

# リモート SCP サーバへの WSA ログの転送

## 目次

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[確認](#)

[トラブルシューティング](#)

## 概要

この資料にリモート Secure Copy ( SCP ) サーバに Cisco Web セキュリティ アプライアンス ( WSA ) からログを転送する方法を記述されています。 SCP プロトコルの外部サーバにときログ ロールオーバーがラップ転送されるように WSA ログを、アクセスおよび認証ログのような設定できます。

この文書に記載されている情報は 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、またログ ローテーションルールを設定する方法を記述します。

## 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

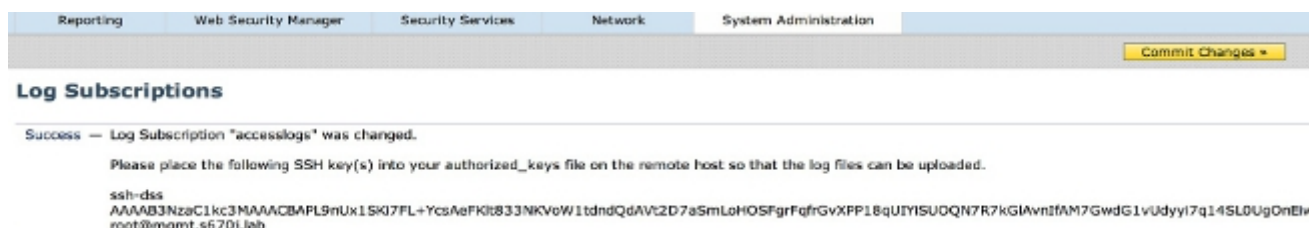
このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

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

リモートサーバの SCP と retrieved できるように WSA ログを設定するためにこれらのステップを完了して下さい:

1. WSA Web GUI にログイン して下さい。
2. システム 管理 > ログ サブスクリプションへのナビゲート。
3. この検索方式を設定することを望むアクセス ログのようなログの名前を選択して下さい。
4. 検索方式フィールドで、リモートサーバの SCP を選択して下さい。
5. SCP サーバの SCP ホスト名か IP アドレスを入力して下さい。
6. SCP ポート番号を入力して下さい。  
注: デフォルト設定はポート 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て下さい。
8. SCP サーバ認証済みユーザ向けのユーザ名を入力して下さい。
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したいと思う場合ホストキー チェックを有効に して下さい。
10. [Submit] をクリックします。SCP サーバ **authorized\_keys** にファイルを置く SSH キーは **編集ログ サブスクリプション** ページの上の近くで今現われる必要があります。WSA からの **successfulmessage** の例はここにあります:



11. [Commit Changes] をクリックします。
12. SCP がでしたり Linux または UNIXサーバまたはマッキントッシュ マシン、SSH ディレクトリにある **authorized\_keys** ファイルに貼り付ければ WSA からの SSH キーを断絶すれば:  
**ユーザ > <username> > .ssh** ディレクトリにナビゲート して下さい。

WSA SSH キーを **authorized\_keys** ファイルに貼り付け、変更を保存して下さい。

注: 1 つが SSH ディレクトリにない場合手動で **authorized\_keys** ファイルを作成して下さい。

## 確認

ログが SCP サーバに正常に転送されることを確認するためにこれらのステップを完了して下さい:

1. WSA ログ サブスクリプション ページへのナビゲート。
  2. ロールオーバー カラムで、SCP 検索のために設定したログを選択して下さい。
  3. ロールオーバーを今見つけ、クリックして下さい。
  4. ログ検索のために設定したナビゲート し、ログがその位置に転送されることを確認して下さい SCP サーバー フォルダーに。
- WSA からの SCP サーバへのログ転送を監視するためにこれらのステップを完了して下さい:

1. SSH によって WSA CLI にログインして下さい。
2. `grep` コマンドを入力して下さい。
3. 監視したいと思うログのための適切な桁数を入力して下さい。たとえば、`system_logs` のためのグレップ リストから `31` を入力して下さい。
4. SCP トランザクションだけ監視できるようにログをフィルタリングするためにグレップ プロンプトに入力で `SCP` を正規表現入力して下さい。
5. `Y` を無感覚なケースでほしいですこの検索に入力して下さいか。プロンプトで発行します。
6. `Y` をログの後につきたいと思います入力して下さいか。プロンプトで発行します。
7. `N` を出力にページを付けたいと思います入力して下さいか。プロンプトで発行します。  
WSA はそれからリアルタイムの SCP トランザクションをリストします。WSA `system_logs` からの正常な SCP トランザクションの例はここにあります:

```
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。