Configurar Parâmetro de Desempenho em Logs de Acesso

Contents

Introdução

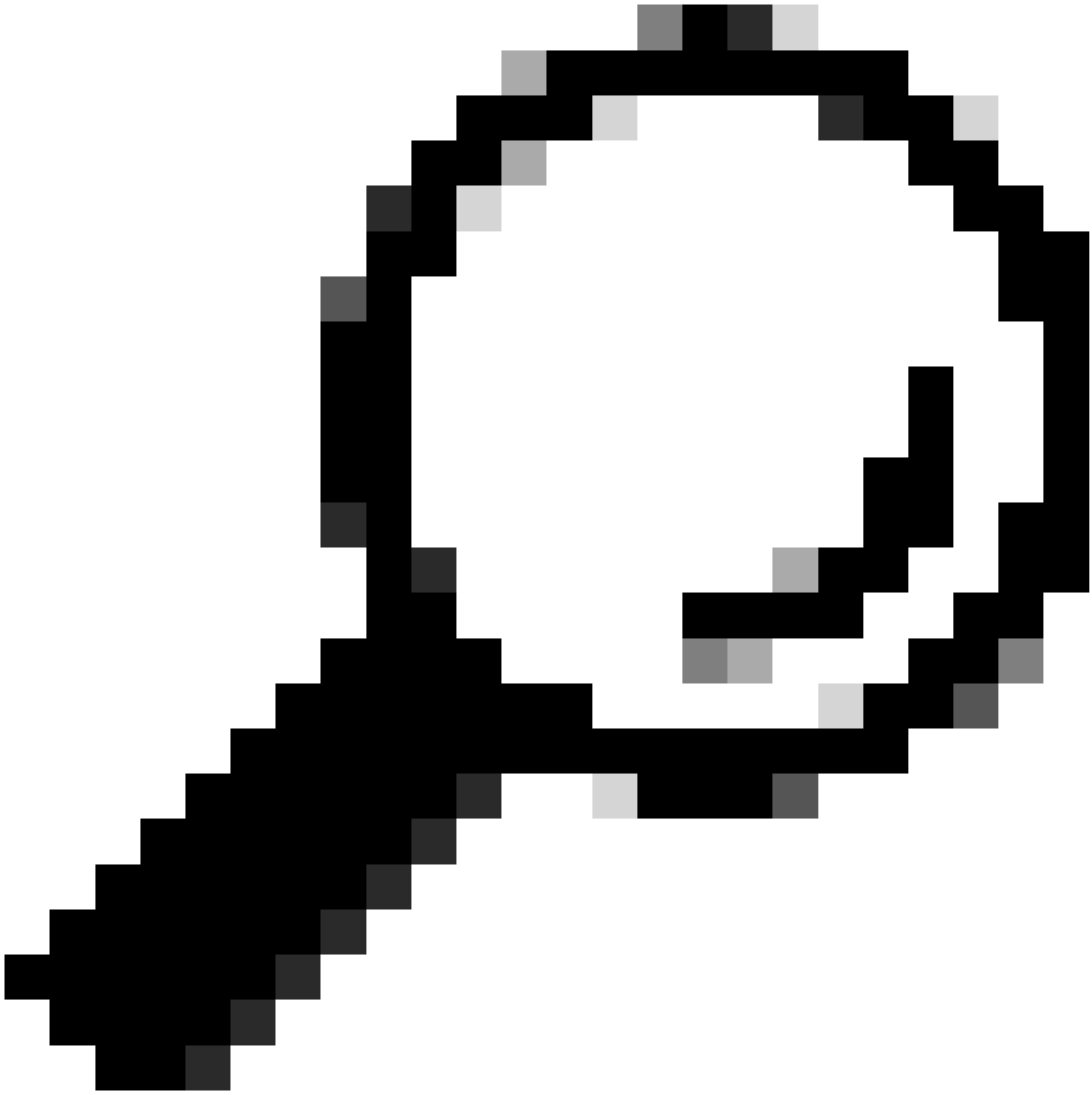
Este documento descreve as etapas para adicionar o campo personalizado Parâmetro de desempenho ao Log de acesso do Secure Web Appliance (SWA).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Acesso SSH (Secure Shell Protocol) à interface de gerenciamento do SWA.
- Acesso à Interface Gráfica do Usuário (GUI - Graphical User Interface) para a interface de gerenciamento do SWA.



Tip: É melhor ter mais de 20% de espaço livre em disco na partição de dados SWA. Você pode verificar o uso do disco na Interface de Linha de Comando (CLI) na saída do comando status detail.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Quando há um problema de latência e o tráfego recebe proxy por meio de um SWA, os Logs de acesso podem ser úteis para solucionar a causa raiz da latência. Você pode alterar as configurações atuais de Logs de acesso ou criar novos Logs de acesso com Parâmetros de desempenho adicionados ao Campo personalizado.

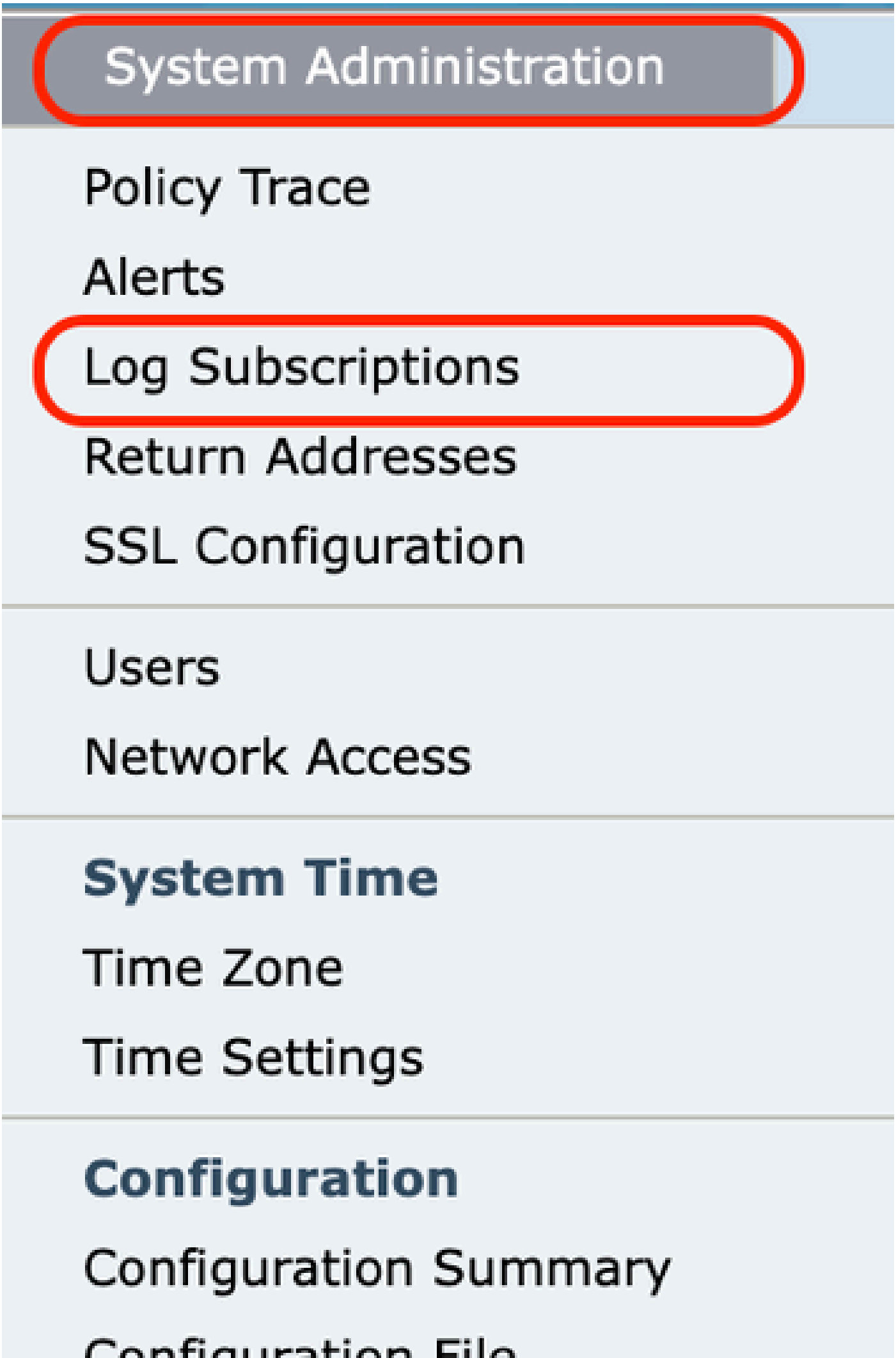
Criar log de acesso adicional

Em algumas condições, devido a políticas internas ou alguma outra configuração, não é possível alterar o Log de Acesso atual. Para superar essa limitação, você pode criar outros Logs de acesso e adicionar o parâmetro de Desempenho personalizado nos novos Logs de acesso.

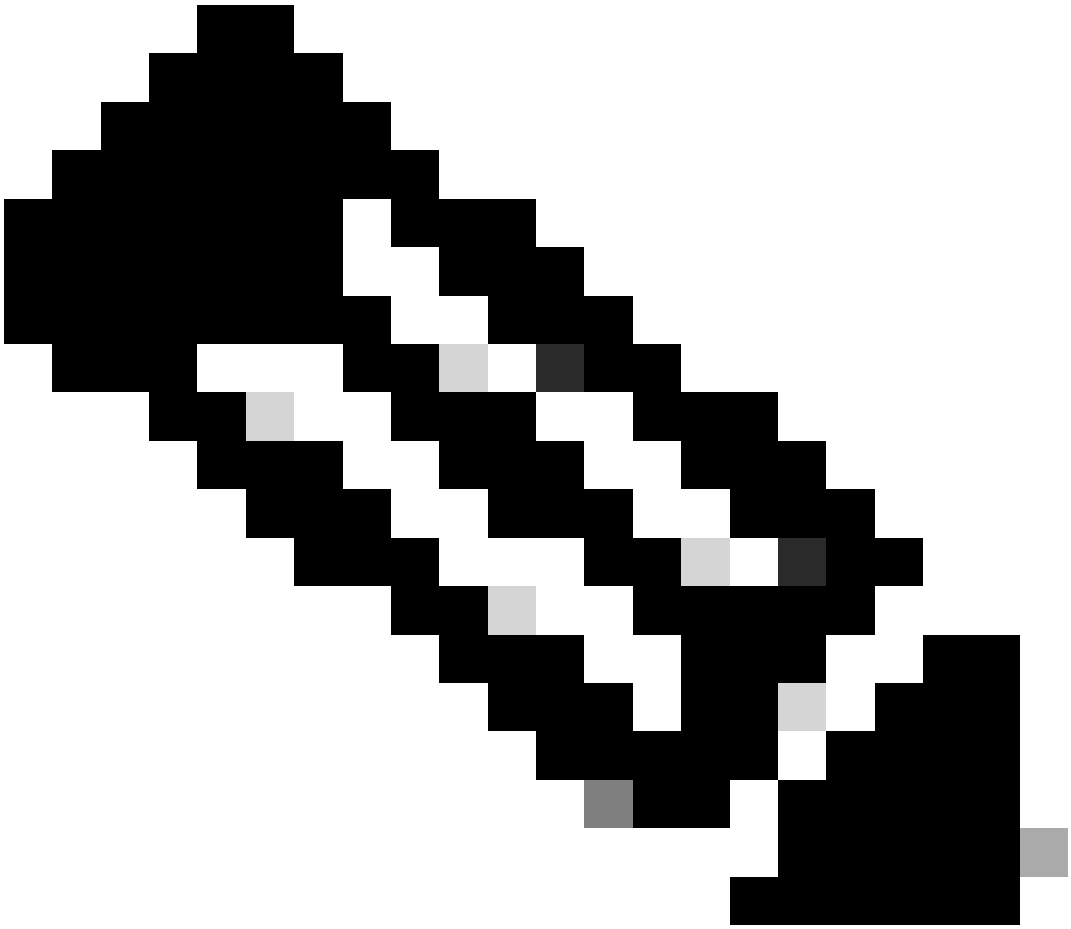
Criar novo log de acesso a partir da GUI

Etapa 1. Efetue login na GUI.

Etapa 2. No menu System Administration (Administração do sistema), escolha Log Subscriptions (Inscrições de log).


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

Insira um valor entre 102400 (100 Kilobytes) e 10737418240 (10 Gigabytes) para o tamanho do arquivo (em bytes) antes de atribuir funções SWA no log para um novo arquivo. O número deve ser um inteiro e você pode adicionar M para indicar o tamanho em megabyte, K para indicar o tamanho do arquivo em kilobyte e G para gigabyte.



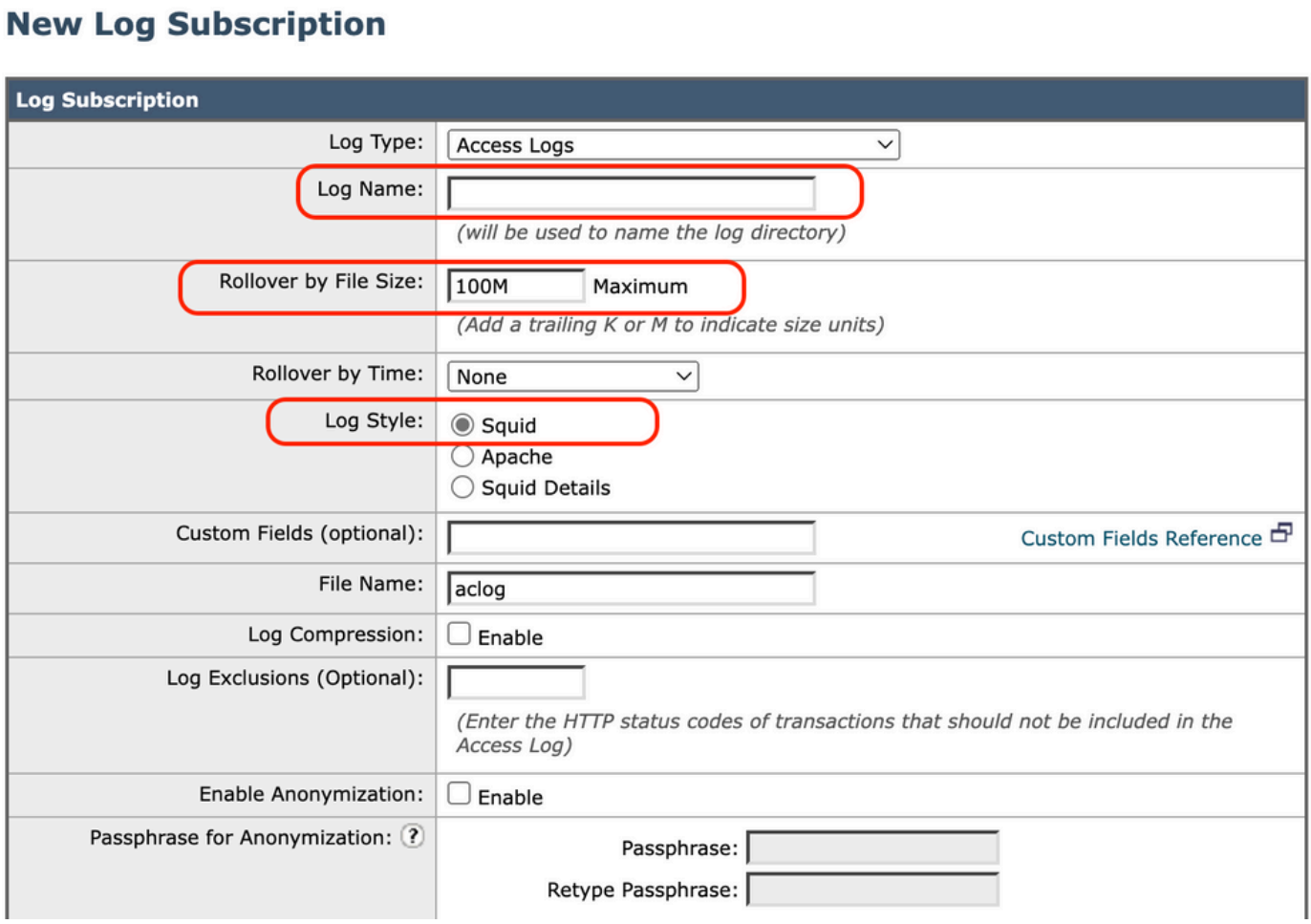
> Note: O SWA arquiva (faz rollover) as assinaturas de log quando um arquivo de log atual atinge um limite especificado pelo usuário de tamanho máximo de arquivo ou tempo máximo desde a última rollover.

Etapa 7. Escolha Squid para o estilo de log.

Etapa 8. O Nome do Arquivo é usado para definir o nome da Pasta e o nome do arquivo de log para este novo log. Recomenda-se que seja igual ao nome do log, que neste exemplo, era TAC_access_logs.

Etapa 9. Você pode Ativar a compactação de log para compactar o arquivo de log ou manter os logs como um arquivo de texto.

Etapa 10. A Exclusão do Log é filtrar o código de resposta do protocolo HTTP. Não filtrar códigos de Status HTTP.



Preencha os campos obrigatórios

Etapa 11. Escolha FTP poll para manter os logs no SWA. Digite 1 e pressione Enter.

Etapa 12. Enviar e confirmar as alterações.

Configurar novo log de acesso a partir da CLI

Etapa 1. Faça login na CLI.

Etapa 2. Execute logconfig.

Etapa 3. Para criar um novo log, digite New e pressione Enter.

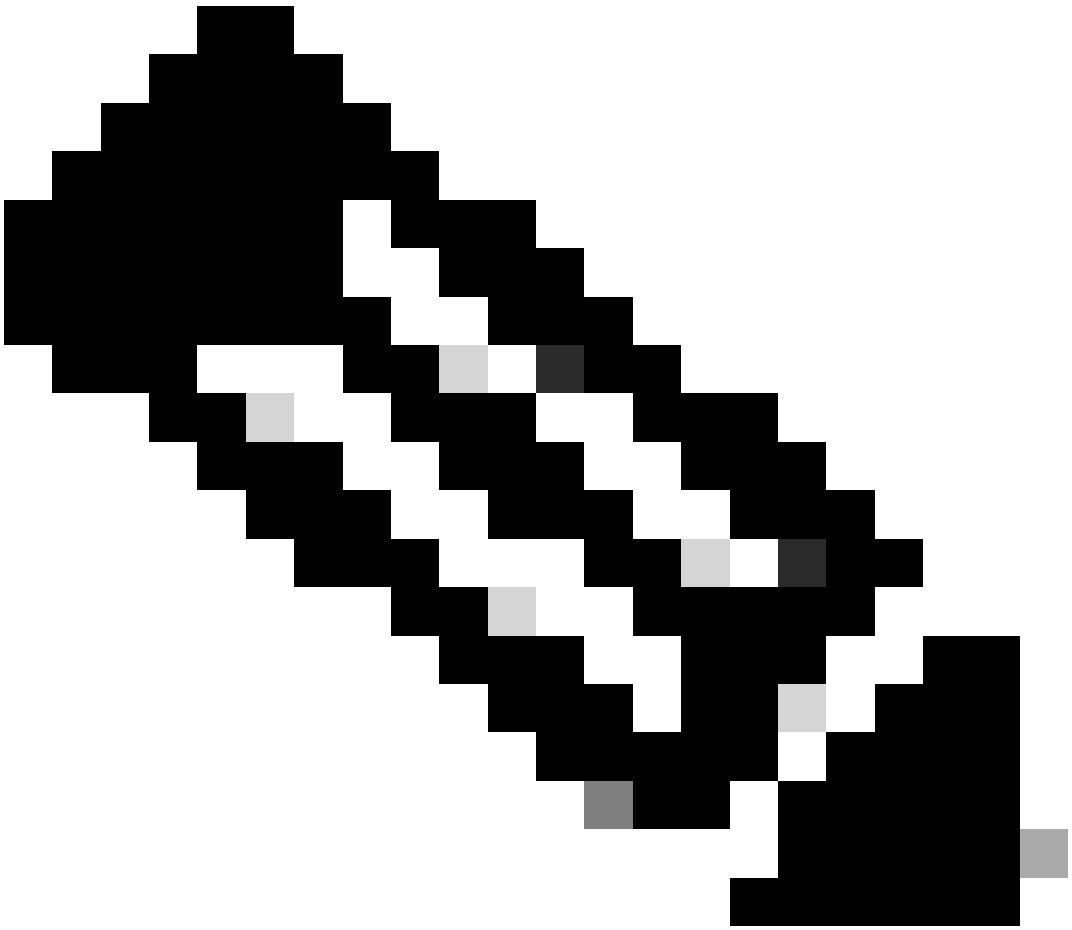
Etapa 4. Localize os Logs de Acesso na lista, digite o número associado a ele e pressione Enter.

Etapa 5. Digite um nome para o novo Log.

Etapa 6. Digite 1 para escolher Squid para o estilo de log desta assinatura e pressione Enter.

Etapa 7. Não filtre os códigos de Status de Erro HTTP. Pressione Enter para navegar até a próxima etapa.

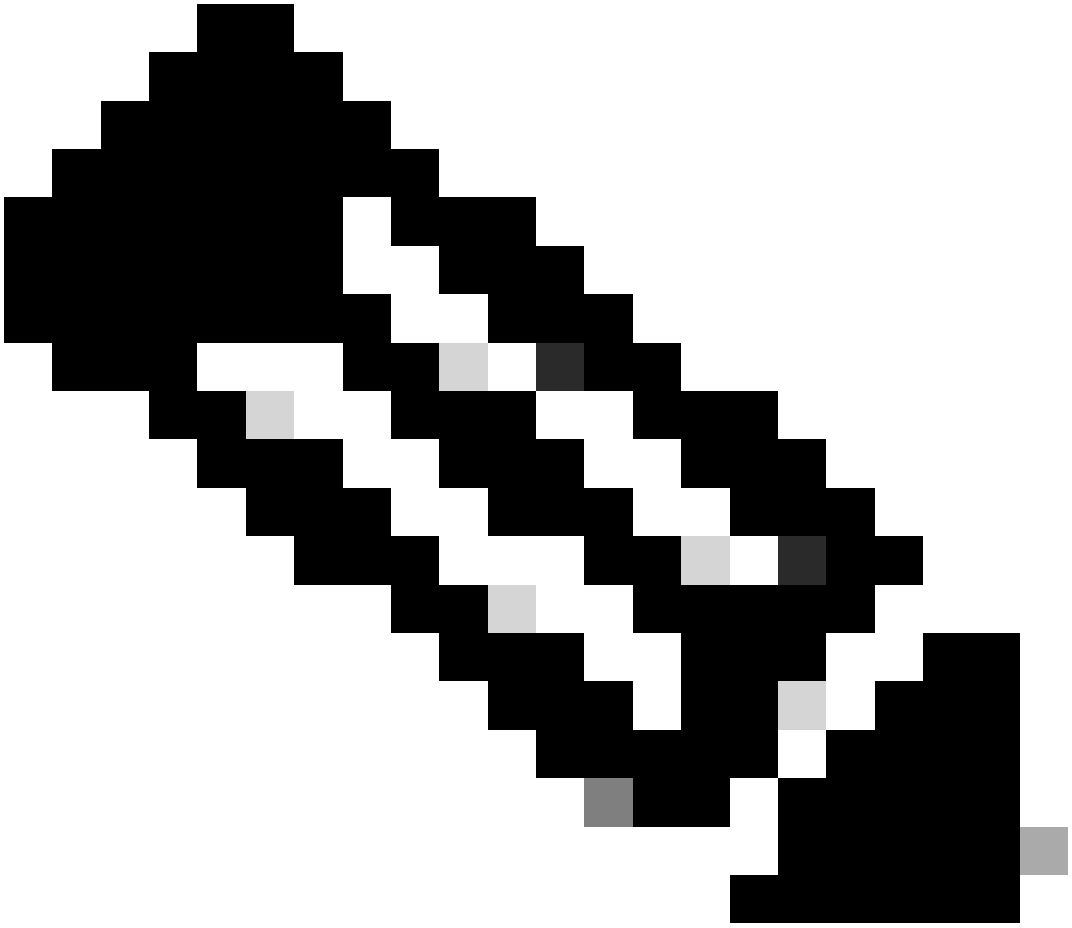
Etapa 8. Escolha FTP poll para manter os logs no SWA. Digite 1 e pressione Enter.



Note: Para enviar os logs para o servidor FTP, o servidor SCP ou o servidor Syslog. Você pode escolher opções relacionadas a elas.

Etapa 9. Esta etapa é para definir o nome da pasta e o nome do arquivo para o novo log. É melhor ser igual ao nome do log e pressionar Enter.

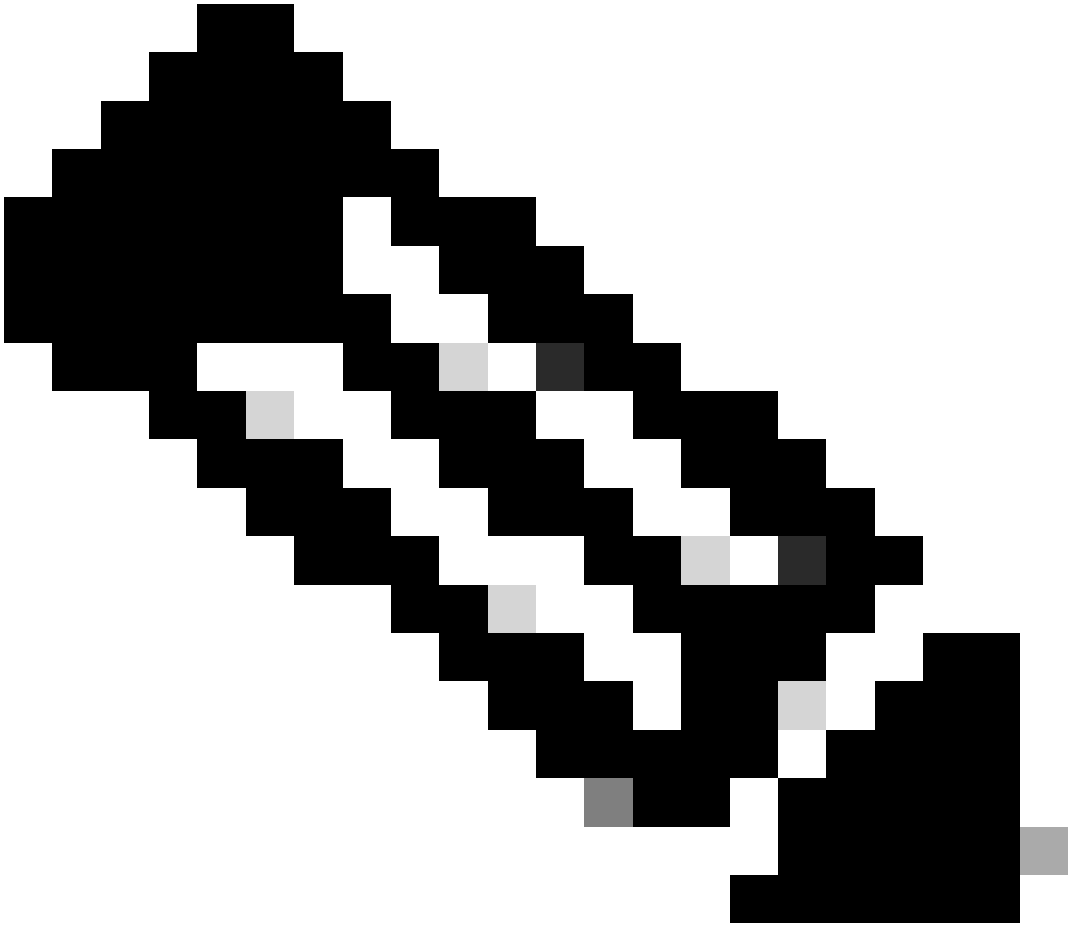
Etapa 10. Insira um valor entre 102400 (100 Kilobytes) e 10737418240 (10 Gigabytes) para o tamanho do arquivo (em bytes) antes da função SWA sobre o log para um novo arquivo.



Note: O SWA arquiva (faz rollover) as assinaturas de log quando um arquivo de log atual atinge um limite especificado pelo usuário de tamanho máximo de arquivo ou tempo máximo desde a última rollover.

Etapa 11. O número máximo de arquivos indica o número de arquivos de log armazenados no dispositivo. Se o número total de arquivos de log atingir esse valor, os logs mais antigos serão excluídos do SWA. O valor padrão é 10 arquivos e você pode digitar o número de logs, devido ao espaço em disco disponível e a outras configurações de logs, e pressionar Enter.

Etapa 12. Nesta etapa, você pode optar por compactar os logs ou mantê-los como um arquivo de texto. Digite Y para Yes e N para No e pressione Enter.



Note: Depois que o tamanho do arquivo atingiu o tamanho máximo, ele foi compactado. A taxa de compactação depende do comportamento do tráfego de rede e pode variar entre os arquivos de log.

Etapa 13. Pressione Enter para sair do assistente de configuração de log.

Etapa 14. Digite commit para salvar as alterações.

```
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
```

Adicionar Campos Personalizados para Parâmetro de Desempenho aos Logs de Acesso

Etapa 1. Efetue login na GUI.

Etapa 2. No menu System Administration (Administração do sistema), escolha Log Subscriptions (Inscrições de log).

Etapa 3. Na coluna Nome do Log, clique em accesslogs ou no nome do recém-criado. Neste exemplo, TAC_access_logs.

Etapa 4. Na seção Campos personalizados, cole esta cadeia de caracteres:

```
[ 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 = %
```

Etapa 5. Enviar e confirmar as alterações.

Verifique as alterações

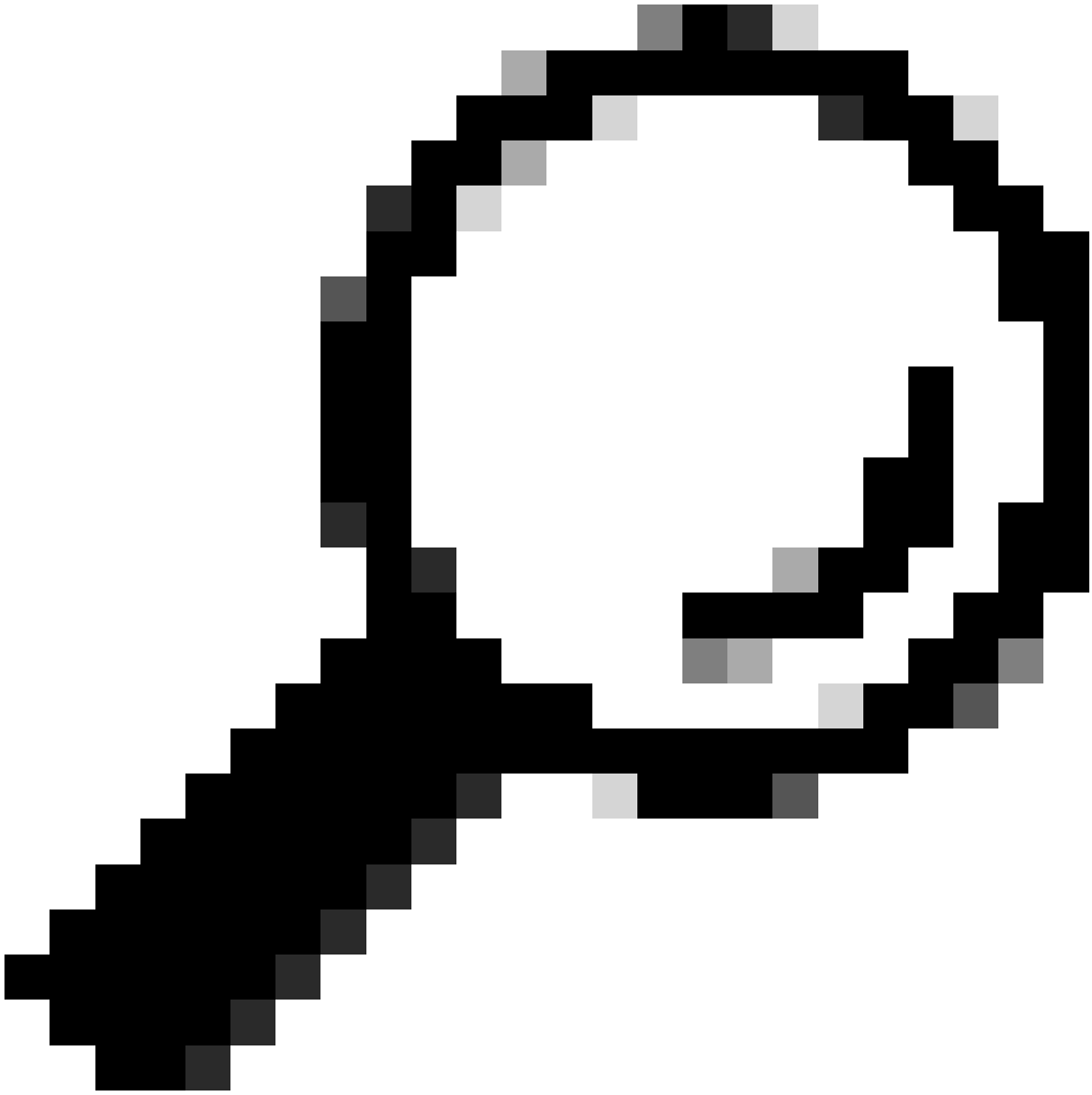
Etapa 1. Faça login na CLI.

Etapa 2. Digite tail e pressione enter.

Etapa 3. Localize o número associado aos Logs de acesso que adicionaram o Parâmetro de Desempenho. Digite o número e pressione Enter.

Você pode ver que há informações adicionais adicionadas aos Logs de acesso, como neste exemplo.

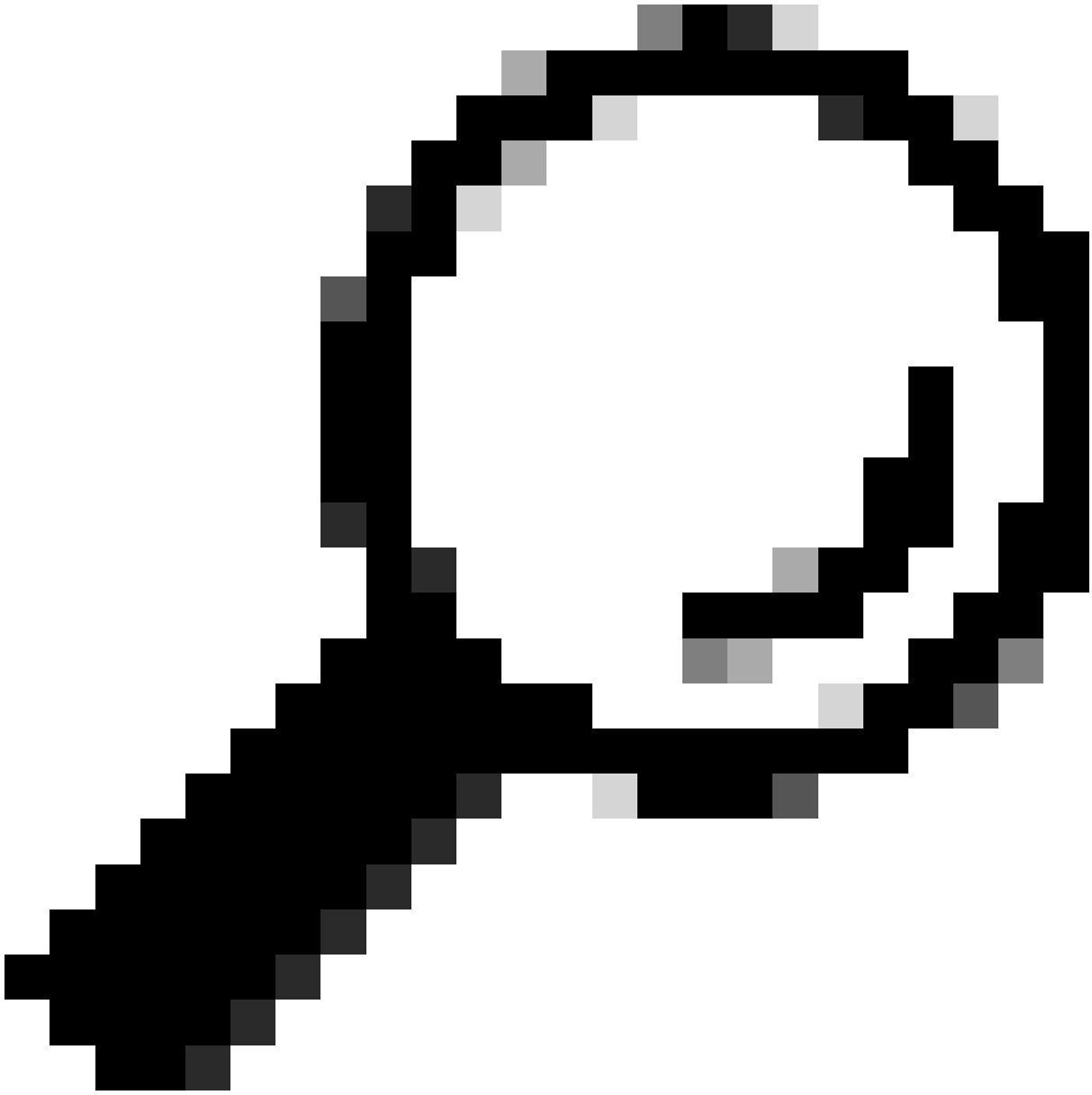
```
1680893872.492 1131 172.18.122.156 TCP_MISS/200 379725 GET http://www.cisco.com/en/US/docs/security/wsa

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



Tip: Você pode sair do comando tail mantendo a tecla Control pressionada e pressionando C. Se isso não tiver saído do comando tail, digite q.

Campos Descrição em Campos Personalizados

Os valores usados no campo Parâmetro de desempenho personalizado são mapeados para estas informações:



Tip: Latência = AMP total + Anti-Spyware total + Webroot total + Sophos total + McAfee total + AVC total + WBRS total + Auth total

Nome do campo personalizado	Campo Personalizado	Descrição
Cabeçalho da solicitação	%:<h	Tempo de espera para gravar cabeçalho de solicitação no servidor após o primeiro byte.
Solicitação ao servidor	%:<b	Tempo de espera para gravar corpo de solicitação no servidor após cabeçalho.
1º byte para o cliente	%:1>	Tempo de espera para o primeiro byte gravado no cliente.

Corpo do cliente	%:b>	Tempo de espera para a gravação completa do corpo no cliente.
Tempo de Espera de Rx (em ms): 1º byte de solicitação	%:1<	O tempo que leva do momento em que o Web Proxy começa a se conectar ao servidor até o momento em que é capaz de gravar primeiro no servidor. Se o Web Proxy tiver que se conectar a vários servidores para concluir a transação, será a soma desses horários.
Cabeçalho da solicitação	%:h<	Tempo de espera para cabeçalho completo do cliente após o primeiro byte.
Corpo do cliente	%:b<	Tempo de espera para completar o corpo do cliente.
1º byte de resposta	%:>1	Tempo de espera para o primeiro byte de resposta do servidor.
Cabeçalho de resposta	%:>h	Tempo de espera para o cabeçalho do servidor após o primeiro byte de resposta.
Resposta do servidor	%:>b	Isso significa basicamente que o SWA obteve cabeçalhos HTTP do servidor, mas o SWA espera pelos bytes de resposta depois disso e qual seria o conteúdo real do servidor.
Cache de disco	%:>c	Tempo necessário para que o Web Proxy leia uma resposta do cache de disco.
Resposta de autenticação	%:<a	Tempo de espera para receber a resposta do processo de autenticação do Web Proxy depois que o Web Proxy enviou a solicitação.
Total de autenticação	%:>a	O tempo de espera para receber a resposta do processo de autenticação do Web Proxy inclui o tempo necessário para que o Web Proxy envie a solicitação.
resposta DNS	%:<d	Tempo gasto pelo Web Proxy para enviar a solicitação de DNS (Domain Name Request) ao processo DNS do Web Proxy.

Total de DNS	%:>d	Tempo gasto pelo processo DNS do Web Proxy para enviar de volta um resultado DNS ao Web Proxy.
resposta WBRS	%:<r	Tempo de espera para receber a resposta dos Filtros do Web Reputation depois que o Web Proxy enviou a solicitação.
Total de WBRS	%:>r	O tempo de espera para receber o veredito dos Filtros de Reputação da Web inclui o tempo necessário para que o Web Proxy envie a solicitação.
resposta AVC	%:A>	Tempo de espera para receber a resposta do processo de visibilidade e controle de aplicativos (AVC), depois que o Web Proxy enviou a solicitação.
Total AVC	%:A<	O tempo de espera para receber a resposta do processo AVC inclui o tempo necessário para que o Web Proxy envie a solicitação.
resposta de DCA	%:C>	Tempo de espera para receber a resposta do mecanismo de Análise de Conteúdo Dinâmico, depois que o Web Proxy enviou a solicitação.
Total de DCA	%:C<	O tempo de espera para receber o veredito do mecanismo de análise de conteúdo dinâmico inclui o tempo necessário para que o Web Proxy envie a solicitação.
resposta da McAfee	%:m>	Tempo de espera para receber a resposta do mecanismo de varredura da McAfee depois que o Web Proxy enviou a solicitação.
Total da McAfee	%:m<	O tempo de espera para receber o veredito do mecanismo de varredura da McAfee inclui o tempo necessário para que o Web Proxy envie a solicitação.
resposta Sophos	%:p>	Tempo de espera para receber a resposta do mecanismo de verificação Sophos depois que o Web Proxy enviou a solicitação.

Total do Sophos	%:p<	O tempo de espera para receber o veredito do mecanismo de verificação Sophos inclui o tempo necessário para que o Web Proxy envie a solicitação.
resposta AMP	%:e>	Tempo de espera para receber a resposta do mecanismo AMP, depois que o Web Proxy enviou a solicitação.
Total da AMP	%:e<	O tempo de espera para receber o veredito do mecanismo AMP inclui o tempo necessário para que o Web Proxy envie a solicitação.
Latência	% x; % L	Latência e Hora local da solicitação em formato legível por humanos: DD/MMM/AAAA: hh:mm:ss +nnnn. Esse campo é gravado com aspas duplas nos logs de acesso. Esse campo permite que você correlacione logs a problemas sem ter que calcular a hora local da época para cada entrada de log.
Porta do cliente	% F	Número de porta usado do lado do cliente.
Endereço IP do servidor	% k	Endereço IP do servidor da Web.
Número da porta do servidor	% p	Número da porta do servidor Web.

Informações Relacionadas

- Guia do usuário do AsyncOS 14.5 para Cisco Secure Web Appliance - GD (General Deployment) - Cisco
- Diretrizes de práticas recomendadas do Cisco Web Security Appliance - Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.