

PROJET ANIMUS EXTENDUS

Livrable 1

Groupe 1

Une image contenant symbole, logo, blanc, clipart

Description générée automatiquement

Florian Brochot

Hugo Laplace

Table des matières

[Contexte 3](#_Toc148002145)

[Problématique 3](#_Toc148002146)

[Livrable 1 3](#_Toc148002147)

[Analyse du système existant 3](#_Toc148002148)

[Analyse 3](#_Toc148002149)

[Cartographie 3](#_Toc148002150)

[Gestion des identités et accès aux données 3](#_Toc148002151)

[Conclusion 5](#_Toc148002152)

# 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.

# 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.

# Analyse du système existant

## Analyse du premier LAN

On dispose d’un PC principale, le « Master 2019 », tournant sur Windows server 2019. Il agit comme switch virtuel sur le LAN d’ABSTERGO. Sur celui-ci nous avons trouvés trois Machines virtuelles (VM), simulant le LAN:

Une image contenant texte, Police, capture d’écran, ligne

Description générée automatiquement

*Aperçu des VM dispos sur le Master*

Une VM sous Debian11 (Debian-Abstergo), faisant tourner un serveur APACHE2 qui héberge les sites de « abstergo.internal », mais également celui de l’ERP Dollibar

Une VM sous Windows 10 permettant d’accéder à l’utilisateur Pierre Morin, utilisateur de test pour le service comptabilité.

Et une VM Windows Server 2019 servant de Domain Master sur le Lan-Abstergo dont les 3 VM font parties. Elle héberge aussi plusieurs services :

* Un Active Directory pour centraliser le contrôle des utilisateurs,
* Un Server Web IIS,
* Un DNS pour permettre l’accés à internet pour le Lan,
* Un serveur DHCP pour attribuer dynamiquement les ip aux ordinateurs du LAN,
* Et WSUS (Windows serveur update service) pour centraliser les mise a jour des pc du LAN

Une image contenant texte, diagramme, capture d’écran, Plan

Description générée automatiquement

*Cartographie du LAN*

## Analyse du second LAN

# Gestion des identités et accès aux données

On retrouve 2 Utilisateurs du réseau Lan-Abstergo :

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

L’administrateur du réseau qui s’apparenterais au Serveur Windows, L’invité est un utilisateur par défaut créer par le système mais est désactivés, krbtgt est un utilisateur built-in de l’active-directory et nous permettra d’ajouter un système d’authentification.

Le second « vrai » utilisateur est pmorin qui correspond à Pierre Morin un utilisateur du groupe comptabilité créer spécialement pour en vérifier les problèmes remonté.

Le Windows server possède tous les rôles FSMO (Maitre d’opération) :

Une image contenant texte, capture d’écran, Police, logiciel

Description générée automatiquement

SchemaMaster; DomainNamingMaster; PDCEmulator; RIDMaster; InfrastructureMaster.

Tous les informations des utilisateurs peuvent être trouvé via une commande Powershell disponible avec l’AD :

Une image contenant texte, capture d’écran, logiciel

Description générée automatiquement

On peut voir dans la catégorie « DistinguishedName » 3 types : DC ; CN ; OU

DC : Domain Components serait les branches les plus hautes de l’arbre (niveau domaine)

Ou : Organizational Units qui servent à stocker des objets (users, groups,)

CN : Common Name nom commun de l’objet (ex : pour l’utilisateur Pierre Morin, CN Pierre Morin

# Conclusion