Infrastructure réseau sécurisée

Ce document présente l'installation ainsi que la configuration des différentes machines afin d'avoir une infrastructure sécurisé.

ITIC PARIS

Version : 2.0

Documentation

29/05/2025

Kevin ORTIZ / 24-25 INIT-M1-MPI-CS

AUTEUR

Nom	Prénom	Fonction	Signature
ORTIZ	Kevin	Service Informatique	

VALIDATEUR

Formateur	Fonction	Signature
M. RADO L.	Formateur	

DIFFUSION

Société	Site	Fonction	Période
ITIC Paris	Paris	Documentation	2025-2026

SUIVI DES VERSIONS

Version	Date	Raison	Auteur
1.0	23/04/2025	Création du document	Kevin Ortiz
2.0	29/04/2025	Ajout de la deuxième partie du TP : Haute disponibilité.	Kevin Ortiz

CONTEXTE

Description
Ce document a pour objectif de présenter en détail la mise en place d'une infrastructure réseau. Dans la première partie du projet, nous procéderons à l'installation de pfSense avec un réseau LAN, à la mise en place d'un contrôleur de domaine Active Directory, ainsi qu'à la configuration d'un poste client. Un second réseau LAN (OPT1) sera ensuite ajouté sur pfSense. Nous détaillerons également la configuration de ce nouveau réseau, le déploiement des différentes GPO pour les utilisateurs du domaine, ainsi que l'importation d'une liste d'utilisateurs à partir d'un fichier CSV dans l'Active Directory. Dans la deuxième partie, nous mettrons en place un second PfSense afin de garantir la haute disponibilité : en cas de panne du premier pare-feu, le second prendra automatiquement le relais pour assurer la continuité du service.

Table des matières

1) Présentation de la première partie du projet

1.1) Contexte

Pour la première partie du TP, nous allons mettre en place une infrastructure réseau virtualisée visant à reproduire un environnement d'entreprise sécurisé. L'objectif est de permettre la gestion centralisée des utilisateurs, des ressources partagées et des politiques de sécurité.

L'infrastructure sera composée d'un pare-feu (PfSense), d'un contrôleur de domaine (Active Directory) et d'un poste client. Après avoir configuré un réseau local (LAN) via PfSense, nous intégrerons le poste client au domaine. Nous ajouterons ensuite un second réseau (OPT1) pour simuler un sous-réseau distinct.

Le projet inclut également le déploiement de stratégies de groupe (GPO), la configuration des services réseau essentiels (DHCP, DNS, partage de dossiers), ainsi que l'importation d'une liste d'utilisateurs à partir d'un fichier CSV dans l'Active Directory.

1.2) Prérequis

Pour la réalisation de ce TP, l'environnement de virtualisation PROXMOX a été utilisé afin de simuler l'ensemble de l'infrastructure réseau. Trois machines virtuelles ont été créées :

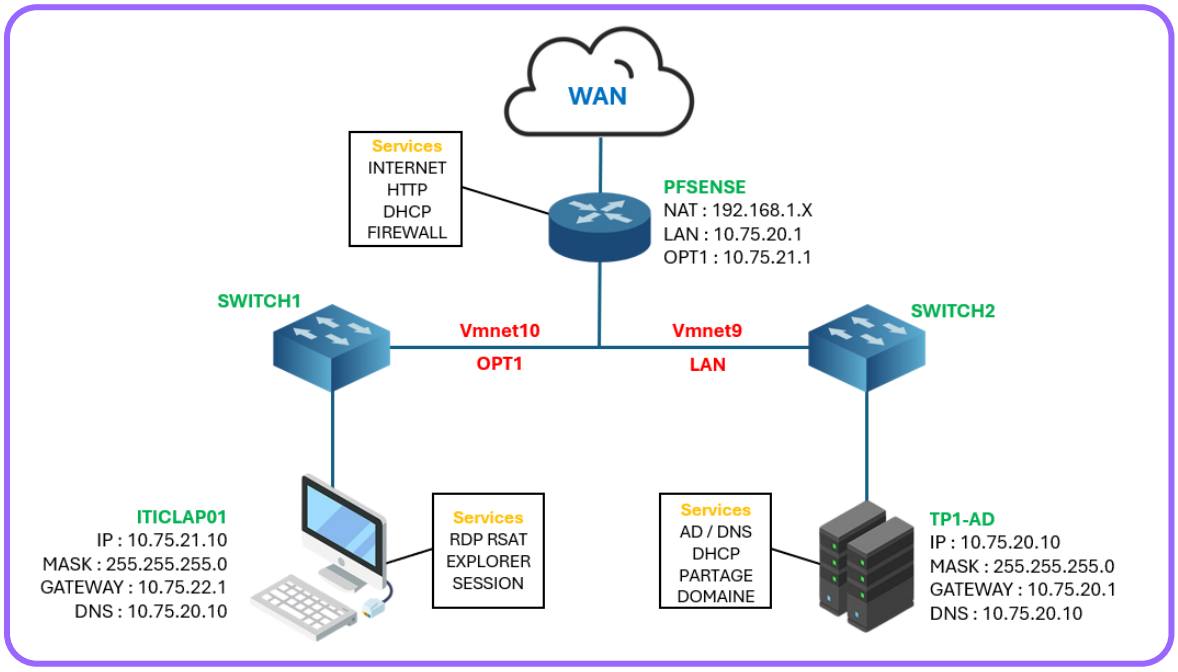
- **PfSense** : Équipement intermédiaire chargé d'assurer la sécurité et la communication entre les réseaux virtuels et l'accès à Internet.
  - Interfaces réseau :
    - WAN : Connectée à internet (NAT)
    - LAN : réseau principal pour le domaine Active Directory
    - OPT1 : réseau secondaire isolé destiné à accueillir d'autres clients ou services à part du LAN
  - Services configurés :
    - Accès internet (NAT)
    - Serveur DHCP pour distribuer les adresses IP aux machines
    - Accès HTTP pour l'interface d'administration

- **Contrôleur de domaine (Windows Server)** : Serveur central du domaine permettant la gestion des utilisateurs et des politiques de sécurité.
  - Services installés :
    - Active Directory (AD) : Gestion des comptes utilisateurs et des machines
    - DNS : résolution de noms internet au domaine
    - DHCP : distribution d'adresses IP
    - Partage de dossiers : Pour centraliser les documents utilisateurs
    - Gestion du domaine : Intégration des clients et application des GPO

- **Poste client (Windows)** : Poste de travail intégré au domaine pour tester l'environnement utilisateur
  - Utilisation prévue :
    - Connexion au domaine Active Directory
    - Application des stratégies de groupe (GPO)
    - Accès aux partages de dossiers du serveur
    - Utilisation des services comme RSAT (Remote Server Administration Tools)

1.3) Schéma réseau

Le schéma ci-dessous illustre l'architecture réseau mise en place dans ce TP, composée de trois machines virtuelles interconnectées via **PfSense**, avec deux réseaux distincts (**LAN et OPT1**), permettant de simuler un environnement d'entreprise structuré et sécurisé.



2) Déploiement et configuration de la VM Pfsense

2.1) Création de la VM Pfsense

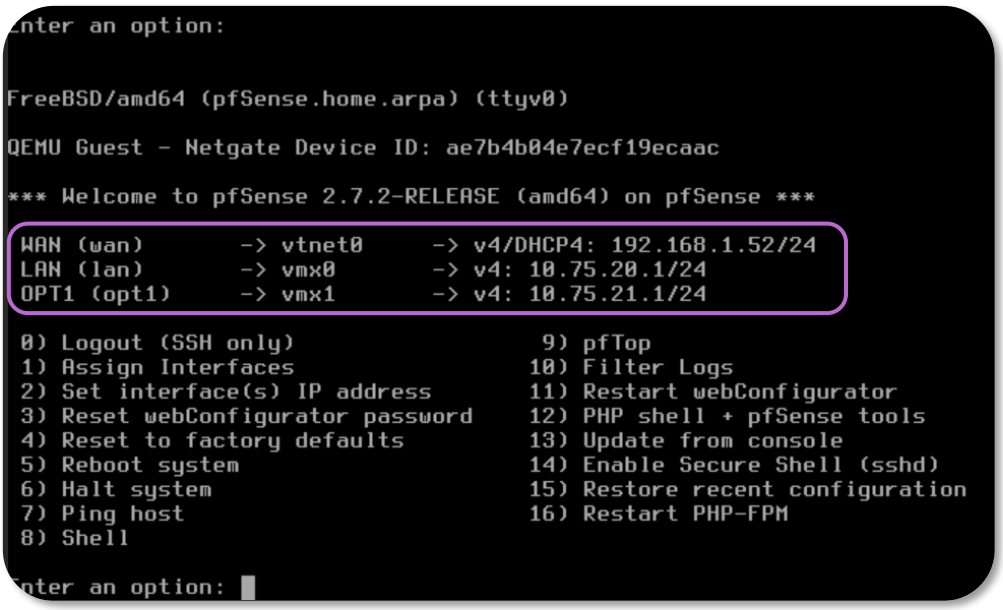
La première machine virtuelle mise en place est celle de **pfSense**, qui jouera le rôle de pare-feu et de routeur pour notre infrastructure. Elle permet la séparation des réseaux et la gestion du trafic entre les différentes machines.

Dans **Proxmox**, la VM a été configurée avec les ressources suivantes :

Pour cette VM, j'ai attribué 2 Go de RAM, ainsi qu'un seul socket et un core pour le processeur, car elle n'aura pas besoin de beaucoup de ressources.

2.2) Configuration des interfaces réseau

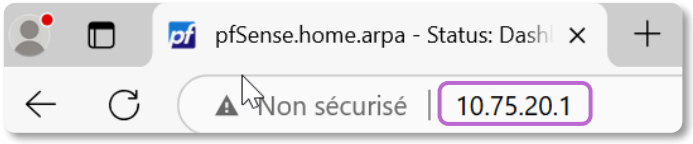
Une fois l'installation de pfSense terminée, nous procéderons à la configuration des interfaces réseau, y compris le NAT, le LAN et l'OPT1. Le NAT, qui correspond à l'interface WAN, sera configuré en DHCP, car c'est cette interface qui nous fournira l'accès à Internet.
Pour l'interface **LAN**, nous lui attribuerons l'IP **10.75.20.1/24**, tandis que pour l'interface **OPT1**, l'IP sera **10.75.21.1/24**. Le masque de sous-réseau **/24 (255.255.255.0)** est choisi car il permet de créer un sous-réseau avec jusqu'à 254 adresses IP utilisables, ce qui est suffisant pour une utilisation typique dans un réseau interne de taille moyenne.



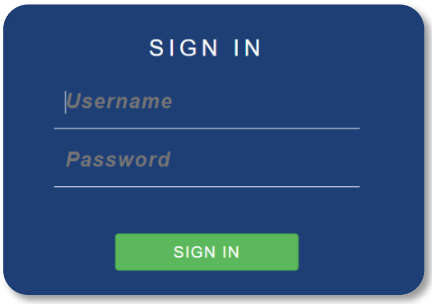
2.3) Règles de pare-feu Pfsense

Une fois les interfaces configurées, il est nécessaire de mettre en place des règles de pare-feu dans pfSense afin d'autoriser la communication entre les machines du réseau **OPT1** et celles du **LAN**. Par défaut, pfSense bloque le trafic inter-réseaux ; il faudra donc créer des règles spécifiques sur l'interface OPT1 pour **permettre le trafic sortant** vers le LAN, tout en garantissant un niveau de sécurité adapté à notre infrastructure.

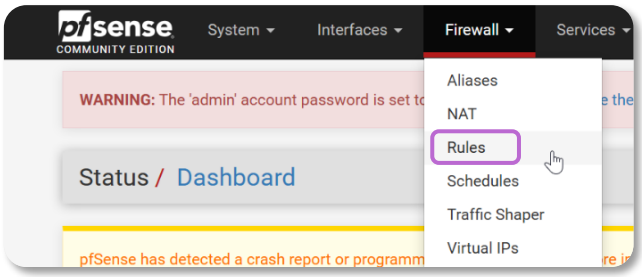
Pour commencer, nous allons accéder à l'interface d'administration de pfSense. Pour cela, il suffit d'ouvrir un navigateur web depuis une machine connectée au réseau **LAN** ou **OPT1**, puis de saisir l'adresse IP correspondante (par exemple, **10.75.20.1 pour le LAN** ou **10.75.21.1 pour l'OPT1**) dans la barre d'adresse.



Ensuite, nous entrerons les identifiants par défaut de pfSense pour accéder à l'interface. En général, le nom d'utilisateur est **admin** et le mot de passe peut être **admin** ou **Pfsense**, selon la version ou l'image installée. Il est donc conseillé de tester les deux, car cela peut varier selon le modèle ou la source d'installation.

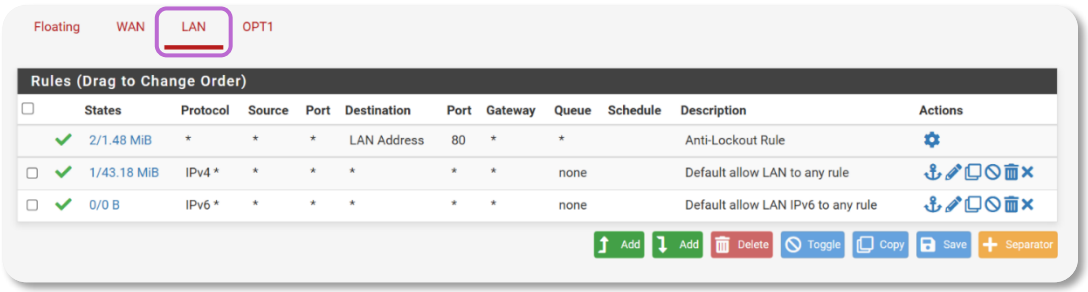


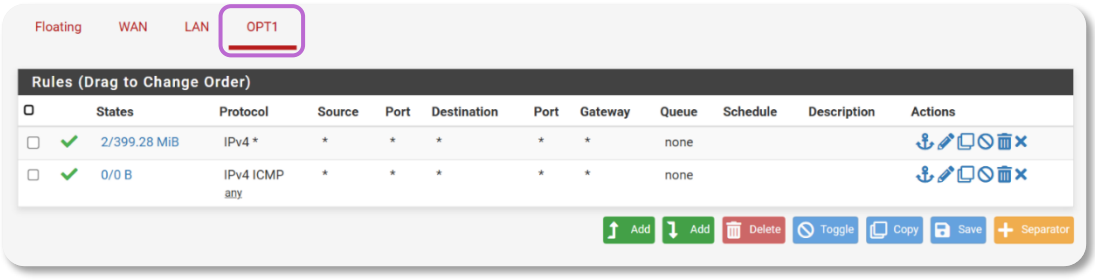
Une fois connecté nous allons aller sur Firewall et sur Rules afin de modifier les règles de notre Pfsense :



Ensuite, nous devons modifier les règles de pare-feu pour les interfaces **LAN** et **OPT1**.
Pour le **LAN**, nous allons éditer la règle existante et la configurer en **ANY**, afin d'autoriser tout le trafic sortant, quelle que soit la source ou la destination.

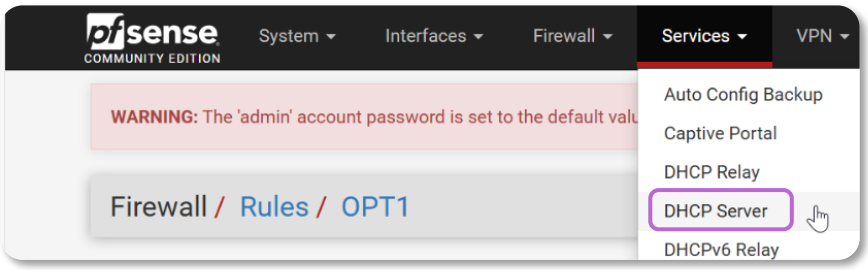
Concernant **OPT1**, cette interface n'a aucune règle par défaut. Il faudra donc ajouter manuellement une ou plusieurs règles, également en **ANY**, pour permettre à toutes les communications de passer. Cela est nécessaire pour autoriser les échanges entre les machines situées sur **OPT1** et celles du **LAN**.



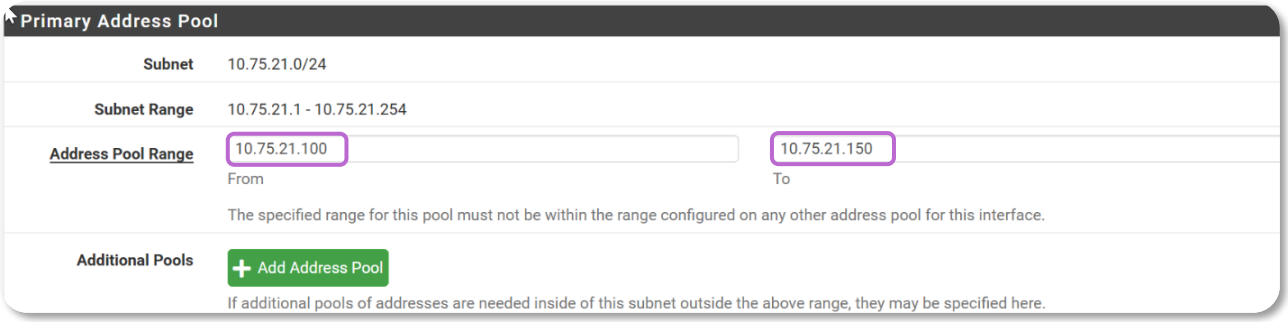


2.4) Configuration du DHCP

Pour configurer le service DHCP dans pfSense, nous allons nous rendre dans l'interface d'administration, cliquer sur **"Services"**, puis sur **"DHCP Server"**. Le service **DHCP (Dynamic Host Configuration Protocol)** permet d'attribuer automatiquement une adresse IP et d'autres paramètres réseau (comme la passerelle et le DNS) aux machines connectées. Cela évite d'avoir à configurer manuellement chaque poste. Dans notre cas, nous allons activer le DHCP **uniquement pour l'interface OPT1**, afin que les machines connectées à ce réseau reçoivent automatiquement une configuration IP compatible avec le sous-réseau **10.75.21.0/24**.



Dans le champ **Primary Address Pool** du serveur DHCP, nous allons définir la plage d'adresses IP que le serveur pourra attribuer aux machines connectées au réseau OPT1. Cela implique de spécifier l'adresse IP de **début** et l'adresse IP de **fin** de la plage.



Dans notre cas nous allons mettre **10.75.20.100** comme IP de début et **10.75.20.150** comme IP de fin.

Puis nous allons cliquer sur ''**Save**'' pour enregistrer notre configuration pour le DHCP

Une fois que nous aurons configuré tous les paramètres nécessaires, y compris l'activation du serveur **DHCP** pour l'interface **OPT1**, ainsi que les règles de communication entre les réseaux **LAN** et **OPT1**, nous aurons un pfSense entièrement configuré, prêt à être utilisé. Cette configuration permettra aux machines du **réseau OPT1** de recevoir des **adresses IP automatiquement** et de communiquer librement avec celles du **réseau LAN**, assurant ainsi une **gestion fluide** du trafic réseau entre les **différentes interfaces**.

3) Déploiement et configuration de la VM Contrôleur de domaine

3.1) Création de la VM Contrôleur de domaine

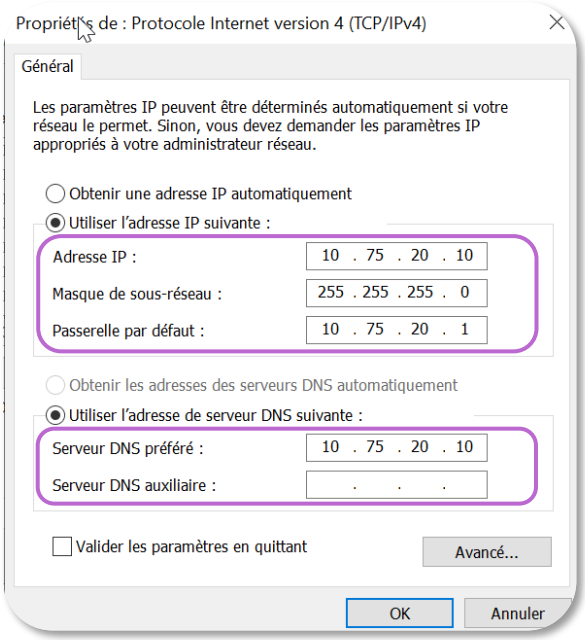
La deuxième machine virtuelle mise en place est celle de **Active Directory (AD)**, qui servira à gérer les utilisateurs, les groupes et les ressources réseau au sein du domaine. Elle assurera également la gestion des politiques de sécurité, des services DNS et DHCP, et facilitera l'administration centralisée de l'infrastructure.

Dans **Proxmox**, la VM a été configurée avec les ressources suivantes :

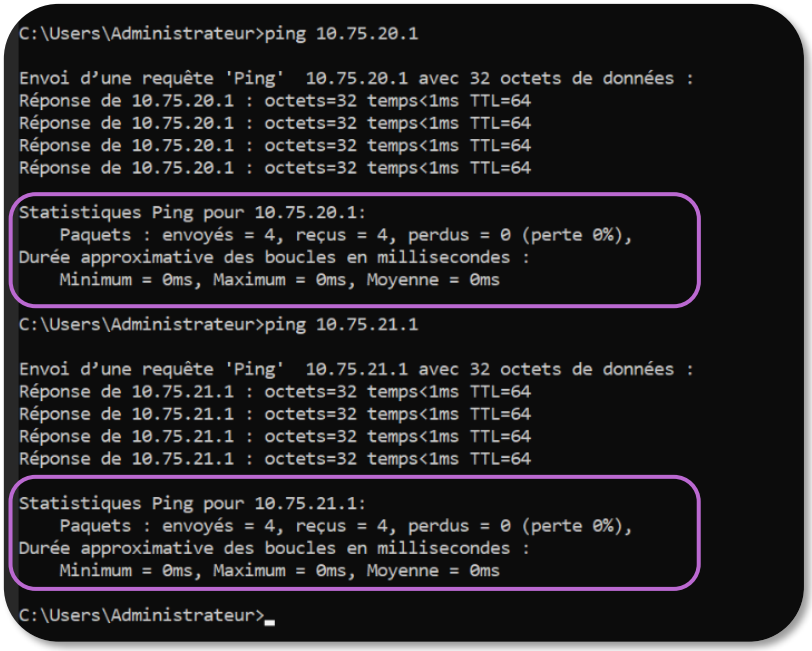
Pour cette VM, j'ai attribué 8 Go de RAM, avec un seul socket et deux cœurs pour le processeur, car le contrôleur de domaine nécessite un peu plus de ressources pour fonctionner

3.2) Configuration des interfaces réseau

Pour la configuration réseau de notre contrôleur de domaine, nous allons lui attribuer une adresse IP disponible dans le réseau **LAN**, à savoir **10.75.20.10**. Comme passerelle par défaut, nous lui assignons l'adresse **IP** du **LAN** (**10.75.20.1**), afin qu'il puisse accéder à Internet et **communiquer avec les autres réseaux via PfSense**. En ce qui concerne le serveur DNS, nous configurons l'adresse IP de notre contrôleur de domaine (**10.75.20.10**) comme serveur DNS, car il est responsable de la gestion des résolutions de noms au sein du domaine et permettra aux machines de résoudre les noms de domaine internes.



Une fois que nous avons terminé la configuration de l'interface réseau de notre contrôleur de domaine, nous allons effectuer un test pour vérifier si celui-ci peut bien communiquer avec les réseaux **LAN** et **OPT1**. Pour cela, nous utiliserons la commande **ping** depuis le contrôleur de domaine :

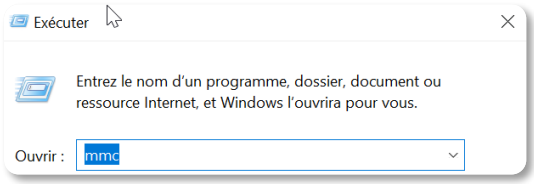


Comme on peut le voir on arrive à ping OPT1 et LAN, donc l'interface réseau de notre contrôleur de domaine ainsi que notre Pfsense sont bien configurés.

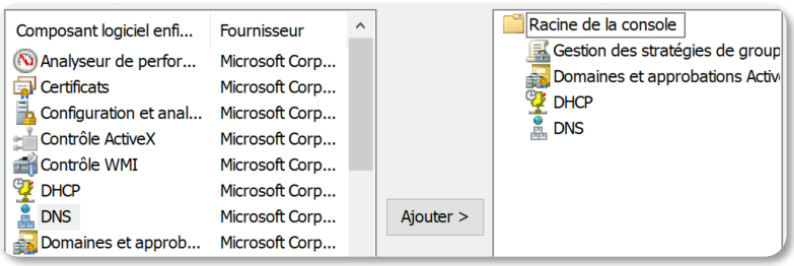
3.3) Création d'un raccourci MMC sur le bureau

Avant de poursuivre la configuration de notre contrôleur de domaine, nous allons créer un raccourci vers le **MMC** (**Microsoft Management Console**) afin de centraliser tous les outils d'administration que nous utiliserons.

Pour cela nous allons faire un **Win + R** et nous allons écrire MMC



Une fois dans MMC nous allons aller sur fichier et ensuite sur ''**Ajouter/supprimer un composant logiciel enfichable**'' puis nous allons **ajouter** les composants logiciels que nous allons utiliser :

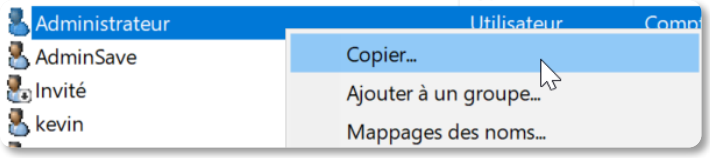


Ensuite, nous allons enregistrer notre console **MMC** sur le bureau ou dans un emplacement de notre choix. Il est toutefois recommandé de l'enregistrer sur le bureau afin d'y accéder rapidement lorsqu'on a besoin de gérer un service.

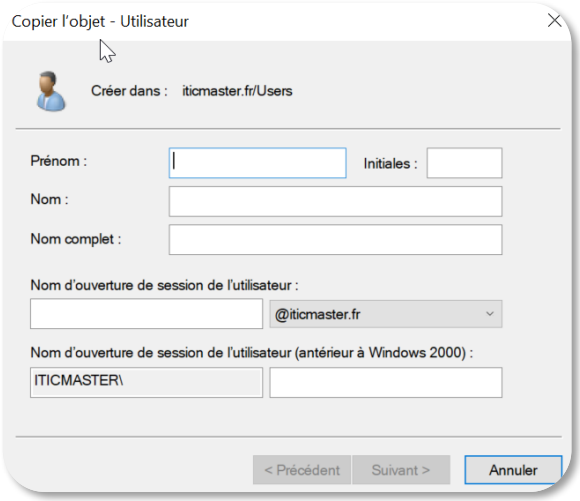
3.4) Création d'un compte d'administrateur de secours

Maintenant, nous allons créer une copie du compte administrateur principal. Ce compte de secours peut être très utile en cas de **problème** avec le compte Admin principal (**compte corrompu, mot de passe perdu, etc.**). Il permettra de garder un **accès au contrôleur de domaine** et d'assurer la **continuité de l'administration du système**.

Pour cela, nous allons ouvrir notre console MMC, accéder à "**Utilisateurs et ordinateurs Active Directory**", puis aller dans notre domaine **iticmaster.fr**. Ensuite, dans le dossier **Utilisateurs**, nous cherchons le compte **Administrateur**, faisons un clic droit dessus et sélectionnons **Copier** afin de créer un nouveau compte administrateur de secours avec des droits équivalents.



Et ensuite, nous allons renseigner les informations nécessaires pour ce nouveau compte, comme le **prénom**, le **nom**, le **nom d'ouverture de session (Nom d'utilisateur)**, ainsi qu'un **mot de passe** sécurisé. On s'assure aussi de cocher les options utiles comme "**L'utilisateur doit changer le mot de passe à la prochaine ouverture de session**" si besoin, ou au contraire décocher cette option si le compte est uniquement destiné à l'administration.



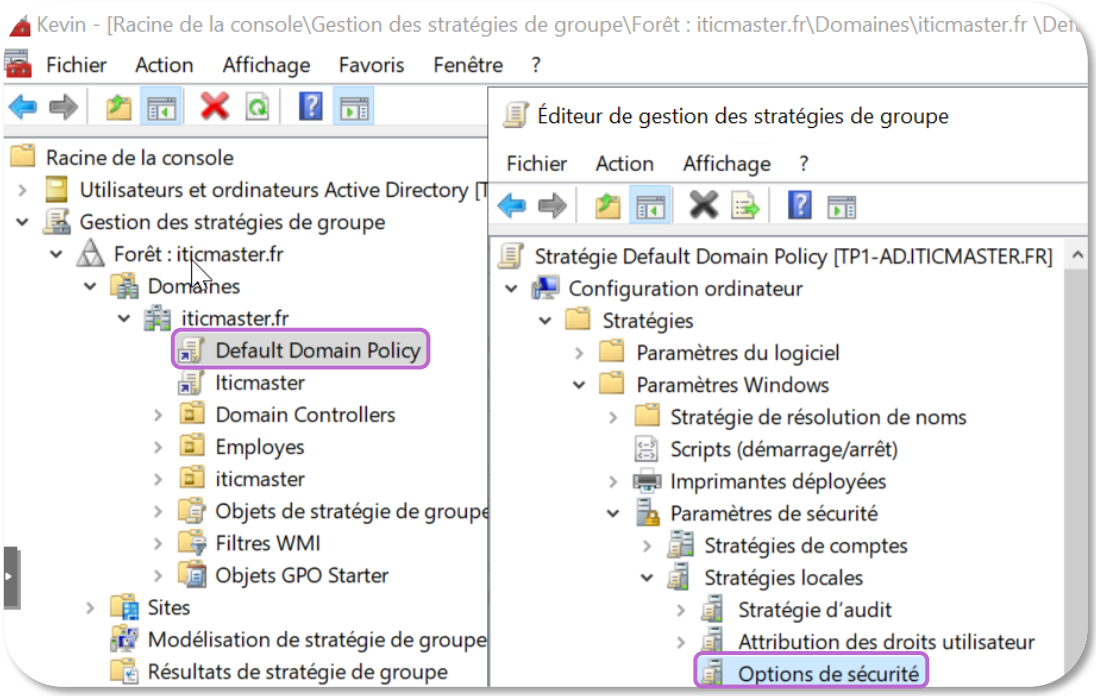
Dans notre cas, l'administrateur de secours sera nommé **AdminBackup** :

3.5) Options de sécurité

Dans cette section, nous allons explorer des options de sécurité pour renforcer davantage la protection de notre contrôleur de domaine.

Nous commencerons par accéder à la gestion des stratégies de groupe, puis sélectionner notre domaine **iticmaster.fr** pour modifier les stratégies du **Default Domain Policy**.

Nous allons aller sur les options de sécurité :

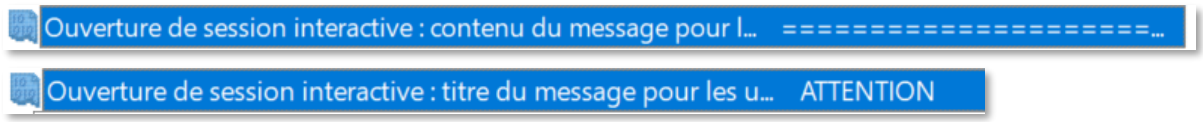


Une fois dans les options de sécurité, nous allons modifier les **paramètres des stratégies** suivantes :

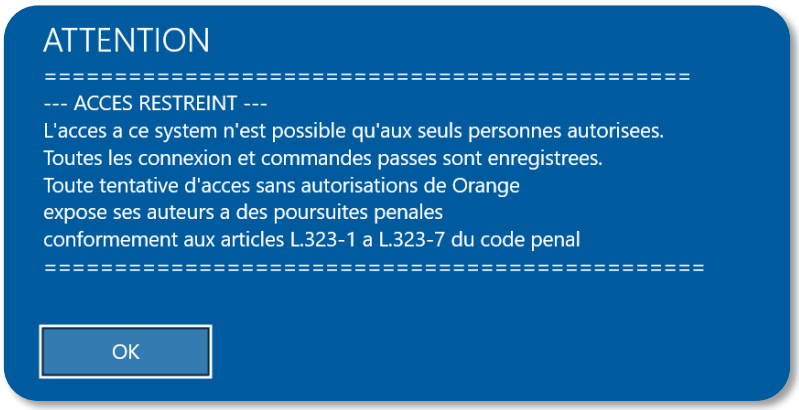
- On va définir ce paramètre de stratégie sur "Désactivé" afin de désactiver le compte invité et empêcher son utilisation.

- On va renommer le compte administrateur pour renforcer la sécurité. En effet, un attaquant tentera souvent en premier d'accéder au compte nommé "**Administrateur**". En le renommant, on complique considérablement ses tentatives d'intrusion.

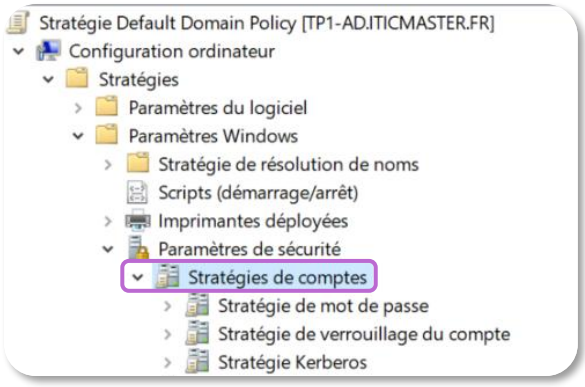
- Pour renforcer la sécurité et informer les utilisateurs, nous allons configurer un titre et un message affichés lors de l'ouverture de session.



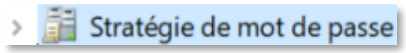
Ainsi, à chaque ouverture de session, ce message sera automatiquement affiché aux utilisateurs :



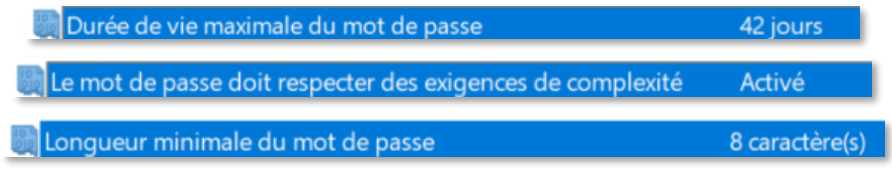
Une fois que nous aurons terminé de configurer les options de sécurité des stratégies locales, nous passerons à la stratégie de comptes.



Dans stratégie de mot de passe **:**



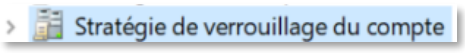
Nous allons définir la longueur minimale du mot de passe, la durée de vie maximale, ainsi que les exigences de complexité afin de renforcer la sécurité des comptes utilisateurs :



Pour rappel les règles pour un mot de passe :

- Minimum 8 caractères
- Au moins une lettre majuscule (ex. : A, B, C…)
- Au moins une lettre minuscule (ex. : a, b, c…)
- Au moins un chiffre (ex. : 0–9)
- Au moins un caractère spécial (ex. : !, @, #, $, %, &, *)

Puis pour finir dans stratégie de verrouillage du compte :



Nous allons définir la durée de verrouillage des comptes, le délai de réinitialisation après verrouillage ainsi que le seuil de tentatives avant le verrouillage du compte

Grâce à ces options de sécurité, nous renforçons considérablement la protection de notre contrôleur de domaine. Nous disposons désormais d'un **administrateur de secours**, de **stratégies de groupe adaptées** pour **encadrer les connexions**, d'un **message d'ouverture de session** pour **sensibiliser les utilisateurs**, ainsi que d'une **politique de mot de passe** et de **verrouillage de compte qui limite les tentatives de connexion non autorisées**.

3.6) Exportation des utilisateurs dans l'Active Directory

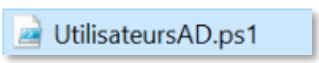
Nous disposons d'un fichier **.csv** contenant une liste d'utilisateurs, ainsi que les **groupes de sécurité** et les **unités d'organisation (UO)** auxquels ils appartiennent. Pour automatiser l'ajout de ces éléments dans l'Active Directory, nous utilisons **cinq scripts PowerShell**. Ces scripts permettent de créer les UO, d'ajouter les utilisateurs, d'attribuer les mots de passe, de les intégrer aux bons groupes de sécurité, et de structurer correctement l'arborescence du domaine, en suivant les informations fournies dans le fichier CSV.

1 - importexcel.ps1 | 2 - creationgroupes.ps1 | 3 - creationdegroupeparis.ps1 | 4 - attributionutilisateur.ps1 | 5 - ajoutgroupesdansgroupes.ps1

```powershell
Import-Module ActiveDirectory
Import-Module 'Microsoft.PowerShell.Security'

$users = Import-Csv -Delimiter ";" -Path "C:\doc\INFORMATIQUE\TECNIC\Employes\import.csv"

#********************Création des OU*********************************

New-ADOrganizationalUnit -Name "Employés" -Path "dc=iticmaster,dc=fr"
New-ADOrganizationalUnit -Name "Londres" -Path "ou=Employés,dc=iticmaster,dc=fr"
New-ADOrganizationalUnit -Name "Paris" -Path "ou=Employés,dc=iticmaster,dc=fr"
New-ADOrganizationalUnit -Name "Berlin" -Path "ou=Employés,dc=iticmaster,dc=fr"

#*******Ajout de chaque utilisateur dans son OU spécifique*******

foreach ($user in $users){

    $name = $user.firstName + " " + $user.lastName
    $fname = $user.firstName
    $lname = $user.lastName
    $login = $user.firstName + "." + $user.lastName
```

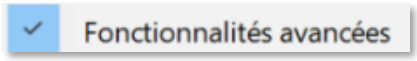
Notre objectif est de **regrouper les cinq scripts existants en un seul script PowerShell complet**, capable d'automatiser l'ensemble du processus.

Pour simplifier le déploiement et centraliser l'automatisation, on a décidé de **regrouper les cinq scripts existants en un seul fichier PowerShell**, nommé **UtilisateursAD.ps1**. Ce script exécute successivement toutes les étapes nécessaires à l'importation des utilisateurs.

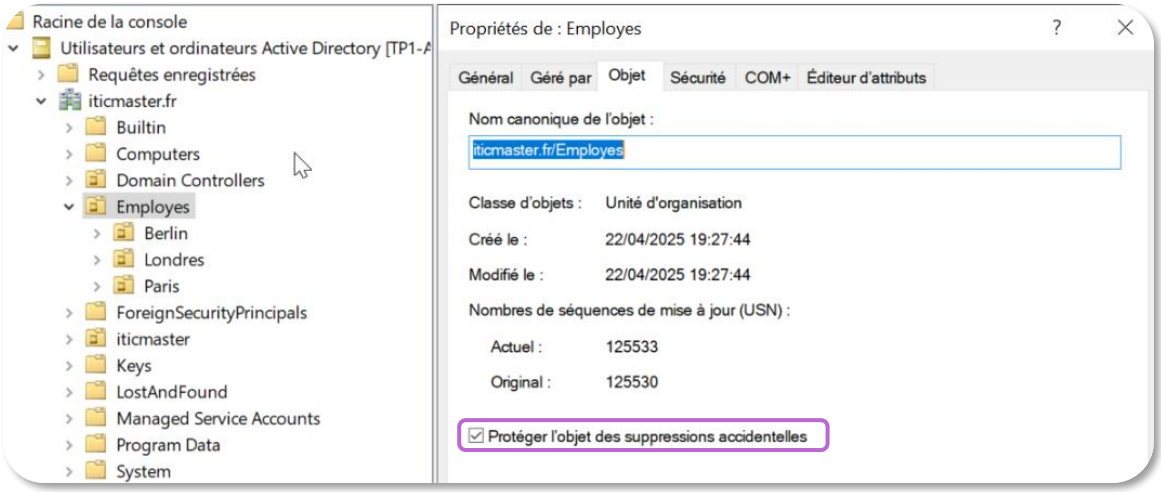


Vous trouverez le script correspondant joint à ce document.

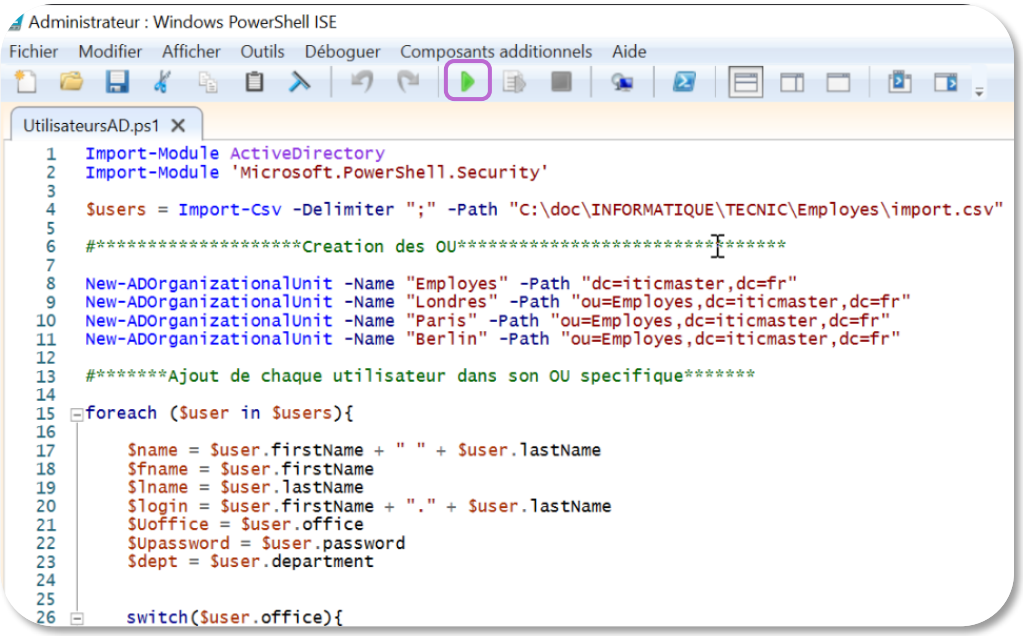
Pour tester ce script, nous allons supprimer l'unité d'organisation. Pour cela, nous ouvrirons notre console MMC et, dans le menu Affichage, nous activerons les **fonctionnalités avancées** afin de pouvoir accéder à certains onglets supplémentaires.



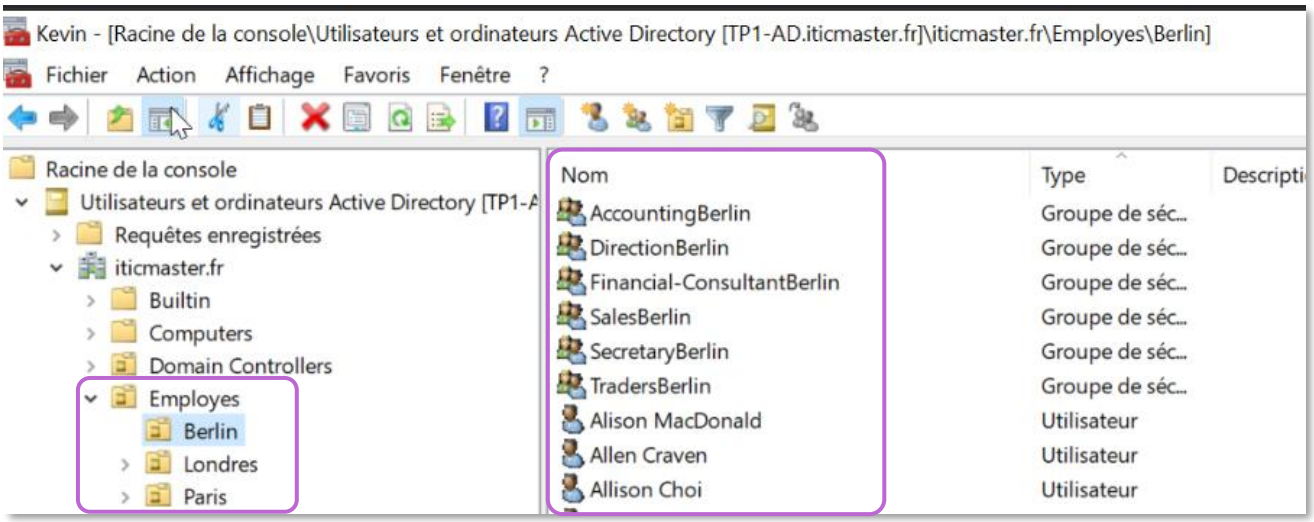
Ensuite, nous allons accéder aux propriétés de l'UO ''**Employés**'' et dans l'onglet ''**Objet**'', nous décocherons l'option ''**Protéger l'objet contre les suppressions accidentelles**''. Nous désactivons cette protection car, en cas de suppression de l'UO, tous les éléments qu'elle contient, comme les groupes de sécurité ou les utilisateurs, seront également supprimés. **En décochant cette case, nous permettons la suppression de l'UO, mais cela nécessite une action intentionnelle**.



Ensuite, nous allons ouvrir Windows PowerShell ISE en tant qu'administrateur et exécuter notre script ''**UtilisateursAD.ps1**''.

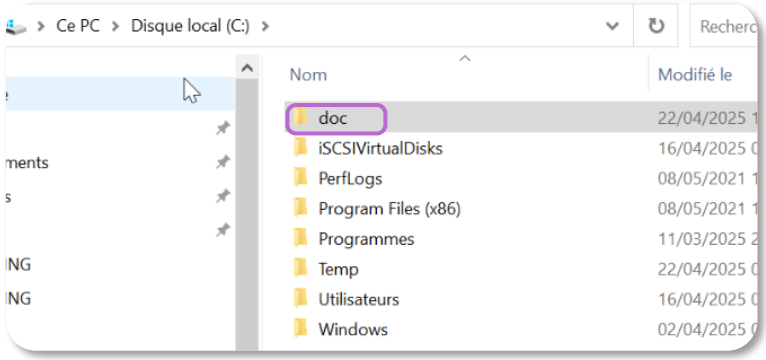


Après avoir exécuté notre script ‘’**UtilisateursAD.ps1**’’, nous n'avons rencontré aucun problème. Pour vérifier son bon déroulement, nous nous rendons dans ‘’**Utilisateurs et ordinateurs Active Directory**’’ via notre console MMC. Dans notre domaine **Iticmaster.fr**, une **unité d’organisation a bien été créée**. Nous pouvons également voir les unités d'organisation correspondant aux différents sites. En accédant à un site, les groupes de sécurité et les utilisateurs créés sont présents. Ainsi, notre script **fonctionne correctement**.

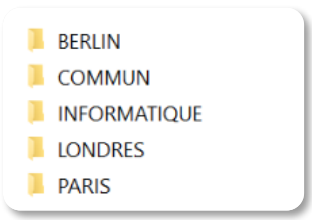


3.7) Création des dossiers partagés

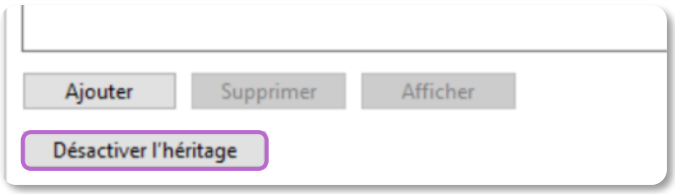
Maintenant, nous allons passer à la création des dossiers partagés. Pour cela, nous allons créer un dossier nommé **"Doc"** à la racine du disque **C:**.



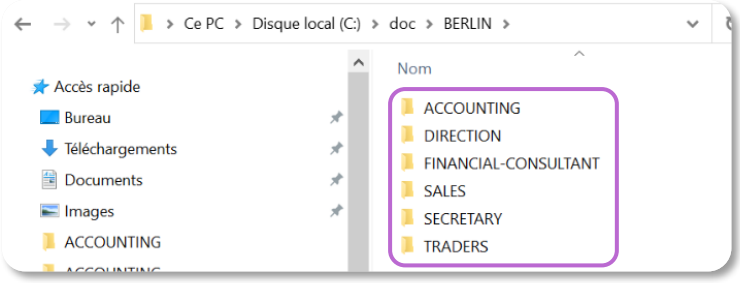
Dans le dossier **Doc**, nous allons créer plusieurs dossiers : un sous-dossier par site (**Berlin**, **Paris** et **Londres**), un dossier pour le **service informatique** où seront stockés les scripts et applications nécessaires au déploiement des GPO, ainsi qu’un dossier nommé **COMMUN**, accessible à tous les utilisateurs du domaine, afin de leur permettre de partager des documents entre eux.



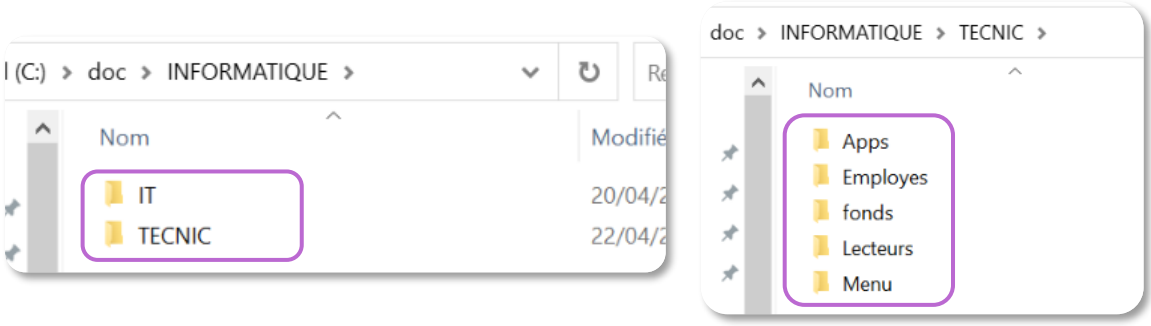
Une fois les dossiers principaux créés, nous allons **désactiver l'héritage** afin de pouvoir **définir des permissions spécifiques**. Il faudra également **désactiver l'héritage sur tous les sous-dossiers** que nous **allons créer**, afin de **modifier leurs autorisations indépendamment**.



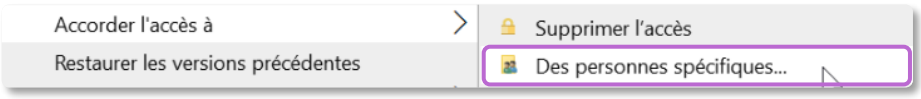
Ensuite, dans chaque dossier de site (Berlin, Paris, Londres), nous créerons des sous-dossiers pour les différents services, en nous basant sur **les groupes des unités d'organisation de chaque site**, tels que **AccountingBerlin**, **DirectionLondres**, **TradersParis**, etc. Il est important de **désactiver l'héritage des permissions** sur ces dossiers, car cela nous permettra de personnaliser les droits d'accès selon les besoins spécifiques de chaque service :



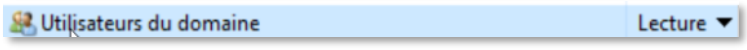
Dans notre dossier **INFORMATIQUE**, nous avons créé deux sous-dossiers : un pour **L'IT** et un autre nommé **TECNIC** destiné aux scripts liés aux GPO. Ces dossiers sont visibles par les utilisateurs, car ils contiennent des applications que le technicien pourra installer en cas d'intervention sur un poste, ainsi que les scripts nécessaires pour les GPO, tels que le mappage de lecteurs réseau, l'application des fonds d'écran, ou encore le menu de support IT.



Une fois que nous aurons créé les différents dossiers, nous allons les partager. Pour cela, nous allons aller à la racine du disque **C:**, puis accéder aux propriétés du dossier ''**Doc**'' et sélectionner ''**accorder accès a**'' puis ''**Des personnes spécifiques**'' :



Ensuite, nous allons ajouter le groupe ''**Utilisateurs du domaine**'' pour leur permettre d'accéder aux dossiers partagés.



Ensuite, nous allons attribuer les droits d'accès pour chaque dossier et sous-dossier. Le tableau ci-dessous résume les permissions accordées à chaque dossier :

	BERLIN					
Groupes de sécurité	ACCOUNTING	DIRECTION	FINANCIAL-CONSULTANT	SALES	SECRETARY	TRADERS
AccountingBerlin	X	X	X	X	X	X
DirectionBerlin	X	X	X	X	X	X
Financial-ConsultantBerlin	X	X	X	X	X	X
SalesBerlin	X	X	X	X	X	X
SecretaryBerlin	X	X	X	X	X	X
TradersBerlin	X	X	X	X	X	X

	LONDRES					
Groupes de sécurité	ACCOUNTING	DIRECTION	FINANCIAL-CONSULTANT	SALES	SECRETARY	TRADERS
AccountingParis	X	X	X	X	X	X
DirectionParis	X	X	X	X	X	X
Financial-ConsultantParis	X	X	X	X	X	X
SalesParis	X	X	X	X	X	X
SecretaryParis	X	X	X	X	X	X
TradersParis	X	X	X	X	X	X

	PARIS					
Groupes de sécurité	ACCOUNTING	DIRECTION	FINANCIAL-CONSULTANT	SALES	SECRETARY	TRADERS
AccountingLondres	X	X	X	X	X	X
DirectionLondres	X	X	X	X	X	X
Financial-ConsultantLondres	X	X	X	X	X	X
SalesLondres	X	X	X	X	X	X
SecretaryLondres	X	X	X	X	X	X
TradersLondres	X	X	X	X	X	X

	INFORMATIQUE	
Groupes de sécurité	IT	TECNIC
Utilisateurs du Domaine	X	X
GSINFORMATIQUE	X	X

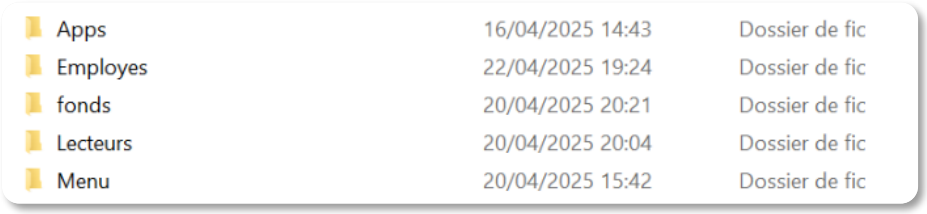
	COMMUN
Groupes de sécurité	COMMUN
Utilisateurs du Domaine	X

LEGENDE POUR LES DROITS / CODE COULEUR	
X	Modification, Lecture et exécution, Affichage du contenu du dossier, Lecture et Ecriture
X	Lecture et éxécution, Affichage du contenu du dossier et Lecture
X	Pas de droits

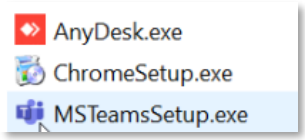
3.8) Mise en place de stratégies de groupe (GPO)

Nous allons maintenant créer des GPO pour définir un fond d'écran personnalisé selon l'unité d'organisation des utilisateurs, monter automatiquement les lecteurs réseau associés aux dossiers partagés, et ajouter un menu IT affichant l'adresse IP, les applications installées, et d'autres informations utiles.

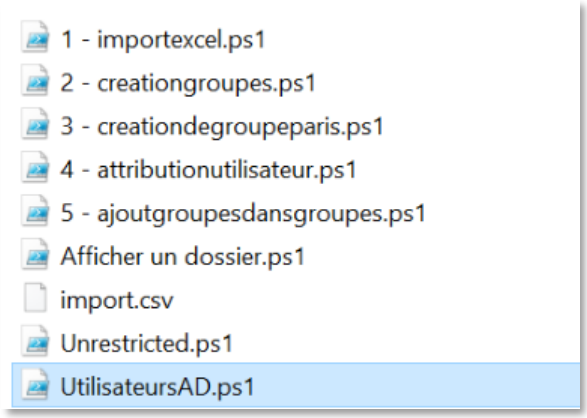
Avant de commencer, nous allons dans **\\TP1-AD\Doc\INFORMATIQUE\TECNIC** pour y créer un sous-dossier dédié à chaque GPO que nous allons mettre en place :



- **Dans le dossier Apps**, l'utilisateur pourra trouver des logiciels que le technicien pourra utiliser pour les installer sur le poste de travail :

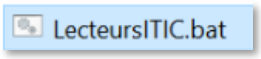


- **Dans le dossier Employes**, nous allons trouver notre script UtilisateursAD.ps1 ainsi que les autres scripts et le fichiers .csv contenant les utilisateurs :

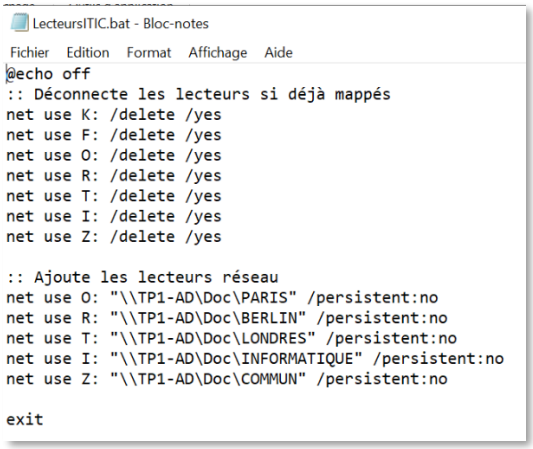


- **Dans le dossier fonds**, nous allons trouver trois fonds d'écran pour les trois sites, Berlin, Paris et Londres :

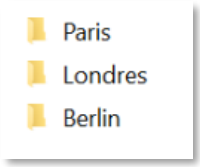
- **Dans le dossier Lecteurs**, nous trouverons un script pour le mappage des lecteurs réseau afin d'accéder aux dossiers partagés pour les utilisateurs :



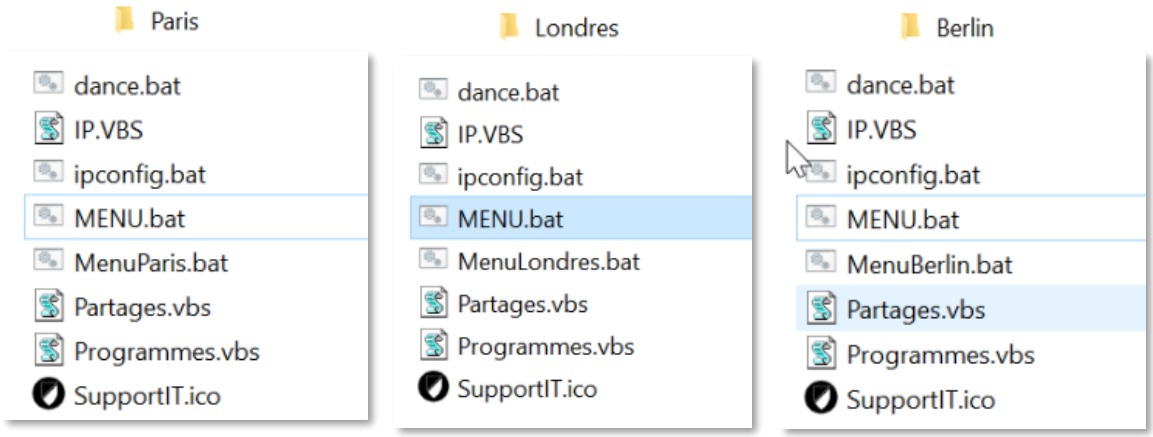
Le script va d'abord supprimer les lecteurs existants, puis mapper les nouveaux dossiers. Ainsi, lors de leur connexion, les utilisateurs verront les dossiers INFORMATIQUE, COMMUN, ainsi qu'un autre dossier spécifique s'ils ont les droits d'accès.



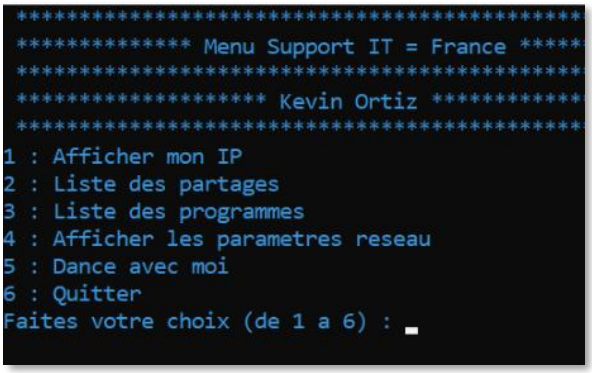
- **Dans le dossier Menu**, nous allons trouver les trois Menu du support IT pour chaque site :

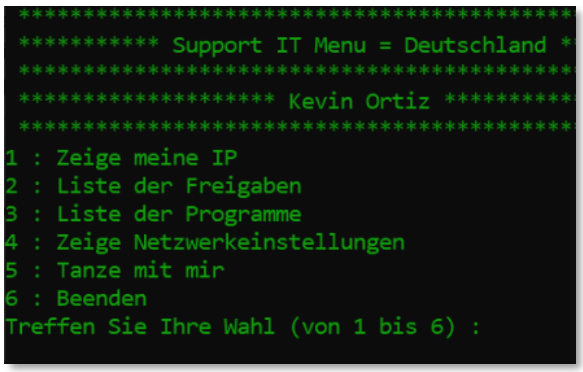


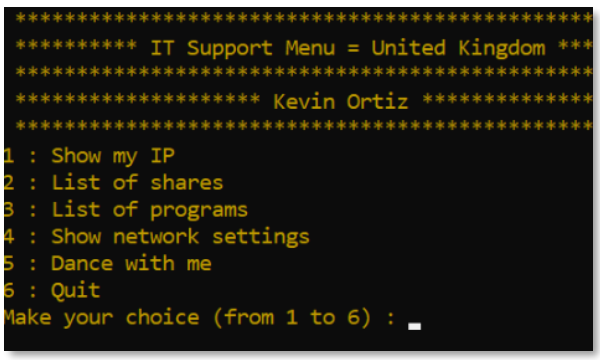
Dans chaque dossier, nous allons intégrer un menu Support IT personnalisé. Étant donné qu'il y a **trois sites**, nous avons décidé de créer des **menus Support IT distincts pour chaque site**, et ces menus pourront être **déployés via les GPO**.



Et les **menu Support IT** sont :





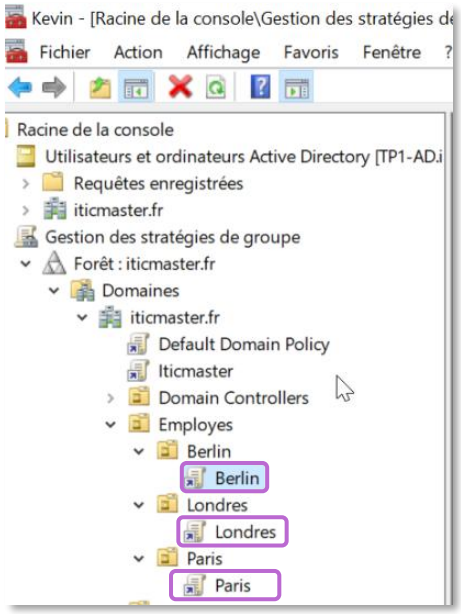


Comme vous pouvez le constater, chaque menu est personnalisé en fonction de l'utilisateur et du site auquel il appartient.

Pour le déploiement des Menu Support IT j'ai crée un script qui est :

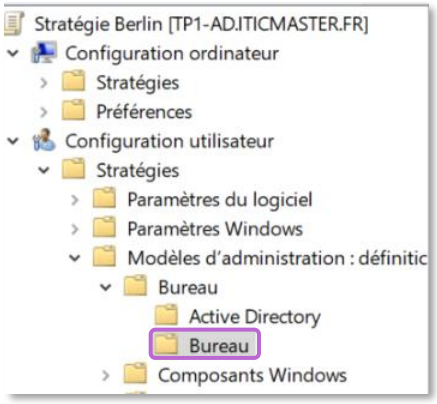
Un pour chaque Menu, **Ce script crée un dossier** Berlin, Paris ou Londres dans C:\Temp (s'il n'existe pas), y copie une tout les fichiers qui sont dans Menu, puis crée un raccourci sur le bureau de l'utilisateur pointant vers un fichier batch (MENU.bat) dans ce dossier. Il supprime d'abord tout contenu existant dans le dossier de destination, vérifie si l'icône est présente et, si tout est en ordre, génère un raccourci avec l'icône SupportIT.ico pour lancer le fichier MENU.bat.

Maintenant, pour la GPO, nous allons ouvrir notre console MMC, puis accéder à la gestion des stratégies de groupe. Nous sélectionnerons notre domaine, puis notre unité d'organisation. À partir de là, nous allons créer des stratégies de groupe personnalisées pour Berlin, Paris et Londres.



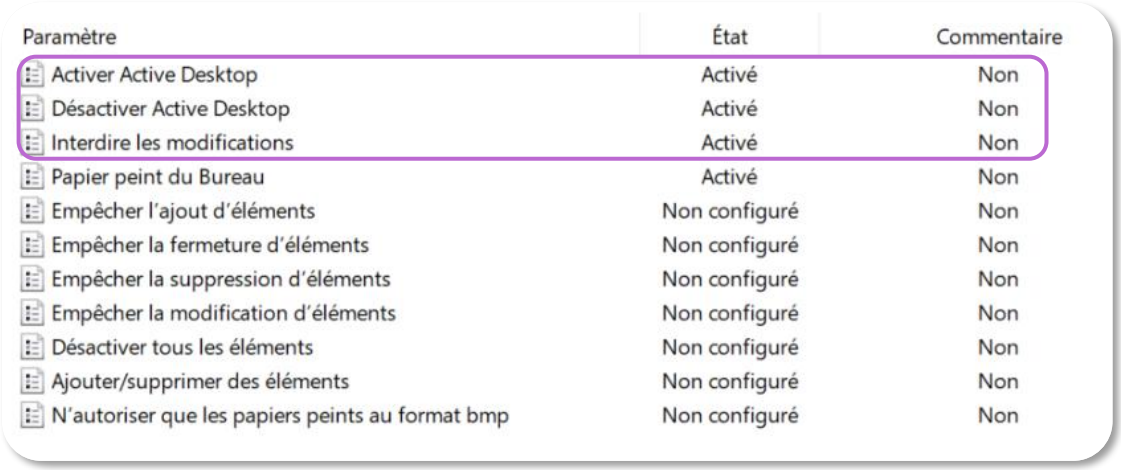
3.9) Stratégie de groupe pour la gestion des fonds d'écran

Pour commencer, nous ferons un clic droit sur la stratégie de groupe créée, puis nous sélectionnerons l'option "**Modifier**" pour configurer les paramètres souhaités.



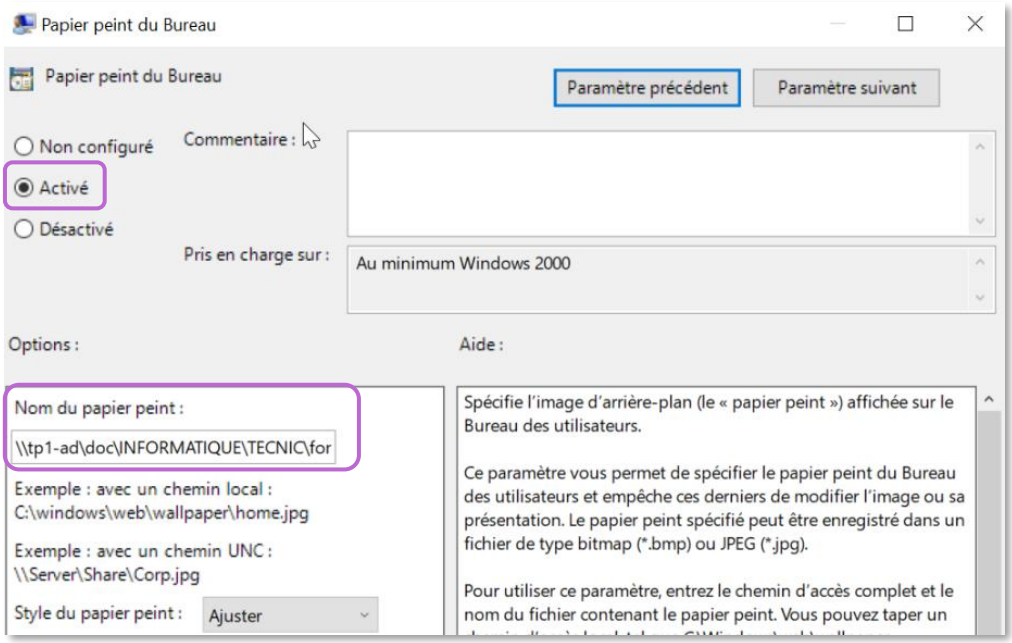
Puis, nous allons aller dans la section "**Bureau**", suivant le chemin indiqué dans l'image ci-dessus.

Puis nous allons activer ‘’**Activer Active Desktop**’’, ‘’**Désactiver Active Desktop**’’ et ‘’**Interdire les modifications**’’ pour que les utilisateurs ne puissent pas modifier le fond d’écran déployé



Paramètre	État	Commentaire
Activer Active Desktop	Activé	Non
Désactiver Active Desktop	Activé	Non
Interdire les modifications	Activé	Non
Papier peint du Bureau	Activé	Non
Empêcher l’ajout d’éléments	Non configuré	Non
Empêcher la fermeture d’éléments	Non configuré	Non
Empêcher la suppression d’éléments	Non configuré	Non
Empêcher la modification d’éléments	Non configuré	Non
Désactiver tous les éléments	Non configuré	Non
Ajouter/supprimer des éléments	Non configuré	Non
N’autoriser que les papiers peints au format bmp	Non configuré	Non

Puis pour le fond d’écran nous allons double cliquer sur ‘’**Papier peint du Bureau**’’ :



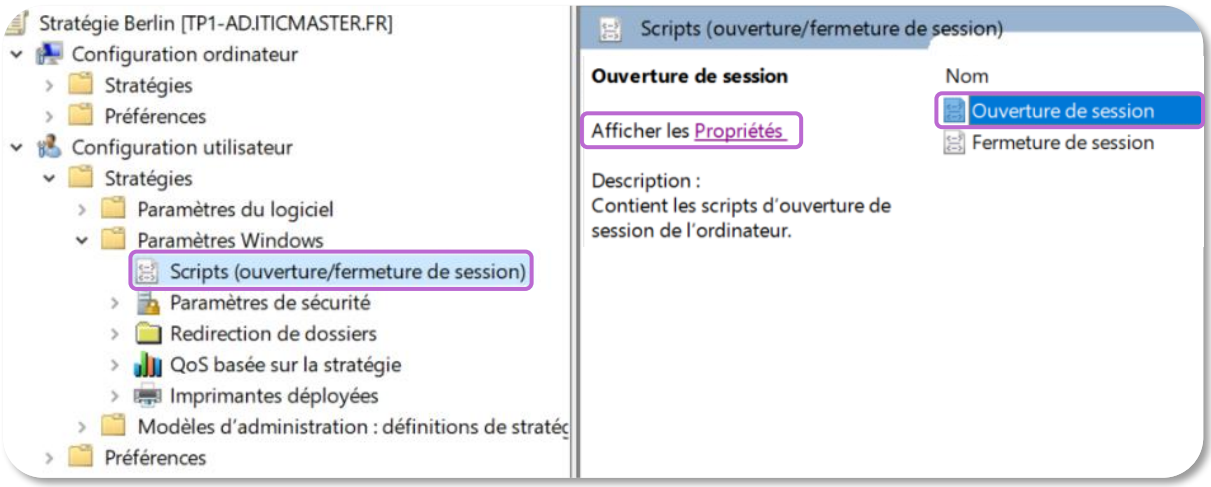
Nous allons cliquer sur "**Activé**", puis dans "**Nom du papier peint**", nous allons entrer le chemin qui mène à l'image que nous souhaitons déployer comme fond d'écran. Dans le cas de la stratégie de groupe pour Berlin, nous allons spécifier l'image de Berlin, donc nous allons renseigner le chemin

\\TP1-AD\Doc\INFORMATIQUE\TECNIC\Fonds\Berlin.png

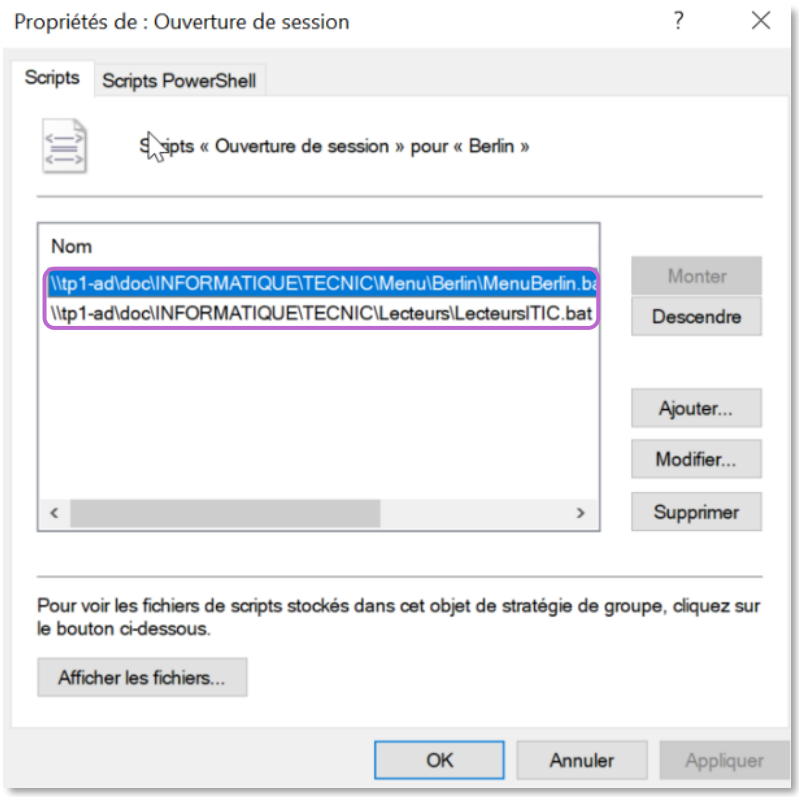
Puis une fois finis nous allons appliquer puis cliquer sur **OK**.

Maintenant, nous allons passer au déploiement de la GPO pour le mappage des lecteurs réseau ainsi que le MENU support IT.

Comme nous sommes toujours sur la stratégie de groupe de Berlin, nous allons aller dans "**Scripts**" **(Ouverture / Fermeture de session)**.



Puis, nous allons cliquer sur "**Ouverture de session**", puis sur "**Propriétés**" :



Une fois dans cette page, nous allons cliquer sur "**Ajouter**" et renseigner les chemins de nos scripts pour le **mappage des lecteurs réseau** et pour le **Menu Support IT**.

Ainsi, pour le mappage des lecteurs, nous entrerons le chemin suivant :

\\TP1-AD\Doc\Informatique\TECNIC\Lecteurs\LecteursITIC.bat.

Pour le **Menu Support IT**, nous entrerons :

\\TP1-AD\Doc\Informatique\TECNIC\Menu\Berlin\MenuBerlin.bat.

Enfin, nous cliquerons sur "OK" pour valider les modifications et appliquer les scripts lors de l'ouverture de session des utilisateurs.

Pour les autres sites, Paris et Londres, il faudra effectuer la même manipulation, mais en prenant leurs dossiers respectifs

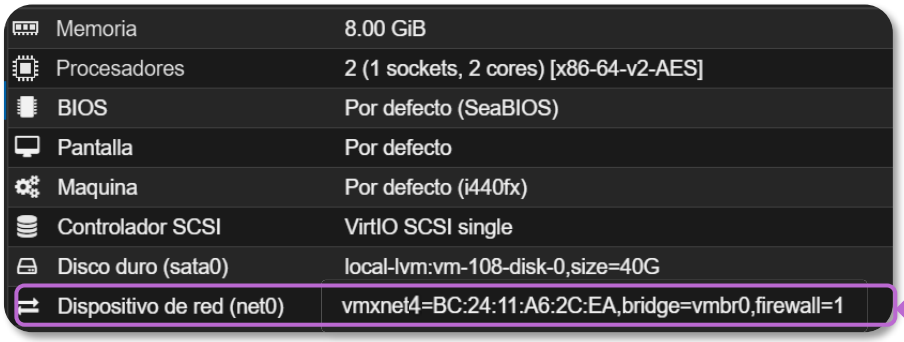
En conclusion, nous avons configuré notre contrôleur de domaine en mettant en place des stratégies de groupe (GPO) pour personnaliser les fonds d'écran, le mappage des lecteurs réseau, et les menus de support IT pour chaque site. Nous avons également renforcé la sécurité en appliquant des politiques de mot de passe strictes, des stratégies de verrouillage de compte et d'autres paramètres de sécurité. Ces configurations garantissent une gestion centralisée et sécurisée des utilisateurs et des ressources sur notre domaine.

4) Déploiement et configuration de la VM Poste client

4.1) Création de la VM Poste client

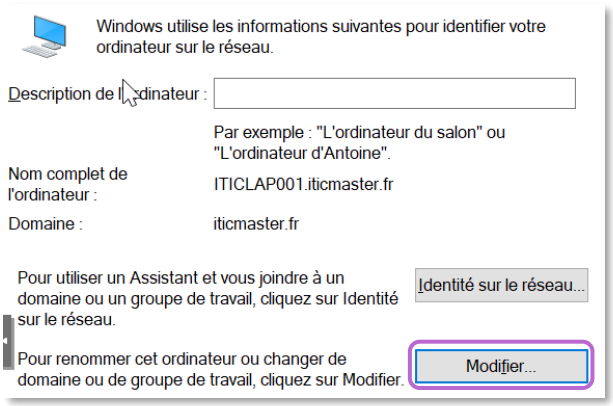
La configuration de la machine cliente consiste à l'intégrer au domaine Active Directory, à appliquer les GPO de groupe spécifique à son site, et à assurer la connectivité aux ressources partagées telles que les lecteurs réseau et le support informatique.

Dans **Proxmox**, la VM a été configurée avec les ressources suivantes :

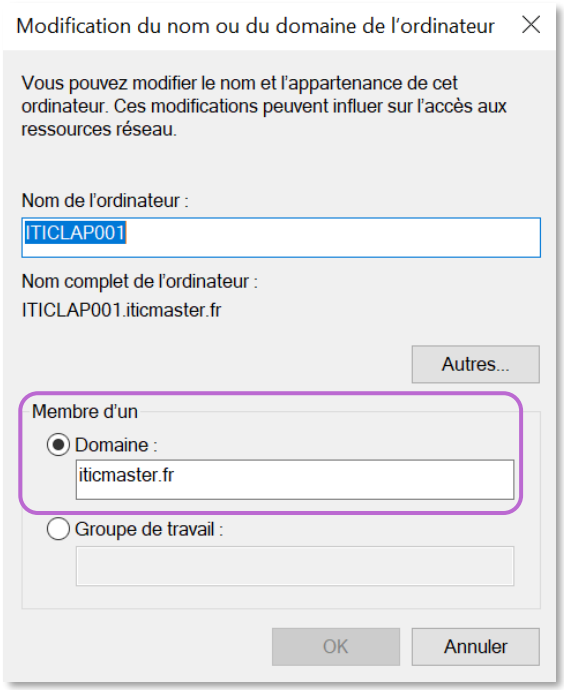


Pour cette VM, j'ai attribué 8 Go de RAM, avec un seul socket et deux cœurs pour le processeur

Une fois que nous aurons installé et configuré notre poste client, il faudra le joindre au contrôleur de domaine, pour cela nous allons faire un **Win + R** et écrire **Sysdm.cpl** :



Ensuite, nous allons cliquer sur ''**Modifier**'' et dans le champ ''**Domaine**'', nous allons entrer **iticmaster.fr**. Lors de la validation, il nous sera demandé de saisir les identifiants de l'administrateur. Attention ! Il ne faut pas entrer ''**Administrateur**'', car lors de la configuration du contrôleur de domaine, nous avons renommé le compte administrateur. Nous allons donc nous identifier avec le compte **AdminMaster** :



Puis, une fois la validation effectuée, il nous sera demandé de redémarrer notre poste pour appliquer les modifications.

4.2) Installation de RSAT (Remote server Administration Tools)

Pour installer **RSAT**, nous allons nous connecter avec un compte administrateur sur le poste client, ouvrir une fenêtre PowerShell en tant qu'administrateur, puis exécuter les deux commandes suivantes :

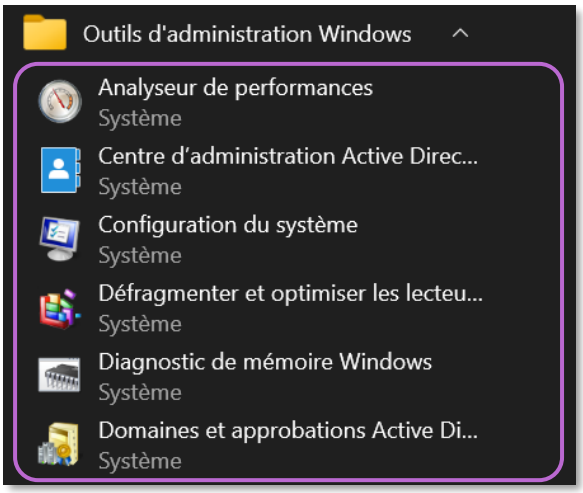
Premièrement, en exécutant ce script, il va vérifier si les outils RSAT sont installés sur le système en affichant une liste des fonctionnalités RSAT disponibles et leur état d'installation (si elles sont installées ou non).

Get-WindowsCapability -Name RSAT* -Online | Select-Object -Property DisplayName, State

La commande suivante permet d'ajouter les outils RSAT nécessaires pour administrer Active Directory sur un système Windows :

Add-WindowsCapability -online -Name Rsat.ActiveDirectory.DS-LDS.Tools~~~~0.0.1.0

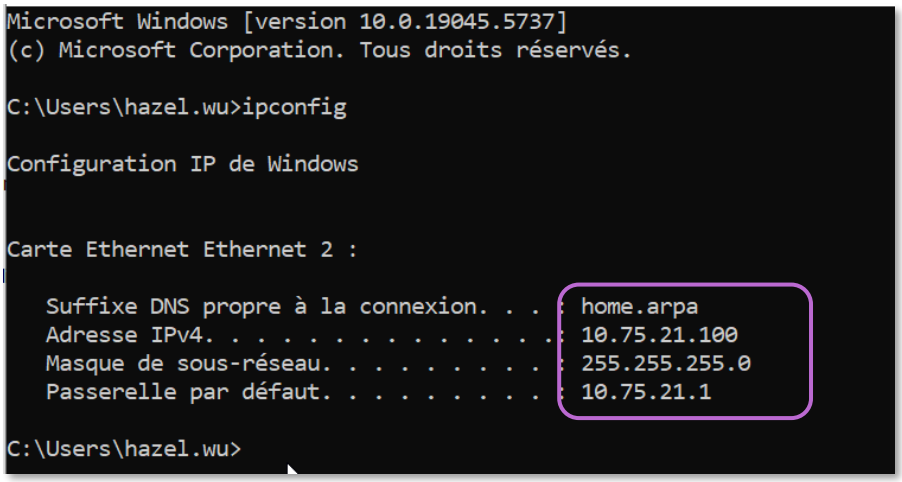
Si les deux commandes ont été exécutées avec succès sur votre poste client, un dossier intitulé "**Outils d'administration Windows**" apparaîtra dans vos recherches Windows.



Comme on peut le voir, les différents services de notre contrôleur de domaine sont désormais disponibles sur notre poste client.

4.3) Vérification de la configuration réseau

Maintenant, nous allons vérifier les paramètres réseau. Nous allons ouvrir le terminal sur le poste client et taper la commande ipconfig pour afficher la configuration réseau de la machine :



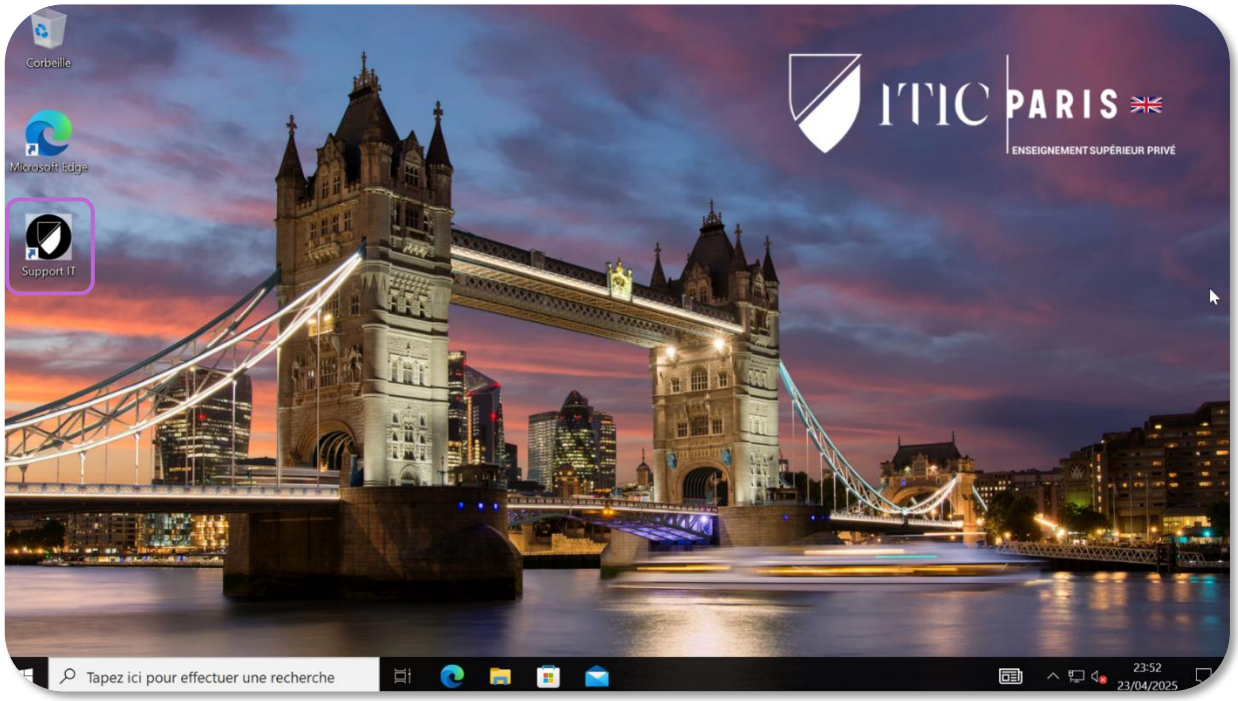
Comme on peut le voir, nous avons obtenu une adresse IP de **10.75.21.100**, ce qui indique que le serveur DHCP de notre Pfsense fonctionne correctement.

Pour finir, nous allons nous connecter avec un utilisateur afin de vérifier si toutes nos GPO ont bien été appliquées correctement.

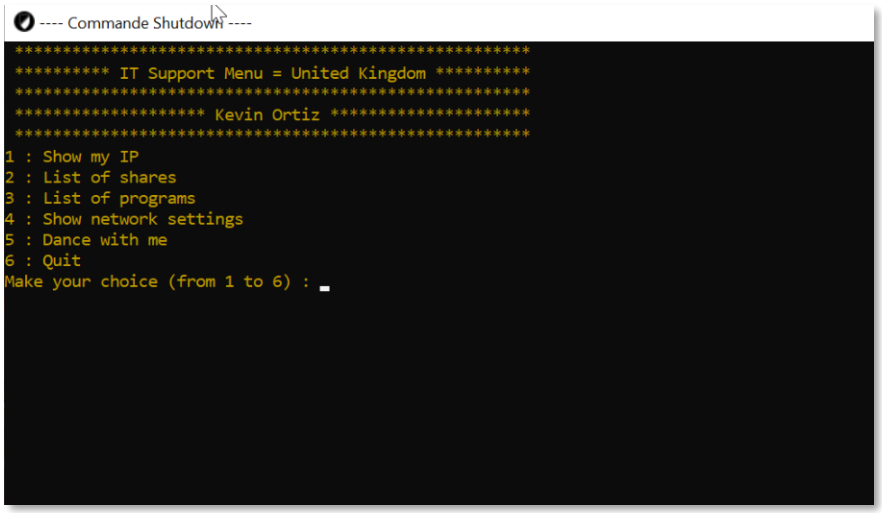
4.4) Connexion avec un utilisateur au poste client

Pour commencer le test, nous allons nous connecter avec un utilisateur de l'un des sites. Dans notre cas, nous utiliserons le compte de **Beth McKena**, qui appartient au service **Direction du site de Londres** :

Une fois connecté, nous constatons que le fond d'écran s'est bien appliqué, tout comme le raccourci du menu Support IT sur le bureau, avec l'icône personnalisée que nous avons configurée.

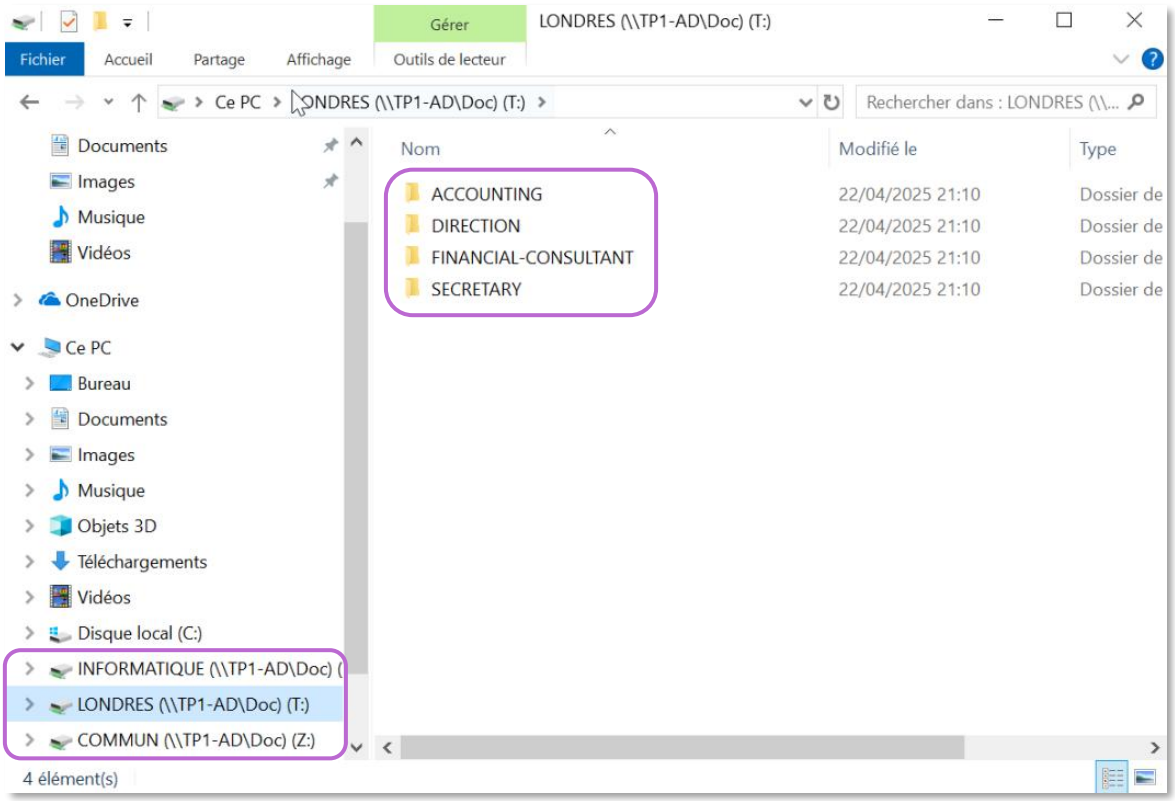


Lorsqu'on double-clique sur **Support IT**, une fenêtre s'ouvre affichant un menu interactif personnalisé :



Donc notre GPO pour le Menu Support fonctionne correctement.

Maintenant, nous allons ouvrir l'explorateur de fichiers afin de vérifier si les lecteurs réseau se sont bien montés automatiquement, comme prévu par la GPO.



Comme on peut le voir, les lecteurs réseau se sont bien montés et seuls les dossiers auxquels l'utilisatrice a accès apparaissent. Cela confirme que nos stratégies de groupe ainsi que les règles d'accès aux dossiers **partagés fonctionnent correctement**.

5) Présentation de la deuxième partie du projet

5.1) Contexte

Dans cette seconde partie du projet, nous mettrons en place une solution de haute disponibilité (HA) avec deux pare-feu PfSense configurés en cluster. Cette architecture permettra de maintenir la connexion réseau : si le premier pare-feu rencontre une défaillance, le second prendra automatiquement le relais sans interruption perceptible pour les utilisateurs. L'objectif est d'assurer la résilience de l'infrastructure réseau, d'améliorer la fiabilité du système et de garantir la sécurité et la disponibilité des services pour tous les utilisateurs du domaine.

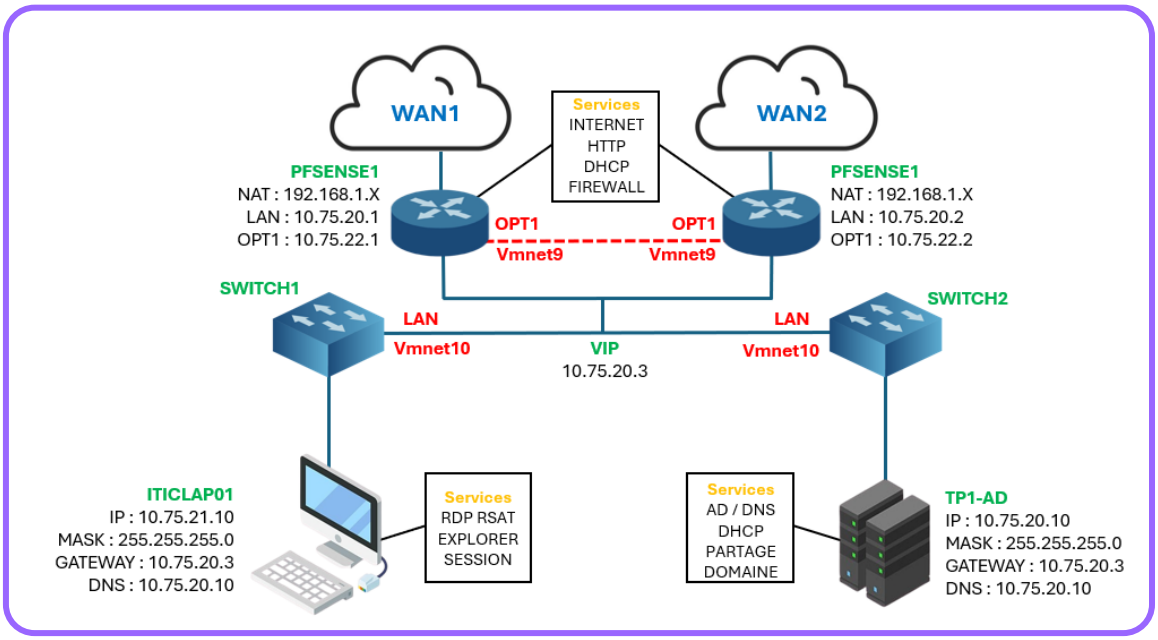
5.2) Prérequis

Avant de procéder à la mise en place de la haute disponibilité, il est essentiel de préparer l'infrastructure réseau en ajoutant un second pare-feu PfSense, configuré avec trois interfaces réseau, ainsi qu'une Virtual IP partagée entre les deux PfSense pour garantir la continuité de service en cas de défaillance.

- Un second pare-feu Pfsense installé sur une nouvelle machine virtuelle ou machine physique.
- Trois interfaces réseau :
  - WAN : Connectée à internet (NAT)
  - LAN : Pour le réseau interne principal (poste client, serveur AD...)
  - OPT1 : Pour le second réseau interne destiné à d'autres services
- Création d'un **Virtual IP (VIP)**.
- Configuration de **CARP** (**Common Address Redundancy Protocol**) pour la gestion des VIP.
- Synchronisation de la configuration entre les deux PfSense (Sync).
- Interconnexion réseau stable entre les deux PfSense pour assurer la réplication (pfsync).

5.3) Schéma réseau

Le schéma ci-dessous illustre l'architecture réseau mise en place dans ce TP, composée de trois machines virtuelles interconnectées via **PfSense**, avec deux réseaux distincts (**LAN et OPT1**), permettant de simuler un environnement d'entreprise structuré et sécurisé.



6) Haute disponibilité

6.1) Création de la VM Pfsense

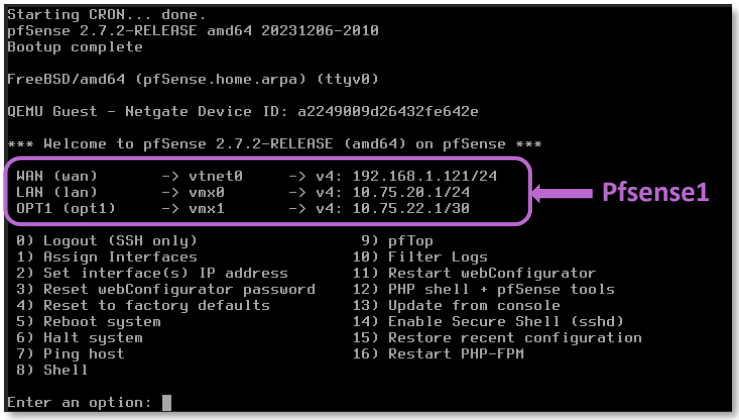
Le second pfSense assurera la haute disponibilité du réseau en prenant automatiquement le relais en cas de défaillance du premier pare-feu, garantissant ainsi la continuité de service pour les utilisateurs. Pour cela, trois interfaces réseau seront nécessaires : une interface WAN pour l'accès à Internet, une interface LAN pour connecter les différentes machines du réseau, et une interface OPT1 dédiée à la communication entre les deux pfSense.

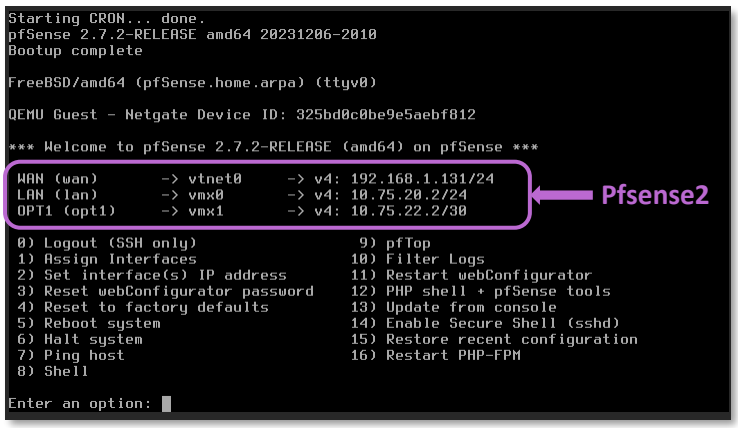
Dans **Proxmox**, la VM a été configurée avec les ressources suivantes :

Pour cette VM, j'ai attribué a nouveau 2 Go de RAM, ainsi qu'un seul socket et un core pour le processeur.

6.2) Configuration des interfaces réseau

Pour la configuration réseau du second PfSense, l'adresse IP du LAN sera définie sur **10.75.20.2/24** et celle de l'interface OPT1 sur **10.75.22.2/24**. Ainsi, la répartition des adresses IP pour les deux PfSense sera la suivante :

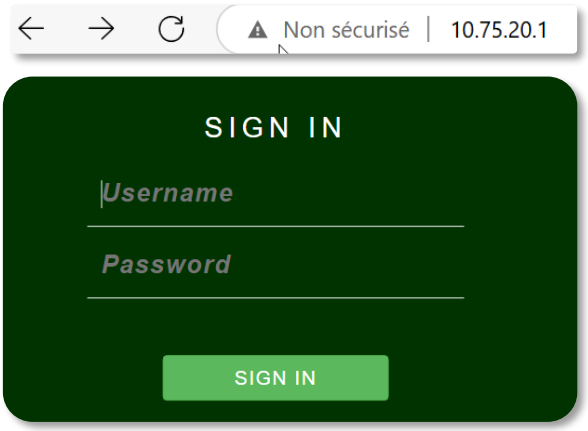




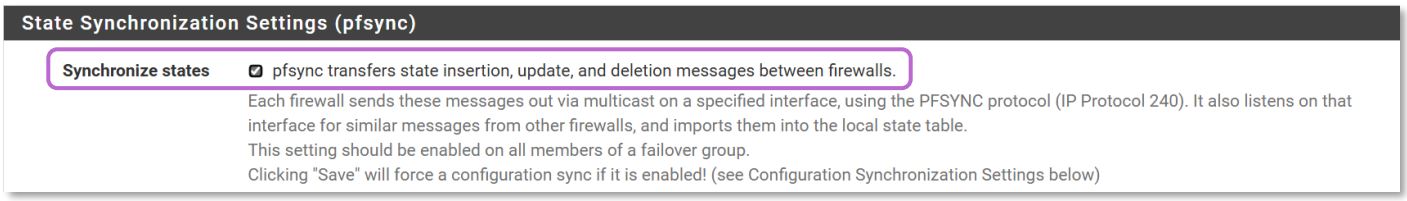
6.3) Mise en place de la Haute disponibilité

Pour la mise en place de la haute disponibilité nous devons faire quelques configurations dans le Pfsense1 et le Pfsense2, on va commencer par le **Pfsense 1** :

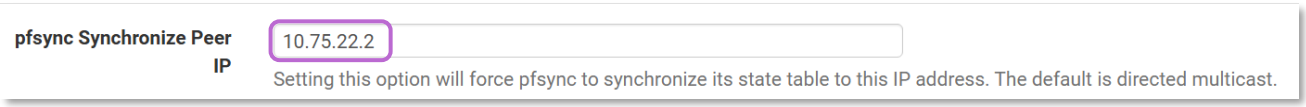
Pour commencer on va se connecter sur le **Pfsense1** en tapant **10.75.20.1** sur notre navigateur web :



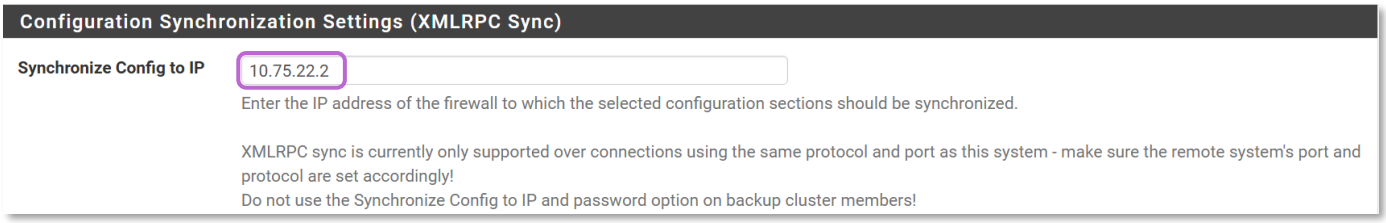
Ensuite on va aller dans ''**System**'' puis dans ''**High Availability**'' et nous allons cocher ''**Synchrnize states**'' :



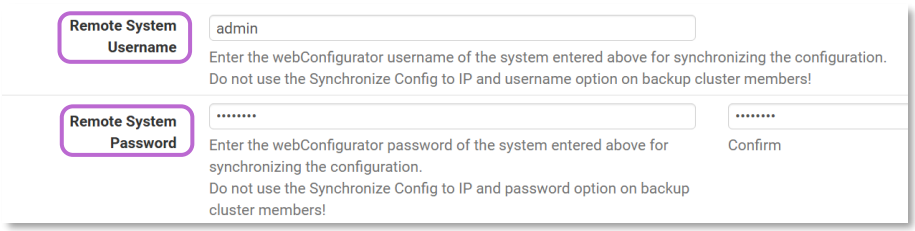
Puis dans ''**pfsync synchronize Peer IP**'' nous allons mettre l'IP de **l'interface OPT1** du deuxième Pfsense, donc :



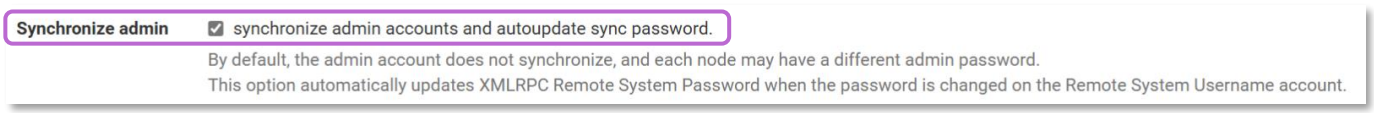
Ensuite dans la partie ''**Configuration Synchronization Settings (XMLRPC Sync)**'' nous allons renseigner dans ''**Synchronize Config to IP**'' nous allons mettre a nouveau **l'IP de l'interface OPT1 du deuxième Pfsense** :



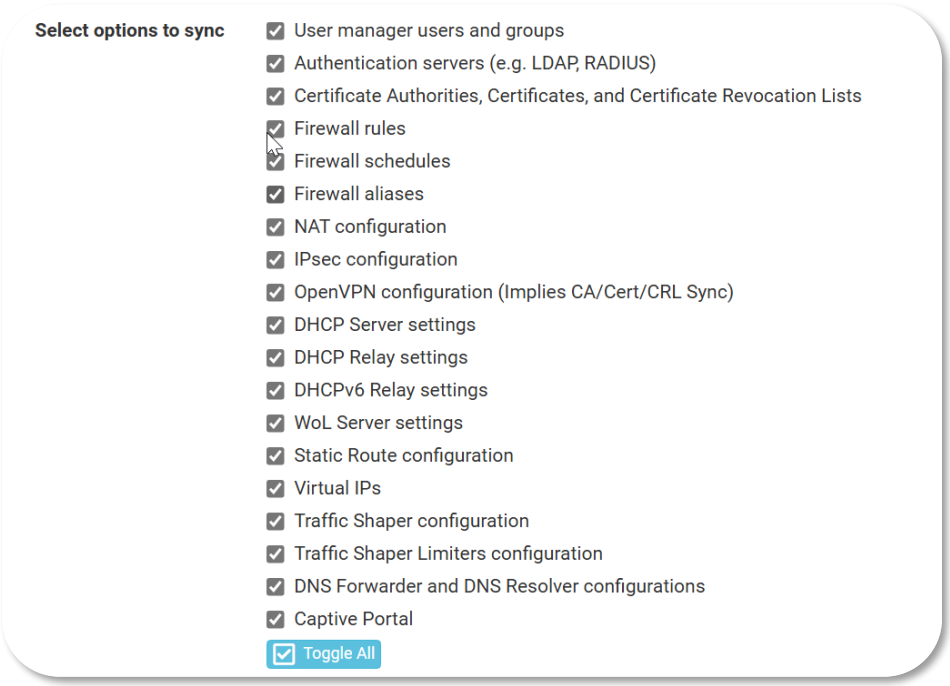
Nous devons aussi renseigner le login et le mot de passe du deuxième Pfsense :



Ensuite, il est nécessaire de cocher l'option **"Synchronize admin passwords"** afin de permettre la synchronisation entre les deux **PfSense** :

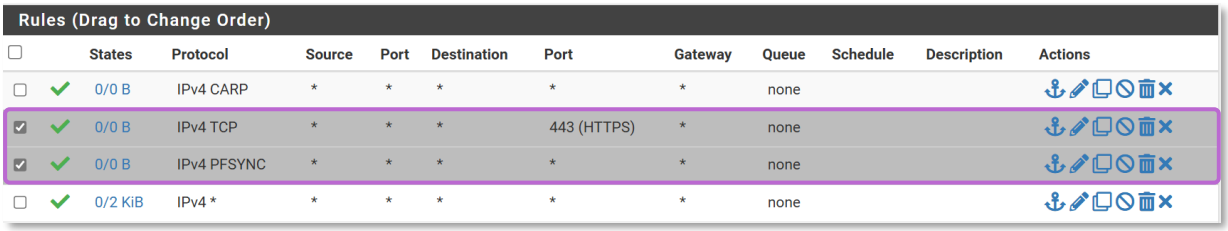


Ensuite, dans les options de synchronisation, il est recommandé de tout sélectionner afin que l'ensemble des configurations (règles de pare-feu, services, paramètres système, etc.) soit automatiquement synchronisé entre le **premier** et le **deuxième** PfSense :



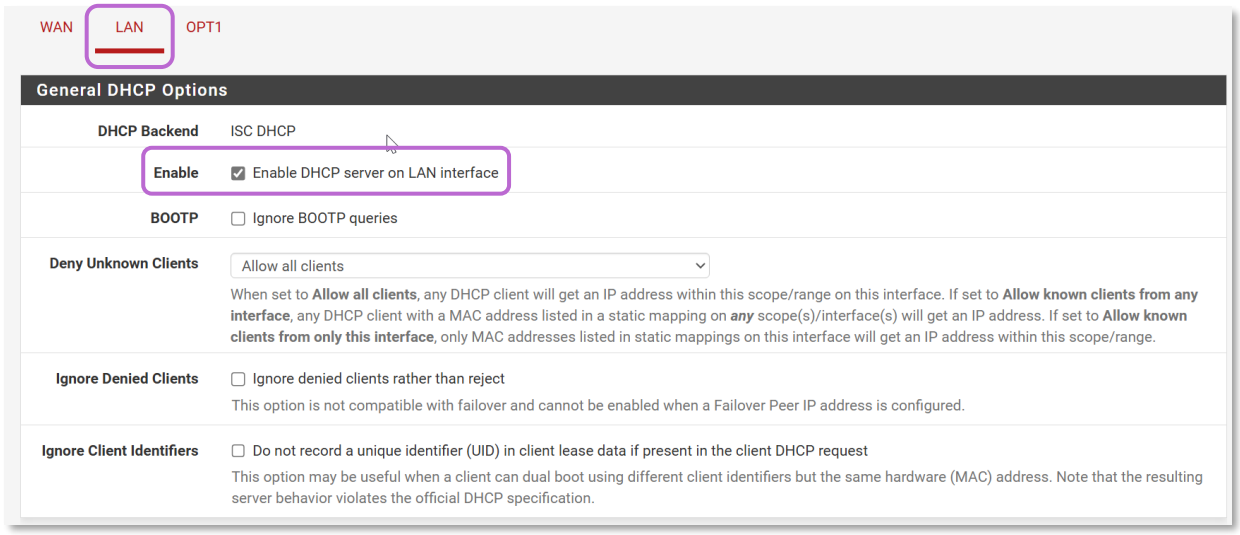
Puis pour finir nous allons cliquer sur ''**Save**'' :

Ensuite nous allons aller dans ''**Firewall**'', puis ''**Rules**'' et nous allons ajouter deux règles de pare-feu pour l'interface OPT1 qui sont :



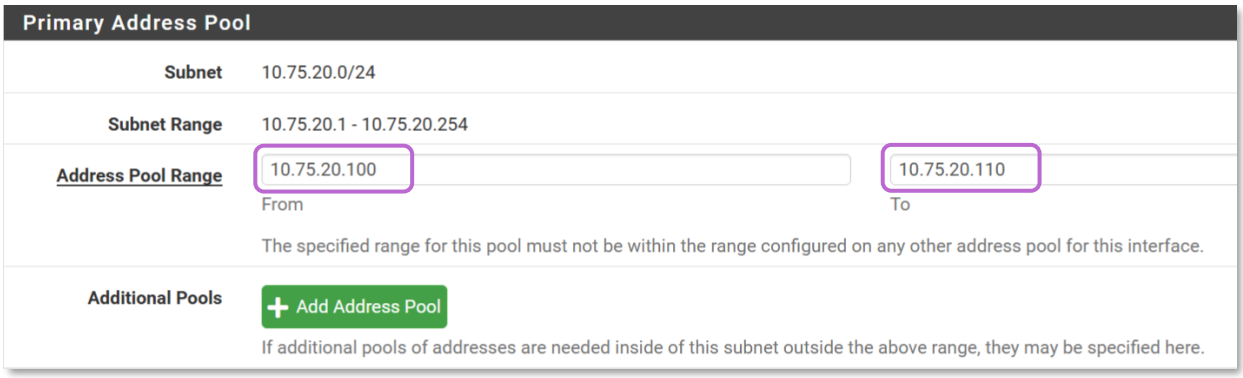
Nous choisissons d'activer le protocole **PFSYNC**, car il permet la synchronisation en temps réel des états de connexion entre les deux PfSense, assurant ainsi une bascule transparente en cas de panne. Nous activons également le protocole **TCP** pour permettre la communication HTTPS entre les deux PfSense, indispensable pour l'interface d'administration sécurisée, et nous les configurons en **Any** afin de laisser tout le trafic passer sans restriction entre eux.

Maintenant nous allons configurer le **serveur DHCP** pour le Pfsense1, pour cela nous allons aller sur ''**Services**'' puis ''**DHCP Server**'' **:**

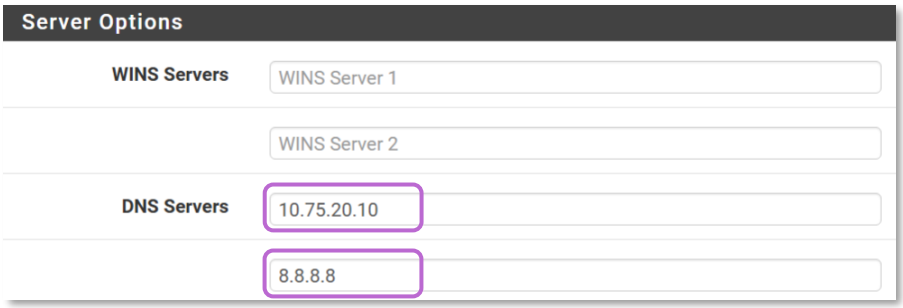


Nous choisissons l'interface **LAN**, car c'est celle à laquelle les machines du réseau seront connectées. Ensuite, nous cochons l'option **Enable** afin d'activer le service sur cette interface.

Ensuite nous allons renseigner une **adresse IP de début** et **une adresse IP de fin** pour notre serveur DHCP :

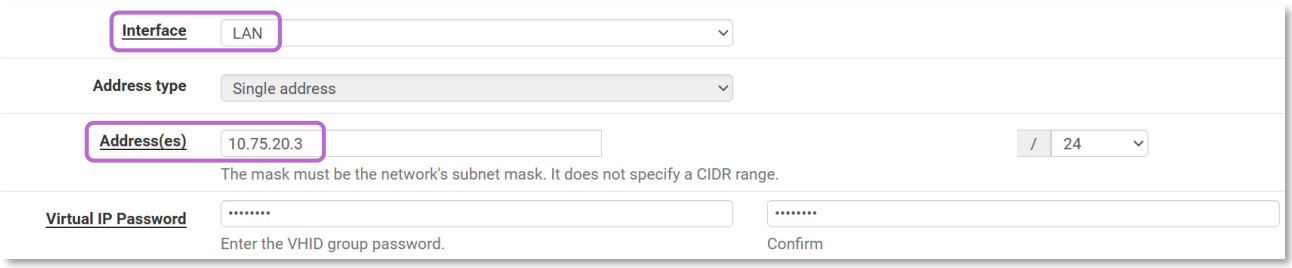


Comme Serveur DNS nous allons renseigner l'IP de notre contrôleur de domaine et nous allons mettre comme deuxième serveur DNS 8.8.8.8 pour avoir une connexion à internet :



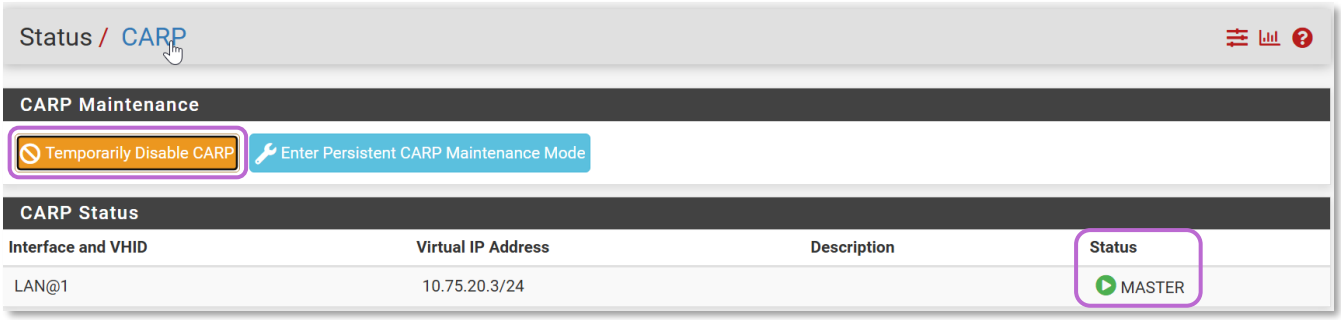
Puis pour finir nous allons cliquer sur ''**Save**'' et sur ''Apply Changes'' pour appliquer les changements :

Ensuite nous allons paramétrer l'IP virtuelle, pour cela nous allons aller dans ''**Firewall**'' puis ''**Virtual IPs**'' et nous allons cliquer sur ''**Add**'' pour créer notre IP virtuelle :



Nous allons choisir l'interface LAN, puis nous allons lui mettre comme IP **10.75.20.3/24** et nous allons lui attribuer un mot de passe.

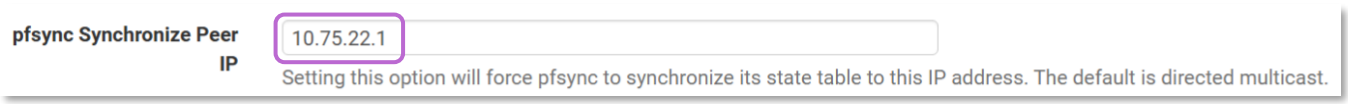
Donc une fois qu'on aura crée notre IP virtuel nous allons aller dans ''**Status**'' puis sur ''**CARP (Failover)**'' :



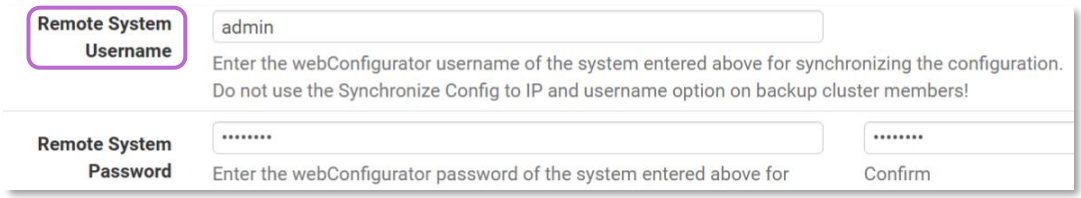
Comme vous pouvez le constater, le service est opérationnel et son **statut** est défini sur **Master**, ce qui indique que le premier PfSense agit en tant que maître. Avant de procéder à la configuration du second PfSense, nous allons **désactiver temporairement le service CARP** afin d'éviter d'éventuels conflits durant la synchronisation. Une fois la configuration du second PfSense terminée, nous pourrons **réactiver CARP** pour finaliser la mise en place de la haute disponibilité.

Une fois cette étape terminée, nous passerons à la configuration nécessaire du second PfSense afin de compléter la mise en place de la haute disponibilité.

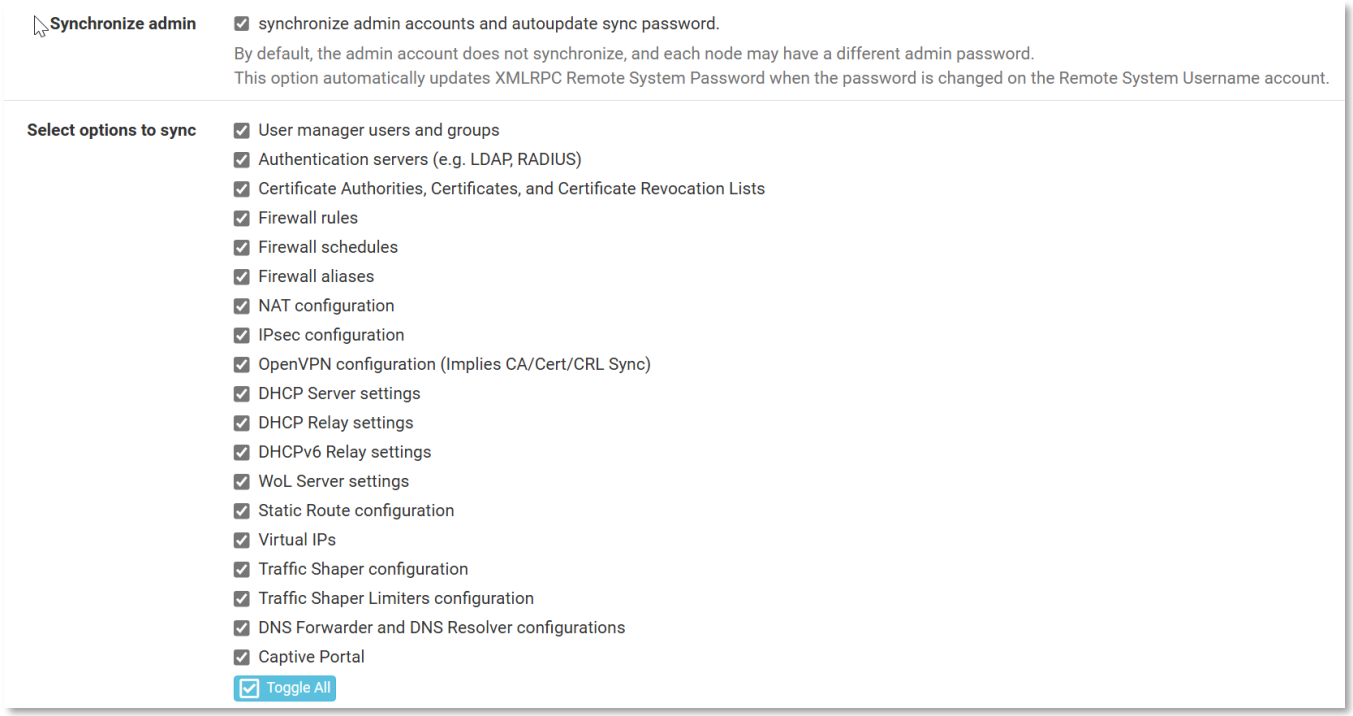
Pour commencer, nous allons nous connecter à l'interface web du second PfSense. Ensuite, nous nous rendrons dans le menu **System > High Availability** pour activer le service. Dans la section **PFsync Synchronize Peer IP**, nous renseignerons l'adresse IP du premier PfSense afin d'établir la synchronisation entre les deux pare-feux :



Ensuite nous allons renseigner le **login** et le **mot de passe** du **premier Pfsense** :

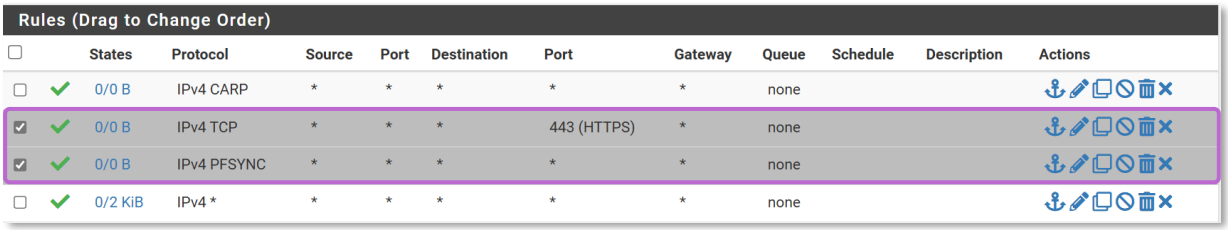


Ensuite, pour les options de synchronisation, nous sélectionnerons tous les éléments comme sur le premier pfSense afin d'assurer une synchronisation complète des données entre les deux pare-feux, dans les deux sens :



Puis pour finir nous allons cliquer sur ‘’**Save**’’ :

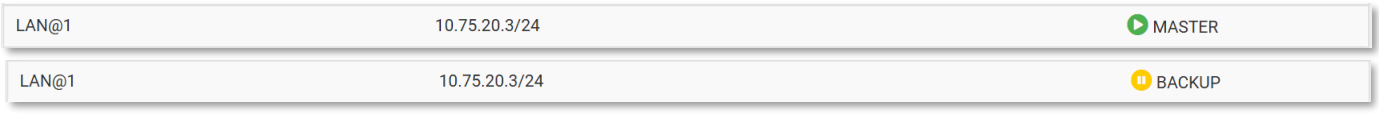
Ensuite nous allons aller dans ‘’**Firewall**’’, puis ‘’**Rules**’’ et nous allons ajouter deux règles de pare-feu pour l’interface OPT1 qui sont :



Puis nous allons **configurer un serveur DHCP** comme nous avons fait **pour le premier Pfsense**.

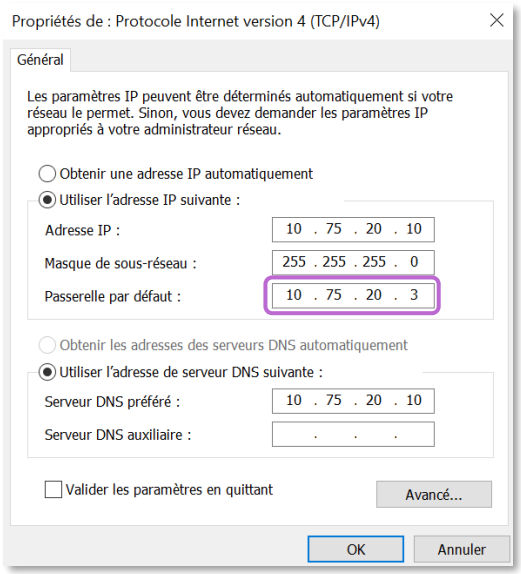
Une fois qu’on aura finis la configuration du deuxième Pfense, nous allons retourner sur le premier Pfsense et nous allons activer le service CARP puis nous allons redémarrer nos deux Pfsense.

Une fois que nos deux Pfsense auront finis de redémarrer lorsqu’on va voir le statut du service CARP, nous allons trouver le statut **Master** pour le premier Pfsense et le statut **Backup** pour le deuxième Pfsense :



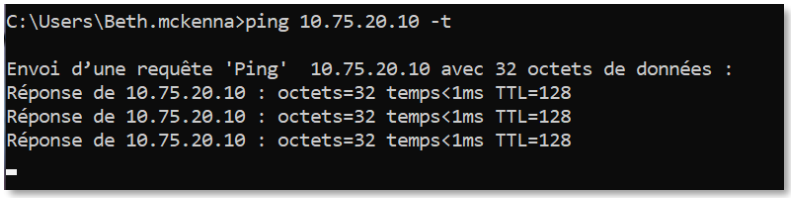
6.4) Configuration des postes

Une fois qu'on aura finis la configuration des deux Pfsense, nous allons modifier un petit paramètre pour les différentes machines, pour la passerelle par default nous allons **mettre l'IP virtuel** car c'est celle-ci notre **passerelle par default** qui sera **toujours disponible** même en cas de **panne d'un des deux Pfsense** :

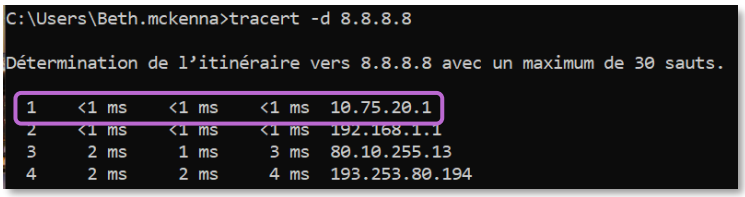


6.5) réalisations des tests

Afin de vérifier le bon fonctionnement de notre service de haute disponibilité, nous allons effectuer des tests depuis le **poste client**. Pour cela, nous **lancerons un ping en continu vers l'adresse IP de notre contrôleur de domaine** :



Et en parallèle, nous exécuterons un **tracert** afin de déterminer par lequel des deux PfSense le trafic transite actuellement pour accéder à Internet :



Comme nous pouvons le constater, le trafic passe actuellement par **pfSense 1**, qui agit comme **maître**. Nous allons maintenant **éteindre pfSense 1** afin d'observer le comportement du réseau et vérifier si la **haute disponibilité** fonctionne correctement. Nous prêterons attention au **ping en continu** vers l'adresse IP de notre contrôleur de domaine pour détecter toute **interruption temporaire** ou reprise automatique de la connectivité :

```
C:\Users\Beth.mckenna>ping 10.75.20.10 -t

Envoi d'une requête 'Ping'  10.75.20.10 avec 32 octets de données :
Réponse de 10.75.20.10 : octets=32 temps<1ms TTL=128
Réponse de 10.75.20.10 : octets=32 temps<1ms TTL=128
Réponse de 10.75.20.10 : octets=32 temps<1ms TTL=128
Réponse de 10.75.20.10 : octets=32 temps<1ms TTL=128
Réponse de 10.75.20.10 : octets=32 temps<1ms TTL=128
Réponse de 10.75.20.10 : octets=32 temps<1ms TTL=128
Réponse de 10.75.20.10 : octets=32 temps<1ms TTL=128
Réponse de 10.75.20.10 : octets=32 temps<1ms TTL=128
Réponse de 10.75.20.10 : octets=32 temps<1ms TTL=128
Réponse de 10.75.20.10 : octets=32 temps<1ms TTL=128
Réponse de 10.75.20.10 : octets=32 temps<1ms TTL=128
Réponse de 10.75.20.10 : octets=32 temps<1ms TTL=128
Réponse de 10.75.20.10 : octets=32 temps<1ms TTL=128
Réponse de 10.75.20.10 : octets=32 temps<1ms TTL=128
Réponse de 10.75.20.10 : octets=32 temps<1ms TTL=128
Réponse de 10.75.20.10 : octets=32 temps<1ms TTL=128
```

Comme nous pouvons le constater, aucune interruption ni perte de paquets n'a été observée lors du ping en continu. **Nous allons maintenant relancer un tracert afin de vérifier par quel pfSense le trafic passe à présent**, ce qui nous permettra de confirmer que le **deuxième pfSense a bien pris le relais** après la mise hors service du premier :

```
C:\Users\Beth.mckenna>tracert -d 8.8.8.8

Détermination de l'itinéraire vers 8.8.8.8 avec un maximum de 30 sauts.

  1    <1 ms    <1 ms    <1 ms  10.75.20.2
  2    <1 ms     2 ms     3 ms  192.168.1.1
  3     2 ms     2 ms     1 ms  80.10.255.13
  4     2 ms     2 ms     2 ms  193.253.80.194
```

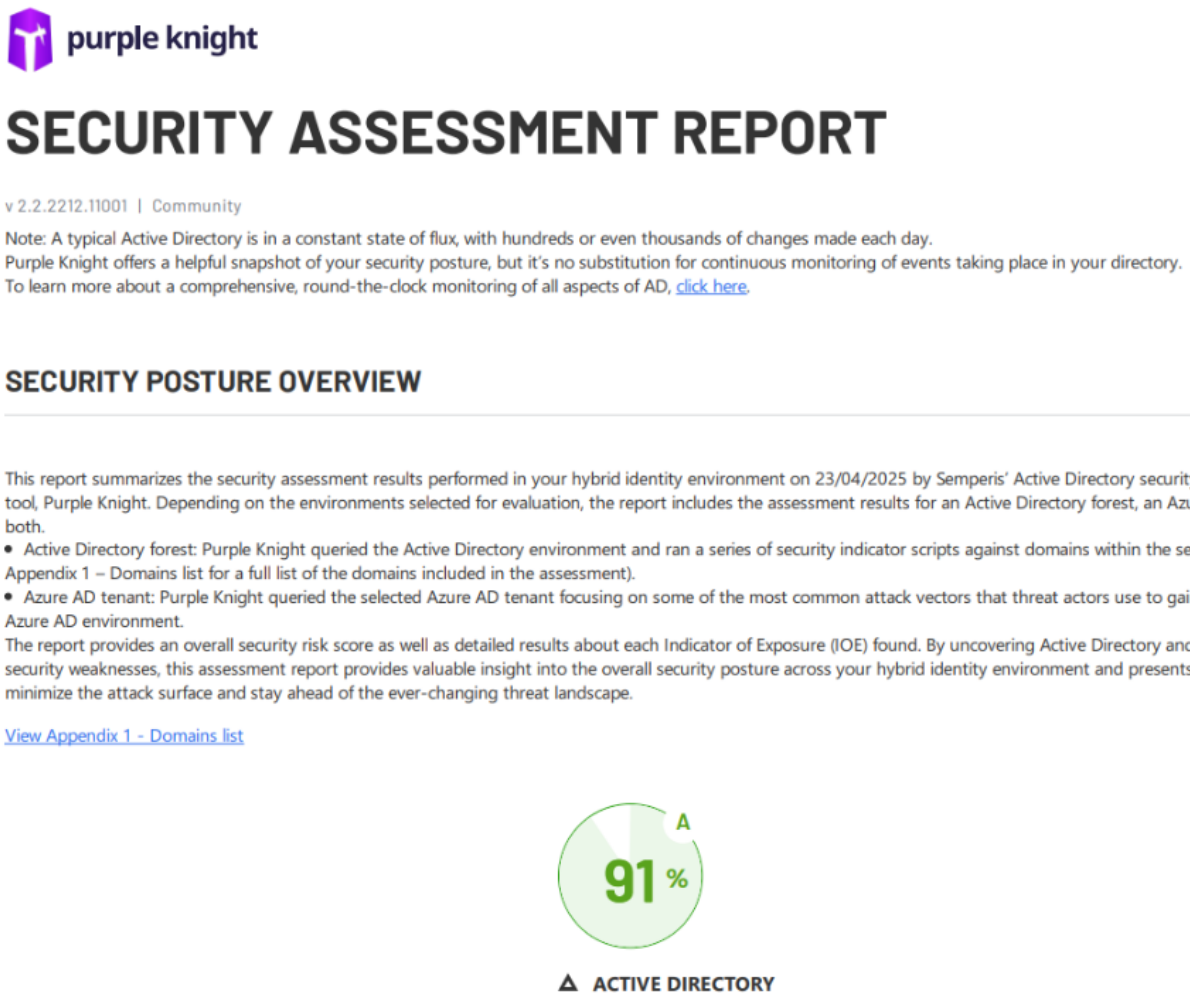
Et comme nous pouvons le constater, nous passons désormais par le deuxième pfSense, qui est passé en Maître, confirmant ainsi que notre mécanisme de haute disponibilité fonctionne correctement.

7) Conclusion

Nous arrivons à la fin de ce TP. L'installation et la configuration du contrôleur de domaine ont été réalisées avec succès, en intégrant Active Directory, la gestion des utilisateurs et des unités d'organisation. Les stratégies de groupe ont été déployées pour automatiser la configuration des fonds d'écran, le mapping des lecteurs réseau et l'accès au menu IT personnalisé selon le site. L'ajout des outils RSAT permet l'administration à distance depuis un poste client.

Dans la deuxième partie du TP, nous avons mis en place une solution de haute disponibilité avec pfSense, en configurant deux instances pfSense avec un réseau LAN et OPT1 pour assurer une redondance. La synchronisation entre les deux pfSense a été réalisée à l'aide de PFSYNC et CARP, garantissant une continuité de service en cas de défaillance du premier pfSense. Les tests effectués, y compris le ping continu et le tracert, ont confirmé que la haute disponibilité fonctionne correctement, permettant au second pfSense de prendre le relais sans interruption de service.

Pour compléter la validation de la sécurité de notre infrastructure, nous avons utilisé Purple Knight afin d'analyser la configuration de notre Active Directory, et nous avons obtenu un score de 91, confirmant ainsi un niveau de sécurité élevé. Si toutes les étapes ont été correctement suivies, le résultat est un environnement centralisé, fonctionnel et sécurisé, prêt à être utilisé en production.



purple knight

SECURITY ASSESSMENT REPORT

v 2.2.2212.11001 | Community

Note: A typical Active Directory is in a constant state of flux, with hundreds or even thousands of changes made each day.
Purple Knight offers a helpful snapshot of your security posture, but it's no substitution for continuous monitoring of events taking place in your directory.
To learn more about a comprehensive, round-the-clock monitoring of all aspects of AD, click here.

SECURITY POSTURE OVERVIEW

This report summarizes the security assessment results performed in your hybrid identity environment on 23/04/2025 by Semperis' Active Directory security assessment tool, Purple Knight. Depending on the environments selected for evaluation, the report includes the assessment results for an Active Directory forest, an Azure AD tenant, or both.

- Active Directory forest: Purple Knight queried the Active Directory environment and ran a series of security indicator scripts against domains within the selected forest (see Appendix 1 – Domains list for a full list of the domains included in the assessment).
- Azure AD tenant: Purple Knight queried the selected Azure AD tenant focusing on some of the most common attack vectors that threat actors use to gain access to the Azure AD environment.

The report provides an overall security risk score as well as detailed results about each Indicator of Exposure (IOE) found. By uncovering Active Directory and Azure AD security weaknesses, this assessment report provides valuable insight into the overall security posture across your hybrid identity environment and presents opportunities to minimize the attack surface and stay ahead of the ever-changing threat landscape.

View Appendix 1 - Domains list

A
91 %
ACTIVE DIRECTORY

Tous les documents et scripts utilisés pour la configuration des stratégies de groupe sont joints à ce document, afin de permettre une consultation complète ou une réutilisation dans un autre environnement similaire.