使用SHD日誌排除安全Web裝置效能故障

目錄

簡介

本文檔介紹系統運行狀況守護程式日誌(shd_logs)，以及如何解決此日誌中的安全Web裝置(SWA)效能問題。

必要條件

需求

思科建議您瞭解以下主題：

- 已安裝物理或虛擬安全網路裝置(SWA)。
- 許可證已啟用或已安裝。
- 安全殼層(SSH)使用者端。
- 安裝嚮導已完成。

- 對SWA的管理訪問。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

什麼是SHD日誌

SHD日誌每分鐘儲存一次SWA中大多數與效能相關的進程統計資訊。

以下是SHD日誌行的示例：

```
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
```

命令列介面(CLI)和檔案傳輸協定(FTP)可以接受SHD日誌。沒有從圖形使用者介面(GUI)檢視日誌的選項。

訪問SHD日誌

在CLI上：

1. 在CLI中鍵入grep或tail。
2. 從清單中查詢「shd_logs Type: SHD Logs Retrieval: FTP Poll」，然後鍵入關聯的編號。
3. 在Enter the regular expression to grep中。 可以鍵入正規表示式在日誌中搜尋，例如，可以鍵入日期和時間。
4. 是否希望此搜尋不區分大小寫？[Y]>您可以將此選項保留為預設值，除非您需要搜尋區分大小寫的SHD_Logs中不需要此選項。
5. 是否要搜尋不匹配的行？[N]>您可以將此行設定為預設值，除非您需要搜尋除Grep正規表示式之外的所有內容。
6. 是否要跟蹤日誌？[N]>此選項僅在grep的輸出中可用，如果將此選項設定為預設值(N)，則它會顯示當前檔案第一行中的SHD日誌。
7. 是否要對輸出進行分頁？[N]>如果選擇「Y」，則輸出與less命令的輸出相同，您可以在行與頁面之間導航，還可以在日誌中搜尋(鍵入/然後鍵入關鍵字並按Enter)，通過鍵入q退出日誌視圖。

從FTP:

1. 確保從GUI > Network > Interfaces啟用FTP。
2. 通過FTP連線到SWA。
3. Shd_logs資料夾，包含日誌。

SHD日誌欄位

詳細的SHD日誌中的欄位：

欄位編號	名稱	識別碼	說明
8	CPULd	百分比% 0 ~ 99	CPU負載 作業系統報告的系統上CPU使用總百分比
10	DskUti	百分比% 0 ~ 99	磁碟利用率 在/data分割槽上間隔使用

12	RAMUtil	百分比% 0 ~ 99	RAM利用率 作業系統報告的可用記憶體百分比
14	需求	請求/秒	要求 過去一分鐘內平均事務（請求）數
16	頻段	Kb/s	節省的頻寬 過去一分鐘內節省的平均頻寬。 — 相當於過去一分鐘內平均節省的SNMP頻寬
18	延遲[1]	毫秒（毫秒）	最後一分鐘的平均延遲（響應時間） 使用訪問日誌中的第二個欄位 — 顯示TCP連線從終端使用者到WSA所花費的時間（如果連線未解密，則從終端使用者到Web伺服器所花費的時間） WSA對過去幾分鐘內登入訪問日誌的每個請求的次數進行累計，並將其除以這些請求的次數，從而獲得SHD的平均延遲
20	CacheHit	編號#	快取過去一分鐘內平均命中率。 — 相當於過去一分鐘的SNMP快取命中平均值
22	CliConn	編號#	當前客戶端連線總數

			從客戶端到WSA — 相當於SNMP當前客戶端連線總數
24	SrvConn	編號#	當前伺服器連線總數 從WSA到Web伺服器 — 相當於SNMP當前伺服器連線總數。
26	MemBuf [2]	百分比% 0 ~ 99	記憶體緩衝區 當前可用的代理緩衝區記憶體總量。
28	SwpPgOut	編號#	OS報告的換出頁數。 Page File或Paging file是硬碟驅動器上的空間，用作當RAM充分利用時儲存資訊的臨時位置。
30	ProxId	百分比% 0 ~ 99	代理進程負載 負責處理所有傳入請求的進程 (HTTP/HTTPS/FTP/SOCKS)
32	Wbrs_WucLd	百分比% 0 ~ 99	Web聲譽取心負載 用於實際WBRS掃描引擎的進程。代理進程與請求進程互動以執行WBRS掃描。

34	LogLd	百分比% 0 ~ 99	代理日誌載入
36	RptLd	百分比% 0 ~ 99	報表引擎負載 負責建立報表資料庫的進程。「reportd」與「haystackd」互動以建立Web跟蹤資料庫。
38	WebrootLd	百分比% 0 ~ 99	Webroot反惡意軟體載入
40	SophosLd	百分比% 0 ~ 99	Sophos防病毒載入
42	McafeeLd	百分比% 0 ~ 99	Mcafee防病毒載入
44	WTTLd	百分比% 0 ~ 99	Web流量分流器

46	AMPLd	百分比% 0 ~ 99	進階惡意軟體防護

1. 有時，可以預期在SHD日誌中看到延遲的高峰，例如，如果WSA上的請求數量不多，並且在某個時間點完成了一個長持續時間的連線，例如幾天。這樣，當該請求完成並登入訪問日誌時，該請求會增加該分鐘的延遲。

2.如書所寫：

> "RAM使用率 working 因為系統未使用的RAM由Web對象快取使用，所以效率可以高於90%。如果您的系統不是 experiencing 嚴重的效能問題，並且此值不會停滯在100%，系統將 operating 正常情況下。」

注意：代理緩衝區記憶體是使用此RAM的一個元件

SHD日誌故障排除

其他進程高負載

如果另一個進程的負載很高，請檢查本文的表–1並讀取與該進程相關的日誌。

高延遲

如果您在SHD日誌中看到高延遲，您必須檢查/data/pub/track_stats/中的Proxy_track日誌。 查詢延遲較高的時段。 在代理路徑中，您有與延遲相關的兩條記錄。 每個部分前面的數字是自上次重新引導以來發生的總次數。例如，在此代碼中：

```
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分鐘內，耗時6309.6毫秒或更高的客戶端請求數是80個請求。因此，您必須在每個時間範圍內減去數字，才能獲得準確值，您必須考慮以下事項：

客戶端時間：從客戶端到SWA所用的時間。

命中時間：緩存命中數：請求的資料位於快取中，可以傳遞給客戶端。

錯過時間：快取未命中：請求的資料不在快取中，或者不是最新資料，無法傳遞給客戶端。

伺服器事務時間：從SWA到Web伺服器所用的時間。

此外，在效能檢查過程中還必須考慮以下值：

使用者時間：160.852(53.33%)
系統時間：9.768(3.256%)

在跟蹤狀態日誌中，每5分鐘（300秒）記錄一次資訊。 在此示例中，使用者時間160.852是CPU載入處理使用者請求的任務的時間（以秒為單位）。 系統時間是SWA處理網路事件（如路由決策等）的時間。 這兩個百分比的總和就是該時間的CPU總負載。 如果使用者時間較長，則意味著您需要考慮高度複雜的配置。

相關資訊

- 《 WSA AsyncOS發佈說明》
- Cisco Secure Email and Web Manager的相容性清單
- 升級和更新連線檢查
- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。