

# Livrable 1 :

## *Administration du Système d'Information*



# Sommaire

I.	Résumé .....	2
II.	Introduction .....	2
1.	<i>Contexte</i> .....	2
2.	<i>Problématique</i> .....	2
III.	Cartographie du Système Existant.....	2
IV.	Propositions .....	5
V.	Détection de l'Annuaire .....	7
VI.	Schématisation du nouveau Système d'Information.....	9
VII.	Conclusion.....	10

# I. Résumé

En résumé, nous allons étudier le système existant, proposer des solutions de sécurité pour le renforcer, et élaborer une nouvelle cartographie du système d'information.

# II. Introduction

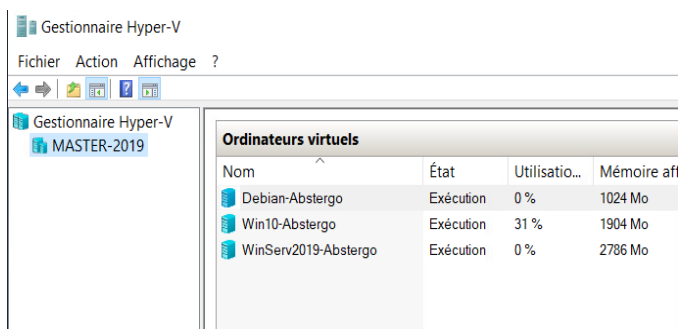
## Contexte

L'entreprise ABSTERGO cherche à améliorer son infrastructure. Pour faire ceci, nous devons d'abord comprendre et documenter son infrastructure existante. Nous proposerons ensuite des solutions pour améliorer cette dernière.

## Problématique

Quelles sont les limites du système informatique chez ABSTERGO et que pouvons-nous faire pour l'améliorer ?

# III. Cartographie du Système Existant

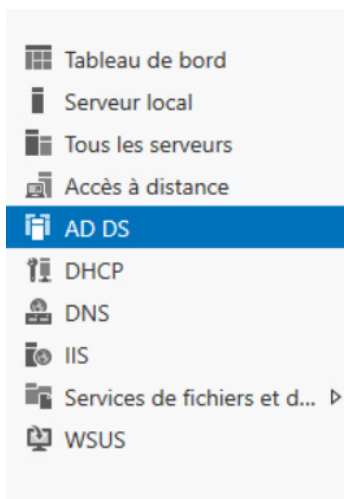


The screenshot shows the Hyper-V Manager window. On the left, the 'Gestionnaire Hyper-V' tree is expanded to show 'MASTER-2019'. The main pane displays a table titled 'Ordinateurs virtuels' with the following data:

Nom	État	Utilisatio...	Mémoire aff
Debian-Abstergo	Exécution	0 %	1024 Mo
Win10-Abstergo	Exécution	31 %	1904 Mo
WinServ2019-Abstergo	Exécution	0 %	2786 Mo

Figure 1: Liste des machines

Nous observons que le Système existant est décrit de trois machines virtuelles : une sous Windows Server 2019 « WinServ2019-Abstergo », une sous Windows 10 « Win10-Abstergo » et la dernière sous Linux Server « Debian-Abstergo ». Ces machines sont reliées entre elles grâce au SWITCH virtuel « LAN-Abstergo ».



Dans un premier temps, nous voyons que la machine Windows Server 2019 « WinServ2019-Abstergo » contient le serveur « SRV-WIN-01 » qui est le serveur principal. Elle a pour rôles l'AD DS, le DNS, le DHCP, le IIS, le WSUS et les Services de fichiers et de stockages :

- **AD DS** (Active Directory Domain Services) : Service de gestion d'annuaire utilisé pour gérer et organiser les ressources réseau, notamment les utilisateurs, les groupes, les ordinateurs, les imprimantes et autres objets réseau. L'AD DS est au cœur de la gestion de l'authentification, de l'autorisation, de la sécurité et de la gestion des ressources au sein d'un réseau Windows.

- **DNS** (Domain Name System) : Service informatique distribué qui associe les noms de domaine Internet avec leurs adresses IP ou d'autres types d'enregistrements. Il permet de résoudre les noms d'ordinateurs en adresses IP et facilite l'identification des ressources réseau au sein du domaine.

Figure 2: Rôles du serveur "SRV-WIN-01"

- **DHCP** (Dynamic Host Configuration Protocol) : Protocole de réseau qui permet aux ordinateurs et aux autres appareils connectés à un réseau IP (Internet Protocol) d'obtenir automatiquement une configuration réseau, y compris une adresse IP, un masque de sous-réseau, une passerelle par défaut et les serveurs DNS, sans avoir besoin d'une configuration manuelle. Il simplifie grandement le processus de configuration des appareils sur un réseau en attribuant automatiquement les informations de réseau nécessaires.
- **IIS** (Internet Information Services) : Logiciel de serveur web développé par Microsoft. L'IIS est conçu pour fonctionner sur les systèmes d'exploitation Windows, et il est utilisé pour héberger des sites web et des applications web sur des serveurs Windows. L'IIS est principalement un serveur web, ce qui signifie qu'il gère les requêtes HTTP et HTTPS et répond aux demandes des navigateurs web en fournissant des pages web, des fichiers, des services web, des applications web, et d'autres contenus en ligne.
- **WSUS** (Windows Server Update Service) : Application serveur développée par Microsoft qui permet aux administrateurs de systèmes informatiques de gérer la distribution des mises à jour de logiciels Microsoft aux ordinateurs clients exécutant des systèmes d'exploitation Windows au sein d'un réseau. C'est un outil essentiel pour les administrateurs de systèmes Windows qui souhaitent maintenir leurs réseaux en conformité avec les mises à jour de sécurité et autres mises à jour logicielles de Microsoft. Il simplifie le processus de gestion des mises à jour et contribue à renforcer la sécurité et la stabilité des systèmes.

- **Services de fichiers et de stockages :** Fonctionnalité intégrée au système d'exploitation Windows Server de Microsoft. Ils fournissent un ensemble de services et de fonctionnalités permettant de gérer et de stocker des données sur un réseau d'entreprise. Ils fournissent une infrastructure complète pour la gestion, le partage, la protection et la disponibilité des données sur un réseau d'entreprise. Ils sont essentiels pour les entreprises qui doivent gérer de grandes quantités de données de manière fiable et sécurisée.

« WinServ2019-Abstergo » est également équipée d'un Pare-feu Windows Defender et se connecte à internet grâce au « WAN-Abstergo » de IPv4 attribuée par un serveur DHCP externe.

D'autre part, nous avons la machine « Win10-Abstergo ». Celle-ci contient le poste de travail d'un des employés de l'entreprise Abstergo Pierre Morin.

Enfin, la machine « Debian-Abstergo » est un Serveur WEB. Celle-ci stocke les fichiers nécessaires au fonctionnement des sites web qu'utilise Abstergo. Le serveur sert des pages HTML et centralise la réécriture d'URL, les certifications SSL, une base de données MariaDB et les langages de programmation. Nous accédons aux données en donnant des instructions à l'invite de commande Linux.

Nous pouvons modéliser le Système d'Information ainsi :

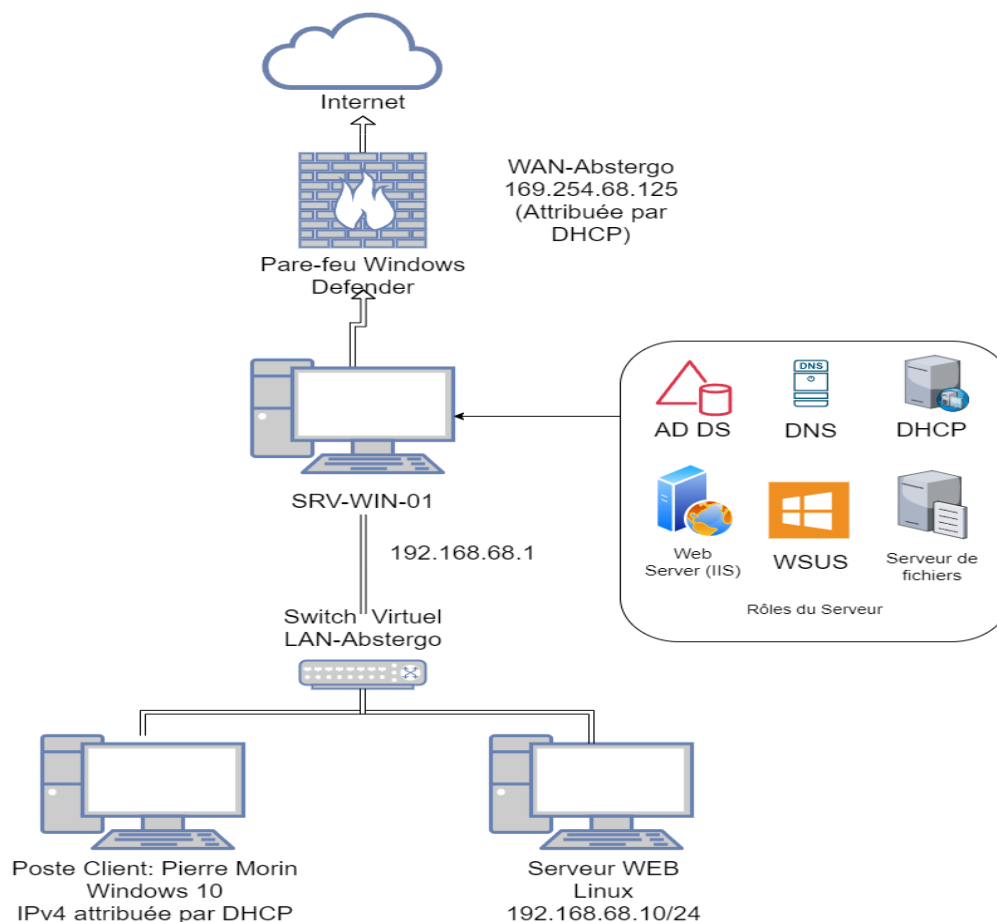


Figure 3: Cartographie du S.I existant

## IV. Propositions



Source de figure: The importance of Auditing the Active Directory Services – Kiban

1. **Effectuer des Audits Réguliers de votre Environnement AD** : Commencez par des audits fréquents de votre Active Directory pour détecter les comptes d'utilisateurs non conformes, non autorisés, ou avec des privilèges inappropriés. Ceci permet une approche proactive pour appliquer des correctifs.
2. **Appliquer le Principe du Moindre Privilège** : Restreignez les droits à haut privilège aux utilisateurs légitimes, en particulier aux administrateurs du domaine et de l'entreprise. Cela réduit les risques d'infiltration et garantit que chaque employé ait les privilèges nécessaires à son travail.
3. **Gestion des Comptes Privilégiés** : Les comptes à privilèges doivent être protégés avec des mesures de sécurité renforcées, telles que l'authentification multifactor. Ces accès ne doivent pas être permanents et doivent être réexaminés régulièrement.
4. **Sécurisation des Contrôleurs de Domaine** : Protégez au maximum les contrôleurs de domaine en les plaçant dans des environnements sécurisés. Utilisez la dernière version de Windows Server et déployez une configuration sécurisée initiale grâce aux objets de stratégie de groupe.
5. **Mise en Place d'une Politique de Mot de Passe** : Établissez une politique de mot de passe qui exige des mots de passe complexes, la confidentialité des mots de passe, l'utilisation d'identifiants différents pour différents services, et, si nécessaire, une authentification forte.



Source de figure : Quelle est le meilleur antivirus à choisir en 2023 -20minutes.fr

6. **Installation d'Antivirus sur les Postes de Travail** : Installez et maintenez à jour vos logiciels antivirus pour protéger votre système contre les vulnérabilités. Surveillez également les suppressions ou désactivations de ces outils.

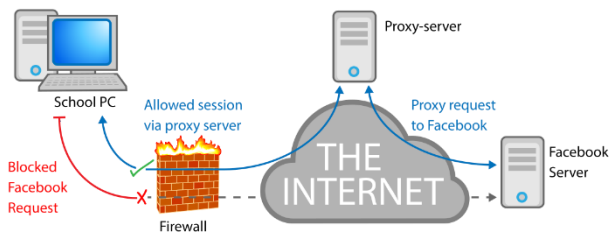
7. **Effectuer des Sauvegardes Régulières** : Effectuez des sauvegardes régulières de votre AD sur plusieurs emplacements, y compris un support amovible. Effectuez des tests sur ces sauvegardes pour garantir une récupération rapide en cas de problème.



Source de figure: futura-sciences.com

8. **Ajouter d'un Serveur de Messagerie** : Reprenez le contrôle total sur votre messagerie électronique. Protégez la confidentialité de vos communications et filtrez les courriels indésirables en ayant une liaison plus rapide et efficace.

9. **Ajouter un Serveur Proxy** : Protégez vos applications web contre les cyber-attaques avec les fonctionnalités de pare-feu applicatif web (WAF) du proxy. Bloquez également l'accès aux sites web et aux logiciels malveillants en filtrant et en surveillant le trafic.



Source de figure : Qu'est-ce qu'un proxy ? – proxyvpn.fr

## V. Détection de l'Annuaire

Nous accédons au contrôleur de domaine « SRV-WIN-01 ». Dans celui-ci nous remarquons qu'il y a un domaine nommé « ABSTERGO.INTERNAL » où, en dehors des conteneurs pré-instaurés, est placé l'Unité d'Organisation « utilisateurs.Abstergo ». A l'intérieur de celle-ci on retrouve une autre Unité d'Organisation « Comptabilité » qui contient un Utilisateur « Pierre Morrin » rattaché au poste de travail « Win10-Abstergo ».

Nous trouvons également une GPO « Raccourcis-Utilisateurs » dans l'Unité d'Organisation « utilisateurs.Abstergo » qui crée un raccourci sur le Bureau des personnes concernées qui permet d'accéder à la ERP Dolibarr.

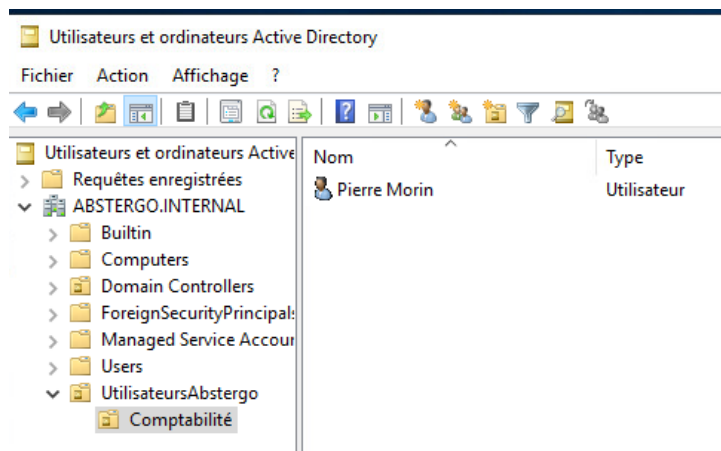


Figure 4: Domaine ABSTERGO.INTERNAL



Figure 5: GPO "Raccourcis-Utilisateurs"



Voilà comment nous modélisons l'Active Directory :

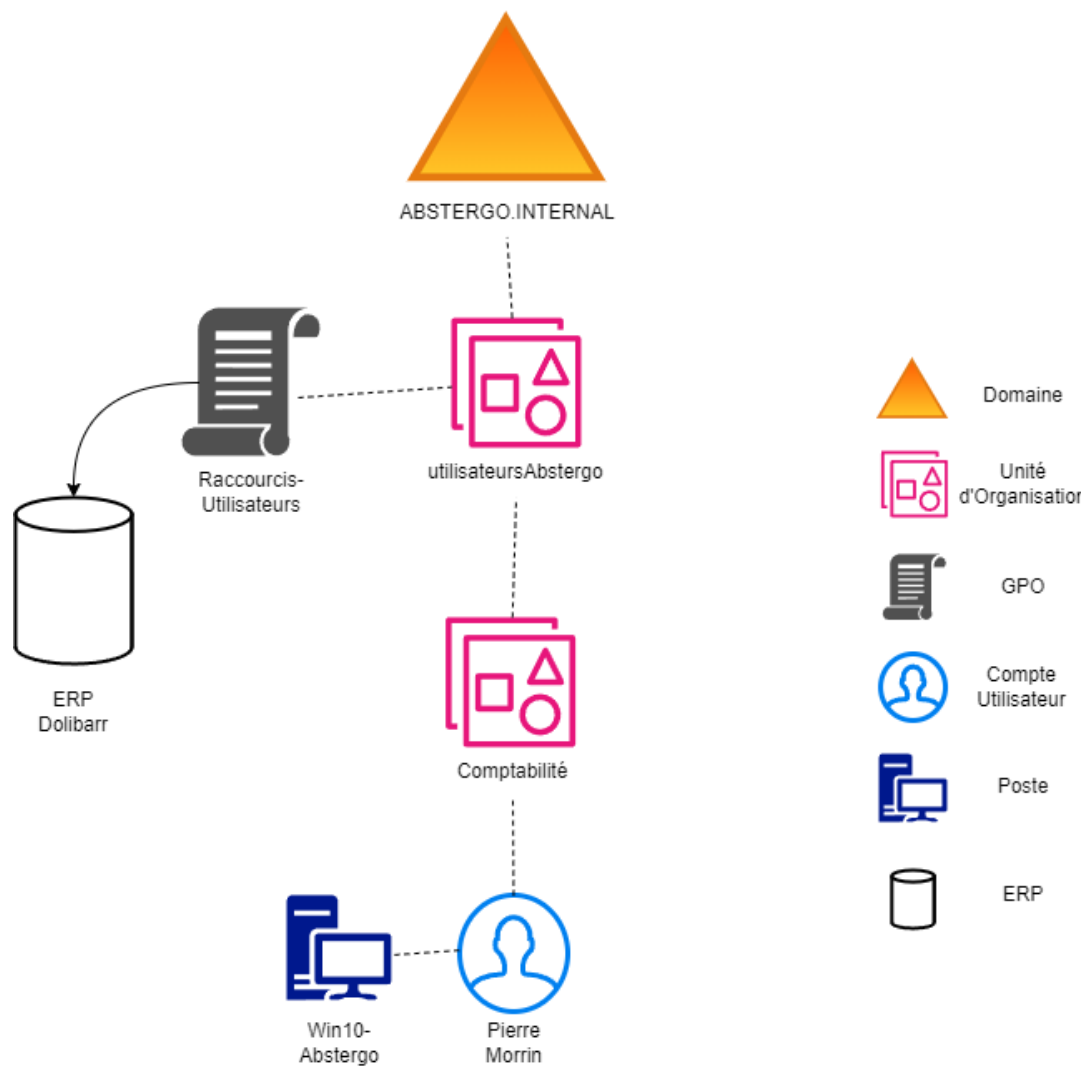


Figure 6: Cartographie de l'Active Directory

## VI. Schématisation du nouveau Système d'Information

Nous ajoutons alors au Système d'Information existant le rôle de serveur de messagerie et nous établissons un lien avec un Serveur Proxy.

Nous obtenons alors le nouveau Système d'Information ci-dessous :

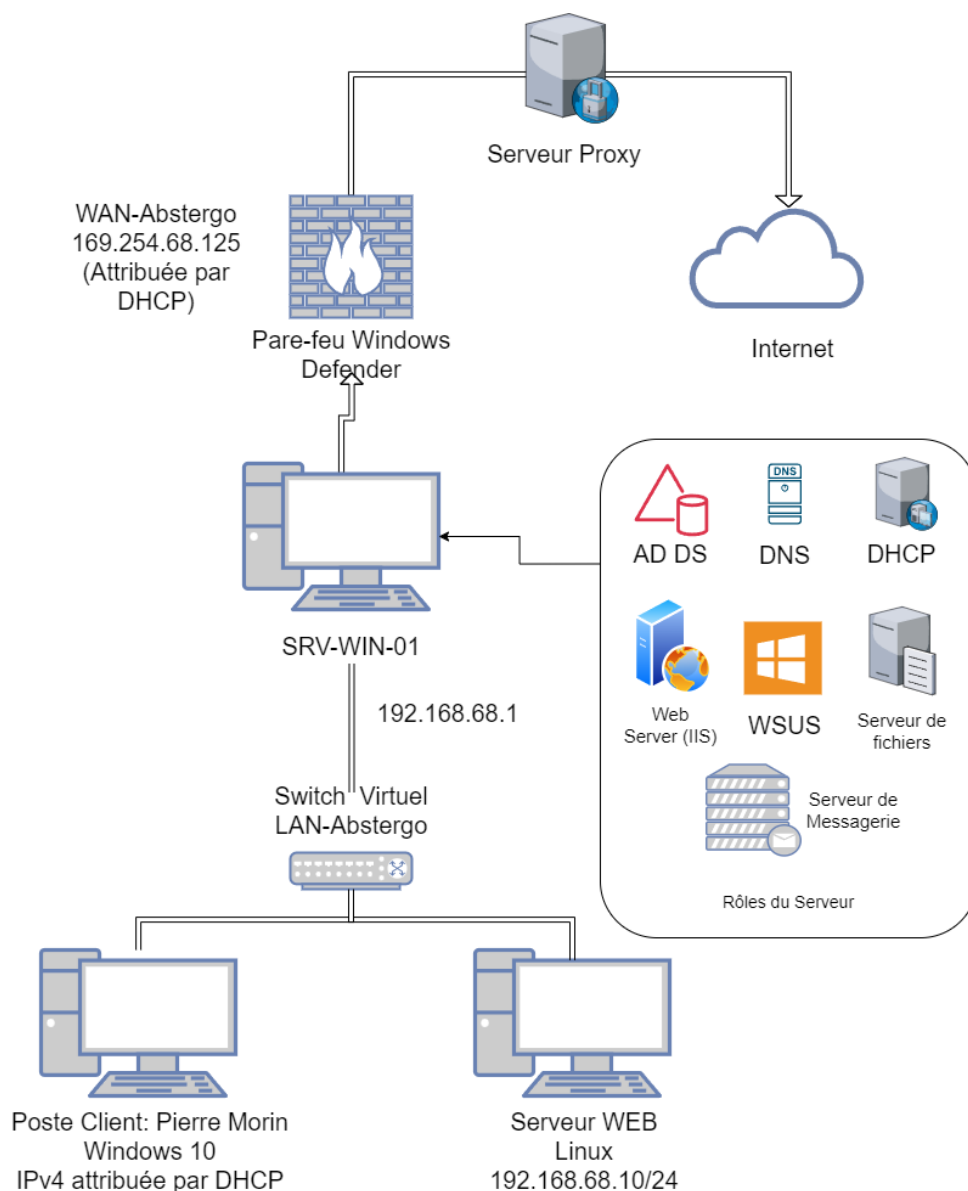


Figure 7: Cartographie du Nouveau Système d'Information

Nous ajoutons également un antivirus sur les postes de travail et une politique de mot de passe plus exigeante. Nous pouvons faire ceci avec l'application des GPO sur l'Unité d'Organisation « utilisateurs-Abstergo ».

Nous obtenons alors ce nouveau Active Directory :

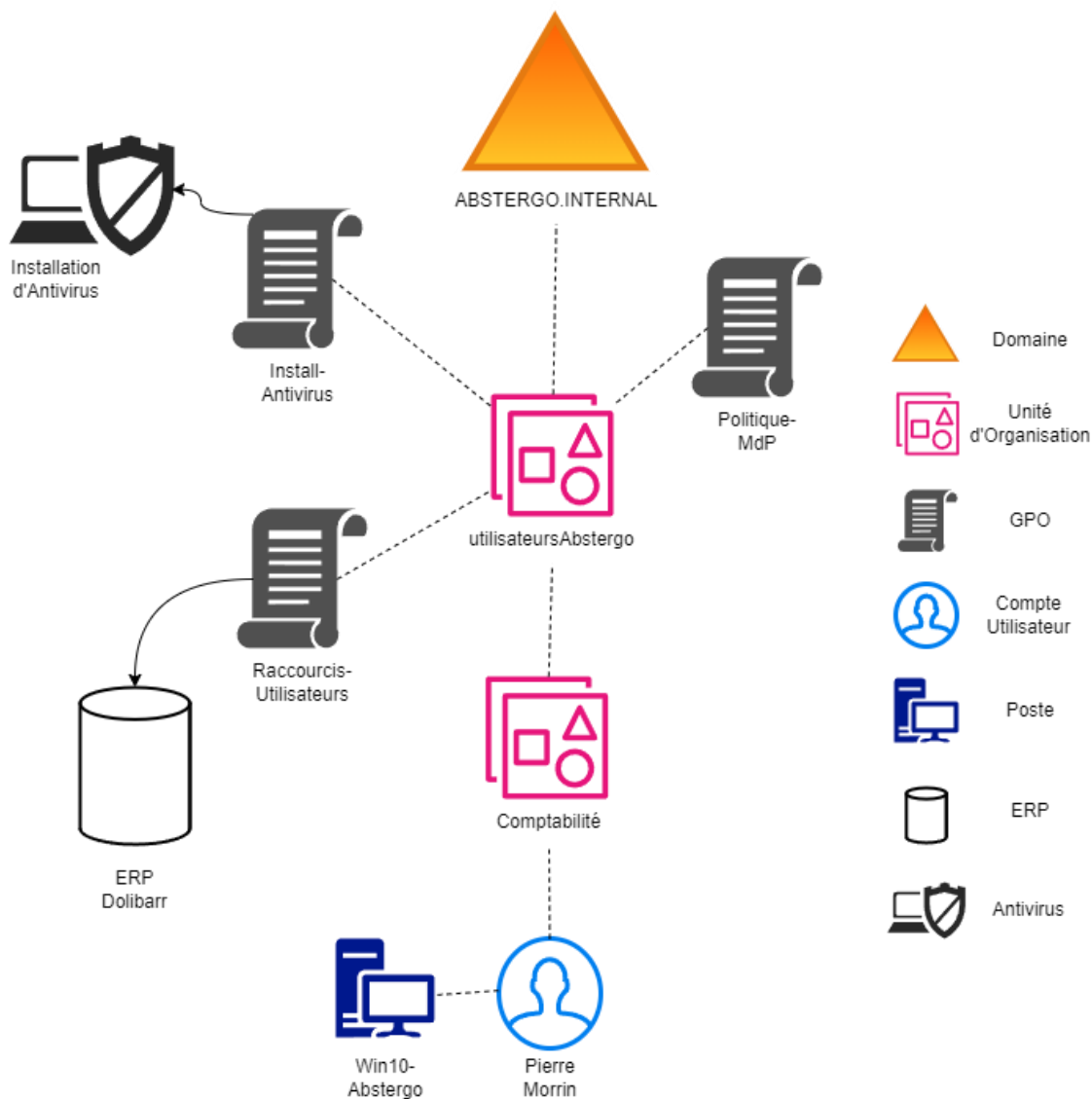


Figure 8: Cartographie du Nouveau Active Directory

## VII. Conclusion

### Bilan de groupe

Dans ce livrable, nous avons travaillé en groupe pour étudier l'Active Directory Abstergo au sein du Digitlab. Nous avons débuté par une observation de l'existant, réalisé une étude du système d'information, et élaboré une cartographie en vue d'améliorer le système en proposant des solutions de sécurité et une nouvelle cartographie.

## Bilan Personnel

J'ai étudié le système d'information et pris des notes sur l'existant en vue de réaliser la cartographie que nous avons élaborée ensemble. J'ai également effectué des captures d'écran de l'existant et recherché des méthodes pour améliorer ce système d'information en utilisant les solutions que nous avons déjà mentionnées afin de faire la nouvelle cartographie.

J'ai amélioré mes compétences techniques pour manipuler le système d'information de manière plus efficace, ainsi que mes compétences pour travailler en groupe.