Activités en entreprise

Activité 1 - Utilisation de DIADEME

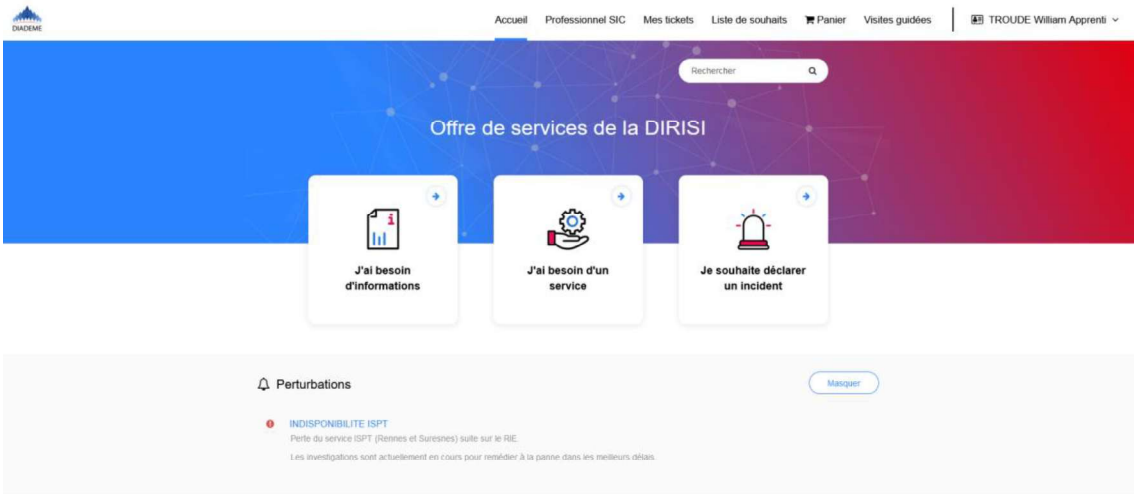
1/ Introduction

DIADEME est un outil de gestion de tickets basé sur l'outil de Servicenow. Il a été adapté et mis en place au sein du Ministère en 2020 pour remplacer APSI-GI et améliorer les capacités de l'outil. DIADEME est plus qu'un outil de gestion de tickets même si cela reste sa fonction primaire au niveau du SDK. Il permet à tous les usagers du Ministère des Armées d'effectuer des demandes catalogues et/ou de demander l'intervention d'un technicien lorsqu'ils rencontrent un problème.
DIADEME est en partie géré par le Centre de Compétences DIADEME (CCD) mais le système permet à chaque unité d'administrer son tableau de bord.

2/ Interface utilisateur DIADEME

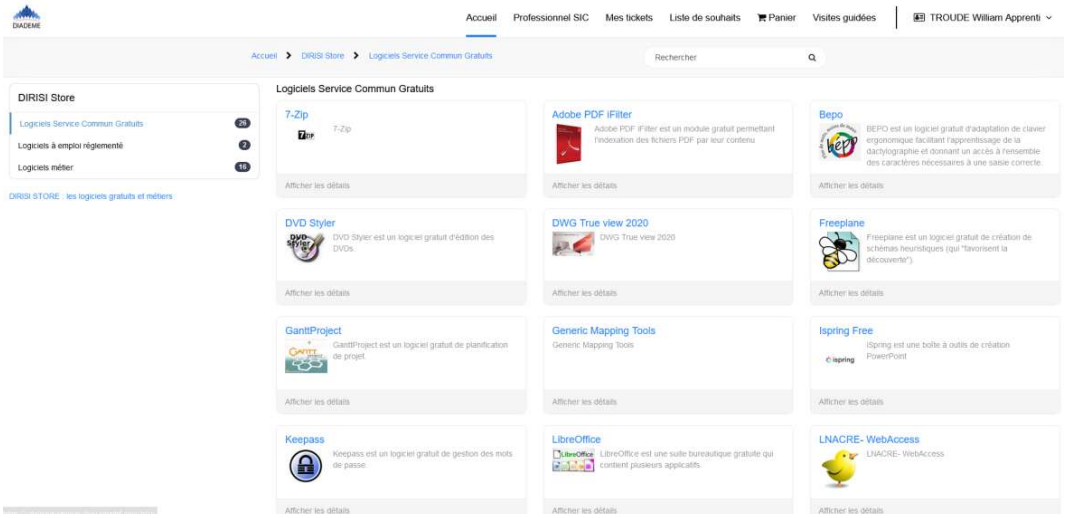
DIADEME possède deux interfaces principales : l'interface utilisateur et l'interface technicien.

Ici, l'interface utilisateur. Elle est disponible sur tous les postes directement sur le bureau afin d'être accessible le plus simplement possible, permettant ainsi d'y accéder malgré les problèmes que peuvent rencontrer les usagers du ministère.



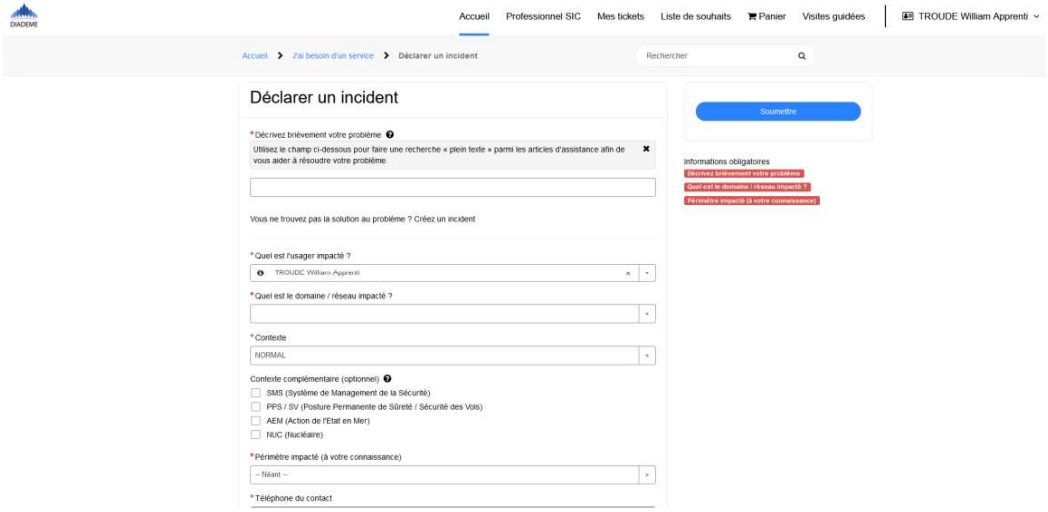
Cette interface permet à l'utilisateur d'accéder à de nombreuses fonctionnalités. Dans un premier temps, sur cette page d'accueil, les personnes peuvent voir les pannes généralisées connues et leur statut.

Ensuite, il est possible d'accéder au DIRISI Store :



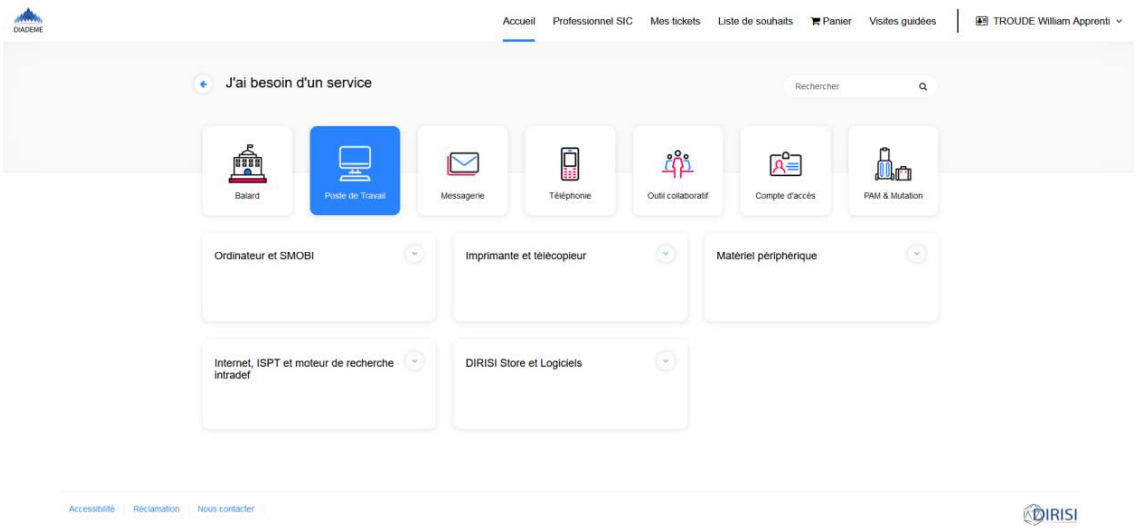
Le DIRISI Store permet à tous les utilisateurs d'effectuer une demande d'installation de logiciel ou de driver sans avoir à passer par un ticket d'installation classique. Cette option a pour but d'alléger la charge d'installation auprès des techniciens et ainsi de faciliter et d'accélérer le processus pour les utilisateurs.

La partie la plus importante : La création de tickets. DIADEME permet aux utilisateurs d'accéder à deux types de demande. Tout d'abord les tickets d'incidents :



La création de ticket d'incident est la plus simple. Les utilisateurs donnent leurs informations : Nom, Prénom de la personne concernée, poste de travail concerné (les utilisateurs informent le numéro d'UC – Unité Centrale), l'environnement et l'unité concernés. Ce paramètre est important puisqu'il permet au Front Office du Service Desk d'aiguiller les tickets vers les services concernés si c'est nécessaire, par exemple, les tickets à propos de systèmes classifiés ne doivent pas être traités par les techniciens du Front Office et sont donc automatiquement redirigés vers le service concerné. Pour finir, ils décrivent le problème rencontré.

Enfin, les demandes catalogues. Ici, les utilisateurs accèdent à une liste supposée exhaustive de types de demandes. Ces dernières sont réparties dans plusieurs catégories pour affiner et simplifier le traitement, que ce soit pour l'usager que pour le technicien qui s'en occupera.

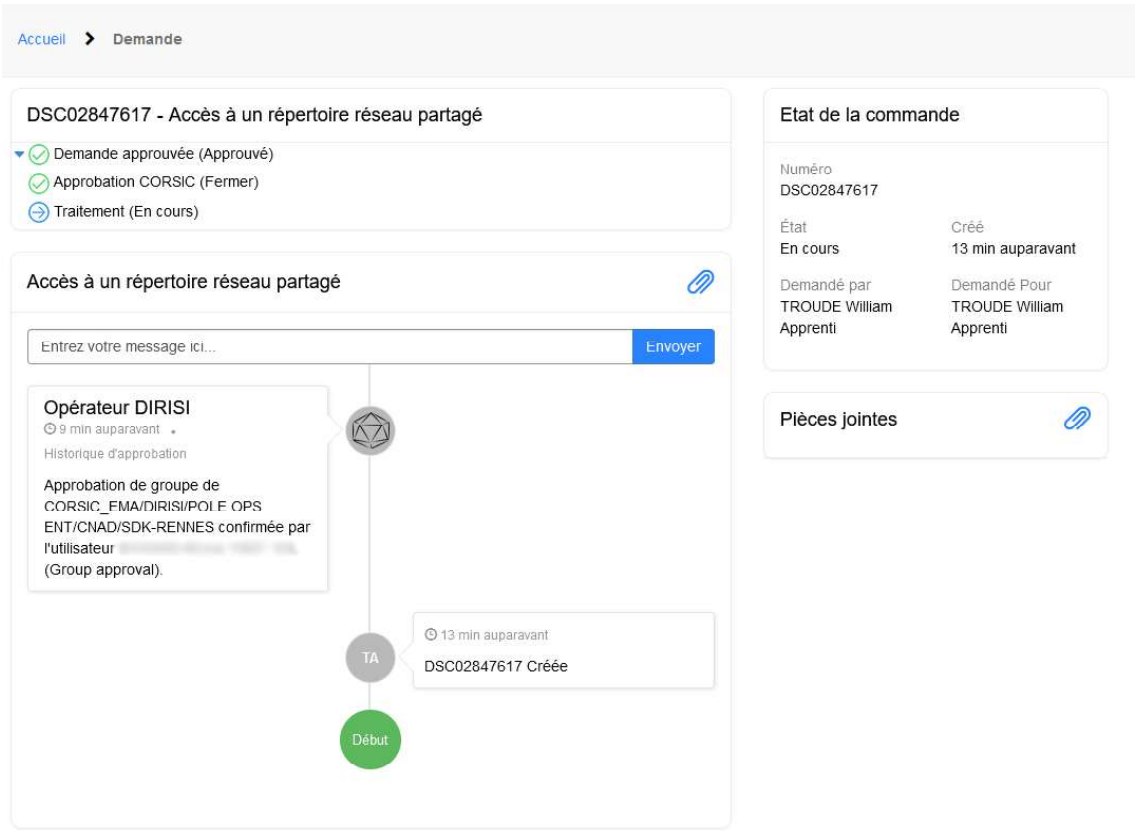


Ici, j'ai pris pour exemple la FC 362 : Demande d'accès à un répertoire réseau partagé. Les informations qui doivent être remplies changent en fonction du ticket ce qui, comme je le disais plus haut, sert à la simplification de la demande pour les utilisateurs et permet au technicien d'avoir toutes les informations dès la réception du ticket.

Dans le cas de la demande d'accès, il doit y être renseigné, la personne pour qui la demande est effectuée, son compte « Windows » qui correspondant à l'identifiant qui lui a été attribué lorsque son compte a été créé sur l'AD (Active Directory) et enfin le plus important, le groupe correspondant au répertoire souhaité. Ce groupe est indispensable. Il est renseigné dans un arbre de l'AD et détermine le ou les dossiers auxquels l'utilisateur pourra accéder sur un serveur de partage de fichiers. Il faut donc également préciser si le droit doit être donné en lecture uniquement ou lecture/écriture. Ces groupes peuvent également servir à accorder des accès à certaines fonctionnalités ou à des services à l'aide des GPO mises en place sur les postes du Ministère.

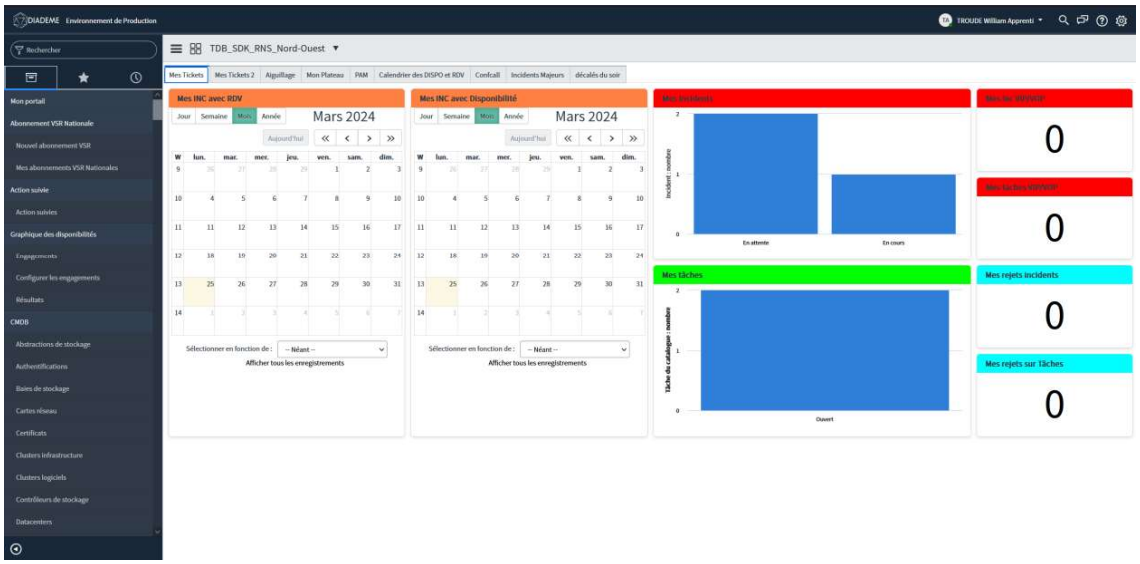
Une fois toutes ces informations renseignées et si elles sont bien renseignées, l'utilisateur n'a alors plus besoin de revenir dessus. Ces informations inclues lors de la création du ticket suffisent au technicien pour effectuer le travail souhaité.
Cependant, le ticket possède évidemment une interface prenant la forme d'une frise permettant à l'utilisateur de prendre connaissance de l'évolution de sa demande et de prendre contact directement avec le technicien en chattant sur cet onglet.

Ici, on peut voir le déroulement des évènements : La demande a été créée il y a 13 minutes. Un numéro commençant par DSC lui a été attribué. Ce dernier correspond à la demande et non à la tâche en elle-même. On verra plus tard qu'il est possible d'avoir plusieurs tâches pour une demande et que ces dernières se voient attribuer un numéro SCTASK et sont toutes reliées à la demande DSC. Elle passe ensuite en attente d'approbation CORSIC. Lorsque ce dernier approuve, un évènement se place et la demande est désormais visible dans la panière de tâches des techniciens.

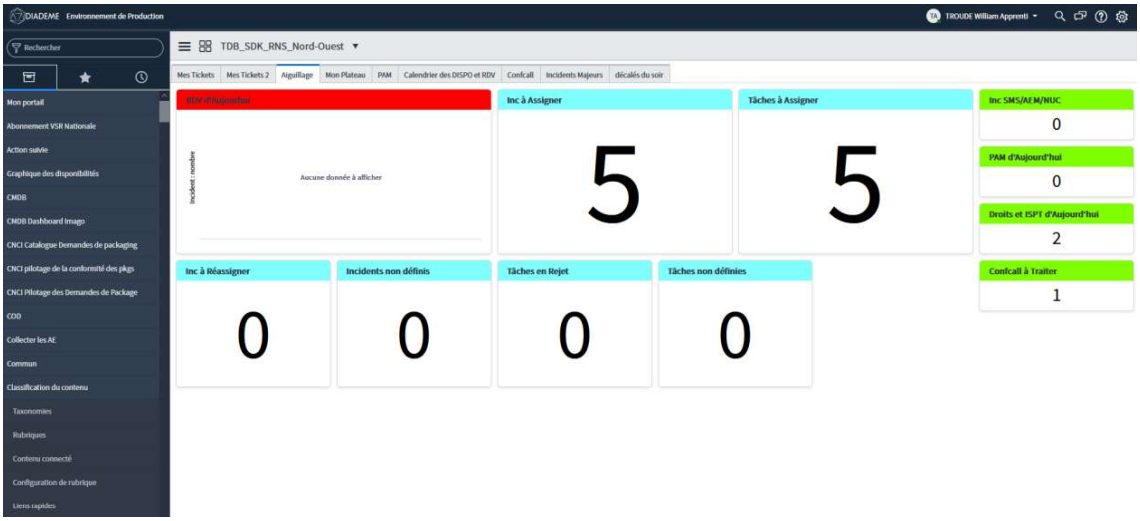


3/ L'interface Administrateur

Le technicien possède lui une interface totalement différente et pas accessible de la même façon.

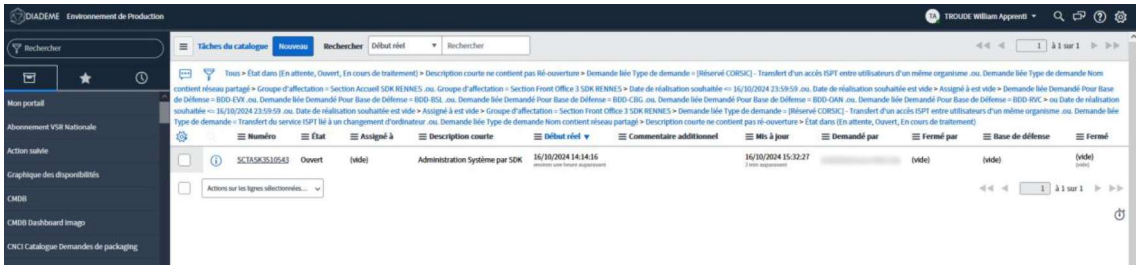


Sur la photo ci-dessus se trouve le tableau de bord du portail technicien de DIADEME. Il varie en fonction des services et des besoins des unités mais sont uniformisés pour les techniciens d'une même unité afin d'assurer la continuité du service.
Ce tableau de bord comporte plusieurs onglets. Tout d'abord, un premier affichage nous donne le nombre de tickets présents dans ce qu'on appelle la « panière d'aiguillage ».

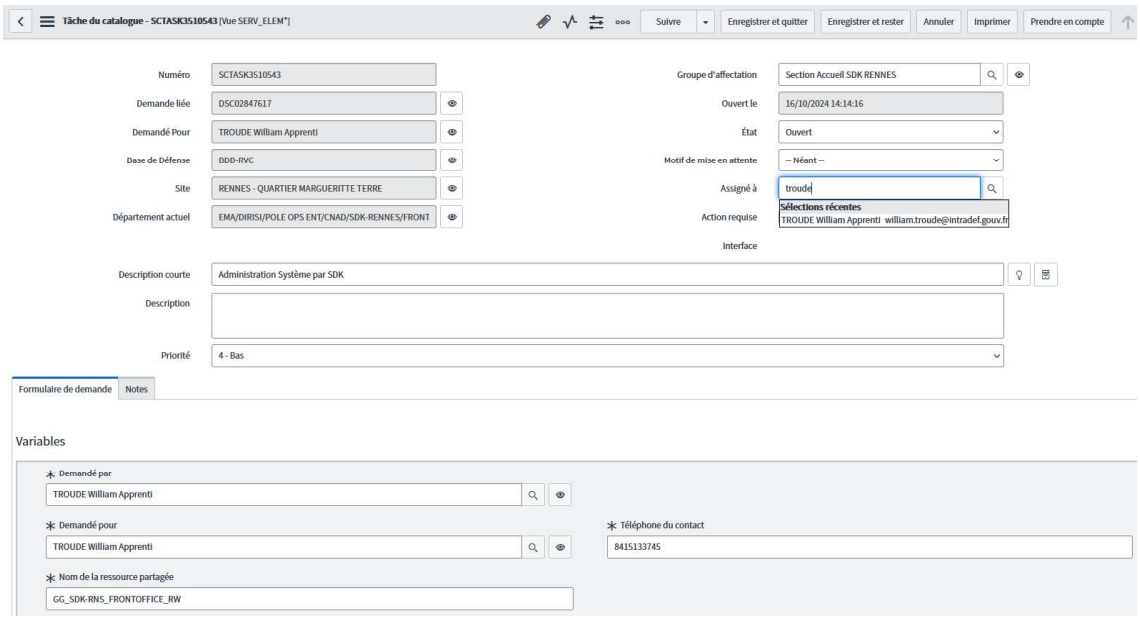


La première tâche d'un technicien du Service Desk est l'aiguillage. Étant membre du Front Office, il est en première ligne face à la demande de l'usager. Ainsi, au SDK Rennes, sur chaque plateau, un technicien se voit attribuer la tâche d'aiguillage pour une demi-journée. Elle consiste en, la vérification de la bonne réalisation des tickets par les utilisateurs et si c'est le cas, il les aiguille aux autres techniciens afin qu'ils réalisent la tâche demandée.

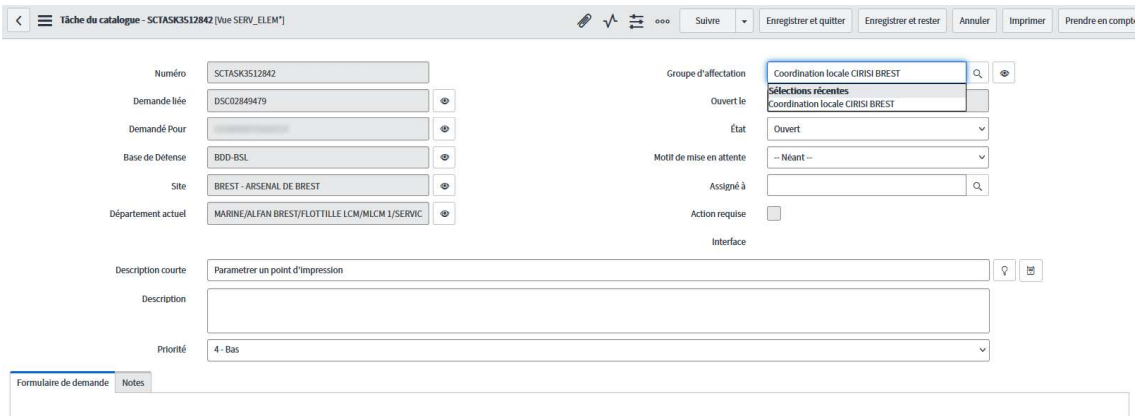
Prenons l'exemple du ticket que j'ai créé précédemment. Ici, on peut voir qu'il apparait dans la panière « Droits et ISPT d'Aujourd'hui ». Ces catégories sont définies par une liste de filtres. On voit qu'il n'est assigné à personne pour le moment, on voit la description courte et quelques autres informations.



Lorsque l'on clique dessus, on accède à une nouvelle page où l'on voit le formulaire de la demande, des informations supplémentaires, les notes où le technicien peut laisser un message dans les notes de travail pour que cela ne soit visible que par les techniciens. Cette option permet principalement de tracer les actions et potentiellement de communiquer des informations pour les services vers lesquels les demandes peuvent être transférées. Le commentaire additionnel permet de communiquer directement avec l'utilisateur. On peut donc aiguiller ce ticket vers un technicien.



De plus, la panière du SDK reçoit un grand nombre de tickets qui sont hors compétences du service. Ainsi, l'une des tâches les plus importantes est la prise d'information et la redirection vers les services concernés par les demandes en question. Deux exemples qui reviennent souvent démontrent parfaitement la mission du technicien. Tout d'abord, dans le cas de la gestion des serveurs d'impression : Les serveurs d'impression n'étant pas gérés par le SDK mais par les CIRISI* locaux, s'il est nécessaire d'enrôler, de supprimer, ou toute autre gestion de carte d'impression, le SDK vérifie que la demande est bien rédigée puis transmet ce ticket à la coordination locale du CIRISI concerné.



Autre exemple, lors de la récupération de fichiers sur un lecteur réseau : Les serveurs dédiés aux lecteurs réseaux des unités possèdent des sauvegardes et sont gérés par le CNMO-SI de Rennes. Lorsqu'un utilisateur fait une demande de récupération de fichiers sur un lecteur réseau, nous devons vérifier s'il précise bien :

- Le nom du lecteur réseau en question
- La date et l'heure de récupération du fichier/dossier souhaité
- L'emplacement exact du fichier/dossier souhaité

Si ces trois informations sont bien présentes dans le ticket, il est envoyé vers la coordination locale du CNMO-SI (Centre National de Mise en Œuvre – Systèmes d'Information) de Rennes pour qu'ils puissent récupérer la sauvegarde du fichier/dossier souhaité. Si les informations ne sont pas présentes, il est du ressort du technicien à l'aiguillage de diriger le ticket vers un technicien afin qu'il prenne contact avec le rédacteur du ticket pour récupérer ces informations nécessaires.

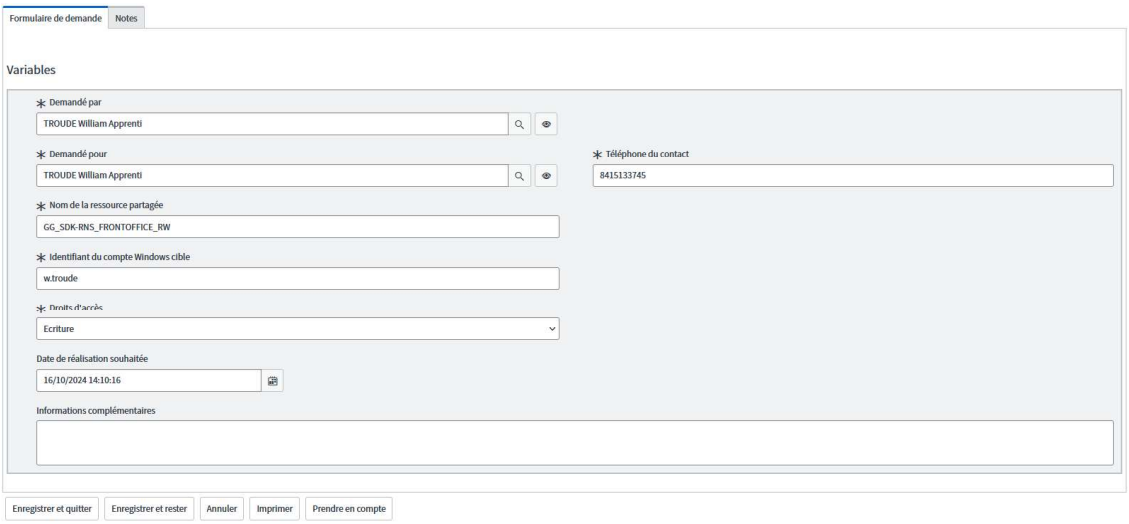
*Centre Interarmées des Réseaux d'Infrastructure et des Systèmes d'Information

Comme on peut le voir sur les précédentes captures d'écran, les tickets sur DIADEME contiennent un grand nombre d'informations sur la demande, sur le rédacteur et sur la personne pour qui le ticket a été rédigé. On y retrouve :

- Le nom de la personne ayant rédigé le ticket
- Le nom de la personne pour qui le ticket a été rédigé (cela peut être la même que celle ayant rédigé)
- Le ou les numéros de téléphone
- L'unité dans laquelle se trouve la personne
- Le créneau de disponibilité de l'utilisateur (uniquement en cas de ticket d'incident)

Toutes ces informations se trouvent sur la partie supérieure gauche de l'affichage du ticket.

En plus de ces informations présentes sur tous les tickets, chaque demande catalogue inclut des informations liées à la demande qui vont permettre au technicien de réaliser les demandes dès la réception du ticket. Reprenons l'exemple de l'accès à un répertoire partagé.

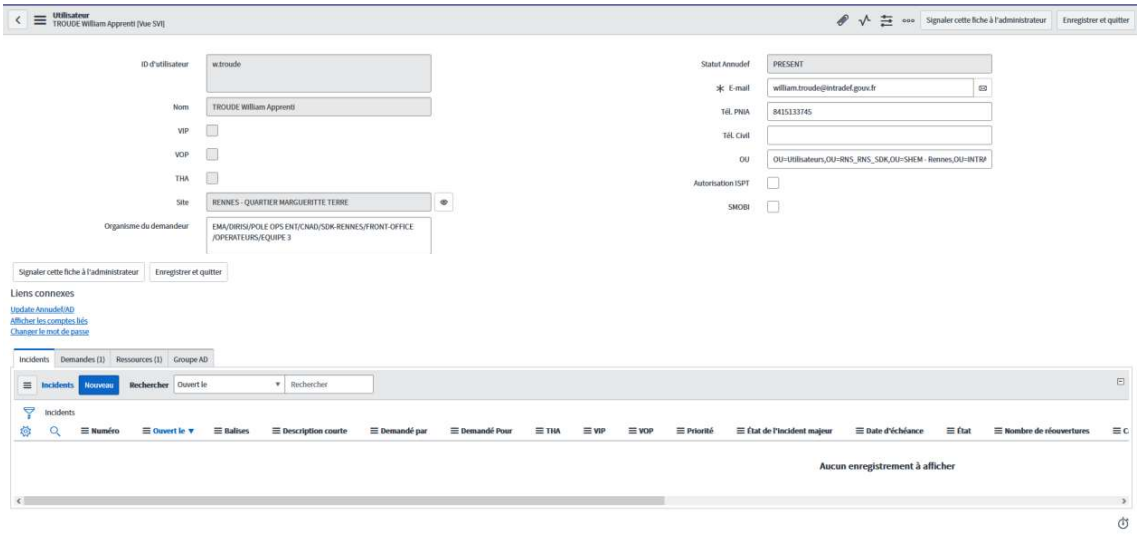


On retrouve les informations renseignées par l'utilisateur. Le rédacteur, la personne concernée, l'identifiant Windows cible, le groupe ainsi que les Informations complémentaires. La création d'une demande catalogue n'étant pas toujours très intuitive, il arrive très souvent que le rédacteur du ticket mette les informations dans cette case pour être sûr de ne pas remplir n'importe quoi. Il est donc très important de vérifier si ces informations sont remplies ou non pour être fixé sur l'action demandée.

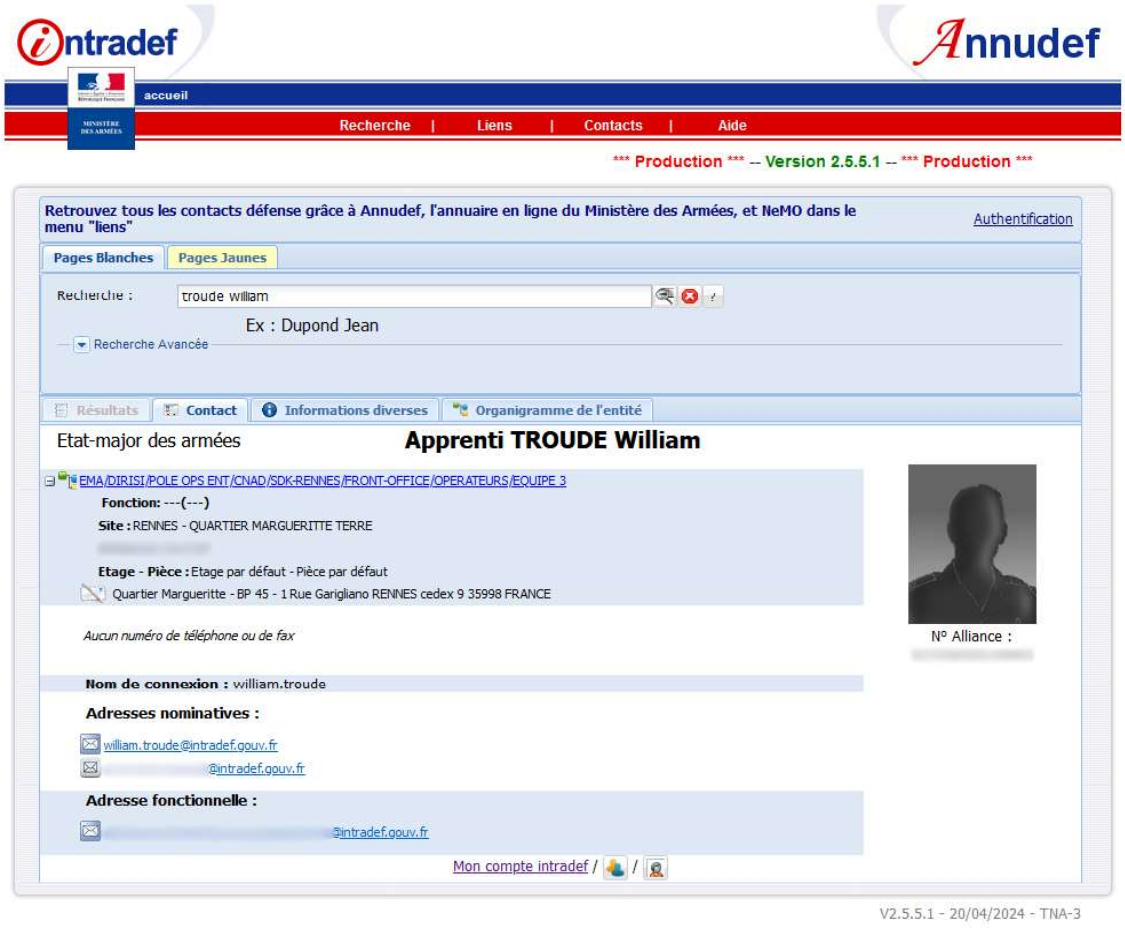
4/La gestion de parc avec DIADEME

Au-delà de la création et de la gestion des tickets, DIADEME permet notamment un inventaire et un accès à un grand nombre d'informations pour la gestion du parc informatique du Ministère. Ces informations sont souvent tirées d'autres outils mais DIADEME permet de les regrouper et d'y accéder par un seul endroit.

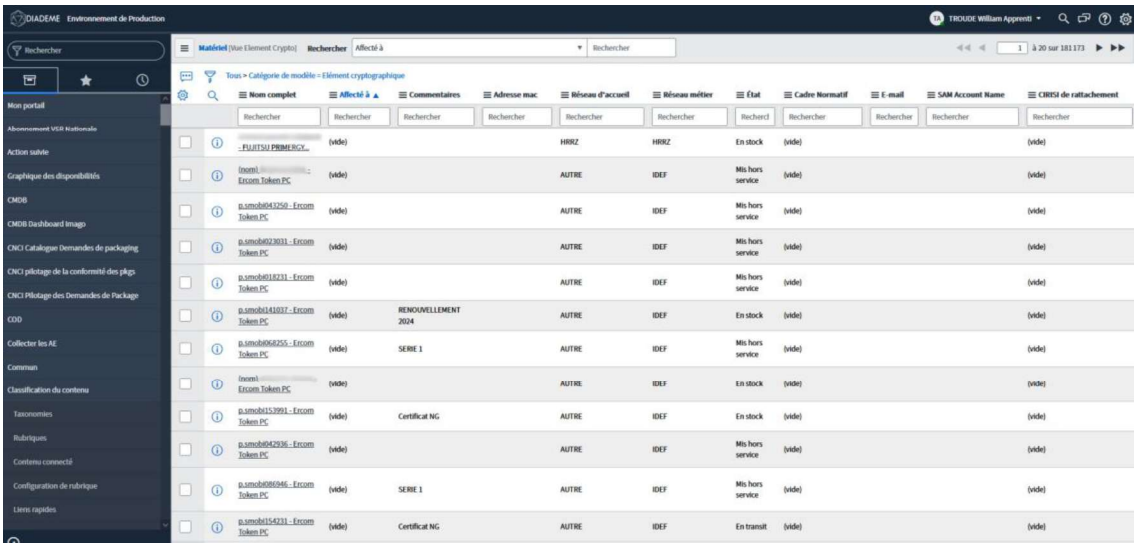
Tout d'abord au niveau des utilisateurs, DIADEME concentre un grand nombre d'informations et nous permet notamment de retrouver d'anciens tickets ouverts par ou pour l'utilisateur en question. Cela nous aide par exemple lorsqu'il nous informe qu'un problème avait été résolu dans un précédent ticket ou que son problème est survenu depuis une intervention mais qu'il ne possède plus les informations du ticket. Aussi, on y retrouve toutes les informations nécessaires pour prendre contact avec lui.



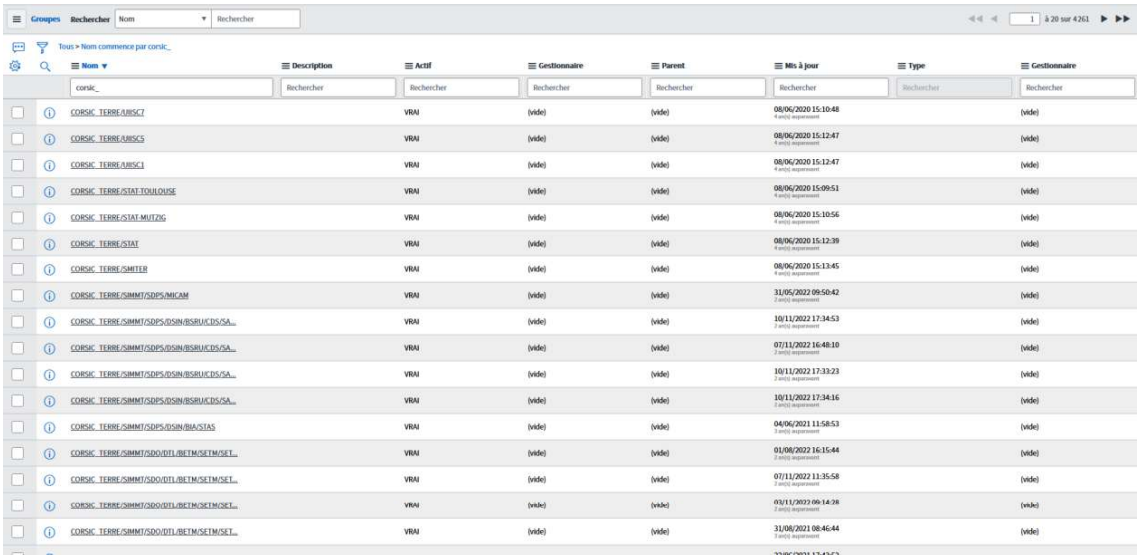
Cependant, pour les informations de contact d'un utilisateur, ANNUDEF est un outil bien plus pratique. Possédant beaucoup plus d'informations, il nous permet notamment d'accéder directement aux informations de son compte Intradef. Il nous permet aussi d'accéder à son unité et de remonter l'arbre ou même de savoir s'il est en mutation.

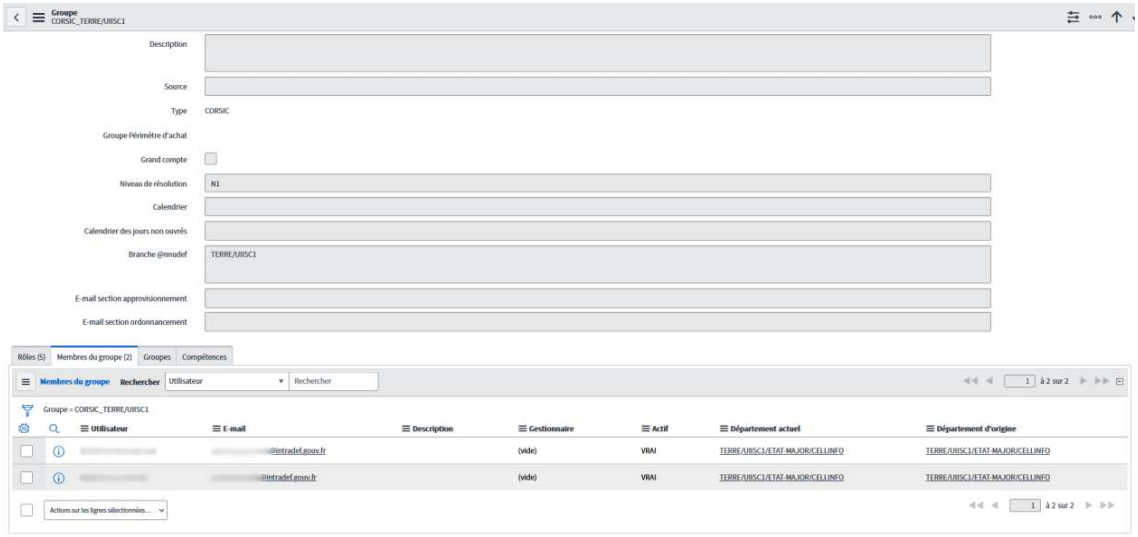


Au niveau de la gestion de parc informatique plus concrète, DIADEME nous permet d'accéder aux informations des clés Token et des téléphones portables de la solution SMOBI (Solution de MOBilité d'Intradef). Lorsqu'un utilisateur a un problème avec un « token » lui permettant de se connecter au réseau Intradef à distance ou avec son téléphone portable SMOBI, on peut consulter DIADEME. Parmi la liste des « token », on accède à des informations nécessaires à certaines interventions comme la personne à qui le token est attribué, ou bien les codes PUK indispensables pour réinitialiser le mot de passe du token lorsque ce dernier est bloqué.



DIADEME possède également une liste des Groupes CORSIC (CORrespondant Systèmes d'Informations et de Communications). Les CORSIC sont des personnes désignées pour transmettre des informations, valider les demandes catalogues et répondre parfois aux questions des utilisateurs. Ils sont présents dans chaque arbre d'unités et possèdent des droits supérieurs aux utilisateurs classiques pour pouvoir valider les demandes ou accéder à certaines informations concernant leurs unités. Ainsi, il nous est important, lorsque l'on a un utilisateur au téléphone, de vérifier qui est le CORSIC de son unité ou de vérifier si le CORSIC a bien ses droits à jour sur DIADEME.





5/Conclusion

Pour finir, DIADEME est un outil complet nous permettant d'obtenir un grand nombre d'information pour réaliser au mieux notre travail d'administration. Aussi, il nous permet d'être au plus près de l'utilisateur et de ses besoins. Malgré diverses difficultés d'utilisation, il s'agit d'un outil important et plus qu'utile même au-delà de la simple gestion des tickets. Il s'agissait du premier outil à maîtriser lors de mon arrivée au SDK et je trouvais important de parler de ce pan de notre travail.

Activité 2 – Mise en place d'une infrastructure MCM et utilisation au sein du SDK

1/ Installation de l'infrastructure MCM

Pour fonctionner correctement, MCM nécessite au minimum 3 serveurs :

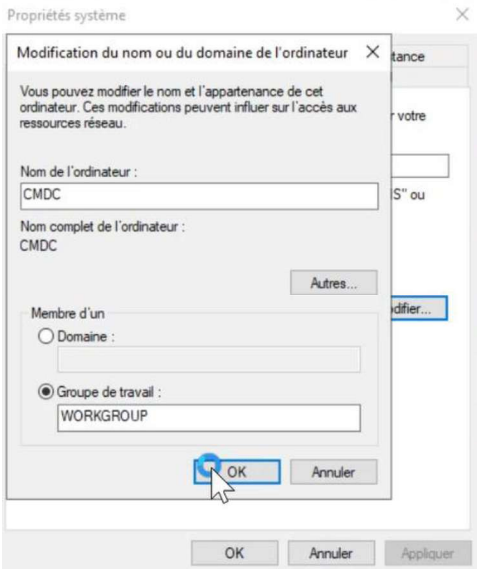
- Un contrôleur de domaine Active Directory
- Un serveur MCM
- Un serveur SQL

1.1/ Installation des machines

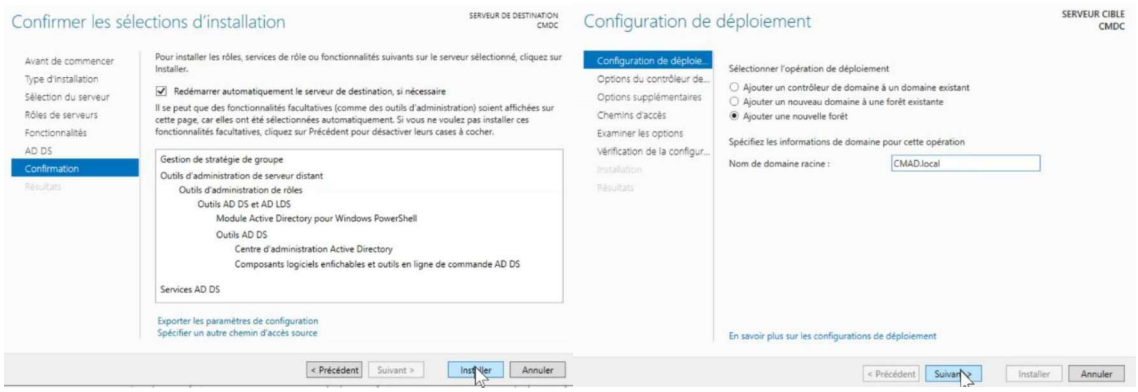
Pour commencer on va préparer les trois machines et les faire rejoindre le domaine.

On débute donc par **le contrôleur de domaine.**

Comme pour chaque installation de l'Active Directory, on vient renommer le serveur. Ici on l'appellera « CMDC ».

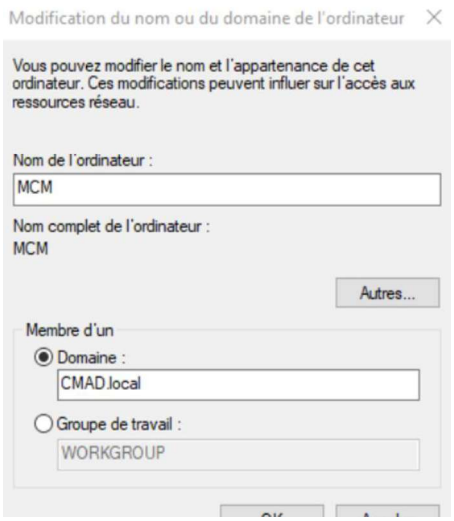


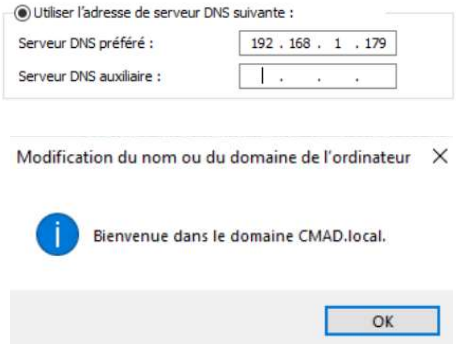
On redémarre le serveur et on passe ensuite à l'ajout des rôles. On vient donc sélectionner le rôle AD DS qui va installer automatiquement les fonctionnalités nécessaires. Par la suite on promeut CMDC en tant que contrôleur de domaine et on définit le nom de domaine racine :



Serveur MCM

Dans un premier temps on vient indiquer l'adresse IP du contrôleur de domaine en tant que serveur DNS préféré. Par la suite on change le nom du serveur et on lui fait rejoindre le domaine.





Serveur SQL

Pour le serveur SQL, c'est comme pour le serveur MCM, on change son nom en CMSQL et on l'ajoute au domaine.

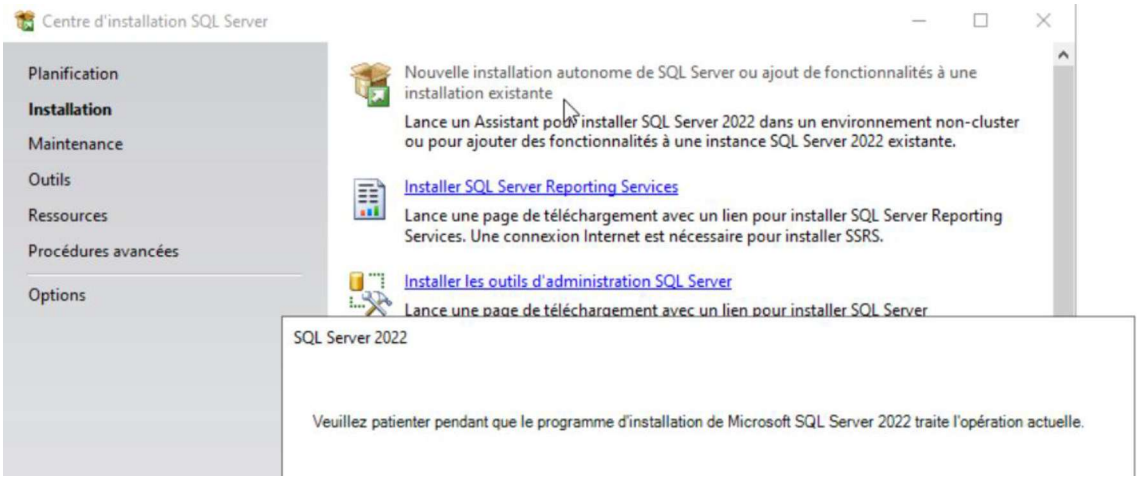
1.2/ Paramétrage des prérequis

Pour les prérequis, on va commencer par installer la base de données SQL. On ajoute le serveur MCM en tant qu'administrateur du serveur SQL dans la gestion de l'ordinateur. Il s'agit d'un prérequis pour l'installation de MCM 2403.
On vient faire trois partitions du disque pour séparer le disque local, une partition pour SQL (E:) et une partition pour les logs (L:).

Après on télécharge l'exécutable pour développeur de SQL Server 2022. On le lance et on choisit de télécharger le média. Ça nous laisse l'opportunité de récupérer l'image ISO et de la monter. Ce qui nous donne :

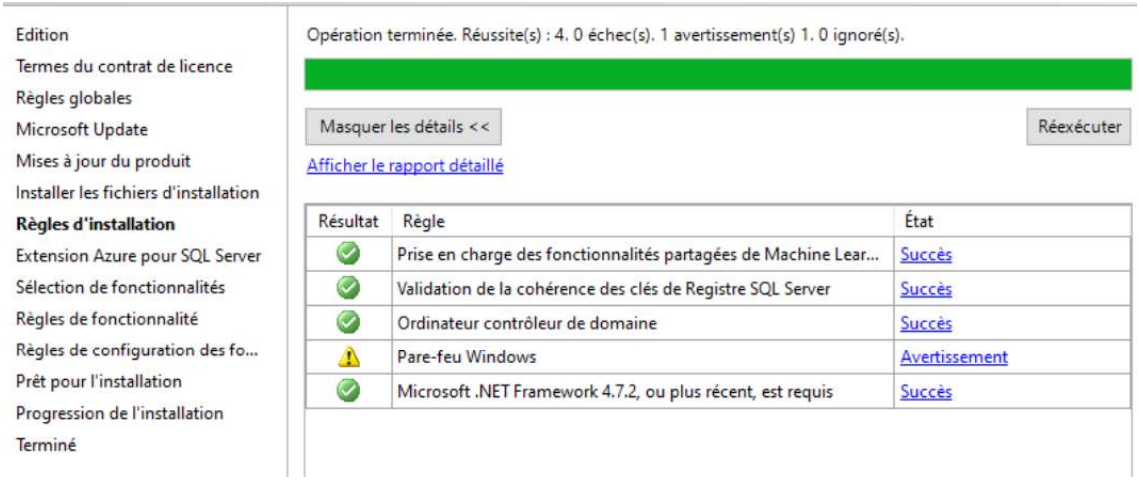
Maintenant on vient ouvrir le lecteur F et on exécute le setup.exe ce qui nous amène sur la fenêtre suivante :

On va dans « Installation » et on choisit « Nouvelle installation autonome… ».



On laisse l'édition « Developer » parce que je n'ai pas de licence puis on laisse par défaut.

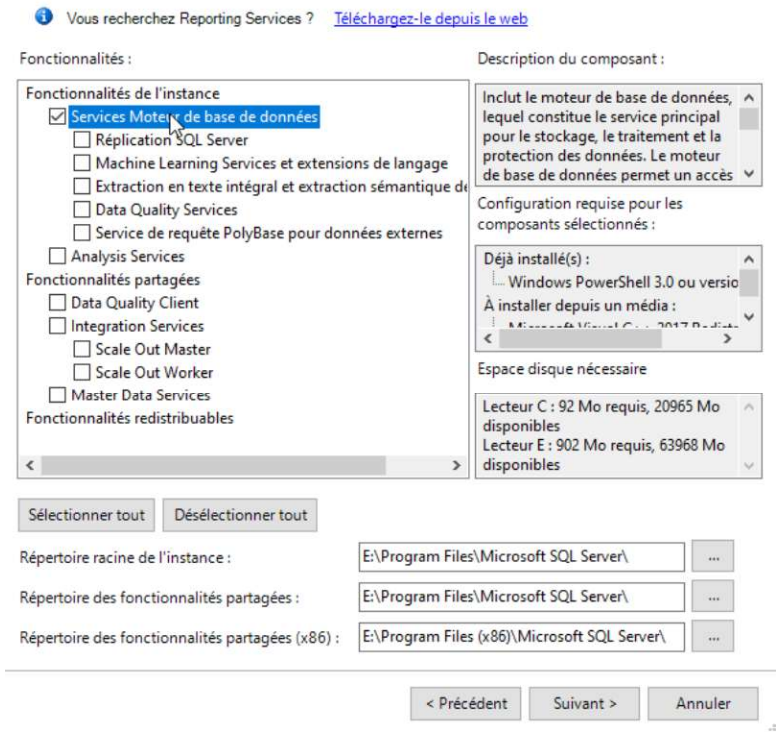
La vérification des règles d'installation s'est bien déroulée. Elle nous affiche simplement un avertissement pour le pare-feu car il est activé et que les règles pour SQL ne sont pas encore définies.



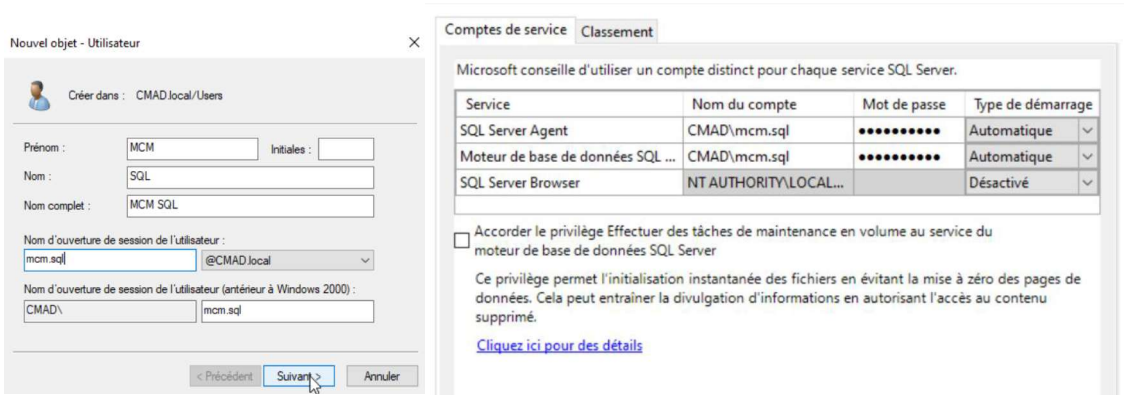
Pour résoudre ce potentiel problème, on va venir ajouter ces deux règles de pare-feu :

```
PS C:\Users\Administrateur.CMAD> New-NetFirewallRule -DisplayName "SQLServer Autorisation Entrant" -Direction Inbound -LocalPort 1433 -Protocol TCP -Action Allow


Name                            : {beb32879-cc6f-4bc1-9c1f-7ccbc50a67a9}
DisplayName                     : SQLServer Autorisation Entrant
Description                     :
DisplayGroup                    :
Group                           :
Enabled                         : True
Profile                         : Any
Platform                        : {}
Direction                       : Inbound
Action                          : Allow
EdgeTraversalPolicy             : Block
LooseSourceMapping              : False
LocalOnlyMapping                : False
Owner                           :
PrimaryStatus                   : OK
Status                          : La règle a été analysée à partir de la banque. (65536)
EnforcementStatus               : NotApplicable
PolicyStoreSource               : PersistentStore
PolicyStoreSourceType           : Local
RemoteDynamicKeywordAddresses   : {}

PS C:\Users\Administrateur.CMAD> New-NetFirewallRule -DisplayName " SQLServer Browser Service" -Direction Inbound -LocalPort 1434 -Protocol UDP -Action Allow


Name                            : {0e5a85cc-90df-4939-a066-16fa32b40a12}
DisplayName                     :  SQLServer Browser Service
Description                     :
DisplayGroup                    :
Group                           :
Enabled                         : True
Profile                         : Any
Platform                        : {}
Direction                       : Inbound
Action                          : Allow
EdgeTraversalPolicy             : Block
LooseSourceMapping              : False
LocalOnlyMapping                : False
Owner                           :
PrimaryStatus                   : OK
Status                          : La règle a été analysée à partir de la banque. (65536)
EnforcementStatus               : NotApplicable
PolicyStoreSource               : PersistentStore
PolicyStoreSourceType           : Local
RemoteDynamicKeywordAddresses   : {}
```

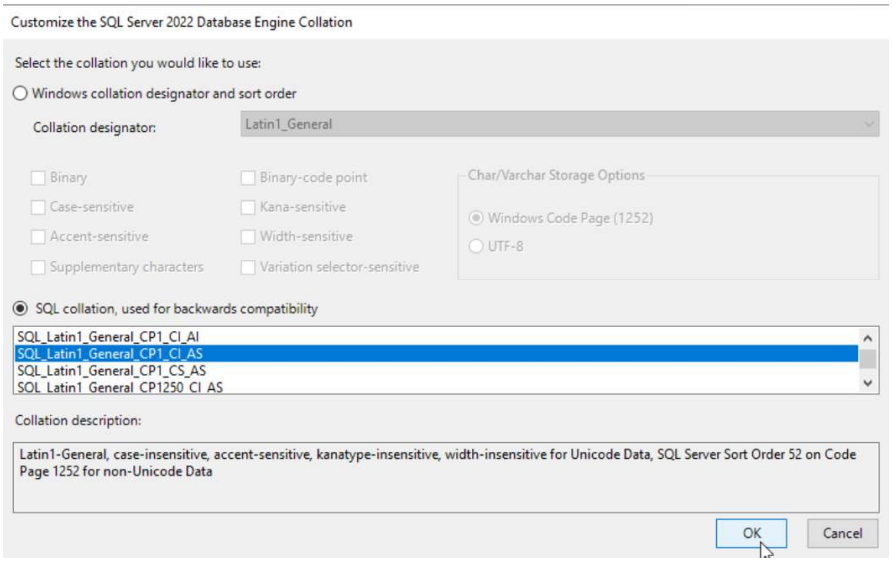
Ensuite, de nouveau dans l'installateur de SQLServer on vient cocher « Services Moteur de base de données » et on remplace dans les répertoires, le C par E qui correspond à la partition que l'on a libérée pour SQL.



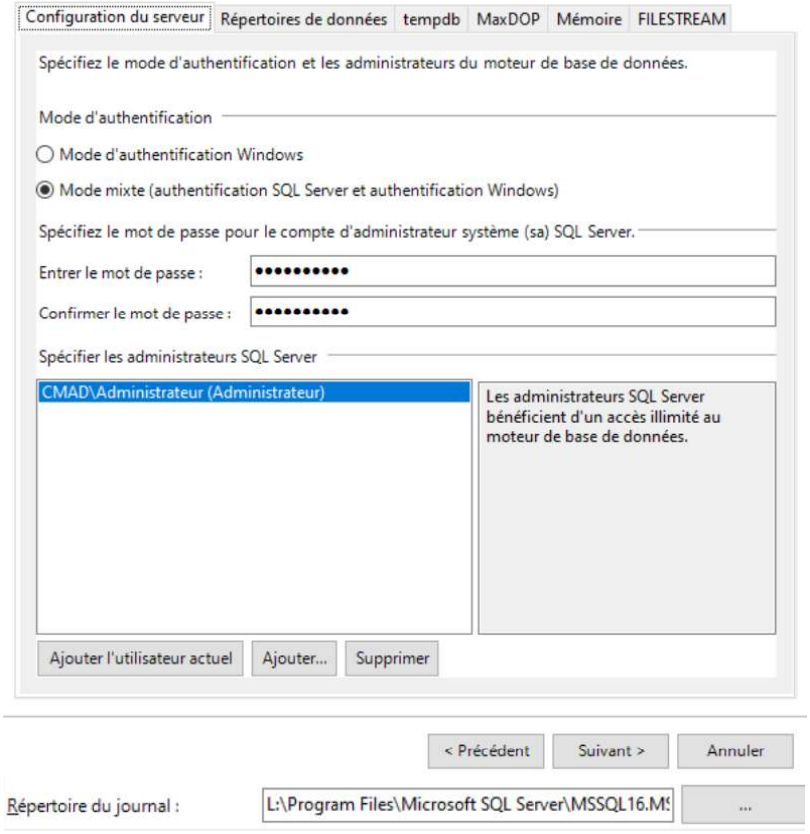
On crée un utilisateur dédié à l'administration du serveur SQL et on vient le renseigner dans les comptes de service.



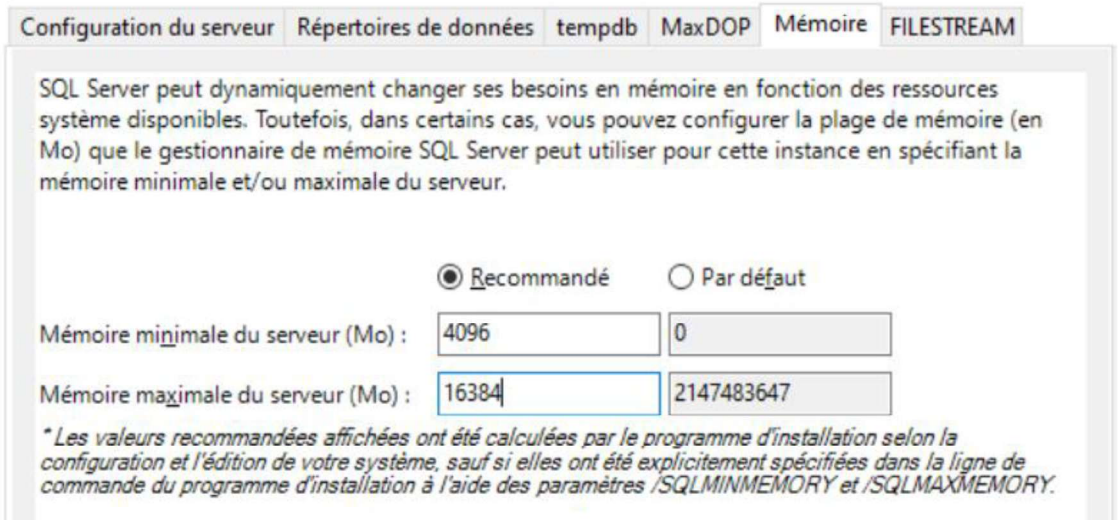
Avant de faire suivant, il faut impérativement aller dans « Classement » ou « Collation » en anglais et modifier comme tel :



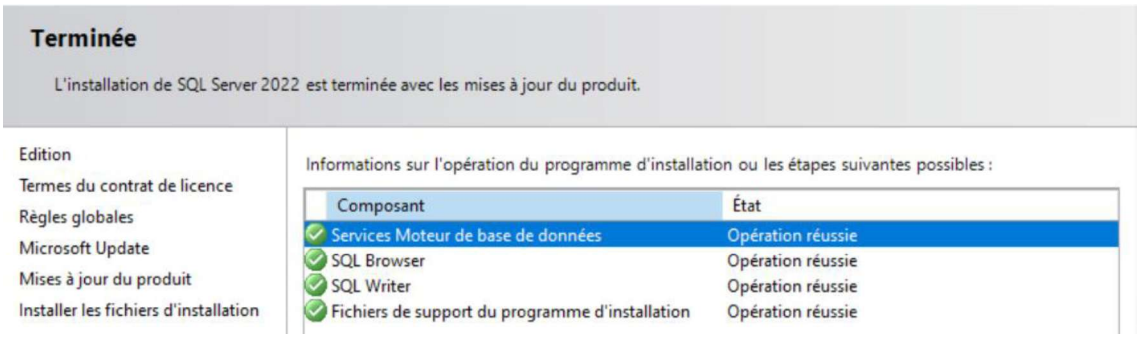
Pour la configuration du moteur de base de données, on choisit « Mode mixte », on ajoute un mot de passe et on ajoute par sécurité le compte administrateur du domaine. Ensuite on vient vérifier dans « Répertoires de données » que le bon chemin est renseigné. Pour les logs on va préciser le disque L que l'on a créé en amont.



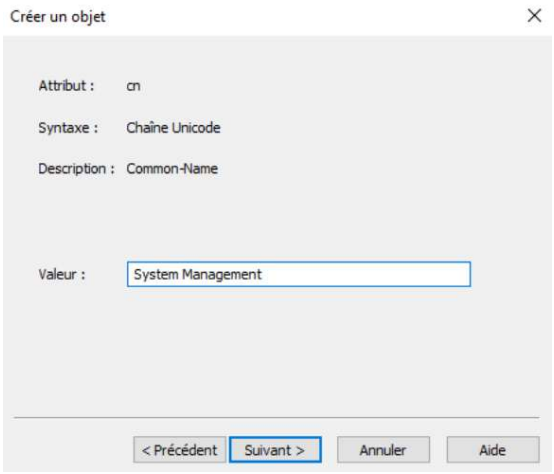
Pour la mémoire, on vient fixer le minimum et le maximum, ici 4 à 16Go.



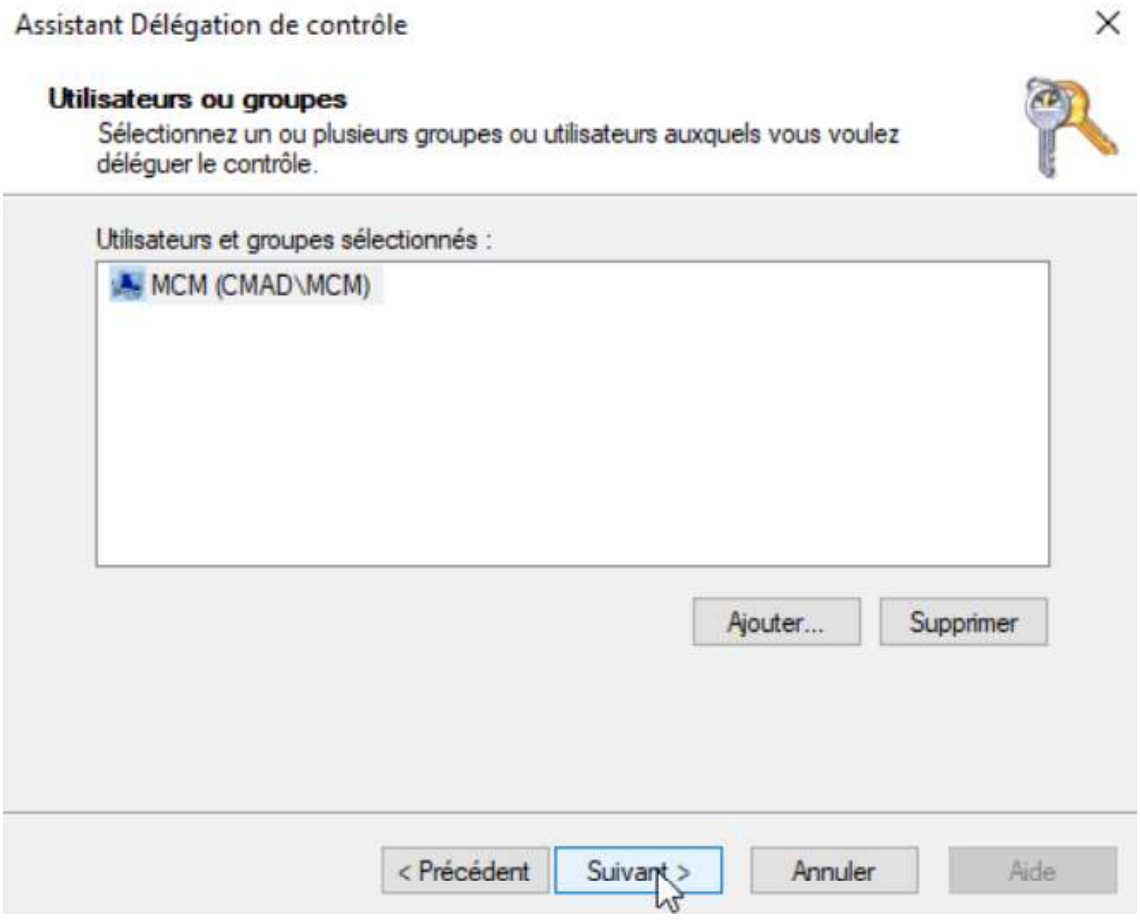
On lance l'installation et on voit que tout s'est parfaitement installé :



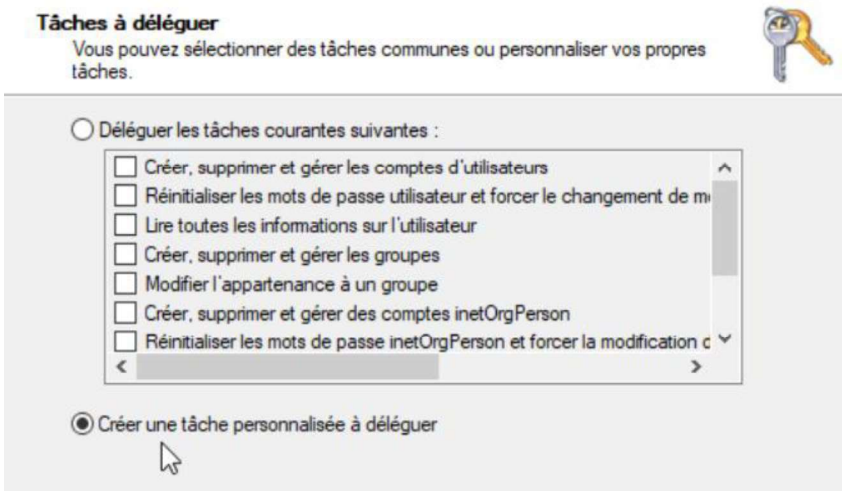
Sur le contrôleur de domaine, on se rend dans « Modification ADSI ». Clic droit, se connecter, on laisse tout par défaut et on se connecte. Par la suite on déroule et on vient à nouveau faire clic droit sur System, Nouveau > Objet > Container et on vient rentrer exactement « System Management ».



Dans « Utilisateurs et Ordinateurs Active Directory », sous « System » on fait une délégation de contrôle dans le dossier System Management que l'on vient d'ajouter. Dans l'assistant, on vient ajouter un objet auquel déléguer le contrôle et on choisit le serveur MCM.

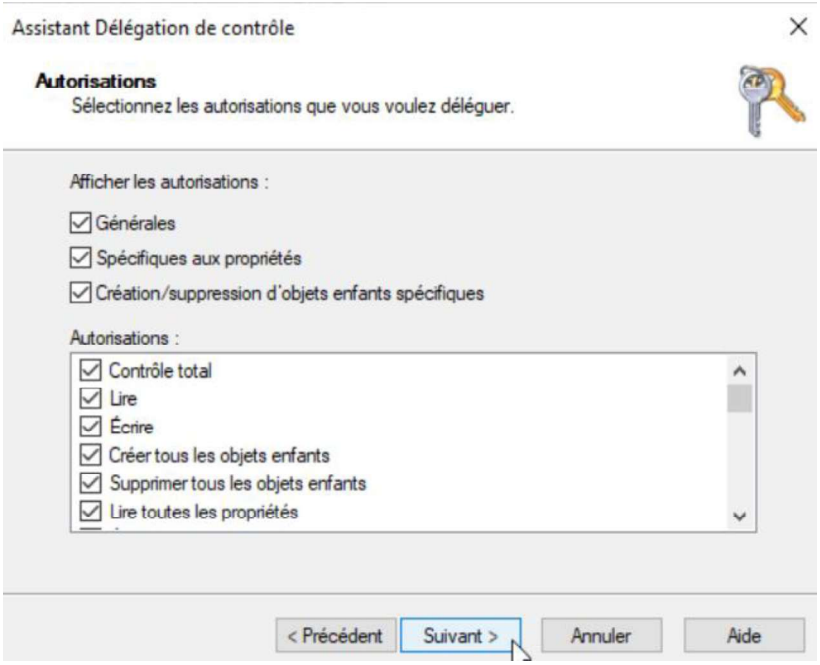


Ensuite on sélectionne « Créer une tâche personnalisée à déléguer ».

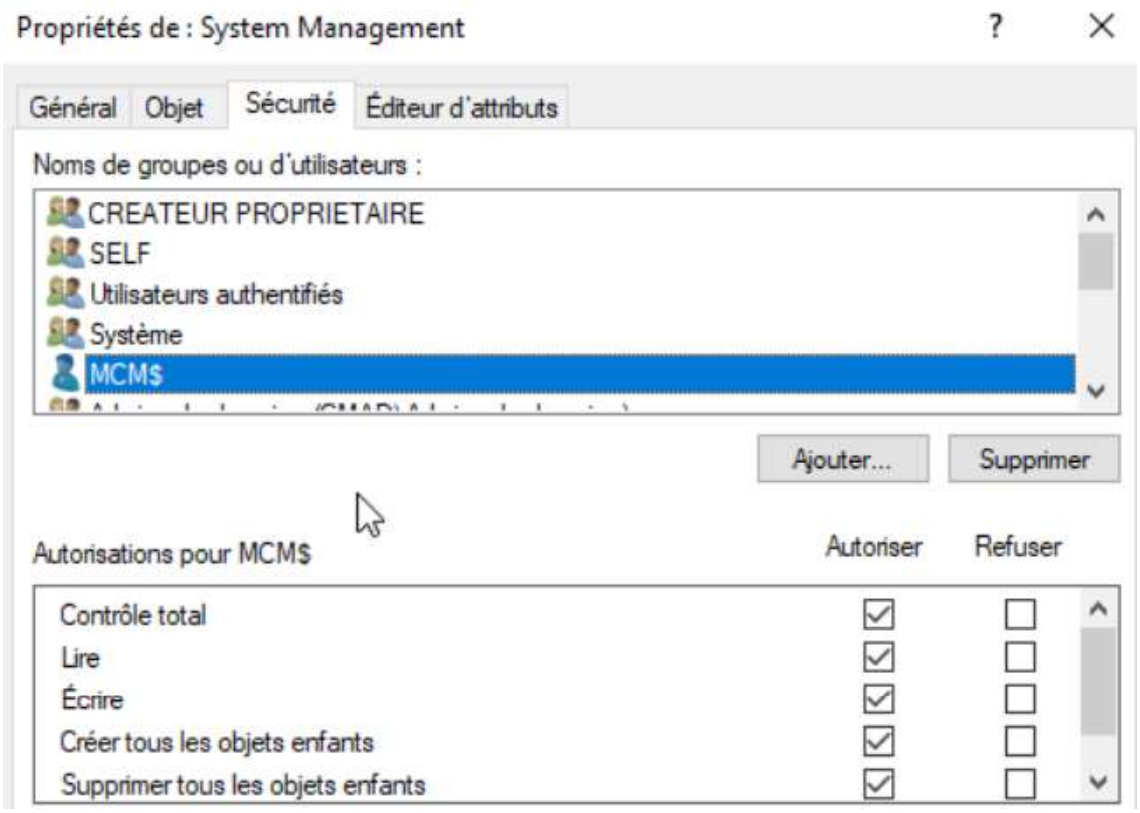


Ici on laisse par défaut.

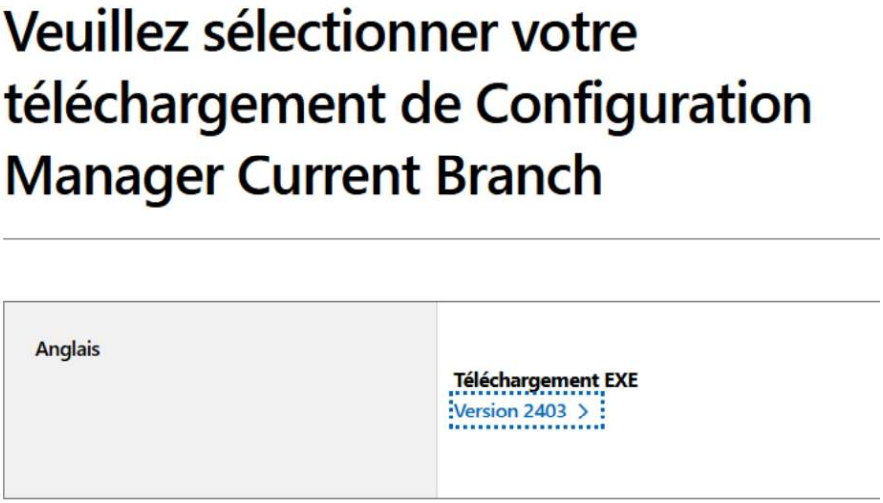
Et on vient cocher les trois premières et « Contrôle total » qui va cocher à son tour toutes les suivantes :



On peut vérifier dans les propriétés de « System Management » que MCM a bien les droits de contrôle total.



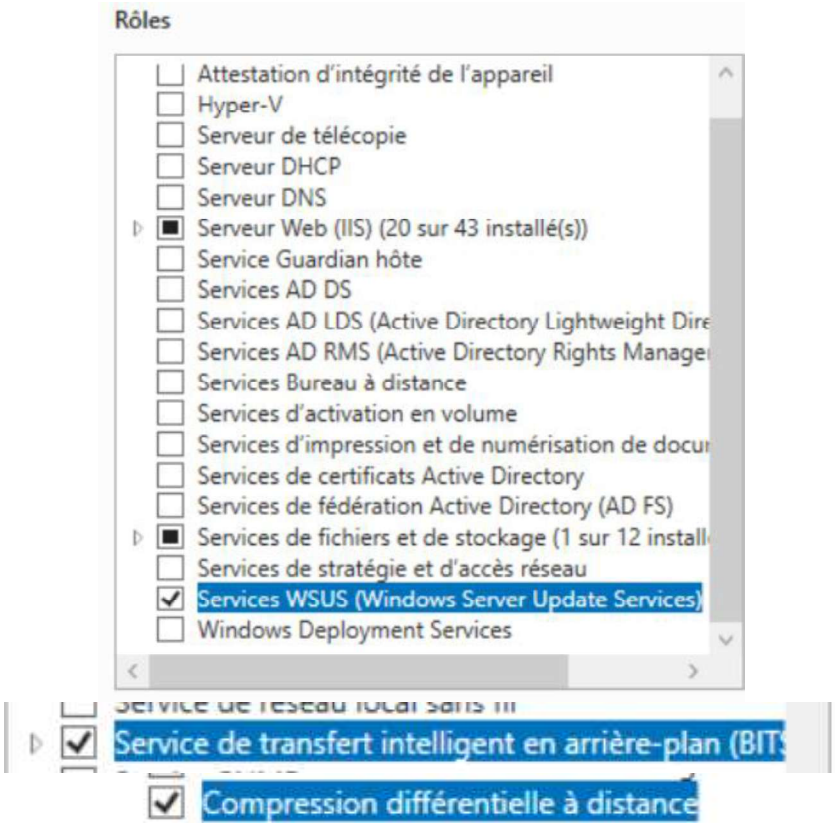
Maintenant, on vient étendre le schéma de notre Active Directory. On télécharge et on lance le .exe de la version actuelle de MCM ce qui va extraire un dossier cd.retail.LN qui contient les documents nécessaires.

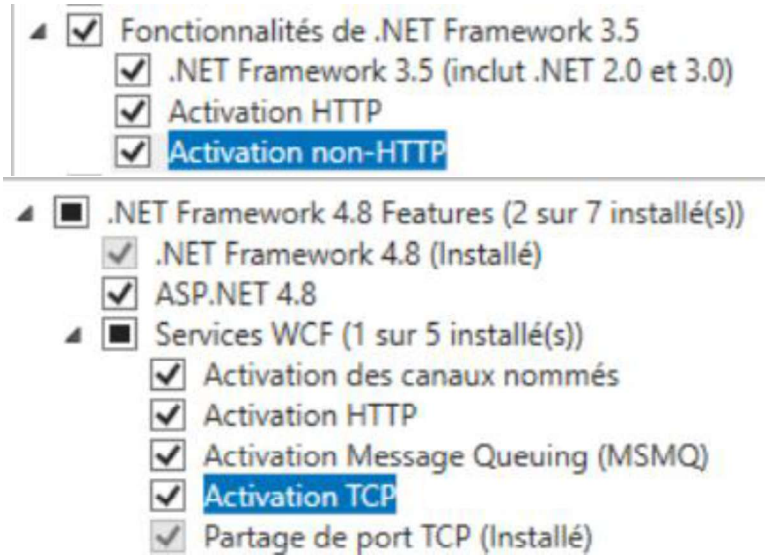


On exécute, dans l'invite de commandes, en tant qu'administrateur le fichier extadsch.exe qui signifie « Extended Active Directory Schema ». Ci-dessous on voit que l'opération s'est déroulée avec succès.

```
C:\Users\Administrateur>"C:\Users\Administrateur\Downloads\cd.retail.LN\SMSSETUP\BIN\X64\extadsch.exe"

Microsoft Microsoft Configuration Manager v5.00 (Build 9128)
Copyright (C) 2011 Microsoft Corp.


Successfully extended the Active Directory schema.
```

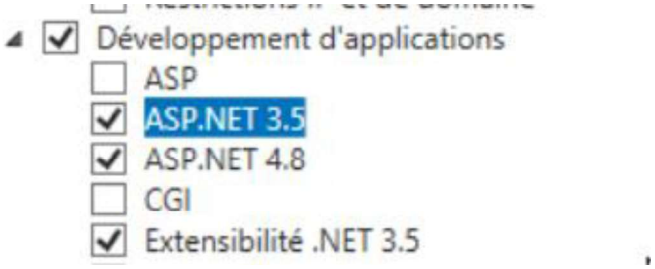
Sur le serveur MCM, on commence par télécharger et exécuter le Windows ADK et le module complémentaire Windows PE puis on vient ajouter le rôle de serveur WEB (IIS), WSUS ainsi que les fonctionnalités suivantes :



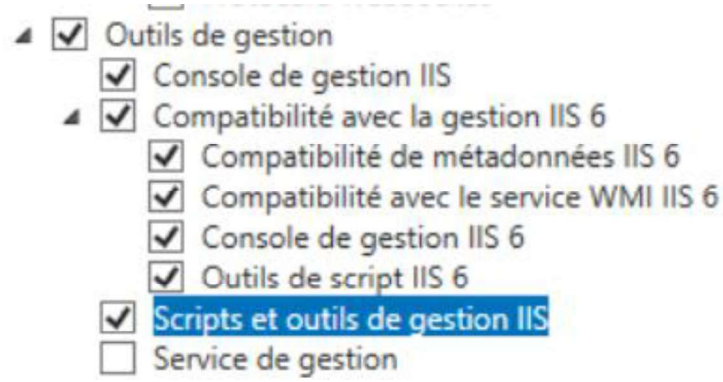


Ensuite dans les services de rôle :

ASP.NET 3.5 dans Développement d'applications

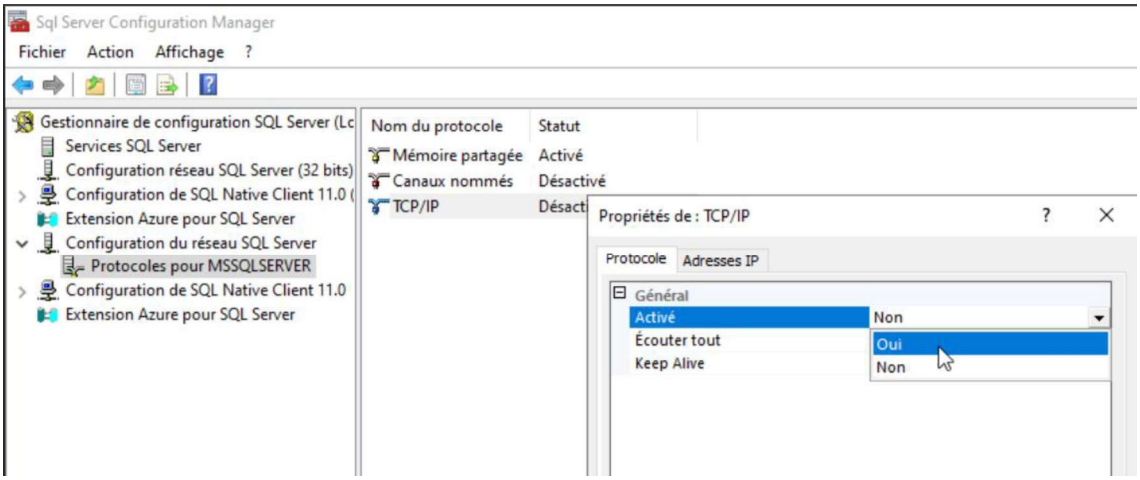


Dans « Outils de gestion » on vient cocher Scripts et outils de gestion IIS ainsi que Compatibilité avec la gestion IIS 6 et tout ce qu'il contient.

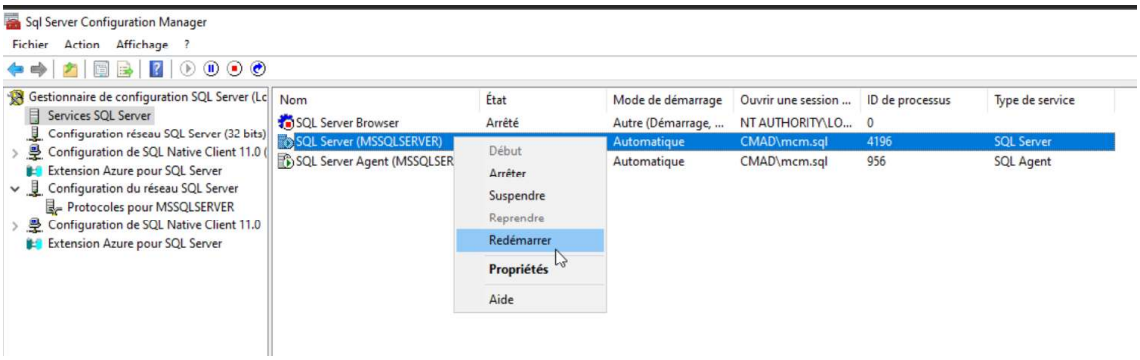


On remplace WID par SQL et on précise l'emplacement de stockage des mises à jour WSUS :

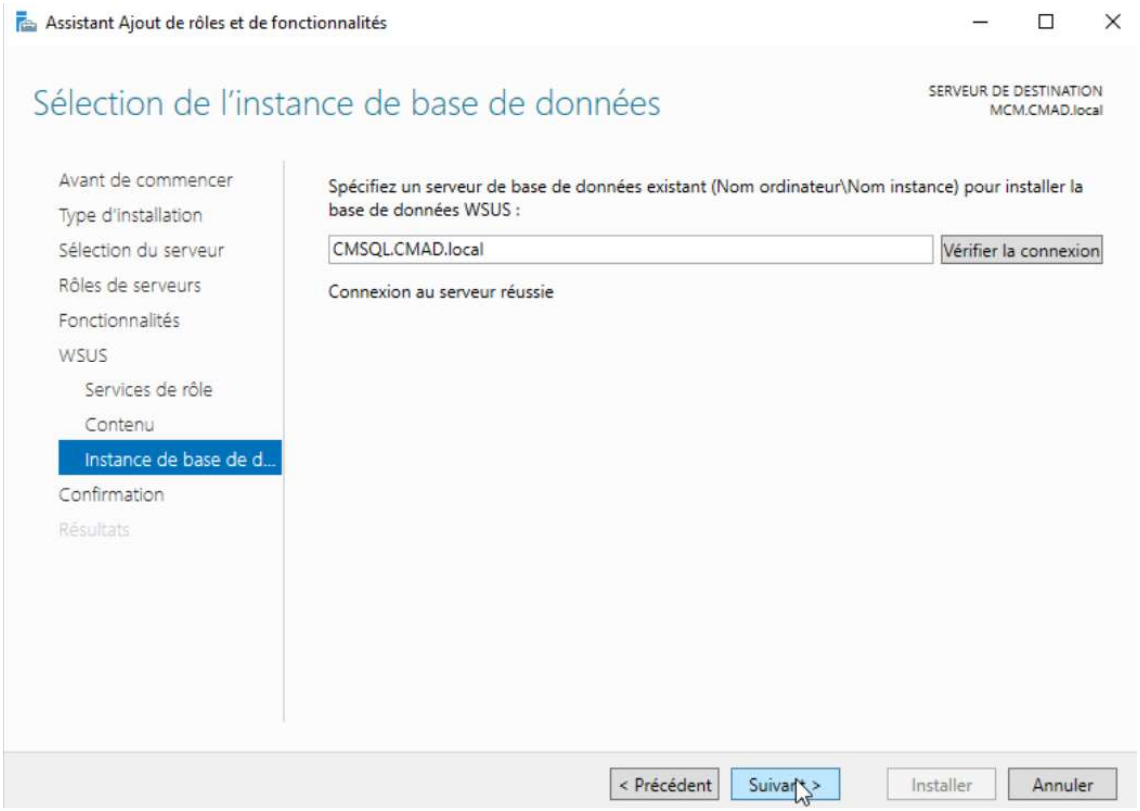
Sur le serveur SQL, on vient vérifier dans SQL Server Configuration Manager que dans les protocoles, TCP/IP soit bien activé, de même pour Canaux nommés au besoin.



Ensuite toujours dans le Gestionnaire de configuration du serveur SQL, dans les services, on vient redémarrer le serveur.



Ce qui nous permet donc d'indiquer le serveur SQL en tant qu'instance de base de données pour le rôle WSUS.



Une fois ces rôles installés, on clique sur lancer les tâches de post-installation et le rôle est installé.

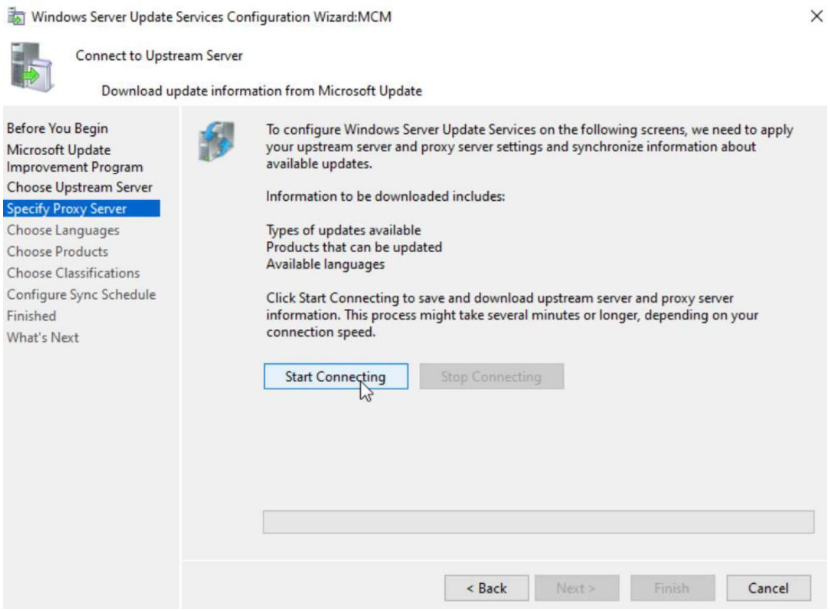
Après vérification dans la console, il m'était impossible de me connecter au serveur. J'ai donc vérifié si les rôles étaient bien installés et j'ai ensuite essayé de forcer à nouveau la post-installation. Celle-ci était en échec car il y avait déjà une partie de la base de données qui s'était installée sur le serveur SQL.

```
PS C:\Users\Administrateur.CMAD> Get-WindowsFeature -Name UpdateServices*

Display Name                                            Name                    Install State
------------                                            ----                    -------------
[X] Services WSUS (Windows Server Update Services)      UpdateServices              Installed
    [ ] WID Connectivity                                UpdateServices-WidDB        Available
    [X] WSUS Services                                   UpdateServices-Services     Installed
    [X] SQL Server Connectivity                         UpdateServices-DB           Installed
        [X] Outils des services WSUS (Windows Server... UpdateServices-RSAT         Installed
            [X] API et applets de commande PowerShell   UpdateServices-API          Installed
            [X] Console de gestion de l'interface ut... UpdateServices-UI           Installed


PS C:\Users\Administrateur.CMAD> Get-WsusServer
Get-WsusServer : Impossible de se connecter au serveur distant
Au caractère Ligne:1 : 1
+ Get-WsusServer
+ ~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidData : (Microsoft.Updat...usServerCommand:GetWsusServerCommand) [Get-WsusServer], WebException
    + FullyQualifiedErrorId : ServerIsInvalid,Microsoft.UpdateServices.Commands.GetWsusServerCommand

PS C:\Users\Administrateur.CMAD> & "C:\Program Files\Update Services\Tools\WsusUtil.exe" postinstall SQL_INSTANCE_NAME="CMSQL" CONTENT_DIR="W:\WSUS"
Le fichier journal est situé dans C:\Users\Administrateur.CMAD\AppData\Local\Temp\\WSUS_PostInstall_20250401T181830.log
Démarrage de la post-installation
Erreur irrécupérable : La version du schéma de la base de données provient d'une version de WSUS
plus récente que celle qui est installée. Appliquez un correctif logiciel à votre serveur WSUS au moins jusqu'à
cette version ou supprimez la base de données.
```

J'ai donc supprimé la base SUSDB sur le serveur SQL ainsi que ses connections actives et j'ai relancé la commande. Comme on peut le voir tout s'est bien déroulé et j'ai désormais accès au Wizard de la console WSUS.

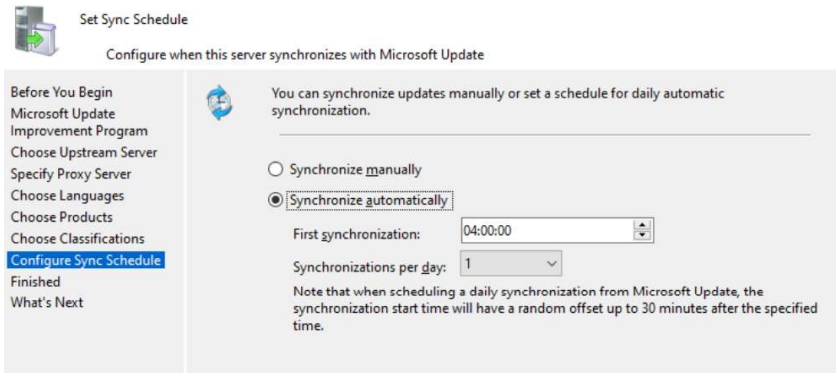
```
PS C:\Users\Administrateur.CMAD> & "C:\Program Files\Update Services\Tools\WsusUtil.exe" postinstall SQL_INSTANCE_NAME="CMSQL" CONTENT_DIR="W:\WSUS"
Le fichier journal est situé dans C:\Users\Administrateur.CMAD\AppData\Local\Temp\\WSUS_PostInstall_20250401T183146.log
Démarrage de la post-installation
La post-installation s'est correctement terminée
PS C:\Users\Administrateur.CMAD> Get-WsusServer

Name : MCM

PS C:\Users\Administrateur.CMAD>
```

Pour le wizard on laisse tout par défaut jusqu'à la connexion aux serveurs Windows Update.

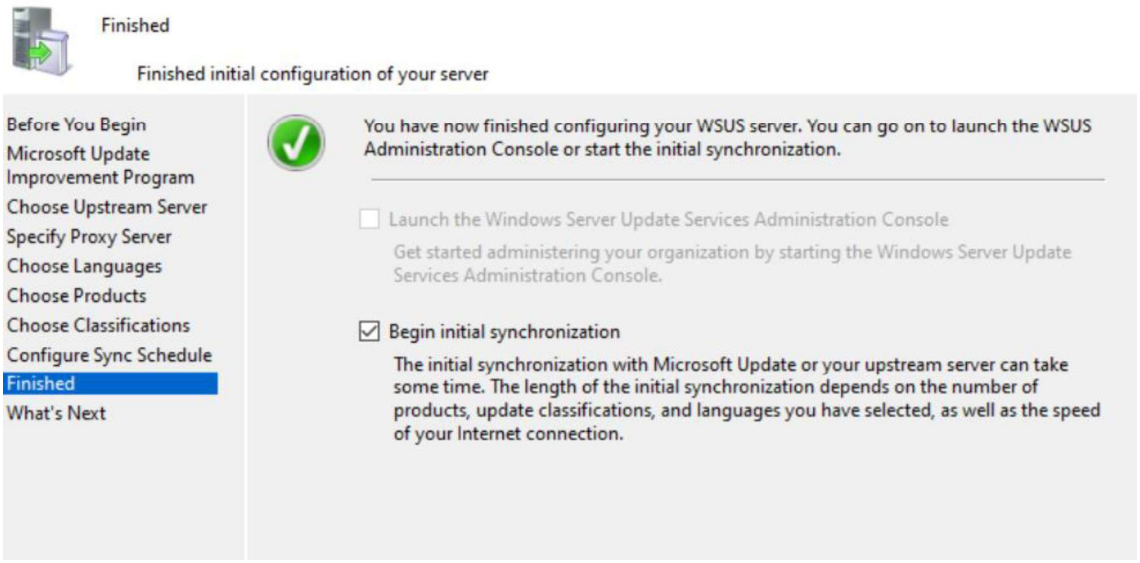


Une fois terminée, on sélectionne les produits qui nous intéressent. En l'occurrence dans notre cas ce seront les produits liés à Windows 10, 11, Server 2019 ainsi que SQL Server 2022, SSMS v20.

Ensuite on vient activer la synchronisation automatique à 4h du matin.



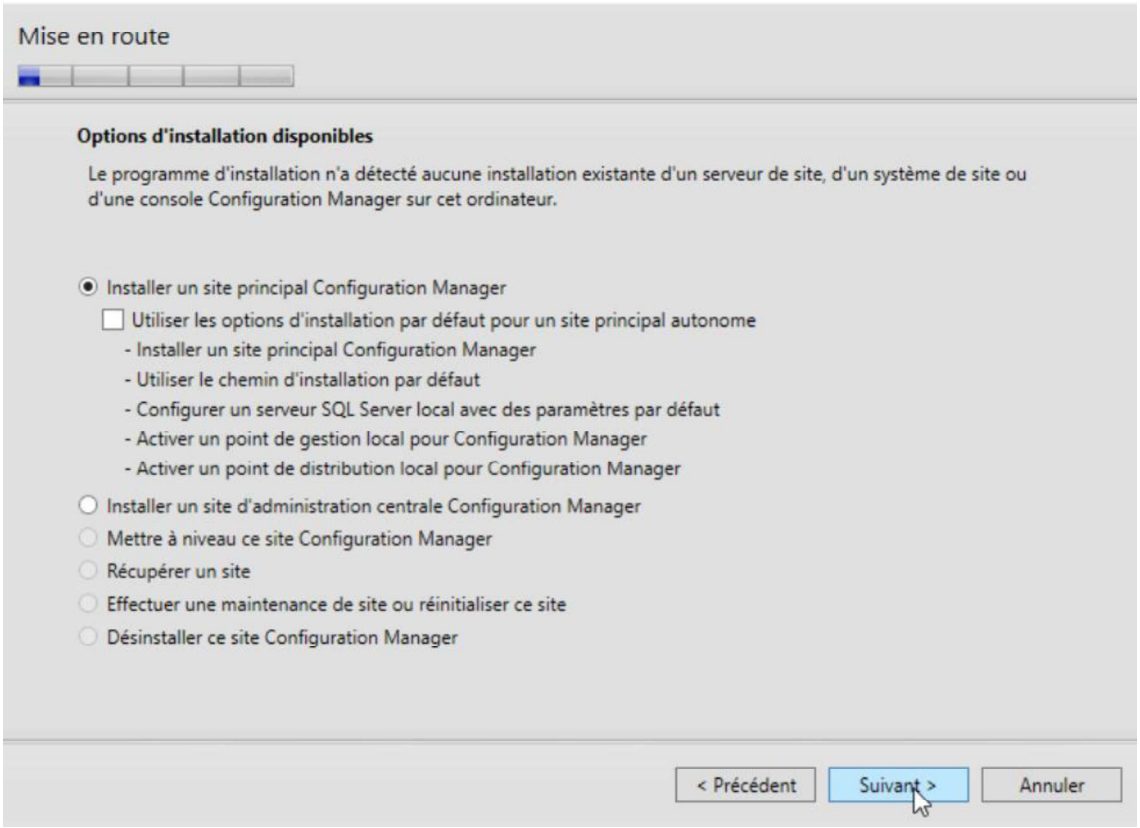
Et on effectue la première synchronisation :



1.3/ Installation de MCM

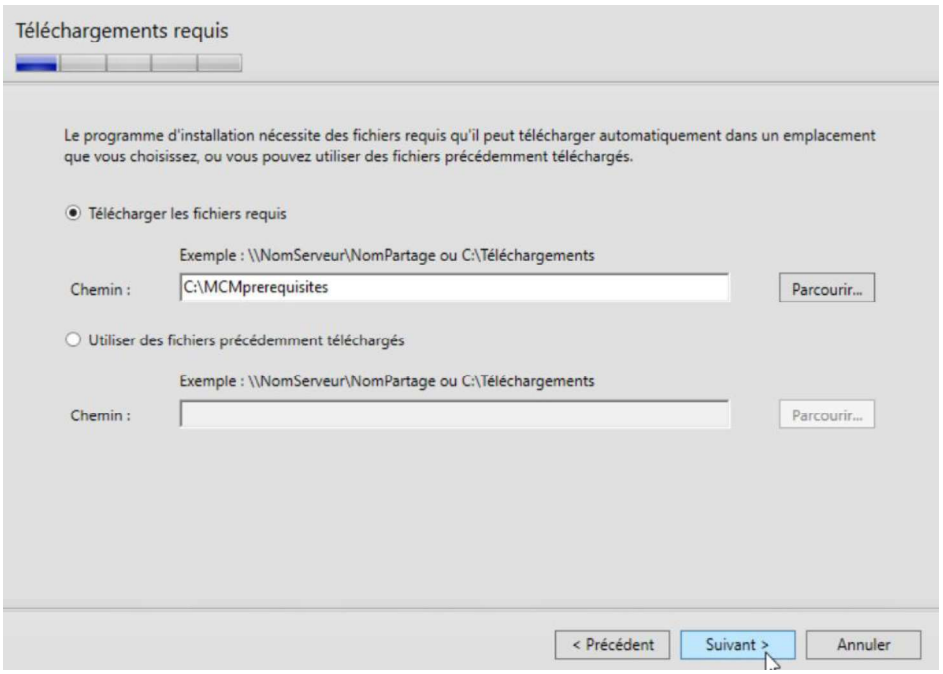
Dans un premier temps il nous faut installer les deux composants ci-dessous. D'abord VC_redist.x64.exe nécessaire pour installer msodbcsql.msi.

On peut donc commencer l'installation de MCM tranquillement. On choisit d'abord « Installer un site principal ».

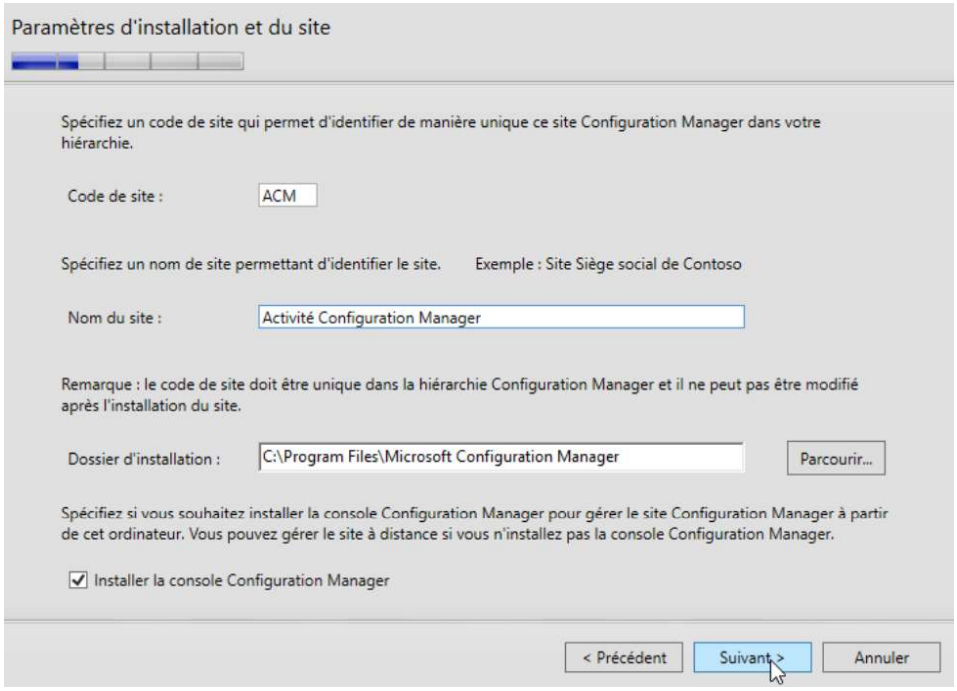


Installer la version d'évaluation car comme pour SQL, je n'ai pas de licence.

On vient ensuite choisir le dossier pour installer les fichiers. Dans mon cas j'ai créé un dossier MCMprerequisites dans le C. On effectue le téléchargement.

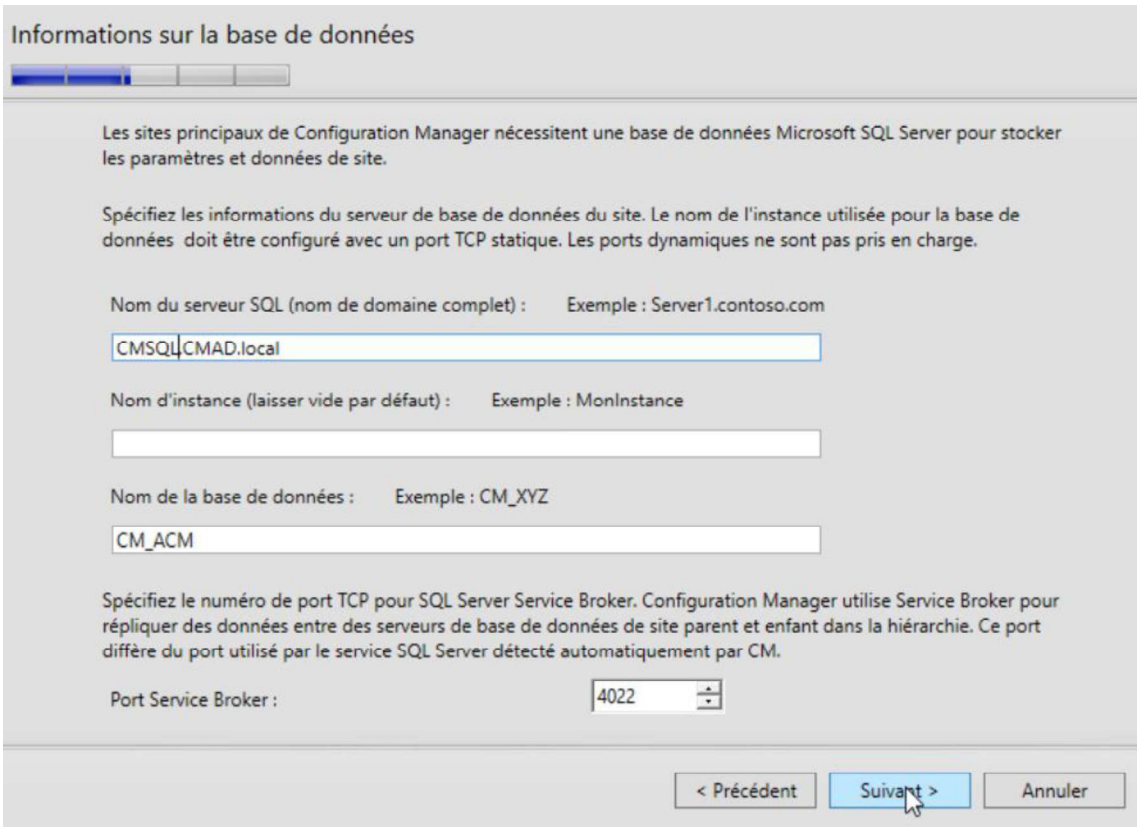


On précise le code de site ainsi que son nom.

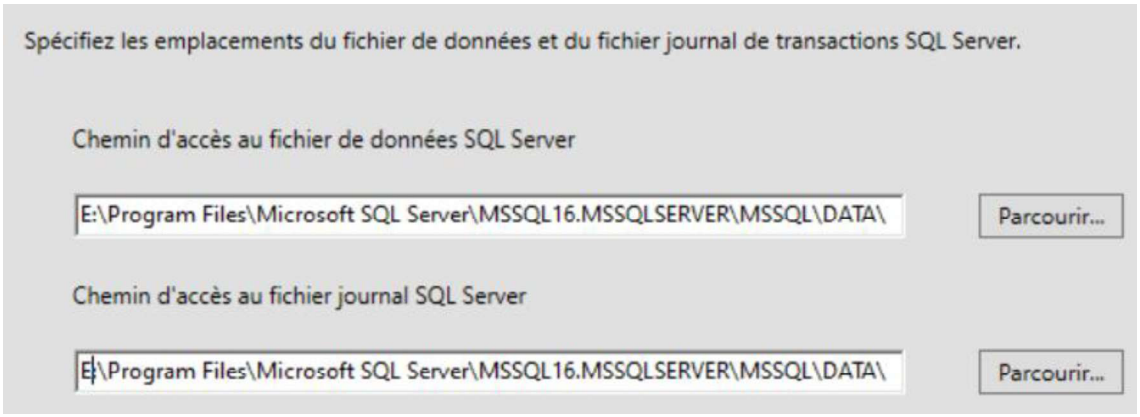


On choisit « Installer le site principal en tant que site autonome » car dans notre infrastructure il n'y a pas d'autre site.

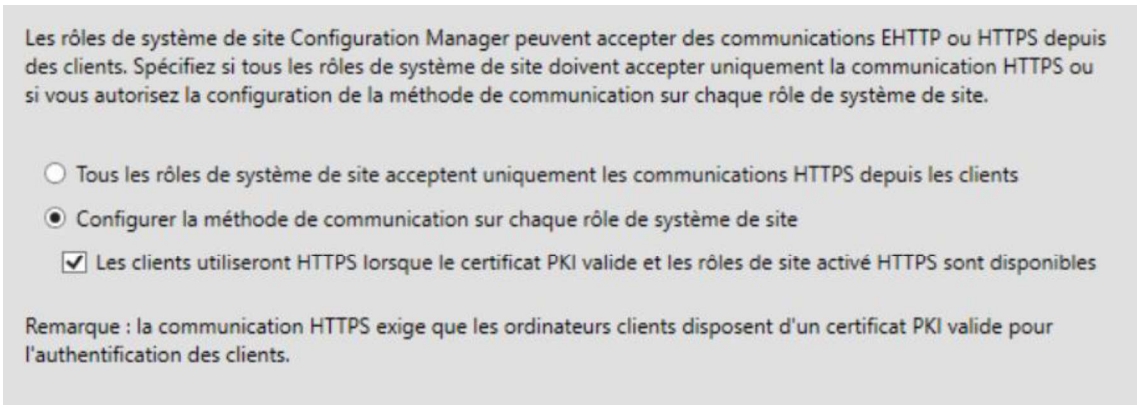
On modifie le nom du serveur SQL pour qu'il corresponde à celui que l'on a créé séparément.



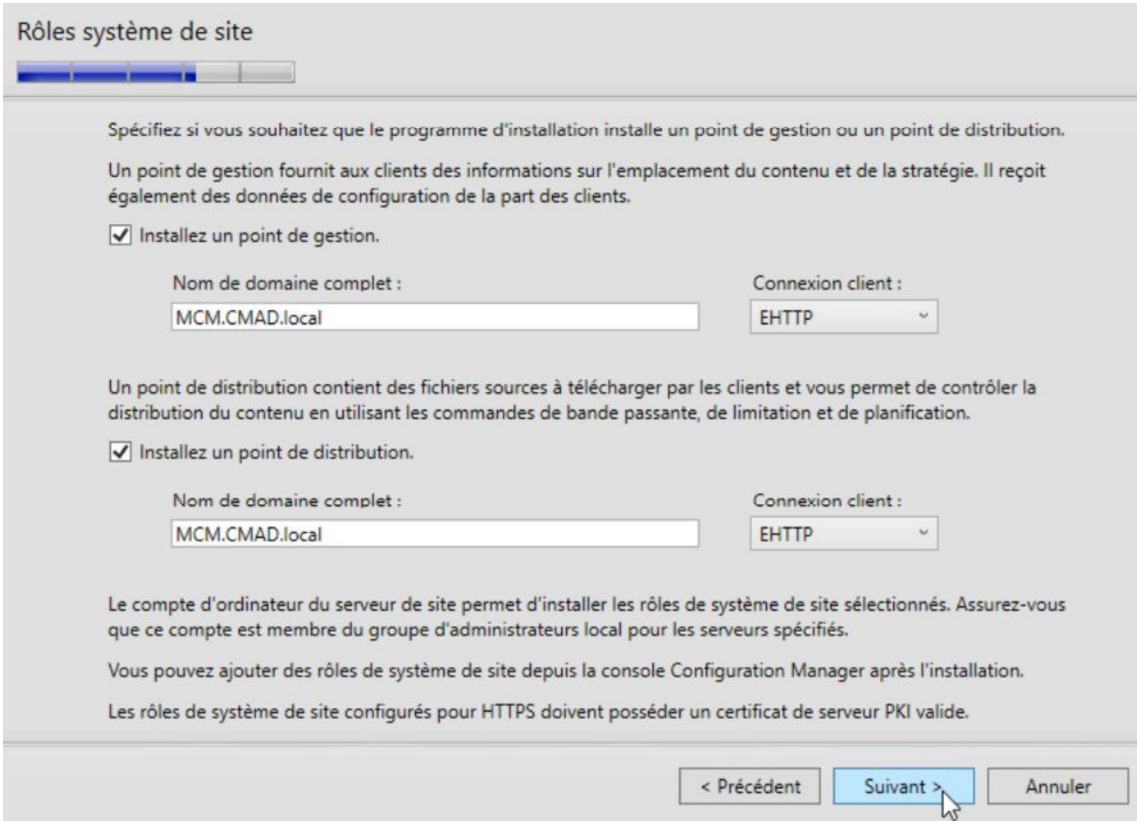
Les chemins d'accès ont bien été détectés.



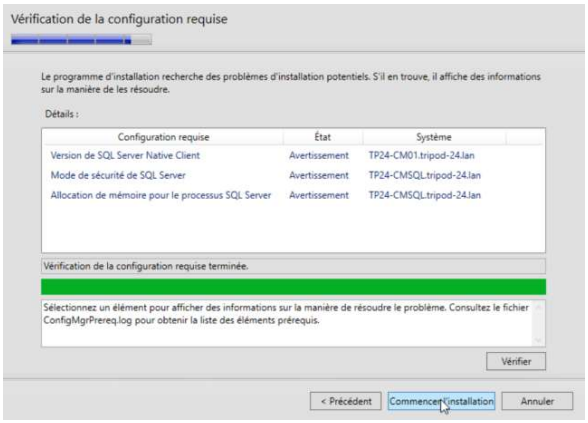
On laisse la page d'après par défaut puis on vient modifier les paramètres de communication comme tels.



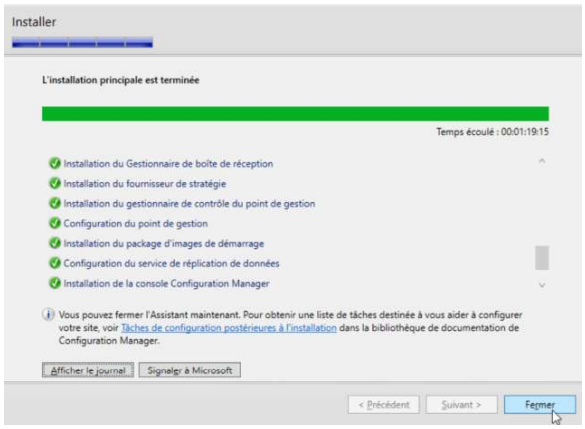
Pour le point de gestion et le point de distribution, on laisse par défaut on vient juste préciser le type de connexion en EHTTP.



Une vérification se lance et on peut enfin commencer l'installation de MCM.



Et une fois terminée cela donne :



L'installation est désormais complète. On accède à la console. Pour une utilisation au sein d'une entreprise, il faudrait paramétrer le site et ajouter du contenu pour les séquences de tâches, les mises à jour etc…

2/ L'utilisation de MCM par le SDK

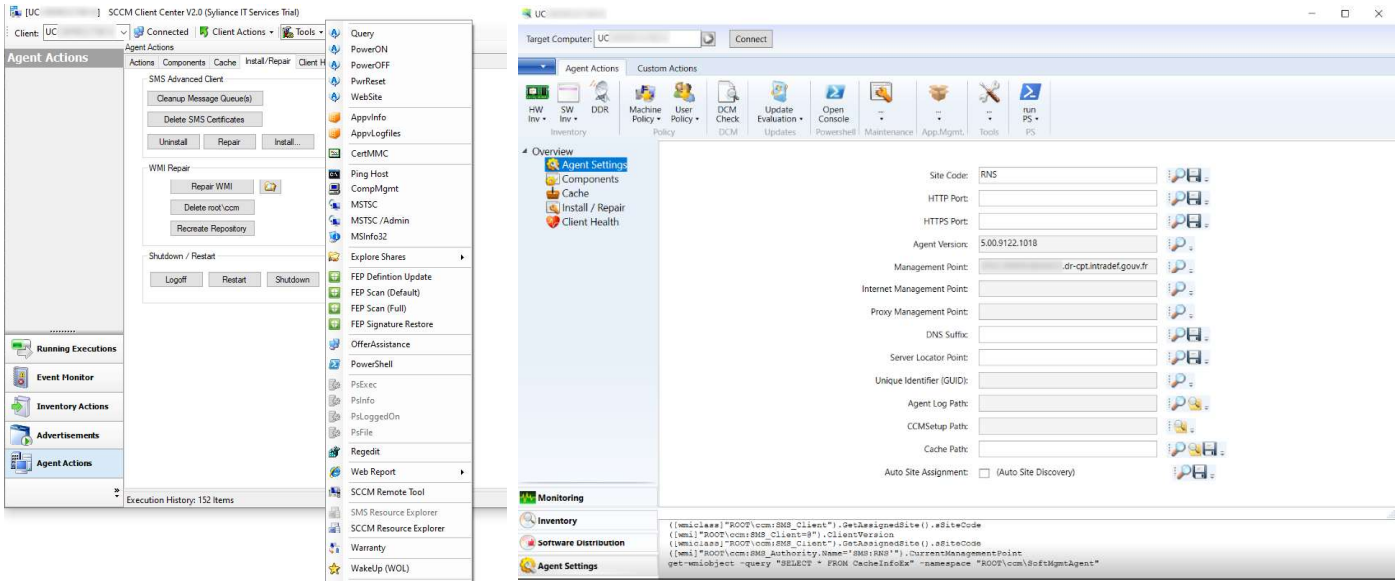
Pour Intradef, MECM représente 593 serveurs répartis entre :

- 1 CAS (Central Administration Site)
- 1 WSUS (Windows Server Update Services)
- 4 Sites principaux (Paris, Rennes, Metz, Toulon)
- 15 Serveurs SQL pour les bases de données
- 572 Points de distribution sur les serveurs de proximité.

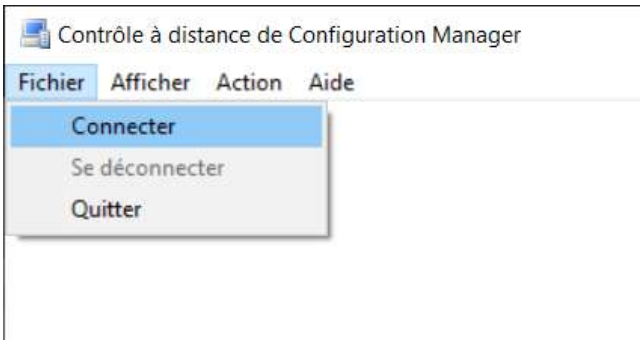
Au Front Office du SDK, nous utilisons MCM et ses utilitaires pour deux raisons principales : l'administration à distance des postes et l'installation de logiciels.

2.1/ L'administration à distance

Avec MCM et son client présent sur les postes Intradef, l'administration à distance est concentrée mais complète.
Tout d'abord, le client remonte beaucoup d'informations que l'on retrouve dans les « Client Center », outils pour l'administration des clients MCM.
A gauche, l'ancien Client Center, on voit sur l'image les différents outils et les actions à distance qui peuvent être effectuées sur les postes. Ces dernières nous permettent d'effectuer des vérifications, d'ajouter des fichiers ou réaliser des actions directement sur le client. A droite la plus récente que l'on ait, celle-ci permet quelques actions différentes mais nous permet surtout la désinstallation de logiciels sans passer par une séquence de tâches de désinstallation.



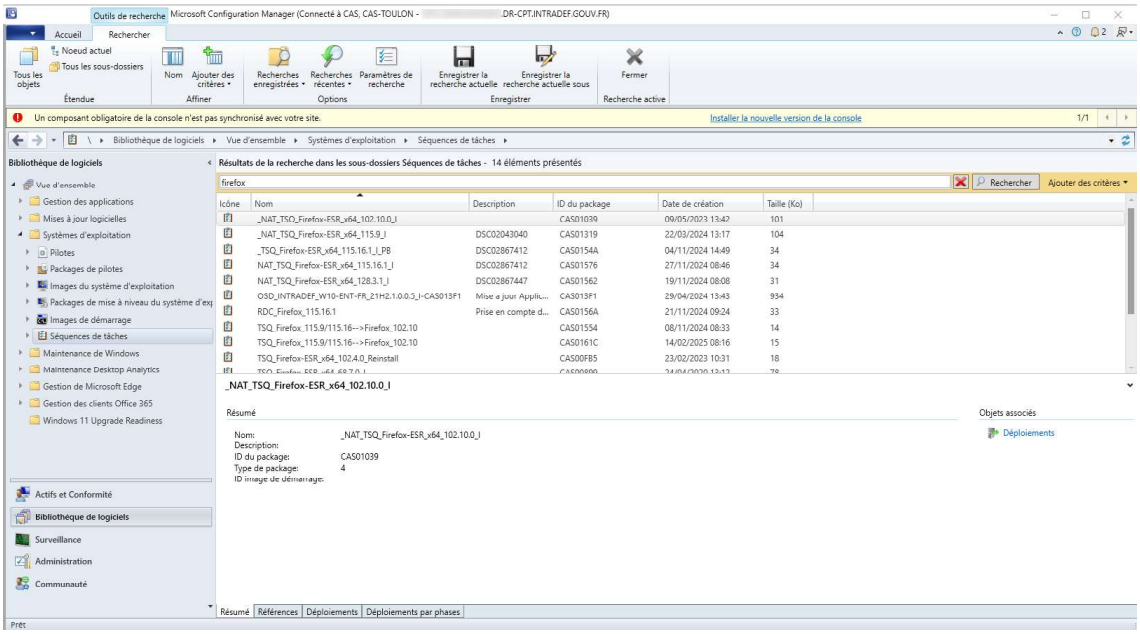
De plus, MCM permet la prise en main à distance grâce au « Contrôle à distance de Configuration Manager ».



A la grande différence du Remote Desktop Protocol de Windows, il nous permet de nous connecter à distance sur la session de l'utilisateur tout en le laissant connecté. On se retrouve donc à partager la main avec l'utilisateur. Cela nous permet notamment de pouvoir lui demander de nous montrer en direct le problème rencontré et de garder une certaine transparence sur les actions effectuées car il continue de voir l'action en cours sur le poste. L'inconvénient du contrôle à distance de configuration manager est sa consommation de ressources. L'utilitaire est assez gourmand pour le poste client mais permet de ne pas avoir à passer par un logiciel tiers.

2.2/ Déploiement de logiciels

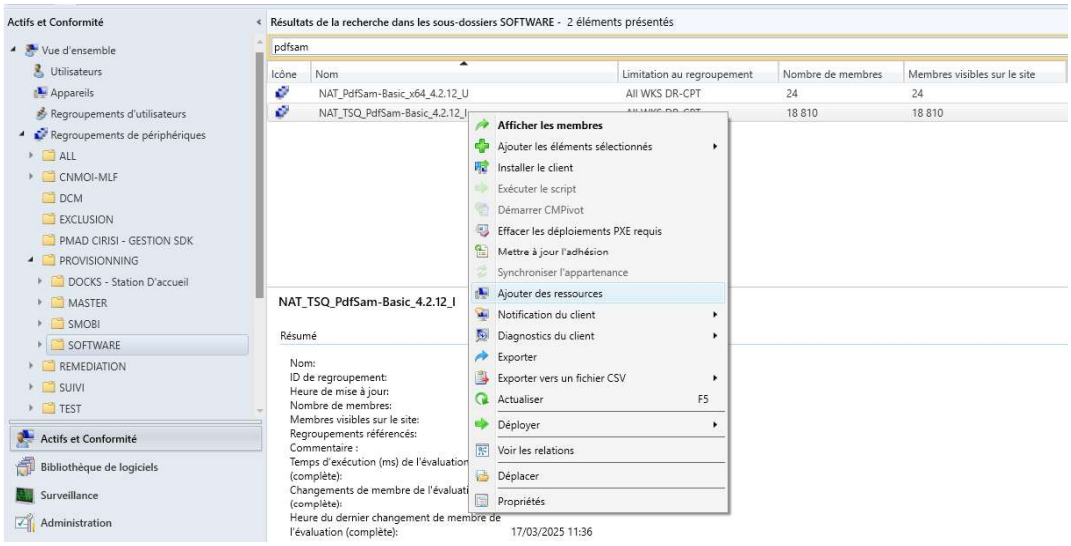
Les installations que nous faisons via MCM passent en grande majorité par des packages déployés via des séquences de tâches renseignées sur les serveurs MCM. On peut accéder à la liste des logiciels et des séquences de tâches disponibles grâce la Console MCM.

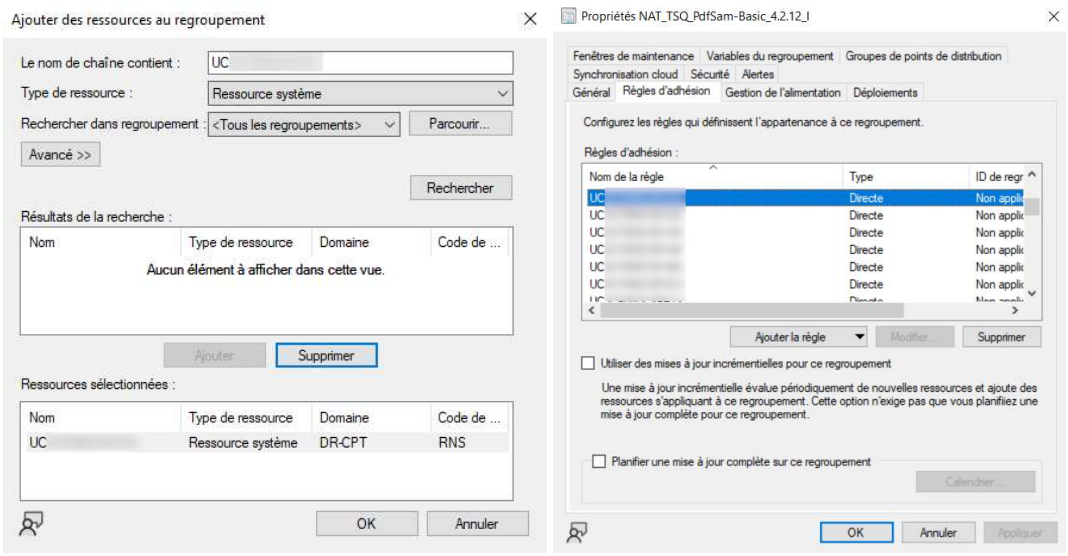


Le package contenant les fichiers de la séquence de tâches est mis en place sur les points de distribution dès sa création par le CNCI.
Pour installer un logiciel sur un poste il y a deux manières de faire :

- Directement sur la console MCM
- En utilisant le site sharepoint appelé PSAUM

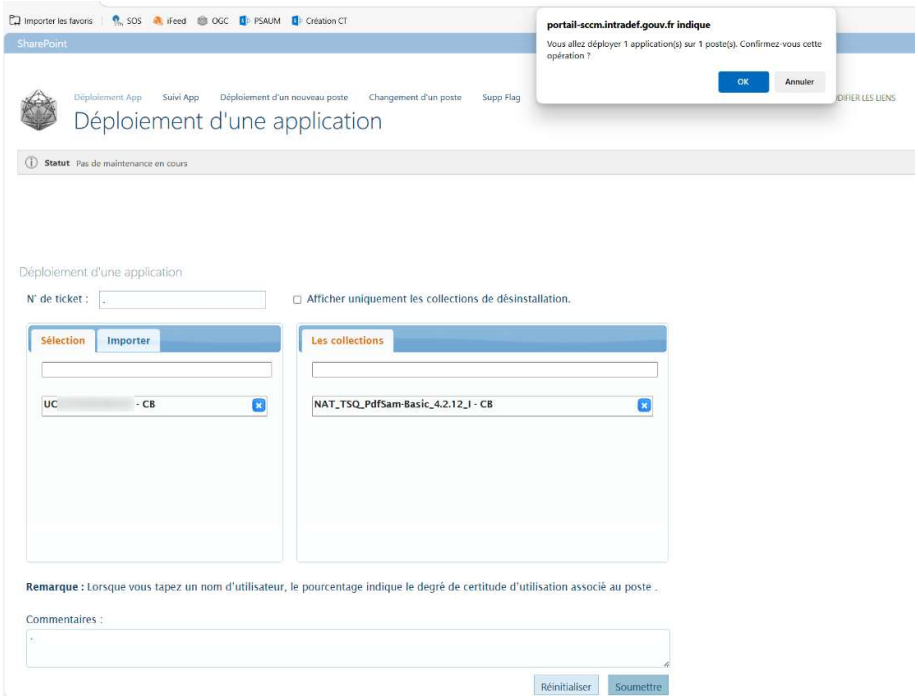
Via la console MCM, il faut aller sur le logiciel souhaité, sélectionner « Ajouter des ressources » puis indiquer le nom d'UC du poste souhaité :



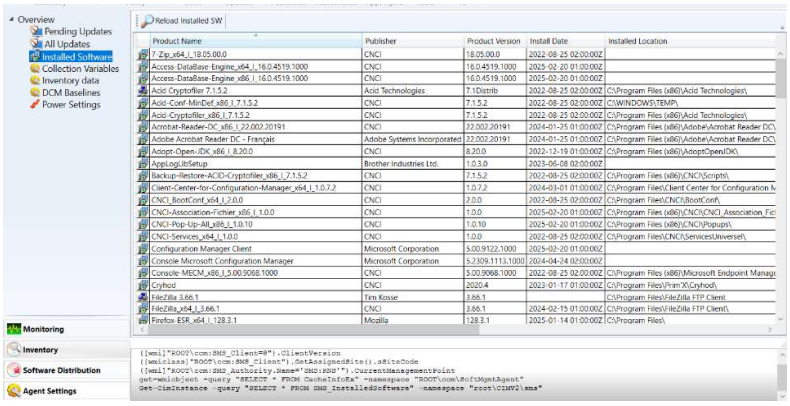


Sur la troisième photo, on voit les règles d'adhésion et la ressource ajoutée sur la photo précédente se trouve désormais dans ces règles d'adhésion et va bientôt recevoir la séquence de tâches NAT_TSQ_PdfSam-Basic…

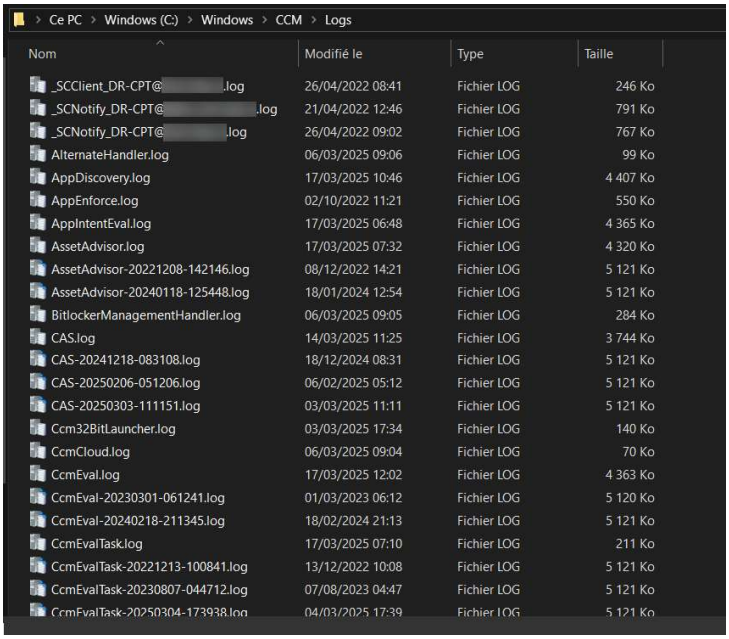
Via le site Sharepoint « PSAUM » c'est un peu plus rapide pour le technicien car il y a un « moteur de recherche » pour les logiciels et nous permet également de sélectionner plusieurs postes et logiciels différents en une fois.



Lorsque le technicien envoie la demande sur PSAUM, le serveur de site (1 des 4 principaux) va informer le serveur de proximité faisant office de point de gestion de la conduite à tenir (nom du poste et package souhaités).
Ensuite, l'agent Client Center présent sur tous les postes du Ministère effectue une vérification plusieurs fois par heure (peut être forcé via le Client Center) pour savoir s'il est concerné par une action.
A la suite de cette vérification, le point de gestion (MP – Management Point) informe le poste qu'il doit aller récupérer les fichiers de la séquence de tâches auprès du point de distribution (DP – Distribution Point) défini.
Le package est ensuite téléchargé par le poste depuis le DP puis est ensuite exécuté.
L'agent Client Center fait par la suite un compte rendu au MP.
Le technicien peut vérifier que tout s'est bien installé depuis les Client Center :



Ou en allant vérifier les logs du Client Center Manager (CCMlogs).



D'autres tâches de déploiement se passent par MCM et PSAUM comme la masterisation de postes et l'installation de serveurs mais ne sont pas effectuées par le SDK de Rennes.

Activité 3 – Solution de Mobilité d'Intradef

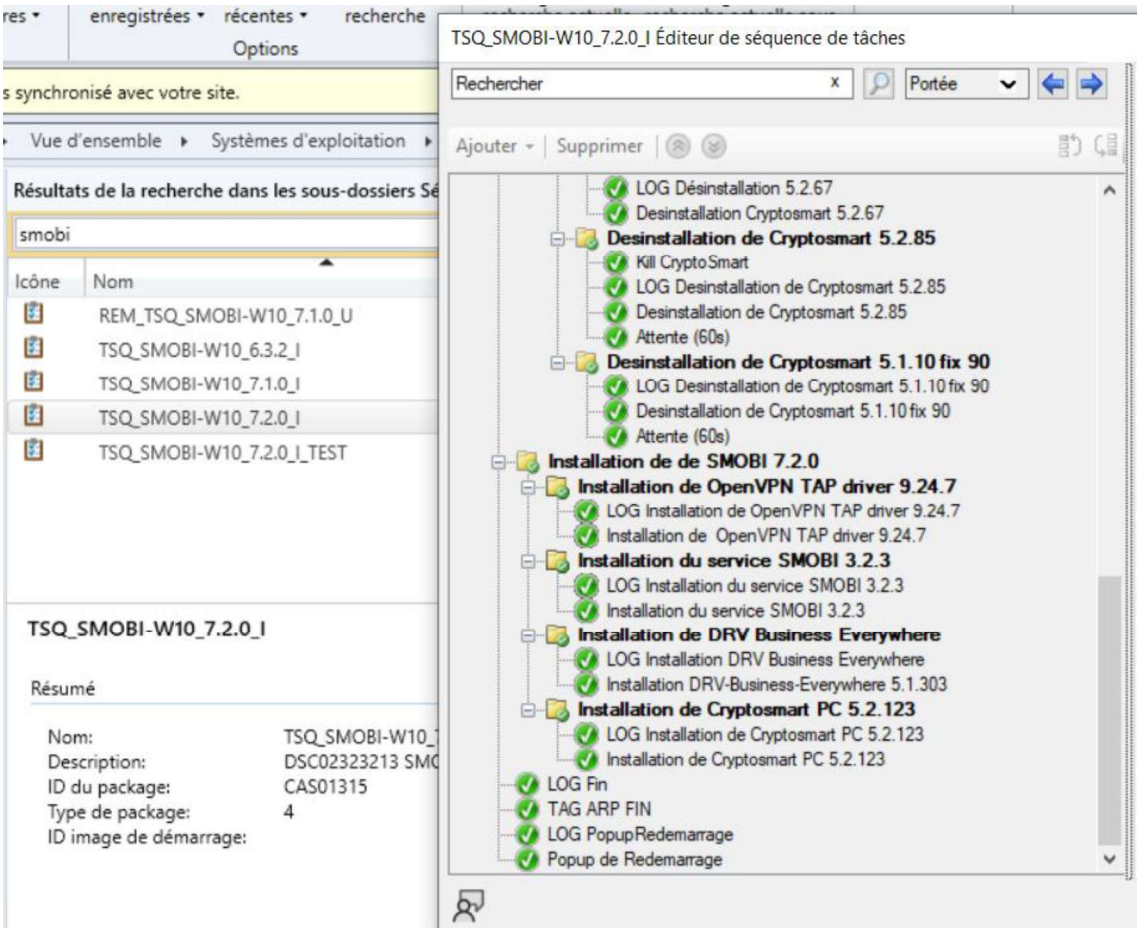
La Solution de MOBilité de l'Intradef ou SMOBI est une solution mise en place pour permettre aux usagers du Ministère d'accéder aux services disponibles sur Intradef en dehors des infrastructures du Ministère. Cette solution principalement utilisée pour effectuer du télétravail, se retrouve sur des ordinateurs et des téléphones portables.

1/ Mise en place du service

La mise en place du service se fait à distance, parfois avant l'utilisation par les usagers lorsque les CIRISI (Centre Interarmées des Réseaux d'Infrastructures et des Systèmes d'Information) réinitialisent ou initialisent l'ordinateur portable et effectuent une demande DIADEME à destination du SDK pour une installation des services SMOBI.

1.1/ Déploiement via PSAUM/MCM

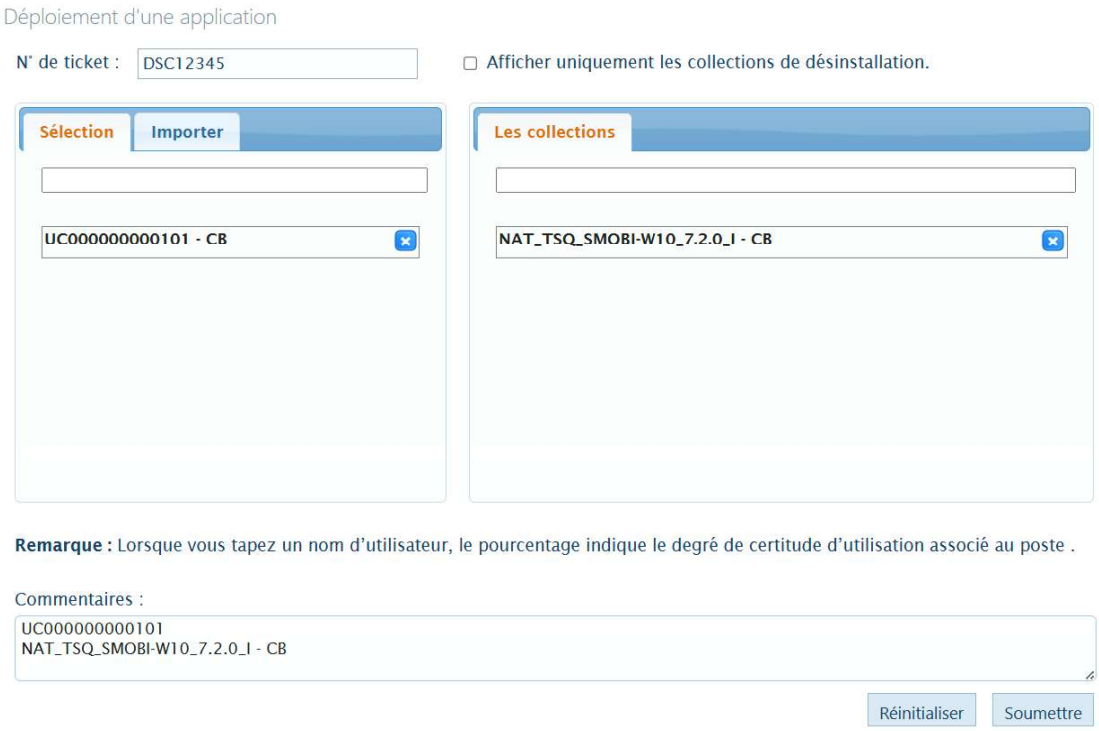
Pour l'installation des services, le SDK déploie via PSAUM une séquence de tâches. Cette séquence contient plusieurs logiciels et drivers : le service SMOBI, Cryptosmart, OpenVPN TAP et Business everywhere.



Cryhod permet le chiffrement du poste. Il est présent de base sur tous les postes du Ministère mais intervient dès le démarrage pour les postes SMOBI.

Cryptosmart est le client et avec le driver OpenVPN TAP ils permettent d'établir la connexion au VPN d'Intradef. Cryptosmart permet également la vérification du token et du PIN rentré par l'utilisateur.
Le driver Business Everywhere permet d'utiliser le réseau cellulaire pour se connecter au VPN.

Lors de la réception du ticket DIADEME, le technicien récupère le numéro d'UC qui s'écrit « UC+Adresse MAC ». Ce numéro est renseigné dans la base de données MCM et dans les ordinateurs de l'AD. Il nous permet donc d'identifier le poste correspondant. Une étape de vérification est d'abord effectuée : le technicien vérifie que le poste est bien un ordinateur portable, qu'il ne se trouve pas dans les groupes Active Directory liés à SMOBI et qu'il ne possède pas déjà l'installation. Si tout est bon, on le désigne ensuite dans PSAUM avec la séquence de tâches souhaitée qui est nommée « TSQ_SMOBI_n°Version » sur les serveurs MCM.



1.2/ Utilisation de l'Active Directory

Les groupes Active Directory sont utilisés pour uniformiser ou spécifier mais surtout pour simplifier la gestion des utilisateurs et des ordinateurs du domaine.

Les GPO définissent les paramètres de sécurité, y compris les politiques de mots de passe, les restrictions d'accès et les configurations de sécurité du système. Cela garantit que tous les postes accédant au réseau via le VPN respectent les normes de sécurité qui sont mises en place habituellement pour les postes dans les bâtiments du Ministère.

En intégrant les postes dans deux groupes AD précis, nous pouvons appliquer des GPO spécifiques qui vont permettre aux postes SMOBI de fonctionner correctement à distance et en toute sécurité.

Une des GPO attribuées configure l'utilisation de Cryhod, logiciel choisi pour le chiffrement du disque des postes. Ce dernier est essentiel pour protéger les données sensibles et/ou une utilisation frauduleuse du poste en cas de perte ou de vol.

Parmi les modifications apportées par les GPO, certaines concernent des paramètres spécifiques de l'éditeur de registre. Notamment, un des paramètres informe le poste de la passerelle correspondant à celle utilisée par les postes en mobilité. Ce paramètre est indispensable car les serveurs reliés aux bâtiments ne sont accessibles que par les postes présents dans les bâtiments ou par ces serveurs de mobilité pour assurer la sécurité des échanges de données.

1.3/ Fin de l'installation et chiffrement

Pour résumer, l'installation par le technicien se fait tout d'abord en vérifiant si le poste est présent ou non dans les groupes AD. Si le poste est présent, il faut impérativement l'en retirer avant l'installation du package car les GPO pourraient bloquer le poste et empêcher son démarrage car il attend que la couche CRYHOD soit passée mais celle-ci n'a pas encore été installée. Ensuite, l'installation via PSAUM/MECM se fait rapidement et pour finir il y a le rajout des groupes AD.

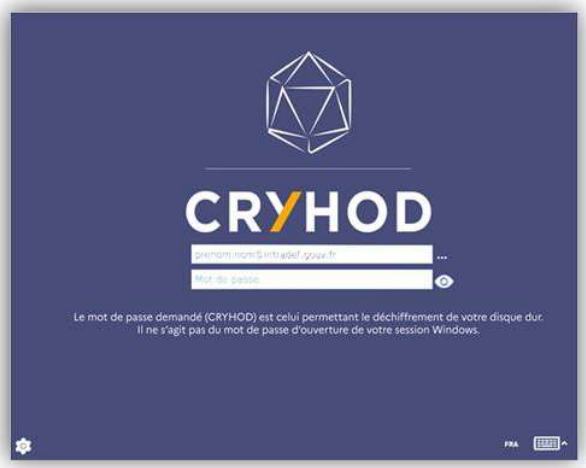
Après l'ajout des groupes, le poste doit être chiffré, pour cela, il faut accéder au centre de chiffrement, utilitaire présent en partie sur tous les postes mais activé avec l'installation de SMOBI. Dans cet utilitaire, il va falloir chiffrer le disque en se connectant avec l'identifiant de la forme UID + domaine, soit william.troude@intradef.gouv.fr dans mon cas et avec un mot de passe différent de celui du compte Active Directory. Par la suite, il sera demandé par le centre de chiffrement de redémarrer à plusieurs reprises pour valider les politiques CRYHOD au démarrage et faire passer CRYHOD en premier sur la séquence de boot afin d'arriver sur la page de connexion dès l'allumage du PC. Il peut nous arriver de prendre la main à distance après l'ajout des groupes AD sur le poste pour aider l'utilisateur à effectuer les différentes étapes de chiffrement.

2/ Utilisation du service SMOBI

Depuis la crise du COVID, l'utilisation du service SMOBI n'a fait qu'augmenter. De plus en plus de personnes ont la possibilité d'effectuer du télétravail, et des postes SMOBI sont même déployés pour des personnels uniquement en présentiel en prévention d'une nouvelle éventuelle crise nécessitant une bascule rapide et efficace vers un télétravail important. Ainsi, le service est de plus en plus présent et il est important, en tant que technicien, de comprendre son fonctionnement et d'apprendre à utiliser le côté « client ».

2.1/ Déchiffrement du poste

Tous les postes SMOBI sont chiffrés avec la solution CRYHOD. Cela protège en cas de vol ou de tentative d'intrusion. Les disques sont chiffrés par CRYHOD et ne sont accessibles qu'après une connexion réussie.
L'utilisateur doit donc déverrouiller cette première partie à l'aide de leur adresse Intradef et du mot de passe défini spécifiquement pour CRYHOD. Il aura été nécessaire qu'un administrateur ou une personne ayant déjà un compte CRYHOD déverrouille le poste pour que les données de l'utilisateur soient présentes et s'enregistrent dans la cartographie du poste. Ci-dessous se trouve la page qui accueille les utilisateurs lors du démarrage de leur poste SMOBI.



Une fois la partie CRYHOD passée, on accède à l'écran de connexion Windows. Cependant le poste n'est pas encore connecté au réseau Intradef. L'utilisateur peut quand même se connecter grâce à la LSA (Local Security Authority) qui est la base de données chiffrée contenant les informations de connexion stockées dans le cache de l'ordinateur. Sans ça, l'utilisateur ne pourrait accéder à sa session. Ensuite, pour se connecter au VPN et rejoindre le réseau du domaine, une nouvelle sécurité s'impose pour activer les services SMOBI.

2.2/ Utilisation du Token et Cryptosmart

Toutes les personnes possédant un PC doté de la solution SMOBI reçoivent impérativement un Token qui fera office de « certificat » pour prouver l'identité de l'utilisateur.
Lorsque l'utilisateur a passé la couche CRYHOD, il insère le Token qui prend la forme d'une clé USB et rendre un code PIN qu'il a défini.

Ce Token et son code vont activer Cryptosmart qui va activer à la suite plusieurs services. Tout d'abord, il va vérifier la présence et le fonctionnement de l'antivirus. Une fois ceci fait, il va vérifier la présence du driver OpenVPN TAP et tenter de se connecter aux serveurs de mobilités à l'aide de ce dernier.
Lorsque cette connexion est au vert, bien souvent, Skype se lance et vient confirmer la connexion au domaine DR-CPT, correspondant à Intradef. Les personnes pourront donc ensuite travailler dans le domaine.

3/ Problèmes rencontrés

La solution SMOBI peut rencontrer des problèmes d'origines différentes.
Je vais en présenter quelques-uns et parler des solutions trouvées pour les résoudre.

3.1/ Déconnexion intempestives

Tout d'abord, la solution SMOBI peut rencontrer des problèmes de déconnexions intempestives. Lorsqu'un utilisateur passe du mode mobilité au mode bureau, des déconnexions peuvent se produire en raison des différences de configuration et de réseau entre ces deux environnements. Ces déconnexions sont souvent dues à des paramètres réseau spécifiques ou à des configurations de proxy qui changent entre les deux modes de fonctionnement.
La solution la plus courante pour résoudre ces déconnexions est de recharger la configuration du VPN et des paramètres réseau dans les paramètres de la solution SMOBI.

Pour accompagner l'utilisateur dans la résolution de ce problème, il y a plusieurs moyens. Par exemple, il est fourni en amont un article de la base de connaissance (KB) accessibles sur l'interface utilisateur et technicien de DIADEME. Cet article contient les problèmes récurrents et les premières manipulations que l'utilisateur peut tenter de faire. Si l'utilisateur n'a pas été mis au courant de l'article il va certainement contacter le 13 (numéro correspondant au standard du SDK). Lorsque l'on reçoit l'appel, nous sommes contraints de travailler à l'aveugle car le poste n'étant pas encore connecté, nous ne pouvons effectuer aucune manipulation à distance. Il faut donc réussir à comprendre le réel problème de l'utilisateur et réussir également à correctement lui faire comprendre les manipulations qu'il va devoir effectuer pour résoudre son problème.

Aussi il peut arriver que les cartes réseaux des postes de travail dysfonctionnent, causant des déconnexions intermittentes ou permanentes. Ce problème est particulièrement complexe à résoudre en mobilité, car comme dit au-dessus la prise en main à distance n'est pas possible dans cet environnement. Les cartes réseaux peuvent nécessiter une intervention physique pour être reparamétrées, réinitialisées ou remplacées par les CIRISI de rattachement.

Un autre problème potentiel concerne les paramètres du BIOS qui parfois se réactivent automatiquement ou n'ont pas été correctement configurés (Wi-FI désactivé). Les paramètres du BIOS peuvent affecter la performance réseau et la stabilité de la connexion VPN. Ce problème ne peut également pas être résolu à distance et bien heureusement sinon cela poserait de sérieux problèmes en matière de sécurité informatique.

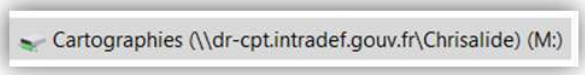
3.2/ Perte de mot de passe CRYHOD

L'un des problèmes que l'on rencontre le plus si ce n'est le problème le plus courant de la solution SMOBI, vient simplement de l'utilisateur. Il arrive fréquemment que les utilisateurs oublient leur mot de passe, notamment après une période prolongée d'absence comme les vacances. Cette situation peut poser des problèmes importants, en particulier pour passer la couche de sécurité Cryhod où il est indispensable de rentrer son mot de passe pour déchiffrer le poste et accéder à Windows.

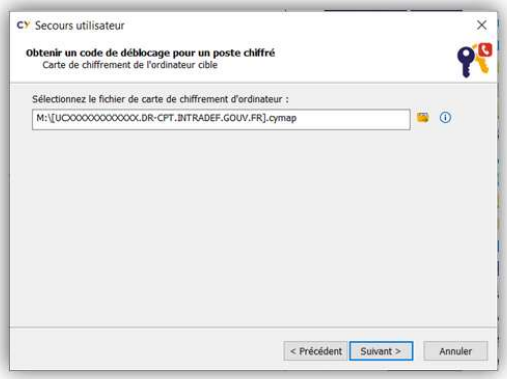
Pour résoudre ce problème, une procédure complète est prévue à cet effet :

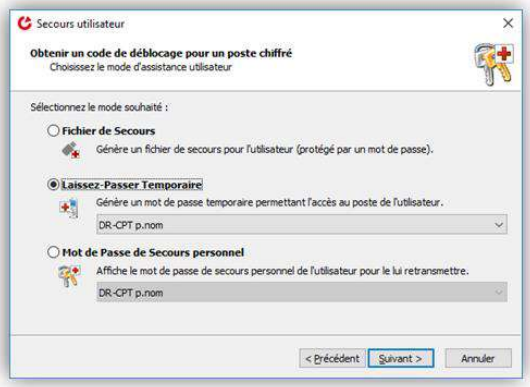
Sur la page où ils doivent rentrer leur mot de passe, il leur est possible d'appuyer sur un petit écrou au niveau de la partie inférieure gauche ou en faisant F7 pour accéder à une liste d'options. La numéro 4 permet d'initier une procédure de secours.
Lorsqu'elle est initiée, une page rouge s'affiche sur leur écran, indiquant le numéro « France Télécom » du SDK, un numéro de ticket qu'il faut fournir au technicien après qu'un collègue ait fait un ticket DIADEME pour la perte du mot de passe de chiffrement.

Le technicien récupère la cartographie du poste avec le numéro d'UC qui est également fourni sur la page rouge. Les postes SMOBI, lorsqu'ils sont connectés au domaine, transmette automatiquement leur cartographie à un serveur appelé CHRISALIDE. Cela nous permet ensuite d'y accéder pour ce genre de cas où nous avons besoin d'accéder à la cartographie pour la réinitialisation du mot de passe.

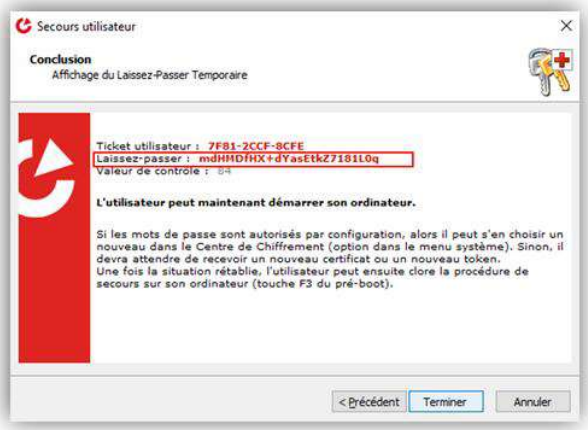


Il entre la cartographie dans le logiciel dédié et indique le numéro de ticket. Ensuite, on choisit la personne présente sur la cartographie à qui souhaite fournir un laisser-passer temporaire.





On déverrouille la partition et ensuite on arrive sur une page qui donne un très long code de déblocage qu'il faut citer à l'utilisateur ainsi qu'une valeur de contrôle.



L'utilisateur tape le code et obtient à son tour une valeur de contrôle. Si celle-ci est identique, tout est bon, l'utilisateur peut dès à présent changer son mot de passe, sinon il faut vérifier le code de déblocage.

Autre option, un autre utilisateur (souvent le CORSIC) est également présent sur la cartographie du poste et peut donc passer la couche CRYHOD. Cela nous permet ainsi de prendre la main à distance après que l'utilisateur dont le mot de passe est oublié se soit connecté à sa session Windows. Une fois qu'on a la main, on peut faire à peu près la même manipulation mais cette fois-ci, nous n'avons rien à dicter et tout est beaucoup plus rapide. L'utilisateur n'a plus qu'à taper un nouveau mot de passe respectant les règles définies. On reste en ligne jusqu'à ce qu'il teste son nouveau mot de passe en déverrouillant la couche CRYHOD.

Activité 4 – Déploiement d'OpenVPN avec authentification LDAP depuis un Active Directory

Cette activité a été réalisée en commun avec Mathis Guillard, également apprenti au sein du SDK de Rennes, pour correspondre à la réalisation « travailler en mode projet ». Cette collaboration permet d'y répondre efficacement. Ainsi nous avons fait le choix d'utiliser la méthode de cycle en V.

D'abord, nous avons déterminé une « demande client ». Nous avons considéré que la demande était de mettre en place un accès distant au réseau de l'entreprise avec une authentification identique à celle des utilisateurs du domaine sur place.
Une fois cette demande déterminée, la première étape est de l'analyser : le client nécessite un accès distant sécurisé, il faut donc mettre en place un VPN. Cet accès doit être sécurisé avec une connexion grâce aux identifiants du domaine, cela implique une authentification via LDAP.

N'ayant pas l'opportunité de le faire au sein de notre entreprise, nous avons simulé une infrastructure classique de l'Active Directory avec un Contrôleur de Domaine que l'on nomme « DC » ainsi qu'un Contrôleur de Domaine Supplémentaire que l'on nomme « ADC ».

Ainsi, pour correspondre aux attentes de l'authentification LDAP et du certificat fourni lors de l'interrogation du serveur, il nous faut un reverse proxy pour répartir la charge entre les serveurs et utiliser une adresse IP virtuelle qui redirige vers les deux contrôleurs de domaine. On utilisera donc HAProxy qui répond à ces attentes tant en termes d'efficacité que de rapidité.

Pour encapsuler le réseau, héberger le VPN, le serveur HAProxy et gérer les certificats, on a fait le choix d'utiliser pfSense qui regroupe tout cela.

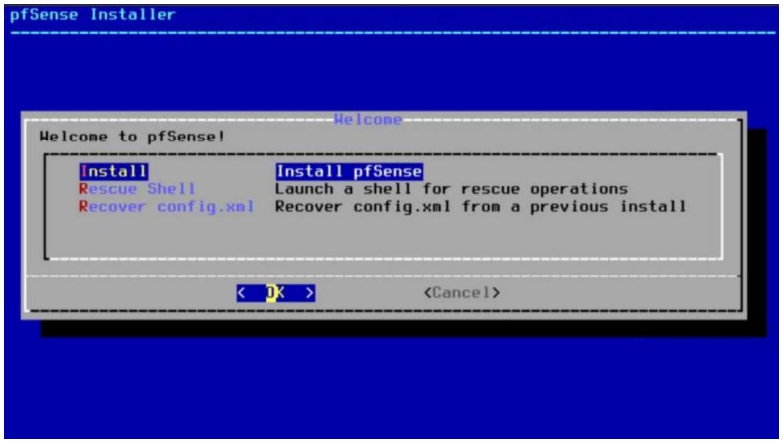
Par la suite il a fallu se répartir les tâches et faire les tests après chaque étape :

	William	Mathis
Etape 1	Installation pfSense	Installation DC
Test	Essai de la connexion et de l'appartenance au réseau	
Etape 2	Installation ADC	Installation Machine Cliente
Test	Intégration de la machine cliente au domaine et test réplication	
Etape 3	Paramétrage AD et pfSense pour HAProxy et VPN	
Test	Essai de connexion LDAP depuis pfSense + connexion du client depuis le « WAN » et test du failover	

1/ Etape 1

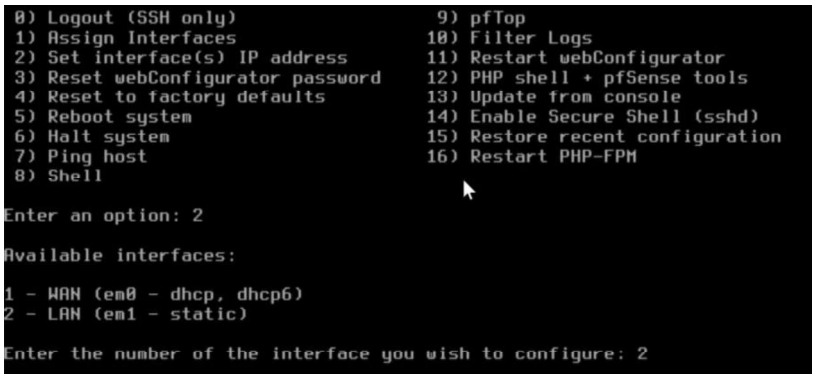
1.1/ Installation de pfSense et de DC

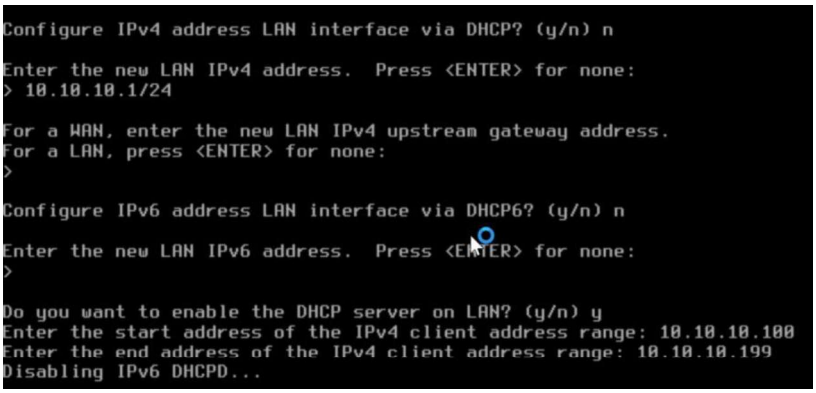
Tout d'abord l'installation de pfSense



Une fois la partie « Installer » terminée, on définit les interfaces et les réseaux.
Ici, le WAN est défini avec une adresse dans un sous-réseau 192.168.1.0/24 qui correspond à mon réseau local dans lequel se trouve mon serveur Proxmox qui héberge les machines de cette activité.

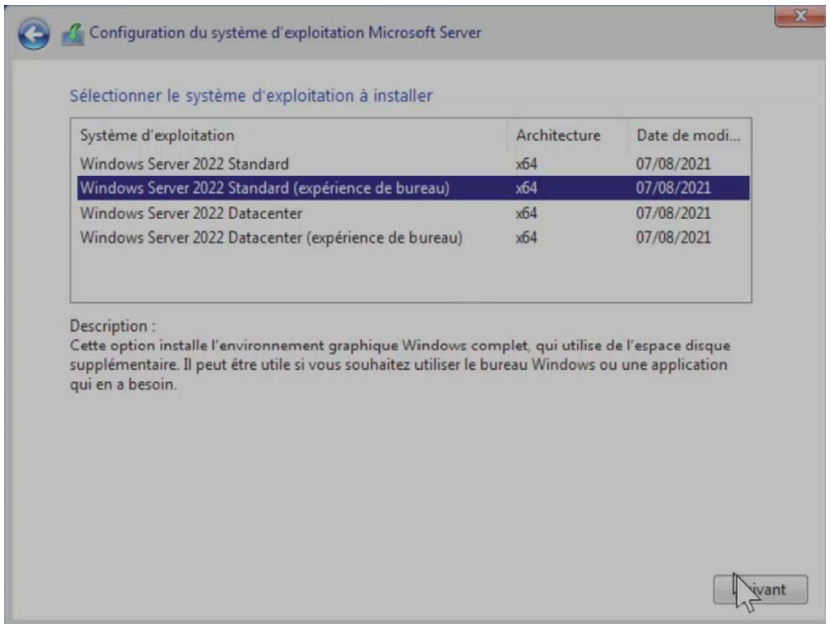
On doit donc configurer le LAN :





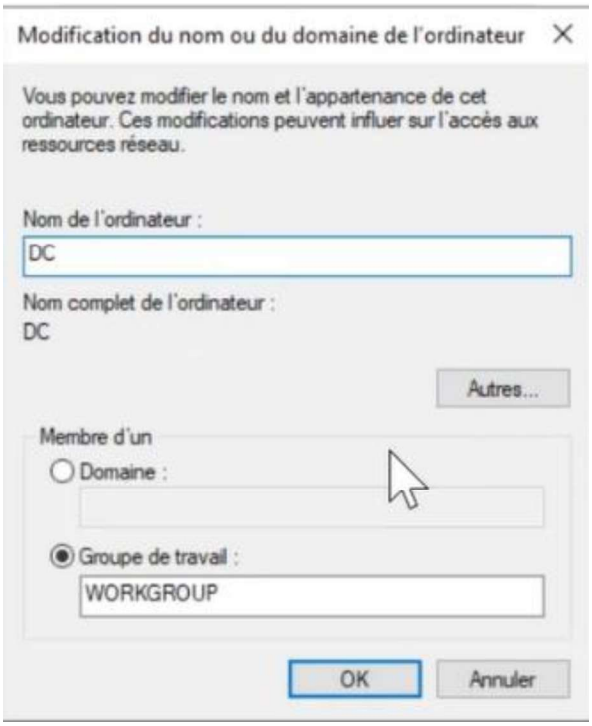
Maintenant l'installation de DC :

On choisit intentionnellement Windows Server Standard avec expérience de bureau

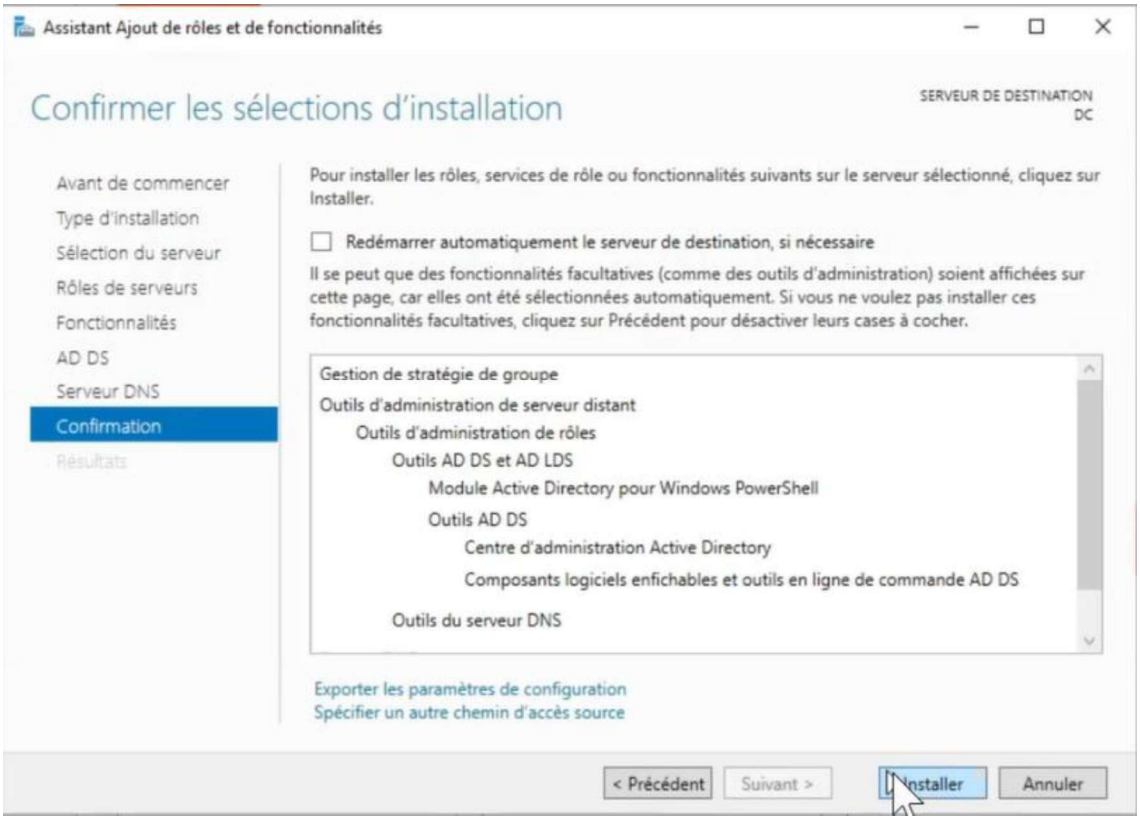


On définit ses paramètres réseaux. Une IP fixe en .10, la passerelle en .1 et on prévoit en ajoutant en DNS la future adresse IP du contrôleur de domaine supplémentaire (ADC).

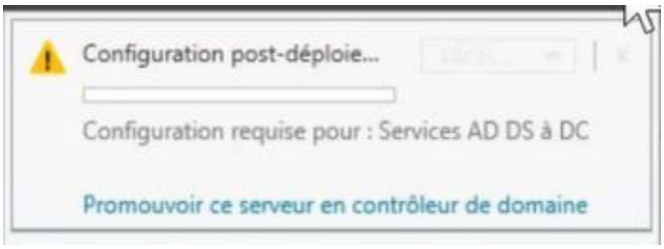
Et on renomme le poste « DC » :

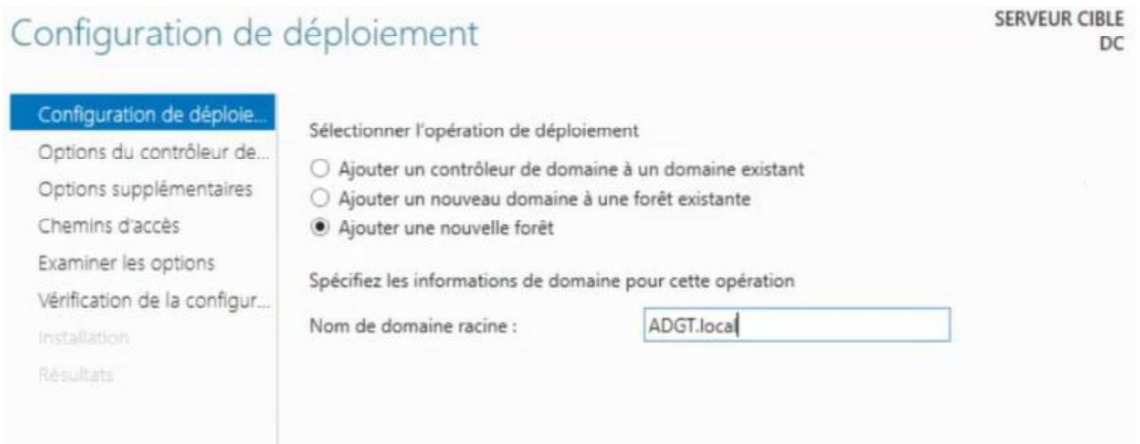


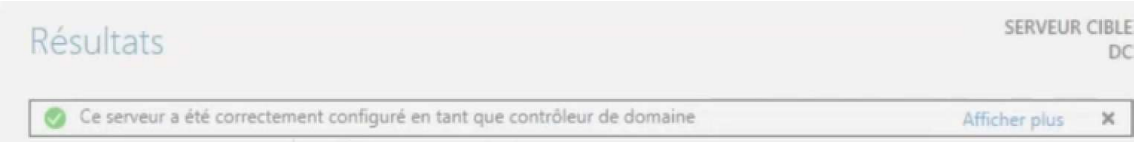
On ajoute le rôle et les outils AD DS ainsi que les outils DNS :



Et par la suite, on promeut le serveur en tant que contrôleur de domaine, on crée une nouvelle forêt avec comme nom de domaine racine ADGT.local :







1.2/ Tests Etape 1

Cette étape est la seule où les tests ont dû se dérouler entre les deux parties. J'ai d'abord paramétré l'adresse IP LAN et le DHCP depuis pfSense pour que Mathis puisse accéder au réseau en paramétrant le contrôleur de domaine.

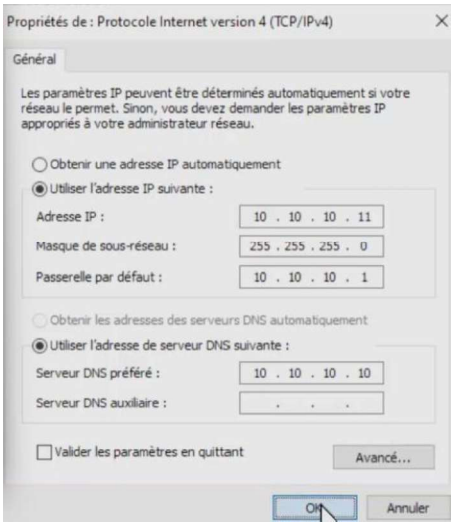
On peut voir dès le démarrage du serveur qu'il reçoit bien une adresse depuis le DHCP, que la passerelle est bien définie et qu'il accède bien au WAN :

```
C:\Users\Administrateur>ipconfig

Configuration IP de Windows


Carte Ethernet Ethernet :

   Suffixe DNS propre à la connexion. . . : home.arpa
   Adresse IPv6 de liaison locale. . . . .: fe80::d03d:93b2:fd41:80c5%6
   Adresse IPv4. . . . . . . . . . . . . .: 10.10.10.101
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . : 10.10.10.1

C:\Users\Administrateur>ping 1.1.1.1

Envoi d'une requête 'Ping'  1.1.1.1 avec 32 octets de données :
Réponse de 1.1.1.1 : octets=32 temps=9 ms TTL=56
Réponse de 1.1.1.1 : octets=32 temps=9 ms TTL=56
```

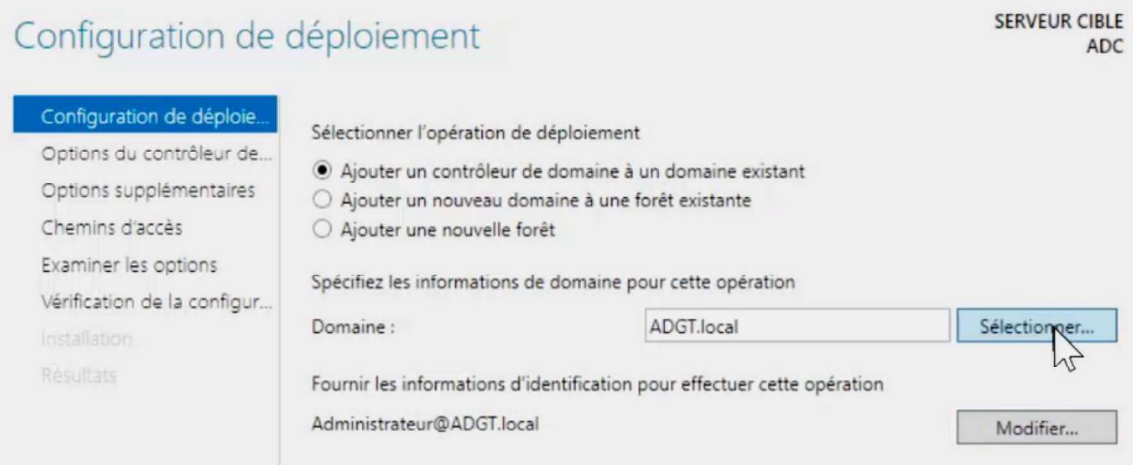
2/ Etape 2

2.1/ Installation ADC et machine cliente

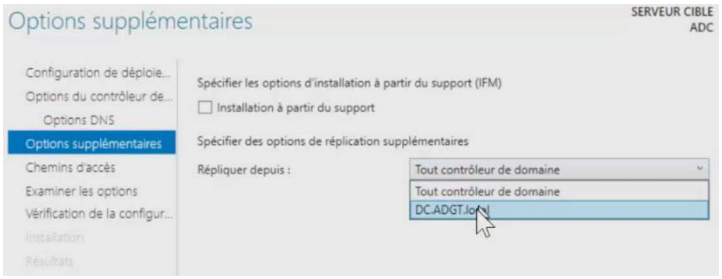
Pour l'installation de l'ADC, c'est très semblable à celle du DC. Excepté pour les paramètres IP et au moment de promouvoir en tant que contrôleur de domaine.



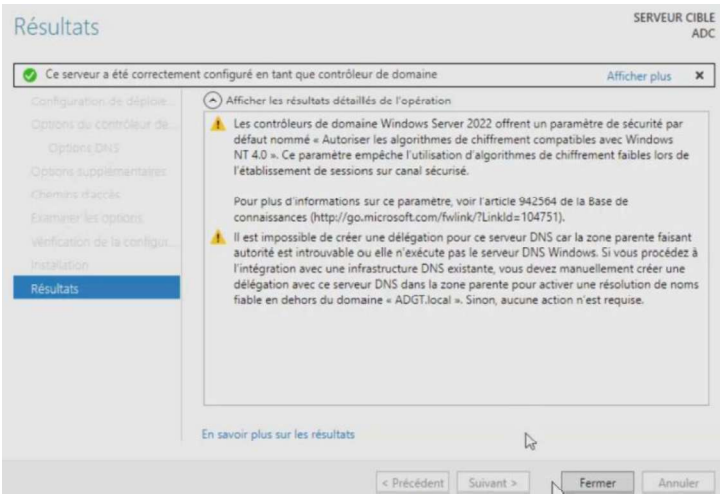
On choisit « Ajouter un contrôleur de domaine à un domaine existant ». Pour se simplifier la tâche, on rentre directement les informations d'identification qui sont Administrateur@ADGT.local et le mot de passe correspondant. Cela va détecter automatiquement le domaine que l'on souhaite rejoindre et nous y accorder les droits. C'est également permis grâce à l'IP de DC renseignée en tant que DNS préféré.



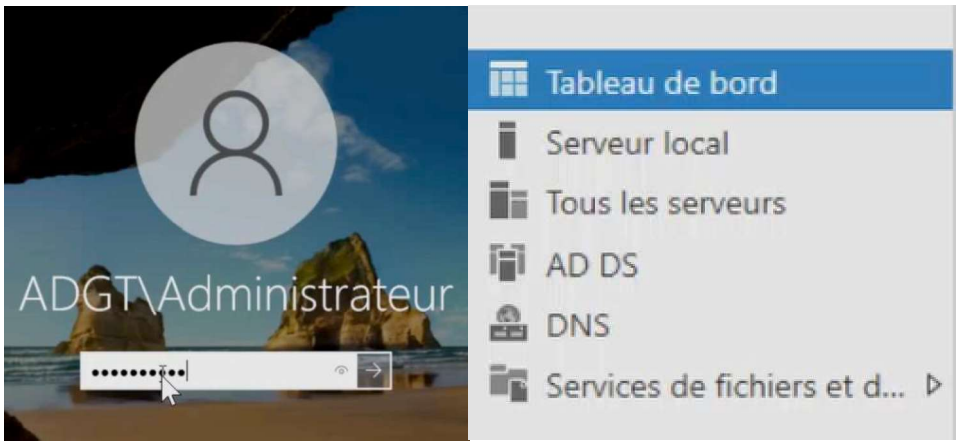
De plus, dans les options supplémentaires, on sélectionne répliquer depuis DC.ADGT.local. Dans notre situation c'est facultatif, mais cela peut être utile si l'on est sur un domaine avec plus de deux contrôleurs et que l'on veut préciser.



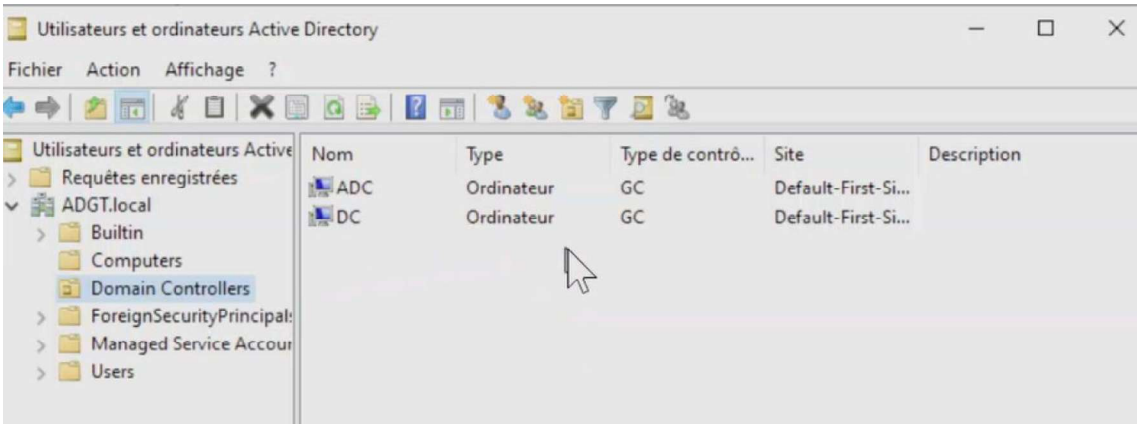
Les tests de réplication se sont bien déroulés, on peut désormais fermer l'assistant et une fois que le poste aura redémarré il sera bien contrôleur du domaine.



On peut désormais se connecter en tant qu'administrateur du domaine et les rôles sont bien descendus :



On voit également dans l'outil « Utilisateurs et ordinateurs Active Directory » les deux contrôleurs de domaine :



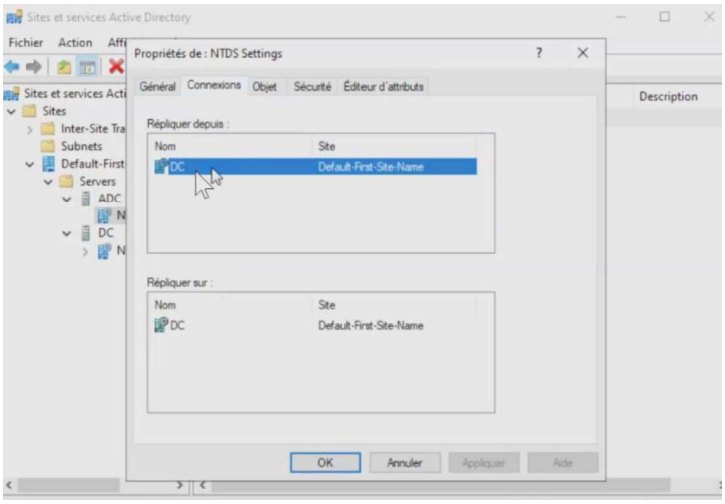
Pendant ce temps, la machine cliente s'installe. Nous avons choisi un Windows 10 en 22H2. On l'installe en tant que Windows 10 Pro pour qu'elle puisse rejoindre un domaine. On la laisse prendre une adresse IP via le DHCP mais on vient forcer les DNS en 10.10.10.10 et 10.10.10.11.

2.2/ Tests Etape 2

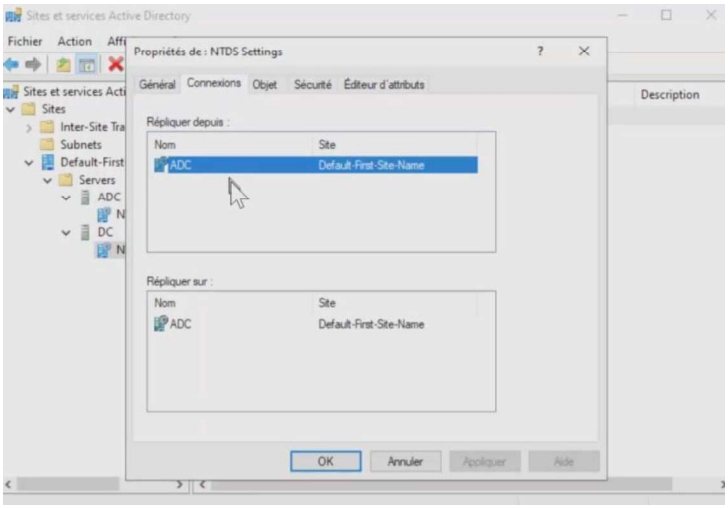
Tout d'abord on teste la réplication entre les contrôleurs de domaine :

Dans un premier temps, on va se rendre dans « Sites et services Active Directory » et on vérifie que les contrôleurs répliquent bien l'un sur l'autre :

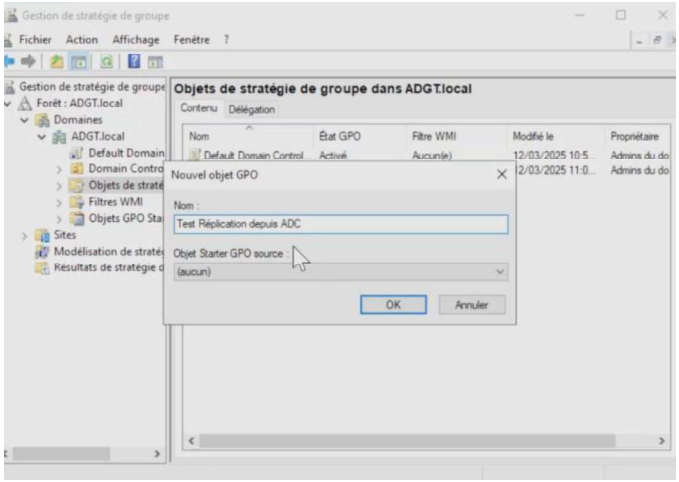
Pour l'ADC :



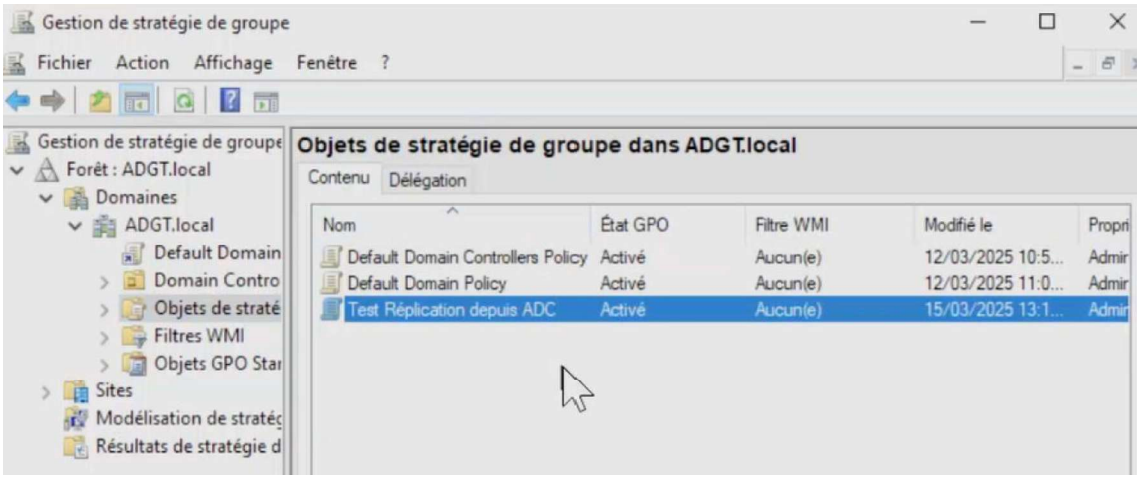
Pour DC :



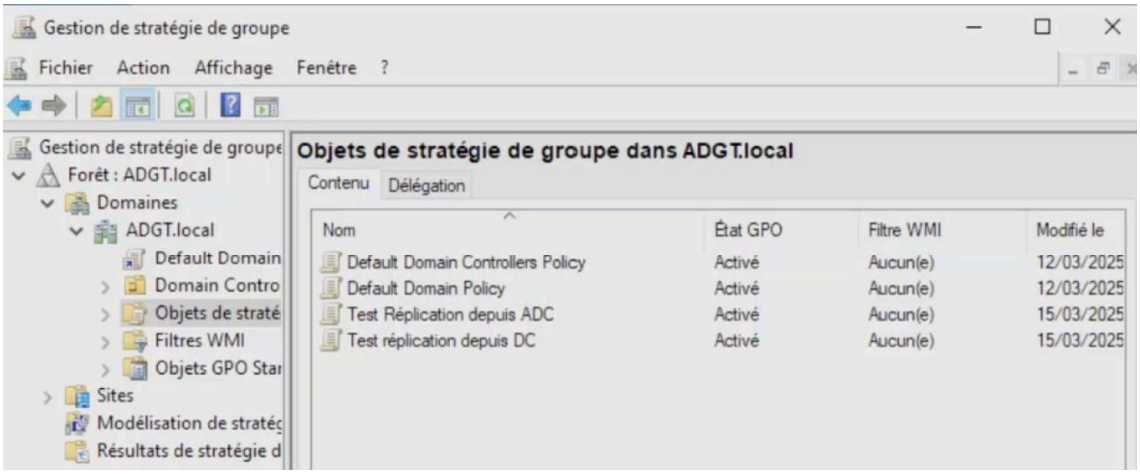
On crée également une GPO depuis l'ADC pour voir si elle sera bien répliquée dans les GPO sur DC :



Et on la voit bien depuis DC :



On fait pareil dans l'autre sens et tout se passe bien :

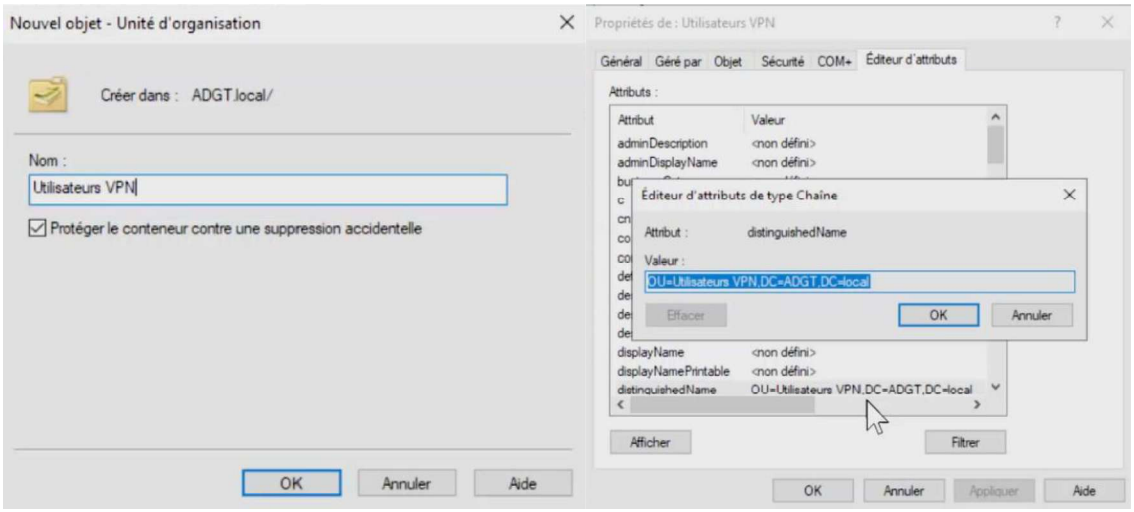


3/ Etape 3

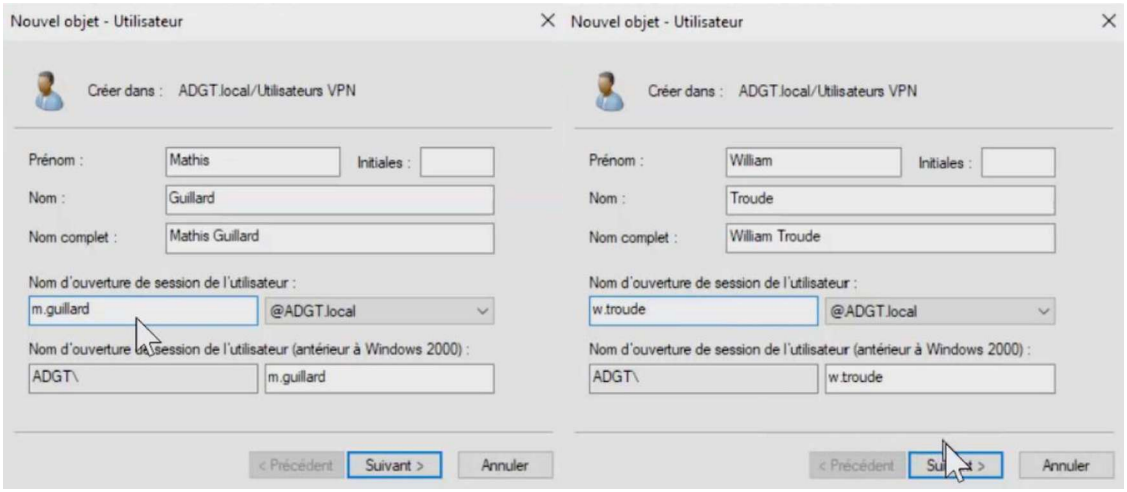
3.1/ Paramétrage AD et pfSense

Avant de configurer pfSense, il est nécessaire de créer une Unité d'Organisation (OU) intitulée Utilisateurs VPN, dans laquelle seront ajoutés les comptes utilisateurs destinés à utiliser le VPN.

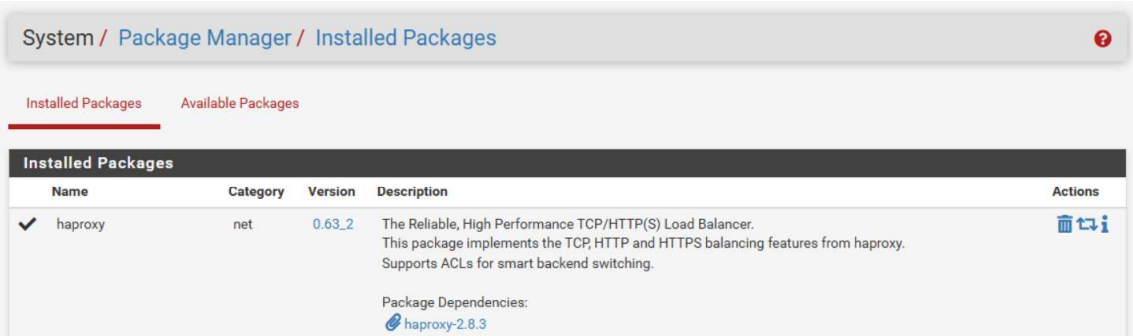
On crée donc d'abord l'OU puis on récupère son DN pour plus tard :



Et on crée des utilisateurs qui auront la possibilité de se connecter au VPN :

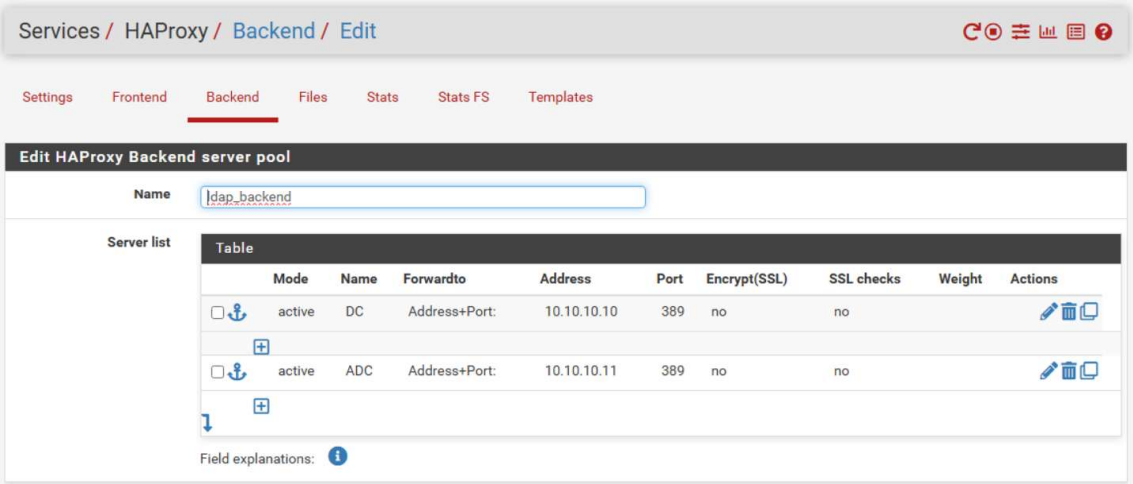


Passons maintenant au paramétrage de pfSense. On va commencer par installer le package HAProxy :

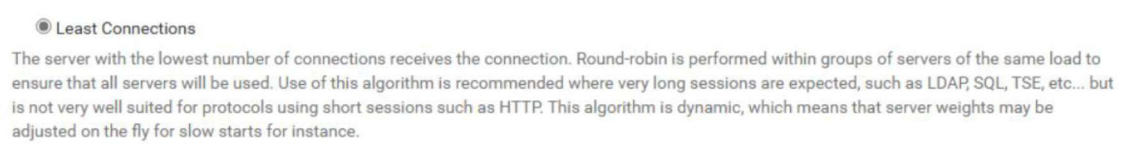


Avant de le configurer, on ajoute une IP virtuelle sur le même réseau que le LAN qui permettra à HAProxy d'écouter sur cette dernière.

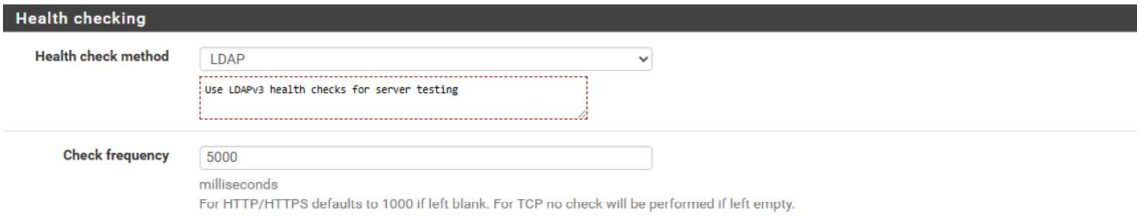
On configure le backend en ajoutant d'abord les deux contrôleurs de domaine, leurs IP ainsi que le port utilisé pour LDAP :



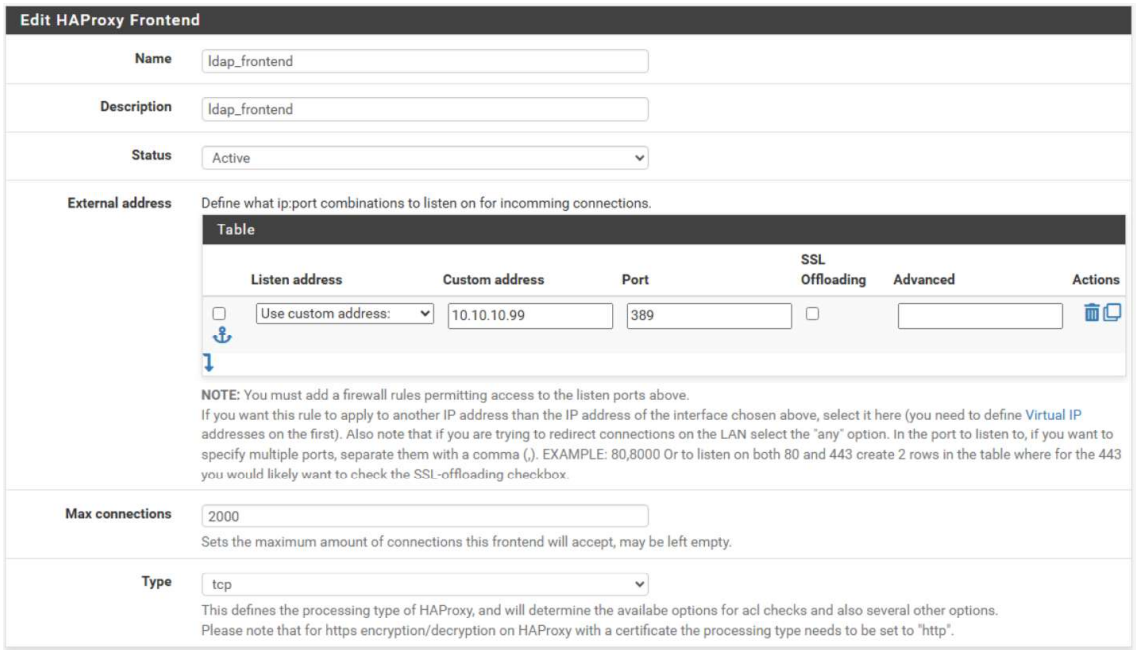
Pour le loadbalancing, on choisit « Least connections » qui nous parait le plus approprié pour une utilisation du VPN dans une PME par exemple :



Pour « health checking », on choisit bien LDAP avec un intervalle de 5 secondes :



Maintenant, pour le frontend, on indique l'IP virtuelle sur laquelle écoutera HAProxy, le port pour LDAP ainsi que le nombre max de connexions et le protocole TCP :



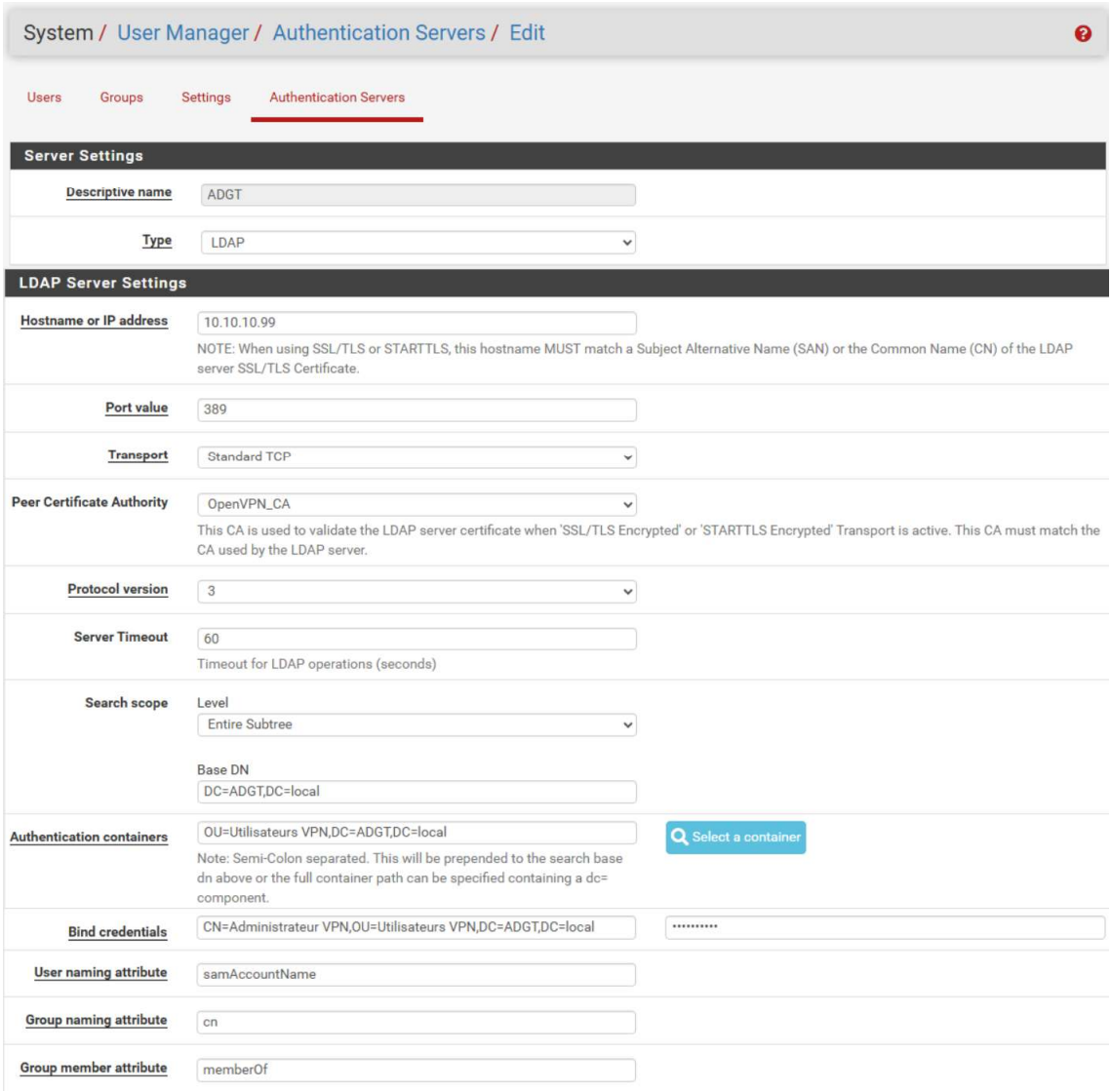
Et on lui indique le backend que l'on a paramétré juste avant :

Pour le VPN maintenant, il va d'abord falloir créer une autorité de certification pour créer le certificat serveur. Ensuite on va renseigner le serveur d'authentification et définir le serveur OpenVPN.

Une fois l'autorité de certification créée, on peut ajouter un certificat pour le serveur en indiquant l'autorité comme émettrice :

Et le certificat :

On paramètre ensuite le serveur d'authentification. On y précise le type : LDAP, l'IP d'écoute d'HAProxy qui interrogera à son tour les deux contrôleurs de domaine. Ensuite on renseigne le DN de l'OU que nous avons créée en amont pour les utilisateurs VPN. Le DN renseigné désigne le conteneur qui sera interrogé pour savoir si les utilisateurs qui tenteront de se connecter en ont bien l'autorisation. On renseigne ensuite le DN et le mot de passe d'un administrateur. On aura créé auparavant un « Administrateur VPN ». Ce compte serait utile dans le cadre d'une entreprise où la gestion des services serait segmentée.



Pour le VPN on indique dès le début la méthode d'authentification en sélectionnant le serveur créé juste avant. Ensuite, on choisit le protocole, l'interface et son port d'écoute. On coche également l'utilisation d'une clé TLS en précisant le certificat que l'on a créé et son autorité.

Pour le tunnel, on choisit pour la facilité de compréhension un réseau en 10.10.20.0/24. On force aussi la redirection vers la passerelle. On indique le nombre de connections simultanées et on autorise la communication entre les clients. On précise quelques paramètres et on indique les informations pour les serveurs DNS. Pour plus d'efficacité, nous aurions pu ajouter une écoute sur le port 53 par le HAProxy et n'ajouter que l'IP en .99 dans les DNS du client. Ensuite on active le NetBIOS over TCP/IP.
Pour finir, on crée une route pour permettre aux clients VPN de communiquer avec le LAN ainsi que des règles de pare-feu pour autoriser les communications.

3.2/ Tests Etape 3

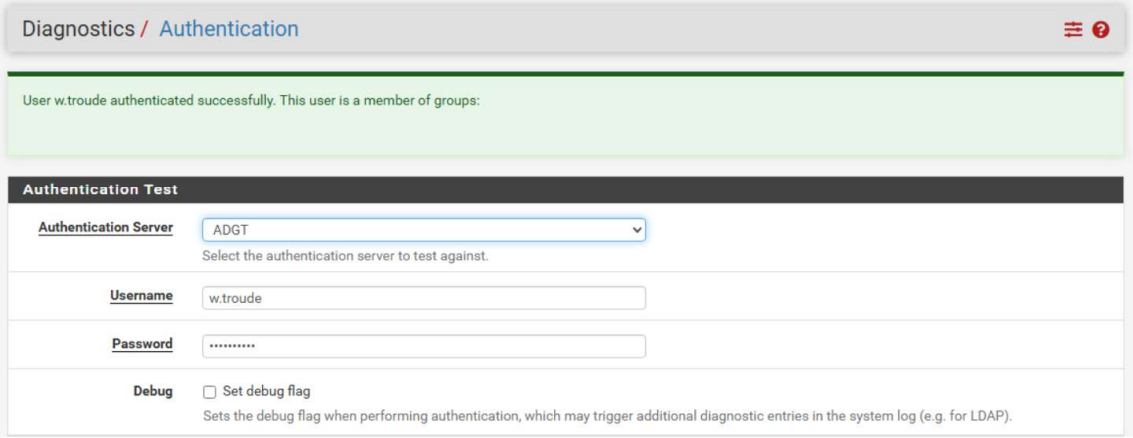
Depuis le shell pfsense, on effectue un test avec la commande suivante :

```
[2.7.2-RELEASE][admin@pfSense.home.arpa]/root: ldapsearch -x -H ldap://10.10.10.99 -D "CN=Administrateur,CN=Users,DC=adgt,DC=local" -W -b "OU=Util
isateurs VPN,DC=adgt,DC=local" "(objectClass=user)"
Enter LDAP Password:
```

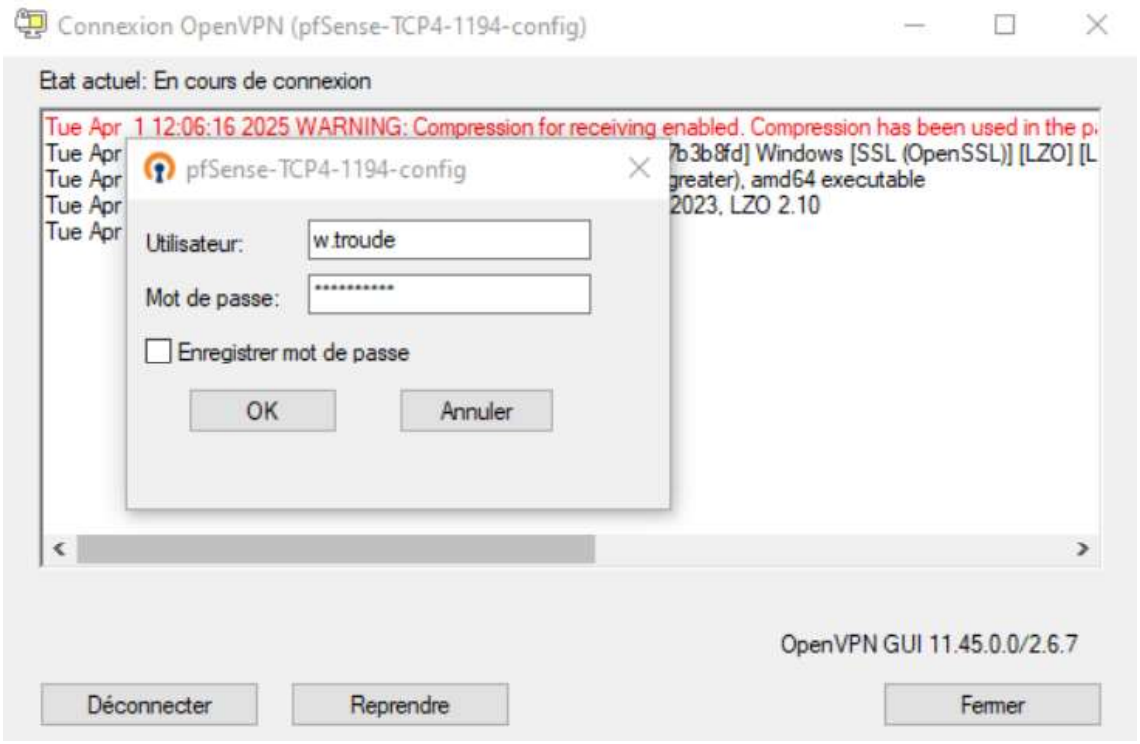
Cette dernière permet de vérifier que le HAProxy fonctionne, que les contrôleurs de domaine répondent bien (en coupant l'un, puis l'autre) et que le DN de l'OU est correct.
On obtient donc une réponse avec les trois utilisateurs présents dans l'OU et un message de réussite.

```
# search result
search: 2
result: 0 Success
```

On peut également tester le serveur d'authentification dans « Diagnostics » puis « Authentication ». On voit ci-dessous que le test s'est bien déroulé.



Il nous reste plus qu'à tester la connexion via VPN. On installe le package OpenVPN-Client-export pour installer le client sur la machine d'un utilisateur. On se connecte donc avec la configuration VPN donnée par le Client Export en indiquant les identifiants d'un utilisateur de l'OU :



Et on voit que l'on prend bien une IP du tunnel.

```
Carte Ethernet Ethernet :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6. . . . . . . . . . . . . .: 2a01:e0a:267:a8b0:6829:b3a1:cd74:9e6
   Adresse IPv6 temporaire . . . . . . . .: 2a01:e0a:267:a8b0:f0e9:fa3a:27a1:f93d
   Adresse IPv6 de liaison locale. . . . .: fe80::fe68:841b:ab18:37d4%5
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.1.46
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . : fe80::3a07:16ff:fec1:4043%5
                                            192.168.1.254

Carte inconnue OpenVPN TAP-Windows6 :

   Suffixe DNS propre à la connexion. . . : ADGT.local
   Adresse IPv6 de liaison locale. . . . .: fe80::19e8:461f:94bd:c2c1%16
   Adresse IPv4. . . . . . . . . . . . . .: 10.10.20.2
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . :
```

On arrive bien à ping les deux serveurs qui sont sur le LAN :

```
C:\Users\Administrateur>ping 10.10.10.10

Envoi d'une requête 'Ping'  10.10.10.10 avec 32 octets de données :
Réponse de 10.10.10.10 : octets=32 temps=2 ms TTL=127
Réponse de 10.10.10.10 : octets=32 temps=2 ms TTL=127
Réponse de 10.10.10.10 : octets=32 temps=5 ms TTL=127
Réponse de 10.10.10.10 : octets=32 temps=2 ms TTL=127

Statistiques Ping pour 10.10.10.10:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 2ms, Maximum = 5ms, Moyenne = 2ms

C:\Users\Administrateur>ping 10.10.10.11

Envoi d'une requête 'Ping'  10.10.10.11 avec 32 octets de données :
Réponse de 10.10.10.11 : octets=32 temps=2 ms TTL=127
Réponse de 10.10.10.11 : octets=32 temps=2 ms TTL=127
Réponse de 10.10.10.11 : octets=32 temps=2 ms TTL=127
Réponse de 10.10.10.11 : octets=32 temps=6 ms TTL=127

Statistiques Ping pour 10.10.10.11:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 2ms, Maximum = 6ms, Moyenne = 3ms
```

Maintenant pour tester le failover on va arrêter l'un des deux contrôleurs. On ping bien l'un et pas l'autre. On essaie de se reconnecter au VPN à chaque fois et la connexion se fait correctement.

```
C:\Users\Administrateur>ping 10.10.10.10

Envoi d'une requête 'Ping'  10.10.10.10 avec 32 octets de données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.

Statistiques Ping pour 10.10.10.10:
    Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),

C:\Users\Administrateur>ping 10.10.10.11

Envoi d'une requête 'Ping'  10.10.10.11 avec 32 octets de données :
Réponse de 10.10.10.11 : octets=32 temps=2 ms TTL=127
Réponse de 10.10.10.11 : octets=32 temps=47 ms TTL=127
Réponse de 10.10.10.11 : octets=32 temps=70 ms TTL=127
Réponse de 10.10.10.11 : octets=32 temps=53 ms TTL=127

Statistiques Ping pour 10.10.10.11:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 2ms, Maximum = 70ms, Moyenne = 43ms
```

```
C:\Users\Administrateur>ping 10.10.10.10

Envoi d'une requête 'Ping'  10.10.10.10 avec 32 octets de données :
Réponse de 10.10.10.10 : octets=32 temps=9 ms TTL=127
Réponse de 10.10.10.10 : octets=32 temps=42 ms TTL=127
Réponse de 10.10.10.10 : octets=32 temps=2 ms TTL=127
Réponse de 10.10.10.10 : octets=32 temps=46 ms TTL=127

Statistiques Ping pour 10.10.10.10:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 2ms, Maximum = 46ms, Moyenne = 24ms

C:\Users\Administrateur>ping 10.10.10.11

Envoi d'une requête 'Ping'  10.10.10.11 avec 32 octets de données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.

Statistiques Ping pour 10.10.10.11:
    Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),
```

Activité 5 – Installation de pfSense et paramétrage de pfBlockerNG

Pour cette installation il nous faut une machine pfSense avec au moins deux interfaces réseau. J'installerai par la suite le paquet pfBlockerNG et déploierai une machine cliente pour effectuer les tests de fonctionnement.

Cette réalisation a été effectuée au sein de mon homelab notamment dans l'optique d'utiliser ses services pour une utilisation personnelle. De plus, ayant pour souhait de poursuivre mes études dans la cybersécurité, cette réalisation fait lien entre l'administration des systèmes et réseaux de mon cursus actuel et la sécurité de ces derniers.

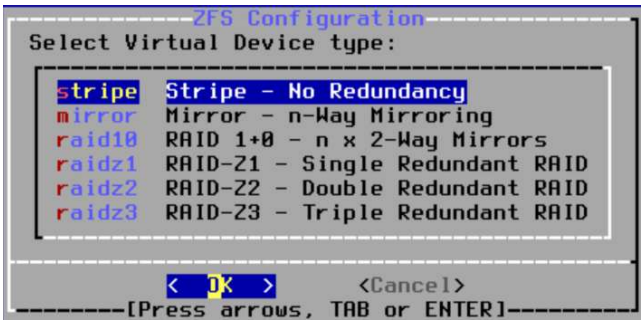
1/ Installation

1.1/Installation de pfSense

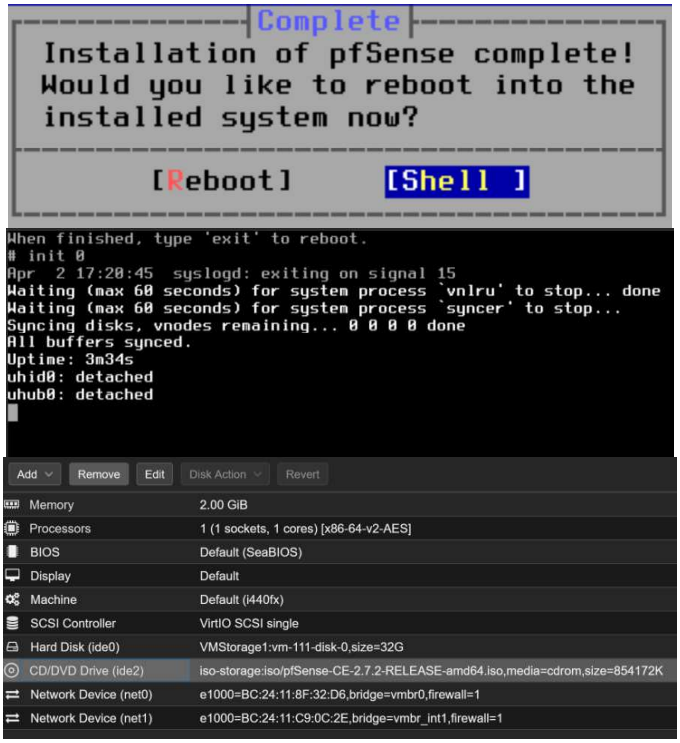
Je vais donc installer pfSense sur mon serveur Proxmox. 1 cœur et 2GB de RAM suffiront. Une interface réseau qui récupère le WAN et une autre pour le LAN sur laquelle j'activerai le DHCP.

Pour l'installation, je vais laisser par défaut ces trois premiers choix.

Ici on va laisser stripe. Dans tous les cas de la redondance est faite sur les disques de mon proxmox et une sauvegarde de mes VMs est effectuée automatiquement vers mon NAS.



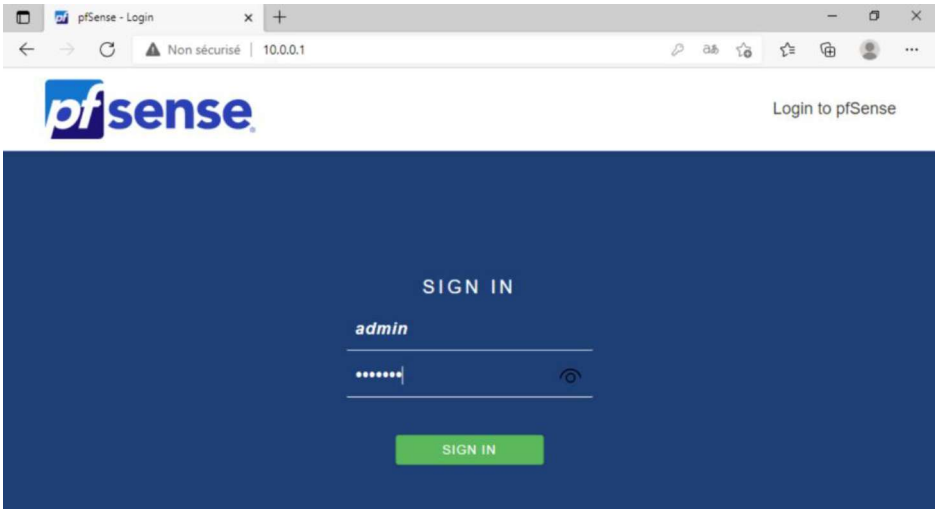
Par réflexe je vais rentrer dans le shell pour rentrer la commande init 0. Il me semble que sur proxmox, après l'installation, la VM boot sur le bon disque mais par sécurité je vais retirer l'ISO.



Maintenant je viens choisir l'interface n°2 qui correspond à celle du LAN. Je lui applique l'adresse 10.0.0.1 avec un sous-réseau en 255.255.255.0. Pas d'IPv6, un DHCP de 10.0.0.100 à .199.

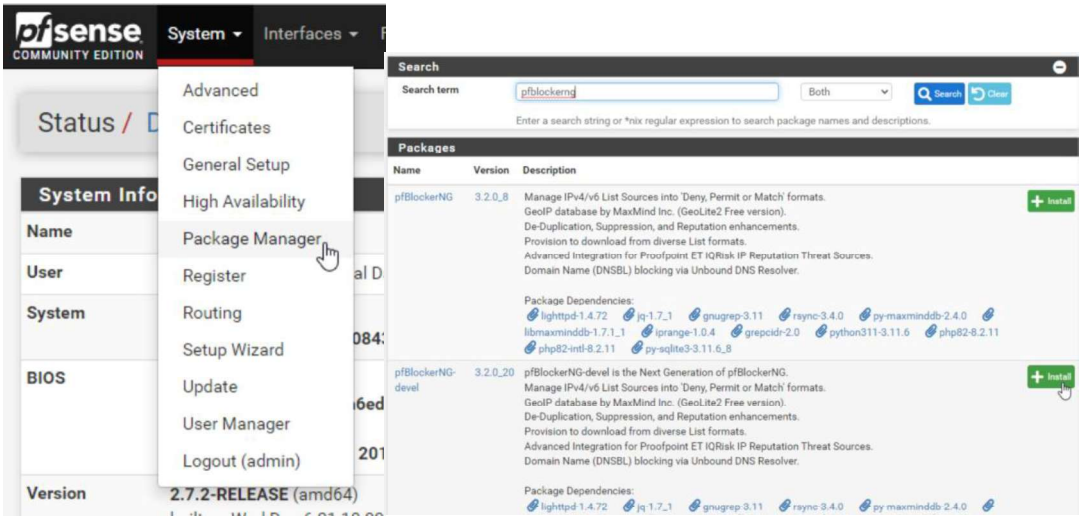
```
Enter an option: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2

Configure IPv4 address LAN interface via DHCP? (y/n) n

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 10.0.0.1/24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address LAN interface via DHCP6? (y/n) n

Enter the new LAN IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 10.0.0.100
Enter the end address of the IPv4 client address range: 10.0.0.199
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) y

Please wait while the changes are saved to LAN...
 Reloading filter...
 Reloading routing configuration...
 DHCPD...
 Restarting webConfigurator...

The IPv4 LAN address has been set to 10.0.0.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                http://10.0.0.1/

Press <ENTER> to continue.
```

Je peux désormais accéder à l'interface WEB depuis une machine cliente.

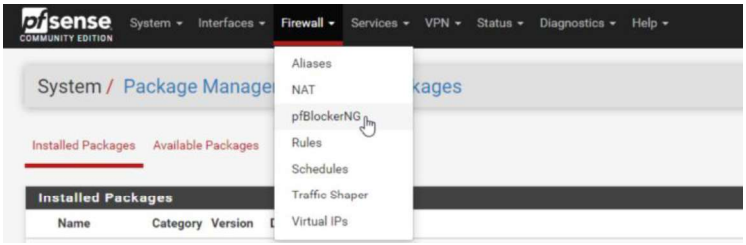


Je laisse la plupart des informations du Wizard par défaut excepté pour les DNS que je viens préciser.

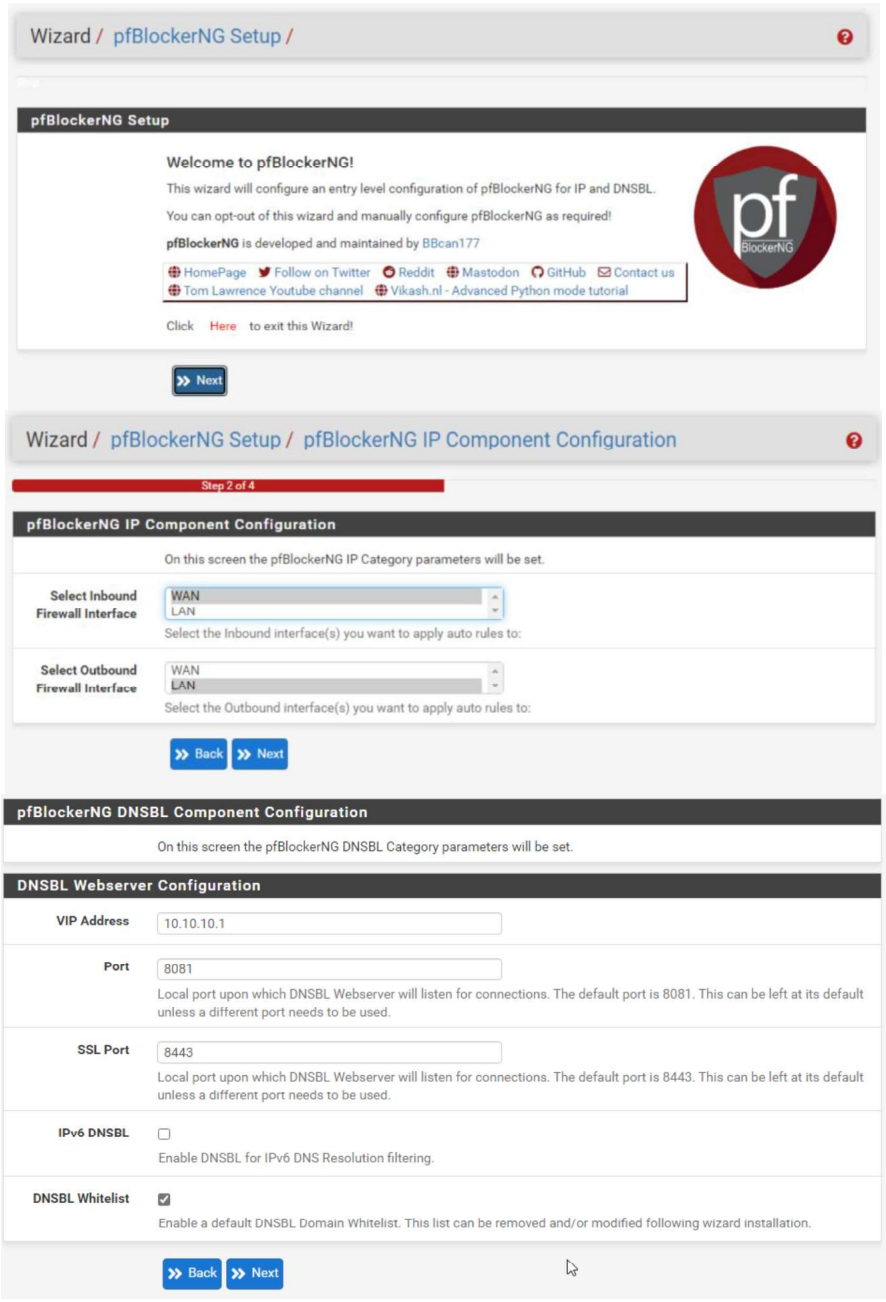
Je me rends ensuite dans le gestionnaire des paquets pour y installer le paquet pfBlockerNG-devel.



J'y accède par la suite depuis l'onglet firewall.



J'arrive directement sur le wizard. Je viens sélectionner les interfaces pour le trafic entrant et sortant, ainsi que les paramètres pour le DNSBL Web Server.



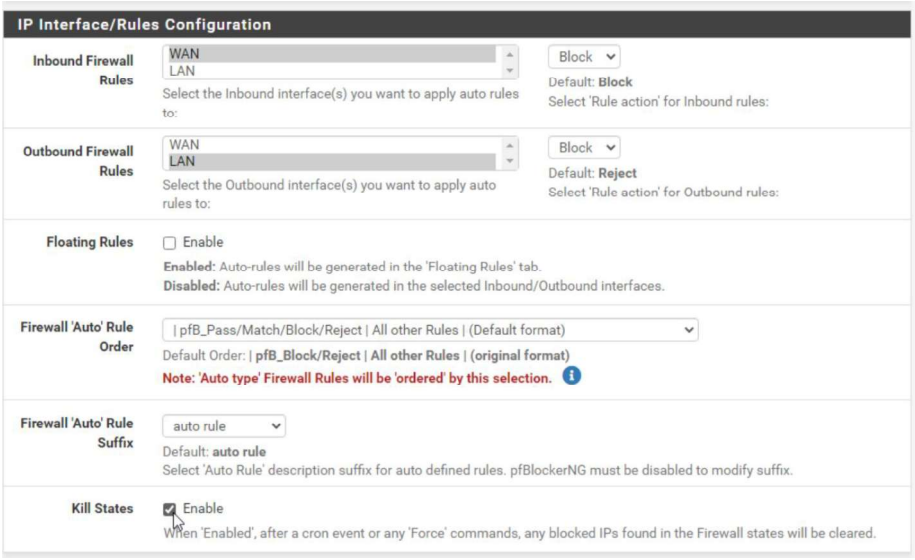
On vérifie que le service DNS Resolver soit bien activé pour le fonctionnement de DNSBL.

1.2/ Paramétrage pfBlockerNG

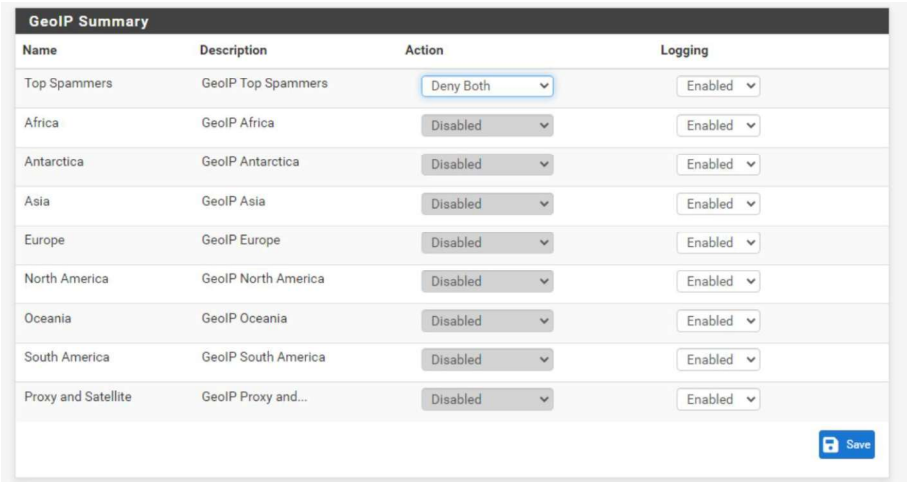
IP

On va commencer par la partie IP. Dans un premier temps je viens indiquer mon ID ainsi que ma clé de licence pour la base de MaxMind.

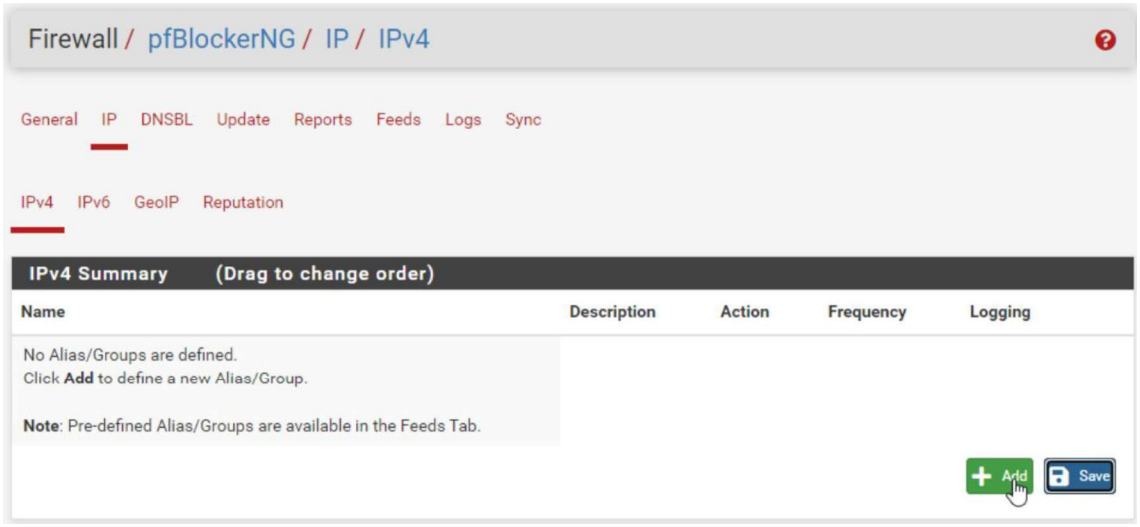
Je viens vérifier les règles et je coche « Kill States ». Si une connexion est déjà existante vers une IP bloquée, pfBlockerNG sera en mesure de supprimer la connexion et bien mettre en marche la blacklist prévue.



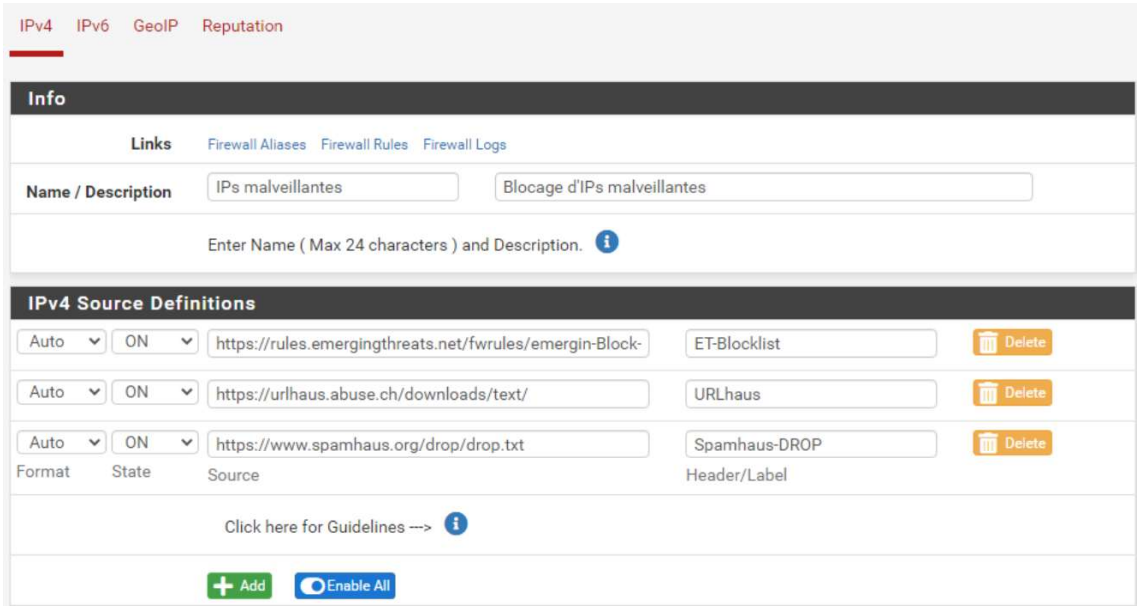
Dans l'onglet GeoIP on accède directement à une liste incluant les continents ainsi que deux autres options. Je vais choisir « Deny Both » pour bloquer les requêtes internes et externes pour les Top Spammers recensés dans les bases de données de MaxMind.



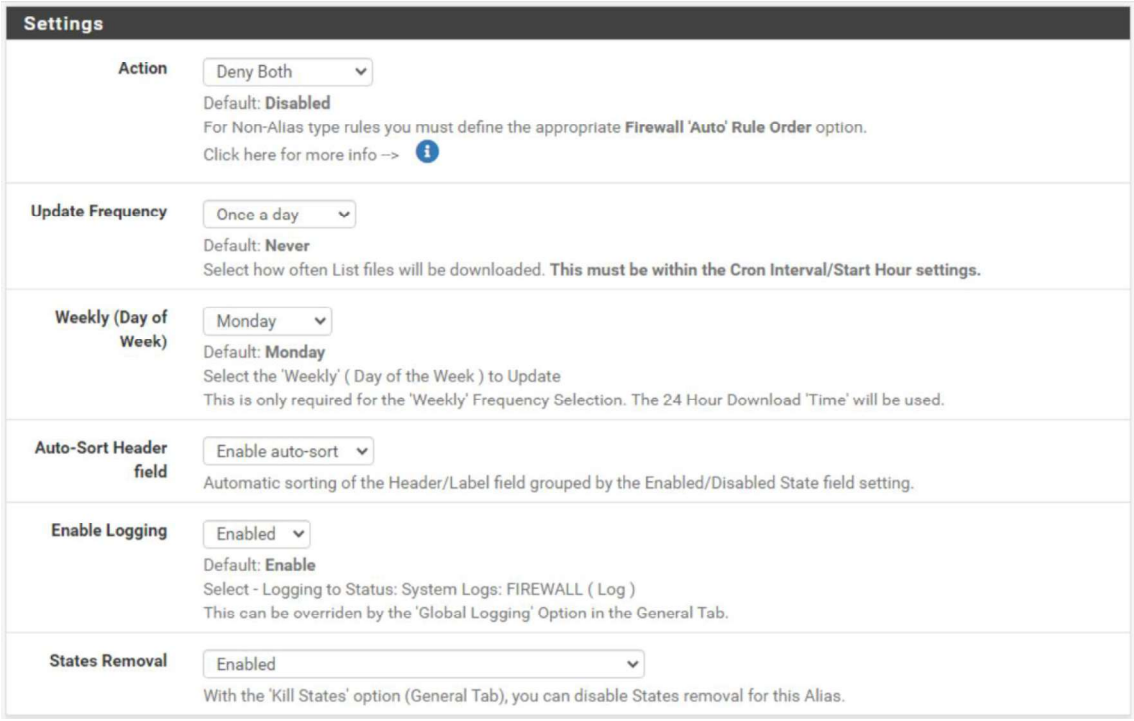
On peut également bloquer des IPs directement. On se rend dans IPv4 et on clique sur « add ».



Je définis son nom, une petite description et ensuite j'ajoute des sources connues. Les trois regroupent des IPs recensées comme malveillantes, que ce soit des IPs de serveurs malwares, des IPs associées à des spams ou des botnets,…

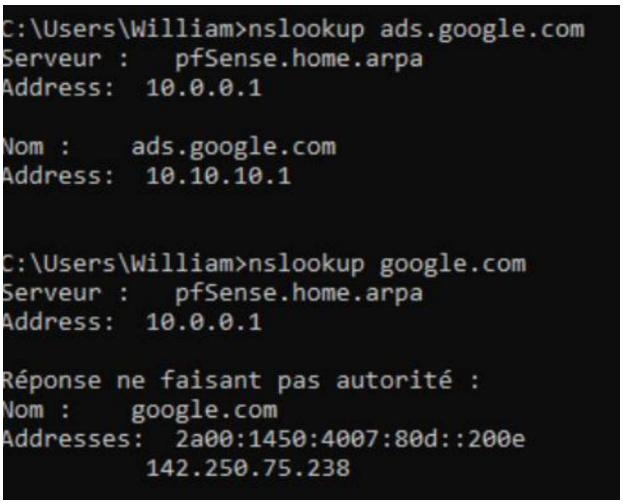


Ensuite dans les paramètres, je viens choisir « Deny Both ». Une mise à jour des listes par jour et je viens vérifier que les logs soient bien activés et on voit que c'est le cas. De même pour state removal.

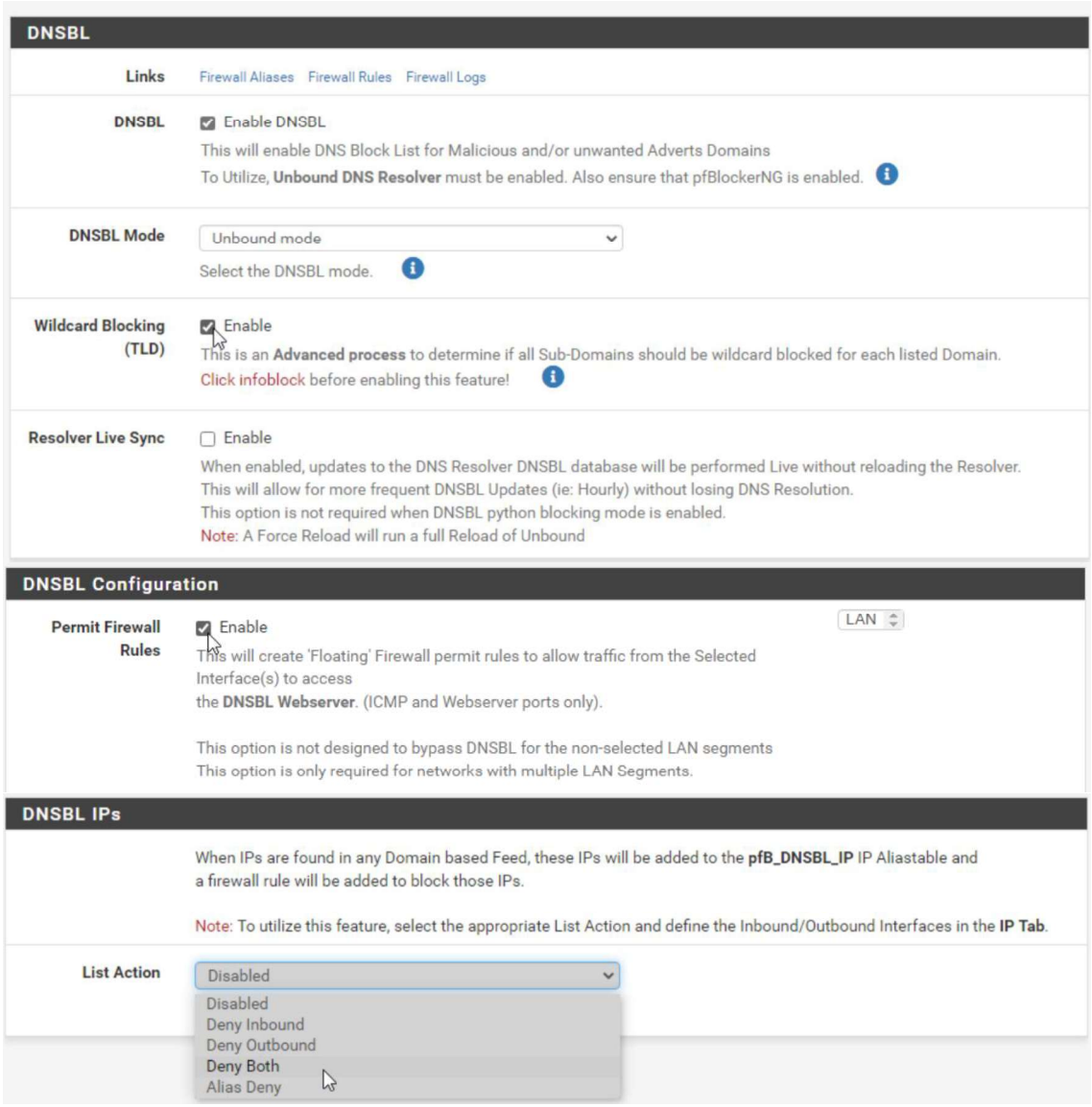


DNSBL

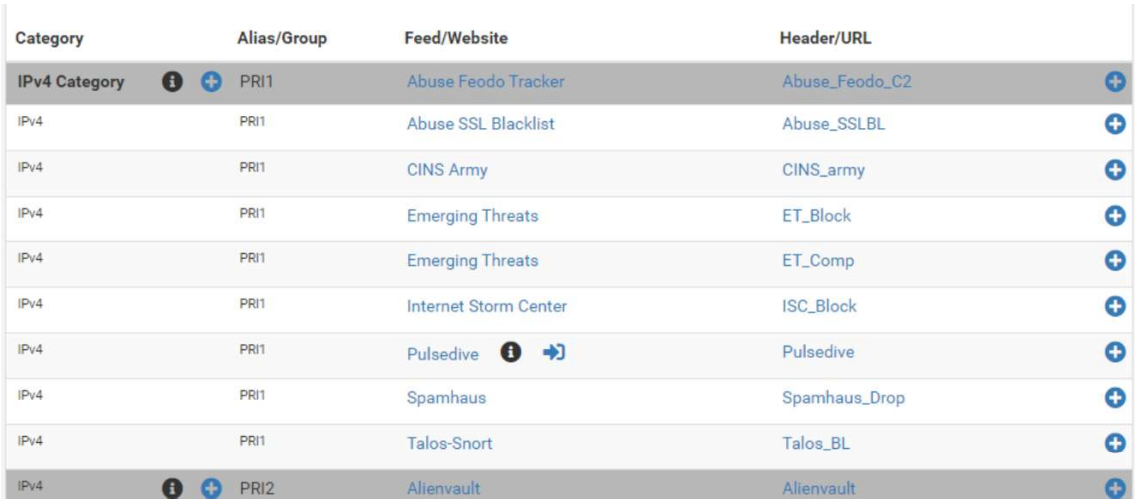
Maintenant la partie DNSBL. Par défaut, lorsqu'il est activé, le packet pfBlockerNG-devel bloque les publicités avec DNSBL comme on peut le voir ci-dessous. Lorsque l'on tente de résoudre un domaine connu pour diffuser de la publicité, pfBlockerNG intercepte via le DNS Resolver et renvoie une fausse adresse locale.



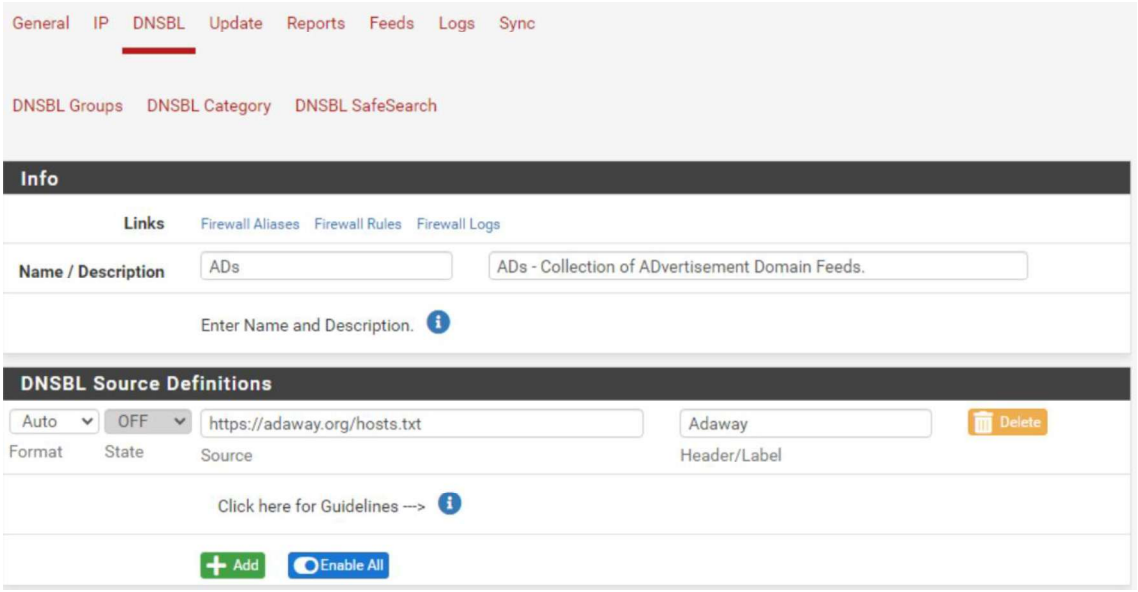
DNSBL sert à bloquer aussi bien les domaines connus pour diffuser de la publicité mais également ceux hébergeant des malwares, ceux connus pour effectuer du phishing et d'autres encore.



Depuis l'onglet feeds, on dispose d'une liste non exhaustive de listes d'IPs et de noms de domaine que l'on peut blacklister. Je viens ajouter les flux qui m'intéressent. Dans un premier temps je vais ajouter AdAway, une très bonne listes en complément de Steven Black pour bloquer les publicités et le tracking.
Lorsque je les sélectionne, cela m'emmène directement dans l'ajout d'une règle DNSBL.

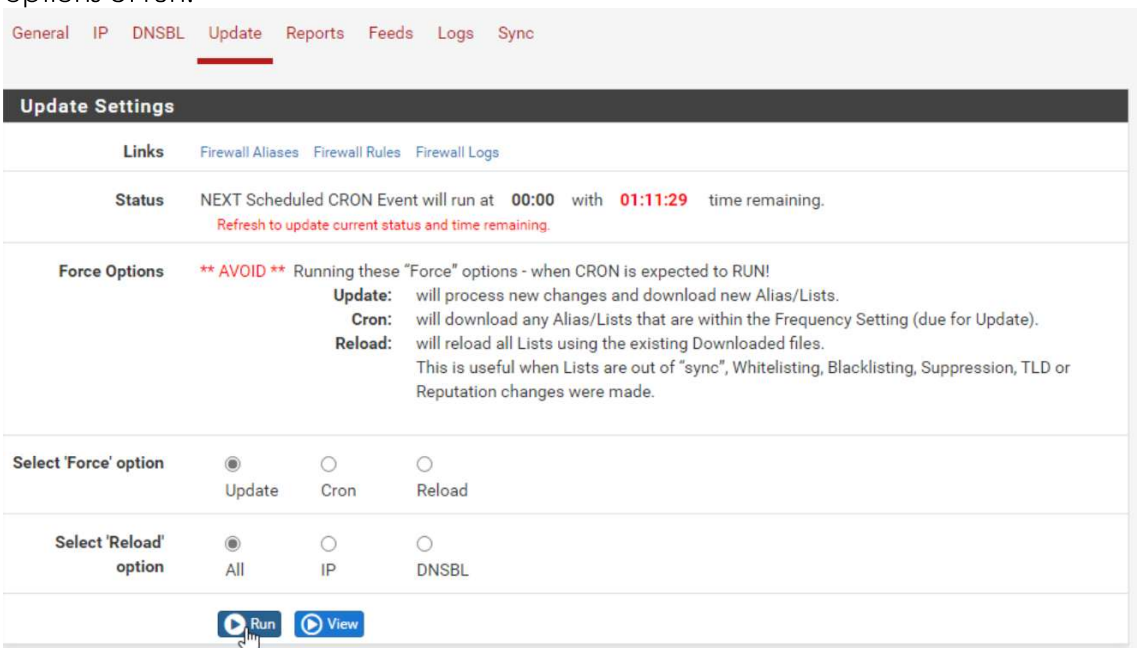


Ici on paramètre donc les actions pour la liste choisie.



Et je viens sélectionner Unbound pour bien rejeter les domaines de la liste.

Une fois les modifications effectuées, on peut se rendre dans Update, choisir les options et run.



2/ Résultats

On voit par exemple, lorsque j'essaye de contacter le domaine ads.google.com, j'ai ce résultat.

Également, dans l'onglet Reports > Alerts, on peut voir tous les domaines bloqués.

DNSBL Block - Last 25 Alert Entries

Date	IF	Source		Domain/Referer|URI|Agent	Feed/Group
Apr 2 21:57:51		10.0.0.100 DESKTOP-N37N6O7		~~www.googletagmanager.com~~ www.googletagmanager.com [~~DNSBL~~ | TLD] DNSBL-Full | -|PRI|HTTP/2.0|-	StevenBlack_ADs DNSBL_ADs_Basic
Apr 2 21:57:40		10.0.0.100 DESKTOP-N37N6O7		srtb.msn.com [DNSBL] DNSBL-Full | -|PRI|HTTP/2.0|-	StevenBlack_ADs DNSBL_ADs_Basic
Apr 2 21:57:37		10.0.0.100 DESKTOP-N37N6O7		c.bing.com [DNSBL] DNSBL-Full | -|PRI|HTTP/2.0|-	StevenBlack_ADs DNSBL_ADs_Basic
Apr 2 21:57:37		10.0.0.100 DESKTOP-N37N6O7		~~sb.scorecardresearch.com~~ sb.scorecardresearch.com [~~DNSBL~~ | TLD] DNSBL-Full | -|PRI|HTTP/2.0|-	StevenBlack_ADs DNSBL_ADs_Basic
Apr 2 21:57:30		10.0.0.100 DESKTOP-N37N6O7		c.bing.com [DNSBL] DNSBL-Full | -|PRI|HTTP/2.0|-	StevenBlack_ADs DNSBL_ADs_Basic
Apr 2 21:57:29		10.0.0.100 DESKTOP-N37N6O7		srtb.msn.com [DNSBL] DNSBL-Full | -|PRI|HTTP/2.0|-	StevenBlack_ADs DNSBL_ADs_Basic
Apr 2 21:42:25		10.0.0.100 DESKTOP-N37N6O7		id5-sync.com [~~DNSBL~~ | TLD] DNSBL-Full | -|PRI|HTTP/2.0|-	StevenBlack_ADs DNSBL_ADs_Basic

On a également la possibilité de whitelist ces domaines en cliquant sur le + si jamais l'un d'entre eux nous est nécessaire.

Activité 6 – Déploiement d'un serveur WEB via Flask pour la veille cyber

Aussi bien pour mon parcours professionnel que pour ce dossier, j'ai choisi de présenter la façon dont je me renseignais sur la cybersécurité. Le problème avec la veille cyber c'est que l'on a énormément d'informations éparpillées, bien souvent plus datée que l'on ne le croit. Pour répondre à ces problématiques, j'ai fait le choix d'héberger sur mon proxmox un site ou plutôt une sorte d'interface web qui fonctionne avec Flask. Ce serveur me permet de regrouper les informations qui m'ont semblées utiles à surveiller, toutes datées et accessibles en un clic. De plus, le fait de pouvoir agrémenter en fonction de mes découvertes aussi simplement est également un gros plus pour l'accessibilité.

1/ Installation des prérequis

Sur une VM Debian 12 Core, je viens donc installer les prérequis suivants.

```
user@veilleweb:~$ sudo apt install -y python3 python3-pip python3-venv git curl
```

Git servira pour un versionning ultérieur et curl servira pour debug et pour certains flux que j'ajouterai également plus tard.

Je viens ensuite créer le dossier qui contiendra les fichiers du projet.

```
user@veilleweb:~$ sudo mkdir -p /opt/veillecyber
```

Et je viens donner les droits à l'utilisateur « user ».

```
user@veilleweb:~$ sudo chown $USER:$USER /opt/veillecyber
```

Dans le dossier veillecyber, je crée l'environnement python.

```
user@veilleweb:/opt/veillecyber$ python3 -m venv venv
```

Et dans l'environnement virtuel, je viens installer requests et flask qui vont me servir respectivement à gérer les requêtes vers les flux et faire fonctionner le site.

```
user@veilleweb:/opt/veillecyber$ source venv/bin/activate
(venv) user@veilleweb:/opt/veillecyber$ pip install requests flask
```

2/ Fichiers de configuration

Le premier fichier qu'il va falloir écrire est « app.py ». C'est celui que l'on va appeler dans l'environnement virtuel pour faire fonctionner le site.

Pour commencer je viens importer les bibliothèques nécessaires pour les fonctions.

```
from flask import Flask, render_template, request
from datetime import datetime, timedelta
import requests, feedparser
```

Je crée ensuite l'app Flask et lui passe « __name__ » pour qu'elle sache où elle se trouve.

```
app = Flask(__name__)
```

Je commence ensuite par déclarer les fonctions de récupération des informations en débutant par la récupération des CVE.

```
def fetch_all_recent_cves(days=30):
    base_url = "https://services.nvd.nist.gov/rest/json/cves/2.0"
    end_date = datetime.utcnow()
    start_date = end_date - timedelta(days=days)

    pub_start = start_date.strftime("%Y-%m-%dT%H:%M:%SZ")
    pub_end = end_date.strftime("%Y-%m-%dT%H:%M:%SZ")

    all_cves = []
    start_index = 0
    results_per_page = 2000

    while True:
        params = {
            "pubStartDate": pub_start,
            "pubEndDate": pub_end,
            "resultsPerPage": results_per_page,
            "startIndex": start_index
        }

        try:
            response = requests.get(base_url, params=params)
            response.raise_for_status()
            data = response.json()
        except Exception as e:
            print("Erreur API NVD :", e)
            break

        results = data.get("vulnerabilities", [])
        all_cves.extend(results)

        total_results = data.get("totalResults", 0)
        start_index += results_per_page

        if start_index >= total_results:
            break
```

Toujours dans la fonction, on trie pour que les plus récentes s'affichent en premier.

```
    all_cves = [cve for cve in all_cves if cve.get("cve", {}).get("published")]

    all_cves.sort(key=lambda c: c["cve"]["published"], reverse=True)


    return all_cves
```

Ensuite la fonction pour les malwares depuis ThreatFox.

```
def fetch_threatfox(limit=100):
    url = "https://threatfox-api.abuse.ch/api/v1/"
    payload = {
        "query": "get_iocs",
        "limit": limit
    }

    try:
        response = requests.post(url, json=payload)
        response.raise_for_status()
        data = response.json()

        if data.get("query_status") != "ok":
            print("Erreur ThreatFox : query_status =", data.get("query_status"))
            return []

        return data.get("data", [])

    except Exception as e:
        print("Erreur API Threatfox :", e)
        return []
```

Et enfin le plus facile, la récupération du flux RSS d'Exploit Database.

```
def fetch_exploits_rss(limit=20):
    url = "https://www.exploit-db.com/rss.xml"
    feed = feedparser.parse(url)
    exploits = []

    for entry in feed.entries[:limit]:
        exploits.append({
            "title": entry.title,
            "link": entry.link,
            "published": entry.published
        })

    return exploits
```

Ensuite je viens déclarer les 4 routes qui sont présentes.

```python
@app.route('/')
def index():
        return render_template('index.html')
```

```python
@app.route('/malwares')
def malwares():
    all_data = fetch_threatfox(limit=100)
    page = int(request.args.get('page', 1))
    per_page = 20

    start = (page - 1) * per_page
    end = start + per_page

    malwares_page = all_data[start:end]
    total_pages = (len(all_data) + per_page - 1) // per_page

    return render_template(
        'malwares.html',
        malwares=malwares_page,
        current_page=page,
        total_pages=total_pages
    )
```

```python
@app.route('/cve')
def cve():
    all_cves = fetch_all_recent_cves(days=30)
    page = int(request.args.get('page', 1))
    per_page = 20
    start = (page - 1) * per_page
    end = start + per_page

    cves_page = all_cves[start:end]
    total_pages = (len(all_cves) + per_page - 1) // per_page

    return render_template(
        'cve.html',
        cves=cves_page,
        current_page=page,
        total_pages=total_pages
    )
```

```python
@app.route("/exploits")
def exploits():
    exploits = fetch_exploits_rss()
    return render_template("exploits.html", exploits=exploits)
```

Pour finir je viens faire un petit debug qui s'affichera lorsqu'on exécutera le fichier.

```python
if __name__ == '__main__':
        app.run(debug=True, host='0.0.0.0')
```

Pour les fichiers html, on va utiliser base.html qui sera appelé dans tous les autres pour afficher l'entête et le pied de page. De plus, pour éviter d'avoir à gérer le CSS (même si je vais parfois le forcer) je viens utiliser simplecss.

```html
<!DOCTYPE html>
<html lang="fr">
<head>
        <meta charset="UTF-8">
        <Title>{{ title or "Veille Cyber"}}</title>
        <link rel="stylesheet" href="https://cdn.simplecss.org/simple.min.css">
</head>
<body>
        <header>
                <h1>Veille Cyber</h1>
                <nav>
                        <a href="/">Accueil</a>
                        <a href="/malwares">Malwares</a>
                        <a href="/cve">CVE</a>
                        <a href="/exploits">Exploits</a>
                </nav>
        </header>

        <main>
                {% block content %}{% endblock %}
        </main>

        <footer>
                <p>© William Troude, Présentation Veille Cyber - 2025.</p>
        </footer>
</body>
</html>
```

Pour la page d'accueil on a.

```html
{% extends "base.html" %}
{% block content %}
<h2>Portail de veille cyber.</h2>
<ul>
        <li><a href="/malwares"> Malwares récents</a></li>
        <li><a href="/cve">Vulnérabilités (CVE)</a></li>
        <li><a href="/exploits">Exploits</a></li>
</ul>
{% endblock %}
```

Pour les CVE on a :

```html
{% extends "base.html" %}

{% block content %}
  <div class="max-w-7xl mx-auto px-4 sm:px-6 lg:px-8 py-8">
    <h1 class="text-3xl font-bold mb-8 text-center">Vulnérabilités récentes (NVD)</h1>

    <div class="overflow-x-auto">
      <table class="min-w-full divide-y divide-gray-700 border border-gray-700">
        <thead class="bg-gray-800">
          <tr>
            <th class="px-6 py-3 text-left text-sm font-medium text-white uppercase tracking-wider">CVE ID</th>
            <th class="px-6 py-3 text-left text-sm font-medium text-white uppercase tracking-wider">Score</th>
            <th class="px-6 py-3 text-left text-sm font-medium text-white uppercase tracking-wider">Description</th>
            <th class="px-6 py-3 text-left text-sm font-medium text-white uppercase tracking-wider">Date</th>
          </tr>
        </thead>
        <tbody class="bg-gray-900 divide-y divide-gray-800">
          {% for cve in cves %}
            <tr>
              <td class="px-6 py-4 whitespace-nowrap">{{ cve.cve.id or 'None' }}</td>
              <td class="px-6 py-4 whitespace-nowrap">
                {% if cve.cve.metrics.cvssMetricV31 %}
                  {{ cve.cve.metrics.cvssMetricV31[0].cvssData.baseScore }}
                {% elif cve.cve.metrics.cvssMetricV30 %}
                  {{ cve.cve.metrics.cvssMetricV30[0].cvssData.baseScore }}
                {% elif cve.cve.metrics.cvssMetricV2 %}
                  {{ cve.cve.metrics.cvssMetricV2[0].cvssData.baseScore }}
                {% else %}
                  N/A
                {% endif %}
              </td>
              <td class="px-6 py-4 whitespace-normal">{{ cve.cve.descriptions[0].value or 'None' }}</td>
              <td class="px-6 py-4 whitespace-nowrap">{{ cve.cve.published[:10] or 'None' }}</td>
            </tr>
          {% endfor %}
        </tbody>
      </table>
    </div>
```

Avec le système de pagination :

```
    <div class="flex justify-center mt-6 space-x-4">
      {% if current_page > 1 %}
        <a href="{{ url_for('cve', page=current_page-1) }}" class="px-4 py-2 bg-gray-700 hover:bg-gray-600 rounded">Précédent</a>
      {% endif %}
      {% if current_page < total_pages %}
        <a href="{{ url_for('cve', page=current_page+1) }}" class="px-4 py-2 bg-gray-700 hover:bg-gray-600 rounded">Suivant</a>
      {% endif %}
    </div>
  </div>
{% endblock %}
```

Pour les malwares :

```
{% extends 'base.html' %}
{% block content %}
  <h2 class="text-3xl font-bold mb-6 text-center">Malwares récents (ThreatFox)</h2>

  <div style="display: flex; justify-content: center;">
    <table style="margin: 0 auto;">
      <thead>
        <tr>
          <th>Malware</th>
          <th>Type</th>
          <th>IOC</th>
          <th>Date</th>
        </tr>
      </thead>
      <tbody>
        {% for malware in malwares %}
          <tr>
            <td>{{ malware.malware }}</td>
            <td>{{ malware.threat_type }}</td>
            <td style="word-break: break-all;">{{ malware.ioc }}</td>
            <td>{{ malware.first_seen }}</td>
          </tr>
        {% endfor %}
      </tbody>
    </table>
  </div>
```

Avec également une pagination.

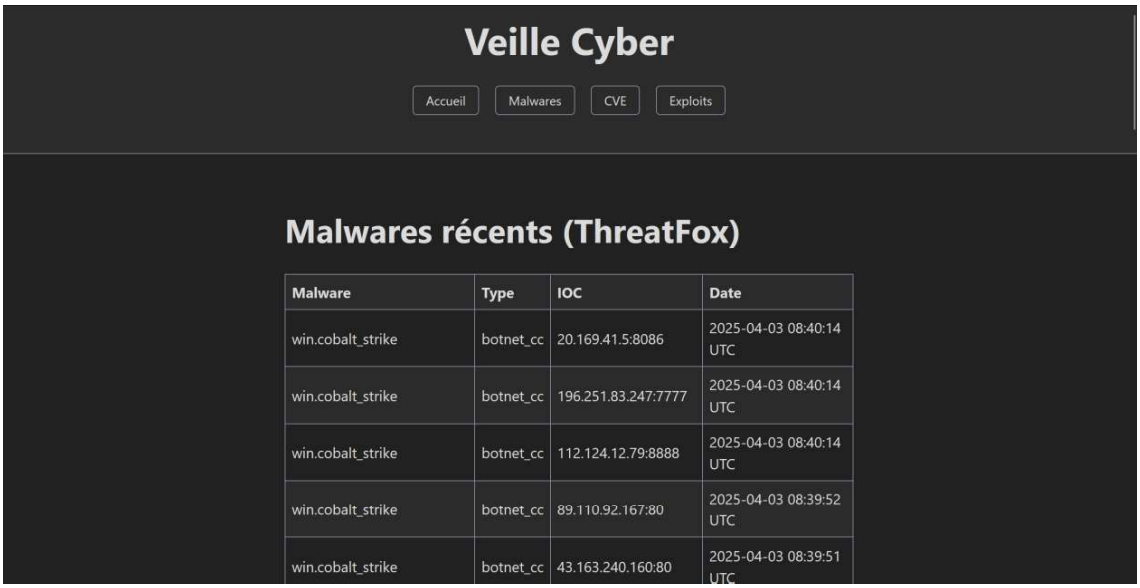
```
  <div class="flex justify-center mt-6 space-x-2">
    {% if current_page > 1 %}
      <a href="?page={{ current_page - 1 }}" class="px-3 py-1 border rounded">&laquo; Préc</a>
    {% endif %}

    {% for page_num in range(1, total_pages + 1) %}
      {% if page_num == current_page %}
        <span class="px-3 py-1 border rounded bg-gray-700">{{ page_num }}</span>
      {% else %}
        <a href="?page={{ page_num }}" class="px-3 py-1 border rounded">{{ page_num }}</a>
      {% endif %}
    {% endfor %}

    {% if current_page < total_pages %}
      <a href="?page={{ current_page + 1 }}" class="px-3 py-1 border rounded">Suiv &raquo;</a>
    {% endif %}
  </div>

{% endblock %}
```

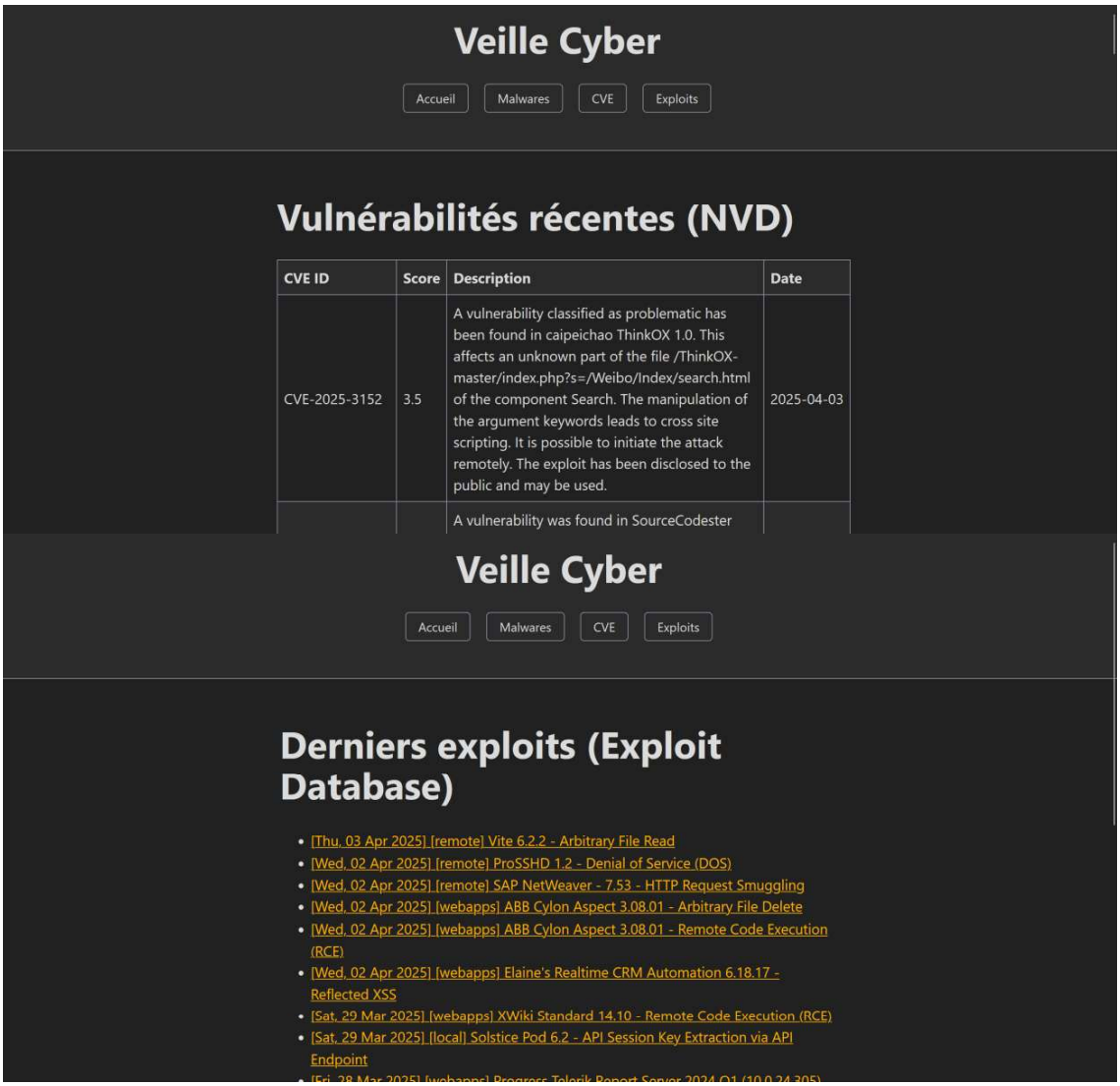
Et pour les exploits :

```
{% extends "base.html" %}

{% block content %}
  <div class="max-w-4xl mx-auto px-4 py-8">
    <h1 class="text-3xl font-bold mb-6 text-center">Derniers exploits (Exploit Database)</h1>

    {% if exploits %}
      <ul class="space-y-4">
        {% for exploit in exploits %}
          <li class="border-b border-gray-700 pb-2">
            <a href="{{ exploit.link }}" target="_blank" class="text-blue-400 hover:underline">
              [{{ exploit.published[:16] }}] {{ exploit.title }}
            </a>
          </li>
        {% endfor %}
      </ul>
    {% else %}
      <p class="text-center text-gray-400">Aucun exploit trouvé.</p>
    {% endif %}
  </div>
{% endblock %}
```

3/ Rendu


Veille Cyber
Accueil
Malwares
CVE
Exploits
Portail de veille cyber.
Malwares récents
Vulnérabilités (CVE)
Exploits
© William Troude, Présentation Veille Cyber - 2025.


Veille Cyber
Accueil
Malwares
CVE
Exploits
Malwares récents (ThreatFox)
Malware
Type
IOC
Date
win.cobalt_strike
botnet_cc
20.169.41.5:8086
2025-04-03 08:40:14 UTC
win.cobalt_strike
botnet_cc
196.251.83.247:7777
2025-04-03 08:40:14 UTC
win.cobalt_strike
botnet_cc
112.124.12.79:8888
2025-04-03 08:40:14 UTC
win.cobalt_strike
botnet_cc
89.110.92.167:80
2025-04-03 08:39:52 UTC
win.cobalt_strike
botnet_cc
43.163.240.160:80
2025-04-03 08:39:51 UTC


Veille Cyber
Accueil
Malwares
CVE
Exploits
Vulnérabilités récentes (NVD)
CVE ID
Score
Description
Date
CVE-2025-3152
3.5
A vulnerability classified as problematic has been found in caipeichao ThinkOX 1.0. This affects an unknown part of the file /ThinkOX-master/index.php?s=/Weibo/Index/search.html of the component Search. The manipulation of the argument keywords leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.
2025-04-03
A vulnerability was found in SourceCodester
Veille Cyber
Accueil
Malwares
CVE
Exploits
Derniers exploits (Exploit Database)
[Thu, 03 Apr 2025] [remote] Vite 6.2.2 - Arbitrary File Read
[Wed, 02 Apr 2025] [remote] ProSSHD 1.2 - Denial of Service (DOS)
[Wed, 02 Apr 2025] [remote] SAP NetWeaver - 7.53 - HTTP Request Smuggling
[Wed, 02 Apr 2025] [webapps] ABB Cylon Aspect 3.08.01 - Arbitrary File Delete
[Wed, 02 Apr 2025] [webapps] ABB Cylon Aspect 3.08.01 - Remote Code Execution (RCE)
[Wed, 02 Apr 2025] [webapps] Elaine's Realtime CRM Automation 6.18.17 - Reflected XSS
[Sat, 29 Mar 2025] [webapps] XWiki Standard 14.10 - Remote Code Execution (RCE)
[Sat, 29 Mar 2025] [local] Solstice Pod 6.2 - API Session Key Extraction via API Endpoint

4/ Conclusion

Cette interface était assez solide mais trop simple pour réunir une masse d'informations sur la veille cyber. Le plus intéressant reste la partie exploits. Pour les CVE j'essaye actuellement sur une autre version de rendre l'utilisation plus efficace avec plus d'informations. De plus, il manque des articles qui sont intéressants pour la veille et une interface plus agréable.
Je suis donc en train de travailler sur une nouvelle version que j'ai appelée Argosys en référence à Argos Panoptes, le géant aux cent yeux. Cette fois-ci j'utilise bootstrap pour le CSS. Le site inclut une page d'accueil avec des articles, les CVE critiques récents et pareil pour les malwares (c'est encore en cours de réalisation). Cela me permet à la fois de travailler sur la mise en service d'un serveur WEB tout en me permettant d'effectuer une veille sur la cybersécurité.