リモート SCP サーバへの WSA ログの転送

目次

概要

このドキュメントでは、Cisco Web セキュリティ アプライアンス（WSA）から、リモートの Secure Copy（SCP）サーバにログを転送する方法について説明します。 WSA ログ（アクセス ログや認証ログなど）のロールオーバーまたは循環時に、これらのログを SCP プロトコルで外部サーバに転送できるように、ログを設定できます。

このドキュメントの情報は、ログ ローテーション ルールの設定方法と、SCP サーバへの正常な転送に必要なセキュア シェル（SSH）キーの設定方法について説明しています。

前提条件

要件

このドキュメントに関しては個別の要件はありません。

使用するコンポーネント

このドキュメントは、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。

本書の情報は、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、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

設定

リモート サーバ上で SCP を使用して WSA ログを取得できるように設定するには、次の手順を実行します。

1. WSA Web GUI にログインします。

2. [システム管理（System Administration）]> [サブスクリプション（Log Subsctiptions）] に移動します。

3. この取得メソッドを設定するログの名前（**access logs** など）を選択します。

4. [Retrieval Method] フィールドで、[SCP on Remote Server]を選択します。

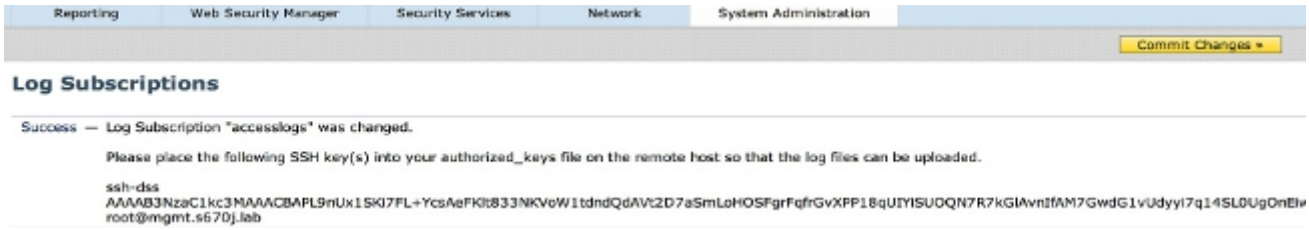
5. SCP ホスト名または SCP サーバの IP アドレスを入力します。

6. SCP ポート番号を入力します。
   注: デフォルトの設定は **port 22** です。
7. ログが転送される SCP サーバ ターゲット ディレクトリのフル パス名を入力します。

8. SCP サーバ認証ユーザのユーザ名を入力します。

9. 自動的にホスト キーをスキャンするか、または手動でホスト キーを入力するには、**ホスト キー検査**を有効化します。

10. [Submit] をクリックします。 これで SCP サーバの **authorized_keys** ファイル内に置く SSH キーは、[Edit Log Subscription] ページの上部付近に表示されます。 WSA からの成功メッセージの例を以下に示します。



11. [Commit Changes] をクリックします。

12. SCP サーバが Linux サーバまたは Unix サーバ、あるいは Macintosh マシンである場合は、SSH キーを WSA から SSH ディレクトリ内にある **authorized_keys** ファイルにペーストします。

    Users > <username> > .ssh ディレクトリに移動します。

    WSA SSH キーを **authorized_keys** ファイルにペーストし、変更を保存します。
    注: authorized_keys ファイルが SSH ディレクトリ内に存在しない場合は、手動で作成する必要があります。

確認

ログが SCP サーバに正常に転送されたことを確認するには、次の手順を実行します。

1. WSA の [Log Subscriptions]ページに移動します。
2. [Rollover]列で、SCP 取得用に設定したログを選択します。
3. [Rollover Now]を見つけてクリックします。
4. ログ取得用に設定した SCP サーバ フォルダに移動し、ログがその場所に転送されていることを確認します。

WSA から SCP サーバへのログ転送をモニタするには、次の手順を実行します。

1. SSH を使用して WSA CLI にログインします。
2. **grep** コマンドを入力します。
3. モニタするログの該当する番号を入力します。 たとえば、grep リストからは **system_logs** に対しては **31** と入力します。
4. ログをフィルタ処理して SCP トランザクションのみをモニタできるようにするには、[Enter the regular expression to grep] プロンプトに **scp** と入力します。
5. [Do you want this search to be case insensitive?] プロンプトには **Y** と入力します。 プロンプトで発行します。
6. [Do you want to tail the logs?] プロンプトには **Y** と入力します。 プロンプトで発行します。
7. [Do you want to paginate the output?] プロンプトには **N** と入力します。 プロンプトで発行します。 こうすると WSA は、SCP トランザクションをリアルタイムでリストします。 以下に示すのは、WSA system_logs からの正常な SCP トランザクションの例です。

```
Wed Jun 11 15:06:14 2014 Info: Push success for subscription <the name of the log>:
Log aclog@20140611T145613.s pushed to remote host <IP address of the SCP Server>:22
```

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。