Configuring SSH and/or FTP to Receive Data

Go back to Pandora FMS documentation index

SSH Configuration to Get Data in Pandora FMS

Sometimes, it is not possible to use the standard file transfer method in Pandora FMS (Tentacle) because one might be using a Unix system that does not have Perl (as in ESX systems for example) and that would mean using the old shellscript agent. When this happens, the options are using FTP or SSH to transfer the file.

Pandora FMS can use the SSH protocol to copy XML data packages, generated by the agents, to the server. To configure it, follow these steps:

Step 1. Create a “pandora” user in the host where your Pandora FMS server is installed, which will receive the data through SSH. If you already have Pandora FMS server installed, then this user must have already been created. Set a strong password for this user with the command:

```
passwd pandora
```

Step 2. Once within the server, create the /home/pandora/.ssh directory with 750 permissions and pandora:root user.

Step 3. In each system where you have an agent that must use SSH, create a pair of keys. To do so, execute the following command with the **same user that will be used to execute the Pandora FMS agent**:

```
# ssh-keygen
```

A few questions will be shown, which are answered by simply pressing Enter. A public/private key for this user will be created in the system. Now, copy it to the target system, the Pandora FMS server where data must be sent to.

Step 4. Copy the public key to the Pandora FMS server. There are two ways to copy the created public key:

Manually, copying the content of the public key file from the system where the agent is, to the remote key file in Pandora FMS server, located at /home/pandora/.ssh/authorized_keys (that should have pandora:root ownership and 600 permissions).

The public key file, generated in the system where the agent is, is /root/.ssh/id_rsa.pub. This file will contain something similar to this:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEAzqyZwhAge5LvRgC8uSm3tWaFV9O6fHQek7PjxmbBUxTWfvNb
bswbFsF0esD3COavziQAUl3rP8DC28vtdWHFRHq+RS8fmJbU/VpFpN597hGeLPCbDzr2WlMvctZw
ia7pP4tX9tJI7oyCvDxZ7ubUUi/bvY7tfgi7b1hJHYyWPa8ik3kGhPbcffbEX/PaWbZ6TM8aOxwc
HSi/4mtjCdowRwdOJ4dQPkZp+aok3Wubm5dlZCNLOZJzd9+9haGtqNoAY/hkgSe2BKs+IcrOAf6A
```

```
16yiOZE/GXuk2zsaQv1iL28rOxvJuY7S4/JUvAxySI7V6ySJSljg5iDesuWoRSRdGw==
root@dragoon
```

Automatically using the following command:

```
ssh-copy-id pandora@server_ip
```

It will ask the password of the “pandora” user server, and once this has been confirmed, it will show a message like this one:

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

Do this test to verify that the automatic connection to the Pandora FMS server with the “pandora” user from the agent's machine with root user is possible. The agent will not be able to send data through SSH until it works.

This method will be used by agents to copy data to the /var/spool/pandora/data_in Pandora FMS server directory.

Make sure that the directory /var/spool/pandora/data_in already exists and that the user «pandora» has writing permissions, otherwise it will not work.

Finally, modify the agent configuration to specify the copying method as ssh and not tentacle. This is modified in the */etc/pandora/pandora_agent.conf* file and in the *transfer_mode* configuration token.

FTP configuration to receive data in Pandora FMS

Client configuration to send data through FTP allows to specify the user and password that will be sent. So it becomes quite easy to implement copying through FTP instead of Tentacle.

Besides configuring the Pandora FMS agents for sending data by means of FTP, set a FTP server in Pandora FMS server, set a password for the “pandora” user (that will be the one to be uses in the Pandora FMS agents) and grant writing access to the “pandora” user to the /var/spool/pandora/data_in directory and to lower ones.

This implies configuring the FTP server to tailor it to these needs. Therefore, vsFTPd is used throughout this guide.

SSH Server Securization

Pandora FMS uses sftp/ssh2 (scp), among others, to copy data files from agents to the server. Therefore, you will need at least one data server with a SSH2 server that listens to «pandora» user. This could be an important risk for a network that needs to be strictly securized. Open SSH2 is **highly** safe, but regarding Computer Security, there is nothing that is absolutely safe, so take action in order

to make it “safer”.

If is equally possible to ban access through SSH to certain users, as well as setting restrictions to access through FTP.

To proceed, modify the “pandora” user. This user must have a password. Its login shell will be changed to restrict access by SSH to the user, and its home directory, to prevent him from accessing other folders:

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

In Debian systems, the shell route is /usr/sbin/nologin.

With these user changes, it will not be possible to login through SSH.

Vsftpd securization

The cons about using FTP instead of Tentacle is that sending data through FTP is not as safe, since having an FTP running on Pandora FMS server makes it more vulnerable to FTP system design inherent failures. The following sections describe how to provide basic server safety.

Therefore, and similar to how the login through SSH for *pandora* user was disabled for safety reasons, a safe access method through FTP must be set. A simple and safe method is creating a PAM rule for vsftpd. Therefore, create a /etc/pam.d/ftp file that contains the following:

```
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
```

In Debian systems, the shell path is /usr/sbin/nologin.

Look for the pam_service_name token in the vsftpd (/etc/vsftpd.conf) configuration file and type in the name of the created file:

```
pam_service_name=ftp
```

With this configuration, only users that belong to the *pandora* group and have *nologin* as associated shell will be able to access Pandora FMS though FTP. As a result, the group «pandora» including «pandora» user must be created, if it does not exist yet.

Just by adjusting a couple of things in the /etc/vsftpd.conf file, access to users that login through FTP to their direct root can be restricted. The parameters are the following:

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

In case some user needs to be excluded and restricting it to its Chroot must be avoided, just include said user in the vsftpd.nochroot_list file (one user per line).

Other options for higher security are these:

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

Remember restarting the vsftpd service after modifying the configuration file so that the changes become effective.

With these settings, the user will be limited to its root directory (*/var/spool/pandora/data_in* for «pandora» user specifically). The user can carry out FTP transferences to send files but it cannot list files.

Try logging in with the «pandora» user in FTP, change directory and list files, if you cannot, the setup has been successful.

Go back to Pandora FMS documentation index