Documentation FOG

Prérequis

Voici la liste des prérequis que vous devez avoir à votre disposition avant d’effectuer cette installation :

- Une machine cliente pouvant accéder à l’adresse IP du serveur FOG sur le port 443
- Un serveur Windows avec un rôle Active Directory avec un module LDAPS de configurer
- Un serveur de fichier (peux être sur le serveur Active Directory) avec une lecture dans le dossier partagée pour tous les ordinateurs du domaine
- Une autorité de certification local configurée sur une base Debian 13 avec le service EASY-RSA

- Un serveur DHCP (peux être sur le serveur Active Directory) pour les clients du domaine
- Une machine avec minimum 2 CPU Virtuel, 2 Giga de RAM, avec un système Debian 13 CLI d'installé dessus, cette machine est celle que l'on va utiliser pour la mise en place de notre serveur FOG

1. Configuration de la machine

1.1 Configuration Adresse IP / DNS

1. Nous allons commencer par attribuer une adresse IP à notre machine en créant le fichier de conf dans l'interfaces à l'aide de cette commande :

```
nano /etc/network/interfaces.d/<Nom de l'interface>.cfg
```

2. Mettre dans ce fichier ceci :

```
auto <Nom de l'interface>
iface <Nom de l'interface> inet static
    address <Adresse IP>
    gateway <passerelle par défaut>
    dns-nameservers <Adresse IP DNS 1>
    dns-nameservers <Adresse IP DNS 2>
```

3. Aller modifier le "resolv.conf" ce qui permet de configurer les DNS voici la commande :

```
nano /etc/resolv.conf
```

4. Supprimer tout le contenu de ce fichier et mettre ceci à la place

```
domain <Domaine>
search <Domaine>
nameserver <Adresse IP DNS 1>
nameserver <Adresse IP DNS 2>
```

5. Pour mettre à jour ces paramètres vous pouvez redémarrer le service réseau, voici la commande :

```
systemctl restart networking
```

1.2 Modification du nom de la machine

1. Le fichier à aller modifier pour modifier le nom de la machine est “hostname” voici la commande pour le modifier

```
nano /etc/hostname
```

2. Supprimer le contenu de ce fichier et y mettre le nom que vous voulez lui attribuer de cette façon :

```
<Nom de la machine>
```

3. Pour mettre à jour ces paramètres vous pouvez redémarrer votre machine avec la commande :

```
reboot
```

1.3 SSH

1.3.1 Création d’un utilisateur

1. La commande pour créer l’utilisateur “admin” est celle si :

```
adduser admin
```

2. Suite à cette commande vous devriez rentrer certaine information que vous pouvez laisser vide de cette façon juste lors du mot du passe vous vous devez d’en renseigner 1 :

```
root@nextcloud:~# adduser admin
Ajout de l'utilisateur « admin » ...
Ajout du nouveau groupe « admin » (1001) ...
Ajout du nouvel utilisateur « admin » (1001) avec le groupe
« admin » (1001) ...
Création du répertoire personnel « /home/admin » ...
Copie des fichiers depuis « /etc/skel » ...
Nouveau mot de passe :
Retapez le nouveau mot de passe :
passwd : mot de passe mis à jour avec succès
Modifier les informations associées à un utilisateur pour a
dmin
Entrer la nouvelle valeur, ou appuyer sur ENTER pour la val
eur par défaut
        NOM []:
        Numéro de chambre []:
        Téléphone professionnel []:
        Téléphone personnel []:
        Autre []:
Cette information est-elle correcte ? [O/n]o
Ajout du nouvel utilisateur « admin » aux groupes supplémen
taires « users » ...
Ajout de l'utilisateur « admin » au groupe « users » ...
```

1.3.2 Installation / Configuration SSH

1. Nous allons commencer par installer le module SSH sur notre machine Linux à l'aide de cette commande :

```
apt update && apt upgrade && apt install ssh
```

2. Maintenant nous pouvons configurer le port par défaut du SSH pour cela nous pouvons aller modifier le fichier :

```
nano /etc/ssh/sshd_config
```

3. Vous pouvez modifier cette dans le fichier de cette façon :

```
#Port 22 -> Port <Port SSH>
```

4. Pour mettre à jour ces paramètres vous pouvez redémarrer le service SSH, voici la commande :

```
systemctl restart ssh
```

2. Configuration de FOG

2.1 Installation FOG

1. Dans en premier donc nous allons commencer par l'installation de FOG sur le serveur, pour cela nous allons commencer par installer le composant qui nous permettra de récupérer les fichiers d'installation nommé "git", voici la commande pour cela :

```
apt install git
```

2. Suite à l'installation du composant git sur le serveur FOG nous pouvons passer au téléchargement de l'archive de FOG à l'aide de cette commande :

```
git clone https://github.com/FOGProject/fogproject.git
```

3. Suite à cela nous allons configurer la branche que nous voulons utiliser lors de l'installation, dans notre cas nous allons utiliser la branche "normal", voici les commandes pour cela :

```
cd /root/fogproject
git fetch --all
git checkout stable
git pull
```

4. Suite à la sélection de la branche principal nous pouvons passer à l'installation de l'outil FOG sur le serveur, pour cela vous pouvez effectuer ces commandes :

```
cd /root/fogproject/bin
./installfog.sh
```

2.2 Remplacement des certificats

2.2.1 Création CSR

1. Suite à l'installation de FOG nous avons donc des certificats auto-signé donc nous allons pouvoir changer ça par des certificats signer par notre autorité de certification, donc dans un premier temps nous allons créer notre demande de signature à l'aide de ces commandes :

```
mkdir -p /etc/ssl/csr
openssl genrsa -out /etc/ssl/private/prv-fog.key 2048
openssl req -new -key /etc/ssl/private/prv-fog.key -out /et
c/ssl/csr/csr-fog.csr
```

2. Suite à la création des certificats nous pouvons passer au transfert de notre fichier CSR sur le serveur PKI à l'aide d'une commande de transfert de fichier, voici celle que nous pouvons utiliser

```
scp -P <Port SSH serveur PKI> /etc/ssl/csr/csr-fog.csr shar
e@<Adresse IP serveur PKI>:/tmp/
```

2.2.2 Signature du certification / Récupération du certificat de l'autorité de certification

1. Suite au transfert du fichier CSR sur votre serveur PKI vous pouvez vous rendre sur celui si et vous rendre dans voter dossier d'administration de EASY-RSA (dans mon cas mon dossier d'administration est nommé "easyrsa"), vous pouvez donc effectuer ces commandes :

```
cd /root/easyrsa
./easyrsa import-req /tmp/csr-fog.csr crt-fog
./easyrsa --days=365 --subject-alt-name="IP:<Adresse IP de
voter serveur FOG>" sign-req server crt-fog
```

2. Nous pouvons donc passer au transfert des fichiers de certificat FOG et le certificat de l'autorité de certification sur notre serveur FOG à l'aide de ces commandes :

```
scp -P <Port SSH serveur FOG> /root/easyrsa/pki/issued/crt-
fog.crt adminlocal@<Adresse IP serveur FOG>:/tmp/
scp -P <Port SSH serveur FOG> /root/easyrsa/pki/ca.crt admi
nlocal@<Adresse IP serveur FOG>:/tmp/
```

2.2.3 Modification des certificats sur le serveur FOG

1. Suite à la signature du certificat et au transfert des fichiers de certificats sur le serveur FOG nous pouvons passer à l'administration des certificats sur le serveur FOG, dans un premier nous allons déplacer les 2 certificats à leur emplacement prédéfini à l'aide de ces commandes :

```
mv /tmp/crt-fog.crt /etc/ssl/certs/crt-fog.crt
mv /tmp/ca.crt /usr/local/share/ca-certificates/ca.crt
```

2. Dès maintenant nous pouvons passer à la mise à jour des certificats sur la machine à l'aide de la commande si dessous :

```
update-ca-certificates
```

3. Suite à ça nous pouvons passer au changement des certificats dans notre de configuration apache2, vous pouvez vous rendre dans le fichier nommé "001-fog.conf" et modifier les lignes :
    - SSLCertificateFile
    - SSLCertificateKeyFile
    - SSLCACertificateFile

Vous pouvez modifier ces lignes par ceci :

```
SSLCertificateFile /etc/ssl/certs/crt-fog.crt
SSLCertificateKeyFile /etc/ssl/private/prv-fog.key
SSLCACertificateFile /usr/local/share/ca-certificates/c
a.crt
```

4. Nous pouvons ensuite passer à l'administration des fichiers TFTP de FOG pour cela nous allons regénérer les fichiers TFTP les déplacés et y affecter les bons droits pour la bon fonctionnement de FOG :

```
mv /tftpboot /tftpboot.bak
mkdir -p /tftpboot
cp /tftpboot.bak/default.ipxe /tftpboot/
cd /root/fogproject/utils/FOGiPXE/
./buildipxe.sh /usr/local/share/ca-certificates/ca.crt
cp -r ../../packages/tftp/* /tftpboot
chown -R fogproject:www-data /tftpboot
```

Ne pas interrompre la génération des fichiers TFTP car cela peut prendre tour de même un petit moment mais en aucun il faut le stopper pour éviter toutes erreurs ensuite.

2.3 Configuration LDAPS

2.3.1 Administration CLI Debian

1. Maintenant nous pouvons passer à la configuration du LDAPS sur notre serveur FOG dans un premier nous pouvons configurer le fichier de configuration du ldap à l'aide de ces commandes :

```
echo "TLS_CACERT /etc/ssl/certs/ca-certificates.crt" >>
/etc/ldap/ldap.conf
echo "TLS_REQCERT demand" >> /etc/ldap/ldap.conf
```

2. Suite à ça nous allons redémarrer le service WEB pour la prise en compte des modifications, voici la commande permettant cela :

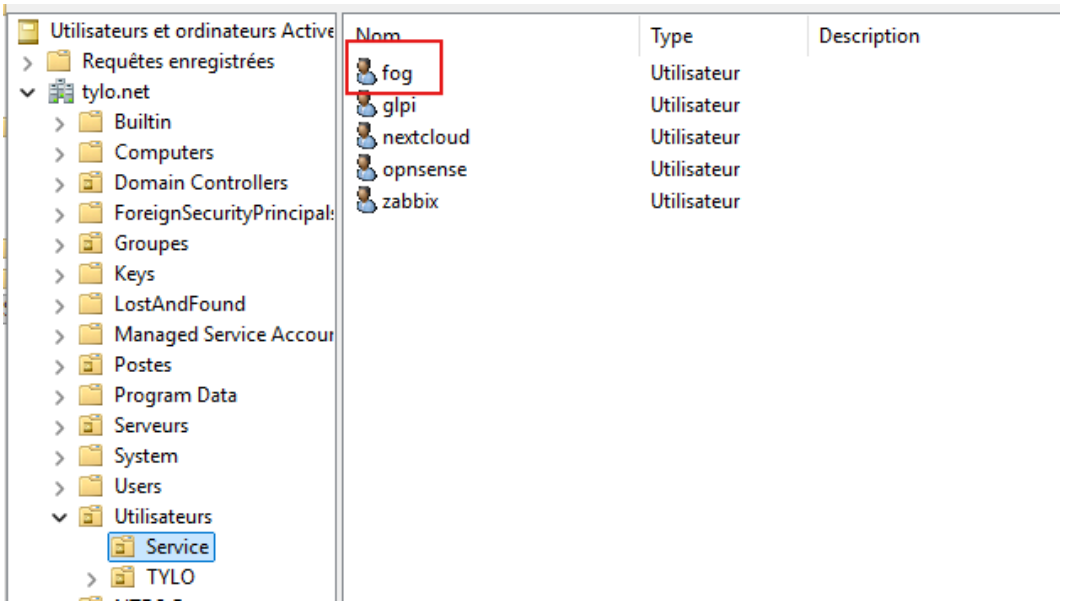
```
systemctl restart apache2
```

Cela va permettre de rajouter ces deux au lignes à la fin fichier nommé “ldap.conf” ces deux lignes vont permettre d’aller chercher le certificat du LDAPS de notre serveur Active Directory et de filtrer le passage juste avec le certificat.

2.3.2 Administration AD

1. Suite au paramétrage du LDAP sur le serveur LDAP nous allons créer les groupes et l’utilisateur de service qui vont être utilisée pour le LDAPS, vous pouvez donc vous rendre dans l’application nommé “Utilisateurs et ordinateurs Active Directory”

2. Suite à ça nous allons commencer par la création de l’utilisateur de service nommé “fog”, dans mon cas cette utilisateur va être unité d’organisation à part qui contient tous les comptes de service de cette façon :



Il ne faut pas oublier de bien enregistrer le mot de passe de l’utilisateur de service pour la réutilisation de celui si dans les prochaines étapes.

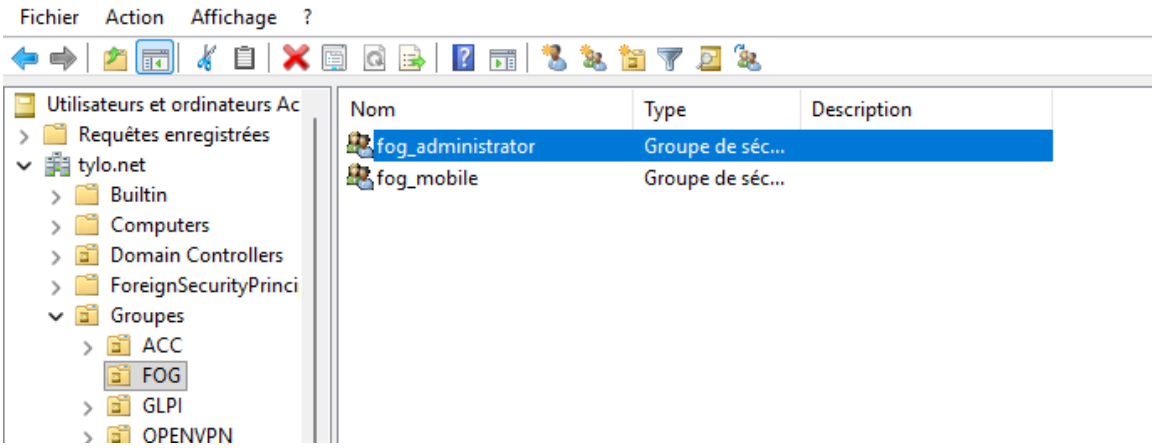
3. Suite à la création de l’utilisateur nous allons passer à la création des groupes Active Directory de filtrage donc dans mon cas je créer mes

groupes dans une unité d'organisation à part.

Donc nous allons créer deux groupes :

- fog_administrator
- fog_mobile

Voici donc l'arborescence des groupes suite à la création de ceux si :



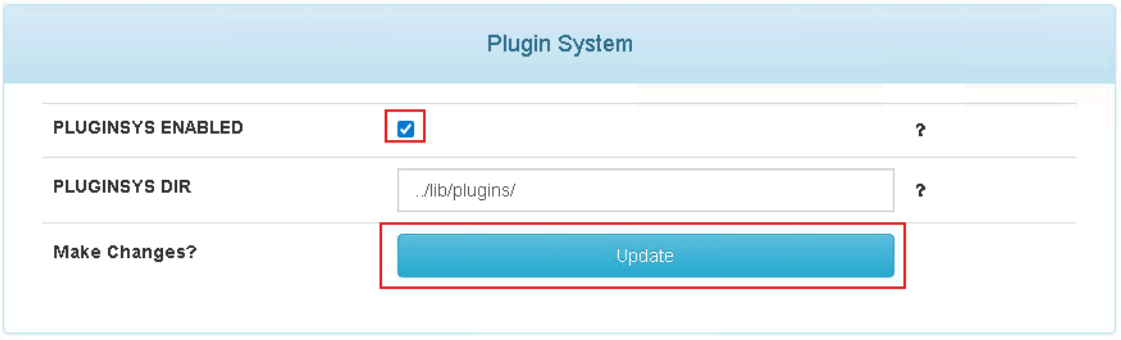
2.3.3 Administration WEB

1. Ensuite vous pouvez vous rendre sur l'interface WEB de votre serveur FOG et vous y connecter avec les identifiants :

   - Identifiant : fog
   - Mot de Passe : password

   Ensuite vous pouvez vous rendre dans les onglets : FOG Configuration > FOG Settings > Plugin System

   Ensuite vous pouvez activer ce service dans FOG et cliquer sur "Update" de cette façon :

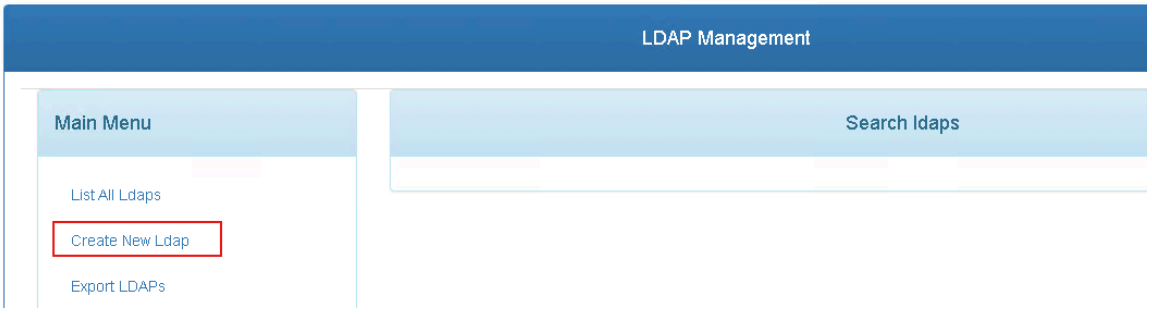


2. Ensuite vous pouvez vous rendre dans l'onglet "Plugins" suite à l'activation du menu "Plugin System"

   Vous pouvez rechercher dans le menu Description "LDAP" ceci va donc va vous ressortir un plugin et vous pouvez cliquer sur le nom du plugin de cette façon :

   Suite à ça vous pouvez retrouver le plugin LDAP dans le menu "Install Plugin", après être aller dans ce menu vous pouvez recliquer sur le nom du plugin et ensuite vous descendre et cliquer sur "Install" de cette façon :

3. Suite à l'installation du plugin LDAP vous pouvez vous rendre dans le nouveau menu nommé "LDAP Servers" et ensuite aller dans le menu "Create New Ldap" pour commencer la création de notre lien LDAPS entre notre serveur FOG et notre serveur.

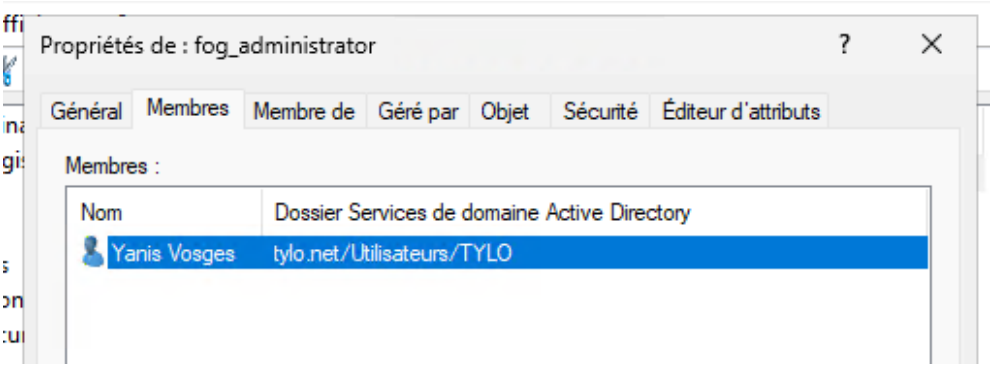


4. Voici les informations que vous pouvez rentrer dans formulaire de création du LDAP :
    - LDAP Connection Name : LDAPS01
    - LDAP Server Address : ldaps://<Nom DNS AD COMPLET>
    - LDAP Server Port : 636
    - Use Group Matching (Recommanded) : Check
    - Enable Nested Group Matching (Active Directory only) : Uncheck
    - Search Base DN : Ceci correspond au DN de l'utilité d'organisation qui contient les utilisateurs de l'Active Directory (exemple : ou=tylo,ou=utilisateurs,dc=tylo,dc=net)
    - Group Search DN : Ceci correspond au DN de l'utilité d'organisation qui contient les groupes Active Directory de filtrage (exemple : ou=fog,ou=groupes,dc=tylo,dc=net)
    - Admin Group : fog_administrator
    - Mobile Group : fog_mobile
    - Initial Template : Microsoft AD
    - User Name Attribute : samAccountName
    - Group Member Attribute : member
    - Search Scope : Subtree Only
    - Bind DN : Ceci correspond au DN de notre utilisateur de service
    - Bind Password : Ceci correspond au mot de passe de l'utilisateur "fog" préalablement enregistrée

    Après avoir compléter tout le formulaire vous pouvez finir par cliquer sur "Create" pour valider la création de votre entrer LDAPS.

2.3.4 Test LDAPS

1. Suite à toute l'administration du LDAPS nous pouvons donc passer au test de connexion avec un compte Active Directory, donc dans un premier temps si ce n'est pas déjà fait nous allons ajouter un utilisateur au groupe fog_administrator dans notre Active Directory.



2. Suite à ça vous pouvez tester de vous connecter à l'aide du compte utilisateur et de son mot de passe d'ouverture de session sur l'interface WEB du notre serveur FOG, de cette façon :

Vous pouvez finir par cliquer sur "Login".

2.4 Configuration DHCP

2.4.1 Configuration

Lorsque que nous utilisons un serveur FOG pour permettre l'accès au serveur lorsque nous utilisons le PXE Boot dans le Boot Manager nous devons configurer deux options (66 et 67) dans notre serveur DHCP, les voici :

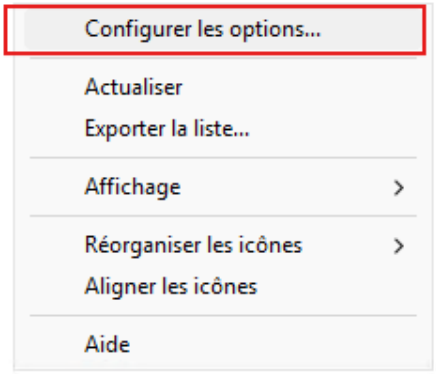
- 66 : Nom d'hôte du serveur de démarrage
- 67 : Nom du fichier de démarrage

Voici comment vous pouvez le configurer :

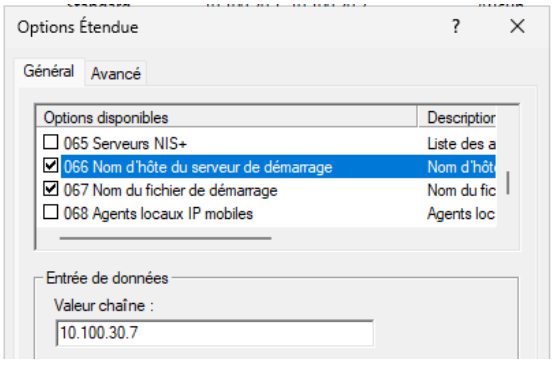
1. Vous pouvez commencer par vous rendre dans l'application DHCP sur votre serveur ou ce service est installé.

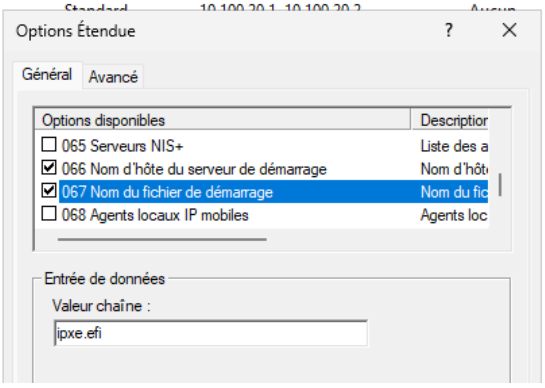
   Vous pouvez ensuite vous rendre dans les menus suivant : <Nom Serveur> > IPv4 > Etendue > Options d'étendue

   Ensuite vous pouvez faire un clique droit sur partie vide de la page et cliquer sur "Configurer les options..." de cette façon :



2. Ensuite vous pouvez descendre jusqu'au options 66 et 67, vous pouvez ensuite cocher les deux cases des 2 options pour permettre leurs activations, voici ce que vous rentrer dans chacune des options :
   - 66 : Adresse IP / Nom DNS de votre serveur FOG
   - 67 : ipxe.efi (fichier tftp du serveur fog)





Vous pouvez finir par cliquer sur "OK"

2.4.2 Test de Boot

1. Vous pouvez vous rendre sur votre poste client qui reçoit son adresse IP par DHCP et ouvrir l'application "Invites de commande" en tant qu'administrateur.

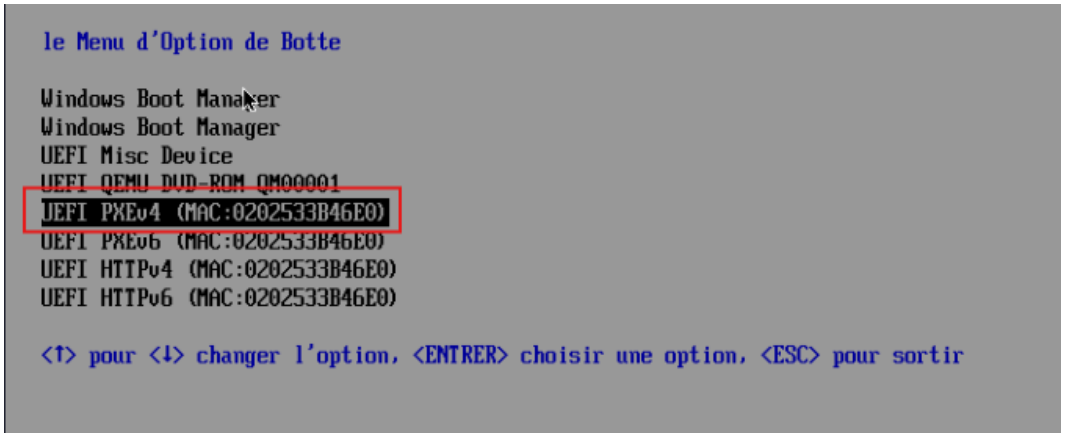
Vous pouvez éxecuter les commandes suivante dans l'invite de commande pour la mise à jour du poste client avec DHCP

```
ipconfig /release
ipconfig /renew
```

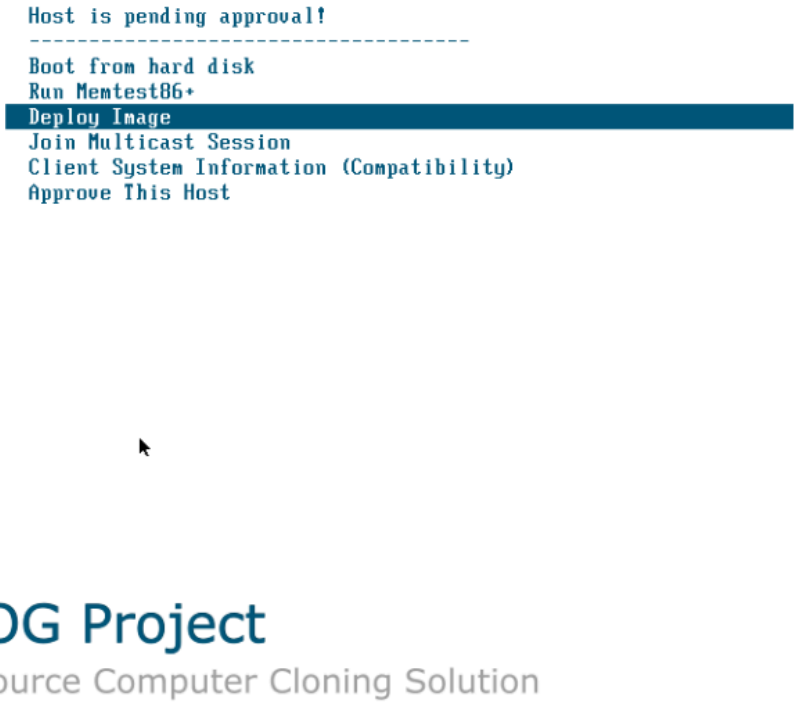
2. Après avoir exécuter ces deux commandes vous pouvez redémarrer votre poste et tenter de boot l'espace de boot manager voici souvent les touches qui sont utilisée pour l'accès au Boot Manager :

   - Echap
   - F10
   - F12

   Après avoir boot dans le Boot Manager vous pouvez boot sur le UEFI PXEv4, pour cela vous pouvez vous placer sur le UEFI PXEv4 et cliquer sur Entrer



   Suite à un petit temps de chargement vous devriez voir afficher la page d'accueil de boot de FOG sur le poste de cette façon :



Ceci veut donc dire que la partie de boot pour FOG Project fonctionne bien en HTTPS avec la configuration de certificat que nous avons effectuer au part avant.