Documentation d'installation

Reset mot de passe ou utilisateurs contrôleur de domaine

Windows 10

18/03/2018

Yohan Fresneau

Sommaire

1. Dans quel cas Réinitialisation le mot de passe

Il y a différentes situations qui nous force à réinitialiser notre mot de passe, comme par exemples ces situations :

- ➔ Perte du mot de passe ou de l'identifiant administrateur
- ➔ Pirate du compte
- ➔ Changement du mot de passe par accident
- ➔ Pour une blague (qui ne ferra rire que vous)
- ➔ Possibilité de rentrer en administrateur sur une machine (illégale si elle ne vous appartient pas)
- ➔ Toutes les situations possibles

Nous allons voir maintenant comment le faire

2. Comment procéder

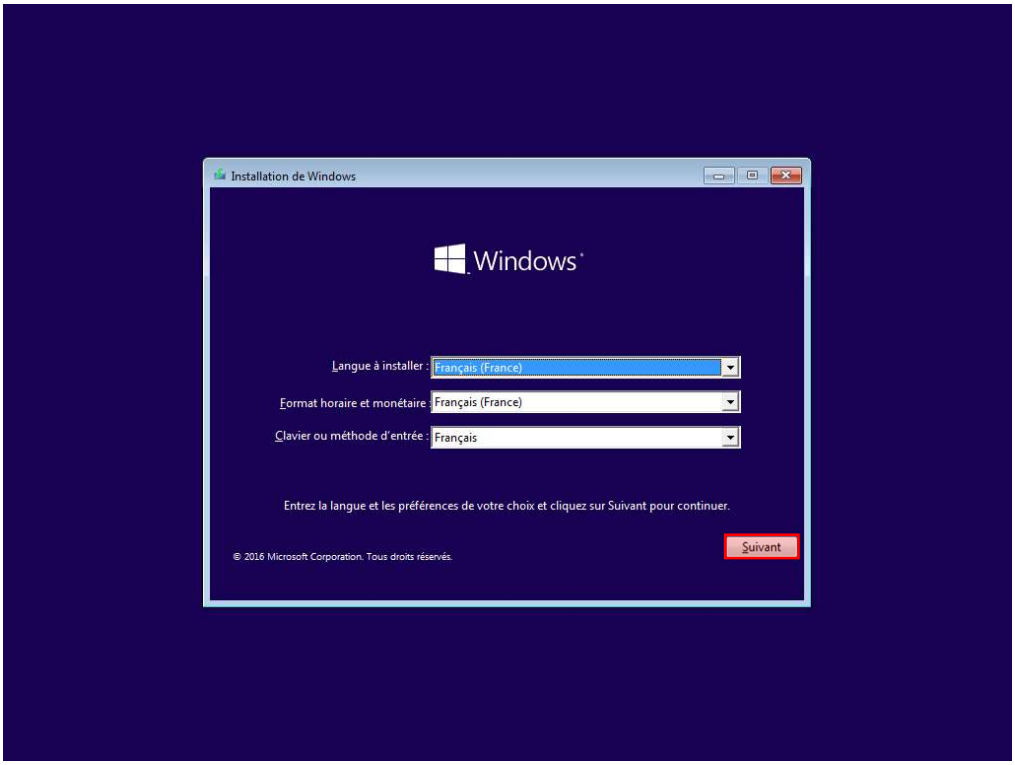
Pour faire cette manipe, nous allons devoir prendre un CD ou une clé d'installation Windows serveur ou une installation de Windows 8, 10 ou serveur 2012, 2016.

Cette faille va exploiter les outils d'ergonomie, qui se trouve au moment de saisir le mot de passe de Windows.

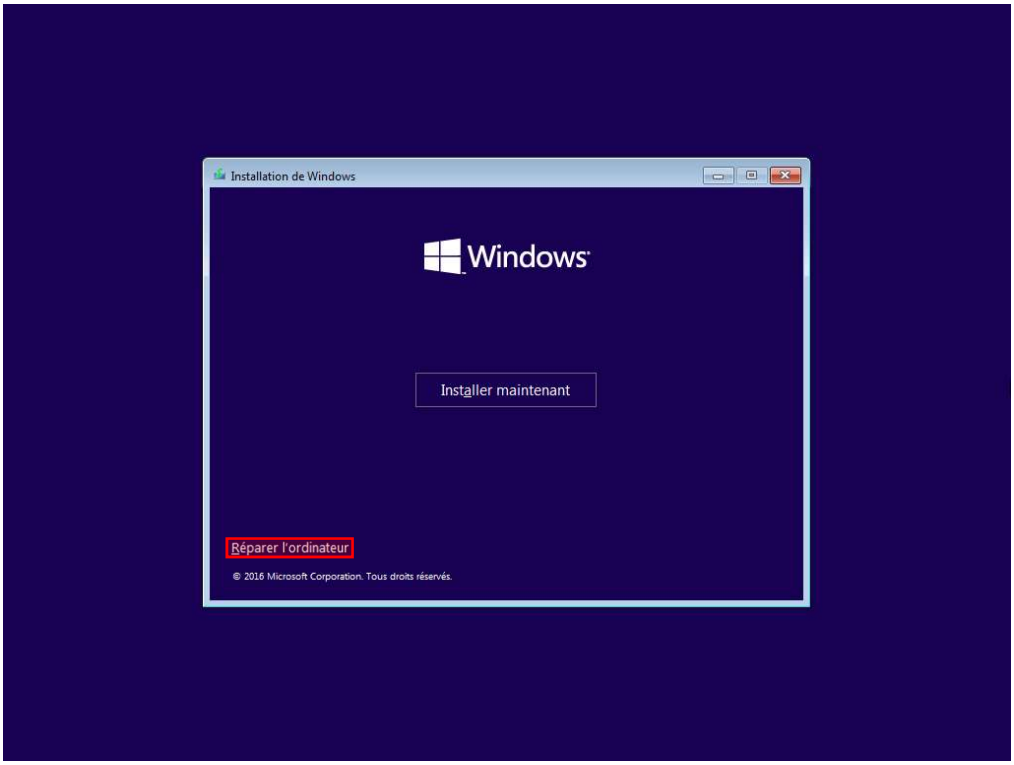
Le but de cette manipe est de cliquer sur la loupe et avoir un invité de commande en administrateur et changer le mot de passe Windows.

3. Mise en place de la faille

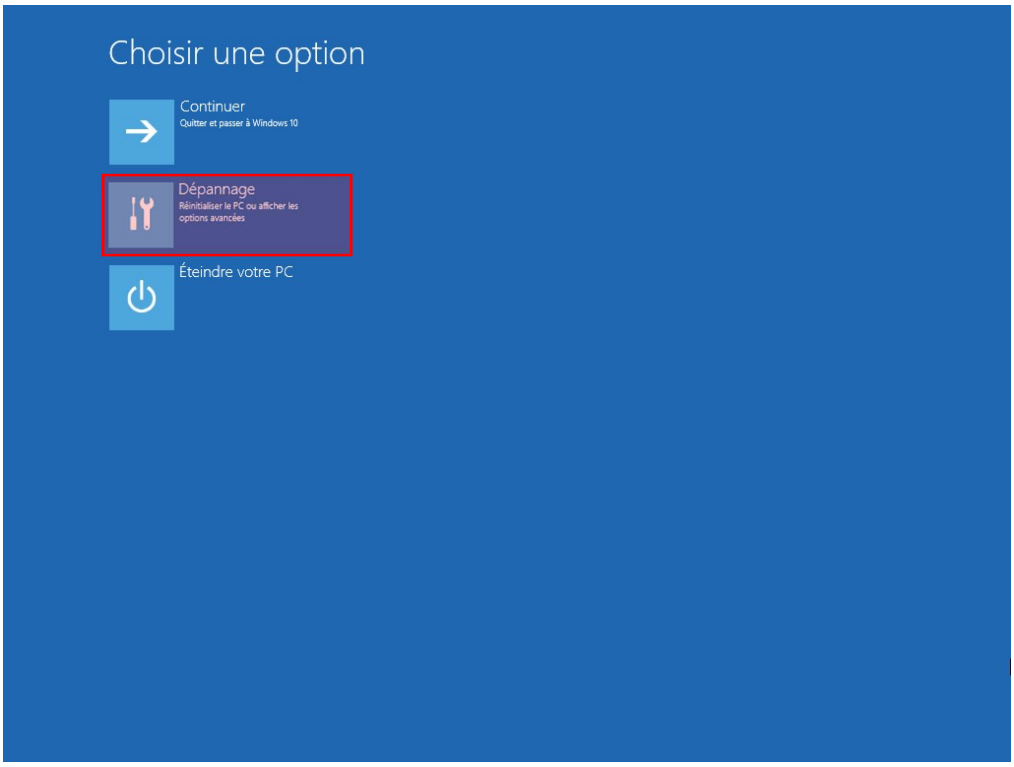
Pour mettre en place ceci, nous allons avoir besoin de démarrer sur la clé USB d'installation.



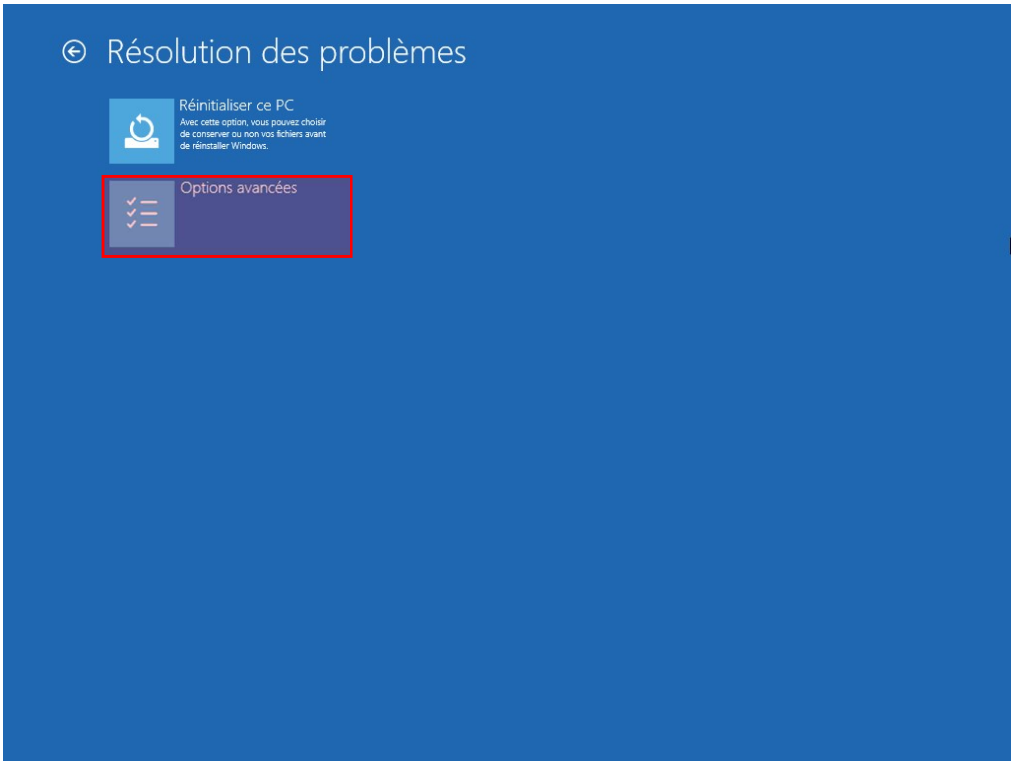
*Cliquez sur "**suivant**" pour continuer*



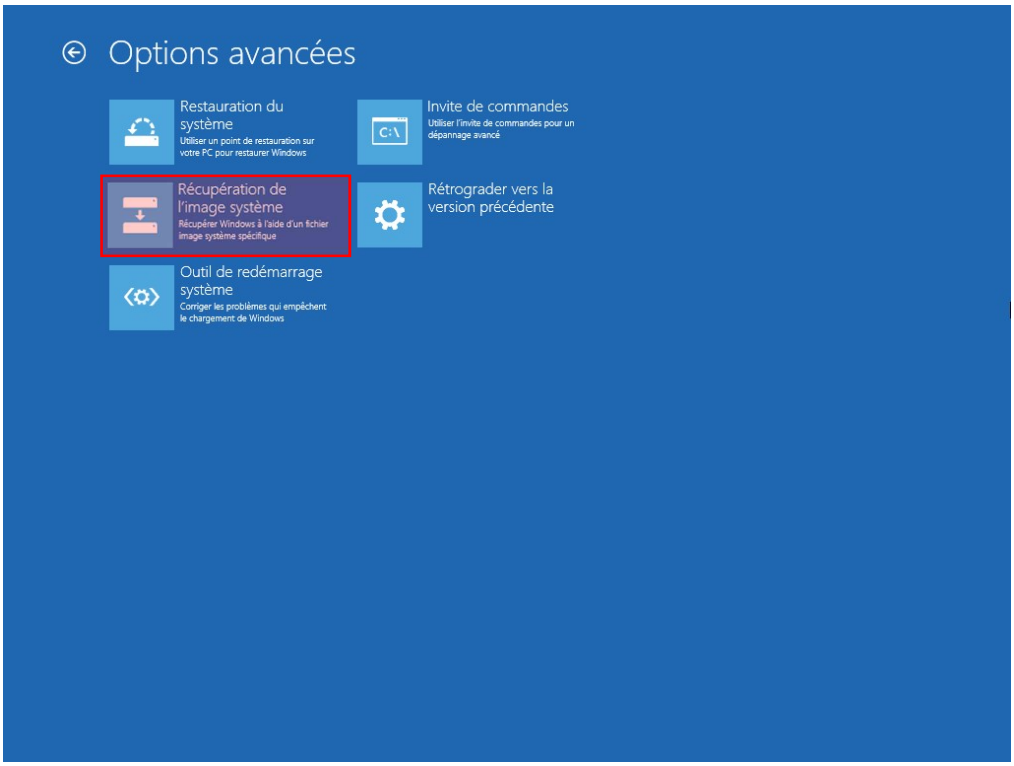
*Choisir "**Réparer l'ordinateur**"*



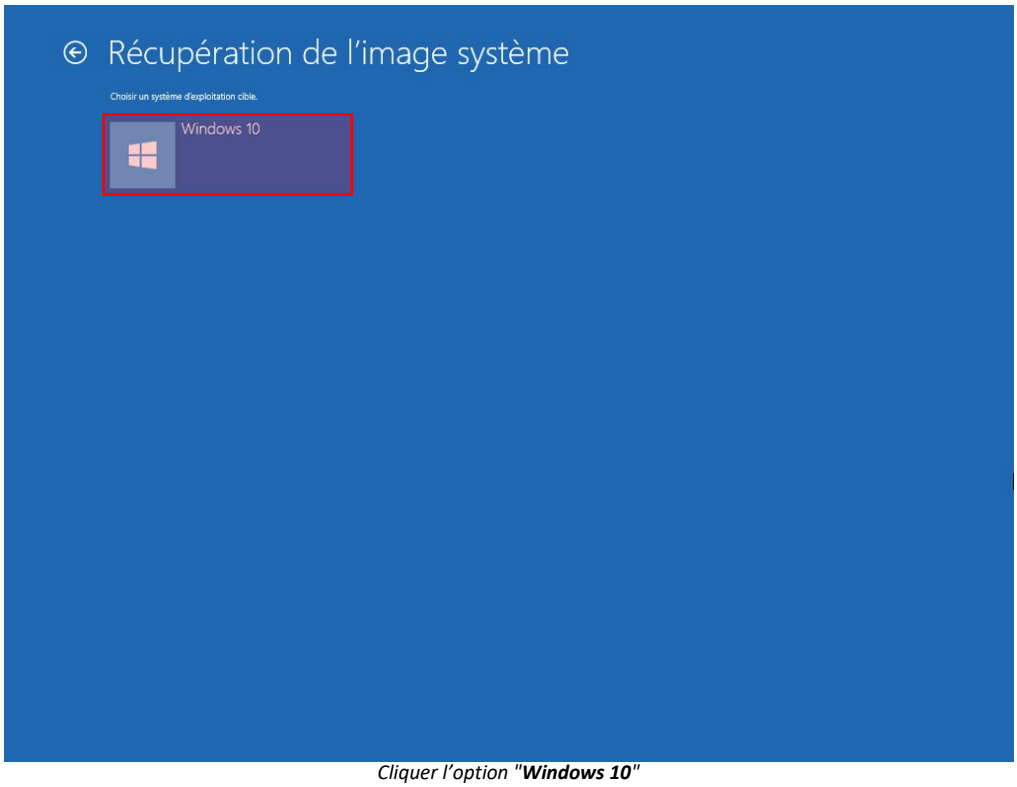
*Sélectionner l'option "**Dépannage**"*



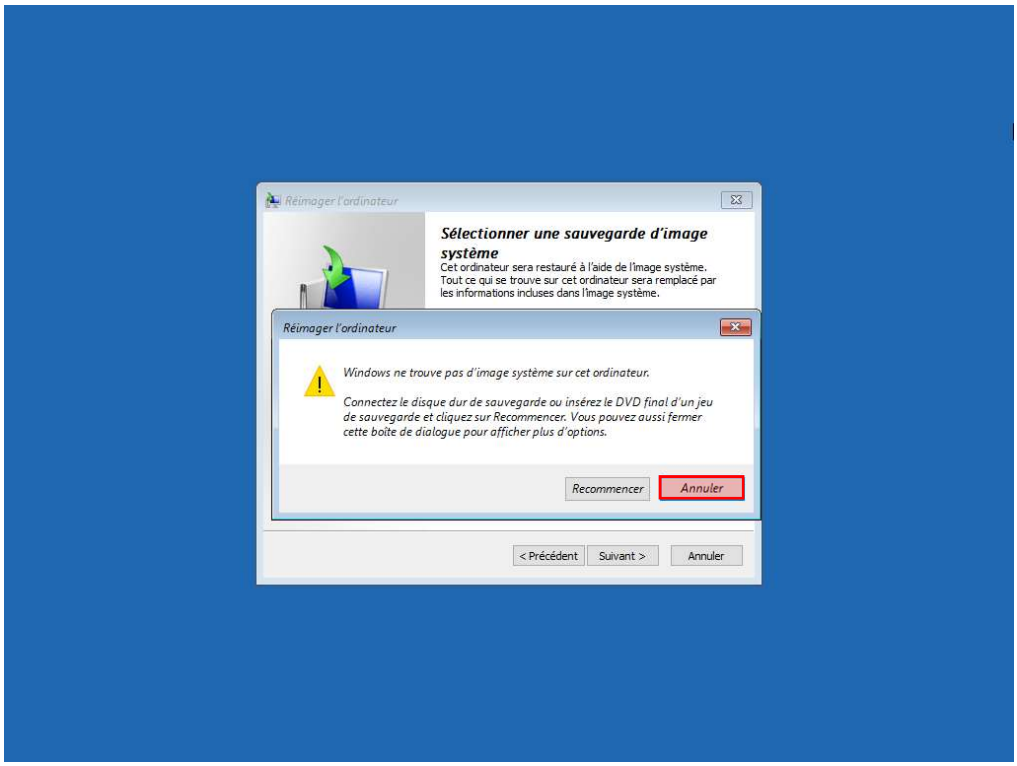
*Choisir l'option "**Réinitialiser ce PC**"*



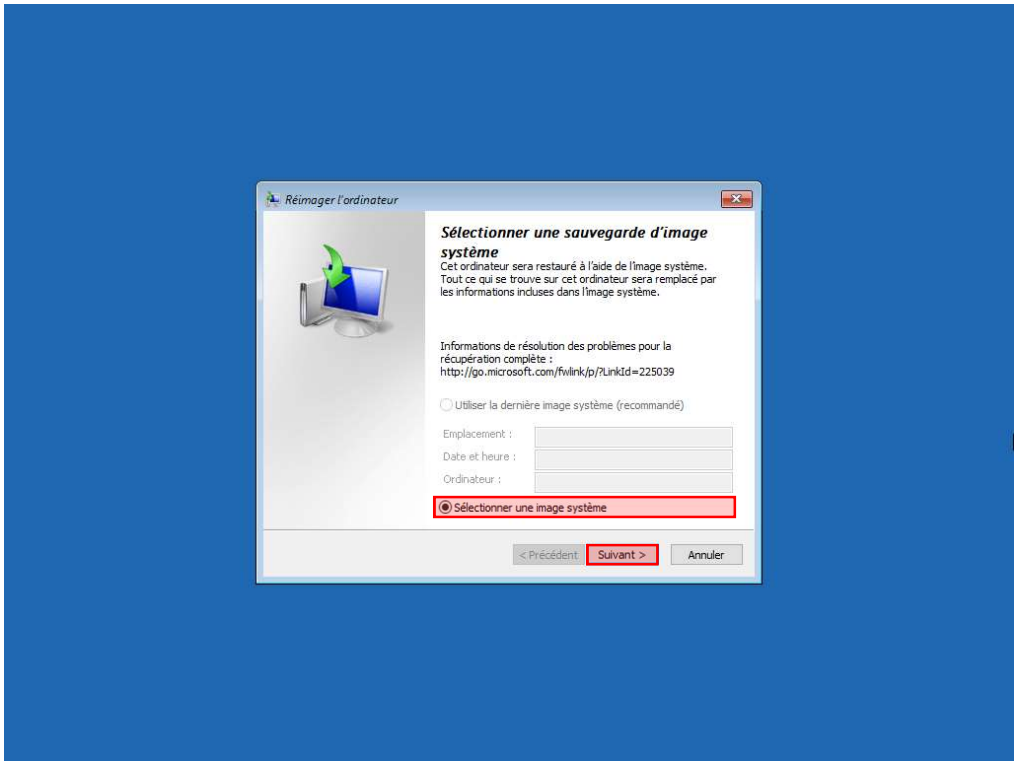
*Cliquer l'option "**Récupération du l'image système**"*



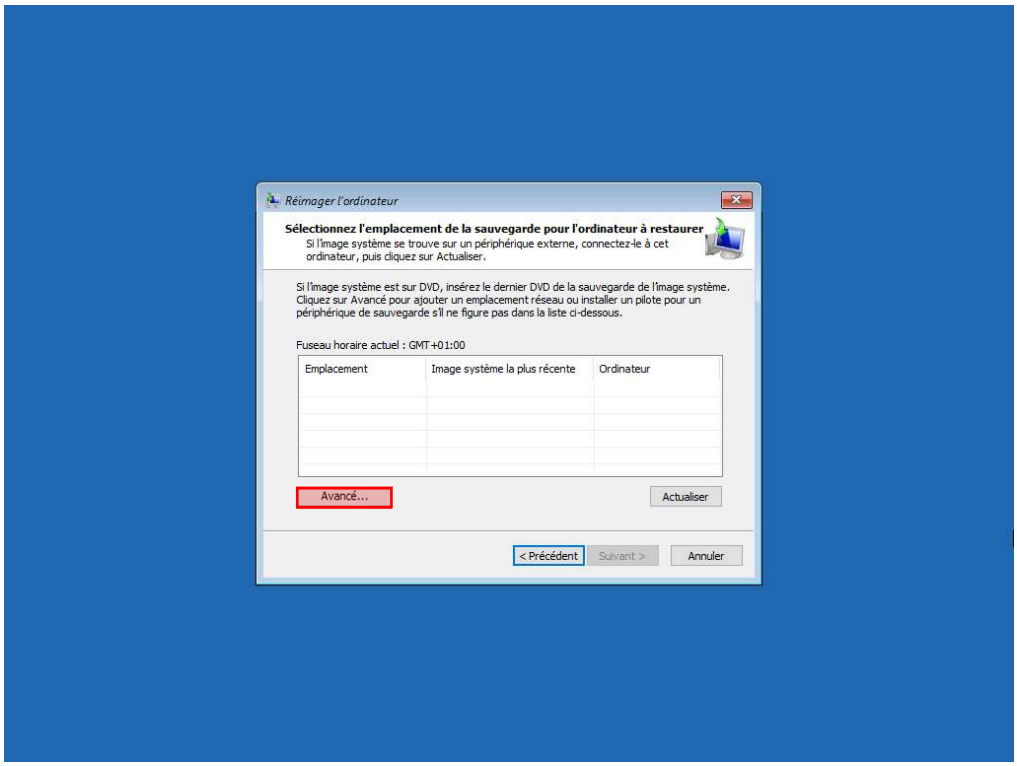
*Cliquer l'option "**Windows 10**"*



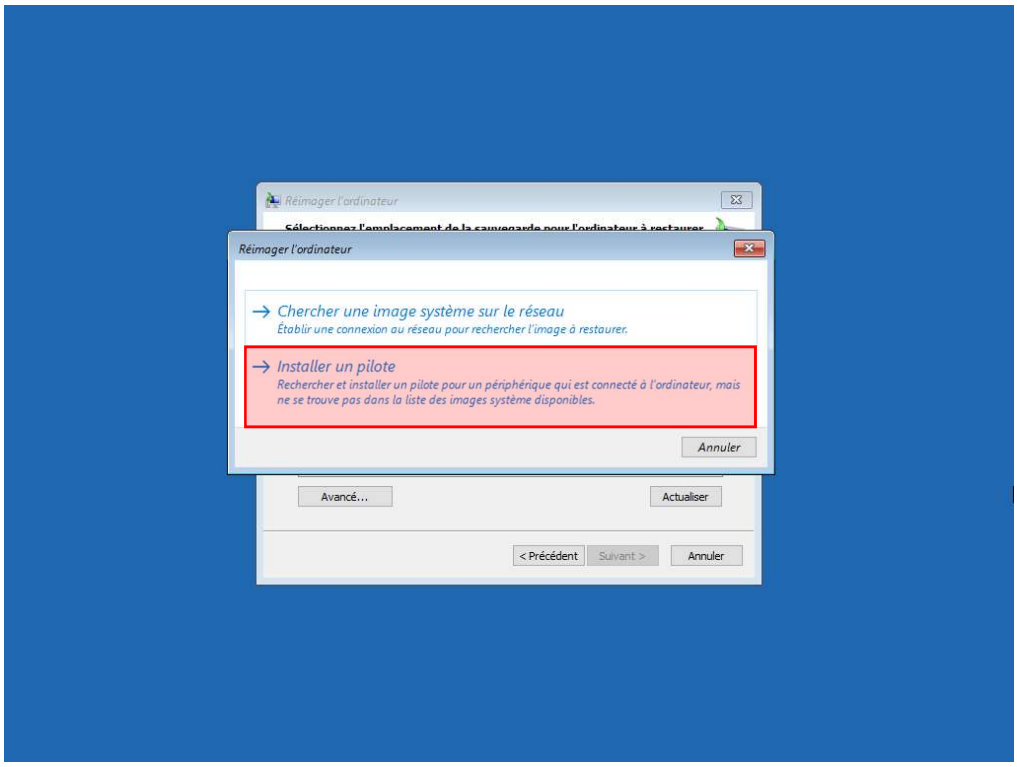
*Il ne trouve pas d'image, on va donc fait "**annuler**"*



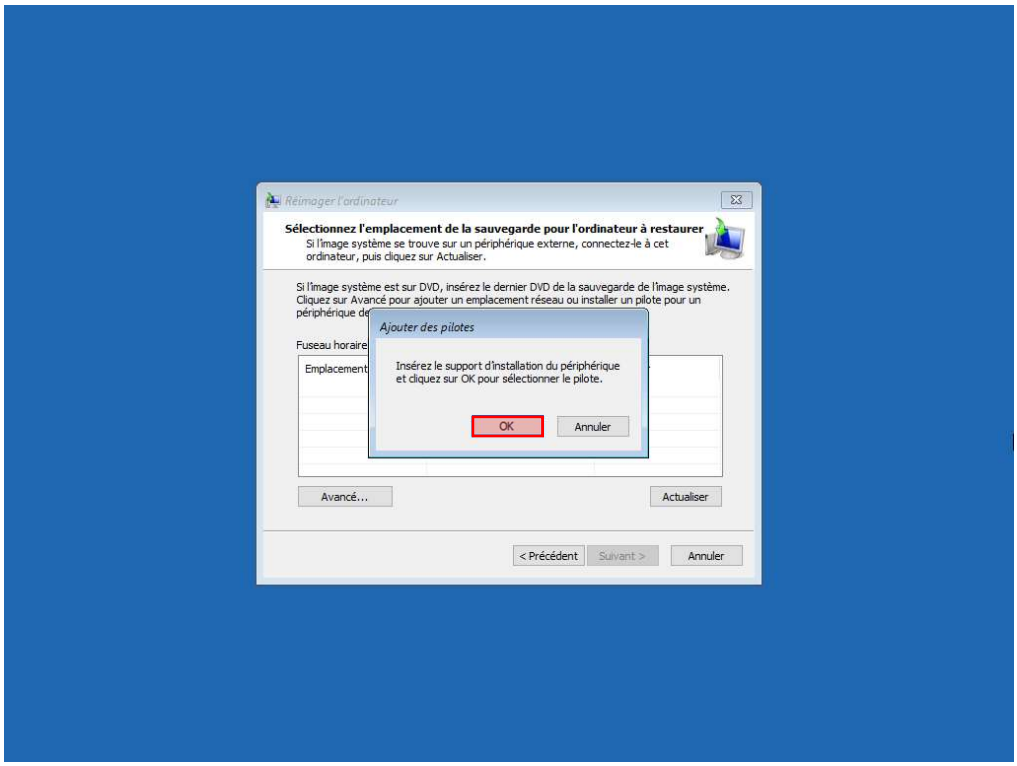
*On va donc spécifier "**Sélectionner une image système**", puis "**suivant**"*



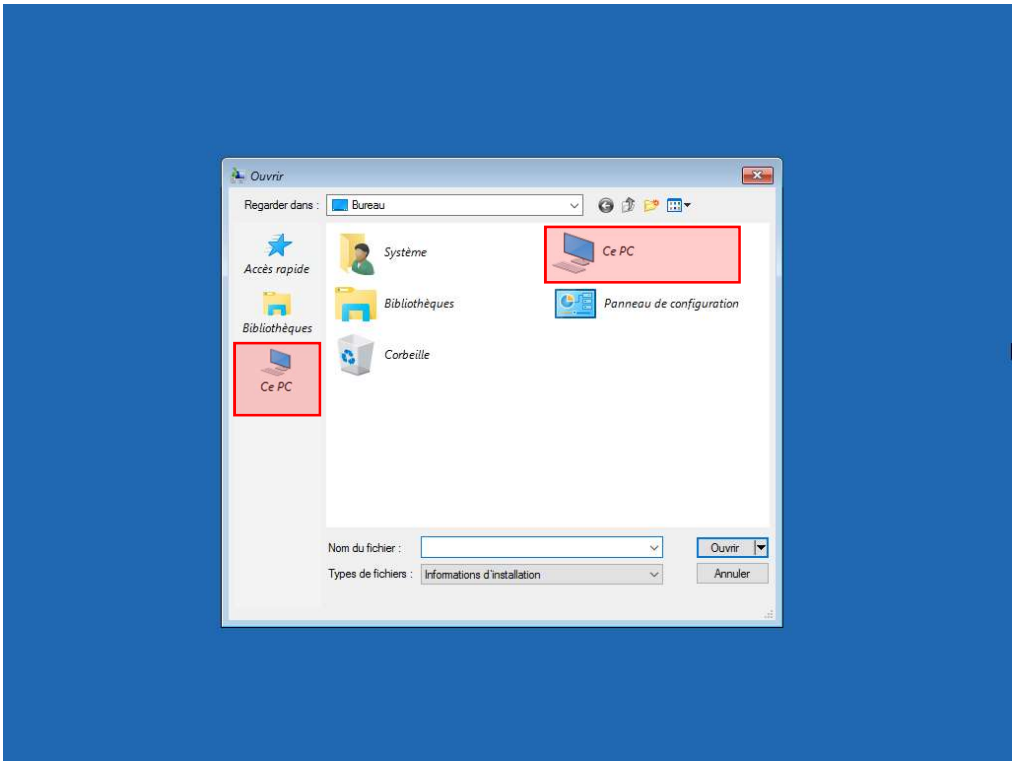
*Cliquez sur "**avancer**", ce qui permet normalement de sélectionner notre image.*



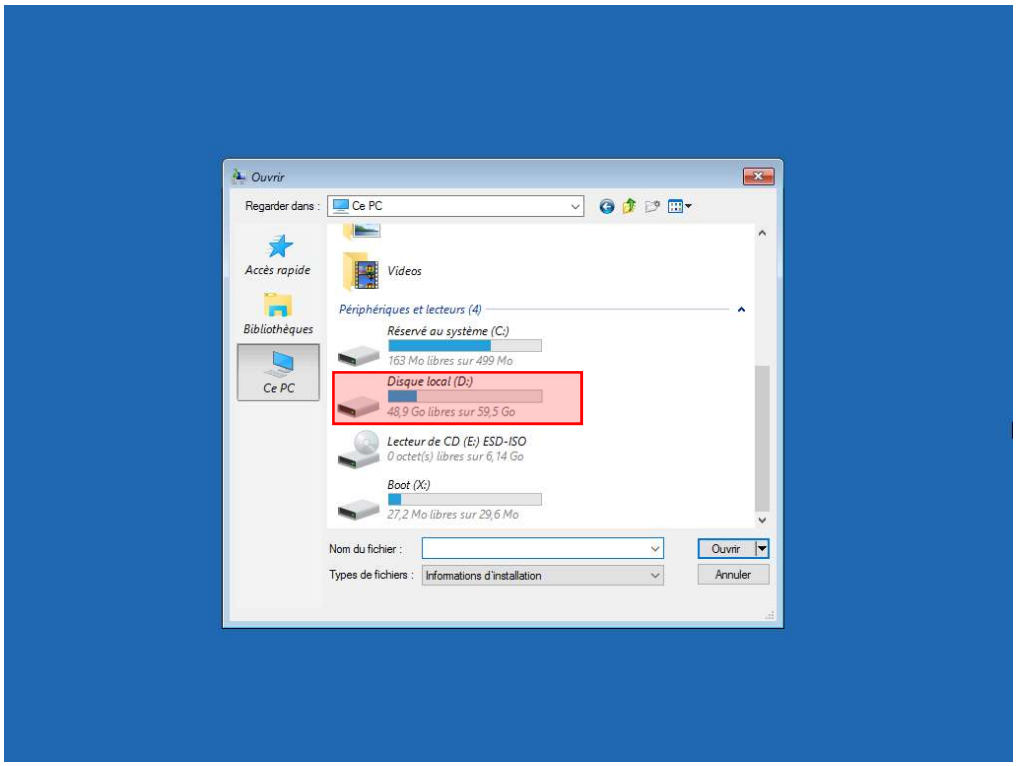
*Sélectionner "**Installer un pilote**"*



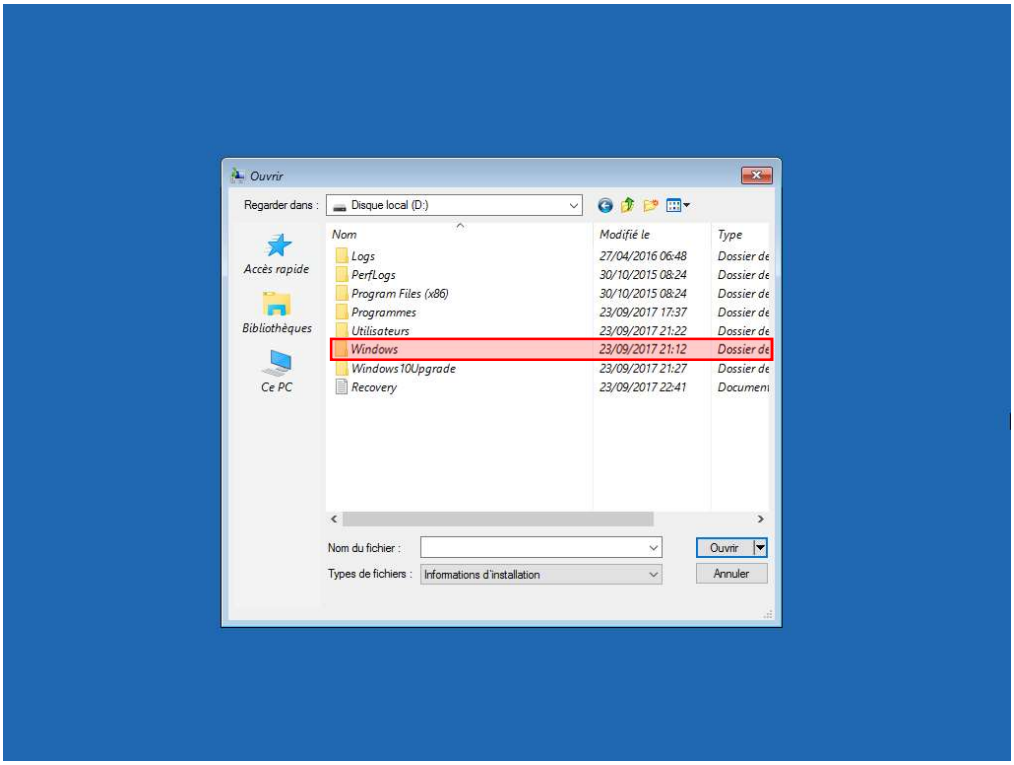
*Cliquez sur "**OK**", pour ouvrir le gestionnaire de fichiers*



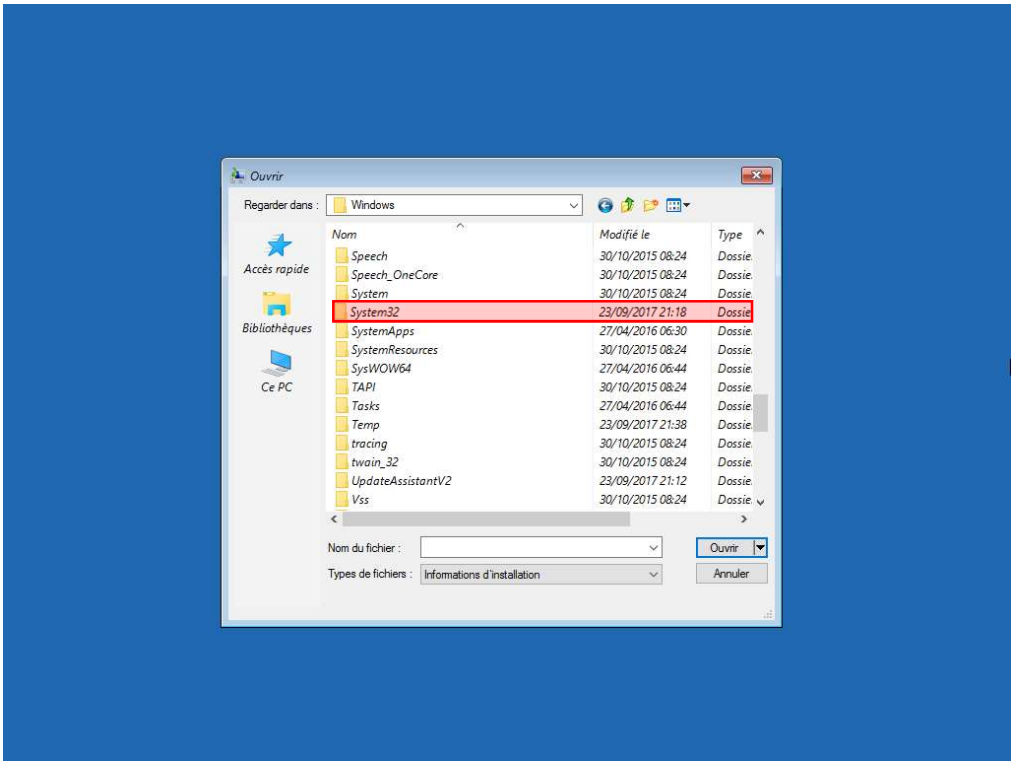
*Nous avons donc le gestionnaire de fichiers qui s'ouvre, nous allons dans "**Ce PC**"*



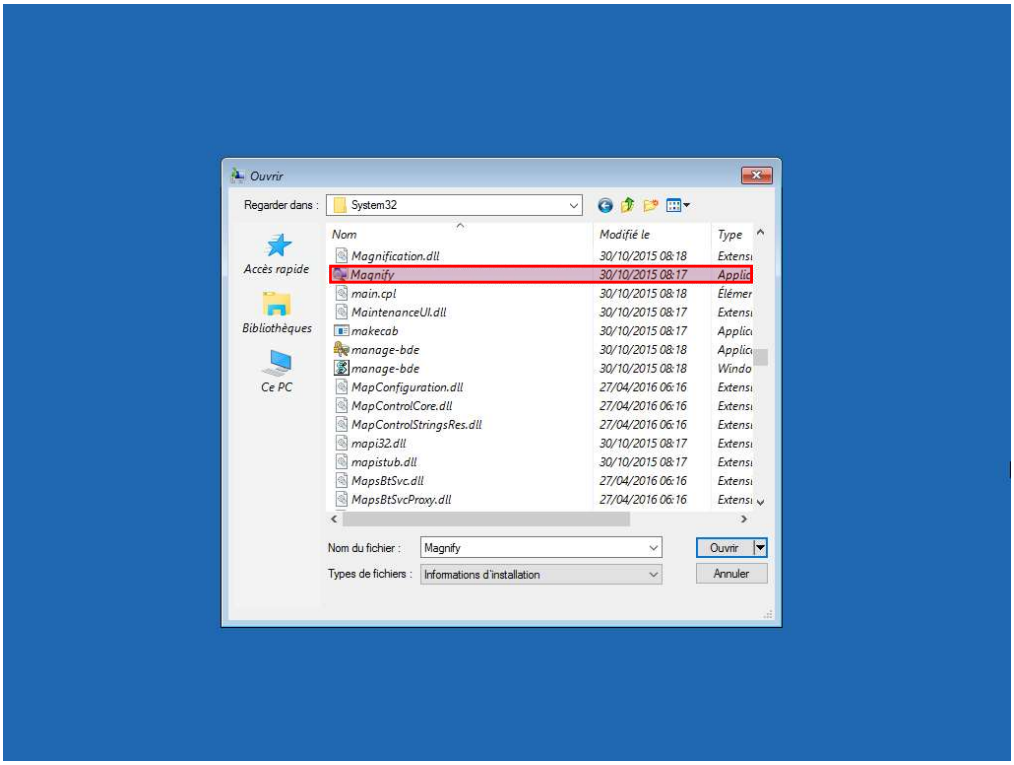
*Nous avons donc bien nos disques, dont le Disque "**D:**" qui en réalité est le disque "**C:**" système*



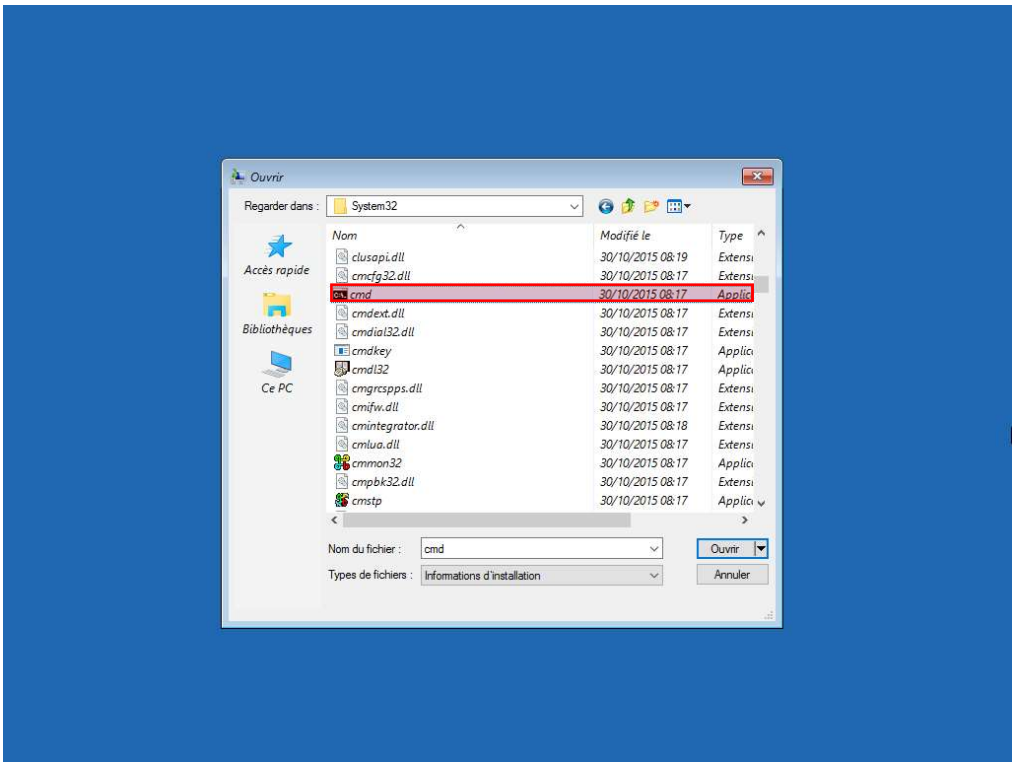
*Nous allons ensuite dans "**Windows**"*



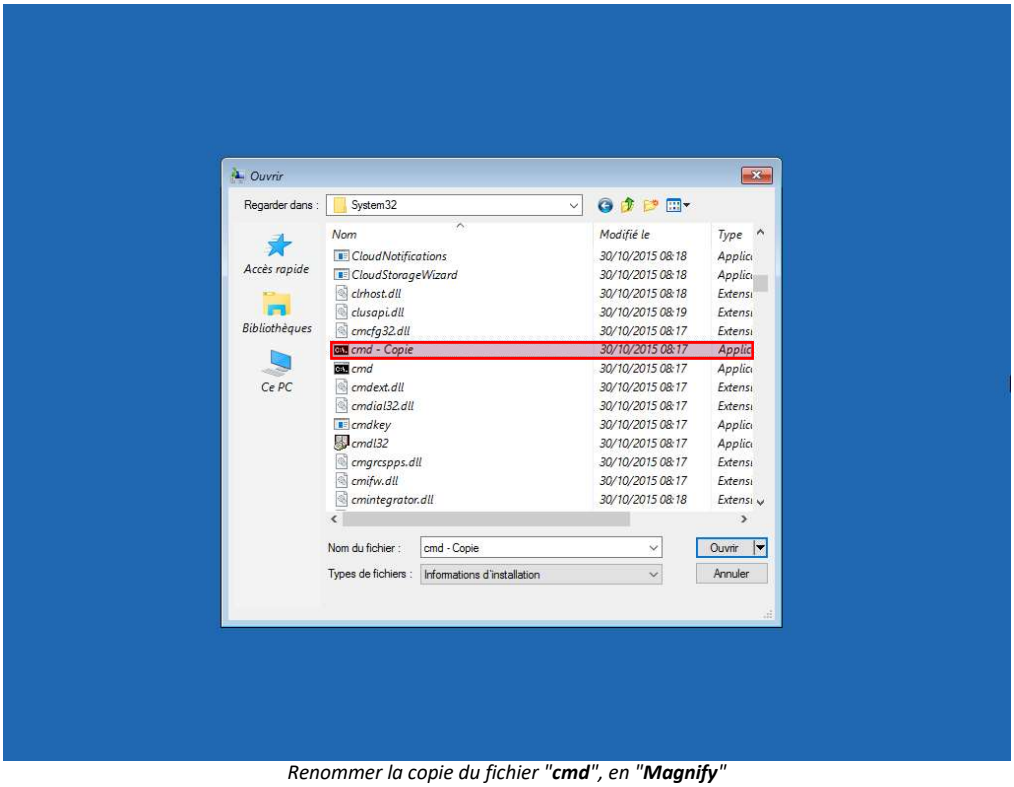
*Nous allons ensuite dans "**System32**"*



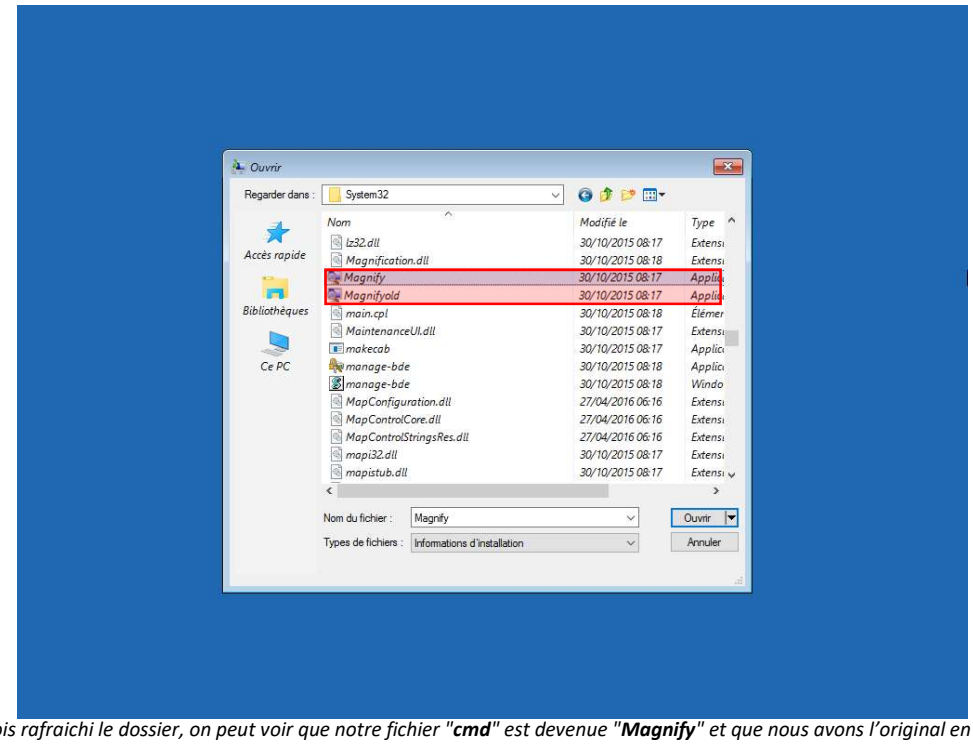
*Localiser le fichier "**Magnify**" et le renommer en "**Magnifyold**"*



*Localiser le fichier "**cmd**", en faire une copie*



*Renommer la copie du fichier "**cmd**", en "**Magnify**"*



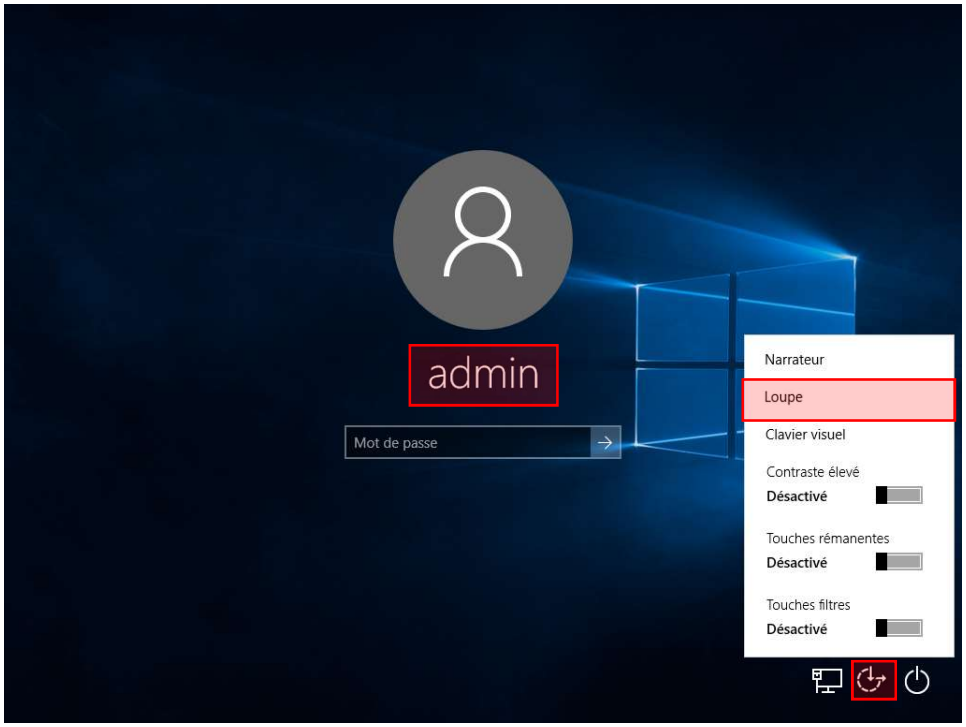
*Une fois rafraichi le dossier, on peut voir que notre fichier "**cmd**" est devenue "**Magnify**" et que nous avons l'original en "**Magnifyold**"*

Nous pouvons redémarrer l'ordinateur directement et enlever le CD ou la clé Bootable

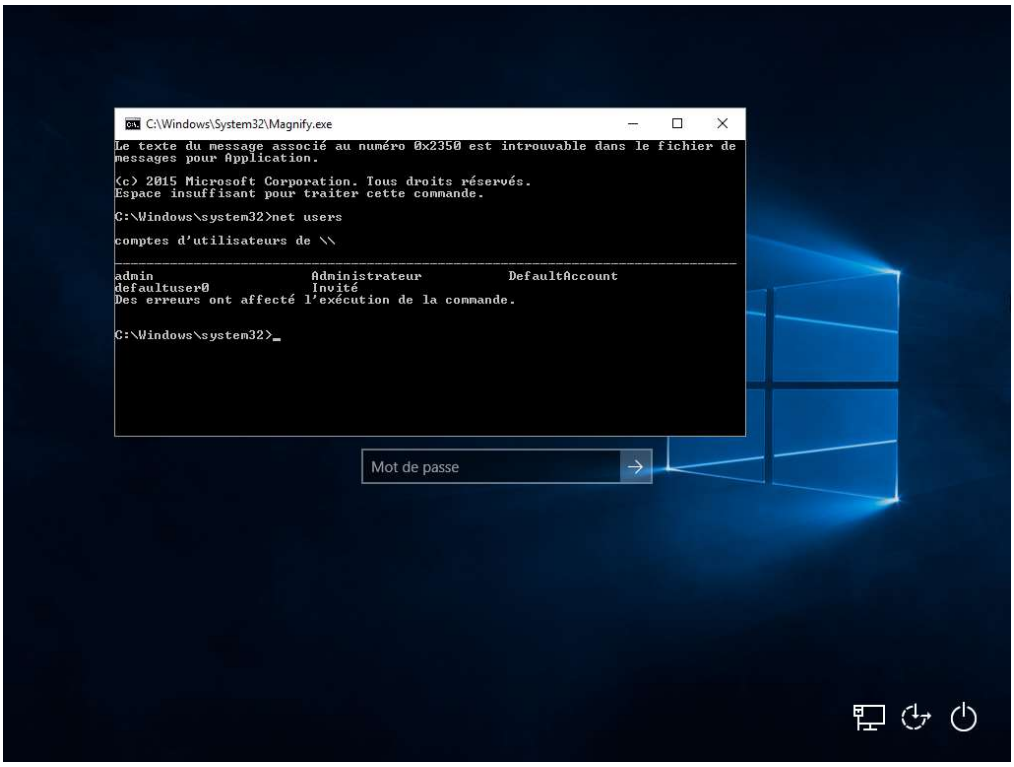
4. Exploitation de la faille

a. Compte utilisateur local

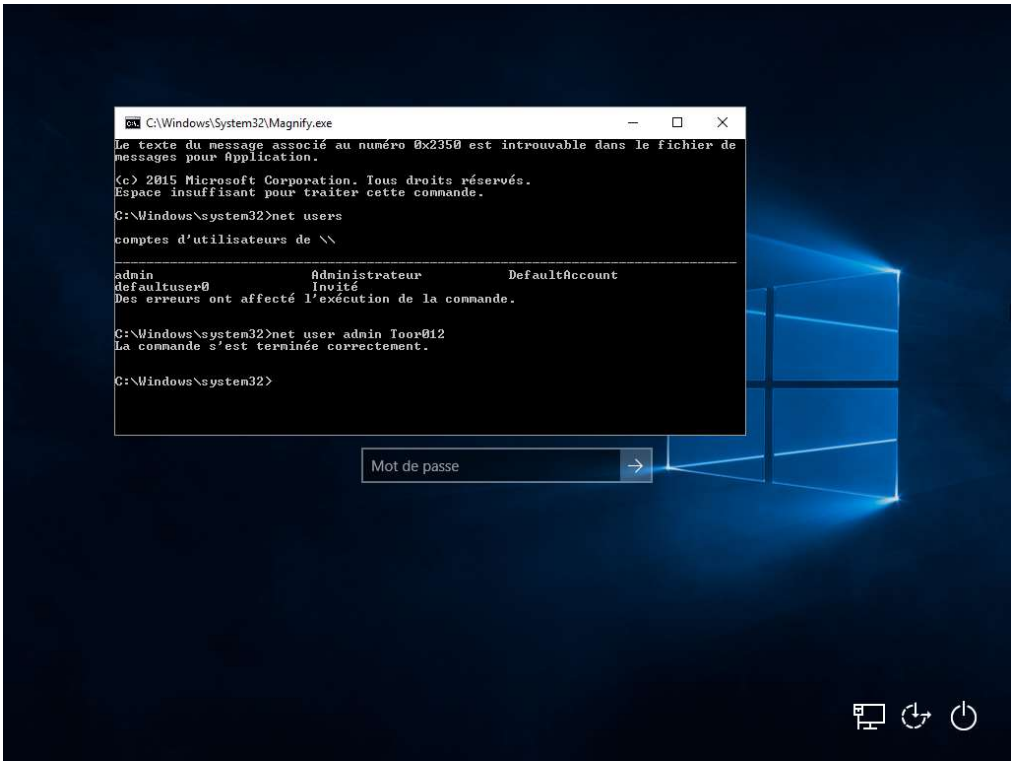
Démarrage de "**L'invite de commande**" grâce à la loupe



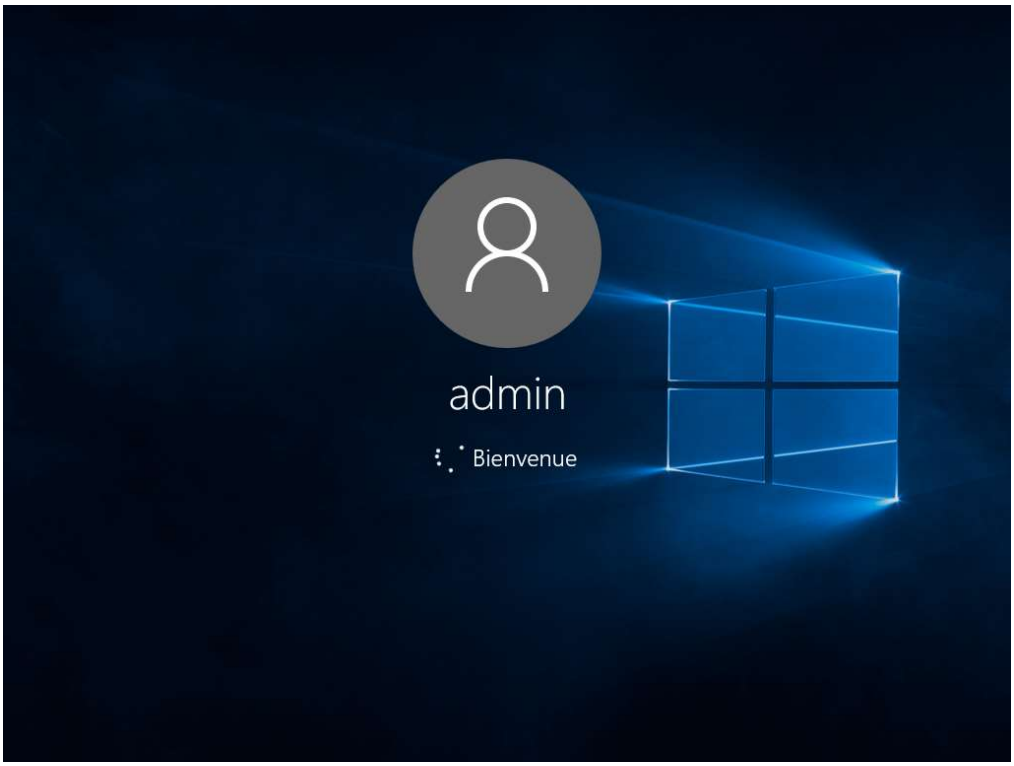
*Le mot de passe à réinitialiser est celui du compte administrateur, pour cela aller sur "**les options d'ergonomie**" et plus cliquer sur "**loupe**"*



*Nous avons donc l'invité de commande qui est exécuté, on peut faire un "**net users**", pour voir les utilisateurs de la machine*



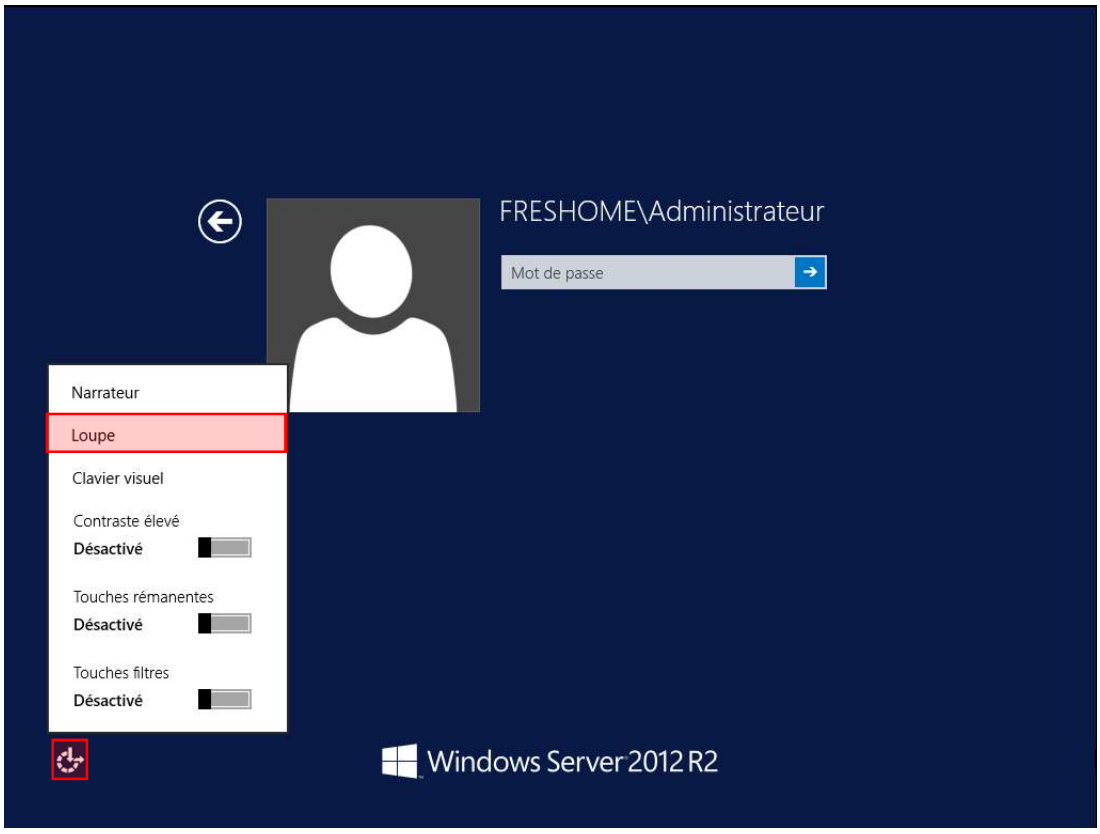
*Pour modifier le mot de passe, nous devons faire la commande "**net user <utilisateur> <nouveau mot de passe>**"*



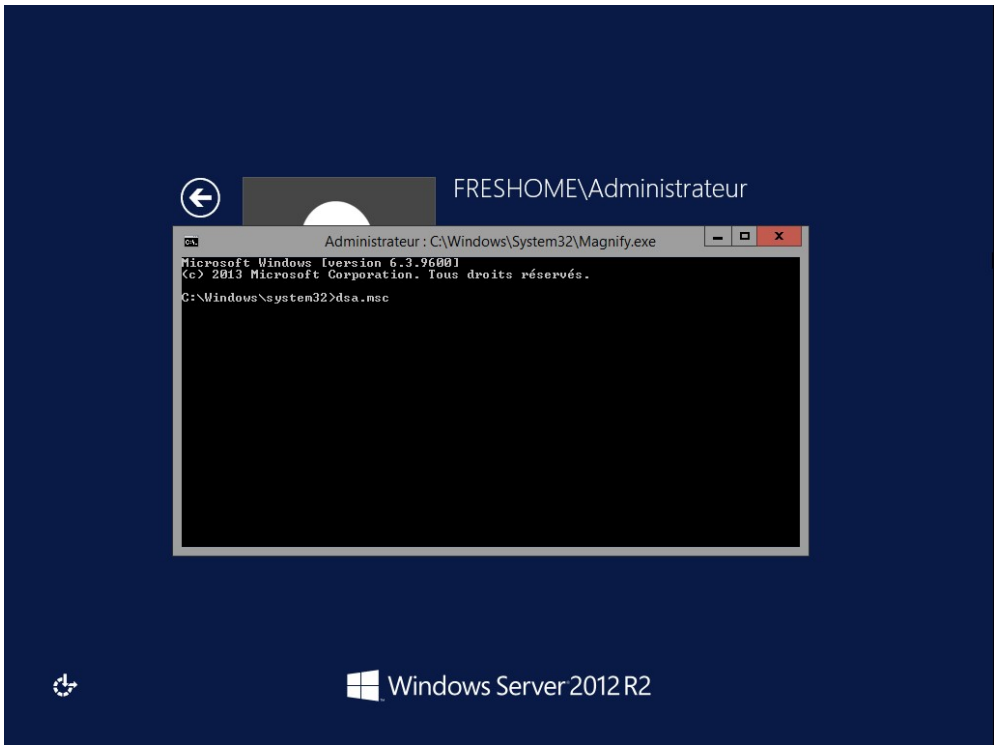
Voilà, le mot de passe a été réinitialisé

b. Contrôleur de domaine

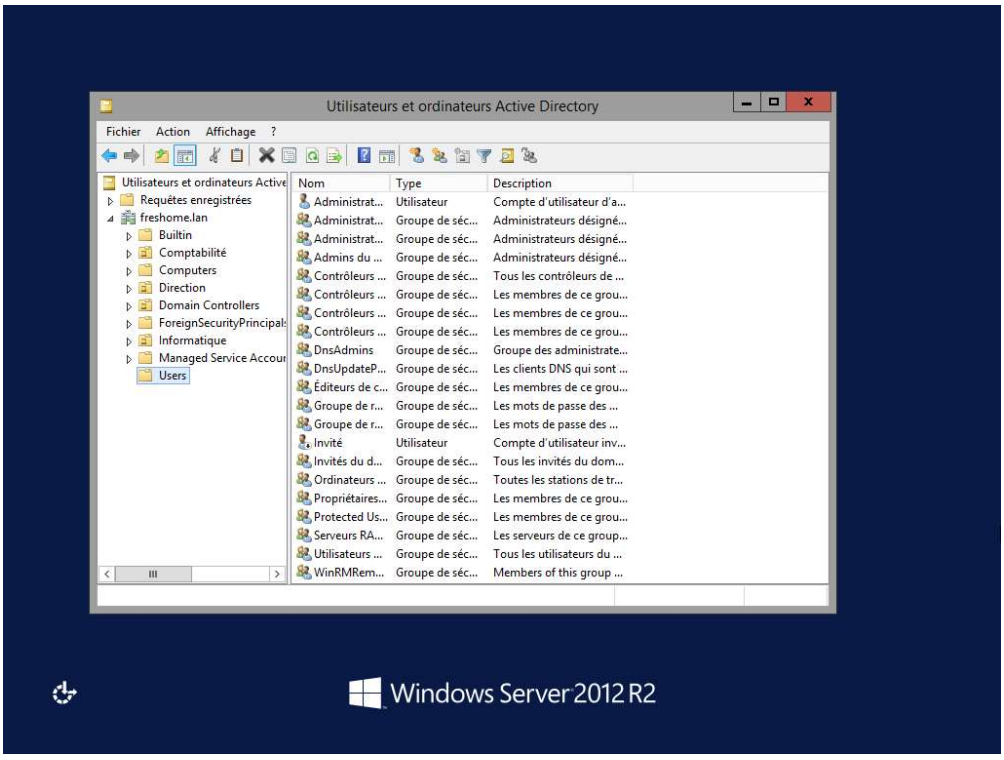
Démarrage de "**L'invite de commande**" grâce à la loupe



*Pour lancer le contrôleur de domaine, aller sur "**les options d'ergonomie**" et plus cliquer sur "**loupe**"*



*Nous avons donc l'invité de commande qui est exécuté, on peut faire un "**dsa.msc**" afin d'ouvrir le contrôleur de domaine*



Nous avons accès au contrôleur de domaine, avec des droits administrateurs

5. Comment remettre tout en ordre

Pour remettre comme avant, il suffise de booter sur le CD ou la clé USB bootable et de supprimer le fichier "**Magnify**" créer précédemment et renommer le fichier "**Magnifyold**" en "**Magnify**".