WSA-Protokollübertragung an einen Remote-SCP-Server

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Protokolle von der Cisco Web Security Appliance (WSA) auf einen SCP-Server (Remote Secure Copy) übertragen werden. Sie können die WSA-Protokolle, z. B. Zugriffs- und Authentifizierungsprotokolle, so konfigurieren, dass sie bei einem Rollover oder Wrap der Protokolle an einen externen Server mit SCP-Protokoll weitergeleitet werden.

Die Informationen in diesem Dokument beschreiben, wie die Rotation der Protokolle sowie die Secure Shell (SSH)-Schlüssel konfiguriert werden, die für eine erfolgreiche Übertragung auf einen SCP-Server erforderlich sind.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Gehen Sie wie folgt vor, um die WSA-Protokolle so zu konfigurieren, dass sie mit SCP auf einem Remote-Server wiederhergestellt werden können:

1. Melden Sie sich bei der Web-GUI der WSA an.

2. Navigieren Sie zu **Systemverwaltung > Protokollabonnements**.

3. Wählen Sie den Namen der Protokolle aus, für die Sie diese Abrufmethode konfigurieren möchten, z. B. **Zugriffsprotokolle**.

4. Wählen Sie im Feld Retrieval Method (Abrufmethode) die Option **SCP auf Remote-Server aus**.

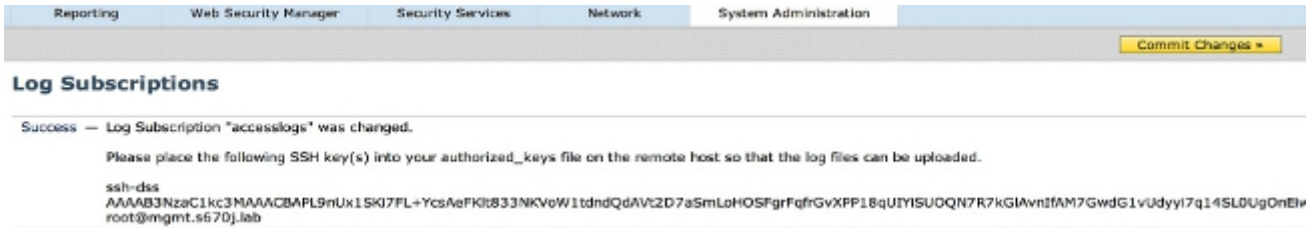
5. Geben Sie den SCP-Hostnamen oder die IP-Adresse des SCP-Servers ein.

6. Geben Sie die SCP-Portnummer ein.
   Hinweis: Die Standardeinstellung ist **Port 22**.
7. Geben Sie den vollständigen Pfadnamen des SCP-Server-Zielverzeichnisses ein, in das die Protokolle übertragen werden.

8. Geben Sie den Benutzernamen für den vom SCP-Server authentifizierten Benutzer ein.

9. Wenn Sie den Hostschlüssel automatisch prüfen oder den Hostschlüssel manuell eingeben möchten, aktivieren Sie die **Host Key Checks (Host-Schlüsselüberprüfung)**.

10. Klicken Sie auf **Senden**. Der SSH-Schlüssel, den Sie in die Datei **authorized_keys** des SCP-Servers eingeben, sollte nun am oberen Rand der Seite **"Protokoll-Subscription bearbeiten"** angezeigt werden. Hier ein Beispiel für eine erfolgreiche Nachricht von der WSA:



11. Klicken Sie auf **Änderungen bestätigen**.

12. Wenn der SCP-Server ein Linux-, Unix- oder Macintosh-Server ist, fügen Sie die SSH-Schlüssel aus der WSA in die Datei **authorized_keys** im SSH-Verzeichnis ein:

    Navigieren Sie zum Verzeichnis **Users > <username> > .ssh**.

    Fügen Sie den WSA SSH-Schlüssel in die Datei **authorized_keys ein**, und speichern Sie die Änderungen.

Hinweis: Sie müssen eine **authorized_keys-**Datei manuell erstellen, wenn diese im SSH-Verzeichnis nicht vorhanden ist.

Überprüfen

Gehen Sie wie folgt vor, um zu überprüfen, ob die Protokolle erfolgreich auf den SCP-Server übertragen wurden:

1. Navigieren Sie zur Seite "WSA **Log Subscriptions"** (WSA-**Protokoll-Subscriptions**).
2. Wählen Sie in der Spalte **Rollover** das Protokoll aus, das Sie für den SCP-Abruf konfiguriert haben.
3. Suchen und klicken Sie auf **Jetzt Rollover**.
4. Navigieren Sie zum SCP-Serverordner, den Sie für den Protokollabruf konfiguriert haben, und überprüfen Sie, ob die Protokolle an diesen Speicherort übertragen werden.

Gehen Sie wie folgt vor, um die Protokollübertragung von der WSA zum SCP-Server zu überwachen:

1. Melden Sie sich über SSH bei der WSA-CLI an.
2. Geben Sie den Befehl **grep ein**.
3. Geben Sie die entsprechende Nummer für das Protokoll ein, das Sie überwachen möchten. Geben Sie beispielsweise **31** aus der grep-Liste für **system_logs ein**.
4. Geben Sie **scp** bei der Aufforderung *Geben Sie den regulären Ausdruck für grep ein*, um die Protokolle so zu filtern, dass Sie nur die SCP-Transaktionen überwachen können.
5. Geben Sie **Y** bei der *Suche ein. Soll die Groß-/Kleinschreibung nicht beachtet werden?* eingeben.
6. Geben Sie **Y** im Feld *Möchten Sie die Protokolle zurückstellen?* eingeben.
7. Geben Sie **N** an der *Seite Möchten Sie die Ausgabe paginieren?* eingeben. Die WSA listet dann die SCP-Transaktionen in Echtzeit auf. Im Folgenden finden Sie ein Beispiel für erfolgreiche SCP-Transaktionen aus den WSA-System_Logs:

```
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
```

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.