



WAKANDA
Shoes

CESI
GMSI 44
AOÛT 2018

PROJET EVOLUTION

GRAJDEANU ALEXANDRU
GUINOT ROMAIN
TENQUEREL MÉDÉRIC



Projet
EVOLUTION



Sommaire

<i>I. INTRODUCTION</i>	5
A. Présentation du projet et rappel du contexte.....	5
B. Choix du matériel.....	5
C. Infrastructure.....	5
<i>II. LES SERVEURS WINDOWS</i>	5
A. Environnement	5
B. Installation Windows Serveur	5
C. Remote Server Admin Tools (RSAT).....	6
D. Choix des rôles	8
E. Installation DC1 et Active Directory (AD).....	8
1. Installation AD	11
F. Installation et configuration DC2.....	11
G. DNS (Domain Name System).....	11
1. Installation DNS	11
2. Configuration DNS.....	12
H. Les unités d'organisation (OU)	13
1. Création des OU.....	13
I. Serveur d'impression	13
1. Installation Serveur d'impression	13
2. Configuration Serveur d'impression	14
J. DFS (Distributed File System)	17
1. Installation DFS.....	18
2. Configuration DFS	19
3. Création des dossiers partagé	22
4. La déduplication	22
5. Configuration des clichés instantanés.....	22
6. Configuration des quotas.....	22
7. Configuration des audits	22
K. Les GPO	22

L.	Accès à distance.....	41
M.	Création des scripts	41
III.	<i>LES SERVEURS LINUX</i>	41
A.	Installation de l'environnement	41
1.	Partitionnement	41
2.	Configuration Réseau.....	44
B.	Configuration de base et intégration dans l'AD	45
1.	Mise à jour et intégration de l'autocomplétions.....	45
2.	Intégration dans l'AD.....	45
C.	Les serveurs de fichiers	48
1.	Le service FTP	49
2.	Le service Samba.....	50
3.	Le service NFS	50
4.	Le client NFS et la sauvegarde automatique.....	51
D.	Le service DHCP	51
IV.	<i>LA BASE DE DONNEES</i>	52
A.	Analyse de la (BDD) base de données.....	52
B.	Création et importation de la BDD	52
V.	<i>L'APPLICATION</i>	52
A.	Site web intranet	52
B.	Beau gosse GLPI.....	52
VI.	<i>GLOSSAIRE</i>	53
VII.	<i>ANNEXES</i>	54
A.	Installation serveur Linux.....	59
1.	Le service DHCP HA	59
2.	Le service NFS et SMB.....	65
3.	Le service FTP	71
4.	Le Serveur WEB	77
5.	Le Serveur GLPI.....	77
VIII.	<i>SOURCES</i>	86

I. INTRODUCTION

- A. Présentation du projet et rappel du contexte
- B. Choix du matériel
- C. Infrastructure

II. LES SERVEURS WINDOWS

A. Environnement

Pour nos serveurs nous avons choisi Windows Server 2016, que nous allons installer en « version core »

Les versions core nous permettent une économie de ressources.

Il y a moins de services ce qui signifie moins de processus et donc moins de ressources consommées. Ainsi, deux éléments de nos serveurs seront les premiers satisfaits : la mémoire vive (RAM) et le disque dur.

La mémoire vive sera moins sollicitée et le disque dur se remplira moins vite. Le gain de ressources avec Windows Server Core est réellement intéressant et permet d'optimiser au mieux l'utilisation des ressources pour des services plus importants, et une réduction de la surface d'attaque.

La surface d'attaque représente tous les points d'entrées possibles sur notre serveur, c'est-à-dire qui peuvent être potentiellement utilisés par un attaquant pour compromettre notre serveur.

Grâce à une installation en mode core, la surface d'attaque logicielle sera réduite puisqu'il y a moins de composants à installer, donc moins de points d'entrées.

À titre d'exemple, des vulnérabilités sont découvertes régulièrement au sein du navigateur Internet Explorer, comme il n'est pas installé lors d'une installation core, nous ne sommes pas concernés. De ce fait, la surface d'attaque est réduite.

En résumé, Windows Server Core améliore la sécurité du système en réduisant le nombre de composants installés.

B. Installation Windows Serveur

Cf. Annexe

C. Remote Server Admin Tools (RSAT)

Pour la gestion de nos serveurs nous avons choisi d'utiliser les RSAT.

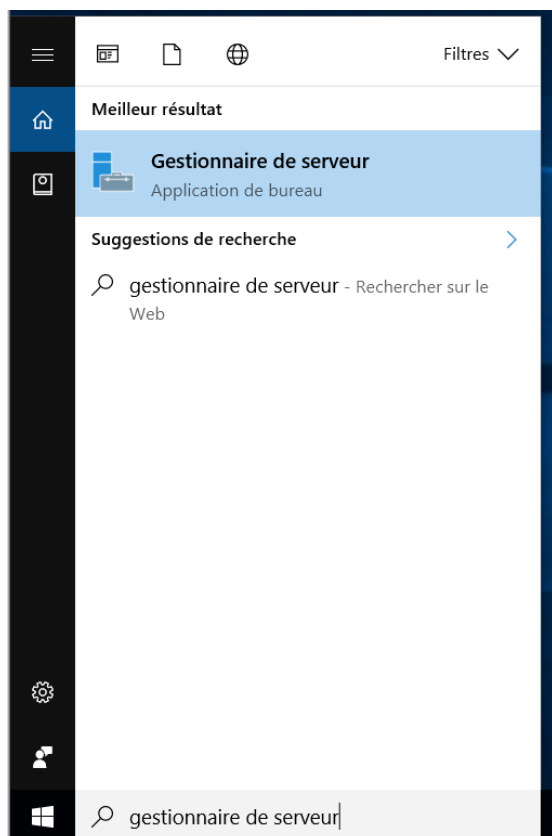
Les outils RSAT (Outils d'administration de serveur distant) permettent aux administrateurs informatiques de gérer à distance les rôles et les fonctionnalités de Windows Server 2012

Depuis une machine dites « cliente » nous téléchargeons un KB qui nous permet d'obtenir les RSAT

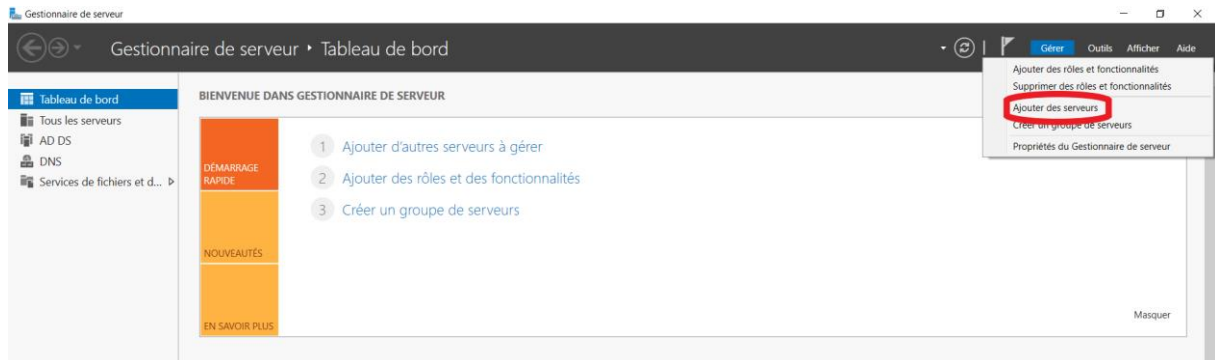
<https://www.microsoft.com/fr-FR/download/details.aspx?id=45520>

La machine doit être dans le même domaine que notre serveur.

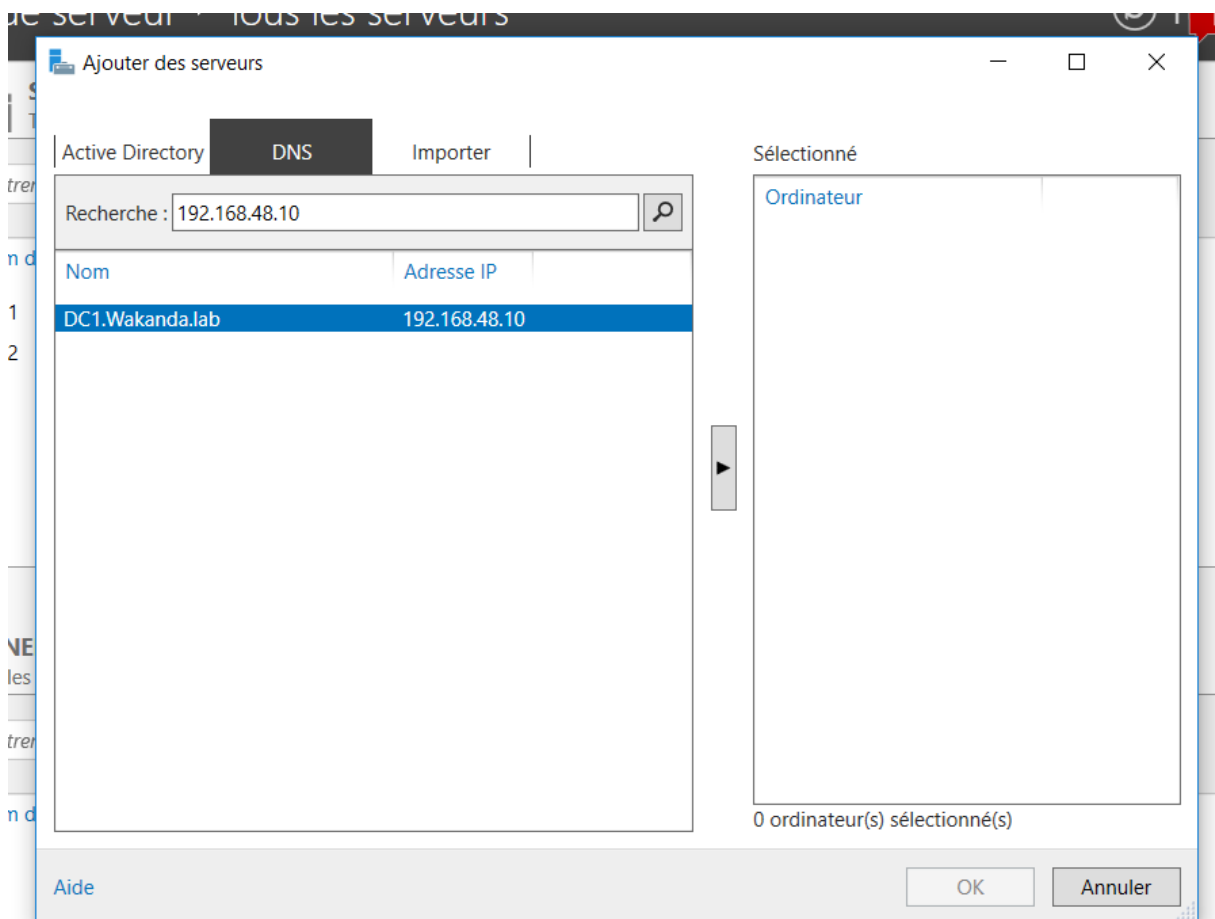
Nous allons utiliser le « Gestionnaire de Serveur » :



Nous allons donc ajouter notre serveur :



Nous allons faire une recherche DNS avec l'adresse de notre serveur en l'occurrence

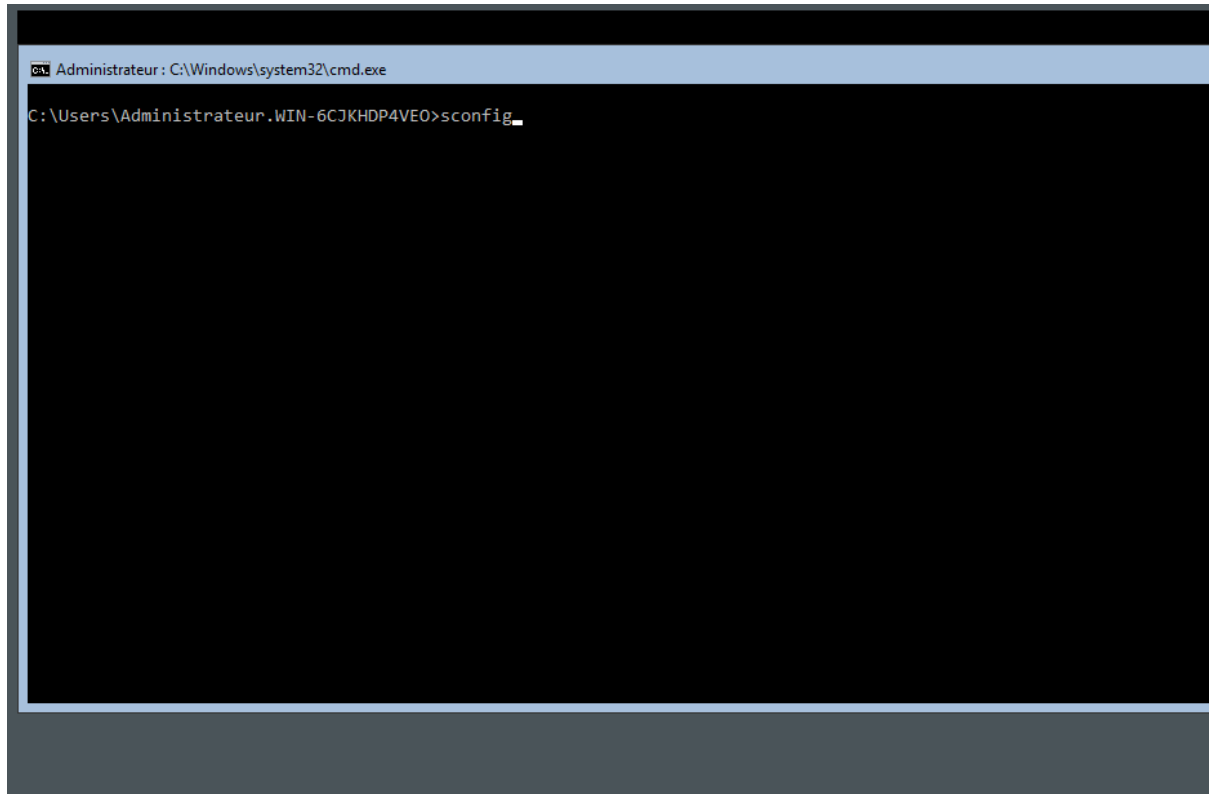


Une fois le serveur ajouté nous pouvons entièrement le gérer à distance.

D. Choix des rôles

E. Installation DC1 et Active Directory (AD)

Tout d'abords nous allons configurer les paramètres de notre DC1 via la commande « *sconfig* »



Cette commande nous permet d'afficher un menu complet nous permettant le paramétrage principal, en l'occurrence nous allons lui attribuer une IP fixe : 192.168.48.10, nous ajouterons également en DNS principal notre contrôleur de domaine numéro 2

```

C:\Windows\system32\cmd.exe - sconfig
Microsoft (R) Windows Script Host Version 5.812
Copyright (C) Microsoft Corporation. Tous droits réservés.

Inspection en cours du système...

=====
Configuration du serveur
=====

1) Domaine ou groupe de travail :      Groupe de travail:  WORKGROUP
2) Nom d'ordinateur :                  WIN-6CJXHDP4VE0
3) Ajouter l'administrateur local
4) Configurer l'administration à distance  Activé
5) Paramètres de Windows Update :      DownloadOnly
6) Télécharger et installer les mises à jour
7) Bureau à distance :                 Désactivé

8) Paramètres réseau
9) Date et Heure
10) Paramètres de télémétrie            Renforcée
11) Activation de Windows

12) Fermer la session utilisateur
13) Redémarrer le serveur
14) Arrêter le serveur
15) Quitter pour revenir à la ligne de commande

Entrez un nombre pour sélectionner une option : 1

C:\Windows\system32\cmd.exe - sconfig
Description                  Intel(R) 82574L Gigabit Network Connection
Adresse IP                   169.254.5.41    fe80::48ed:9e09:8424:529
Masque de sous-réseau        255.255.0.0
DHCP activé                  Vrai
Passerelle par défaut
Serveur DNS préféré
Serveur DNS auxiliaire

1) Définir l'adresse de la carte réseau
2) Définir les serveurs DNS
3) Effacer les paramètres du serveur DNS
4) Retourner au menu principal

Sélectionner une option : 1

Sélectionner (D)HCP, IP (s)tatique (Vide=Annuler) : s

Définir IP statique
Entrer une adresse IP statique : 192.168.48.10
Entrer un masque de sous-réseau (Vide = par défaut 255.255.255.0) :
Entrez la passerelle par défaut : 192.168.48.254
Affectation d'une adresse IP statique à la carte réseau...

-----
Paramètres de carte réseau
-----

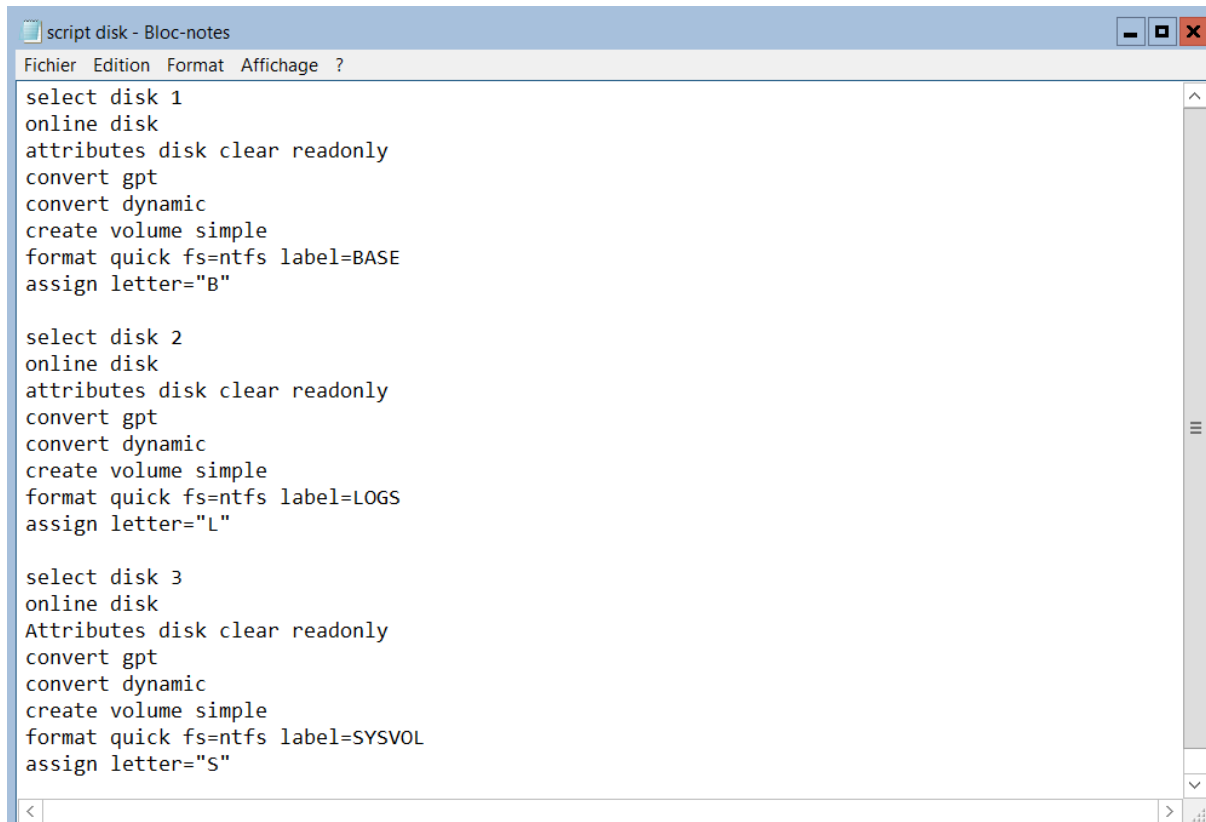
Index NIC                    0
Description                  Intel(R) 82574L Gigabit Network Connection
Adresse IP                   192.168.48.10    fe80::48ed:9e09:8424:529
Masque de sous-réseau        255.255.255.0
DHCP activé                  Faux
Passerelle par défaut        192.168.48.254
Serveur DNS préféré
Serveur DNS auxiliaire

1) Définir l'adresse de la carte réseau
2) Définir les serveurs DNS
3) Effacer les paramètres du serveur DNS
4) Retourner au menu principal

Sélectionner une option : 1

```

Nous allons également exécuter un script (dans diskpart) permettant de gérer les disques du contrôleur de domaine.



```

select disk 1
online disk
attributes disk clear readonly
convert gpt
convert dynamic
create volume simple
format quick fs=ntfs label=BASE
assign letter="B"

select disk 2
online disk
attributes disk clear readonly
convert gpt
convert dynamic
create volume simple
format quick fs=ntfs label=LOGS
assign letter="L"

select disk 3
online disk
Attributes disk clear readonly
convert gpt
convert dynamic
create volume simple
format quick fs=ntfs label=SYSVOL
assign letter="S"
  
```

Nous mettons en place 4 disques afin d'améliorer la sécurité et de séparé les parties essentiels.

Il y aura un disque qui contient le système Windows du Serveur.

Les autres seront :

Disk 1 = Notre BASE, c'est l'endroit où l'AD est stocké

Disk 2 = Les LOGS, où seront stocké les logs qu'on peut traduire par les événements passés

Disk 3 = SYSVOL, l'endroit où seront stocké les GPO et les scripts

1. Installation AD

L'installation de notre AD se fera via un script :

Install AD Core.ps1

```
1 Install-WindowsFeature -name AD-Domain-Services -IncludeManagementTools
2 pause
3 Install-ADDSForest -CreateDnsDelegation:$false -DatabasePath "E:\NTDS" -DomainName "wakanda.lan" -DomainNetbiosName "WAKANDA"
  -InstallDNS :$true -LogPath "G:\LOGS" -SysvolPath "F:\SYSVOL" -Force :$true
```

Ce script nous permettra donc d'installer le rôle AD, de créer notre forêt, le nom de notre domaine le nom NETBIOS, installer le rôle DNS, et d'installer dans les différents disques précédemment configurés notre datapath, Les LOGS et le répertoire SYSVOL.

F. Installation et configuration DC2

G. DNS (Domain Name System)

Le Domain Name System, généralement abrégé DNS, qu'on peut traduire en « système de noms de domaine », est le service informatique distribué utilisé pour traduire les noms de domaine Internet en adresse IP ou autres enregistrements.

1. Installation DNS

L'installation du DNS est comprise dans l'installation du rôle ADDS

Nous allons configurer les zones de recherches

La zone de recherche direct qui permet convertir un nom en adresse IP

Et la zone de recherche indirect qui permet à l'inverse de convertir une adresse IP en nom

H. Les unités d' organisation (OU)

1. Création des OU

I. Serveur d' impression

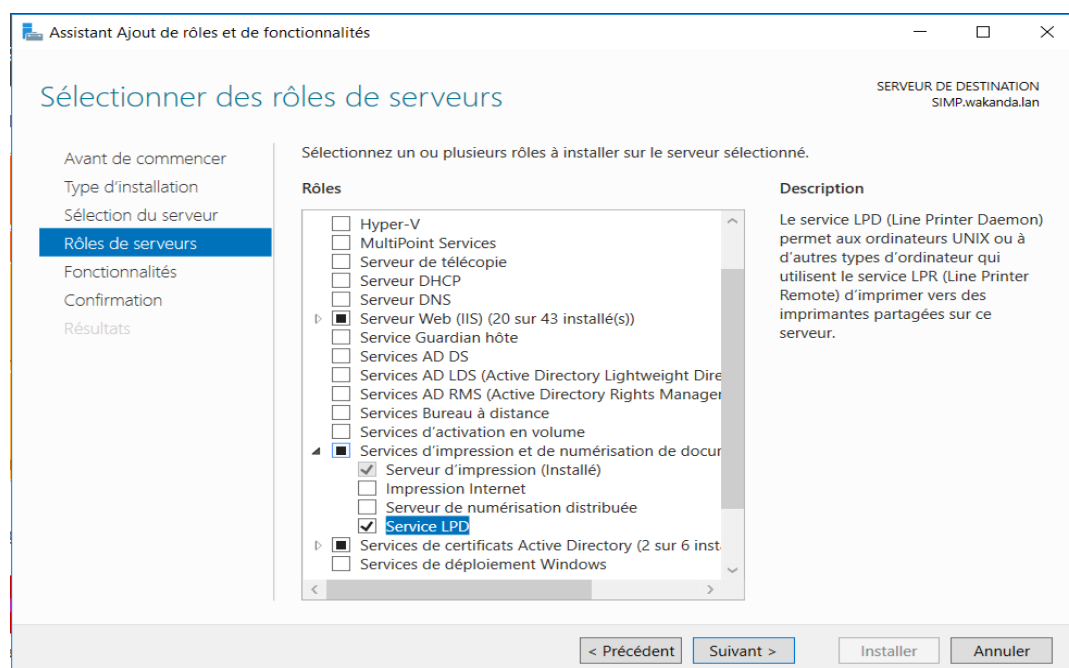
Un serveur d'impression est une application logicielle, un périphérique réseau ou un ordinateur qui gère les demandes d'impression et rend les informations d'état de la file d'attente d'imprimantes accessibles aux utilisateurs finaux et aux administrateurs réseau.

Les serveurs d'impression sont utilisés dans les réseaux des Grandes Entreprises, PME (petites et moyennes entreprises), TPE (très petite entreprise).

Ils sont connectés à un réseau informatique afin de répondre à la nécessité d'imprimer des travaux dans un réseau qui peut contenir plus d'une imprimante.

1. Installation Serveur d' impression

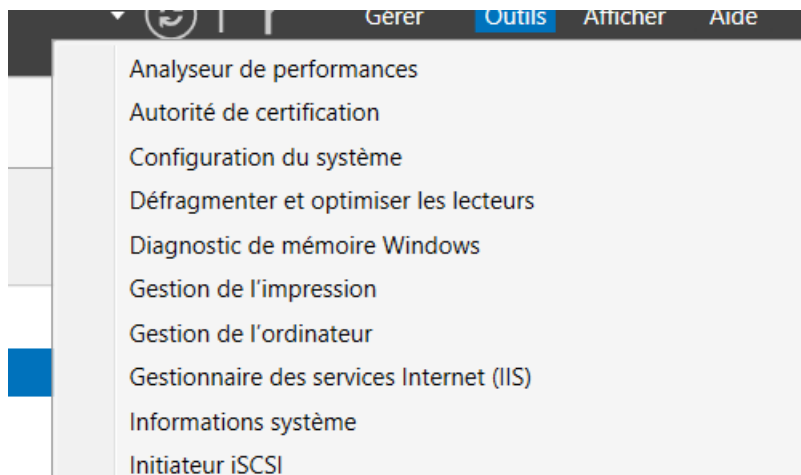
Nous utiliserons une License Windows Server 2016 sur lequel nous ajouterons le rôle « Services d'impression et de numérisation de document »



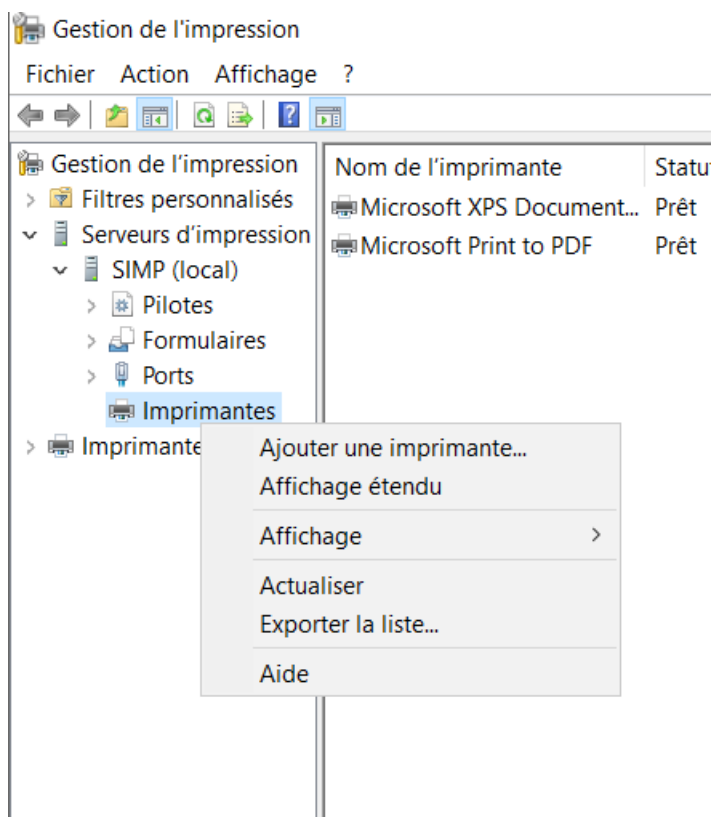
2. Configuration Serveur d' impression

Comme il est demandé nous avons mis en place une imprimante par Service, ainsi qu'une imprimante dites « Public » accessible par tout le monde sur le réseau.

Nous nous rendrons dans la console « Gestion de l'impression »



Nous ajouterons une imprimante



Nous ajouterons une imprimante TCP/IP ou des services Web par adresse IP ou nom d'hôte.

Assistant Installation d'imprimante réseau

Installation de l'imprimante
Choisissez une méthode d'installation.

☐ Rechercher les imprimantes du réseau
☒ Ajouter une imprimante TCP/IP ou de services Web par adresse IP ou nom d'hôte
☐ Ajouter une nouvelle imprimante via un port existant : LPT1: (Port imprimante)
☐ Créer un autre port et ajouter une nouvelle imprimante : Local Port

< Précédent **Suivant >** Annuler

On ajoute donc l'adresse ip de notre imprimante :

Assistant Installation d'imprimante réseau

Adresse de l'imprimante
Vous pouvez entrer le nom réseau de l'imprimante ou son adresse IP.

Type de périphérique : Périphérique TCP/IP
 Nom d'hôte ou adresse IP : 192.168.48.24
 Nom du port : 192.168.48.24
☒ Détecter automatiquement le pilote d'imprimante à utiliser.

< Précédent **Suivant >** Annuler

Nous allons partager cette imprimante et définir le nom du partage :

Assistant Installation d'imprimante réseau

Nom de l'imprimante et paramètres de partage
Vous pouvez donner un nom convivial à l'imprimante et spécifier si elle peut être utilisée par d'autres personnes.

Nom de l'imprimante :

☒ Partager cette imprimante

Nom du partage :

Emplacement :

Commentaire :

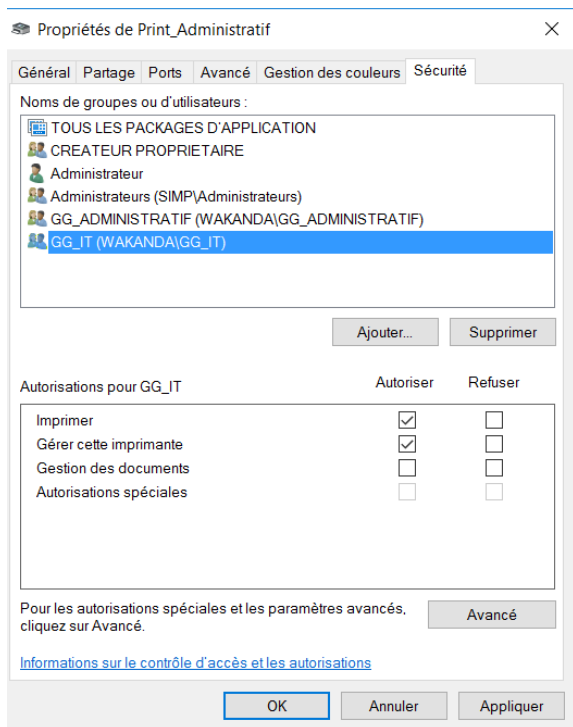
< Précédent Suivant > Annuler

Une fois toutes les imprimantes créées nous les sélectionnerons toutes, et nous cliquerons sur « Répertorier dans l'annuaire » afin de les référencer dans L'AD



Nous les déploierons par GPO par la suite et les paramétrons dans ces même GPO.

On paramétrera également les droits sur les imprimantes, pour que le service informatique puisse gérer cette imprimante



J. DFS (Distributed File System)

L'acronyme DFS signifie Distributed File System c'est à dire Système de fichiers distribués.

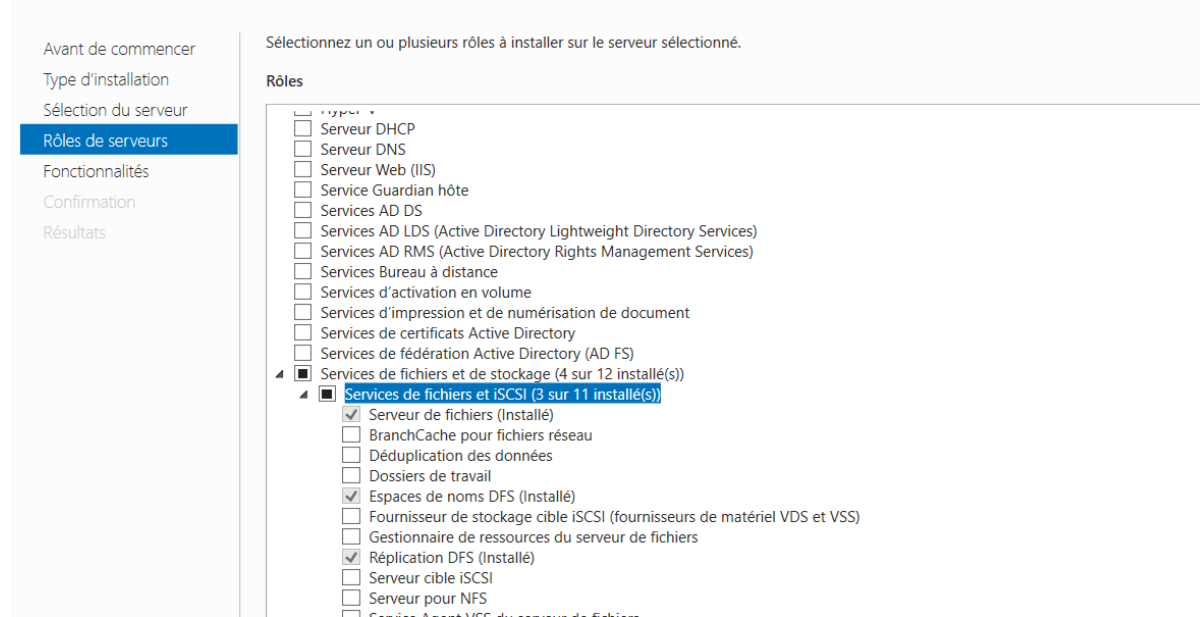
Ce système de fichier hiérarchisé permet de structurer les fichiers partagés sur différents serveurs du réseau de façon logique. Il permet de référencer un ensemble de partages qu'il faudra rendre accessibles de manière uniforme puis, de centraliser l'ensemble des espaces disponibles sur cet ensemble de partages.

Avec le DFS, l'utilisateur final ne visualise pas le nom du serveur sur lequel il accède pour lire les données, cela est totalement transparent. L'avantage c'est que si le serveur vient à changer à cause d'une panne ou pour cause d'évolution, le chemin d'accès restera le même.

1. Installation DFS

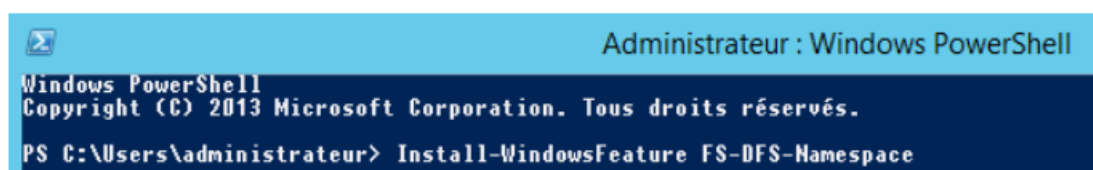
Tout d'abord nous allons installer le rôle « Service de fichiers et de stockage », « Services de fichiers et iSCSI » puis « Espaces de nom DFS ». sur un Windows Server 2016 vierge.

Sélectionner des rôles de serveurs



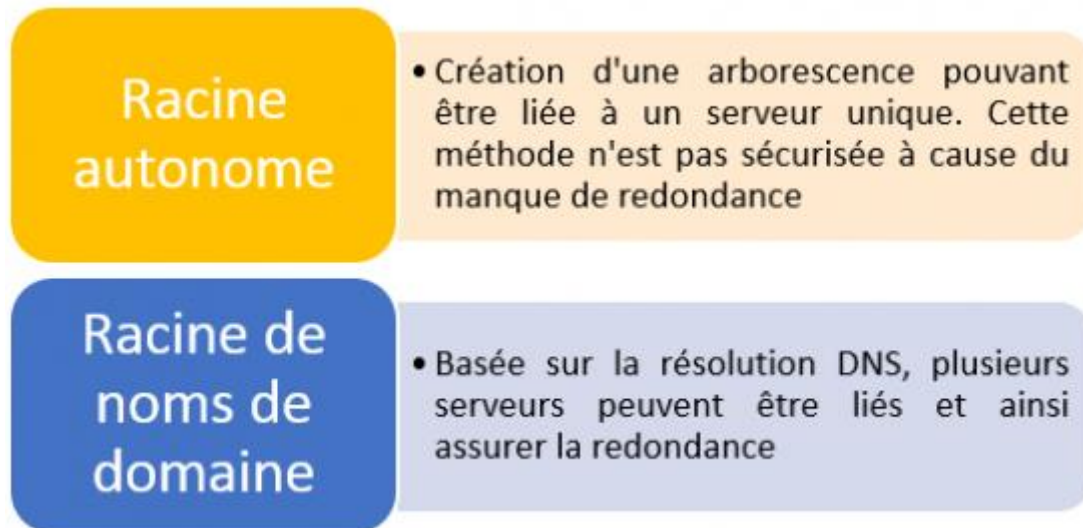
Via la commande powershell « Install-WindowsFeature FS-DFS-Namespace »

Ainsi que « Install-WindowsFeature FS-DFS-Replication »



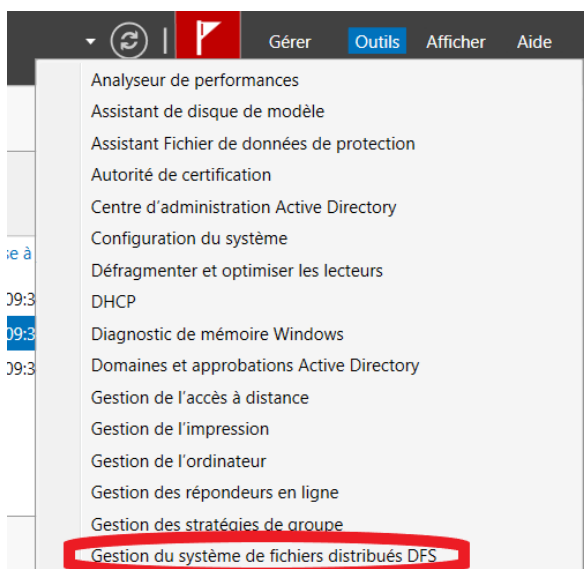
2. Configuration DFS

Le serveur DFS est désormais installé, passons à la configuration. Avant cela, sachez qu'il existe deux types de racine DFS : Racine autonome et racine de noms de domaine.

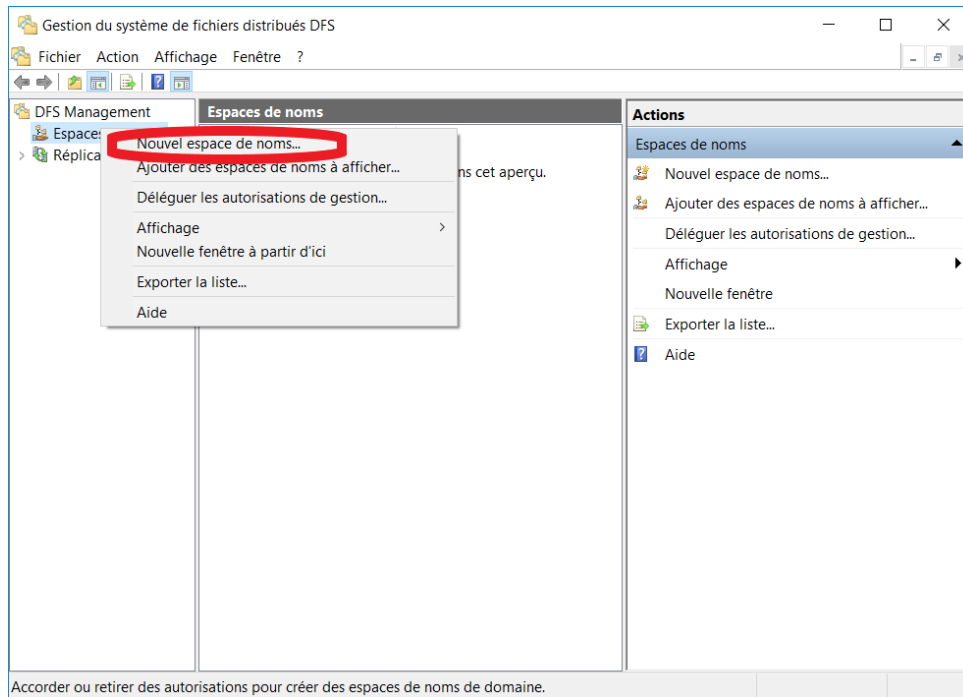


Nous allons donc créer une racine de noms de domaine, c'est un bon moyen d'assurer une redondance.

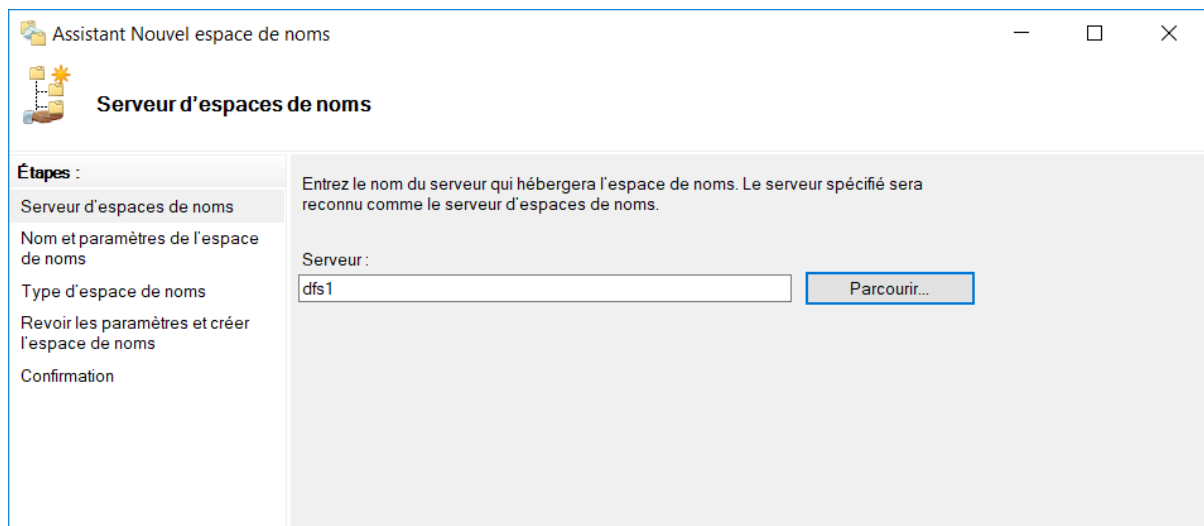
Pour ce faire :



Depuis cette console nous allons créer un nouvel espace de nom



Ensuite indiquer notre serveur



Entrez un nom pour notre espace de nom

Assistant Nouvel espace de noms

Nom et paramètres de l'espace de noms

Étapes :

- Serveur d'espaces de noms
- Nom et paramètres de l'espace de noms
- Type d'espace de noms
- Revoir les paramètres et créer l'espace de noms
- Confirmation

Entrez un nom pour l'espace de noms. Ce nom apparaîtra après le nom du serveur ou du domaine dans le chemin d'accès de l'espace de noms, par exemple \\Serveur\Nom or \\Domaine\Nom.

Nom :

Exemple : Public

Au besoin, l'Assistant créera un dossier partagé sur le serveur d'espaces de noms. Pour modifier les paramètres du dossier partagé (chemin d'accès ou autorisations), cliquez sur Modifier les paramètres...

Modifier les paramètres...

Nous sélectionnons « Espace de noms de domaine »

Assistant Nouvel espace de noms

Type d'espace de noms

Étapes :

- Serveur d'espaces de noms
- Nom et paramètres de l'espace de noms
- Type d'espace de noms
- Revoir les paramètres et créer l'espace de noms
- Confirmation

Sélectionnez le type d'espace de noms à créer.

☒ Espace de noms de domaine

Un espace de noms de domaine est stocké sur un ou plusieurs serveurs d'espaces de noms et dans les services de domaine Active Directory. Vous pouvez accroître la disponibilité d'un espace de noms de domaine en utilisant plusieurs serveurs. Lorsqu'il est créé dans le mode Windows Server 2008, l'espace de noms prend en charge une plus grande extensibilité et énumération basée sur l'accès.

☒ Activer le mode Windows Server 2008

Aperçu de l'espace de noms de domaine :

☐ Espace de noms autonome

3. Création des dossiers partagé
4. La déduplication
5. Configuration des clichés instantanés
6. Configuration des quotas
7. Configuration des audits

K. Les GPO

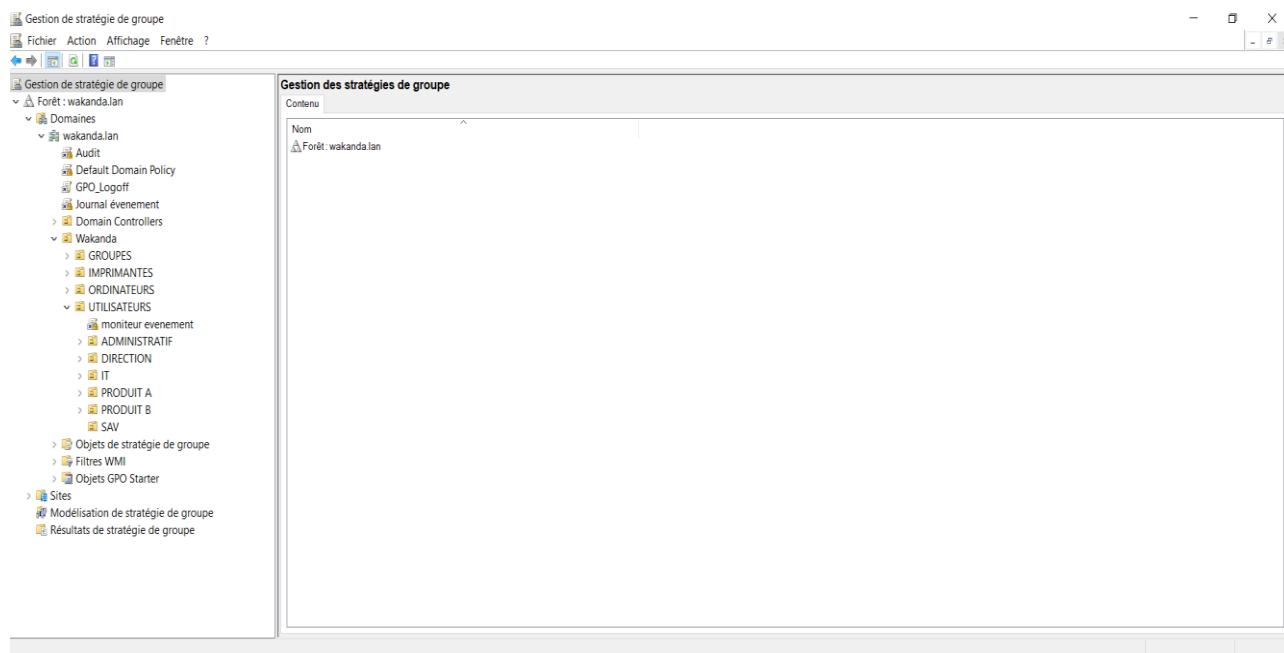
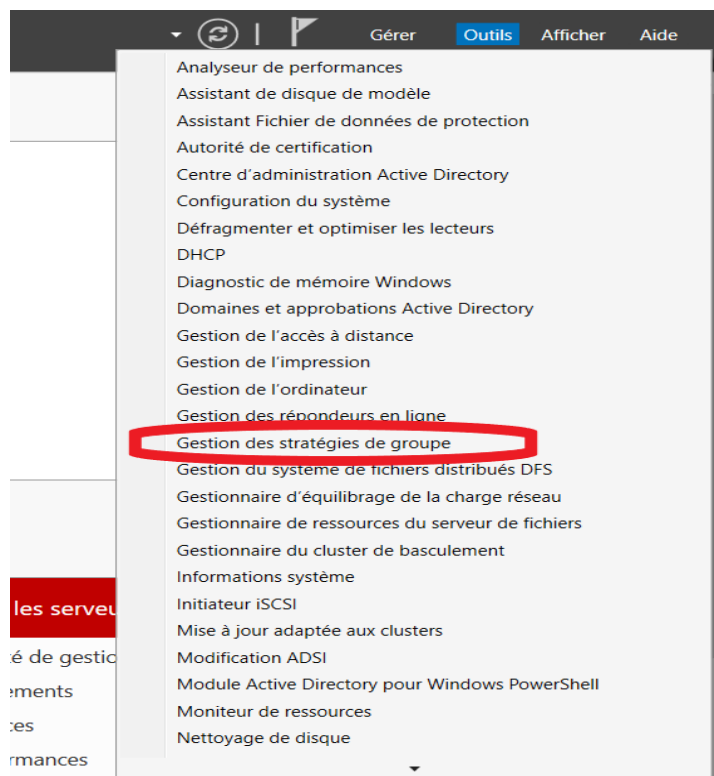
Les stratégies de groupe ou GPO (Group Policies Object) permettent de configurer des restrictions d'utilisation de Windows où des paramètres à appliquer soit sur un ordinateur donné soit sur un compte utilisateur donné.

Il est ainsi possible d'agir sur :

- La définition d'un environnement adapté : Il est possible par exemple de rediriger certains répertoires leurs contenus
- Le déploiement de logiciels : Une automatisation complète de l'installation des programmes sur les postes clients est possible en fonction du profil de l'utilisateur
- L'application des paramètres de sécurité : Le contexte de sécurité de l'environnement utilisateur peut être modifier

Les GPO ne peuvent être appliquées qu'à des conteneurs : site, domaine ou encore unité d'organisation mais elles peuvent être assignées plusieurs fois à des conteneurs différents. Le contenu d'une GPO sera donc appliqué sur les comptes utilisateurs et ordinateurs contenus dans le conteneur et plusieurs GPO peuvent être liée à un même conteneur.

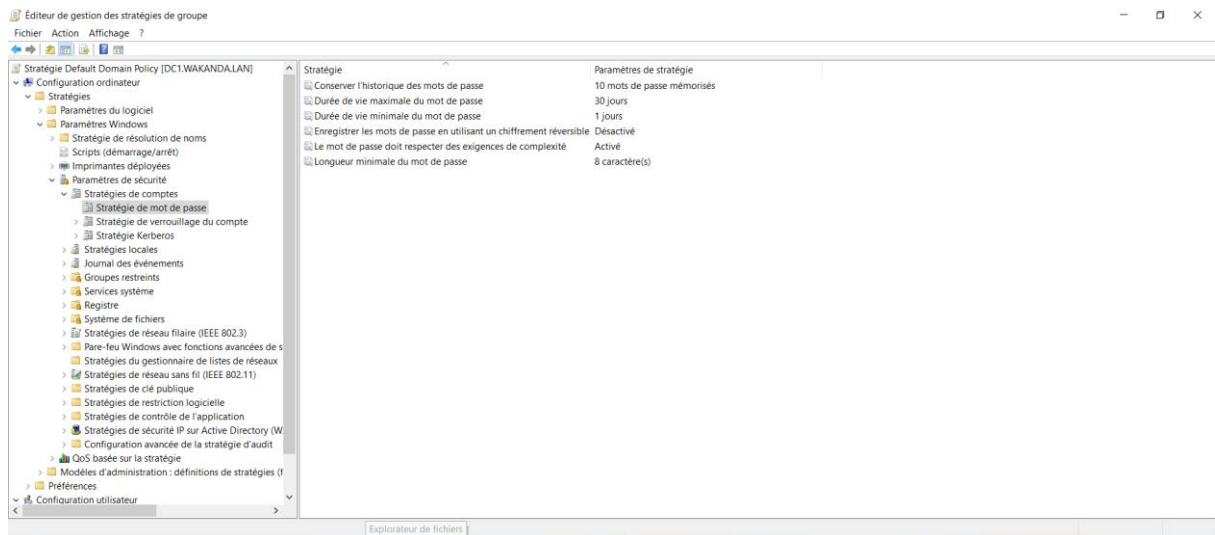
Premièrement, il faut accéder à la console de stratégies de groupe :



Une fois sur cette console qui nous permet de gérer les GPO, nous allons faire suite au cahier des charges, où il est demandé le déploiement de certaines GPO.

« Mot de passe doit répondre aux exigences de complexité ; 8 caractères minimum »

Pour la partie dites de « sécurité », nous avons déployer cette GPO :



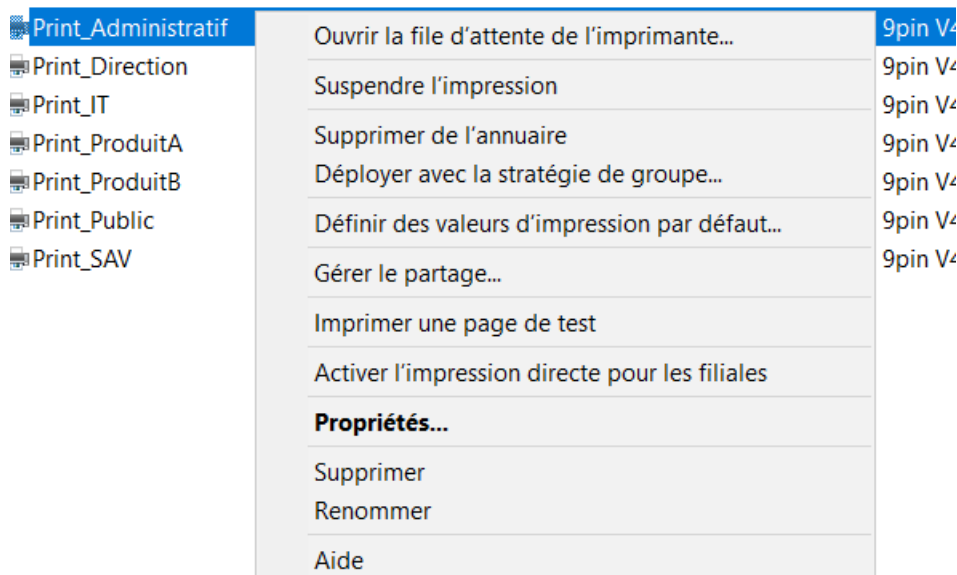
Les conditions des mots de passe sont désormais les suivantes :

- Historique des mots de passe : 10
- Durée de vie maximale du mot de passe : 30 jours
- Durée de vie minimal : 1 jour
- Le mot de passe doit respecter les exigences de complexité : Activé
- Longueur minimal du mot de passe : 8 caractères

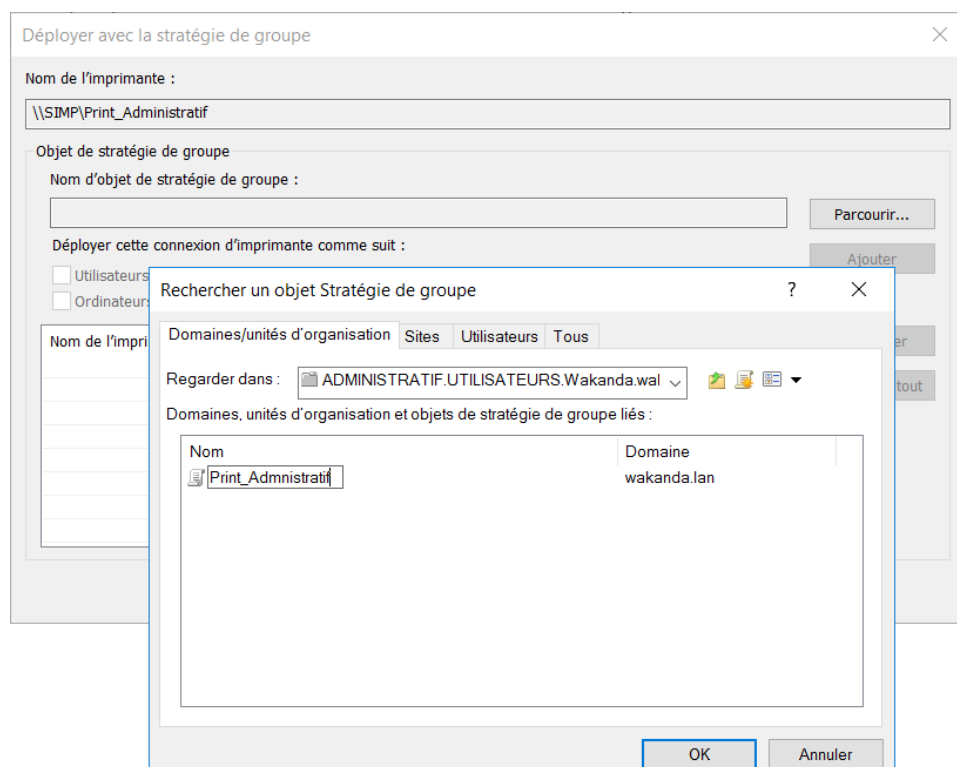
« Il faut 1 imprimante pour chaque service nommée Printnom du service »

Les imprimantes précédemment créées, nous allons maintenant les déployer par GPO.

Il faut donc cliquer sur « Déployer avec la stratégie de groupe »



Nous allons administrer une GPO dans un OU souhaité



Nous sélectionnerons utilisateur auxquels cet objet de stratégie de groupe (par utilisateur)
puis cliquer sur Ajouter :

Déployer avec la stratégie de groupe

Nom de l'imprimante :

Objet de stratégie de groupe
Nom d'objet de stratégie de groupe :

Parcourir...

Déployer cette connexion d'imprimante comme suit :
☒ Utilisateurs auxquels s'applique cet objet de stratégie de groupe (par utilisateur)
☐ Ordinateurs auxquels s'applique cet objet de stratégie de groupe (par ordinateur)

Nom de l'imprimante	Objet stratégie de groupe	Type de connexion

Supprimer
Supprimer tout

OK Annuler Appliquer

Déployer avec la stratégie de groupe

Nom de l'imprimante :

Objet de stratégie de groupe
Nom d'objet de stratégie de groupe :

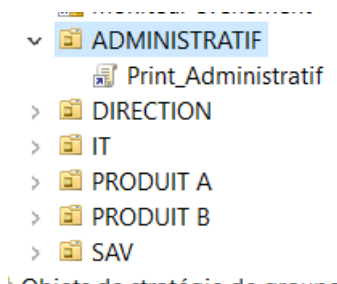
Parcourir...

Déployer cette connexion d'imprimante comme suit :
☐ Utilisateurs auxquels s'applique cet objet de stratégie de groupe (par utilisateur)
☐ Ordinateurs auxquels s'applique cet objet de stratégie de groupe (par ordinateur)

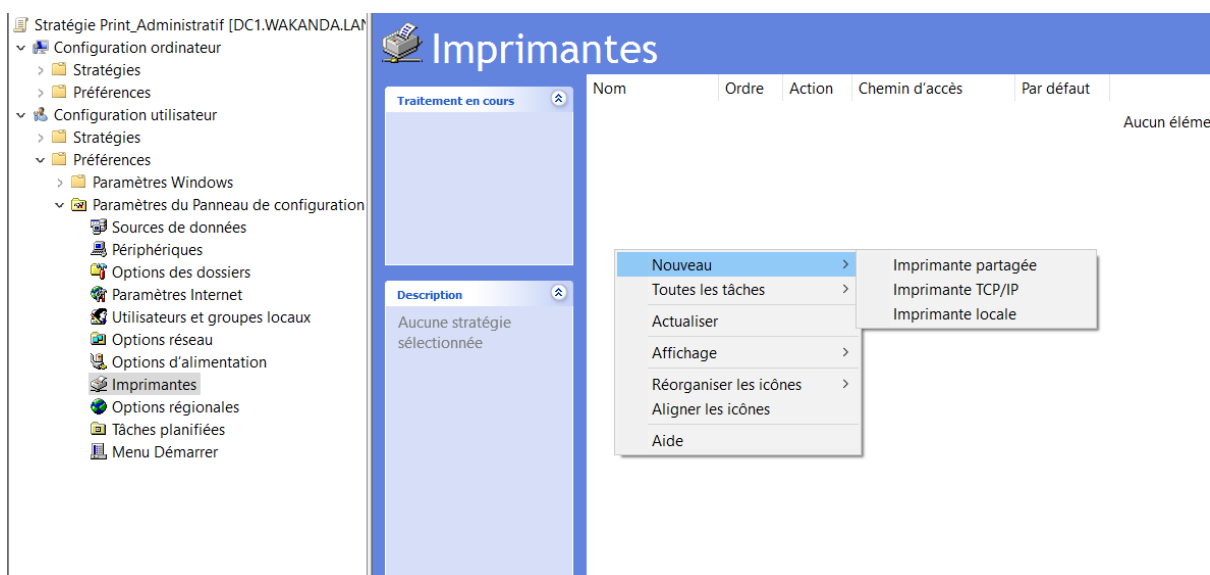
Nom de l'imprimante	Objet stratégie de groupe	Type de connexion
\\SIMP\Print_Administratif	Print_Administratif	Par utilisateur

Supprimer
Supprimer tout
OK Annuler Appliquer

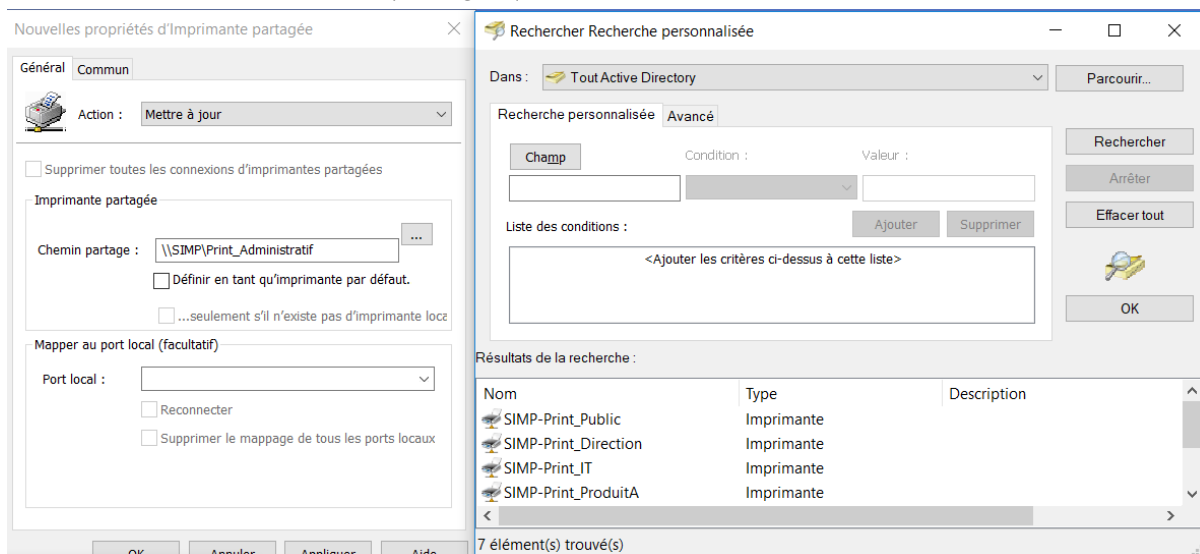
Nous irons donc chercher la GPO précédemment créée qui se situe dans la console de gestion des stratégies de groupe



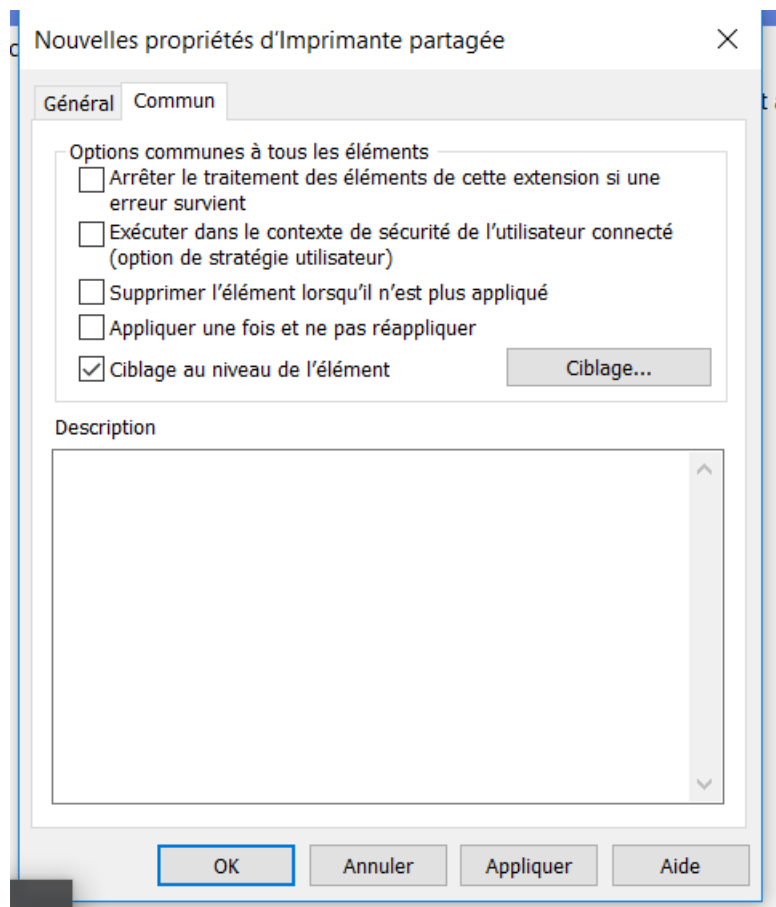
Nous allons créer une imprimante partagée dans la configuration utilisateur :



Nous mettrons le chemin de partage que l'on souhaite :



Nous irons également cibler les utilisateurs concernés ou le groupe souhaité



« En dehors de la direction, des services informatiques, personne ne peut installer de logiciels sur sa machine »

Nous avons paramétré un paramètre de stratégie empêche les utilisateurs d'installer des programmes à partir de médias amovibles.

Et un paramètre de stratégie indique à Windows Installer d'utiliser des autorisations élevées lors de l'installation d'un programme sur le système.

interdite installation logiciel 1

Etendue Détails Paramètres Délégation

interdire installation logiciel 1
Données recueillies le : 21/08/2018 16:05:33 afficher tout

Configuration ordinateur (activée) masquer

Aucun paramètre n'est défini.

Configuration utilisateur (activée) masquer

Stratégies masquer

Modèles d'administration masquer

Définitions de stratégies (fichiers ADMX) récupérées à partir de l'ordinateur local.

Composants Windows/Windows Installer masquer

Stratégie	Paramètre	Commentaire
Éviter l'utilisation de la source de média amovible pour toutes les installations	Activé	
Toujours installer avec des droits élevés	Activé	

Pour être appliqué, ce paramètre de stratégie doit être activé pour l'ordinateur et l'utilisateur.

« Les lecteurs disquette et CD sont désactivés sur les postes des services Produit A et B

o Les services Produit A et B, SAV ne peuvent parcourir ou ouvrir les dossiers ou fichiers à partir d'une disquette ou d'un disque compact »

interdiction CD/disquette

Etendue Détails Paramètres Délégation

interdiction CD/disquette
Données recueillies le : 21/08/2018 16:10:26 afficher tout

Configuration ordinateur (activée) masquer

Aucun paramètre n'est défini.

Configuration utilisateur (activée) masquer

Stratégies masquer

Modèles d'administration masquer

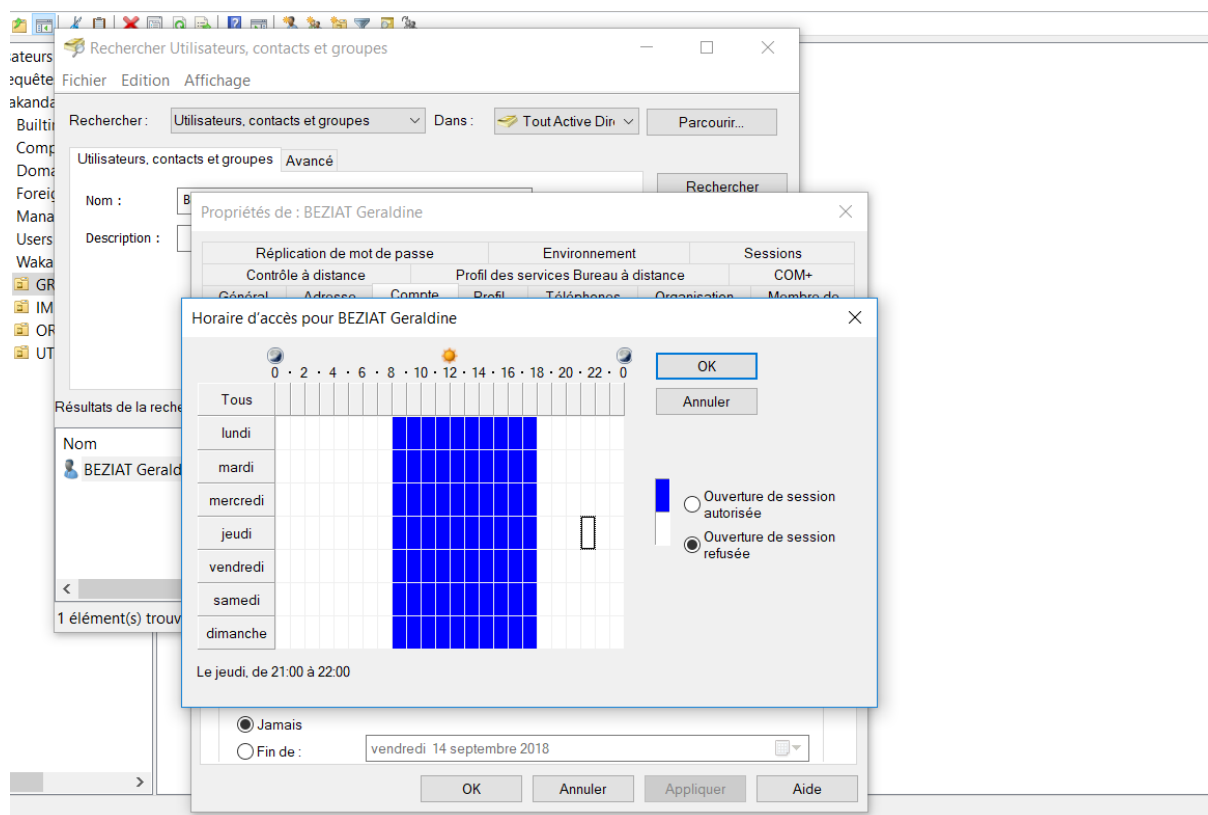
Définitions de stratégies (fichiers ADMX) récupérées à partir de l'ordinateur local.

Système/Accès au stockage amovible masquer

Stratégie	Paramètre	Commentaire
CD et DVD : refuser l'accès en écriture	Activé	
CD et DVD : refuser l'accès en lecture	Activé	
Disques amovibles : refuser l'accès en écriture	Activé	
Disques amovibles : refuser l'accès en lecture	Activé	
Lecteurs de disquettes : refuser l'accès en écriture	Activé	
Toutes les classes de stockage amovible : refuser tous les accès	Activé	

« Mme BEZIAT, ELLA, AYO et ACIEN ne peuvent se connecter qu'entre 08 heures et 18 heures et à 19 heures elles doivent être déconnectées (elles sont du service Produit A) »

Nous avons donc défini dans l'active directory (Propriété du profil) des Horaires D'accès



Et afin qu'elles soient déconnectées à 19h, nous avons en place deux tâches planifiées :

- Une qui prévient l'utilisateur qu'il va être déconnecter
- L'autre qui éteint la session de l'utilisateur

Pour accéder aux tâches planifiées il faut se rendre donc dans :

Configuration Utilisateurs – Préférence – Paramètre du panneau de configuration – Tâche planifiée

Voici la configuration de la première tâche :

Propriétés de : Déconnexion

Général Déclencheurs Actions Conditions Paramètres Commun

Action : Mettre à jour

Nom : Message déconnexion

Auteur : WAKANDA\Administrateur

Description :

Options de sécurité

Lors de l'exécution de la tâche, utilisez le compte d'utilisateur suivant :

NT AUTHORITY\System

Utilisateur ou groupe...

☒ N'exécuter que si l'utilisateur est connecté

☐ Exécuter même si l'utilisateur n'est pas connecté

☐ Ne pas stocker le mot de passe. La tâche n'aura accès qu'aux ressources locales.

☒ Exécuter avec les privilèges les plus élevés

☐ Masquer

Configurer pour : Windows Vista™ ou Windows Server™ 2008

OK Annuler Appliquer Aide

Nouveau déclencheur

Commencer la : À l'heure programmée

Paramètres

☐ Une fois
☐ Tous les jours
☒ Hebdomadaire
☐ Tous les mois

Démarrage : 19/08/2018 18:30:00 ☒ Synchroniser fuseaux horaires

Répéter toutes : 1 semaines,

☐ dimanche ☒ Lundi ☒ mardi ☒ Mercredi
☒ jeudi ☒ vendredi ☐ Samedi

Paramètres avancés

☐ Report maximal de la tâche (aléatoire) : 1 heure
☒ Répéter la tâche toutes les : 5 minutes pour une durée de : 30 minutes
☐ Arrêter toutes les tâches à l'issue de la durée de répétition
☐ Arrêter la tâche si elle s'exécute plus de : 3 jours
☐ Expiration : 19/08/2018 16:37:23 ☐ Synchroniser fuseaux horaires
☒ Activée

OK Annuler

Nouvelles propriétés de Tâche (au minimum Windows 7)

Général Déclencheurs Actions Conditions Paramètres Commun

Lorsque vous créez une tâche, vous pouvez lui assigner une action.

Action : Afficher un message

Nouveau... Modifier...

Nouvelle action

Vous devez spécifier l'action que cette tâche effectuera.

Action : Afficher un message

Paramètres

Cette action affiche un message sur le Bureau.

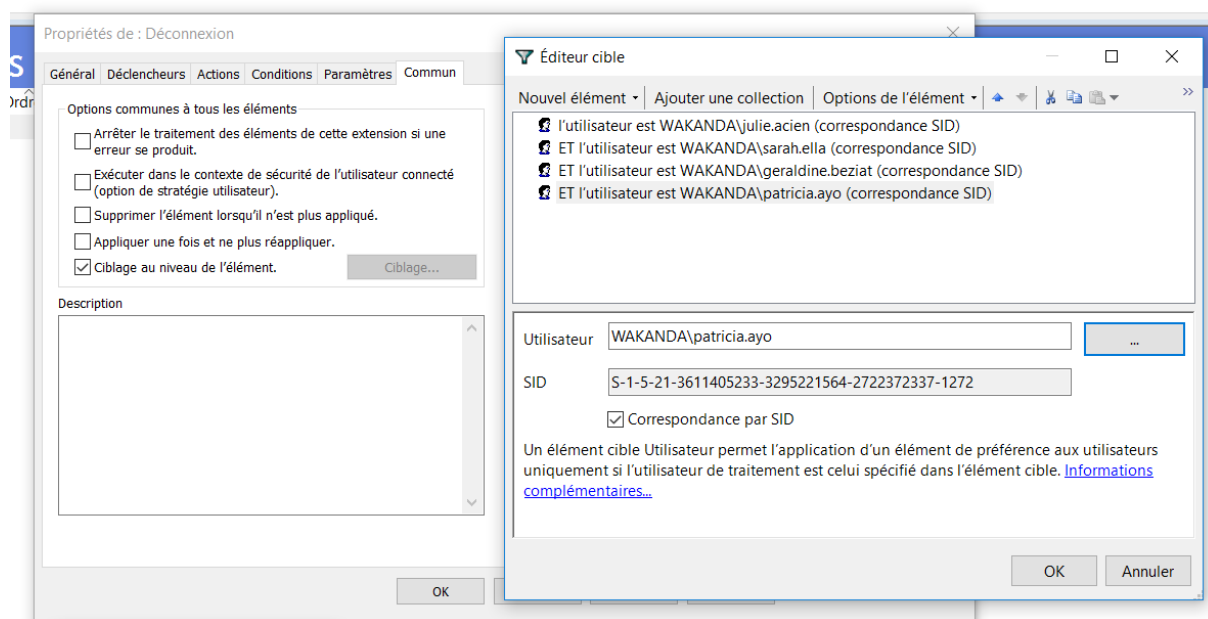
Titre : Déconnexion

Message : Vous allez être déconnecté

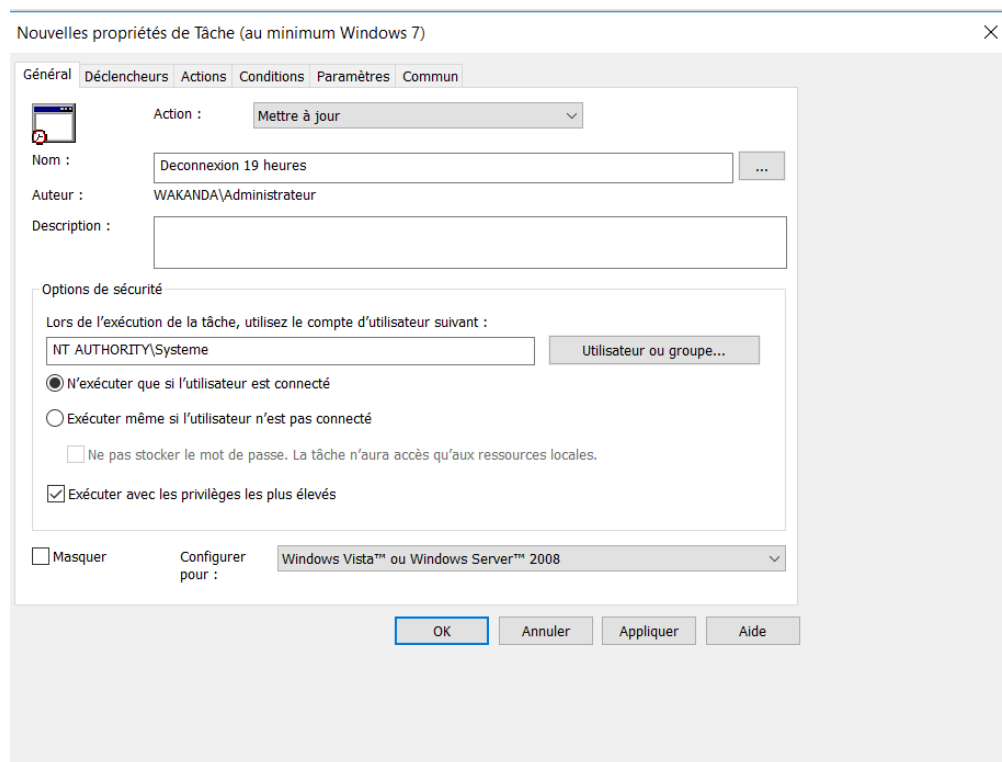
OK Annuler

Utilisateurs et ordinateurs Activ...

Une fois le paramétrage de ces tâches nous allons faire un « ciblage » d'un groupe d'utilisateur en l'occurrence les personnes précédemment nommées



Et ensuite la tâche qui concerne la déconnexion de l'utilisateur :



Nouveau déclencheur

Commencer la : À l'heure programmée

Paramètres

☐ Une fois
☐ Tous les jours
☒ Hebdomadaire
☐ Tous les mois

Démarrage : 19/08/2018 19:00:00 ☒ Synch. fuseaux horaires

Répéter toutes : 1 semaines,

☐ dimanche ☒ Lundi ☒ mardi ☒ Mercredi
☒ jeudi ☒ vendredi ☐ Samedi

Paramètres avancés

☐ Report maximal de la tâche (aléatoire) : 1 heure
☐ Répéter la tâche toutes les : 1 heure pour une durée de : 1 jour
☐ Arrêter toutes les tâches à l'issue de la durée de répétition
☐ Arrêter la tâche si elle s'exécute plus de : 3 jours

☐ Expiration : 21/08/2018 14:38:12 ☐ Synch. fuseaux horaires
☒ Activée

OK Annuler

En Action nous sélectionnerons un script permettant la déconnexion de l'utilisateur

Nouvelle action

Vous devez spécifier l'action que cette tâche effectuera.

Action : Démarrer un programme

Paramètres

Programme/script : \\DC1\sysvol\wakanda.lan\scripts\logoff Parcourir...

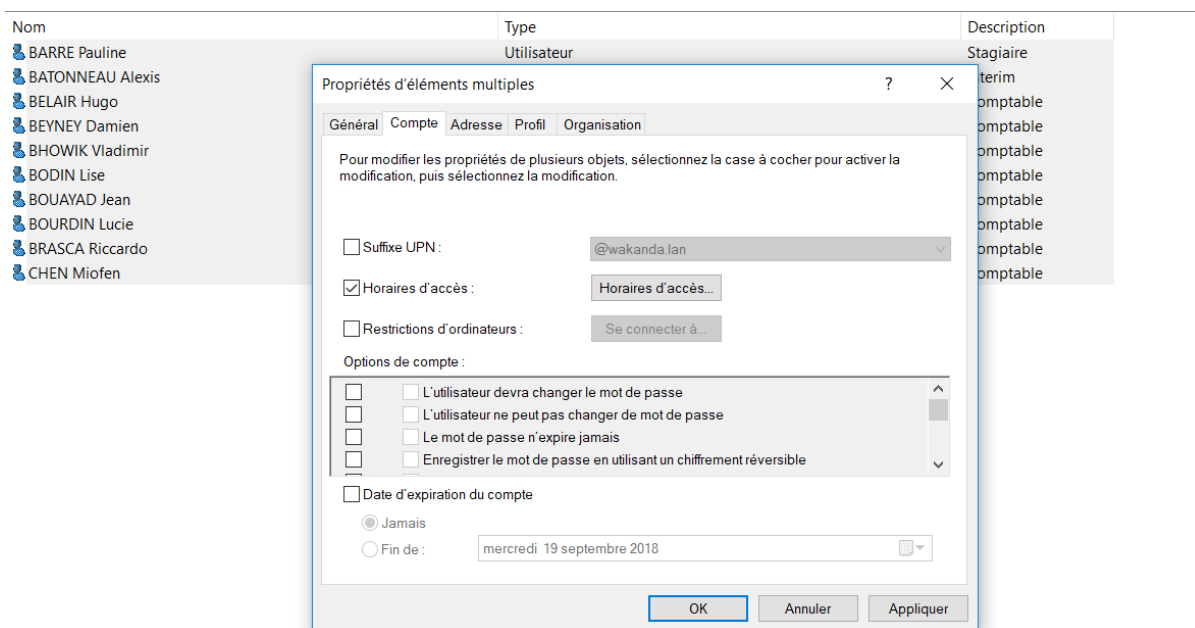
Ajouter arguments (facult.) :

Commencer dans :

OK Annuler

« Aucun salarié sauf la direction, le SAV et l'informatique ne peut se connecter entre 20 heures et 07 heures du matin »

Nous avons donc paramétré les horaires d'accès avec une sélection multiple et via clique droit > Propriété > Compte > on coche horaire d'accès et on paramètre autant aux heures que l'on souhaite :



Nous avons également donc mis en place un groupe dans l'OU « GROUPE » qui regroupe tous les utilisateurs ayant une plage horaire de 7h à 20h, et nous y avons appliqué une GPO

gpo deco 7h-20h	
Étendue	Détails Paramètres Délégation
gpo deco 7h-20h	
Données recueillies le : 20/08/2018 20:50:59	
afficher tout	
Configuration ordinateur (activée)	
masquer	
Stratégies	
masquer	
Paramètres Windows	
masquer	
Paramètres de sécurité	
masquer	
Stratégies locales/Options de sécurité	
masquer	
Serveur Réseau Microsoft	
masquer	
Stratégie	Paramètre
Serveur réseau Microsoft : déconnecter les clients à l'expiration du délai de la durée de session	Activé
Configuration utilisateur (activée)	
masquer	
Aucun paramètre n'est défini.	

Ce paramètre de sécurité détermine s'il faut déconnecter les utilisateurs qui sont connectés à l'ordinateur local en dehors des heures d'ouverture de session valides du compte de l'utilisateur.

« En dehors de la direction, des services informatiques, personne modifier l'heure sur sa machine »

Nous avons donc déployer qui regroupe uniquement la direction et le service informatique :

gpo deco 7h-20h	
Étendue	Détails Paramètres Délégation
gpo deco 7h-20h	
Données recueillies le : 20/08/2018 20:50:59	
afficher tout	
Configuration ordinateur (activée)	
masquer	
Stratégies	
masquer	
Paramètres Windows	
masquer	
Paramètres de sécurité	
masquer	
Stratégies locales/Options de sécurité	
masquer	
Serveur Réseau Microsoft	
masquer	
Stratégie	Paramètre
Serveur réseau Microsoft : déconnecter les clients à l'expiration du délai de la durée de session	Activé
Configuration utilisateur (activée)	
masquer	
Aucun paramètre n'est défini.	

Ce droit d'utilisateur détermine quels utilisateurs et groupes peuvent changer la date et l'heure sur l'horloge interne de l'ordinateur.

« Configurer au moins 3 journaux à 3 jours »

3 journaux

Étendue Détails Paramètres Délégation

Données recueillies le : 21/08/2018 16:19:05

Configuration ordinateur (activée) [masquer](#)

Stratégies [masquer](#)

Paramètres Windows [masquer](#)

Paramètres de sécurité [masquer](#)

Journal des événements [masquer](#)

Stratégie	Paramètre
Conserver le journal de sécurité	3 jours
Conserver le journal des applications	3 jours
Conserver le journal système	3 jours
Méthode de conservation du journal de sécurité	Par jour
Méthode de conservation du journal des applications	Par jour
Méthode de conservation du journal système	Par jour

Configuration utilisateur (activée) [masquer](#)

Aucun paramètre n'est défini.

o « Désactiver le moniteur d'évènements »

moniteur evenement

Étendue Détails Paramètres Délégation

Données recueillies le : 16/08/2018 20:50:58

Configuration ordinateur (activée) [masquer](#)

Stratégies [masquer](#)

Modèles d'administration [masquer](#)

Définitions de stratégies (fichiers ADMX) récupérées à partir de l'ordinateur local.

Système [masquer](#)

Stratégie	Paramètre	Commentaire
Afficher le moniteur d'événements de mise hors tension	Désactivé	

Configuration utilisateur (activée) [masquer](#)

Aucun paramètre n'est défini.

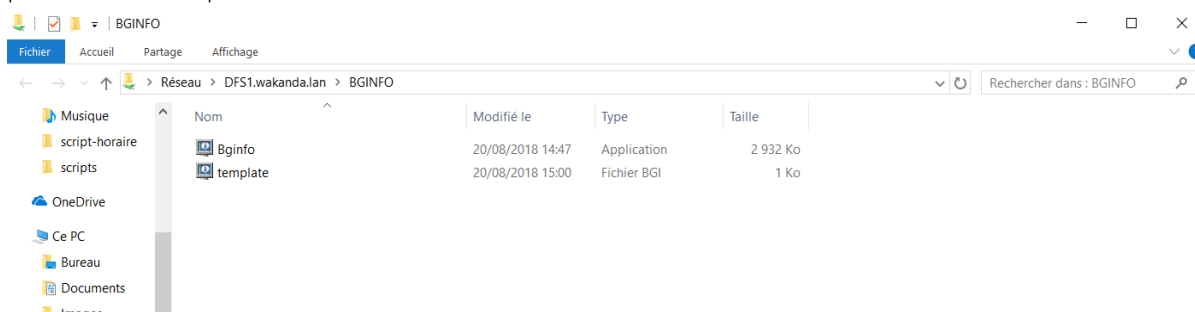
« Déploiement de BG info : »

Nous avons décider de deployer également BGinfo qui est un petit utilitaire qui permet d'afficher différents paramètre souhaité sur le fond d'écran, ce qui peut aider pour l'administration à distance : visibilité direct du nom de la machine, nom du domain par exemple.

Pour l'installation, nous avons crée un partage sur notre DFS1 nommé BGinfo

DFS1 (5)			
commun	Nouveau partage...	SMB	Non-cluster
perso	Actualiser	SMB	Non-cluster
public	C:\DFSRoots\public	SMB	Non-cluster
services	E:\services	SMB	Non-cluster
BGINFO	C:\Shares\BGINFO	SMB	Non-cluster

A l'intérieur de ce partage nous avons insérer « BGinfo.exe » ainsi qu'un template préalablement paramétrer.



Nous avons ensuite créé un script dans le but de le déployer lors de la connexion de chaque utilisateur :

```
1 \\DFS1.wakanda.lan\BGINFO\Bginfo.exe /accepteula \\DFS1.wakanda.lan\BGINFO\template.bgi /timer:0
```

EXPLIQUER LE SCRIPT

[\\DFS1.wakanda.lan\BGINFO\Bginfo.exe](#) = le chemin de l'exécutable

/accepteula = il est demandé à l'utilisateur d'approuver ou refuser « l'End User Licence Agreement », avec cette commande ce sera accepté directement

[\\DFS.wakanda.lan\BGINFO\template.bgi](#) = le chemin de notre template

/timer :0 = aucun temps d'attente

Ensuite, une GPO sera créé dans notre domaine pour que chaque utilisateur dispose de cette utilitaire, premièrement nous configurons « le délai des scripts d'ouverture de session »

Configurer le délai des scripts d'ouverture de session

Paramètre précédent Paramètre suivant

☐ Non configuré ☒ Activé ☐ Désactivé

Commentaire :

Pris en charge sur : Au minimum Windows Server 2012 R2, Windows 8.1 ou Windows RT 8.1

Options : minute : 0

Aide :

Entrez « 0 » pour désactiver le délai des scripts d'ouverture de session.

Ce paramètre de stratégie vous permet de configurer la durée pendant laquelle le client de la stratégie de groupe attend après l'ouverture de

Étendue Détails Paramètres Délégation

BGINFO
Données recueillies le : 20/08/2018 15:25:02 afficher tout

Configuration ordinateur (activée) masquer

Stratégies masquer

Modèles d'administration afficher

Configuration utilisateur (activée) masquer

Stratégies masquer

Paramètres Windows masquer

Scripts masquer

Ouvrir la session masquer

For this GPO, Script order: Les scripts Windows PowerShell s'exécuteront en premier.

Nom	Paramètres
\\Dc1\sysvol\wakanda.lan\scripts\BGINFO script.ps1	

Et ci-dessus le script d'ouverture de session pour chaque utilisateur qui pointe vers le script précédemment expliqué

- L. Accès à distance
- M. Création des scripts

III. LES SERVEURS LINUX

A. Installation de l' environnement

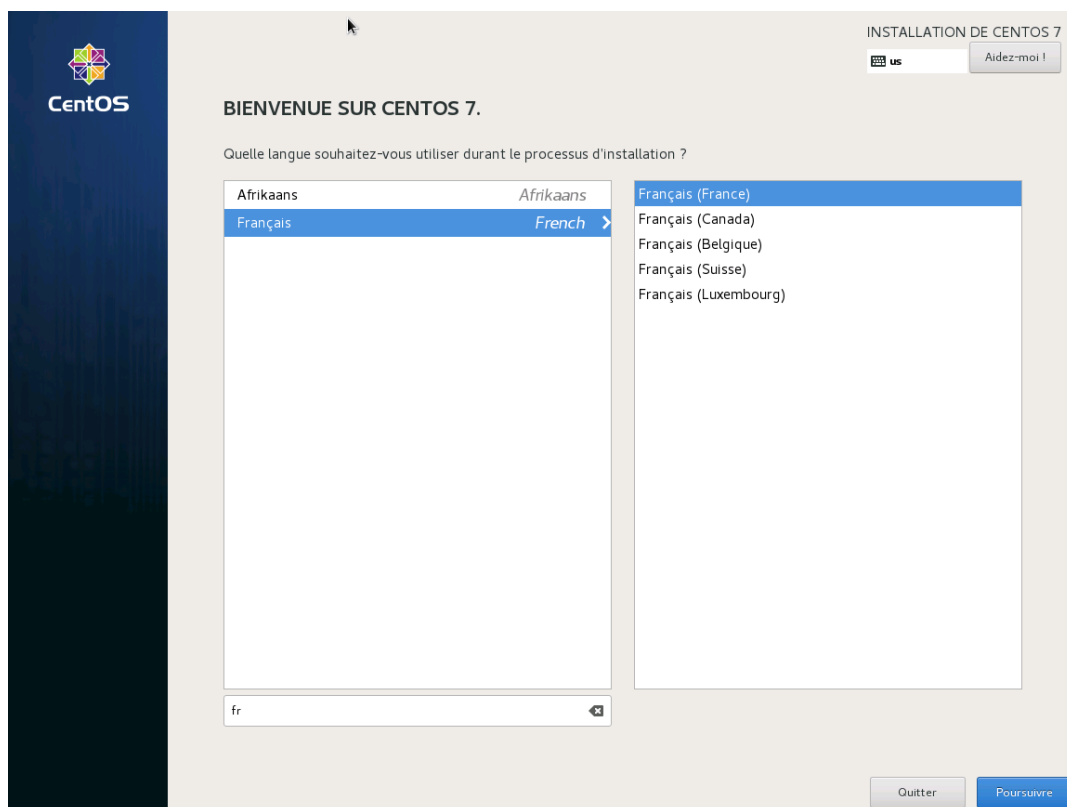
Dans ce projet nous utiliserons le système d'exploitation CentOS de la distribution GNU/Linux.

En effet ce système d'exploitation est le plus utilisée pour les entreprises pour des raisons de stabilité et de sécurité.

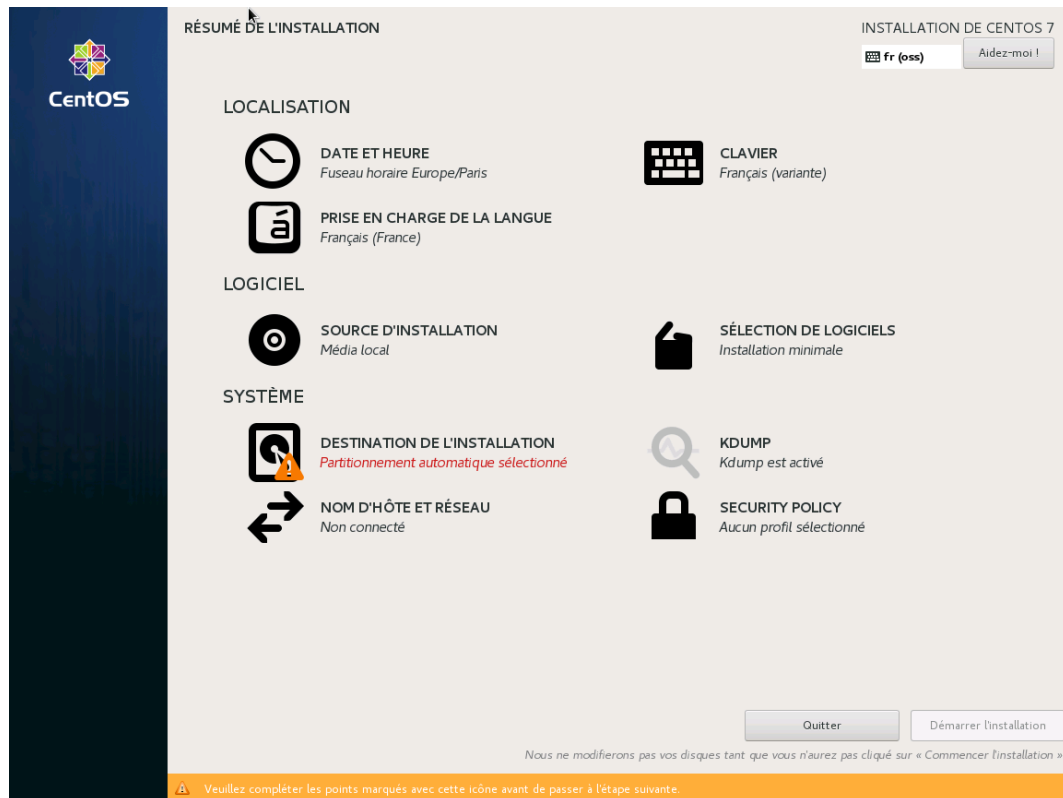
Nous utiliserons pour ce projet la version 7 de CentOS.

1. Partitionnement

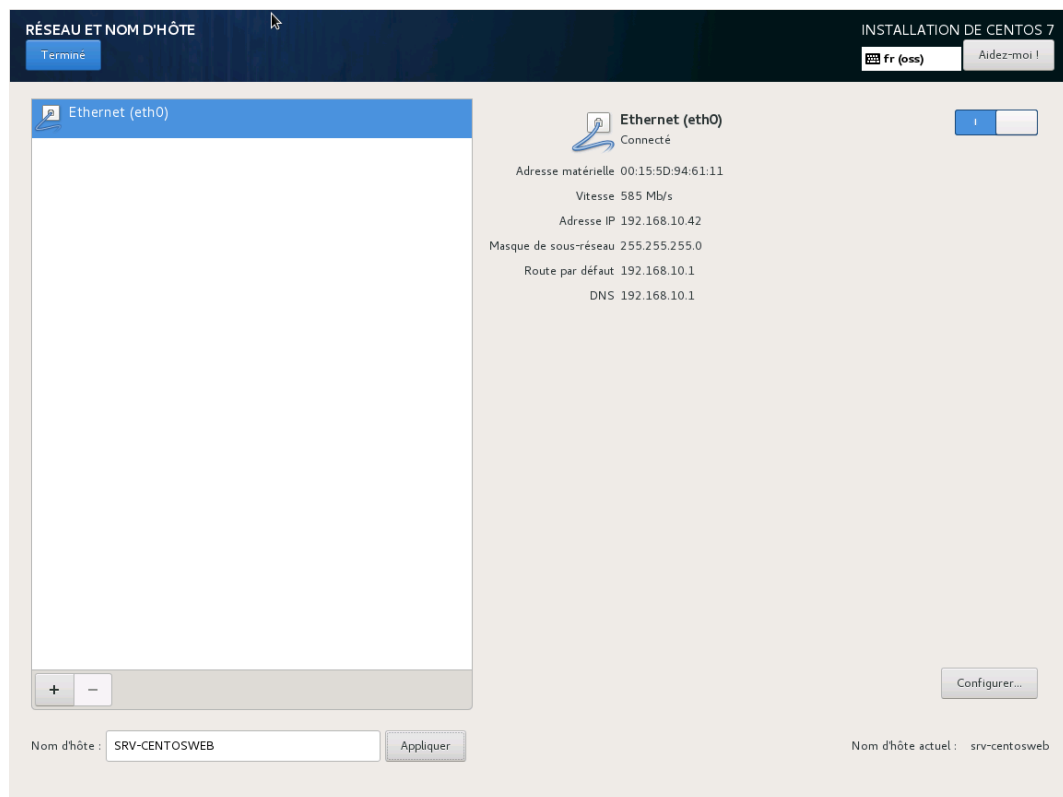
- Choisir la langue « Français »



- Vérifier les valeurs de localisation



- Définir le nom d'hôte et activer la carte réseau



- Dans général « se connecter à ce réseau » et passer « Paramètres IPV6 » en mode ignorer.

► Configurer le partitionnement en mode manuel

CIBLE DE L'INSTALLATION

Termine

INSTALLATION DE CENTOS 7

Fr (oss)


Aidez-moi !

Sélection des périphériques

Sélectionnez le périphérique sur lequel vous souhaitez faire l'installation. Il restera intact jusqu'à ce que vous cliquiez sur le bouton « Commencer l'installation » du menu principal.

Disques locaux standards


127 GiO



Msft Virtual Disk
sda / 127 GiO d'espace libre

Les disques décochés ne seront pas modifiés.

Disques spéciaux et réseau



Ajouter un disque...

Les disques décochés ne seront pas modifiés.

Autres options de stockage

Partitionnement

☐ Configurer automatiquement le partitionnement.
☒ Je vais configurer le partitionnement.

☐ Je voudrais libérer plus d'espace.

Chiffrement

☐ Chiffrer mes données. Vous définirez une phrase de passe plus tard.

[Résumé complet du disque et du chargeur de démarrage...](#)

1 disque sélectionné ; 127 GiO de capacité ; 127 GiO d'espace libre [Rafraichir...](#)

- LVM (Logical Volume Manager, ou gestionnaire de volumes logiques en français) permet la création et la gestion de volumes logiques sous Linux. L'utilisation de volumes logiques remplace en quelque sorte le partitionnement des disques.
- IL est conseillé de séparer les dossiers qui hébergent des données pouvant évoluer trop rapidement et bloquer le système d'exploitation.

- Choisir LVM et cliquer « Cliquer ici pour créer automatiquement »
- Installation du serveur en mode LVM en séparant les dossier /var, /home, swap
- Choisir les paquets d'installation, « installation minimale »

2. Configuration Réseau

- Afin de configurer les paramètres réseaux nous utiliserons l'utilitaire nmtui.

B. Configuration de base et intégration dans l' AD

1. Mise à jour et intégration de l' autocomplétions

- Réalisation des mises à jour

```
yum upgrade -y
```

- Installation de l'autocomplétions

```
yum install bash-completion -y
```

2. Intégration dans l' AD

- Paquets à installer pour de l'intégration CENTOS 7 dans active directory

```
yum install realmd oddjob oddjob-mkhomedir sssd adcli openldap-clients  
policycoreutils-python samba-common samba-common-tools krb5-workstation ntp -  
y
```

```

libcgroupp                               x86_64
libdhash                                 x86_64
libipa_hbac                              x86_64
libkadm5                                 x86_64
libsemanage-python                       x86_64
libsmclient                              x86_64
libsss_autofs                             x86_64
libsss_certmap                           x86_64
libsss_idmap                             x86_64
libsss_nss_idmap                         x86_64
libsss_sudo                              x86_64
ntpdate                                  x86_64
psmisc                                   x86_64
python-IPy                               noarch
python-sssdconfig                        noarch
setools-libs                             x86_64
sssd-ad                                  x86_64
sssd-client                              x86_64
sssd-common                              x86_64
sssd-common-pac                          x86_64
sssd-ipa                                  x86_64
sssd-krb5                                x86_64
sssd-krb5-common                         x86_64
sssd-ldap                                 x86_64
sssd-proxy                               x86_64

Résumé de la transaction
=====
Installation    9 Paquets (+33 Paquets en dépendance)

Taille totale des téléchargements : 9.7 M
Taille d'installation : 22 M
Is this ok [y/d/N]:

```

- Ajouter la résolution IP/AD dans le fichier hosts

```

127.0.0.1    localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6
192.168.48.10 dc1.wakanda.lan dc1

```

- Synchroniser l'heure du serveur avec le DC en modifiant le fichier ntp.conf (ligne 25)

```

19 # Use public servers from the pool.ntp.org project.
20 # Please consider joining the pool (http://www.pool.ntp.org/join.html).
21 #server 0.centos.pool.ntp.org iburst
22 #server 1.centos.pool.ntp.org iburst
23 #server 2.centos.pool.ntp.org iburst
24 #server 3.centos.pool.ntp.org iburst
25 server dc1.wakanda.lan iburst

```

- Lancer le service et configurer son lancement dès le démarrage

```
[root@SRV-SMB-NFS ~]# systemctl enable ntpd
Created symlink from /etc/systemd/system/multi-user.target.w
/usr/lib/systemd/system/ntpd.service.
[root@SRV-SMB-NFS ~]# systemctl start ntpd
[root@SRV-SMB-NFS ~]#
```

- Ajouter l'ordinateur au domaine

```
realm join --user=administrateur dc1.wakanda.lan
```

```
[root@SRV-SMB-NFS ~]# realm join --user=administrateur dc1.wakanda.lan
Password for administrateur:
[root@SRV-SMB-NFS ~]# realm list
wakanda.lan
  type: kerberos
  realm-name: WAKANDA.LAN
  domain-name: wakanda.lan
  configured: kerberos-member
  server-software: active-directory
  client-software: sssd
  required-package: oddjob
  required-package: oddjob-mkhomedir
  required-package: sssd
  required-package: adcli
  required-package: samba-common-tools
  login-formats: %U@wakanda.lan
  login-policy: allow-realm-logins
```

C. Les serveurs de fichiers

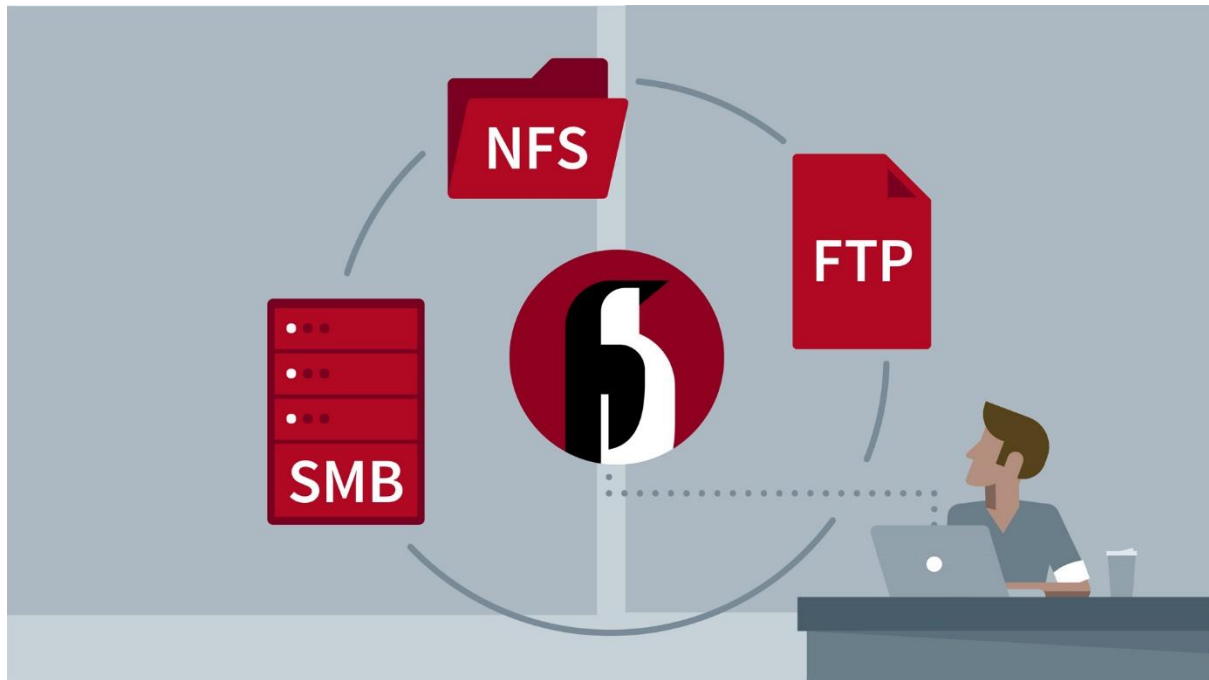
Comme demandé dans le cahier des charges nous allons mettre en place 3 protocoles de partages de répertoires sous Linux.

Nous allons répartir ces protocoles sur deux serveurs :

Un serveur FTP qui contiendra un client Nfs avec une sauvegarde automatique des données et le service ftpd.

Un autre serveur contiendra les deux autres protocoles (Samba et NFS).

Pour les étapes d'installations complètes des serveurs veuillez-vous référer aux annexes.



1. Le service FTP

File Transfer Protocol (protocole de transfert de fichier), ou FTP, est un protocole de communication destiné au partage de fichiers sur un réseau TCP/IP. Il permet, depuis un ordinateur, de copier des fichiers vers un autre ordinateur du réseau, ou encore de supprimer ou de modifier des fichiers sur cet ordinateur.



La mise en place d'un serveur FTP dans notre infrastructure nous permettra d'avoir une plateforme sécurisée d'échange entre linux et Windows.

2. Le service Samba

Le logiciel Samba est un outil permettant de partager des dossiers et des imprimantes à travers un réseau local. Il permet de partager et d'accéder aux ressources d'autres ordinateurs fonctionnant avec des systèmes d'exploitation Microsoft Windows et Apple Mac OS X, ainsi que des systèmes GNU/Linux, dans lesquels une implémentation de Samba est installée.

Pour partager de manière simple des ressources entre plusieurs ordinateurs, l'utilisation de Samba est conseillée.



3. Le service NFS

Network File System (ou NFS), littéralement *système de fichiers en réseau* qui permet à un ordinateur d'accéder via un réseau à des fichiers distants. Ce système de fichiers en réseau permet de partager des données principalement entre systèmes UNIX. Des versions existent pour Macintosh ou Microsoft Windows.



Ce protocole aura pour rôle d'établir des dossiers partagés uniquement entre système LINUX.

4. Le client NFS et la sauvegarde automatique

Afin de sauvegarder les fichiers NFS nous installerons sur le serveur FTP le client NFS grâce à la commande :

► `yum install -y nfs-utils`

Puis nous avons planifier chaque soir de la semaine un script qui copie les fichiers du dossier partagés Nfs sur un disque du serveur FTP.

```
30 22 * * 1 /home/backup/scripts/backup_lundi.sh
30 22 * * 2 /home/backup/scripts/backup_mardi.sh
30 22 * * 3 /home/backup/scripts/backup_mercredi.sh
30 22 * * 4 /home/backup/scripts/backup_jeudi.sh
30 22 * * 5 /home/backup/scripts/backup_vendredi.sh
```

Nous avons donc des sauvegardes totales des fichiers NFS avec une rétention d'une semaine.

Contenue script sauvegarde lundi :

```
cp -R /mnt/nfs /backup_nfs/lundi/
```

D. Le service DHCP

Dynamic Host Configuration Protocol (DHCP, protocole de configuration dynamique des hôtes) est un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station ou d'une machine, notamment en lui attribuant automatiquement une adresse IP et un masque de sous-réseau. Le service DHCP peut aussi configurer l'adresse de la passerelle par défaut, des serveurs de noms DNS et des serveurs de noms NBNS (connus sous le nom de serveurs WINS sur les réseaux de la société Microsoft).



Dans ce projet nous mettons en place 2 serveurs DHCP Linux CentOS en HA (High-Availability). La haute disponibilité (HA) est un terme souvent utilisé en informatique, à

propos d'architecture de système ou d'un service pour désigner le fait que cette architecture ou ce service a un taux de disponibilité convenable.

Le service DHCP permettant à nos pc clients d'obtenir une adresse IP et donc de communiquer avec le réseau, il nous est donc nécessaire de mettre en place une haute disponibilité sur ce service.

En effet, une interruption du service DHCP sans reprise continue provoquerait un arrêt de production.

IV. LA BASE DE DONNEES

- A. Analyse de la (BDD) base de données
- B. Création et importation de la BDD

V. L' APPLICATION

- A. Site web intranet

- B. Beau gosse GLPI

GLPI (Gestionnaire Libre de Parc Informatique)¹ est un logiciel libre de gestion des services informatiques et de gestion des services d'assistance.



Cette solution libre est éditée en PHP. GLPI est une application web qui aide les entreprises à gérer leur système d'information. Parmi ses caractéristiques, cette solution est capable de construire un inventaire de toutes les ressources de la société.

Les fonctionnalités de cette solution aident les Administrateurs IT à créer une base de données regroupant des ressources techniques et de gestion, ainsi qu'un historique des actions de maintenance. La fonctionnalité de gestion d'assistance ou helpdesk fournit aux utilisateurs un service leur permettant de signaler des incidents ou de créer des demandes, ceci par la création d'un ticket d'assistance.

La mise en place d'un serveur GLPI répond donc à toutes les exigences du cahier des charges et bien plus encore.

En effet nous avons installer le plug in Fusion Inventory sur le serveur GLPI en plus du paquet php-ldap.



Nous avons donc un serveur web avec les fonctionnalités suivantes :

- Inventorisation automatique du parc informatique avec Fusion Inventory dans GLPI.
- Possibilité de créer des tickets GLPI pour des demandes ou des déclarations d'incident après la mise en place du projet.
- Importation des utilisateurs de l'AD avec php-ldap dans GLPI afin que l'accès à l'application soit disponible à tous les utilisateurs avec leurs identifiants Windows.

VI. GLOSSAIRE

AD = Active Directory est la mise en œuvre par Microsoft des services d'annuaire LDAP pour les systèmes d'exploitation Windows.

L'objectif principal d'Active Directory est de fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateurs utilisant le système Windows.

LDAP= Lightweight Directory Access Protocol est à l'origine un protocole permettant l'interrogation et la modification des services d'annuaire (il est une évolution du protocole DAP).

GPO= Le sigle GPO peut se référer à : Group Policy Object ou stratégies de groupe, fonctions de gestion centralisée de Microsoft Windows.

DNS = Le Domain Name System, généralement abrégé DNS, qu'on peut traduire en « système de noms de domaine », est le service informatique distribué utilisé pour traduire les noms de domaine Internet en adresse IP ou autres enregistrements.

DC= Contrôleur de domaine/Domain est le serveur qui centralise la liste des utilisateurs et des machines d'un domaine. Il délivre aussi les autorisations d'accès à ce domaine.

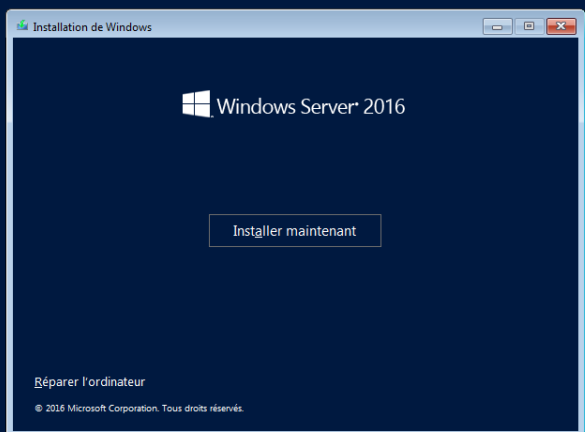
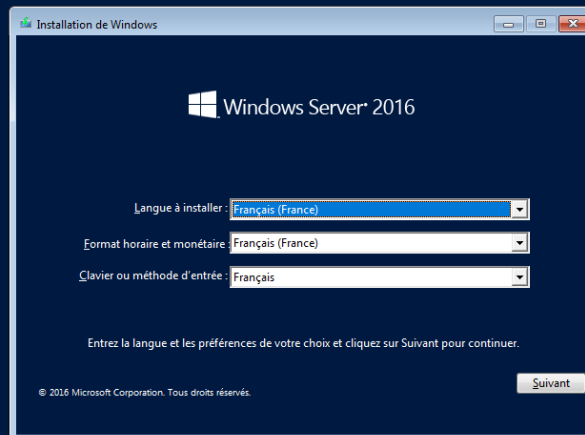
DHCP = protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station ou d'une machine, notamment en lui attribuant automatiquement une adresse IP et un masque de sous-réseau

Serveur FTP = Le serveur FTP permet, comme son nom l'indique, de transférer des fichiers par Internet ou par le biais d'un réseau informatique local

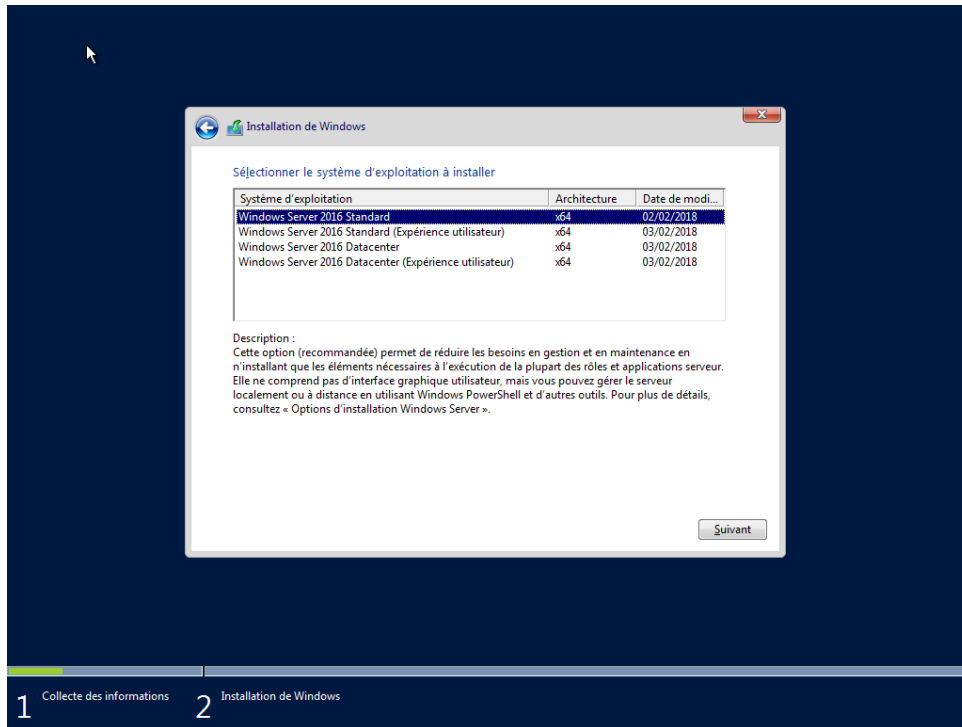
Backup= Une sauvegarde de données

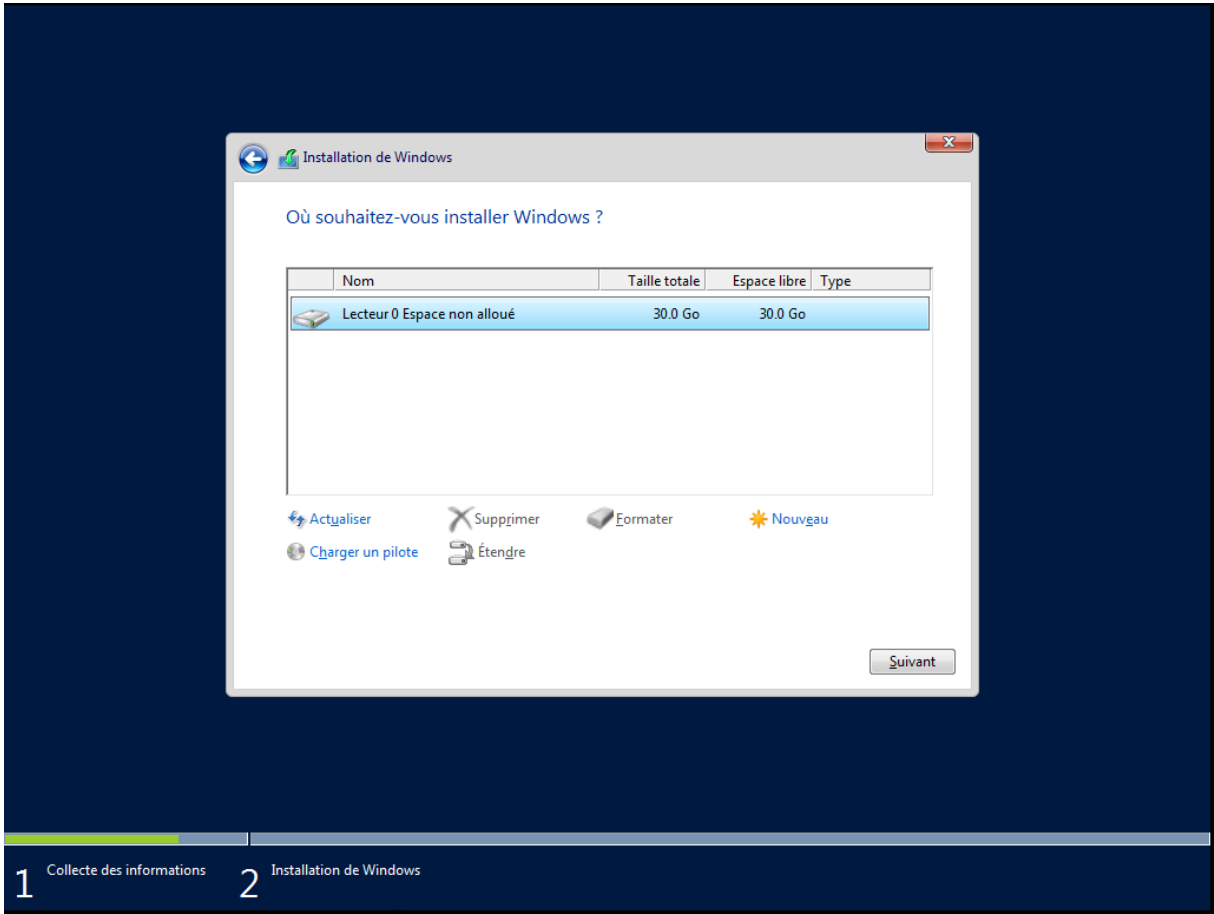
VII. ANNEXES

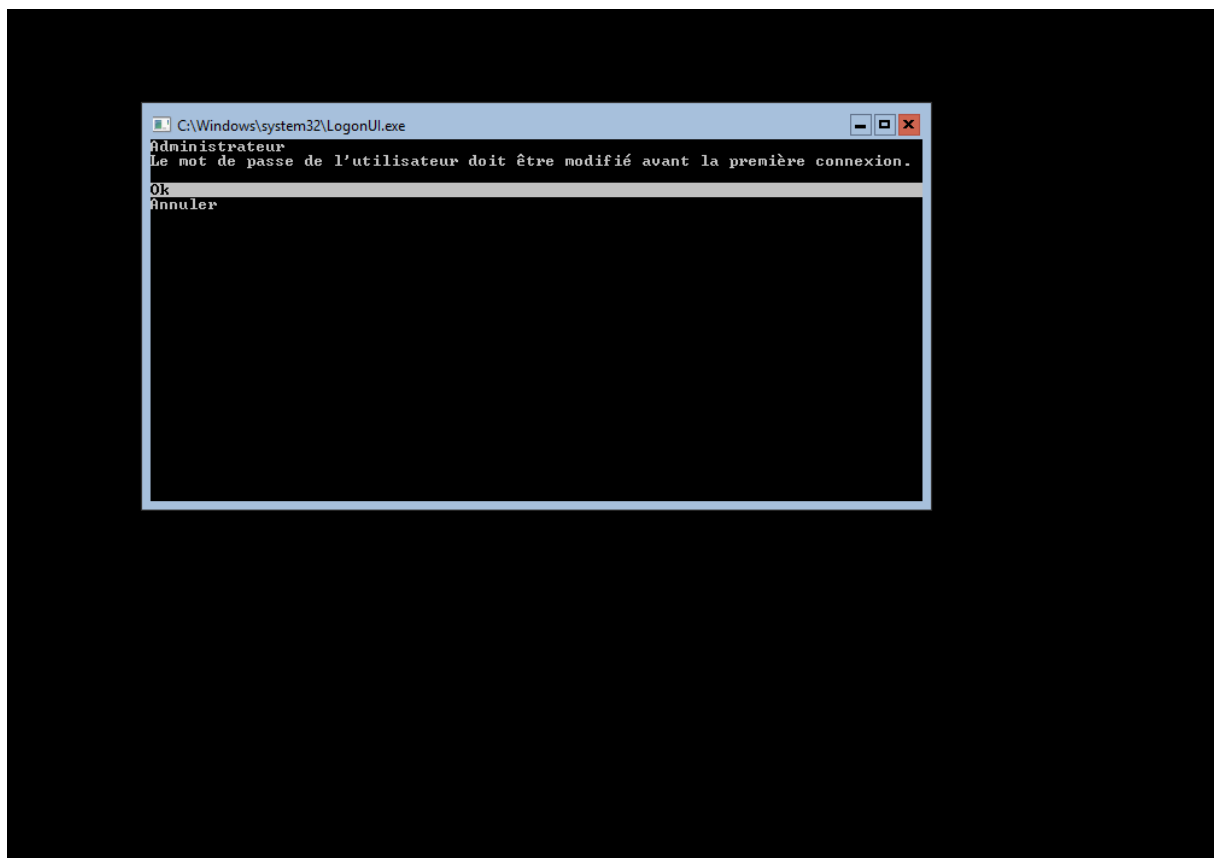
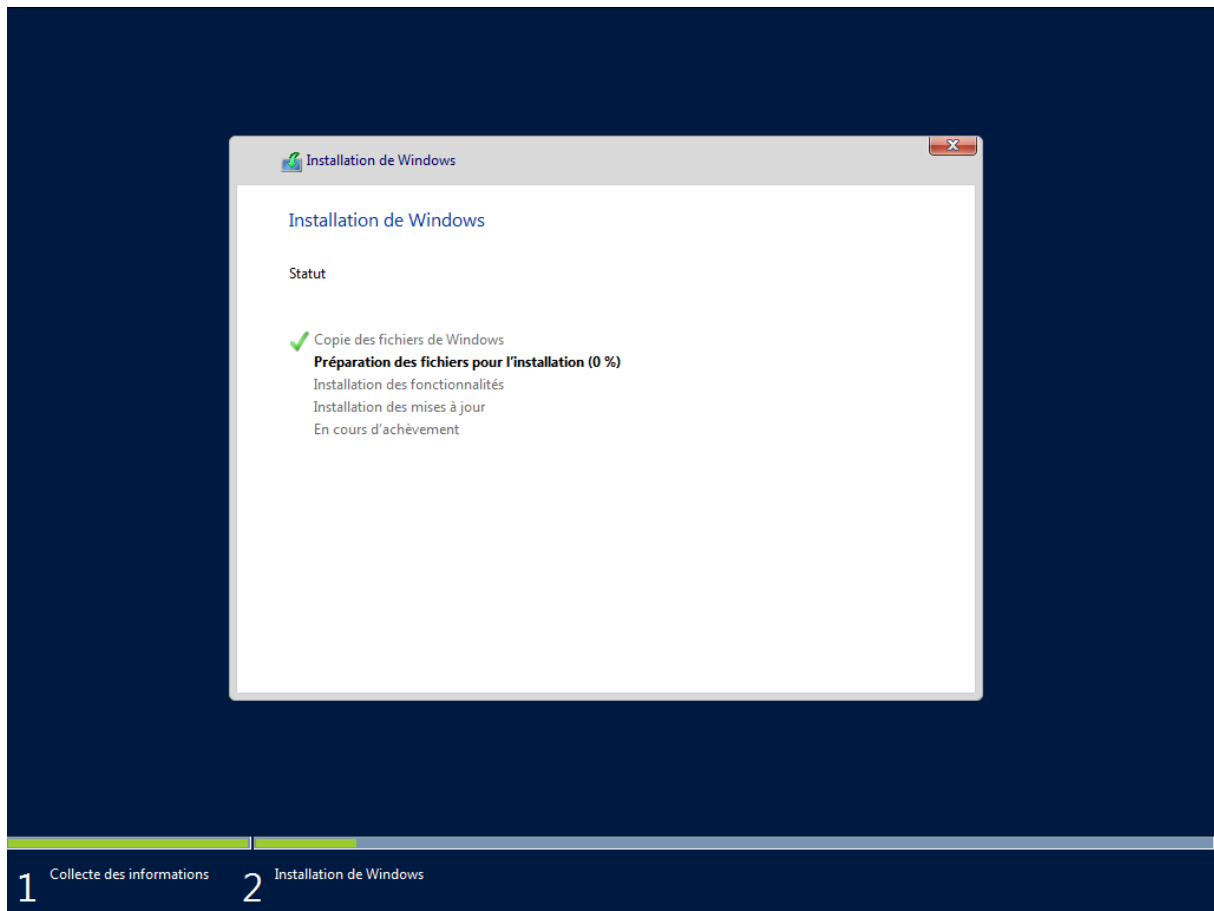
INSTALLATION WINDOWS SERVER



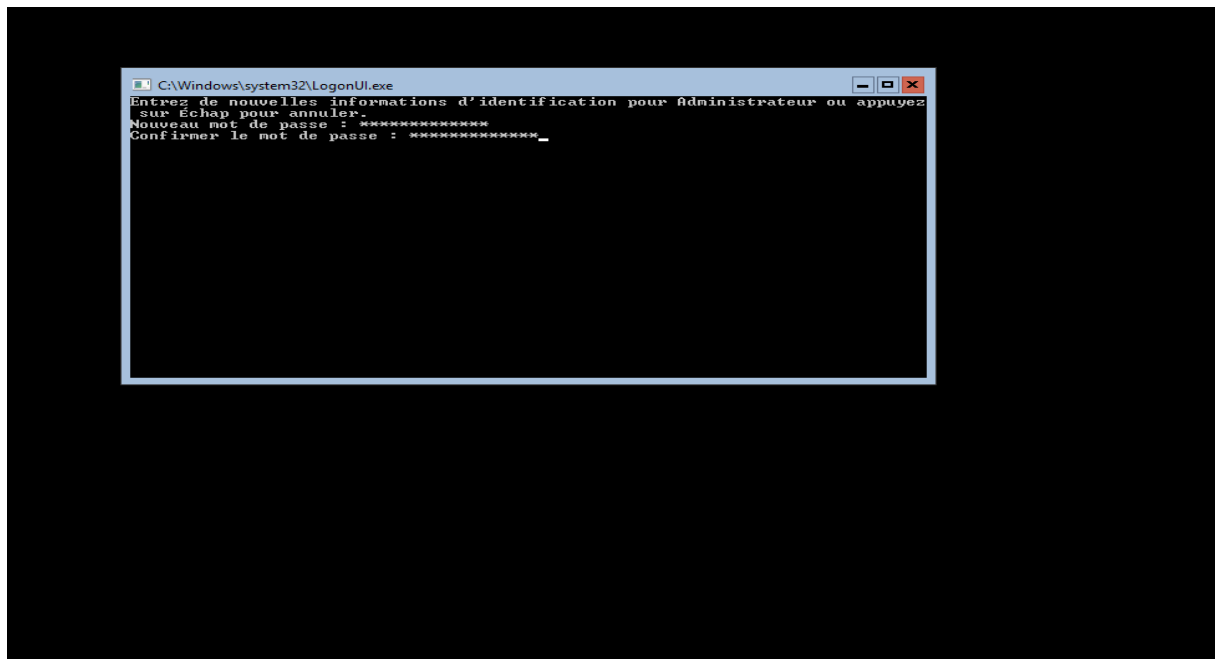
Sélectionner la version souhaitée : Core ou Graphique







Définissions d'un mot de passe



A. Installation serveur Linux

1. Le service DHCP HA

Le service DHCP sera exécuté sur les serveurs SRV-DHCP1 et SRV-DHCP2.

La configuration de ces serveurs est la suivante :

Configuration physique des serveurs SRV-DHCP1 & SRV-DHCP2	
RAM :	2 GB
Nombre de processeur :	1
Nombre de cœurs par processeur :	1
Disque 1 :	20 GB

Dans un premier temps configurons notre serveur SRV-DHCP1 :

- Installation du serveur

```
yum install dhcp -y
```


- Lancer le service au démarrage du serveur

```
systemctl enable dhcpd
```

- Démarrer le service serveur DHCP

```
systemctl start dhcpd
```

- Déblocage du firewall

```
firewall-cmd --add-service=dhcp --permanent
```

```
firewall-cmd --reload
```

- La config du serveur dhcp se trouve dans le fichier:

```
vi /etc/dhcp/dhcpd.conf
```

```
default-lease-time 86400; # Bail de 24H
max-lease-time 172800; # Bail maxi de 48H
# Déclaration d'un réseau
subnet 192.168.48.0 netmask 255.255.255.0 {
    option domain-name-servers      192.168.48.10,192.168.48.18; #DNS
    option routers                   192.168.48.254; # Passerelle
    pool {
        range 192.168.48.100 192.168.48.200;
    }
}
```

Ensuite nous complétons le fichier de configuration avec les arguments ci -dessous :

- failover peer "dhcp-failover"

Nom arbitraire donné à la définition du failover.

- Primary

Le serveur est désigné comme master.

- address 192.168.48.14

L'adresse IP du serveur maître.

- port 647

Port d'écoute du serveur maître pour le DHCP-Failover.

- peer address 192.168.48.20

Adresse IP du partenaire, le serveur DHCP slave, assurant la redondance du service DHCP.

- peer port 647

Port d'écoute du serveur esclave pour le DHCP-Failover.

- max-response-delay 60

Temps en secondes au bout duquel si un des serveurs ne reçoit pas de réponses de son partenaire la connexion sera considérée comme interrompue.

- max-unacked-updates 10

Nombre maximal de messages BNDUPD (un bail a été attribué et doit être synchronisé avec le partenaire) que peut envoyer un des serveurs DHCP sans recevoir d'accusé de réception BNDACK (accusé de réception du bail attribué) de son partenaire. Si ce nombre est dépassé, le partenaire à l'initiative des messages BNDUPD considère la connexion interrompue.

- load balance max seconds 3

Temps au bout duquel, si un client ne reçoit pas de réponse à son message de type DHCPDISCOVER ou DHCPREQUEST par un serveur DHCP, le serveur partenaire prend le relai et traite la demande de ce client.

- mclt 1800

Temps pendant lequel, suite à la défaillance d'un des serveurs DHCP, son partenaire assure seul le rôle de serveur DHCP (délégation temporaire).

- Ajouter les critères de configuration en HA

```
failover peer "dhcp-failover" {
    primary;
    address 192.168.10.251;
    port 647;
    peer address 192.168.10.252;
    peer port 647;
    max-response-delay 60;
```

```
max-unacked-updates 10;
mclt 3600;
split 128;
load balance max seconds 3;
}

pool {

failover peer "dhcp-failover";

}
```

```
# DHCP Server Configuration file.
#

failover peer "dhcp-failover" {
primary;
address 192.168.48.14;
port 647;
peer address 192.168.48.20;
peer port 647;
max-response-delay 60;
max-unacked-updates 10;
mclt 3600;
split 128;
load balance max seconds 3;
}

default-lease-time 86400; # Bail de 24H
max-lease-time 172800; # Bail maxi de 48H
# Déclaration d'un réseau
subnet 192.168.48.0 netmask 255.255.255.0 {
    option domain-name-servers      192.168.48.10,192.168.48.18; #DNS
    option routers                   192.168.48.254; # Passerelle
    pool {
        failover peer "dhcp-failover";
        range 192.168.48.100 192.168.48.200;
    }
}
```

Dans un second temps configurons notre serveur SRV-DHCP2 :

- Installation du serveur

```
yum install dhcp -y
```

- Lancer le service au démarrage du serveur

```
systemctl enable dhcpd
```

- Démarrer le service serveur DHCP

```
systemctl start dhcpd
```

- Déblocage du firewall

```
firewall-cmd --add-service=dhcp --permanent
```

```
firewall-cmd --reload
```

- Sur le serveur SRV-DHCP2 , éditer le fichier de configuration

```
vi /etc/dhcp/dhcpd.conf
```

- Ajouter la définition de la plage DHCP

```
default-lease-time 86400; # Bail de 24H
max-lease-time 172800; # Bail maxi de 48H
# Déclaration d'un réseau
subnet 192.168.48.0 netmask 255.255.255.0 {
    option domain-name-servers      192.168.48.10,192.168.48.18; # DNS
    option routers                   192.168.48.254; # Passerelle
    pool {
        range 192.168.48.100 192.168.48.200;
```

- Ajouter les critères de configuration en HA

```
failover peer "dhcp-failover" {
```

```
secondary;
```

```
address 192.168.48.20;
```

```
port 647;
```

```
peer address 192.168.48.14;
```

```
peer port 647;
```

```
max-response-delay 60;
```

```
max-unacked-updates 10;
```

```
load balance max seconds 3;
```

```
}
```

```
pool {  
  
failover peer "dhcp-failover";  
  
}
```

```
#  
# DHCP Server Configuration file.  
#  
failover peer "dhcp-failover" {  
secondary;  
address 192.168.48.20;  
port 647;  
peer address 192.168.48.14;  
peer port 647;  
max-response-delay 60;  
max-unacked-updates 10;  
load balance max seconds 3;  
}  
  
default-lease-time 86400; # Bail de 24H  
max-lease-time 172800; # Bail maxi de 48H  
# Déclaration d'un réseau  
subnet 192.168.48.0 netmask 255.255.255.0 {  
    option domain-name-servers      192.168.48.10,192.168.48.18; # DNS  
    option routers                   192.168.48.254; # Passerelle  
    pool {  
        failover peer "dhcp-failover";  
        range 192.168.48.100 192.168.48.200;  
    }  
}
```

- Débloquer le port 647 TCP sur les deux serveurs

```
firewall-cmd --add-port=647/tcp --permanent
```

```
firewall-cmd --reload
```

2. Le service NFS et SMB

Les service NFS et SMB seront exécutés sur le serveur SRV-SMB-NFS.

La configuration de ce serveur est la suivante :

Configuration physique du serveur SRV-SMB-NFS	
RAM :	2 GB
Nombre de processeur :	1
Nombre de cœurs par processeur :	1
Disque 1 :	40 GB
Disque 2 :	50 GB

Nous commencerons par l'installation du service NFS :

- Installation du serveur NFS

```
yum install nfs-utils
```

- Ajouter une règle dans le firewall

```
firewall-cmd --add-service=nfs --permanent
```

```
firewall-cmd --reload
```

- Vérifier la présence du disque dans le répertoire /dev

```
ls /dev/sd*
```

- Créer une partition sdb1 de type xfs

```
fdisk /dev/sdb
```

- Formater la partition

```
mkfs.xfs /dev/sdb1
```

- Créer un dossier destiné au montage de la nouvelle partition

```
mkdir /nfs
```

- Ajouté le montage de la nouvelle partition au démarrage de la machine

vi /etc/fstab

```
#
# /etc/fstab
# Created by anaconda on Sat Jul  7 16:10:56 2018
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
/dev/mapper/centos_srv--smb--nfs-root / xfs defaults 0 0
UUID=4056cafb-e390-4202-893c-616a05208db1 /boot xfs defaults 0 0
/dev/mapper/centos_srv--smb--nfs-home /home xfs defaults 0 0
/dev/mapper/centos_srv--smb--nfs-var /var xfs defaults 0 0
/dev/mapper/centos_srv--smb--nfs-swap swap swap defaults 0 0
/dev/sdb1 /nfs xfs defaults 0 0
```

- Changer les droits du dossier

chmod -R 755 /nfs

- Changer les groupes propriétaires

chown nfsnobody:nfsnobody /nfs

- Créer le partage

vi /etc/exports

- Ajouter

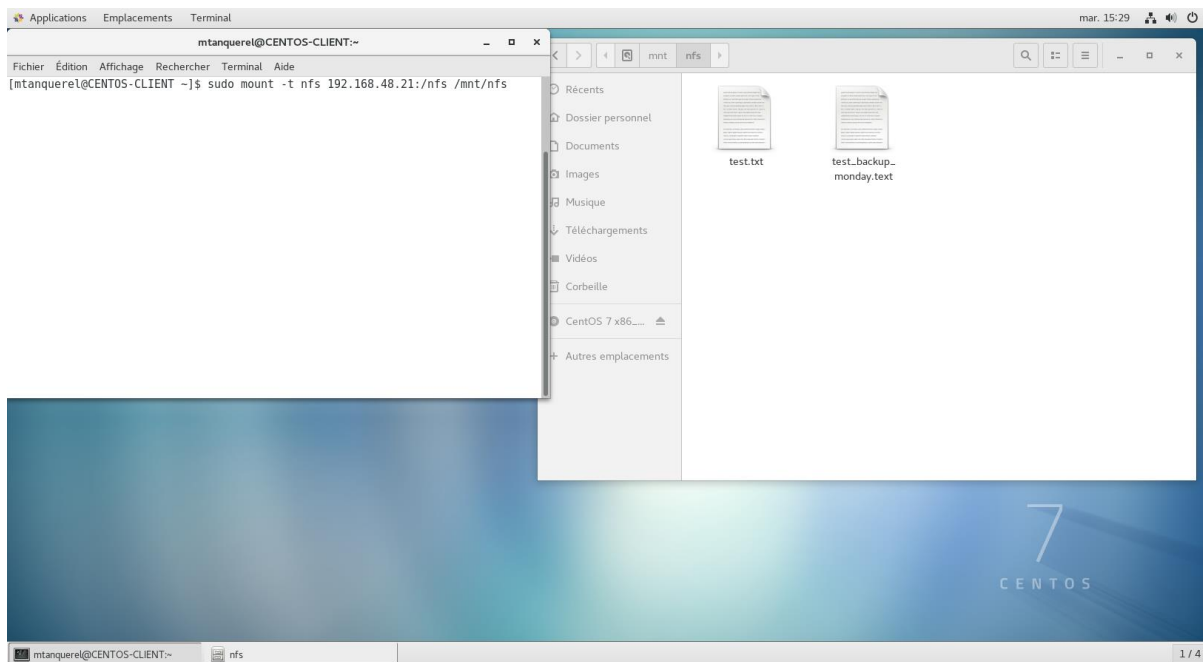
/nfs 192.168.100.0/24(rw,sync,no_root_squash,no_all_squash)

```
#nfs 192.168.48.0/24(rw,sync,no_all_squash)
```

- Tester le montage du dossier nfs depuis un poste linux

```
mkdir /mnt/nfs
```

```
sudo mount -t nfs 192.168.48.21:/nfs /mnt/nfs
```

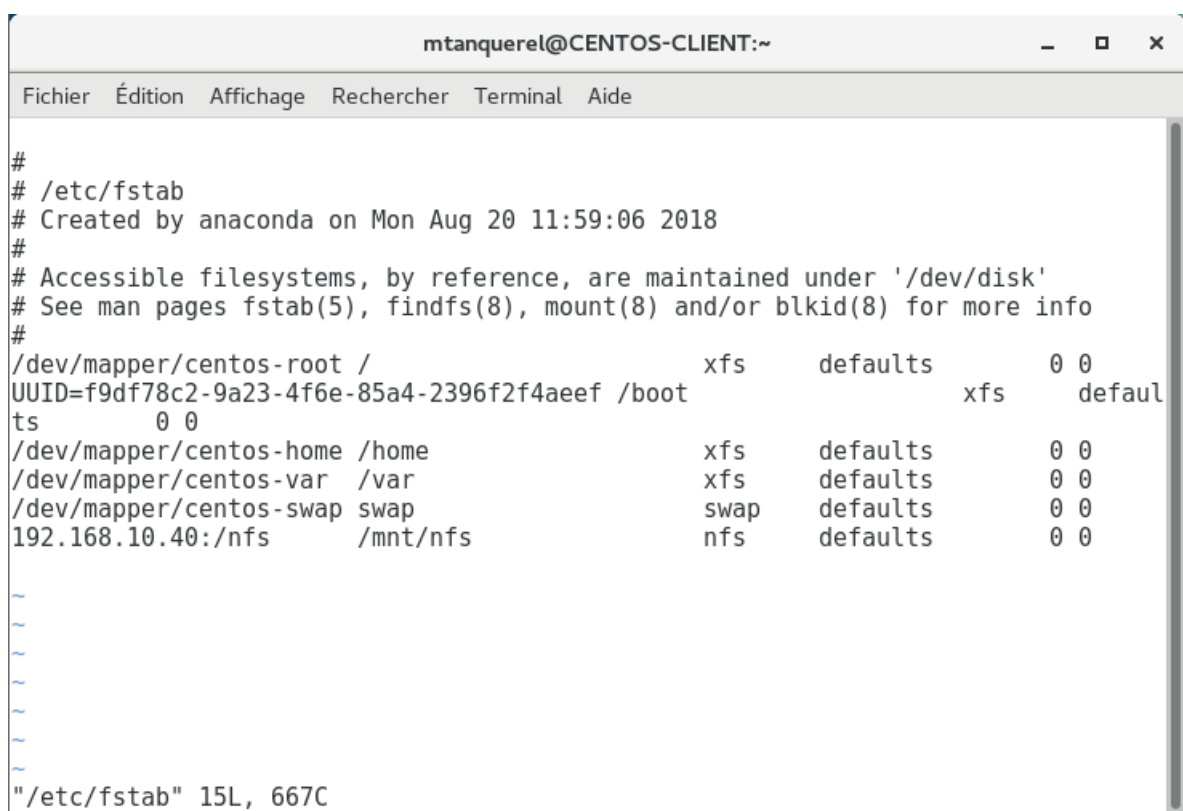


- Pour que le point de montage soit actif dès le démarrage du système, il est nécessaire de l'ajouter dans le fichier fstab

vi /etc/fstab

- Ajouter à la suite du fichier :

```
192.168.10.40:/nfs /mnt/nfs nfs defaults 0 0
```



```
mtanquerel@CENTOS-CLIENT:~  
Fichier  Édition  Affichage  Rechercher  Terminal  Aide  
#  
# /etc/fstab  
# Created by anaconda on Mon Aug 20 11:59:06 2018  
#  
# Accessible filesystems, by reference, are maintained under '/dev/disk'  
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info  
#  
/dev/mapper/centos-root / xfs defaults 0 0  
UUID=f9df78c2-9a23-4f6e-85a4-2396f2f4aeef /boot xfs default  
ts 0 0  
/dev/mapper/centos-home /home xfs defaults 0 0  
/dev/mapper/centos-var /var xfs defaults 0 0  
/dev/mapper/centos-swap swap swap defaults 0 0  
192.168.10.40:/nfs /mnt/nfs nfs defaults 0 0  
~  
~  
~  
~  
~  
~  
"/etc/fstab" 15L, 667C
```

Nous finissons par l'installation du service SMB :

- Installation de Samba

```
yum install samba.x86_64
```

- Autoriser le programme Samba à passer le firewall

```
firewall-cmd --permanent --zone=public --add-service=samba
```

- Recharger le firewall

```
firewall-cmd --reload
```

- Création utilisateur mederick

```
Useradd mederick -p
```

- Créer un compte pour authentifier l'utilisateur mederick

```
smbpasswd -a mederick
```

- Créer le groupe "rh_user"

```
groupadd rh_user
```

- Affectation de l'utilisateur mederick au groupe

```
usermod -aG rh_user mederick
```

- Affectation d'un compte samba à mederick

```
smbpasswd -a mederick
```

- Ajouter dans le fichier smb.conf

vi /etc/samba/smb.conf

[RH]

```
path = /samba/rh
valid users = @rh_user
guest ok = no
writable = yes
browsable = yes
```

```
# See smb.conf.example for a more detailed config file or
# read the smb.conf manpage.
# Run 'testparm' to verify the config is correct after
# you modified it.

[RH]
path = /samba/rh
valid users = @rh_user
guest ok = no
writable = yes
browsable = yes
```

- Affectation des droits

chmod -R 0777 /samba/rh

chcon -t samba_share_t -R /samba/rh

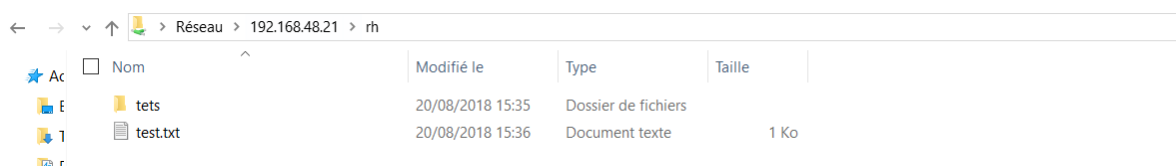
- Création du dossier rh

mkdir /samba/rh

- Relancer le service samba pour charger la configuration

systemctl restart samba

- Tester la connexion depuis un poste Windows



3. Le service FTP

Le service FTP sera exécuté sur le serveur SRV-FTP.

La configuration de ce serveur est la suivante :

Configuration physique du serveur SRV-FTP	
RAM :	1 GB
Nombre de processeur :	1
Nombre de cœurs par processeur :	1
Disque 1 :	20 GB
Disque 2 :	500 GB

- Installation du serveur

```
yum install vsftpd
```

- Vérifier si le compte ftp a bien été créé

```
getent passwd ftp
```

- Changer le mot de passe du compte ftp

```
passwd ftp
```

- Ajouter les règles dans le firewall

```
firewall-cmd --permanent --add-port=21/tcp
```

```
firewall-cmd --permanent --add-port=40000-40100/tcp
```

```
firewall-cmd --permanent --add-service=ftp
```

- Recharger la configuration

```
firewall-cmd --reload
```

- Lancer le service vsftpd au démarrage

```
systemctl enable vsftpd
```

- Démarrer le service

```
systemctl start vsftpd
```

- Vérifier l'état du service

```
systemctl status vsftpd
```

- Editer le fichier de configuration

```
vi /etc/vsftpd/vsftpd.conf
```

- Ajouter les lignes

```
allow_writeable_chroot=YES
```

```
pasv_enable=YES
```

```
pasv_min_port=40000
```

```
pasv_max_port=40100
```

- Ajouter les droits SELinux

```
setsebool -P allow_ftpd_full_access on
```

- Création utilisateur standard « user_ftp » et utilisateur « backup »

```
useradd backup -p Formation2018 -G ftp
```

```
passwd backup
```

```
useradd user_ftp -p Formation2018 -G ftp
```

```
passwd user_ftp
```

- Modifier la liste des utilisateurs autorisé à se connecter en FTP

vi /etc/vsftpd/user_list

```
# vsftpd userlist
# If userlist_deny=NO, only allow users in this file
# If userlist_deny=YES (default), never allow users in this file, and
# do not even prompt for a password.
# Note that the default vsftpd pam config also checks /etc/vsftpd/ftpusers
# for users that are denied.
root
bin
daemon
adm
lp
sync
shutdown
halt
mail
news
uucp
operator
games
nobody
ftp
mederick
user_ftp
backup
```

- Bloquer l'utilisateur dans son dossier « home »

chroot_local_user=yes # décommenter ligne 100

- Débloquer l'utilisateur backup du dossier « home »

chroot_list_enable=YES #décommenter ligne 101

chroot_list_file=/etc/vsftpd/chroot_list #décommenter ligne 103

- Création du dossier certificat

mkdir /etc/ssl/private

- Création d'un certificat

openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/vsftpd.pem
-out /etc/ssl/private/vsftpd.pem

- Modification des droits du certificat

```
chmod 600 /etc/ssl/private/vsftpd.pem
```

```
chown root:root /etc/ssl/private/vsftpd.pem
```

- Dans le fichier de configuration ajouter
- Le chemin du certificat

```
rsa_cert_file=/etc/ssl/private/vsftpd.pem
```

```
rsa_private_key_file=/etc/ssl/private/vsftpd.pem
```

- Activation du SSL

```
ssl_enable=YES
```

```
anonymous_enable=NO # modifier la ligne 12
```

```
force_local_data_ssl=YES
```

```
force_local_logins_ssl=YES
```

- Refus des anciens protocole SSL

```
ssl_sslv2=NO
```

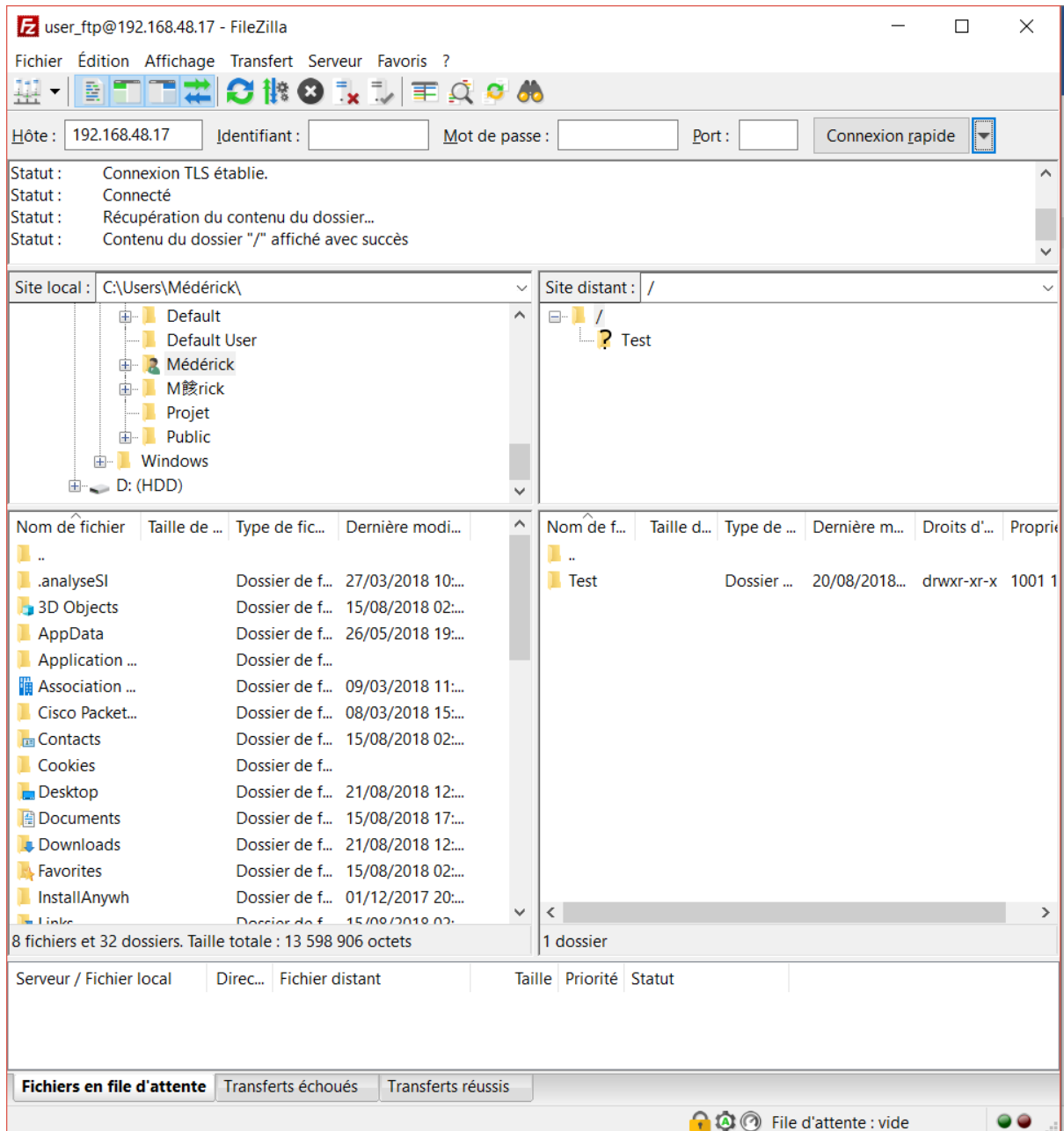
```
ssl_sslv3=NO
```

- Activer le TLS

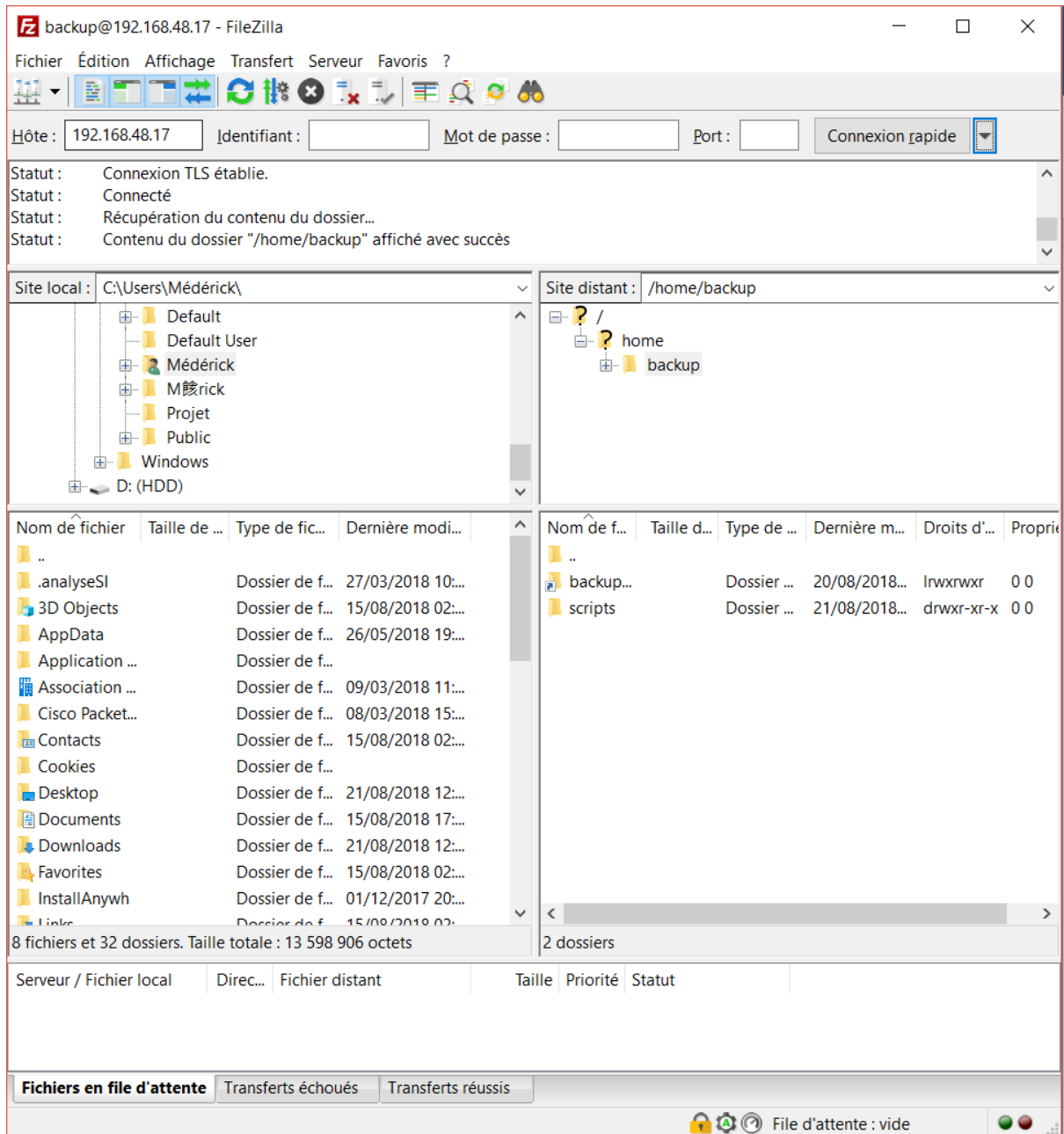
```
ssl_tlsv1=YES
```

```
pam_service_name=vsftpd
userlist_enable=YES
userlist_deny=NO
tcp_wrappers=YES
allow_writeable_chroot=YES
pasv_enable=YES
pasv_min_port=40000
pasv_max_port=40100
rsa_cert_file=/etc/ssl/private/vsftpd.pem
rsa_private_key_file=/etc/ssl/private/vsftpd.pem
ssl_enable=YES
force_local_data_ssl=YES
force_local_logins_ssl=YES
ssl_sslv2=NO
ssl_sslv3=NO
ssl_tlsv1=YES
```

- Tester l'accès FTP pour l'utilisateur user_ftp avec un utilitaire comme filezilla



- Tester l'accès FTP pour l'utilisateur backup avec un utilitaire comme filezilla



4. Le Serveur WEB

5. Le Serveur GLPI



- Installation des prérequis avec les modules php-mysql php-gd, et php-mbstring.

```
yum install httpd php php-{gd,mysql,mbstring} mariadb-server
```

- On démarre les services httpd et mariadb :

```
systemctl start httpd mariadb
```

- On vérifie leur statut :

```
systemctl is-active httpd mariadb
```

- On active les services httpd et mariadb au démarrage :

```
systemctl enable httpd mariadb
```

- Autoriser le HTTP et le HTTPS dans firewalld

```
firewall-cmd --zone=public --add-port=http/tcp --permanent
```

```
firewall-cmd --zone=public --add-port=https/tcp --permanent
```

- Recharger la configuration avec la commande :

firewall-cmd --reload

```
[root@srvcentos ~]# systemctl start httpd mariadb
[root@srvcentos ~]# systemctl is-active httpd mariadb
active
active
[root@srvcentos ~]# systemctl enable httpd mariadb
Created symlink from /etc/systemd/system/multi-user.target.wants/httpd.service to /usr/lib/systemd/system/httpd.service.
Created symlink from /etc/systemd/system/multi-user.target.wants/mariadb.service to /usr/lib/systemd/system/mariadb.service.
[root@srvcentos ~]# systemctl is-enabled httpd mariadb
enabled
enabled
[root@srvcentos ~]# firewall-cmd --zone=public --add-port=http/tcp --permanent
success
[root@srvcentos ~]# firewall-cmd --zone=public --add-port=https/tcp --permanent
success
[root@srvcentos ~]# firewall-cmd --reload
success
[root@srvcentos ~]# firewall-cmd --list-all
public (default, active)
  interfaces: eth0
  sources:
  services: dhcpv6-client ssh
  ports: 443/tcp 80/tcp
  masquerade: no
  forward-ports:
  icmp-blocks:
  rich rules:
```

Nous allons maintenant créer la base de données et un utilisateur pour glpi.

- Se connecter à MariaDB

mysql -u root

- Créer la base de données pour GLPI

create database glpi;

- Création de l'utilisateur avec son mot de passe

create user 'glpiuser'@'localhost' identified by 'glpipassword';

- Attribution des droits

grant all privileges on glpi.* to 'glpiuser'@'localhost';

- Nous vérifions que la base de données glpi et l'utilisateur glpiuser ont bien été créés.

show databases;

select host, user from mysql.user;

```
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 3
Server version: 5.5.56-MariaDB MariaDB Server

Copyright (c) 2000, 2017, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> show databases;
+-----+
| Database |
+-----+
| information_schema |
| glpi |
| mysql |
| performance_schema |
| test |
+-----+
5 rows in set (0.15 sec)

MariaDB [(none)]> select host, user from mysql.user;
+-----+-----+
| host | user |
+-----+-----+
| 127.0.0.1 | root |
| ::1 | root |
| localhost |  |
| localhost | glpiuser |
| localhost | root |
| srv-glpi |  |
| srv-glpi | root |
+-----+-----+
7 rows in set (0.00 sec)
```

- On se place ensuite dans le répertoire /var/www/html

```
cd /var/www/html
```

- On télécharge la dernière version de GLPI :

```
wget https://github.com/glpi-project/glpi/releases/download/0.90.5/glpi-0.90.5.tar.gz
```

- On décompresse l'archive et on la supprime une fois terminé.

```
tar -xzf glpi-0.90.5.tar.gz && rm -rf glpi-0.90.5.tar.gz
```

- On modifie les permissions.

```
chown -R apache:apache /var/www/html/glpi
```

```
find /var/www/html/glpi -type d -exec chmod 775 {} \;
```

```
find /var/www/html/glpi -type f -exec chmod 664 {} \;
```

```
[root@SRV-GLPI html]# ls -l glpi
total 144
drwxrwxrwx.  2 apache apache  4096 19 août  12:01 ajax
-rwxrwxrwx.  1 apache apache   194 27 juil.  2016 AUTHORS.txt
-rwxrwxrwx.  1 apache apache    64 27 juil.  2016 CHANGELOG.txt
drwxrwxrwx.  2 apache apache   104 19 août  16:45 config
-rwxrwxrwx.  1 apache apache 18092 27 juil.  2016 COPYING.txt
drwxrwxrwx.  4 apache apache   207 19 août  12:01 css
drwxrwxrwx. 13 apache apache   180 19 août  16:45 files
drwxrwxrwx.  2 apache apache 20480 19 août  12:01 front
drwxrwxrwx.  2 apache apache 16384 19 août  12:01 inc
-rwxrwxrwx.  1 apache apache  6833 27 juil.  2016 index.php
drwxrwxrwx.  3 apache apache  4096 19 août  16:42 install
drwxrwxrwx. 16 apache apache   272 19 août  12:01 lib
-rwxrwxrwx.  1 apache apache   145 27 juil.  2016 LISEZMOI.txt
drwxrwxrwx.  2 apache apache  4096 19 août  12:01 locales
drwxrwxrwx.  6 apache apache  8192 19 août  12:01 pics
drwxrwxrwx.  3 apache apache    95 19 août  16:49 plugins
-rwxrwxrwx.  1 apache apache   124 27 juil.  2016 README.txt
-rwxrwxrwx.  1 apache apache 22063 27 juil.  2016 script.js
drwxrwxrwx.  2 apache apache   186 19 août  12:01 scripts
-rwxrwxrwx.  1 apache apache  6409 27 juil.  2016 status.php
```

- Modifier le fichier glpi.conf

```
<VirtualHost 192.168.48.15:80>
  ServerName srv-glpi
  DocumentRoot /var/www/html/glpi
  <Directory /var/www/html/glpi>
    Options Indexes FollowSymLinks MultiViews
    AllowOverride All
    Require all granted
  </Directory>
  ServerSignature off
  ErrorLog /var/log/http.log
  CustomLog /var/log/access.log combined
</VirtualHost>
```

- Pour terminer, on redémarre Apache :

apachectl restart

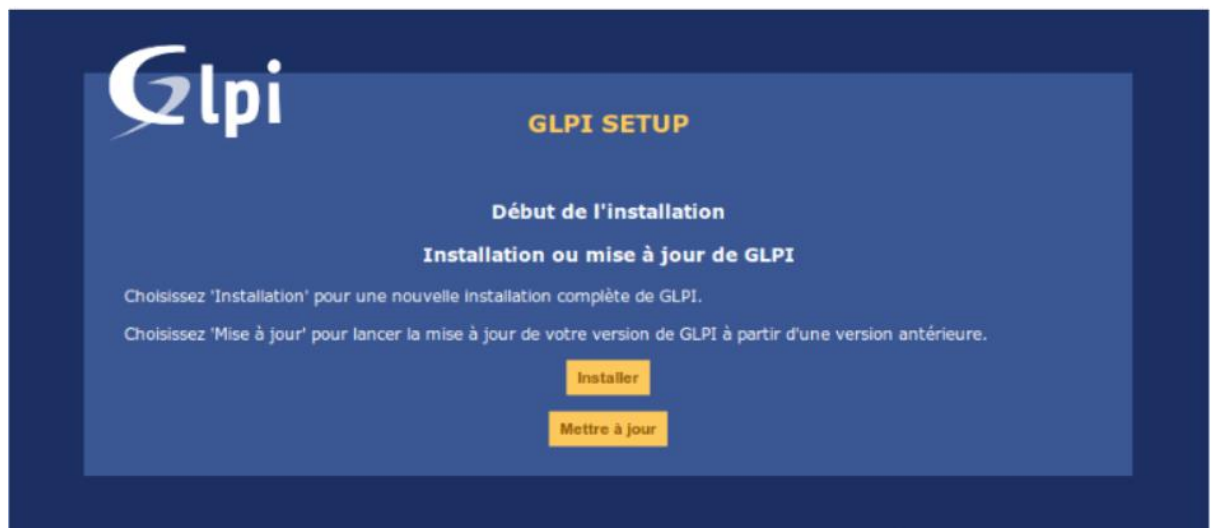
- Se connecter au serveur GLPI par l'interface web (<http://192.168.48.15/glpi>)
- Choisir votre langue via le menu déroulant.



- Accepter les termes de la licence.



- Choisir le type d'installation souhaitée (ici il s'agit d'une nouvelle installation).



- Une vérification de la compatibilité de votre environnement avec GLPI va être effectuée.



The screenshot shows the GLPI SETUP interface. At the top left is the GLPI logo. To its right, the text 'GLPI SETUP' is displayed. Below this, 'Étape 0' is centered, followed by the subtitle 'Vérification de la compatibilité de votre environnement avec l'exécution de GLPI'. The main content is a table with two columns: 'Tests effectués' and 'Résultats'. The table lists 24 tests, all of which have a green checkmark in the 'Résultats' column. At the bottom right of the table area is a yellow button labeled 'Continuer'.

Tests effectués	Résultats
Test du Parseur PHP	✓
Test de l'extension MySQLi	✓
Test des sessions	✓
Test de l'utilisation de Session use_trans_sid	✓
Test sur l'extension magic_quotes_sybase	✓
Test sur les fonctions ctype	✓
Test sur l'extension fileinfo	✓
Test sur les fonctions Json	✓
Test sur l'extension mbstring	✓
Test sur l'extension GD	✓
Test sur l'extension zlib	✓
Test de la mémoire allouée	✓
Test d'écriture du fichier de configuration	✓
Test d'écriture de fichiers documents	✓
Test d'écriture de fichiers dump	✓
Test d'écriture des fichiers de sessions	✓
Test d'écriture des fichiers des actions automatiques	✓
Test d'écriture des fichiers de graphiques	✓
Test d'écriture des fichiers de verrouillage	✓
Test d'écriture des documents des plugins	✓
Test d'écriture des fichiers temporaires	✓
Test d'écriture de fichiers rss	✓
Test d'écriture des fichiers téléchargés	✓
Test d'écriture de fichiers photos	✓
Test d'écriture des fichiers de journal	✓
SELinux en mode Disabled	✓

- Entrer les paramètres de connexion à la base de données créée précédemment.



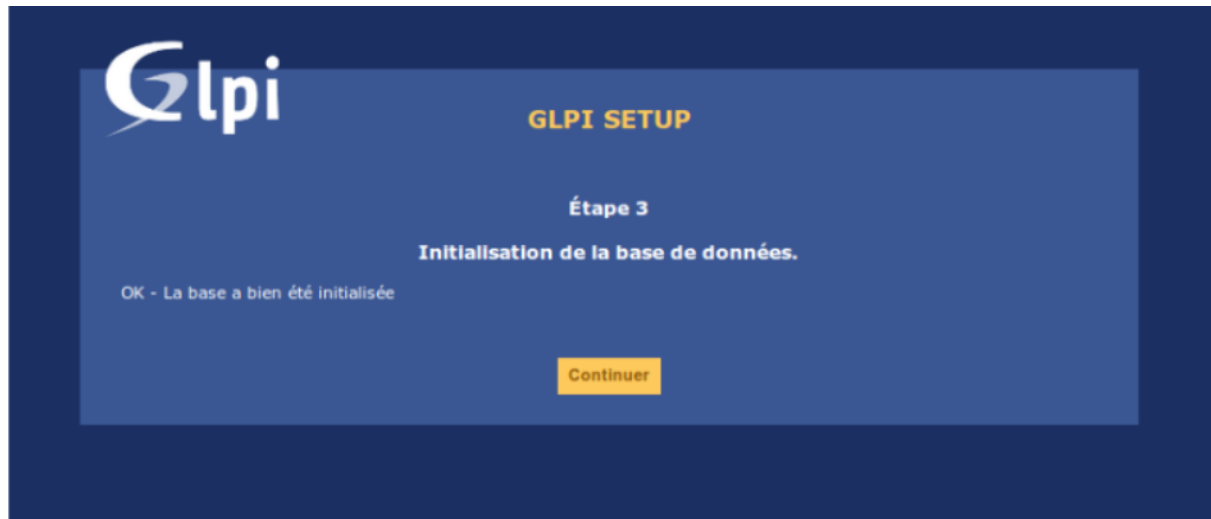
The screenshot shows the GLPI SETUP interface for Step 1. The title is "GLPI SETUP" and the subtitle is "Étape 1 Configuration de la connexion à la base de données". Below this, there is a section titled "Paramètres de connexion à la base de données" with three input fields: "Serveur MySQL" (localhost), "Utilisateur MySQL" (glpiuser), and "Mot de passe MySQL" (masked with asterisks). A yellow "Continuer" button is at the bottom right.

- Sélectionner la base de données qui a également été créée précédemment.



The screenshot shows the GLPI SETUP interface for Step 2. The title is "GLPI SETUP" and the subtitle is "Étape 2 Test de connexion à la base de données". Below this, it says "Connexion à la base de données réussie". Then, it asks "Veuillez sélectionner une base de données :" and lists three options: "glpi" (selected with a yellow radio button), "test", and "Créer une nouvelle base ou utiliser une base existante :". A yellow "Continuer" button is at the bottom right.

- Si tous les paramètres de la connexion à la base de données sont bons, celle-ci sera alors initialisée. L'installation sera alors terminée.



- GLPI nous donne la liste des différents identifiants / mots de passe de connexion par défaut.



- On supprime maintenant le fichier install.php situé dans /var/www/html/glpi/install.

VIII. SOURCES