Resolve Secure Web Appliance Full Disk Error

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Errors Related to Full Disk

Monitor Disk Usage

- View Disk Usage in GUI
- View Disk Usage in CLI

Disk Structure and Troubleshoot Full Partition

- Root Partition is Full
- Next Root Partition is Full
- Var Partition is Full
- The Operating System Partition at XX% Capacity
- Reporting/Logging Partition is Full
  - Log Files Occupy Too Much Disk Space
  - Core Files on the Device
  - Reporting Occupies Too Much Disk Space
  - Internal Logs Occupy Disk

Related Content

Introduction

This document describes the steps to resolve Full Disk Space Errors in Secure Web Appliance (SWA).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- FTP Access to SWA
- Access to CLI of SWA

- Administrative Access to SWA

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Errors Related to Full Disk

There are various errors and warnings in SWA that indicate the disk is full or the disk space is nearly full. This is a list of errors and warnings. These logs vary in each software version due to the delivery methods, such as alerts, system logs, or the output of the displayalerts command from the CLI.

```
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
```

Monitor Disk Usage

You can monitor and view disk usage from both the GUI and CLI.

View Disk Usage in GUI

After you log in to the SWA GUI, in the **My-Dashboard Page**, you can view the **Reporting / Logging Disk** usage from the **System Overview** section.

Note: SWA reports and logs are stored in a single partition, known as the **DATA** Partition.

Also in the GUI, under the **Reporting Menu**, navigate to System Status. You can also view the disk usage from the **Overview** section, under the Reporting menu.

View Disk Usage in CLI

From the output of the **status** or **status detail**, you can view the **Reporting / Logging Disk** usage:

```
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%
```

From the output of **ipcheck**, you can view the allocated disk space to each partition and the percentage of used space per partition:

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

In the SHD Logs, the Reporting / Logging Disk utilization for every minute is shown as **DskUtil**. To access the SHD Logs, use these steps:

1. Type **grep** or **tail** in the CLI.

2. Find **shd_logs Type: SHD Logs Retrieval**: **FTP Poll**, from the list and enter the associated number.

3. In **Enter the regular expression to grep**, you can enter a regular expression to search inside the logs. For example, you can type the date and time.

4. **Do you want this search to be case insensitive? [Y]>**, you can leave this as the default, unless you need to search for case sensitivity, which, in the SHD logs, you do not need this option.

5. **Do you want to search for non-matching lines? [N]>**, you can set this line as default, unless you need to search for everything except your regular grep expression.

6. **Do you want to tail the logs? [N]**>, This option is only available in the output of the grep, if you leave this as default (N), it shows the SHD Logs from the first line of current file.

7. **Do you want to paginate the output? [N]**>, If you select Y, the output is the same as the output of the less command. You can navigate between lines and pages. Also, you can search inside the logs (Type **/** then the keyword and press **Enter**). To exit the log, type q.

In this example 52.2% of the **Reporting / Logging Disk** is consumed:

```
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
```

Disk Structure and Troubleshoot Full Partition

As mentioned previously from the output of ipcheck, there are seven partitions in SWA:

Partition Name	**Description**
Root	Keeps internal operation system files
Nextroot	This partition is used for upgrades
Var	Keeps internal operation system files
Log	Holds logs and reporting files
DB	Configuration and internal databases
Swap	SWAP memory
Proxy Cache	Keeps cached data

Root Partition is Full

If the root partition (known as **rootfs** or /) is full or more than 100%, which is sometimes expected, and the SWA removes unnecessary files. If you see some system performance drop, first, try to reboot the appliance,

then check the disk capacity of the root partition. If the issue persists, contact Cisco Customer Service to open a TAC Case.

Next Root Partition is Full

If your upgrade fails, ensure your Next Root partition has enough free space for the upgrade.

Initially, virtual SWA, Email Security Appliance (ESA), and Virtual Security Management Appliance) SMA images were built with a Next Root partition with a size less than 500 MB. Over the years, and with newer AsyncOS releases that include additional features, upgrades have used this partition throughout the upgrade process. When you try to upgrade from older versions, upgrades fail because of the partition size.

From upgrade logs in the CLI, you can view these errors:

```
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
```

For a virtual SWA, download a new image file from the Cisco Secure Email and Web Virtual Appliance Installation Guide. Then import the configuration backup from the older version to the newly installed SWA. If you see a **Configuration Import Error**, open a Service Request Case.

For SMA and ESA, you can find a workaround for this issue: How to Apply the Workaround for Cisco vESA/vSMA Upgrade Fail Due to Small Partition Size - Cisco.

Var Partition is Full

If the **var** partition is full, you can receive these errors when you log in to CLI or from the **Displayalerts** command in CLI:

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

To resolve this issue, first, restart the appliance. If the capacity of the /var partition is more than 100%, contact Cisco TAC Support.

The Operating System Partition at XX% Capacity

If you receive the "The operating system partition is at 91% capacity" error, this is usually related to the /nextroot partition. From the CLI, run the **ipcheck** command:

```
SWA_CLI> ipcheck
...

  Disk 0                1024GB VMware Virtual disk 1.0 at mpt0 bus 0 scbus2 target 0 lun 0
  Disk Total            1024GB

  Root                  2GB 95%
  Nextroot              2GB 92%
  Var                   400MB 60%
  Log                   808GB 21%
  DB                    2GB 0%
  Swap                  8GB
  Proxy Cache           200GB
```

If the size of Next Root Partition is 2 GB, due to Field Notice: FN72230, you must install a new Virtual Machine version greater than 14.5 in the Next Root Partition and it must be 4 GB. You must also migrate from the old SWA to the new SWA.

For more information, refer to How to Apply the Workaround for Cisco vESA/vSMA Failing Upgrade Due to Small Partition Size.

Reporting/Logging Partition is Full

If the Reporting / Logging partition is full, these are some errors you can encounter:

```
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
```

The root cause of these errors can be categorized as:

1. Log files occupy too much disk space.

2. There are some core files generated on the device that leads to full disk usage.

3. Reporting occupies too much disk space.

4. Web Tracking occupies too much disk space.

5. Some internal logs occupy too much disk space.

Log Files Occupy Too Much Disk Space

To view log files, you can connect to the SWA via FTP to the management interface.

 **Note**: FTP by default is disabled.

To enable FTP from the GUI, use these steps:

1. Log in to the GUI.

2. Click **Interfaces** under the **Network** Menu.

3. Click **Edit Settings**.

4. Select **FTP** from the **Appliance Management Services** section.

5. (Optional): You can change the default FTP Port.

6. Click **Submit**.

7. **Commit** Changes.

After the FTP connection, you can view the logs, creation date, and size of each log file. If you need to archive the logs, you can download them via FTP. Or to free up disk space, you can remove old logs.

Use these steps to resolve this issue:

Tip: If you see the log files did not occupy much disk space, the issue most likely is related to reports or core files.

Core Files on the Device

To view if SWA has core files, from CLI use these steps:

1. Log in to CLI.

2. Run the **diagnostic** command (it is a hidden command and cannot be auto-filled with TAB).

3. Type **PROXY**.

4. Type **LIST**.

The output shows if there are any core files. To remove the core files, contact Cisco Support Service, a TAC Engineer must investigate the cause of core files, then they can remove the files.

Reporting Occupies Too Much Disk Space

There are two types of reports in SWA: Reporting and WebTracking. WebTracking occupies most of the disk space. To check the history of WebTracking, navigate to **WebTracking** from the GUI. Under the **Reporting** menu, from the **Time Range** section, select **Custom Range**. The highlighted dates show the **WebTracking Report History**.

To take a back-up from WebTracking, you can export the report to .CSV from the **Printable Download** link in the report.

Tip: Avoid the generation of WebTracking reports for long time periods, which depends on the normal daily web traffic. Reports for longer durations can cause SWA to became unresponsive.

At the time this article was written, there is no feature to manually delete older reports (Cisco bug

ID: CSCun82094).

To delete some of your reports, you must contact TAC Support, or you can delete all the reports from the CLI with these steps:

1. Log in to CLI.

2. Run the **diagnostic** command (it is a hidden command and cannot be auto completed with TAB).

3. Type **REPORTING** and press **Enter**.

4. Type **DELETEDB** and press **Enter**.

⚠ **Caution**: This command deletes all reports data and it cannot be aborted.

If you have SWA S195 or S190, consider this defect as well: Cisco bug ID CSCwd83093.

Internal Logs Occupy Disk

If your device has the conditions of the Cisco bug ID: CSCvy69039, you must open a TAC Case to check the internal logs from the back-end and remove the large log files manually.

This is a temporary workaround, however, on the affected version, the log file is auto created after deletion and the file size repeatedly grows from 0 again.

Related Content

- WSA AsyncOS Release Notes
- Technical Support & Documentation - Cisco Systems