



# SYSTEMES D'EXPLOITATION

Labo 2 – Windows serveur

## RESUME

Durant ce laboratoire, vous allez découvrir le système d'exploitation Microsoft Windows serveur.

Au même titre que Linux (Labo1), il est largement utilisé en entreprise.

Olivier Masit

SE - BLOC1 - UE02 - Systèmes d'exploitation – Labo 2

## DUREE ESTIMEE

1H30

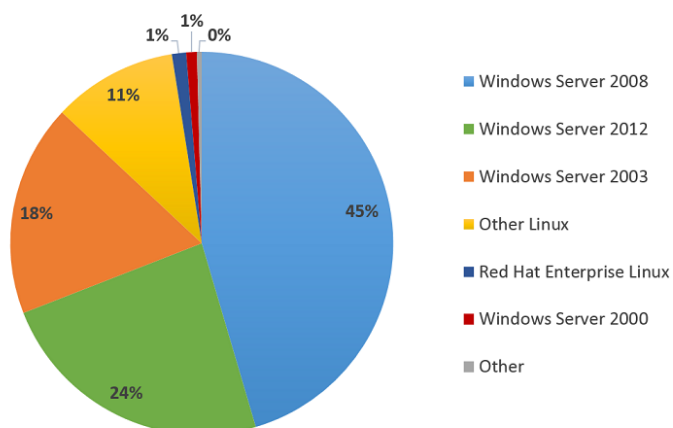


## 1 Introduction à Windows Serveur

### 1.1 Parts de marché

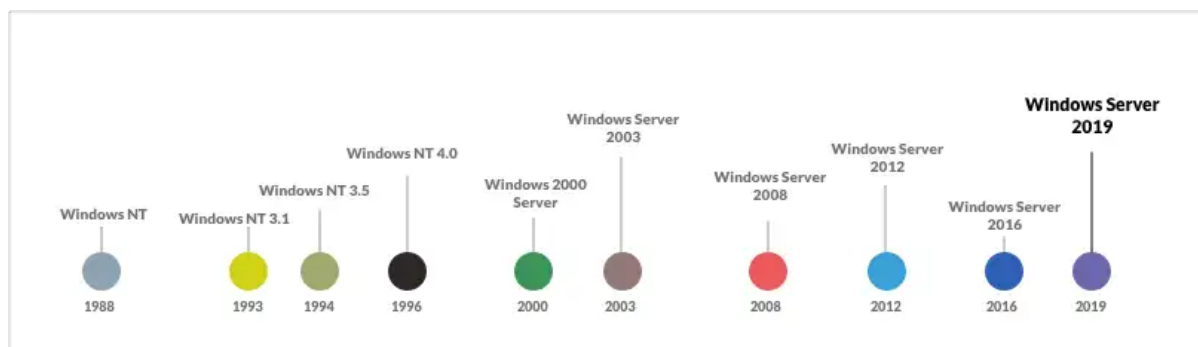
Windows server est le système d'exploitation le plus utilisé par les entreprises dans le monde, il est donc important de vous familiariser avec lui. Il côtoie en général des serveurs Linux et d'autres systèmes tels que les mainframes.

On-Premises Server Operating System Market Share in 2016



### 1.2 Historique

Windows serveur est l'évolution du premier OS de type serveur de Microsoft appelé Windows NT (New Technology) dont la première version est apparue en 1988. Windows NT a été très largement déployé dès 1993 dans sa version 3.1 détrônant alors les concurrents sur le marché des OS de type serveur x86.



### 1.3 Les versions actuelles

Certaines entreprises tournent encore des version 2008 et 2008R2 (release 2) en « extended support ». En effet cet OS n'est plus supporté par Microsoft car il est EOL (End-of-Life). En théorie, les versions que vous rencontrerez ne devraient pas être plus anciennes que la version 2012 sauf exceptions. Depuis la version 2019, Microsoft a adopté deux différents « services channels » comme Ubuntu Linux. Une version LTSC (long time service channel) supportée pendant 10 ans et une version semi-annuelle supportée 18 mois. Les versions semi-annuelles ne portent pas le nom Windows server



2019 mais sont nommées par leur version de « build », exemple Windows serveur 1903 ou encore Windows serveur 2004.

Pour plus d'information, vous pouvez consulter <https://docs.microsoft.com/en-us/windows-server/get-started-19/servicing-channels-19>.

## 2 Labo – Introduction

Dans le cadre de ce laboratoire, vous utiliserez une version 2016 avec GUI. En effet Windows serveur est disponible avec ou sans interface graphique. La recommandation étant de l'installer en version core (sans GUI) sauf si les logiciels devant tourner dessus nécessitent une interface graphique.

La version core réduit l'empreinte sur le stockage, offre une surface d'attaque beaucoup plus petite, nécessite moins d'updates et offre de meilleures performances pour un « sizing » équivalent.

Contrairement aux administrateurs Linux (qui dans le passé n'offrait pas de GUI), les administrateurs Windows ont toujours eu l'habitude de manipuler une interface graphique car les versions antérieures à 2008 n'offraient pas de version core (sans GUI). Les versions core ont été plus largement déployées depuis 2016.

Dans ce labo vous aurez donc l'opportunité de vous familiariser avec le(s) Shell et le GUI.

### 2.1 Exercice 1 – Installation de votre serveur dans VMware

Pour ce labo, le serveur a été préinstallé par votre professeur. Au démarrage, il vous demandera d'entrer un nouveau mot de passe pour l'utilisateur appelé « Administrator » (équivalent du root en linux).

Une fois terminé, loggez-vous dans le serveur en tant que « administrator »



### 2.2 Exercice 2 – Renommer votre serveur

Chaque machine possède un nom unique sur le réseau, ce nom a été auto-généré lors de la procédure d'installation packagée par votre professeur.

Dans le menu « démarrer » tapez PowerShell et choisissez Windows PowerShell

 Windows PowerShell

PowerShell est un des Shell récent, il est extrêmement puissant et orienté objet. Chaque commande PowerShell suit un standard « Verb-Noun ». Exemple : Get-Help.

En PowerShell les commandes s'appellent des cmdlet.

Tapez la commande get-computerinfo



```
PS C:\Users\Administrator> Get-ComputerInfo

WindowsBuildLabEx           : 17763.1.amd64fre.rs5_release.180914-1434
WindowsCurrentVersion       : 6.3
WindowsEditionId            : ServerDatacenter
WindowsInstallationType     : Server
WindowsInstallDateFromRegistry : 30-09-20 10:59:38
```

Ensuite, entrez la commande `Get-ComputerInfo -Property CsName`.

Remarquez la différence, félicitations, vous venez d'afficher une seule propriété d'un objet. Le retour de la commande vous affiche le nom actuel de votre système.

Affichez les différents « verbs » en utilisant la commande `get-verb`

```
PS C:\Users\Administrator> Get-Verb_
```

Repérez le « verb » qui vous serait utile pour renommer votre OS.

Trouvez la commande permettant de renommer la machine à l'aide de la cmdlet `get-command`.

```
PS C:\Users\Administrator> Get-Command_
```

Une fois la commande trouvée, utiliser l'aide pour comprendre le fonctionnement de la commande et renommez votre OS.

Le nom ne sera pris en compte qu'après reboot.

Via le servermanager du GUI, vérifiez que le nom de votre machine a bien été modifié.

## Server Manager

### 2.3 Exercice 3 – gestion des comptes utilisateurs et des groupes

Tout comme en Linux, la gestion des groupes et des utilisateurs est primordiale. Cependant, Windows server est différent de linux car il existe un grand nombre de types de groupes en fonction de l'infrastructure générale. Nous nous concentrerons sur la gestion des groupes et des utilisateurs locaux.

- A l'aide de PowerShell, trouvez la commande servant à ajouter un groupe
- Ajouter les groupes « student » et « whitehat »
- Listez les groupes et vérifiez qu'ils ont bien été créés
- Trouvez la commande permettant d'ajouter un utilisateur
- Ajoutez votre propre utilisateur
  - Le mot de passe doit être passé à la commande sous forme de Secure string (un string encrypté).
  - Pour se faire utiliser le code suivant :

```
$mot_de_passe = read-host -AsSecureString
```
  - Passez ensuite la variable `$mot_de_passe` dans votre commande
    - Le compte ne doit jamais expirer, ne doit pas être désactivé.
    - Ajoutez-le dans le groupe student et dans le groupe administrateur.
    - Vérifiez que votre utilisateur fait bien partie du groupe Administrators



- Vérifiez les group « membership »
- Loggez-vous dans la session locale avec vos « credentials »
- Ajoutez l'utilisateur hacker
  - Le compte doit expirer le 24 décembre de cette année.
  - L'utilisateur doit pouvoir se logger interactivement. (allow log on locally)
    - Utilisez gpedit
- Ouvrez une session PowerShell en tant que « hacker ».
- Essayez à nouveau de changer le nom du server