Fehlerbehebung bei der Leistung sicherer Web-Appliances mit SHD-Protokollen

Inhalt

Einleitung

Dieses Dokument beschreibt die Protokolle des Systemintegritätsdämons (shd_logs) und wie Sie Probleme mit der SWA-Leistung (Secure Web Appliance) dieses Protokolls beheben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Physische oder Virtual Secure Web Appliance (SWA) installiert.
- Lizenz aktiviert oder installiert.
- Secure Shell (SSH)-Client.
- Der Setup-Assistent ist abgeschlossen.

- Administratorzugriff auf die SWA.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Was ist SHD LOGS?

SHD-Protokolle enthalten die meisten leistungsbezogenen Prozessstatistiken in SWA für jede Minute.

Hier ist ein Beispiel für eine SHD-Protokollzeile:

```
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-Protokolle können über die Befehlszeilenschnittstelle (CLI) und über das File Transfer Protocol (FTP) empfangen werden. Es gibt keine Optionen zum Anzeigen des Protokolls über die grafische Benutzeroberfläche (GUI).

Zugriff auf SHD-Protokolle

Über die CLI:

1. Geben Sie **grep** oder **tail** in CLI ein.
2. Suchen Sie **"shd_logs Type: SHD Logs Retrieval: FTP Poll** aus der Liste und geben Sie die zugehörige Nummer ein.
3. Geben Sie **unter Geben Sie den zu grep gehörenden regulären Ausdruck ein.** Sie können reguläre Ausdrücke eingeben, um in den Protokollen zu suchen, z. B. Datum und Uhrzeit.
4. **Soll bei dieser Suche die Groß-/Kleinschreibung beachtet werden? [Y]>** Sie können dies als Standard beibehalten, es sei denn, Sie müssen nach Groß- und Kleinschreibung suchen, die Sie in SHD_Logs nicht benötigen.
5. **Möchten Sie nach nicht übereinstimmenden Posten suchen? [N]>** Sie können diese Zeile als Standard festlegen, es sei denn, Sie müssen nach allem mit Ausnahme des regulären Grep-Ausdrucks suchen.
6. **Möchten Sie die Protokolle verfolgen? [N]>** Diese Option ist nur in der Ausgabe des grep verfügbar. Wenn Sie dies als Standard (N) zulassen, werden die SHD-Protokolle aus der ersten Zeile der aktuellen Datei angezeigt.
7. **Möchten Sie die Ausgabe paginieren? [N]>** Wenn Sie "Y" wählen, ist die Ausgabe die gleiche wie die Ausgabe von weniger Befehl, können Sie zwischen Zeilen und Seiten auch Sie können innerhalb der Protokolle suchen (Geben Sie /dann das Schlüsselwort und drücken Sie die Eingabetaste), um die Log-Ansicht nach Typ **q** zu verlassen.

Über FTP:

1. Stellen Sie sicher, dass FTP über die **GUI > Network > Interfaces (Netzwerk > Schnittstellen)** aktiviert ist.
2. Stellen Sie über FTP eine Verbindung mit SWA her.
3. Shd_logs Ordner, enthält die Protokolle.

SHD-Protokollfelder

Die Felder in den SHD-Protokollen sind detailliert:

Feldnummer	Name	Identifikator	Beschreibung
8	CPULd	Prozentsatz % 0 - 99	CPU-Last Gesamtprozentsatz der vom Betriebssystem auf dem System verwendeten CPU
10	Festplattendienstprogramm	Prozentsatz % 0 - 99	Festplattenauslastung auf der /data-Partition verwendeter

			Speicherplatz
12	RAMUtil	Prozentsatz % 0 - 99	RAM-Auslastung Prozentsatz des freien Speichers, der vom Betriebssystem gemeldet wird
14	Anforderungen	Anforderung/Sekunden	Anfragen Durchschnittliche Anzahl von Transaktionen (Anfragen) in der letzten Minute
16	Band	KB/s	Eingesparte Bandbreite Durchschnittliche Bandbreiteneinsparung in der letzten Minute. - Äquivalent zum Durchschnitt der in der letzten Minute eingesparten SNMP-Bandbreite
18	Latenz [1]	Millisekunden (ms)	Durchschnittliche Latenz (Reaktionszeit) in der letzten Minute Ermittelt das zweite Feld in den Zugriffsprotokollen, das anzeigt, wie lange die TCP-Verbindung von Endbenutzer zu WSA (oder von Endbenutzer zu Webserver, wenn die Verbindung nicht entschlüsselt wurde) dauert. WSA fasst die Zeiten für jede angemeldete Anforderung in den Zugriffsprotokollen für die letzten Minuten zusammen und teilt sie in

			die Anzahl dieser Anforderungen auf. So wird eine durchschnittliche Latenz für SHD erzielt.
20	CacheHit	Nummer	Der Cache hat in der letzten Minute den Durchschnitt erreicht. - Entspricht dem SNMP-Cache-Trefferdurchschnitt der letzten Minute
22	CliConn	Nummer	Gesamtanzahl der aktuellen Clientverbindungen Von Clients zu WSA - entspricht der aktuellen Gesamtzahl der SNMP-Clientverbindungen
24	SrvConn	Nummer	Gesamtanzahl der aktuellen Serververbindungen Von WSA zu Webserver - Entspricht der aktuellen Gesamtanzahl an SNMP-Serververbindungen.
26	MemBuf [2]	Prozentsatz % 0 - 99	Speicherpuffer Die aktuelle Gesamtmenge des freien Proxy-Pufferspeichers.
28	SpPgAus	Nummer	Anzahl der vom Betriebssystem gemeldeten ausgetauschten Seiten Auslagerungsdatei oder Auslagerungsdatei ist Speicherplatz auf einer

			Festplatte, die als temporärer Speicherort zum Speichern von Informationen verwendet wird, wenn der RAM voll ausgelastet ist.
30	ProxLd	Prozentsatz % 0 - 99	Prox-Prozesslast Prozess, der für die Verarbeitung aller eingehenden Anfragen verantwortlich ist (HTTP/HTTPS/FTP/SOCKS)
32	WBRS_WUCld	Prozentsatz % 0 - 99	Webreputations-Auslastung Prozess, der für die eigentliche WBRS-Scan-Engine verwendet wird. Der Proxyprozess interagiert mit dem Anforderungsprozess, um WBRS-Scans durchzuführen.
34	ProtokollLd	Prozentsatz % 0 - 99	Laden des Proxyprotokolls
36	RptLd	Prozentsatz % 0 - 99	Report Engine-Last Der für die Erstellung der Berichtsdatenbank verantwortliche Prozess. 'reportd' interagiert mit 'haystackd', um die Web Tracking-Datenbank zu erstellen.

38	WebrootLd	Prozentsatz % 0 - 99	Webroot-Anti-Malware-Laden
40	SophosLd	Prozentsatz % 0 - 99	Sophos Antivirus-Workload
42	McafeeLd	Prozentsatz % 0 - 99	McAfee-Antivirenauslastung
44	WTTLd	Prozentsatz % 0 - 99	Anzapfen des Webverkehrs
46	AMPLd	Prozentsatz % 0 - 99	Advanced Malware Protection (AMP)

1. Manchmal kann man davon ausgehen, dass die Latenz in den SHD-Protokollen einen hohen Spitzenwert erreicht, wenn es beispielsweise auf der WSA nicht viele Anfragen gibt und irgendwann eine Verbindung mit langer Dauer hergestellt wurde, z. B. mehrere Tage. Diese eine Anforderung kann die Latenz für diese Minute erhöhen, wenn die Zugriffsprotokolle abgeschlossen und angemeldet werden.

2. Wie geschrieben in:

"RAM-Nutzung für ein System, das working effizient kann mehr als 90 % betragen, da RAM, der vom System nicht anderweitig verwendet wird, vom Webobjekt-Cache verwendet wird. Wenn Ihr System nicht experiencing schwerwiegende Leistungsprobleme auftreten und dieser Wert nicht bei 100 % liegt, ist das System operating normal."

Hinweis: Proxy-Pufferspeicher ist eine Komponente, die diesen RAM verwendet

Fehlerbehebung mit SHD-Protokollen

Andere Prozesse mit hoher Last

Wenn die Last des anderen Prozesses hoch ist, überprüfen Sie die Tabelle-1 aus diesem Artikel und lesen Sie die Protokolle zu diesem Prozess.

Hohe Latenz

Wenn Sie eine hohe Latenz in den SHD-Protokollen festgestellt haben, müssen Sie die Proxy_track-Protokolle in /**data/pub/track_stats/** überprüfen. Finden Sie den Zeitrahmen, in dem die Latenz hoch ist. In der Proxy-Spur haben Sie einige Datensätze, die mit der Latenz zusammenhängen. Die Zahlen vor den einzelnen Abschnitten geben die Gesamtanzahl der Vorfälle seit dem letzten Neustart an. Beispiel für diesen Code:

```
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
```

Innerhalb von 5 Minuten betrug die Anzahl der Anfragen von Clients, die 6309,6 ms oder mehr beanspruchten, 80. Sie müssen also die Zahlen in jedem Zeitrahmen subtrahieren, um den genauen Wert zu erhalten, den Sie für diese Elemente berücksichtigen müssen:

Client Time (Client-Zeit): Zeit, die zwischen Client und SWA vergeht

Trefferzeit: Cachetreffer: Die angeforderten Daten befinden sich im Cache und können an den Client übermittelt werden.

Fehlzeit: Fehlgeschlagener Cache: Die angeforderten Daten befinden sich nicht im Cache oder sind nicht aktuell und können nicht an den Client übermittelt werden.

Servertransaktionszeit: Zeit, die zwischen SWA und Webserver vergeht

Auch diese Werte müssen bei der Leistungsprüfung berücksichtigt werden:

Benutzerzeit: 160.852 (53,33%)
Systemzeit: 9,768 (3,256%)

In Track-Status-Protokollen werden die Informationen alle 5 Minuten (300 Sekunden) protokolliert. In diesem Beispiel ist die Benutzerzeit 160.852 die Zeit (in Sekunden), in der die CPU mit Aufgaben zur Bearbeitung von Benutzeranfragen geladen wurde. Die Systemzeit ist die Zeit, zu der die SWA Netzwerkereignisse verarbeiteten, z. B. Routing-Entscheidungen. Die Summe dieser beiden Prozentwerte gibt die Gesamt-CPU-Last zu diesem Zeitpunkt an. Wenn die Benutzerzeit zu lang ist, müssen Sie eine

Konfiguration mit hoher Komplexität berücksichtigen.

Zugehörige Informationen

- **WSA AsyncOS - Versionshinweise**
- **Kompatibilitätsmatrix für Cisco Secure Email und Web Manager**
- **Konnektivitätsprüfung für Upgrades und Updates**
- **Technischer Support und Downloads von Cisco**

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.