WSA-bestandsoverdracht naar een externe SCP-server

Inhoud

Inleiding

In dit document wordt beschreven hoe u logbestanden van Cisco Web Security Appliance (WSA) naar een externe Secure Kopie (SCP) server kunt overdragen. U kunt de WSA logboeken, zoals toegang en authenticatie logboeken configureren, zodat ze naar een externe server met SCP protocol worden doorgestuurd wanneer de logbestanden worden overgedragen of opgehaald.

De informatie in dit document beschrijft hoe u de regels voor logrotatie kunt configureren, evenals de toetsen Secure Shell (SSH) die vereist zijn voor een succesvolle overdracht naar een SCP-server.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

Voltooi deze stappen om de WSA-logs te configureren zodat ze met SCP op een externe server kunnen worden teruggezet:

1. Log in op de WSA web GUI.

2. Navigeer naar **systeembeheer > Log abonnementen**.

3. Selecteer de naam van de loggen(s) waarvoor u deze methode wilt configureren, zoals **toegangsbestanden**.

4. Kies **SCP op** een **externe server** in het veld Retourenmethode.

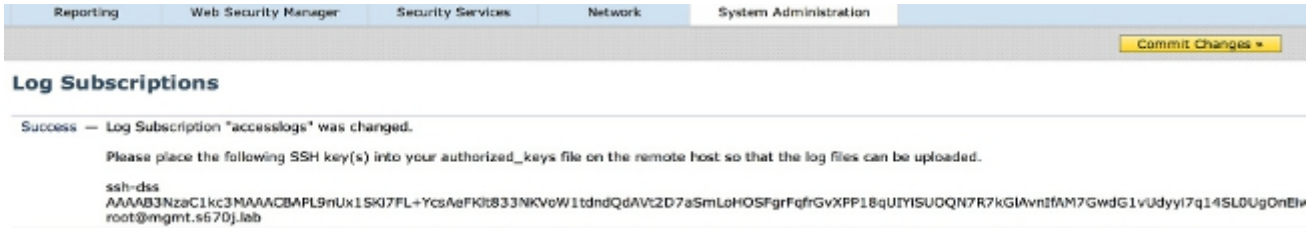
5. Voer de SCP host-naam of het IP-adres van de SCP-server in.

6. Voer het SCP poortnummer in.
   Opmerking: De standaardinstelling is **poort 22**.
7. Voer de volledige padnaam in van de SCP server target folder naar welke de logbestanden zullen worden overgebracht.

8. Voer de gebruikersnaam in voor de SCP-server voor de geauthentiseerde gebruiker.

9. Als u de host-toets automatisch wilt scannen of handmatig de host-toets wilt invoeren, schakelt u **Host Key Checking** in.

10. Klik op **Inzenden**. De SSH-toets die u in het bestand met **geautoriseerde_keys op** de SCP-server wilt plaatsen, moet nu boven op de pagina **Abonneis** bewerken verschijnen. Hier is een voorbeeld van een succesvolle boodschap van de WSA:



11. Klik op **Aanmelden wijzigingen**.

12. Als de SCP server een Linux of Unix server of een Macintosh machine is, plak dan de SSH toetsen vanaf de WSA in het **geautoriseerde_keys** bestand in de SSH-map:

    Navigeer naar de **Gebruikers > <gebruikersnaam> .ssh** folder.

    Plakt de WSA SSH-toets in het **geautoriseerde_keys** bestand en slaat de wijzigingen op.
    Opmerking: U moet handmatig een **geautoriseerd_keys** bestand maken als er geen bestaat in de SSH folder.

Verifiëren

Voltooi deze stappen om te controleren of de logbestanden met succes zijn overgebracht naar de SCP-server:

1. Navigeer naar de WSA pagina met **inlogabonnementen**.
2. Kies in de kolom Rollover het logbestand dat u hebt ingesteld voor het ophalen van SCP.
3. Zoek en klik op **Rollover nu**.
4. Navigeer naar de SCP servermap die u voor het ophalen van het logbestand hebt ingesteld en controleer of de logbestanden naar die locatie worden overgebracht.

Voltooi deze stappen om de logoverdracht naar de SCP server vanaf de WSA te controleren:

1. Log in op de WSA CLI via SSH.
2. Typ de opdracht **vet**.
3. Geef het juiste nummer op voor het logbestand dat u wilt controleren. Voer bijvoorbeeld **31** in de grep list voor het **system_logs**.
4. Voer **scp in** in *Voer de reguliere expressie in om de* melding *te grep* om de logbestanden te filteren, zodat u alleen de SCP-transacties kunt controleren.
5. Voer **Y in** op het *tabblad Is deze zoekopdracht hoofdlettergevoelig?* .
6. Voer **Y in** bij de *weblog.* .
7. Voer **N** in bij de *optie Wilt u de uitvoer pagineren?* . De WSA maakt dan een lijst van de transacties SCP in real time. Hier is een voorbeeld van succesvolle SCP transacties van het WSA systeem_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
```

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.