使用SHD日志对安全Web设备性能进行故障排除

目录

简介

先决条件

- 要求
- 使用的组件

什么是SHD日志

访问SHD日志

简介

本文档介绍系统运行状况守护程序日志(shd_logs)以及如何解决此日志中的安全Web设备(SWA)性能问题。

先决条件

要求

Cisco 建议您了解以下主题：

- 已安装物理或虚拟安全网络设备(SWA)。
- 许可证已激活或已安装。
- 安全外壳(SSH)客户端。
- 安装向导已完成。
- 对SWA的管理访问。

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。

什么是SHD日志

SHD日志会每分钟保存一次SWA中大多数与性能相关的进程统计信息。

以下是SHD日志行的示例：

```
Mon Jun 9 23:46:14 2022 Info: Status: CPULd 66.4 DskUtil 5.2 RAMUtil 11.3 Reqs 0 Band 0 Latency 0 Cache
```

```
SrvConn 0 MemBuf 0 SwpPgOut 0 ProxLd 0 Wbrs_WucLd 0.0 LogLd 0.0 RptLd 0.0 WebrootLd 0.0 SophosLd 0.0 Mc
```

命令行界面(CLI)和文件传输协议(FTP)可以接受SHD日志。没有从图形用户界面(GUI)查看日志的选项。

访问SHD日志

在CLI中：

1. 在CLI中键入grep或tail。
2. 从列表中查找"shd_logs Type: SHD Logs Retrieval: FTP Poll并键入关联编号。
3. 在Enter the regular expression to grep中。 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. 是否希望此搜索不区分大小写？[Y]>您可以将此选项保留为默认值，除非您需要在SHD_Logs中搜索不区分大小写的选项。
5. 是否要搜索不匹配的行？[N]>除非您需要搜索除Grep正则表达式之外的所有内容，否则可以将此行设置为默认值。
6. 是否要跟踪日志？[N]>此选项仅在grep的输出中可用，如果将此选项设为默认值(N)，则它显示当前文件第一行中的SHD日志。
7. 是否要对输出进行分页？[N]>如果选择“Y”，则输出与较少命令的输出相同，您可以在行与页面之间导航，也可以在日志中搜索(键入/然后键入关键字，按Enter)，通过键入q退出日志视图。

从FTP:

1. 确保从GUI > Network > Interfaces启用了FTP。
2. 通过FTP连接到SWA。
3. Shd_logs文件夹，包含日志。

SHD日志字段

详细的SHD日志中的字段：

字段编号	名称	标识符	描述
8	CPULd	百分比% 0 ~ 99	CPU负载 操作系统报告的系统上CPU使用总百分比
10	DskUti	百分比% 0 ~ 99	磁盘利用率 在/data分区上间隔使用

12	RAMUtil	百分比% 0 ~ 99	RAM利用率 操作系统报告的可用内存百分比
14	要求	请求/秒	请求 过去一分钟内事务（请求）的平均数量
16	频段	Kb/s	节省的带宽 过去一分钟内节省的平均带宽。 — 相当于过去一分钟内平均节省的SNMP带宽
18	延迟[1]	毫秒(ms)	过去一分钟的平均延迟（响应时间） 采用访问日志中的第二个字段 — 显示TCP连接从最终用户到WSA所花费的时间（如果连接未解密，则从最终用户到Web服务器所花费的时间） WSA对登录访问日志的每条请求在最后几分钟内的时间进行汇总，然后将其划分为这些请求的数量并获得SHD的平均延迟
20	CacheHit	编号	过去一分钟内缓存命中平均值。 — 相当于过去一分钟的SNMP缓存命中平均值
22	CliConnect	编号	当前客户端连接总数

			从客户端到WSA — 相当于SNMP当前客户端连接总数
24	SrvConnect	编号	当前服务器连接总数 从WSA到Web服务器 — 相当于SNMP当前服务器连接总数。
26	MemBuf [2]	百分比% 0 ~ 99	内存缓冲区 当前可用的代理缓冲区内存总量。
28	SwpPgOut	编号	操作系统报告的交换页数。 页面文件或分页文件，是指硬盘驱动器上的空间，当RAM被充分利用时，该空间用作存储信息的临时位置。
30	ProxId	百分比% 0 ~ 99	代理进程负载 负责处理所有传入请求的进程 (HTTP/HTTPS/FTP/SOCKS)
32	Wbrs_WucLd	百分比% 0 ~ 99	Web信誉取心负载 用于实际WBRS扫描引擎的过程。代理进程与请求进程交互以执行WBRS扫描。

34	LogLd	百分比% 0 ~ 99	代理日志加载
36	RptLd	百分比% 0 ~ 99	报告引擎负载 负责创建报告数据库的进程。“reportd”与“haystackd”相互作用以创建Web跟踪数据库。
38	WebrootLd	百分比% 0 ~ 99	Webroot反恶意软件负载
40	SophosLd	百分比% 0 ~ 99	Sophos防病毒加载
42	McafeeLd	百分比% 0 ~ 99	Mcafee防病毒加载
44	WTTLd	百分比% 0 ~ 99	Web流量分接头

46	AMPLd	百分比% 0 ~ 99	高级恶意软件防护 (AMP)

1. 有时，可能在SHD日志中看到延迟的高峰，例如，如果WSA上的请求数量不多，并且在某些点上完成了长时间连接（例如几天）。然后，此单个请求可以在完成并登录访问日志时增加该分钟的延迟。

2.如书所写：

> “RAM使用率对于一个 working 因为系统未使用的RAM由Web对象缓存使用，所以效率可以高于90%。如果您的系统不是 experiencing 严重的性能问题，并且此值未停滞在100%，系统已 operating 通常如此。”

注意：代理缓冲区内存是使用此RAM的一个组件

使用SHD日志进行故障排除

其他进程高负载

如果其他进程的负载很高，请检查本文的table-1并读取与该进程相关的日志。

高延迟

如果在SHD日志中看到高延迟，则必须在/data/pub/track_stats/中检查Proxy_track日志。 查找延迟较高的时间段。 在代理跟踪中，您有与延迟相关的几个记录。 每个部分前面的数字是自上次重新启动后出现的总数。例如，在此代码中：

```
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
```

在5分钟内，耗时6309.6毫秒或以上的客户端请求数是80个请求。因此，您必须在每个时间范围内减去数字，才能获得准确值，您必须考虑以下项：

客户端时间：从客户端到SWA所用的时间。

命中时间：缓存命中数：请求的数据在缓存中，可以传送到客户端。

未命中时间：缓存未命中：请求的数据不在缓存中，或者不是最新数据，无法传送到客户端。

服务器事务时间：从SWA到Web服务器所用的时间。

此外，在性能检查过程中还必须考虑以下值：

用户时间：160.852(53.33%)
系统时间：9.768(3.256%)

在跟踪状态日志中，每5分钟（300秒）记录一次信息。 在本示例中，用户时间160.852是CPU加载处理用户请求的任务的时间（以秒为单位）。 系统时间是SWA处理网络事件（例如路由决策等）的时间。 这两个百分比的总和是当时的CPU总负载。 如果用户时间较长，则意味着您需要考虑高度复杂的配置。

相关信息

- WSA AsyncOS版本说明
- Cisco Secure Email and Web Manager的兼容性矩阵
- 升级和更新连接检查
- 思科技术支持和下载

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）。