Transfert de log WSA à un serveur du distant SCP

Contenu

Introduction

Ce document décrit comment virer des logs de l'appliance de sécurité Web de Cisco (WSA) sur un serveur distant de Secure Copy (SCP). Vous pouvez configurer les logs WSA, tels que des logs d'accès et d'authentification, de sorte qu'ils soient expédiés à un serveur externe avec le protocole SCP quand les logs se renversent ou s'enveloppent.

Les informations dans ce document décrivent comment configurer les règles de rotation de log aussi bien que les clés de Protocole Secure Shell (SSH) qui sont exigées pour un transfert réussi à un serveur SCP.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

[Composants utilisés](#)

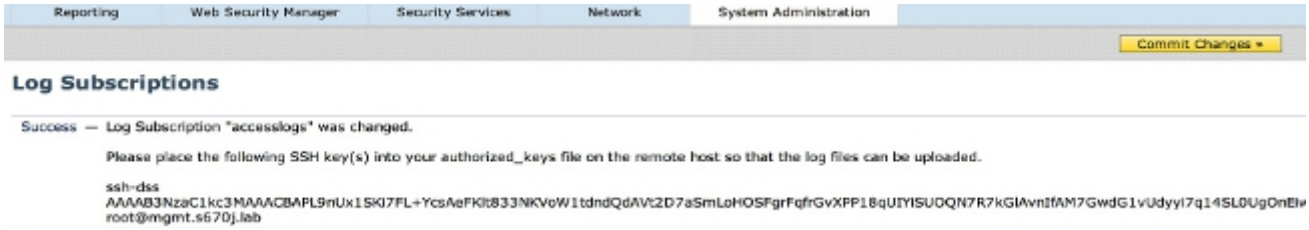
Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Configurez

Terminez-vous ces étapes afin de configurer les logs WSA de sorte qu'ils puissent retreived avec le SCP sur un serveur distant :

1. Connectez-vous dans le GUI de Web WSA.
2. Naviguez vers des **abonnements d'administration système >** de **log**.
3. Sélectionnez le nom des logs pour lesquels vous désirez configurer cette méthode de récupération, telle que des **logs d'accès**.
4. Dans le domaine de méthode de récupération, choisissez le **SCP sur le serveur distant**.
5. Écrivez le nom d'hôte SCP ou l'adresse IP du serveur SCP.
6. Introduisez le numéro de port SCP.
   Note: La valeur par défaut est le **port 22**.
7. Écrivez le nom de chemin d'accès complet du répertoire cible de serveur SCP vers lequel les les logs seront transférés.
8. Écrivez le nom d'utilisateur pour l'utilisateur authentifié par serveur SCP.
9. Si vous voulez analyser automatiquement la clé de hôte ou introduire manuellement la clé de hôte, alors **vérifier de clé de hôte d'**enable.
10. Cliquez sur **Submit**. Le ssh key que vous placerez dans les **authorized_keys de** serveur SCP le fichier devrait maintenant apparaître près du dessus de la page d'**abonnement de log d'éditer**. Voici un exemple d'un successfulmessage du WSA :



11. **Modifications de validation de** clic.
12. Si le SCP divisent est un Linux ou un serveur Unix ou un ordinateur de Macintosh, alors colle les ssh key du WSA dans le fichier situé d'**authorized_keys** dans le répertoire de SSH :

    Naviguez vers les **utilisateurs > le <username> > le** répertoire **.ssh**.

    Collez le ssh key WSA dans les **authorized_keys** classent et sauvegardent les modifications.
    Note: Vous devez manuellement créer des **authorized_keys** classez si on n'existe pas dans le répertoire de SSH.

Vérifiez

Terminez-vous ces étapes afin de vérifier que les logs sont avec succès transférés vers le serveur SCP :

1. Naviguez vers la page d'**abonnements de log** WSA.
2. Dans la colonne **inversée**, choisissez le log que vous avez configuré pour la récupération SCP.
3. Localisez et cliquez sur le **renversement maintenant**.
4. Naviguez vers le répertoire de serveur SCP que vous avez configuré pour la récupération de log et vérifiez que les logs sont transférés vers cet emplacement.

Terminez-vous ces étapes afin de surveiller le transfert de log au serveur SCP à partir du WSA :

1. Connectez-vous dans le WSA CLI par l'intermédiaire du SSH.
2. Sélectionnez la commande de **grep**.
3. Introduisez le numéro approprié pour le log que vous voulez surveiller. Par exemple, écrivez **31 de la** liste de grep pour les **system_logs**.
4. Écrivez le **scp à l'***entrer l'expression régulière à la* demande de *grep* afin de filtrer les logs de sorte que vous puissiez surveiller seulement les transactions SCP.
5. Écrivez **Y au** *vous veulent que cette recherche soit ne distinguant pas majuscules et minuscules ?* demande.
6. Écrivez **Y au** *vous veulent suivre les logs ?* demande.
7. Écrivez **N au** *vous veulent paginer la sortie ?* demande. Le WSA répertorie alors les transactions SCP en temps réel. Voici un exemple des transactions réussies SCP des system_logs WSA :

```
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
```

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.