



PROJET ANIMUS EXTENDUS

Livrable 2

Groupe 2



Florian Brochot

Hugo Laplace

Table des matières

Répartition des tâches.....	3
Contexte	3
Problématique.....	4
Rappel livrable 1	4
Objectif livrable 2	5
Authentification.....	6
Virtualisation	7
Supervision	8
Politique de Sauvegarde.....	9
Schéma du réseau	10
Organisations des utilisateurs ADDS et OU	13
Sécurité.....	14
Scripting.....	15
Premier script	15
Deuxième script.....	15
Troisième script	15
Conclusion	16

Répartition des tâches

En amont du projet, nous avons établi une liste pour la répartition des tâches en fonction des préférences de chacun. Elle a été conçue de manière que chaque membre du groupe ait le même nombre de tâches à effectuer pour les livrables 2 et 3.

Livable 2	Authentification	Virtualisation	Supervision	Sauvegarde	Schéma	Scripts
Brochot Florian		X	X	X		X
Laplace Hugo	X	X	X		X	X

X	doit faire
	ne doit pas faire
	a fait
	a pas fait
	entraîn de faire

Dernière actualisation le 13/11 à 15h52.

Contexte

ABSTERGO est une PME fondée en 1981, spécialisée dans la conception de capteurs et de solutions IoT. Elle compte parmi ses clients de grands groupes automobiles et envisage de se développer en ligne en se lançant dans le B2C. L'entreprise emploie 100 personnes réparties sur 6 services.

ABSTERGO possède un site distant à Lyon, où se trouvent 15 employés du service R&D. Cependant, cette entité connaît des difficultés depuis quelques années en raison de mauvaises décisions.

Récemment, des rumeurs circulent au sein d'ABSTERGO selon lesquelles la direction envisage de se rapprocher du grand groupe ANIMUS.

Suite à cette nouvelle, plusieurs employés, dont l'administrateur système et le technicien du support utilisateur, ont démissionné.

Problématique

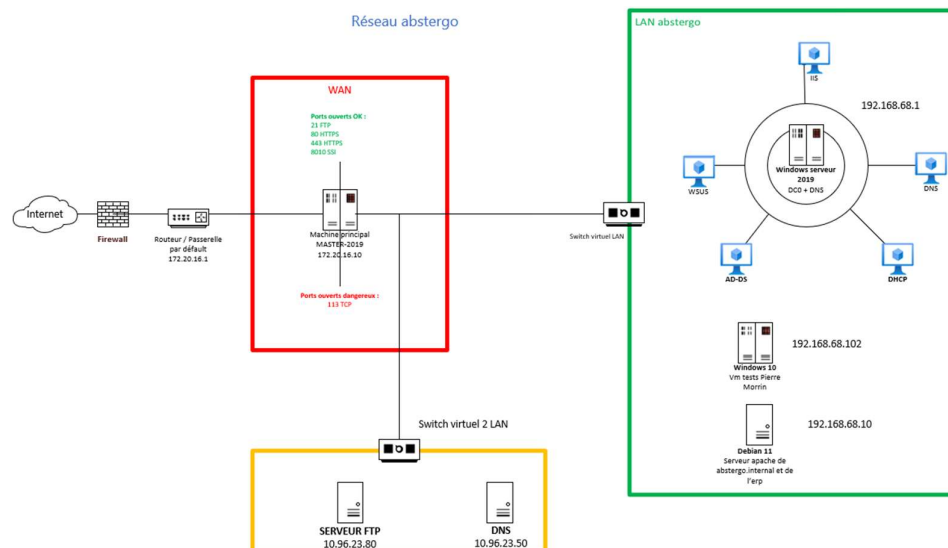
Nous avons donc été embauchée par ABSTERGO avec pour mission de comprendre l'infrastructure de l'entreprise, de la documenter, de l'améliorer et de mettre en œuvre des bonnes pratiques. Tout cela doit être réalisé dans un délai court, car la société s'est engagée dans une démarche de certification qualité ISO 9001. Un audit est prévu dans moins de 2 mois, et le système d'information fait partie du périmètre de la norme.

L'obtention de cette certification est cruciale.



Rappel livrable 1

L'objectif de ce premier livrable été d'effectuer une analyse du système existant et d'en faire une cartographie. Mais également de faire un état des lieux sur la gestion des identités et l'accès aux données de l'entreprise. Nous avons abouti sur le schéma ci-dessous.



Objectif livrable 2

L'objectif de ce second livrable est d'expliquer le plan concernant la nouvelle infrastructure qui sera présenté dans la semaine, nous allons ici présenter tout ce qui sera présent sur la maquette et de justifier nos choix notamment en termes de sécurité.

Authentification

Kerberos est un protocole d'authentification réseau qui assure la sécurité des échanges entre utilisateurs et services sur un réseau. Au cœur de son fonctionnement se trouve le concept de tickets. Lorsqu'un utilisateur s'authentifie, le serveur d'authentification lui délivre un "Ticket Granting Ticket" (TGT). Ce TGT est ensuite utilisé pour obtenir des "tickets de service" spécifiques à chaque service auquel l'utilisateur souhaite accéder.



Les tickets (plus souvent appelés certificats) sont des informations cryptées attestant de l'identité de l'utilisateur et contenant des clés de session pour sécuriser les communications. L'utilisateur présente son TGT au serveur de tickets, qui délivre un ticket de service pour le service demandé. Ces tickets ont une durée de validité limitée, réduisant les risques en cas de compromission. La cryptographie des tickets renforce la sécurité en garantissant que seuls les utilisateurs authentiques peuvent accéder aux services concernés.

Comparé à d'autres solutions comme OAuth, Kerberos se distingue par son approche spécialisée dans l'authentification réseau. Son architecture centralisée et son utilisation efficace des tickets en font une solution plus robuste et sécurisée. Ainsi, la combinaison de l'utilisation de tickets, de leur cryptographie et de l'architecture spécifique de Kerberos en fait une solution d'authentification réseau supérieure dans de nombreux contextes. Il a aussi l'avantage d'être assez peu coûteux ce qui n'est pas négligeable dans le cas d'Abstergo.

De par cette analyse c'est tout naturellement que notre choix s'est porté sur la solution Kerberos.

Virtualisation

Pour la virtualisation au sein de notre entreprise ABSTERGO, nous avons choisi d'utiliser la solution de supervision de Windows Server : Hyper-V. Notre choix a été principalement justifié par le fait qu'Hyper-V est bien intégré dans l'écosystème Windows, ce qui facilite la gestion pour les administrateurs familiers avec Windows. Il offre également des fonctionnalités avancées de sauvegarde, de reprise après sinistre et de compatibilité avec les applications Windows. Notre choix a été principalement justifié par le fait qu'une PME comme ABSTERGO ne possède pas de moyens financiers colossaux et possède également de nombreux appareils sous Windows.



Un autre système de virtualisation populaire est Docker. Docker est une plateforme de conteneurisation qui offre une virtualisation légère, rapide et efficace. Il permet d'encapsuler des applications et leurs dépendances dans des conteneurs, offrant ainsi une grande flexibilité pour le déploiement d'applications. Docker est particulièrement adapté aux environnements de développement et de déploiement d'applications, permettant des mises à jour rapides et une gestion efficace des ressources. Cependant, il est important de noter que Docker est plus axé sur la virtualisation au niveau de l'application, tandis que Hyper-V se concentre sur la virtualisation au niveau de la machine virtuelle ce qui offre une isolation plus stricte entre les environnements, pour cette raison Hyper-V est considéré comme plus sécurisé que Docker.

Au-delà de ça, Docker ne peut virtualiser que des conteneurs sur le même système d'exploitation que le système hôte. Concrètement, un Docker sur Debian aura tous ses conteneurs basés sur Debian. Dans notre cas, il nous faudra un client Windows et un Linux, ce qui ne peut pas être fait avec un Docker.

Un autre système de virtualisation populaire est KVM (Kernel-based Virtual Machine). KVM est une solution open source qui offre une virtualisation légère, performante et évolutive. Elle est idéale pour les environnements Linux et offre une grande flexibilité pour les charges de travail variées. Cependant, sa gestion peut nécessiter des compétences techniques plus avancées, ce qui peut constituer un défi pour certaines PME. KVM reste un choix intéressant pour une PME orientée vers Linux.

Pour une PME qui utilise principalement des systèmes Windows, Hyper-V est un choix logique en raison de son intégration native avec l'environnement Windows, offrant une gestion simplifiée et des fonctionnalités avancées pour garantir la disponibilité des services.

Supervision

Dans le cas d'Habstergo, nous avons envisagé d'utiliser Centreon, un système de supervision open source robuste et polyvalent qui présente de nombreux avantages pour une PME comme la nôtre.



Tout d'abord, il offre une large compatibilité avec une variété de systèmes d'exploitation et d'applications, ce qui en fait une solution adaptée à un environnement informatique diversifié comme le nôtre (avec plusieurs systèmes d'exploitation). Il permet de surveiller les performances, la disponibilité et l'état de l'ensemble de l'infrastructure, des serveurs aux réseaux, en passant par les applications.

En outre, Centreon propose une interface web conviviale et une configuration flexible qui facilite la personnalisation des alertes et des rapports. Cela permet aux administrateurs de surveiller les éléments essentiels pour l'entreprise, de réagir rapidement aux problèmes potentiels et d'optimiser les performances du réseau. La création de tableaux de bord personnalisés permet de visualiser rapidement l'état du système et de prendre des décisions éclairées.

Enfin, en tant que solution open source, Centreon offre un coût d'entrée abordable pour une société de notre taille, car elle ne nécessite pas de licences coûteuses. Elle est également soutenue par une communauté active, ce qui signifie que les mises à jour et les correctifs de sécurité sont régulièrement disponibles.

Nous avons également envisagé d'utiliser Nagios, un système de supervision open source bien établi avec une grande flexibilité pour la configuration. Il dispose d'une bibliothèque de plugins étendue pour surveiller divers types d'équipements et d'applications. Cependant, il peut nécessiter plus d'efforts de configuration par rapport à Centreon.

Politique de Sauvegarde

Un script permettant la sauvegarde automatisée sera mis en place par l'administrateur. Ce script enverra une confirmation à chaque fois qu'une sauvegarde sera effectuée avec succès. En cas de non-réception de cette confirmation, l'administrateur devra effectuer une vérification manuelle et intervenir si besoin.

Pour commencer, il nous faut déterminer la fréquence à laquelle les données seront sauvegardées. Comme nous sommes dans le cas d'une entreprise, on peut envisager d'effectuer une sauvegarde complète une fois par semaine (le vendredi soir, car personne ne travaille le samedi). Une sauvegarde différentielle, qui enregistrera les nouvelles données, sera effectuée deux fois par jour du lundi au vendredi : à 12h30 (lorsque tout le monde prend sa pause) et le soir après le service. Cela permettra que si une personne perd son fichier l'après-midi, elle pourra récupérer une sauvegarde assez récente, ce qui ne la ralentira pas dans son travail.

Pour la sauvegarde complète des fichiers, nous avons choisi d'utiliser le modèle de sauvegarde 3-2-1. Ce modèle est l'un des meilleurs pour garantir la sécurité des données. Il consiste à avoir trois copies des données (3), stockées sur au moins deux supports différents (2), avec une copie hors site (1) pour une protection maximale contre les pertes de données. Cette approche permet de se prémunir contre les pannes matérielles, les erreurs humaines et les catastrophes, assurant ainsi une récupération fiable des informations importantes.

Dans notre cas, nous avons envisagé deux sauvegardes sur site : une sur un cloud local (ou un serveur NAS en RAID 5, solution moins onéreuse), et une sur un disque dur externe rangé dans un coffre sécurisé. Pour la troisième sauvegarde, il faudra établir à chaque sauvegarde complète une copie des données dans un cloud sécurisé OneDrive ou Snowflake.

Schéma du réseau

Pour l'infrastructure du nouveau réseau, nous avons tout repris de zéro. La première partie en dehors du LAN est une structure très simple : l'arrivée d'Internet dans notre pare-feu (firewall) tournant sur PFSense, lui-même branché à une DMZ. Pour rappel, une DMZ, ou zone démilitarisée, est une zone intermédiaire entre le réseau interne sécurisé et Internet, permettant d'isoler les services publics tout en renforçant la protection des systèmes internes. Le firewall est également relié au routeur servant de passerelle par défaut.

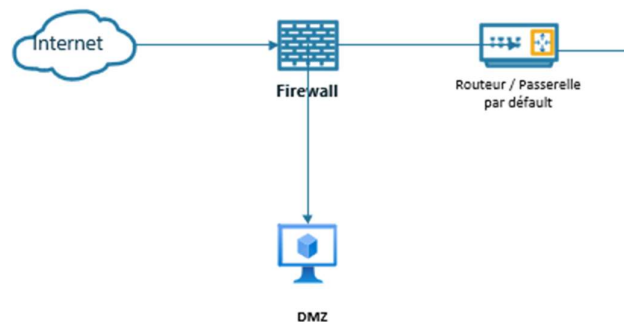


Schéma du réseau hors du LAN

Le routeur est ensuite relié au LAN, cœur de notre système. Notre système simplifié est composé de 3 machines : un client Windows 10, un client Linux (Ubuntu 20.04 LTS) et un serveur Windows 2019. Le serveur Windows héberge plusieurs services :

- Un DNS, ou Système de Noms de Domaine, joue un rôle essentiel dans la résolution des noms de domaine en adresses IP, facilitant ainsi la navigation sur Internet. Il agit comme un annuaire, traduisant les noms compréhensibles par les humains en adresses IP, assurant ainsi la connectivité fluide des ressources en ligne.

- Un AD-DS, ou Active Directory Domain Services, est un service de gestion des identités de Microsoft. AD-DS facilite la gestion centralisée des utilisateurs, des groupes et des ressources réseau au sein d'un environnement informatique, offrant ainsi une infrastructure sécurisée et organisée. Il y avait déjà un AD dans l'ancien système, mais celui-ci était mal configuré.

- Un FTP, ou File Transfer Protocol, est un protocole standard utilisé pour le transfert de fichiers entre un client et un serveur sur un réseau, souvent via Internet. Il permet le téléchargement et le téléversement de fichiers de manière bidirectionnelle, offrant une méthode efficace pour partager des données entre des systèmes informatiques distants.

- Un IIS, ou Internet Information Services, est un serveur web développé par Microsoft pour les systèmes d'exploitation Windows. IIS joue un rôle central dans l'hébergement et la

gestion de sites web, offrant des fonctionnalités avancées telles que le traitement des requêtes HTTP, la gestion des protocoles de communication, et la prise en charge d'applications web. Il remplacera notamment dans notre cas le serveur Apache de l'ancienne infrastructure.

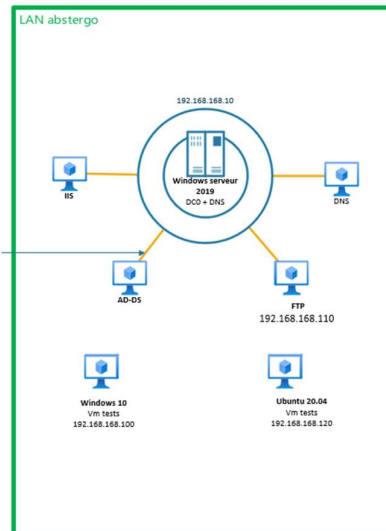


Schéma du LAN

En résumé, les changements opérés dans le nouveau réseau vont permettre de supprimer des machines qui n'étaient pas bien utilisées dans l'ancien réseau, également le fait de minimiser le nombre de machines va permettre de réduire la surface d'attaque quand à d'éventuels actions malveillantes.

Réseau abstergo

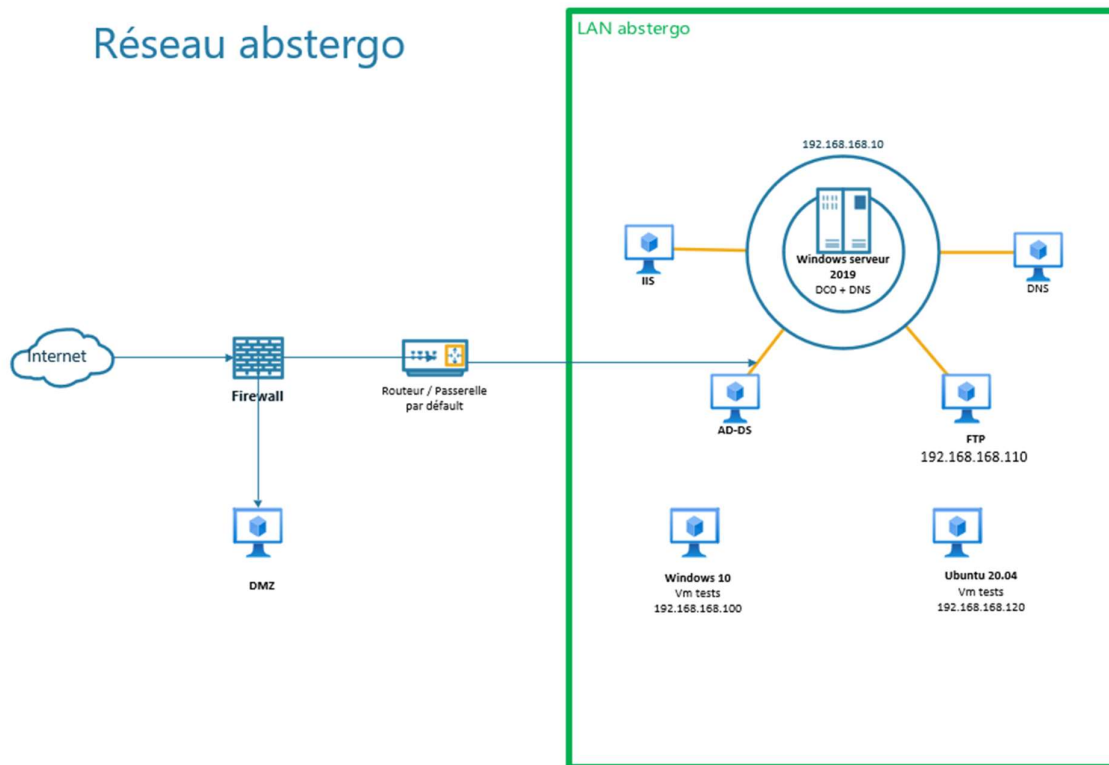


Schéma du nouveau réseau

Organisations des utilisateurs ADDS et OU

Des unités d'organisations et des groupes sont créés pour chacun des services d'Abstergo, cela permet un meilleur partage de fichiers, il ciblera le groupe désiré. De plus cela permet d'avoir une GPO globale pour l'ensemble des groupes et une autre plus spécifique à chacun des groupes. Chaque groupe n'ont pas forcément les mêmes besoins en termes de logiciel préinstallé par exemple.

	Login	Mdp	Groupes	OU
Users	Alex Ception	Abstergo+33	IT, Domain Users	IT
	Test	tttttt+33	Domain Users	Users
	Compta	cccccc+33	Comptabilité, Domain Users	Compta
Administrateur	Administrator	Abstergo_		

Liste des utilisateurs par OU

Les mots de passes choisis sont temporaires et devront être changés le plus rapidement possible, en respectant la politique de choix de mot de passe décrites ci-après, issu du site de l'ANSII :

- Choisir avec soin son mot de passe (notamment méthodes phonétiques ou des premières lettres), mot de passes différent, stocker dans keepass
- Mettre à jour régulièrement les softs
- Être aussi prudent avec smartphone et tablette
- Protéger les données en déplacement
- Être prudent avec la messagerie
- Télécharger ses programmes sur les sites officiels des éditeurs
- Être vigilant lors d'un paiement sur Internet
- Séparer les usages personnels des usages professionnels




























Ces mots de passe seront changés à l'aide d'un script demandant à tous les utilisateurs du domaine de changer leur mot de passe à leur prochain log-on.

Sécurité

Pour sécuriser l'accès au réseau interne, nous avons mis en place plusieurs règles de sécurité :

- Ouvrir le port 389 (LDAP) pour permettre à l'AD les requêtes d'annuaires
- Ouvrir le port 21 (FTP) pour permettre le bon fonctionnement du serveur ftp
- Ouvrir le port 80 (HTTP) pour permettre le fonctionnement de Centreon

Pare-feu / Règles / LAN											   
Flottant(e) WAN LAN DMZ											
Règles (Faire glisser pour changer l'ordre)											
<input type="checkbox"/>	États	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnancement	Description	Actions
<input type="checkbox"/>	 0/0 B	IPv4 TCP/UDP	*	*	192.168.168.10	389 (LDAP)	*	aucun			     
<input type="checkbox"/>	 0/0 B	IPv4 TCP/UDP	*	*	192.168.168.10	21 (FTP)	*	aucun			     
<input type="checkbox"/>	 0/0 B	IPv4 TCP	*	*	192.168.168.20	80 (HTTP)	*	aucun			     

Scripting

Premier script

Le premier script que nous avons réalisé est un script assez simple forçant le changement de mot de passes des utilisateurs, pour des questions de sécurité.

```
Set-ADUser -Identity $utilisateur.SamAccountName -ChangePasswordAtLogon $true
```

Il doit être mis dans les GPO pour affecter tous les utilisateurs.

Deuxième script

Ce second script est très utile pour des fins de sécurités ou d'administration, il nous permet de connaître la date et l'heure de la dernière connexion de chaque utilisateur de l'AD sur les pc du domaine.

```
# Importe le module Active Directory
Import-Module ActiveDirectory

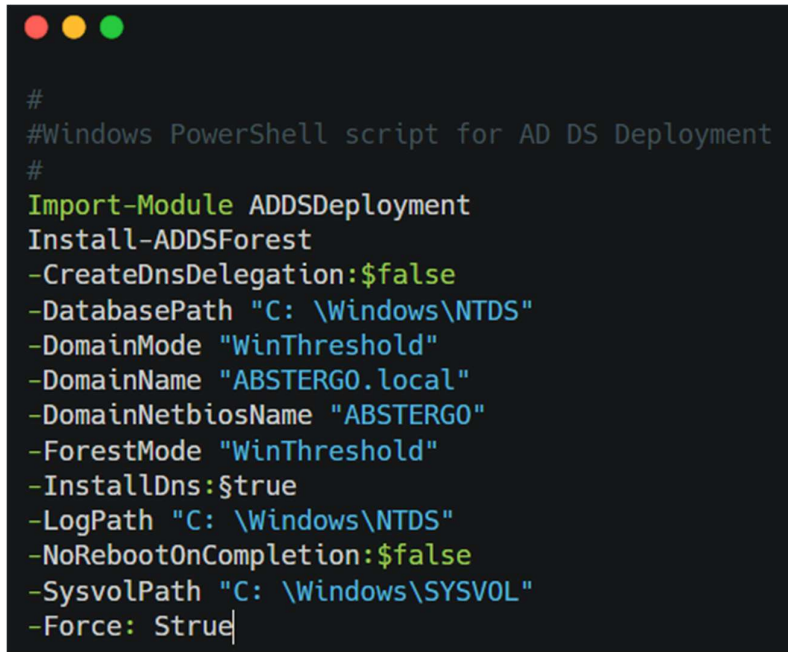
# Récupère tous les utilisateurs du domaine Abstergo.local
$users = Get-ADUser -Filter * -Properties LastLogon

# Affiche les informations de dernière connexion
foreach ($user in $users) {
    $lastLogon = [DateTime]::FromFileTime($user.LastLogon)
    Write-Host "$($user.SamAccountName) - Dernière connexion : $lastLogon"
}
```

Il peut être exécuté sur la session master via le PowerShell.

Troisième script

En cas de soucis critique sur notre Active Directory nous avons gardés un script permettant sur un nouveau server de le redéployer :



```
#  
#Windows PowerShell script for AD DS Deployment  
#  
Import-Module ADDSDeployment  
Install-ADDSForest  
-CreateDnsDelegation:$false  
-DatabasePath "C: \Windows\NTDS"  
-DomainMode "WinThreshold"  
-DomainName "ABSTERGO.local"  
-DomainNetbiosName "ABSTERGO"  
-ForestMode "WinThreshold"  
-InstallDns:$true  
-LogPath "C: \Windows\NTDS"  
-NoRebootOnCompletion:$false  
-SysvolPath "C: \Windows\SYSVOL"  
-Force: Strue|
```

Script non-testé

Conclusion

Les systèmes en places répondent donc bien aux demandes pour l'obtention de la norme iso, la maquette est prête pour la présentation de demain.