配置訪問日誌中的效能引數

目錄

簡介

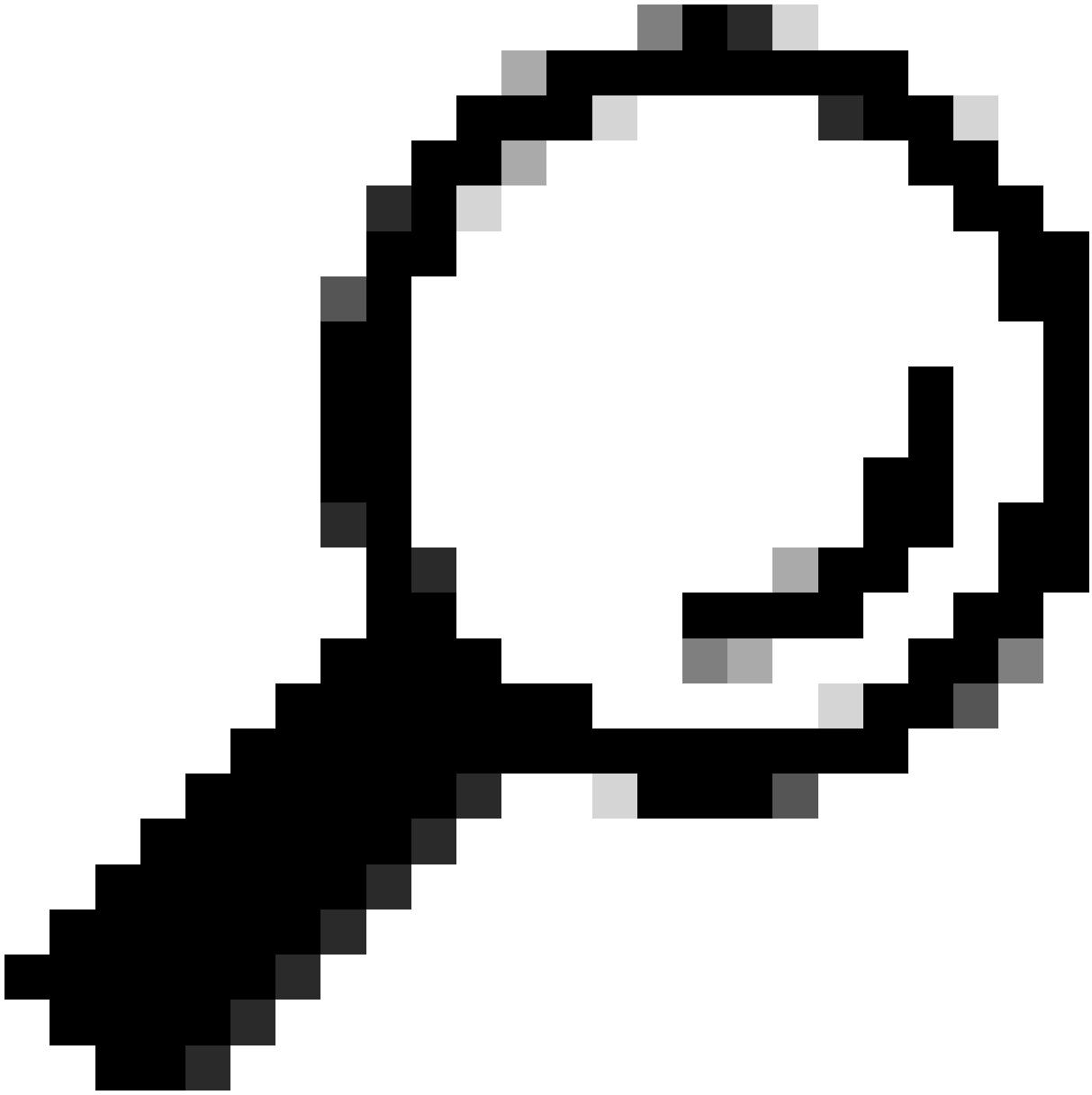
本文檔介紹將Performance parameter custom欄位新增到Secure Web Appliance(SWA)訪問日誌的步驟。

必要條件

需求

思科建議您瞭解以下主題：

- 安全殼層協定(SSH)訪問SWA管理介面。
- 圖形使用者介面(GUI)訪問SWA管理介面。



提示：最好在SWA資料分割槽上具有超過20%的可用磁碟空間。您可以在status detail命令的輸出中通過命令列介面(CLI)檢查磁碟使用情況。

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。

背景資訊

當存在延遲問題且流量通過SWA代理時，訪問日誌有助於排除延遲的根本原因。您可以更改當前的

訪問日誌設定，或使用新增到自定義欄位的效能引數建立新的訪問日誌。

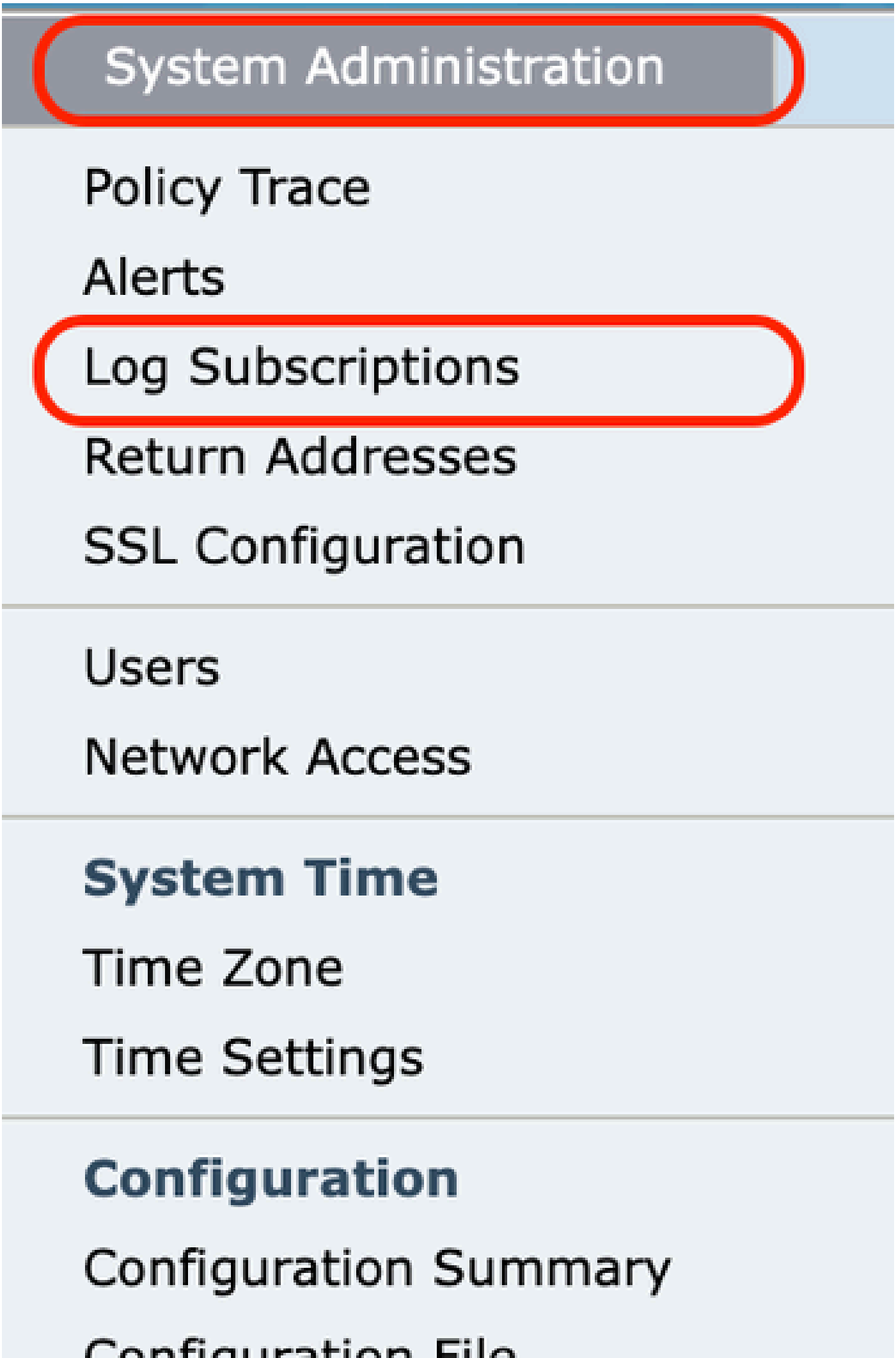
建立額外訪問日誌

在某些條件下，由於內部策略或其他某些配置，無法更改當前訪問日誌。為克服此限制，您可以建立另一個訪問日誌並在新的訪問日誌中新增自定義效能引數。

從GUI建立新訪問日誌

步驟1.登入GUI。

步驟2.從System Administration選單中選擇Log Subscriptions。


System Administration
Policy Trace
Alerts
Log Subscriptions
Return Addresses
SSL Configuration
Users
Network Access
System Time
Time Zone
Time Settings
Configuration
Configuration Summary

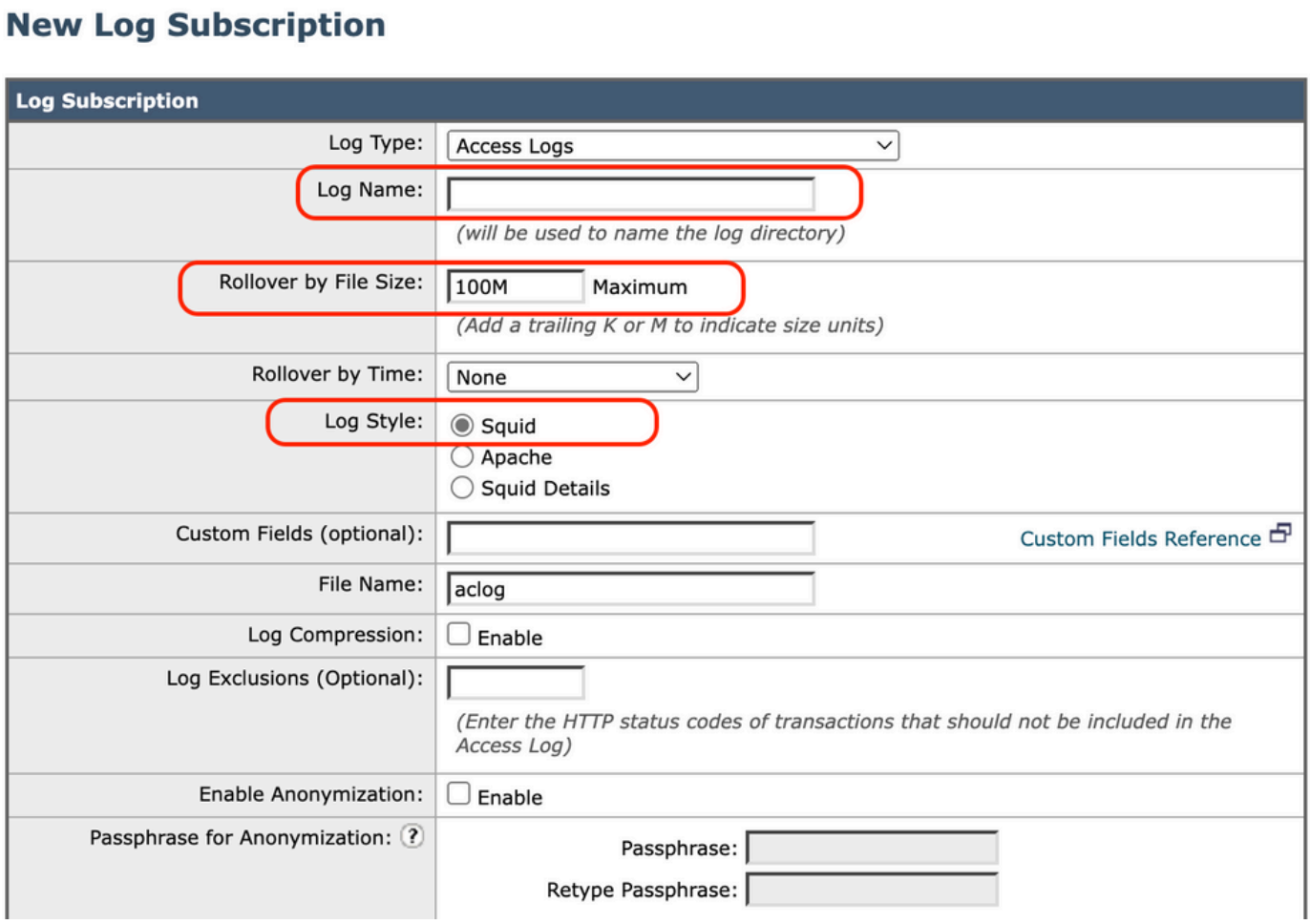
在當前日誌檔案達到使用者指定的最大檔案大小限制（或自上次滾動後的最長時間）時存檔（滾過）日誌訂閱。

步驟7.選擇Squid作為日誌樣式。

步驟8.檔名是為這個新日誌定義資料夾名稱和日誌檔名稱。建議與日誌名稱相同，在本例中為TAC_access_logs。

步驟9.您可以啟用日誌壓縮以壓縮日誌檔案，或者將日誌保留為文本檔案。

步驟10.日誌排除用於過濾超文本傳輸協定(HTTP)響應代碼。請勿過濾HTTP狀態代碼。



填寫必填欄位

步驟11.選擇FTP輪詢以將日誌保留在SWA中。輸入1並按Enter。

步驟12. Submit和commit更改。

從CLI配置新的訪問日誌

步驟1.登入到CLI。

步驟2.執行logconfig。

步驟3.要建立新日誌，請鍵入New並按Enter鍵。

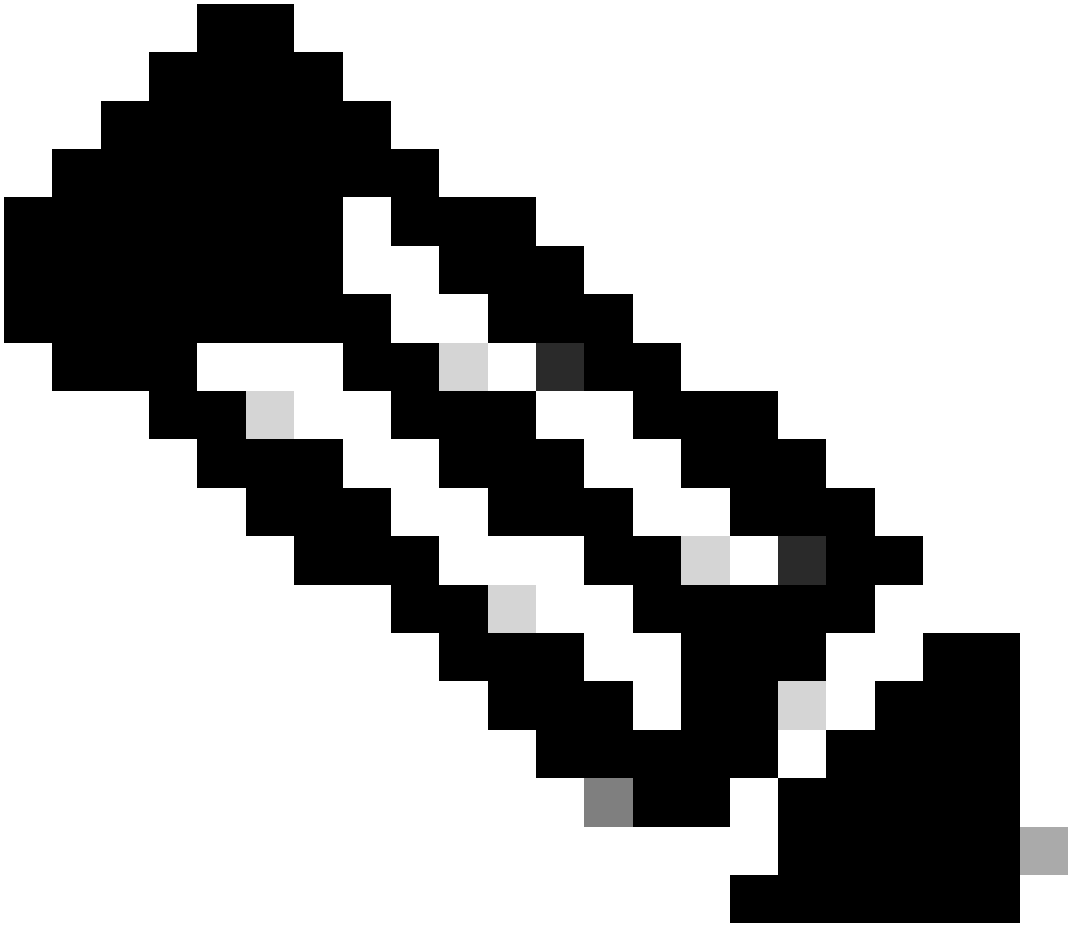
步驟4.在清單中查詢Access Logs，鍵入與其相關的數字並按Enter鍵。

步驟5.鍵入新日誌的名稱。

步驟6.鍵入1為此訂閱的日誌樣式選擇Squid，然後按Enter。

步驟7.不篩選HTTP錯誤狀態代碼。按Enter導航到下一步。

步驟8.選擇FTP輪詢以保留SWA中的日誌。輸入1並按Enter。

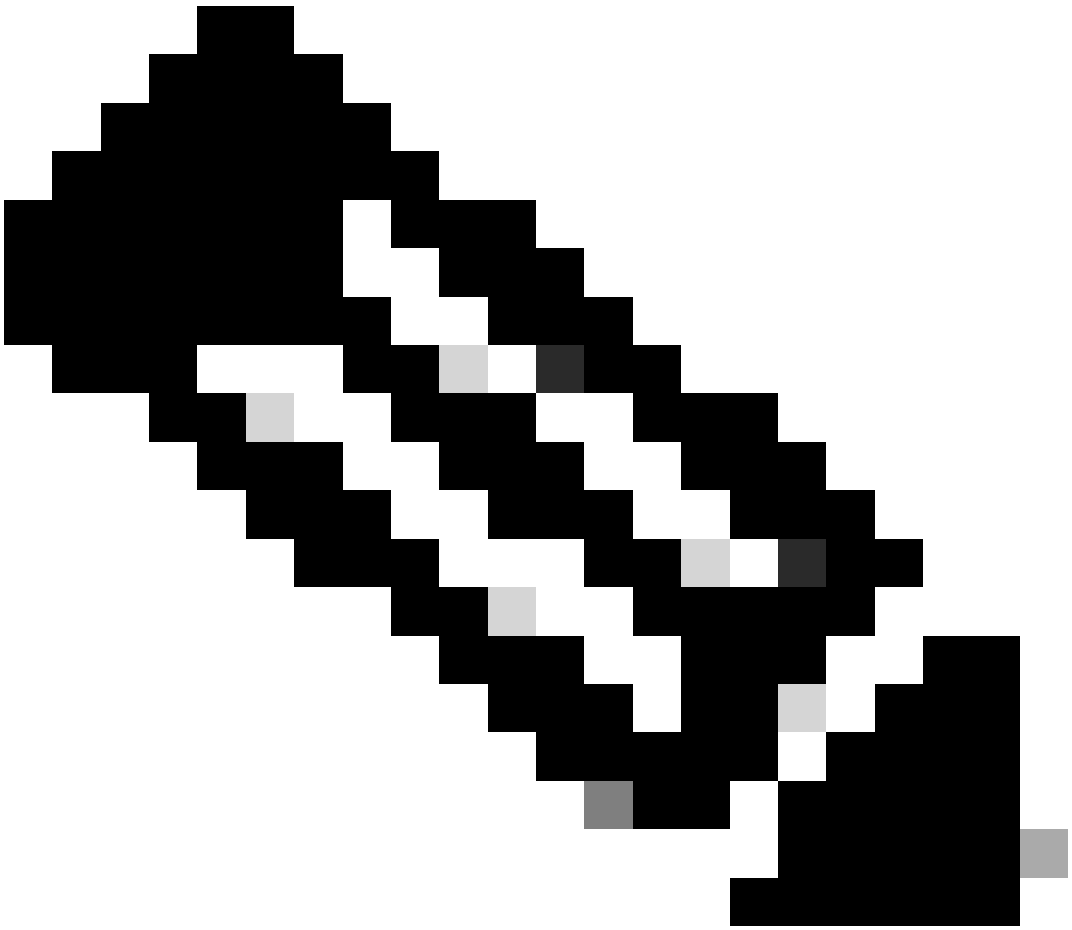


附註：若要將日誌推送到檔案傳輸通訊協定(FTP)伺服器、安全複製通訊協定(SCP)伺服器或系統日誌伺服器。您可以選擇與其相關的選項。

步驟9.此步驟是為新日誌定義資料夾名稱和檔名。最好與日誌名稱相同，然後按Enter鍵。

步驟10.在102400(100 KB)到10737418240(10 GB)之間輸入SWA角色在日誌中轉到新檔案之前的檔

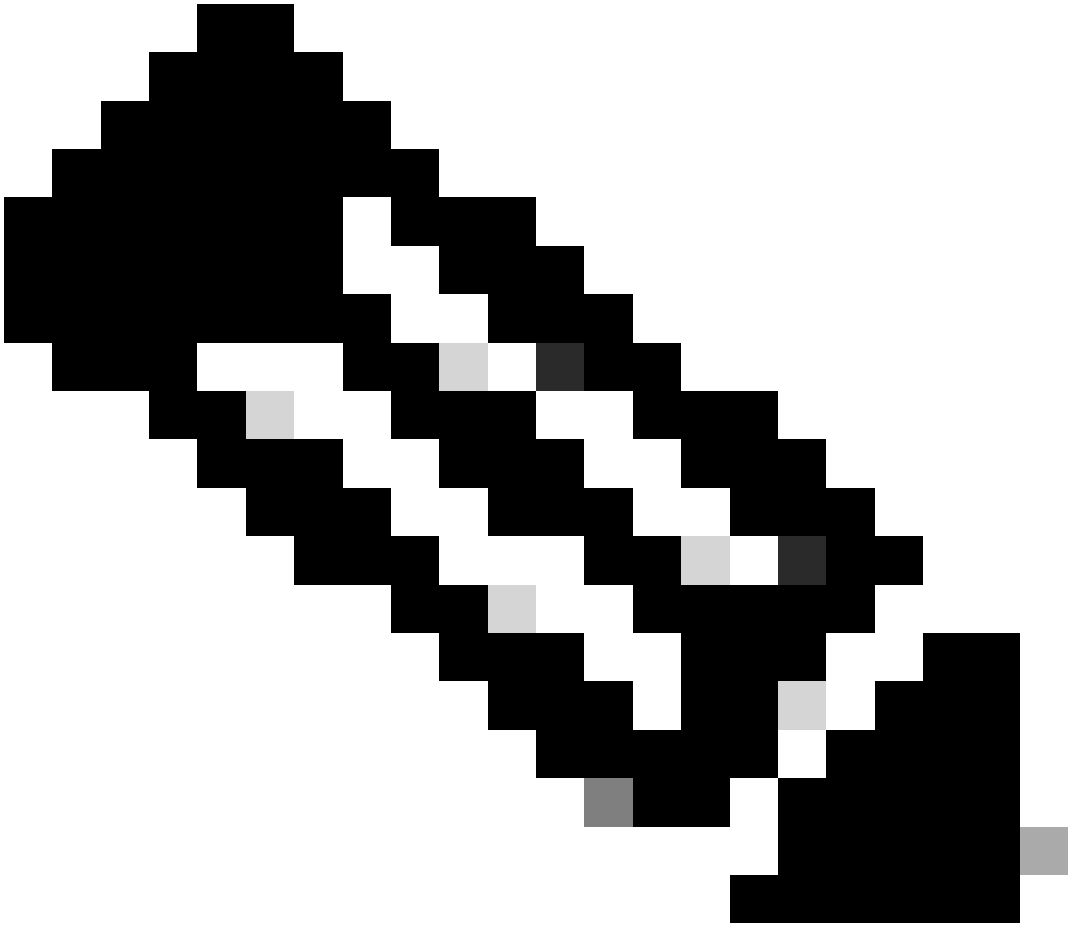
案大小（以位元組為單位）值。



附註：SWA在當前日誌檔案達到使用者指定的最大檔案大小限制（或自上次滾動後的最長時間）時存檔（滾過）日誌訂閱。

步驟11.最大檔案數表示裝置中儲存的日誌檔案數。如果日誌檔案總數達到此值，則會從SWA中刪除較舊的日誌。預設值為10個檔案，由於可用磁碟空間和其他日誌配置，您可以鍵入日誌數，然後按Enter鍵。

步驟12.在此步驟中，您可以選擇壓縮日誌或將其保留為文本檔案。輸入Y表示Yes，輸入N表示No，然後按下Enter。



附註：在檔案大小達到最大檔案大小後，對其進行壓縮。壓縮比取決於網路流量行為，並且可能因日誌檔案而異。

步驟13.按Enter退出日誌配置嚮導。

步驟14.鍵入commit以儲存更改。

```
SWA_CLI> logconfig
...
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.
[]> NEW

Choose the log file type for this subscription:
1. AVC Engine Framework Logs
2. AVC Engine Logs
```

```
3. Access Control Engine Logs
4. Access Logs
....
58. Webroot Logs
59. Welcome Page Acknowledgement Logs
[1]> <=== type the number assosiated with Access Logs and press Enter

Please enter the name for the log:
[]> <=== Chose desiered name, in this example, TAC_access_logs

Choose the log style for this subscription:
1. Squid
2. Apache
3. Squid Details
[1]> <=== Press Enter to keep the default value

Enter the HTTP Error Status codes (comma separated list of 4xx and 5xx codes) you want to filter out fr
[]> <=== Press Enter to keep the default value

Choose the method to retrieve the logs:
1. FTP Poll
2. FTP Push
3. SCP Push
4. Syslog Push
[1]> <=== Choose FTP poll to keep the logs in the SWA

Filename to use for log files:
[aclog]> <=== It is better to have teh same file name as the log, in this example, TAC_access_logs

Do you want to configure time-based log files rollover? [N]> <=== Enter the desiered answer

Please enter the maximum file size:
[104857600]> <=== Enter the desiered answer, or you can leave as default

Please enter the maximum number of files:
[100]> <=== Enter the desiered answer, it depends on free disk space and log file size

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

Do you want to compress logs (yes/no)
[n]> <=== Enter the desiered answer

Currently configured logs:
1. "Splunk Logs" Type: "Access Logs" Retrieval: FTP Push - Host 10.0.0.1
2. "TAC_access_logs" Type: "Access Logs" Retrieval: FTP Poll
3. "accesslogs" Type: "Access Logs" Retrieval: FTP Poll
....
40. "webrootlogs" Type: "Webroot Logs" Retrieval: FTP Poll
41. "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.
[]> <=== Press Enter to exit the log configuration wizard

SWA_CLI> commit
Please enter some comments describing your changes:
[]> <=== Type the change description and press Enter
```

為訪問日誌新增效能引數的自定義欄位

步驟1.登入GUI。

步驟2.從「系統管理」選單中選擇「日誌訂閱」。

步驟3.在「日誌名稱」列中，按一下訪問日誌或新建立的名稱。在本例中，TAC_access_logs。

步驟4.在「自定義欄位」部分，貼上以下字串：

```
[ Request Details: ID = %I, User Agent = %u, AD Group Memberships = ( %m ) %g ] [ Tx Wait Times (in ms)

       , Response Header = %:h>, Client Body = %:b> ] [ Rx Wait Times (in ms): 1st request byte = %:1<,

        a; DNS response = %:

         d, WBRS response = %:

           r, AVC response = %:A>, AVC total = %:A<, DCA response = %:C>, DCA total = %:C<, McAfee respo

            s; AMP response = %:e>, AMP total = %:e<; Latency = %x; %L ] [Client Port = %F, Server IP = %
```

步驟5. Submit和commit變更。

驗證變更

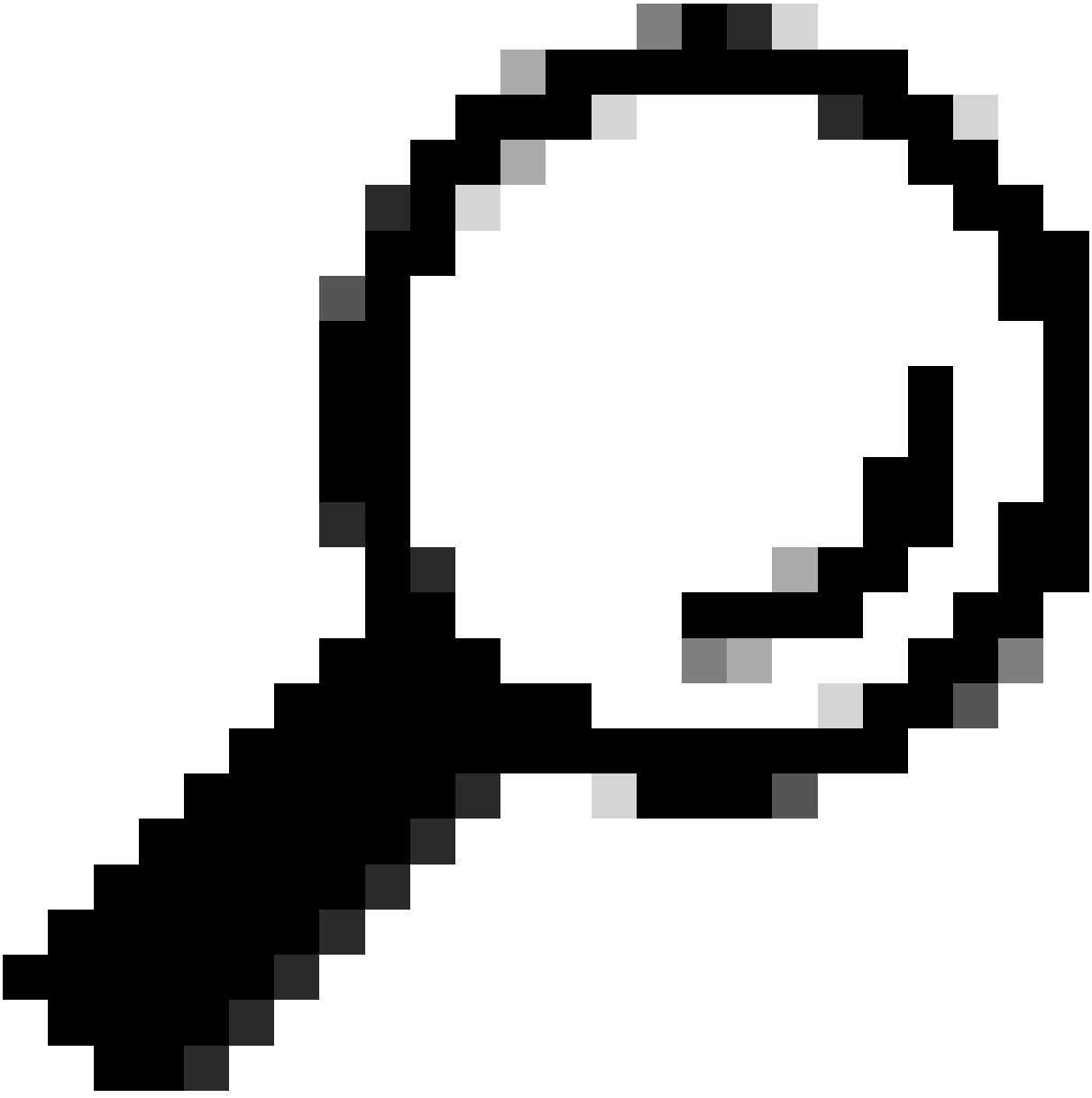
步驟1.登入到CLI。

步驟2.鍵入tail，然後按Enter。

步驟3.查找與新增了效能引數的訪問日誌關聯的編號。輸入編號並按Enter。

您可以看到有額外的資訊新增到訪問日誌，與本示例中的相同。

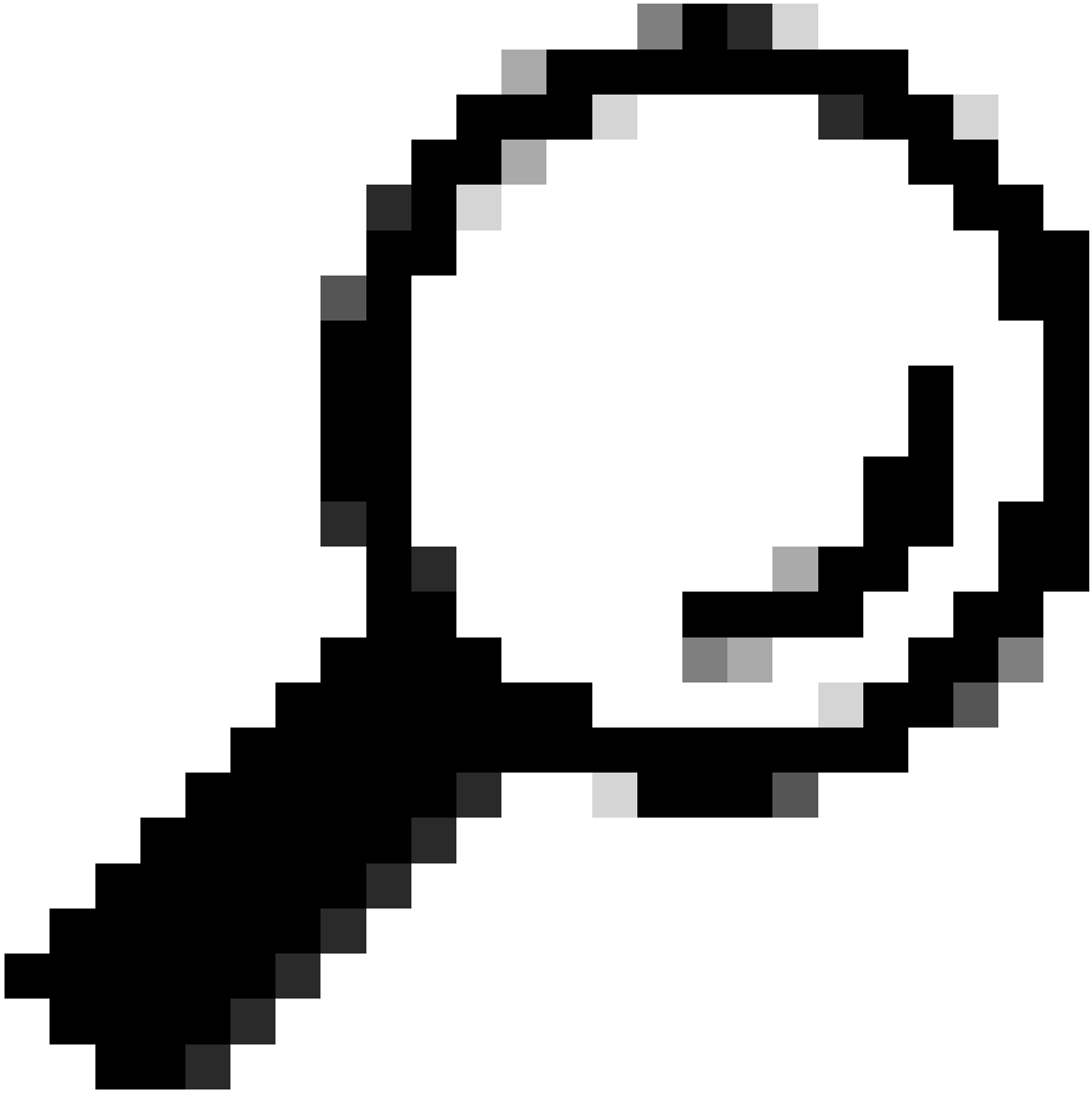
```
1680893872.492 1131 172.18.122.156 TCP_MISS/200 379725 GET http://www.cisco.com/en/US/docs/security/wsa
        - " [ Request Details: ID = 104, User Agent = "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:24.0) Gec
```



提示：按住Control鍵並按C時，可以退出tail命令。如果沒有退出tail命令，請鍵入q。

自定義欄位中的欄位說明

「自定義效能引數」欄位中使用的值將對映到以下資訊：



提示：延遲= AMP總計+反間諜軟體總計+ Webroot總計+ Sophos總計+ McAfee總計+ AVC總計+ WBRS總計+身份驗證總計

自定義欄位名稱	自定義欄位	說明
請求標題	%:<h	在第一個位元組之後將請求報頭寫入伺服器的等待時間。
請求伺服器	%:<b	在標頭之後將請求正文寫入伺服器的等待時間。

第1個位元組到客戶端	%:1>	寫入客戶端的第一個位元組的等待時間。
客戶端正文	%:b>	寫入客戶端的完整正文等待時間。
Rx等待時間（毫秒）：第一個請求位元組	%:1<	從Web代理開始連線到伺服器到它首次能夠寫入伺服器所用的時間。如果Web代理必須連線到多台伺服器才能完成事務，則是這些時間的總和。
請求標題	%:h<	第一個位元組後完成客戶端報頭的等待時間。
客戶端正文	%:b<	等待完整的客戶端正文。
第一個響應位元組	%:>1	伺服器第一個響應位元組的等待時間。
響應報頭	%:>h	第一個響應位元組之後的伺服器報頭的等待時間。
伺服器響應	%:>b	這基本上意味著SWA從伺服器獲取了HTTP報頭，但SWA會等待之後的響應位元組數，以及伺服器中的實際內容。
磁碟快取	%:>c	Web代理從磁碟快取讀取響應所需的時間。
身份驗證響應	%:<a	Web代理傳送請求後，從Web代理身份驗證進程接收響應的等待時間。
身份驗證總計	%:>a	從Web代理身份驗證進程接收響應的等待時間，包括Web代理傳送請求所需的時間。
DNS響應	%:<d	Web代理將域名請求(DNS)請求傳送到Web代理DNS進程所用的時間。
DNS總計	%:>d	Web代理DNS進程將DNS結果傳送回Web代理所用的時間。
WBRS響應	%:<r	Web代理傳送請求後，從Web信譽過濾器接收響應的等待時間。
WBRS總計	%:>r	從Web信譽過濾器接收裁決的等待時間，包括Web代理傳送請求所需的時間。

AVC響應	%:A>	Web代理傳送請求後，從應用可視性與可控性(AVC)進程接收響應的等待時間。
AVC總計	%:A<	從AVC進程接收響應的等待時間，包括Web代理傳送請求所需的時間。
DCA響應	%:C>	Web代理傳送請求後，從動態內容分析引擎接收響應的等待時間。
DCA總計	%:C<	從動態內容分析引擎接收判定結果的等待時間，包括Web代理傳送請求所需的時間。
McAfee響應	%:m>	Web代理傳送請求後，從McAfee掃描引擎接收響應的等待時間。
McAfee總計	%:m<	從McAfee掃描引擎接收判定結果的等待時間，包括Web代理傳送請求所需的時間。
Sophos響應	%:p>	Web代理傳送請求後，從Sophos掃描引擎接收響應的等待時間。
Sophos總計	%:p<	從Sophos掃描引擎接收判定結果的等待時間，包括Web代理傳送請求所需的時間。
AMP響應	%:e>	Web代理傳送請求後，從AMP引擎接收響應的等待時間。
AMP總計	%:e<	從AMP引擎接收判定結果的等待時間，包括Web代理傳送請求所需的時間。
延遲	%x;%L	延遲和請求本地時間（採用人工可讀格式）：DD/MMM/YYYY :hh:mm:ss +nnnn。在訪問日誌中用雙引號編寫此欄位。 此欄位允許您將日誌與問題關聯起來，而無需為每個日誌條目計算從歷代開始的本地時間。
客戶端埠	%F	從客戶端使用的埠號。
伺服器IP地址	%k	Web伺服器IP地址。
伺服器埠號	%p	Web伺服器埠號。

相關資訊

- 思科安全網路裝置AsyncOS 14.5使用手冊 — GD（常規部署） — 思科
- 思科網路安全裝置最佳實踐指南 — 思科

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）。