Configuración de SSH y/o FTP para recibir datos

Configuración de SSH y/o FTP para recibir datos

Introducción

El método de transferencia estándar en Pandora FMS para transmitir ficheros, Tentacle, necesita del lenguaje de programación Perl instalado. Algunos dispositivos, como por ejemplo Sistemas ESX (UNIX), carecen de dicha herramienta. Cuando esto ocurre, las alternativas son usar FTP o SSH para transferir datos de monitorización.

Pandora FMS puede usar el FTP o el protocolo SSH para copiar los paquetes de datos XML generados por los agentes software hacia el servidor PFMS.

Configuración SSH para recibir datos en Pandora FMS

Tenga siempre en cuenta la Arquitectura de Seguridad de Pandora FMS.

Considere el servidor de Pandora FMS como Servidor y cada uno de los dispositivos que ejecutan el Agente Software como Cliente. En todo momento podrá consultar con cuál usuario está trabajando por medio del comando whoami.

Creación de usuario en Servidor

Paso 1: Crear un usuario `pandora` en la máquina donde ejecuta el servidor Pandora FMS. Dicha máquina recibirá los datos por SSH. Si ya ha instalado un servidor Pandora FMS seguramente ese usuario ya está creado. Establezca una contraseña robusta para ese usuario con el comando:

```
passwd pandora
```

Configuración de usuario en Servidor

Paso 2: En el servidor, crear un directorio `/home/pandora/.ssh` con permisos `750` y usuario `pandora:root` .

Creación de llaves en Cliente

Paso 3: Crear, en cada máquina que ejecute un Agente Software que utilizará SSH, una pareja de llaves (privada y pública). Para ello, ejecute el comando siguiente con el mismo usuario con el que

se ejecuta el Agente Software de Pandora FMS:

```
ssh-keygen
```

Se mostrarán una serie de preguntas a las que tendrá que contestar simplemente pulsando la tecla Intro. Con esto ha creado una llave pública y una privada para ese usuario en la máquina. Ahora debe copiarla a la máquina de destino, que es el servidor de Pandora FMS a donde quiere enviar los datos de monitorización.

Copia de llave pública al Servidor

Paso 4: Copiar la llave pública al Servidor de Pandora FMS. La llave pública que acaba de generar se puede copiar de dos maneras.

Copia manual

El fichero de llave pública generado en el Cliente es:

```
/home/<user>/.ssh/id_rsa.pub
```

Donde `<user>` es el nombre de usuario que ejecuta el Agente Software de Pandora FMS en el Cliente. Si el par de llaves fue generada como usuario raíz o *root*, estará en:

```
/root/.ssh/id_rsa.pub
```

Este fichero tendrá un contenido similar a este:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEAzqyZwhAge5LvRgC8uSm3tWaFV9O6fHQek7PjxmbBUxTWfvNbbswb
FsF0esD3COavziQAUl3rP8DC28vtdWHFRHq+RS8fmJbU/VpFpN597hGeLPCbDzr2WlMvctZwia7pP4tX
9tJI7oyCvDxZ7ubUUi/bvY7tfgi7b1hJHYyWPa8ik3kGhPbcffbEX/PaWbZ6TM8aOxwcHSi/4mtjCdow
RwdOJ4dQPkZp+aok3Wubm5dlZCNLOZJzd9+9haGtqNoAY/hkgSe2BKs+IcrOAf6A16yiOZE/GXuk2zsa
Qv1iL28rOxvJuY7S4/JUvAxySI7V6ySJSljg5iDesuWoRSRdGw== root@dragoon
```

Dicho contenido debe adicionarlo al final del fichero `authorized_keys` en el Servidor. Su ruta es:

```
/home/pandora/.ssh/authorized_keys
```

El archivo `authorized_keys` en el Servidor debe pertenecer (*ownership*) al usuario `pandora:root` y debe tener permisos `600`.

Copia automática

Utilice el siguiente comando en el Cliente:

```
ssh-copy-id pandora@<server_address>
```

Donde `< server_address >` es la dirección IP o URL del Servidor.

Preguntará la contraseña del usuario `pandora` del servidor (establecida en el paso 1) y, una vez que lo confirme, mostrará un mensaje similar al siguiente:

```
Now try logging into the machine, with "ssh 'pandora@<server_address>'", and
check in:
  .ssh/authorized_keys
to make sure we haven't added extra keys that you weren't expecting.
```

Realice esa prueba para verificar que la conexión automática al Servidor Pandora FMS con el usuario `pandora` desde el Cliente (con el usuario que ejecuta el Agente Software):

```
ssh pandora@<server_address>
```

Una vez logre conectar al Servidor de la manera indicada, el Agente Software en el Cliente podrá comenzar a enviar datos de monitorización.

Configuración del Cliente

Una vez haya verificado la conexión por medio de SSH, este será el método empleado por los agentes software para copiar datos en el directorio del Servidor de Pandora FMS. Dicho directorio está ubicado en:

```
/var/spool/pandora/data_in
```

Asegúrese igualmente de que el directorio `/var/spool/pandora/data_in` existe y el usuario `pandora` tiene permisos de escritura, pues de lo contrario no funcionará.

Por último, modifique la configuración del agente software en el Cliente para especificar que el método de copia es SSH. Esto se modifica en el fichero `/etc/pandora/pandora_agent.conf`, en el token de configuración `transfer_mode`. Recuerde que debe reiniciar luego el servicio del agente software en cada Cliente luego de este cambio.

Aseguramiento del servidor SSH

Pandora FMS emplea, entre otros, sftp/ssh2 (SCP) para copiar ficheros de datos desde los agentes software al servidor. Debido a esto, necesitará al menos un servidor de datos con un servidor SSH2 a la escucha del usuario `pandora`. Esto podría resultar un riesgo significativo en una red que necesita estar estrictamente asegurada. OpenSSH2 es muy seguro, pero respecto a seguridad informática no existe nada que resulte absolutamente seguro; por tanto, se deben tomar medidas para hacerlo «más» seguro.

Es posible prohibir el acceso por SSH para ciertos usuarios, así como configurar restricciones al acceso por FTP.

Para ello, deberá modificar el usuario `pandora` en el Servidor. Este usuario debe tener una contraseña robusta. Se cambiará su *shell* de inicio de sesión para restringir el acceso por SSH al usuario, y su directorio `home`, para evitar su acceso a otras carpetas:

```
usermod -s /sbin/nologin -d /var/spool/pandora/data_in pandora
```

Con estos cambios en el usuario `pandora` en el Servidor, al iniciar sesión por SSH no podrá ejecutar comandos con él en una terminal interactiva.

- Consulte los sistemas operativos recomendados para Pandora FMS.
- En sistemas Debian la ruta de la *shell* es `/usr/sbin/nologin`.

Configuración FTP para recibir datos en Pandora FMS

La configuración en el cliente para enviar datos por FTP permite especificar el usuario y el contraseña que se va a enviar, con lo que es bastante sencillo implementar la copia por FTP en lugar de por Tentacle.

Además de configurar los agentes software de Pandora FMS para el envío de datos con FTP, tendrá que configurar un servidor FTP en donde ejecute el servidor Pandora FMS, establecer una contraseña para el usuario `pandora` y permitir acceso de escritura al usuario `pandora` al directorio `/var/spool/pandora/data_in` y sus subdirectorios.

Esto supone que deberá configurar el servidor FTP para adecuarlo a estas necesidades; para ello, en esta guía se usa vsftpd .

Instalación de vsftpd

El inconveniente de usar FTP en lugar de Tentacle es que el envío de datos por FTP es menos seguro, ya que al tener un FTP funcionando en el servidor de Pandora FMS, esto lo hace más

vulnerable a fallos inherentes al diseño del sistema FTP. En los apartados siguientes se indicará cómo configurar de manera mínima el servidor vsftpd (llamado simplemente Servidor)

Por ello, y de la misma manera que se ha deshabilitado por seguridad el *login* por SSH para el usuario `pandora`, debe establecerse un método de acceso seguro para los usuarios por FTP. Un método seguro y sencillo para esto es crear una regla PAM para vsftpd. Para esto debe crear un archivo llamado `/etc/pam.d/ftp` que contenga lo siguiente:

```
auth    required        pam_listfile.so item=user sense=deny file=/etc/ftpusers
onerr=succeed
# Standard pam includes
@include common-account
@include common-session
@include common-auth
auth    required    pam_succeed_if.so quiet user ingroup pandora
auth    required    pam_succeed_if.so quiet shell = /sbin/nologin
```

En el archivo de configuración de vsftpd (`/etc/vsftpd.conf`) busque el token `pam_service_name` y establezca el nombre del archivo creado:

```
pam_service_name=ftp
```

Con esta configuración, solo los usuarios que pertenezcan al grupo `pandora` y tengan `nologin` como *shell* asociada podrán conectar a Pandora FMS por FTP, *por lo que debe crear el grupo* `pandora` que incluya al usuario `pandora`. En todo caso verifique que ambos existan en el Servidor.

Con una última configuración del archivo `/etc/vsftpd.conf`, se restringirá el acceso de los usuarios que accedan por FTP a su directorio raíz. Los parámetros son los siguientes:

```
chroot_local_user=YES
chroot_list_enable=YES
chroot_list_file=/etc/vsftpd.nochroot_list
```

En caso de que se necesite excluir algún usuario de este comportamiento y evitar restringirlo a su Chroot, solo habrá que incluir dicho usuario en este archivo `vsftpd.nochroot_list` (un usuario por línea).

Otras opciones a configurar para establecer una mayor seguridad son las siguientes:

```
dirlist_enable=NO
download_enable=NO
deny_file=authorized_keys
deny_file=.ssh
chroot_local_user=YES
```

Recuerde reiniciar el servicio vsftpd tras hacer cambios en el fichero de configuración para que estos surtan efecto.

Con esta configuración, el usuario estará restringido a su directorio raíz (`/var/spool/pandora/data_in` en el caso del usuario `pandora`). El usuario podrá realizar transferencias vía FTP (enviar archivos), pero no podrá listar archivos.

Intente iniciar sesión con el usuario `pandora` en el FTP, cambiar de directorio y listar archivos; si no lo consigue, la configuración habrá sido un éxito.

Volver al Índice de Documentación Pandora FMS