ProFTPD FTPS & FTPES

>>> FTP Implicit SSL & FTP Explicit SSL

Description :

Le but de cet article est de vous apprendre à configurer et mettre en place un serveur FTP sécurisé avec SSL/TLS. Nous aborderons ici les deux modes "Implicit" et "Explicit".

ProFTPD FTPS & FTPES

>>> FTP Implicit SSL & FTP Explicit SSL

Sommaire :

I) Introduction

Dans un précèdent article, j'ai expliqué comment configurer ProFTPD. Je vais maintenant vous expliquer comment mettre en place un serveur FTP sécurisé.

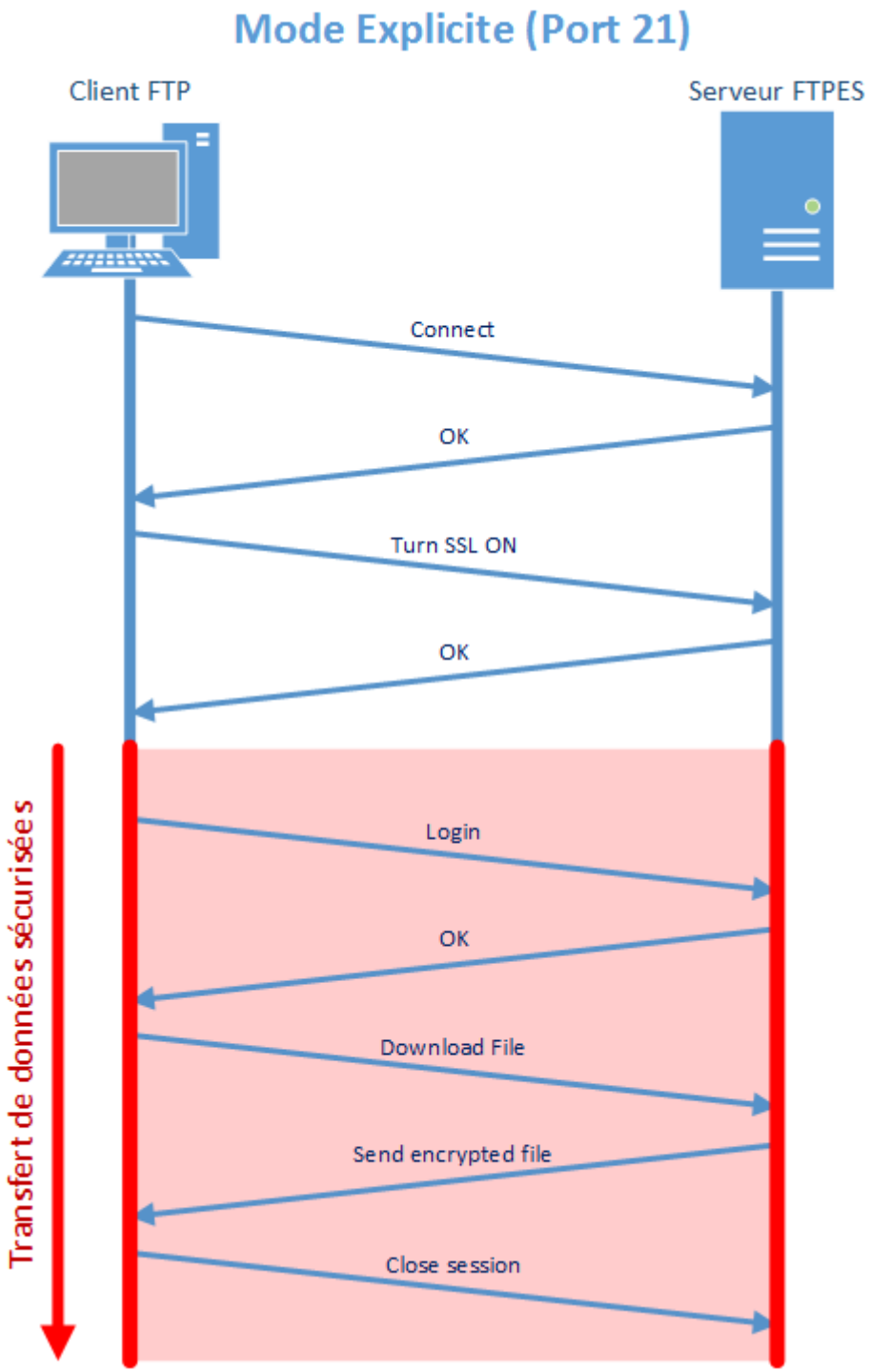
Il existe trois types de FTP sécurisé :
- SFTP : Connexion FTP utilisant le protocole SSH (FTP over SSH)
- FTPES : Connexion FTP utilisant le protocole SSL ou TLS en mode Explicit
- FTPS : Connexion FTP utilisant le protocole SSL/TLS en mode Implicit

Comme l'indique le titre de l'article, l'article concerne uniquement la configuration et la mise en place du FTPS et FTPES.

Pour plus d'explication, voici la différence entre le FTP explicit SSL et le FTP implicit SSL :
- Explicit FTP over SSL/TLS :

- La connexion s'effectue sur le port 21, le port de commande FTP standard, et soit :
    - La commande **"AUTH TLS"** demande au serveur de chiffrer le transfert de commande en TLS, et le chiffrement du transfert de données se fait par la commande **"PROT P"** ;
    - La commande **"AUTH SSL"** (non standard) demande au serveur de chiffrer le transfert de commande et de données en SSL.
- Cette approche est compatible avec les serveurs ou clients FTP ne supportant pas le chiffrement SSL/TLS, auquel cas une connexion non chiffrée pourra être utilisée ou bien refusée.
- Le schéma d'URI est ftpes :// ou simplement ftp://.

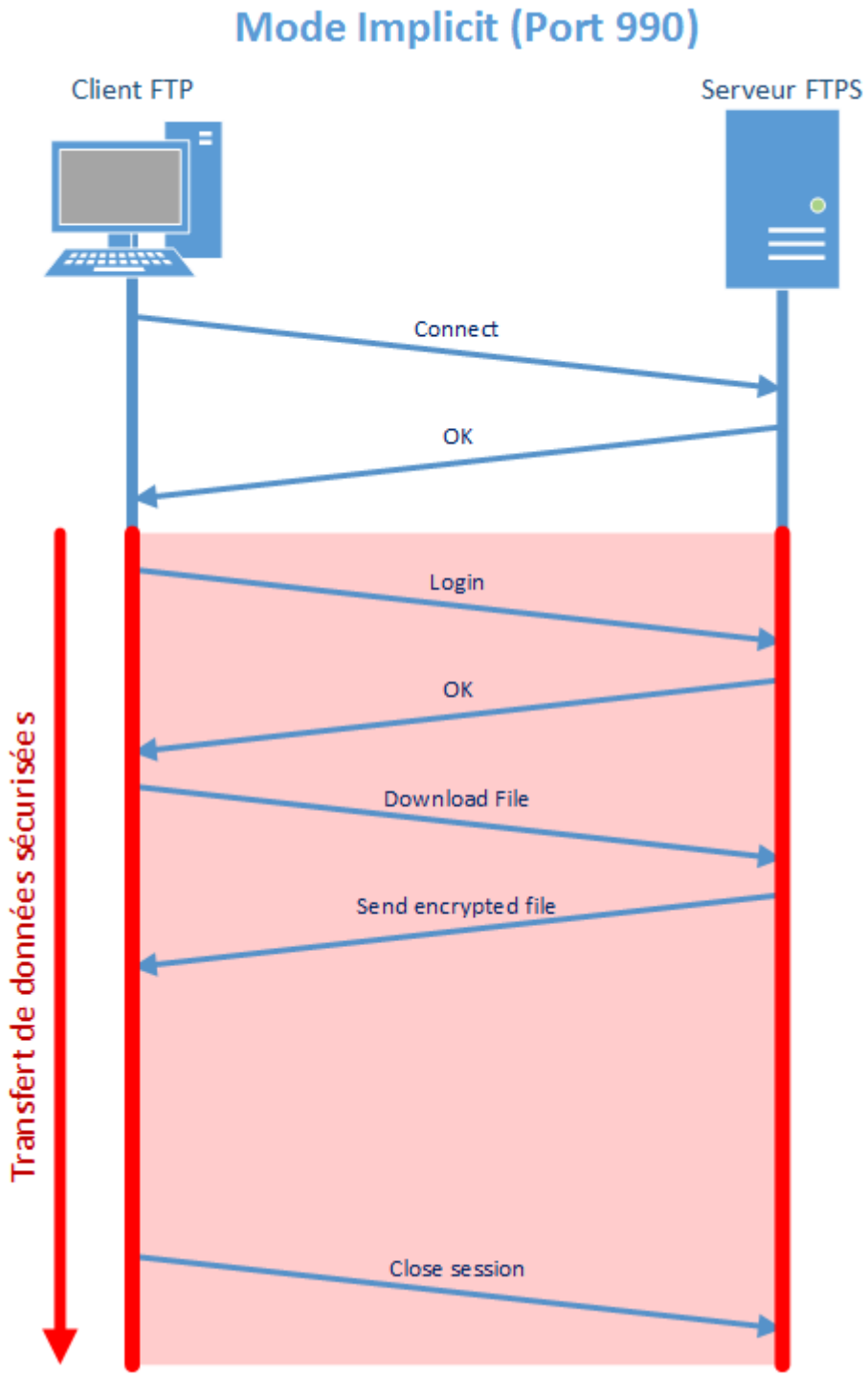
Voici un diagramme des échanges :



- Implicit SSL/TLS encrypted FTP :

- La connexion au serveur se fait sur le port 990 qui est le port de commande et sur lequel la négociation SSL/TLS s'effectue. Le port de données est le 989 et est lui aussi chiffré.
- Cette approche plus ancienne que la méthode explicite n'est pas soutenue par l'IETF.
- Cette approche est semblable au fonctionnement du HTTPS décrit dans la RFC 28183 car la négociation SSL/TLS se fait lors de la connexion.
- Le schéma d'URI est ftps ://.

Voici un diagramme des échanges :



II) Installation

1) Installation

Pour installer le paquet "**Proftpd**", tapez la commande suivante :

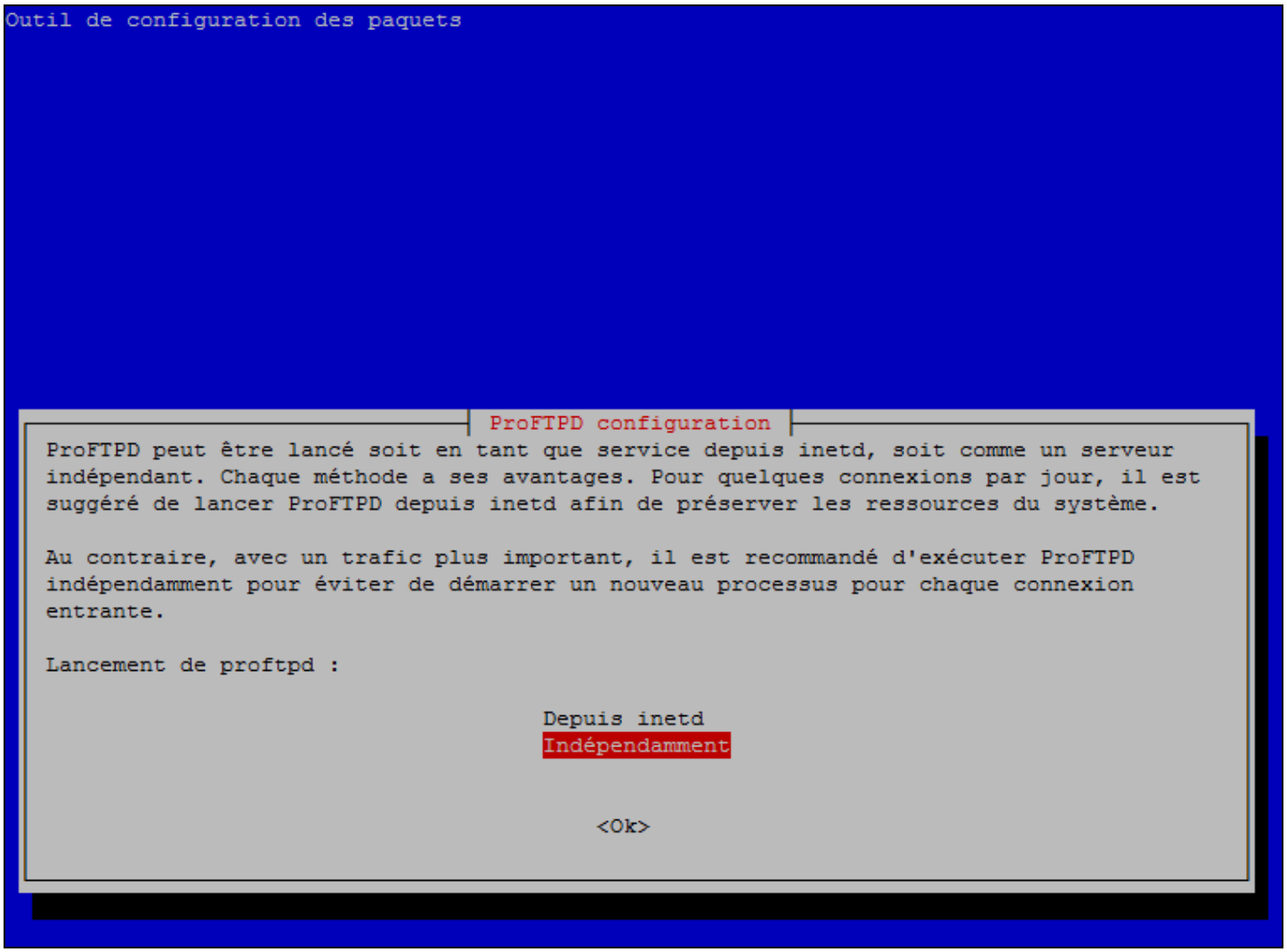
```
aptitude install proftpd
```

Lors de l'installation, ProFTPD vous propose deux modes :
- Inetd
- Standalone

ProFTPD peut être lancé soit en tant que service depuis inetd, soit comme un serveur indépendant. Chaque

méthode a ses avantages. Pour quelques connexions par jour, il est suggéré de lancer ProFTPD

depuis inetd afin de préserver les ressources du système.
Au contraire, avec un trafic plus important, il est recommandé d'exécuter ProFTPD indépendamment pour éviter de démarrer un nouveau processus pour chaque connexion entrante.



Le serveur FTP fonctionne par défaut après installation. Vous trouverez le fichier de configuration dans le répertoire "/etc/proftpd/".

2) Configuration de base

- Éditez le fichier de configuration de ProFTPD

```
vim /etc/proftpd/proftpd.conf
```

- Modifiez les paramètres suivants :

```
UseIPv6 off
IdentLookups off
ServerName "Debian"
```

3) Configuration du module TLS

- Éditez le fichier de configuration de ProFTPD

```
vim /etc/proftpd/proftpd.conf
```

- Décommentez la ligne suivante :

```
Include /etc/proftpd/tls.conf
```

III) Configuration FTP Explicit SSL

1) Génération du certificat et de la clef

Avant de configurer le module TLS, vous devez générer le certificat et la clef.

- Commencez par créer un répertoire pour stocker le certificat et la clef.

```
mkdir /etc/proftpd/ssl
```

- Tapez la commande suivante pour générer le certificat et la clef auto-signé.

  - **-newkey rsa:2048** : Correspond à la taille de la clef
  - **-keyout /etc/proftpd/ssl/proftpd.key** : Correspond au chemin ou sera enregistré la clef
  - **-out /etc/proftpd/ssl/proftpd.crt** : Correspond au chemin ou sera enregistré le certificat
  - **-days 365** : Correspondant à la durée de validité du certificat

```
openssl req -x509 -newkey rsa:1024 -keyout /etc/proftpd/ssl/proftpd.key -out
/etc/proftpd/ssl/proftpd.crt -nodes -days 365
```

- Vous devez obtenir ceci :

```
Generating a 1024 bit RSA private key
........++++++
...++++++
writing new private key to '/etc/proftpd/ssl/proftpd.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:FR
State or Province Name (full name) [Some-State]:France
Locality Name (eg, city) []:Nantes
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Idum
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:Deb-Idum-LAB.idum.eu
Email Address []:
```

- Modifiez les droits du certificat et de la clef. Afin de définir les deux fichiers en lecture seule.

```
chmod 0640 /etc/proftpd/ssl/proftpd.key
```

```
chmod 0640 /etc/proftpd/ssl/proftpd.crt
```

2) Configuration du module TLS

- Éditez le fichier de configuration du module **tls.conf**.

```
vim /etc/proftpd/tls.conf
```

- Décommentez et modifiez les lignes suivantes :

- **TLSEngine** : Active le module
- **TLSLog** : Définit l'emplacement et le nom du fichier de LOG
- **TLSProtocol** : Définit le protocole

```
TLSEngine on
TLSLog /var/log/proftpd/tls.log
TLSProtocol SSLv23
```

- Décommentez et modifiez les lignes suivantes :

- **TLSRSACertificateFile** : Définit l'emplacement et le nom du certificat
- **TLSRSACertificateKeyFile** : définit l'emplacement et le nom de la clef privé

```
TLSRSACertificateFile /etc/proftpd/ssl/proftpd.crt
TLSRSACertificateKeyFile /etc/proftpd/ssl/proftpd.key
```

- Redémarrez le service ProFTPD.

```
service proftpd restart
```

- Normalement votre serveur FTPES fonctionne.

3) Options TLS

Plusieurs options sont disponibles, voir les Docs officiels de ProFTPD.

- Pour forcer l'utilisation du FTPES et interdire les connexions FTP simple. Décommentez et modifier la ligne suivante dans le fichier **"tls/conf"**.

```
TLSRequired on
```

- Pour arrêter la connexion si le client essaie de lancer une renégociation. Décommentez et modifier la ligne suivante dans le fichier **"tls/conf"**.

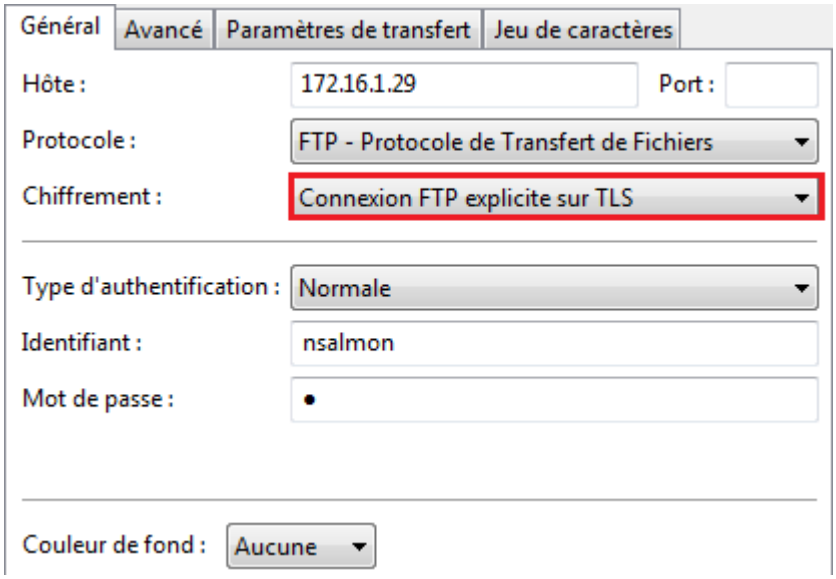
```
TLSOptions AllowClientRenegotiations
```

- Pour autoriser les renégociations SSL/TLS lorsque le client les demande, mais ne pas forcer les renégociations. Certains clients ne prennent pas en charge renégociations SSL/TLS. Quand **mod_tls** force une renégociation, ces Clients fermeront la connexion de données ou il y aura un délai d'attente sur une connexion de données inactive.

```
TLSRenegotiate required off
```

4) Configuration du client FTP

Voici la configuration que vous devez appliquer sur votre client FTP, afin de pouvoir établir une connexion FTPES :



IV) Configuration FTP Implicit SSL

1) Configuration du module TLS

Pour rappel, le FTP Implicit Secure n'est plus soutenu par l'IETF.

Pour mettre en place le FTP Implicit Over SSL/TLS, éditez le fichier de configuration **"tls.conf"**.

```
vim /etc/proftpd/tls.conf
```

- Puis ajoutez les deux lignes suivantes :

```
Port 990
TLSOptions UseImplicitSSL
```

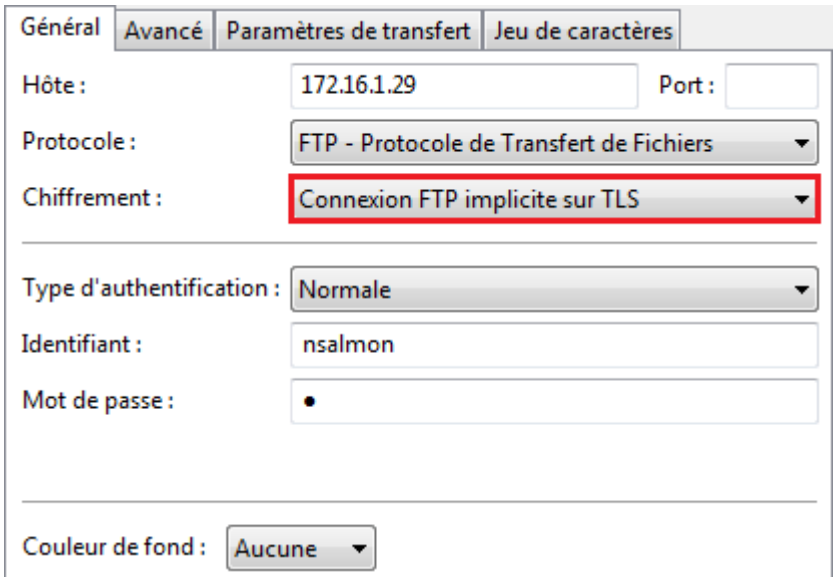
- Redémarrez le service ProFTPD.

```
service proftpd restart
```

- Votre serveur FTPS fonctionne.

2) Configuration du client FTP

Voici la configuration que vous devez appliquer sur votre client FTP, afin de pouvoir établir une connexion FTPS :


Général
Avancé
Paramètres de transfert
Jeu de caractères
Hôte :
172.16.1.29
Port :
Protocole :
FTP - Protocole de Transfert de Fichiers
Chiffrement :
Connexion FTP implicite sur TLS
Type d'authentification :
Normale
Identifiant :
nsalmon
Mot de passe :
•
Couleur de fond :
Aucune