Solucionar problemas de desempenho do Secure Web Appliance com registros SHD

Contents

Introdução

Este documento descreve os logs do daemon de integridade do sistema (shd_logs) e como solucionar problemas de desempenho do Secure Web Appliance (SWA) com esse log.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Dispositivo da Web seguro (SWA) físico ou virtual instalado.
- Licença ativada ou instalada.
- Cliente Secure Shell (SSH).
- O assistente de instalação foi concluído.

- Acesso administrativo ao SWA.

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.

O que é SHD LOGS

Os registros SHD mantêm a maioria das estatísticas de processo relacionadas ao desempenho no SWA a cada minuto.

Aqui está um exemplo de uma linha de log 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
```

Os registros SHD são aceitáveis a partir da interface de linha de comando (CLI) e do protocolo de transferência de arquivos (FTP). Não há opções para visualizar o registro na Interface gráfica do usuário (GUI).

Acessar Logs SHD

Na CLI:

1. Digite **grep** ou **tail** na CLI.
2. Localize **"shd_logs Type: SHD Logs Retrieval: FTP Poll** na lista e digite o número associado.
3. Em **Insira a expressão regular para grep.** Você pode digitar expressões regulares para pesquisar dentro dos logs; por exemplo, você pode digitar data e hora.
4. **Deseja que esta pesquisa não diferencie maiúsculas de minúsculas? [Y]>** Você pode deixar como padrão, a menos que precise procurar por casos que diferenciem maiúsculas de minúsculas, que em SHD_Logs você não precisa desta opção.
5. **Deseja procurar linhas não correspondentes? [N]>** Você pode definir essa linha como padrão, a menos que precise pesquisar tudo, exceto sua expressão regular Grep.
6. **Deseja encerrar os logs? [N]>** Essa opção só está disponível na saída do grep; se você deixar isso como padrão (N), ela mostrará os logs do SHD da primeira linha do arquivo atual.
7. **Deseja paginar a saída? [N]>** Se selecionar "Y", a saída é a mesma saída de menos comando, você pode navegar entre linhas e páginas também você pode pesquisar dentro dos logs (Digite / depois a palavra-chave e pressione enter), para sair da visualização do log pelo tipo **q.**

Do FTP:

1. Certifique-se de que o FTP esteja ativado em **GUI > Rede > Interfaces**.
2. Conecte-se ao SWA via FTP.
3. Pasta Shd_logs, contém os logs.

Campos do Log do SHD

Os campos nos registros SHD detalham:

Número do campo	Nome	Identifier	Descrição
8	CPULd	Porcentagem % 0 a 99	CARGA DE CPU Percentual total de CPU usada no sistema conforme relatado pelo SO
10	DskUti	Porcentagem % 0 a 99	Utilização de disco espaçado usado na partição /data
12	RAMUtil	Porcentagem %	Utilização de RAM

		0 a 99	Porcentagem de memória livre relatada pelo SO
14	Solicitações	Solicitação/Segundos	Solicitações Número médio de transações (solicitações) no último minuto
16	Banda	Kb/s	Largura de banda economizada Largura de banda média salva no último minuto. - Equivalente à média de largura de banda SNMP salva no último minuto
18	Latência [1]	Milissegundos (ms)	Latência média (tempo de resposta) no último minuto usa o segundo campo nos logs de acesso - que mostra quanto tempo a conexão TCP leva do usuário final para o WSA (ou do usuário final para o servidor Web se a conexão não tiver sido descriptografada) O WSA soma os tempos, para cada solicitação conectada nos logs de acesso dos últimos minutos, divide-a nos números dessas solicitações e obtém uma latência média para o SHD
20	Acerto deCache	Número	Média de acertos do cache no último minuto. - Equivalente à média de acertos do cache SNMP no último minuto

22	CliConn	Número	Número total de Conexões de Cliente atuais De clientes para o WSA - equivalente ao total atual de conexões de cliente SNMP
24	SrvConn	Número	Número total de Conexões de Servidor atuais Do WSA para o servidor Web - Equivalente ao total atual de conexões de servidor SNMP.
26	MemBuf [2]	Porcentagem % 0 a 99	Buffer de Memória Quantidade total atual de Memória de Buffer do Proxy que está livre.
28	SaídaPgSwp	Número	Número de páginas trocadas, conforme relatado pelo SO. Arquivo de paginação ou arquivo de paginação é o espaço em um disco rígido usado como um local temporário para armazenar informações quando a RAM é totalmente utilizada.
30	ProxLd	Porcentagem % 0 a 99	A carga do processo de proxy O processo responsável por processar todas as solicitações de entrada (HTTP/HTTPS/FTP/SOCKS)

32	Wbrs_WucLd	Porcentagem % 0 a 99	Carga do Web Reputation Coring Processo usado para o mecanismo de varredura WBRS real. O processo de proxy interage com o processo reqscand para executar varreduras WBRS.
34	LogLd	Porcentagem % 0 a 99	Carga de Log do Proxy
36	RptLd	Porcentagem % 0 a 99	Carregar mecanismo de relatório O processo responsável por criar o banco de dados de Relatórios. 'reportd' interage com 'haystackd' para criar o banco de dados de Rastreamento da Web.
38	WebrootLD	Porcentagem % 0 a 99	Carregamento do Antimalware do Webroot
40	SophosLd	Porcentagem % 0 a 99	Carga do antivírus Sophos
42	McafeeLd	Porcentagem % 0 a 99	Carga Do Mcafee Antivirus

44	WTTLd	Porcentagem % 0 a 99	Toque no tráfego da Web
46	AMPLd	Porcentagem % 0 a 99	Proteção avançada contra malware (AMP)

1. Às vezes, pode-se esperar um pico alto na latência em logs SHD, por exemplo, se não houver muitas solicitações no WSA e em algum momento tiver sido concluída uma conexão de longa duração - por exemplo, vários dias. Em seguida, essa única solicitação pode aumentar a latência nesse minuto quando terminar e fizer login nos logs de acesso.

2. Tal como escrito em :

> "Uso de RAM para um sistema que é working eficientemente pode ser superior a 90%, porque a RAM que não está sendo usada pelo sistema é usada pelo cache de objetos da Web. Se o seu sistema não estiver experiencing problemas sérios de desempenho e esse valor não ficar preso a 100%, o sistema está operating normalmente."

Observação: a memória de buffer do proxy é um componente que usa essa RAM

Solucionar problemas com registros SHD

Outro Processo de Alta Carga

Se a carga do outro processo for alta, verifique a tabela 1 deste artigo e leia os logs relacionados a esse processo.

Alta latência

Se você observou alta latência nos logs SHD, você deve verificar os logs Proxy_track em **/data/pub/track_stats/** . Localize o intervalo de tempo em que a latência está alta. No rastreamento de proxy, você tem dois registros relacionados à latência. Os números na frente de cada seção são o número total de ocorrências desde a última reinicialização. Por exemplo, neste 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
```

Em 5 minutos, o número de solicitações de clientes que levaram 6309,6 ms ou mais é de 80 solicitações. Portanto, você tem que subtrair os números em cada intervalo de tempo para obter o valor preciso que você deve considerar estes itens:

Hora do cliente: tempo que leva do cliente para o SWA.

Tempo de Acerto: Acertos do Cache: Os Dados Solicitados estão no cache e podem ser entregues ao Cliente.

Tempo de Perda: Perda de cache: Os Dados Solicitados não estão no cache ou não estão atualizados e não podem ser entregues ao Cliente.

Tempo de Transação do Servidor: Tempo que leva do SWA para o Servidor Web.

Também estes valores devem ser considerados no processo de verificação de desempenho:

tempo de uso: 160,852 (53,33%)
tempo do sistema: 9,768 (3,256%)

Nos registros de estatísticas de rastreamento, as informações são registradas a cada 5 minutos (300 segundos). Neste exemplo, tempo de usuário 160,852 é o tempo (em segundos), que a CPU foi carregada com tarefas para tratar solicitações de usuários. A hora do sistema é a hora em que o SWA processou eventos de rede, como decisão de roteamento e assim por diante. A soma desses dois percentuais é a carga total da CPU nesse tempo. Se o tempo do usuário for alto, isso significa que você precisa considerar uma configuração de alta complexidade.

Informações Relacionadas

- **Notas da versão do WSA AsyncOS**
- **Matriz de compatibilidade do Cisco Secure Email e Web Manager**
- **Verificação de Conectividade de Atualizações e Atualizações**
- **Suporte técnico e downloads da 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.