

GLPI

Installations à faire

Pour pouvoir avoir un GLPI fonctionnel, il va falloir installer plusieurs logiciels et dependences. Pour cela, il va falloir exécuter l'ensemble de ces commandes:

```
apt install apache2 php mariadb-server -y
apt install php-{mysql,mbstring,curl,gd,xml,intl,ldap,apcu,xmlrpc,zip,bz2}
-y
```

Il va falloir maintenant configurer mariadb:

Sécurisation de Mariadb en tapant la commande `mariadb-secure-installation`

```
root@debian12:/# mariadb-secure-installation
NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
SERVERS IN PRODUCTION USE! PLEASE READ EACH STEP CAREFULLY!

In order to log into MariaDB to secure it, we'll need the current
password for the root user. If you've just installed MariaDB, and
haven't set the root password yet, you should just press enter here.

Enter current password for root (enter for none):
OK, successfully used password, moving on..

Setting the root password or using the unix_socket ensures that nobody
can log into the MariaDB root user without the proper authorisation.

You already have your root account protected, so you can safely answer 'n'.

Switch to unix_socket authentication [Y/n]
Enabled successfully!
Reloading privilege tables..
... Success!

You already have your root account protected, so you can safely answer 'n'.

Change the root password? [Y/n]
New password:
Re-enter new password:
Password updated successfully!
Reloading privilege tables..
... Success!

By default, a MariaDB installation has an anonymous user, allowing anyone
to log into MariaDB without having to have a user account created for
them. This is intended only for testing, and to make the installation
go a bit smoother. You should remove them before moving into a
production environment.
```

```
Remove anonymous users? [Y/n]
... Success!

Normally, root should only be allowed to connect from 'localhost'. This
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n]
... Success!

By default, MariaDB comes with a database named 'test' that anyone can
access. This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n]
- Dropping test database...
... Success!
- Removing privileges on test database...
... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n]
... Success!

Cleaning up...

All done! If you've completed all of the above steps, your MariaDB
installation should now be secure.

Thanks for using MariaDB!
root@debian12:/#
```

Création et configuration de la BDD

Tout d'abord on va accéder à mariadb avec la commande `mysql` puis on va taper les commandes suivantes:

```
root@debian12:/# mysql
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 52
Server version: 10.11.14-MariaDB-0+deb12u2 Debian 12

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

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

MariaDB [(none)]> create database db_glpi;
Query OK, 1 row affected (0,000 sec)

MariaDB [(none)]> grant all privileges on db_glpi.* to root@localhost identified by "glpi";
Query OK, 0 rows affected (0,008 sec)

MariaDB [(none)]> exit
Bye
root@debian12:/#
```

Mise en place d'un Active Directory redondant d'entreprise - Proxmox

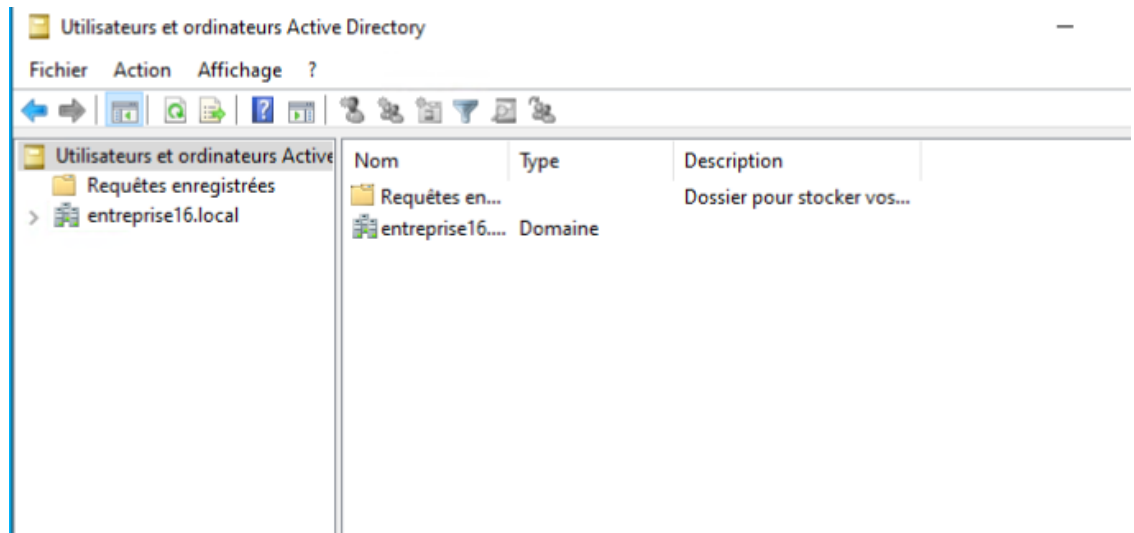
L'installation de l'Active Directory, la création du nom de domaine et la configuration du DHCP ne seront pas détaillées ici, car elles sont déjà expliquées dans le TP.

Creation d'utilisateurs

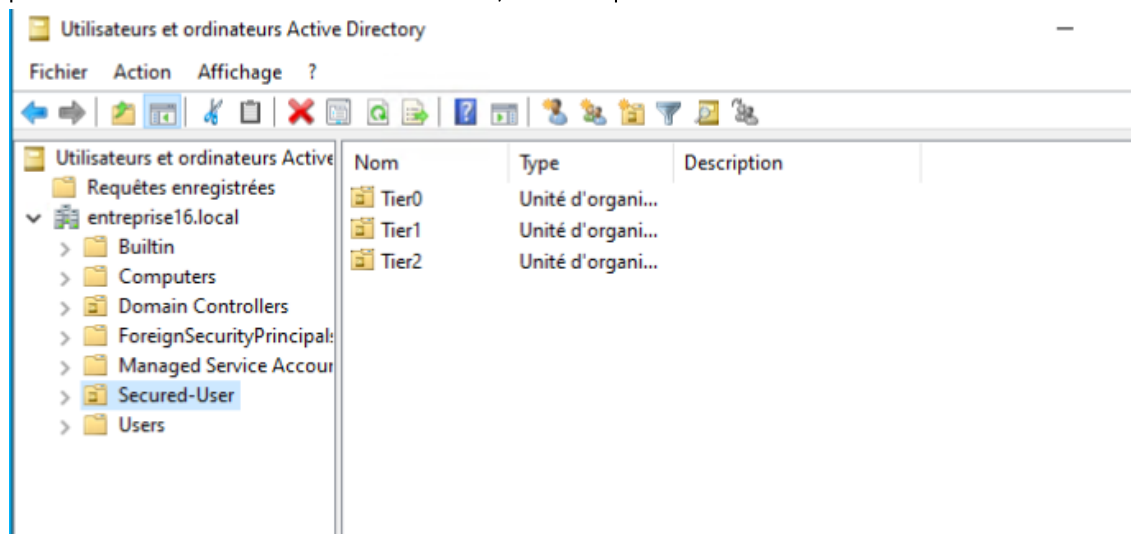
- Microsoft recommande une séparation des postes d'administration selon trois niveaux de sensibilité permettant de limiter les risques en cas de compromission :
 - Tier 0 : ressources critiques du SI (Contrôleurs de domaine, PKI, serveurs AD)
 - Tier 1 : administration des serveurs et applications (Serveurs Windows/Linux, hyperviseurs)
 - Tier 2 : postes utilisateurs
- L'objectif est d'éviter qu'un attaquant ayant compromis un poste utilisateur (Tier 2) puisse compromettre le domaine (Tier 0).
- Un administrateur ne doit jamais administrer un contrôleur de domaine depuis une machine jointe au domaine, car cela favoriserait :
 - la récupération de mots de passe administrateurs,
 - la possibilité d'escalade directe vers le Tier 0.

L'administration doit donc être réalisée depuis un poste d'administration dédié, ici appelé Admin, à l'aide d'un compte sécurisé AdminTier1.

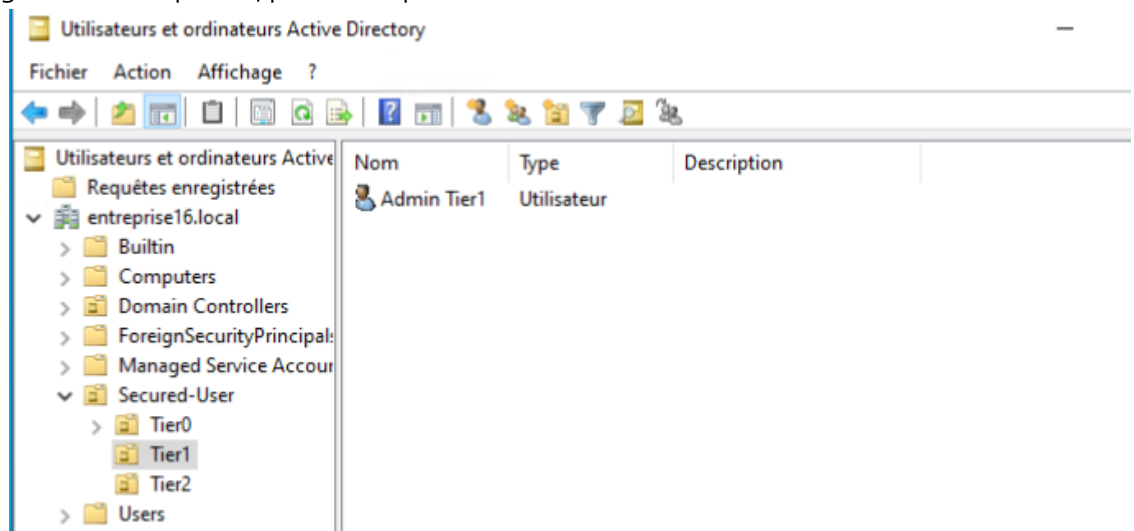
- Ce compte permettra notamment d'administrer :
 - Active Directory Users and Computers (ADUC),
 - les GPO,
 - le DNS,
 - le DHCP,
 - les scripts PowerShell AD.
- Pour ce faire voici les étapes pour créer l'utilisateur AdminTier1 dans l'OU Tier1:
 - Faut aller dans Utilisateurs et ordinateurs Active Directory dans la barre Windows:



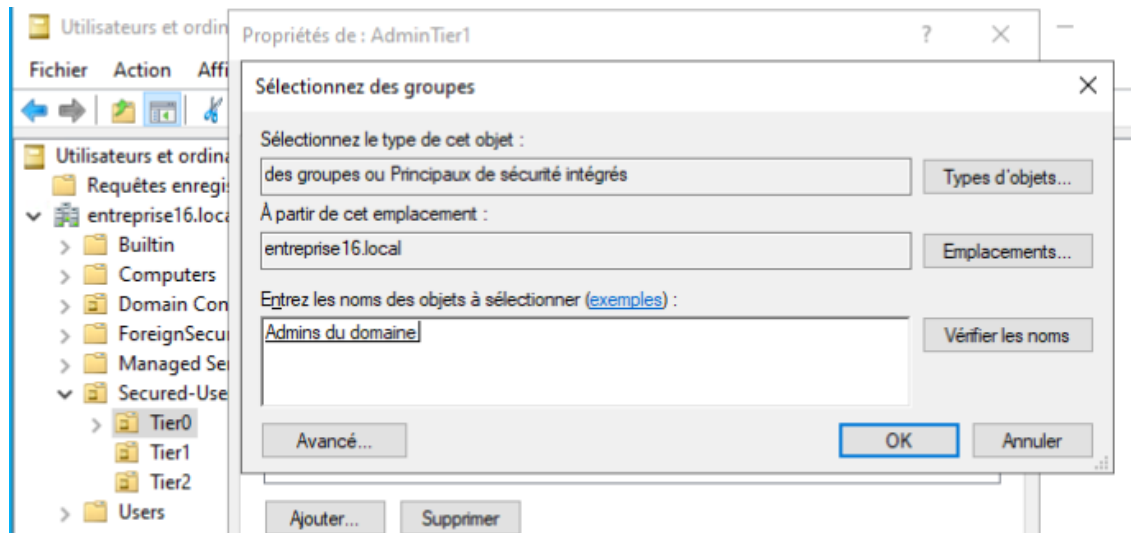
- Ensuite, on clique sur le nom de domaine pour déployer tous les dossiers.
- On se place dans le dossier Secured-Accounts, c'est là que nous avons mis nos UO.



- Dans Tier1, on fait clic droit → Nouveau → Utilisateur.
- On remplit les champs (Admin, Tier1, AdminTier1), on met un mot de passe en décochant "changer le mot de passe", puis on clique sur Terminer.



- Ensuite, on ouvre les propriétés du compte et on l'ajoute au groupe Administrateurs du domaine(admins du domaine).



Une GPO (Group Policy Object), ou Objet de stratégie de groupe, est un ensemble de paramètres permettant aux administrateurs Active Directory de contrôler et de configurer automatiquement le comportement des postes clients, des utilisateurs, et parfois des serveurs au sein d'un domaine Windows.

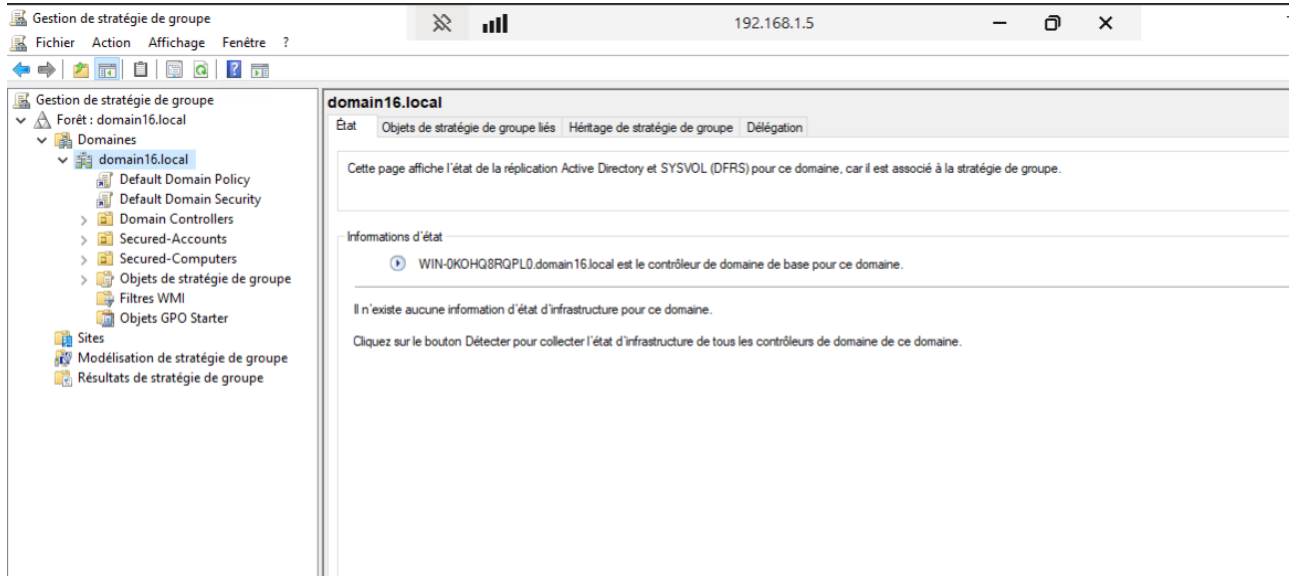
- Les GPO servent à appliquer des réglages centralisés, comme par exemple :
 - des paramètres de sécurité (mots de passe, verrouillages, restrictions),
 - des configurations système (fond d'écran, accès au panneau de configuration, scripts),
 - des déploiements de logiciels (via fichiers MSI),
 - des restrictions applicatives (PowerShell, CMD, installations).
- Elles sont hébergées dans l'Active Directory et s'appliquent automatiquement selon l'endroit où elles sont liées :
 - au niveau du domaine,
 - au niveau d'une Unité d'Organisation (UO),
 - ou au niveau d'un site.

VI/3 GPO Hardening postes utilisateurs

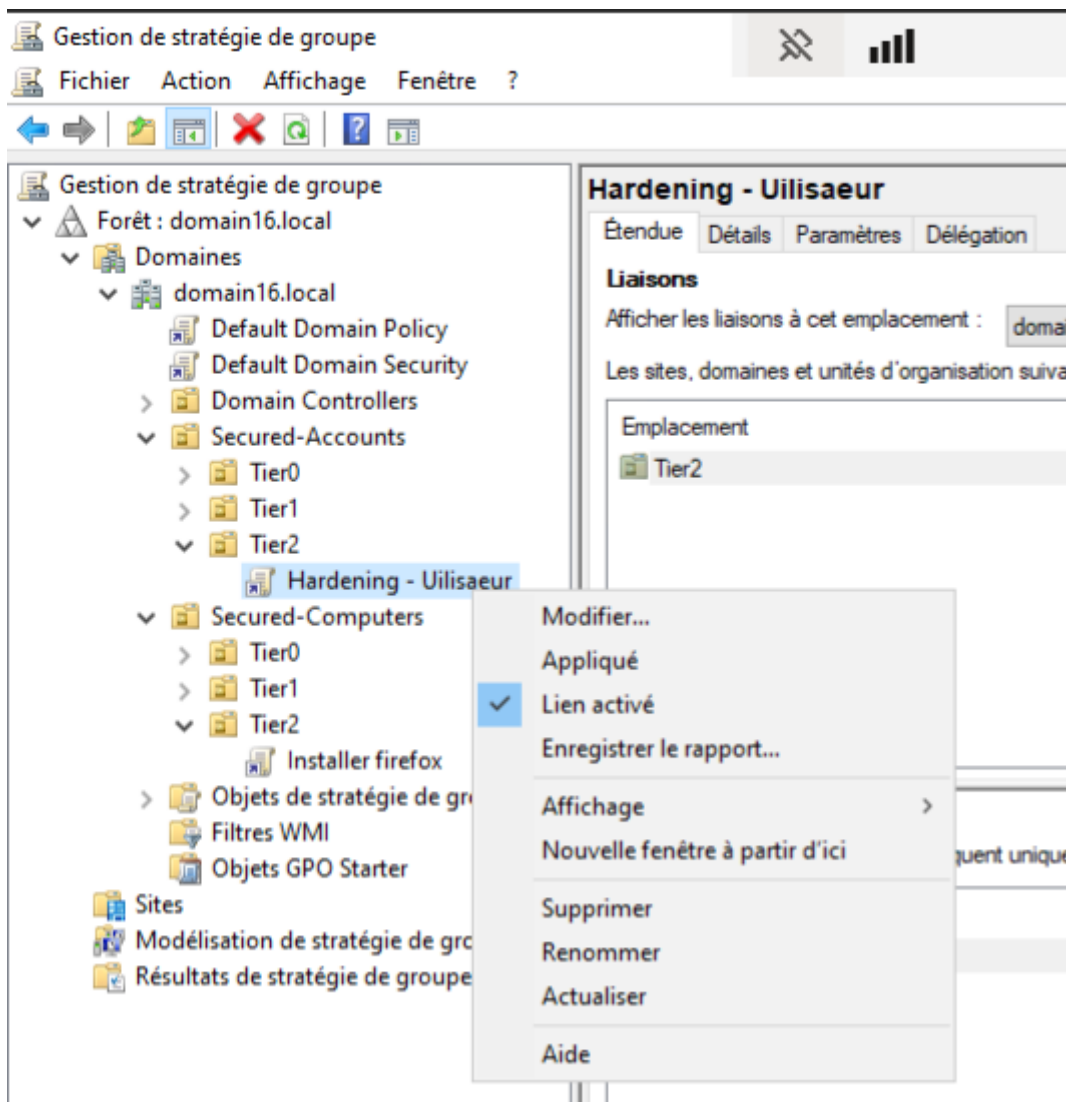
Moi, j'ai créé une seule GPO pour tout. Cependant, il est recommandé de créer différentes GPO pour chaque type de restriction, afin de faciliter la gestion et le dépannage.

Créer une GPO désactivant le panneau de configuration et les paramètres pour les utilisateurs clients

- Tout d'abord on rentre sur **Gestion de stratégie de groupe** et on se positionne au niveau de notre domaine, dans mon cas c'est `domain16.local`:

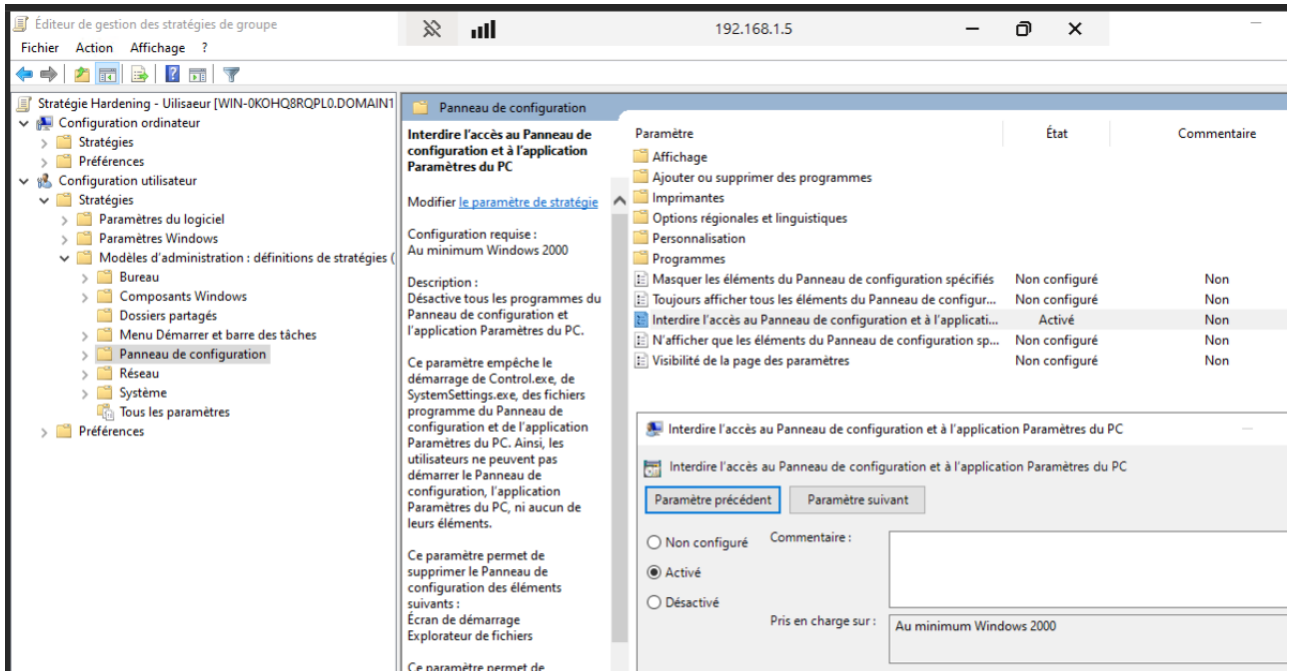


- Ensuite, on crée une nouvelle GPO en faisant un clic droit à l'endroit où se trouvent nos utilisateurs.
- On lui donne un nom clair, puis, une fois la GPO créée, il suffit de cliquer dessus et de sélectionner Modifier pour commencer la configuration. Dans mon cas je l'ai mis dans Secured-Accounts , dans Tier2 .



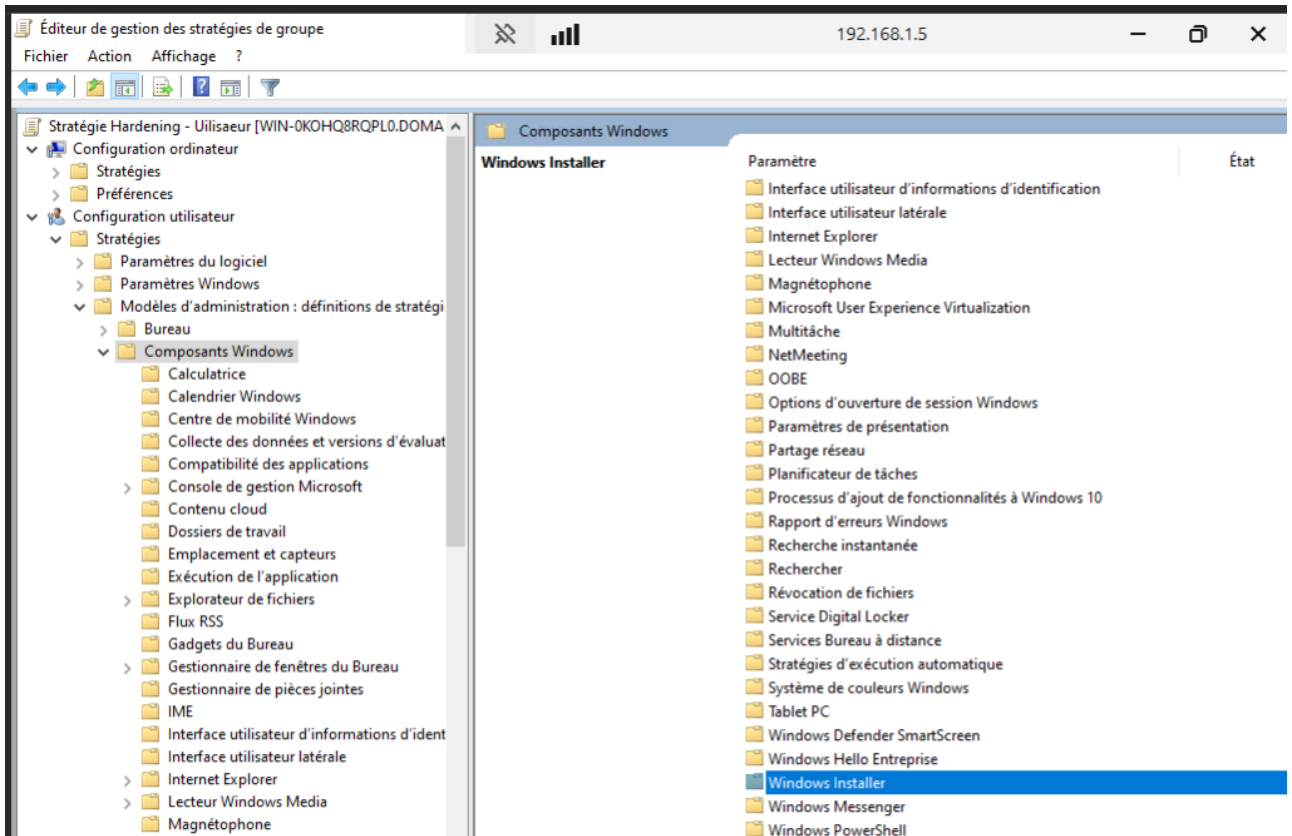
- Lorsque l'on clique sur Modifier, on accède directement à la configuration de la GPO.

- Ici, nous voulons interdire l'accès au Panneau de configuration ainsi qu'aux Paramètres de Windows.
- Pour cela, on va dans :
 - Configuration de l'utilisateur → Stratégies → Modèles d'administration → Panneau de configuration.
- Ensuite, on sélectionne la règle "Interdire l'accès au Panneau de configuration et aux Paramètres du PC", puis on l'active.

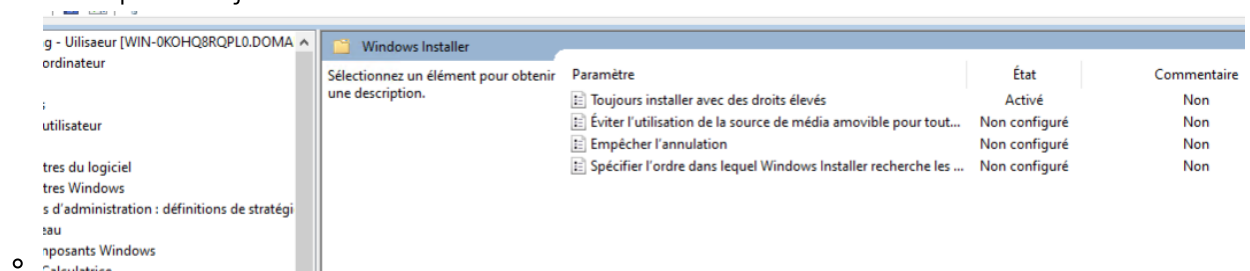


Créer une GPO pour empêcher les utilisateurs clients d'installer des logiciels

- Puisque nous utilisons une seule GPO regroupant toutes les restrictions, il suffit simplement d'ajouter la règle correspondante dans cette GPO.
- On va sur :
 - Configuration de l'utilisateur → Stratégies → Modèles d'administration → Composants Windows → Windows Installer

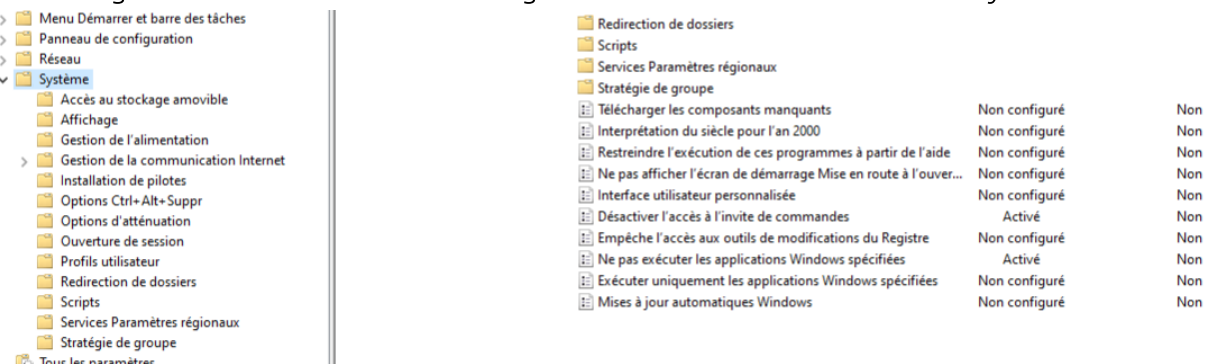


- On active l'option toujours installer avec des droits élevés:

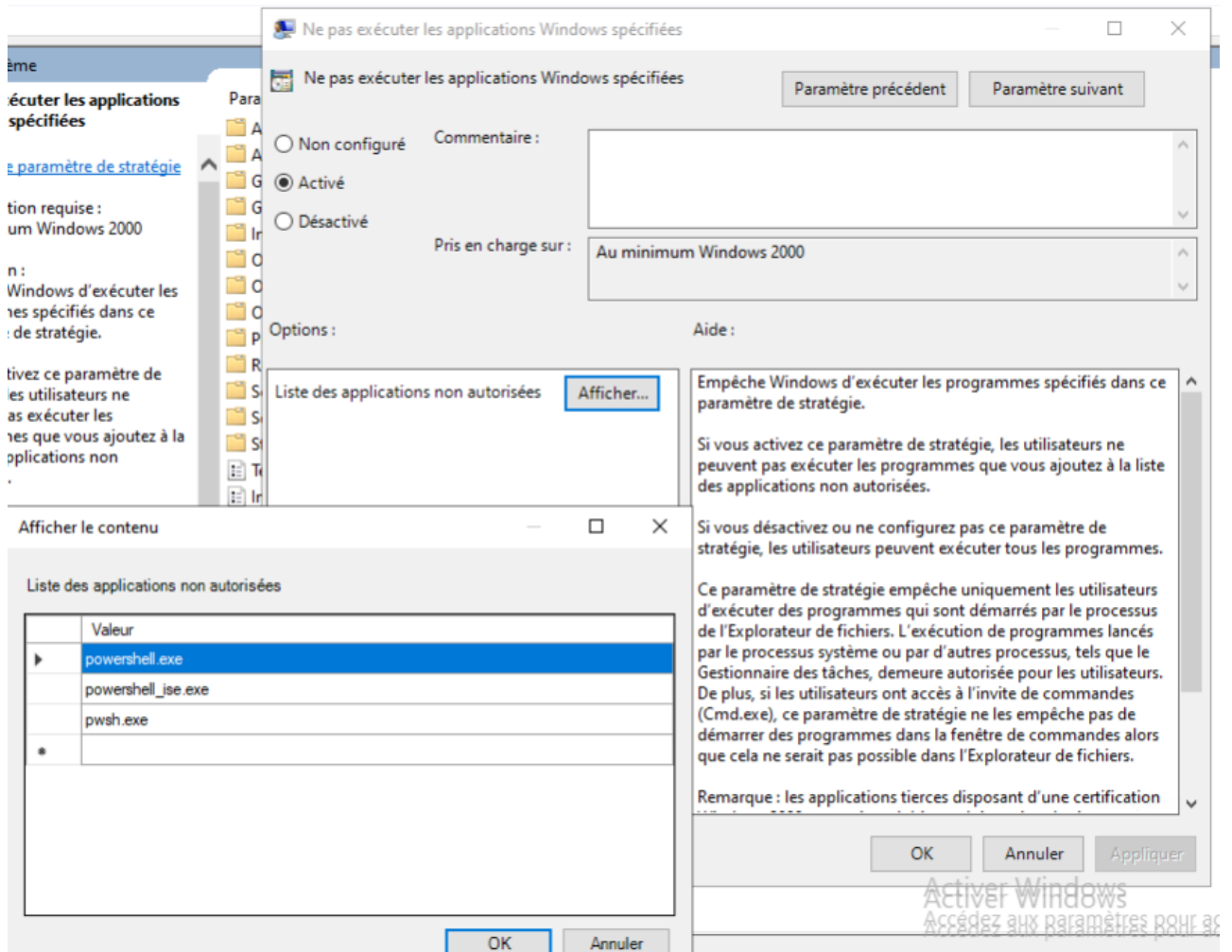


Créer une GPO pour empêcher les utilisateurs clients d'accéder à l'invite de commande ainsi qu'au PowerShell

- Pour se faire on se replace sur COnfiguration de l'utilisateur:
 - Configuration de l'utilisateur → Stratégies → Modèles d'administration → Système

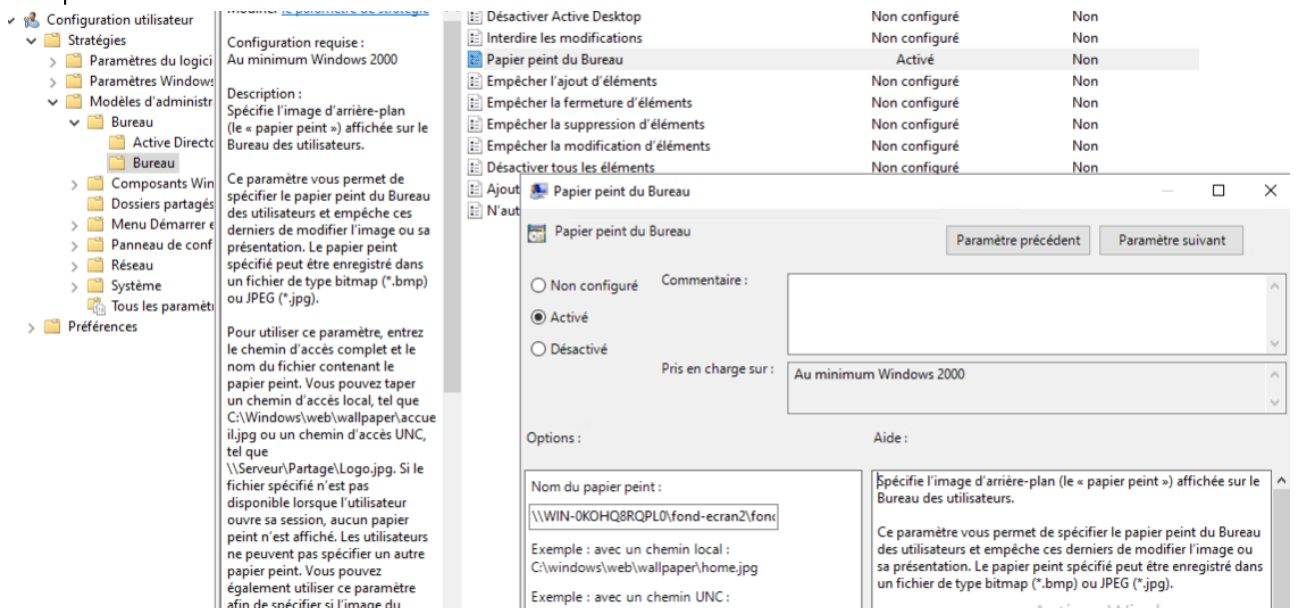


- On active l'option desactiver l'accès à l'invite de commande
- Et dans l'option "Ne pas exécuter les applications spécifiées", on met powershell.



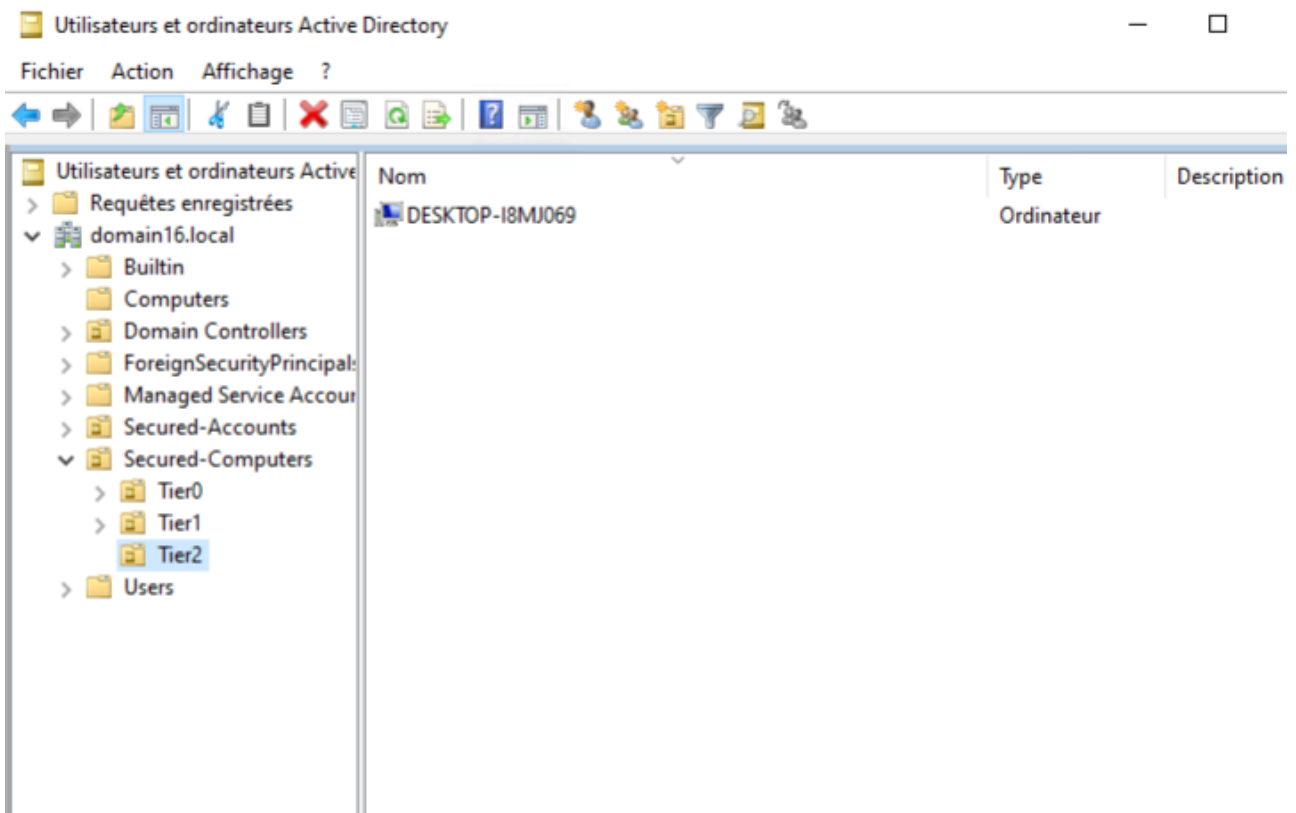
Créer une GPO pour forcer le fond d'écran des sessions utilisateurs client

- Pour cette etape on se place sur:
 - Configuration de l'utilisateur → Stratégies → Modèles d'administration → Bureau → Bureau
- Dans l'option "Fond d'écran du Bureau", on sélectionne Activé et on indique le chemin réseau vers le dossier partagé contenant le fond d'écran. Le dossier partagé doit être accessible automatiquement à chaque session de l'utilisateur.

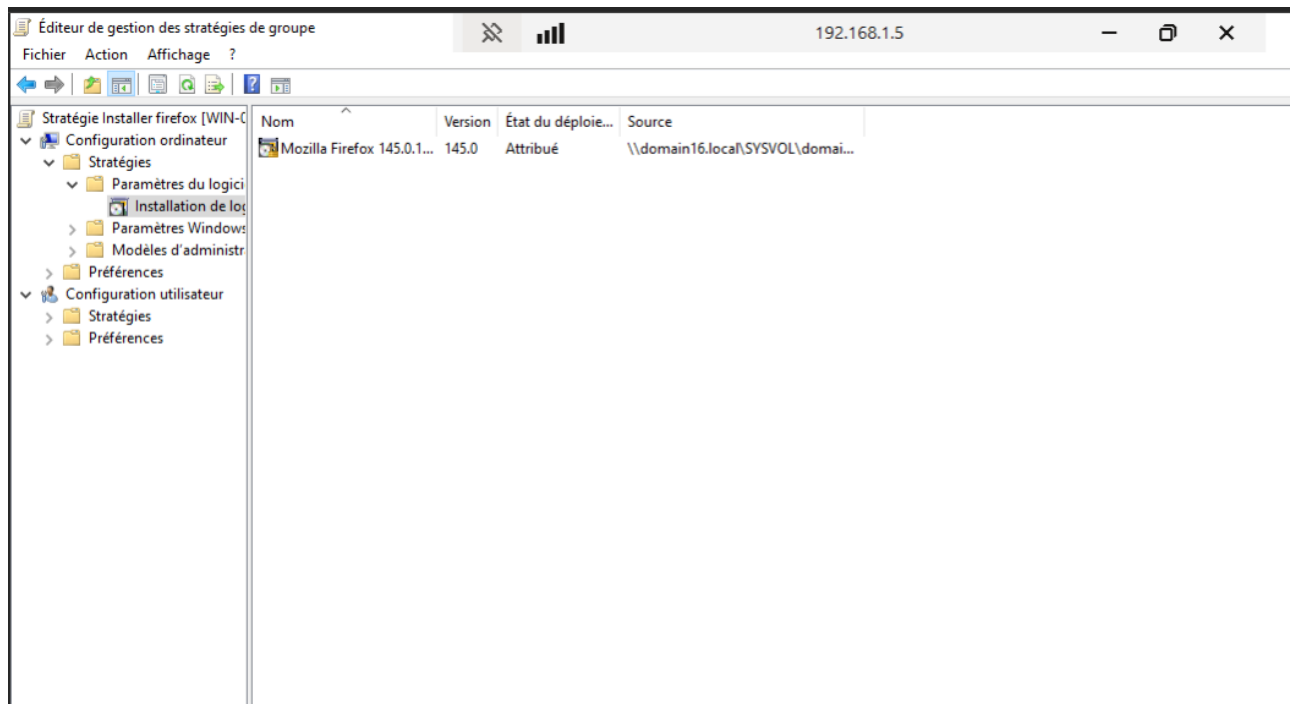


VI/4 GPO spécifique : déploiement de logiciel

- Pour cet exemple, nous allons déployer Firefox. Nous avons placé le fichier d'installation dans le dossier C:\Windows\SYSVOL\domain\software (le dossier software a été créé et contient le logiciel Firefox).
- Tout d'abord, nous allons déplacer le poste client qui se trouve dans Computers vers l'UO que nous avons créée, Secured-Computers, plus précisément dans Tier2.



- Une fois déplacé, on se rend dans Gestion des stratégies de groupe pour créer une nouvelle GPO dans Secured-Computers, sous Tier2.
- Une fois la GPO créée et nommée, on clique sur Modifier et on va dans :
 - Configuration de l'ordinateur → Stratégies → Parametre du logiciel
- À cet endroit, on fait un clic droit → Nouveau → Package et on sélectionne le logiciel via le chemin réseau : \domain16.local\SYSVOL\domain16.local\software (et non pas le chemin local C:\Windows\SYSVOL\domain\software). Le chemin local est lié au chemin réseau, et c'est ce dernier qu'on attribue pour que le déploiement fonctionne correctement \domain16.local\SYSVOL\domain16.local\software\Firefox....



Redondance d'AD en binome

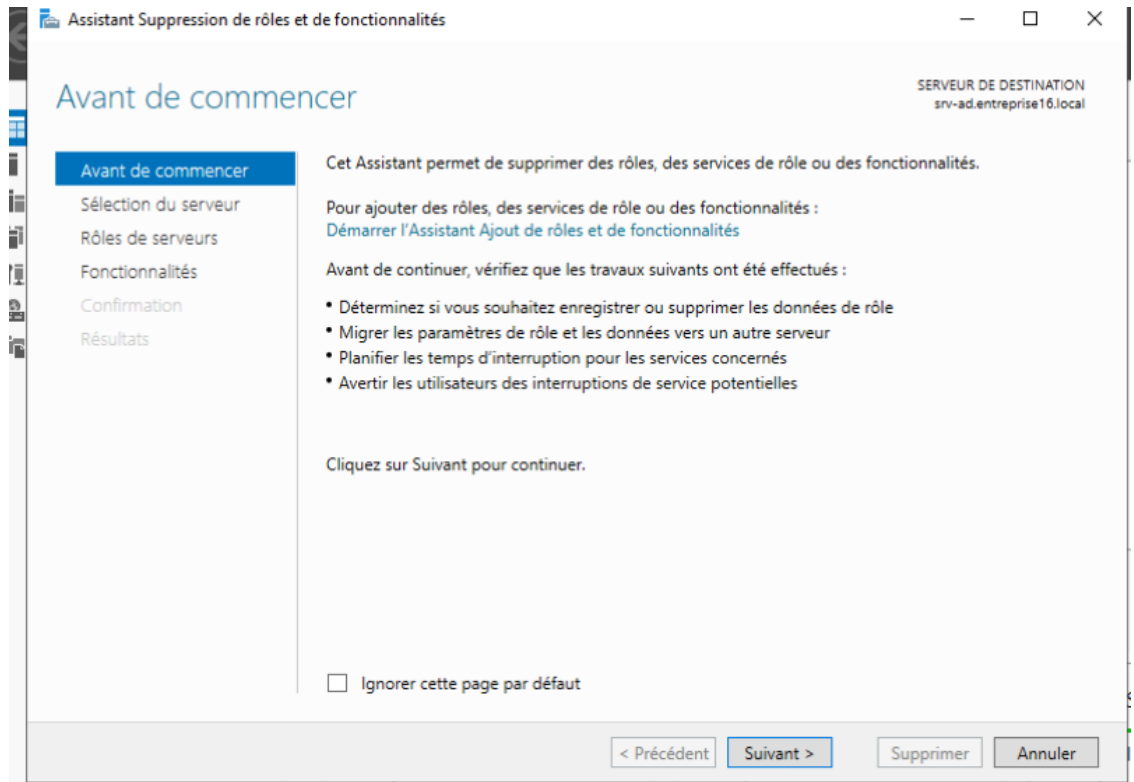
- Avant le déploiement en binôme, il a fallu s'assurer que les deux environnements Proxmox soient configurés de manière identique :
 - Même plan d'adressage réseau (LAN en 192.168.1.0/24)
 - pfSense configuré en 192.168.1.1
 - Deux serveurs AD avec adresses fixes (étudiant A : 192.168.1.5, étudiant B : 192.168.1.6)
 - Un domaine commun(on va voir comment on fait)

Domaine en coummun

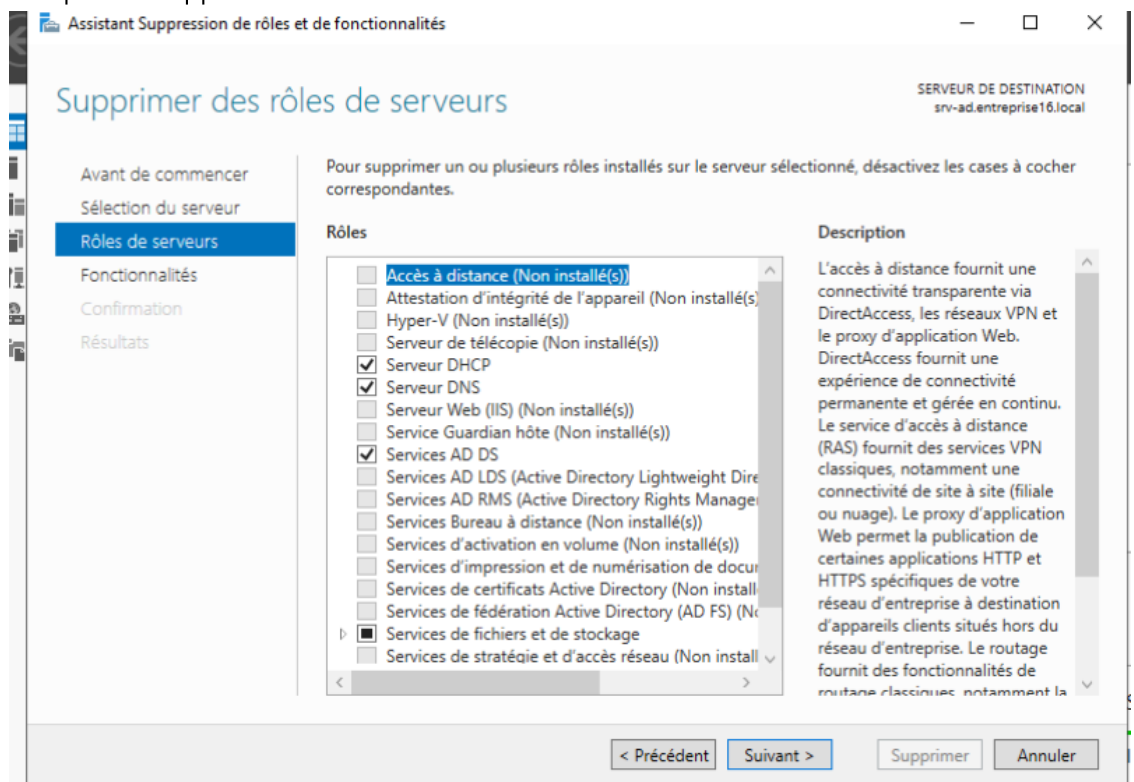
- Au début du TP, chaque étudiant avait installé son propre Active Directory avec un domaine différent. Lors de la mise en binôme, il fallait obligatoirement travailler dans un domaine commun, ce qui a nécessité la rétrogradation des deux serveurs AD.

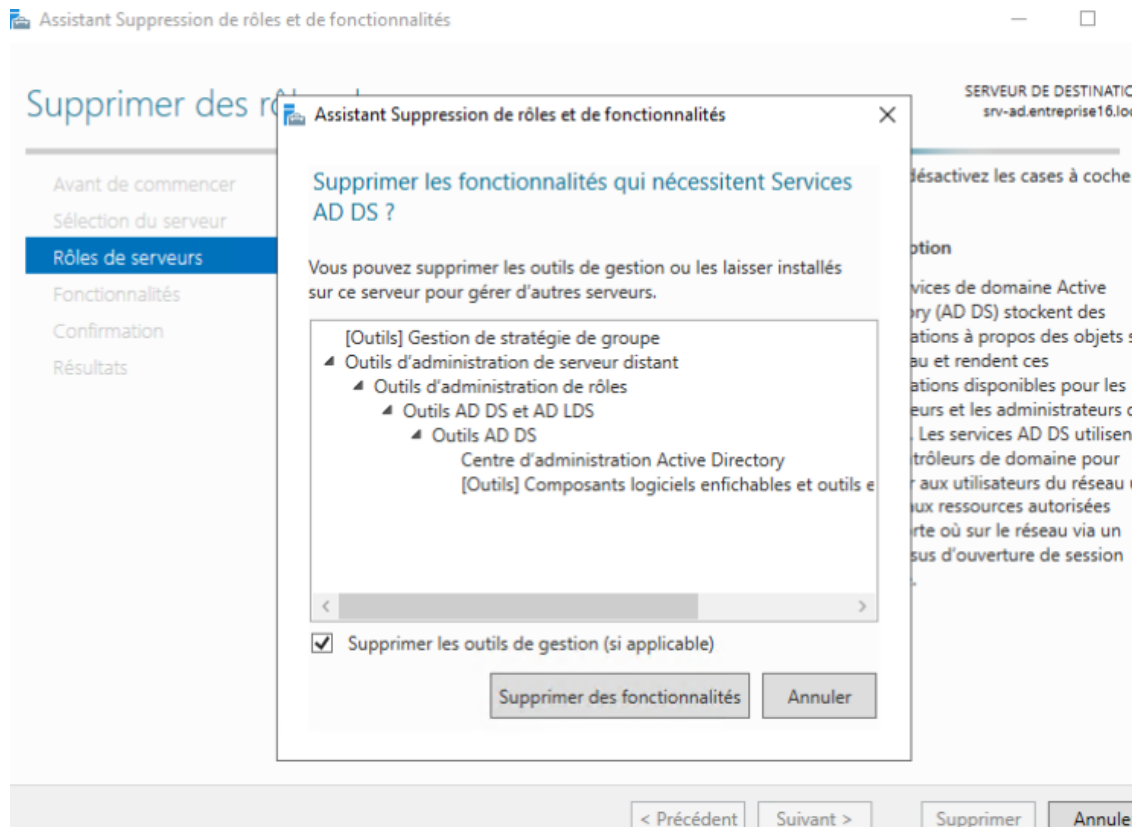
Rétrogradation de mon AD(AD-A)

- De mon côté, j'ai rétrogradé mon serveur pour qu'il ne soit plus contrôleur de domaine et redevienne un serveur standard:
 - J'ai ouvert le Gestionnaire de serveur, puis je me suis placé dans Gérer en haut à droite pour cliquer sur Supprimer des rôles et fonctionnalités.



- Ensuite, on clique sur Suivant à deux reprises, on appuie sur AD DS pour arriver avec l'assistant, puis on clique sur Supprimer des fonctionnalités:

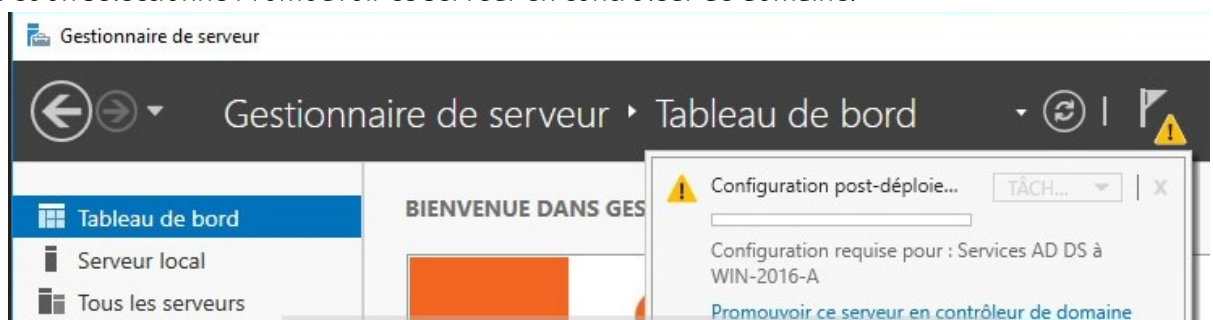




- Une erreur lors de la validation va alors s'afficher à l'écran, on vous indique que le serveur doit être rétrogradé avant de pouvoir supprimer ce rôle. Cliquez sur "Rétrograder le contrôleur de domaine", un second assistant va s'exécuter.
- On coche forcer la suppression de ce contrôleur de domaine ensuite sur suivant.
- Ya un avertissement on met suivant, on laisse par défaut et on met suivant.
- On creer un mot de passe (on peut reutiliser le meme)
- On clique sur retrograder et on attends
- Ensuite on confime et on met supprimer pour redemarer.

Promotion des serveurs Active Directory après rétrogradation

- Une fois le serveur redémarré, on ouvre le Gestionnaire de serveur, on clique sur le drapeau en haut à droite et on sélectionne Promouvoir ce serveur en contrôleur de domaine.



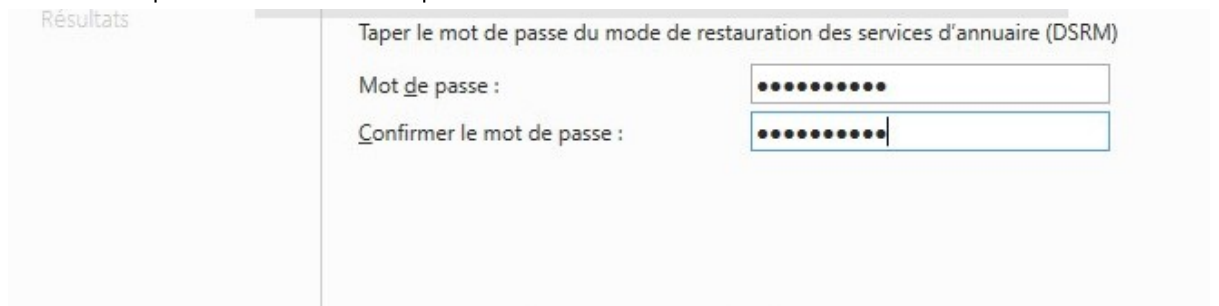
- Une fois dedans, on arrive sur configuration de déploiement et la on selectionne "ajouter une nouvelle forêt"



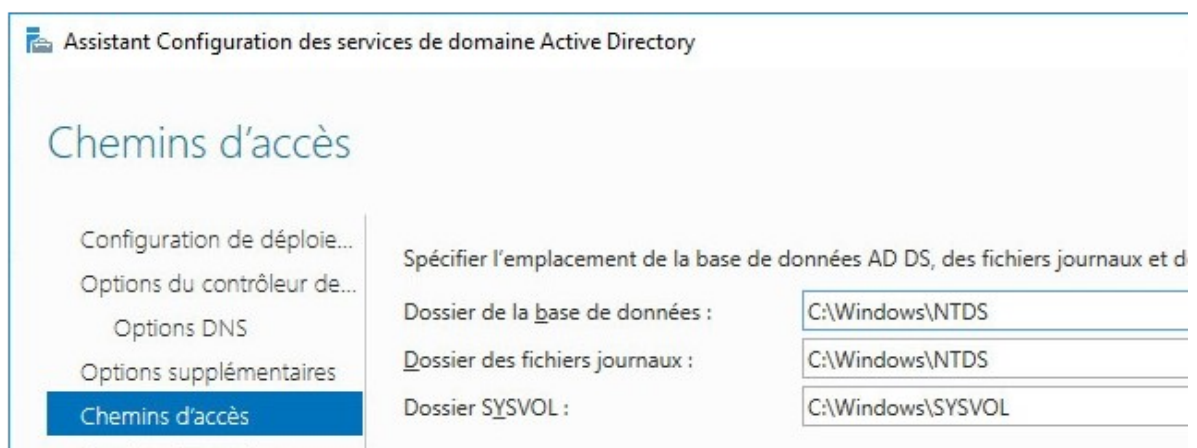
- On arrive sur les options du contrôleur de domaine et on met les options suivantes:



- Dans la même étape on met un mot de passe:



- Sur l'option de DNS on met suivant, pour le NetBios on met suivant.
- Sur le chemin d'accès on laisse par défaut:



- Dans 'Examiner les options', on vérifie les paramètres puis on clique sur 'Suivant'.
- On attend la fin de l'installation, puis le système redémarre automatiquement.

Pour AD-B

- Pour AD-B, il faut faire la même procédure de rétrogradation et de promotion. La différence est que, lors de la promotion, il ne faut pas créer une nouvelle forêt, mais rejoindre un domaine existant

(entreprise16.local), afin que les deux serveurs fassent partie du même domaine pour la redondance.

Création d'un réseau inter-site et connectivité

- Pour permettre la communication entre nos deux contrôleurs de domaine (AD-A et AD-B), nous avons configuré un réseau point-à-point et ajouté une deuxième carte réseau sur chaque VM.
- Les deux serveurs Proxmox sont reliés par un câble Ethernet sur l'interface physique eno2.
 - Le pont virtuel vubr10 est associé à cette interface (eno2), ce qui permet aux machines virtuelles connectées à vubr10 de communiquer directement via ce câble.

enx901b0ed3012c						
vubr10	Linux Bridge	Yes	Yes	No	eno2	

- Configuration IP :
 - AD-A : 10.10.10.1/30 avec le premier DNS de 127.0.0.1 et le deuxième de AD-B
 - AD-B : 10.10.10.2/30 avec le premier DNS de AD-A et le deuxième 127.0.0.1
 - Pas de gateway configurée sur cette carte réseau.
- Pour tester la connectivité il suffit juste de pinger les deux machines entre eux.
 - Le ping de AD-A vers AD-B:

```
Microsoft Windows [version 10.0.20348.169]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\AdminTier1.ENTREPRISE16>ping 10.10.10.2

Envoi d'une requête 'Ping' 10.10.10.2 avec 32 octets de données :
Réponse de 10.10.10.2 : octets=32 temps<1ms TTL=128
Réponse de 10.10.10.2 : octets=32 temps<1ms TTL=128
Réponse de 10.10.10.2 : octets=32 temps<1ms TTL=128

_
```

- On vérifie aussi les résolutions DNS depuis AD-B avec les commandes
 - nslookup entreprise16.local

```
Invite de commandes

Microsoft Windows [version 10.0.20348.169]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\AdminTier1.ENTREPRISE16>nslookup entreprise16.local
Serveur : localhost
Address: 127.0.0.1

Nom : entreprise16.local
Addresses: 10.10.10.2
           192.168.1.5
           10.10.10.1
           192.168.1.6

C:\Users\AdminTier1.ENTREPRISE16>_
```

- nslookup SRV-AD(AD-A).entreprise16.local

```
C:\Users\AdminTier1.ENTREPRISE16>nslookup srv-ad.entreprise16.local
Serveur : localhost
Address: 127.0.0.1

Nom :     srv-ad.entreprise16.local
Addresses: 192.168.1.5
           10.10.10.1

C:\Users\AdminTier1.ENTREPRISE16>
```

Vérifier la réplication et la redondance

- L'objectif ici est de s'assurer que les deux contrôleurs de domaine (AD-A et AD-B) ont les mêmes données et que la réplication fonctionne correctement.
- Sur AD-A et AD-B, exécuter les commandes suivantes :
 - repadmin /replsummary
 - repadmin /showrepl
- Sur le AD-A et AD-B exécuter:
 - Get-ADUser -Filter * | measure
 - Les deux AD doivent renvoyer le même nombre d'utilisateurs, confirmant que la réplication fonctionne.

```
PS C:\Users\AdminTier1.ENTREPRISE16> Get-ADUser -Filter * | measure
Count      : 5
Average    :
Sum        :
Maximum    :
Minimum    :
Property   :
```

- Depuis un client du LAN de A exécuter:
 - whoami /fqdn
 - nltest /dsgetdc:entreprise16.local
 - Ça doit tomber parfois sur l'AD-A et AD-B
- Depuis un client du LAN de B refaire de meme et faut avoir le meme resultat.

Test en cas de panne

- Éteindre AD-A puis refaire les tests depuis les clients.
 - L'AD actif doit être AD-B >> Rallumer AD-A, éteindre AD-B, refaire les tests.
 - L'AD actif doit être AD-A.

Cela permet de vérifier que la redondance fonctionne et que les services restent accessibles même si un DC tombe.

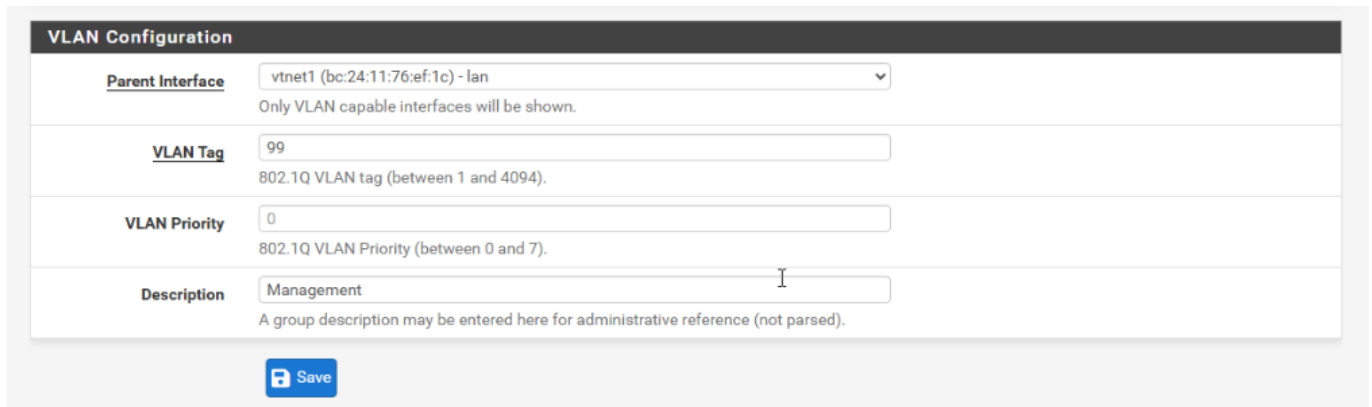
Sécurisation, supervision et services réseau - Proxmox

I - Cloisonnement et durcissement du réseau

I/I - VLAN Management

I/I/I - Création du VLAN Management

Tout d'abord, il va falloir créer une interface VLAN 99 qui va correspondre au VLAN Management, pour cela il va falloir aller sur: **Interfaces -> Assignements -> VLANs** puis cliquer sur **Add**.



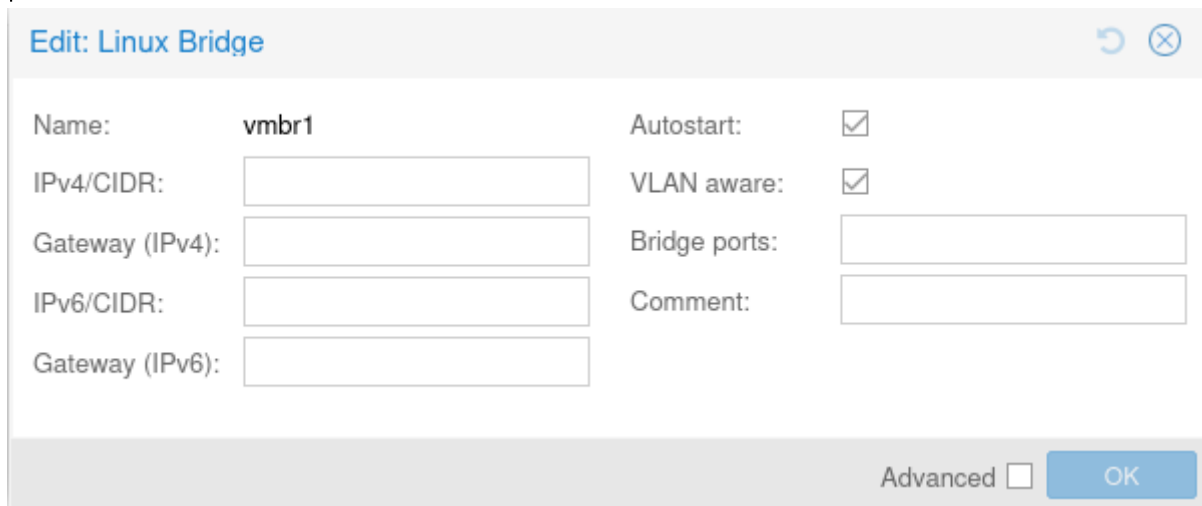
The screenshot shows the 'VLAN Configuration' form in Proxmox. It has the following fields:

- Parent interface:** A dropdown menu showing 'vtnet1 (bc:24:11:76:ef:1c) - lan'. Below it, a note says 'Only VLAN capable interfaces will be shown.'
- VLAN Tag:** A text input field containing '99'. Below it, a note says '802.1Q VLAN tag (between 1 and 4094).'
- VLAN Priority:** A text input field containing '0'. Below it, a note says '802.1Q VLAN Priority (between 0 and 7).'
- Description:** A text input field containing 'Management'. Below it, a note says 'A group description may be entered here for administrative reference (not parsed).'

At the bottom of the form, there is a blue 'Save' button.

Après l'avoir configuré, clique sur **Save**.

Il ne faut pas oublier d'activer le support de VLANs sur l'interface *vbr1* qui correspond à l'interface LAN. Pour cela il va falloir se rendre sur: **Datacenter -> pve -> System -> Network**. On clique sur l'interface *vbr1*, puis sur le bouton **Edit** et on coche la case **VLAN aware**.



The screenshot shows the 'Edit: Linux Bridge' configuration window for the interface *vbr1*. It has the following fields:

- Name:** vbr1
- Autostart:**
- IPv4/CIDR:**
- VLAN aware:**
- Gateway (IPv4):**
- Bridge ports:**
- IPv6/CIDR:**
- Comment:**
- Gateway (IPv6):**

At the bottom right, there is an 'Advanced' checkbox (unchecked) and an 'OK' button.

I/I/II - Configuration du VLAN Management sur pfSense

On se rend sur le pfSense puis on introduit l'option 1) *Assign Interfaces* en tapant le chiffre 1. Le rendu final doit être le suivant:

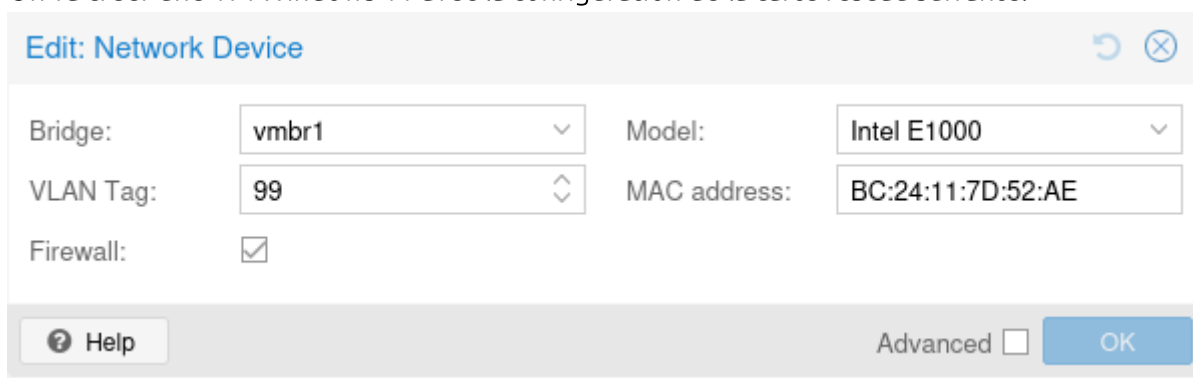
```
The interfaces will be assigned as follows:  
WAN   -> vtnet0  
LAN   -> vtnet1  
OPT1  -> vtnet2  
OPT2  -> vtnet1.99  
  
Do you want to proceed [y|n]? y
```

Ensuite il va falloir configurer l'adresse IP du VLAN Management. Pour cela il faut choisir l'option 2) *Set interface(s) IP address* en tapant le chiffre 2. Le rendu final doit être le suivant:

```
MANAGEMENT (opt2) -> vtnet1.99 -> v4: 192.168.99.1/24
```

I/I/III - Ajout d'une VM Windows Admin

On va créer une VM Windows 11 avec la configuration de la carte réseau suivante:



Bridge: Model:
VLAN Tag: MAC address:
Firewall:

Help Advanced OK

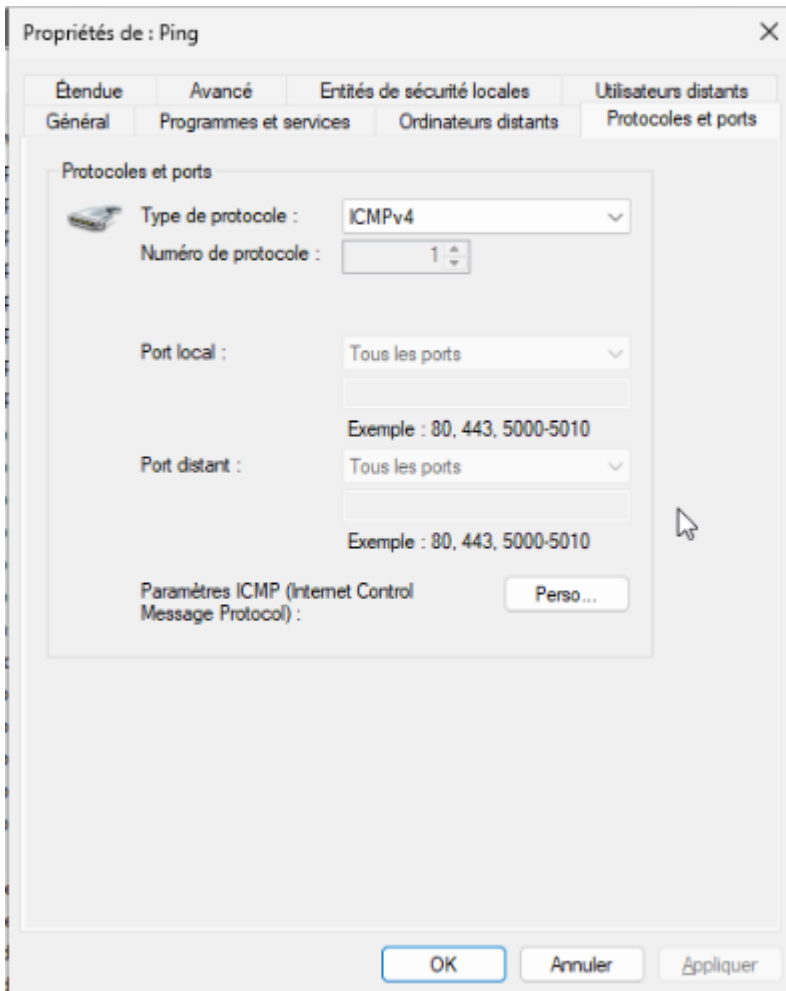
Et la configuration IP suivante:

Attribution d'adresse IP :	Manuel
Adresse IPv4 :	192.168.99.10
Masque IPv4:	255.255.255.0
Passerelle IPv4 :	192.168.99.1

Pour communiquer avec notre passerelle, il va falloir créer la règle pare-feu suivante:

<input type="checkbox"/>	<input checked="" type="checkbox"/>	5/12.08 MiB	IPv4*	MANAGEMENT subnets	*	This Firewall (self)	*	*	none	
--------------------------	-------------------------------------	-------------	-------	--------------------	---	----------------------	---	---	------	--

Ainsi que la création d'une règle ping sur le pare-feu de la VM Admin:



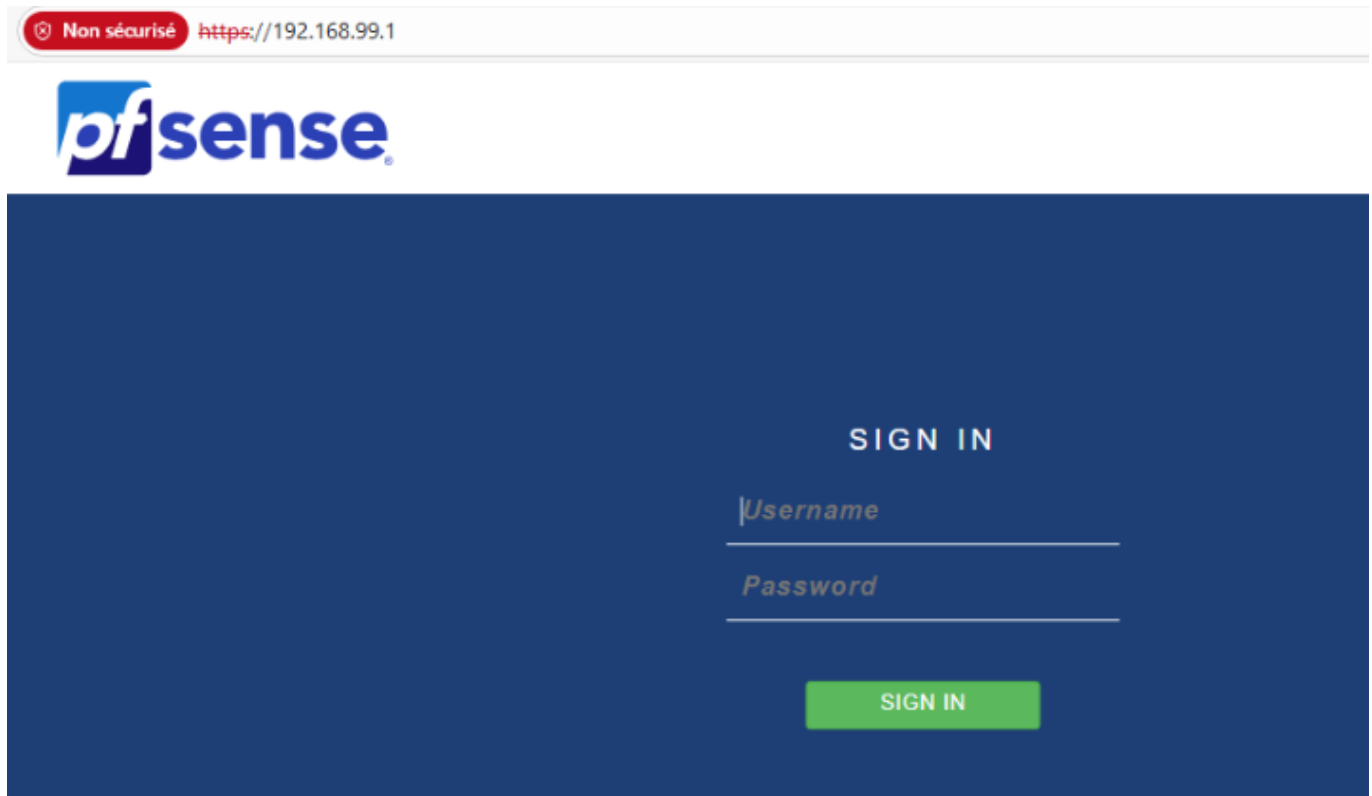
Test de Ping de la VM Admin vers sa passerelle par défaut:

```
C:\Users\Windows11-client>ping 192.168.99.1

Envoi d'une requête 'Ping' 192.168.99.1 avec 32 octets de données :
Réponse de 192.168.99.1 : octets=32 temps<1ms TTL=64
Réponse de 192.168.99.1 : octets=32 temps<1ms TTL=64
Réponse de 192.168.99.1 : octets=32 temps<1ms TTL=64
Réponse de 192.168.99.1 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 192.168.99.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

Connexion à l'interface de configuration du pfSense:



I/I/IV - Configuration du pfSense pour limiter l'accès à lui-même

Sur pfSense :

- **System -> Advanced -> Admin Access**

- Activer uniquement HTTPS
- Limiter l'écoute à Management. Pour cela il va falloir créer des règles pare-feu sur toutes les interfaces sauf Management:

<input type="checkbox"/>		0/0 B	IPv4 TCP	LAN subnets	*	This Firewall (self)	*	*	none
--------------------------	--	-------	----------	-------------	---	----------------------	---	---	------

- Désactiver HTTP et SSH pour les autres interfaces. Tout d'abord on crée l'Alias suivant. Pour cela il faut se rendre sur **Firewall -> Aliases -> Ports**:

Firewall Aliases Ports				
Name	Type	Values	Description	Actions
WEB_PORTS	Port(s)	80, 443		

Puis sur chaque interface, on crée les règles suivantes:

<input type="checkbox"/>		0/0 B	IPv4 TCP	*	*	This Firewall (self)	WEB_PORTS	*	none	
<input type="checkbox"/>		0/0 B	IPv4 TCP	*	*	This Firewall (self)	22 (SSH)	*	none	

Normalement, les autres appareils peuvent encore se connecter sur l'interface de configuration du pfSense. Pour régler ce problème il va falloir se rendre sur **System -> Advanced -> Admin Access**. Et on coche l'option suivante:

Anti-lockout Disable webConfigurator anti-lockout rule

When this is unchecked, access to the webConfigurator on the LAN interface is always permitted, regardless of the user-defined firewall rule set. Check this box to disable this automatically added rule, so access to the webConfigurator is controlled by the user-defined firewall rules (ensure a firewall rule is in place that allows access, to avoid being locked out!) *Hint: the "Set interface(s) IP address" option in the console menu resets this setting as well.*

II - Mise en place d'un DNS local et d'un proxy

II/I - DNS local sur pfSense

Tout d'abord il va falloir activer le DNS Resolver (Unbound) depuis l'interface de configuration du pfSense. Puis on se rend sur **Services -> DNS Resolver** et on coche *Enable DNS Resolver*.

Ensuite, sur *Network Interfaces*, on va selectionner les interfaces LAN, Management et Localhost.

Enfin, il faut cocher *Register DHCP leases in the DNS Resolver* et *Register DHCP static mappings in the DNS Resolver*.












Pour ajouter les enregistrements manuels, on se rend sur: **Services -> DNS Resolver -> onglet Hosts Overrides** et on ajoute les lignes suivantes:

Host Overrides				
Host	Parent domain of host	IP to return for host	Description	Actions
pfSense	local	192.168.99.1		 
webdmz	local	192.168.2.100		 

II/II - Proxy Squid + filtrage SquidGuard

II/II/I - Installation de Proxy Squid

Pour installer Proxy Squid, il faut se rendre sur: **System -> Package Manager -> Available Packages** et on installe *squid* et *squidGuard*.

Installed Packages		Available Packages		
Name	Category	Version	Description	Actions
✓ squid	www	0.4.46	High performance web proxy cache (3.5 branch). It combines Squid as a proxy server with its capabilities of acting as a HTTP / HTTPS reverse proxy. It includes an Exchange-Web-Access (OWA) Assistant, SSL filtering and antivirus integration via C-ICAP.	  
Package Dependencies:				
 squidclamav-7.2  squid_radius_auth-1.10  squid-6.3  c-icap-modules-0.5.5_1				
✓ squidGuard	www	1.16.19	High performance web proxy URL filter.	 
Package Dependencies:				
 squidguard-1.4_15  pfSense-pkg-squid-0.4.46				

II/II/II - Configuration de Proxy Squid

Tout d'abord on se rend sur: **Services -> Squid Proxy Server** et on le configure de la façon suivante:

- Cocher *Enable Squid Proxy*.
- Cocher *Allow Users on interface*.
- Cocher *Transparent HTTP Proxy*.

- *Transparent Proxy Interface(s)* : LAN.

II/II/III - Configuration de SquidGuard

Tout d'abord on se rend sur: **Services -> SquidGUard Proxy Filter** et on le configure de la façon suivante:

- Cocher *Enable*.
- Cocher *Enable GUI log*.
- Cocher *Enable log*.
- Cocher *Blacklist* et renseigner l'url `http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gz` dans la zone de texte *Blacklist URL*.
- Cliquer sur *Save*.
- Aller dans l'onglet **Services -> SquidGUard Proxy Filter -> Blacklist** et télécharger la blacklist `http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gz` en appuyant sur *Download*.

Blocage de certains sites



Pour bloquer certaines catégories de sites Web, il va falloir se rendre sur **Services -> SquidGUard Proxy Filter -> Common ACL**. Puis on clique sur le +:



On va *deny* les catégories *social_networks*, *adult* et *malware*.

- Cocher *Do not allow IP-Addresses in URL* ainsi que *Log* puis *Save*.
- Redémarrer le service squid et squidGuard en allant dans **Status -> Services**.

Sur la VM client du LAN, on peut encore accéder à `http://facebook.com` même après avoir vidé le cache avec la commande `ipconfig /flushdns`. Pour le bloquer, il va falloir se rendre sur **Services -> DNS Resolver -> onglet Hosts Overrides** et on ajoute un nouveau avec la configuration suivante:

www	facebook.com	127.0.0.1	 
-----	--------------	-----------	---

Si on essaie d'accéder au site, cela ne fonctionnera pas.

III - Supervision et journalisation centralisée

III/I - Création d'une VM Debian

Tout d'abord, il faut créer une VM Debian sur le LAN avec la configuration suivante:

- Nom : Serveur-Logs
- Bridge : vmbr1
- Adresse IP : 192.168.1.20/24
- Passerelle : 192.168.1.1
- DNS : 192.168.1.1

III/II - Installation et configuration de rsyslog

Pour installer *rsyslog*, il faut utiliser la commande suivante `apt install rsyslog`.

Ensuite, on utilise la commande `nano /etc/rsyslog.conf` pour décommenter les lignes suivantes:

```
# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514")

# provides TCP syslog reception
module(load="imtcp")
input(type="imtcp" port="514")
```

Et on redémarre `rsyslog` avec la commande `systemctl restart rsyslog` et `systemctl enable rsyslog`.

Il va falloir ensuite ouvrir le port 514 TCP et UDP sur le pfSense:



Configuration de pfSense pour envoyer ses logs

Tout d'abord il faut se rendre sur **Status -> System Logs -> Settings** et faire la configuration suivante:

- Cocher *Enable Remote Logging*.
- *Remote log servers* : 192.168.1.20/24.
- Sélectionner System Events, Firewall Events, VPN Events sur *Remote Syslog Contents*.
- *Save*.

On peut vérifier la réception sur la Debian avec la commande suivante `sudo tail -f /var/log/syslog`.

III/III - ntopng (supervision graphique)

Pour avoir une supervision graphique, on va utiliser le logiciel `ntopng`. Pour cela, il faut taper les commandes suivantes sur le serveur de logs:

```
get https://packages.ntop.org/apt/bullseye/all/apt-ntop.deb
apt install ./apt-ntop.deb
apt-get clean all
apt-get update
apt-get install ntopng
```

Pour accéder à cette interface, j'utilise l'URL `192.168.1.20:3000` sur la VM client sur le LAN.

IV - Sauvegarde, restauration et automatisation

IV/I - Activation du service SSH

Sur l'interface de configuration du pfSense, on se rend sur **System -> Advanced -> Admin Access** et on coche *Secure Shell Server*. Ensuite sur le pfSense, on choisit l'option `8) Shell` et on tape la commande suivante:

```
Enter an option: 8
[2.7.2-RELEASE][root@pfSense.home.arpa]/root: pfssh.php playback svc restqrt ssh
d
```

Ensuite, on va créer une clé SSH et la copier sur l'entrée admin de 192.168.1.1, pour cela on va taper les commandes suivantes sur le serveur de logs:

```
ssh-keygen  
ssh-copy-id admin@192.168.1.1
```

On peut maintenant se connecter via SSH au pfSense:

```
root@debian12:~# ssh admin@192.168.1.1  
(admin@192.168.1.1) Password for admin@pfSense.home.arpa:  
QEMU Guest - Netgate Device ID: 2548397f117e269cb31d  
  
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***  
  
WAN (wan)      -> vtnet0      -> v4/DHCP4: 10.50.0.54/8  
LAN (lan)      -> vtnet1      -> v4: 192.168.1.1/24  
DMZ (opt1)     -> vtnet2      -> v4: 192.168.2.1/24  
MANAGEMENT (opt2) -> vtnet1.99   -> v4: 192.168.99.1/24  
  
0) Logout (SSH only)          9) pfTop  
1) Assign Interfaces          10) Filter Logs  
2) Set interface(s) IP address 11) Restart webConfigurator  
3) Reset webConfigurator password 12) PHP shell + pfSense tools  
4) Reset to factory defaults  13) Update from console  
5) Reboot system              14) Disable Secure Shell (sshd)  
6) Halt system                 15) Restore recent configuration  
7) Ping host                   16) Restart PHP-FPM  
8) Shell  
  
Enter an option: _
```

IV/II - Sauvegarde automatisée

Tout d'abord on crée le répertoire sur le serveur de logs avec la commande `mkdir /backup`. Puis la commande `crontab -e` et on tape la ligne suivante:

```
0 20 * * * scp admin@192.168.1.1:/cf/conf/config.xml /backup/pfsense-$(date +%F) .xml
```