PANDORAFMS

Configuración de SSH y/o FTP para recibir datos

20-09-2021

Configuración de SSH y/o FTP para recibir datos

Volver al Índice de Documentación Pandora FMS

Configuración SSH para recibir datos en Pandora FMS

En ocasiones, no podemos utilizar el método de transferencia estándar en Pandora FMS para transmitir ficheros (Tentacle) porque podemos estar usando un sistema Unix que no tiene Perl (por ejemplo Sistemas ESX) y tenemos que usar el agente antiguo en shellscript. Cuando esto ocurre, las alternativas son usar FTP o SSH para transferir el archivo.

Pandora FMS puede usar el protocolo SSH para copiar los paquetes de datos XML generados por los agentes hacia el servidor. Para ello, tiene que llevar a cabo los siguientes pasos:

Paso 1: Crear un usuario “pandora” en el host donde está su servidor Pandora FMS, que va a recibir los datos por SSH. Si ya ha instalado un servidor Pandora FMS, ya tendrá seguramente ese usuario creado. Establezca una contraseña robusta para ese usuario con el comando:

```
passwd pandora
```

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

Paso 3: Crear, en cada máquina donde tenga un agente que quiera usar SSH, una pareja de llaves. Para ello, ejecute el comando siguiente **con el mismo usuario con el que se ejecutará el agente** de Pandora FMS:

```
# ssh-keygen
```

Saldrá una serie de preguntas a las que tendrá que contestar simplemente pulsando Enter. Con esto ha creado una llave pública/privada para ese usuario en la máquina. Ahora tiene que copiarla a la máquina de destino, que es el servidor de Pandora FMS a donde quiere mandar los datos.

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

Manualmente, incluyendo el contenido del fichero de llave pública que se encuentra en

la máquina donde está el agente, sobre el fichero de llaves remotas que se encuentra en el servidor de Pandora FMS, ubicado en /home/pandora/.ssh/authorized_keys (que debe tener ownership pandora:root y permisos 600).

El fichero de llave pública generado en la máquina donde está el agente es /root/.ssh/id_rsa.pub. Este fichero tendrá un contenido similar a este:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEAzqyZwhAge5LvRgC8uSm3tWaFV9O6fHQek7PjxmbBUxTWfvNbbswbFsF0esD3COavziQAUl3rP8DC28vtdWHFRHq+RS8fmJbU/VpFpN597hGeLPCbDzr2WlMvctZwia7pP4tX9tJI7oyCvDxZ7ubUUi/bvY7tfgi7b1hJHYyWPa8ik3kGhPbcffbEX/PaWbZ6TM8aOxwcHSi/4mtjCdowRwdOJ4dQPkZp+aok3Wubm5dlZCNLOZJzd9+9haGtqNoAY/hkgSe2BKs+IcrOAf6A16yiOZE/GXuk2zsaQv1iL28rOxvJuY7S4/JUvAxySI7V6ySJSljg5iDesuWoRSRdGw== root@dragoon
```

De forma automática, con el siguiente comando:

```
ssh-copy-id pandora@ip_del_host_del_servidor
```

Le preguntará la password del usuario “pandora” del servidor y, una vez que lo confirme, le mostrará un mensaje similar al siguiente:

```
Now try logging into the machine, with "ssh
'pandora@ip_del_host_del_servidor'", 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 de Pandora FMS con el usuario “pandora” desde la máquina del agente con el usuario root es posible. Hasta que esto no sea posible, el agente no podrá mandar datos por SSH.

Este método será empleado por los agentes para copiar datos en el directorio del servidor de Pandora FMS /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 para especificar que el método de copia es ssh y no tentacle. Esto se modifica en el fichero */etc/pandora/pandora_agent.conf*, en el token de configuración *transfer_mode*.

Configuración FTP para recibir datos en Pandora FMS

La configuración en el cliente para enviar datos por FTP permite especificar el usuario y el password 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 de Pandora FMS para el envío de datos con FTP, tendrá que configurar un servidor de FTP en el servidor de Pandora FMS, establecer una password para el usuario “pandora” (indicado en el apartado anterior) y permitir acceso de escritura al usuario “pandora” al directorio /var/spool/pandora/data_in y directorios inferiores.

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

Securización del servidor SSH

Pandora FMS emplea, entre otros, sftp/ssh2 (scp) para copiar ficheros de datos desde los agentes 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 securizada. 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 modificarse el usuario «pandora». Este usuario debe tener contraseña. 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
```

En sistemas Debian la ruta de la shell es /usr/sbin/nologin.

Con estos cambios en el usuario, no podrá iniciar sesión por SSH con él.

Securización 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 *securizar* mínimamente su 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 creamos un archivo /etc/pam.d/ftp que contiene 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 sistemas Debian la ruta de la shell es /usr/sbin/nologin.

En el archivo de configuración de vsftpd (/etc/vsftpd.conf) buscamos el token pam_service_name y establecemos 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 conectarse a Pandora FMS por FTP, por lo que debe crear el grupo «pandora» que incluya al usuario «pandora», si no existe ya.

Con una última configuración del archivo /etc/vsftpd.conf, podremos restringir 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 puede realizar transferencias FTP para enviar ficheros, 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