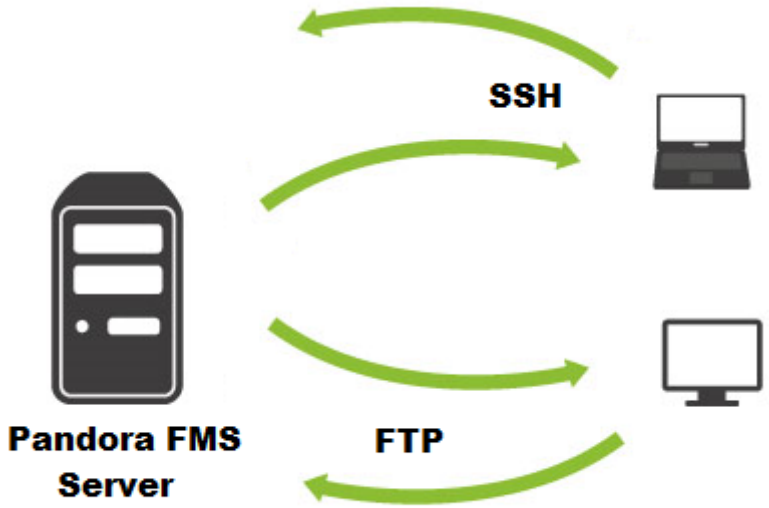
SSH および FTP でのデータ転送設定

SSH および FTP でのデータ転送設定

Pandora FMS ドキュメント一覧に戻る

概要

Pandora FMS で標準の転送方法(tentacle)を使用できない場合があります。これは、Perl が無い Unix システム(ESX システムなど)を使用している場合で、古いシェルスクリプトのエージェントを使用する場合です。 この場合は、FTP または SSH を使用してファイルを転送することができます。



Pandora FMS は、SSH プロトコルを使用して、ソフトウエアエージェントによって生成された XML データパッケージをサーバにコピーできます。

Pandora FMS へのデータ取り込みのための SSH 設定

常に、Pandora FMS の セキュリティアーキテクチャ に注意
してください。

Pandora FMS サーバを サーバ と見なし、ソフトウェアエージェントを実行している各デバイスを クライアント と見なします。 whoami コマンドを使用して、作業しているユーザをいつでも確認できます。

サーバでのユーザ作成

ステップ 1: Pandora FMS サーバがインストールされているホストに pandora ユーザを作成します。

このユーザーは SSH を介してデータを受信します Pandora FMS サーバがすでにインストールされている場合は、このユーザはすでに作成済です。 次のコマンドを使用して、このユーザに強力なパスワードを設定します。

```
passwd pandora
```

サーバのユーザ設定

ステップ 2: サーバ内で、パーミッション 750 およびユーザ pandora:root で /home/pandora/.ssh ディレクトリを作成します。

クライアントでの鍵作成

ステップ 3: SSH を使用する必要があるエージェントの各システムで、鍵のペア(秘密鍵と公開鍵)を作成します。 これを行うには Pandora FMS エージェントの実行に使用されるユーザで次のコマンドを実行します。

```
ssh-keygen
```

いくつかの質問が表示されます Enter キーを押すだけで回答できます。 このユーザの公開/秘密鍵がシステムに作成されます。 次に、データの送信先である Pandora FMS サーバであるターゲットシステムにコピーします。

公開鍵のサーバへのコピー

ステップ 4: 公開鍵を Pandora FMS サーバにコピーします。 作成された公開鍵をコピーするには、2 つの方法があります。

手動コピー

クライアント で生成された公開鍵は以下にあります。

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

ここで、<user> は、クライアントで Pandora FMS ソフトウエアエージェントを実行するユーザ名です。鍵のペアを root ユーザで生成した場合は、以下にあります。

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

このファイルには次のようなものが含まれます。

```
ssh-rsa
```

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

この内容を、サーバ の authorized_keys ファイルの最後に追加する必要があります。パスは次の通りです。

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

サーバの authorized_keys ファイルの所有者とグループは pandora:root で、パーミッションは 600 である必要があります。

自動コピー

クライアント にて次のコマンドを利用します。

```
ssh-copy-id pandora@<Server-address>
```

ここで、<Server-address> は、サーバ の IP アドレスまたは URL です。

pandora ユーザのパスワード(ステップ 1 で設定)を要求します。これが確認されると、次のようなメッセージが表示されます。

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

クライアント (のソフトウエアエージェント実行ユーザ)から Pandora FMS サーバの pandora ユーザへ自動接続が可能であることを確認します。

```
ssh pandora@<Server-address>
```

上記のように サーバ に接続できるようになると、クライアントのソフトウェアエージェントは監視データの送信を開始できるようになります。

クライアント設定

SSH を介した接続を確認できたら、これがソフトウェアエージェントがデータを Pandora FMS サーバディレクトリにコピーするために使用される方法になります。 このディレクトリは次の場所にあります。

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

また、/var/spool/pandora/data_in ディレクトリが存在し、ユーザ pandora に書き込み権限があることを確認してください。そうでない場合は機能しません。

最後に、クライアントの ソフトウエアエージェント設定を変更して、コピー方法を tentacle ではなく ssh に設定します。 これは /etc/pandora/pandora_agent.conf ファイルの transfer_mode 設定トークンで行います。この変更後は、クライアントのソフトウエアエージェントサービスを再起動することを忘れないでください。

SSH サーバのセキュリティ強化

Pandora FMS は、特に sftp/ssh2(scp) を使用して、エージェントからサーバにデータファイルをコピーします。 このため、pandora ユーザを待ち受ける SSH2 サーバを備えた少なくとも 1つのデータサーバが必要です。 これは、厳密にセキュリティ保護する必要があるネットワークにとって重大なリスクになる可能性があります Open SSH2 は 非常に 安全ですが、コンピュータのセキュリティに関しては、絶対に安全なものはないため、“ より安全 ” にするための対策を講じてください。

常に、Pandora FMS の セキュリティアーキテクチャ に注意してください。

FTP を介したアクセスに制限を設定するのと同じように SSH を介した特定のユーザのアクセスを禁止することも可能です。

それを行うするには、サーバ の pandora ユーザの設定を変更します。 このユーザには強力なパスワードが必要です。 他のフォルダーへのアクセスを回避するために、ログインシェルを変更しホームディレクトリを変更します。

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

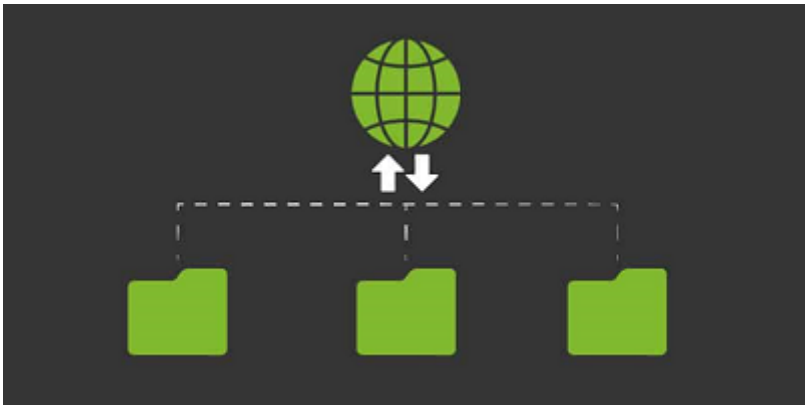
サーバ の pandora ユーザに対するこの変更で、該当ユーザが SSH でログインした際にはターミナ

ルでコマンドを実行できなくなります。

(Pandora FMS の 推奨 OS を確認してください) Debian システムでは、シェルは /usr/sbin/nologin です。

FTP にてサーバがデータを受け取る設定

FTP 経由でデータを送信するクライアント設定は、送信するユーザとパスワードの指定で可能です。tentacle の代わりに FTP を介してコピーを実装するのは非常に簡単です。



FTP を使用してデータを送信するように Pandora FMS エージェントを設定するほか、Pandora FMS サーバに FTP サーバを設定し、ユーザ pandora (Pandora FMS エージェントで使用する)のパスワードを設定し、pandora ユーザに /var/spool/pandora/data_in 以下の書き込みアクセスを許可します。

ニーズに合わせて FTP サーバを設定します。このガイドでは vsFTPd を使用します。

Vsftpd でのセキュリティ強化

Tentacle の代わりに FTP を使用することの短所は、FTP を介したデータ送信は安全ではないため、Pandora FMS サーバで FTP サーバを実行することが脆弱になります。 以下のセクションでは、サーバーの安全性を最小限にする方法について説明します。

安全上の理由で pandora ユーザの SSH 経由のログインを無効にするのと同様に、FTP 経由の安全なアクセス方法を設定する必要があります。簡単で安全な方法は、vsftpd の PAM ルールを作成することです。 次の内容の /etc/pam.d/ftp ファイルを作成します。

```
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
```

(Pandora FMS の 推奨 OS を確認してください) Debian システムでは、シェルは /usr/sbin/nologin です。

vsftpd の設定ファイル(/etc/vsftpd.conf) で、pam_service_name トークンを探し、作成したファイル名を入力します。

```
pam_service_name=ftp
```

この設定により、pandora グループに属し、nologin のシェルを持つユーザのみが FTP 経由でPandora FMS にアクセスできます。 そのため、pandora ユーザを含むグループ pandora を作成する必要があります(存在しない場合)。

/etc/vsftpd.conf ファイルにて、いくつかの設定を調整するだけでFTP 経由でログインするユーザの root へのアクセスを制限できます。 パラメータは次のとおりです。

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

一部のユーザを除外し、Chroot に制限することを避ける必要がある場合は、vsftpd.nochroot_list ファイルにそのユーザを含めます(1行に1ユーザー)。

セキュリティを強化するための他のオプションは次のとおりです。

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

設定を変更した際は、それを反映するために vsftpd サービスを再起動する必要があります。

これらの設定により、ユーザはそのルートディレクトリ (pandora ユーザの場合は /var/spool/pandora/data_in に限定されます)。 ユーザは FTP 転送を実行してファイルを送信できますが、ファイルの一覧は見ることができません

FTP でユーザ pandora を使用してログインし、ディレクトリの移動とファイル一覧の取得を試してみてください。できない場合は、正しくセットアップができています。

Pandora FMS ドキュメント一覧に戻る