Secure Web Applianceでの要求デバッグログの設定

内容

はじめに

このドキュメントでは、Secure Web Appliance(SWA)でデバッグログを要求する手順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推奨されます。

- SWAのCommand Line Interface(CLI；コマンドラインインターフェイス)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たものです。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。

デバッグログの要求

SWAのデバッグログの要求は、特定のHTTPまたはHTTPSトランザクションやクライアントマシンに関する非常に詳細なエンドツーエンドのデバッグ情報と最高レベルのトレースレベルの情報をキャプチャするように設計された、特殊なログタイプです。多数の要求にわたる集約されたイベントを記録する標準のプロキシログとは異なり、要求デバッグログは、特定の要求の処理に関係するすべてのWebプロキシモジュール（認証、URLフィルタリング、復号化、マルウェアスキャン、レピュテーションサービスなど）からのデバッグ出力を1つの相関ログストリームに集約します。このログタイプは純粋に詳細な診断を目的としており、GUIではなくCLIでのみ作成できます

要求デバッグログは、標準のログに十分な詳細が含まれていない、複雑または断続的なプロキシの問題をトラブルシューティングする際に不可欠です。これにより、管理者とCisco TACは、各処理段階で単一の要求がどのように処理されたかを正確に追跡でき、予期しないポリシーの一致、スキャンの遅延、認証の失敗、エンジン間の判定の不整合などの根本原因を突き止めることができます。ログは1つのトランザクションに重点を置いているため、システム全体ですべてのプロキシモジュールに対してデバッグログを有効にすることによって運用上のオーバーヘッドやパフォーマンスに影響を与えることなく、最大限の可視性が得られます。このため、要求デバッグログは、高度な調査時に正確で効率的かつ低リスクの診断ツールとなります。

要求デバッグログの設定

ステップ 1：CLIにログインし、logconfigを実行してnewを選択します。

ステップ 2 Request Debug Logsに関連付けられている番号を選択し、Enterキーを押します。

ステップ 3 ログの名前を入力します。

ステップ 4 ロギングレベルとしてTraceを選択します。

ステップ 5拡張ロギングの収集を要求された場合は、モジュールを選択します。 複数の項目を選択する場合は、カンマ区切りリストまたは範囲リスト（1、3、4、3-7など）を使用します。

ヒント:TACから特定のモジュールの要求がない場合は、すべてのモジュール（1 ~ 30など）を選択することをお勧めします。

ステップ 6 拡張ロギングを有効にする要求の数を指定します。この数の要求がキャプチャされる

と、ロギングは自動的に停止します。

注:トラブルシューティング時には、トラフィックの状態に基づいて妥当な値を選択することが重要です。たとえば、専用のテストマシンが使用されており、バックグラウンドトラフィックが最小限の場合は、より少ないリクエスト数で十分です。ただし、オペレーティングシステムの更新、ブラウザのバックグラウンド要求、Webexなどのアプリケーションなど、バックグラウンドのアクティビティが多い環境では、高い値を選択することで関連するトランザクションが確実にキャプチャされます。

ステップ 7 クライアントIPアドレス、宛先IPアドレス、または宛先ドメインを選択して、拡張ロギングの要求一致基準を定義します。

注：ほとんどの場合、単一のWebサイトへのアクセスのトラブルシューティングを行う場合でも、クライアントIPアドレスを選択することを推奨します。このアプローチでは、ページのロード中に生成されたすべてのWeb要求がキャプチャされます。追加のURLへのバックグラウンド要求は、すぐには表示されない可能性があります。 ただし、この方法は、バックグラウンドのインターネットトラフィックが最小限の専用テストマシンを使用する場合に最も効果的です。クライアントによって大量の追加トラフィック（オペレーティングシステムのアップデート、ブラウザのバックグラウンドサービス、Webexのようなアプリケーションなど）が生成される環境では、宛先ドメインまたは宛先IPアドレスでフィルタリングする方が適切です。

ヒント:正確な障害ポイントが不明な場合は、ブラウザのHAR口グを収集して問題が発生している特定のURLまたはドメイン（たとえば、ページの読み込み障害や高い遅延）を特定し、そのドメインを要求デバッグログの基準で設定できます。

ステップ 8口グを取得する方法を選択します。FTP Pollを選択すると、ログはSWAに保存されます。

ステップ 9 ログファイルに使用するファイル名を定義するか、[Enter]を押して現在生成されているファイル名を受け入れます。

ステップ 10 時間ベースのログファイルのロールオーバーでは、定義された数の要求が満たされた後にログ記録が停止するため、[いいえ]を選択します。

ステップ 11 最大ファイルサイズをバイト単位で定義するか、[Enter]を押して現在の値を受け入れます。

ヒント:ログファイルのサイズを大きく定義すると、ログのダウンロードとレビューがより困難になる場合があります。個々の口グファイルのサイズを増やす代わりに、ログファイル

の数を増やすことをお勧めします（次の手順）。 このアプローチにより、管理容易性が向上すると同時に、非常に大きなファイルを作成することなく、必要なすべてのデバッグ情報を確実にキャプチャできます。

ステップ 12 ステップ5でロギング用に選択したプロキシモジュールの数と、ステップ7で定義した要求一致基準に基づいて、ログファイルの最大数を設定します。適切なファイル制限を選択することは、すべての関連デバッグ情報が早期にログを停止せずにキャプチャされるようにするために重要です。この結果、ログが不完全または欠落する可能性があります。

ステップ 13「Should an alert when files are removed due to the maximum number of files allowed?」というプロンプトが表示されたら、「No」を選択します。 これにより、特にトラブルシューティングの目的でRequest Debug Logsが意図的に生成される場合に、通常のログローテーション中に不要なアラートが回避されます。

手順 14： Do you want to compress logs (yes/no)?というプロンプトが表示されたら、Noを選択します。 これにより、ログファイルが圧縮解除され、トラブルシューティング中の確認と分析が容易になります。

手順 15： Enterを押してウィザードを終了します

ステップ 16：commitと入力してEnterキーを押し、変更を保存します

```
SWA_CLI> logconfig

Currently configured logs:
1. "accesslogs" Type: "Access Logs" Retrieval: FTP Poll
2. "adc_logs" Type: "ADC Engine Logs" Retrieval: FTP Poll
...
[Output removed to simplify readability]
...
55. "welcomeack_logs" Type: "Welcome Page Acknowledgement Logs" Retrieval: FTP Poll

Choose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- HOSTKEYCONFIG - Configure SSH host keys.
- AUDITLOGCONFIG - Adjust settings for audit logging.
[]> new

Choose the log file type for this subscription:
1. ADC Engine Framework Logs
2. ADC Engine Logs
...
[Output removed to simplify readability]
...
53. Request Debug Logs
...
```

```
[Output removed to simplify readability]
...
[1]> 53

Please enter the name for the log:
[]> Request_Debug_Logs

Log level:
1. Critical
2. Warning
3. Information
4. Debug
5. Trace
[3]> 5

Choose modules where enhanced request logging is to be performed.
Multiple selections can be made in the form of a comma separated or range list (e.g. 1,3,4 or 3-7)
Choosing the Default Proxy will enable enhanced logging across modules:
1. Default Proxy
2. Access Control Engine
3. Proxy Configuration
4. Disk Manager
5. Memory Manager
6. McAfee Integration Framework
7. Sophos Integration Framework
8. Webroot Integration Framework
9. Webcat Integration Framework
10. Connection Management
11. Authentication Framework
12. HTTPS
13. FTP proxy
14. WCCP Module
15. License Module
16. SNMP Module
17. WBRS Integration Framework
18. Logging Framework
19. Data Security Module
20. Miscellaneous Proxy Modules
21. DCA Engine Framework
22. AVC Engine Framework
23. Cloud Connector
24. SOCKS Proxy
25. Advanced Malware Protection
26. ArchiveScan module in proxy
27. Web Traffic Tap module in proxy
28. Bandwidth Control
29. Http2 proxy
30. ADC Engine Framework
[1]> 1-30

Please enter the number of requests for which to perform enhanced logging:
[1]> 100

Choose the request criteria for logging:
1. Client IP Address
2. Destination Domain
3. Destination IP Address
[1]> 1

Specify source IP address
[]> 10.20.3.15
```

```
Choose the method to retrieve the logs:
1. FTP Poll
2. FTP Push
3. SCP Push
[1]> 1

Filename to use for log files:
[Request_Debug_Logs.text]>

Do you want to configure time-based log files rollover? [N]>

Please enter the maximum file size:
[10485760]>

Please enter the maximum number of files:
[10]> 50

Should an alert be sent when files are removed due to the maximum number of files allowed? [N]>

Do you want to compress logs (yes/no)
[n]>

Currently configured logs:
1. "Request_Debug_Logs" Type: "Request Debug Logs" Retrieval: FTP Poll
2. "accesslogs" Type: "Access Logs" Retrieval: FTP Poll
3. "adc_logs" Type: "ADC Engine Logs" Retrieval: FTP Poll
...
[Output removed to simplify readability]
...
56. "welcomeack_logs" Type: "Welcome Page Acknowledgement Logs" Retrieval: FTP Poll


SWA_LIC> commit

Warning: In order to process these changes, the proxy
process will restart after Commit. This will cause a brief
interruption in service. Additionally, the authentication
cache will be cleared, which might require some users to
authenticate again.
```

関連情報

- AsyncOS 15.2 for Cisco Secure Web Applianceユーザガイド
- セキュアなWebアプライアンスのベストプラクティスの使用
- セキュアなWebアプライアンスの口グへのアクセス
- Microsoft Serverを使用したSWAでのSCPプッシュ口グの設定

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。