Configurar registros de depuración de solicitudes en el dispositivo web seguro

Contenido

Introducción

Este documento describe los pasos para Solicitar registros de depuración en Secure Web Appliance (SWA).

Prerequisites

Requirements

Cisco recomienda conocer estos temas:

- Acceso administrativo a la interfaz de línea de comandos (CLI) de SWA.

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.

Solicitar registros de depuración

Los registros de depuración de solicitud en SWA son un tipo de registro especializado diseñado para capturar información extremadamente detallada, de depuración de extremo a extremo y hasta el nivel de seguimiento para una transacción HTTP o HTTPS específica o una máquina cliente. A diferencia de los registros de proxy estándar que registran eventos resumidos en muchas solicitudes, los registros de depuración de solicitud agregan la salida de depuración de todos los módulos de proxy web implicados en el procesamiento de una solicitud concreta (como la autenticación, el filtrado de URL, el descifrado, el análisis de malware y los servicios de reputación) en un flujo de registro correlacionado. Este tipo de registro está destinado exclusivamente a diagnósticos detallados y solo se puede crear a través de la CLI, no a través de la GUI

Los registros de depuración de solicitudes son esenciales cuando se solucionan problemas de proxy complejos o intermitentes en los que los registros estándar carecen de detalles suficientes. Permiten a los administradores y al TAC de Cisco rastrear exactamente cómo se gestionó una única solicitud en cada etapa de procesamiento, lo que permite identificar las causas principales, como coincidencias de políticas inesperadas, retrasos en el análisis, fallos de autenticación o veredictos incoherentes entre motores. Dado que el registro se centra en una transacción, proporciona la máxima visibilidad sin la sobrecarga operativa y el impacto en el rendimiento de habilitar el registro de depuración en todos los módulos proxy de todo el sistema. Esto convierte a los registros de depuración de solicitudes en una herramienta de diagnóstico precisa, eficaz y de bajo riesgo durante las investigaciones avanzadas.

Configuración de los Registros de Depuración de Solicitudes

Paso 1. Inicie sesión en CLI, ejecute logconfig y elija new.

Paso 2. Seleccione el número asociado a Solicitar registros de depuración y presione Intro.

Paso 3. Introduzca el nombre del registro.

Paso 4. Elija Trace como nivel de registro.

Paso 5. Seleccione los módulos que desee para recopilar el registro mejorado. Se pueden realizar varias selecciones en forma de una lista de rangos o una lista separada por comas (como 1,3,4 o 3-7).

Consejo: Si el TAC no solicita ningún módulo específico, es mejor seleccionar todos los módulos (como 1-30).

Paso 6. Especifique el número de solicitudes para las que se activará el registro mejorado. Una vez que se ha capturado este número de solicitudes, el registro se detiene automáticamente.

Nota: Es importante seleccionar un valor razonable basado en las condiciones del tráfico durante la resolución de problemas. Por ejemplo, si se está utilizando un equipo de prueba dedicado y el tráfico en segundo plano es mínimo, es suficiente con un número menor de solicitudes. Sin embargo, en entornos con mayor actividad en segundo plano (como actualizaciones del sistema operativo, solicitudes en segundo plano del navegador o aplicaciones como Webex), la elección de un valor superior garantiza que se capture la transacción correspondiente.

Paso 7. Defina los criterios de coincidencia de solicitud para el registro mejorado seleccionando la dirección IP del cliente, la dirección IP de destino o el dominio de destino.

Nota: En la mayoría de los casos, se recomienda seleccionar la dirección IP del cliente, incluso cuando se soluciona el problema de acceso a un único sitio web. Este enfoque garantiza que se capturan todas las solicitudes web generadas durante la carga de la página, incluidas las solicitudes en segundo plano a direcciones URL adicionales que posiblemente no sean visibles inmediatamente. Sin embargo, este método es más eficaz cuando se utiliza un equipo de prueba dedicado con un tráfico de Internet en segundo plano mínimo. En entornos en los que el cliente genera un tráfico adicional significativo (como actualizaciones del sistema operativo, servicios en segundo plano del navegador o aplicaciones como Webex), es mejor filtrar por dominio de destino o dirección IP de destino.

Consejo: Si se desconoce el punto exacto de la falla, los registros HAR del navegador se pueden recopilar para identificar la URL o el dominio específico que presenta problemas (por ejemplo, fallas de carga de página o latencia alta), y ese dominio se puede configurar en los criterios del registro de depuración de solicitud.

Paso 8. Elija el método para recuperar los registros. Si selecciona FTP Poll, los registros se almacenan en el SWA.

Paso 9. Defina el nombre de archivo que se utilizará para los archivos de registro o pulse Intro para aceptar el nombre de archivo generado actualmente.

Paso 10. Seleccione No para la sustitución de archivos log basados en tiempo, ya que el registro se detiene después de que se haya satisfecho el número de solicitudes definido.

Paso 11. Defina el tamaño máximo del archivo en Bytes o pulse Intro para aceptar el valor actual.

Consejo: Definir un tamaño de archivo de registro mayor puede dificultar la descarga y revisión de los registros. En lugar de aumentar el tamaño de los archivos de registro individuales, se recomienda aumentar el número de archivos de registro (Siguiente paso). Este enfoque mejora la capacidad de administración al tiempo que garantiza que toda la información de depuración necesaria se capture sin crear archivos demasiado grandes.

Paso 12. Configure el número máximo de archivos log basado en el número de módulos proxy seleccionados para el registro en el Paso 5 y los criterios de coincidencia de solicitudes definidos en el Paso 7. Seleccionar un límite de archivo razonable es importante para asegurarse de que toda la información de depuración relevante se capture sin detener el registro prematuramente, lo que podría dar lugar a registros incompletos o faltantes.

Paso 13. Seleccione No cuando se le pregunte ¿Debe enviarse una alerta cuando se eliminan archivos debido al número máximo de archivos permitidos? Esto evita alertas innecesarias durante la rotación normal del registro, especialmente cuando se generan registros de depuración de solicitudes intencionalmente para solucionar problemas.

Paso 14. Seleccione No cuando se le pregunte ¿Desea comprimir los registros (sí/no)? Esto mantiene los archivos de registro sin comprimir, lo que facilita su revisión y análisis durante la resolución de problemas.

Paso 15. Pulse Intro para salir del asistente

Paso 16. Escriba commit y presione Intro para guardar los cambios

```
SWA_CLI> logconfig

Currently configured logs:
1. "accesslogs" Type: "Access Logs" Retrieval: FTP Poll
2. "adc_logs" Type: "ADC Engine Logs" Retrieval: FTP Poll
...
[Output removed to simplify readability]
...
55. "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.
- AUDITLOGCONFIG - Adjust settings for audit logging.
[]> new

Choose the log file type for this subscription:
```

```
1. ADC Engine Framework Logs
2. ADC Engine Logs
...
[Output removed to simplify readability]
...
53. Request Debug Logs
...
[Output removed to simplify readability]
...
[1]> 53

Please enter the name for the log:
[]> Request_Debug_Logs

Log level:
1. Critical
2. Warning
3. Information
4. Debug
5. Trace
[3]> 5

Choose modules where enhanced request logging is to be performed.
Multiple selections can be made in the form of a comma separated or range list (e.g. 1,3,4 or 3-7)
Choosing the Default Proxy will enable enhanced logging across modules:
1. Default Proxy
2. Access Control Engine
3. Proxy Configuration
4. Disk Manager
5. Memory Manager
6. McAfee Integration Framework
7. Sophos Integration Framework
8. Webroot Integration Framework
9. Webcat Integration Framework
10. Connection Management
11. Authentication Framework
12. HTTPS
13. FTP proxy
14. WCCP Module
15. License Module
16. SNMP Module
17. WBRS Integration Framework
18. Logging Framework
19. Data Security Module
20. Miscellaneous Proxy Modules
21. DCA Engine Framework
22. AVC Engine Framework
23. Cloud Connector
24. SOCKS Proxy
25. Advanced Malware Protection
26. ArchiveScan module in proxy
27. Web Traffic Tap module in proxy
28. Bandwidth Control
29. Http2 proxy
30. ADC Engine Framework
[1]> 1-30

Please enter the number of requests for which to perform enhanced logging:
[1]> 100

Choose the request criteria for logging:
1. Client IP Address
```

```
2. Destination Domain
3. Destination IP Address
[1]> 1

Specify source IP address
[]> 10.20.3.15

Choose the method to retrieve the logs:
1. FTP Poll
2. FTP Push
3. SCP Push
[1]> 1

Filename to use for log files:
[Request_Debug_Logs.text]>

Do you want to configure time-based log files rollover? [N]>

Please enter the maximum file size:
[10485760]>

Please enter the maximum number of files:
[10]> 50

Should an alert be sent when files are removed due to the maximum number of files allowed? [N]>

Do you want to compress logs (yes/no)
[n]>

Currently configured logs:
1. "Request_Debug_Logs" Type: "Request Debug Logs" Retrieval: FTP Poll
2. "accesslogs" Type: "Access Logs" Retrieval: FTP Poll
3. "adc_logs" Type: "ADC Engine Logs" Retrieval: FTP Poll
...
[Output removed to simplify readability]
...
56. "welcomeack_logs" Type: "Welcome Page Acknowledgement Logs" Retrieval: FTP Poll


SWA_LIC> commit

Warning: In order to process these changes, the proxy
process will restart after Commit. This will cause a brief
interruption in service. Additionally, the authentication
cache will be cleared, which might require some users to
authenticate again.
```

Información Relacionada

- Guía del usuario de AsyncOS 15.2 para Cisco Secure Web Appliance
- Uso de las prácticas recomendadas de Secure Web Appliance
- Acceder a registros de appliances web seguros
- Configuración de registros de inserción de SCP en SWA con Microsoft Server

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).