在Secure Web Appliance中配置請求調試日誌

目錄

簡介

本文檔介紹在Secure Web Appliance(SWA)中請求調試日誌的步驟。

必要條件

需求

思科建議瞭解以下主題：

- 對SWA的命令行介面(CLI)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。

請求調試日誌

SWA中的請求調試日誌是一種專門化的日誌型別，旨在捕獲單個特定HTTP或HTTPS事務或客戶端

電腦中極其詳細的端到端調試和跟蹤級別資訊。與記錄許多請求中的彙總事件的標準代理日誌不同，請求調試日誌將來自處理特定請求（如身份驗證、URL過濾、解密、惡意軟體掃描和信譽服務）所涉及的所有Web代理模組的調試輸出聚合到一個相關的日誌流中。此日誌型別僅用於深度診斷，只能通過CLI建立，而不能通過GUI建立

在排除標準日誌缺乏足夠詳細資訊的複雜或間歇性代理問題時，請求調試日誌至關重要。它們使管理員和Cisco TAC能夠準確跟蹤每個處理階段處理單個請求的方式，從而能夠查明根本原因，例如意外策略匹配、掃描延遲、身份驗證失敗或引擎之間的判定不一致。由於日誌集中於一個事務，因此它提供了最大的可視性，而不會影響系統範圍內在所有代理模組之間啟用調試日誌記錄所帶來的運營開銷和效能影響。這使得請求調試日誌在高級調查期間成為準確、高效且低風險的診斷工具。

配置請求調試日誌

步驟1.登入到CLI，運行logconfig，然後選擇new。

步驟2.選擇與Request Debug Logs關聯的編號，然後按Enter。

步驟3.輸入日誌的名稱。

步驟4.選擇Trace作為日誌記錄級別。

步驟5.選擇請求收集增強日誌記錄的模組。可以用逗號分隔或範圍清單（如1、3、4或3-7）的形式進行多個選擇。

提示：如果TAC未請求任何特定模組，則最好選擇所有模組（例如1-30）。

步驟6.指定要啟用增強日誌記錄的請求數。一旦捕獲了此數量的請求，日誌記錄將自動停止。

附註：在故障排除過程中，根據流量條件選擇合理值非常重要。例如，如果使用的是專用測試電腦，並且後台流量最小，則只需較低數量的請求就足夠了。但是，在後台活動較高的環境中（如作業系統更新、瀏覽器後台請求或Webex等應用程式），選擇較高的值可確保捕獲相關事務。

步驟7.通過選擇Client IP address、Destination IP address或Destination domain，定義用於增強日誌記錄的請求匹配條件。

附註：在大多數情況下，建議選擇客戶端IP地址，即使對訪問單個網站進行故障排除時，這種

方法仍可確保捕獲在頁面載入期間生成的所有Web請求，包括對可能不可立即看到的其他URL的後台請求。但是，當使用具有最少背景Internet流量的專用測試電腦時，此方法最有效。在客戶端產生大量額外流量的環境中（如作業系統更新、瀏覽器後台服務或Webex等應用），最好按目標域或目標IP地址進行過濾器。

提示：如果確切故障點未知，則可以收集瀏覽器HAR日誌，以識別出現問題（例如頁面載入失敗或高延遲）的特定URL或域，然後可以在請求調試日誌條件中配置該域。

步驟8.選擇檢索日誌的方法。如果選擇「FTP Poll」，則會在SWA上儲存日誌。

步驟9.定義用於日誌檔案的檔名，或按Enter接受當前生成的檔名。

步驟10.為基於時間的日誌檔案滾動更新選擇No，因為日誌記錄將在達到定義的請求數後停止。

步驟11.定義最大檔案大小（以位元組為單位），或按Enter接受當前值。

提示：定義更大的日誌檔案大小會增加下載和檢視日誌的難度。建議增加日誌檔案的數量，而不是增加單個日誌檔案的大小（下一步）。 此方法提高了可管理性，同時確保捕獲所有所需的調試資訊而不會建立過大的檔案。

步驟12.根據為在步驟5中記錄而選擇的代理模組數和在步驟7中定義的請求匹配條件來配置日誌檔案的最大數量。選擇合理的檔案限制對於確保捕獲所有相關調試資訊而不提前停止日誌記錄非常重要，因為日誌記錄可能導致日誌不完整或丟失。

步驟13.如果系統提示由於允許的最大檔案數而刪除檔案時，是否傳送警報？請選擇No。這樣可以防止在正常日誌旋轉過程中產生不必要的警報，特別是出於故障排除目的故意生成「請求調試日誌」時。

步驟14.出現Do you want to compress logs(yes/no)? 提示時，選擇No。這樣可以保持日誌檔案的未壓縮狀態，使其在故障排除期間更易於檢視和分析。

步驟15.按Enter退出嚮導

步驟16.鍵入commit，然後按Enter儲存更改

```
SWA_CLI> logconfig

Currently configured logs:
```

```
1. "accesslogs" Type: "Access Logs" Retrieval: FTP Poll
2. "adc_logs" Type: "ADC Engine Logs" Retrieval: FTP Poll
...
[Output removed to simplify readability]
...
55. "welcomeack_logs" Type: "Welcome Page Acknowledgement Logs" Retrieval: FTP Poll

Choose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- HOSTKEYCONFIG - Configure SSH host keys.
- AUDITLOGCONFIG - Adjust settings for audit logging.
[]> new

Choose the log file type for this subscription:
1. ADC Engine Framework Logs
2. ADC Engine Logs
...
[Output removed to simplify readability]
...
53. Request Debug Logs
...
[Output removed to simplify readability]
...
[1]> 53

Please enter the name for the log:
[]> Request_Debug_Logs

Log level:
1. Critical
2. Warning
3. Information
4. Debug
5. Trace
[3]> 5

Choose modules where enhanced request logging is to be performed.
Multiple selections can be made in the form of a comma separated or range list (e.g. 1,3,4 or 3-7)
Choosing the Default Proxy will enable enhanced logging across modules:
1. Default Proxy
2. Access Control Engine
3. Proxy Configuration
4. Disk Manager
5. Memory Manager
6. McAfee Integration Framework
7. Sophos Integration Framework
8. Webroot Integration Framework
9. Webcat Integration Framework
10. Connection Management
11. Authentication Framework
12. HTTPS
13. FTP proxy
14. WCCP Module
15. License Module
16. SNMP Module
17. WBRS Integration Framework
18. Logging Framework
19. Data Security Module
20. Miscellaneous Proxy Modules
21. DCA Engine Framework
```

```
22. AVC Engine Framework
23. Cloud Connector
24. SOCKS Proxy
25. Advanced Malware Protection
26. ArchiveScan module in proxy
27. Web Traffic Tap module in proxy
28. Bandwidth Control
29. Http2 proxy
30. ADC Engine Framework
[1]> 1-30

Please enter the number of requests for which to perform enhanced logging:
[1]> 100

Choose the request criteria for logging:
1. Client IP Address
2. Destination Domain
3. Destination IP Address
[1]> 1

Specify source IP address
[]> 10.20.3.15

Choose the method to retrieve the logs:
1. FTP Poll
2. FTP Push
3. SCP Push
[1]> 1

Filename to use for log files:
[Request_Debug_Logs.text]>

Do you want to configure time-based log files rollover? [N]>

Please enter the maximum file size:
[10485760]>

Please enter the maximum number of files:
[10]> 50

Should an alert be sent when files are removed due to the maximum number of files allowed? [N]>

Do you want to compress logs (yes/no)
[n]>

Currently configured logs:
1. "Request_Debug_Logs" Type: "Request Debug Logs" Retrieval: FTP Poll
2. "accesslogs" Type: "Access Logs" Retrieval: FTP Poll
3. "adc_logs" Type: "ADC Engine Logs" Retrieval: FTP Poll
...
[Output removed to simplify readability]
...
56. "welcomeack_logs" Type: "Welcome Page Acknowledgement Logs" Retrieval: FTP Poll


SWA_LIC> commit

Warning: In order to process these changes, the proxy
process will restart after Commit. This will cause a brief
interruption in service. Additionally, the authentication
cache will be cleared, which might require some users to
authenticate again.
```

相關資訊

- Cisco Secure Web Appliance AsyncOS 15.2使用手冊
- 使用安全Web裝置最佳做法
- 訪問安全Web裝置日誌
- 使用Microsoft Server配置SWA中的SCP推送日誌

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）。