[Exploitation/Windows] Reset mot de passe admin local

Introduction

Nous allons voir les manipulations à faire lorsque vous souhaitez accéder à un poste Windows dont vous n'avez pas le mot de passe mais que vous avez un accès physique et un accès au disque dur contenant les partitions systèmes non chiffré.

Cette technique est vérifiée sur **Windows 7**, **8** et **10** (à tester sur Windows 11).

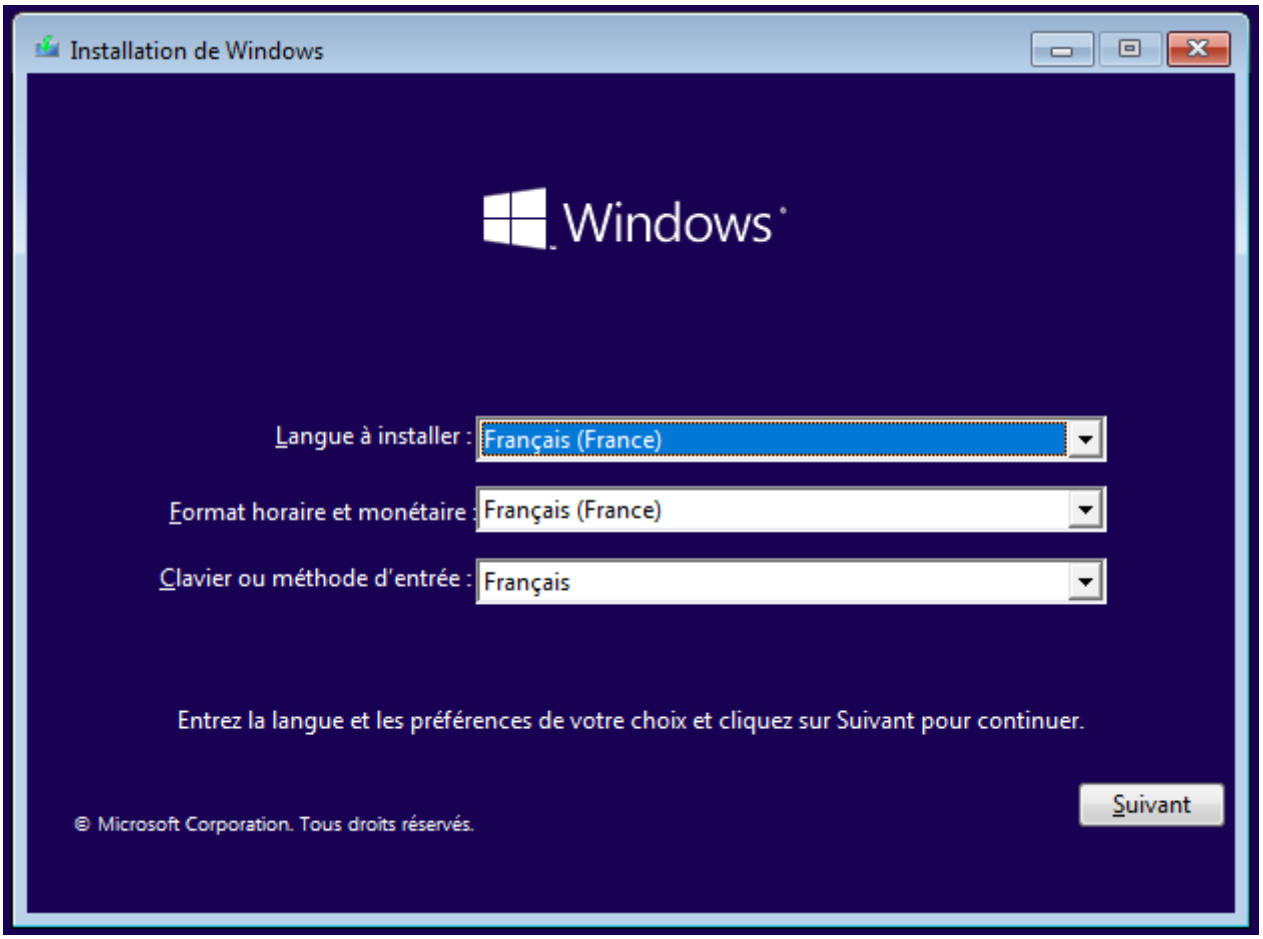
Prérequis

- Clé bootable Windows
- Un pc où on peut démarrer sur cette clé et avoir accès au disque dur système.

Procédure

Tout d'abord, ouvrir le boot menu pour démarrer sur la clé avec Windows.

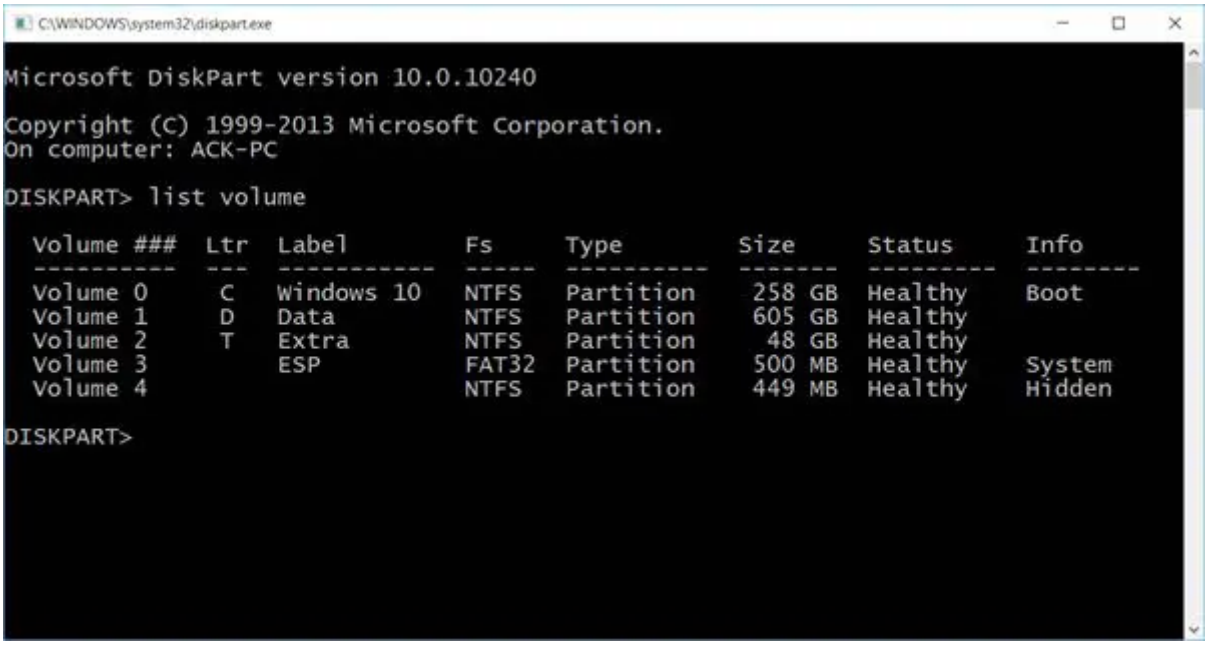
Une fois sur ce menu d'installation, exécutez la combinaison **Shift + F10** :



Une invite de commande devrait apparaître.

La première étape consiste à repérer la lettre du volume de la partition système de Windows.

Pour cela, lancez l'utilitaire **diskpart** et exécutez la commande **list volume** :



Sur cette capture il s'agit du volume C sauf que votre système live il y a très peu de chance que cela se produise.

En général il s'agit du **volume D** et parfois E.

L'étape suivante consiste à copier le binaire de l'invite de commande **cmd.exe** en **Magnify.exe** qui est l'outil loupe que nous pouvons lancer depuis l'écran de connexion.

Il faut pour cela renommer le véritable utilitaire loupe pour le rendre inexécutable :

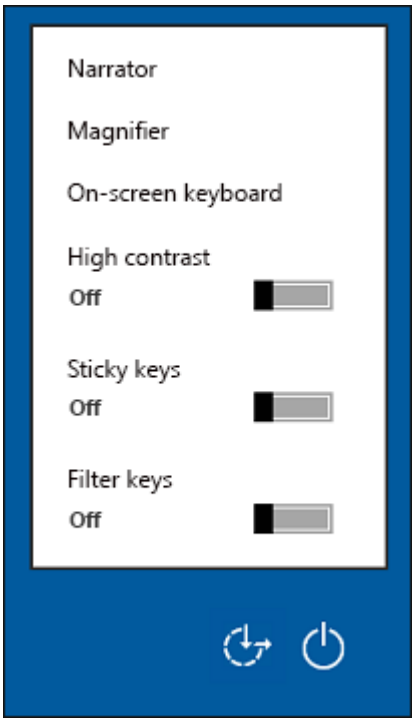
```
copy C:\Windows\System32\Magnify.exe C:\Windows\System32\Magnify.exe.bak
```

Puis on fait une copie du cmd que l'on nomme exactement pareil que l'outil loupe original :

```
copy C:\Windows\System32\cmd.exe copy C:\Windows\System32\Magnify.exe
```

Éteignez l'ordinateur et **redémarrez**.

Une fois sur l'écran de connexion, cliquez sur les **options d'ergonomie** et lancez la **loupe** :



Un invite de commande avec les droit **NT system** devrait s'ouvrir.

Vous n'avez plus qu'à **modifier le mot de passe** de l'administrateur local ou de votre utilisateur grâce à la commande suivante :

```
net user administrateur <PASSWORD>
```

Remarque : Selon la langue du système et la version de windows, il se peut que ce ne soit pas **administrateur** mais **administrator**.

Revision #2
Created 15 September 2023 13:50:28 by Elieroc

Updated 3 May 2024 13:11:32 by Elieroc