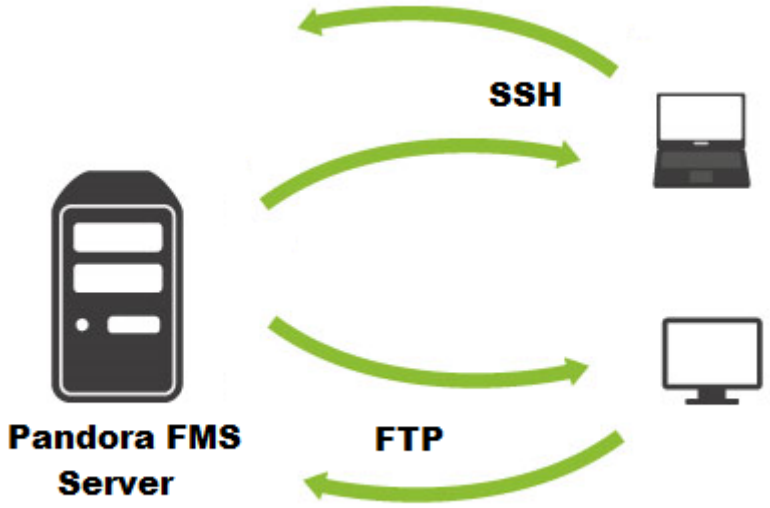
# Configuration SSH et/ou FTP pour recevoir des données

# Configuration SSH et/ou FTP pour recevoir des données

## Introduction

La méthode de transfert standard dans Pandora FMS pour transmettre des fichiers, Tentacle, nécessite le langage de programmation Perl installé. Certains appareils, tels que les systèmes ESX (UNIX), ne disposent pas de cet outil. Lorsque cela se produit, les alternatives sont d'utiliser FTP ou SSH pour transférer les données de supervision.




Pandora FMS peut utiliser le protocole FTP ou SSH pour copier les packages de données XML générés par les agents logiciels vers le serveur PFMS.

## Configuration SSH pour recevoir des données dans Pandora FMS

Toujours tenir compte de l'architecture de sécurité Pandora FMS.

Considérez le serveur Pandora FMS en tant que serveur et chacun des appareils exécutant l'agent logiciel en tant que Client. Vous pouvez à tout moment vérifier avec quel utilisateur vous travaillez à l'aide de la commande whoami.

### Création d'un utilisateur sur un serveur

Étape 1 : Créer un utilisateur `pandora` sur la machine sur laquelle le serveur Pandora FMS est exécuté. Cette machine recevra les données par SSH. Si vous avez déjà installé un serveur Pandora FMS, cet utilisateur est probablement déjà créé. Définissez un mot de passe sûr pour cet utilisateur à l'aide de la commande :

```
passwd pandora
```

### Configuration d'un utilisateur sur un serveur

Étape 2 : Sur le serveur, créez un répertoire `/home/pandora/.ssh` avec les autorisations `750` et l'utilisateur `pandora :root`.

### Création de clés dans le client

Étape 3 : Créer, sur chaque machine exécutant un agent logiciel qui utilisera SSH, une paire de clés (privée et publique). Pour ce faire, exécutez la commande suivante avec le même utilisateur que l'agent logiciel Pandora FMS :

```
ssh-keygen
```

Vous verrez une série de questions auxquelles vous devrez répondre en appuyant simplement sur la touche Entrée. Avec cela, vous aurez créé une clé publique et une clé privée pour cet utilisateur sur la machine. Vous devez maintenant la copier sur la machine cible, qui est le serveur Pandora FMS vers lequel vous souhaitez envoyer les données de supervision.

### Copie de clé publique au serveur

Étape 4 : Copier la clé publique sur le serveur Pandora FMS. La clé publique que vous venez de générer peut être copiée de deux manières.

#### Copie manuelle

Le fichier de clé publique généré dans le Client est :

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

Où est le nom d'utilisateur `<user>` que l'agent logiciel Pandora FMS exécute sur le client. Si la paire de clés a été générée en tant qu'utilisateur racine ou *root*, elle se trouve dans :

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

Ce fichier aura un contenu similaire à celui-ci :

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

Ce contenu doit être ajouté à la fin du fichier `authorized_keys` sur le Serveur. Son chemin est :

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

Le fichier `authorized_keys` sur le Serveur doit appartenir (*ownership*) à l'utilisateur `pandora:root` et doit avoir des autorisations `600`.

#### Copier automatiquement

Utilisez la commande suivante dans le client :

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

Où `< server_address >` est l'adresse IP ou l'URL du serveur.

Il demandera le mot de passe de l'utilisateur `pandora` du serveur (défini à l'étape 1) et, une fois confirmé, affichera un message similaire au suivant:

```
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.
```

Effectuez ce test pour vérifier la connexion automatique au Serveur Pandora FMS avec l'utilisateur `pandora` depuis le Client (avec l'utilisateur exécutant l'Agent Logiciel):

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

Une fois que vous avez réussi à connecter le serveur de la manière indiquée, l'agent logiciel du client peut commencer à envoyer des données de supervision.

### Configuration du client

Une fois la connexion vérifiée via SSH, il s'agit de la méthode utilisée par les agents logiciels pour copier des données dans le répertoire du serveur Pandora FMS. Ce répertoire est situé à :

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

Assurez-vous également que le répertoire`/var/spool/pandora/data_in` existe et que l'utilisateur `pandora` dispose d'autorisations d'écriture, sinon cela ne fonctionnera pas.

Enfin, modifiez les paramètres de l'agent logiciel dans le Client pour spécifier que la méthode de copie est SSH. Ceci est modifié dans le fichier `/etc/pandora/pandora_agent.conf`, dans le jeton de configuration `transfer_mode`. N'oubliez pas que vous devez ensuite redémarrer le service de l'agent logiciel sur chaque client après cette modification.

### Sécurisation du serveur SSH


Pandora FMS utilise, entre autres, sftp/ssh2 (SCP) pour copier des fichiers de données des agents logiciels vers le serveur. Pour cette raison, vous aurez besoin d'au moins un serveur de données avec un serveur SSH2 à l'écoute de l'utilisateur `pandora`. Cela pourrait entraîner un risque important sur un réseau qui doit être strictement sécurisé. OpenSSH2 est très sûr, mais en ce qui concerne la sécurité informatique, rien n'est absolument sûr ; par conséquent, des mesures doivent être prises pour le rendre « plus » sûr.

Toujours tenir compte de l'architecture de sécurité Pandora FMS.

Il est possible d'interdire l'accès par SSH à certains utilisateurs, ainsi que de configurer des restrictions d'accès par FTP.

Pour ce faire, vous devez modifier l'utilisateur `pandora` sur le serveur. Cet utilisateur doit avoir un mot de passe robuste. Votre *shell* de connexion sera modifié pour restreindre l'accès par SSH à l'utilisateur, et votre répertoire `home`, pour empêcher l'accès à d'autres dossiers :

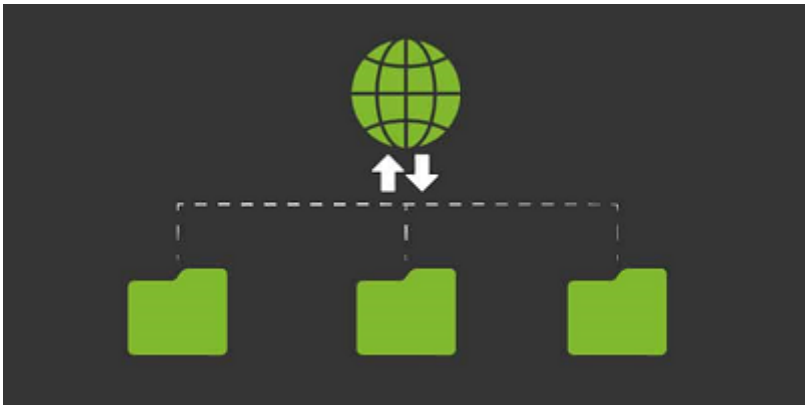
```
usermod -s /sbin/nologin -d /var/spool/pandora/data_in pandora
```

Avec ces modifications apportées à l'utilisateur `pandora` sur le Serveur, l'ouverture de session par SSH ne peut pas exécuter de commandes avec lui sur un terminal interactif.

(Veuillez consulter les systèmes d'exploitation recommandés pour Pandora FMS.) Dans les systèmes Debian, le chemin d'accès du *shell* est `/usr/sbin/nologin`.

## Configuration FTP pour recevoir des données dans Pandora FMS

La configuration sur le client pour envoyer des données par FTP permet de spécifier l'utilisateur et le mot de passe à envoyer, ce qui rend assez simple la mise en œuvre de la copie par FTP plutôt que par Tentacle.



En plus de configurer les agents logiciels Pandora FMS pour l'envoi de données avec FTP, vous devrez configurer un serveur FTP sur lequel le serveur Pandora FMS s'exécute, définir un mot de passe pour l'utilisateur `pandora` et autoriser l'accès en écriture de l'utilisateur `pandora` au répertoire `/var/spool/pandora/data_in` et à ses sous-répertoires.

Cela signifie que vous devrez configurer le serveur FTP pour répondre à ces besoins ; pour cela, ce guide utilise vsftpd .

### Sécurisation de vsftpd

L'inconvénient d'utiliser FTP au lieu de Tentacle est que l'envoi de données par FTP est moins sécurisé, car avoir un FTP fonctionnant sur le serveur Pandora FMS le rend plus vulnérable aux défaillances inhérentes à la conception du système FTP. Dans les sections suivantes, il sera indiqué comment sécuriser de manière minimale le serveur vsftpd (appelé simplement Serveur)

Par conséquent, et de la même manière qu'on a `pandora` a été désactivé pour des raisons de sécurité le *login* pour SSH pour l'utilisateur `pandora`, une méthode d'accès sécurisée doit être établie pour les utilisateurs par FTP. Une méthode sûre et simple pour cela est de créer une règle PAM pour vsftpd. Pour cela, vous devez créer un fichier appelé `/etc/pam.d/ftp` qui contient les éléments suivants :

```
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
```

(Veuillez consulter les systèmes d'exploitation recommandés pour Pandora FMS.) Dans les systèmes Debian, le chemin d'accès du *shell* est `/usr/sbin/nologin`.

Dans le fichier de configuration vsftpd (`/etc/vsftpd.conf`), recherchez le jeton `pam_service_name` et définissez le nom du fichier créé :

```
pam_service_name=ftp
```

Avec cette configuration, seuls les utilisateurs qui appartiennent au groupe `pandora` et qui ont `nologin` en tant que *shell* associé pourront se connecter à Pandora FMS par FTP, *vous devez donc créer le groupe* `pandora` qui inclut l'utilisateur `pandora`. Dans tous les cas, vérifiez que les deux existent sur le Serveur.

Avec une configuration finale du fichier `/etc/vsftpd.conf`, l'accès des utilisateurs qui accèdent par FTP à son répertoire racine sera restreint. Les paramètres sont les suivants:

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

Si vous devez exclure un utilisateur de ce comportement et éviter de le restreindre à son Chroot, vous n'aurez qu'à inclure cet utilisateur dans ce fichier `vsftpd.nochroot_list` (un utilisateur par ligne).

Les autres options à configurer pour établir une plus grande sécurité sont les suivantes :

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

N’oubliez pas de redémarrer le service vsftpd après avoir apporté des modifications au fichier de configuration pour qu’elles prennent effet.

Avec cette configuration, l’utilisateur sera limité à son répertoire racine (`/var/spool/pandora/data_in` dans le cas de l’utilisateur `pandora`). L’utilisateur pourra effectuer des transferts via FTP (envoyer des fichiers), mais ne pourra pas répertorier les fichiers.

Essayez de vous connecter avec l’utilisateur `pandora` au FTP, modifiez le répertoire et répertoriez les fichiers ; si vous ne réussissez pas , la configuration aura été un succès.

Retour à l'index de documentation Pandora FMS