解决Secure Web Appliance Full Disk错误

目录

简介

本文档介绍解决安全Web设备(SWA)中的磁盘空间满错误的步骤。

先决条件

要求

Cisco 建议您了解以下主题：

- 访问SWA的CLI
- 对SWA的管理访问
- 通过FTP访问SWA

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

与全磁盘相关的错误

SWA中存在不同的错误和警告，表明磁盘已满或磁盘空间已接近满。以下是错误和警告列表。这些日志在每个软件版本中因交付方式（如警报、系统日志或的输出）而异。 displayalerts 命令。

```
Processing of collected reporting data has been disabled due to lack of logging disk space. Disk usage
User admin  Disk space for /data has exceeded threshold value 90% with current capacity of 99 %

The reporting/logging disk is full on a WSA
```

```
This appliance has disk usage that is higher than expected.
WARNING: Data partition utilization on appliance is high and can cause issues
```

监控磁盘使用情况

您可以从GUI和CLI监控和查看磁盘使用情况。

在GUI中查看磁盘使用情况

登录SWA GUI后，在My-Dashboard Page中，您可以看到 **Reporting / logging Disk** 使用 **System Overview** 部分。

 注意：在SWA中，报告和日志存储在单个分区(称为DATA Partition)中。

在GUI中，在 **Reporting** 菜单，导航至 System Status.或者，您可以从以下位置查看磁盘使用情况：**Overview** 部分，在 Reporting 菜单.

在CLI中查看磁盘使用情况

- 从 **status** 或 status detail，您可以看到 **Reporting / logging Disk** 使用率

```
SWA.CLI> status

Enter "status detail" for more information.

Status as of:                  Sun Feb 19 19:55:13 2023 CET
Up since:                      Sat Feb 11 14:00:56 2023 CET (8d 5h 54m 17s)
System Resource Utilization:
  CPU                                    25.9%
  RAM                                    13.6%
  Reporting/Logging Disk                 58.1%
```

- 从 **ipcheck**，您可以看到分配给每个分区的磁盘空间以及每个分区已用空间的百分比。

```
SWA.CLI> ipcheck
...
  Disk 0                200GB VMware Virtual disk 1.0 at mpt0 bus 0 scbus2 target 0 lun 0
  Disk Total            200GB
=== Skiped ===
  Root                  4GB 65%
  Nextroot              4GB 1%
  Var                   400MB 29%
  Log                   130GB 8%
  DB                    2GB 0%
  Swap                  8GB
  Proxy Cache           50GB
```

```
=== Skiped ===
```

- 在SHD日志中， **Reporting / logging Disk** 每分钟的利用率显示为 DskUtil.要访问SHD日志，请执行以下步骤：

1. 类型grep 或tail 在CLI中
2. 查找 **shd_logs**.type： SHD Logs Retrieval: FTP Poll，并键入相关号码。
3. 在 Enter the regular expression to grep，可以键入正则表达式在日志中搜索。例如，可以键入日期和时间。
4. Do you want this search to be case insensitive? [Y]>，您可以将此选项保留为默认值，除非您需要搜索区分大小写（在SHD日志中，不需要此选项）。
5. Do you want to search for non-matching lines? [N]>，您可以将此行设置为默认值，除非您需要搜索除grep正则表达式之外的所有内容。
6. **Do you want to tail the logs? [N]>**.此选项仅在grep的输出中可用，如果将其设为默认值(N)，则它显示当前文件第一行中的SHD日志。
7. **Do you want to paginate the output? [N]>**.如果您选择 Y输出与less命令的输出相同。您可以在行和页面之间导航。此外，您还可以在日志中搜索(键入/然后键入关键字，然后按 Enter影响。要退出日志，请键入 q.

在本示例中，52.2%的 **Reporting / logging Disk** 已使用。

```
Mon Feb 20 23:46:14 2023 Info: Status: CPULd 66.4 DskUtil 52.2 RAMUtil 11.3 Reqs 0 Band 0 Latency 0 Cac
```

I

磁盘结构和完全分区故障排除

正如前面从输出中提到的 ipcheck,SWA中有七个分区：

分区名称	描述
根	保留内部操作系统文件
下一根	此分区用于升级
Var	保留内部操作系统文件
日志	保留日志和报告文件
DB	配置和内部数据库
交换	交换内存
代理缓存	保留缓存的数据

根分区已满

如果根分区(称为rootfs或/)已满或超过100%（有时这是预期值），则SWA会删除不必要的文件。

如果看到系统性能下降，请首先尝试重新启动设备，然后再次检查根分区的磁盘容量。如果问题仍然存在，请联系思科客户服务以打开TAC案例。

下一个根分区已满

如果升级失败，请确保下一个根分区可用或有足够的可用空间进行升级，

最初，虚拟SWA、邮件安全设备(ESA)和虚拟安全管理设备(SMA)SMA映像的下一根分区大小小于500MB。多年以来，随着包含其他功能的较新AsyncOS版本的推出，升级在整个升级过程中不得不越来越多地使用此分区中的更多内容。有时，当您尝试从较旧版本升级时，升级会因分区大小而失败。

从CLI的升级日志中，您可以看到以下错误：

```
Finding partitions... done.
Setting next boot partition to current partition as a precaution... done.
Erasing new boot partition... done.
Extracting eapp done.
Extracting scanerroot done.
Extracting splunkroot done.
Extracting savroot done.
Extracting ipasroot done.
Extracting ecroot done.
Removing unwanted files in nextroot done.
Extracting distroot
/nextroot: write failed, filesystem is full
./usr/share/misc/termcap: Write failed
./usr/share/misc/pci_vendors: Write to restore size failed
./usr/libexec/getty: Write to restore size failed
./usr/libexec/ld-elf.so.1: Write to restore size failed
./usr/lib/libBlocksRuntime.so: Write to restore size failed
./usr/lib/libBlocksRuntime.so.0: Write to restore size failed
./usr/lib/libalias.so: Write to restore size failed
./usr/lib/libarchive.so: Write to restore size failed
```

对于虚拟SWA，请根据本文档下载新的映像文件：思科安全邮件和网络虚拟设备安装指南

然后，尝试将配置备份从旧版本导入到新安装的SWA。如果您看到 **Configuration Import Error**，请创建服务请求案例。

对于SMA和ESA，您可以通过此链接找到此问题的解决方法：如何应用Cisco vESA/vSMA升级的解决方法由于分区大小较小而失败 — Cisco

Var分区已满

如果 **Var** 分区已满，当您登录CLI或从 Displayalerts 命令：

```
/var: write failed, filesystem is full
The temporary data partition is at 99% capacity
```

要解决此问题，请首先重新启动设备。如果/var分区的容量仍大于100%，请联系Cisco TAC支持。

报告/日志记录分区已满

如果报告/日志记录分区已满，错误可能为：

```
Processing of collected reporting data has been disabled due to lack of logging disk space. Disk usage
User admin  Disk space for /data has exceeded threshold value 90% with current capacity of 99 %

The reporting/logging disk is full on a WSA

WARNING: Data partition utilization on appliance is high and can cause issues
```

这些错误的根本原因可分类为：

1. 日志文件占用太多磁盘空间。
2. 设备上生成的一些核心文件导致磁盘使用率达到全满。
3. 报告占用太多磁盘空间。
4. Web跟踪占用了过多的磁盘空间。
5. 某些内部日志占用了过多的磁盘空间。

日志文件占用太多磁盘空间

要查看日志文件，可以通过FTP连接到SWA到管理接口。

注意：默认情况下，FTP处于禁用状态。

要从GUI启用FTP，请执行以下步骤：

步骤1:登录到GUI。

第二步：点击 **Interfaces** 在 **Network** 菜单.

第三步：点击 Edit Settings.

第四步：选择 **FTP** 从 Appliance Management Services 部分。

步骤5.(可选)您可以更改默认FTP端口。

第六步：点击 Submit.

步骤 7.提交更改。

在FTP连接后，可以查看每个日志文件的日志、创建日期和大小。如果需要归档日志，可以从FTP下载它们。或者，为了释放磁盘空间，您可以删除旧日志。

使用以下步骤解决此问题：

提示：如果您看到日志文件没有占用太多磁盘空间，则问题很可能与报告或核心文件有关。

设备上的核心文件

要查看SWA是否具有核心文件，请从CLI使用以下步骤：

步骤1:登录到CLI。

第二步：执行命令： **diagnostic** （它是一个隐藏的命令，不能用TAB自动填充）。

第三步：类型 PROXY.

第四步：类型 **LIST**.

输出显示是否有任何核心文件。要删除核心文件，请联系思科支持服务，TAC工程师需要调查核心文件的原因，然后他们可以删除这些文件。

报告占用太多磁盘空间

SWA中有两种类型的报告：报告和网络跟踪。WebTracking占用了大部分磁盘空间。

要检查WebTracking的历史记录，请导航至 WebTracking 从GUI。在 **Reporting** 菜单，从 **Time Range** 部分，选择 **Custom Range**，突出显示的日期显示WebTracking报告历史记录。

要从WebTracking进行备份，您可以从以下位置将报告导出到CSV: **Printable Download** 链接。

提示：避免长时间生成WebTracking报告，这取决于正常的日常Web流量。持续时间较长的报告可能导致SWA变得无响应。

在撰写本文时，没有手动删除旧报告的功能。(思科漏洞ID CSCun82094)

要删除某些报告，您需要联系TAC支持，或者通过以下步骤从CLI删除所有报告：

步骤1:登录到CLI。

第二步：执行 **diagnostic** 命令。（这是一个隐藏命令，无法通过TAB自动完成。）

第三步：类型 REPORTING 并按 **Enter**.

第四步：类型 DELETEDB 并按 Enter.

⚠ 注意：此命令删除所有报告数据。无法中止。

内部日志占用磁盘

如果您的设备存在以下缺陷：Cisco Bug ID CSCvy69039，您需要打开TAC案例以检查后端的内部日志并手动删除大型日志文件。

这是一种临时解决方法，但在受影响的版本中，日志文件将在删除后自动创建，并且文件大小会再次从0重复增长。

相关信息

- WSA AsyncOS版本说明
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。