Veritas Access 版本说明

Linux

7.4

VERITAS

Veritas Access 版本说明

上次更新日期： 2018-05-28

文档版本：7.4 Rev 0

法律声明

Veritas、Veritas 徽标、Veritas InfoScale 和 NetBackup 是 Veritas Technologies LLC 或其附属机构在美国和其他国家/地区的商标或注册商标。其他名称可能为其各自所有者的商标，特此声明。

此产品可能包含 Veritas 必须保证归属于第三方的第三方软件（以下称“第三方程序”）。部分第三方程序是以开源或免费软件许可方式获得的。本软件随附的授权许可协议并未改变这些开源或免费软件许可所规定的任何权利或义务。请参考此 Veritas 产品随附的第三方法律声明文档，或从以下网址获取该文档：

https://www.veritas.com/licensing/process

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

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

根据 FAR 12.212 定义，授权许可的软件和文档被视为“商业计算机软件”，受 FAR Section 52.227-19“Commercial Computer Software - Restricted Rights”（商业计算机软件受限权利）和 DFARS 227.7202“Commercial Computer Software and Commercial Computer Software Documentation”（商业计算机软件和商业计算机软件文档）中的适用规定以及所有后续法规中规定的权利的制约，无论 Veritas 以本地服务还是托管服务提供都是如此。美国政府仅可根据本协议的条款对授权许可的软件和文档进行使用、修改、复制发行、执行、显示或披露。

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 概述

本章节包括下列主题：

关于此版本

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。

本文档提供了 Veritas Access 产品的版本信息，包括此版本中的变更内容。

重要版本信息

在安装产品之前，请阅读这些版本说明（本文档）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

此版本中的变更内容

本节介绍了 Veritas Access 7.4 版本中的主要新增功能和增强功能。

与 SDS 管理平台的集成

软件定义存储 (SDS) 管理平台与 Veritas Access 集成后，提供了一个用于集成来自企业（不仅仅是数据中心）内各种源的数据的平台，从而为整个环境提供单一的集成视图。SDS 管理平台使用一个简单直观的平台，将 Veritas Access 和 Veritas NetBackup 集成在一起，可满足长期保留和其他用例的需求。

有关详细信息，请参见 *Veritas Access Software-Defined Storage (SDS) Management Platform Solutions Guide*（《Veritas Access 软件定义存储 (SDS) 管理平台解决方案指南》）。

基于容量的授权许可模式

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。

有关授权许可的更多详细信息，请参见《Veritas Access 安装指南》。

支持 AWS 签名版本 2 或版本 4 身份验证

Veritas Access 支持 AWS 签名版本 2 或版本 4 身份验证。

对 GUI 的更改

对 GUI 进行了以下更新：

- 在 **Service Management** 页面上，添加了 **iSCSI Target Service Management** 选项。可以使用此选项将 iSCSI 服务器设置为联机或脱机。
- 在 Dashboard 页面上的 **Quick Actions** > **Provision Storage** 下，添加了以下选项：
  - CIFS
    - 采用连续性复制
    - 采用间歇性复制
    - 采用加密
    - 采用复制和加密

        - 不采用复制和加密
    - Enterprise Vault 的存储
        - 采用复制
        - 不采用复制
    - NFS
        - 采用连续性复制
        - 采用间歇性复制
        - 采用加密
        - 采用复制和加密
        - 不采用复制和加密
    - iSCSI 块存储
        - 配置 iSCSI LUN
    - NetBackup 的 S3 存储
        - 采用云层
        - 不采用云层

支持 RHEL 和 OL 操作系统

Veritas Access 7.4 版本支持以下操作系统：

- 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

为国际化 (I18N) 提供支持

此版本的 Veritas Access 提供中文、日语、韩语 (CJK) 字符的 I18N 支持。Veritas Access 接受 CJK 字符输入。输出和其他标题消息为英语。

支持包括：

- **Storage**、**ObjectAccess**、**NFS**、**CIFS**、**FTP** 和 **SmartIO** 模块支持 CJK 字符。
- 只能在对象名称中使用 CJK 字符。
- 在 `list`、`show` 和 `status` 命令中，使用 CJK 字符创建的对象显示方式相同。

- 您可以按与其余进行了 I18N 移植的命令相同的方式，对使用 CJK 字符创建的对象执行所有操作。
- CLISH 和 GUI 支持 CJK 字符。
- 对于 RHEL 支持的其他语言，尚未进行测试。

支持不包括：

- 除上述模块外，其他模块不接受 CJK 字符输入。
- 通过 **Storage**、**ObjectAccess**、**NFS**、**CIFS**、**FTP** 和 **SmartIO** 模块使用包含 CJK 字符的名称创建的对象，不能作为尚未进行 I18N 移植的模块中的命令输入。
  例如，使用 CJK 语言创建的文件系统不能用于在尚未进行 I18N 移植的模块中创建对象。
- **横向扩展文件系统**的名称不能使用英语以外的任何其他语言。

表 1-1 支持 I18N 的功能

模块名称	对象
池	`pool_name`
文件系统	`pool_name` `fs_name`
策略	`policy_name` `pattern`
Worm	`fs_name`
配额	`fs_name`

回滚	`fs_name`
	`rollback_name`
	`cache_name`

快照	`fs_name`
	`snapshot_name`
	`schedule_name`

FSCK 或碎片整理	`fs_name`

模块名称	对象
压缩	fs_name pattern schedule_name
NFS	share path **注意：** GNFS 仅支持英语的共享名称。
CIFS	file system path、directory path share_name 主目录的 fs_name **注意：** Local user name 和 group management name 只支持使用英语。
FTP	主目录中的 fs_name 目录中匿名日志中的 fs_name
SmartIO	fs_name cache_name file_name

本版本不支持

本版本不支持以下功能：

- Veritas Access 不支持对 PAM 或其他操作系统安全设置进行更改。如果对 PAM 或其他安全设置进行任何更改，则身份验证设置可能不起作用。
  例如，您可能无法为使用 CLISH 添加的主用户和新用户更改密码。
- IPv6 地址不支持复制。

技术预览功能

以下功能可用作此版本中的技术预览功能：

Veritas Access Streamer 作为 Enterprise Vault 的存储类型

在此版本中，“选择 Veritas Access Streamer 作为 Enterprise Vault 的存储类型”是一项技术预览功能。

注意：仅测试和开发环境支持此功能。生产环境不支持。

您需要运行 Enterprise Vault 11 及更高版本。

您可以使用 Veritas Access Streamer 安装向导安装 Veritas Access Streamer。Veritas Access Streamer 安装程序位于以下位置：

`dvd1-redhatlinux/rhel7_x86_64/EV_Streamer/Veritas_Access_Streamer_Setup.msi`

安装 Veritas Access Streamer

1. 运行 Veritas Access Streamer 安装程序。系统将提示您选择要安装的位置。必须选择默认位置。

   单击 **Next**。

2. 安装程序已准备好在系统上安装 Veritas Access Streamer。单击 **Next** 开始安装。

3. 弹出一个窗口，其中显示安装进度。安装完成后，单击 **Close** 退出安装。

4. 打开管理员命令提示符并导航到 `C:\program files(x86)\Enterprise Vault\Veritas Access Streamer`。

5. 运行 `regsvr32 VeritasAccessStreamer.dll`。将弹出一条消息，指明注册成功。

6. 转到 `C:\program files(x86)\Enterprise Vault\Veritas Access Streamer\xml`，以获取 `EvExtendedSetttings.xml` 文件，并将 Veritas Access Streamer 配置为 Enterprise Vault 的存储类型，以便 Enterprise Vault 管理控制台能够识别 Veritas Access Streamer 设备。

   请参见第 11 页的“将 Veritas Access Streamer 配置为 Enterprise Vault 的存储类型”。

7. 创建新分区，并验证 Veritas Access Streamer 是否列为存储选项之一。

可以在 Enterprise Vault 服务器上执行以下步骤。

将 Veritas Access Streamer **配置为** Enterprise Vault **的存储类型**

1. 打开 Windows 资源管理器，然后导航到 **<Program Files (x86)>\Enterprise Vault\InitialConfigurationData\en\Policies**。

2. 创建 `EVExtendedSettings.xml` 的副本。

3. 将 `EVExtendedSettings.xml` 替换为 Veritas 提供的版本。使用在 `C:\Program Files(x86)\Enterprise Vault\Veritas Access Stream\xml` 中创建的 xml 文件。安装 `Veritas Access Streamer setup.msi` 后会提供此 xml 文件。

   请参见第 11 页的“安装 Veritas Access Streamer”。

4 更新注册表值：
`[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KVS\Enterprise Vault\Admin] "PopulateExtendedSettingTypes"="1"`。

5 关闭并重新启动 Enterprise Vault 管理控制台 (VAC)。

6 导航到 **Policies > Exchange**。

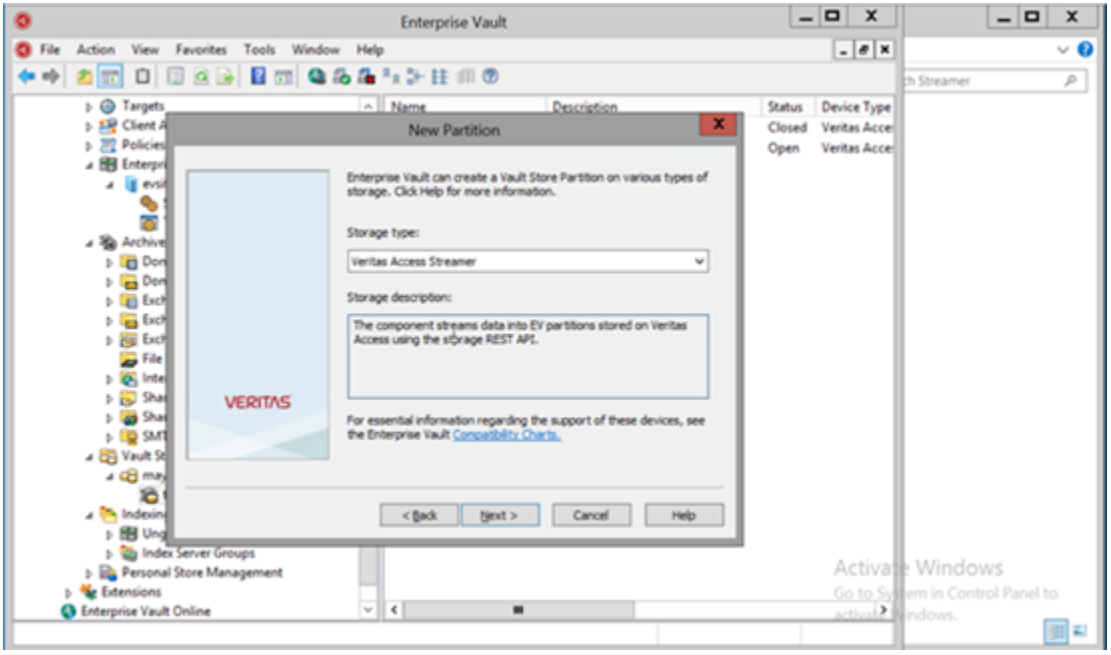
7 右键单击 **Exchange**，然后单击 **Populate Setting Types**。

将显示一条消息，指明已成功填充目录数据库中的 **SettingsType** 表。

8 使用 Veritas Access Streamer 作为存储，在所有 Enterprise Vault 存储服务器上重新启动存储服务。

服务启动后，配置分区时，Veritas Access Streamer 将作为一种存储类型显示出来。

9 选择 **Veritas Access Streamer**，然后单击 **Next**。

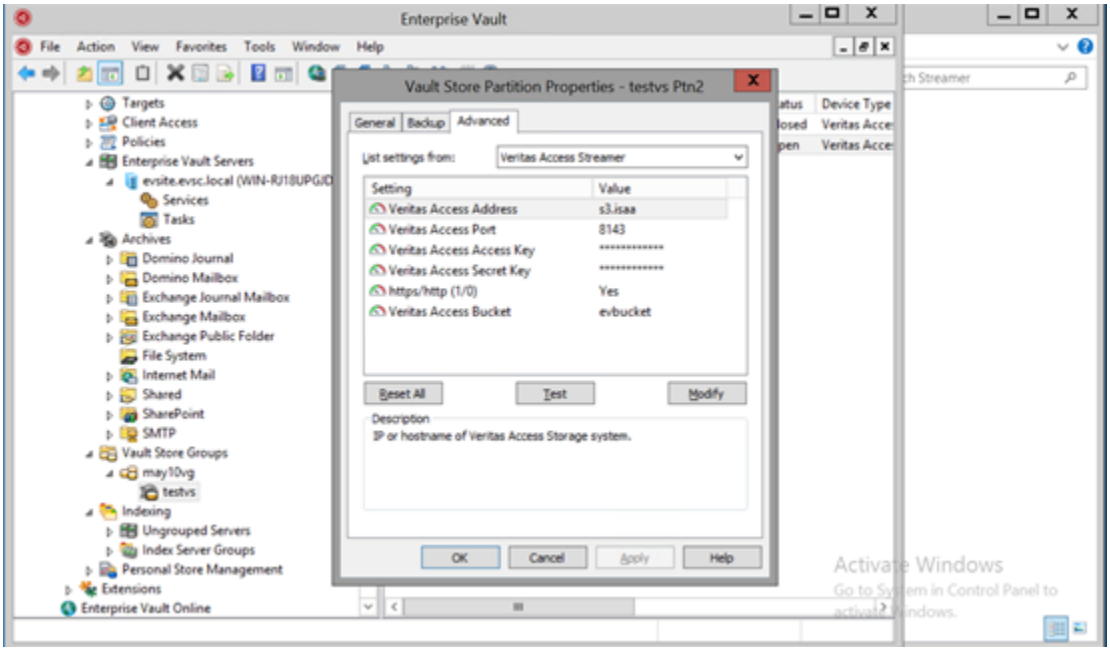


现在，必须配置 Veritas Access Streamer。

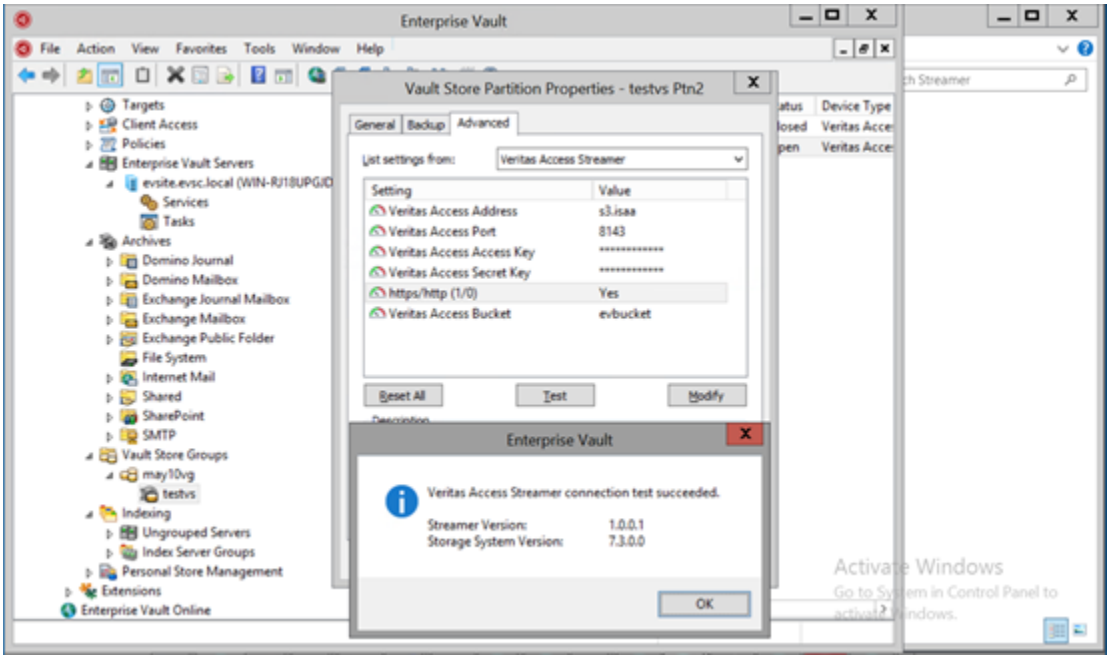
配置 Veritas Access Streamer

1 配置 Veritas Access Streamer 的属性。

名称	定义	示例值
Veritas Access 地址	Veritas Access 存储系统的主机名。	s3.isaa
Veritas Access 端口	Veritas Access 存储系统上的服务器侦听 http 请求的端口。	8143
Veritas Access 访问密钥	用户访问存储桶所用的访问密钥。	********
Veritas Access 密钥	用户访问存储桶所用的密钥。	********
http/https	表示是否应使用 SSL 连接到服务器。	是
Veritas Access 存储桶	存储分区数据的存储桶。	evbucket



2 转到分区设置上的 **Advanced**，然后单击 **Test**。将弹出一条消息，指明连接测试成功。



对于基于 S3 协议的 LTR 用例，支持在横向扩展文件系统中使用纠删码

在此版本中，“对于基于 S3 协议的 LTR 用例，支持在横向扩展文件系统中使用纠删码”功能是一项技术预览功能。

对于 LTR 用例，可以使用纠删码布局创建横向扩展文件系统。

不使用 EC log 配置纠删码 (EC)，以便提高性能。

可通过 LTR 策略和 Veritas Access 创建横向扩展文件系统纠删码存储桶。

有关 LTR 策略的详细信息，请参见 *Veritas Access Online Help*（《Veritas Access 联机帮助》）。

要通过 Veritas Access 创建横向扩展纠删码存储桶，请在 Veritas Access (ObjectAccess) 中使用以下命令设置参数。

```
ObjectAccess> set fs_type largefs ecoded 4 2 16k stripe_aligned=yes
stripe_tag=disk rotating_parity=yes
```

注意：在此版本中，除了基于 S3 协议的 LTR 用例外，对于其他用例，不支持在横向扩展文件系统中使用纠删码。

有关横向扩展纠删码文件系统参数的信息，请参见 *Veritas Access Command Reference Guide*（《Veritas Access 命令参考指南》）。

Veritas Access 简单存储服务 (S3) API

表 1-2 列出了 Veritas Access 简单存储服务 (S3) API。

表 1-2 Veritas Access 简单存储服务 (S3) API

API	说明
abort-multipart-upload	中止多部分上传。
complete-multipart-upload	通过组合以前上传的部分完成多部分上传。
create-multipart-upload	启动多部分上传。
delete-bucket	删除存储桶。
delete-object	删除存储桶中的指定对象。
get-bucket-acl	获取存储桶的 ACL。
get-bucket-(list objects) Version 1	列出存储桶中所有对象。
get-bucket-(list objects) Version 2	列出存储桶中所有对象。
get-bucket-location	获取对象的存储桶区域。
get-object	从 Veritas Access S3 存储桶中检索对象。
get-service	列出经过身份验证的发件人拥有的所有存储桶。
head-bucket	确定存储桶是否存在。
head-object	从对象中检索元数据，但不返回对象本身。
initiate-multipart-upload	启动多部分上传并返回上传 ID。
list-multipart-uploads	列出正在进行的多部分上传。
list-parts	列出某个特定多部分上传中已上传的部分。

API	说明
put-bucket	创建新的存储桶。
put-bucket-acl	使用 ACL 对现有存储桶设置权限。
put-object-copy	为已存储在 Veritas Access S3 服务器中的对象创建副本。
put-object	将对象添加到存储桶中。
upload-part	在多部分上传中上传一部分。
upload-part-copy	通过从现有对象复制数据来上传一部分。

有关 Veritas Access 简单存储服务 (S3) API 的详细信息，请参见 *Veritas Access Restful API Guide*（《Veritas Access Restful API 指南》）。

2

已解决的问题

本章节包括下列主题：

此版本中已解决的问题

本节介绍自上一版本以来解决的问题。

表 2-1 自上一版本以来解决的问题

已解决的问题	说明
IA-9087	删除或修改与 OpenDedup 卷关联的虚拟 IP 会导致 OpenDedup 卷进入不一致状态
IA-9659	如果禁用再重新启用防火墙，则会阻止 OpenDedup 端口
IA-9730	重新启动操作后，OpenDedup 卷不会在介质服务器上通过 /etc/fstab 自动装入
	如果删除 OpenDedup 卷使用其 IP 地址的网络设备，会影响使用该卷的备份作业
IA-1943	对块大小为 5 MB 的 10 GB 文件执行多部分上传时，ObjectAccess 服务器进入故障状态
IA-5737	启用 SSL 后，ObjectAccess 操作在虚拟托管式寻址中不会正确运行
IA-7434	对于多部分上传，存储桶中可能存在临时对象
IA-8747、IA-8649	如果 FTP 会话超过 1000 个，FTP> session showdetails 命令需要很长时间才会响应或者挂起
IA-9697	LIO 不支持大写形式的目标名称

已解决的问题	说明
IA-7685	为 Enterprise Vault 用户设置归档目录的完全访问权限时出错

3

软件限制

本章节包括下列主题：

使用共享 LUN 的相关限制

以下限制与 Veritas Access 中的共享 LUN 相关。

Veritas Access 不支持精简 LUN

Veritas Access 不支持精简 LUN。如果使用了精简 LUN，则某些 CLISH 命令可能会失败。

灵活存储共享的相关限制

以下问题与 Veritas Access 灵活存储共享 (FSS) 相关。

如果群集具有 DAS 磁盘，则安装时必须将该群集名称限制为 10 个字符

格式化 DAS 磁盘时，需为磁盘提供唯一名称。该名称包括嵌入的群集名称。DAS 磁盘名称的长度限制为 25 个字符。为具有 DAS 磁盘的群集选择群集名称时，必须将该群集名称限制为 10 个字符。

与安装和升级相关的限制

以下限制与安装和升级相关。

如果未配置所需的 VIP，则 NFS、CIFS 和 S3 等服务无法正常运行

如果安装过程中未配置所需的 VIP 数量，则 NFS、CIFS 和 S3 等服务将无法正常运行。如果未正确配置 VIP，高可用性也会受到影响。

使用以下 CLISH 命令添加每个服务所需的 VIP 数量：

```
# network ip addr add <ipaddr> <netmask> <type (virtual)> [device]
[nodename]
```

CLISH 不支持滚动升级

仅支持使用安装程序执行滚动升级。

备份模式下的限制

如果执行 `Cluster> del` 操作时备份组处于联机状态，则 `Cluster> del` 操作失败并显示以下错误消息：

```
CPI WARNING V-9-40-6450 Active backup jobs are running on access_01.
Deleting this node from the cluster may cause the backup to fail.
```

Veritas Access IPv6 限制

IPv6 不支持以下 Veritas Access 模块：

- NIS

CIFS 不支持以下 IPv6 功能：

- CIFS 不支持对域控制器使用 IPv4/IPv6 混合模式。需要从 DNS 服务器中移除 IPv4 DNS 条目。
- CIFS 不支持在 Veritas Access CLI 中对域控制器使用 IPv6 地址。域控制器条目只能使用 FQDN。FQDN 可解析为 IPv6 地址。

FTP 限制

以下限制与 FTP 相关。

- 不支持使用 NFS、CIFS 等其他协议对 FTP 进行多协议访问。

Intel Spectre Meltdown 限制

以下限制与 Intel Spectre Meltdown 相关。

Veritas Access 建议将内核升级到以下版本之一，这些版本将会解决由内核造成的 Intel Spectre Meltdown 问题。

- RHEL 7.4：3.10.0-693.21.1.el7.x86_64
- RHEL 7.3：3.10.0-514.36.5.el7.x86_64

Retpoline 是 spectre v2 缓解技术。应在采用 Retpoline 支持的情况下编译内核和产品代码特权部分。编译 Veritas Access 代码时不采用 Retpoline 支持。

Samba ACL 性能相关问题

为了使 ACL 改进生效（减少了属性节点数），用于创建文件和目录的默认掩码已设置为 775。先前，创建掩码设置为 744。

如果将掩码更改为 775 以外的值，则 ACL 改进可能无效，因为 POSIX ACL 的计算将在掩码更改时发生明显变化。

性能改进还取决于文件打开模式。当前实现方式考虑的是使用 Windows 资源管理器或命令窗口打开正常文件。Samba 可以计算不同的打开模式，具体取决于父目录

的权限以及 Windows 客户端发出的实际打开请求。这些考虑事项将影响性能的实际改进效果。

在 Veritas Access 群集中使用 InfiniBand NIC 的限制

- 除非 InfiniBand NIC 已连接到公用网络或已被排除，否则该 NIC 为首选专用 NIC。
- 如果在同一网卡上，NIC 的 PCI ID 均相同，则 InfiniBand NIC 可能不支持 NIC 绑定功能。

  注意：Mellanox 卡上会出现这种情况。

- InfiniBand NIC 支持 NIC 排除功能，但在排除操作期间，具有相同 PCI ID 的所有 NIC 都会被排除。

  注意：Mellanox 卡上会出现这种情况。

- 新添加的节点应当具有相同的 InfiniBand NIC 配置。例如，如果 Veritas Access 群集使用 LLT over RDMA，则新添加的节点应将 RDMA NIC 作为专用 NIC 进行连接。
- Veritas Access 不支持混合的 LLT 连接，这意味着如果计划使用 LLT over RDMA，则群集节点中的所有节点都应使用 InfiniBand NIC。否则，请在 Veritas Access 安装过程中使用 NIC 排除功能来排除 InfiniBand NIC。

在非 SSH 环境中与命令相关的限制

仅当为 root 用户配置了无密码 SSH 时，某些 CLISH 命令才起作用。如果 `/opt/VRTSnas/con/communication.conf` 文件存在，则 `CommunicationType` 项设置为 `SSH`。

例如：

```
# cat /opt/VRTSnas/conf/communication.conf
{
    "WorkingVersion": "1",
    "Version": "1",
    "CommunicationType": "SSH"
}
```

仅当为 root 用户启用了无密码 SSH 通信时，以下命令才起作用：

- `Backup> install`
- `Cluster> addnode`
- `Cluster> delnode`
- `Cluster> reboot`
- `Cluster> shutdown`
- `FTP> logupload`
- `License> add`
- 所有 `Replication>` 命令
- `Report> exportevents`
- `Report> snmp exportmib`
- `Storage> fencing on`（用于基于多数的防护）
- `Storage> fencing off`（用于基于多数的防护）
- `System> config import`
- `System> config import remote`
- `System> config export`
- `System> config export remote`
- 所有 `Support>` 命令
- `Upgrade> add`
- `Upgrade> install`

在虚拟机环境中使用 Veritas Access 的相关限制

基于 KVM 的虚拟机不支持 Veritas Access。

NFS-Ganesha 限制

以下限制适用于 NFS-Ganesha：

- 无法动态添加客户端。在添加某个导出之后，无法再向该导出中添加更多客户端。解决方法是在创建共享时添加网络组。网络组成员资格可以动态更改。
- NFS-Ganesha v3 不支持 `fcntl lock failover`。
- NFS-Ganesha 不支持 secure_locks、insecure_locks、wdelay、no_wdelay、subtree_check、no_subtree_check 和 fsid 等导出选项。

- NFS-Ganesha 仅支持 OpenStack Cinder。它不支持 OpenStack Manila。
- Veritas Access 不支持 NFS v4 ACL。
- NFS-Ganesha 不支持共享保留。
- NFS-Ganesha 不支持委派。
- NFS 服务器不支持非 ASCII 字符。

基于内核的 NFS v4 限制

以下限制适用于基于内核的 NFS v4：

- Veritas Access 不支持 NFS v4 ACL。
- 不支持 NFS v4 共享保留。
- 不支持 NFS v4 委派。

文件系统限制

以下限制与 Veritas Access 文件系统相关。

- 通过 CLISH 执行的任何直接 NLM 操作可能会导致系统不稳定
  请勿在网络锁定管理器 (NLM) 上通过 CLISH 执行与文件系统相关的任何操作，因为它供内部使用。如果使用 NLM，则 Veritas Access 无法保证群集的稳定性。
- 当创建第一个文件系统时，还会创建一个附加文件系统用于保存锁定和配置信息。用户不可直接操作此附加文件系统。此附加文件系统仅供内部使用。
  在 Veritas Access 中创建第一个存储池时，建议使用尽可能多的节点中的磁盘。对于群集节点中的磁盘都是本地磁盘的非共享环境，会在所有这些节点间创建附加的文件系统镜像。这可确保即使在其上创建附加文件系统的其中一个节点可用，Veritas Access 配置也可用。
  对于 SAN 环境，会在两个磁盘之间镜像附加文件系统。
- 横向扩展文件系统不支持内部分层。
- 群集文件系统中的内部分层只支持一个主层和一个辅助层。

Veritas Access S3 服务器限制

如需下载大于 100 M 的对象，应使用 `Range` 标题且范围不应超过 100 M。

对象必须分不同部分下载。

长期数据保留 (LTR) 限制

以下限制与 LTR 相关。

- 在 Veritas NetBackup 长期保留 (LTR) 用例中，Veritas Access 不支持 GUI 中 S3 存储桶的 HTTPS 应用程序协议。
- 如果为 LTR 用例选择 CC，则需要手动修改数据移动策略。
- 如果为 OpenDedup 卷提供服务的群集节点崩溃，则该特定 OpenDedup 卷上正在进行的 NetBackup 作业可能会失败。但是，在 NetBackup 自动触发的下一次重试时，相同的 NetBackup 作业将会成功。崩溃的节点恢复且 IP 故障回退时，NetBackup 作业可能会再次重新启动。

与复制相关的限制

以下问题与 Veritas Access 中的复制相关。

与间歇性复制身份验证相关的限制

创建间歇性复制链接时，必须提供 master 用户凭据以对用于间歇性复制的不同群集进行身份验证。

与连续性复制相关的限制

- 连续性复制不支持在配置复制之后更改复制模式（同步或异步）。
- 配置复制时，连续性复制不接受采用纠删码 (ecoded) 布局和加密卷的文件系统。
- 在连续性复制下配置的文件系统不支持某些 Veritas Access 文件系统操作，例如增大、缩小、调整大小、添加或移除列、镜像或分层（*largefs* 的云分层除外）。

4

已知问题

本章节包括下列主题：

Veritas Access 已知问题

以下已知问题与 Veritas Access 命令相关。

备份问题

本节介绍与备份相关的已知问题。

启用 SAN 客户端时，在 BackupGrp 切换或故障转移到其他节点之后，备份或还原状态可能显示无效状态

通过 SAN 正在执行备份作业或还原作业且 BackupGrp 切换或故障转移到其他节点时，CLISH 中备份作业的状态选项可能会显示错误状态。

解决办法：

没有解决办法。

CIFS 问题

本节介绍与 CIFS 相关的已知问题。

无法在附加或添加到 homedir 列表的文件系统上启用配额

启用 `Storage> quota cifshomedir` 命令之后，如果将其他文件系统设置为 `cifshomedir`，则默认情况下，该文件系统上不会启用配额。如果使用 `Storage> quota cifshomedir enable` 命令启用配额，则该操作可能成功，也可能失败，具体取决于您将文件系统指定为 `cifshomedir` 时采用的顺序。

`Storage> quota cifshomedir` 仅为 `cifshomedir` 列表中的第一个文件系统启用命令检查。如果该文件系统上已启用配额，则不会在列表中其余文件系统上启用配额。

解决办法：

要解决此问题，请执行以下步骤：

1 运行 `Storage> quota cifshomedir disable` 命令。这将在所有 homedir 文件系统上禁用配额。

2 运行 `Storage> quota cifshomedir enable` 命令。这将在所有 homedir 文件系统上启用配额。

删除 CIFS 共享时，将重置同一文件系统上其他 CIFS 共享的默认所有者和组权限

删除 CIFS 共享时，文件系统上的所有者和组均会恢复为默认权限。所有者和组的默认值均会设置为 root。如果同一文件系统上存在多个 CIFS 共享，此行为可能是个问题。此外，删除其中任何共享时，还会重置文件系统上其他共享的所有者和组。

如果先前已为保留的 CIFS 共享设置所有者权限或组权限，则必须再次设置权限。

解决办法：

如果先前已为保留的 CIFS 共享设置所有者权限或组权限，则必须使用以下命令，再次为文件系统上的 CIFS 共享设置所有者权限或组权限：

`CIFS>` **share modify**

默认 CIFS 共享的所有者不是 root

如果 CIFS 共享 (*share1*) 是使用具有文件系统 (*fs1*) 的非默认所有者（*CIFSuser1*，非 root 用户）创建的，而另一个共享 (*share2*) 是使用默认设置（root 用户作为所有者）通过相同文件系统 (*fs1*) 创建的，则 *share2* 具有非默认所有者 (*CIFSuser1*)。

解决办法：

如果要将同一个文件系统作为不同的 CIFS 共享导出，则使所有共享的 CIFS 共享所有者保持相同。否则，使用不同的文件系统创建不同的 CIFS 共享。

无法在 Windows 服务器或客户端上列出 Veritas Access 群集上创建的 CIFS 共享

如果尝试从使用 Veritas Access 群集 IP (\\10.209.192.85) 的 Windows 客户端计算机列出所有 CIFS 共享，从 Windows 资源管理器呈现列表将失败并显示错误消息：网络共享不可访问。这是因为，为解决漏洞 CVE-2017-7494，Samba 团队添加了新参数 `nt pipe support = no`。

解决办法：

此问题没有解决办法。

CIFS> mapuser 命令无法将所有用户从 Active Directory (AD) 映射到所有 NIS/LDAP 用户

将所有 CIFS 用户映射到 NIS/LDAP 用户时，CLISH 命令不接受特殊字符 *。

解决办法：

使用从 Active Directory (AD) 用户到 NIS/LDAP 用户的一对一用户映射。

Windows 客户端显示的 CIFS 主目录共享大小不正确

在 Windows 客户端上映射 CIFS 共享后，Windows 客户端上显示的 CIFS 主目录共享大小不正确。

解决办法：

没有解决办法。您可以通过 CLISH 运行 `Storage> fs list` 命令，获取正确的 CIFS 主目录共享大小。

重复数据删除问题

本节介绍与重复数据删除相关的已知问题。

移除已启用重复数据删除的装入点的 lost+found 文件时，可能会导致出现重复数据删除问题

对于已启用重复数据删除的装入点，`lost+found` 目录包括一些与重复数据删除相关的文件。如果移除 `lost+found` 文件，则重复数据删除作业可能不会正常工作。

解决办法：

如果意外删除 `lost+found` 目录中的重复数据删除文件，请执行以下步骤来启用重复数据删除。

启用重复数据删除作业：

1 禁用重复数据删除作业。

2 启用重复数据删除作业。

Enterprise Vault 连接的已知问题

以下已知问题与 Enterprise Vault 连接相关。

Enterprise Vault 归档策略未在共享目录中创建 ev_archival 文件夹

Veritas Access GUI 为 Enterprise Vault 的存储配置提供了归档策略。此存储配置过程中，会在 CIFS 共享中创建一个名为 `ev_archival` 的空文件夹。此目录将用作 Enterprise Vault 保管库存储分区的位置。Enterprise Vault 需要在 `ev_archival` 文件夹上具有完全访问权限和所有权，才可将其配置为保管库存储分区。如果归档策略未创建 `ev_archival` 文件夹，则您必须显式创建此文件夹并检查此文件夹的所有权，然后将此文件夹作为分区分配给 Enterprise Vault。

解决办法：

创建一个空文件夹，并将其配置为归档策略创建的共享内的保管库存储分区。

FTP 问题

以下问题与 Veritas Access FTP 命令相关。

如果文件系统用作 FTP 的 homedir 或 anonymous_login_dir，则无法销毁此文件系统

FTP 中没有清除命令可更改 `homedir` 或 `anonymous_login_dir` 来清空其值。可以使用 FTP 设置命令来清空上述两个字段的值。更新上述全部或任一字段（指向其他文件系统或将其清空）之后，即可销毁原始文件系统。

解决办法：

使用 `FTP> set` 命令清除 `homedir` 和/或 `anoymous_login_dir` 的值。

```
# isa> ftp set homedir_path
```

FTP> server start 命令报告 FTP 服务器处于联机状态，即使它未联机也会报告此状态

`FTP> server start` 命令有时报告已成功启动 FTP 服务器，但由于内部问题，联机操作实际上失败了。

解决办法：

使用 `FTP> server status` 命令验证 FTP 服务的状态。如果 FTP 服务处于脱机状态，请再次运行 `FTP> server start` 命令，或运行 `Support> service autofix` 命令修复故障（如果存在）。

FTP> session showdetails user=<AD username> 命令不起作用

`FTP> session showdetails` 命令需要使用 *AD username* 作为其他过滤器参数。您可以指定用户名来过滤出属于该特定用户的会话。如果 *AD username* 采用 DOMAINNAME/USERNAME 格式，则此命令不起作用。这是因为存在内部分析问题。

解决办法：

在域名与 AD 用户名之间添加转义符 (\)。

例如，如果用户名为 *domain\username*，请在 `FTP> session showdetails user=<AD username>` 命令中使用 *domain\\username*。

如果 CIFS 中的安全性未设置为 Active Directory (AD)，则无法通过 AD 用户登录到 FTP

Veritas Access 中的 AD 配置在各协议之间通用。它是通过 `CIFS> set domain/domaincontroller/domainuser` 命令配置的。因此，如果用户要将 AD 用作 FTP 中的安全性，必须通过 CIFS 进行 AD 配置。如果 CIFS 中的安全性未设置为 AD，则无法通过 AD 用户登录到 FTP。通过 CIFS 会话对 AD 配置进行的任何更改也会对 FTP 产生影响。

解决办法：

此问题没有解决办法，因为在 Veritas Access 中，AD 配置在所有协议之间通用。确保使用 `CIFS> set` 命令正确配置 AD。要在 CIFS 之外的协议中使用，请将 CIFS 中的安全性设置为 AD。

当安全性设置为本地时，如果是全新的操作系统和 Veritas Access 安装，则 FTP 不起作用

当安全性设置为本地时，控制台节点上不存在 `+/home/ftpuse+r` 目录。因此，不能使用 FTP 登录。

解决办法：

使用其他节点（非主节点）的虚拟 IP 登录。

GUI 问题

以下问题与 GUI 相关。

同时设置连续性复制链接和间歇性复制链接时，使用高可用性和数据保护策略配置存储不起作用

执行以下步骤时会出现这种情况：

- 同时设置连续性复制链接和间歇性复制链接。
- 激活高可用性和数据保护策略。
- 通过配置存储向导，使用其中一个策略配置存储。
- 设置间歇性复制作业任务失败。

这是因为，即使选择了间歇性复制链接，在存储配置期间，GUI 仍会选择连续性复制链接来设置间歇性复制作业，从而导致任务失败。

解决办法：

使用上述两个策略配置存储时，不要同时创建连续性复制链接和间歇性复制链接。由于这两个策略都使用文件系统复制链接，因此仅创建间歇性复制链接即可。

添加新节点或安装并配置新群集时，故障转移后，GUI 可能无法在控制台节点上启动

某控制台节点执行节点故障转移后，GUI 服务应在此故障转移的控制台节点上自动启动。但它无法启动，因为 GUI 未在所有节点上正确配置。您无法使用 GUI 管理存储群集。

解决办法：

发生故障转移时：

- 登录到控制台节点并运行以下命令：

  ```
  # python /opt/VRTSnas/isagui/init_application.py production
  ```

- 等待应用程序完成配置并显示消息：

  ```
  Application started on Node JS
  ```

- 输入 CTRL-C，终止应用程序。
- 输入以下命令：

  ```
  # service vamgmt start
  ```

您可以使用 GUI 访问存储群集。

升级早期版本的 Veritas Access 群集时，GUI 显示过时和不完整的数据

如果升级旧群集并启动 GUI，GUI 页面上会显示旧事件和不完整的数据。

解决办法：

升级群集后，请从控制台节点运行以下命令：

```
# /opt/VRTSnas/pysnas/bin/isaconfig
```

作为命令的一部分重新启动服务器以添加和删除证书会在 RHEL 7 上显示错误

将外部证书添加到 Veritas Access 后，会隐式执行 Web 服务器重新启动，以启动新提供的证书。Web 服务器隐式启动在 RHEL7 中不起作用，因为 RHEL6 和 RHEL7 中的命令不同。

解决办法：

在 CLISH 中运行 `System> guienable` 命令以启动服务器。

使用 OpenSSL ocsp 验证客户端证书在 RHEL7 上不起作用

2FA 需要执行客户端证书验证。可在 RHEL6 中成功验证证书。在 RHEL7 中，需要传递名为 *–VAfile* 的显式参数和签名者证书，但没有传递。因此，使用证书验证客户端在 RHEL7 上不起作用。

解决办法：

此问题没有解决办法。

安装和配置问题

以下问题与 Veritas Access 安装和配置相关。

重新启动使用 RDMA LLT 的节点后，LLT 不起作用，或 gabconifg –a 命令显示危险状态

默认情况下，Veritas Access 群集节点上将启用 iptable。iptables 可能会影响 RDMA 网络的 LLT 功能。

由于 LLT 使用 UDP 在 RDMA 网络中进行通信，因此，应将规则添加到 iptables 中以允许 LLT 连接。

iptable 规则在加载 LLT 模块之前生效。iptables 规则由 Veritas Access 脚本管理，该脚本在 VCS 启动之后执行（VCS Service Group 处于联机状态时启动）。加载 LLT 时，iptables 处于默认状态，通过 UDP 进行的 LLT 连接将被阻止。

解决办法：

如果在 RDMA LLT **环境中重新配置** Veritas Access：

1 完成所有配置之后，登录到每个节点并通过输入以下内容禁用 iptables：

```
# chkconfig --level 123456 iptables off
```

2 重新启动所有节点。如果重新启动过程无法卸载 OPENIB 模块，请通过电源管理重置节点。

如果在 RDMA LLT **环境中添加** Veritas Access **节点**：

1 添加节点完成之后，登录到每个节点（包括新添加的节点）并通过输入以下内容禁用 iptables：

```
# chkconfig --level 123456 iptables off
```

2 重新启动所有节点。如果重新启动过程无法卸载 OPENIB 模块，请通过电源管理重置节点。

运行各个 Veritas Access 脚本时可能会返回不一致的返回代码

Veritas Access 中各个脚本的设计目的不是要独立运行。CLISH 是 Veritas Access 中唯一支持所有操作的界面。如果单独运行 Veritas Access 脚本，则返回代码在某些情况下无法保证结果一致。

SSH 连接断开时使用安装程序配置 Veritas Access 失败

使用安装程序安装和配置 Veritas Access 时，可能会看到以下错误消息：

```
CPI ERROR V-9-20-1073 Failed to copy /opt/VRTSsnas/conf/conf.tar
```

在极少数情况下，当安装程序因 ssh 连接断开而无法将配置文件复制到群集中的节点时，会出现此消息。

解决办法：

解决此问题：

1 手动恢复 ssh 连接。

2 卸载 Veritas Access。

3 重新安装 Veritas Access。

使用响应文件配置 Veritas Access 时，从配置中排除 PCI 失败

如果使用响应文件配置 Veritas Access，Veritas Access 不会排除那些标记为要排除的 PCI。在配置期间，安装程序将跳过要排除的 NIC。

解决办法：

使用标准配置方法，或在响应文件中同时配置 NIC 绑定和排除。

在 I/O 防护配置期间初始化磁盘之后，安装程序没有立即列出已初始化的磁盘

在安装程序启动进程之后，选择配置 I/O 防护时，至少应当有三个已初始化的共享磁盘。如果没有三个共享磁盘，则安装程序可初始化共享磁盘。安装程序初始化磁盘之后，安装程序不会立即列出已初始化的磁盘。

解决办法：

初始化磁盘之后，如果在安装程序列表中未看到新磁盘，请等待几秒钟。然后，选择 **y** 继续配置 I/O 防护。安装程序将列出已初始化的磁盘。

如果同一驱动节点同时用于两个安装，则第二个安装显示第一个安装的进度状态

Veritas Access 安装程序不支持同时从同一驱动节点进行多个安装。这是专门设计的。如果从同一驱动节点启动两个安装，则第二个安装还会显示第一个安装的进度状态。

解决办法：

不要同时在同一驱动节点上执行多个安装。

如果同一驱动节点同时用于两个或多个安装，则第一个安装会话将终止

Veritas Access 安装程序不支持同时从同一驱动节点进行多个安装。这是专门设计的。如果从同一驱动节点启动两个安装，则第一个安装将终止。

解决办法：

不要同时在同一驱动节点上执行多个安装。

当从属节点处于重新启动、关闭或崩溃状态时，如果运行 Cluster> show 命令，则从属节点将引发异常

在特定流中，如果处于重新启动、关闭或崩溃状态的节点正在运行，则系统将计算正在运行的节点的列表。当该命令开始计算 CPU 或网络统计信息时，它在 SSH 上变为不可访问。内部库将引发异常。

当节点状态处于关闭、重新启动或崩溃状态时，从属节点在 Veritas Cluster Server (VCS) 中将从 RUNNING 更改为 FAULTED。`Cluster> show` 命令可恢复其正常行为。即：它不会显示任何异常，且可提供预期输出。

解决办法：

此问题没有解决办法。系统将自行恢复。您需要稍等片刻并再次运行 `Cluster> show` 命令。

如果为 PCI 排除添加重复的 PCI ID，Cluster> add node name 命令将会失败

要添加具有要排除的唯一 PCI ID 的新节点，需要使用 `Network> pciexclusion add` 命令通过 CLISH 添加这些唯一 PCI ID。如果这些唯一的 PCI ID 已存在于 Veritas Access 的 PCI 排除配置中，则生成的配置将具有重复条目。为 PCI 排除生成配置之后，如果继续使用已添加的节点，则操作将会失败。`Cluster> add node` 操作无法处理 PCI 排除配置中的重复条目。

解决办法：

请联系技术支持，从 Veritas Access PCI 排除配置文件中移除重复的 PCI ID。然后，可以运行 `Cluster> add node` 命令。

如果从群集节点开始使用响应文件进行安装，则安装会话在配置 NIC 阶段完成后终止

如果使用响应文件从群集节点安装 Veritas Access，则安装程序不会在配置 NIC 之后提供重新连接到安装的警告消息。

解决办法：

1 使用新的公用 IP 地址登录到 Veritas Access。

2 执行以下命令以继续安装：

```
# /opt/VRTS/install/bin/tmux attach-session -t VA_INSTALL
```

完成系统验证检查之后，安装程序显示一条有关缺少第三方 RPM 的警告消息

完成系统验证检查之后，安装程序显示一条有关缺少所需的第三方 RPM 或需要升级这些 RPM 的警告消息。该警告消息指示验证检查已成功完成。

在安装过程中，系统将通过 Veritas Access ISO 映像安装或升级缺少的所需第三方 RPM。

解决办法：

您可以放心地忽略此警告消息。

使用 installaccess 命令从群集节点中安装和配置该产品时，安装程序看上去会挂起

如果尝试使用 `installaccess` 命令从群集节点中安装和配置本产品，安装程序在“Redefining network configurations”会话之后看上去似乎已挂起。但实际上，安装程序并未挂起，只是需要较长时间执行。

解决办法：

等待安装程序完成配置。重新定义网络配置之后，安装程序大约需要 20 分钟才能完成其余任务。此外，也可以通过 `access72` 命令从第三个节点中安装和配置产品，以避免此问题。

滚动升级的第 1 阶段在第一个节点上完成之后，在第二个节点上出现崩溃

在 Veritas Access 群集上执行滚动升级时，当第 1 阶段在第一个节点上完成之后，第二个节点上出现崩溃。之所以会触发崩溃，是因为第一个节点为新产品版本，而第二个节点仍保留使用旧的产品版本。

解决办法：

等待第二个节点从崩溃中恢复正常。这大约需要 10 分钟。然后，可以在群集上继续滚动升级过程。

如果在完成群集配置之后从 CLISH 创建另一个 VLAN 设备，则 VLAN 设备的虚拟组不会联机

如果 CPI 安装程序配置过程中在绑定设备上创建 VLAN 设备，然后尝试在完成群集配置之后从 CLISH 创建另一个 VLAN 设备，则 VLAN 设备的虚拟组不会成功联机。

解决办法：

如果 VLAN 设备的虚拟组处于 *OFFLINE* 或 *FAULTED* 状态，则输入以下命令：

```
# hagrp -clear <group-name>
# hagrp -online <group-name> -any
# hagrp -state <group-name>
```

虚拟组的状态变为 *ONLINE*。

如果在系统上预配置 LDAP 或 autofs 主目录，Veritas Access 安装会失败

如果存在以下情况，Veritas Access 安装 (7.x) 可能会失败：

- 在系统上配置 LDAP
- 在系统上配置 autofs 主目录

这会在安装 Veritas Access 安装所需的用户主目录时引发问题。

解决办法：

安装 Veritas Access 之前，不要在系统上配置 LDAP 或 autofs 主目录。

在 RHEL 7.3 上执行从 Veritas Access 7.3.0.1 到 7.4 的滚动升级时，在节点升级到 Veritas Access 7.4 后，CIFS 服务进入故障状态

在群集节点上完成滚动升级后，不会为CIFS配置文件创建软链接。因此，CIFS服务不会联机。这会导致 CIFS I/O 路径很长时间不可用。

解决办法：

在群集的每个节点上完成升级后，手动为相应节点上的CIFS配置文件创建软链接。这将使该节点上的 CIFS 服务联机。在群集的每个节点上完成滚动升级后，在相应节点上运行以下命令：

```
# ln -sf /opt/VRTSnas/scripts/cifs/SambaServer_online
/opt/VRTSvcs/bin/SambaServer/online
# ln -sf /opt/VRTSnas/scripts/cifs/cifs_va_options /etc/sysconfig/samba
```

完成 Veritas Access 安装后，安装程序不会清除触发安装的 Veritas Access 节点上驱动节点的 SSH 密钥。

从驱动节点安装 Veritas Access 时，安装程序不会删除保存在 */root/.ssh/authorized_keys* 中的 SSH 密钥。因此，即使在完成安装后，您也可以在不使用密码的情况下通过 SSH 连接到 Veritas Access 节点。

解决办法：

检查驱动节点的 SSH 密钥，并从群集的所有 Veritas Access 节点中删除该密钥。

如果节点的 yum 存储库较旧，且没有 Internet 连接，无法访问 RHN 存储库，则 Veritas Access 安装将失败

如果您尝试安装 Veritas Access，而节点中的 yum 存储库已过期，则安装程序将尝试访问 RHN 存储库以更新 yum 存储库。如果您没有 Internet 连接，安装将失败。

解决办法：

删除 `/etc/yum.repos.d` 中存在的 yum 存储库的 yum 配置文件。然后，运行 `yum clean all` 命令，以刷新 yum 存储库信息。重新运行 Veritas Access 安装程序。

在滚动升级后，某些虚拟组不会联机

在滚动升级后，由于虚拟组的某些资源处于脱机状态，因此某些虚拟组不会联机。Phantomgroup_pubeth<number> 的 phantomproc_<interface_name> 资源不会联机。因此，Phantomgroup_pubeth<number> 不会联机。

解决办法：

使用以下命令使资源联机。

```
[root@varnic_01 ~]# hares -online phantomproc_ens161 -sys varnic_01
[root@varnic_01 ~]# hares -state phantomproc_ens161
#Resource          Attribute             System     Value
phantomproc_ens161 State                 varnic_01  ONLINE
phantomproc_ens161 State                 varnic_02  ONLINE
[root@varnic_01 ~]#
```

如果您不知道完整的资源名称，请执行以下步骤查找资源名称，然后使其联机。

查找资源名称，然后使其联机

1 使用 hastatus -sum 命令查找处于脱机状态的虚拟组的名称。

2 使用以下命令查找虚拟组的资源。

```
[root@varnic_01 ~]# hagrp -resources Phantomgroup_pubeth0
phantomproc_ens161
phantomNIC_ens161
```

3 使用以下命令检查资源的状态。

```
[root@varnic_01 ~]# hares -state phantomproc_ens161
#Resource          Attribute             System     Value
phantomproc_ens161 State                 varnic_01  OFFLINE
phantomproc_ens161 State                 varnic_02  ONLINE
```

4 使用以下命令使资源联机。

```
[root@varnic_01 ~]# hares -online phantomproc_ens161 -sys varnic_01
[root@varnic_01 ~]# hares -state phantomproc_ens161
#Resource          Attribute             System     Value
phantomproc_ens161 State                 varnic_01  ONLINE
phantomproc_ens161 State                 varnic_02  ONLINE
[root@varnic_01 ~]#
```

5 验证虚拟组的状态。现在，虚拟组应为联机状态。

```
[root@varnic_01 ~]# hagrp -state Phantomgroup_pubeth0
#Group               Attribute             System     Value
Phantomgroup_pubeth0 State                 varnic_01  |ONLINE|
Phantomgroup_pubeth0 State                 varnic_02  |ONLINE|
[root@varnic_01 ~]#
```

在执行滚动升级后，节点上的协议版本不同

在群集节点上执行滚动升级时，可能会发生以下情况：在某一群集节点上未成功执行第 1 阶段，但在所有节点上执行了第 2 阶段。在这种情况下，发生故障的节点上的协议版本较低。因此，由于节点上的协议版本不同，节点无法形成一个群集。

解决办法：

在群集的所有节点上执行滚动升级的第 1 阶段。如果在所有节点上成功执行了第 1 阶段，则在节点上执行第 2 阶段。这样，将会在所有节点中升级协议版本，在滚动升级后，节点将能够形成一个群集。

使用预配置的 VLAN 和预配置的绑定安装 Veritas Access 失败

如果尝试使用预配置的 VLAN 和预配置的绑定安装 Veritas Access，则安装会失败。这是因为在安装期间，您可以预配置VLAN，也可以将绑定预配置为公用设备，但不能同时预配置二者。

解决办法：

在安装后，您可以使用 `Network> bond create` 命令基于特定网络接口创建绑定。您可以使用 `Network> vlan create` 命令创建 VLAN。

国际化 (I18N) 问题

本节介绍与 I18N 相关的已知问题。

命令中出现外语字符时，CLISH 提示符将消失

英语和非英语字符具有不同的字符编码。因此，命令中有外语字符且您尝试使用向上和向下箭头键修改命令时，CLISH 提示符将消失。

解决办法：

您可以使用以下任一方法：

- 注销并再次登录到 CLISH。
- 按 `Ctrl + C`。
- 将区域设置设为预期的非英语语言。启动 CLISH。
  支持的语言包括中文、日语和韩语。

网络问题

本节介绍与网络相关的已知问题。

CVM 服务组意外进入故障状态

当存储连接中断且恢复到正常状态时，会发生此问题。如果触发“minor number mismatch”问题，则 Veritas Volume Manager (VxVM) 无法加入该节点上的群集。

解决办法：

重新引导出现此问题的节点。

在混合了 IPv4 和 IPv6 VIP 的网络设置中，IP 平衡不考虑 IP 类型

在混合了 IPv4 和 IPv6 的设置中，IP 平衡不考虑 IP 类型。此行为意味着群集中的节点上最终可能没有 IPv6 VIP。IP 平衡应当考虑 IP 类型。

解决办法：

根据需要，手动将节点上相应 IP 类型的 VIP 设为联机。

如果在 LDAP 中未找到条目，则网络组搜索不会在 NIS 中继续搜索

如果 nsswitch 设置中的网络组查找顺序是先搜索 LDAP、然后搜索 NIS，那么当 LDAP 中未找到网络组条目时，网络组搜索不会在 NIS 中继续搜索。在这种情况下，如果使用网络组导出共享，则 NFS 客户端上的 NFS 装入将失败。

解决办法：

更改网络组查找顺序，使 NIS 在 LDAP 之前搜索：

```
Network> nsswitch conf netgroups nis ldap
```

如果托管 VIP 和 PIP 的接口并非当前 IPv6 默认网关接口，则 VIP 和 PIP 在当前 IPv6 子网之外不可访问

在非默认网关接口上配置的 IPv6 地址不可从当前子网外部进行访问。即：无法使用当前默认网关。使用网关时，只有当前默认 IPv6 网关接口上托管的 IPv6 地址才可访问。

解决办法：

不使用当前在默认网关接口上处于未联机状态的 VIP 进行当前子网外部的群集通信。

在两个专用 NIC 之间或一个专用 NIC 与一个公用 NIC 之间交换网络接口后，不探测从属节点上的服务组

要在两个专用 NIC 之间或一个专用 NIC 与一个公用 NIC 之间执行网络接口交换，群集中应只存在一个节点。如果存在多个节点，则网络接口交换后不会探测其余节点。

解决办法：

在未探测其资源的所有节点上执行以下命令：

```
# hastart
```

在操作系统升级后无法导入网络模块

Veritas Access 7.4 版本支持 NIC 名称保留功能。因此，如果您执行操作系统升级，则无法导入网络模块。

解决办法：

在安装 Veritas Access 7.4 之前，将公用 NIC 重命名为 public0、public1 等。将专用 NIC 重命名为 priveth0 和 priveth1。

如果升级 Veritas Access，则带有 'SSL on' 的 LDAP 不起作用

如果将 Veritas Access 从 7.3.x 升级到 7.4，由于升级路径中存在一个错误，即不要求用户提供正确的 LDAP 证书，因此以下命令不起作用。

```
# network> ldap set ssl on
```

因此，在升级后，带有 'SSL on' 的 LDAP 不起作用。

解决办法：

升级完成后，使用以下命令再次设置 'SSL on' 选项：

```
# network> ldap set ssl on
```

网络负载平衡器未配置 IPv6

如果使用 CLISH 为负载平衡器配置了 IPv6 虚拟 IP，负载平衡器配置看起来成功了，但并不在后台对负载进行平衡。这是因为不支持对负载平衡器使用 IPv6。

解决办法：

没有解决办法。

NFS 问题

本节介绍 NFS 问题。

使用 NFS-Ganesha 版本 4 的 Solaris 10 客户端性能低下

对于 NFS-Ganesha 服务器目录操作 `mkdir`、`rmdir` 和 `open`，从 Solaris 客户端中执行时操作速度较慢。

解决办法：

对于使用 Solaris 平台的性能关键型工作量，请使用基于内核的 NFS 版本 3 服务器。

使用 Linux 客户端的 NFS-Ganesha 的随机写入性能降低

使用 Linux 客户端的 NFS-Ganesha 的随机写入性能会降低。使用 Solaris 客户端时，性能不会降低。

解决办法：

对于高性能随机写入工作量，请使用基于内核的 NFS 服务器。

如果节点之间的时间不同步，则客户端无法查看服务器的最新目录内容

如果更新多个节点中的共享，则客户端上并不会立即显示实际的服务器目录内容，而是需要一些时间。目录内容的缓存无效取决于目录的修改时间。由于时间在群集节点上未同步，因此会显示此缓存无效。

解决办法：

在服务器上配置 NTP 以同步所有节点的时间。

如果重新启动群集节点，则 NFS> share 可能会在一段时间内将共享列为故障状态

在群集中重新启动 NFS-Ganesha 服务器时，可能会发生此问题。它不会影响任何正在进行的 NFS 加载。

解决办法：

等待一段时间，直到 NFS-Ganesha 共享显示为联机状态。

导入 NFS 配置后，NFS-Ganesha 共享出现故障

如果使用 `System> config import` 命令导入任何 NFS 配置，则所有现有 NFS 共享将变为故障状态。

解决办法：

重新启动 NFS 服务。

当共享数超过 500 时，NFS-Ganesha 共享可能不会联机

如果 NFS-Ganesha 共享数达到 500 左右或更多，则在重新启动过程中，NFS-Ganesha 共享可能不会处于联机状态，或者要花更多时间才能联机。

解决办法：

使用网络组或 Kerberos，而不是创建大量的单独共享。

通过多次导出将单个路径导出到多个客户端对 NFS-Ganesha 不起作用

由于 NFS-Ganesha 的特定限制，通过多次导出将路径导出到多个客户端（具有相同或不同权限）在 Veritas Access 中不起作用。

解决办法：

使用网络组将相同路径导出到具有相同权限的多个客户端。不支持将相同路径导出到具有不同权限的多个客户端。

对于 NFS-Ganesha 服务器，将大量共享设为联机或脱机需要较长时间

当存在大量资源（即：导出的文件系统路径）时，NFS-Ganesha 服务器的性能会降低。此行为可能会导致服务器故障后恢复较慢。启动或停止 NFS 服务器也可能需要较长时间。

解决办法：

结合使用网络组和 NFS-Ganesha 服务器。如果遇到此问题，请减少共享数量。仅当具有大量共享时才会出现此问题。

NFS 客户端应用程序可能会在节点重新引导时失败并显示文件句柄过时错误

节点重新启动时，该节点的所有虚拟 IP 均会切换回已重新启动的节点。为保留锁定信息，将在此节点上重新启动 NFS-Ganesha 服务器。VIP 会在共享重新添加到 NFS Ganesha 服务器之前短时间可用。此行为会导致应用程序失败并显示文件句柄过时错误。

解决办法：

如果遇到此错误，则客户端应重试该操作。

NFS> share show 命令不区分脱机共享与联机共享

`NFS> share show` 命令不区分脱机共享与联机共享。发生故障的共享则会正确列出。仅使用 CLISH 命令无法确定共享的状态是联机还是脱机。

解决办法

可以使用 Linux `showmount -e` 命令的输出获取从该特定群集节点中导出的共享列表。

NFS> share show 与 Linux showmount 命令的输出存在差异

使用 `NFS> share show` 命令时，将显示已导出 NFS 客户端的主机名。使用 Linux `showmount` 命令时，将显示已导出 NFS 客户端的 IP 地址。

NFS-Ganesha 服务器始终将给定的主机名解析为 IP 地址，并将 NFS 共享导出到该 IP 地址。与基于内核的 NFS 服务器不同，Linux `showmount` 命令将返回 IP 地址，而不是 export 命令中提供的主机名。这不会影响任何功能，但两个命令的输出有所不同。

解决办法：

可以使用 DNS 验证给定的 IP 地址。

在切换 NFS 服务器之后，客户端上的 NFS 装入会暂停

在将 NFS 服务器从内核 NFS 切换到 NFS-Ganesha（反之亦然）时，客户端上的现有 NFS 装入不再处于活动状态。这是由于在切换服务器之后，服务器上的所有导出都移到新服务器，内核 NFS 和 NFS-Ganesha 服务器的文件处理方法不同。因此，客户端上的 NFS 装入将暂停。

解决办法：

客户端可以重新装入导出内容以访问共享。

在节点崩溃的情况下无法正确地进行内核 NFS v4 锁故障转移

使用内核 NFS v4 共享，在节点崩溃的情况下处于活动状态的锁无法故障转移到群集中的另一个节点。

解决办法：

此问题没有解决办法。

网络组的内核 NFS v4 导出装入无法正常运行

无法使用内核 NFS v4 动态更改网络组成员资格。因此，网络组的内核 NFS v4 导出装入无法按预期运行。

解决办法：

重新启动 NFS 服务。

用于 IPv6 子网的 NFS-Ganesha 共享无法工作，NFS 共享进入故障状态

启用 NFS-Ganesha (GNFS) 服务器后，不支持向 IPv6 子网的 NFS 导出。因此，NFS 共享进入故障状态。这是 GNFS 级别的限制。

解决办法：

没有解决办法。您必须为每个客户端创建单独的 NFS 导出。

ObjectAccess 问题

本节介绍 ObjectAccess 问题。

尝试通过 SSLS3 连接到 S3 服务器时，客户端应用程序可能会发出类似于“SSL3_GET_SERVER_CERTIFICATE:certificate verify failed”的警告

Veritas Access 将生成 SSL 自签名证书。此证书不属于默认的受信任 CA。因此，S3 客户端无法信任它。

解决办法：

客户端应忽略该警告并继续通过 SSL 进行通信。

如果已从早期版本升级到 Veritas Access 7.4，而且群集名称包含大写字母，则对 S3 服务器的访问将失败

如果群集名称包含大写字母，对 S3 服务器的访问将失败。这是因为用于接受 S3 请求的基础库存在限制。

解决办法：

全部使用小写字母访问 S3 服务器。

如果群集名称未遵循 DNS 主机名限制，则无法在 Veritas Access 中使用 ObjectAccess 服务

群集名称不能包含除连字符以外的任何特殊符号。如果群集名称包含除连字符以外的特殊符号，则 S3 服务不起作用，因为没有遵循 DNS 主机名限制。

解决办法：

此问题没有解决办法。有关可用于命名 Veritas Access 群集的有效字符，请参见：

https://technet.microsoft.com/en-us/library/cc959336.aspx

创建存储桶可能失败并显示超时错误

如果创建存储桶花费很长时间，则存储桶创建请求可能会失败并显示错误消息，即使存储桶创建成功也是如此。

解决办法：

您可以验证存储桶是否存在，即使请求失败也是如此。

删除存储桶可能失败并显示“No such bucket”或“No such key”错误

如果上一个存储桶删除请求完成之前重试客户端请求，后续重试可能会获取过时信息。存储桶删除请求失败并显示错误消息。

解决办法：

即使请求失败，客户端也需要验证存储桶删除。

如果组名中包含空格，则组配置在 ObjectAccess 中不起作用

如果组名中包含空格，那么，即使为该组设置了配置，该组的用户也无法使用该配置创建存储桶。相反，将使用默认配置创建存储桶。

管理员不应当为名称中包含空格字符的组配置 ObjectAccess。

在 OpenDedup 从 Veritas Access 7.3.0.1 升级到 7.4 后，对现有存储桶运行 Objectaccess> bucket show 命令时，输出中未显示池名称

从 Veritas Access 7.3.0.1 升级到 7.4 时，不可导入 ObjectAccess 配置。因此，在升级后，对于现有存储桶，池字段为空。`objectaccess> bucket show` 命令的输出中未显示池名称。这不会影响任何功能。

解决办法：

此问题没有解决办法。

如果启用了 SSL，则在 get_object API 中使用 portald 时会发生崩溃，同时发送有关负载较大的响应

如果启用了 SSL，则在 `get_object` API 中使用 `portald` 时会发生崩溃，同时发送有关负载较大的响应。在启用了 SSL 的情况下使用条件参数时，也会出现此问题。

解决办法：

在使用条件参数时禁用 SSL。

OpenDedup 问题

本节介绍与 OpenDedup 相关的已知问题。

删除 OpenDedup 卷后不回收文件系统存储

使用 CLISH 命令删除 OpenDedup 卷时，不会删除存储桶中的 OpenDedup 数据内容。因此，不会回收相应文件系统的空间。

解决办法：

使用任何 S3 客户端手动删除 OpenDedup 内容。

Storage> fs online 命令失败并显示 EBUSY 错误

如果存储桶或 OpenDedup 卷位于横向扩展文件系统上且 I/O 操作正在运行，`Storage> fs offline` 命令会成功，但 `Storage> fs online` 命令可能会失败或者 S3 服务器可能无法按预期工作。

解决办法：

执行 `Storage> fs offline` 命令之前，验证 ObjectAccess 存储桶或 OpenDedup 卷是否位于该文件系统上以及是否未运行任何 I/O 操作。

对使用单个存储桶且装入在两个不同介质服务器上的 OpenDedup 卷运行 df-h 命令时，输出不匹配

如果两个 OpenDedup 卷使用单个存储桶且装入在两个不同的介质服务器上，对这两个卷运行 `df -h` 命令时，会显示不同的输出。

解决办法：

确保两个介质服务器上的 OpenDedup 卷 XML 中的序列号条目相同。

如果 OpenDedup> volume create 命令在执行期间失败，不会还原所做更改

如果 `Opendedup> volume create` 命令在执行期间失败，不会还原所做更改。

解决办法：

执行 `Opendedup> volume list` 命令，检查是否创建了卷但卷处于脱机状态。如果卷处于脱机状态，请使用 `Opendedup> volume delete <volume-name>` 命令删除卷，并尝试重新创建卷。

升级后，其中一些 OpenDedup 卷统计数据重置为零

如果在卷处于联机状态时导出 OpenDedup 卷配置，则导出的数据并未正确反映卷的状态。这会导致在导入 OpenDedup 卷配置时其中一些统计数据重置为零。

解决办法：

在导出 OpenDedup 卷配置之前，使所有卷脱机，然后导出配置。

OpenDedup 卷装入操作失败并显示错误

尝试装入 OpenDedup 卷时，操作失败并显示以下错误：

```
Still running according to PID file /var/run/S3fs********.pid,
PID is ****. Service exit with a return value of 122
```

卸载 OpenDedup 卷后，出现过时的 `jsvc` 进程。因此，卷重新装入失败。

解决办法：

手动终止过时的 `jsvc` 进程，并尝试再次装入 OpenDedup 卷。

从 AWS Glacier 还原数据失败

数据上传到 AWS Glacier 云后，尝试使用 NetBackup 还原功能从云中还原这些数据，操作失败并显示以下错误：

```
socket read failed errno = 62 - timer expired
```

解决办法：

- 在 `/etc/sdfs/*-volume-cfg.xml` 文件中，将 `glacier-archive-days` 值从 0 更改为 30。
- 检查用于执行还原操作的介质服务器的 `Client Read Timeout` 值。
  在 NetBackup 管理控制台中，您可以在 **Host properties** > **Media Servers** > **Timeouts** > **Client Read Timeout** 处找到 `Client Read Timeout`。

在 UNIX 介质服务器上，查看 /usr/openv/netbackup/bp.conf 文件中的 CLIENT_READ_TIMEOUT 值。将 CLIENT_READ_TIMEOUT 值设置为较大数字，如 3600、7200 或 10800。
有关更多详细信息，请参见
https://www.veritas.com/support/en_US/article.100006172

在升级 OpenDedup 后，如果群集名称发生更改，则 OpenDedup 卷不会联机

OpenDedup 卷的配置文件包含基于先前群集名称的 S3 端点。因此，升级之后，在具有不同名称的群集上，由于 S3 端点发生更改，卷不会联机。

解决办法：

请联系 Veritas 技术支持，以更新配置文件中的 S3 端点。

如果 OpenDedup 位于介质服务器上且正在运行还原作业，则重新启动 Veritas Access 主节点时，还原的文件可能处于不一致状态

如果 OpenDedup 位于介质服务器上且正在运行还原作业，则重新启动 Veritas Access 主节点时，还原的文件可能与备份的源文件不一致。

解决办法：

执行以下操作：

- 确保停止当前正在运行的所有备份和还原作业。
- 卸载 OpenDedup 卷。如果有任何过时的 jsvc 进程正在运行，手动将其终止。
- 要删除缓存，请删除 /opt/sdfs/volumes/<volume-name>/chunkstore/chunks/ 文件中的所有内容，然后重新装入 OpenDedup 卷。
- 重新启动还原作业。

OpenDedup> volume list 命令可能不显示卷的节点 IP

在某些情况下，Opendedup> volume list 命令不显示 OpenDedup 卷的节点 IP。

解决办法：

可以使用以下命令获取 OpenDedup 卷的关联节点 IP。

```
# hares -display $(grep <OpenDedup_volume_name>
/opt/VRTSnas/conf/odd_vipgrp_map.conf | awk '{ print $2 }' |
tr -d 'group') -attribute Address | tail -1 | awk '{ print $NF }'
```

其中 <*OpenDedup_volume_name*> 是未显示其节点 IP 的 OpenDedup 卷的名称。

OpenStack 问题

以下问题与 OpenStack 相关。

无法通过 CLISH 区分 Cinder 和 Manila 共享

对于使用 `OPENSTACK> cinder share` 命令通过 NFS 导出的任何文件系统，以及通过 NFS 从 OpenStack Manila 导出的任何文件系统，无法通过 CLISH 进行区分。

解决办法：

使用 `OPENSTACK> manila resource list` 命令，仅查看通过 Manila 导出的共享。无法仅查看 Cinder 共享。

在目标端发生故障后，创建 Cinder 卷失败

有时 Cinder 卷创建操作会失败。这是一个中间问题。由于 `_vrts_get_targets_store` 函数返回空白的目标列表输出，卷创建操作失败。如果您检查 Cinder 日志，会看到以下错误消息：

```
ERROR oslo_messaging.rpc.server return target_list
['output']['output']['targets']
ERROR oslo_messaging.rpc.server TypeError:
'bool' object has no attribute '_getitem'_
```

解决办法：

使用 `service openstack-cinder-volume restart` 命令重新启动 Cinder 卷服务。

Cinder 卷可能无法连接到实例

由于 `_/lib/udev/scsi_id --page 0x83 --whitelisted /dev/disk/by-path/ip-10.182.97.58:3260-iscsi-iqn.2018-02.com.veritas:target02-lun-4_` 命令返回错误，Cinder 卷无法连接到实例。

解决办法：

检查 Cinder 日志。如果卷连接失败，并出现错误 *_ scsi_id: cannot open /dev/disk/by-path/ip-10.182.97.58:3260-iscsi-iqn.2018-02.com.veritas:target02-lun-4: No such device or address_*，则删除该卷。创建新卷并尝试连接该卷。

复制问题

本节介绍与间歇性复制和连续性复制相关的已知问题。

在相同源上运行间歇性复制和重复数据删除时，间歇性复制文件系统在某些情况下会失败

在同一个源间歇性复制文件系统上出现以下情况时，间歇性复制作业可能会失败：

1. NFS 的 I/O 工作量十分繁重。
2. 并行运行的重复数据删除创建了多个共享扩展盘区。

解决办法：

没有解决办法。

System> config import 命令无法导入间歇性复制密钥和作业

`System> config import` 命令将导入通过 `System> config export` 命令导出的配置。在导入过程中，系统将正确导入间歇性复制循环整数和调度。该命令无法导入密钥和作业。

解决办法：

先运行 `Replication> episodic config import` 命令，然后执行以下步骤。

1 确保新目标绑定了间歇性复制 IP，因为间歇性复制 IP 在新源上不会更改。

2 在源和目标上运行 `Replication> episodic config import_keys` 命令。

3 在源和目标上运行 `Replication> episodic config auth` 命令。

4 从新源 `/shared/replication/jobs # rm -rf` *`jobname/`* 中删除作业目录。

5 从新源中创建作业。

作业在间歇性复制故障转移之后使用目标上的调度

如果源群集和目标群集上的调度名称相同、但间隔不同，会发生此问题。间歇性复制故障转移到目标之后，作业将使用目标上的调度。

解决办法：

不在源群集和目标群集上使用相同的调度名称。

如果目标节点进行故障转移，则间歇性复制失败并显示错误“connection reset by peer”

间歇性复制操作在源和目标之间创建连接以复制数据。间歇性复制操作使用目标节点之一来访问文件系统以复制数据。如果因重新引导等错误导致与此节点的连接中断，间歇性复制将会失败并显示一条错误消息。如果存在调度间歇性复制作业，则下次迭代将继续此失败的间歇性复制会话，但可能使用目标中的新节点。

解决办法：

如果没有任何调度间歇性复制作业，当该目标节点启动之后，需要发出 Replication> episodic job sync 命令来启动复制作业。

升级后无法识别在 Veritas Access 7.2.1.1 或更低版本中创建的间歇性复制作业

如果尝试访问或修改在 Veritas Access 7.2.1.1 或更低版本中创建的间歇性复制作业，则命令不起作用，因为作业处于无法识别状态。

解决办法：

销毁作业，然后重新创建。

对于间歇性复制，不支持通过 GUI 设置带宽

bwlimit show 未在 CLISH 中显示预期输出。

```
Replication> episodic bwlimit show
ERROR V-288-0 No job is configured with current node as replication
 source
```

因此，GUI 不支持 bwlimit show。

解决办法：

可以使用以下命令设置带宽：

```
 Replication> episodic bwlimit set src_to_tgt 10
```

在执行作业移除和添加链接操作后，加密的间歇性复制作业失败，并显示 SSL 证书错误

从加密的已配置作业中移除链接并向同一作业重新添加新链接后，下一个间歇性复制周期将会失败并显示错误：

```
SSL certificate error.
```

解决办法：

执行以下步骤以解决此问题：

1. 执行 Replication> episodic job remove_link 命令，并在源和目标上退出 CLISH 提示。
2. 在源和目标的群集节点上，创建 ln -s /shared/replication/SSL/cluster_cert /opt/VRTSfsadv/cert 链接。
3. 执行 Replication> episodic job add_link 命令，重新将链接添加到作业并启用或同步间歇性复制作业。

间歇性复制作业状态显示已移除链接的条目

如果多目标作业中的某个间歇性复制目标已被移除，在使用 `Replication> episodic job remove_link` 命令时，仅会将此目标标记为要移除。链接的实际移除将在下一次间歇性复制迭代时发生。

在链接完全移除之前，`Replication> episodic job show` 命令仍会显示所移除链接之前的状态。

解决办法：

使用 `Replication> episodic job show` 命令验证链接何时完全移除。

间歇性复制作业修改失败

间歇性复制具有在目标端提供多恢复点目标 (RPO) 报告的功能。`Replication> episodic job modify rep_dest_ckpt_cnt` 命令控制 RPO。默认值为 10。在目标端上提供 RPO 会占用目标端的一些空间，因此间歇性复制可能会失败并显示 ENOSPC 错误。在这种情况下，任何间歇性复制作业修改命令均会失败。

解决办法：

增大目标文件系统，提供更多空间。修改间歇性复制作业，设置适当的 `rep_dest_ckpt_cnt` 值。除非当前的间歇性复制会话成功完成，否则此修改值不会生效。应用此修改值之后，将根据新值调整现有 RPO。

间歇性复制故障转移不起作用

如果尝试在源群集出现故障时将目标群集作为新的源群集，则不起作用。因此，对间歇性复制群集进行故障转移将不成功。

解决办法：

此问题没有解决办法。

在目标上手动重新启动 had 后台驻留程序时连续性复制失败

如果在目标上停止并重新启动 had 后台驻留程序，连续性复制将失败。这是因为用于连续性复制的 IP 表规则不会还原。

解决办法：

- 在目标上，设置以下规则。

  # iptables -I INPUT 2 -p tcp -d *<replication_ip of target>* --dport 56987 -j ACCEPT

- 保存规则。

```
# service iptables save
```

- 重新启动 IP 表。

```
# service iptables restart
```

如果存储复制日志已满，则连续性复制无法进入复制状态

将数据从源群集复制到目标群集时，如果存储复制日志 (SRL) 已满，则将进入数据更改映射 (DCM) 模式。在 DCM 模式下，不会将状态显示为 *replicating*。

```
Replication> continuous status test_fs
Name                    value
====================  ============================================
Replicated Data Set    rvg_test_fs
Replication Role       Primary
Replication link       link1

Primary Site Info:

Host name           10.10.2.70
RVG state           enabled for I/O

Secondary Site Info:

Host name           10.10.2.72
Configured mode     synchronous-override
Data status         inconsistent
Replication status  resync in progress (dcm resynchronization)
Current mode        asynchronous
Logging to          DCM (contains 551200 Kbytes) (SRL protection
logging)
```

解决办法：

对于连续性数据复制，在源群集上运行以下命令。

```
# vxrvg -g <dg_name> resync <rvg_name>
```

此命令将重新同步源和目标群集。可以通过输入以下命令查看状态：

```
Replication> continuous status test_fs
Name                    value
====================  ======================
Replicated Data Set    rvg_test_fs
```

```
Replication Role        Primary
Replication link        link1

Primary Site Info:

Host name               10.10.2.70
RVG state               enabled for I/O

Secondary Site Info:

Host name               10.10.2.72
Configured mode         synchronous-override
Data status             consistent, up-to-date
Replication status      replicating (connected)
Current mode            synchronous
Logging to              SRL
Timestamp Information   behind by  0h 0m 0s
```

如果群集节点之间的 IPTABLE 规则通信不正常，则连续性复制中的计划外故障转移和故障回退可能会失败

对于计划外故障转移和故障回退，IPTABLE 规则可能无法正确还原。因此，节点之间的通信无法正常进行。

解决办法：

刷新主站点与辅助站点上群集内所有节点上的 IPTABLES。

```
# iptables -F
```

如果连续性复制 IP 在主节点上未处于联机状态，而在另一个节点上处于联机状态，则连续性复制配置可能会失败

在目标站点上，可能存在这样一种情况：管理控制台在连续性复制 IP 处于联机状态的节点上未处于联机状态。在这种情况下，配置连续性复制可能会失败，因为内部命令需要在主节点上运行。

解决办法：

确保可以通过主节点访问 CLISH 且连续性复制 IP 也在主节点上处于联机状态。如果没有，请使用以下命令将管理控制台位置切换到主节点。

```
# hagrp -switch ManagementConsole -to <system_name>
```

如果重新启动主群集或辅助群集中的任何节点，复制可能会进入 PAUSED 状态

重新启动主群集或辅助群集中的任何节点时，群集节点之间的 IPTABLE 规则通信不正常。这将导致复制进入 PAUSED 状态。

解决办法：

刷新主站点与辅助站点上群集内所有节点上的 IPTABLES。

```
# iptables -F
```

SDS 已知问题

以下问题与 SDS 模块相关。

轮换 SDS 日志后，来自 Veritas Access 或 SDS 插件的日志消息进入轮换的文件中，而不是新文件中

SDS 日志（位于 `/var/log/sds.log`）每天轮换一次。SDS 包含两个服务：SDS 插件和 Veritas Access 插件，它们共享日志文件。由于 Python 中的错误，会发生争用情况，其中一个服务开始在新文件中进行日志记录，而另一个服务仍在轮换的文件中进行日志记录。

解决办法：

检查当前日志文件和轮换的日志文件的上次更新时间戳，并将来自不同服务的日志相互关联以进行调试。

SmartIO 问题

以下问题与 Veritas Access SmartIO 命令相关。

文件系统先脱机再联机之后，该文件系统的 SmartIO 写回缓存模式更改为读取模式

使用 SmartIO 功能，可以在文件系统上设置写回或读取缓存模式。在文件系统上设置缓存模式之后，当文件系统保持联机状态时，该模式将一直保留。如果文件系统脱机后再次联机，则先前的缓存模式不会保留，而是重置为读取缓存模式。

解决办法：

当文件系统联机之后，重新手动设置缓存模式。

存储问题

以下问题与 Veritas Access 存储命令相关。

如果设置快照配额，快照装入可能会失败

如果设置快照配额且快照磁盘使用情况达到配额硬限制，那么即使存在可移除快照，检查点装入也可能会失败。如果文件系统空间不足或超过快照配额，则快照操作可触发快照移除，以释放部分磁盘空间。但是，快照装入无法触发此空间清理操作，因此在极少数情况下，快照装入可能失败。

解决办法：

移除最旧的检查点并重试。

有时 Storage> pool rmdisk 命令不会输出消息

在极少数情况下，`Storage> pool rmdisk` 命令会因输出重定向问题而不输出错误消息或成功消息。

解决办法：

使用 `history` 命令检查命令状态。也可以使用 `Storage> pool list` 命令验证是否已从池中移除磁盘。

Storage> pool rmdisk 命令有时会显示错误，指出未输出文件系统名称

如果要移除的磁盘中具有 NLM，则 `Storage> pool rmdisk` 命令将采用不同的方式进行处理，且不会输出文件系统名称。是否出现此错误取决于多种因素，例如，池大小、NLM 如何使用磁盘以及磁盘中的分布。

解决办法：

没有解决办法。

无法为新添加到 CIFS 主目录列表中的文件系统启用配额

如果将新文件系统作为 CIFS 主目录添加，默认情况下不会启用配额。

解决办法：

通过 CLISH 运行以下命令：

```
Storage> quota cifshomedir disable

Storage> quota cifshomedir enable
```

销毁文件系统可能不会移除装入点的 /etc/mtab 条目

销毁文件系统时，`/etc/mtab` 条目应当会移除。如果文件系统 `umount` 命令在销毁操作期间挂起，则 `/etc/mtab` 条目可能不会移除。文件系统将会销毁，但您无法使用相同的名称创建新文件系统。

解决办法：

重新引导群集节点。

Storage> fs online 命令返回错误，但文件系统在几分钟后处于联机状态

`Storage> fs online` 命令返回以下错误：

```
access.Storage> fs online fs1

ACCESS fs ERROR V-288-1873 filesystem fs1 not mounted on nodes
access_01 access_02.
```

在装入具有多个检查点的文件系统时，Veritas Cluster Server (VCS) 资源可能会在 100 多秒之后才响应。这将导致 CFS 命令超时。

解决办法：

即使报告联机故障，文件系统仍将处于联机状态。

如果存在 DCO，则从池中移除磁盘失败

如果创建文件系统时在命令行上指定磁盘，则 Veritas Access 可能会在除指定磁盘以外的磁盘上创建数据更改对象 (Data Change Object, DCO)。如果池中具有可用磁盘，则 Veritas Access 首选将这些磁盘用于 DCO。DCO 对于处理镜像与原始卷之间的同步操作必不可少。当包含数据卷的磁盘失败时，需要使用 DCO。

如果您尝试从池中移除该磁盘，则会显示以下错误，因为 DCO 正在使用该磁盘。

```
SFS pool ERROR V-288-2891 Disk(s) sde are used by the following:
DCO of primary tier of fs_mirror, Primary tier of filesystem fs_mirror
```

解决办法：

没有解决办法。

即使 df 命令显示文件系统中有可用空间，横向扩展文件系统仍会返回 ENOSPC 错误

即使 Linux `df` 命令显示文件系统中有可用空间，横向扩展文件系统仍会返回 ENOSPC 错误。

在以下任一情况下，可能会出现这种问题：

- 横向扩展文件系统使用哈希算法在存储容器之间分配数据。该算法确保数据在所有容器之间均匀分配，且根据数据类型，其中某一存储容器比其他容器的使用率更高。横向扩展文件系统可能会提前达到 100% 使用率。在这种情况下，所有向已达到 100% 使用率的容器进行分配的操作均会返回 ENOSPC 错误。

- 横向扩展文件系统包含一个元数据容器和多个数据容器。元数据容器的空间在创建文件系统时进行分配。如果所有数据容器均已满而元数据容器有可用空间，文件系统不会使用元数据容器中的空间。因此，Linux `df` 命令可能显示仍有可用空间，但在写入文件系统时应用程序将显示 ENOSPC 错误。

解决办法：

增加文件系统容量。

在运行 Storage> fs growby 或 growto 命令之后运行回滚时，回滚刷新失败

如果在运行 `Storage> fs growby` 或 `Storage> fs growto` 命令之后运行回滚，回滚刷新将会失败。

创建文件系统的回滚。创建文件系统的回滚之后，使用 `Storage> fs growby` 或 `Storage> fs growto` 命令增加文件系统的大小。如果在先前创建的回滚上执行 `Storage> rollback refresh`，操作将失败。

目前，`Storage> rollback` 命令设计为仅允许使用 `Storage> rollback refresh` 命令中的相同大小作为源文件系统的大小。在执行回滚刷新之前自动调整快照大小非常复杂，特别是当存储池没有足够的空间时更是如此。自动调整快照大小的功能尚未实现。

解决办法：

没有解决办法。

如果导出的 DAS 磁盘处于错误状态，使用 Storage> list 时，它在本地节点上显示 ERR，在远程节点上显示 NOT_CONN

如果导出的 DAS 磁盘进入错误状态，则其属性在远程节点上不可用。`Storage> disk list` 命令在远程节点上显示 `NOT_CONN`。

解决办法：

无需解决办法。如果磁盘在本地节点上联机，那么它在所有节点上也是联机。

禁用 I/O 防护时，在管理服务关闭的情况下群集状态不一致

当某一节点关闭时，如果禁用 I/O 防护，则会导致 Veritas Access 群集处于不一致的状态。

解决办法：

没有解决办法。请确保禁用 I/O 防护时已启动群集中的所有节点。

Storage> tier move 命令无法对节点进行故障转移

如果运行 `Storage> tier move` 命令的节点关闭，则该命令不会故障转移到另一个节点。

解决办法：

再次从 CLISH 运行 `Storage> tier move` 命令。

Storage> scanbus 操作在 I/O 防护操作时挂起

`Storage> scanbus` 操作在 I/O 防护操作期间挂起。

解决办法：

没有解决办法。请与 Veritas 技术支持联系。

当相关的缓存对象已满时，回滚服务组进入故障状态且无法清除该状态

当缓存对象已满后，此问题与 I/O 错误相关。发生缓存备份回滚时，如果因大量 I/O 导致缓存已满，则会在快照中产生 I/O 错误，且快照将自动从主文件系统分离。快照将进入故障状态。解决此问题需要清除故障回滚状态并执行回滚刷新。CLISH 命令无法处理这些情况。需要 Veritas 技术支持手动干预才能保留回滚。

解决办法：

没有解决办法。

当缓存对象已满时，未生成事件消息

对于回滚缓存已满的情况，此问题与客户可见的事件相关。

解决办法：

没有解决办法。

Veritas Access CLISH 界面不应允许同时在相同文件上运行解压缩和压缩操作

对于压缩和解压缩这两种操作，Veritas Access CLISH 界面不会在其中一种操作运行时阻止另一种操作。这是旧式行为，应当会在将来的版本中修复。

解决办法：

在同一文件上运行压缩或解压缩操作的同时，不要在相同文件上启动另一种操作（解压缩或压缩）。

存储设备出现故障并显示 SIGBUS 信号，导致横向扩展文件系统后台驻留程序异常终止

当存储设备出现故障并发出 SIGBUS 信号（总线错误）时，导致横向扩展文件系统后台驻留程序异常终止。恢复过程不会将横向扩展文件系统以及该文件系统所关联虚拟 IP 的 NFS 共享迁移到声明的同一节点。NFS 客户端上的 Linux `df` 命令输出将显示已装入横向扩展文件系统的 NFS 共享的错误大小和使用情况（`Size Used`、`Avail` 和 `Use%`）。

发生这种情况时，应用程序应先停止使用横向扩展文件系统的 NFS 共享，然后再解决此问题。

解决办法：

通过登录 Veritas Access 管理控制台重新导出横向扩展文件系统，并运行 CLISH 命令删除 NFS 共享，然后重新添加。如有必要，也请在应用程序的 NFS 客户端上重新装入 NFS 共享。

如果重新引导群集节点之一，Storage> tier move list 命令将会失败

除非群集节点重新启动并恢复运行，否则 `Storage> tier move list` 命令将会失败。

解决办法：

没有解决办法。

指定为 Storage> fs policy add 过滤条件的模式有时会错误传输不符合条件的文件

使用 `Storage> fs policy add` 命令时，如果指定 `**/*.txt` 模式为过滤条件，则会出现此问题。运行该策略时，会选择传输或删除 `txt` 目录内没有 `.txt` 扩展名的文件。根据预期，任何没有扩展名 `.txt` 的文件都不应被选中进行传输或删除。

解决办法：

没有解决办法。

在发出 Storage> fs policy resume 之后完成策略运行时，总数据量和文件总数可能与 Storage> fs policy 状态中显示的移动数据量和文件计数不匹配

`Storage> fs policy pause` 命令会立即停止策略执行。如果在执行此命令时传输任何文件，则不会对要完成的传输停止命令。报告 `Storage> policy run` 命令的状态时，Veritas Access 不考虑执行 `Storage> fs policy pause` 命令时正在传送的文件的数据大小和文件计数。

解决办法：

您应再次执行同一策略的 `Storage> fs policy dryrun`，检查是否在传输中丢失了任何文件。也可以使用 `Storage> tier mapfiles` 和 `Storage> tier listfile` 命令验证文件的位置。

Storage> fs addcolumn 操作失败，但不发送错误通知

`Storage> fs addcolumn` 操作在后台失败，但由于 CLISH 中未出现错误消息，因此不发送失败通知。失败原因之一是给定的池中没有足够的存储。

解决办法：

如果未添加所需的列数，请在添加足够的存储之后再次尝试。

Storage> fs-growto 和 Storage> fs-growby 命令返回独立磁盘错误

即使具有足够的空间，`Storage> fs growto` 和 `Storage> fs growby` 命令仍会返回 *Not enough space* 错误。当发生以下情况时，此操作将失败：

1. 文件系统是在正常池上创建的。但是，对于 `fs growto` 和 `fs growby` 操作，提供的是独立池中的磁盘。

2. 文件系统是在独立池上创建的。但是，对于 `fs growto` 和 `fs growby` 操作，提供的是正常池或不同独立池中的磁盘。

解决办法：

如果文件系统是在正常池中创建的，则对于 `fs-growto` 和 `fs-growby` 操作，提供正常池中的磁盘。如果文件系统是在独立池上创建的，则将磁盘添加到同一独立池中，并为 `fs-growto` 和 `fs-growby` 操作提供这些磁盘。

存在分层时，无法创建空间优化回滚

在分层文件系统中，创建优化空间回滚失败。当主层启用 `fastresync`、而辅助层不启用 `fastresync` 时，将出现该故障。

当发生以下情况时，辅助层禁用 `fastresync`：

1. 该层已镜像，但手动禁用了 `fastresync`。

2. 在不能启用 `fastresync` 的情况下，该层为简单层或已条带化。

解决办法：

如果辅助层已镜像，则在辅助层上启用 `fastresync`。

如果辅助层为简单层（或已条带化）且主层已镜像，则将镜像添加到辅助层。

确保如果主层启用 `fastresync`，则辅助层也启用 `fastresync`。

针对包含 Volume Manager 对象的设置启用 I/O 防护将无法导入磁盘组

如果针对包含 Volume Manager 对象的设置启用 I/O 防护，则无法导入磁盘组，并且会收到以下错误消息：

```
Disk <diskname> does not support SCSI-3 PR, Skipping PGR operations

for this disk
```

如果存在 Volume Manager 对象（如卷和卷集）而且启用了 I/O 防护，则在加入群集过程中将不导入共享磁盘组。

甚至使用 `vxdg -s import <dgname>` 命令手动导入磁盘组也会失败，并出现以下错误消息：

```
SCSI-3 PR operation failed
```

之所以出现此问题，是由于已使用 disk map 命令隐式导出的磁盘上缺少导出标志。如果磁盘组包含不支持 SCSI3 PR 的磁盘，则会发生此问题。

解决办法：

在启用基于多数的防护之前，使用以下命令从群集的所有节点显式导出所有 DAS 磁盘。

```
# vxdisk -f export <DAS disk Name>
```

现在可以启用 I/O 防护了。

池仅包含一个磁盘时创建文件系统失败

池中只有一个磁盘时，`fs creation` 命令无法在文件系统上创建 NLM，而是尝试使用其他选项创建文件系统。

解决办法：

确保池中有多个磁盘。

启动备份服务后，BackupGrp 在某些节点上进入 FAULTED 状态

BackupGrp 只在一个节点上联机。备份服务启动后，它会在所有群集节点上探测该组，并尝试在多个节点上联机。但是，由于这是一个故障转移组，因此无法在多个节点上联机。因此，它将在某些节点上进入 FAULTED 状态。

解决办法：

使用以下命令清除故障：

```
BacupGrp> hagrp -clear BackupGrp
```

使用精简 LUN 创建简单布局的横向扩展文件系统可能会在 Storage> fs list 命令中显示分层布局

如果使用精简 LUN，FMR 默认处于启用状态。启用 FMR 功能时，会创建 DCO 卷。系统上存在 DCO 卷时，`Storage> fs list` 命令会错误地导出横向扩展文件系统的布局。该命令显示卷布局不正确，或者如果布局正确，镜像数显示不正确。这是输出显示问题，横向扩展文件系统具有正确的布局。

解决办法：

使用 `Storage> fs list fs_name` 命令查找有关文件系统的详细信息。

使用 largefs-striped 或 largefs-mirrored-stripe 布局创建的文件系统可能会在 Storage> fs list 命令中显示错误的列数

如果使用 largefs-striped 或 largefs-mirrored-stripe 布局创建文件系统，则 `Storage> fs list` 命令导出的文件系统布局详细信息不正确。或者，此命令显示的列数不正确。这是输出显示问题。

解决办法：

没有解决办法。

使用 SSD 池创建文件系统失败

池包含来自两个或多个节点的 SSD 时，使用 `layout=mirror` 操作创建文件系统将失败。

解决办法：

使用可用的 SAN/DAS 磁盘创建文件系统。

对于类型为 SSD 的池中存在的磁盘，请以 `Support` 用户身份从 bash shell 运行以下命令，导出磁盘以物理方式存在的所有节点上的磁盘。

```
Support> vxdisk export disk name
```

池中的所有磁盘从各自的群集节点导出后，继续从 Veritas Access CLISH 创建文件系统。

执行 Storage> fencing off/on 命令后，横向扩展文件系统可能会进入故障状态

执行 `Storage> fencing on` 和 `Storage> fencing off` 操作时，相关横向扩展文件系统中的 VCS 资源会进入故障状态。

解决办法：

使用 `Support> service autofix` 命令修复处于故障状态的文件系统。如果服务组未联机，则重新启动横向扩展文件系统的 VCS 服务组处于故障状态的节点。使用以下命令查看检查群集节点的 VCS 服务组的状态。

```
Support> services showall
```

将 Azure 层添加到横向扩展文件系统后，无法将文件移至 Azure 层，且 Storage> tier stats 命令可能会失败

将 Azure 层添加到横向扩展文件系统后，无法将文件移至 Azure 层，且 `Storage> tier stats` 命令可能会失败并显示以下错误：

```
ACCESS tier ERROR V-493-10-2059 Failed to display access statistics
 of cloud
tier aztierx2 (errnum=22).
```

解决办法：

使用 `Storage> fs offline fs_name` 命令使具有 Azure 层的横向扩展文件系统脱机，再使用 `Storage> fs online fs_name` 命令使其联机。或者，可以在群集的所有节点上终止 `tfsd` 后台驻留程序。

重新启动管理控制台节点后，CVM 服务组进入故障状态

运行 `Cluster> reboot` 命令时，有时 CVM 服务组会在重新启动的节点上进入故障状态。此问题通常是由 CVM 共享磁盘组对象（如卷、卷集或复制卷组 (RVG)）和专用磁盘组对象之间存在次要编号冲突所致。确认专用磁盘组对象的次要编号与加入 CVM 从属节点上的 CVM 磁盘组对象不重叠。

https://www.veritas.com/support/en_US/article.000107801

解决办法：

使 CVM 服务组联机

1 在 CVM 服务组处于故障状态的节点上运行以下命令

```
# hastop -local
```

2 使所有文件系统脱机。从管理控制台处于联机状态的另一个节点运行以下命令。

```
Storage> fs offline <file system name>
```

3 使用以下命令逐出所有磁盘组：

```
# vxdg -s deport <disk_group>
```

4 使用以下命令导入所有磁盘组：

```
# vxdg -s import <disk_group>
```

5 启动 VCS。

```
# hastart
```

如果文件系统未联机，则运行以下命令，使所有文件系统联机：

```
Storage> fs online <file system name>
```

如果群集的其中一个节点处于未知状态，Storage> fs create 命令无法正确显示输出

如果群集的其中一个节点处于未知状态，则 `Storage> fs create` 命令的行为有所不同。虽然已成功创建文件系统，但无法正确显示输出。

解决办法：

如果要使用 GUI 创建文件系统，请使节点联机。要么，即使有一个节点处于未知状态，您仍要创建文件系统，请通过 CLISH 创建文件系统。您可以使用 `Storage> fs list` 命令，验证是否已创建文件系统。

如果文件系统或存储桶的大小已满，Storage> fs growby 和 Storage> fs growto 命令将失败

如果文件系统或存储桶中没有可用空间，`Storage> fs growby` 和 `Storage> fs growto` 命令将失败。

解决办法：

没有解决办法。您可以手动删除文件以创建可用空间。

为 NetBackup 配置 S3 存储桶时，如果设备保护选为纠删码且故障域选为磁盘，则存储桶创建操作将失败

当您使用 Veritas Access GUI 尝试为 NetBackup 配置 S3 存储桶时，如果设备保护选为纠删码且故障域选为磁盘，则存储桶创建操作将失败。这是因为选择故障域作为磁盘不会传递到 `vxassist` 命令。如果未指定故障域，则默认情况下，该命令将故障域作为节点。因此，存储桶创建操作将失败。

解决办法：

没有解决办法。从 Veritas Access GUI 配置存储时，对于纠删码布局，无法将故障域选为磁盘，因为此版本不支持这一操作。

防护磁盘的操作系统名称在 Veritas Access 群集中不一致，这可能会导致出现问题

用于在群集中进行防护的磁盘的操作系统名称可能不同。例如，某个磁盘在一个节点上名为 *sda*，而在另一个节点上可能为 *sdf*。这意味着，两个节点上的 *sda* 磁盘不相同。在设置基于磁盘的 SCSI3 防护时，这可能会导致在非预期磁盘上进行写入。

解决办法：

确保用于在群集中进行防护的所有磁盘使用相同的操作系统磁盘名称。

启用了防护时，磁盘组导入操作失败，且所有服务会进入故障状态

如果磁盘不与 SCSI-3 兼容，则必须从 Volume Manager 端关闭 SCSI-3 永久保留查询。否则，当您尝试启用防护时，所有服务都会进入故障状态。

解决办法：

您可以按照以下任一方法对非 SCSI3 磁盘启用防护。

使用 cluster> reboot all 命令对非 SCSI3 磁盘启用防护

1 在未启用防护的情况下安装 Veritas Access。

2 在所有节点上执行 `vxdctl scsi3_pr off`。

3 通过 CLISH 执行 `Cluster> reboot all`。

4 在系统重新启动后，通过 CLISH 执行 `Storage> fencing on majority`。

5 创建池和文件系统。

在不重新启动的情况下对非 SCSI3 磁盘启用防护

1 停止群集服务。

```
# hastop -all
```

2 在所有服务都关闭后，在群集中的所有节点上关闭 SCSI3 永久保留。

```
# vxdctl scsi3pr off
```

3 获取 `vxconfigd` 的进程 ID，并在群集的所有节点上终止 `vxconfigd` 进程。

4 在群集的所有节点上重新启动 `vxconfigd`。

```
# /sbin/vxconfigd -k -x syslog
```

5 启动群集的所有节点。

```
# vxclustadm -m vcs startnode
```

等待导入磁盘组。

6 在群集的所有节点上启动 HA 服务。

```
#hastart
```

现在，您可以启用防护。

创建纠删码文件系统时，在执行 Storage> fs create 命令过程中显示一条误导消息，导致出现问题

使用 `Storage> fs create` 命令创建纠删码文件系统时，在帮助消息中会显示以下内容：

```
eclogdisk : comma separated list of disks from at least ndata+nparity

failure domains to be used for EC log allocation. To use default
disks,
pass eclogdisk=default []
```

这是误导消息，如果您指定 `eclogdisk=default` 作为选项，该命令将无法成功执行。

解决办法：

忽略 `eclogdisk` 的帮助说明。创建文件系统时，以 *"default"* 方式传递 `eclogdisk` 的值，而不是使用 `eclogdisk=default` 进行传递。

在 Veritas Access 群集节点恢复期间，如果在重新启动后有另一个节点加入群集，可能会从群集中显式弹出或中止该节点

如果所有群集节点上有任何文件系统资源处于故障状态，则会发生此问题。

解决办法：

对中止的节点触发群集加入操作，然后手动使文件系统联机。

系统问题

以下问题与 Veritas Access 系统命令相关。

System> ntp sync 命令在没有任何参数时似乎无法正常运行

`System> ntp sync` 命令在没有任何参数时无法按预期运行。将显示一条消息，指示即使未同步日期，日期也会在所有节点上同步。

解决办法：

执行 `System> ntp sync` 命令时应将 NTP 服务器作为用于在所有节点上执行同步操作的显式参数。

目标问题

本节介绍与目标相关的已知问题。

使用 Veritas Access 目标中的 LUN 时，存储配置命令在 Veritas Access 启动器上挂起

在 Veritas Access 目标上，具有 iSCSI LUN 的文件系统从故障状态转为联机状态后，Veritas Access 启动器无法识别这些 LUN。

解决办法：

在 Veritas Access 目标上重新启动目标服务。

5

获取帮助

本章节包括下列主题：

显示联机帮助

您可以单击问号图标，通过 Veritas Access 的管理控制台来访问联机帮助。

显示手册页

您可以在系统控制台上输入 Veritas Access 命令，或使用安全套接字 Shell (Secure Socket Shell, ssh) 通过会话从可以访问 Veritas Access 的任何主机中输入命令。

Veritas Access 提供了以下功能帮助您在命令行中输入命令：

- 命令行帮助：在命令后键入问号 (?)
- 命令行手册页帮助：键入 `man` 和命令名称
- 要退出手册页，键入 `q` 即可。

使用 Veritas Access 产品文档

从 Veritas Services and Operations Readiness Tools (SORT) 网站可以获取最新版本的 Veritas Access 产品文档。

https://sort.veritas.com/documents

需要指定产品和平台并应用其他过滤条件来查找相应文档。

请确保您使用的是最新版本的文档。每个指南的第 2 页提供了文档版本信息。每个文档的标题页上会显示出版日期。文档会定期更新以纠正错误或更正内容。

从 SORT 站点可以获取以下文档：

- *Veritas Access Administrator's Guide*（《Veritas Access 管理指南》）
- *Veritas Access Cloud Storage Tiering Solutions Guide*（《Veritas Access 云存储分层解决方案指南》）
- *Veritas Access Command Reference Guide*（《Veritas Access 命令参考指南》）
- 《Veritas Access Enterprise Vault 解决方案指南》
- *Veritas Access Getting Started Guide*（《Veritas Access 快速入门指南》）
- *Veritas Access Installation Guide*（《Veritas Access 安装指南》）
- *Veritas Access NetBackup Solutions Guide*（《Veritas Access NetBackup 解决方案指南》）
- *Veritas Access Quick Start Guide*（《Veritas Access 快速入门指南》）
- *Veritas Access Release Notes*（《Veritas Access 版本说明》）
- *Veritas Access RESTful API Guide*（《Veritas Access RESTful API 指南》）
- *Veritas Access Software-Defined Storage (SDS) Management Platform Solutions Guide*（《Veritas Access 软件定义存储 (SDS) 管理平台解决方案指南》）
- *Veritas Access Third-Party License Agreements*（《Veritas Access 第三方授权许可协议》）
- *Veritas Access Troubleshooting Guide*（《Veritas Access 故障排除指南》）