在ESA上配置郵件日誌的SCP推送

目錄

簡介

本文說明如何設定和設定從思科電子郵件安全裝置(ESA)到外部系統日誌伺服器的郵件記錄（或其他記錄型別）的安全複製推送(SCP)。

背景資訊

管理員可能收到錯誤通知，指出無法使用SCP推送日誌，或者可能有錯誤日誌指出金鑰不匹配。

必要條件

在ESA將SCP日誌檔案到的系統日誌伺服器上：

1. 確保要使用的目錄可用。
2. 檢視「/etc/ssh/sshd_config」以檢視AuthorizedKeysFile設定。 這指示SSH接受authorized_keys，並在使用者的主目錄中查詢以.ssh/authorized_keys檔案編寫的key_name字串：
   ```
   AuthorizedKeysFile      %h/.ssh/authorized_keys
   ```
3. 驗證要使用的目錄的許可權。 您可能需要更改許可權： 對「$HOME」的許可權設定為755。「$HOME/.ssh」上的許可權設定為755。「$HOME/.ssh/authorized_keys」上的許可權設定為600。

UNIX/Linux上的檔案級限制和許可權

有三種型別的訪問限制：

```
Permission Action chmod option ===================================== read (view) r or 4 write
```

```
(edit) w or 2 execute (execute) x or 1
```
還有三種型別的使用者限制：

```
User ls output ================== owner -rwx------ group ----rwx--- other -------rwx
```
資料夾/目錄許可權：

```
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
```
數字元號：

另一種表示Linux許可權的方法是八進位制記法，如所示 `stat -c %a`.此符號至少包含三個數字。最右邊的三個數字分別代表不同的許可權元件：所有者、組和其他人。

這些數字中的每一個數字都是二進位制數字系統中其元件位的總和：

```
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
```
對於步#3，將$HOME目錄設定為755的建議是：7=`rwx` 5=`r-x` 5=`r-x`

這表示目錄具有預設許可權 `-rwxr-xr-x` （以八進位制記法表示為0755）。

在ESA上配置郵件日誌的SCP推送

1. 運行CLI命令**logconfig**。
2. 選擇**new**選項。
3. 為此訂閱選擇日誌檔案型別，對於IronPort文本郵件日誌，該型別將為「1」，或者您選擇的任何其他日誌檔案型別。
4. 輸入日誌檔案的名稱。
5. 選擇適當的日誌級別。 通常，您需要選擇「3」作為「資訊」級別，或者您選擇的任何其他日誌級別。
6. 當系統提示「Choose the method to retrieve the logs」時，為**SCP Push**選擇「3」。
7. 輸入IP地址或DNS主機名以將日誌傳送到。
8. 輸入要連線到遠端主機上的埠。
9. 輸入遠端主機上的目錄以放置日誌。
10. 輸入用於日誌檔案的檔名。
11. 如果需要，配置基於系統的唯一識別符號，如*$hostname*和*$serialnumber*，以附加到日誌檔名。
12. 在傳輸之前設定Maximum filesize。
13. 配置日誌檔案的基於時間的滾動更新（如果適用）。
14. 當詢問「Do you want to enable host key checking？」時，輸入「Y」。
15. 系統隨即會顯示「請將以下SSH金鑰放入您的authorized_keys檔案中，以便可以上傳日誌檔案。」
16. 複製該金鑰，因為您需要將SSH金鑰放在Syslog伺服器上的「authorized_keys」檔案中。 將logconfig中提供的金鑰貼上到Syslog伺服器上的$HOME/.ssh/authorized_keys檔案中。

17. 從ESA運行CLI命令**commit**以儲存和提交配置更改。

日誌的配置也可以通過GUI完成：**系統管理>日誌訂閱**

附註：請檢視《ESA使用手冊》的「記錄」一章，瞭解完整的詳細資訊和詳細資訊。

確認

Hostkeyconfig

執行命令**logconfig > hostkeyconfig**。 您應該會看到配置為「ssh-dss」的系統日誌伺服器的條目，該條目帶有與配置過程中提供的金鑰相似的縮寫金鑰。

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

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

系統記錄

系統日誌記錄以下內容：引導資訊、虛擬裝置許可證過期警報、DNS狀態資訊以及使用者使用commit命令鍵入的註釋。系統日誌對於排除裝置的基本狀態故障非常有用。

從CLI運行**tail system_logs**命令將讓您即時檢視系統狀態。

您還可以選擇CLI命令**rollovernow**，然後選擇與日誌檔案關聯的編號。 您將在system_logs中看到日誌檔案SCP到您的系統日誌伺服器：

```
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
```

高級故障排除

如果從本地主機使用ssh連線到系統日誌伺服器時繼續出現問題，請運行「ssh testuser@hostname -v」以詳細模式測試使用者訪問。 這有助於進行故障排除，以顯示ssh連線未成功之處。

```
$ 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
```