Trasferimento del registro WSA a un server SCP remoto

Sommario

Introduzione

In questo documento viene descritto come trasferire i log da Cisco Web Security Appliance (WSA) a un server Secure Copy (SCP) remoto. È possibile configurare i log WSA, ad esempio i log di accesso e di autenticazione, in modo che vengano inoltrati a un server esterno con protocollo SCP quando i log vengono riportati o riportati a capo.

In questo documento viene descritto come configurare le regole di rotazione del log e le chiavi SSH (Secure Shell) necessarie per un trasferimento riuscito su un server SCP.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Completare questa procedura per configurare i log WSA in modo che possano essere recuperati con SCP su un server remoto:

1. Accedere all'interfaccia utente Web WSA.

2. Passare a **Amministrazione sistema > Sottoscrizioni log**.

3. Selezionare il nome del log o dei log per i quali si desidera configurare questo metodo di recupero, ad esempio **i log degli accessi**.

4. Nel campo Metodo di recupero, scegliere **SCP su server remoto**.

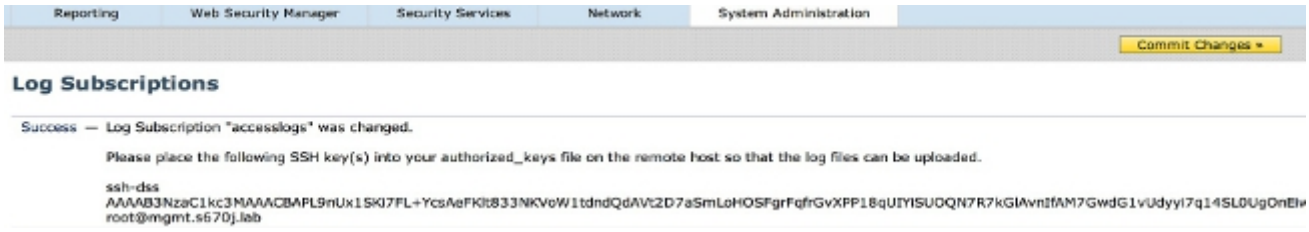
5. Immettere il nome host SCP o l'indirizzo IP del server SCP.

6. Immettere il numero della porta SCP.
   Nota: L'impostazione predefinita è **la porta 22**.
7. Immettere il percorso completo della directory di destinazione del server SCP in cui verranno trasferiti i log.

8. Immettere il nome utente per l'utente autenticato del server SCP.

9. Se si desidera eseguire la scansione automatica della chiave host o immetterla manualmente, abilitare il **controllo della chiave host**.

10. Fare clic su **Invia**. La chiave SSH che verrà inserita nel file **authorized_keys** del server SCP dovrebbe essere visualizzata nella parte superiore della pagina **Modifica log di sottoscrizione**. Di seguito è riportato un esempio di messaggio che ha avuto esito positivo dal WSA:



11. Fare clic su **Commit modifiche**.

12. Se il server SCP è un server Linux o Unix o un computer Macintosh, incollare le chiavi SSH dal server WSA nel file **authorized_keys** situato nella directory SSH:

    Passare alla directory **Utenti > <nomeutente> > .ssh**.

    Incollare la chiave SSH WSA nel file **authorized_keys** e salvare le modifiche.
    Nota: Se il file **authorized_keys** non esiste nella directory SSH, è necessario crearlo manualmente.

Verifica

Per verificare che il trasferimento dei log sul server SCP sia stato completato, completare la procedura seguente:

1. Passare alla pagina **Sottoscrizioni log** WSA.
2. Nella colonna **Rollover**, scegliere il log configurato per il recupero di SCP.
3. Individuare e fare clic su **Esegui rollover**.
4. Passare alla cartella del server SCP configurata per il recupero del log e verificare che i log vengano trasferiti in tale percorso.

Completare questa procedura per monitorare il trasferimento del log al server SCP dal server WSA:

1. Accedere alla CLI di WSA tramite SSH.
2. Immettere il comando **grep**.
3. Immettere il numero appropriato per il registro che si desidera monitorare. Ad esempio, immettete **31** dall'elenco grep per **system_logs**.
4. Immettere **scp** nel prompt *Enter the legal expression to grep* per filtrare i log in modo da poter monitorare solo le transazioni SCP.
5. Immettere **Y** in *Non si desidera effettuare la ricerca con distinzione tra maiuscole e minuscole?* .
6. Immettere **Y** in *Terminare i log?* .
7. Immettere **N** in corrispondenza di *Eseguire l'impaginazione dell'output?* . Il WSA elenca quindi in tempo reale le transazioni SCP. Di seguito è riportato un esempio di transazioni SCP riuscite dai log di sistema 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
```

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.