Stealthwatch® System

6.10.x

プロキシ ログの設定ガイド

著作権および商標

NOTICE

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

目次

1

はじめに

概要

Stealthwatch System プロキシ ログのネットワーク プロキシ サーバからユーザ情報を収集するには、フロー コレクタが情報を受信でき、SMC によって[フロ—プロキシレコード(Flow Proxy Records)] ページに情報が表示されるように、プロキシ サーバ ログを設定する必要があります。このページには、プロキシ サーバを経由するネット—ワーク内のトラフィックの URL とアプリケーション名が表示されます。

このドキュメントでは、さまざまなプロキシ サーバのログを設定するために必要なさまざまな手順について説明します。対象サーバは、Blue Coat、McAfee、Cisco WSA、Squid です。このドキュメントでは、プロキシ サーバがネットワークの一部としてすでに実行されていることを前提としています。手順では、フロー コレクタに必要なファイルが指定され、情報が提供されるように、プロキシのログを設定する方法について説明します。

Stealthwatch プロキシ ログを設定するには、次の手順を実行します。

1. プロキシ サーバを設定します。
    a. Blue Coat
    b. McAfee
    c. Cisco WSA
    d. Squid
2. フローコレクタを設定します。
3. フローを確認します。

設定時の重要なガイドライン

いずれかのプロキシ ログを設定する場合、必ず次のガイドラインに従う必要があります。

- フロー コレクタとプロキシは、フロー レコードとプロキシ レコードを一致させるために、同じ NTP サーバを使用するか、共通のソースから時間を受信する必要があります。
- フロー コレクタの IP アドレスを設定するときに、プロキシ ログで調査する必要があるエクスポータとエンド ポイントからデータを収集するフロー コレクタを選択してください。

サポートへの問い合わせ

テクニカル サポートが必要な場合は、次のいずれかを実行してください。

- 最寄りのシスコ パートナーにご連絡ください。
- Cisco Stealthwatch サポートのお問い合わせ先 :
  - Web でケースを開く場合 : http://www.cisco.com/c/en/us/support/index.html
  - 電子メールでケースを開く場合 : tac@cisco.com
  - 電話でサポートを受ける場合 : 800-553-2447(米国)
  - ワールドワイド サポート番号 : www.cisco.com/en/US/partner/support/tsd_cisco_worldwide_contacts.html

2

Blue Coat プロキシ ログの設定

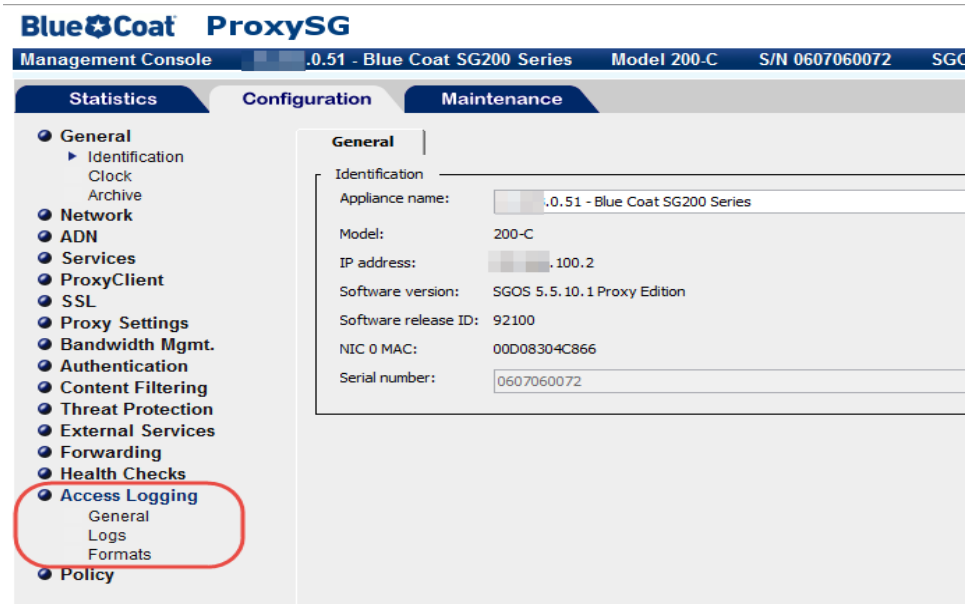
この章では、Stealthwatch System に配信するために Blue Coat プロキシ ログを設定する手順について説明します。

> **(注)** テストに使用された Blue Coat プロキシ バージョンは、SG V100、SGOS 6.5.5.7 SWG Edition でした。

形式の作成

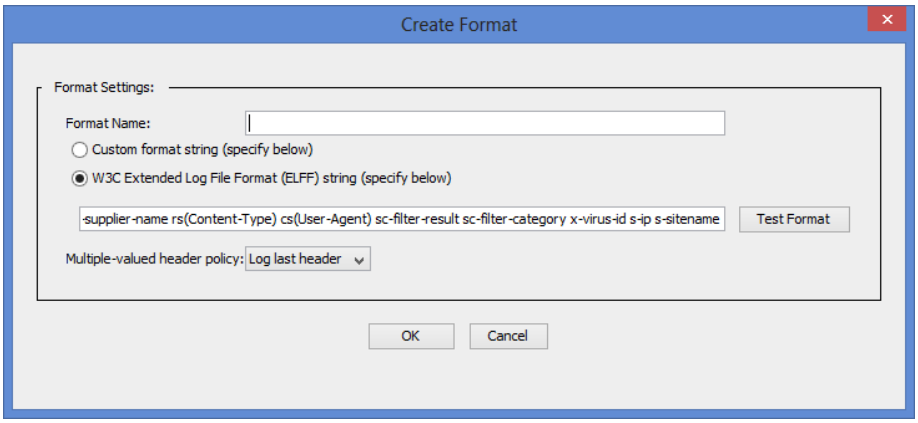
新しいログ形式を作成するには、次の手順を実行します。

1. ブラウザで、Blue Coat プロキシ サーバにアクセスします。
2. [設定(Configuration)] タブをクリックします。



3. 管理コンソールのメイン メニューで、[アクセスログ(Access Logging)] > [形式(Formats)] をクリックします。

4. ページの下部にある [新規(New)] ボタンをクリックします。[形式の作成(Create Format)] ページが開きます。



5. [形式名(Format Name)] フィールドに、新しい形式の名前を入力します。
6. [W3C拡張ログファイル形式(ELFF)(W3C Extended Log File format (ELFF))]のオプションを選択します。
7. [形式(Format)] フィールドに、次の文字列を入力します。

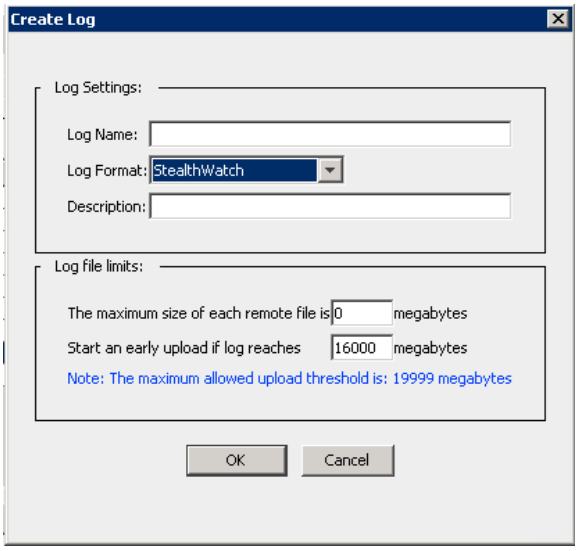
```
timestamp duration c-ip c-port r-ip r-port s-ip s-port cs-bytes sc-bytes cs-user cs-host cs-uri
```

8. [OK] をクリックします。次の項「新規ログの作成」に進みます。

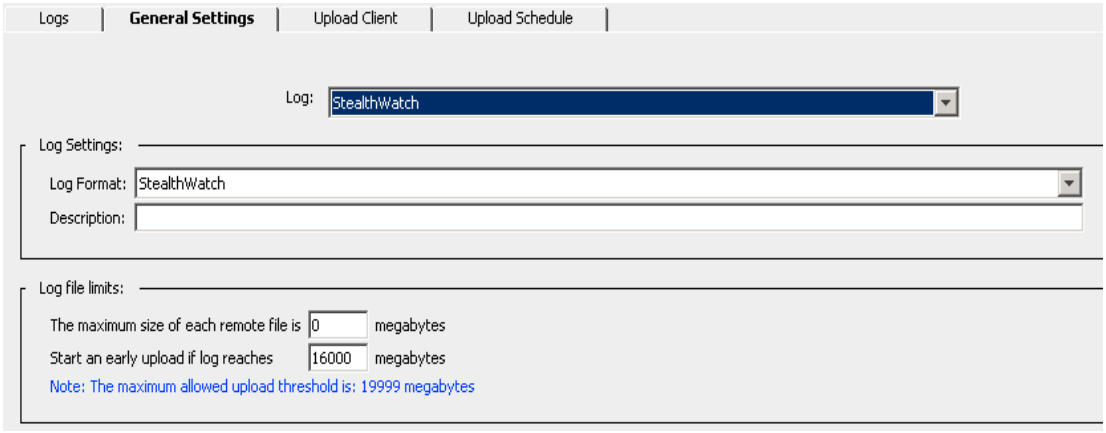
新規ログの作成

ログを作成するには、次の手順に従います。

1. メイン メニューで、[アクセスログ(Access Logging)] > [ログ(Logs)] をクリックし、新しいログ形式を選択します。[ログ(Log)] ページが開きます。



2. [一般設定(General Settings)] タブをクリックします。

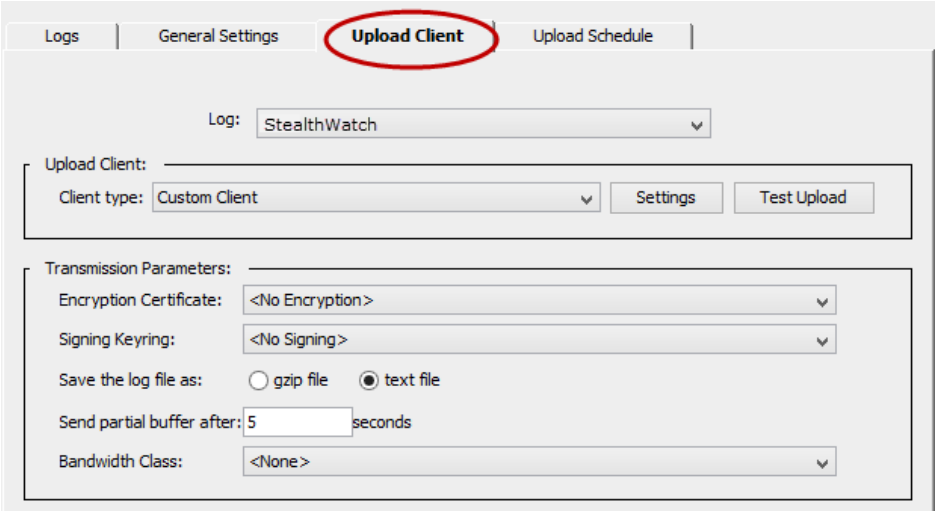


3. [ログ形式(Log Format)] ドロップダウン リストから、手順 1 で作成したログを選択します。
4. [説明(Description)] フィールドに、新規ログの説明を入力します。
5. ページの下部にある [適用(Apply)] ボタンをクリックします。次の項「アップロード クライアントの設定」に進みます。

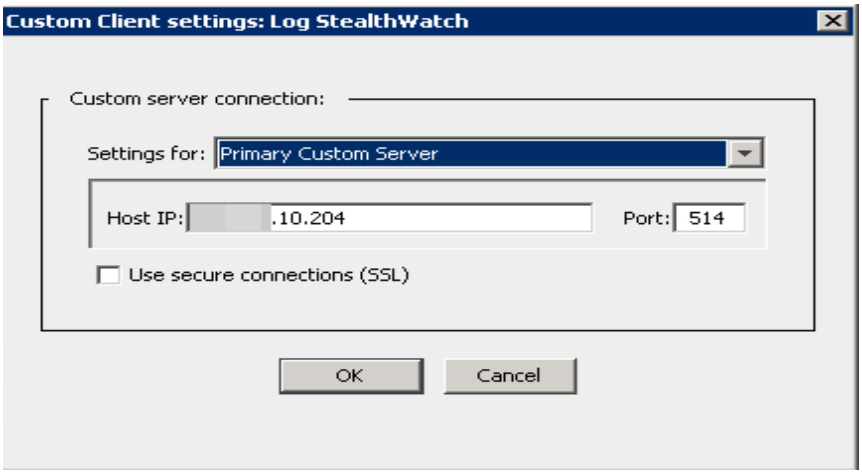
アップロード クライアントの設定

アップロード クライアントを設定するには、次の手順を実行します。

1. [アップロード クライアント(Upload Client)] タブをクリックします。[アップロード クライアント(Upload Client)] ページが開きます。



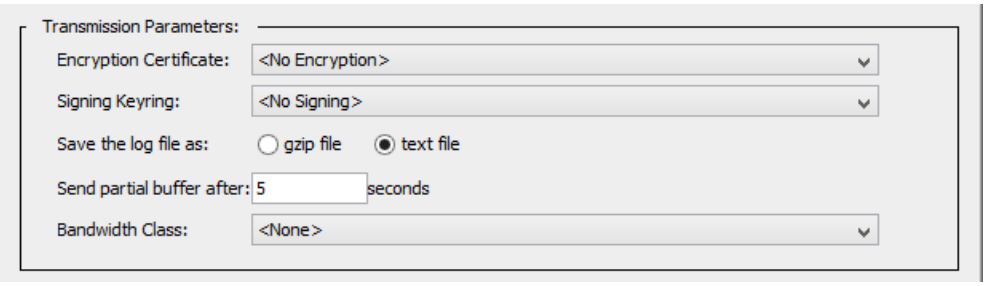
2. [クライアントタイプ(Client type)] ドロップダウン リストから、[カスタムクライアント(Custom Client)] を選択します。
3. [設定(Settings)] ボタンをクリックします。[カスタムクライアント設定(Custom Client settings)] ページが開きます。



4. 該当するフィールドに、フロー コレクタの IP アドレスとプロキシ パーサーのリスニング ポートを入力します。

> **(注)** この時点では SSL はサポートされていません。

5. [OK] をクリックします。

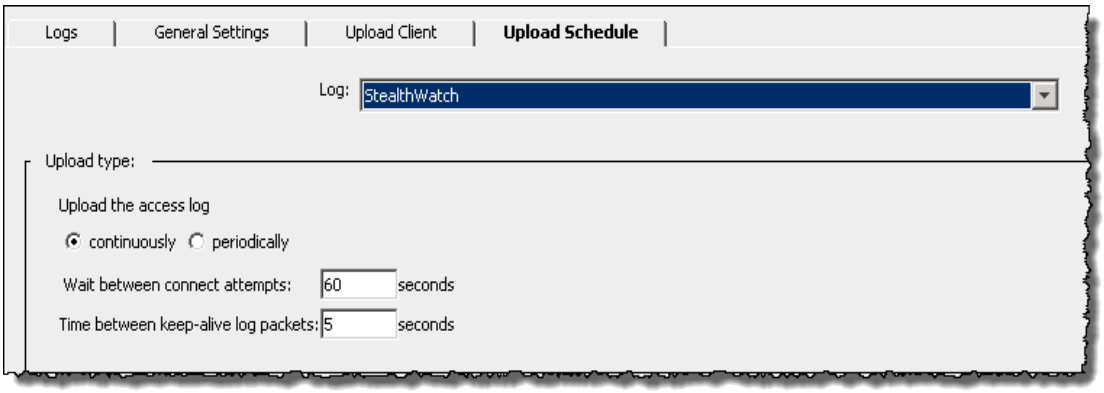


6. 送信パラメータでは、次の手順を実行します。
   a. [暗号化証明書(Encryption Certificate)] で、[暗号化なし(No encryption)] を選択します。
   b. [キーリングの署名(Signing Keyring)] ドロップダウン リストから、[署名なし(no signing)] を選択します。
   c. [ログファイルの保存形式(Save the log file as)] から、[テキストファイル(Text file)] オプションを選択します。
   d. [部分バッファを送信するまでの時間(Send partial buffer after)] テキスト ボックスに 5 と入力します。
   e. [アップロード スケジュール(Upload Schedule)] タブをクリックし、[アクセスログのアップロード(Upload the access log)] で [継続的(continuously)] オプションを選択します。
   f. [接続試行の間隔(Wait between connect attempts)] フィールドに 60 と入力します。
   g. [キープアライブログパケット間の時間(Time between keep-alive log packets)] フィールドに 5 と入力します。
7. ページ下部の [適用(Apply)] ボタンをクリックします。次の項「アップロード スケジュールの設定」に進みます。

アップロード スケジュールの設定

アップロード スケジュールを設定するには、次の手順を実行します。

1. [アップロード スケジュール(Upload Schedule)] タブをクリックします。



2. [アクセスログのアップロード(Upload the access log)] で [継続的(continuously)] を選択します。
3. [接続試行の間隔(Wait between connect attempts)] は 60 秒です。
4. [キープアライブログパケット間の時間(Time between keep-alive log packets)] は 5 秒です。
5. ページ下部の [適用(Apply)] ボタンをクリックします。

これで、フロー コレクタの Blue Coat プロキシ ログの設定が完了しました。

注記

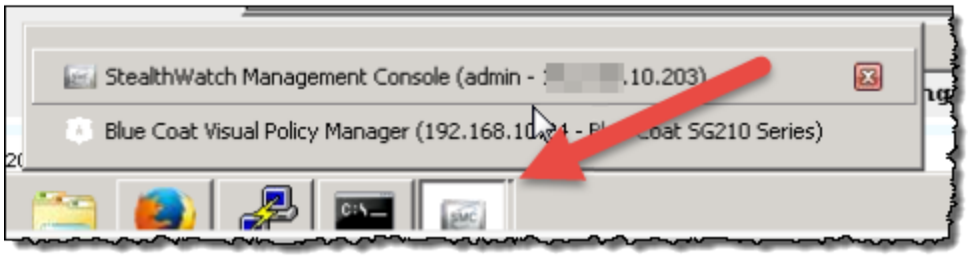
設定に関する補足説明を示します。

- フロー コレクタとプロキシは、フロー レコードとプロキシ レコードを一致させるために、同じ NTP サーバにあるか、共通のソースから時間を受信する必要があります。
- サポートされているプロキシのログ出力メカニズムは 1 つのみです。特定の理由ですでにログをエクスポートしている場合は、プロキシ レコードを取得して解析することはできません。
- UDP はサポートされていません。

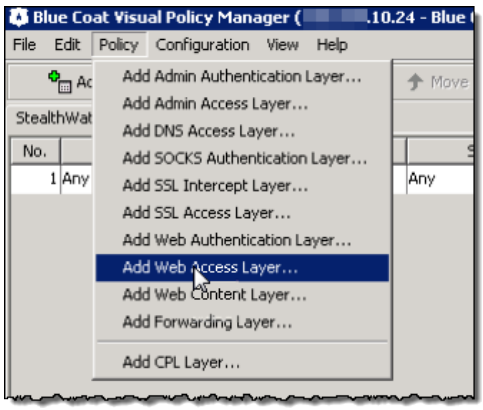
Visual Policy Manager の設定

Visual Policy Manager の設定を使用すると、プロキシ ログがフロー コレクタに送信されていることを確認できます。

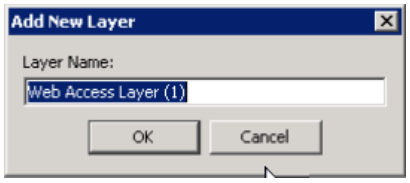
1. メイン メニューの [設定(Configuration)] タブ ページで、[ポリシー(Policy)] > [Visual Policy Manager] をクリックします。Visual Policy Manager が開きます。



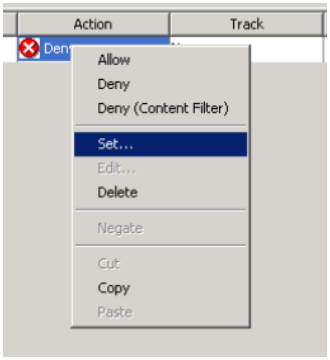
2. 設定されているログの下部にある [起動(Launch)] ボタンをクリックします。ログ ウィンドウの Visual Policy Manager が開きます。



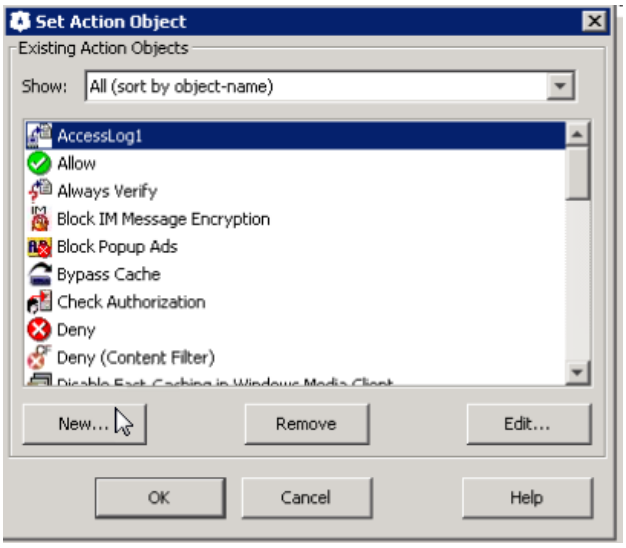
3. [ポリシー(Policy)] > [Webアクセスレイヤを追加(Add Web Access Layer)] をクリックします。[新規レイヤの追加(Add New layer)] 画面が表示されます。



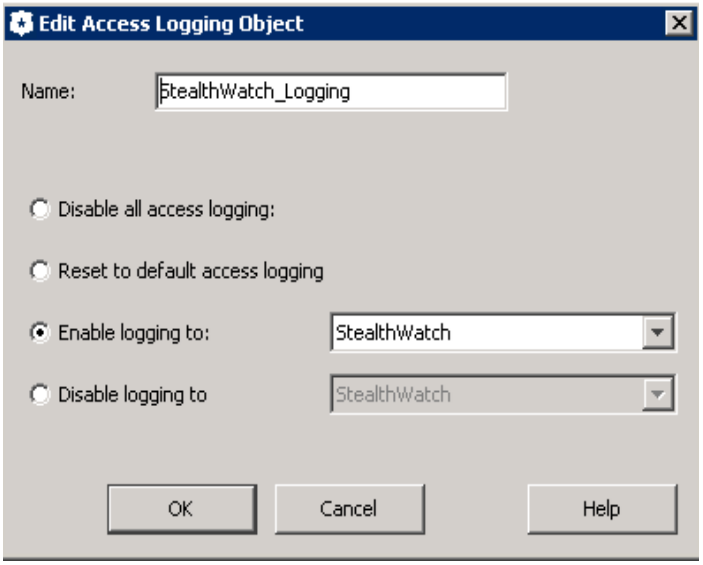
4. 新しいレイヤの名前を入力して、[OK] をクリックします。



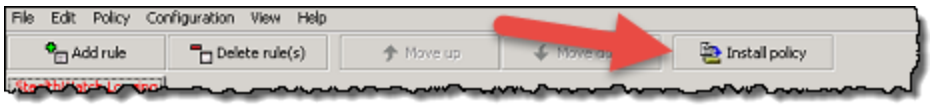
5. [アクション(Action)] 列の [拒否(Deny)] を右クリックしてから、[設定(Set)] をクリックします。[アクションオブジェクトの設定(Set Action Object)] ダイアログが開きます。



6. [新規(New)] をクリックし、[アクセスログを変更(Modify Access Logging)] を選択します。[アクセスログオブジェクトの編集(Edit Access Logging Object)] ダイアログが表示されます。

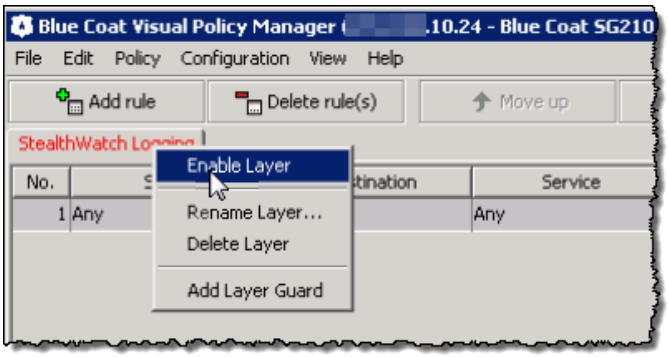


7. [次へのログを有効化(Enable logging to)] をクリックします。
8. ログの名前を入力し、ログを選択します。
9. [OK] をクリックします。オブジェクトが追加されます。
10. [アクションオブジェクトの設定(Set Action Object)] ダイアログで、[OK] をクリックします。



11. 右上にある [ポリシーをインストール(Install Policy)] ボタンをクリックします。
12. [いいえ(No)] をクリックし、次のウィンドウで [OK] をクリックします。

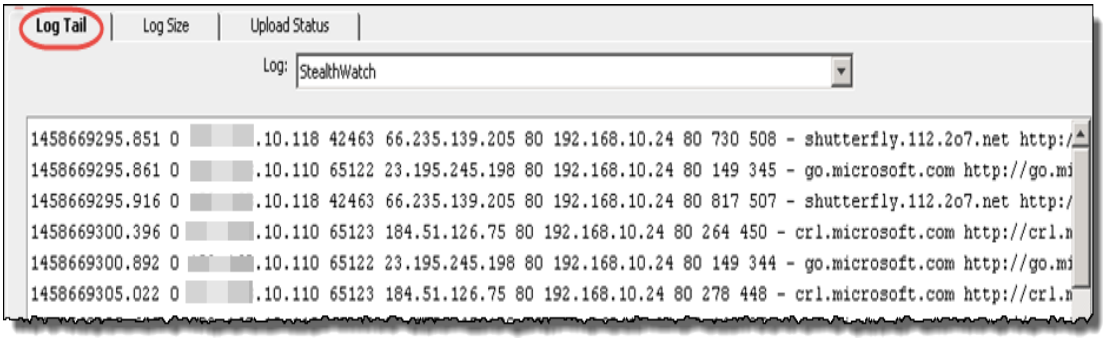
13. Blue Coat Visual Policy Manager を再度起動します。



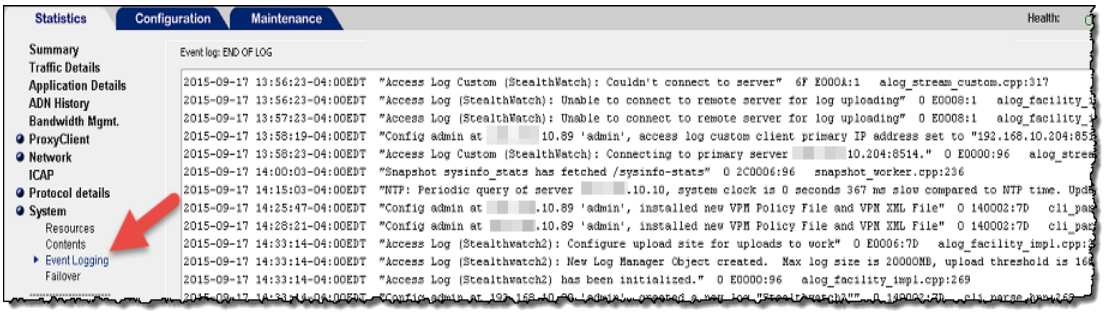
14. [ロギング(Logging)] タブを右 クリックしてから、[レイヤの有 効 化(Enable Layer)] を選 択します。
15. [ポリシーをインストール(Install Policy)] ボタンをクリックします。[インストールされたポリシー(Policy Installed)] が開きます。
16. [OK] をクリックして、

17. [統 計(Statistics)] タブをクリックし、ログ メニューでログを選 択します。

18. メイン メニューで、[アクセスログ(Access Logging)] をクリックしてから、[ログテール(Log Tail)] タブをクリックします。[ログテール(Log Tail)] ウィンドウが開きます。



19. ページの下部にある [テールの開始(Start Tail)] ボタンをクリックします。
20. 統計のメイン メニューで、[システム(System)] > [イベントロギング(Event Logging)] をクリックします。このページでは、ログ ファイルがフロー コレクタにアップロードされ、変更が行われたかどうかを示します。プロキシがフロー コレクタに接続されているかどうかを示します。



21. 続いて「フローコレクタの設定」の章に進み、syslog 情報を受信するようにフロー コレクタを設定します。

3

McAfee プロキシ ログの設定

この章では、Stealthwatch System に配信するために McAfee Web Gateway の McAfee プロキシ ログを設定する手順について説明します。

重要： McAfee プロキシの XML コンフィギュレーション ファイルをダウンロードしていることを確認してください。Stealthwatch ダウンロードおよびライセンス センター(https://lancope.flexnetoperations.com) にアクセスして、ファイル、Readme、プロキシ ログの XML コンフィギュレーション ファイルを取得してください。

(注) テストに使用された McAfee プロキシ バージョンは 7.4.2.6.0 - 18721 でした。

McAfee プロキシ ログを設定するには、次の手順を実行します。

1. XML ファイル(FlowCollector_[date]_McAfee_Log_XML_Config_[v].xml) をダウンロードし、適切な場所に保存します。

   (注) 「date」は XML ファイルの日付を示し、「v」は McAfee プロキシ バージョンのバージョンを示します。必ず McAfee プロキシと同じバージョン番号の XML ファイルを選択してください。

   次の手順に従って取得します。

   a. Stealthwatch ダウンロードおよびライセンス センター(https://lancope.flexnetoperations.com) にアクセスします。ログイン ページが開きます。

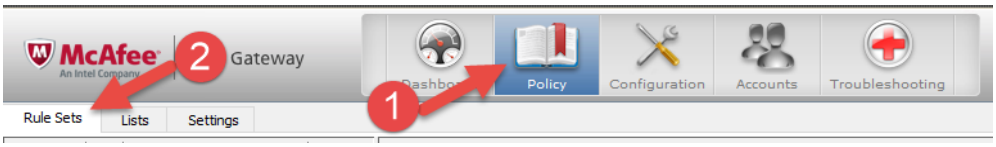
   b. ログイン ID とパスワードを該当するフィールドに入力し、[ログイン(Login)] をクリックします。製品ホームページが開きます。

   c. [ダウンロード(Downloads)] をクリックします。

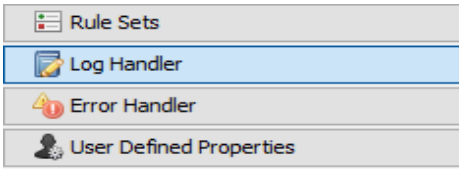
   d. リンク「vX.X Updates for the FlowCollector NetFlow Series」を選択します。

   e. XML ファイルをダウンロードして保存します。

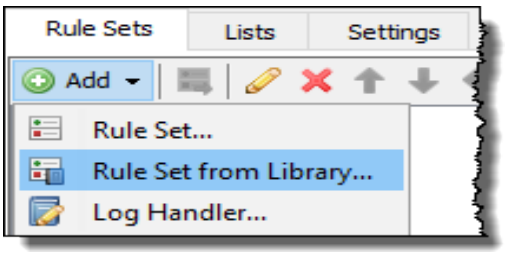
2. McAfee プロキシ サーバにログインします。



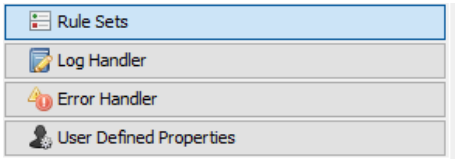
3. [ポリシー(Policy)] アイコンをクリックし、[ルールセット(Rule Sets)] タブをクリックします。



4. [ログハンドラ(Log Handler)] を選択し、[デフォルト(Default)] を選択します。



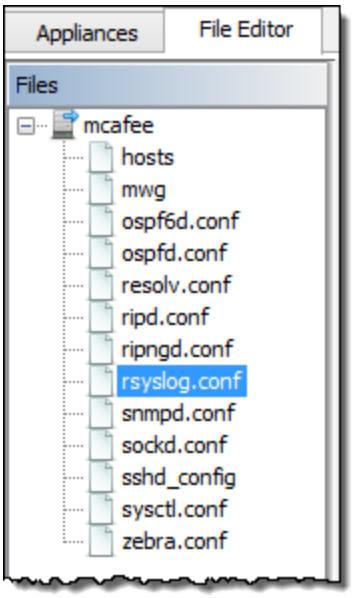
5. [追加(Add)] > [ライブラリのルールセット(Rule Set from the Library)] をクリックします。



6. [ファイルからのインポート(Import from file)] をクリックし、XML ファイルを選択します。
7. インポートされたログ ハンドラから [mcafeelancopelog] を選択します。

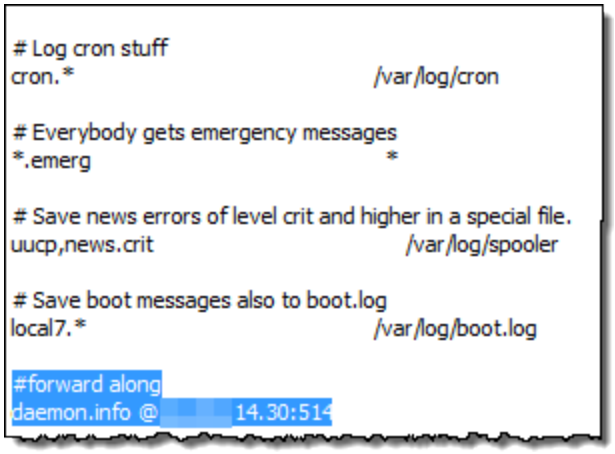
> **(注)** ルール セットと「create access logline」および「send to syslog」のルールが有効になっていることを確認します。

8. ページの上部にある [設定(Configuration)] アイコンをクリックします。
9. ページの左側にある [ファイルエディタ(File Editor)] タブをクリックし、rsyslog.conf ファイルを選択します。



10. テキスト ボックスの下部（ファイル リストの横）に、次のテキストを入力します。

```
daemon.info @[FlowCollector IP Address:514]
```



> **重要**：プロキシ ログで調査する必要があるエクスポータとエンド ポイントからデータを収集するフローコレクタを選択していることを確認してください。

11. 次の行をコメント アウトします。`*.info;mail.none;authpriv.none;cron.none`
12. 次の行を追加します。`*.info;daemon.!=info;mail.none;authpriv.none;cron.none -/var/log/messages`
13. ページの右上にある [変更の保存（Save Changes）] ボタンをクリックします。

14. 続いて「フローコレクタの設定」の章に進み、syslog 情報を受信するようにフロー コレクタを設定します。

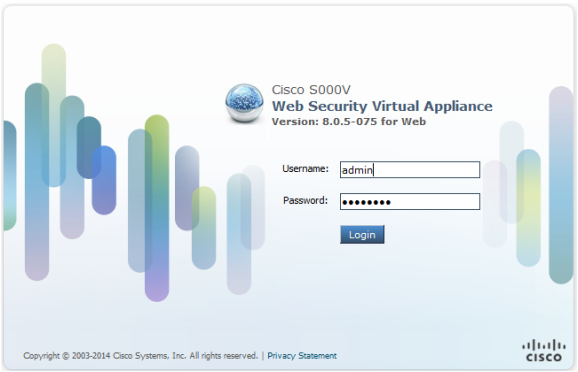
4

Cisco Web Security Appliance (WSA) プロキシ ログの設定

この章では、Stealthwatch System に配信するために Cisco プロキシ ログを設定する手順について説明します。

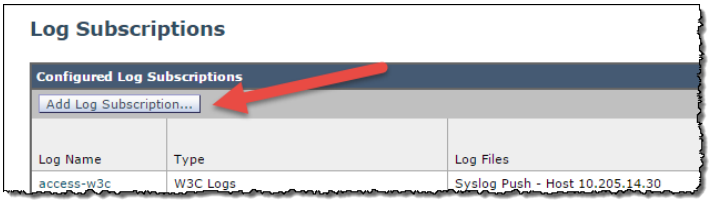
(注) Cisco WSA プロキシは、プロキシ デバイスの追加に関して仮想 IP をサポートしていません。

Cisco プロキシ ログを設定するには、次の手順を実行します。

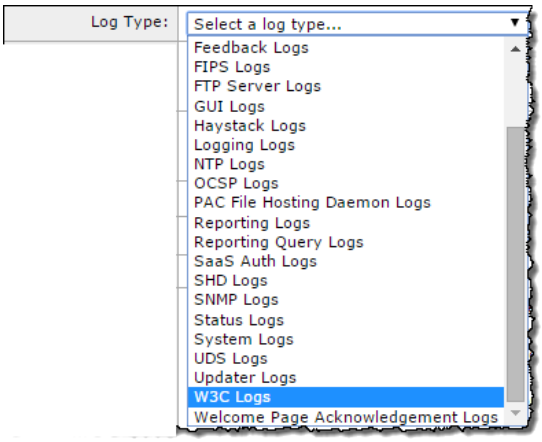


1. Cisco プロキシ サーバにログインします。

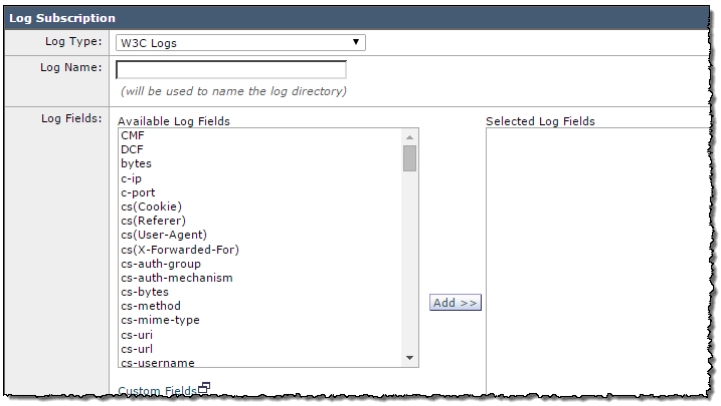
2. メイン メニューで、[システム管理(System Administration)] > [ログサブスクリプション(Log Subscriptions)] をクリックします。[ログサブスクリプション(Log Subscriptions)] ページが開きます。



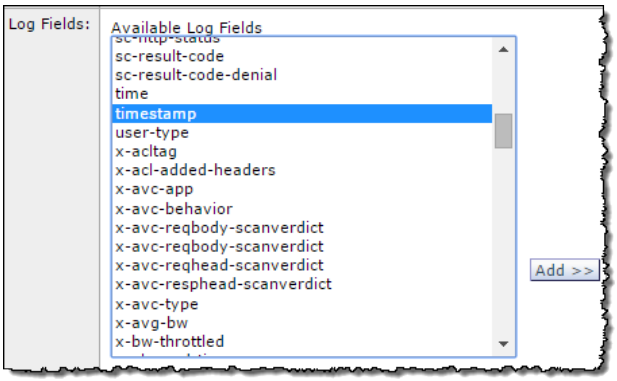
3. [ログサブスクリプションを追加(Add Log Subscriptions)] ボタンをクリックします。新しい [ログサブスクリプション(Log Subscriptions)] ページが開きます。



4. [ログタイプ(Log Type)] ドロップダウン リストから、[W3Cログ(W3C Logs)] を選択します。使用可能な W3C ログ フィールドが表示されます。



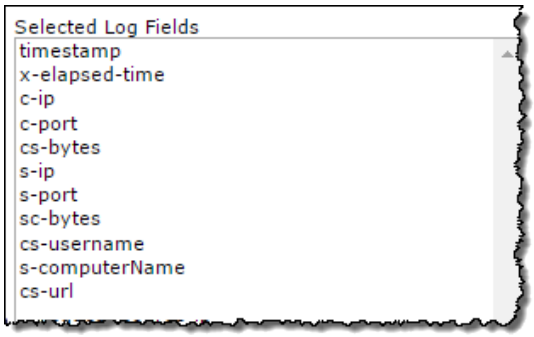
5. [ログ名(Log Name)] フィールドに、使用するログの名前を入力します。



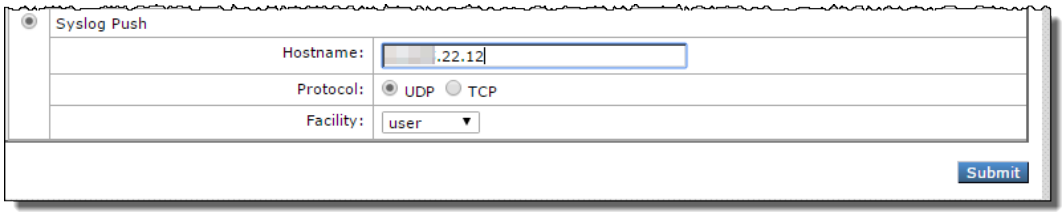
6. [使用可能なログフィールド(Available Log Fields)] リストから [タイムスタンプ(Timestamp)] を選択し、[追加(Add)] ボタンをクリックして [選択されたログフィールド(Selected Log Fields)] リストに移動させます。
7. 次の各ログ フィールドに対して前の手順を順に繰り返します。

    a. x-elapsed-time
    b. c-ip
    c. c-port
    d. cs-bytes
    e. s-ip
    f. s-port
    g. sc-bytes
    h. cs-usernames
    i. s-computerName
    j. cs-url

    [選択されたログフィールド(Selected Log Fields)] リストには、これらのフィールドが図のように含まれている必要があります。



8. ページの下部までスクロールし、[Syslog送信(Syslog Push)] オプションを選択します。



9. [ホスト名(Hostname)] フィールドに、フローコレクタの IP アドレスまたはプロキシがログを送信するホスト名を入力します。

重要：プロキシ ログで調査する必要があるエクスポータとエンド ポイントからデータを収集するフローコレクタを選択していることを確認してください。

10. [送信（Submit）] をクリックします。新しいログが [ログサブスクリプション（Log Subscriptions）] リストに追加されます。
11. 続いて「フローコレクタの設定」の章に進み、syslog 情報を受信するようにフロー コレクタを設定します。

5

SQUID プロキシ ログの設定

この章では、Stealthwatch System に配信するために Squid プロキシ ログを設定する手順について説明します。ログを設定するには、SSH を使用してプロキシ サーバ上のファイルを編集する必要があります。

Squid プロキシ ログを設定するには、次の手順を実行します。

1. Squid を実行しているマシンのシェルにログインします。
2. squid.conf が含まれているディレクトリ(通常は /etc/squid) に移動して、エディタで開きます。
3. squid.conf に次の行を追加して、ロギングを設定します。

```
logformat access_format %ts%03tu %<tt %>a %>p %>st %<A %<st %<la %<lp %la %lp
%un %ru
access_log syslog:user.6 access_format
```

4. 次を使用して squid を再起動します。

```
/etc/init.d/squid3 restart
```

5. フロー コレクタにログを転送するように、Squid サーバの syslog サービスを設定します。これは Linux ディストリビューションによって異なりますが、syslog-ng の場合は次を /etc/syslog-ng に追加します。

```
# Audit Log Facility BEGIN
filter bs_filter { filter(f_user) and level(info) };
destination udp_proxy { udp("10.205.14.15" port(514)); };
log {
source(s_all);
filter(bs_filter);
destination(udp_proxy);
};
# Audit Log Facility END
```

重要: プロキシ ログで調査する必要があるエクスポータとエンド ポイントからデータを収集するフロー コレクタを選択していることを確認してください。

6. `/etc/init.d/syslog-ng` restart を使用して `syslog-ng` を再起動します。
7. 続いて「フローコレクタの設定」の章に進み、syslog 情報を受信するようにフロー コレクタを設定します。

6

フロー コレクタの設定

プロキシ サーバを設定したら、データを受信するようにフロー コレクタを設定する必要があります。

syslog 情報を受信するようにフロー コレクタを設定するには、次の手順を実行します。

1. フロー コレクタの管理インターフェイスにログインします。
2. メイン メニューで、[設定(Configuration)] > [プロキシの取得(Proxy Ingest)] をクリックします。[プロキシサーバ(Proxy Servers)] ページが開きます。
3. プロキシ サーバの IP アドレスを入力します。
4. [プロキシタイプ(Proxy Type)] ドロップダウン リストから、プロキシ サーバを選択します。

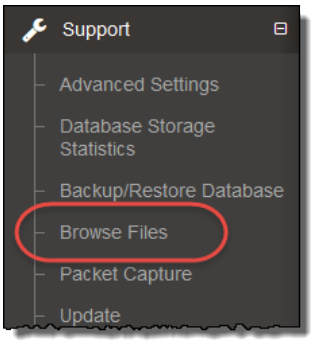
(注) プロキシ サーバのタイプがリストにない場合、この時点ではプロキシ ログを使用できません。

5. [プロキシID(Proxy ID)] フィールドに、プロキシ サーバの IP アドレスを入力します。
6. [プロキシサービスポート(Proxy Service Port)] フィールドに、プロキシ サーバのポート番号を入力します。
7. プロキシ サーバによってアラームをトリガーするには、[アラームから除外(Excluded from Alarming)] チェックボックスをオフにします。
8. [追加(Add)] をクリックします。
9. [適用(Apply)] をクリックします。ページ上部にある [プロキシの取得(Proxy Ingest)] テーブルに、プロキシ サーバが表示されます。
10. 次の章「フローの確認」に進みます。

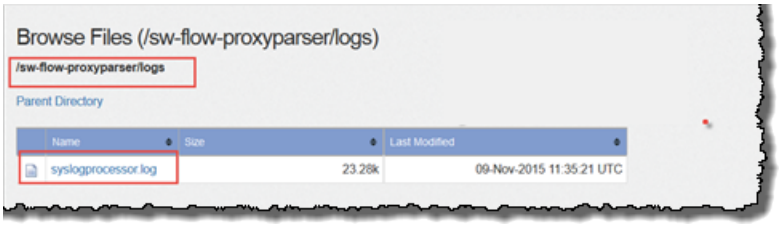
7

フローの確認

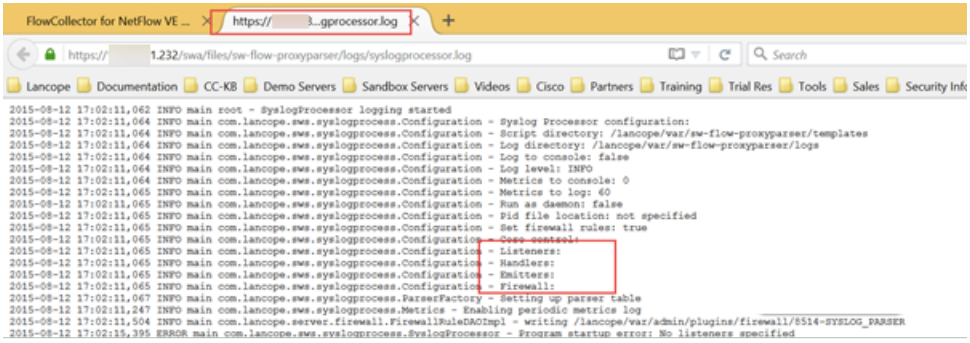
フローを受信していることを確認するには、次の手順を実行します。



1. フロー コレクタの管理インターフェイスで、メイン メニューの [サポート(Support)] > [ファイルの参照(Browse Files)] をクリックします。[ファイルの参照(Browse Files)] ページが開きます。



2. syslog ファイルを開きます。



3. マークされているファイルがブランクではないことを確認します。ブランクである場合、問題があります。

- Listeners にはプロキシの数が表示されます。
- Handlers は 1 つのみで、データを解析します。
- エミッタはハンドラから解析済みのデータを取得し、エンジンが求めている形式に変換します。
- ファイアウォール

4. カウントが増加し、データの受信を示していることを確認します。