Configurar el parámetro de rendimiento en registros de acceso

Contenido

Introducción

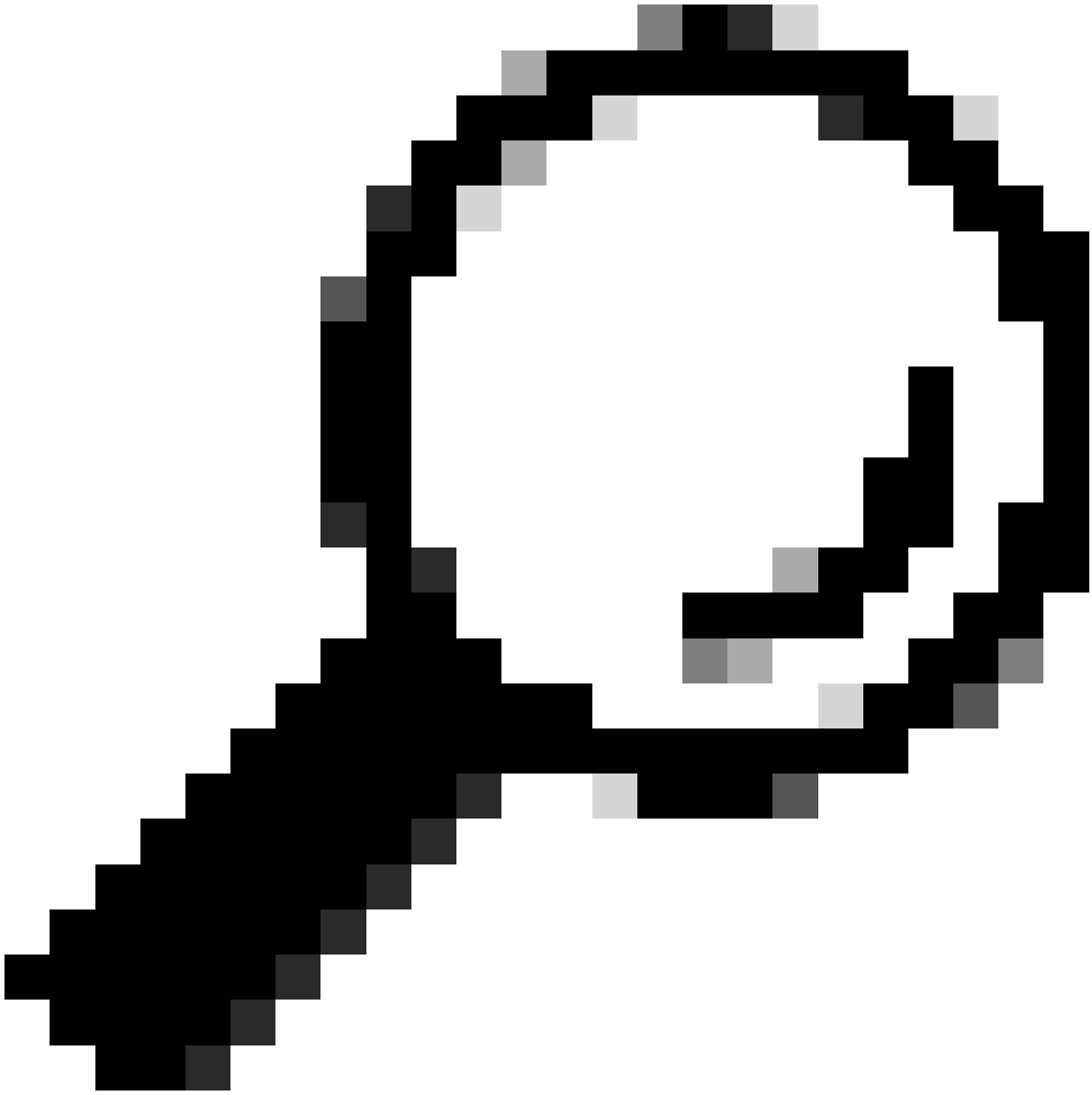
Este documento describe los pasos para agregar el campo personalizado de parámetro de rendimiento al registro de acceso de Secure Web Appliance (SWA).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Acceso mediante protocolo de shell seguro (SSH) a la interfaz de gestión de SWA.
- Acceso mediante la interfaz gráfica de usuario (GUI) a la interfaz de gestión de SWA.



Consejo: Es mejor tener más del 20% de espacio libre en disco en la partición de datos SWA. Puede comprobar el uso del disco desde la interfaz de línea de comandos (CLI) en la salida del comando status detail.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Cuando hay un problema de latencia y el tráfico es procesado a través de un SWA, los Access Logs pueden ser útiles para resolver la causa raíz de la latencia. Puede cambiar la configuración actual de Access Logs o crear nuevos Access Logs con parámetros de rendimiento agregados al campo personalizado.

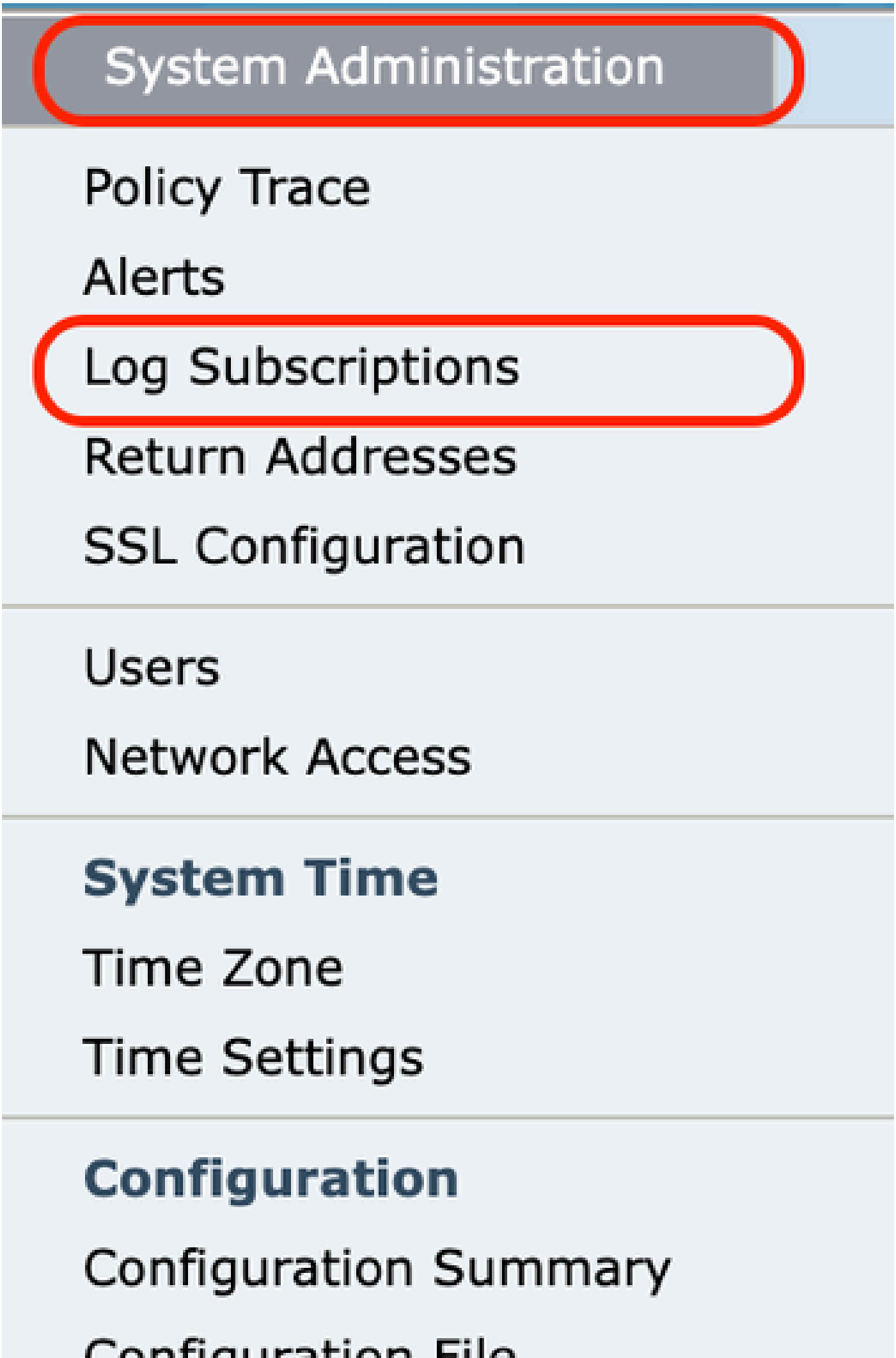
Crear registro de acceso adicional

En algunas condiciones, debido a las políticas internas o a alguna otra configuración, no es posible realizar cambios en el registro de acceso actual. Para superar esta limitación, puede crear otros registros de acceso y agregar el parámetro de rendimiento personalizado en los nuevos registros de acceso.

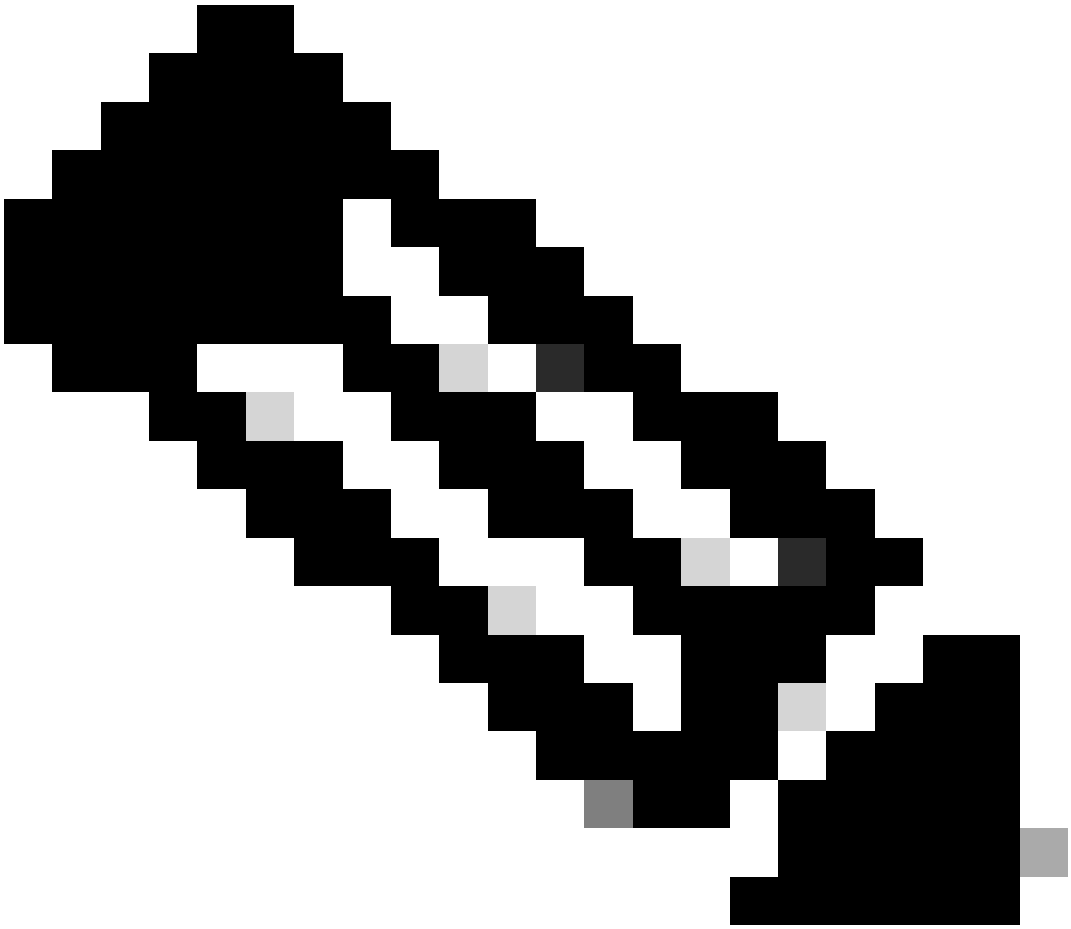
Crear nuevo registro de acceso desde la GUI

Paso 1. Inicie sesión en la GUI.

Paso 2. En el menú Administración del sistema, elija Registrar suscripciones.


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

Introduzca un valor entre 102400 (100 Kilobytes) y 10737418240 (10 Gigabytes) para el tamaño del archivo (en bytes) antes de que las funciones SWA pasen del registro a un nuevo archivo. El número debe ser un número entero, y puede agregar M para indicar el tamaño en Megabyte, K para indicar el tamaño del archivo en kilobyte y G para gigabyte.



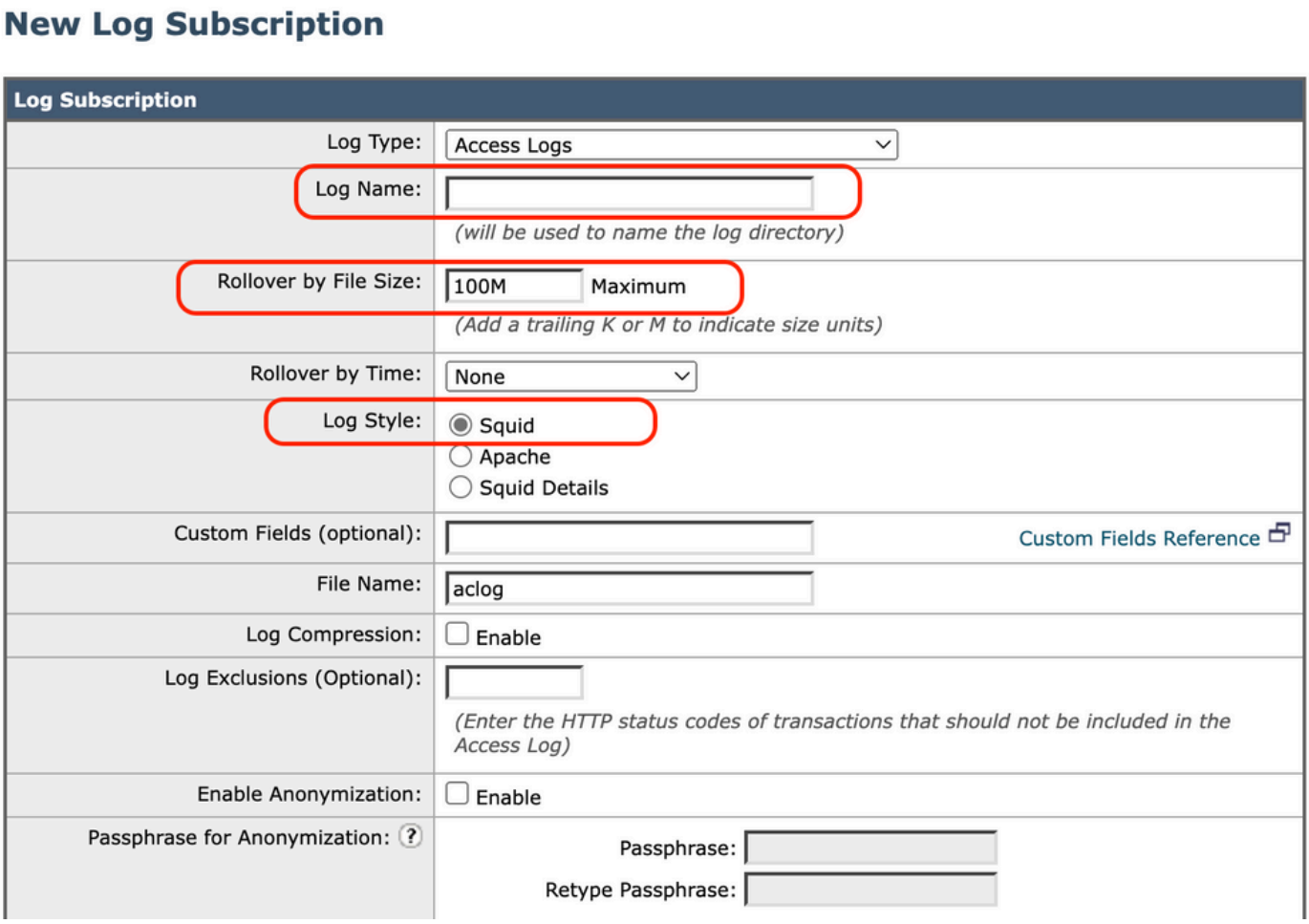
> Nota: SWA archiva (revierte) las suscripciones de registro cuando un archivo de registro actual alcanza un límite especificado por el usuario de tamaño máximo de archivo, o el tiempo máximo desde la última reversión.

Paso 7. Elija Squid para el estilo de registro.

Paso 8. El nombre de archivo es para definir el nombre de la carpeta y el nombre del archivo de registro para este nuevo registro. Se recomienda que sea el mismo que el nombre de registro, que en este ejemplo, era TAC_access_logs.

Paso 9. Puede Habilitar la compresión de registros para comprimir el archivo de registro o mantener los registros como un archivo de texto.

Paso 10. La exclusión del registro consiste en filtrar el código de respuesta del Protocolo de transferencia de hipertexto (HTTP). No filtre los códigos de estado HTTP.



Rellene los campos obligatorios

Paso 11. Elija FTP poll para mantener los registros en el SWA. Escriba 1 y presione Enter.

Paso 12. Envíe y confirme los cambios.

Configurar nuevo registro de acceso desde CLI

Paso 1. Inicie sesión en CLI.

Paso 2. Ejecute logconfig.

Paso 3. Para crear un nuevo registro, escriba Nuevo y presione Intro.

Paso 4. Busque Registros de acceso en la lista, escriba el número asociado a ese registro y presione Intro.

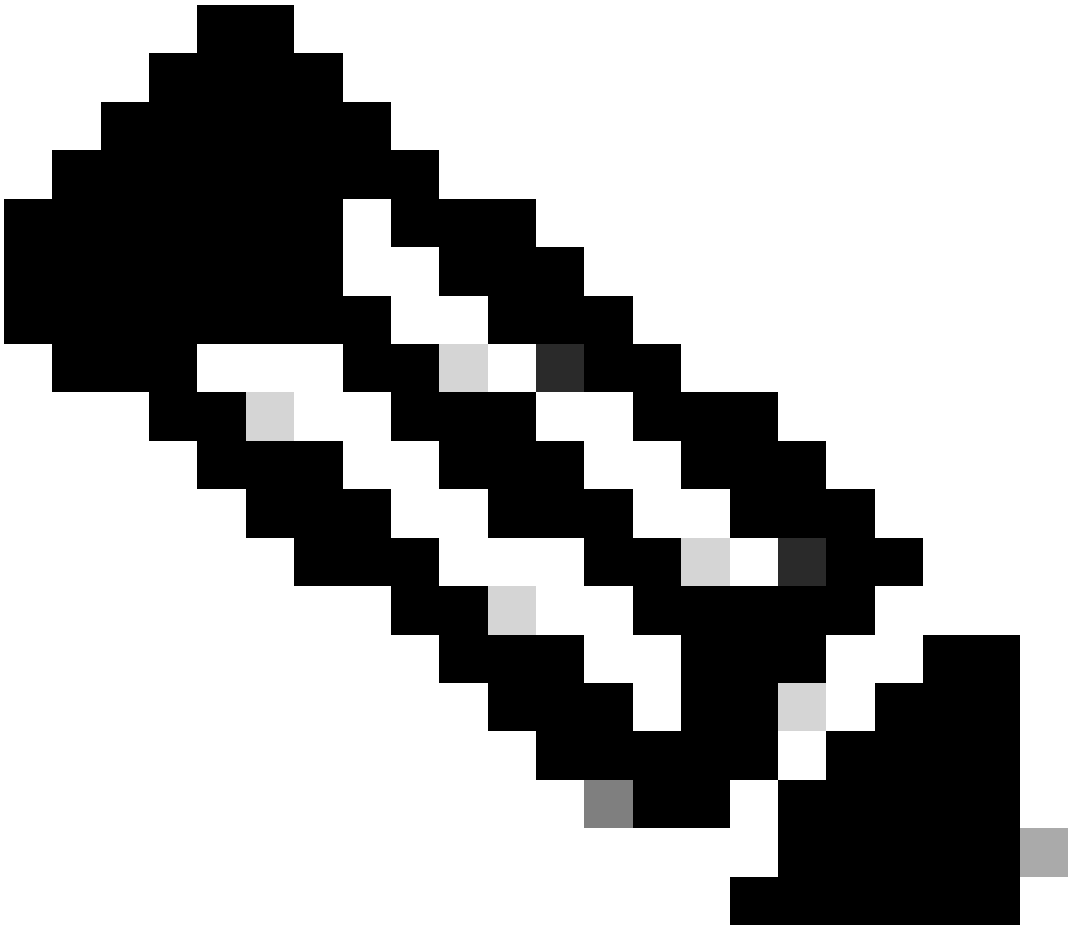
Paso 5. Escriba un nombre para el nuevo registro.

Paso 6. Escriba 1 para elegir Squid para el estilo de registro de esta suscripción y presione Intro.

Paso 7. No filtre los códigos de estado de error de HTTP. Presione Intro para desplazarse al

siguiente paso.

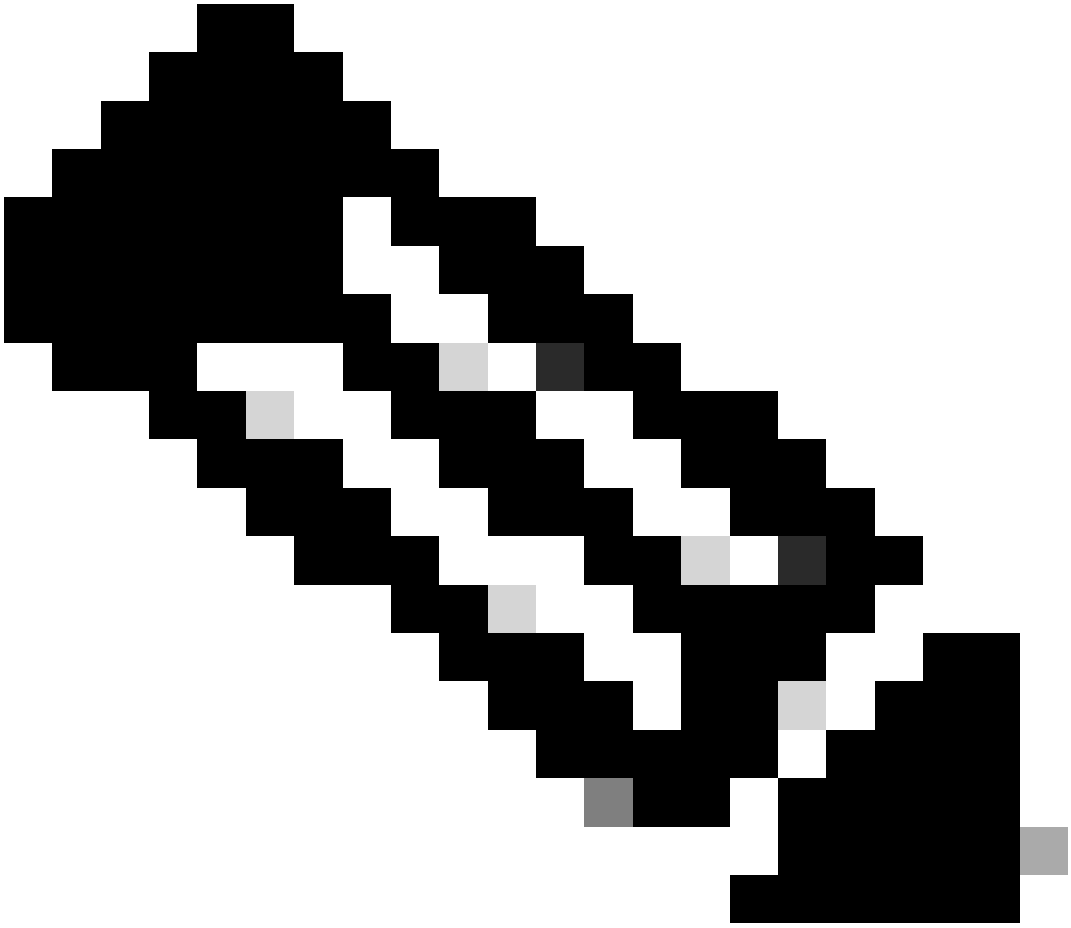
Paso 8. Elija sondeo FTP para mantener los registros en el SWA. Escriba 1 y presione Enter.



Nota: Para enviar los registros al servidor FTP (File Transfer Protocol), al servidor SCP (Secure Copy Protocol) o al servidor Syslog. Puede elegir opciones relacionadas con ellos.

Paso 9. Este paso consiste en definir el nombre de carpeta y el nombre de archivo para el nuevo registro. Es mejor que sea el mismo que el nombre del registro y presione Enter.

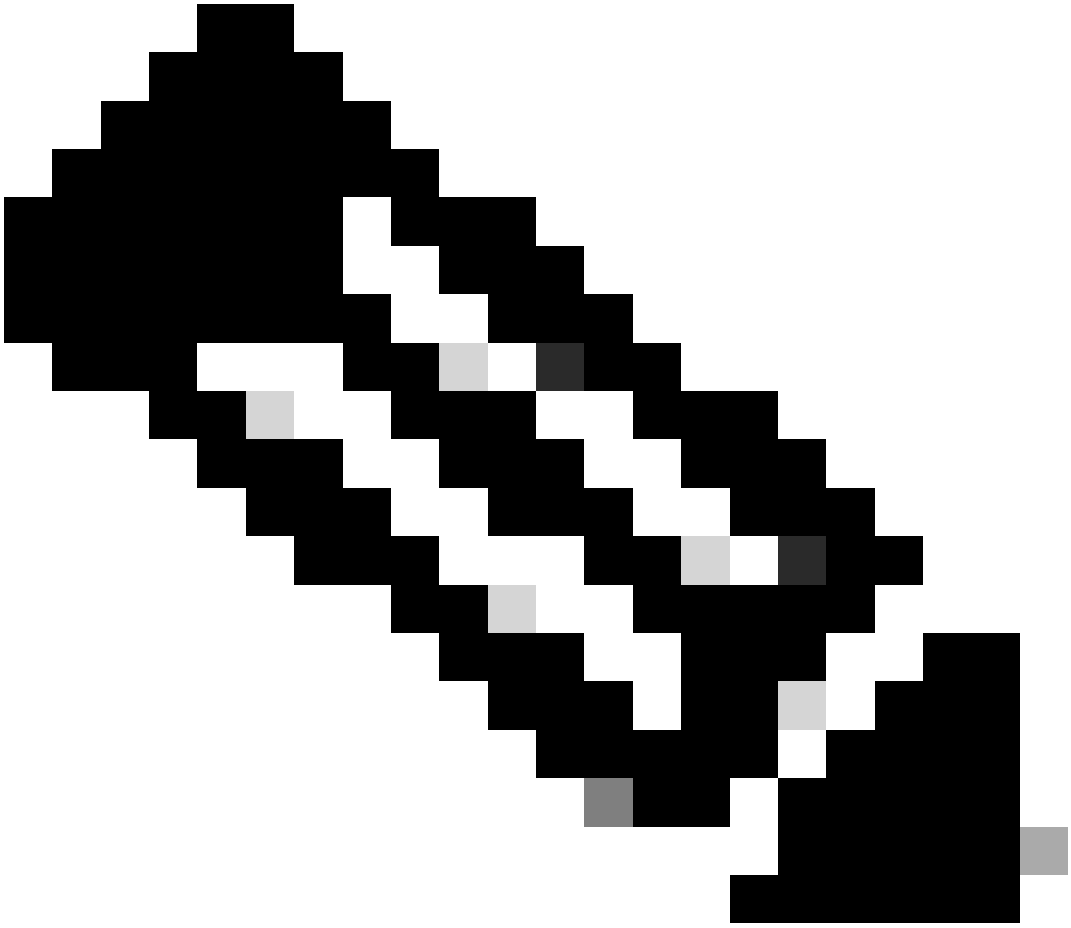
Paso 10. Introduzca un valor entre 102400 (100 Kilobytes) y 10737418240 (10 Gigabytes) para el tamaño del archivo (en bytes) antes de la función SWA sobre el registro a un nuevo archivo.



Nota: SWA archiva (revierte) las suscripciones de registro cuando un archivo de registro actual alcanza un límite especificado por el usuario de tamaño máximo de archivo, o el tiempo máximo desde la última reversión.

Paso 11. Número máximo de archivos indica el número de archivos de registro almacenados en el dispositivo. Si el número total de archivos de registro alcanza este valor, los registros más antiguos se eliminan de SWA. El valor predeterminado es 10 archivos y puede escribir el número de registros, debido al espacio en disco disponible y a la configuración de otros registros, y luego presionar Enter.

Paso 12. En este paso, puede optar por comprimir los registros o conservarlos como archivo de texto. Escriba Y para Yes y N para No y presione Enter.



Nota: Después de que el tamaño del archivo alcanzó el tamaño máximo, se comprime. La relación de compresión depende del comportamiento del tráfico de red y puede variar entre los archivos de registro.

Paso 13. Presione Intro para salir del asistente de configuración de registro.

Paso 14. Escriba commit para guardar los cambios.

```
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
```

Agregar campos personalizados para parámetros de rendimiento a registros de acceso

Paso 1. Inicie sesión en la GUI.

Paso 2. En el menú Administración del sistema, elija Registrar suscripciones.

Paso 3. En la columna Nombre del Log, haga clic en accesslogs o en el nombre del recién creado. En este ejemplo, TAC_access_logs.

Paso 4. En la sección Campos personalizados, pegue esta cadena:

```
[ 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 = %
```

Paso 5. Envíe y confirme los cambios.

Verificar los cambios

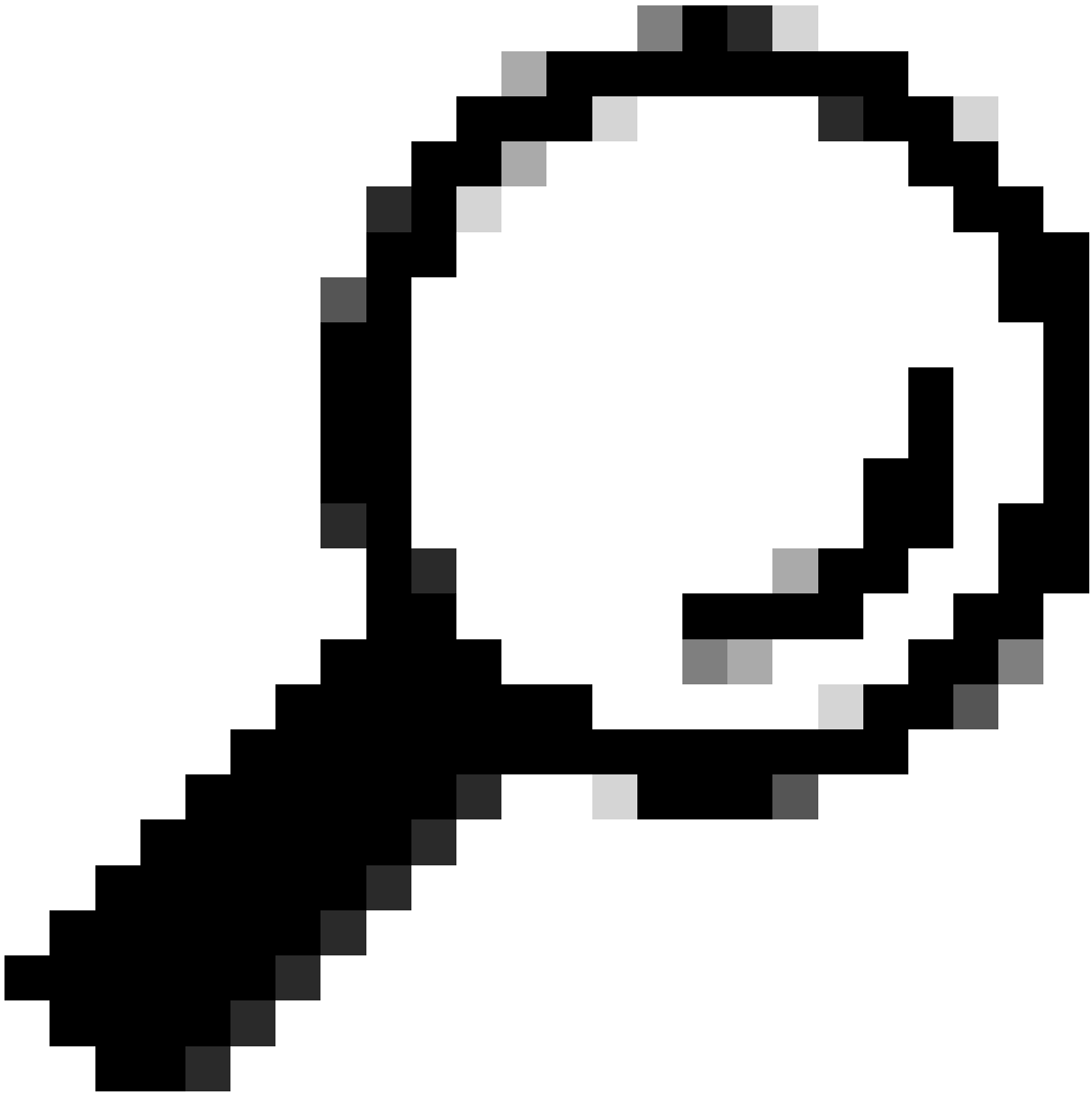
Paso 1. Inicie sesión en CLI.

Paso 2. Escriba tail y presione Enter.

Paso 3. Busque el número asociado a los registros de acceso que agregaron el parámetro de rendimiento. Escriba el número y pulse Intro.

Puede ver que hay información adicional agregada a los registros de acceso, igual que en este ejemplo.

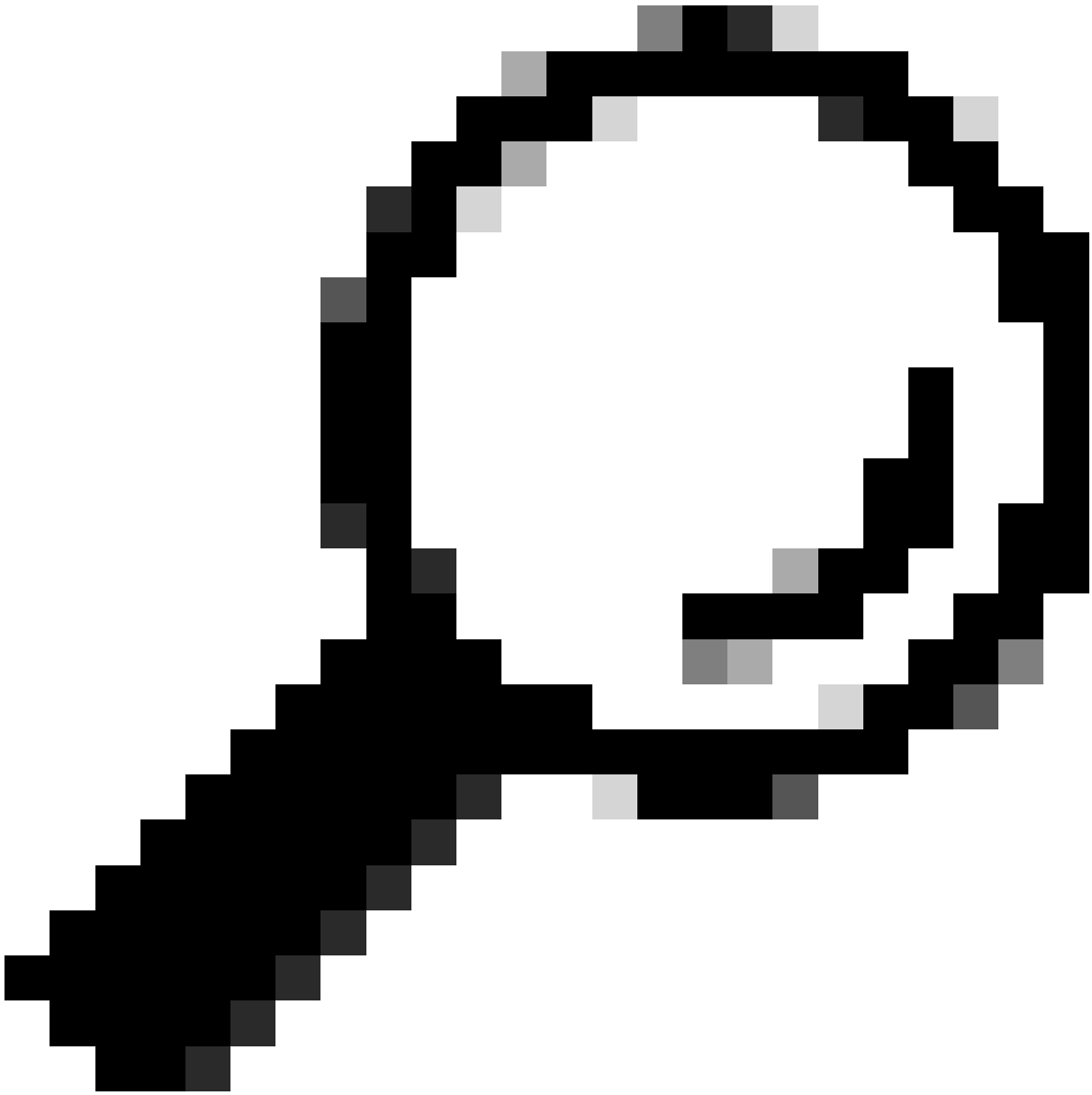
```
1680893872.492 1131 172.18.122.156 TCP_MISS/200 379725 GET http://www.cisco.com/en/US/docs/security/wsa/

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



Consejo: Puede salir del comando tail cuando mantenga presionada la tecla Control y presione C. Si eso no salió del comando tail, escriba q.

Descripción de campos en campos personalizados

Los valores utilizados en el campo de parámetro de rendimiento personalizado se asignan a la siguiente información:



Consejo: Latencia = total de AMP + total de Anti-Spyware + total de Webroot + total de Sophos + total de McAfee + total de AVC + total de WBRS + total de autenticación

Nombre de campo personalizado	Campo personalizado	Descripción

Encabezado de solicitud	%:<h	Tiempo de espera para escribir el encabezado de solicitud en el servidor después del primer byte.
Solicitud al servidor	%:<b	Tiempo de espera para escribir el cuerpo de la solicitud en el servidor después del encabezado.
1er byte para el cliente	%:1>	Tiempo de espera para el primer byte escrito en el cliente.
Cuerpo del cliente	%:b>	Tiempo de espera para el cuerpo completo escrito al cliente.
Tiempos de espera Rx (en ms): 1er byte de solicitud	%:1<	El tiempo que tarda desde el momento en que el proxy web comienza a conectarse al servidor hasta el momento en que puede escribir por primera vez en el servidor. Si el proxy web tiene que conectarse a varios servidores para completar la transacción, es la suma de esas veces.
Encabezado de solicitud	%:h<	Tiempo de espera para el encabezado de cliente completo después del primer byte.
Cuerpo del cliente	%:b<	Tiempo de espera para el cuerpo completo del cliente.
1er byte de respuesta	%:>1	Tiempo de espera para el primer byte de respuesta del servidor.
Encabezado de respuesta	%:>h	Tiempo de espera para el encabezado del servidor después del primer byte de respuesta.
Respuesta del servidor	%:>b	Esto significa básicamente que SWA obtuvo encabezados HTTP del servidor, pero SWA espera los bytes de respuesta después de eso y cuál sería el contenido real del servidor.
Caché de disco	%:>c	Tiempo necesario para que el proxy web lea una respuesta de la caché de disco.
Respuesta de autenticación	%:<a	Tiempo de espera para recibir la respuesta del proceso de autenticación de proxy web, después de que el proxy web envió la solicitud.

Total de autenticación	%:>a	El tiempo de espera para recibir la respuesta del proceso de autenticación de proxy web incluye el tiempo necesario para que el proxy web envíe la solicitud.
respuesta DNS	%:<d	Tiempo que tarda el proxy web en enviar la solicitud de DNS (petición de nombre de dominio) al proceso DNS del proxy web.
Total de DNS	%:>d	Tiempo que tarda el proceso DNS del proxy web en devolver un resultado DNS al proxy web.
respuesta WBRS	%:<r	Tiempo de espera para recibir la respuesta de los filtros de reputación de Web, después de que el proxy de Web haya enviado la solicitud.
total de WBRS	%:>r	El tiempo de espera para recibir el veredicto de los filtros de reputación de Web incluye el tiempo necesario para que el proxy de Web envíe la solicitud.
respuesta AVC	%:A>	Tiempo de espera para recibir la respuesta del proceso de visibilidad y control de aplicaciones (AVC, Application Visibility and Control), después de que el proxy web haya enviado la solicitud.
Total de AVC	%:A<	El tiempo de espera para recibir la respuesta del proceso AVC incluye el tiempo necesario para que el proxy web envíe la solicitud.
respuesta DCA	%:C>	Tiempo de espera para recibir la respuesta del motor de análisis de contenido dinámico, después de que el proxy de web haya enviado la solicitud.
total de DCA	%:C<	El tiempo de espera para recibir el veredicto del motor de análisis de contenido dinámico incluye el tiempo necesario para que el proxy web envíe la solicitud.
respuesta de McAfee	%:m>	Tiempo de espera para recibir la respuesta del motor de exploración de McAfee, después de que el proxy de Web haya enviado la solicitud.

Total de McAfee	%:m<	El tiempo de espera para recibir el veredicto del motor de exploración de McAfee incluye el tiempo necesario para que el proxy web envíe la solicitud.
respuesta de Sophos	%:p>	Tiempo de espera para recibir la respuesta del motor de análisis de Sophos, después de que el proxy de Web enviara la solicitud.
Total de Sophos	%:p<	El tiempo de espera para recibir el veredicto del motor de análisis de Sophos incluye el tiempo necesario para que el proxy web envíe la solicitud.
respuesta de AMP	%:e>	Tiempo de espera para recibir la respuesta del motor de AMP, después de que el proxy web haya enviado la solicitud.
total de AMP	%:e<	El tiempo de espera para recibir el veredicto del motor de AMP incluye el tiempo necesario para que el proxy web envíe la solicitud.
Latencia	%x; %L	Latencia y solicitud de hora local en formato legible por las personas: DD/MMM/AAAA: hh:mm:ss +nnnn. Este campo se escribe con comillas dobles en los registros de acceso. Este campo permite correlacionar registros con problemas sin tener que calcular la hora local de cada época para cada entrada de registro.
Puerto del cliente	%F	Número de puerto utilizado desde el lado del cliente.
Dirección IP del servidor	%k	Dirección IP del servidor Web.
Número de puerto del servidor	%p	Número de puerto del servidor web.

Información Relacionada

- Guía del usuario de AsyncOS 14.5 para Cisco Secure Web Appliance - GD (implementación general) - Cisco
- Directrices sobre prácticas recomendadas de Cisco Web Security Appliance: Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).