Microsoftサーバを使用したセキュアWebアプライアンスでのSCPプッシュログの設定

内容

はじめに

このドキュメントでは、Secure Web Appliance(SWA)のログを別のサーバに自動的にコピーするようにSecure Copy(SCP)を設定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。

- SCPの仕組み。
- SWA管理。
- Microsoft WindowsまたはLinuxオペレーティングシステムの管理。

Cisco では次の前提を満たす推奨しています。

- 物理または仮想SWAがインストールされている。

- ライセンスの有効化またはインストール
- セットアップウィザードが完了しました。

- SWAグラフィカルユーザインターフェイス(GUI)への管理アクセス。
- Microsoft Windows(Windows Server 2019またはWindows 10（ビルド1809）以降)、またはLinux System Installed。

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。

SCP

Secure Copy(SCP)の動作は、Berkeley r-toolsスイート（Berkeley大学独自のネットワーキングアプリケーションセット）から提供されるRemote Copy(RCP)の動作と似ていますが、SCPがセキュリティのためにセキュアシェル(SSH)に依存する点が異なります。また、SCPでは、認証、許可、アカウンティング(AAA)許可を設定して、ユーザが正しい特権レベルを持っているかどうかをデバイスが判断できるようにする必要があります

リモートサーバ上のSCP方式（SCPプッシュと同じ）では、Secure Copy Protocol(SCP)によってログファイルが定期的にリモートSCPサーバにプッシュされます。この方法では、SSH2プロトコルを使用するリモートコンピュータ上にSSH SCPサーバが必要です。サブスクリプションには、リモートコンピュータ上のユーザ名、SSHキー、および宛先ディレクトリが必要です。ログファイルは、ユーザが設定したロールオーバースケジュールに基づいて転送されます。

SWAログサブスクリプション

ログファイルのタイプごとに複数のログサブスクリプションを作成できます。サブスクリプションには、次のようなアーカイブおよびストレージの構成の詳細が含まれます。

- ロールオーバー設定。ログファイルのアーカイブ時期を決定します。
- アーカイブ· ログの圧縮設定。
- アーカイブされたログの取得設定。ログをリモートサーバにアーカイブするか、アプライアンスに保存するかを指定します。

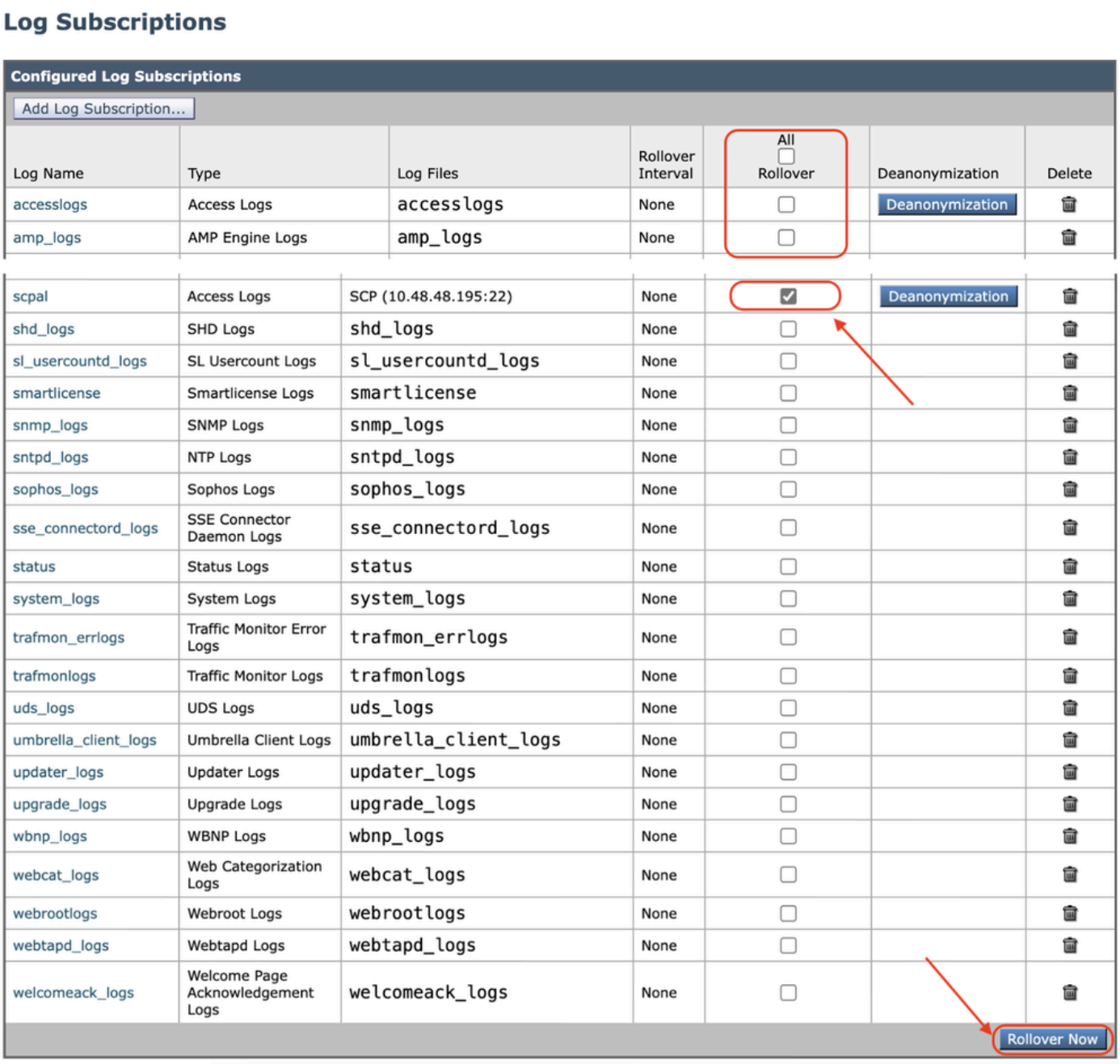
ログ· ファイルのアーカイブ

AsyncOSは、現在のログファイルがユーザ指定の最大ファイルサイズ制限または最後のロールオーバー以降の最大時間に達すると、ログサブスクリプションをアーカイブ（ロールオーバー）します。

これらのアーカイブ設定は、ログサブスクリプションに含まれています。

- ファイルサイズによるロールオーバー
- 時間によるロールオーバー
- ログ圧縮
- 検索方法

ログファイルを手動でアーカイブ（ロールオーバー）することもできます。
ステップ 1：System Administration > Log Subscriptionsの順に選択します。
ステップ 2：アーカイブするログサブスクリプションのロールオーバーカラムのチェックボックスをオンにするか、Allチェックボックスをオンしてすべてのサブスクリプションを選択します。
ステップ3:選択したログをアーカイブするには、ロールオーバーをクリックします。



イメージ – ロールオーバーGUI

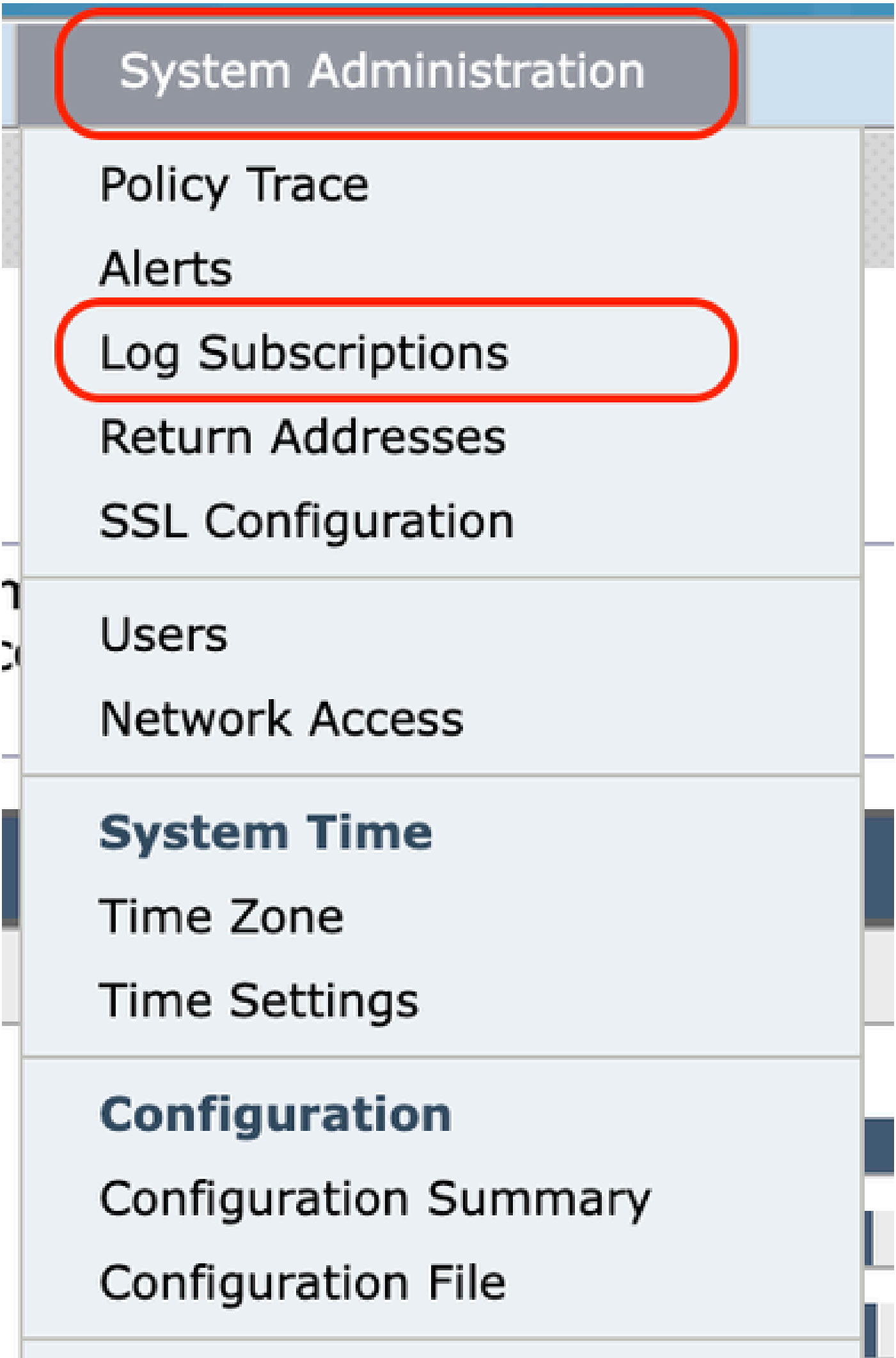
リモートサーバでのSCPによるログ取得の設定

SCPを使用してSWAからリモートサーバにログを取得するには、主に2つの手順があります。

1. ログをプッシュするようにSWAを設定します。
2. ログを受信するようにリモートサーバを設定します。

GUIからSCPリモートサーバにログを送信するためのSWAの設定

ステップ 1：SWAにログインし、System Administrationで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

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。