Configura parametro prestazioni nei log degli accessi

Sommario

Introduzione

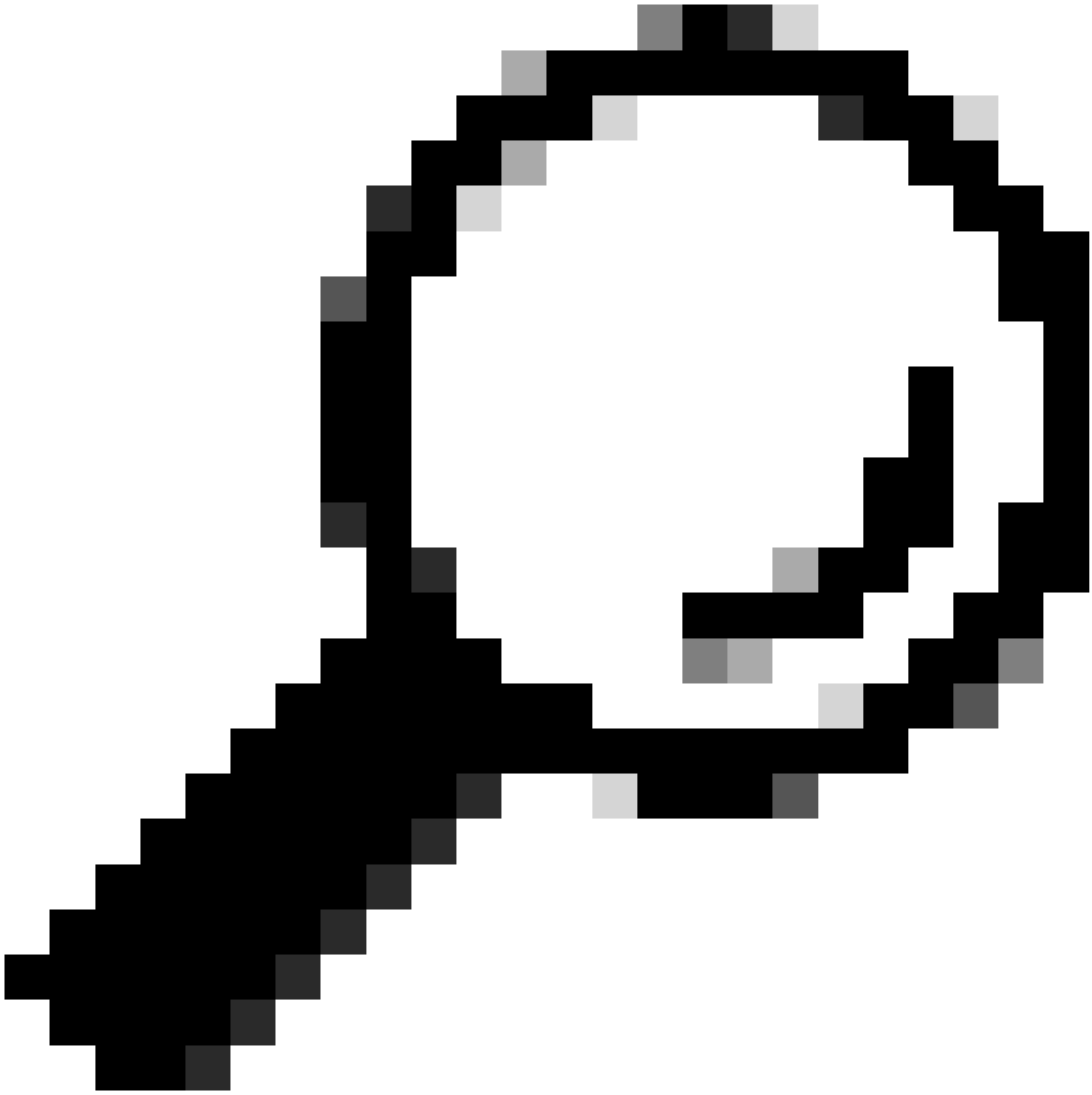
In questo documento viene descritto come aggiungere un campo personalizzato relativo al parametro Performance al registro di accesso di Secure Web Appliance (SWA).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Accesso SSH (Secure Shell Protocol) all'interfaccia di gestione SWA.
- Accesso all'interfaccia grafica dell'utente (GUI) all'interfaccia di gestione SWA.



Suggerimento: È consigliabile disporre di più del 20% di spazio libero su disco nella partizione dati SWA. È possibile controllare l'utilizzo del disco da Command Line Interface (CLI) nell'output del comando status detail.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Quando si verifica un problema di latenza e il traffico viene inoltrato tramite SWA, i log degli accessi possono essere utili per risolvere la causa principale della latenza. È possibile modificare le impostazioni correnti dei log degli accessi o creare nuovi log degli accessi con i parametri delle prestazioni aggiunti al campo personalizzato.

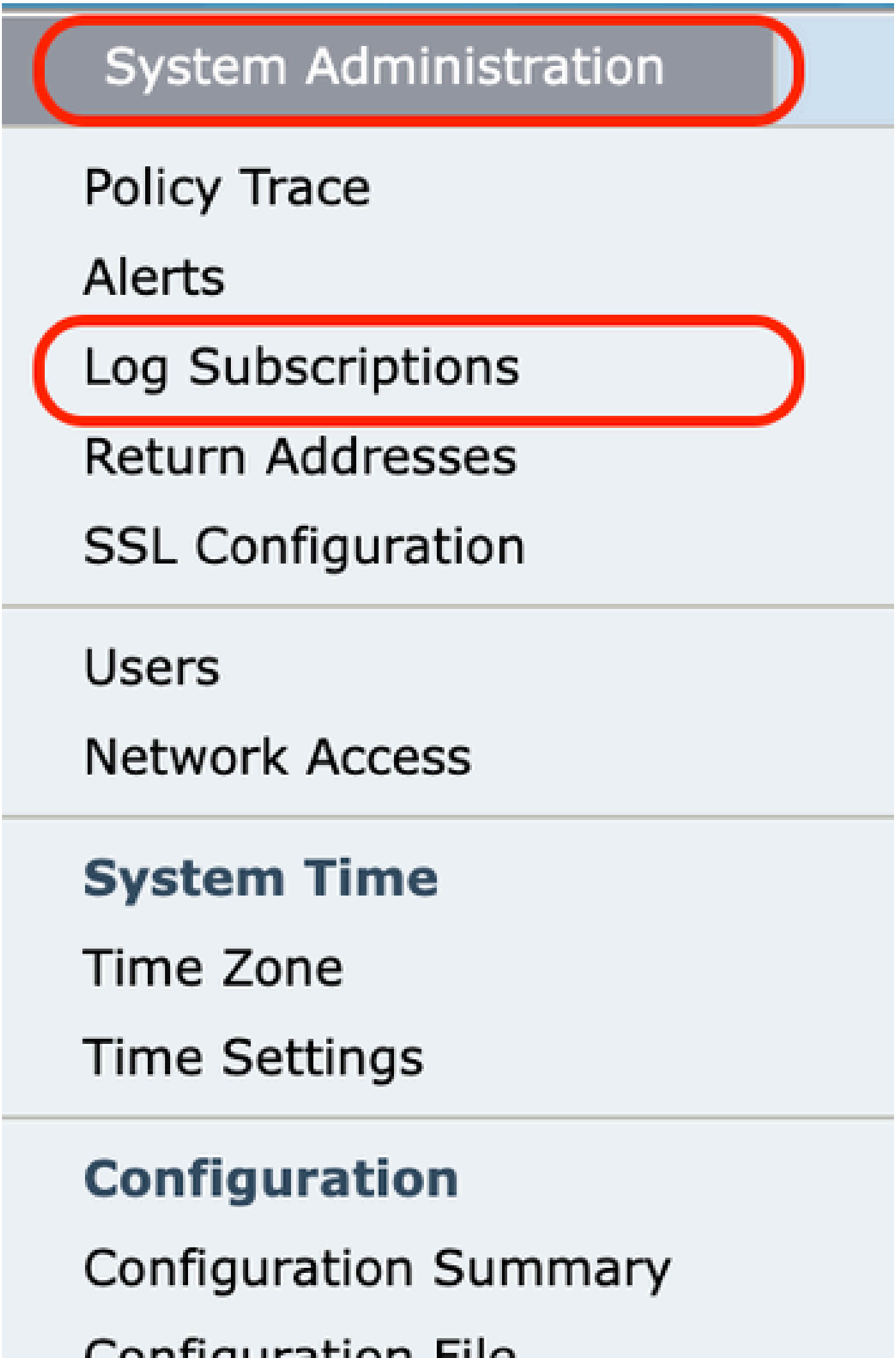
Crea log degli accessi aggiuntivo

In alcune condizioni, a causa di criteri interni o di altre configurazioni, non è possibile modificare il log degli accessi corrente. Per superare questo limite, è possibile creare un altro log degli accessi e aggiungere il parametro Prestazioni personalizzato nei nuovi log degli accessi.

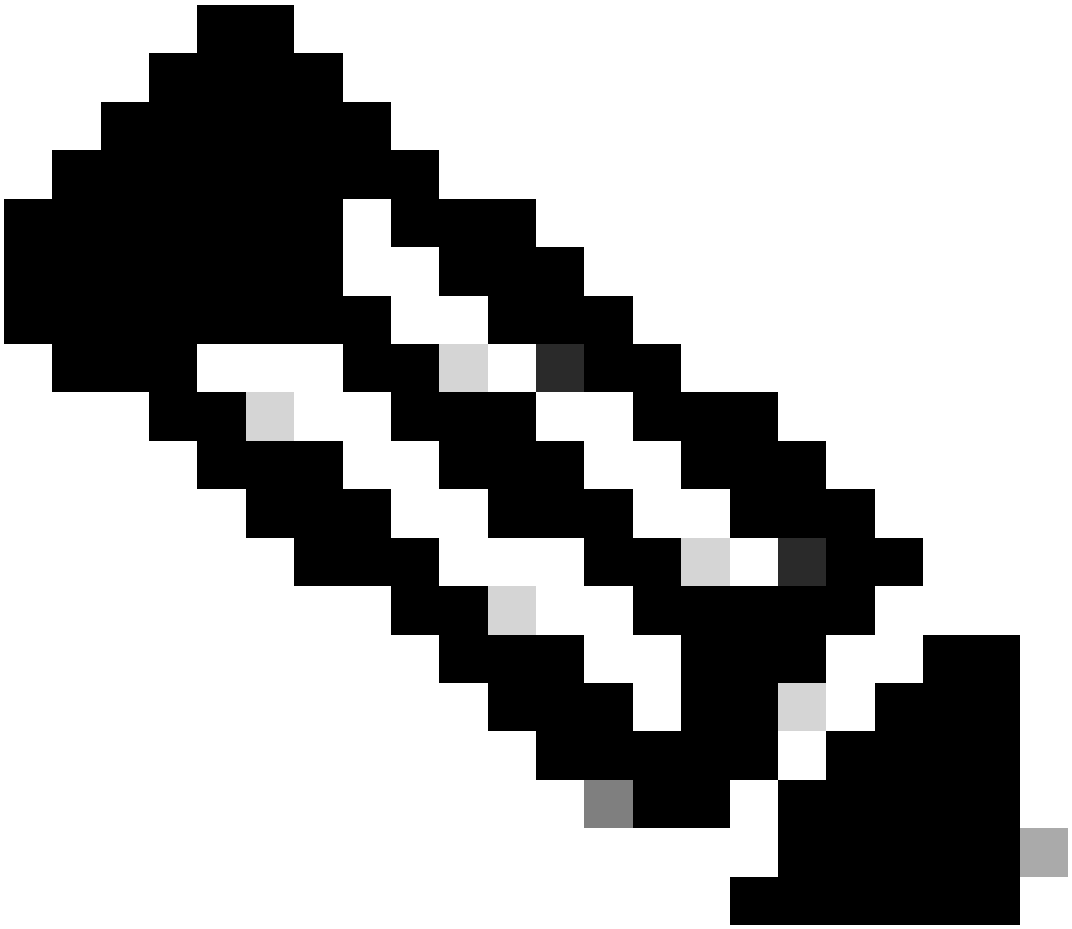
Crea nuovo log degli accessi dalla GUI

Passaggio 1. Accedere alla GUI.

Passaggio 2. Dal menu Amministrazione sistema scegliere Registra sottoscrizioni.


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

Immettere un valore compreso tra 102400 (100 kilobyte) e 10737418240 (10 Gigabyte) per le dimensioni del file (in byte) prima che SWA esegua il rollover del log in un nuovo file. Num deve essere un numero intero ed è possibile aggiungere M per indicare le dimensioni in megabyte, K per indicare le dimensioni del file in kilobyte e G per gigabyte.



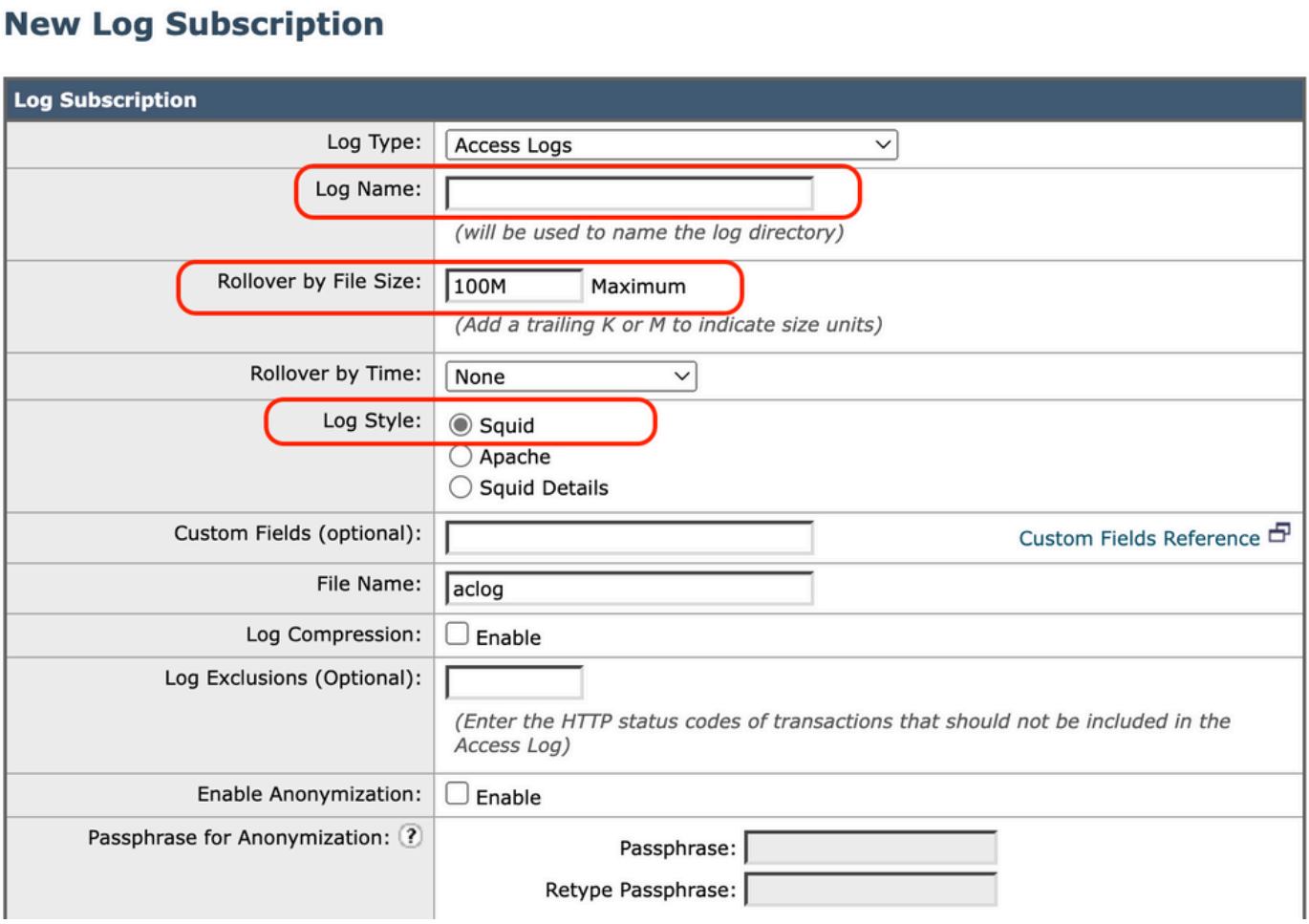
> Nota: Gli archivi SWA (eseguono il rollover) delle sottoscrizioni di log quando un file di log corrente raggiunge un limite specificato dall'utente per le dimensioni massime del file o il tempo massimo dall'ultimo rollover.

Passaggio 7. Scegliere Squid per lo stile del log.

Passaggio 8. Nome file consente di definire il nome della cartella e il nome del file di registro per il nuovo registro. Si consiglia di utilizzare lo stesso nome del registro, che nell'esempio riportato è TAC_access_logs.

Passaggio 9. È possibile abilitare la compressione del log per comprimere il file di log o mantenere i log come file di testo.

Passaggio 10. L'esclusione dal log consente di filtrare il codice di risposta HTTP (Hypertext Transfer Protocol). Non filtrare i codici di stato HTTP.



Compilare i campi obbligatori

Passaggio 11. Scegliere Polling FTP per conservare i log nell'SWA. Digitare 1 e premere Invio.

Passaggio 12. Sottomettere e confermare le modifiche.

Configurazione del nuovo log degli accessi dalla CLI

Passaggio 1. Accedere alla CLI.

Passaggio 2. Eseguire logconfig.

Passaggio 3. Per creare un nuovo registro, digitare New e premere Invio.

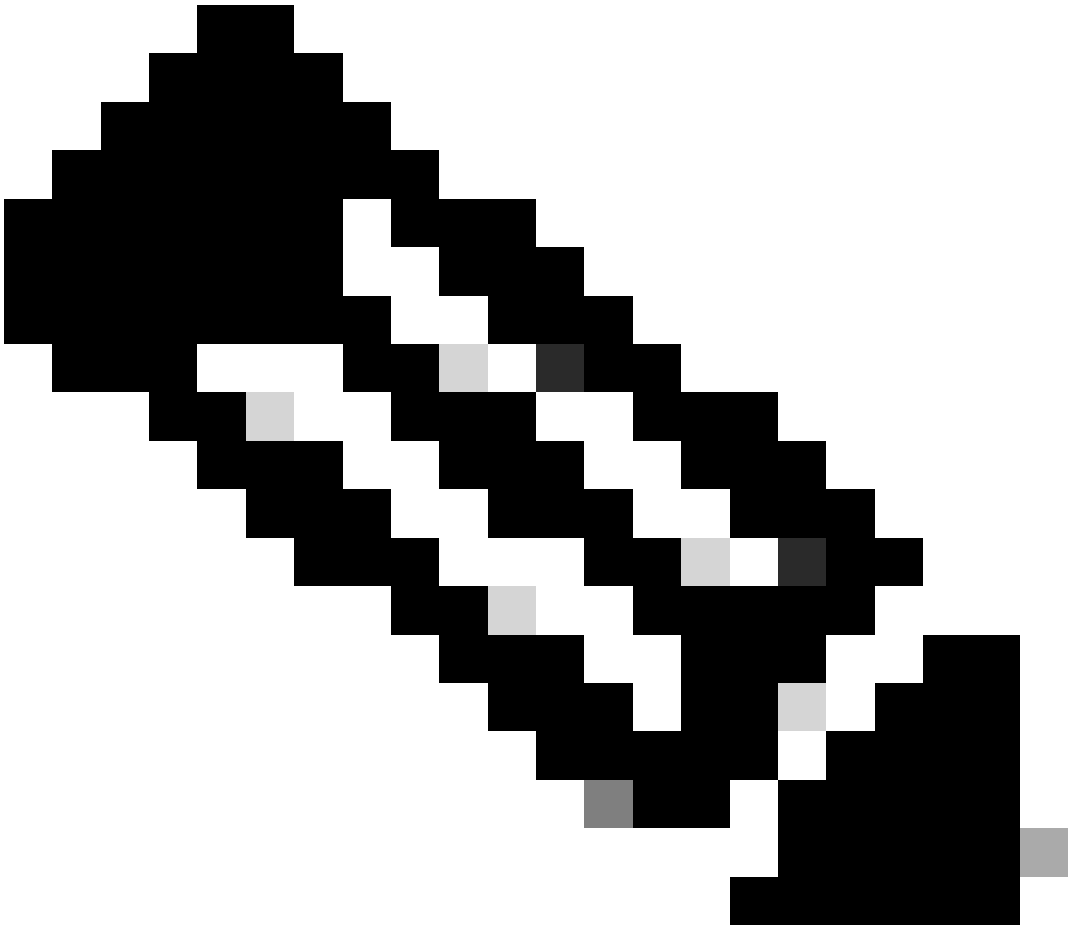
Passaggio 4. Individuare i log degli accessi nell'elenco, digitare il numero associato a tale log e premere Invio.

Passaggio 5. Digitare un nome per il nuovo registro.

Passaggio 6. Digitare 1 per scegliere Squid per lo stile del log per questa sottoscrizione e premere Invio.

Passaggio 7. Non filtrare i codici di stato dell'errore HTTP. Premere Invio per passare al passaggio successivo.

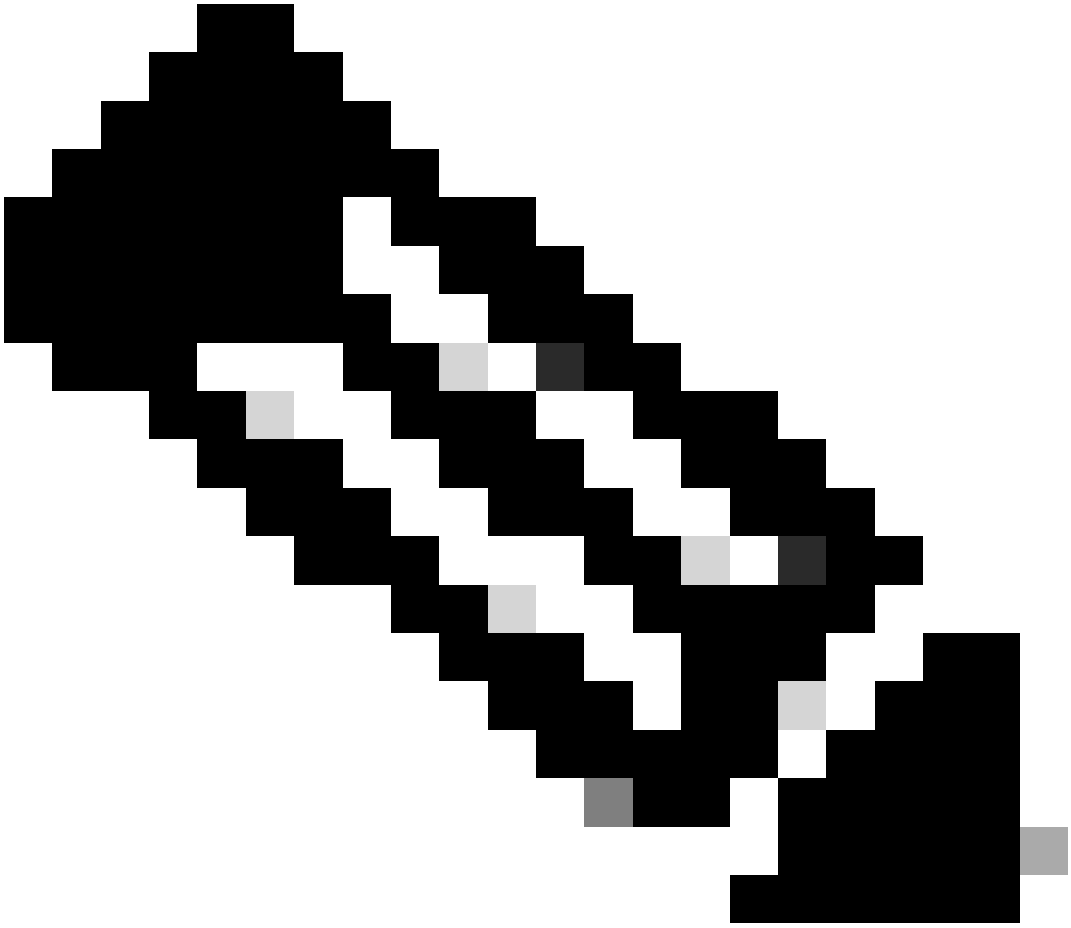
Passaggio 8. Scegliere Polling FTP per conservare i log nell'SWA. Digitare 1 e premere Invio.



> Nota: Per eseguire il push dei registri nel server FTP (File Transfer Protocol), SCP (Secure Copy Protocol) o Syslog. È possibile scegliere le opzioni correlate.

Passaggio 9. In questo passaggio vengono definiti il nome della cartella e il nome del file per il nuovo registro. È preferibile che il nome del registro sia uguale a quello del registro e premere Invio.

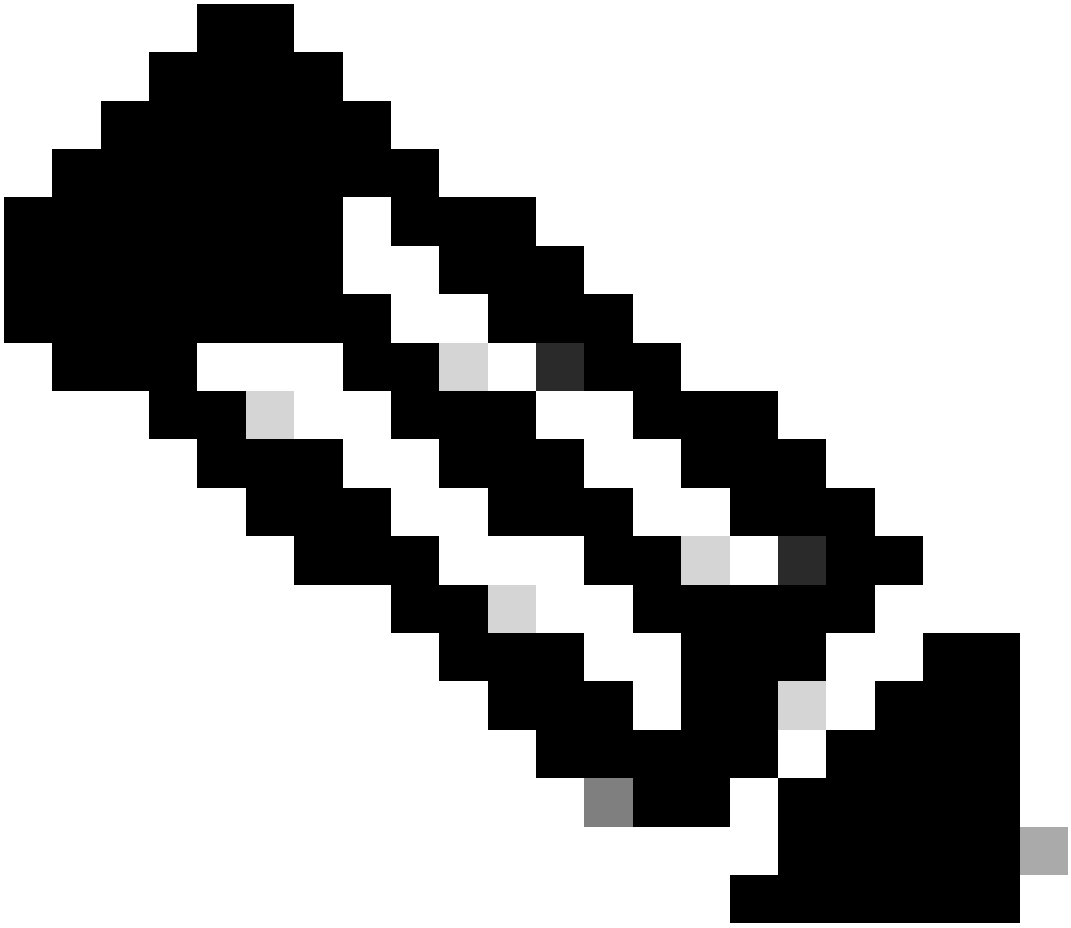
Passaggio 10. Immettere un valore compreso tra 102400 (100 kilobyte) e 10737418240 (10 Gigabyte) per le dimensioni del file (in byte) prima del ruolo SWA sul log in un nuovo file.



Nota: Gli archivi SWA (eseguono il rollover) delle sottoscrizioni di log quando un file di log corrente raggiunge un limite specificato dall'utente per le dimensioni massime del file o il tempo massimo dall'ultimo rollover.

Passaggio 11. Il numero massimo di file indica il numero di file di registro archiviati nel dispositivo. Se il numero totale di file di log ha raggiunto questo valore, i log meno recenti vengono eliminati da SWA. Il valore predefinito è 10 file ed è possibile digitare il numero di log, a causa dello spazio su disco disponibile e di altre configurazioni di log, quindi premere Invio.

Passaggio 12. In questo passaggio è possibile scegliere di comprimere i log o di mantenerli come file di testo. Digitare Y per Sì e N per No e premere Invio.



Nota: Una volta raggiunta la dimensione massima del file, il file viene compresso. Il rapporto di compressione dipende dal comportamento del traffico di rete e può variare tra i file di registro.

Passaggio 13. Premere Invio per uscire dalla configurazione guidata del registro.

Passaggio 14. Digitare commit per salvare le modifiche.

```
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
```

Aggiungi campi personalizzati per il parametro Performance ai registri di accesso

Passaggio 1. Accedere alla GUI.

Passaggio 2. Dal menu Amministrazione di sistema, scegliere Registra sottoscrizioni.

Passaggio 3. Dalla colonna Nome log, fare clic su accesslogs o sul nome del nuovo log creato. Nell'esempio, TAC_access_logs.

Passaggio 4. Nella sezione Custom Fields, incollare la seguente stringa:

```
[ 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 = %
```

Passaggio 5. Sottomettere e confermare le modifiche.

Verifica delle modifiche

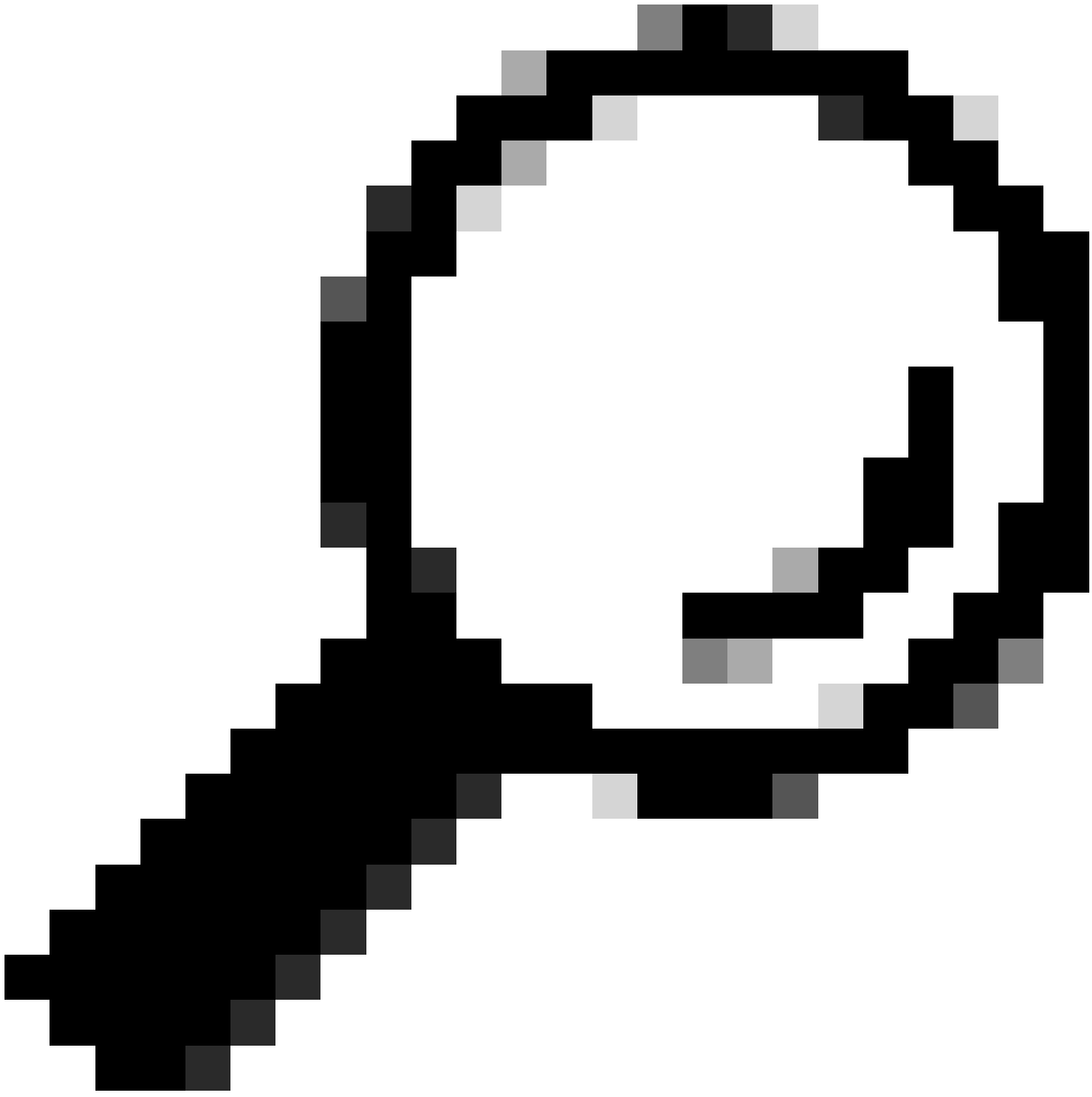
Passaggio 1. Accedere alla CLI.

Passaggio 2. Digitare tail e premere Invio.

Passaggio 3. Individuare il numero associato ai log degli accessi che hanno aggiunto il parametro Performance. Digitare il numero e premere Invio.

Come in questo esempio, ai log degli accessi sono state aggiunte ulteriori informazioni.

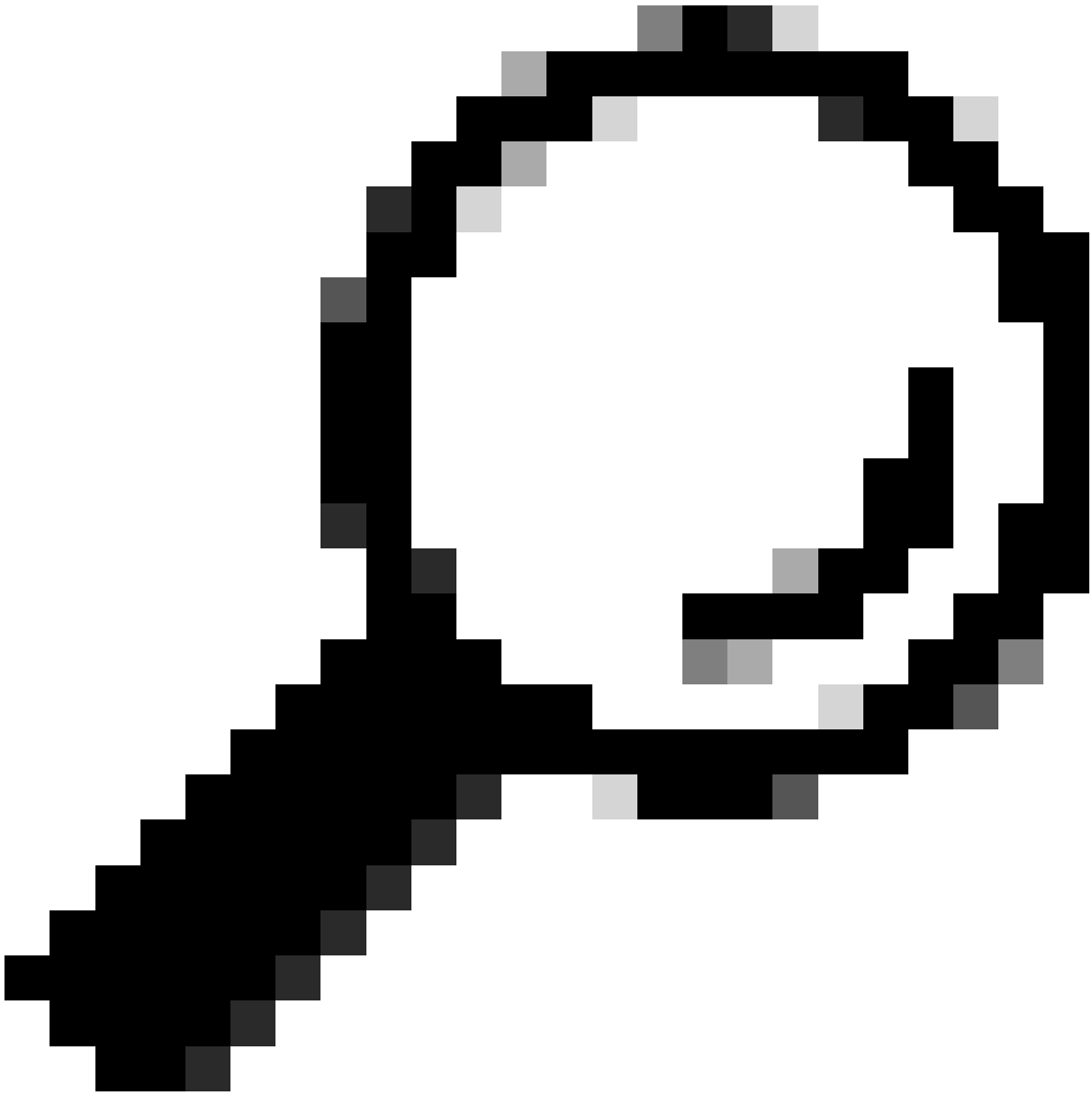
```
1680893872.492 1131 172.18.122.156 TCP_MISS/200 379725 GET http://www.cisco.com/en/US/docs/security/wsa/

        - " [ Request Details: ID = 104, User Agent = "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:24.0) Gec
```



Suggerimento: Per uscire dal comando tail, tenere premuto il tasto Ctrl e premere C. Se il comando tail non è stato chiuso, digitare q.

Descrizione campi nei campi personalizzati

I valori utilizzati nel campo Parametro prestazioni personalizzato corrispondono alle seguenti informazioni:



Suggerimento: Latenza = totale AMP + totale antispyware + totale Webroot + totale Sophos + totale McAfee + totale AVC + totale WBRS + totale Auth

Nome campo personalizzato	Campo personalizzato	Descrizione

Intestazione richiesta	%:<h	Tempo di attesa per la scrittura dell'intestazione della richiesta sul server dopo il primo byte.
Richiesta al server	%:<b	Tempo di attesa per la scrittura del corpo della richiesta nel server dopo l'intestazione.
1° byte per il client	%:1>	Tempo di attesa per il primo byte scritto sul client.
Corpo client	%:b>	Tempo di attesa per la scrittura del corpo completo sul client.
Tempi di attesa Rx (in ms): Primo byte di richiesta	%:1<	Il tempo necessario dal momento in cui il proxy Web inizia a connettersi al server al momento in cui è in grado di scrivere sul server per la prima volta. Se il proxy Web deve connettersi a più server per completare la transazione, corrisponde alla somma di tali orari.
Intestazione richiesta	%:h<	Tempo di attesa per l'intestazione client completa dopo il primo byte.
Corpo client	%:b<	Tempo di attesa per il corpo completo del client.
Primo byte di risposta	%:>1	Tempo di attesa per il primo byte di risposta dal server.
Intestazione risposta	%:>h	Tempo di attesa per l'intestazione del server dopo il primo byte di risposta.
Risposta del server	%:>b	Questo significa in pratica che SWA ha ottenuto intestazioni HTTP dal server, ma SWA attende i byte di risposta dopo di ciò e quale sarebbe il contenuto effettivo dal server.
Cache disco	%:>c	Tempo necessario al proxy Web per leggere una risposta dalla cache del disco.
Risposta di autenticazione	%:<a	Tempo di attesa per la ricezione della risposta dal processo di autenticazione del proxy Web, dopo l'invio della richiesta da parte del proxy Web.

Totale autenticazione	%:>a	Tempo di attesa per la ricezione della risposta dal processo di autenticazione del proxy Web. Include il tempo necessario al proxy Web per inviare la richiesta.
risposta DNS	%:<d	Tempo impiegato dal proxy Web per inviare la richiesta DNS (Domain Name Request) al processo DNS del proxy Web.
Totale DNS	%:>d	Tempo impiegato dal processo DNS del proxy Web per restituire un risultato DNS al proxy Web.
risposta WBRS	%:<r	Tempo di attesa per ricevere la risposta dai filtri Web Reputation, dopo l'invio della richiesta da parte del proxy Web.
Totale WBRS	%:>r	Tempo di attesa per la ricezione del verdetto dai filtri Web Reputation. Include il tempo necessario al proxy Web per inviare la richiesta.
Risposta AVC	%:A>	Tempo di attesa per ricevere la risposta dal processo di visibilità e controllo dell'applicazione (AVC), dopo l'invio della richiesta da parte del proxy Web.
Totale AVC	%:A<	Tempo di attesa per la ricezione della risposta dal processo AVC, incluso il tempo necessario al proxy Web per inviare la richiesta.
Risposta DCA	%:C>	Tempo di attesa per la ricezione della risposta dal motore di analisi del contenuto dinamico dopo l'invio della richiesta da parte del proxy Web.
Totale DCA	%:C<	Tempo di attesa per la ricezione del verdetto dal motore di analisi del contenuto dinamico, incluso il tempo necessario al proxy Web per inviare la richiesta.
Risposta di McAfee	%:m>	Tempo di attesa per ricevere la risposta dal motore di scansione McAfee, dopo che il proxy Web ha inviato la richiesta.
Totale McAfee	%:m<	Tempo di attesa per ricevere il verdetto dal motore di

		scansione McAfee, incluso il tempo necessario al proxy Web per inviare la richiesta.
Risposta di Sophos	%:p>	Tempo di attesa per ricevere la risposta dal motore di scansione Sophos, dopo l'invio della richiesta da parte del proxy Web.
Sophos totale	%:p<	Tempo di attesa per ricevere il verdetto dal motore di scansione Sophos, incluso il tempo necessario al proxy Web per inviare la richiesta.
risposta AMP	%:e>	Tempo di attesa per ricevere la risposta dal motore AMP dopo l'invio della richiesta da parte del proxy Web.
AMP totale	%:e<	Tempo di attesa per ricevere il verdetto dal motore AMP, incluso il tempo necessario al proxy Web per inviare la richiesta.
Latenza	%x %L	Latenza e ora locale richiesta in formato leggibile: GG/MMM/AAAA : hh:mm:ss +nnnn. Questo campo viene scritto tra virgolette nei log degli accessi. Questo campo consente di correlare i registri ai problemi senza dover calcolare l'ora locale da un momento all'altro per ciascuna voce di registro.
Porta client	%F	Numero di porta utilizzato dal lato client.
Indirizzo IP del server	%k	Indirizzo IP del server Web.
Numero porta server	%p	Numero porta server Web.

Informazioni correlate

- Guida per l'utente di AsyncOS 14.5 per Cisco Secure Web Appliance - GD (General Deployment) - Cisco
- Linee guida sulle best practice di Cisco Web Security Appliance - Cisco

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).