Solución de problemas de rendimiento de appliances web seguros con registros SHD

Contenido

Introducción

Este documento describe los registros de System Health Daemon (shd_logs) y cómo resolver problemas de rendimiento de Secure Web Appliance (SWA) con este registro.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Dispositivo web seguro (SWA) físico o virtual instalado.
- Licencia activada o instalada.
- Cliente Secure Shell (SSH).
- El asistente de configuración ha finalizado.

- Acceso administrativo al 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.

¿Qué es SHD LOGS

Los registros SHD contienen la mayor parte de las estadísticas de procesos relacionados con el rendimiento en SWA cada minuto.

Aquí hay un ejemplo de una línea de registro SHD:

```
Mon Jun 9 23:46:14 2022 Info: Status: CPULd 66.4 DskUtil 5.2 RAMUtil 11.3 Reqs 0 Band 0 Latency 0 CacheH
SrvConn 0 MemBuf 0 SwpPgOut 0 ProxLd 0 Wbrs_WucLd 0.0 LogLd 0.0 RptLd 0.0 WebrootLd 0.0 SophosLd 0.0 Mca
```

Los registros SHD son aceptables desde la interfaz de línea de comandos (CLI) y desde el protocolo de transferencia de archivos (FTP). No hay opciones para ver el registro desde la interfaz gráfica de usuario (GUI).

Acceder a registros SHD

Desde la CLI:

1. Escriba **grep** o **tail** en CLI.
2. Busque **"shd_logs Type: SHD Logs Retrieval: FTP Poll** en la lista y escriba el número asociado.
3. En **Introduzca la expresión regular a grep.** Puede escribir expresiones regulares para buscar dentro de los registros; por ejemplo, puede escribir fecha y hora.
4. **¿Desea que esta búsqueda no distinga entre mayúsculas y minúsculas? [Y]>** Puede dejar esta opción como predeterminada a menos que necesite buscar distingue entre mayúsculas y minúsculas, que en SHD_Logs no necesita.
5. **¿Desea buscar líneas que no coincidan? [N]>** Puede establecer esta línea como predeterminada a menos que necesite buscarlo todo excepto su expresión regular Grep.
6. **¿Quieres seguir los registros? [N]>** Esta opción sólo está disponible en la salida del grep; si la deja como predeterminada (N), mostrará los registros SHD de la primera línea del archivo actual.
7. **¿Desea paginar el resultado? [N]>** Si selecciona "Y", la salida es la misma que la salida de comando less, puede navegar entre líneas y páginas también puede buscar dentro de los registros (Escriba /luego la palabra clave y presione Enter), para salir de la vista de registro por tipo **q**.

Desde FTP:

1. Asegúrese de que FTP esté habilitado desde **GUI > Network > Interfaces**.
2. Conéctese a SWA a través de FTP.
3. Shd_logs, contiene los registros.

Campos de registro de SHD

Los campos de los registros SHD detallan:

Número de campo	Nombre	Identifier	Descripción
8	CPULd	Porcentaje % 0 - 99	CARGA DE CPU Porcentaje total de la CPU utilizada en el sistema según lo informado por el SO
10	DskUti	Porcentaje % 0 - 99	Utilización del disco espaciado utilizado en la partición /data
12	RAMUtil	Porcentaje %	Utilización de RAM

		0 - 99	Porcentaje de memoria libre notificado por el SO
14	Solicitudes	Solicitud/segundos	Solicitudes Número medio de transacciones (solicitudes) en el último minuto
16	Banda	Kb/s	Ancho de banda guardado Ancho de banda medio ahorrado en el último minuto. - Equivalente al promedio de ahorro de ancho de banda de SNMP del último minuto
18	Latencia [1]	Milisegundos (ms)	Latencia media (tiempo de respuesta) en el último minuto toma el segundo campo de los registros de acceso, que muestra cuánto tiempo tarda la conexión TCP del usuario final a WSA (o del usuario final al servidor web si la conexión no se descifró) WSA resume las horas, para cada solicitud conectada, los registros de acceso de los últimos minutos, y los divide en los números de estas solicitudes y obtiene una latencia media para SHD
20	CacheHit	Número #	Alcanzó el promedio de caché en el último minuto. - Equivalente al promedio de aciertos de caché

			SNMP del último minuto
22	CliConn	Número #	Número total de conexiones de cliente actuales De clientes a WSA - equivalente al total de conexiones de cliente SNMP actuales
24	SrvConn	Número #	Número total de conexiones de servidor actuales De WSA a servidor web - Equivalente a las conexiones totales del servidor SNMP actuales.
26	MemBuf [2]	Porcentaje % 0 - 99	Búfer de memoria Cantidad total actual de memoria de búfer de proxy disponible.
28	SwpPgOut	Número #	Número de páginas que se han intercambiado, según lo informado por el sistema operativo. Archivo de paginación o archivo de paginación, es el espacio de un disco duro utilizado como ubicación temporal para almacenar información cuando la RAM se utiliza por completo.
30	ProxLd	Porcentaje % 0 - 99	La carga de prox Process Proceso responsable para procesar todas las solicitudes entrantes (HTTP/HTTPS/FTP/SOCKS)

32	Wbrs_WucLd	Porcentaje % 0 - 99	Carga de puntuación de Web Reputation Proceso utilizado para el motor de análisis WBRS real. El proceso de proxy interactúa con el proceso de solicitud para realizar exploraciones WBRS.
34	LogLd	Porcentaje % 0 - 99	Carga de registro de proxy
36	RptLd	Porcentaje % 0 - 99	Carga del motor de informes Proceso responsable para crear la base de datos de informes. 'reportd' interactúa con 'haystackd' para crear la base de datos de rastreo web.
38	WebrootLd	Porcentaje % 0 - 99	Carga de antimalware de Webroot
40	SophosLd	Porcentaje % 0 - 99	Carga de Sophos Antivirus
42	McafeeLd	Porcentaje %	Carga De Mcafee

		0 - 99	Antivirus
44	WTTLd	Porcentaje % 0 - 99	Toque Tráfico web
46	AMPLd	Porcentaje % 0 - 99	Protección frente a malware avanzado (AMP)

1. A veces se podría esperar un pico alto de latencia en los registros SHD, por ejemplo, si no hay muchas solicitudes en WSA y en algún momento se terminó una conexión de larga duración, por ejemplo, varios días. A continuación, esta única solicitud puede aumentar la latencia de ese minuto cuando haya finalizado y haya iniciado sesión en los registros de acceso.

2. Según se indica en :

> "Uso de RAM para un sistema que working eficientemente puede ser superior al 90%, ya que la memoria caché de objetos web utiliza la memoria RAM que no está siendo utilizada por el sistema de otro modo. Si su sistema no está experiencing graves problemas de rendimiento y este valor no se bloquea en el 100%, el sistema operating normalmente".

Nota: La memoria del búfer del proxy es un componente que utiliza esta RAM

Resolución de problemas con registros SHD

Carga alta de otro proceso

Si la carga del otro proceso es alta, verifique la tabla-1 de este artículo y lea los registros relacionados con ese proceso.

Latencia alta

Si vio latencia alta en los registros SHD, debe verificar los registros de Proxy_track en **/data/pub/track_stats/** . Busque el intervalo de tiempo en el que la latencia es alta. En la pista de proxy tiene un par de registros que están relacionados con la latencia. Los números delante de cada sección son el número total de apariciones desde el último reinicio. Por ejemplo, en este código:

```
Current Date: Wed, 11 Jun 2022 20:03:32 CEST
...
   Client Time    6309.6 ms    109902
...
Current Date: Wed, 11 Jun 2022 20:08:32 CEST
...
   Client Time    6309.6 ms    109982
```

En 5 minutos, el número de solicitudes de clientes que tardaron 6309,6 ms o más es 80 solicitudes. Por lo tanto, debe restar los números de cada intervalo de tiempo para obtener el valor exacto que debe tener en cuenta estos elementos:

Tiempo del cliente: Tiempo que se tarda del cliente al SWA.

Tiempo de acierto: Aciertos de caché: los datos solicitados están en la caché y se pueden entregar al cliente.

Tiempo perdido: Pérdida de caché: los datos solicitados no están en la caché o no están actualizados y no se pueden entregar al cliente.

Tiempo de transacción del servidor: tiempo que se tarda del SWA al servidor web.

Además, estos valores deben tenerse en cuenta en el proceso de comprobación del rendimiento:

> **tiempo de usuario: 160 852 (53,33%)**
> **hora del sistema: 9,768 (3,256%)**

En Registros de estado de seguimiento, Información registrada cada 5 minutos (300 segundos). En este ejemplo, el tiempo de usuario 160.852 es el tiempo (en segundos) que la CPU cargó con tareas para manejar las solicitudes de los usuarios. La hora del sistema es la hora en la que SWA procesó los eventos de red, como la decisión de routing, etc. La suma de estos dos porcentajes es la carga total de CPU en ese tiempo. Si el tiempo del usuario es alto, significa que debe considerar una configuración de complejidad alta.

Información Relacionada

- **Notas de la versión de WSA AsyncOS**
- **Matriz de compatibilidad para Cisco Secure Email and Web Manager**
- **Actualizaciones y comprobación de conectividad de actualizaciones**
- **Asistencia técnica y descargas de 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).