

アクセスログのパフォーマンスパラメータの設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[追加のアクセスログの作成](#)

[GUIからの新しいアクセスログの作成](#)

[CLIからの新しいアクセスログの設定](#)

[ログにアクセスするためのパフォーマンスパラメータのカスタムフィールドの追加](#)

[変更の確認](#)

[カスタムフィールドのフィールドの説明](#)

[関連情報](#)

はじめに

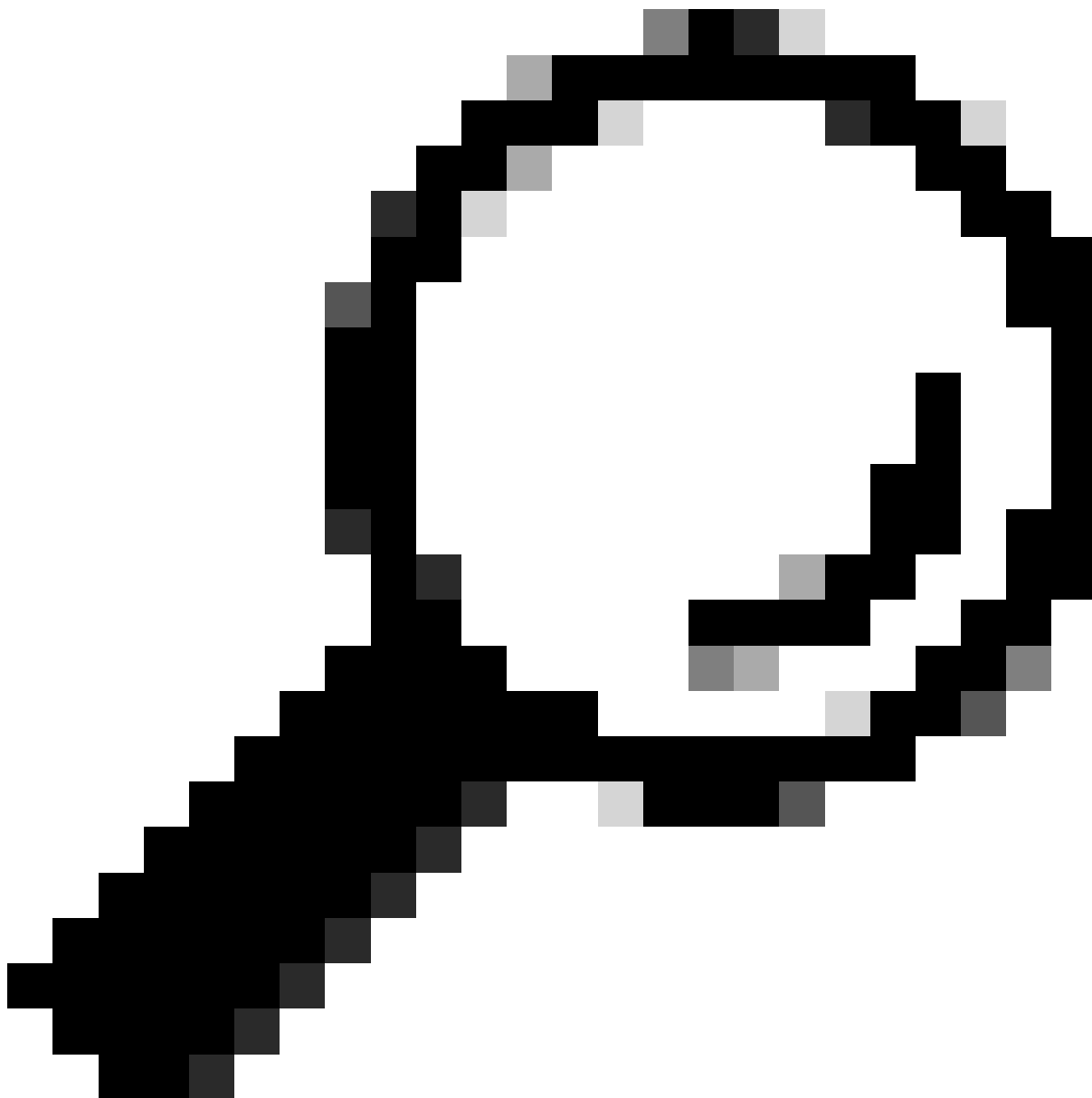
このドキュメントでは、Performance parameter (PM ; パフォーマンスパラメータ) のカスタムフィールドをSecure Web Appliance(SWA)のアクセスログに追加する手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- SWA管理インターフェイスへのセキュアシェルプロトコル(SSH)アクセス。
- SWA管理インターフェイスへのグラフィカルユーザインターフェイス(GUI)アクセス



ヒント:SWAデータパーティションの20 %以上の空きディスク領域を確保するのが最適です。コマンドラインインターフェイス(CLI)のstatus detailコマンドの出力で、ディスクの使用状況を確認できます。

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。

背景説明

遅延の問題があり、トラフィックがSWA経由でプロキシされる場合、遅延の根本原因のトラブルシューティングにアクセスログが役立ちます。現在のアクセスログの設定を変更したり、カスタムフィールドにパフォーマンスパラメータを追加して新しいアクセスログを作成したりできます。

追加のアクセスログの作成

状況によっては、内部ポリシーまたはその他の設定が原因で、現在のアクセスログを変更できない場合があります。この制限を克服するために、別のアクセスログを作成し、新しいアクセスログにカスタムパフォーマンスパラメータを追加できます。

GUIからの新しいアクセスログの作成

ステップ 1 : GUIにログインします。

ステップ 2 : System Administration メニューから、Log Subscriptionsを選択します。

System Administration

Policy Trace

Alerts

Log Subscriptions

Return Addresses

SSL Configuration

Users

Network Access

System Time

Time Zone

Time Settings

Configuration

Configuration Summary

Configuration File

要求ヘッダー	:%:<h	最初のバイトの後に要求ヘッダーをサーバに書き込む待機時間。
サーバへの要求	:%:<b	ヘッダーの後に要求本文をサーバーに書き込むまでの待機時間です。
クライアントへの 1番目のバイト	:%:1>	クライアントに書き込まれた最初のバイトの待機時間。
クライアント本体	:%:b>	完全な本文がクライアントに書き込まれるまでの待機時間。
Rx待機時間（ミ リ秒）：最初の要 求バイト	:%:1<	Webプロキシがサーバへの接続を開始してから、最初にサーバへの書き込みが可能になるまでの時間。Webプロキシがトランザクションを完了するために複数のサーバに接続する必要がある場合は、それらの回数の合計になります。
要求ヘッダー	:%:h<	最初のバイトの後の完全なクライアントヘッダーの待機時間。
クライアント本体	:%:b<	完全なクライアント本体の待機時間。
第1応答バイト	:%:>1	サーバからの最初の応答バイトの待機時間。
応答ヘッダー	:%:>h	最初の応答バイトの後のサーバヘッダーの待機時間。
サーバ応答	:%:>b	これは基本的に、SWAがサーバからHTTPヘッダーを取得したが、その後の応答バイトを待っていることを意味します。これは、サーバからの実際の内容です。
ディスクキャッシ ュ	:%:>c	Webプロキシがディスクキャッシュから応答を読み取るのに必要な時間。
認証応答	:%:<a	Webプロキシが要求を送信した後、Webプロキシ認証プロセスから応答を受信するまでの待機時間。
認証の合計	:%:>a	Webプロキシ認証プロセスからの応答を受信するための待機時間には、Webプロキシが要求を送信するために必要な時間が含まれます。
DNS応答	:%:<d	Webプロキシがドメイン名要求(DNS)要求をWebプロキシDNSプロセスに送信するのに要した時間です。

DNS合計	:%:>d	DNS結果をWebプロキシに返すためにWebプロキシDNSプロセスが要した時間。
WBRs応答	:%:<r	Webプロキシが要求を送信した後、Webレピュテーションフィルタからの応答を受信するまでの待機時間。
WBRs合計	:%:>r	Webレピュテーションフィルタから判定を受け取るまでの待機時間には、Webプロキシが要求を送信するために必要な時間が含まれます。
AVC応答	:%:A>	Webプロキシが要求を送信した後、Application Visibility and Control(AVC)プロセスから応答を受信するまでの待機時間。
AVC合計	:%:A<	AVCプロセスからの応答を受信するための待機時間には、Webプロキシが要求を送信するために必要な時間が含まれます。
DCA応答	:%:C>	Webプロキシが要求を送信した後、動的コンテンツ分析エンジンから応答を受信するまでの待機時間。
DCA合計	:%:C<	動的コンテンツ分析エンジンから判定を受信するまでの待機時間には、Webプロキシが要求を送信するために必要な時間が含まれます。
McAfee応答	:%:m>	Webプロキシが要求を送信した後、McAfeeスキャンエンジンから応答を受信するまでの待機時間。
McAfee合計	:%:m<	McAfeeスキャンエンジンから判定を受け取るまでの待機時間には、Webプロキシが要求を送信するために必要な時間が含まれます。
Sophos応答	:%:p>	Webプロキシが要求を送信した後、Sophosスキャンエンジンから応答を受信するまでの待機時間。
Sophos合計	:%:p<	Sophosスキャンエンジンから判定を受け取るまでの待機時間には、Webプロキシが要求を送信するために必要な時間が含まれます。
AMP応答	:%:e>	Webプロキシが要求を送信した後、AMPエンジンから応答を受信するまでの待機時間。
合計AMP	:%:e<	AMPエンジンから判定を受信するまでの待機時間には、Webプロキシが要求を送信するために必要な時間が含まれます。

遅延	%x; %L	遅延とリクエストの現地時間 (YYYY:hh:mm:ss +nnnn、DD/MMM/YYYYの形式で人間が読み取れる形式)。このフィールドは、アクセスログに二重引用符で囲まれて書き込まれます。 このフィールドを使用すると、各ログエントリのエポック時間からのローカル時間を計算しなくても、ログを問題に関連付けることができます。
クライアントポート	%F	クライアント側から使用されるポート番号。
サーバ IP アドレス	%k	WebサーバのIPアドレス。
サーバポート番号	%p	Webサーバポート番号。

関連情報

- [AsyncOS 14.5 for Cisco Secure Web Applianceユーザガイド – GD \(一般導入\) – シスコ](#)
- [Cisco Webセキュリティアプライアンスのベストプラクティスガイドライン – Cisco](#)

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。