Troubleshoot Secure Web Appliance Performance with SHD Logs

Contents

Introduction

This document describes System Health Daemon logs (shd_logs) and how to troubleshoot Secure Web Appliance (SWA) performance issue with this log.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Physical or Virtual Secure Web Appliance (SWA) Installed.
- License activated or installed.
- Secure Shell (SSH) Client.
- The setup wizard is completed.

- Administrative Access to the 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.

What is SHD LOGS

SHD logs hold most of the performance related process statistics in SWA for every one minute.

Here is an example a SHD log line:

```
Mon Jun 9 23:46:14 2022 Info: Status: CPULd 66.4 DskUtil 5.2 RAMUtil 11.3 Reqs 0 Band 0 Latency 0 CacheH
SrvConn 0 MemBuf 0 SwpPgOut 0 ProxLd 0 Wbrs_WucLd 0.0 LogLd 0.0 RptLd 0.0 WebrootLd 0.0 SophosLd 0.0 Mca
```

SHD logs are acceptable from Command line interface (CLI) and from File Transfer Protocol (FTP). There are no options to view the log from Graphical User interface (GUI).

Access SHD Logs

From the CLI:

1. Type **grep** or **tail** in CLI.
2. Find **"shd_logs Type: SHD Logs Retrieval: FTP Poll** from the list and type the associated number.
3. In **Enter the regular expression to grep.** You can type regular expressions to search inside the logs, for example, you can type date and time.
4. **Do you want this search to be case insensitive? [Y]>** You can leave this as default unless you need to search for case sensitive which in 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 Grep regular expression.
6. **Do you want to tail the logs? [N]>** This option is only available in the output of the grep, if you let 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 select "Y", the output is same as output of less command, you can navigate between lines and pages also you can search inside the logs (Type **/** then the keyword and hit enter), to exit the log view by type **q**.

From FTP:

1. Make sure FTP is enabled from **GUI > Network > Interfaces**.
2. Connect to SWA via FTP.
3. Shd_logs folder, contains the logs.

SHD Log Fields

The fields in the SHD logs detailed:

Field Number	Name	Identifier	Description
8	CPULd	Percentage % 0 ~ 99	CPU LOAD Total Percent of CPU used on the system as reported by the OS
10	DskUti	Percentage % 0 ~ 99	Disk Utilization spaced used on the /data partition
12	RAMUtil	Percentage % 0 ~ 99	RAM Utilization Percentage of free memory reported by OS

14	Reqs	Request / Seconds	Requests Average number of transactions (requests) in past minute
16	Band	Kb/s	Bandwidth Saved Average bandwidth saved in the past minute. - Equivalent to SNMP bandwidth saved average for the past minute
18	Latency [1]	Milliseconds (ms)	Average latency (response time) in the last minute takes the second field in access logs - that shows how much time the TCP connection takes from end user to WSA (or from end user to web server if connection was not decrypted) WSA sum up the times, for each request logged in access logs for last minutes and divide it into the numbers of these requests and get an average latency for SHD
20	CacheHit	Number #	Cache hit average in the past minute. - Equivalent to SNMP cache hit average for the past minute
22	CliConn	Number #	Total number of current Client Connections From Clients to WSA - equivalent to SNMP current total client

			connections
24	SrvConn	Number #	Total number of current Server Connections From WSA to Web server - Equivalent to SNMP current total server connections.
26	MemBuf [2]	Percentage % 0 ~ 99	Memory Buffer Current total amount of Proxy Buffer Memory that are free.
28	SwpPgOut	Number #	Number of pages that were swapped out, as reported by OS. Page File or Paging file, is space on a hard drive used as a temporary location to store information when RAM is fully utilized.
30	ProxLd	Percentage % 0 ~ 99	The prox Process load Process responsible to process all incoming requests (HTTP/HTTPS/FTP/SOCKS)
32	Wbrs_WucLd	Percentage % 0 ~ 99	Web Reputation Coring load Process used for actual WBRS scan engine. Proxy process interacts with reqscand process to perform WBRS scans.

34	LogLd	Percentage % 0 ~ 99	Proxy Log Load
36	RptLd	Percentage % 0 ~ 99	Report engine Load Process responsible to create Reporting database. 'reportd' interacts with 'haystackd' to create the Web Tracking database.
38	WebrootLd	Percentage % 0 ~ 99	Webroot Antimalware Load
40	SophosLd	Percentage % 0 ~ 99	Sophos Antivirus Load
42	McafeeLd	Percentage % 0 ~ 99	Mcafee Antivirus Load
44	WTTLd	Percentage % 0 ~ 99	Web Traffic Tap

46	AMPLd	Percentage % 0 ~ 99	Advanced Malwaer Protection (AMP)

1. Sometimes it could be expected to see a high peak in Latency in SHD logs, for example if there are not many requests on WSA and at some point there was finished a long duration connection - for example several days. Then this single request can increase the Latency for that minute when it finished and logged in access logs.

2. As written in :

> "RAM usage for a system that is working efficiently can be higher than 90%, because RAM that is not otherwise in use by the system is used by the web object cache. If your system is not experiencing serious performance issues and this value is not stuck at 100%, the system is operating normally."

> **Note**: Proxy Buffer Memory is one component that uses this RAM

Troubleshoot with SHD Logs

Other Process High Load

If the load of the other process is high, check the table-1 from this article and read the logs related to that process.

High Latency

If you saw high latency in the SHD logs, you must check the Proxy_track logs in **/data/pub/track_stats/** . Find the time frame which the latency is high. In the proxy track you have couple of records which are related to latency. The numbers in front of each section is the total number of occurrence since the last reboot. For example, in this code:

```
Current Date: Wed, 11 Jun 2022 20:03:32 CEST
...
   Client Time    6309.6 ms    109902
...
Current Date: Wed, 11 Jun 2022 20:08:32 CEST
...
   Client Time    6309.6 ms    109982
```

In 5 minutes, the number of clients requests which took 6309.6 ms or higher is 80 requests. So you have to subtracts the numbers in each time frame to get the accurate value you must consider these items:

Client Time: Time it takes from Client to SWA.

Hit Time: Cache hits: The Requested Data is in the cache and can be deliver to Client.

Miss Time: Cache miss: The Requested Data is not in the cache Or is not up-to-dated and cannot be delivered to Client.

Server Transaction Time: Time it takes from SWA to web Server.

Also these values must be considered in the process of performance check:

> **user time: 160.852 (53.33%)**
> **system time: 9.768 (3.256%)**

In Track Stat logs, Information logged every 5 minutes (300 seconds). In this example user time 160.852, is the time (in seconds), which CPU was loaded with tasks to handle user requests. System time is a the time that SWA processed network events, such as routing decision and so on. The sum of these two percentages is the total CPU Load on that time. If user time is high, it means that you need to consider a high complexity configuration.

Related Information

- **WSA AsyncOS Release Notes**
- **Compatibility Matrix for Cisco Secure Email and Web Manager**
- **Upgrades and Updates Connectivity Check**
- **Cisco Technical Support & Downloads**