Konfigurieren von Leistungsparametern in Zugriffsprotokollen

Inhalt

Einleitung

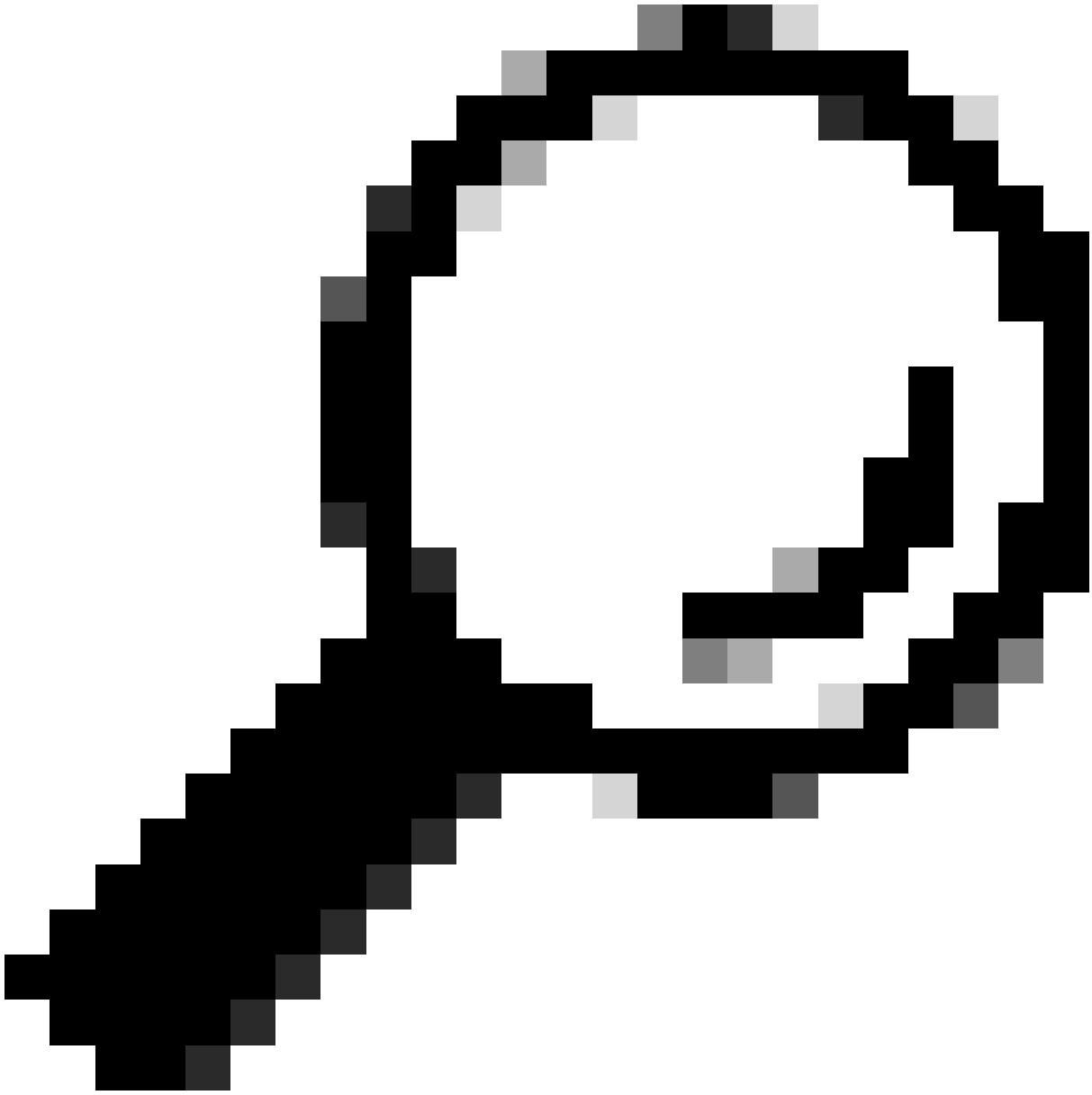
In diesem Dokument werden die Schritte beschrieben, um dem Zugriffsprotokoll der Secure Web Appliance (SWA) ein benutzerdefiniertes Feld für Leistungsparameter hinzuzufügen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- SSH-Zugriff (Secure Shell Protocol) auf die SWA-Verwaltungsschnittstelle
- Grafische Benutzeroberfläche (GUI) für den Zugriff auf die SWA-Verwaltungsoberfläche



Tipp: Es ist am besten, mehr als 20 % freien Speicherplatz auf der SWA-Datenpartition zu haben. Sie können die Datenträgerverwendung über die Befehlszeilenschnittstelle (CLI) in der Ausgabe des Befehls status detail überprüfen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Wenn ein Latenzproblem vorliegt und der Datenverkehr über ein SWA geleitet wird, können die Zugriffsprotokolle nützlich sein, um die Ursache der Latenz zu beheben. Sie können die aktuellen Einstellungen für Zugriffsprotokolle ändern oder neue Zugriffsprotokolle mit Leistungsparametern erstellen, die dem benutzerdefinierten Feld hinzugefügt wurden.

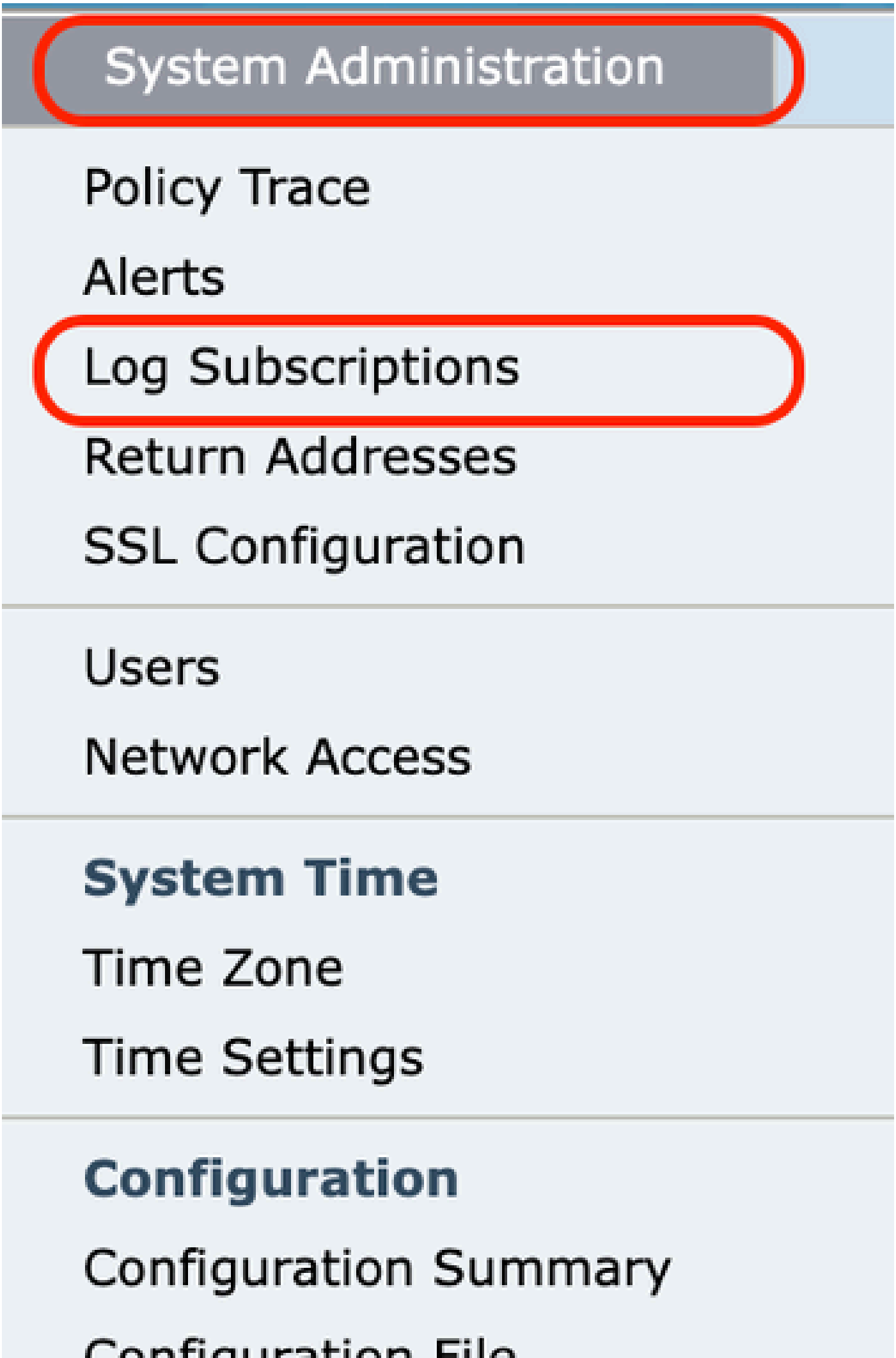
Erstellen eines zusätzlichen Zugriffsprotokolls

Unter bestimmten Umständen ist aufgrund interner Richtlinien oder einer anderen Konfiguration keine Änderung des aktuellen Zugriffsprotokolls möglich. Um diese Einschränkung zu umgehen, können Sie weitere Zugriffsprotokolle erstellen und den benutzerdefinierten Leistungsparameter in die neuen Zugriffsprotokolle einfügen.

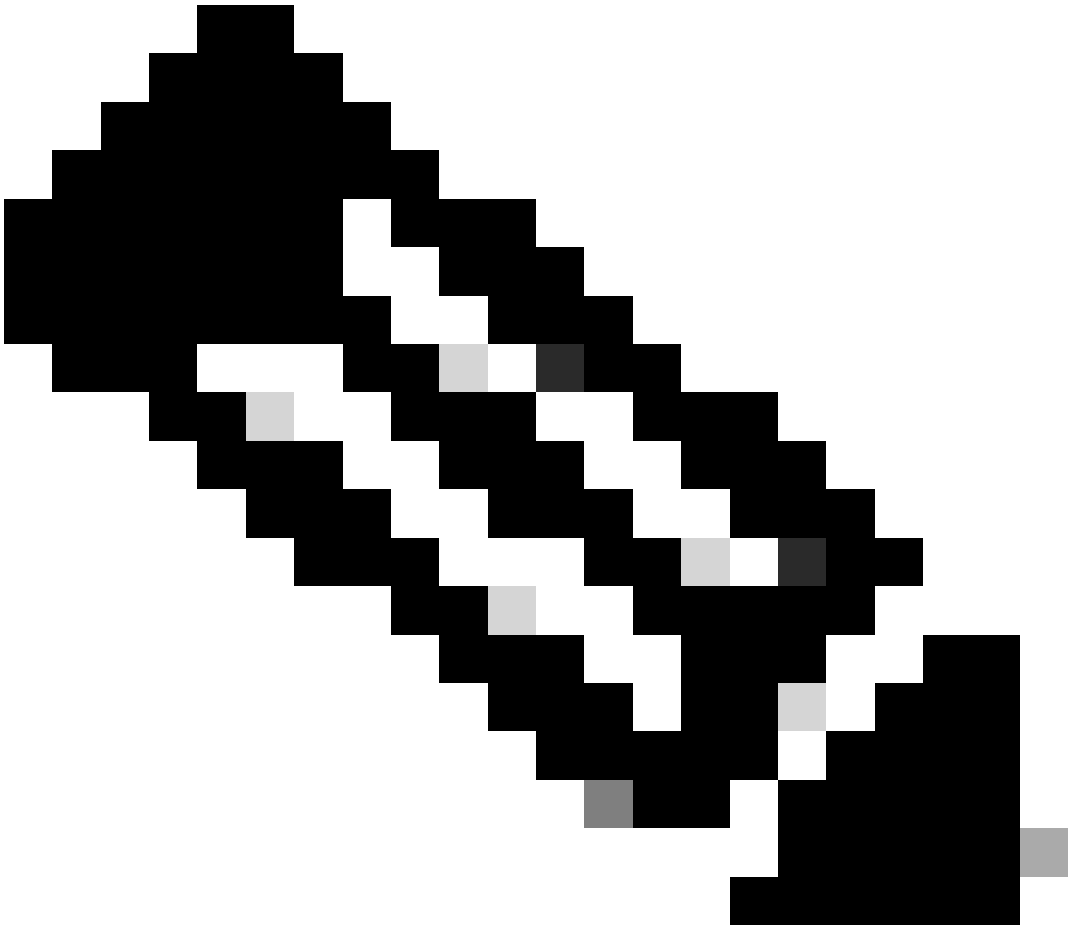
Neues Zugriffsprotokoll über die GUI erstellen

Schritt 1: Melden Sie sich bei der GUI an.

Schritt 2. Wählen Sie im Menü Systemverwaltung Protokollabonnements aus.


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

Geben Sie einen Wert zwischen 102400 (100 Kilobyte) und 10737418240 (10 Gigabyte) für die Dateigröße (in Byte) ein, bevor SWA-Rollen das Protokoll in eine neue Datei übernehmen. Die Zahl muss eine ganze Zahl sein, und Sie können M hinzufügen, um die Größe in Megabyte anzugeben, K, um die Dateigröße in Kilobyte anzugeben, und G für Gigabyte.



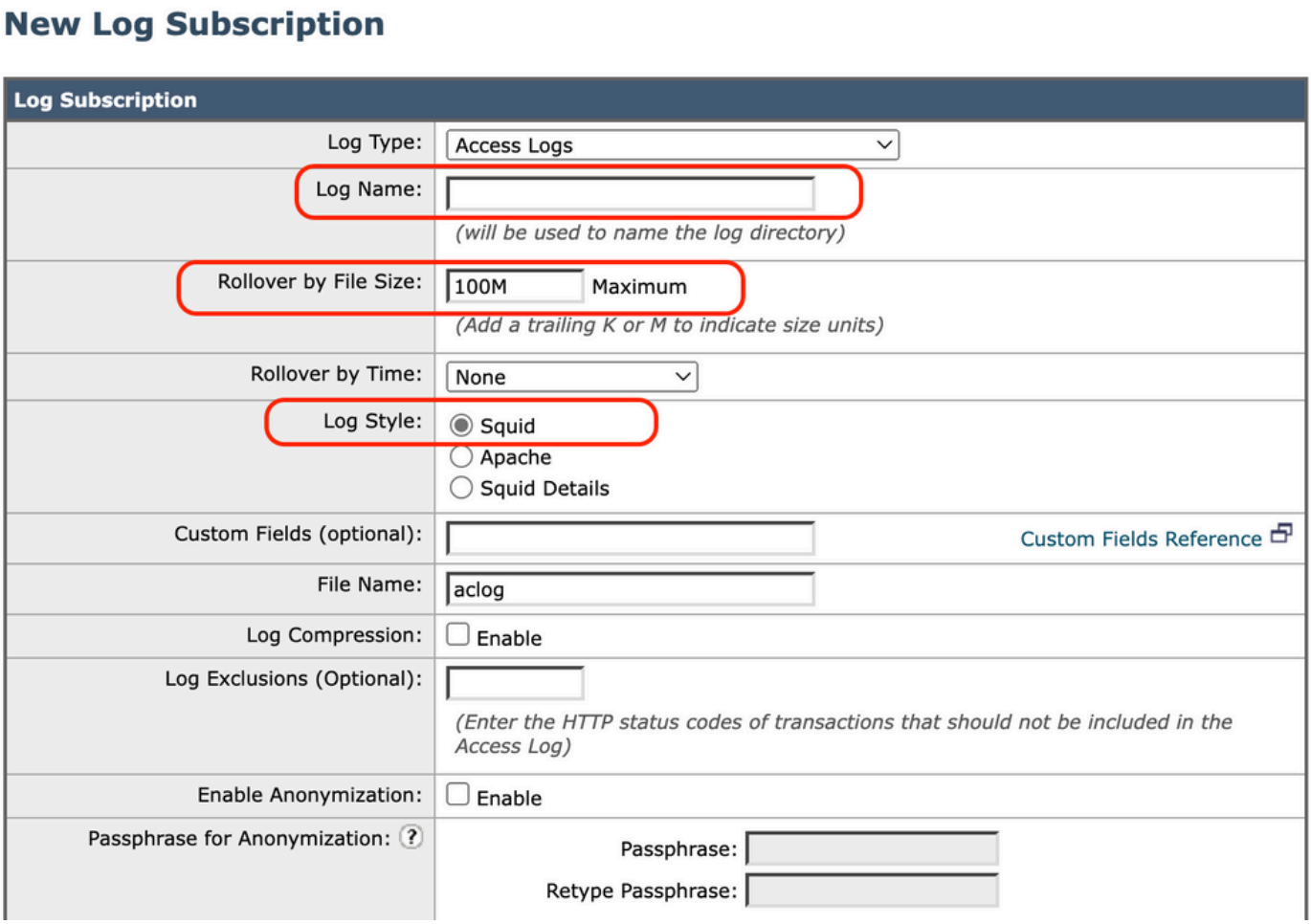
> Anmerkung: SWA archiviert (rollt über) Protokoll-Subscriptions, wenn eine aktuelle Protokolldatei eine vom Benutzer festgelegte Obergrenze für die maximale Dateigröße oder die maximale Zeit seit dem letzten Rollover erreicht.

Schritt 7. Wählen Sie Squid für Protokollstil.

Schritt 8: Der Dateiname definiert den Ordnernamen und den Protokolldateinamen für dieses neue Protokoll. Es wird empfohlen, mit dem Protokollnamen identisch zu sein, in diesem Beispiel TAC_access_logs.

Schritt 9: Sie können die Protokollkomprimierung aktivieren, um die Protokolldatei zu komprimieren, oder die Protokolle als Textdatei speichern.

Schritt 10. Der Protokollausschluss dient zum Filtern des HTTP-Antwortcodes (Hypertext Transfer Protocol). HTTP-Statuscodes nicht filtern.



Pflichtfelder ausfüllen

Schritt 11: Wählen Sie "FTP poll" aus, um die Protokolle im SWA zu speichern. Geben Sie 1 ein, und drücken Sie die Eingabetaste.

Schritt 12: Änderungen übermitteln und bestätigen.

Konfigurieren eines neuen Zugriffsprotokolls über die CLI

Schritt 1. Melden Sie sich bei CLI an.

Schritt 2: Führen Sie logconfig aus.

Schritt 3: Um ein neues Protokoll zu erstellen, geben Sie Neu ein, und drücken Sie die Eingabetaste.

Schritt 4: Suchen Sie in der Liste nach Zugriffsprotokollen, geben Sie die zugehörige Nummer ein, und drücken Sie die Eingabetaste.

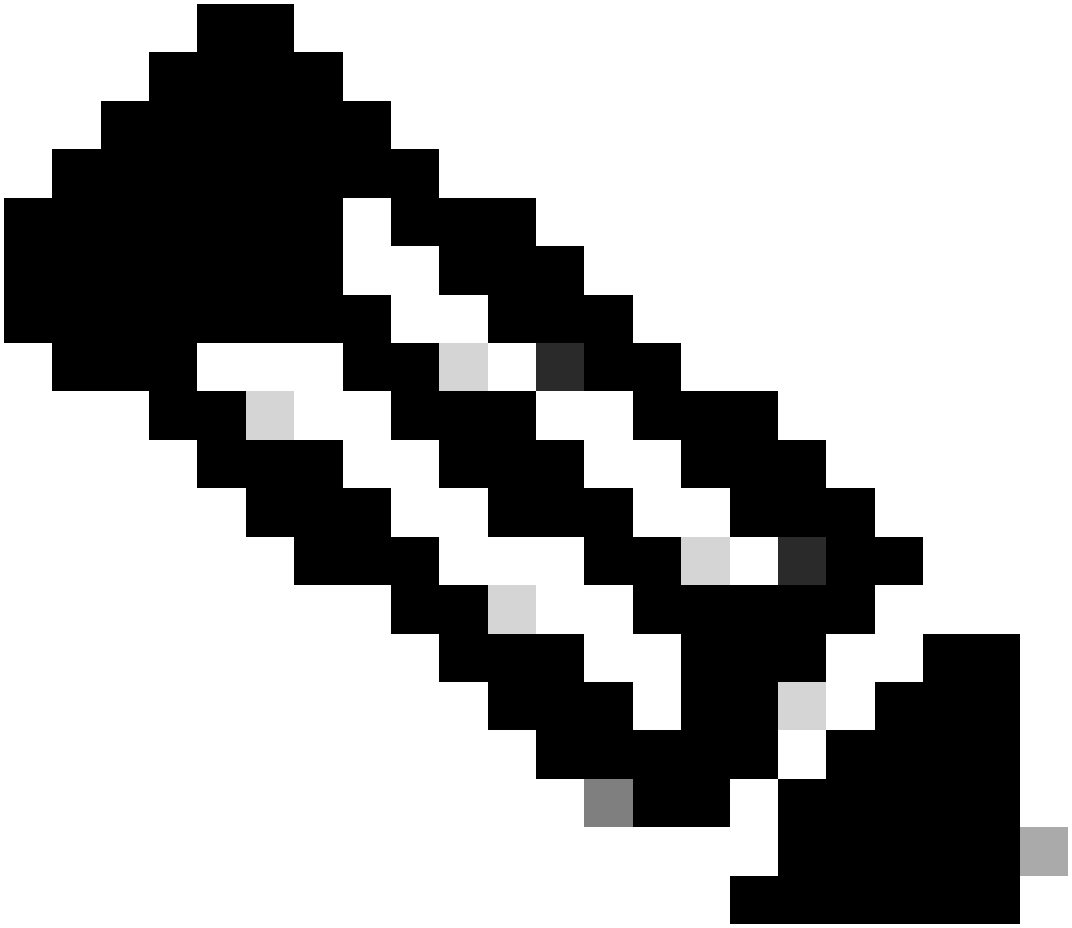
Schritt 5. Geben Sie einen Namen für das neue Protokoll ein.

Schritt 6. Geben Sie 1 ein, um Squid als Protokollstil für dieses Abonnement auszuwählen, und

drücken Sie die Eingabetaste.

Schritt 7. HTTP-Fehlerstatuscodes nicht filtern. Drücken Sie die Eingabetaste, um zum nächsten Schritt zu navigieren.

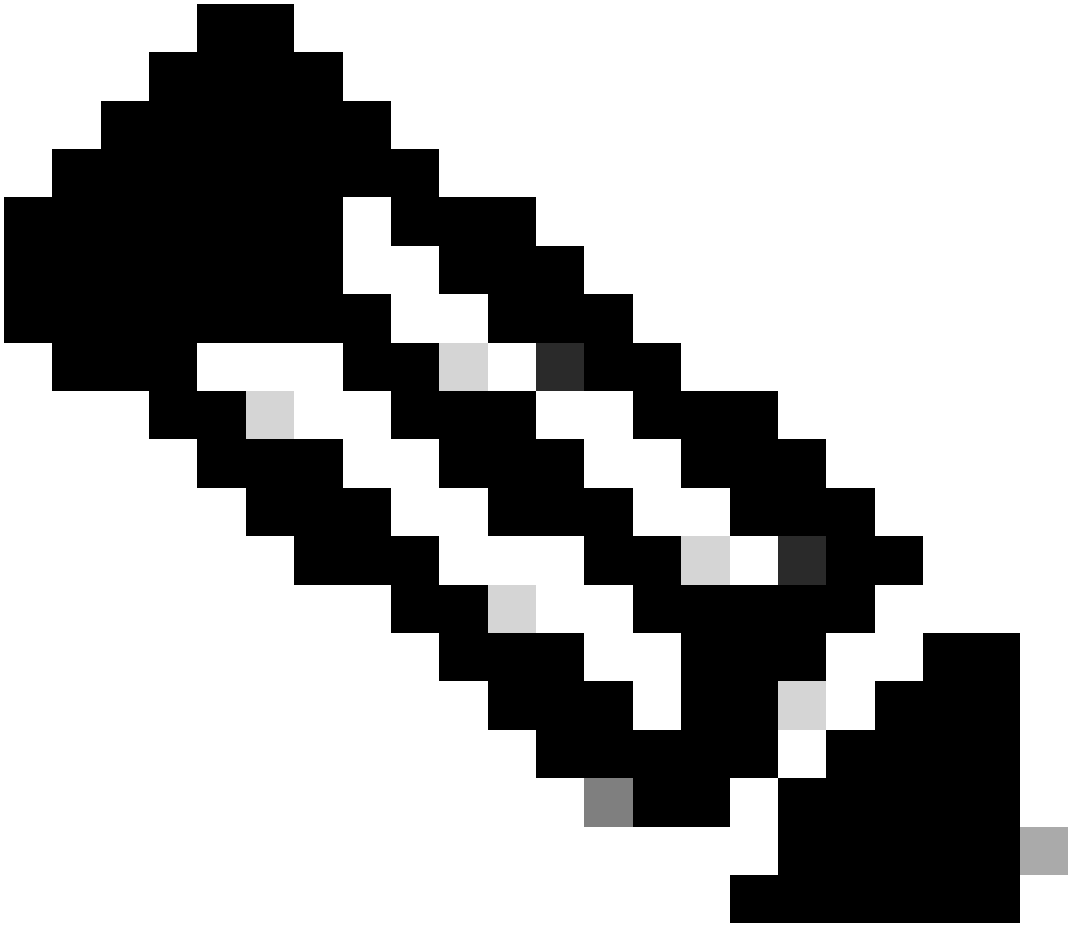
Schritt 8: Wählen Sie "FTP poll", um die Protokolle im SWA zu speichern. Geben Sie 1 ein, und drücken Sie die Eingabetaste.



> Anmerkung: Um die Protokolle per Push an einen FTP-Server (File Transfer Protocol), SCP-Server (Secure Copy Protocol) oder Syslog-Server zu übertragen. Sie können die entsprechenden Optionen auswählen.

Schritt 9. In diesem Schritt werden der Ordner- und Dateiname für das neue Protokoll definiert. Es ist besser, den gleichen Protokollnamen zu verwenden und die Eingabetaste zu drücken.

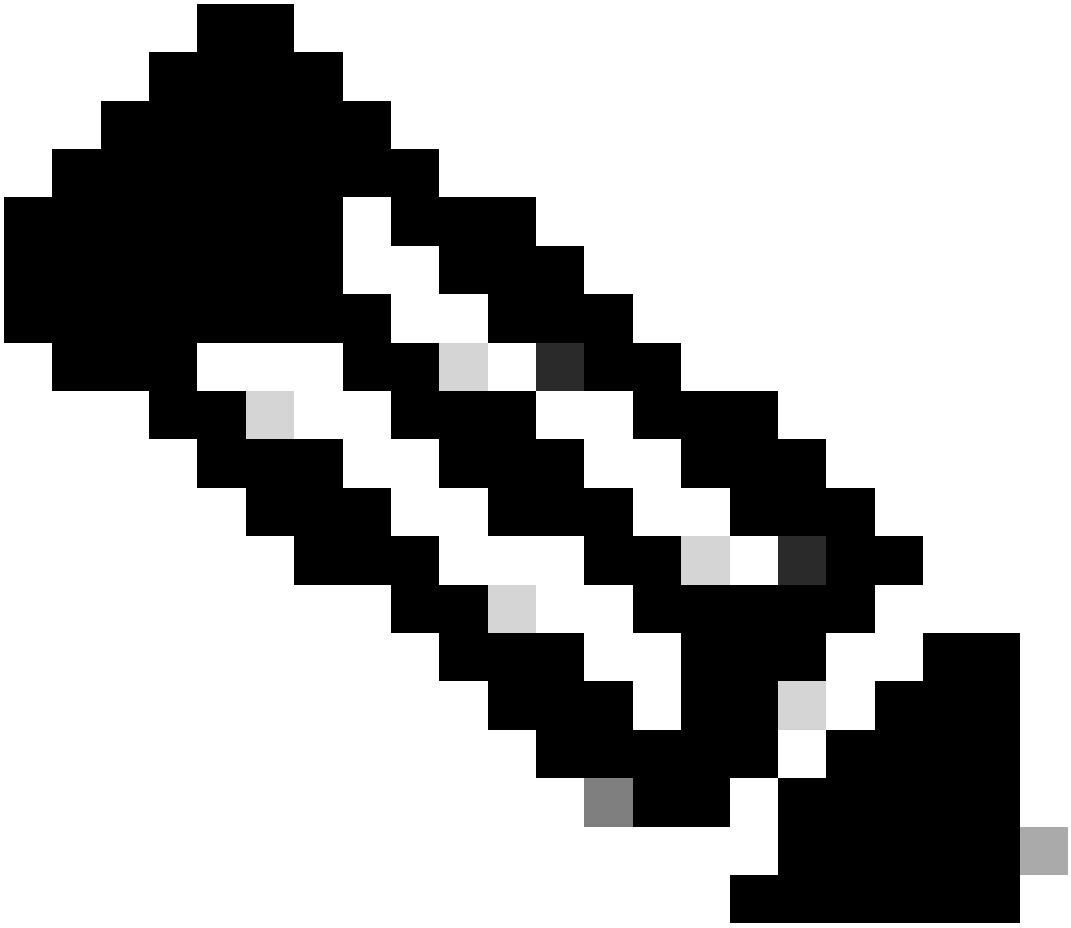
Schritt 10: Geben Sie einen Wert zwischen 102400 (100 Kilobyte) und 10737418240 (10 Gigabyte) für die Dateigröße (in Byte) vor der SWA-Rolle über das Protokoll in eine neue Datei ein.



Anmerkung: SWA archiviert (rollt über) Protokoll-Subscriptions, wenn eine aktuelle Protokolldatei eine vom Benutzer festgelegte Obergrenze für die maximale Dateigröße oder die maximale Zeit seit dem letzten Rollover erreicht.

Schritt 11: Die maximale Anzahl von Dateien gibt die Anzahl der auf dem Gerät gespeicherten Protokolldateien an. Wenn die Gesamtanzahl der Protokolldateien diesen Wert erreicht, werden die älteren Protokolle aus SWA gelöscht. Der Standardwert ist 10 Dateien, und Sie können die Anzahl der Protokolle eingeben, aufgrund des verfügbaren Speicherplatzes und anderer Protokollkonfigurationen, und dann die Eingabetaste drücken.

Schritt 12. In diesem Schritt können Sie die Protokolle komprimieren oder als Textdatei speichern. Geben Sie Y für Ja und N für Nein ein, und drücken Sie die Eingabetaste.



Anmerkung: Nachdem die Dateigröße die maximale Dateigröße erreicht hat, wird sie komprimiert. Das Komprimierungsverhältnis hängt vom Verhalten des Netzwerkverkehrs ab und kann je nach Protokolldatei variieren.

Schritt 13. Drücken Sie die Eingabetaste, um den Protokollkonfigurationsassistenten zu beenden.

Schritt 14. Geben Sie commit ein, um die Änderungen zu speichern.

```
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
```

Hinzufügen benutzerdefinierter Felder für Leistungsparameter zu Zugriffsprotokollen

Schritt 1: Melden Sie sich bei der GUI an.

Schritt 2: Wählen Sie im Menü "Systemverwaltung" die Option "Protokoll-Subscriptions".

Schritt 3: Klicken Sie in der Spalte "Protokollname" auf Accesslogs oder den Namen des neu erstellten. In diesem Beispiel ist dies TAC_access_logs.

Schritt 4. Fügen Sie im Abschnitt Benutzerdefinierte Felder diese Zeichenfolge ein:

```
[ 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 = %
```

Schritt 5: Änderungen übermitteln und bestätigen.

Überprüfen der Änderungen

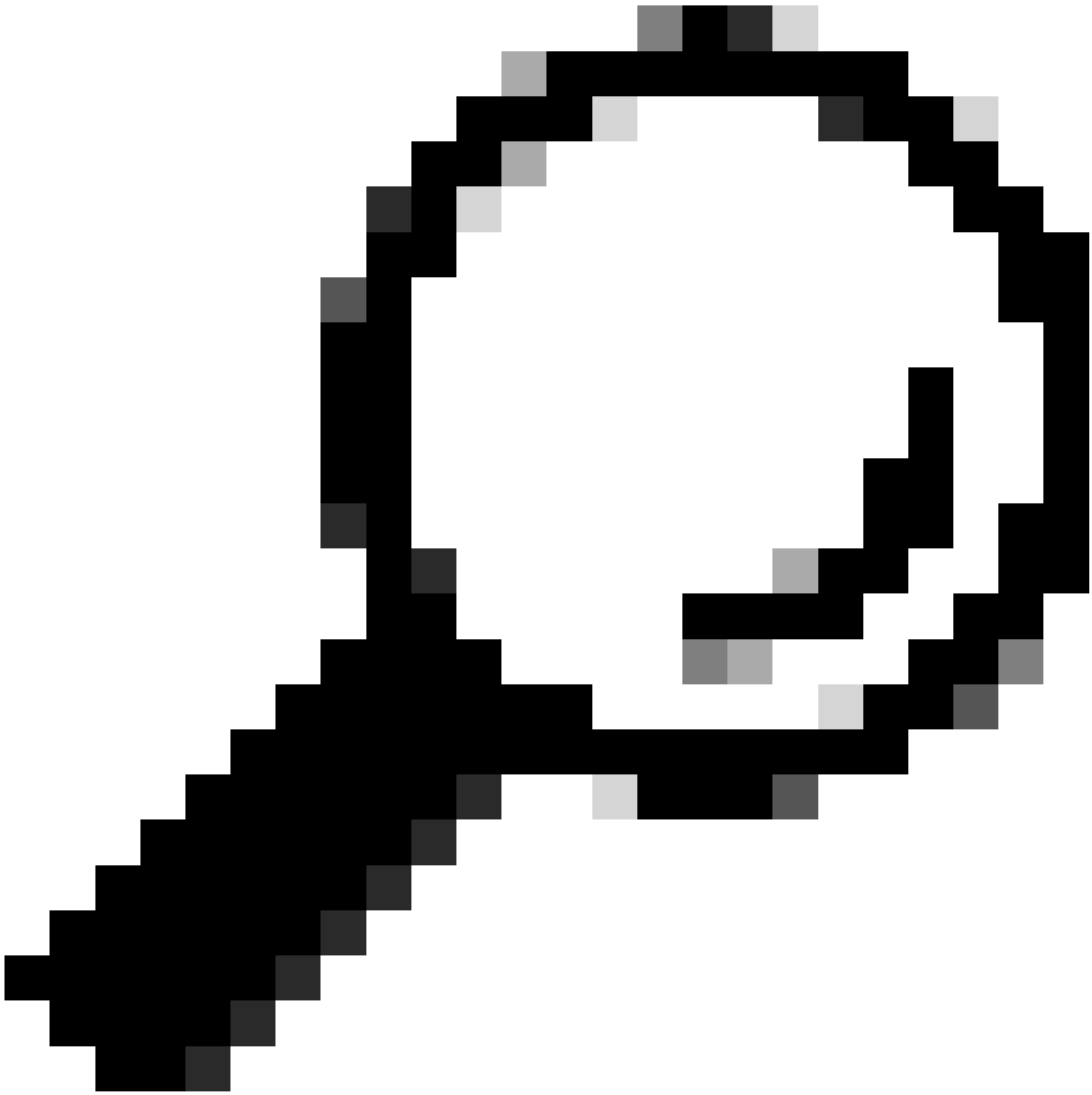
Schritt 1. Melden Sie sich bei CLI an.

Schritt 2. Geben Sie tail ein, und drücken Sie die Eingabetaste.

Schritt 3: Suchen Sie die Nummer, die den Zugriffsprotokollen zugeordnet ist, durch die der Leistungsparameter hinzugefügt wurde. Geben Sie die Nummer ein, und drücken Sie die Eingabetaste.

Den Zugriffsprotokollen wurden wie in diesem Beispiel zusätzliche Informationen hinzugefügt.

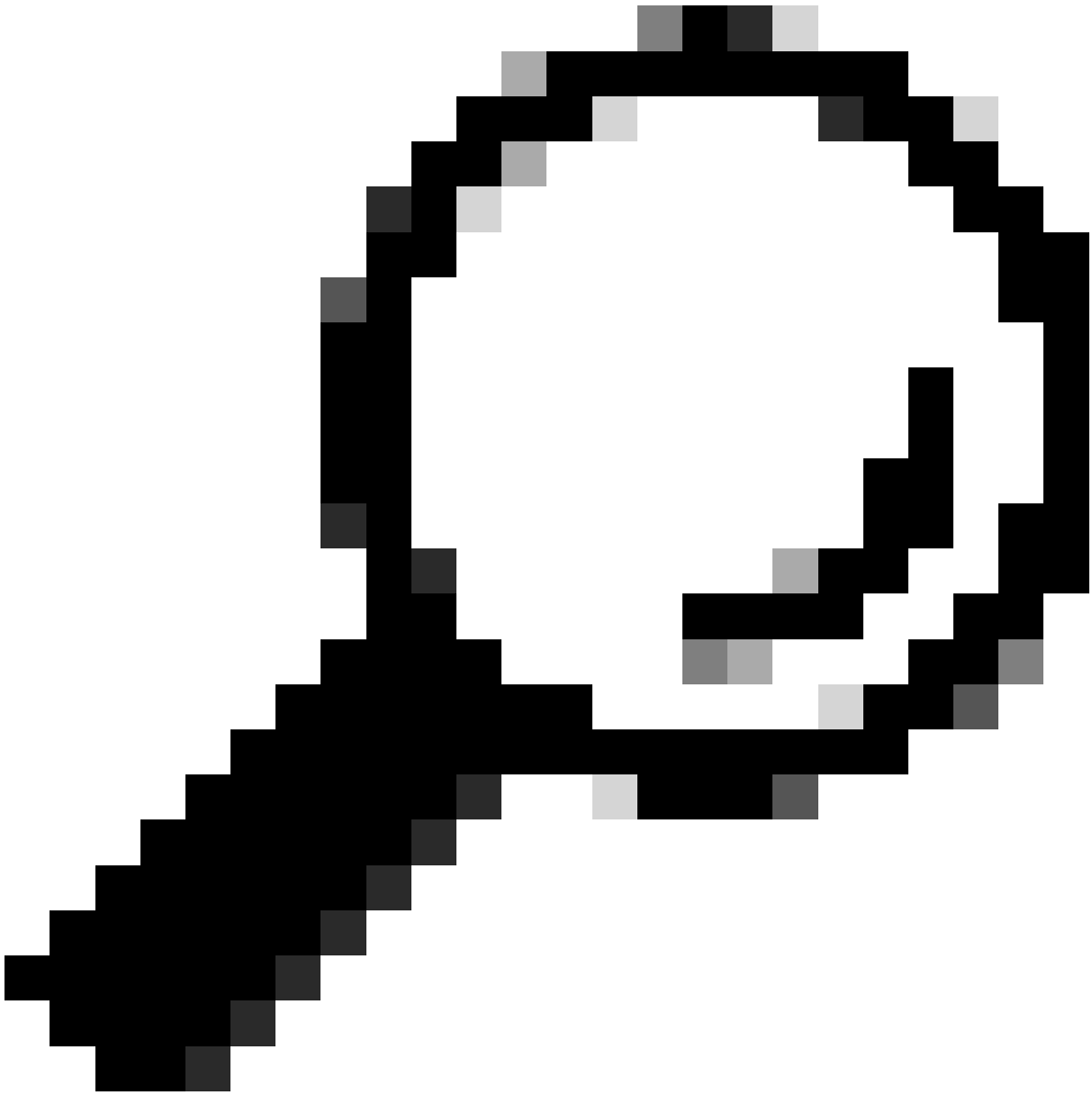
```
1680893872.492 1131 172.18.122.156 TCP_MISS/200 379725 GET http://www.cisco.com/en/US/docs/security/wsa/

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



Tipp: Sie können den Befehl tail beenden, wenn Sie die Strg-Taste gedrückt halten und C drücken. Wenn der Befehl tail nicht beendet wurde, geben Sie q ein.

Beschreibung von Feldern in benutzerdefinierten Feldern

Die im Feld für benutzerdefinierte Leistungsparameter verwendeten Werte entsprechen den folgenden Informationen:



Tipp: Latenz = AMP gesamt + Anti-Spyware gesamt + Webroot gesamt + Sophos gesamt + McAfee gesamt + AVC gesamt + WBRS gesamt + Auth gesamt

Name des benutzerdefinierten	Benutzerdefiniertes Feld	Beschreibung

Felds		
Anforderungs-Header	%:<h	Wartezeit, bis der Anforderungsheader nach dem ersten Byte auf den Server geschrieben wird.
Anfrage an Server	%:<b	Wartezeit, bis der Anforderungstext nach dem Header auf den Server geschrieben wird.
1. Byte an Client	%:1>	Wartezeit für das erste auf den Client geschriebene Byte.
Client-Text	%:b>	Wartezeit für den vollständigen, auf den Client geschriebenen Text.
Rx Wartezeiten (in ms): 1. Anforderungsbyte	%:1<	Die Zeit, die von dem Moment, in dem der Webproxy eine Verbindung mit dem Server herstellt, bis zu dem Zeitpunkt vergeht, in dem er zum ersten Mal auf den Server schreiben kann. Wenn der Webproxy zum Abschließen der Transaktion eine Verbindung mit mehreren Servern herstellen muss, ist dies die Summe dieser Zeiten.
Anforderungs-Header	%:h<	Wartezeit für vollständigen Client-Header nach dem ersten Byte.
Client-Text	%:b<	Wartezeit für vollständigen Client-Text.
1. Antwortbyte	%:>1	Wartezeit für das erste Antwortbyte vom Server.
Antwort-Header	%:>h	Wartezeit für den Server-Header nach dem ersten Antwortbyte.
Serverantwort	%:>b	Das bedeutet im Grunde, dass SWA HTTP-Header vom Server erhalten hat, aber SWA wartet danach auf die Antwortbytes und welches wäre der eigentliche Inhalt vom Server.
Festplatten-Cache	%:>c	Die Zeit, die der Webproxy benötigt, um eine Antwort aus dem Datenträgercache zu lesen.

Auth-Antwort	%:<a	Wartezeit, bis die Antwort vom Webproxy-Authentifizierungsprozess empfangen wird, nachdem der Webproxy die Anforderung gesendet hat.
Auth gesamt	%:>a	Die Wartezeit, bis die Antwort vom Webproxy-Authentifizierungsprozess empfangen wird, umfasst die Zeit, die der Webproxy benötigt, um die Anforderung zu senden.
DNS-Antwort	%:<d	Die Zeit, die der Webproxy benötigt, um die DNS-Anforderung (Domain Name Request) an den Webproxy-DNS-Prozess zu senden.
DNS gesamt	%:>d	Die Zeit, die der Webproxy-DNS-Prozess benötigt, um ein DNS-Ergebnis an den Webproxy zurückzusenden.
WBRS-Antwort	%:<r	Die Wartezeit, bis die Antwort von den Webreputations-Filtern empfangen wird, nachdem der Webproxy die Anforderung gesendet hat.
WBRS gesamt	%:>r	Die Wartezeit, nach der das Urteil von den Webreputations-Filtern empfangen wird, umfasst die Zeit, die der Webproxy benötigt, um die Anforderung zu senden.
AVC-Antwort	%:A>	Wartezeit, bis die Antwort vom AVC-Prozess (Application Visibility and Control) empfangen wird, nachdem der Webproxy die Anforderung gesendet hat.
AVC gesamt	%:A<	Die Wartezeit, bis die Antwort vom AVC-Prozess empfangen wird, umfasst die Zeit, die der Webproxy zum Senden der Anforderung benötigt.
DCA-Antwort	%:C>	Wartezeit, bis die Antwort vom dynamischen Inhaltsanalysemodul empfangen wird, nachdem der Webproxy die Anforderung gesendet hat.
DCA gesamt	%:C<	Die Wartezeit, nach der das Urteil vom Dynamic Content Analysis Engine empfangen wird, umfasst die Zeit, die der Webproxy benötigt, um die Anforderung zu

		senden.
McAfee-Antwort	%:m>	Wartezeit, bis die Antwort vom McAfee-Scanmodul empfangen wird, nachdem der Webproxy die Anforderung gesendet hat.
McAfee gesamt	%:m<	Die Wartezeit für den Empfang des Urteils vom McAfee-Scanmodul umfasst die Zeit, die der Webproxy benötigt, um die Anforderung zu senden.
Sophos-Antwort	%:p>	Wartezeit, bis die Antwort vom Sophos-Scanmodul empfangen wird, nachdem der Webproxy die Anforderung gesendet hat.
Sophos gesamt	%:p<	Die Wartezeit, nach der das Urteil vom Sophos-Scanmodul eingeht, umfasst die Zeit, die der Webproxy benötigt, um die Anforderung zu senden.
AMP-Antwort	%:e>	Wartezeit, bis die Antwort vom AMP-Modul empfangen wird, nachdem der Webproxy die Anforderung gesendet hat.
AMP gesamt	%:e<	Die Wartezeit, bis das Verdict von der AMP-Engine empfangen wird, beinhaltet die Zeit, die der Webproxy benötigt, um die Anforderung zu senden.
Latenz	%x; %L	Latenz und lokale Zeit anfordern in einem für Menschen lesbaren Format: TT/MMM/JJJJ: hh:mm:ss +nnn. Dieses Feld wird in den Zugriffsprotokollen mit doppelten Anführungszeichen geschrieben. In diesem Feld können Sie Protokolle mit Problemen korrelieren, ohne für jeden Protokolleintrag die lokale Zeit aus der Epochenzeit berechnen zu müssen.
Client-Port	%F	Von Client-Seite verwendete Portnummer
Server-IP-Adresse	%k	Webserver-IP-Adresse
Server-Portnummer	%p	Webserver-Portnummer

Zugehörige Informationen

- Benutzerhandbuch für AsyncOS 14.5 für Cisco Secure Web Appliance - GD (Allgemeine Bereitstellung) - Cisco
- Best Practices-Richtlinien für Cisco Web Security Appliances - Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.