Risoluzione dei problemi relativi alle prestazioni di Secure Web Appliance con i registri SHD

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Che cos'è SHD LOGS](#)
[Accedi a registri SHD](#)

Introduzione

In questo documento vengono descritti i log del daemon di stato del sistema (shd_logs) e viene spiegato come risolvere i problemi di prestazioni di Secure Web Appliance (SWA) con questo log.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Installazione di Physical o Virtual Secure Web Appliance (SWA) completata.
- Licenza attivata o installata.
- Client Secure Shell (SSH).
- Installazione guidata completata.

- Accesso amministrativo all'SWA.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Che cos'è SHD LOGS

I registri SHD contengono la maggior parte delle statistiche di processo relative alle prestazioni in SWA per ogni minuto.

Di seguito è riportato un esempio di riga di 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
```

I registri SHD sono accettabili dall'interfaccia della riga di comando (CLI) e dal protocollo FTP (File Transfer Protocol). Non sono disponibili opzioni per visualizzare il registro dall'interfaccia utente grafica (GUI).

Accedi a registri SHD

Dalla CLI:

1. Digitare **grep** o **tail** nella CLI.
2. Trovare **"shd_logs Tipo: Recupero log SHD: Polling FTP** dall'elenco e digitare il numero associato.
3. In **Immettere l'espressione regolare grep.** È possibile digitare espressioni regolari per eseguire ricerche all'interno dei registri, ad esempio data e ora.
4. **Non si desidera distinguere tra maiuscole e minuscole nella ricerca? [Y]>**È possibile mantenere questa impostazione come predefinita a meno che non sia necessario eseguire una ricerca con distinzione tra maiuscole e minuscole. In SHD_Logs questa opzione non è necessaria.
5. **Cercare le righe non corrispondenti? [N]>** È possibile impostare questa riga come predefinita, a meno che non sia necessario cercare tutti gli elementi tranne l'espressione regolare Grep.
6. **Definire la coda dei registri? [N]>**Questa opzione è disponibile solo nell'output del grep, se la si lascia come predefinita (N), mostra i log SHD dalla prima riga del file corrente.
7. **Impaginare l'output? [N]>** Se si seleziona "Y", l'output è uguale a quello del comando less, è possibile navigare tra le righe e le pagine e anche cercare all'interno dei log (Digitare **/** quindi la parola chiave e premere Invio), per uscire dalla vista del log per tipo **q**.

Da FTP:

1. Verificare che FTP sia abilitato da **GUI > Rete > Interfacce**.
2. Collegamento a SWA tramite FTP.
3. Shd_logs, contiene i log.

Campi registro SHD

I campi nei registri SHD sono dettagliati:

Numero campo	**Nome**	**Identificativo**	**Descrizione**
8	CPULd	% percentuale 0 ~ 99	CARICO CPU Percentuale totale di CPU utilizzata nel sistema come indicato dal sistema operativo
10	Unità disco	% percentuale 0 ~ 99	Utilizzo del disco spaziatura utilizzata nella partizione /data
12	ramutil	% percentuale	Utilizzo della RAM

		0 ~ 99	Percentuale di memoria libera segnalata dal sistema operativo
14	Richieste	Richiesta / Secondi	Richieste Numero medio di transazioni (richieste) nell'ultimo minuto
16	Banda	Kb/s	Larghezza di banda risparmiata Larghezza di banda media salvata nell'ultimo minuto. - Equivalente alla media salvata della larghezza di banda SNMP nell'ultimo minuto
18	Latenza [1]	Millisecondi (ms)	Latenza media (tempo di risposta) nell'ultimo minuto accetta il secondo campo dei log degli accessi, che indica il tempo impiegato dalla connessione TCP da un utente finale a WSA (o da un utente finale a un server Web se la connessione non è stata decrittografata) WSA riepiloga i tempi per ogni richiesta registrata nei log degli accessi negli ultimi minuti e li suddivide nei numeri di queste richieste e ottiene una latenza media per SHD
20	RiscontriCache	Numero #	Media riscontri cache nell'ultimo minuto. - Equivalente alla media dei riscontri nella cache

			SNMP nell'ultimo minuto
22	CliConn	Numero #	Numero totale di connessioni client correnti Da client a WSA - equivalente al totale delle connessioni client SNMP
24	SrvConn	Numero #	Numero totale di connessioni server correnti Da WSA a server Web - Equivalente al totale delle connessioni server SNMP correnti.
26	MemBuf [2]	% percentuale 0 ~ 99	Buffer di memoria Quantità totale corrente di memoria buffer proxy disponibile.
28	UscitaSwp	Numero #	Numero di pagine scambiate, come riportato dal sistema operativo. Il file di paging, o file di paging, è lo spazio su un disco rigido utilizzato come posizione temporanea per memorizzare le informazioni quando la RAM è completamente utilizzata.
30	LedProx	% percentuale 0 ~ 99	Carico del processo proxy Processo responsabile dell'elaborazione di tutte le richieste in ingresso (HTTP/HTTPS/FTP/SOCKS)

32	Wbrs_WucLd	% percentuale 0 ~ 99	Caricamento Web Reputation Coring Processo utilizzato per il motore di analisi WBRS effettivo. Il processo proxy interagisce con il processo di richiesta per eseguire scansioni WBRS.
34	LogId	% percentuale 0 ~ 99	Caricamento log proxy
36	RptId	% percentuale 0 ~ 99	Caricamento modulo di gestione report Processo responsabile della creazione del database di report. 'reported' interagisce con 'haystack' per creare il database di rilevamento Web.
38	WebrootLd	% percentuale 0 ~ 99	Caricamento antimalware Webroot
40	SophosLd	% percentuale 0 ~ 99	Sophos Antivirus Load
42	McafeeLd	% percentuale	Caricamento Antivirus

		0 ~ 99	Mcafee
44	WTTLd	% percentuale 0 ~ 99	Traffic Tap Web
46	AMP	% percentuale 0 ~ 99	Advanced Malware Protection

1. A volte ci si può aspettare di vedere un alto picco di latenza nei registri SHD, ad esempio se non ci sono molte richieste su WSA e a un certo punto è stata completata una connessione di lunga durata - ad esempio diversi giorni. Questa singola richiesta può quindi aumentare la latenza per il minuto al termine e dopo aver eseguito l'accesso ai log degli accessi.

2. Come indicato in:

> "Utilizzo della RAM per un sistema working può essere superiore al 90%, in quanto la RAM che non è altrimenti in uso dal sistema viene utilizzata dalla cache degli oggetti Web. Se il sistema non è experiencing problemi di prestazioni gravi e questo valore non è bloccato al 100%, il sistema è operating normalmente."

> **Nota**: la memoria buffer proxy è un componente che utilizza questa RAM

Risoluzione dei problemi con i registri SHD

Altro processo con carico elevato

Se il carico dell'altro processo è elevato, controllare la tabella 1 da questo articolo e leggere i log relativi a tale processo.

Alta latenza

Se nei log SHD è presente un'alta latenza, è necessario controllare i log Proxy_track in **/data/pub/track_stats/** . Individuare l'intervallo di tempo in cui la latenza è elevata. Nel brano proxy ci sono un paio di record relativi alla latenza. I numeri davanti a ciascuna sezione corrispondono al numero totale di occorrenze dall'ultimo riavvio. Ad esempio, in questo codice:

```
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
```

In 5 minuti, il numero di richieste client che hanno richiesto 6309,6 ms o superiore è 80. Quindi è necessario sottrarre i numeri in ogni intervallo di tempo per ottenere il valore esatto che è necessario considerare questi elementi:

Tempo client: tempo necessario dal client al SWA.

Tempo di accesso: riscontri nella cache: i dati richiesti sono nella cache e possono essere recapitati al client.

Tempo di mancato riscontro nella cache: i dati richiesti non sono presenti nella cache oppure non sono aggiornati e non possono essere recapitati al client.

Tempo di transazione del server: tempo impiegato da SWA al server Web.

Anche questi valori devono essere presi in considerazione nel processo di controllo delle prestazioni:

tempo utente: 160,852 (53,33%)
tempo di sistema: 9,768 (3,256%)

Nei registri di stato del brano, le informazioni vengono registrate ogni 5 minuti (300 secondi). In questo esempio, il tempo utente 160,852 è il tempo (in secondi) durante il quale la CPU è stata caricata con attività per gestire le richieste dell'utente. L'ora di sistema è l'ora in cui SWA ha elaborato gli eventi di rete, ad esempio la decisione di instradamento e così via. La somma di queste due percentuali è il carico totale della CPU in quel periodo. Se il tempo dell'utente è elevato, è necessario prendere in considerazione una configurazione ad alta complessità.

Informazioni correlate

- **Note sulla release di WSA AsyncOS**
- **Matrice di compatibilità per Cisco Secure Email e Web Manager**
- **Controllo connettività aggiornamenti e aggiornamenti**
- **Supporto tecnico e download Cisco**

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).