Configurando el empuje de SCP del correo abre una sesión el ESA

Contenido

Introducción

Este documento describe cómo poner y configurar el empuje de la Copia segura (SCP) de los registros del correo (o de otros tipos del registro) de un dispositivo de seguridad del correo electrónico de Cisco (ESA) a un servidor Syslog externo.

Antecedentes

Un administrador puede recibir las notificaciones de error que expone que los registros no se pueden avanzar usando SCP, o puede haber registros de error que exponen la discrepancia de clave.

Prerequisites

En el servidor de Syslog que el ESA los archivos del registro de SCP a:

1. Asegure que el directorio que se utilizará está disponible.
2. Revise “/etc/ssh/sshd_config” para las configuraciones de AuthorizedKeysFile. Esto dice SSH validar los authorized_keys y mirar en el directorio de inicio del usuario para la picadura del key_name escrita en .ssh/los authorized_keys clasifíe:
   `AuthorizedKeysFile      %h/.ssh/authorized_keys`
3. Verifique los permisos del directorio para ser utilizado. Usted puede necesitar realizar los cambios de los permisos: Los permisos en el “$HOME” se fijan a 755.Los permisos en “$HOME/.ssh” se fijan a 755.Los permisos en “$HOME/.ssh/authorized_keys” se fijan a 600.

Restricciones llanas y permisos del archivo en UNIX/Linux

Hay tres tipos de restricciones de acceso:

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

Hay también tres tipos de restricciones del usuario:

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

Carpeta/permisos del directorio:

```
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
```

Notación numérica:

Otro método para representar los permisos de Linux es una notación octal como se muestra por el `stat - c %a`. Esta notación consiste en por lo menos tres dígitos. Cada uno de los tres dígitos de derecha representa un diverso componente de los permisos: propietario, grupo, y otros.

Cada uno de estos dígitos es la suma de sus bits componentes en el sistema de numeración binario:

```
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
```

Para el paso #3, la recomendación de fijar el directorio $HOME a 755 sería: 7=rwx `5=r-x 5=r-x`

Esto significa que el directorio tiene los permisos predeterminados `- rwxr-XR-x` (representado en la notación octal como 0755).

Configurando el empuje de SCP del correo abre una sesión el ESA

1. Ejecute el **logconfig del** comando CLI.
2. Seleccione la opción **nueva**.
3. Elija el tipo de archivo del registro para esta suscripción, éste será "1" para los registros del correo de texto de IronPort, o cualesquiera otros tipos de archivo del registro de su opción.
4. Ingrese el nombre para el archivo del registro.
5. Seleccione el nivel apropiado del registro. Usted necesitaría típicamente seleccionar el "3" para registro informativo, o el cualquier otro llano de su opción.
6. Cuando se le pregunte “elija el método para extraer los registros”, seleccionan el "3" para el **empuje de SCP**.
7. Ingrese en el IP Address o el nombre del host de DNS para entregar los registros a.
8. Ingrese el puerto para conectar con en el host remoto.
9. Ingrese el directorio en el host remoto para colocar los registros.
10. Ingrese en un nombre de fichero para utilizar para los archivos del registro.

11. Configuración, si es necesario, Identificadores únicos basados en el estudio de sistemas como *$hostname*, *$serialnumber* a añadir al final del fichero al nombre de fichero del registro.
12. Fije el máximo filesize antes de transferir.
13. Configure la renovación del time basado de los archivos del registro, si procede.
14. ¿Cuando está pedido “lo haga usted quisieron habilitar marcar de la clave de host? ”, ingrese “Y”.
15. Le entonces presentan “pone por favor las claves siguientes de SSH en su archivo de los authorized_keys para poder cargar los archivos del registro.”
16. Copie esa clave, pues usted necesitará poner la clave de SSH en su archivo de los “authorized_keys” en el servidor de Syslog. Pegue la clave dada del logconfig al archivo $HOME/.ssh/authorized_keys en el servidor de Syslog.
17. Del ESA, ejecute el **cometer del** comando CLI para salvar y para confiar los cambios de configuración.

La configuración del registro puede también ser realizada del GUI: **Suscripciones de la administración del sistema > del registro**

> **Note**: Revise por favor el capítulo del registro del guía del usuario ESA para los detalles y la Más información completos.

Confirmación

Hostkeyconfig

Ejecute el **logconfig** > el **hostkeyconfig del** comando. Usted debe ver una entrada para el servidor de Syslog configurado enumerado como “SSH-dss” con un similar dominante abreviada a la clave proporcionada durante la configuración.

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

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

Registros del sistema

Los registros del sistema registran el siguiente: inicie la información, las alertas virtuales de la expiración de la licencia del dispositivo, información de estatus DNS, y comenta los usuarios tecleados usando el comando commit. Los registros del sistema son útiles para resolver problemas el estado básico del dispositivo.

Ejecutar los **system_logs del** comando tail del CLI le proporcionará una mirada viva al estado del sistema.

Usted puede también elegir el **rollovernow del** comando CLI y seleccionar el número asociado al archivo del registro. Usted verá esto el archivo del registro SCP a su servidor de Syslog en los 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
```

Solución avanzada de problemas

Si hay problemas continuos con la Conectividad al servidor de Syslog, del host local y ssh con, ejecute el “ssh testuser@hostname - v” para probar el acceso del usuario en el modo detallado. Esto puede troubleshooting del asistente mostrar donde la conexión del ssh no está teniendo éxito.

```
$ 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
```