Probleemoplossing voor prestaties van beveiligde webapplicatie met SHD-logbestanden

Inhoud

Inleiding

In dit document worden de logbestanden van System Health Daemon (shd_logs) beschreven en wordt beschreven hoe u problemen kunt oplossen met de prestaties van Secure Web Applicatie (SWA) met dit logbestand.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Physical of Virtual Secure Web Applicatie (SWA) geïnstalleerd.
- Licentie geactiveerd of geïnstalleerd.
- Secure Shell-client (SSH).
- De setup-wizard is voltooid.

- Administratieve toegang tot de SWA.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Wat is SHD LOGS

SHD-logbestanden houden de meeste prestatiegerelateerde processtatistieken in SWA voor elke minuut.

Hier is een voorbeeld van een SHD-logregel:

```
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
```

SHD-logbestanden zijn acceptabel vanaf Command Line Interface (CLI) en vanaf File Transfer Protocol (FTP). Er zijn geen opties om het logbestand te bekijken vanuit een grafische gebruikersinterface (GUI).

Toegang tot SHD-logs

Van de CLI:

1. Typ **grep** of **tail** in CLI.
2. Vind **"shd_logs Type: SHD Logs Retrieval: FTP Poll** uit de lijst en typ het bijbehorende nummer.
3. In **Voer de reguliere expressie voor grep in.** U kunt reguliere expressies typen om in de logbestanden te zoeken. U kunt bijvoorbeeld datum en tijd typen.
4. **Wil je dat deze zoekopdracht hoofdlettergevoelig is? [Y]>** U kunt dit als standaard laten staan, tenzij u moet zoeken naar hoofdlettergevoeligheid die u in SHD_Logs niet nodig hebt.
5. **Wilt u zoeken naar niet-overeenkomende lijnen? [N]>** U kunt deze regel als standaard instellen, tenzij u moet zoeken naar alles behalve de reguliere expressie van Grep.
6. **Wil je de logboeken volgen? [N]>** Deze optie is alleen beschikbaar in de uitvoer van de map. Als u deze optie standaard (N) laat staan, worden de SHD-logbestanden vanaf de eerste regel van het huidige bestand weergegeven.
7. **Wilt u de uitvoer pagineren? [N]>** Als u "Y" selecteert, is de uitvoer hetzelfde als de uitvoer van minder opdracht, kunt u tussen regels en pagina's navigeren. U kunt ook in de logbestanden zoeken (Type /dan het trefwoord en druk op enter) om de logweergave op type **q** te verlaten.

Van FTP:

1. Zorg ervoor dat FTP is ingeschakeld vanuit **GUI > Netwerk > Interfaces**.
2. Verbind met SWA via FTP.
3. De map Shd_logs bevat de logbestanden.

SHD-logvelden

De velden in de SHD-logbestanden zijn gedetailleerd:

Veldnummer	Name	Identificatie	Beschrijving
8	CPUL d	% % 0-99	CPU-BELASTING Totaal percentage van de op het systeem gebruikte CPUâ€™s zoals gerapporteerd door het besturingssysteem
10	Schoenspel	% % 0-99	Schijfgebruik ruimte gebruikt op de /data partitie
12	RAMUtil	% % 0-99	RAM-gebruik Percentage vrij geheugen

			gemeld door besturingssysteem
14	Verzoeken	Aanvragen / seconden	Verzoeken Gemiddeld aantal transacties (verzoeken) in de voorbije minuut
16	band	Kb/s	Bandbreedte opgeslagen Gemiddelde bandbreedte die in de afgelopen minuut is opgeslagen. - equivalent aan SNMP-bandbreedte opgeslagen gemiddelde voor de afgelopen minuut
18	Latentie [1]	Milliseconden (ms)	Gemiddelde vertraging (responstijd) in de laatste minuut neemt het tweede veld in toegangslogbestanden - dat toont hoeveel tijd de TCP-verbinding vergt van de eindgebruiker naar WSA (of van de eindgebruiker naar de webserver als de verbinding niet is gedecodeerd) WSA vat de tijden samen, voor elk verzoek dat in toegangslogboeken voor laatste minuten wordt geregistreerd en verdeel het in de aantallen deze verzoeken en krijg een gemiddelde latentie voor SHD
20	Cache hit	Nummer #	De cache bereikte de afgelopen minuut een gemiddelde. - Gelijk aan SNMP-cache

			hit gemiddelde voor afgelopen minuut
22	CliConn	Nummer #	Totaal aantal huidige clientverbindingen Van clients tot WSA - equivalent aan de huidige totale clientverbindingen van SNMP
24	SRVConn	Nummer #	Totaal aantal huidige serververbindingen Van WSA naar webserver - equivalent aan de huidige totale SNMP-serververbindingen.
26	MemBuf [2]	% % 0-99	Geheugenbuffer Huidige totale hoeveelheid Proxy Buffer Geheugen die vrij zijn.
28	Uitruilen	Nummer #	Aantal pagina's dat is uitgewisseld, zoals gerapporteerd door OS. Page File of Paging bestand, is ruimte op een harde schijf gebruikt als tijdelijke locatie om informatie op te slaan wanneer RAM volledig wordt gebruikt.
30	ProxLD	% % 0-99	De belasting van het proxproces Verantwoordelijk proces voor de verwerking van alle inkomende verzoeken (HTTP/HTTPS/FTP/SOCKS)

32	WBRS_WUCld	% % 0-99	Webreputatie laden van coring Proces gebruikt voor de eigenlijke WBRS scanengine. Proxy proces interacteert met vraag en proces om WBRS scans uit te voeren.
34	LogLd	% % 0-99	Proxy-logbestand laden
36	RPTld	% % 0-99	Rapporteer de werklast van de motor Verantwoordelijk proces voor aanmaken Rapportagedatabase. 'report' werkt samen met 'haystackd' om de Web Tracking database te creëren.
38	WebrootLd	% % 0-99	Webex Antimalware-lading
40	SophosLd	% % 0-99	lading van Sophos Antivirus
42	McAfeeLd	% % 0-99	McAfee Antivirus-lading

44	WTTLd	% % 0-99	Web traffic tap
46	AMPLd	% % 0-99	Advanced Malware Protection

1. Soms kan worden verwacht dat een hoge piek in Latency in SHD logs te zien, bijvoorbeeld als er niet veel verzoeken op WSA en op een bepaald moment was er een lange duur verbinding - bijvoorbeeld enkele dagen. Dan kan dit enkele verzoek de Latency voor die minuut verhogen wanneer het klaar was en het inlogt toegangslogboeken.

2. Zoals geschreven in:

> "RAM-gebruik voor een systeem dat working efficiënt kan hoger zijn dan 90%, omdat RAM dat niet anders in gebruik is door het web object cache wordt gebruikt. Als uw systeem niet experiencing belangrijke prestatiekwesties en deze waarde niet vastzit aan 100%, het systeem is operating normaal."

Opmerking: Proxy Buffer Memory is een component die dit RAM gebruikt

---

Probleemoplossing met SHD-logbestanden

Andere hoge lading van proces

Als de lading van het andere proces hoog is, controleer tabel-1 van dit artikel en lees de logboeken met betrekking tot dat proces.

Hoge latentie

Als u een hoge latentie zag in de SHD-logboeken, moet u de Proxy_track logboeken in **/data/pub/track_stats/** controleren. Vind het tijdkader dat de latentie hoog is. In de proxy track heb je een paar records die gerelateerd zijn aan latency. De cijfers voor elke sectie zijn het totale aantal gevallen sinds de laatste reboot. In deze code bijvoorbeeld:

```
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 minuten, het aantal klanten verzoeken die 6309.6 ms of hoger hebben genomen is 80 verzoeken. Dus je moet de getallen in elk tijdframe aftrekken om de juiste waarde te krijgen die je moet overwegen deze items:

Tijd van de cliënt: Tijd die het van Cliënt aan SWA vergt.

Hit Time: Cache hits: De gevraagde gegevens zijn in het cache en kunnen worden geleverd aan de klant.

Miss Time: Cache missen: De opgevraagde gegevens zijn niet in het cache of is niet up-to-date en kunnen niet aan client worden geleverd.

Server Transaction Time: tijd die nodig is van SWA naar web server.

Bij de controle van de prestaties moet ook met deze waarden rekening worden gehouden:

> **gebruikstijd: 160.852 (53.33%)**
> **systeemtijd: 9,768 (3,256%)**

In Track Stat-logbestanden wordt elke 5 minuten (300 seconden) informatie vastgelegd. In dit voorbeeld is de gebruikerstijd 160.852 de tijd (in seconden), die CPU was geladen met taken om gebruikersverzoeken te verwerken. De tijd van het systeem is de tijd dat SWA netwerkgebeurtenissen, zoals het routeren van besluit etc. verwerkt. De som van deze twee percentages is de totale CPU-belasting op dat moment. Als de gebruikerstijd hoog is, betekent dit dat u rekening moet houden met een hoge complexiteitsconfiguratie.

Gerelateerde informatie

- **Opmerkingen over WSA Async OS release**
- **Compatibiliteitsmatrix voor Cisco Secure Email and Web Manager**
- **Connectiviteitscontrole voor upgrades en updates**
- **Cisco technische ondersteuning en downloads**

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.