SHD口グを使用したセキュアWebアプライアンスのパフォーマンスのトラブルシューティング

内容

はじめに

このドキュメントでは、システム健全性デーモン(SYD)口グ(shd_logs)と、この口グに関するSecure Web Appliance(SWA)のパフォーマンス問題のトラブルシューティング方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- インストールされている物理または仮想Secure Web Appliance(SWA)。
- ライセンスの有効化またはインストール
- セキュアシェル(SSH)クライアント。
- セットアップウィザードが完了しました。

- SWAへの管理アクセス。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

SHD口グとは

SHDログには、SWAのパフォーマンス関連プロセスの統計情報のほとんどが1分ごとに記録されます。

SHDログ行の例を次に示します。

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

SHDログは、コマンドラインインターフェイス(CLI)およびファイル転送プロトコル(FTP)から使用できます。グラフィカルユーザインターフェイス(GUI)からログを表示するオプションはありません。

SHDログへのアクセス

CLI から、

1. CLIでgrepまたはtailと入力します。
2. リストから「shd_logs Type: SHD Logs Retrieval: FTP Poll」を検索し、関連する番号を入力します。
3. 「正規表現を入力してgrepします。 正規表現を入力してログ内を検索できます。たとえば、日付と時刻を入力できます。
4. Do you want this search to be case insensitive? (この検索で大文字小文字を区別しますか？) [Y]> SHD_Logsでこのオプションが不要な大文字と小文字を区別して検索する必要がない限り、デフォルトのままにしておくことができます。
5. 一致しない行を検索しますか？[N]> Grep正規表現以外のすべてを検索する必要がない場合は、この行をデフォルトとして設定できます。
6. Do you want to tail the logs? (ログの最後を表示しますか？) [N]>このオプションは、grepの出力でのみ使用できます。これをデフォルト(N)にすると、現在のファイルの最初の行のSHDログが表示されます。
7. Do you want to paginate the output? (出力をページングしますか？) [N]> 「Y」を選択すると、出力はlessコマンドの出力と同じです。行とページを移動したり、ログ内を検索したり(/キーワードを入力してEnterキーを押します)、qを入力してログビューを終了したりできます。

FTPから：

1. GUI > Network > Interfacesの順に選択して、FTPが有効になっていることを確認します。
2. FTP経由でSWAに接続します。
3. Shd_logsフォルダ。ログが含まれます。

SHDログフィールド

SHDログの各フィールドの詳細は次のとおりです。

フィールド番号	[名前(Name)]	識別子	説明

8	CPULd	割合% 0～99	CPU負荷 OSによって報告されたシステムで使用されているCPUの合計パーセント
10	デスクトップUi	割合% 0～99	ディスク使用率 /dataパーティションで使用される間隔
12	ラムティル	割合% 0～99	RAM Utilization OSによって報告された空きメモリの割合
14	要求	要求/秒	要求 過去1分間のトランザクション（要求）の平均数
16	帯域	Kb/s	帯域幅の節約 過去1分間に節約された平均帯域幅。 – 過去1分間の平均で節約されたSNMP帯域幅に相当
18	遅延[1]	ミリ秒(ms)	最後の1分間の平均待機時間（応答時間） は、アクセスログの2番目のフィールドを取得します。このフィールドは、TCP接続がエンドユーザからWSA（または、接続が復号化されていない場合はエンドユーザから

			Webサーバ）までにかかる時間を示します WSAは、過去1分間のアクセスログに記録された各要求の時間を合計し、これらの要求数で除算して、SHDの平均遅延を取得します
20	キャッシュヒット	番号	過去1分間のキャッシュヒットの平均。 – 過去1分間のSNMPキャッシュヒット平均に相当
22	CliConn	番号	現在のクライアント接続数 クライアントからWSAへ - SNMPの現在のクライアント接続数の合計に相当
24	SrvConn	番号	現在のサーバー接続の合計数 WSAからWebサーバへ - SNMPの現在の合計サーバ接続数に相当します。
26	MemBuf [2]	割合% 0～99	メモリバッファ 現在の空きプロキシバッファメモリの合計。
28	SwpPgOut	番号	OSによって報告された、スワップアウトされ

			たページの数。 ページファイルまたはページングファイルは、RAMが完全に使用されたときに情報を格納するための一時的な場所として使用されるハードドライブ上の領域です。
30	プロキシLd	割合% 0 ~ 99	proxプロセスのロード すべての着信要求を処理するプロセス (HTTP/HTTPS/FTP/SOCKS)
32	Wbrs_WucLd	割合% 0 ~ 99	Webレピュテーションコーリングロード 実際のWBRSスキャンエンジンに使用されるプロセス。プロキシプロセスは、要求スキャンプロセスと対話してWBRSスキャンを実行します。
34	LogLd	割合% 0 ~ 99	プロキシログのロード
36	RptLd	割合% 0 ~ 99	レポートエンジンロード レポートデータベースを作成するプロセス。'reportd'は'haystackd'と対話してWebトラッキングデータベースを作成します。

38	WebrootLd	割合% 0 ~ 99	Webrootアンチマルウェア負荷
40	SophosLd	割合% 0 ~ 99	Sophosウイルス対策ロード
42	McafeeLd	割合% 0 ~ 99	Mcafee Antivirusロード
44	WTTLd	割合% 0 ~ 99	Webトラフィックタップ
46	AMPLd	割合% 0 ~ 99	高度なマルウェア防御(AMP)

1. たとえば、WSAでの要求が多くなく、ある時点で長時間の接続が終了した場合（数日間など）、SHDログの遅延で高いピークが発生する可能性があります。この単一の要求によって、アクセスログの終了時とログイン時の遅延が増加する可能性があります。

2.次のように記載されています。

「RAMの使用量が working システムで使用されていないRAMがWebオブジェクトキャッシュで使用されるため、効率的に90 %を超える可能性があります。使用しているシステムが experiencing

重大なパフォーマンスの問題があり、この値が100%でスタックしていない場合、システムは operating 正常な状態です。」

注：プロキシバッファメモリは、このRAMを使用するコンポーネントの1つです

SHDログを使用したトラブルシューティング

その他のプロセス高負荷

他のプロセスの負荷が高い場合は、この記事の表1を確認し、そのプロセスに関連するログを読んでください。

高遅延

SHDログで高い遅延が見られた場合は、/data/pub/track_stats/でProxy_trackログを確認する必要があります。 遅延の大きいタイムフレームを見つけます。 プロキシトラックには、遅延に関連するいくつかのレコードがあります。 各セクションの前の数字は、前回のリブート以降の発生回数の合計です。たとえば、次のコードでは次のようになります。

```
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
```

5分間で、6309.6ミリ秒以上かかったクライアント要求の数は80要求です。したがって、正確な値を得るには、各時間枠の数値を減算する必要があります。次の項目を考慮する必要があります。

クライアント時間：クライアントからSWAまでにかかる時間。

ヒットタイム：キャッシュヒット：要求されたデータはキャッシュ内にあり、クライアントに配信できます。

ミス時間：キャッシュミス：要求されたデータがキャッシュにないか、または最新ではないため、クライアントに配信できません。

サーバトランザクション時間：SWAからWebサーバまでにかかる時間。

また、パフォーマンスチェックのプロセスでは、次の値を考慮する必要があります。

ユーザ時間：160.852(53.33 %)

システム時間：9.768(3.256%)

Track Stat口グには、5分（300秒）ごとに情報が記録されます。 この例では、ユーザ時間160.852は、ユーザ要求を処理するためのタスクがCPUにロードされた時間（秒単位）です。 システム時間は、SWAがルーティング決定などのネットワークイベントを処理した時間です。 これら2つのパーセンテージの合計は、その時点でのCPU負荷の合計です。 ユーザ時間が長い場合は、複雑度の高い設定を考慮する必要があることを意味します。

関連情報

- WSA AsyncOSリリースノート
- Cisco Secure Email and Web Managerの互換性マトリクス
- 接続チェックのアップグレードと更新
- シスコテクニカルサポートおよびダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。