Veritas Access 7.2.1 故障排除指南

Linux

7.2.1

VERITAS™

Veritas Access 故障排除指南

上次更新日期： 2017-05-08

文档版本：7.2.1 Rev 0

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（除日本外）	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。请提供所报告文本内容的文档标题、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，提供的信息和工具可自动处理和简化某些耗时的管理任务。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，具体视您的产品而定。要了解 SORT 为您的产品提供了哪些服务和工具，请参见产品资料：

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

目录

1

简介

本章节包括下列主题：

关于故障排除

Veritas Access 的故障排除过程包括以下类型：

- 警报和日志消息审核
- 例行维护任务
- 常用恢复过程
- 特定功能的问题和解决方案

本指南的其他章节分别对上述每种故障排除过程进行了介绍。

其中一些故障排除过程要求您以 `support` 用户身份登录。

请参见第 8 页的“关于 support 用户帐户”。

故障排除过程的通用技巧

对问题进行故障排除时，请考虑以下事项：

- 检查以前是否有先例。
  检查现有的故障排除信息以查看之前是否出现过此问题。有关此类信息，请参见《Veritas Access 版本说明》。版本说明中列出了 Veritas Access 的一些已知问题及其可能的解决方法。
- 考虑最新的变更。
  如果系统在进行某种维护、软件升级或其他更改后立即出现问题，则问题可能与这些更改有关。
- 确定正常运行的部分。
  如果系统未呈现所需的结果，可以看一下有哪些部分是正常运行的。确定没有问题的部分之后，再将重点放在其他地方。保证这些部分正常运行所需的任何组件或子系统应该都是正常的。
- 运用经验进行判断。
  基于您对系统运作的了解，考虑可能会导致此问题的各种故障。检查这些故障。根据实际情况、历史记录或对现有功能弱点的了解，从可能性最大的故障开始。

故障排除过程的一般方法

在通过某些常规故障排除技巧缩小问题范围后，可借助以下方法进一步确定问题所在：

- 交换相同部件。
  在具有相同或并行部件和子系统的系统中，一个很好的方法是在这些子系统之间交换组件，看问题是否与交换的组件一起发生转移。例如，如果群集中的某个节点上出现 Veritas Access 网络连接问题，可交换以太网接口卡以确定问题是否会转移到新的节点。
- 移除并行组件。
  如果系统包含多个在移除后不会影响整个系统的并行或冗余组件，请先移除这些组件（每次一个），看系统是否开始正常运行。例如，在群集中逐个关闭节点，以查看问题是否仍然存在。
- 将系统分为几个部分。
  在具有多个部分或阶段的系统中，仔细测量每个阶段输入和输出的变量，直到找到出现问题的阶段。例如，如果运行复制作业时出现问题，请检查作业以前是否已成功运行，并尝试确定作业开始失败时的具体时间点。
- 监视一段时间内（或位置范围内）的系统行为。
  使用 `Support> services show all` 命令显示服务及其当前状态的列表。
  设置进程（如 `Support> traceroute` 命令或一系列 `Support> iostat` 命令），以监视一段时间内的系统活动，或监视整个网络上的系统活动。这种监视方法尤其有助于跟踪间歇性问题、处理器活动问题、节点连接问题等。

关于 support 用户帐户

通常，要访问 Veritas Access，需要使用 Veritas Access 用户帐户登录到管理控制台。登录后，您将进入命令行界面 shell (CLISH)。命令行选项取决于用户帐户所分配的角色。

在某些情况下，本指南中介绍的故障排除方法需要访问基础 Linux 命令行和其他支持实用程序。通过 support 用户帐户可访问这些实用程序。必须启用 support 用户帐户（默认设置）。

以 support 用户身份登录可以访问 CLISH 之外的日志和其他文件。

警告：以 support 用户身份执行命令时，请务必谨慎。支持命令适用于熟悉 Veritas Access 特点和功能的高级用户。如果遇到任何有关使用这些命令的问题，请与您的 Veritas 技术支持代表联系以获取更多指导。

配置 support 用户帐户

具有 `Master` 角色的 Veritas Access 用户可启用、禁用及更改密码，或者检查 support 用户的状态。

默认情况下，support 用户帐户已启用。

配置 support 用户帐户

1 要启用 support 用户，请输入以下内容：

```
Admin> supportuser enable
Enabling support user.
support user enabled.
```

2 验证是否已启用 support 用户：

```
Admin> supportuser status
support user status : Enabled
```

3 要更改 support 用户密码，请输入以下内容：

```
Admin> supportuser password
Changing password for support.
Old password:
New password:
Re-enter new password:
Password changed
```

禁用 support 用户帐户

1 要禁用 support 用户，请输入以下内容：

```
Admin> supportuser disable
Disabling support user.
support user disabled.
```

2 验证是否已禁用 support 用户：

```
Admin> supportuser status
support user status : Disabled
```

使用 support 帐户登录

以 support 用户身份登录可以访问 CLISH 之外的日志和其他文件。本指南中介绍的一些故障排除方法需要以 support 用户身份登录。

必须由具有 `master` 角色的管理员启用 support 用户帐户。

请参见第 8 页的“配置 support 用户帐户”。

注意： `support` 帐户仅供技术支持和高级用户使用。

使用 support 帐户登录

1 输入以下命令，使用 support 帐户登录到群集的物理 IP 地址：

support

然后输入密码。默认密码为：

veritas

例如：

```
login as: support
support@<ip_address>'s password:
Last login: Tue Apr 26 14:53:32 2016 from 172.31.172.139
************************************************************
*                     Veritas Access                       *
*                                                          *
*                   Enterprise Edition                     *
*       Warning: Only Veritas Access distributed           *
*     patches & RPMs can be installed on this system!      *
*    Do not delete contents of lost+found directory of     *
*    filesystems as it may contain critical temporary      *
*          Veritas Access configuration data!              *
************************************************************

WARNING: System configured with default password. It's recommended
 to
change password now. Please proceed with changing the password :

Changing password for support.
New password:
Re-enter new password:
Password changed
Default password is changed successfully on all the nodes.
ACCESSRC2_01:~ #
```

2 如果您需要访问 CLISH，可以使用以下命令：

```
su - master
```

2

常规故障排除过程

本章节包括下列主题：

关于常规故障排除过程

本章概述了有助于发现和修复问题的常规故障排除过程。

查看 Veritas Access 日志文件

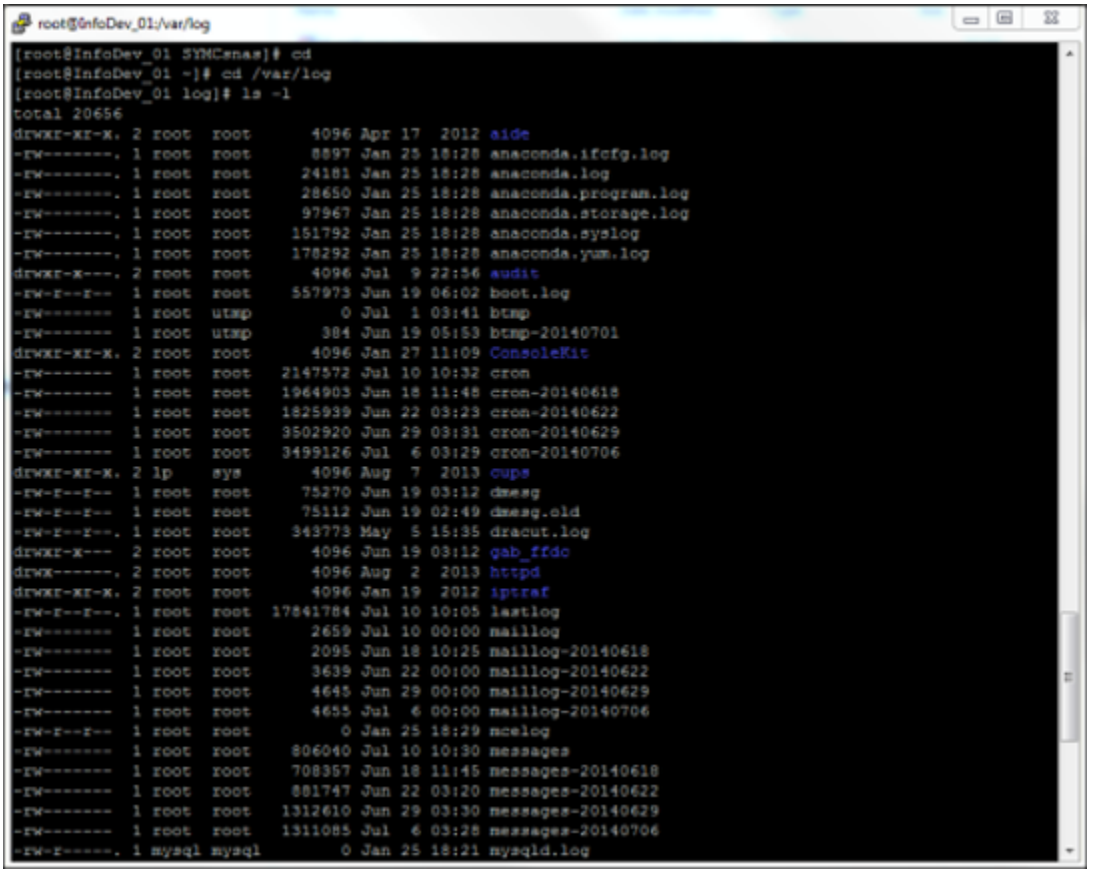
除了 Veritas Access Operations Manager 控制台控制板上的“警报”面板外，也可在 Veritas Access `/var/log` 目录中找到与可能发生的问题相关的更多信息。

查看 Veritas Access **日志文件**

1 使用 support 帐户登录。

2 导航到 `/var/log` 目录。

图 2-1 Veritas Access 日志文件



关于事件日志

除了系统日志外，每个 Veritas Access 功能还具有关联的事件日志。出现问题时，能够最快了解所发生问题的方法之一就是查看这些日志文件。Veritas Access 功能的事件日志存储在 `/opt/VRTSnas/log` 目录中。

注意：进行故障排除时不应删除或更改日志文件，因为这可能会妨碍 Veritas 技术支持进行进一步调查。

查看事件日志：

1 使用 support 帐户登录。

2 导航到 `/opt/VRTSnas/log` 目录。

Veritas Access 功能的事件日志存储在此目录中。

例如，`cifs.log` 包含 CIFS 事件日志。

关于 shell 活动日志

您可以使用 shell 活动日志捕获最终用户或客户执行的任何命令行操作。shell 活动日志可帮助您了解最终用户有意或无意执行的任何不需要的操作。

您可从以下位置找到相应的 shell 活动日志：

- support 帐户 - `/var/log/shell_activity_log`
- CLI 命令 - `/opt/VRTSnas/log/command.log`

设置 CIFS 日志级别

您可以设置 Veritas Access 群集的 CIFS 日志级别，然后将调试信息上传到外部服务器以进行故障排除。

请参见 `support_debug.1` 手册页。

请参见第 15 页的“检索并发送调试信息”。

设置 CIFS 日志级别

- 为 Veritas Access 群集设置与 CIFS 相关的日志级别。

  Support> debuginfo setlog cifs loglevel

  有效的 `loglevel` 范围为 `0` 到 `10`，`10` 是最详细的日志级别。建议提高 CIFS 日志级别，重现 CIFS 问题，然后针对 CIFS 问题上传调试信息。

  默认日志级别为 `2`。

  例如，要将 Veritas Access 群集的 CIFS 日志级别设置为 `10`，请执行以下操作：

  Support> debuginfo setlog cifs 10

设置 NetBackup 客户端日志级别和调试选项

可以设置 NetBackup 客户端日志级别以及不同的调试选项，然后将信息上传到外部 FTP 或 SCP 服务器。可以使用此调试信息发送给 Veritas 技术支持。

请参见第 15 页的"检索并发送调试信息"。

可以使用 `Backup> show` 命令查找 NetBackup 日志信息。请参见 `backup_show(1)` 手册页。

通过执行 `Backup> show` 命令，可以查看已启用哪些 NetBackup 日志级别和调试选项。

有关 NetBackup 日志记录的详细信息，请参见 *Veritas NetBackup Administrator's Guide*（《Veritas NetBackup 管理指南》）第 1 卷。

有效的日志级别值介于 `1` 到 `5` 之间，`5` 表示最详细。请参见 `support_debuginfo(1)` 手册页。

设置 NetBackup 客户端日志级别

1 设置 NetBackup 数据库日志级别：

Support> debuginfo setlog nbu database *loglevel*

2 设置 NetBackup 全局调试日志级别：

Support> debuginfo setlog nbu global *loglevel*

全局日志记录可控制在 NetBackup 管理控制台的 **Logging** 对话框中所设置进程的日志记录级别。

设置 NetBackup 调试选项

1 启用 NetBackup 客户端，在群集中执行可靠的日志记录。

Support> debuginfo setlog nbu enable robust

可靠的日志记录将限制日志目录消耗的磁盘空间量。

2 启用 NetBackup 客户端，在群集中执行关键进程日志记录。

Support> debuginfo setlog nbu enable critical

启用关键进程选项后，可以自动记录 NetBackup 关键进程。在 NetBackup 管理控制台的 **Logging** 主机属性中启用此选项后，系统将为这些关键进程创建日志目录并开始进行日志记录。

检索并发送调试信息

您可以从 Veritas Access 节点检索 Veritas Access 调试信息，并将该信息发送到使用外部 FTP 或 SCP 服务器的服务器。

有关如何为 Veritas 技术支持提供数据的详细信息，请参见以下文章：

http://www.veritas.com/docs/000097935

将调试信息从指定节点上传到外部服务器

- 将调试信息从指定节点上传到外部服务器。

  Support> debuginfo upload *nodenamedebug-URL module*

  例如，要将所有调试信息上传到 FTP 服务器，请输入以下内容：

  Support> debuginfo upload node1_1
  ftp://admin@ftp.docserver.company.com/patches/ all

  例如，要将 CIFS 相关的调试信息上传到 SCP 服务器，请输入以下内容：

  Support> debuginfo upload node1_1
  scp://root@server.company.com:/tmp/node1_1-cifs-debuginfo.tar.gz

nodename	指定从中收集调试信息的 *nodename*。

debug-URL	指定用于上传调试信息的远程文件或目录。
	根据从中上传调试信息的服务器的类型，使用以下示例 URL 格式之一：
	`ftp://admin@ftp.docserver.company.com/patches/`
	`scp://root@server.company.com:/tmp/`
	如果 *debug-URL* 指定了远程文件，则 debuginfo 文件使用该名称保存。如果 *debug-URL* 指定了远程目录，则 debuginfo 文件名称如下所示：
	`nas_debuginfo_nodename_modulename_timestamp.tar.gz`

module 指定 *module* 的值。

支持的模块值如下：

- all - 用于收集所有调试信息
- generic - 用于收集除 Veritas 产品相关信息以外的所有调试信息
- cifs - 用于收集与 CIFS 相关的调试信息
- nas - 用于收集与 Veritas Access 相关的调试信息
- netbackup - 用于收集与 NetBackup 客户端相关的调试信息

`Support> debuginfo` 命令还会收集有关 Red Hat Enterprise Linux (RHEL) 的 `sosreport` 命令的信息。系统会收集除 `selinux` 模块以外的所有已加载模块的 `sosreport`。

3

监视 Veritas Access

本章节包括下列主题：

关于监视 Veritas Access 操作

本章介绍了几个有助于监视 Veritas Access 操作的支持任务。定期执行这些监视任务，以确保 Veritas Access 平稳运行。

使用 Veritas Access 时，请持续记录监视命令所创建的输出。此过程为您提供了判断操作是否正常的基准，并帮助您在潜在问题变得严重之前发现问题。

监视处理器活动

`Support> top` 命令可显示当前正在运行的任务的动态实时视图。它会显示指定节点的用户和进程在给定时间占用的资源。

使用 top 命令

- 要使用 `Support> top` 命令，请输入以下内容：

  Support> top [*nodename*] [*iterations*] [*delay*]

nodename	显示指定节点在给定时间的资源和进程。
iterations	指定要运行的迭代次数。默认值为 3。
delay	指定屏幕更新之间的延迟。默认值为 5 秒。

  例如，要显示节点 `access_01` 上运行的任务的动态实时视图，请输入以下内容：

  Support> top access_01 1 1

```
top - 16:28:27 up 1 day, 3:32, 4 users, load average: 1.00, 1.00,
 1.00
Tasks: 336 total, 1 running, 335 sleeping, 0 stopped, 0 zombie
Cpu(s): 0.1% us, 0.1% sy, 0.0% ni, 99.7% id, 0.0% wa, 0.0% hi,
0.0% si
Mem: 16405964k total, 1110288k used, 15295676k free, 183908k
buffers
Swap: 1052248k total, 0k used, 1052248k free, 344468k cached

PID   USER  PR  NI  VIRT   RES  SHR  S  %CPU  %MEM   TIME+
COMMAND
6314  root  15  0   5340  1296  792  R   3.9   0.0  0:00.02  top
1     root  16  0    640   260  216  S   0.0   0.0  0:04.86  init
```

生成 CPU 和设备利用率报告

使用 iostat 命令

- 要使用 `Support> iostat cpu` 命令，请输入以下内容：

  Support> iostat cpu [*nodename*] [*interval*] [*count*]

nodename	从中生成报告的节点的名称。默认值为 `console`，表示管理控制台。
interval	每次报告之间的间隔时间（秒）。默认值为 2 秒。
count	以 `interval`（秒）为间隔生成的报告数。默认值为一份报告。

  其中 *nodename* 选项要求输入从中生成报告的节点的名称。默认值为 `console`，表示 Veritas Access Operations Manager 控制台。

  例如，要生成控制台节点的 CPU 利用率报告，请输入以下命令：

  Support> iostat cpu access_01

```
Linux 2.6.16.60-0.21-smp (access_01)       02/09/16

avg-cpu:  %user   %nice  %system  %iowait  %steal   %idle
           1.86    0.07     4.53     0.13    0.00   93.40
```

使用 iostat device **命令**

- 要使用 `Support> iostat device` 命令，请输入以下内容：

  Support> iostat device [*nodename*] [*dataunit*] [*interval*] [*count*]

nodename	*nodename* 选项要求输入从中生成报告的节点的名称。默认值为 `console`，表示管理控制台。
dataunit	*dataunit* 选项允许您以块或 KB 为单位生成报告。默认值为块。
interval	每次报告之间的间隔时间（秒）。默认值为 2 秒。
count	以 `interval`（秒）为间隔生成的报告数。默认值为一份报告。

  例如，要生成节点的设备利用率报告，请输入以下命令：

  Support> iostat device access_01 Blk

```
Linux 2.6.16.60-0.21-smp (access_01)       02/09/16

Device:      tps   Blk_read/s   Blk_wrtn/s   Blk_read   Blk_wrtn
hda         4.82        97.81        86.11    1410626    1241992
sda         1.95        16.83         4.05     242712      58342
hdc         0.00         0.01         0.00        136          0
```

监视网络通信

Tethereal 是 Ethereal 的命令行版本，它是 Linux 操作系统支持的一种网络协议分析工具。通过它，您可以从实时网络捕获数据包数据，或者从以前保存的捕获文件读取数据包。

为帮助您监视网络通信，Veritas Access 提供了 `Support> tethereal` 命令，用于显示和导出网络通信数据。

- `Support> tethereal show` 命令可显示从实时网络捕获的打包数据。
- `Support> tethereal export` 命令可导出网络通信详细信息，以进行进一步分析。

导出和显示网络通信详细信息

使用 tethereal **命令**

- 要使用 `Support> tethereal export` 命令，请输入以下内容：

  Support> tethereal export *url* [*nodename*] [*interface*] [*count*] [*source*]

url	提供要导出网络通信详细信息的位置。如果未在 url 中指定文件名，则使用默认文件名 `tethereal.log`。
nodename	从中生成通信详细信息的节点的名称。
interface	指定数据包捕获的网络接口。
count	指定要读取的最大数据包数量。 捕获的网络通信详细信息的文件大小上限为 128 MB。如果“count”值非常大，当文件大小超过 128 MB 时，该命令会停止捕获网络通信详细信息。
source	指定要过滤数据包的节点。

  例如，要导出网络通信详细信息，请输入以下内容：

  Support> tethereal export scp://user1@172.31.168.140:~/

  ```
  Password: *******
  Capturing on pubeth0 ...
  Uploading network traffic details to scp://user1@172.31.168.140:~/

  is completed.
  ```

  导出网络通信详细信息时，按 **Ctrl + C** 键可停止捕获过程并将通信详细信息上传到 URL 站点。

使用 tethereal show 命令

- 要使用 `Support> tethereal show` 命令，请输入以下内容：

  Support> tethereal show [*nodename*] [*interface*] [*count*] [*source*]

nodename	要显示通信详细信息的节点的名称。
interface	指定数据包捕获的网络接口。
count	指定要读取的最大数据包数量。 如果未指定 count 值，将持续显示网络通信，直到您将其中断为止。
source	指定要过滤数据包的节点。

  例如，五个数据包的通信详细信息为：

  ```
  Support> tethereal show access_01 pubeth0 5 172.31.168.140
  0.000000 172.31.168.140 -> 10.209.105.147 ICMP Echo (ping) request
  0.000276 10.209.105.147 -> 172.31.168.140 ICMP Echo (ping) reply
  0.000473 10.209.105.147 -> 172.31.168.140 SSH Encrypted response

  packet len=112
  0.000492 10.209.105.147 -> 172.31.168.140 SSH Encrypted response

  packet len=112
  ```

4

常见恢复过程

本章节包括下列主题：

关于常见的恢复过程

本章提供了一些最常见的恢复过程，可用于对 Veritas Access 问题进行故障排除。

重新启动服务器

某些配置更改只有在关联的服务器重新启动后才会生效。因此，某些配置问题可以通过停止并重新启动关联的服务器来解决。例如，更改 AD 域设置时，您需要重新启动 CIFS 服务器。

表 4-1 显示了可用于启动和停止 Veritas Access 服务器的命令。

表 4-1 启动和停止服务器的命令

命令	定义
`Backup> start`	启动所有已配置的备份服务。
`Backup> stop`	停止所有已配置的备份服务。
`CIFS> server start`	启动 CIFS 服务器。
`CIFS> server stop`	停止 CIFS 服务器。
`FTP> server start`	启动 FTP 服务器。
`FTP> server stop`	停止 FTP 服务器。
`NFS> server start`	启动 NFS 服务器。
`NFS> server stop`	停止 NFS 服务器。
`Storage> iscsi start`	启动 iSCSI 启动器服务。
`Storage> iscsi stop`	停止 iSCSI 启动器服务。

注意：某些命令包含 `server` 参数，某些命令则不包含该参数。此外，某些 `Support>` 命令使用 `service`（而不是 `server`）参数。

使服务联机

`Support> services` 命令可以使 OFFLINE 或 FAULTED 状态的服务恢复为 ONLINE 状态。

注意：使用 `Support> services` 命令后，如果服务仍为脱机或故障状态，则您需要与技术支持联系。

这些服务包括：

- 备份
- 控制台服务
- CIFS 服务器
- FTP
- FS 管理器
- GUI
- IP 地址
- NIC 信息
- NFS 服务器

使用 services 命令

显示服务的状态

◆ 要显示节点上运行的重要服务，请输入以下内容：

```
Support> services show
                          access
Service             01         02
-------           -------- --------
nfs                 ONLINE   ONLINE
cifs                ONLINE   ONLINE
ftp                 ONLINE   ONLINE
iSCSIInitiator     OFFLINE  OFFLINE
gui                 ONLINE   ONLINE
console             ONLINE   ONLINE
nic_pubeth0         ONLINE   ONLINE
nic_pubeth1         ONLINE   ONLINE
fs_manager          ONLINE   ONLINE
```

显示所有服务的状态

- 要显示节点上运行的所有服务，请输入以下内容：

  Support> services showall

```
                          access
Service                01         02
-------              -------- --------
nfs                  ONLINE   ONLINE
cifs                 ONLINE   ONLINE
ftp                  ONLINE   ONLINE
iSCSIInitiator       OFFLINE  OFFLINE
console              ONLINE   ONLINE
gui                  ONLINE   ONLINE
nic_pubeth0          ONLINE   ONLINE
nic_pubeth1          ONLINE   ONLINE
fs_manager           ONLINE   ONLINE
10.182.107.201       ONLINE   ONLINE
10.182.107.202       ONLINE   ONLINE
10.182.107.203       ONLINE   ONLINE
10.182.107.204       ONLINE   ONLINE
/vx/fs1              ONLINE   ONLINE
```

修复所有服务故障

- 要修复所有服务故障，请输入以下内容：

  Support> services autofix

```
Attempting to fix service faults..........done
```

使服务联机

- 要使节点上的服务联机，请输入以下内容：

  Support> services online *servicename*

  其中 *servicename* 是要使其联机的服务的名称。

  例如：

  Support> services online 10.182.107.203

从非正常关闭中恢复

在某些情况下，当节点非正常关闭时（例如，在意外出现系统停止或电源故障期间），可能会在本地节点上收到一条错误消息，要求您使用 Linux `fsck`（文件系统检查）命令修复节点上的文件。

不建议（且可能无法）使用 `fsck` 命令尝试修复节点，而是应该使用群集中正常运行的节点在损坏的节点上重新安装 Veritas Access 软件。

恢复节点

1 使用 `master` 帐户登录 Veritas Access。

2 从群集中删除故障节点。要删除节点，请输入以下内容：

Cluster> del *nodename*

其中 *nodename* 是故障节点的名称。

例如：

Cluster > del access_01

注意：系统将从群集中删除故障节点的信息。当故障节点重新引导时，它将检测到自身已被删除，并将进行自我清理。

---

3 从群集中删除节点后，重新引导已删除的节点，随后即可使用在将该节点添加到群集之前的原始物理 IP 地址访问该节点。

4 通过输入以下内容重新添加节点：

Cluster> add *nodeip*

其中 *nodeip* 是已删除节点的可访问 IP 地址。

例如：

Cluster > add 172.16.113.118

测试网络连接

您可以测试能否通过 IP 网络访问特定主机或网关。

使用 ping 命令

- 要使用 ping 命令，请输入以下内容：

  Network> ping *destination* [*nodename*] [*devicename*] [*packets*]

  例如，您可以使用 node1 对 host1 执行 ping 操作：

  Network> ping host1 node1

destination	指定要将信息发送到的主机或网关。 目标字段可以包含 DNS 名称或 IP 地址。
nodename	指定从中执行 ping 操作的 *nodename*。要从任意节点执行 ping 操作，请在 *nodename* 字段中使用 `any`。*nodename* 字段是可选字段。如果省略 *nodename*，则会任意选择一个节点执行 ping 操作。
devicename	指定要从中执行 ping 操作的设备。要从群集中的任意设备执行 ping 操作，请在 `devicename` 字段中使用 `any` 变量。
packets	指定应发送到目标的数据包数量。 如果省略 packets 字段，则默认将五个数据包发送到目标。 数据包字段必须包含无符号整数。

使用 traceroute 进行故障排除

Traceroute 是 Linux 操作系统支持的一种使用广泛的实用程序。Traceroute 与 ping 十分类似，是确定网络中连接情况的重要工具。Veritas Access `Support> ping` 命令可以揭示两个系统之间的连接情况。而 `Support> traceroute` 命令不但会检查系统连接情况，而且还会列出两个系统之间的中间主机。用户可以看到数据包从一个系统到另一个系统的路由情况。使用 `Support > traceroute` 命令可以查找与远程主机之间的路由。例如，您可以使用 `Support> traceroute` 命令验证群集中每个节点的连接情况。

使用 traceroute 命令

`Support> traceroute` 命令可显示两个节点之间的路由上的所有中间节点。

使用 traceroute **命令**

- 要使用 `Support> traceroute` 命令，请输入以下内容：

  Support> traceroute *destination* [*source*] [*maxttl*]

destination	目标节点。要显示位于网络上两个节点之间的所有中间节点，请输入 *destination* 节点。 对于 IPv4 安装，您需要指定 IPv4 地址；对于 IPv6 安装，您需要指定 IPv6 地址。 可接受的 IPv6 前缀范围为 0-128 之间的整数。
source	指定要开始跟踪的起始 *source* 节点名称。
maxttl	指定最大跃点数。默认值为 7 个跃点。

  例如，要跟踪与网络主机之间的路由，请输入以下内容：

Support> traceroute www.veritas.com fssClus_01 10

```
traceroute to www.veritas.com (23.5.150.79), 10 hops max, 60 byte packets
 1  puna-sli-core-b01-vlan329.net.symantec.com (10.209.192.2) 0.356 ms  0.354 ms 0.376
 ms
 2  punb-vfpi-eng-1-aggregate2-104.net.veritas.com (10.209.186.14) 0.298 ms 0.322 ms
0.379 ms
 3  puna-spi-core-b02-vlan105.net.symantec.com (143.127.185.130) 1.851 ms  1.964 ms
1.940 ms
 4  bnrcatcore01-teng6-2.net.symantec.com (143.127.185.205)  1.902 ms 1.903 ms 1.932 ms

 5  puna-vfpi-main-1-vip.net.veritas.com (10.212.252.50) 1.886 ms 1.945 ms 1.922 ms
```

收集文件系统的元数据保存映像

您可以收集常规文件系统或横向扩展文件系统的元数据保存映像，以便对文件系统问题进行故障排除。元数据是一种数据结构，它包含文件系统内与数据有关的属性，但不包含实际数据本身。元数据映像可用来跟踪文件系统趋势，例如，文件系统中的文件大小、保留时间和信息类型。

注意：使用 `Support> metasave` 命令时，所有群集节点上的文件系统都必须处于脱机状态，才能创建一致的元数据保存映像。收集元数据保存映像之前，通过使用 `Storage> fs offline` 命令使文件系统脱机。收集元数据保存映像是一项耗时冗长的操作。所需的总时间取决于文件系统中存在的元数据信息量。如果是横向扩展文件系统，则可能需要相当长的时间来收集元数据保存映像。运行元数据保存操作时，可以单开另一个终端来运行其他的 Veritas Access 操作。

收集文件系统的元数据保存映像

- 要使用 `Support> metasave` 命令，请输入以下内容：

  ```
  Support> metasave [fsname] [output_location]
  ```

  `fsname` 指定要收集文件系统元数据保存映像的文件系统名称。

  `output_location` 指定元数据保存映像的目录位置。

  对于一个常规文件系统，单个元数据保存映像将保存在由 `output_location` 指定的目录位置。

  对于一个横向扩展文件系统，将根据横向扩展文件系统内的容器文件系统数生成多个元数据保存映像。对于多个横向扩展文件系统，命名空间映射也会包括在元数据保存映像中。

  例如，要收集文件系统 `testfs` 的元数据保存映像并将其保存在 `/tmp/meta_out_dir` 下，请输入以下命令：

```
Support> metasave testfs /tmp/meta_out_dir
Collecting metasave image of file system testfs. This may take some time...
SUCCESS: Metasave image of testfs collected successfully. Image is stored at
/tmp/meta_out_dir.
```

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。

加速复制

在某些情况下，复制作业可能无法像预期那样快速进行。在这种情况下，您可能需要重新同步复制作业。

关于同步复制作业

首次运行复制作业时，Veritas Access 会将全部数据从源位置复制到目标位置。后续作业（手动触发或按调度触发）仅复制增量更改。

在极少数情况下，数据已经位于目标位置，但复制无法进行增量更改。例如：

- 已经数天或数周未运行复制，而通过 VxFS 文件更改日志跟踪的更改已被覆盖（或可能损坏）。此日志是进行复制所必需的。
- 临时禁用并重新启动复制作业后，下一次运行作业时将复制全部数据。

- 已对复制定义进行了一些更改。例如，先前的复制仅包括 fs1/folder1，但您还希望复制 fs1/folder2 中的数据。由于 fs1/folder2 需要完全复制，因此即使 fs1/folder1 只需增量更改，也会再次复制该文件夹。
- 当需要将复制方向反转为从目标到源时。即使大多数数据在目标和源两个位置上都有，但每当在目标位置创建新作业时，首次复制仍将自动触发完全复制。
- 如果管理员意外删除复制的内部数据库且没有备份可用，则创建新作业将触发完全复制，即使新的作业是针对现有配置创建时也是如此。

在这些情况下，您可使用 Replication> job sync 命令利用目标位置的现有数据并避免要求完全复制，而不是等待启动完全复制。Replication> job sync 命令可将复制作业恢复为明确定义的状态，并可使用增量复制。

同步作业后，此作业会重新启用，并且可通过标准作业触发器或设置复制频率来触发增量复制。

注意：只有已启用的作业才支持同步。如果无法从失败的作业中恢复，而您又想使用 Replication> job sync 命令从此状态中恢复，请执行如下步骤：首先，禁用此作业，然后重新启用它。之后，使用 Replication> job sync 命令同步此作业。

注意：无法在已暂停的复制作业上执行同步。如果在已经中止或停止的已暂停作业上执行同步，该暂停作业的最后一个恢复点目标 (RPO) 将不可用。

同步复制作业

同步已启用的复制作业

◆ 要同步已启用的复制作业，请输入以下内容：

```
Replication> job sync job_name
```

job_name 指定要同步的复制作业的名称。

例如：

```
Replication> job sync job14
```

卸载修补程序版本或软件升级

经常会由于已知的产品缺陷而出现问题。缺陷修复后，您可以安装修补程序版本或软件升级来修复问题。

安装修补程序版本或软件升级时：

- 在开始安装之前，请使用 `System> config export` 命令保存一份配置。升级后，可以使用 `System> config import` 命令来还原到该配置。
- 为尽量缩短升级期间的停机时间，您需要获取一组临时 VIP 和 IP 地址，以便在升级过程中使用。或者，也可以在不使用临时 VIP 和 IP 地址的情况下升级，但这样会增加停机时间。

有关升级 Veritas Access 的详细信息，请参考《Veritas Access 安装指南》。

5

Veritas Access 安装和配置问题故障排除

本章节包括下列主题：

查看安装日志

如果安装过程中出现问题，查看安装日志中的条目可能有助于确定问题。

查看 Veritas Access 安装日志

1 安装和配置 Veritas Access 期间，可在 `/var/tmp` 下的临时文件夹中获得安装程序日志。

2 安装和配置 Veritas Access 后，可在以下位置查看安装日志的副本：

Veritas Access 安装后日志	`/opt/VRTS/install/logs/installaccess-`*`timestamp`* 此目录位于从中触发安装程序的节点（驱动节点）。其中包含 Veritas Access 专用安装日志。 例如： `/opt/VRTS/install/logs/installaccess-201602021544AsJ`

Veritas Access 服务组配置日志	`/opt/VRTSnas/log/Install.log`
	此目录包含 Veritas Access 专用配置日志。
	例如：
	`/opt/VRTSsnas/log/Install.log.201407030655`

Veritas Access 网络安装和配置日志	`/opt/VRTSnas/log/install_network.log`
	此目录包含 Veritas Access 网络配置日志。
	例如：
	`/opt/VRTSnas/log/install_network.log.201407030655`

安装失败且未完成

安装失败的一些常见原因包括：

- 内存有限。要在节点上安装 Veritas Access 软件，必须至少具有 32 GB 的内存。
- 单核（单个 CPU）
  要安装 Veritas Access，群集中必须至少有两个节点（或一个双 CPU 系统）。
- 缺少所需的操作系统软件包
  可使用 yum 安装缺少的所需操作系统软件包，或手动安装缺少的所需软件包。有关详细信息，请参见《Veritas Access 安装指南》。
- 网关访问
  Veritas Access 节点必须能够使用公用网络访问默认网关。通过网络管理员验证网关是否可访问。

从群集中排除 PCI ID

在第一个节点上首次安装 Veritas Access 软件期间，可以在群集中排除某些 PCI ID 以备将来使用。在向群集添加其他节点时，您可能希望排除其他 PCI ID。您可以将这些 PCI ID 添加到排除列表。已将 PCI ID 添加到 PCI 排除列表的接口卡不会用作后续群集节点安装的专用或公用接口。在新节点安装期间，其余 PCI 总线接口将作为公用或专用接口进行搜索和添加。

`Network> pciexclusion` 命令可搭配不同选项一起使用：

- `Network> pciexclusion show` 命令用于显示已选择要排除的 PCI ID。同时，它还会通过对相应节点名称显示 y（是）或 n（否）符号来指示其是否已被排除。如果节点处于 INSTALLED 状态，它会显示节点的 UUID。
- 通过 `Network> pciexclusion add` *pcilist* 命令，管理员可以添加要排除的特定 PCI ID。这些值必须在安装之前提供。该命令会从第二个节点安装中排除该 PCI。
  pcilist 是以逗号分隔的 PCI ID 列表。
- 通过 `Network> pciexclusion delete` *pci* 命令，管理员可从排除中删除给定的 PCI ID。此命令必须在安装之前使用才有效。此命令适用于下一个节点安装。
  PCI ID 位格式为十六进制 (XXXX:XX:XX.X)。

要使用 `Network> pciexclusion` 命令，请输入以下内容：

```
Network> pciexclusion show
PCI ID       EXCLUDED    NODENAME/UUID
------       --------    -------------

Network> pciexclusion add FFFF:FF:00.0
ACCESS pciexclusion SUCCESS V-288-1363 Given PCI ID FFFF:FF:00.0 has
 been
added for exclusion

Network> pciexclusion add FFFF:FF:00.1
ACCESS pciexclusion SUCCESS V-288-1363 Given PCI ID FFFF:FF:00.0 has
 been
added for exclusion

Network> pciexclusion show
PCI ID       EXCLUDED    NODENAME/UUID
------       --------    -------------
0000:0e:00.0 y           ACCESS_1
0000:0e:00.0 y           a79a7f43-9fe2-4eeb-aa1f-27a70e7a0820
0000:04:00:1 n
```

```
Network> pciexclusion delete ffff:ff:00.1
ACCESS pciexclusion SUCCESS V-288-1363 Given PCI ID FFFF:FF:00.0 has
 been
added for exclusion ACCESS pciexclusion SUCCESS V-288-1364 Given PCI
 ID
ffff:ff:00.1 has been deleted from exclusion list

Network> pciexclusion show
PCI ID              EXCLUDED       NODENAME/UUID
------              --------       -------------
ffff:ff:00.0         n
Network>
```

需要运行文件系统检查时无法修复 Red Hat Enterprise Linux 操作系统

如果 Red Hat Enterprise Linux 操作系统分区已损坏，您无法执行 `fsck`（即文件系统检查），而需要重新启动节点。尝试重新启动节点时，操作系统提示输入 `root` 用户密码以运行文件系统检查。

有关此问题的解决方案，请参考 Red Hat Enterprise Linux 文档。

https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/3/html/System_Administration_Guide/s1-rescuemode-boot.html

如何查找管理控制台 IP

确定哪个节点是控制台 IP（**管理控制台** IP）

1 确定哪个节点是管理控制台 IP。

```
# hares - state | grep -I console
```

2 使用安全外壳 (Secure Shell, ssh) 访问管理控制台（只有一个节点拥有管理控制台）。

3 在管理控制台中，使用以下命令登录到 CLISH：

```
su - master
```

storage disk list 命令显示空白磁盘名称

由于以下原因，`storage disk list` 命令可能会显示空白磁盘名称：

- 在虚拟环境中，虚拟机磁盘 (Virtual Machine Disk, VMDK) 在群集的节点之间共享。

  解决办法：

  理想情况下，VMDK 磁盘应连接为本地磁盘

- 本地磁盘具有一个并不唯一的“唯一设备标识符”(Unique Device Identifier, UDID)。

  例如，在包含 node1 和 node2 的群集中，连接到 node1 的本地磁盘可能与连接到 node2 的本地磁盘具有相同的 UDID。

  解决办法：

  运行以下命令：

  # **storage disk configure local <*node_name*> <*vendor_id*> <*product_id*> [*serial_num*]**

  其中，<*vendor_id*> 是供应商 ID

  <*product_id*> 是产品 ID

  <*node_name*> 是运行该命令的节点的名称。

  serial_num 应以“opcode/pagecode/offset/length”格式指定，该格式是根据磁盘的序列号仔细计算出的。

  如果要在所有节点上运行该命令，请将 <*node_name*> 值指定为 *all*。

  有关 `storage disk configure local` 命令的详细信息，请参见 *storage_disk* 手册页。

6

Veritas Access CIFS 问题故障排除

本章节包括下列主题：

拒绝用户访问 CTDB 目录共享

在某些情况下，即使为 CTDB 目录共享设置了正确的 ACL，也可能会拒绝用户或组访问该共享。如果父目录包含阻止这些用户或组访问的 ACL，可能会出现此问题。

这是预期行为。要启用访问，请执行以下操作：

- 确保根级别目录（父目录）已添加为 CIFS 共享。
- 要允许访问，请将应用于原始 CTDB 目录共享的相同 ACL 设置应用于父目录。

索引