量	说明
CFG{fencing_dgname}	指定 I/O 防护的磁盘组。该值为 `sfscoorddg`。 列表或标量：标量 可选或必需：对于 I/O 防护为必需
CFG{fencing_newdg_disks}	定义防护磁盘。 列表或标量：列表 可选或必需：对于 I/O 防护为必需
CFG{fencing_option}	指定 I/O 防护配置模式。对于基于磁盘的 I/O 防护，该值为 `2`。 列表或标量：标量 可选或必需：对于 I/O 防护为必需
CFG{fencing_scsi3_disk_policy}	指定要使用 I/O 防护的 SCSI-3 磁盘策略。该值为 `dmp`。 列表或标量：标量 可选或必需：对于 I/O 防护为必需
CFG{fencingenabled}	定义是否启用防护。如果启用，该值为 `1`。 列表或标量：标量 可选或必需：对于 I/O 防护为必需
CFG{opt}{licensefile}	指定 Veritas 永久或订购许可证密钥文件的位置。 列表或标量：标量 可选或必需：必需
CFG{keys}{"node_ip"}	为每个节点指定 Veritas Access 许可证。 列表或标量：标量 可选或必需：必需
CFG{newnodes}	为群集节点指定新的访问 IP。该值应当为每个节点的第一个公用 IP 地址。 列表或标量：列表 可选或必需：必需

变量	说明
CFG{opt}{comcleanup}	清理在配置后由安装程序添加的SSH连接。该值为 1。 列表或标量：标量 可选或必需：必需
CFG{opt}{confignic}	使用所有网络变量值执行NIC配置。该值为 1。 列表或标量：标量 可选或必需：必需
CFG{opt}{configure}	如果已安装软件包，则执行配置。 列表或标量：标量 可选或必需：必需
CFG{opt}{install}	安装 Veritas Access RPMs。以后可使用 -configure 选项执行配置。 列表或标量：标量 可选或必需：可选
CFG{opt}{installallpkgs}	指示安装程序使用此变量并将其值设置为 1 来安装所有 Veritas Access RPMs。 列表或标量：标量 可选或必需：必需
CFG{opt}{noipc}	禁用连接到SORT以执行更新检查。该值为 0。 列表或标量：标量 可选或必需：必需
CFG{opt}{ssh}	确定是否要使用 ssh 在系统之间进行通信。如果启用，该值为 1。 列表或标量：标量 可选或必需：必需
CFG{prod}	定义要安装或卸载的产品。 列表或标量：标量 可选或必需：必需

变量	说明
CFG{publicnetmaskarr}	分配给公用 NIC 或绑定的网络掩码列表。 列表或标量：列表 可选或必需：必需
CFG{publicparr}	分配给公用 NIC 或绑定的公用 IP 列表。 列表或标量：列表 可选或必需：必需
CFG{redhat_subscription_username}	指定用于注册 Red Hat 订购管理的用户名称。 列表或标量：标量 可选或必需：如果系统上缺少某些必需的操作系统 RPM，则为必需 如果用户名包含任何特殊字符，则应使用单引号括起来（例如：'1234@abc'）。
CFG{redhat_subscription_password}	指定用于注册 Red Hat 订购管理的密码。 列表或标量：标量 可选或必需：如果系统上缺少某些必需的操作系统 RPM，则为必需 如果密码包含任何特殊字符，则应使用单引号括起来（例如：'1234@abc'）。
CFG{snas_clustername}	定义产品的群集名称。 列表或标量：标量 可选或必需：必需
CFG{snas_consoleip}	定义产品的控制台 IP。 列表或标量：标量 可选或必需：必需
CFG{snas_defgateway}	定义产品的网关。 列表或标量：标量 可选或必需：必需
CFG{snas_dnsdomainname}	定义产品的 DNS 域名。 列表或标量：标量 可选或必需：必需

变量	说明
CFG{snas_dnsip}	定义产品的 DNS IP。 列表或标量：标量 可选或必需：必需
CFG{snas_ntpserver}	定义产品的 NTP 服务器名称。 列表或标量：标量 可选或必需：必需
CFG{snas_nvip}	定义每个 NIC 上的 VIP 数。 列表或标量：标量 可选或必需：必需
CFG{snas_pipprefix}	定义公用 IP 的前缀（仅限 IPv6 环境）。 列表或标量：标量 可选或必需：必需
CFG{snas_pipstart}	定义公用 IP 的初始 IP。 列表或标量：标量 可选或必需：必需
CFG{snas_pnmaskstart}	定义公用 IP 的网络掩码（仅限 IPv4 环境）。 列表或标量：标量 可选或必需：必需
CFG{snas_sepconsoleport}	定义是否使用单独的控制台端口。1 表示是，0 表示否。 列表或标量：标量 可选或必需：必需
CFG{snas_vipprefix}	定义虚拟 IP 的前缀（仅限 IPv6 环境）。 列表或标量：标量 可选或必需：必需
CFG{snas_vipstart}	定义虚拟 IP 的初始 IP。 列表或标量：标量 可选或必需：必需

变量	说明
CFG{snas_vnmaskstart}	定义虚拟 IP 的网络掩码（仅限 IPv4 环境）。 列表或标量：标量 可选或必需：必需
CFG{systems}	要在其中安装或卸载本产品的系统列表。 列表或标量：列表 可选或必需：必需
CFG{vcs_allowcomms}	指示用户需要设置单节点群集时是启动 LLT 还是 GAB。 列表或标量：标量 可选或必需：必需
CFG{vcs_clusterid}	使用字符串编号定义唯一群集 ID。 列表或标量：标量 可选或必需：必需
CFG{vcs_lltlink<n>}{"new_node_ip"}	定义第一个心跳链路的 NIC 名称。 列表或标量：标量 可选或必需：必需
CFG{vcs_userenpw}	定义加密的用户密码。 列表或标量：标量 可选或必需：必需
CFG{vcs_username}	定义为 VCS 添加的用户名。 列表或标量：标量 可选或必需：必需
CFG{vcs_userpriv}	定义用户权限。 列表或标量：标量 可选或必需：必需
CFG{virtualiparr}	要分配给公用 NIC 或绑定的虚拟 IP 列表。 列表或标量：列表 可选或必需：必需

变量	说明
CFG{virtualnetmaskarr}	要分配给公用NIC或绑定的网络掩码列表。 列表或标量：列表 可选或必需：必需

Veritas Access 安装和配置的响应文件示例

以下示例显示用于安装和配置 Veritas Access 的响应文件。

```
##########################################################
our %CFG;
#Installs Product packages.
$CFG{opt}{install}=1;
$CFG{opt}{installallpkgs}=1;
$CFG{opt}{comsetup}=1;
$CFG{opt}{noipc}=1;
$CFG{opt}{ssh}=1;
$CFG{prod}="SNAS73";
$CFG{opt}{licensefile}="<absolute_path_of_licfile>";

#Performs the configuration if the packages are already installed
$CFG{opt}{configure}=1;

#the PCI IDs of slave NICs
$CFG{bondpool}{bond0}=[ qw(0000:02:09.0 0000:02:07.0) ];
$CFG{bondpool}{bond1}=[ qw(0000:02:04.0 0000:02:08.0) ];

#mode of each bond
$CFG{bondmode}{bond0}=5;
$CFG{bondmode}{bond1}=6;

#names of bond
$CFG{bondname}=[ qw(bond0 bond1) ];

#the PCI IDs of excluded NICs
$CFG{exclusion}=[ qw(0000:02:03.0 0000:02:0a.0) ];

#the PCI IDs of all the bonded NICs
$CFG{publicbond}=[ qw(0000:02:03.0 0000:02:04.0 0000:02:07.0
0000:02:08.0) ];
```

```
#public IPs
$CFG{publiciparr}=[ qw(10.200.58.100 10.200.58.101 10.200.58.102
10.200.58.103 10.200.58.104 10.200.58.105 10.200.58.106 10.200.58.107)
 ];

#netmask for public IPs
$CFG{publicnetmaskarr}=[ qw(192.168.30.10 192.168.30.11 192.168.30.12

192.168.30.13 192.168.30.14 192.168.30.15 192.168.30.16 192.168.30.17)
 ];

#the user name to register with Red Hat subscription management
$CFG{redhat_subscription_username}="rhel_user";

#the password to register with Red Hat subscription management
$CFG{redhat_subscription_password}="rhel_password";

#clustername of SNAS
$CFG{snas_clustername}="testsnas";

#console IP of SNAS
$CFG{snas_consoleip}="192.168.30.40";

#default gateway of SNAS
$CFG{snas_defgateway}="192.168.30.1";

#domain name of DNS
$CFG{snas_dnsdomainname}="cdc.veritas.com";

#IP of DNS
$CFG{snas_dnsip}="192.168.30.2";

#NTP server name
$CFG{snas_ntpserver}="ntp.veritas.com";

#number of VIPs on each NIC
$CFG{snas_nvip}=1;

#netmask of public IPs(only ipv4 environment)
$CFG{snas_pnmaskstart}=255.255.255.0;

#the initial IP of public IPs
$CFG{snas_pipstart}="192.168.30.10";
```

```
#if use separate console port, 1 for yes, 0 for no
$CFG{snas_sepconsoleport}="0";

#netmask of virutal IPs(only ipv4 environment)
$CFG{snas_vnmaskstart}=255.255.255.0;

#the initial IP of virtual IPs
$CFG{snas_vipstart}="192.168.30.18";

#virtual IPs
$CFG{virtualiparr}=[ qw(192.168.30.18 192.168.30.19 192.168.30.20
 192.168.30.21 192.168.30.22 192.168.30.23 192.168.30.24
192.168.30.25) ];

#netmask for virual IPs
$CFG{virtualnetmaskarr}=[ qw(255.255.255.0 255.255.255.0 255.255.255.0

255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0)
 ];

#target systems
$CFG{systems}=[ qw(192.168.30.80 192.168.30.81) ];

#indicates whether to start llt/gab when user wants to setup a single
node cluster
$CFG{vcs_allowcomms}=1;

#define the unique cluser id with a string number
$CFG{vcs_clusterid}=325;

#define the cluster name with a string
$CFG{vcs_clustername}="testsnas";

#define the nic name for the first heartbeat link.
$CFG{vcs_lltlink1}{"192.168.30.10"}="priveth0";
$CFG{vcs_lltlink1}{"192.168.30.13"}="priveth0";
$CFG{vcs_lltlink2}{"192.168.30.10"}="priveth1";
$CFG{vcs_lltlink2}{"192.168.30.13"}="priveth1";

#define the encrypted user password
$CFG{vcs_userenpw}=[ qw(GPQiPKpMQlQQoYQkPN) ];
```

```
#define the added username for VCS
$CFG{vcs_username}=[ qw(admin) ];

#define the user privilege
$CFG{vcs_userpriv}=[ qw(Administrators) ];

1;
##################################################
```

8

显示和添加群集节点

本章节包括下列主题：

关于 Veritas Access 安装状态和条件

表 8-1 介绍了 Veritas Access 安装状态。

表 8-1 Veritas Access 安装状态

安装状态	说明
RUNNING	节点是群集的一部分，且正在运行 Veritas Access 进程。
FAULTED	节点已关闭且/或未运行 Veritas Access 进程。
LEAVING	节点正在正常脱离群集
EXITED	节点已正常退出群集
UNKNOWN	无法确定节点的确切状态

根据表 8-2 中所述的群集条件，`Cluster> show` 命令的输出会有所不同。

表 8-2 群集条件和状态

条件	说明
节点已配置且是群集的一部分，但该节点已经关机。	状态显示为 FAULTED，且没有安装状态或网络统计信息。
节点已配置且是群集的一部分，但该节点物理实体已经从群集中移除。	状态显示为 FAULTED，且没有安装状态或网络统计信息。
节点已配置且是群集的一部分，但已使用 `Cluster> shutdown` 命令将其关闭。	状态从 LEAVING 改为 EXITED。
节点已配置且是群集的一部分，并且您使用 `Cluster> del` 命令。	已从群集中删除节点，且关于已删除节点的信息不再可用。

显示群集中的节点

可以显示过去 15 分钟内群集中的所有节点及其状态、CPU 负载和网络负载。

如果使用 `Cluster> show currentload` 选项，则可显示从现在到下一 5 秒之内收集的 CPU 和网络负载。

显示群集中的节点列表

1 要显示属于群集的节点列表以及可添加到群集的系统，请输入以下命令：

Cluster> show

命令输出包括以下信息。请参见下面的示例。

节点	如果节点已添加到群集，则显示节点名称。如果节点仍在添加到群集的过程中，则显示节点的 IP 地址。
	示例：
	`node_01`
	或
	`192.168.30.10`

状态	显示节点的状态或系统的安装状态及系统 IP 地址（如果已安装系统）。 请参见第 113 页的"关于 Veritas Access 安装状态和条件"。
CPU	指示 CPU 负载。
pubethX	指示公用接口 X 的网络负载。
bondX	指示绑定 NIC X 的网络负载。

2 对于群集中已存在的节点，将显示以下内容：

```
Node     State     CPU(15 min) pubeth0(15 min)    pubeth1(15 min)

                         %       rx(MB/s) tx(MB/s)   rx(MB/s)
tx(MB/s)
------   -------   ----------- -------- --------  --------
--------
snas_01  RUNNING     1.35        0.00     0.00       0.00      0.00
snas_02  RUNNING     1.96        0.00     0.00       0.00      0.00
```

3 对于正在群集中添加/删除的节点以及正在升级的节点，将显示以下进度：

```
Nodes in Transition

Node/IP           Operation       State      Description
------            ---------       -----      -----------
192.168.30.11     Add node        FAILED     Installing packages
snas_03           Delete node     ONGOING    Removing node
snas_01,snas_02   Rolling upgrade ONGOING    Rolling upgrade
phase 2
```

注意： `add node` 和 `delete node` 操作不能同时执行。

4 要显示从现在到下 5 秒之内收集的 CPU 和网络负载，请输入以下命令：

```
Cluster> show currentload
```

输出示例：

```
Node       State    CPU(5 sec)   pubeth0(5 sec)    pubeth1(5 sec)

                        %       rx(MB/s) tx(MB/s)  rx(MB/s)
tx(MB/s)
----       -----    ----------  -------- --------  --------
--------
snas_01    RUNNING    0.26       0.01     0.00      0.01     0.00
snas_02    RUNNING    0.87       0.01     0.00      0.01     0.00
snas_03    RUNNING    10.78      27.83    12.54     0.01     0.00
```

对于群集节点上的每个可用公用接口，将显示网络接口的统计信息。

在群集中添加新节点之前

安装操作系统之后，可以一次安装和配置多个节点 Veritas Access 群集。如果在这之后要将其他节点添加到群集，则需完成以下步骤：

- 在这些要另外添加的节点上安装适当的操作系统软件。
  请参见第 56 页的“在群集的每个节点上安装操作系统”。
- 在新节点上禁用 SELinux。
- 添加这些其他节点之前，无需在节点上安装 Veritas Access 软件。系统会在添加节点时安装 Veritas Access 软件。如果已安装 Veritas Access 软件，则会卸

载，然后再安装该产品（与群集版本相同）。之所以卸载并稍后安装该产品，其原因在于确保新节点与其他群集节点具有完全相同的版本和修补程序级别（如有）。软件包存储在群集节点中，因此在添加新节点期间，无需该产品映像。

- 验证现有群集是否已为新节点提供足够的物理 IP 地址。可以使用 CLISH 命令添加其他 IP 地址：

  Network> **ip addr add command**

  例如：

```
Network> ip addr add 192.168.30.107 255.255.252.0 physical
ACCESS ip addr SUCCESS V-288-1031 ip addr add successful.

Network> ip addr show
IP             Netmask/Prefix  Device  Node       Type     Status
--             --------------  ------  ----       ----     ------
192.168.30.10 255.255.252.0   pubeth0 snas_01    Physical
192.168.30.11 255.255.252.0   pubeth1 snas_01    Physical
192.168.30.12 255.255.252.0   pubeth0 snas_02    Physical
192.168.30.13 255.255.252.0   pubeth1 snas_02    Physical
192.168.30.14 255.255.252.0           ( unused ) Physical
192.168.30.15 255.255.252.0           ( unused ) Physical
192.168.30.16 255.255.252.0   pubeth0 snas_01    Virtual  ONLINE (Con IP)
192.168.30.17 255.255.252.0   pubeth1 snas_01    Virtual  ONLINE
192.168.30.18 255.255.252.0   pubeth1 snas_01    Virtual  ONLINE
192.168.30.19 255.255.252.0   pubeth1 snas_01    Virtual
```

  在此示例中，未使用的 IP 地址 192.168.30.14 和 192.168.30.15 可供新节点用作物理 IP 地址。

注意：新节点上的网络配置应与群集节点的网络配置相同，即，NIC 应具有相同的名称和连接。

如果尚不存在绑定和 VLAN，系统会自动创建它们以匹配群集配置。

- 将节点添加到现有群集中。
  请参见第 117 页的“将节点添加到群集”。

将节点添加到群集

必须先在节点上安装操作系统，然后才能将节点添加到群集。

如果使用基于磁盘的防护，协调器磁盘必须在新添加的节点上可见，这是成功配置 I/O 防护的先决条件。如果没有协调器磁盘，I/O 防护将不会正常加载且此节点将无法获得群集成员资格。

如果使用基于多数的防护，新添加的节点不必具有共享磁盘。

如果要添加新的节点并排除某些唯一 PCI ID，请手动将唯一 PCI ID 添加到每个群集节点上的 `/opt/VRTSsnas/conf/net_exclusion_dev.conf` 文件中。例如：

```
[root@bob_01 ~]# cat /opt/VRTSsnas/conf/net_exclusion_dev.conf
0000:42:00.0 0000:42:00.1
```

注意：只有双节点群集支持写回缓存，因此将节点添加到双节点群集会将缓存更改为只读。

新添加的节点应具有相同的 InfiniBand NIC 配置。

如果您的群集配置了 FSS 池，而池的节点组缺少节点，则新添加的节点将添加到 FSS 节点组中。安装程序会将新节点的本地数据磁盘添加到 FSS 池中。

将新的节点添加到群集

1 使用 `master` 或 `system-admin` 帐户登录 Veritas Access。

2 在 CLISH 中，输入 `Cluster` 命令以进入 `Cluster>` 模式。

3 要将新的节点添加到群集中，请输入以下内容：

```
Cluster> add node1ip, node2ip.....
```

其中 *node1ip,node2ip,....* 是用于 SSH 连接的其他节点的 IP 地址列表。

请务必注意：

- 节点 IP 会保留，额外所需的 IP 将从（未使用的）物理 IP 池中分配。
- 新节点的物理 IP 是从已配置的公用 IP 起始地址开始，所能够找到的可用 IP。
- 虚拟 IP 会通过重新平衡分配到新的节点，但不会再分配其他额外的虚拟 IP。
  添加节点后，转到步骤 6 以将新的虚拟 IP 地址添加到群集。
- 应提供新节点可访问的 IP。
- 新节点可访问的 IP 应位于公用网络中，它们应该能够成功对公用网络的网关执行 ping 操作。

例如：

```
Cluster> add 192.168.30.10
```

注意：当启用写回缓存时，无法将节点添加到双节点群集。在添加节点之前，请将缓存模式更改为读取，然后重试。

4 如果原始群集上存在缓存，则装入 CFS 后，安装程序会提示您选择 SSD 磁盘以在新节点上创建缓存。

```
1) emc_clariion1_242
2) emc_clariion1_243
b) Back to previous menu
Choose disks separate by spaces to create cache on 192.168.30.11
[1-2,b,q] 1
Create cache on snas_02 .....................Done
```

5 如果群集节点已创建FSS池，并且新节点上的本地数据磁盘数超过两个，则安装程序将要求您选择要添加到FSS池的磁盘。请确保至少选择两个磁盘用于条带卷布局。所选磁盘的总大小应不小于 FSS 池的容量大小。

```
Following storage pools need to add disk from the new node:
     1)  fsspool1
     2)  fsspool2
     3)  Skip this step

Choose a pool to add disks [1-3,q] 1
     1)  emc_clariion0_1570 (5.000 GB)
     2)  installres_03_sdc (5.000 GB)
     3)  installres_03_sde (5.000 GB)
     4)  sdd (5.000 GB)
     b)  Back to previous menu


Choose at least 2 local disks with minimum capacity of 10 GB [1-4,b,q] 2 4
Format disk installres_03_sdc,sdd ............................... Done

The disk name changed to installres_03_sdc,installres_03_sdd
    Add disk installres_03_sdc,installres_03_sdd to storage pool fsspool1  Done
```

6 如果需要，请将虚拟 IP 地址添加到群集。添加节点时不会将新的虚拟 IP 地址或服务组添加到群集。

要添加其他虚拟 IP 地址，请在 Network 模式下使用以下命令：

```
Network> ip addr add ipaddr virtual
```

例如：

```
Network> ip addr add 192.168.30.14 255.255.252.0 virtual

ACCESS ip addr SUCCESS V-288-1031 ip addr add successful.
```

如果将节点添加到群集时出现问题（例如，节点暂时断开网络连接），请执行以下操作以修复此问题：

要恢复节点，请执行以下操作：

- 关闭节点电源。
- 使用 `Cluster> del nodename` 命令从群集中删除节点。
- 打开节点电源。
- 使用 `Cluster> add nodeip` 命令将节点添加到群集。

从群集中删除节点

此命令将从群集中删除节点。请使用 `Cluster> show` 命令中显示的节点名称。

注意：单节点群集不支持此命令。

如果已删除的节点在删除前处于 RUNNING 状态，则重新引导节点后，此节点会分配给原始 IP 地址，可以使用该地址将节点重新添加到群集。节点的原始 IP 地址是该节点添加到群集之前使用的 IP 地址。

如果群集已配置 FSS 池，且删除节点后会导致 FSS 池的节点组中仅剩一个节点，则不能使用安装程序删除节点。

从已启用写回缓存的双节点群集中删除节点时，缓存将更改为只读。只有双节点才支持写回缓存。

节点在从群集删除之前使用的 IP 地址仍可访问，直到您执行重新启动操作为止。

从群集中删除节点后，在执行重新启动操作时，将还原旧的 IP 配置。因此，请务必从 Veritas Access 中删除已删除节点的已使用 IP，反之亦然。

从群集中删除节点

1 要显示群集中所有节点的当前状态，请输入以下内容：

```
Cluster> show
```

2 要从群集中删除节点，请输入以下内容：

```
Cluster> del nodename
```

其中，*nodename* 为 `Cluster> show` 命令中的列表显示的节点名称。无法通过 IP 地址指定节点。

例如：

```
Cluster> del snas_01
```

3 从群集中删除节点后，其使用过的物理 IP 地址将标记为未使用的物理 IP 地址。如果添加新的节点，则新节点可使用该 IP 地址。已删除的节点所使用的虚拟 IP 地址不会被移除。删除节点后，会将删除的节点上的虚拟 IP 地址移动到群集中其余的节点上。

例如：

```
Network> ip addr show
IP             Netmask/Prefix  Device     Node            Type     Status
--             --------------  ------     ----            ----     ------
192.168.30.10 255.255.252.0   pubeth0    source_30a_01   Physical
192.168.30.11 255.255.252.0   pubeth1    source_30a_01   Physical
192.168.30.12 255.255.252.0              ( unused )      Physical
192.168.30.13 255.255.252.0              ( unused )      Physical
192.168.30.14 255.255.252.0   pubeth0    source_30a_01   Virtual  ONLINE (Con IP)
192.168.30.15 255.255.252.0   pubeth0    source_30a_01   Virtual  ONLINE
192.168.30.16 255.255.252.0   pubeth0    source_30a_01   Virtual  ONLINE
192.168.30.17 255.255.252.0   pubeth1    source_30a_01   Virtual  ONLINE
192.168.30.18 255.255.252.0   pubeth1    source_30a_01   Virtual  ONLINE
```

如果不打算使用这些物理或虚拟 IP 地址，可使用以下命令将其移除：

```
Network> ip addr del ipaddr
```

例如：

```
Network> ip addr del 192.168.30.18
ACCESS ip addr SUCCESS V-288-1031 ip addr del successful.
```

注意：如果群集已配置 NIC 绑定，则还需要删除交换机上已删除节点的配置。

关闭群集节点

可关闭群集中的单个节点或所有节点。请使用 `Cluster> show` 命令中显示的节点名称。

关闭群集中的一个节点或所有节点

1 要关闭某个节点，请输入以下内容：

```
Cluster> shutdown nodename
```

nodename 表示要关闭的节点的名称。无法通过 IP 地址指定节点。

例如：

```
Cluster> shutdown snas_04
Stopping Cluster processes on snas_04
Sent shutdown command to snas_04. SSH sessions to
snas_04 may terminate.
```

2 要关闭群集中的所有节点，请输入以下内容：

```
Cluster> shutdown all
```

使用 `all` 作为 *nodename* 来关闭群集中的所有节点。

例如：

```
Cluster> shutdown all
Stopping Cluster processes on all
SSH sessions to all nodes may terminate.
Sent shutdown command to snas_02
Sent shutdown command to snas_03
Sent shutdown command to snas_04
Sent shutdown command to snas_01
```

9

升级 Veritas Access和操作系统

本章节包括下列主题：

升级操作系统和 Veritas Access

在 RHEL 上，Veritas Access 支持按以下升级路径升级。

表 9-1 RHEL 上的升级支持的升级路径

升级前的产品版本	升级前的操作系统版本	升级后的操作系统版本	升级后的产品版本
7.3.0.1	RHEL 7 Update 3	RHEL 7 Update 4	7.4
7.3.1	RHEL 7 Update 3	RHEL 7 Update 4	7.4

升级操作系统和 Veritas Access 包括以下步骤：

- 升级前步骤（仅适用于配置了 LTR 的 Veritas Access 群集）
- 使用 Veritas Access 提供的脚本导出 Veritas Access 配置
- 复制配置文件
- 安装 RHEL 7.3 或 7.4
- 安装 Veritas Access 7.4
- 导入 Veritas Access 配置
- 验证导入的 Veritas Access 配置
- 升级后步骤（仅适用于配置了 LTR 的 Veritas Access 群集）

升级前步骤（仅适用于配置了 LTR **的** Veritas Access **群集）**

注意：在 Veritas Access 群集上配置 OpenDedup 卷时，需要执行这些步骤。

1 确保 NetBackup 中的备份或还原作业已停止。

2 如果从 7.3.0.1 升级，则将 `upgrade_scripts/odd_config_export_va7301.py` 脚本从 ISO 复制到管理控制台节点上的 `/`。

如果从 7.3.1 升级，则将 `upgrade_scripts/odd_config_export_va731.py` 脚本从 ISO 复制到管理控制台节点上的 `/`。

3 执行相应的脚本以导出 OpenDedup 配置：

对于 7.3.0.1：`python odd_config_export_va7301.py [filename]`

对于 7.3.1：`python odd_config_export_va731.py [filename]`

注意：如果未提供任何文件名，则使用默认配置文件名 `odd_config.exp`。

导出 Veritas Access **配置**

1 **先决条件：**

安装 RHEL 7.3 版本。

安装了 Veritas Access 7.3.0.1 或 7.3.1 版本。

确保已使用 CLISH 停止与 Veritas Access 相关的所有 I/O 和服务，例如 CIFS、NFS、FTP 等。

使用 `hastop -all` 命令停止所有服务。

2 从 ISO，将 `upgrade_scripts/config_export` 目录复制到管理控制台服务组处于联机状态的群集节点上的 `/`。

3 以 `root` 用户身份从该目录登录 Shell（终端），然后运行以下命令，导出 Veritas Access 配置：

```
/bin/bash -f export_lib.sh export local <filename>
```

验证 Veritas Access **配置导出**

- 在 CLISH 上运行以下命令，查看可用的配置列表：

  ```
  system config list
  ```

  配置文件位于以下位置：

  ```
  /opt/VRTSnas/conf/backup
  ```

  注意：您需要将这些配置文件存储在群集节点之外的节点上，以避免对文件造成任何损坏。

安装 RHEL 7.4

1 **先决条件：**

确保停止 CLISH 上所有正在运行的模块且未运行 I/O。

安装 RHEL 7.4 之前，在 CLISH 上运行 `network ip addr show` 命令和 `cluster show` 命令。记下这些 IP 地址和群集节点名称。确保在安装 RHEL 7.4 后安装 Veritas Access 群集时，使用相同的 IP 地址和群集名称。

示例：

```
upgrade> network ip addr show

IP              Netmask/Prefix  Device     Node            Type     Status
--              --------------  ------     ----            ----     ------
192.168.10.151 255.255.255.0   pubeth0    upgrade_01      Physical
192.168.10.158 255.255.255.0   pubeth1    upgrade_01      Physical
192.168.10.152 255.255.255.0   pubeth0    upgrade_02      Physical
192.168.10.159 255.255.255.0   pubeth1    upgrade_02      Physical
192.168.10.174 255.255.255.0   pubeth0    upgrade_01      Virtual  ONLINE (Con IP)
192.168.10.160 255.255.255.0   pubeth0    upgrade_01      Virtual  ONLINE
192.168.10.161 255.255.255.0   pubeth1    upgrade_01      Virtual  ONLINE

upgrade> cluster show

Node            State      CPU(15 min)    pubeth0(15 min)      pubeth1(15 min)
                                 %        rx(MB/s) tx(MB/s)    rx(MB/s) tx(MB/s)
----            -----      -----------    -------- --------    -------- --------
upgrade_01      RUNNING          11.52       0.67     0.06        0.60     0.00
upgrade_02      RUNNING           4.19       0.61     0.05        0.60     0.00
```

注意：在此示例中，群集名称为 `upgrade`，群集节点名称为 `upgrade_01` 和 `upgrade_02`。

2 重新启动群集的所有节点。

3 在所需节点上安装 RHEL 7.4。

请参见第 57 页的"在目标 Veritas Access 群集上安装操作系统"。

注意：建议选择安装了 RHEL 7.3 的相同磁盘进行安装。请确保未选择任何其他磁盘，因为这些磁盘可能是池的一部分，并可能会导致数据丢失。

安装 Veritas Access 7.4

- 重新启动后，节点启动时，开始通过 CPI 安装 Veritas Access 7.4。

注意：确保使用与 RHEL 7.3 上的 Veritas Access 安装所用的相同 IP 地址和群集名称。

请参见第 59 页的"在目标群集节点上安装 Veritas Access"。

验证 Veritas Access **安装**

1 通过使用控制台 IP，检查是否可以访问 CLISH。

2 在 CLISH 中运行以下命令，查看磁盘是否可以访问：

```
storage disk list
```

注意：如果磁盘在 CLISH 输出中不可见，请在 CLISH 中运行 `storage scanbus force` 命令。

---

3 在 CLISH 中运行以下命令，查看池是否可以访问：

```
storage pool list
```

注意：如果池在 CLISH 输出中不可见，请在 CLISH 中运行 `storage scanbus force` 命令。

---

4 在 CLISH 中运行以下命令，查看文件系统是否可以访问：

```
storage fs list
```

注意：如果文件系统在 CLISH 输出中不可见，请在 CLISH 中运行 `storage scanbus force` 命令。

---

5 确保文件系统处于联机状态。如果文件系统未处于联机状态，需要在 CLISH 中运行以下命令使其联机：

```
storage fs online <fs name>
```

导入 Veritas Access **配置**

1 **先决条件：**

确保文件系统处于联机状态。如果文件系统未处于联机状态，需要在CLISH中运行以下命令使其联机：

```
storage fs online <fs name>
```

注意：确保群集使用与 RHEL 7.3 上的 Veritas Access 安装所用的相同 IP 地址和群集名称。

如果在安装期间未添加 VIP 地址（用于 RHEL 7.3 上的 Veritas Access），请在 RHEL 7.4 上安装 Veritas Access 之后通过 CLISH 添加，然后再导入配置。

2 将导出的配置文件复制到群集节点中的以下位置：

```
/opt/VRTSnas/conf/backup/
```

3 在 CLISH 上运行以下命令，查看可用的导出配置：

```
system config list
```

4 登录到 CLISH 并使用以下命令导入模块配置：

```
system config import local <config-filename> <module-to-import>
```

可以导入以下模块：

```
upgrade> system config import local

system config import local <file_name> [config-type]
 -- Import the configuration which is stored locally

file_name     : configuration file name
config-type   : input type of configuration to import (network/admin/all/report/
system/support/cluster_specific/all_except_cluster_specific/nfs/cifs/ftp/backup/
replication/storage_schedules/storage_quota/storage_fs_alert/storage_fs_policy/
compress_schedules/defrag_schedules/storage_dedup/smartio/target/object_access/
loadbalance/opendedup) [all]

upgrade> system config import local
```

注意：模块名称是在 CLISH 中自动生成的。

升级后步骤（仅适用于配置了 LTR **的** Veritas Access **群集）**

注意：在 Veritas Access 群集上配置 OpenDedup 卷时，除了以上步骤外，还需要执行这些步骤。

1 启用或启动 ObjectAccess 服务使用的所需身份验证服务（AD、LDAP 或 NIS）。

2 如果是从 Veritas Access 7.3.0.1 升级，请为 ObjectAccess 设置池，并按如下所示启用 ObjectAccess。

```
Cluster1> objectaccess set pools pool1
ACCESS ObjectAccess INFO V-493-10-0 Set pools successful. Please make
sure the storage is provisioned as per the requirements of the layout.
Cluster1> objectaccess server enable
100% [********************] Enabling ObjectAccess server.
ACCESS ObjectAccess SUCCESS V-493-10-4 ObjectAccess server enabled.
```

3 使用以下命令启动 ObjectAccess 服务：

```
cluster2> objectaccess server start
ACCESS ObjectAccess SUCCESS V-493-10-4 ObjectAccess started successfully.
```

4 使用以下命令导入 OpenDedup 配置。

```
cluster2> system config import remote <file location> opendedup
```

注意：您导入的 OpenDedup 配置是您通过执行“升级前步骤（仅适用于配置了 LTR 的 Veritas Access 群集）”一节中提供的步骤导出的配置。

5 使用以下命令使所有 OpenDedup 卷脱机：

```
cluster2> opendedup volume offline <vol-name>
```

6 按如下所示更新所有 OpenDedup `config.xml` 文件：

```
"/etc/sdfs/<vol-name>-volume-cfg.xml
```

通过向 **<extended-config>** 标记添加以下参数：

```
dist-layout="false"
```

注意：不应将此参数用于现有 OpenDedup 卷，因为它们可能具有采用默认布局的现有数据。如果使用现有 OpenDedup 卷，则可能会导致数据损坏。

---

7 使用以下命令使所有 OpenDedup 卷联机：

```
cluster2> opendedup volume online <vol-name>
```

10

使用滚动升级来升级 Veritas Access

本章节包括下列主题：

关于滚动升级

此版本的 Veritas Access 支持从 Veritas Access 7.3.0.1 及更高版本滚动升级。RHEL 7.3 和 7.4 支持滚动升级。

滚动升级通过将升级时间限制为其执行服务组故障转移所需的时间量，从而最大限度地减少高可用性群集的服务和应用程序停机时间。可以在一个群集中运行产品版本不同的节点。

滚动升级有两个主要阶段。安装程序在第 1 阶段升级内核 RPMs，在第 2 阶段升级 VCS 代理 RPMs。应分别在每个节点上逐个执行升级。需要先在每个从属节点上执行升级，然后在主节点上执行升级。升级过程会停止正在升级的节点上的所有服务和资源。所有服务（包括 VIP 组）会故障转移到群集中的其他节点之一。在故障转移过程中，连接到节点的 VIP 组的客户端会间歇性中断。对于未超时的客户端，正在升级的节点上的 VIP 组联机后，服务即会恢复。

在第一个节点上运行升级过程时，群集中的其他节点继续为客户端提供服务。在升级第一个节点后，它会重新启动第一阶段节点上的服务和资源。在第一个节点恢复运行后，升级过程将停止下一个从属节点上的服务和资源，依次类推。所有服务和资源均处于联机状态，并为客户端提供服务。同时，滚动升级在其余节点上启动升级过程。在其余节点上完成升级后，群集恢复，服务在整个群集中进行平衡。

滚动升级工作流程

滚动升级包括两个主要阶段：第 1 阶段，安装程序升级内核 RPMs；第 2 阶段，安装程序升级与 VCS 代理相关的非内核 RPMs。

1. 在开始滚动升级之前禁用防护。
2. 在每个节点上逐个执行升级过程。
3. 在第 1 阶段，先在从属节点上执行升级过程。升级过程会停止节点上的所有服务，并将服务组故障转移到群集中的另一个节点。
4. 在故障转移过程中，连接到节点的 VIP 组的客户端会间歇性中断。对于未超时的客户端，服务将在其中一个节点上的 VIP 组联机后恢复。
5. 在第 1 阶段，安装程序在该节点上升级内核 RPMs，其他节点继续为客户端提供服务。
6. 在第一个从属节点上完成第 1 阶段后，将在第二个从属节点上开始升级，依次类推。在升级从属节点后，将升级主节点。主节点中的所有服务组将故障转移到另一个节点。
7. 在第一个节点上成功完成第 1 阶段后，需要检查恢复任务是否也已完成，然后在下一个节点上开始执行升级的第 1 阶段。

   注意：请确保升级后的节点未脱离群集。如果该节点已脱离群集，请等待该节点加入现有群集。

8. 在滚动升级的第 2 阶段期间，同时升级群集所有节点上的其余所有 RPMs。VCS 和 VCS 代理软件包将会升级。内核驱动程序将升级到新协议版本。在第 2 阶段期间，应用程序保持联机。High Availability Daemon (HAD) 停止并重新启动。

请参见第 134 页的“使用安装程序执行滚动升级”。

请参见第 133 页的“RHEL 和 Oracle Linux 上的升级支持的滚动升级路径”。

RHEL 和 Oracle Linux 上的升级支持的滚动升级路径

表 10-1 RHEL 和 Oracle Linux 上的升级支持的升级路径

升级前的产品版本	操作系统版本	升级后的产品版本
7.3.0.1	RHEL 7 Update 3 和 4	7.4
7.3.1	RHEL 7 Update 3 和 4 OL 7 Update 3 和 4	7.4

注意：开始对此表中未显示的其他产品版本执行滚动升级之前，请参见《Veritas Access 版本说明》中的“已知问题”部分。

请参见第 134 页的“使用安装程序执行滚动升级”。

请参见第 132 页的“关于滚动升级”。

使用安装程序执行滚动升级

在开始滚动升级前，请确保群集的所有节点上均在运行 Cluster Server (VCS)。

停止所有不受 VCS 控制的 VxVM 卷的所有活动。例如，停止访问这些卷的任何应用程序（如数据库），并卸载在这些卷上创建的任何文件系统。然后，停止所有卷。

卸载所有不受 VCS 控制的 VxFS 文件系统。

执行滚动升级

1 对于配置了 LTR 的 Veritas Access 群集，请确保 NetBackup 中的备份或还原作业已停止。

2 滚动升级的第 1 阶段将从第二个子群集开始。在第二个子群集上完成准备步骤。

卸载所有不受 VCS 控制的 VxFS 文件系统：

```
# umount mount_point
```

3 如有需要，完成操作系统更新。

确保 Veritas Access 的现有版本支持您所应用的操作系统更新。如果现有的 Veritas Access 版本不支持此操作系统更新，请先将 Veritas Access 升级至支持此操作系统更新的版本。

有关说明，请参见 Red Hat Enterprise Linux (RHEL) 操作系统文档。

将应用程序切换到其余子群集并升级第一个子群集的操作系统。

操作系统完成更新后，节点将重新启动。

4 如果缓存区域处于联机状态，您必须先使该缓存区域脱机，然后再升级 VxVM RPMs。使用以下命令可以使缓存区域脱机：

```
# sfcache offline cachename
```

5 在执行滚动升级之前，使用 `storage fencing off` 命令禁用防护。

6 以超级用户身份登录并装入 Veritas Access 7.4 安装介质。

7 从根目录，启动安装程序。

```
# ./installaccess -rolling_upgrade
```

8 安装程序将检查系统通信、版本兼容性和版本信息，并列出群集名称、ID 和群集节点。安装程序将询问是否允许继续执行滚动升级。

```
Would you like to perform rolling upgrade on the cluster? [y,n,q]
 (y)
```

键入 **y** 继续执行操作。

9 滚动升级的第 1 阶段开始。一次必须在一个节点上执行第 1 阶段。安装程序将要求提供系统名称。

输入要对其执行滚动升级的系统名称（用空格分隔）：[q?]

输入要对其执行滚动升级的其中一个从属节点的名称或 IP 地址。

10 安装程序将对群集中的节点进一步执行预检，并且可能会显示警告。您可以键入 **y** 继续，或者退出安装程序并解决预检的警告。

11 如果引导磁盘已封装并镜像，则可创建备份引导磁盘。

如果选择创建备份引导磁盘，请键入 **y**。提供引导磁盘组的备份名称或接受默认名称。然后，安装程序创建引导磁盘组的备份副本。

12 安装程序检测到联机服务组后，安装程序会提示用户执行以下操作之一：

- 手动切换服务组
- 使用 CPI 自动切换服务组

停机时间是指服务组故障转移所需的时间。

注意：Veritas 建议手动切换服务组。自动切换服务组无法解决依赖性问题。

13 安装程序提示您停止适用的进程。键入 **y** 继续执行操作。

安装程序会将所有服务组转移到目前未升级的节点中。安装程序在要升级的节点上停止并行服务组。

安装程序停止所有相关进程、卸载旧内核 RPMs 并安装新 RPMs。

14 安装程序执行升级配置，并启动相关进程。如果在升级之前封装引导磁盘，则安装程序会提示您在执行升级配置后重新启动节点。

15 在尚未升级的节点上完成准备步骤。

在所有节点上卸载所有不受 VCS 控制的 VxFS 文件系统。

```
# umount mount_point
```

16 如果不需要更新操作系统，则跳过此步骤。

转到步骤 4。

否则，在尚未升级的节点上完成操作系统更新。有关说明，请参见 Red Hat Enterprise Linux (RHEL) 操作系统文档。

对每个节点重复步骤 4 至 14。

17 至此，滚动升级的第 1 阶段在第一个节点上完成。您可以在下一个从属节点上开始执行升级的第 1 阶段。安装程序将再次要求提供系统名称。

在下一个节点上开始执行升级的第 1 阶段之前，需要检查是否正在执行恢复任务。等待几分钟，以便恢复任务开始执行。

在主节点上，输入以下命令：

```
# vxtask list

Check if following keywords are present:
ECREBUILD/ATCOPY/ATCPY/PLXATT/VXRECOVER/RESYNC/RECOV
```

如果正在执行任何恢复任务，请等待该任务完成，然后在下一个节点上开始执行升级的第 1 阶段。

18 在该节点上完成升级的第 1 阶段后，请确保该节点未脱离群集。

输入 `# vxclustadm nidmap` 命令。

如果升级后的节点已脱离群集，请先等待该节点加入群集，然后在下一个节点上开始执行升级的第 1 阶段。

19 在其余节点上将所有缓存区域设置为脱机状态：

```
# sfcache offline cachename
```

安装程序将要求提供要对其执行升级的节点名称。

20 输入要对其执行滚动升级的系统名称（用空格分隔）：[q,?]。

键入群集节点名称或 **q** 退出。

安装程序重复步骤 9 至步骤 14。

对于具有大量节点的群集，此过程可能会重复多次。为支持此升级，服务组会关闭然后再启动。

21 完成滚动升级的第 1 阶段后，手动装入所有不受 VCS 控制的 VxFS 文件系统。开始该升级的第 2 阶段。升级的第 2 阶段包括 VCS 引擎 (HAD) 的停机时间，但不包括应用程序停机时间。键入 **y** 继续执行操作。此时将开始滚动升级的第 2 阶段。

22 安装程序确定要升级的其余 RPMs。按 **y** 继续执行操作。

23 安装程序停止 Cluster Server (VCS) 进程，但应用程序将继续运行。键入 **y** 继续执行操作。

安装程序执行预停、卸载旧 RPMs 并安装新 RPMs。它会执行安装后任务和升级配置。

24 如果您可通过网络连接到 Internet，安装程序将检查是否有更新。

如果发现更新，您可在此时应用这些更新。

25 验证群集的状态：

```
# hastatus -sum
```

26 仅适用于配置了 LTR 的 Veritas Access 群集的升级后步骤：

使用以下命令使所有 OpenDedup 卷脱机：

```
cluster2> opendedup volume offline <vol-name>
```

按如下所示更新所有 OpenDedup `config.xml` 文件：

```
"/etc/sdfs/<vol-name>-volume-cfg.xml
```

通过向 <extended-config> 标记添加以下参数：

```
dist-layout="false"
```

注意：不应将此参数用于现有 OpenDedup 卷，因为它们可能具有采用默认布局的现有数据。如果使用现有 OpenDedup 卷，则可能会导致数据损坏。

使用以下命令使所有 OpenDedup 卷联机：

```
cluster2> opendedup volume online <vol-name>
```

请参见第 133 页的"RHEL 和 Oracle Linux 上的升级支持的滚动升级路径"。

请参见第 132 页的"关于滚动升级"。

11

卸载 Veritas Access

本章节包括下列主题：

- 卸载 Veritas Access 之前
- 使用安装程序卸载 Veritas Access

卸载 Veritas Access 之前

卸载 Veritas Access 之前，请执行以下步骤：

- 从群集内的任何节点（但并非所有节点）中移除 Veritas Access 之前，请确保已从正在运行的群集中删除该节点。可以使用 `Cluster> show` 命令查看群集节点状态，然后使用 `Cluster> delete` 命令从 Veritas Access 群集中删除正在运行的节点。
  有关 `Cluster> show` 和 `Cluster> delete` 命令的详细信息，请参见相关手册页。
- 停止所有通过 NFS、CIFS 或 FTP 访问文件系统的应用程序。
- 销毁群集中的所有复制作业。
  使用 `Replication> job show` 命令列出群集上的所有复制作业。

```
Replication> job show
Job Name Role Job Type Encryption Debug Schedule
======== ====== ======== ========== ===== ========
job1 SOURCE DATA OFF ON sch1
State CKPT Count Exclunit Source repunit Target repunit(s)
======== ========== ======== ============== =================
ENABLED 1 -- scr1 trg1
Link name(s)
============
link1
```

使用 Replication> job destroy 命令销毁复制作业。

```
Replication> job destroy job1
ACCESS replication SUCCESS V-288-0 Removing bandwidth limit on the

link: link1
ACCESS replication SUCCESS V-288-0 Job 'job1' disabled
successfully.
ACCESS replication SUCCESS V-288-0 Job 'job1' deleted successfully.
```

- 使用适当的 CLISH 命令停止 NFS、CIFS、FTP、GUI 和群集上的复制服务。

```
CLISH> cifs server stop
Stopping CIFS Server.....Success.
CLISH>
CLISH> nfs server stop
Success.
CLISH>
CLISH> ftp server stop
Success.
CLISH>
CLISH.Support> gui server stop
GUI service is OFFLINE.
CLISH>
CLISH> replication service stop
ACCESS replication SUCCESS V-288-0 Replication service stopped
CLISH>
```

- 运行以下命令以停止 AMF：

```
# /etc/init.d/amf stop
Stopping AMF...
AMF: Module unloaded
```

- 运行以下命令并等待几分钟：

```
# /opt/VRTS/bin/hastop -all
```

- 运行以下命令并验证您仅看到端口 a 和端口 b：

```
# gabconfig -a
GAB Port Memberships
===================================
```

```
Port a gen 7f2d0a membership 01
Port b gen 7f2d09 membership 01
```

使用安装程序卸载 Veritas Access

您可以卸载 Veritas Access。Veritas Access 卸载程序允许您卸载 Veritas Access，而无需重新安装操作系统。此外，您也可以在 Veritas Access 安装未完成的情况下使用卸载程序。

使用卸载程序同时卸载群集中所有节点上的 Veritas Access 之前，请确保节点之间存在通信。默认情况下，Veritas Access 群集节点可以使用 ssh 相互通信。

如果节点无法相互通信，则必须在群集中的每个节点上运行卸载程序。卸载程序将移除所有 Veritas Access RPMs。

删除 Veritas Access 7.4 RPM

在卸载过程中，卸载程序将停止当前正在运行的 Veritas Access 进程。

卸载 Veritas Access 7.4RPM

1 从要卸载 Veritas Access 的节点中以 support 用户身份登录。

2 启动卸载程序。

```
# cd /opt/VRTS/install

# ./uninstallaccess
```

程序将指定创建日志的目录。程序将显示群集的版权声明和说明。

3 输入要从中卸载 Veritas Access 的节点的 IP 地址。

程序将执行节点验证检查，并要求停止所有正在运行的 Veritas Access 进程。

4 输入 **y** 将停止所有 Veritas Access 进程。

程序将停止 Veritas Access 进程并卸载软件。

卸载程序将执行以下任务：

- 验证节点之间的通信。
- 检查每个节点上的安装，确定要卸载的 RPM。
- 卸载内核模块并移除 RPM。

在卸载程序停止进程时查看输出。

您可以记下移除所有 RPM 之后卸载程序创建的摘要、响应和日志文件的位置。

通过 Veritas Access 7.4 光盘进行卸载

出现以下任一情况时，您可能需要使用 Veritas Access 7.4 光盘上的卸载程序：

- 安装未完成之后，需要卸载 Veritas Access。
- 卸载程序在 `/opt/VRTS/install` 中不可用。

如果将安装介质装入到 `/mnt`，请通过更改目录访问卸载程序。

cd /mnt/

./uninstallaccess

附录 A

安装参考

本附录包括下列主题：

- 安装脚本选项

安装脚本选项

表 A-1 列出了 Veritas Access 安装脚本的可用命令行选项。对于初次安装或升级，通常不需要这些选项。

表 A-1 可用的命令行选项

命令行选项	功能
-configure	安装之后配置未配置的产品。
-install	在系统上安装本产品。
-precheck	安装产品之前，执行检查确认系统已满足产品安装要求。
-license	在指定的系统上注册或更新产品许可证。
-licensefile	指定 Veritas 永久或订购许可证密钥文件的位置。
-requirements	显示安装产品所需的操作系统版本、所需的修补程序、文件系统空间和其他系统要求。
-responsefile *response_file*	不提示输入信息，而是使用文件中存储的信息执行自动安装或卸载。*response_file* 是包含配置定义的文件的完整路径。

命令行选项	功能
-rolling_upgrade	执行滚动升级。通过使用此选项，安装程序自动检测群集系统上的滚动升级状态，而不需要显式指定滚动升级的第 1 阶段或第 2 阶段。
-prestop_script *prestop_script*	在升级过程中停止进程之前，执行用户在每台主机上提供的定制脚本。
-poststart_script *poststart_script*	在升级过程中开始进程之后，执行用户在每个主机上提供的定制脚本。
-uninstall	从系统中卸载本产品。
-updateparameter	更新正在运行的群集的网络参数。

附录 B

配置安全 Shell 进行通信

本附录包括下列主题：

- 手动配置无密码安全外壳 (ssh)
- 使用 pwdutil.pl 实用程序设置 ssh 和 rsh 连接

手动配置无密码安全外壳 (ssh)

安全外壳 (Secure Shell, ssh) 程序支持登录远程系统并执行命令。ssh 支持两个不可信的主机之间通过不安全的网络进行加密通信和身份验证过程。

在此过程中，必须先创建 DSA 密钥对。通过该密钥对，公钥将从源系统附加到目标系统上的 `authorized_keys` 文件。

创建 DSA 密钥对

1 在源系统 (sys1) 上，以 ***root*** 身份登录并导航到根目录。

```
sys1 # cd /root
```

2 要在源系统上生成 DSA 密钥对，请键入以下命令：

```
sys1 # ssh-keygen -t dsa
```

将显示类似以下内容的系统输出：

```
Generating public/private dsa key pair.
Enter file in which to save the key (/root/.ssh/id_dsa):
```

3 按 Enter 接受默认位置 `/root/.ssh/id_dsa`。

4 当程序要求输入通行短语时，请按 Enter 键两次。

```
Enter passphrase (empty for no passphrase):
```

请勿输入通行短语。按 Enter。

```
Enter same passphrase again:
```

再次按 Enter。

5 将显示类似以下行的输出：

```
Your identification has been saved in /root/.ssh/id_dsa.
Your public key has been saved in /root/.ssh/id_dsa.pub.
The key fingerprint is:
1f:00:e0:c2:9b:4e:29:b4:0b:6e:08:f8:50:de:48:d2 root@sys1
```

使用安全文件传输将公钥从源系统附加到目标系统上的 authorized_keys **文件**

1 从源系统 (sys1) 中，将公钥移动到目标系统 (sys2) 上的临时文件。

使用安全文件传输程序。

在此示例中，根目录中的文件名 `id_dsa.pub` 是公钥的临时文件名称。

使用以下命令进行安全文件传输：

```
sys1 # sftp sys2
```

如果是首次在此系统上设置安全文件传输，则将显示类似以下行的输出：

```
Connecting to sys2 ...
The authenticity of host 'sys2 (10.182.00.00)'
can't be established. DSA key fingerprint is
fb:6f:9f:61:91:9d:44:6b:87:86:ef:68:a6:fd:88:7d.
Are you sure you want to continue connecting (yes/no)?
```

2 输入 `yes`。

将显示类似以下内容的输出：

```
Warning: Permanently added 'sys2,10.182.00.00'
(DSA) to the list of known hosts.
root@sys2 password:
```

3 输入 sys2 的 root 密码。

4 在 `sftp` 提示符下，键入以下命令：

```
sftp> put /root/.ssh/id_dsa.pub
```

将显示以下输出：

```
Uploading /root/.ssh/id_dsa.pub to /root/id_dsa.pub
```

5 要退出 SFTP 会话，请键入以下命令：

```
sftp> quit
```

6 将 `id_dsa.pub` 密钥添加到目标系统上的 `authorized_keys` 文件。要在目标系统（在此示例中是 sys2）上开始 `ssh` 会话，请在 sys1 上键入以下命令：

```
sys1 # ssh sys2
```

在系统提示时输入 sys2 的 root 密码：

```
password:
```

在 sys2 上键入以下命令：

```
sys2 # cat /root/id_dsa.pub >> /root/.ssh/authorized_keys
sys2 # rm  /root/id_dsa.pub
```

7 在源安装系统上运行以下命令。如果 ssh 会话已过期或终止，则也可运行这些命令来重续会话。这些命令会将私钥引入 shell 环境，使该密钥全面供 *root* 用户使用。

```
sys1 # exec /usr/bin/ssh-agent $SHELL
sys1 # ssh-add

Identity added: /root/.ssh/id_dsa
```

该 shell 特定的步骤仅在 shell 处于活动状态时有效。如果在会话期间关闭 shell，则必须再次执行上述步骤。

验证是否可以连接到目标系统

1 在源系统 (sys1) 上，输入以下命令：

```
sys1 # ssh -l root sys2 uname -a
```

其中 sys2 是目标系统的名称。

2 该命令应当从源系统 (sys1) 到目标系统 (sys2) 执行，而无需系统请求提供通行短语或密码。

3 对每个目标系统重复此过程。

使用 pwdutil.pl 实用程序设置 ssh 和 rsh 连接

密码实用程序 pwdutil.pl 已捆绑在 7.3 版本中的 /opt/VRTS/repository/ga/images/SSNAS/7.3.0.0/scripts/pwdutil.pl 目录下。用户可以在脚本中运行该实用程序，从而自动设置 ssh 和 rsh 连接。

```
# ./pwdutil.pl -h
Usage:

Command syntax with simple format:

    pwdutil.pl check|configure|unconfigure ssh|rsh <hostname|IP addr>

     [<user>] [<password>] [<port>]

Command syntax with advanced format:

     pwdutil.pl [--action|-a 'check|configure|unconfigure']
                [--type|-t 'ssh|rsh']
                [--user|-u  '<user>']
                [--password|-p '<password>']
                [--port|-P '<port>']
                [--hostfile|-f '<hostfile>']
                [--keyfile|-k '<keyfile>']
                [-debug|-d]
                <host_URI>

     pwdutil.pl -h | -?
```

表 B-1 pwdutil.pl 实用程序的选项

选项	用法
--action|-a 'check|configure|unconfigure'	指定操作类型，默认为“check”。
--type|-t 'ssh|rsh'	指定连接类型，默认为“ssh”。
--user|-u '<user>'	指定用户 ID，默认为本地用户 ID。
--password|-p '<password>'	指定用户密码，默认为用户 ID。
--port|-P '<port>'	指定 ssh 连接的端口号，默认为 22。
--keyfile|-k '<keyfile>'	指定私钥文件。
--hostfile|-f '<hostfile>'	指定列出主机的文件。
-debug	打印调试信息。
-h|-?	打印帮助消息。
<host_URI>	可以为下列格式： <主机名> <用户>:<密码>@<主机名> <用户>:<密码>@<主机名>: <端口>

可以使用 `pwdutil.pl` 实用程序检查、配置和取消配置 ssh 或 rsh。例如：

- 检查 ssh 连接是否仅用于一台主机：

  pwdutil.pl check ssh hostname

- 仅为一台主机配置 ssh：

  pwdutil.pl configure ssh hostname user password

- 仅为一台主机取消配置 rsh：

  pwdutil.pl unconfigure rsh hostname

- 为多台具有相同用户 ID 和密码的主机配置 ssh：

  pwdutil.pl -a configure -t ssh -u user -p password hostname1 hostname2 hostname3

- 为多台具有不同用户 ID 和密码的不同主机配置 ssh 或 rsh：

  pwdutil.pl -a configure -t ssh user1:password1@hostname1 user2:password2@hostname2

- 为多台具有一个配置文件的主机检查或配置 ssh 或 rsh：

  pwdutil.pl -a configure -t ssh --hostfile /tmp/sshrsh_hostfile

- 要使主机配置文件保密，可以使用第三方实用程序对主机文件进行密码加密和解密。
  例如：

```
### run openssl to encrypt the host file in base64 format
# openssl aes-256-cbc -a -salt -in /hostfile -out /hostfile.enc
enter aes-256-cbc encryption password: <password>
Verifying - enter aes-256-cbc encryption password: <password>

### remove the original plain text file
# rm /hostfile

### run openssl to decrypt the encrypted host file
# pwdutil.pl -a configure -t ssh `openssl aes-256-cbc -d -a
-in /hostfile.enc`
enter aes-256-cbc decryption password: <password>
```

- 要使用未位于默认 $HOME/.ssh 目录下的 ssh 身份验证密钥，可以使用 --keyfile 选项来指定 ssh 密钥。例如：

```
### create a directory to host the key pairs:
# mkdir /keystore

### generate private and public key pair under the directory:
# ssh-keygen -t rsa -f /keystore/id_rsa

### setup ssh connection with the new generated key pair under
the directory:
# pwdutil.pl -a configure -t ssh --keyfile /keystore/id_rsa
user:password@hostname
```

可以使用以下命令查看配置文件的内容：

```
# cat /tmp/sshrsh_hostfile
user1:password1@hostname1
```

```
user2:password2@hostname2
user3:password3@hostname3
user4:password4@hostname4

# all default: check ssh connection with local user
hostname5
The following exit values are returned:

0     Successful completion.
1     Command syntax error.
2     Ssh or rsh binaries do not exist.
3     Ssh or rsh service is down on the remote machine.
4     Ssh or rsh command execution is denied due to password is
required.
5     Invalid password is provided.
255   Other unknown error.
```

附录 C

手动部署 Veritas Access

本附录包括下列主题：

在非 SSH 环境中的双节点群集上手动部署 Veritas Access

本节介绍在禁用了 SSH 通信时部署双节点 Veritas Access 群集的手动步骤。

先决条件

- 假定有一个双节点群集。
- 支持的操作系统版本为 RHEL 7.4。
- 假定 Veritas Access 映像位于本地系统中的 `/access_build_dir/rhel7_x86_64/` 位置。
- 群集的名称为 *clus*，群集节点的名称为 *clus_01* 和 *clus_02*。群集名称对所有节点都应该是唯一的。
- 在所有节点上停止 SSH 服务。
- 假定公用 NIC 为 pubeth0 和 pubeth1，专用 NIC 为 priveth0 和 priveth1。NIC 名称在所有节点中均应保持一致。公用 NIC 名称和专用 NIC 名称在所有节点中均应相同。
- 将 `172.16.0.3` 用作 *clus_01* 的专用 IP 地址，将 `172.16.0.4` 用作 *clus_02* 的专用 IP 地址。

在双节点群集上手动部署 Veritas Access

1 将 Veritas Access 映像复制到所需群集的所有节点上。

2 在所有节点上停止 SSH 后台驻留程序。

```
# systemctl stop sshd
```

3 验证是否安装了以下 RPM。如果没有，请从 RHEL 存储库安装 RPM。

```
bash-4.2.46-28.el7.x86_64
lsscsi-0.27-6.el7.x86_64
initscripts-9.49.39-1.el7.x86_64
iproute-3.10.0-87.el7.x86_64
kmod-20-15.el7.x86_64
coreutils-8.22-18.el7.x86_64
binutils-2.25.1-31.base.el7.x86_64
python-requests-2.6.0-1.el7_1.noarch
python-urllib3-1.10.2-3.el7.noarch
```

4 安装所需的操作系统 RPM。

- 创建 `repo` 文件。

  cat /etc/yum.repos.d/os.repo

  ```
  [veritas-access-os-rpms]
  name=Veritas Access OS RPMS
  baseurl=file:///access_build_dir/rhel7_x86_64/os_rpms/
  enabled=1
  gpgcheck=0
  ```

- 运行以下命令：

  ```
  # yum updateinfo
  ```

- 运行以下命令：

  ```
  # cd /access_build_dir/rhel7_x86_64/os_rpms/
  ```

- 在运行以下命令之前，请确保系统中没有任何 RHEL 订购。`yum repolist` 应仅指向 `veritas-access-os-rpms`。

 # /usr/bin/yum -y install --setopt=protected_multilib=false perl-5.16.3-292.el7.x86_64.rpm nmap-ncat-6.40-7.el7.x86_64.rpm perl-LDAP-0.56-5.el7.noarch.rpm perl-Convert-ASN1-0.26-4.el7.noarch.rpm

net-snmp-5.7.2-28.el7_4.1.x86_64.rpm
net-snmp-utils-5.7.2-28.el7_4.1.x86_64.rpm
openldap-2.4.44-5.el7.x86_64.rpm nss-pam-ldapd-0.8.13-8.el7.x86_64.rpm
rrdtool-1.4.8-9.el7.x86_64.rpm wireshark-1.10.14-14.el7.x86_64.rpm
vsftpd-3.0.2-22.el7.x86_64.rpm openssl-1.0.2k-12.el7.x86_64.rpm
openssl-devel-1.0.2k-12.el7.x86_64.rpm
iscsi-initiator-utils-6.2.0.874-4.el7.x86_64.rpm
libpcap-1.5.3-9.el7.x86_64.rpm libtirpc-0.2.4-0.10.el7.x86_64.rpm
nfs-utils-1.3.0-0.48.el7_4.2.x86_64.rpm
kernel-debuginfo-common-x86_64-3.10.0-693.el7.x86_64.rpm
kernel-debuginfo-3.10.0-693.el7.x86_64.rpm
kernel-headers-3.10.0-693.el7.x86_64.rpm
krb5-devel-1.15.1-8.el7.x86_64.rpm
krb5-libs-1.15.1-8.el7.x86_64.rpm
krb5-workstation-1.15.1-8.el7.x86_64.rpm
perl-JSON-2.59-2.el7.noarch.rpm telnet-0.17-64.el7.x86_64.rpm
apr-devel-1.4.8-3.el7_4.1.x86_64.rpm
apr-util-devel-1.5.2-6.el7.x86_64.rpm
glibc-common-2.17-196.el7_4.2.x86_64.rpm
glibc-headers-2.17-196.el7_4.2.x86_64.rpm
glibc-2.17-196.el7_4.2.x86_64.rpm glibc-2.17-196.el7_4.2.i686.rpm
glibc-devel-2.17-196.el7_4.2.x86_64.rpm
glibc-utils-2.17-196.el7_4.2.x86_64.rpm
nscd-2.17-196.el7_4.2.x86_64.rpm sysstat-10.1.5-12.el7.x86_64.rpm
libibverbs-utils-13-7.el7.x86_64.rpm libibumad-13-7.el7.x86_64.rpm
opensm-3.3.19-1.el7.x86_64.rpm opensm-libs-3.3.19-1.el7.x86_64.rpm
infiniband-diags-1.6.7-1.el7.x86_64.rpm
sg3_utils-libs-1.37-12.el7.x86_64.rpm sg3_utils-1.37-12.el7.x86_64.rpm
libyaml-0.1.4-11.el7_0.x86_64.rpm
memcached-1.4.15-10.el7_3.1.x86_64.rpm
python-memcached-1.59-1.noarch.rpm
python-paramiko-2.1.1-4.el7.noarch.rpm
python-backports-1.0-8.el7.x86_64.rpm
python-backports-ssl_match_hostname-3.4.0.2-4.el7.noarch.rpm
python-chardet-2.2.1-1.el7_1.noarch.rpm
python-six-1.9.0-2.el7.noarch.rpm
python-setuptools-0.9.8-7.el7.noarch.rpm
python-ipaddress-1.0.16-2.el7.noarch.rpm
targetcli-2.1.fb46-1.el7.noarch.rpm

fuse-2.9.2-8.el7.x86_64.rpm fuse-devel-2.9.2-8.el7.x86_64.rpm
fuse-libs-2.9.2-8.el7.x86_64.rpm PyYAML-3.10-11.el7.x86_64.rpm
arptables-0.0.4-8.el7.x86_64.rpm ipvsadm-1.27-7.el7.x86_64.rpm
ntpdate-4.2.6p5-25.el7_3.2.x86_64.rpm ntp-4.2.6p5-25.el7_3.2.x86_64.rpm
autogen-libopts-5.18-5.el7.x86_64.rpm ethtool-4.8-1.el7.x86_64.rpm
net-tools-2.0-0.22.20131004git.el7.x86_64.rpm
cups-libs-1.6.3-29.el7.x86_64.rpm avahi-libs-0.6.31-17.el7.x86_64.rpm
psmisc-22.20-15.el7.x86_64.rpm strace-4.12-4.el7.x86_64.rpm
vim-enhanced-7.4.160-2.el7.x86_64.rpm at-3.1.13-22.el7_4.2.x86_64.rpm
rsh-0.17-76.el7_1.1.x86_64.rpm unzip-6.0-16.el7.x86_64.rpm
zip-3.0-11.el7.x86_64.rpm bzip2-1.0.6-13.el7.x86_64.rpm
mlocate-0.26-6.el7.x86_64.rpm lshw-B.02.18-7.el7.x86_64.rpm
jansson-2.10-1.el7.x86_64.rpm ypbind-1.37.1-9.el7.x86_64.rpm
yp-tools-2.14-5.el7.x86_64.rpm perl-Net-Telnet-3.03-19.el7.noarch.rpm
tzdata-java-2018d-1.el7.noarch.rpm
perl-XML-Parser-2.41-10.el7.x86_64.rpm
lsof-4.87-4.el7.x86_64.rpm cairo-1.14.8-2.el7.x86_64.rpm
pango-1.40.4-1.el7.x86_64.rpm libjpeg-turbo-1.2.90-5.el7.x86_64.rpm
sos-3.4-13.el7_4.noarch.rpm traceroute-2.0.22-2.el7.x86_64.rpm
openldap-clients-2.4.44-5.el7.x86_64.rpm

5 安装第三方 RPM：

```
# cd /access_build_dir/rhel7_x86_64/ third_party _rpms/
# /bin/rpm -U -v --oldpackage --nodeps --replacefiles --replacepkgs
ctdb-4.6.6-1.el7.x86_64.rpm
perl-Template-Toolkit-2.24-5.el7.x86_64.rpm
perl-Template-Extract-0.41-1.noarch.rpm
perl-AppConfig-1.66-20.el7.noarch.rpm
perl-File-HomeDir-1.00-4.el7.noarch.rpm
samba-common-4.6.6-1.el7.x86_64.rpm
samba-common-libs-4.6.6-1.el7.x86_64.rpm
samba-client-4.6.6-1.el7.x86_64.rpm
samba-client-libs-4.6.6-1.el7.x86_64.rpm
samba-4.6.6-1.el7.x86_64.rpm
samba-winbind-4.6.6-1.el7.x86_64.rpm
samba-winbind-clients-4.6.6-1.el7.x86_64.rpm
samba-winbind-krb5-locator-4.6.6-1.el7.x86_64.rpm
libsmbclient-4.6.6-1.el7.x86_64.rpm
samba-krb5-printing-4.6.6-1.el7.x86_64.rpm
samba-libs-4.6.6-1.el7.x86_64.rpm
libwbclient-4.6.6-1.el7.x86_64.rpm
samba-winbind-modules-4.6.6-1.el7.x86_64.rpm
libnet-1.1.6-7.el7.x86_64.rpm lmdb-libs-0.9.13-2.el7.x86_64.rpm
nfs-ganesha-2.2.0-0.el7.x86_64.rpm
nfs-ganesha-vxfs-2.2.0-0.el7.x86_64.rpm gevent-1.0.2-1.x86_64.rpm
python-msgpack-0.4.6-1.el7ost.x86_64.rpm
python-flask-0.10.1-4.el7.noarch.rpm
python-itsdangerous-0.23-2.el7.noarch.rpm
libevent-libs-2.0.22-1.el7.x86_64.rpm
python-werkzeug-0.9.1-2.el7.noarch.rpm
python-jinja2-2.7.2-2.el7.noarch.rpm sdfs-7.4.0.0-1.x86_64.rpm
psutil-4.3.0-1.x86_64.rpm
python-crontab-2.2.4-1.noarch.rpm libuv-1.9.1-1.el7.x86_64.rpm
```

在此命令中，可以基于 `/access_build_dir/rhel7_x86_64/ third_party _rpms/` 目录中的 RPM 更新 RPM 版本。

6 安装 Veritas Access RPM。

- 运行以下命令：

```
# cd /access_build_dir/rhel7_x86_64/rpms/repodata/
# cat access73.repo > /etc/yum.repos.d/access73.repo
```

- 在 yum 存储库目录的 `/etc/yum.repos.d/access73.repo` 中更新 *baseurl* 和 *gpgkey* 条目。
  - `baseurl=file:///access_build_dir/rhel7_x86_64/rpms/`
  - `gpgkey=file:///access_build_dir/rhel7_x86_64/rpms/RPM-GPG-KEY-veritas-access7`
- 运行以下命令以刷新 yum 存储库。
  - `# yum repolist`
  - `# yum grouplist`
- 运行以下命令。

  `# yum -y groupinstall ACCESS73`
- 运行以下命令。

  `# /opt/VRTS/install/bin/add_install_scripts`

7 安装 Veritas NetBackup 客户端软件。

```
# cd /access_build_dir/rhel7_x86_64
# /opt/VRTSnas/install/image_install/netbackup/install_netbackup.pl
/access_build_dir/rhel7_x86_64/netbackup
```

8 为 Veritas Access 创建软链接。运行以下命令。

```
# /opt/VRTSnas/pysnas/install/install_tasks.py
all_rpms_installed parallel
```

9 对产品进行授权许可。

- 注册永久 VLIC 密钥。

  `# /opt/VRTSvlic/bin/vxlicinstupgrade -k <Key>`
- 验证是否正确安装了 VLIC 密钥：

```
# /opt/VRTSvlic/bin/vxlicrep
```

- 注册 SLIC 密钥文件：

```
# /opt/VRTSslic/bin/vxlicinstupgrade -k $keyfile
```

- 验证是否正确安装了 SLIC 密钥：

```
# /opt/VRTSslic/bin/vxlicrep
```

10 备份以下文件：

- /etc/sysconfig/network
- /etc/sysconfig/network-scripts/ifcfg-*
- /etc/resolv.conf

11 配置专用 NIC：

```
# cd /etc/sysconfig/network-scripts/
```

- 配置第一个专用 NIC。
  - 运行以下命令。

```
# ip link set down priveth0
```

  - 在 ifcfg-priveth0 文件中更新以下条目：

```
DEVICE=priveth0
NAME=priveth0
BOOTPROTO=none
TYPE=Ethernet
ONBOOT=yes
```

  - 在 ifcfg-priveth0 文件中添加以下条目。

```
HWADDR=<MAC address>
IPADDR= 172.16.0.3  (use IPADDR= 172.16.0.4 for second node)
NETMASK=<netmask>
NM_CONTROLLED=no
```

例如：

```
HWADDR=00:0c:29:0c:8d:69
IPADDR=172.16.0.3
```

```
NETMASK=255.255.248.0
NM_CONTROLLED=no
```

- 运行以下命令。

  # **ip link set up priveth0**

- 配置第二个专用 NIC。
  您可以采用相同方式配置第二个专用 NIC。对第二个节点使用 priveth1（而不是 priveth0）。不需要为 priveth1 提供 IPADDR。

12 配置公用 NIC。

cd /etc/sysconfig/network-scripts/

- 配置第二个公用 NIC pubeth1（还没有为其配置主机 IP）。
  - 运行以下命令：

    # **ip link set down pubeth1**

  - 在 ifcfg-pubeth1 文件中更新以下条目：

    ```
    DEVICE=pubeth1
    NAME=pubeth1
    TYPE=Ethernet
    BOOTPROTO=none
    ONBOOT=yes
    ```

  - 在 ifcfg-pubeth1 文件中添加以下条目。

    ```
    HWADDR=<MAC address>
    IPADDR=<pubeth1_pub_ip>
    NETMASK=<netmask>
    NM_CONTROLLED=no
    ```

  - 运行以下命令。

    # **ip link set up pubeth1**

- 配置第一个公用 NIC pubeth0。
  - 由于第一个公用 NIC 将会关闭，请确保您直接从其控制台访问系统。
  - 运行以下命令：

    # **ip link set down pubeth0**

- 在 ifcfg-pubeth0 文件中更新以下条目：

  ```
  DEVICE=pubeth0
  NAME=pubeth0
  TYPE=Ethernet
  BOOTPROTO=none
  ONBOOT=yes
  ```

- 在 ifcfg-pubeth0 文件中添加以下条目。

  ```
  HWADDR=<MAC address>
  IPADDR=<pubeth0_pub_ip>
  NETMASK=<netmask>
  NM_CONTROLLED=no
  ```

- 运行以下命令。

  ```
  # ip link set up pubeth0
  ```

- 验证 pubeth1 是否已关闭。如果已关闭，则使其联机。

  ```
  # ip link set up pubeth1
  ```

- 对变更内容进行验证。

  ```
  # ip a
  ```

- 运行以下命令。

  ```
  # service network restart
  ```

  如果启动 sshd 服务，应能够通过 SSH 连接上述 IP。

13 配置 DNS。

通过添加以下条目来更新 /etc/resolv.conf 文件：

```
nameserver <DNS>
domain <master node name>
```

例如：

```
nameserver 10.182.128.134
domain clus_01
```

14 配置网关。

更新 /etc/sysconfig/network 文件。

```
GATEWAY=$gateway
NOZEROCONF=yes
```

15 更新 configfileTemplate 文件。

- 输入以下命令：

  # **cd /access_build_dir/rhel7_x86_64/manual_install/network**

- 使用当前系统详细信息更新 configfileTemplate 文件：
  - 对主节点使用 *master* 模式，对其他节点使用 *slave* 模式。
  - 配置实用程序脚本使用此模板文件来创建配置文件。
  - 在 *old_hostname* 和 *new_hostname* 中提供相同名称（当前主机名）。

16 生成网络配置文件。

- 名为 configNetworkHelper.pl 的配置实用程序脚本可创建所需的配置文件。

  # **cd /access_build_dir/rhel7_x86_64/manual_install/network**
  # **chmod +x configNetworkHelper.pl**

- 运行该配置实用程序脚本。

  # **./configNetworkHelper.pl -f configfileTemplate**

- # **cat /opt/VRTSnas/scripts/net/network_options.conf > /opt/VRTSnas/conf/network_options.conf**

- # **sed -i -e '$a\' /opt/VRTSnas/conf/net_console_ip.conf**

- 更新 /etc/hosts 文件。

  # **echo "172.16.0.3 <master hostname>" >> /etc/hosts**
  # **echo "172.16.0.4 <slave node name>" >> /etc/hosts**

  例如：

  # **echo "172.16.0.3 clus_01" >> /etc/hosts**
  # **echo "172.16.0.4 clus_02" >> /etc/hosts**

17 创建 S3 配置文件。

```
# cat /opt/VRTSnas/conf/ssnas.yml
ObjectAccess:
  config: {admin_port: 8144, s3_port: 8143, server_enable: 'no',

  ssl: 'no'}
  defaults:
    fs_blksize: '8192'
    fs_encrypt: 'off'
    fs_nmirrors: '2'
    fs_options: ''
    fs_pdirenable: 'yes'
    fs_protection: disk
    fs_sharing: 'no'
    fs_size: 20G
    fs_type: mirrored
    poollist: []
  filesystems: {}
  groups: {}
  pools: {}
```

18 设置 Storage Foundation 群集。

- **# cd /access_build_dir/rhel7_x86_64/manual_install/network/SetupClusterScripts**
- **# mkdir -p /opt/VRTSperl/lib/site_perl/UXRT72/CPIR/Module/veritas/**
- **# cp sfcfsha_ctrl.sh /opt/VRTSperl/lib/site_perl/UXRT72/CPIR/Module/veritas/sfcfsha_ctrl.sh**
- **# cp module_script.pl /tmp/**
- **# chmod +x /tmp/module_script.pl**
- 在以下命令中更新群集名称、系统名称和 NIC 名称，然后执行该命令：

  # /tmp/module_script.pl veritas::sfcfsha_config '{"cluster_name" => "<Provide cluster name here>","component" => "sfcfsha","state" => "present","vcs_users" => "admin:password:Administrators,user1:passwd1:Operators","vcs_clusterid" => 14865,"cluster_uuid" => "1391a-443ab-2b34c","method" => "ethernet","systems" =>

"<Provide hostnames separated by comma>","private_link" =>
""<provide private nic name separated by comma>"}'

例如，如果群集名称是 *clus*，主机名是 *clus_01* 和 *clus_02*：

```
/tmp/module_script.pl veritas::sfcfsha_config '
{"cluster_name" => "clus","component" => "sfcfsha",
"state" => "present","vcs_users" =>
"admin:password:Administrators,user1:passwd1:Operators",
"vcs_clusterid" => 14865,"cluster_uuid" => "1391a-443ab-2b34c",
"method" => "ethernet","systems" => "clus_01,clus_02",
"private_link" => "priveth0,priveth1"}'
```

- 更新并配置以下文件：
  - **# rpm -q --queryformat '%{VERSION}|%{BUILDTIME:date}|%{INSTALLTIME:date}|%{VERSION}\n' VRTSnas > /opt/VRTSnas/conf/version.conf**
  - **# echo NORMAL > /opt/VRTSnas/conf/cluster_type**
  - **# echo 'path /opt/VRTSsnas/core/kernel/' >> /etc/kdump.conf**
  - **# sed -i '/^core_collector\b/d;' /etc/kdump.conf**
  - **# echo 'core_collector makedumpfile -c --message-level 1 -d 31' >> /etc/kdump.conf**

19 启动 Veritas Access 产品进程。

- 在以下命令中提供当前主机名，然后执行该命令。

  # /tmp/module_script.pl veritas::process '{"state" => "present", "seednode" => "<provide current hostname here>","component" => "sfcfsha"}'

  例如，如果主机名是 *clus_01*：

  # /tmp/module_script.pl veritas::process '{"state" => "present","seednode" => "clus_01","component" => "sfcfsha"}'

  如果在 *clus_02* 上运行该命令，则必须提供 "seednode" => "clus_02"。
- 运行以下命令。

```
# /opt/VRTSnas/pysnas/install/install_tasks.py
all_services_running serial
```

20 创建 CVM 组。

如果 /etc/vx/reconfig.d/state.d/install-db 文件存在，则执行以下命令。

```
# mv /etc/vx/reconfig.d/state.d/install-db
/etc/vx/reconfig.d/state.d/install-db.a
```

如果尚未配置 CVM，则在主节点上运行以下命令。

```
# /opt/VRTS/bin/cfscluster config -t 200 -s
```

21 启用 hacli。

在 /etc/VRTSvcs/conf/config/main.cf 文件中进行验证。如果 HacliUserLevel = COMMANDROOT 存在，则转到步骤 22，否则请按照以下步骤在您的系统中启用 hacli。

```
# /opt/VRTS/bin/hastop -local
```

更新 /etc/VRTSvcs/conf/config/main.cf 文件。

如果不存在以下行，请添加此内容：

```
HacliUserLevel = COMMANDROOT  in cluster <cluster name> ( ) loop
```

例如：

```
cluster clus (
   UserNames = { admin = aHIaHChEIdIIgQIcHF, user1 =
aHIaHChEIdIIgFEb }
   Administrators = { admin }
   Operators = { user1 }
   HacliUserLevel = COMMANDROOT
# /opt/VRTS/bin/hastart
```

验证 hacli 是否正常运行。

```
# /opt/VRTS/bin/hacli -cmd "ls /" -sys clus_01
```

22 验证 HAD 后台驻留程序是否正在运行。

```
# /opt/VRTS/bin/hastatus -sum
```

23 执行步骤 1 到 22，在第二个节点上配置 Veritas Access。

24 验证是否已正确配置系统。

- 验证是否已正确配置 LLT。

  # **lltconfig -a list**

  例如：

```
[root@clus_02 SetupClusterScripts]# lltconfig -a list
Link 0 (priveth0):
  Node    0 clus_01    :    00:0C:29:0C:8D:69
  Node    1 clus_02    :    00:0C:29:F0:CC:B6  permanent

Link 1 (priveth1):
 Node    0 clus_01     :    00:0C:29:0C:8D:5F
 Node    1 clus_02     :    00:0C:29:F0:CC:AC  permanent
```

- 验证是否已正确配置 GAB。

  # **gabconfig -a**

  例如：

```
[root@clus_01 network]# gabconfig -a
GAB           Port   Memberships
================================
Port a gen    43b804 membership 01
Port b gen    43b807 membership 01
Port h gen    43b821 membership 01
```

- 验证 LLT 状态。

  # **lltstat -nvv**

  例如：

```
[root@clus_01 network]# lltstat -nvv
LLT node information:
      Node         State    Link    Status  Address
   * 0 clus_01     OPEN
                            priveth0   UP    00:0C:29:0C:8D:69
                            priveth1   UP    00:0C:29:0C:8D:5F
     1 clus_02     OPEN
                           priveth0   UP      00:0C:29:F0:CC:B6
```

```
                        priveth1    UP      00:0C:29:F0:CC:AC

    2           CONNWAIT
                        priveth0    DOWN
                        priveth1    DOWN
```

- vxconfigd 后台驻留程序应在两个节点上均处于联机状态。

  # **ps -ef | grep vxconfigd**

  例如：

  # **ps -ef | grep vxconfigd**

```
root   13393 1  0 01:33 ?  00:00:00 vxconfigd -k -m disable
-x syslog
```

25 运行 Veritas Access 启动后操作。

- 确保所有节点上都在运行 HAD。

  # **/opt/VRTS/bin/hastatus**

- 在所有节点上，创建 communication.conf 文件以启用 hacli（而不是 ssh）。

```
vim /opt/VRTSnas/conf/communication.conf
{
 "WorkingVersion": "1",
 "Version": "1",
 "CommunicationType": "HACLI"
}
```

- 运行安装程序以安装 Veritas Access。只在主节点上运行以下命令。

  # **/opt/VRTSnas/install/image_install/installer -m master**

26 在从属节点上运行加入操作。

/opt/VRTSnas/install/image_install/installer -m join

27 在两个节点上均运行以下命令。

```
# echo "<first private nic name>" >
/opt/VRTSnas/conf/net_priv_dev.conf
```

例如：

```
# echo "priveth0" > /opt/VRTSnas/conf/net_priv_dev.conf
```

28 启用 NFS 资源。在主节点上运行以下命令。

```
# /opt/VRTS/bin/haconf -makerw
# /opt/VRTS/bin/hares -modify ssnas_nfs Enabled 1
# /opt/VRTS/bin/haconf -dump -makero
```

现在可以使用该双节点 Veritas Access 群集。

在 Veritas Access 中启用内部 sudo 用户通信

默认情况下，Veritas Access 为 root 用户提供的节点间通信方式是 SSH 通信。如果您希望使用基于 sudo 用户的通信，可在成功安装 Veritas Access 后设置内部通信以使用 sudo 用户通信。

您可以按照以下步骤设置 sudo 用户通信。

- 第 1 阶段：在 Veritas Access 群集的每个节点上创建 access_user。
- 第 2 阶段：在每个节点上，在 root 用户与 access_user 之间设置无密码通信
- 第 3 阶段：选择通信类型 SUDO_SSH

第 1 阶段：在 Veritas Access 群集的每个节点上创建 access_user

1 创建 access_user 并设置密码。

例如：

```
[root@access1_01 ~]# useradd access_user
[root@access1_01 ~]# passwd access_user
Changing password for user access_user.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

2 将 access_user 添加到 sudoers 文件中。

例如：

```
[root@access1_01 ~]# echo "access_user ALL=(ALL) NOPASSWD: ALL"
>> /etc/sudoers
```

在群集的所有节点上完成第 1 阶段。

第 2 阶段：在每个节点上，在 root 用户与 access_user 之间设置无密码通信

1 为 root 用户生成 rsa 密钥（如果不存在）。

例如：

```
[root@access1_01 ~]# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Created directory '/root/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:hRIBljcpsmGMCtfUUjyVGOfe957OXyiXcRyiYBprmZk root@access1_01
The key's randomart image is:
+---[RSA 2048]----+
| o o+*=*o.       |
|o *.= O+..       |
|oo + +.+oo.  . . |
|. .    oXo. . ...|
|       ES ... . o|
|      .    . . = |
|             . = .|
|              = ..|
|              .=..|
+----[SHA256]-----+
```

2 对于群集中的每个节点，将 root 用户的 rsakey.pub 复制到 access_user。

例如：

```
[root@access1_01 ~]# ssh-copy-id access_user@access1_01
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed:
"/root/.ssh/id_rsa.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new
key(s),to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed --
if you are prompted now it is to install the new keys
access_user@access1_01's password:

Number of key(s) added: 1
```

第 3 阶段：选择通信类型 SUDO_SSH

- 创建 /opt/VRTSnas/conf/communication.conf 文件。

```
[root@access1_01 ~]# cat /opt/VRTSnas/conf/communication.conf
{
    "WorkingVersion": "1",
    "Version": "1",
    "CommunicationType": "SUDO_SSH"
}
```

索引

Y

Z