Prestatieparameter configureren in toegangslogboeken

Inhoud

Inleiding

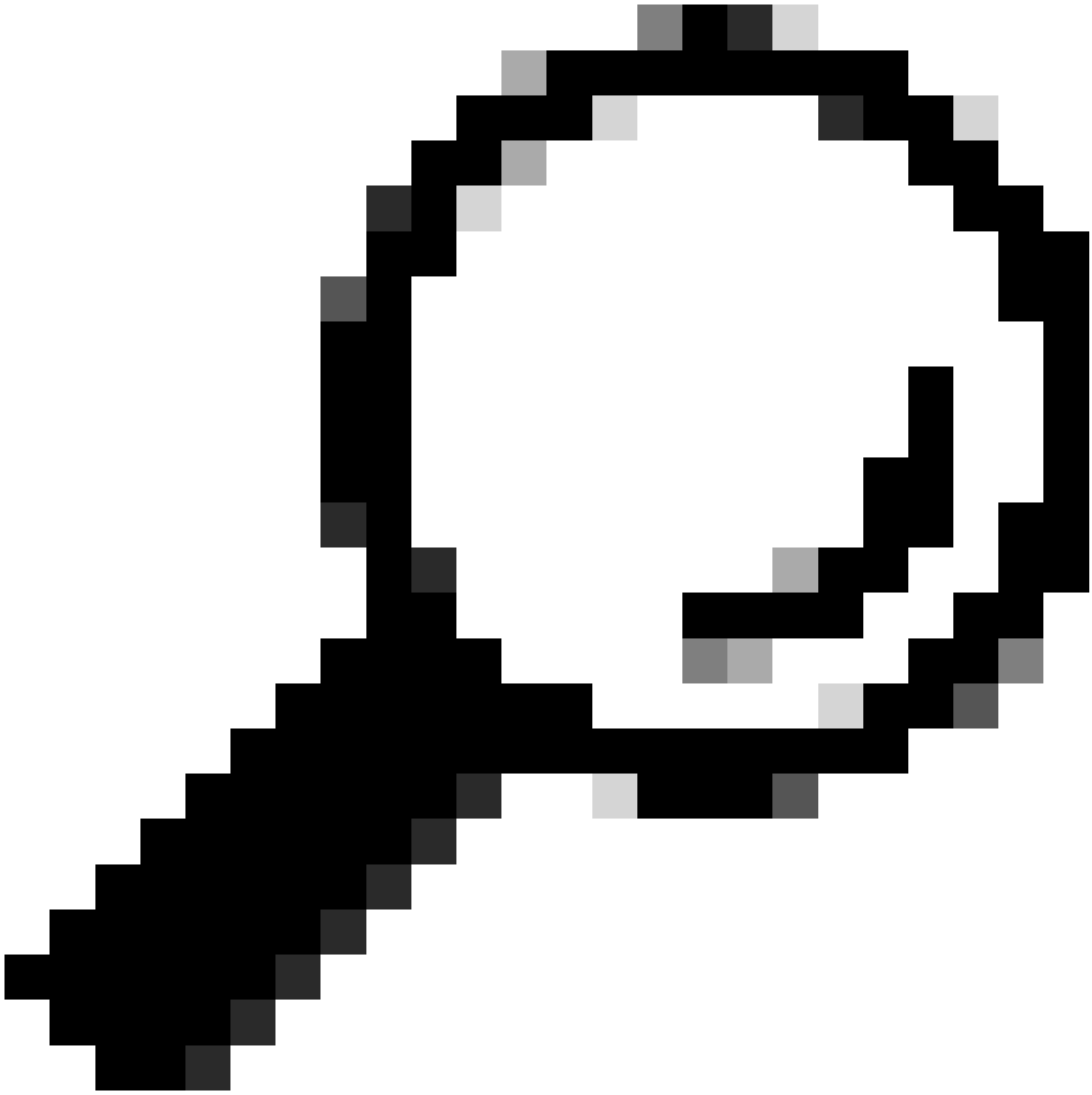
In dit document worden de stappen beschreven voor het toevoegen van een aangepast veld voor de parameter Prestaties aan het SWA-toegangslogboek (Secure Web Appliance).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Secure Shell Protocol (SSH) toegang tot SWA-beheerinterface.
- Graphical User Interface (GUI)-toegang tot de SWA-beheerinterface.



Tip: Het is het beste om meer dan 20% vrije schijfruimte op SWA-gegevenspartitie te hebben. U kunt het schijfgebruik controleren via de Command Line Interface (CLI) in de opdracht Detail van status.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Wanneer er een latentieprobleem is en het verkeer wordt benaderd via een SWA, kunnen de toegangslogboeken nuttig zijn om problemen met de hoofdoorzaak van latentie op te lossen. U kunt de huidige instellingen voor toegangslogboeken wijzigen of nieuwe toegangslogboeken maken met prestatieparameters die aan het aangepaste veld zijn toegevoegd.

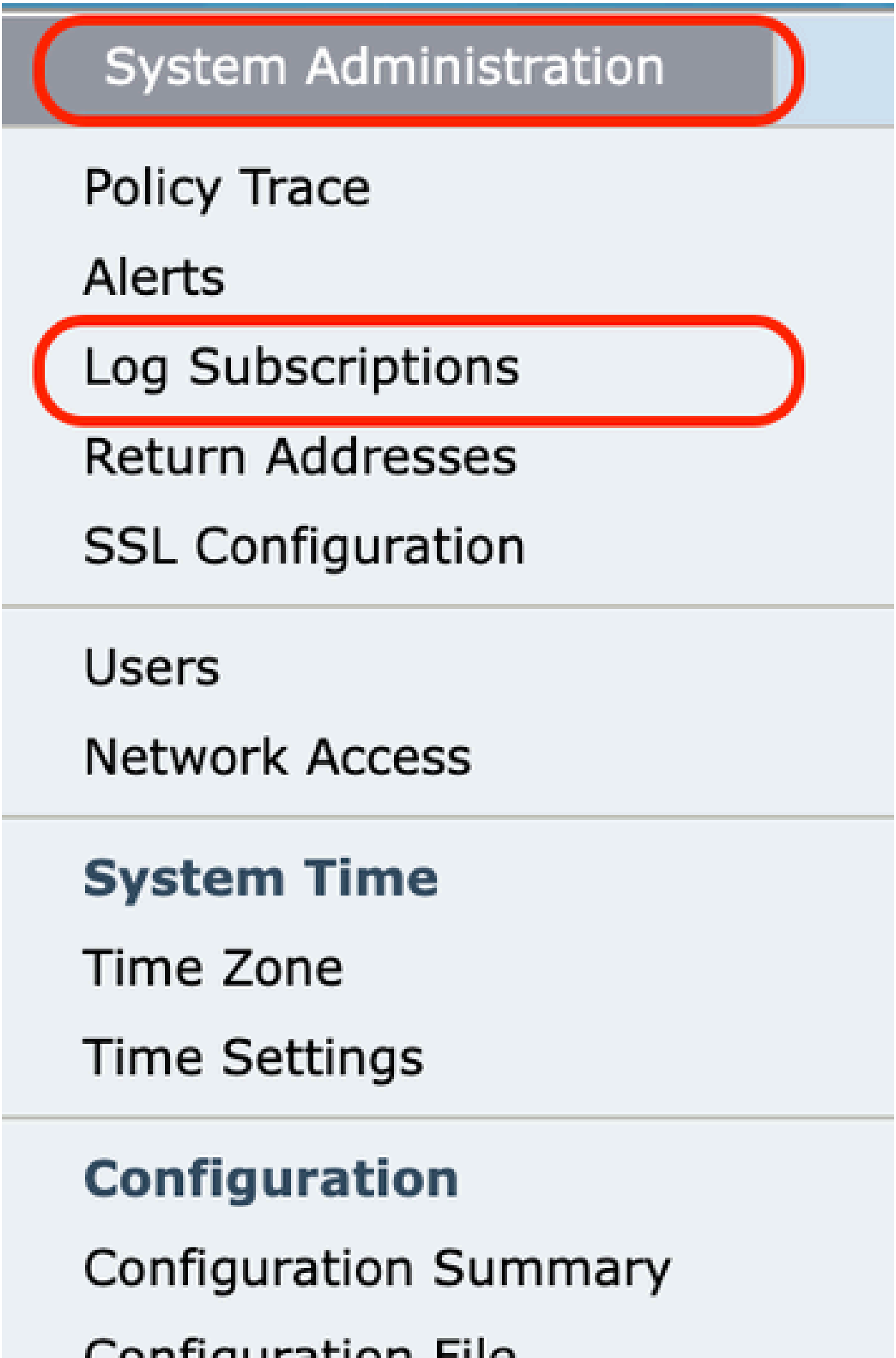
Extra toegangslog maken

Onder bepaalde omstandigheden is het vanwege intern beleid of een andere configuratie niet mogelijk om het huidige toegangslogboek te wijzigen. Om deze beperking te omzeilen, kunt u een ander toegangslogboek maken en de aangepaste parameter Prestaties toevoegen aan de nieuwe toegangslogboeken.

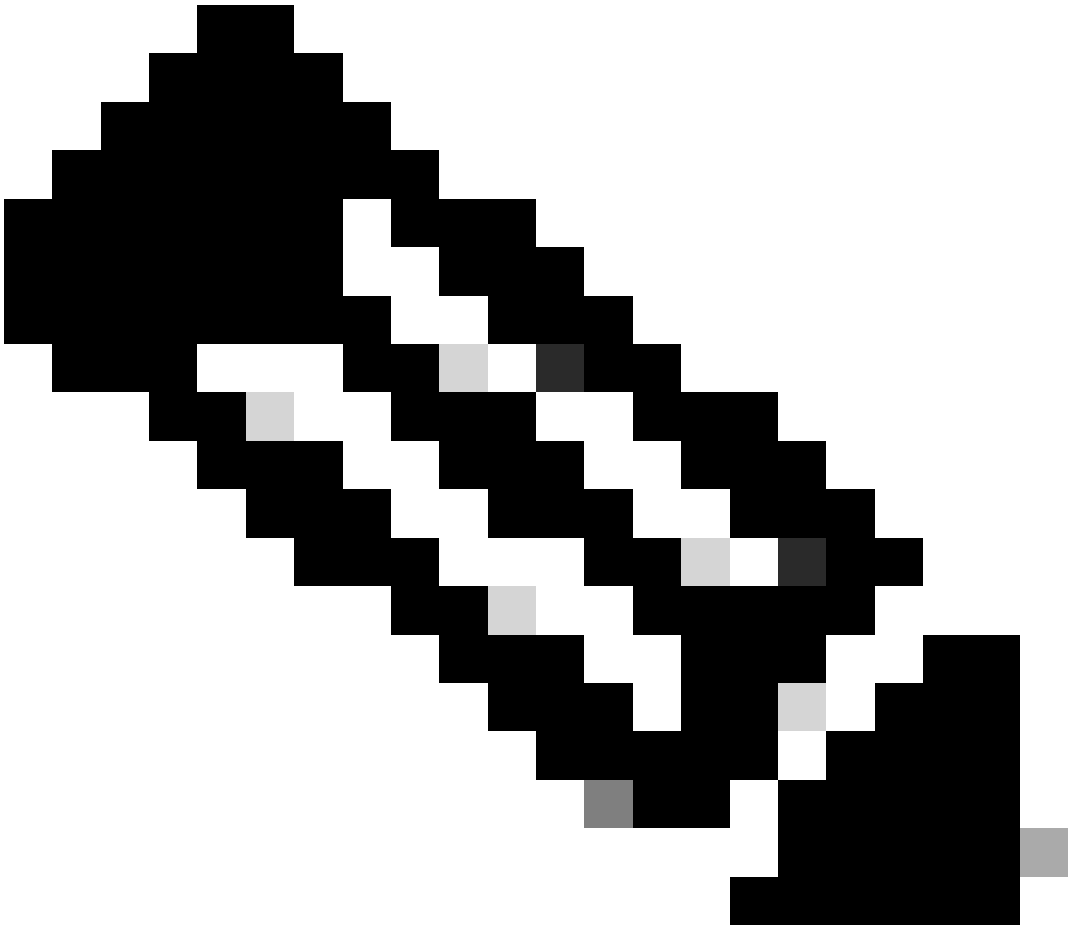
Nieuw toegangslog maken vanuit GUI

Stap 1. Log in op de GUI.

Stap 2. Kies in het menu Systeembeheer de optie Logabonnementen.


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

Voer een waarde in tussen 102400 (100 kilobytes) en 10737418240 (10 gigabytes) voor de bestandsgrootte (in byte) voordat SWA-rollen over het logbestand naar een nieuw bestand worden verplaatst. Het getal moet een geheel getal zijn en u kunt M toevoegen om de grootte aan te geven in Megabyte, K om de bestandsgrootte aan te geven in kilobyte en G voor gigabyte.



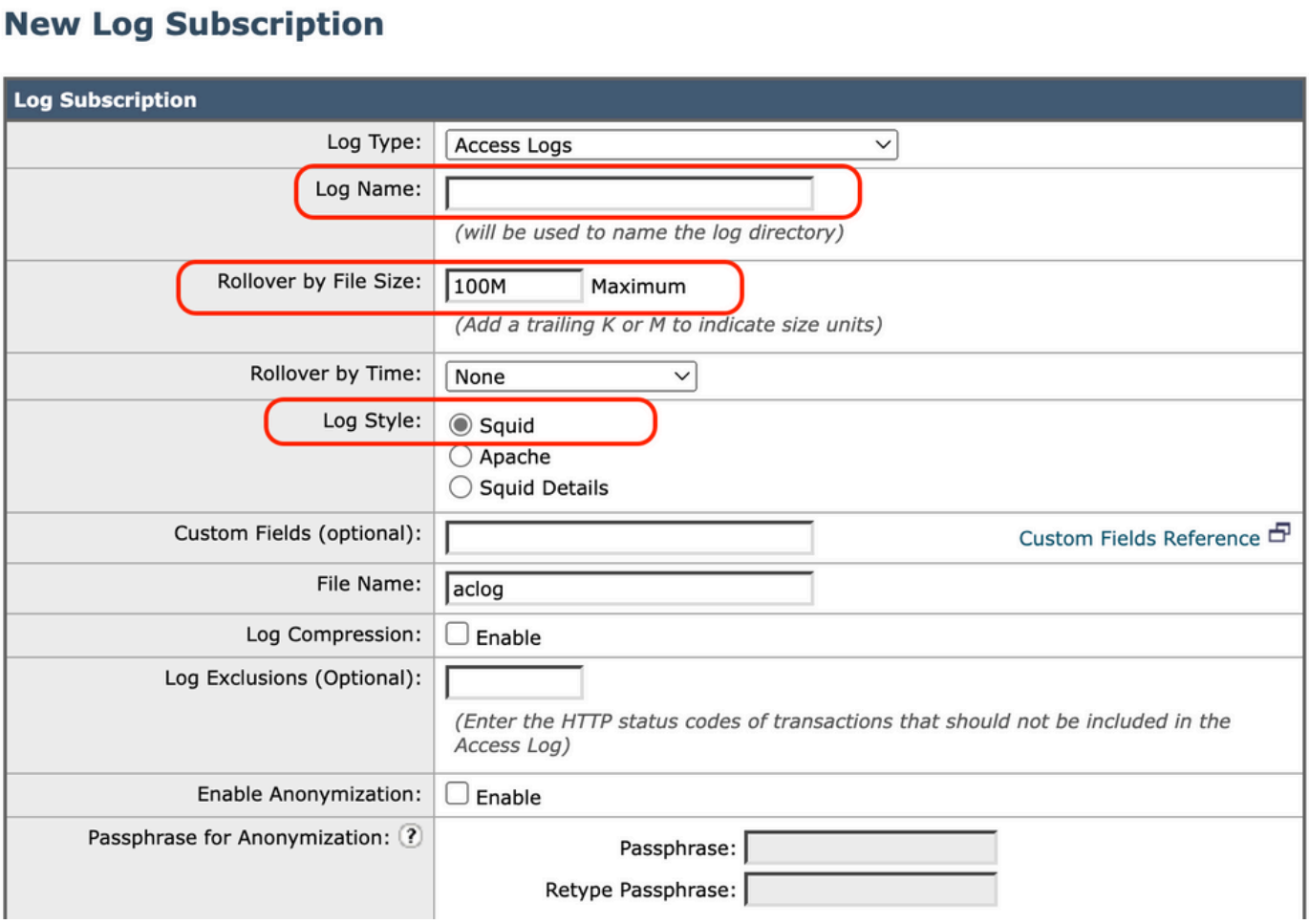
Opmerking: SWA-archieven (rolls over) logboekabonnementen wanneer een huidig logbestand een door de gebruiker opgegeven limiet van maximale bestandsgrootte of maximale tijd sinds de laatste rollover bereikt.

Stap 7. Kies Squid voor logstijl.

Stap 8. Bestandsnaam is om de naam van de map en de naam van het logbestand voor dit nieuwe log te definiëren. Het wordt aangeraden om hetzelfde te zijn als de lognaam, die in dit voorbeeld TAC_access_logs was.

Stap 9. U kunt logcompressie inschakelen om logboekbestanden te comprimeren of de logbestanden als tekstbestand te behouden.

Stap 10. Loguitsluiting is het filteren van de HTTP-responscode (Hypertext Transfer Protocol). Filter geen HTTP-statuscodes.



Vul de verplichte velden in

Stap 11. Kies FTP-poll om de logs in de SWA te houden. Typ 1 en druk op Enter.

Stap 12. Verzenden en vastleggen van wijzigingen.

Nieuw toegangslog configureren vanuit CLI

Stap 1. Log in bij CLI.

Stap 2. Voer logconfig uit.

Stap 3. Als u een nieuw log wilt maken, typt u Nieuw en drukt u op Enter.

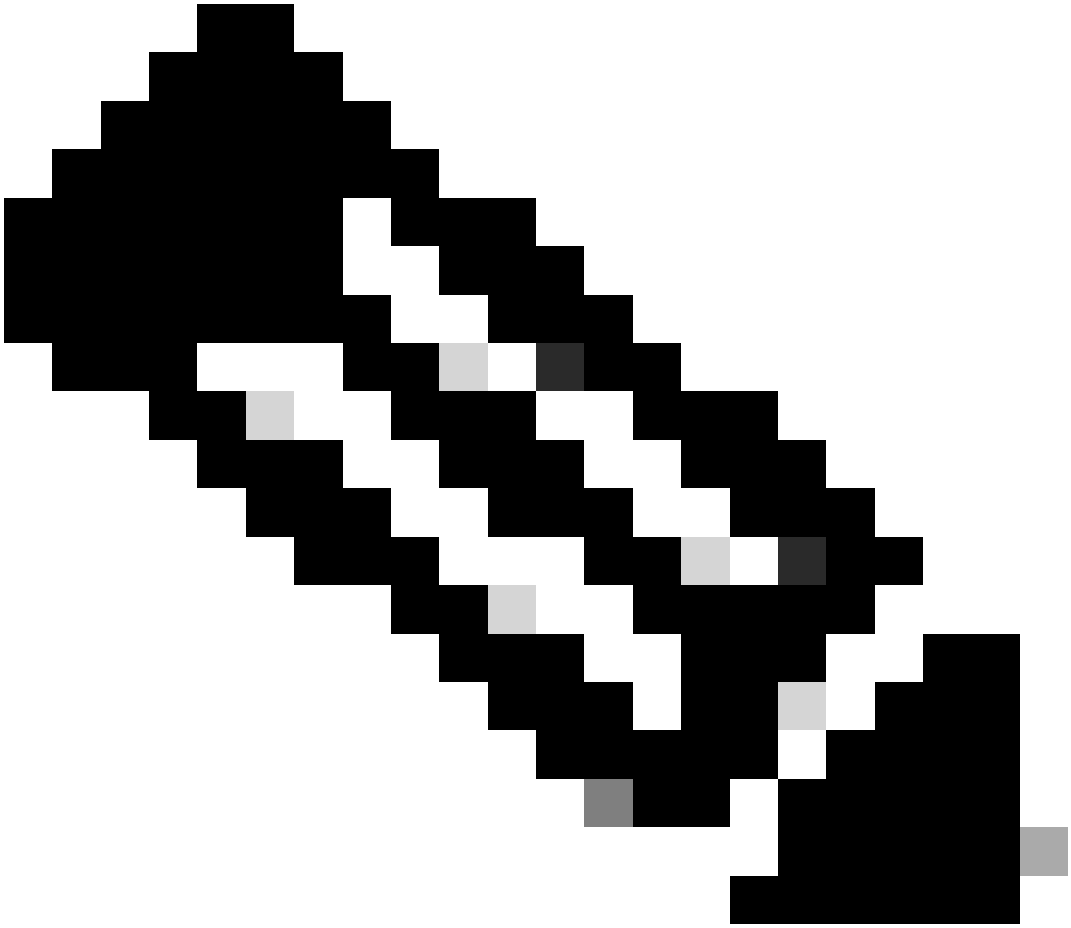
Stap 4. Zoek toegangslogboeken in de lijst, typ het nummer dat aan dat logboek is gekoppeld en druk op Enter.

Stap 5. Typ een naam voor een nieuw log.

Stap 6. Typ 1 om Squid te kiezen voor de logstijl voor dit abonnement en druk op Enter.

Stap 7. Filter geen HTTP-foutstatuscodes. Druk op Enter om naar de volgende stap te gaan.

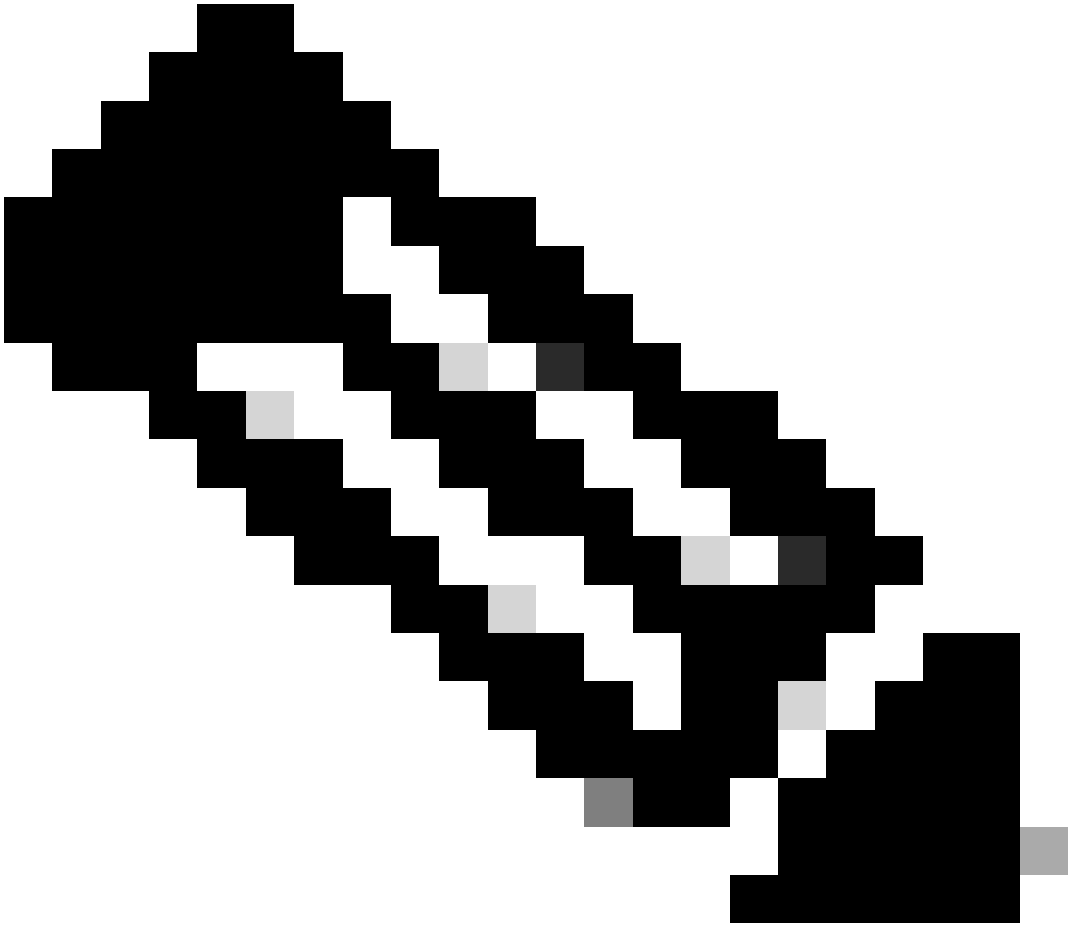
Stap 8. Kies FTP-poll om de logs in de SWA te houden. Typ 1 en druk op Enter.



> Opmerking: als u de logs wilt pushen naar de FTP-server (File Transfer Protocol), de SCP-server (Secure Copy Protocol) of de Syslog-server. U kunt opties kiezen die betrekking hebben op hen.

Stap 9. Deze stap is het definiëren van de naam van de map en de bestandsnaam voor het nieuwe log. Het is beter om dezelfde naam te gebruiken als de lognaam en op Enter te drukken.

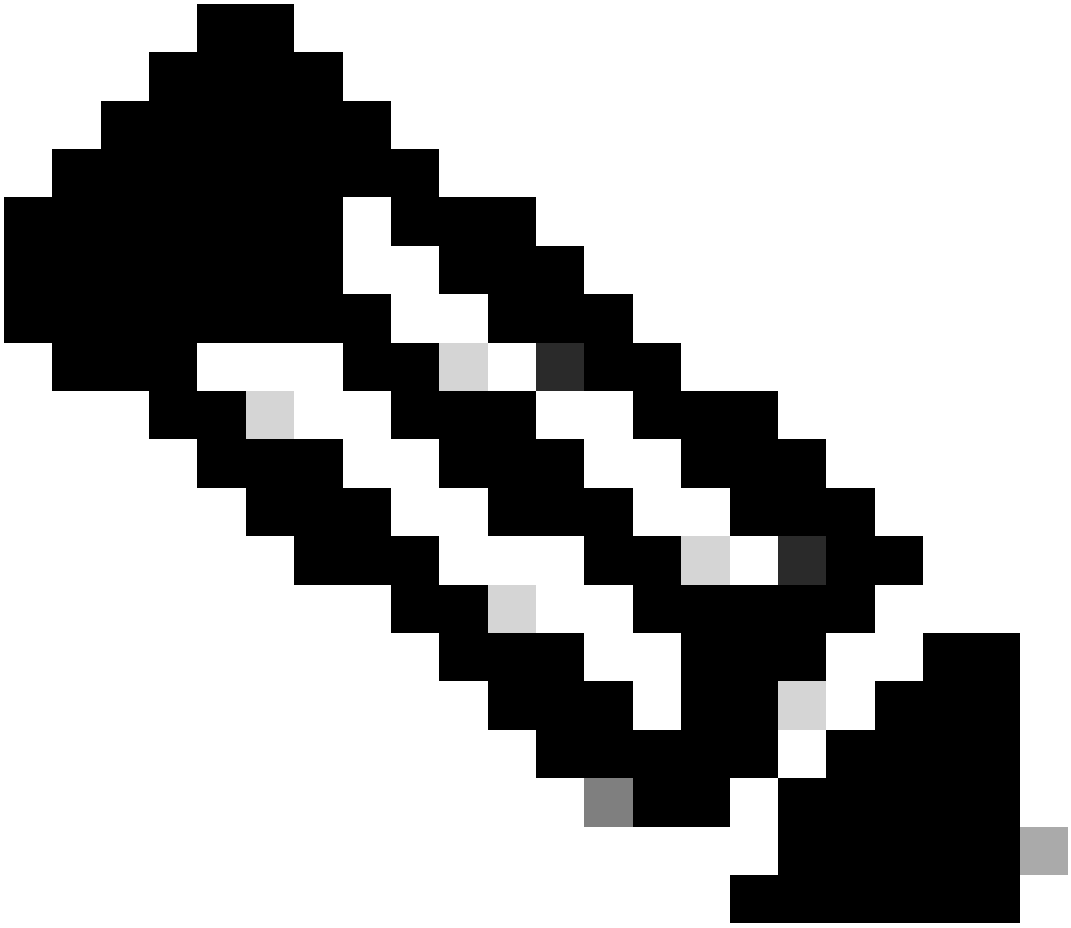
Stap 10. Voer een waarde in tussen 102400 (100 kilobytes) en 10737418240 (10 gigabytes) voor de bestandsgrootte (in byte) voordat SWA-rol over het logbestand naar een nieuw bestand gaat.



Opmerking: SWA-archieven (rolls over) logboekabonnementen wanneer een huidig logbestand een door de gebruiker opgegeven limiet van maximale bestandsgrootte of maximale tijd sinds de laatste rollover bereikt.

Stap 11. Het maximum aantal bestanden geeft het aantal logbestanden aan dat op het apparaat is opgeslagen. Als het totale aantal logbestanden deze waarde heeft bereikt, worden de oudere logbestanden uit SWA verwijderd. De standaardwaarde is 10 bestanden en u kunt het aantal logs typen, vanwege de beschikbare schijfruimte en andere logboekconfiguratie, en vervolgens op Enter drukken.

Stap 12. In deze stap kunt u ervoor kiezen om de logs te comprimeren of als tekstbestand te bewaren. Typ Y voor Ja en N voor Nee en druk op Enter.



Opmerking: Nadat de bestandsgrootte de maximale bestandsgrootte heeft bereikt, wordt deze gecomprimeerd. De compressieverhouding is afhankelijk van het gedrag van het netwerkverkeer en kan variëren tussen logbestanden.

Stap 13. Druk op Enter om de logconfiguratiewizard af te sluiten.

Stap 14. Typ commit om de wijzigingen op te slaan.

```
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
```

Aangepaste velden voor prestatieparameters toevoegen aan toegangslogboeken

Stap 1. Log in op de GUI.

Stap 2. Kies in het menu Systeembeheer de optie Logboekabonnementen.

Stap 3. Klik in de kolom Lognaam op accesslogs of op de naam van de nieuw gemaakte logbestanden. In dit voorbeeld, TAC_access_logs.

Stap 4. Plak deze tekenreeks in de sectie Aangepaste velden:

```
[ 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 = %
```

Stap 5. Verzenden en vastleggen van wijzigingen.

Controleer de wijzigingen

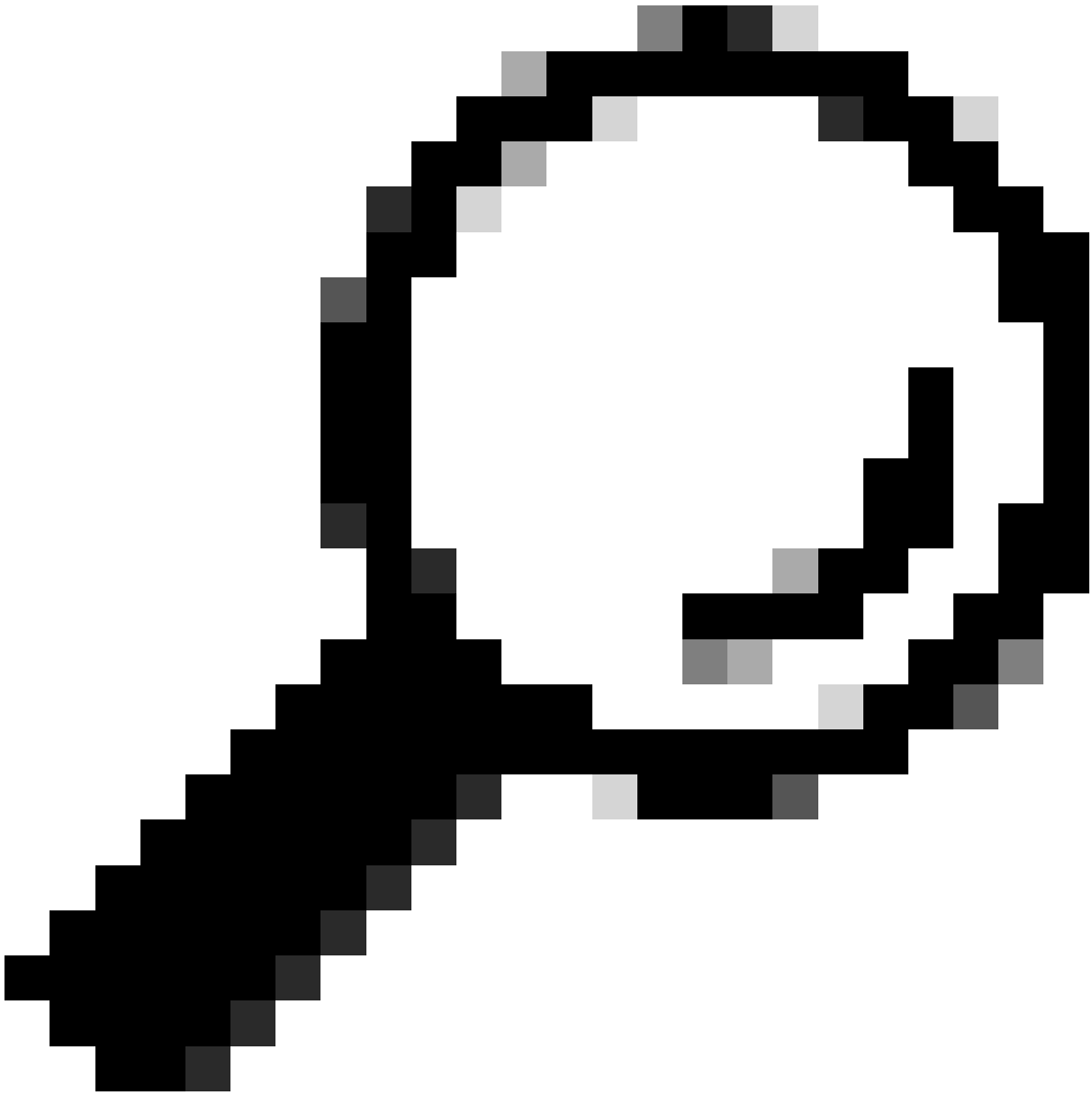
Stap 1. Log in bij CLI.

Stap 2. Typ staart en druk op enter.

Stap 3. Zoek het nummer dat is gekoppeld aan de toegangslogboeken die de prestatieparameter hebben toegevoegd. Typ het nummer en druk op Enter.

U kunt zien dat er extra informatie is toegevoegd aan de toegangslogboeken, hetzelfde als in dit voorbeeld.

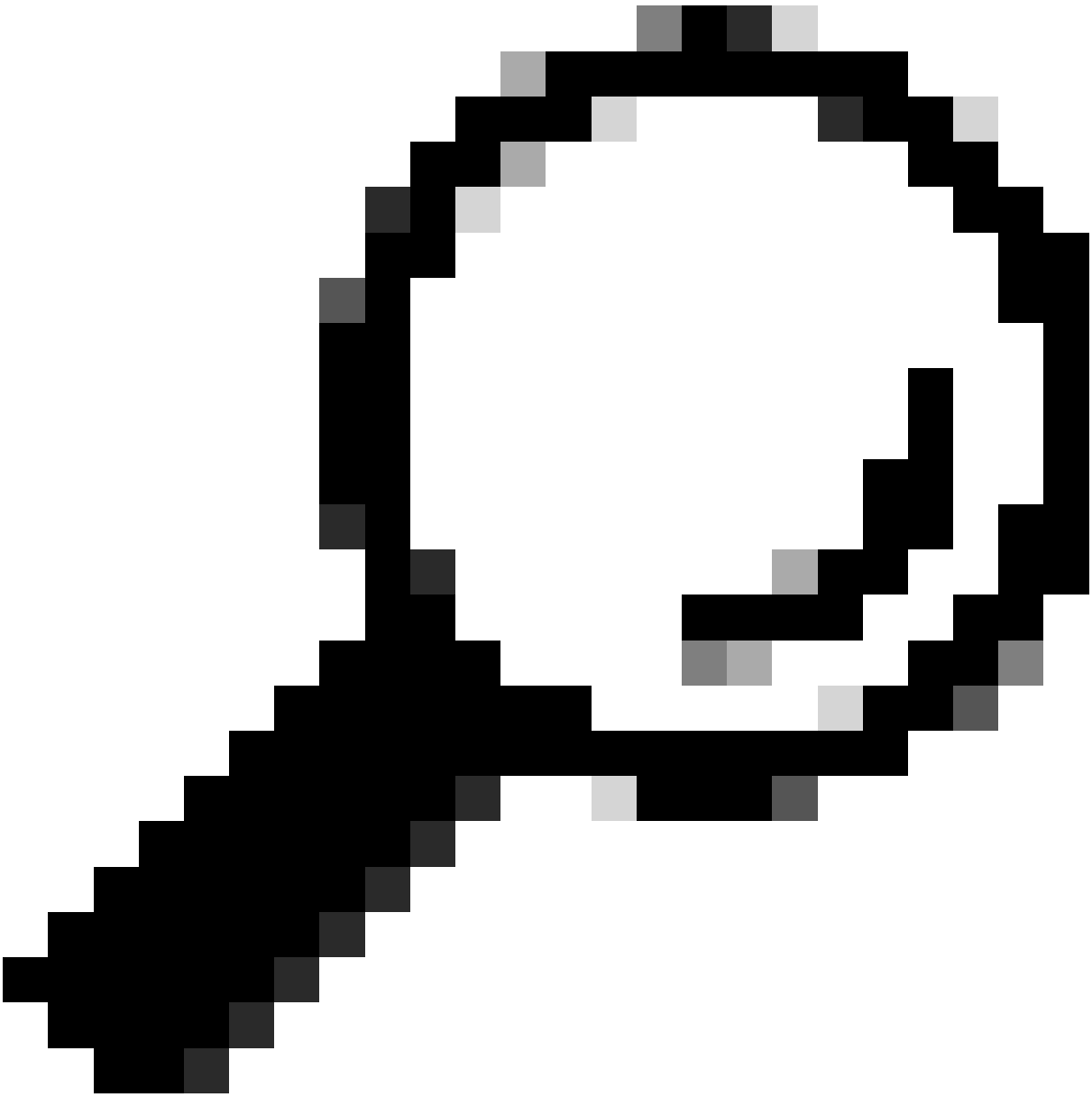
```
1680893872.492 1131 172.18.122.156 TCP_MISS/200 379725 GET http://www.cisco.com/en/US/docs/security/wsa/

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



Tip: U kunt de staart opdracht afsluiten wanneer u de Control-toets ingedrukt houdt en op C drukt. Als dat de staart niet heeft afgesloten, typt u q.

Veldbeschrijving in Aangepaste velden

De waarden die in het veld Aangepaste prestatieparameter worden gebruikt, geven deze informatie weer:



Tip: Latentie = AMP totaal + Anti-Spyware totaal + Webroot totaal + Sophos totaal + McAfee totaal + AVC totaal + WBRS totaal + Auth totaal

Aangepaste veldnaam	Aangepast veld	Beschrijving

Koptekst aanvragen	%: <h	Wachttijd voor het schrijven van de aanvraagheader naar de server na de eerste byte.
Verzoek aan server	%:<b	Wachttijd voor het schrijven van de hoofdtekst van het verzoek naar de server na de koptekst.
1e byte naar client	%:1>	Wachttijd voor eerste byte geschreven naar client.
cliëntenorgaan	%:b>	Wachttijd voor volledige lichaam geschreven aan de klant.
Rx-wachttijden (in ms): 1e verzoekbyte	%:1<	De tijd die nodig is vanaf het moment dat de Web Proxy verbinding maakt met de server tot het moment dat deze voor het eerst naar de server kan schrijven. Als de Web Proxy verbinding moet maken met meerdere servers om de transactie te voltooien, is dit de som van die tijden.
Koptekst aanvragen	%:h<	Wachttijd voor volledige clientkoptekst na eerste byte.
cliëntenorgaan	%:b<	Wachttijd voor volledige cliëntenlichaam.
1e responsbyte	%:>1	Wachttijd voor eerste antwoordbyte van server.
Respons koptekst	%:>h	Wachttijd voor serverheader na eerste antwoordbyte.
Serverrespons	%:>b	Dit betekent in feite dat SWA HTTP-headers van de server heeft gekregen, maar SWA wacht daarna op de antwoordbytes en wat de werkelijke inhoud van de server zou zijn.
Schijfcache	%:>c	Tijd die de Web Proxy nodig heeft om een antwoord uit de schijfcache te lezen.
Auth-respons	%: <a	Wacht tot u het antwoord van het Web Proxy-verificatieproces hebt ontvangen nadat de Web Proxy het verzoek heeft verzonden.
Auth totaal	%:>a	De wachttijd voor het ontvangen van het antwoord van het Web Proxy-verificatieproces omvat de tijd die de Web Proxy nodig heeft om het verzoek te verzenden.

DNS-respons	%:<d	De tijd die de Web Proxy nodig heeft om het DNS-verzoek (Domain Name Request) naar het DNS-proces voor de Web Proxy te verzenden.
DNS totaal	%:>d	De tijd die het Web Proxy DNS-proces nodig heeft om een DNS-resultaat terug te sturen naar de Web Proxy.
WBRS-respons	%:<r	Wachttijd om het antwoord van de Web Reputation Filters te ontvangen, nadat de Web Proxy het verzoek heeft verzonden.
WBRS totaal	%:>r	Wachttijd voor het ontvangen van het vonnis van de Web Reputation Filters, inclusief de tijd die nodig is voor de Web Proxy om het verzoek te verzenden.
AVC-respons	%: A>	Wacht tot u het antwoord van het proces voor zichtbaarheid en controle van de toepassing (AVC) hebt ontvangen nadat de webproxy het verzoek heeft verzonden.
AVC totaal	%:A<	De wachttijd voor het ontvangen van het antwoord van het AVC-proces omvat de tijd die de webproxy nodig heeft om het verzoek te verzenden.
DCA-respons	%:C>	Wacht tot u het antwoord van de Dynamic Content Analysis-engine hebt ontvangen nadat de Web Proxy het verzoek heeft verzonden.
DCA totaal	%:C<	De wachttijd voor het ontvangen van het vonnis van de Dynamic Content Analysis-engine omvat de tijd die de Web Proxy nodig heeft om het verzoek te verzenden.
McAfee-antwoord	%:m>	Wacht tot het antwoord van de McAfee-scanengine is ontvangen nadat de Web Proxy het verzoek heeft verzonden.
McAfee totaal	%:m<	De wachttijd voor het ontvangen van het vonnis van de McAfee-scanengine omvat de tijd die de Web Proxy nodig heeft om het verzoek te verzenden.
Sophos-reactie	%:p>	Wachttijd om het antwoord van de Sophos-scanengine te ontvangen, nadat de Web Proxy het verzoek heeft verzonden.

Sophos totaal	%:p<	Wachttijd om het vonnis van de Sophos-scanengine te ontvangen, omvat de tijd die de Web Proxy nodig heeft om het verzoek te verzenden.
AMP-respons	%:e>	Wachttijd om het antwoord van de AMP-engine te ontvangen, nadat de Web Proxy het verzoek heeft verzonden.
AMP totaal	%:e<	De wachttijd voor het ontvangen van het vonnis van de AMP-engine omvat de tijd die de Web Proxy nodig heeft om het verzoek te verzenden.
latentie	%x; %l	Latentie en lokale tijd aanvragen in menselijk leesbaar formaat: DD/MMM/JJJJ: hh:mm:ss +nnnn. Dit veld wordt geschreven met dubbele aanhalingstekens in de toegangslogboeken. Met dit veld kunt u logs correleren met problemen zonder dat u de lokale tijd vanaf het einde van elke logboekvermelding hoeft te berekenen.
Clientpoort	%F	Poortnummer gebruikt vanaf clientzijde.
IP-adres van server	%k	IP-adres van webserver.
Poortnummer van server	%p	Poortnummer van webserver.

Gerelateerde informatie

- Gebruikershandleiding voor AsyncOS 14.5 voor Cisco Secure Web Appliance - GD (Algemene implementatie) - Cisco
- Richtlijnen voor best practices voor Cisco Web Security-apparaten - Cisco

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.