配置邮件SCP推送注册ESA

目录

简介

本文描述如何设立和配置安全的复制推送(SCP)邮件日志(或其他日志类型)从思科电子邮件安全工具(ESA)到外部系统日志服务器。

背景信息

阐明的管理员可以接收错误通知使用SCP，日志不可能推送，或者可能有陈述的错误日志主要不匹配。

先决条件

在系统日志服务器上ESA SCP日志文件对：

1. 保证将使用的目录是可用的。
2. 查看'/etc/ssh/sshd_config' AuthorizedKeysFile设置的。 这在用户的主目录告诉SSH接受authorized_keys和查找为在.ssh/authorized_keys文件写入的key_name蜇：
   `AuthorizedKeysFile %h/.ssh/authorized_keys`
3. 验证目录的权限使用。 您可能需要做权限变动： 在'$HOME的'权限设置到755。在'$HOME/.ssh的'权限设置到755。在'$HOME/.ssh/authorized_keys的'权限设置到600。

文件级别限制和权限在UNIX/Linux

有访问限制的三种类型：

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

也有用户限制的三种类型：

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

文件夹/目录权限：

```
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
```

数字符号：

代表的Linux权限另一个方法是八符号如显示由`stat - c %a`此符号包括至少三个位。三个最右边的位中的每一个代表权限的不同的组件：所有者，组和其他。

这些位中的每一个是其二进制数system:的组分位的总和

```
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
```

对于步骤#3，建议设置$HOME目录到755是：7=rwx `5=r-x 5=r-x`

这意味着目录有默认权限`- rwxr XRx` (代表在八符号作为0755)。

配置邮件SCP推送注册ESA

1. 运行CLI命令**logconfig**。
2. 选择**新建的**选项。
3. 选择此订阅的日志文件类型，这将是您的选择的"1"为IronPort文本邮件日志，或者其他日志文件类型。
4. 输入名称对于日志文件。
5. 选择适当的日志级别。 典型地您会需要选择"3"信息性，或者其他日志的级您的选择。
6. 当提示'请选择方法检索日志的，请选择"3" **SCP推送的**。
7. 输入在IP地址或DNS主机名提供日志。
8. 输入端口连接到在远程主机。
9. 输入在远程主机的目录放置日志。
10. 输入在文件名使用日志文件。
11. 配置，若需要，系统基于唯一标识符类似*$主机名*，添附的*$serialnumber*对日志文件名。
12. 在转接前设置最大文件大小。
13. 配置日志文件的基于时间的反转，如果适用。
14. 当询问"您要启用主机密钥检查？"，输入"Y"。
15. 然后提交您"请放置以下SSH密钥到您的authorized_keys文件，以便日志文件能上传"。
16. 因为您在您的在系统日志服务器的'authorized_keys的文件将需要放置SSH密钥复制该密钥。粘贴从logconfig给的密钥到在系统日志服务器的$HOME/.ssh/authorized_keys文件。
17. 从ESA，请运行CLI命令**进行**保存和确认配置更改。

日志的配置可以也是实现的从GUI ：**系统管理>日志订阅**

Note:请查看ESA用户指南的记录日志章节完整详细信息和更多信息的。

确认

Hostkeyconfig

运行命令**logconfig > hostkeyconfig**。 您应该为作为“SSH DSS”配置列出的系统日志服务器看到条目与缩写的关键类似于在配置时提供的密钥。

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

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

系统日志

系统日志记录以下：启动信息、虚拟设备许可过期警报、DNS状态信息和使用commit命令被键入的注释用户。系统日志为排除故障设备的基本状态是有用的。

运行tail命令**system_logs**从CLI将提供您实际查看给系统状态。

您可以也选择CLI命令**rollovernow**和选择编号关联对日志文件。 您将看到此日志文件SCP到您的在system_logs的系统日志服务器：

```
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
```

高级故障排除

如果有与连接的继续的问题对系统日志服务器，从本地主机和使用SSH，请运行“SSH testuser@hostname - v”测试在冗长模式的用户访问。 这可能显示的助手故障排除SSH连接不成功的地方。

```
$ 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
```