SCP-druk van e-maillogs configureren op ESA

Inhoud

Inleiding

Dit document beschrijft hoe u een beveiligde kopie van het maillogbestand (SCP) of andere logtypen) kunt instellen en configureren van een Cisco e-mail security applicatie (ESA) naar een externe server.

Achtergrondinformatie

Een beheerder kan foutmeldingen ontvangen waarin staat dat logbestanden niet met SCP kunnen worden geduwd of dat er een of meer foutmeldingen zijn met een of meer fouten.

Voorwaarden

Op de syslogserver waarop het ESA de logbestanden van SCP naar:

1. Zorg dat de te gebruiken map beschikbaar is.
2. Zie '/etc/ssh/sshd_fig' voor de instellingen AuthorizedKeysFile. Dit vertelt SSH om geautoriseerde_keys te accepteren en in de home folder van de gebruiker naar key_name sting geschreven in .ssh/authorised_keys bestand te bekijken:
   ```
   AuthorizedKeysFile      %h/.ssh/authorized_keys
   ```
3. Controleer de permissies van de folder die gebruikt moeten worden. U moet mogelijk wijzigingen in de toegangsrechten aanbrengen: De toegangsrechten op '$Home' zijn ingesteld op 755.Toestemmingen op '$HOME/.ssh' zijn ingesteld op 755.Toestemmingen op '$HOME/.ssh/authorised_keys' worden ingesteld op 600.

Beperkingen en toegangsrechten voor bestandsniveau bij UNIX/Linux

Er zijn drie soorten toegangsbeperkingen:

```
Permission Action chmod option ==================================== read (view) r or 4 write (edit) w or 2 execute (execute) x or 1
```

Er zijn ook drie soorten gebruikersbeperkingen:

```
User ls output ================= owner -rwx------ group ----rwx--- other -------rwx
```

Maprechten/maprechten:

```
Permission Action chmod option ============================================================= read (view contents: i.e., ls command) r or 4 write (create or remove files from dir) w or 2 execute (cd into directory) x or 1
```

Numerieke notatie:

Een andere methode om de Linux-rechten te vertegenwoordigen is een octale notatie zoals getoond door `stat -c %a`. Deze notatie bestaat uit ten minste drie cijfers. Elk van de drie meest rechtse cijfers vertegenwoordigt een verschillende component van de permissies: eigenaar, groep en anderen.

Elk van deze cijfers is de som van zijn componenten bits in het binaire numerieke systeem:

```
Symbolic Notation Octal Notation English ========================================================== ---------- 0000 no permissions --- x--x--x 0111 execute --w--w--w- 0222 write --wx-wx-wx 0333 write & execute -r--r--r-- 0444 read -r-xr-xr-x 0555 read & execute -rw-rw-rw- 0666 read & write -rwxrwxrwx 0777 read. write & execute
```

Voor stap 3 zou een aanbeveling om de $HOME folder op 755 in te stellen de volgende zijn: 7 =`rwx` 5 =`r-x` 5 =`r-x`

Dit betekent dat de folder de standaardrechten heeft `-rwxr-xr-x` (weergegeven in octale notatie als 0755).

SCP-druk van e-maillogs configureren op ESA

1. Start de CLI opdracht **logbestand**.
2. Selecteer de optie **nieuw**.
3. Kies het logbestandstype voor deze abonnement, dit is "1" voor de IronPort Tekst Mail-Logs of een ander logbestandstype naar keuze.
4. Voer de naam voor het logbestand in.
5. Selecteer het juiste logniveau. Meestal moet u "3" selecteren voor Informatie, of een ander logniveau naar keuze.
6. Selecteer "3" voor **SCP Push** wanneer het wordt gevraagd 'Kies de methode om de logs terug te halen.
7. Voer het IP-adres of de DNS-hostname in om de logbestanden te leveren.
8. Geef de poort op om aan te sluiten op de afstandsbediening.
9. Geef de map op de afstandsbediening op om de logbestanden te plaatsen.
10. Typ een bestandsnaam voor logbestanden.
11. Configureer, indien nodig, systeem-gebaseerde unieke identificatoren zoals *$hostname*, *$serialnumber* om aan de bestandsnaam van het logbestand toe te voegen.
12. Stel maximale bestandsgrootte in voordat u overhevelt.

13. Configureer, indien van toepassing, de op de tijd gebaseerde weergave van de logbestanden.
14. Voer "Y" in wanneer u wordt gevraagd om de host-toets in te schakelen?".
15. U wordt vervolgens voorgesteld om de volgende SSH-toets(en) in uw geautoriseerde_keys-bestand te plaatsen, zodat de logbestanden kunnen worden geüpload."
16. Kopieer die toets, omdat u de SSH-toets in uw 'geautoriseerde_keys' bestand op de Syslog server moet zetten. Plakt de toets die wordt gegeven vanaf een logboek naar $HOME/.ssh/authorised_keys bestand op de Syslog server.
17. Vanuit de ESA, voer de CLI opdracht **toe** om configuratieveranderingen op te slaan en vast te leggen.

U kunt het logbestand ook vanuit de GUI configureren: **Systeembeheer > Log abonnementen**

> Opmerking: Zie het Logging-hoofdstuk van de ESA-gebruikershandleiding voor meer informatie.

bevestiging

Hostkeyalle

Start de opdracht **logfig > hostkeyfig**. U dient een bestandsindeling te zien voor de syslogserver die is ingesteld als "ssh-dss" met een afgekort overzicht dat gelijk is aan de toets die tijdens de configuratie is meegeleverd.

```
myesa.local > logconfig
...
[]> hostkeyconfig

Currently installed host keys:
1. 172.16.1.100 ssh-dss AAAAB3NzaC1kc3MAAACBAMUqUBGztO0T...OutUns+DY=
```

Systeemmeldingen

Het systeem logt het volgende op: informatie over de start, waarschuwingen voor het verstrijken van een virtuele machine, DNS-statusinformatie en opmerkingen die gebruikers hebben getypt met behulp van de opdracht. Systeemlogbestanden zijn handig om de basisstatus van het apparaat te verbeteren.

Het uitvoeren van de opdracht **tail system_logs** van de CLI zal u een live blik op de systeemstatus geven.

U kunt ook de CLI opdracht **rollen** kiezen en het nummer selecteren dat aan het logbestand gekoppeld is. U ziet dit het logbestand SCP naar de syslog server in system_logs:

```
myesa.local > tail system_logs

Press Ctrl-C to stop.
Thu Jan 5 11:26:02 2017 Info: Push success for subscription mail_logs: Log
mail_logs.myesa.local.@20170105T112502.s pushed via SCP to remote host 172.16.1.100:22
```

Geavanceerde probleemoplossing

Als er blijvende problemen zijn met connectiviteit op de syslogserver, van lokale gastheer en het gebruik van ssh, voer "ssh testuser@hostname -v" uit om de gebruikerstoegang in breedtemodus te testen. Dit kan een oplossing zijn voor problemen oplossen om aan te tonen waar de ssh-verbinding niet succesvol is.

```
$ ssh testuser@172.16.1.100 -v
OpenSSH_7.3p1, LibreSSL 2.4.1
debug1: Reading configuration data /Users/testuser/.ssh/config
debug1: /Users/testuser/.ssh/config line 16: Applying options for *
debug1: Reading configuration data /etc/ssh/ssh_config
debug1: /etc/ssh/ssh_config line 20: Applying options for *
debug1: Connecting to 172.16.1.100 [172.16.1.100] port 22.
debug1: Connection established.
debug1: identity file /Users/testuser/.ssh/id_rsa type 1
debug1: key_load_public: No such file or directory
debug1: identity file /Users/testuser/.ssh/id_rsa-cert type -1
debug1: identity file /Users/testuser/.ssh/id_dsa type 2
debug1: key_load_public: No such file or directory
debug1: identity file /Users/testuser/.ssh/id_dsa-cert type -1
debug1: key_load_public: No such file or directory
debug1: identity file /Users/testuser/.ssh/id_ecdsa type -1
debug1: key_load_public: No such file or directory
debug1: identity file /Users/testuser/.ssh/id_ecdsa-cert type -1
debug1: key_load_public: No such file or directory
debug1: identity file /Users/testuser/.ssh/id_ed25519 type -1
debug1: key_load_public: No such file or directory
debug1: identity file /Users/testuser/.ssh/id_ed25519-cert type -1
debug1: Enabling compatibility mode for protocol 2.0
debug1: Local version string SSH-2.0-OpenSSH_7.3
debug1: Remote protocol version 2.0, remote software version OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.8
debug1: match: OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.8 pat OpenSSH_6.6.1* compat 0x04000000
debug1: Authenticating to 172.16.1.100:22 as 'testuser'
debug1: SSH2_MSG_KEXINIT sent
debug1: SSH2_MSG_KEXINIT received
debug1: kex: algorithm: curve25519-sha256@libssh.org
debug1: kex: host key algorithm: ssh-dss
debug1: kex: server->client cipher: chacha20-poly1305@openssh.com MAC: <implicit> compression:
zlib@openssh.com
debug1: kex: client->server cipher: chacha20-poly1305@openssh.com MAC: <implicit> compression:
zlib@openssh.com
debug1: expecting SSH2_MSG_KEX_ECDH_REPLY
debug1: Server host key: ssh-dss SHA256:c+YpkZsQyUwi3tkIVJFXHAstwlkdewO1G0s7P2khV7U
debug1: Host '172.16.1.100' is known and matches the DSA host key.
debug1: Found key in /Users/testuser/.ssh/known_hosts:5
debug1: rekey after 134217728 blocks
debug1: SSH2_MSG_NEWKEYS sent
debug1: expecting SSH2_MSG_NEWKEYS
debug1: rekey after 134217728 blocks
debug1: SSH2_MSG_NEWKEYS received
debug1: Skipping ssh-dss key /Users/testuser/.ssh/id_dsa - not in PubkeyAcceptedKeyTypes
debug1: SSH2_MSG_SERVICE_ACCEPT received
debug1: Authentications that can continue: publickey,password
debug1: Next authentication method: publickey
debug1: Offering RSA public key: /Users/testuser/.ssh/id_rsa
debug1: Authentications that can continue: publickey,password
debug1: Trying private key: /Users/testuser/.ssh/id_ecdsa
debug1: Trying private key: /Users/testuser/.ssh/id_ed25519
debug1: Next authentication method: password
testuser@172.16.1.100's password: <<< ENTER USER PASSWORD TO LOG-IN >>>
```

```
debug1: Enabling compression at level 6.
debug1: Authentication succeeded (password).
Authenticated to 172.16.1.100 ([172.16.1.100]:22).
debug1: channel 0: new [client-session]
debug1: Requesting no-more-sessions@openssh.com
debug1: Entering interactive session.
debug1: pledge: exec
debug1: No xauth program.
Warning: untrusted X11 forwarding setup failed: xauth key data not generated
debug1: Requesting authentication agent forwarding.
debug1: Sending environment.
debug1: Sending env LANG = en_US.UTF-8
debug1: Sending env LC_CTYPE = en_US.UTF-8
```