Configuring SSH and/or FTP to Receive Data

Configuring SSH and/or FTP to Receive Data

Introduction

The standard transfer method in Pandora FMS to transmit files, Tentacle, needs the Perl programming language installed. Some devices, such as ESX (UNIX) systems, lack this tool. When this happens, the alternatives are to use FTP or SSH to transfer monitoring data.

Pandora FMS can use the FTP or SSH protocol to copy the XML data packets generated by software agents to PFMS server.

SSH configuration to receive data in Pandora FMS

Always take into account the Security Architecture of Pandora FMS.

Consider Pandora FMS server as Server and each one of the devices running the Software Agent as Client. At any time, it will be possible to check with which user it works by means of the whoami command.

User creation in Server

A `pandora` user should be created in the machine where Pandora FMS server is running. This machine will receive the data through SSH. If a Pandora FMS server was already installed, surely this user is already created. Set a strong password for that user with the command:

```
passwd pandora
```

User configuration in Server

In the server, you should create a directory called `/home/pandora/.ssh` with permissions `750` and user `pandora:root`.

Key Creation in Client

A pair of keys (private and public) has to be created in each machine that runs a Software Agent that will use SSH. To that end, run the following command with the same user with which Pandora FMS Software Agent is executed:

```
ssh-keygen
```

A series of questions will be displayed, which you will have to answer by simply pressing the Enter key. Then a public and a private key will have been created for that user in the machine. Now it should be copied to the destination machine, which is the Pandora FMS server where you need to send the monitoring data.

Copy of public key to Server

The public key that you just generated can be copied in two ways to Pandora FMS Server.

Manual copy

The public key file generated in the Client is:

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

Where <user> is the username that runs Pandora FMS Software Agent in the Client. If the key pair was generated as root user or *root*, it will be in:

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

This file will have a content similar to this one:

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

This content must be added to the end of the authorised_keys file on the Server. Its path is:

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

The `authorized_keys` file on the Server must belong (*ownership*) to the user `pandora:root` and must have `600` permissions.

Automatic copying

Use the following command in the Client:

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

Where `<server_address>` is the IP address or Server URL.

It will ask for the server `pandora` user password (set in the previous step) and once it confirms it, a message similar to the following will be displayed:

```
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.
```

Perform this test to verify the automatic connection to Pandora FMS Server with the user `pandora` from the Client (with the user that runs the Software Agent):

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

Once you are able to connect to the Server as described above, the Software Agent on the Client can start sending monitoring data.

Client Configuration

Once the connection through SSH is verified, this will be the method used by the software agents to copy data to Pandora FMS Server directory. This directory is located at:

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

Verify that the directory `/var/spool/pandora/data_in` exists and the user `pandora` has writing permissions, otherwise it will not work.

Finally, the software agent configuration in the Client is modified to specify that the copy method is SSH. This is modified in file `/etc/pandora/pandora_agent.conf`, in the configuration token `transfer_mode`. The software agent service must be restarted on each Client after this change.

Securing the SSH server

Pandora FMS uses, among others, sftp/ssh2 (SCP) to copy data files from software agents to the server. Because of this, you will need at least one data server with an SSH2 server listening to the `pandora` user. This could be a significant risk in a network that needs to be strictly secured. OpenSSH2 is very secure, but in terms of computer security there is no such thing as absolutely secure, so steps must be taken to make it “more” secure.

It is possible to prohibit SSH access for certain users, as well as to configure restrictions on FTP access.

To do this, the user `pandora` must be modified in the Server. This user must have a strong password. His login *shell* will be changed to restrict SSH access to the user, and his `home` directory, to prevent their access to other folders:

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

With these changes to the user `pandora` on the Server, when logging in via SSH, you will not be able to run commands with it in an interactive terminal.

- See the recommended operating systems for Pandora FMS.
- On Debian systems, the shell path is `/usr/sbin/nologin`.

FTP configuration to receive data in Pandora FMS

The client configuration for sending data through FTP allows you to specify the user and password to be sent, making it fairly easy to implement FTP copying instead of Tentacle.

Besides configuring Pandora FMS software agents for sending data with FTP, you will have to configure an FTP server where Pandora FMS server executes, set a password for the user `pandora` and allow writing access to the user `pandora` to the directory `/var/spool/pandora/data_in` and its subdirectories.

The FTP server must be configured to meet these needs; vsftpd is used in this guide.

Installing vsftpd

The disadvantage of using FTP instead of Tentacle is that sending data through FTP is less secure, because having an FTP running on Pandora FMS server makes it more vulnerable to inherent failures in the design of the FTP system. The following sections will show how to configure in a

minimal way the vsftpd server (simply called Server).

For that reason, and in the same way that disabled for security SSH login for the `pandora` user, a safe access method must be established for FTP users. A safe and simple method for this is to create a PAM rule for vsftpd. To do this, create a file called `/etc/pam.d/ftp` containing 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 the vsftpd configuration file (`/etc/vsftpd.conf`) the `pam_service_name` token is configured:

```
pam_service_name=ftp
```

With this configuration, only the users that belong to the group `pandora` and have `nologin` as associated shell will be able to connect to Pandora FMS by FTP, *so you should create the group* `pandora` *that includes the user* `pandora`. In any case, verify that both exist in the Server.

With a final configuration of the `/etc/vsftpd.conf` file, you will restrict the access of users accessing your home directory through FTP. The parameters are as follows:

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

In case you need to exclude a user from this performance and avoid restricting it to your Chroot, just include that user in this `vsftpd.nochroot_list` file (one user per line).

Other options to be configured to establish greater security measures are as follows:

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

The vsftpd service must be restarted after making changes to the configuration file for them to take effect.

With this configuration, users will be restricted to their home directory (`/var/spool/pandora/data_in` in the case of the `pandora` user). The user will be able to perform FTP transfers (send files), but will not be able to list files.

It is recommended to try to log in with the user `pandora` in the FTP, change directory and list files; if unsuccessful, then the configuration will have been successful.

Back to Pandora FMS Documentation Index