Rapport de projet système et réseau





Contenu

[1. Introduction 4](#_Toc469477459)

[2. Cahier des charges 5](#_Toc469477460)

[A. Maison mère 5](#_Toc469477461)

[B. Filiale Telecom 5](#_Toc469477462)

[3. Gestion de projet 6](#_Toc469477463)

[A. Product Breakdown Structure (PBS) 6](#_Toc469477464)

[B. Work Breakdown Structure (WBS). 7](#_Toc469477465)

[a. GROUP 7](#_Toc469477466)

[b. TELECOM 8](#_Toc469477467)

[C. Organizational Breakdown Structure (OBS) 9](#_Toc469477468)

[Groupe : 11](#_Toc469477469)

[Telecom : 11](#_Toc469477470)

[Domaine : 12](#_Toc469477471)

# Introduction

Le groupe Gouybues est présent dans plusieurs secteurs d’activité : Les médias, le bâtiment et depuis peu les télécoms, suite au rachat d’une jeune entreprise de ce secteur. Au niveau système, la maison mère possède une forêt Active Directory dans laquelle se trouve un domaines gouybues-group.local .

L’entreprise possède également plusieurs filiales possédant également une architecture Active Directory. Ainsi, la filiale média possède une forêt avec un domaine tf42-group.local . La filiale construction possède quant à elle une forêt dans laquelle se trouve le domaine gouybues-construcion.local.

La dernière filiale Telecom possède également une forêt avec un domaine gouybues-telecom.local mais contrôlé par 2 contrôleurs de domaine, un contrôleur principale Active Directory et une réplication sous Debian avec l’utilisation de Samba4.

L’entreprise nous demande de mettre en place l’architecture Active Directory de la maison mère et de la filiale Telecom. Nous ne devons pas prendre en compte les autres filiales. Il nous est également demandé de ne pas prendre en compte le réplica de la maison mère.

# Cahier des charges

## Maison mère

Dans le cas de la maison mère, la direction de gouybues nous demande de créer une forêt Active Directory composé d’un domaine gouybues-group.local. Nous devrons également créer un service DHCP et DNS.

Chaque service aura accès à un répertoire partagé qui se trouvera sur le contrôleur de domaine Active Directory. Il figurera comme lecteur de réseaux sur les postes clients et ne sera accessible qu’aux utilisateurs membre du service sauf pour la Direction qui aura accès à tous les partages. Il se nommera S : (Share)

Les services auront également accès à un répertoire partagé entre tous les services. Il sera également un lecteur de réseau pour les postes Client et se nommera G : (Group).

Enfin, pour le partage de fichiers, tous les utilisateurs du domaine auront accès à un dossier personnel qui sera une redirection du dossier Documents sur le contrôleur de domaine.

Nous configurerons également un partage des imprimantes. Celle-ci sera accessible à tous les membres du domaine connectés.

Au niveau de la gestion des hôtes, nous devons mettre en place un service d’installation automatique du logiciel 7zip qui sera effectué à la première connexion d’un utilisateur du domaine. Tous les hôtes possèderont un fond d’écran commun à leur service qui sera mis en place automatiquement à leur connexion. Et enfin nous devrons désactiver l’exécution automatique des périphériques externes mais ne pas bloquer leurs accès.

Pour des raisons de sécurité nous devons configurer le mot de passe des utilisateurs qui devront se renouveler tous les 90 jours et comporter un minimum de 8 caractères. Un mauvais mot de passe rentré 3 fois verrouillera la session et celle-ci ne pourra être que débloqué par un administrateur.

Enfin la filiale mère possèdera un service de déploiement de poste qui installera automatique un OS Windows 10 et permettra aux futurs utilisateurs d’accéder au domaine automatiquement.

## Filiale Telecom

Tout comme la maison mère, la filiale Telecom aura un DNS, un DHCP et un contrôleur de domaine Active directory possédant une forêt sur le domaine gouybues-telecom.local. Les utilisateurs auront accès au même type de partage que la maison mère, à la différence que le dossier commun se nommera T : (Telecom). Les utilisateurs auront également une redirection de leur dossier Mes documents. La gestion des hôtes, des périphériques et des mots de passe sera la même.

La différence entre les 2 filiales se trouve au niveau de la réplication du contrôleur de domaine Active directory sur un serveur Debian. L’annuaire devra être répliqué sur Samba4 et devra permettre aux utilisateurs d’accéder aux mêmes fonctionnalités que le serveur Windows s’il rencontre un problème.

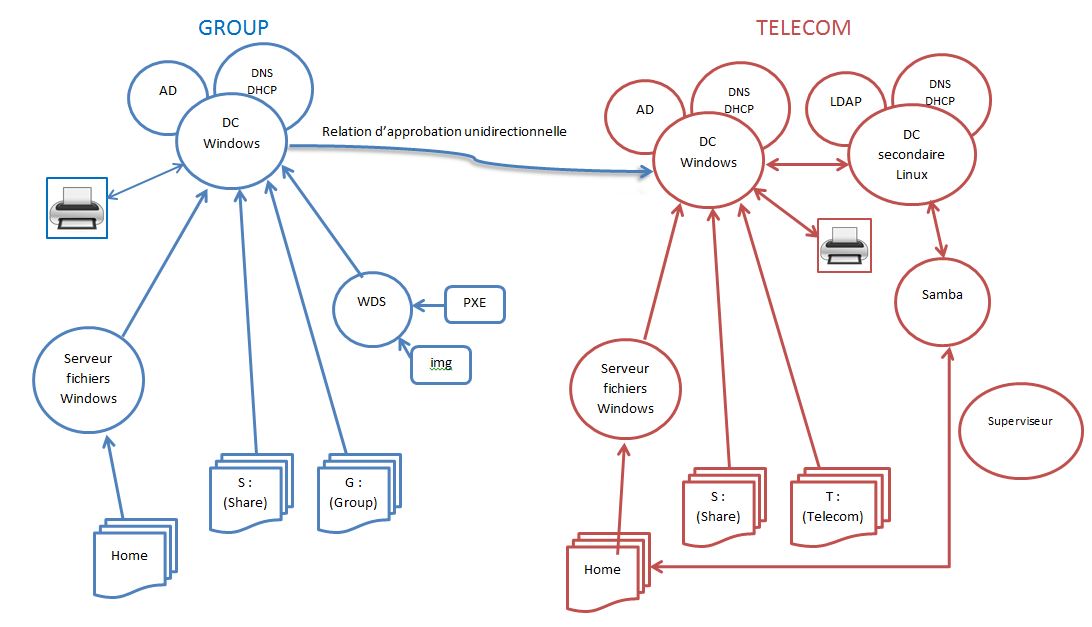
Enfin, la filiale Telecom possèdera un superviseur qui contrôlera le fonctionnement des serveurs DHCP et DNS. Il contrôlera également la charge d’utilisation du CPU, de la mémoire et du disque dur des serveurs Windows et Debian.

Il devra également exister une relation d’approbation unidirectionnelle entre les deux forêts, les utilisateurs du domaine Group pourront accéder aux ressources du domaine Telecom, mais pas l’inverse.

# Gestion de projet

## Product Breakdown Structure (PBS)

Le Product Breakdown Structure est une manière de représenter le résultat visé d’un projet, ici la maquette de l’infrastructure du réseau de Gouybues.

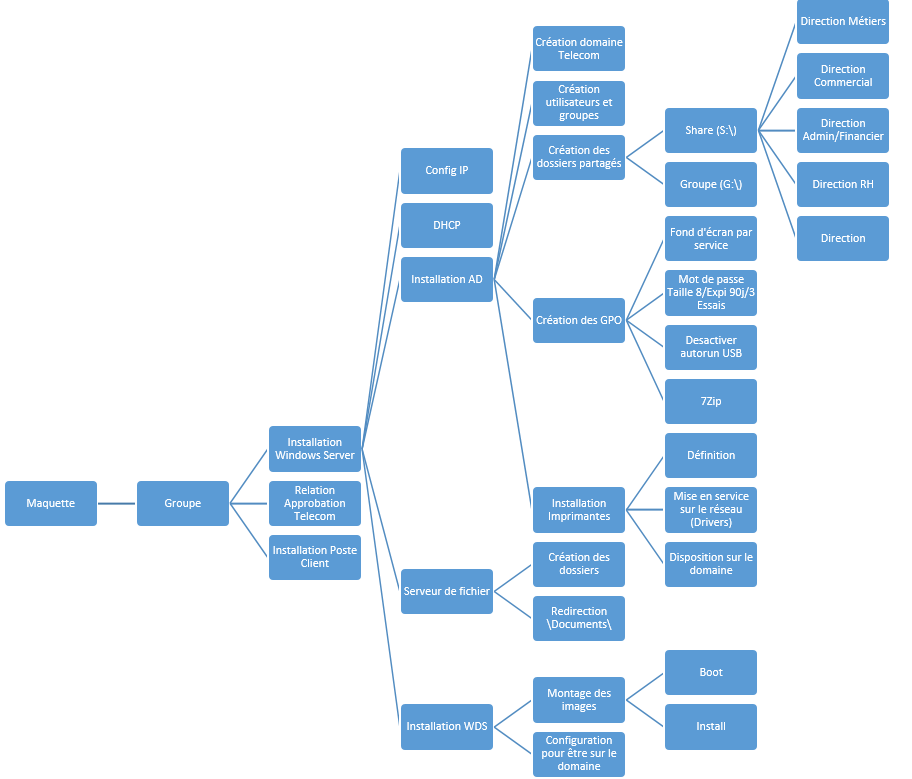


Ce schéma nous permet de bien identifier les principaux livrables du projet afin de pouvoir construire le Work Breakdown Structure.

## Work Breakdown Structure (WBS).

Après avoir découvert le projet et formé les groupes, nous avons dégagé du sujet toutes les tâches demandées. Nous avons donc construit le Work Breakdown Structure.

### GROUP



### TELECOM

Ce schéma nous permet de dégager toutes les tâches à effectuer. Nous allons maintenant construire l’Organizational Breakdown Structure afin de partager les tâches entre les membres de l’équipe.

## Organizational Breakdown Structure (OBS)

Comme dit précédemment, ce schéma permet d’identifier les groupes de tâches que chacun doit effectuer.

Adrien et Gaëtan s’occuperont respectivement de l’installation et de la configuration des Windows Server de Group et Telecom. Pendant que Adrien se chargera de la configuration du service WDS, Gaëtan étudiera les différentes approches dans la relation d’approbation et la mettra en place avec Adrien. Ils réaliseront également un guide qui présentera les différentes étapes de configuration de leurs services.

Laurent est chargé de l’installation et de la configuration du serveur Linux. Il configurera le service Samba4 et la réplication du service de contrôleur de domaine Active Directory. Il réalisera un guide de configuration de ses services et avec Yohann il réalisera le serveur de supervision.

Le chef de projet Yohan est chargé de réaliser toute la partie analyse du besoin, écrit du rapport de projet et création du PPT. Il s’occupera également des fonds d’écran à intégrer dans les serveurs et accompagnera Laurent dans la création du serveur de supervision. Il suivra tout au long du projet l’avancée des missions de chaque membre du groupe.

## Planning prévisionnel

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| GAETAN | mercredi | jeudi | vendredi | Lundi | Mardi | Mercredi |
| 1 : Windows server telecom |  |  |  |  |  |  |
| 1.1 : Configuration IP |  |  |  |  |  |  |
| 1.2 : Configuration DHCP |  |  |  |  |  |  |
| 1.3 : Active directory |  |  |  |  |  |  |
| 1.3.1 : Création domaine Telecom |  |  |  |  |  |  |
| 1.3.2 : Création utilisateurs et groupes |  |  |  |  |  |  |
| 1.3.3 : Création des dossiers partagés |  |  |  |  |  |  |
| 1.3.4 : Création des GPO |  |  |  |  |  |  |
| 1.3.5 : Installation imprimantes |  |  |  |  |  |  |
| 3 : Relation d'appro groupe/telecom |  |  |  |  |  |  |
| 4 : Guide d'installation et de conf |  |  |  |  |  |  |
| 5 : PBS |  |  |  |  |  |  |
| 6 : WBS |  |  |  |  |  |  |
| 7 : OBS |  |  |  |  |  |  |
| ADRIEN | mercredi | jeudi | vendredi | Lundi | Mardi | Mercredi |
| Windows server groupe |  |  |  |  |  |  |
| 1.1 : Configuration IP |  |  |  |  |  |  |
| 1.2 : Configuration DHCP |  |  |  |  |  |  |
| 1.3 Active Directory groupe |  |  |  |  |  |  |
| 1.3.1 : Création domaine group |  |  |  |  |  |  |
| 1.3.2 : Création utilisateurs et groupes |  |  |  |  |  |  |
| 1.3.3 : Création des dossiers partagés |  |  |  |  |  |  |
| 1.3.4 : Création des GPO |  |  |  |  |  |  |
| 1.3.5 : Installation imprimantes |  |  |  |  |  |  |
| 2 : Serveur WDS |  |  |  |  |  |  |
| 2.1 : Monter des images |  |  |  |  |  |  |
| 2.2 : Configuration domaine |  |  |  |  |  |  |
| 3 : Guide d'installation et de conf |  |  |  |  |  |  |
| 4 : PBS |  |  |  |  |  |  |
| 5 : WBS |  |  |  |  |  |  |
| 6 : OBS |  |  |  |  |  |  |
| LAURENT | Mercredi | Jeudi | Vendredi | Lundi | Mardi | Mercredi |
| 1 : Serveur Linux et Telecom |  |  |  |  |  |  |
| 1.1 : Configuration IP |  |  |  |  |  |  |
| 1.2 : DHCP |  |  |  |  |  |  |
| 1.3 : DNS |  |  |  |  |  |  |
| 1.4 : Samba4 |  |  |  |  |  |  |
| 1.4.1 : Réplication DC AD |  |  |  |  |  |  |
| 1.4.2 : Kerberos |  |  |  |  |  |  |
| 1.4.3 : Verif dossiers, GPO, imprimantes. |  |  |  |  |  |  |
| 2 : Guide d'installation et de conf |  |  |  |  |  |  |
| 3 : Superviseur |  |  |  |  |  |  |
| 3.1 : Installation distrib FAN |  |  |  |  |  |  |
| 3.2 : Config IP |  |  |  |  |  |  |
| 3.3 : Installation agents |  |  |  |  |  |  |
| 3.4 : Scripts actifs |  |  |  |  |  |  |
| 3.5 : Scripts passifs |  |  |  |  |  |  |
| 3 : PBS |  |  |  |  |  |  |
| 4 : WBS |  |  |  |  |  |  |
| 5 : OBS |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

## Planning réel

# Solution

## Plan d’adressage

Avant de commencer la configuration de nos services, nous avons créé un plan d’adressage pour configurer correctement nos serveurs :

* Groupe :

|  |  |
| --- | --- |
| Serveur | **Adresse ou Plage d’adresses IP** |
| WINSRVGROUP | 192.168.0.1 /24 |
| ClientGroupe | 192.168.0.10 /24 <-> 192.168.0.50 /24 |

* Telecom :

|  |  |
| --- | --- |
| Serveur | **Adresse ou Plage d’adresses IP** |
| WINSRVTELECOM | 192.168.1.1 /24 |
| LinuxSrvTelecom | 192.168.1.2 /24 |
| ClientTelecom | 192.168.1.10 /24 <-> 192.168.1.50 /24 |
| SuperviseurTelecom | 192.168.1.3 /24 |

Tous nos serveurs sont configurés en statique et possèdent l’adresse IP présenté ci-dessous. Les 2 plages d’adresses seront les adresses IP données dynamiquement par le DHCP sur son domaine.

## WindowsServeur

### Contrôleur de domaine

Active directory est un service d’annuaire développé par Microsoft. Il permet de regrouper toute les informations concernant un réseau comme les utilisateurs, les machines ou/et les applications. Il permet à l’utilisateur de permettre et d’autoriser l’accès d’un utilisateur à différentes données.

Dans un premier temps, nous avons procédés à la création de nos contrôleurs de domaine sur les filiales Group et Telecom. Nous avons donc créé 2 forêts : Chacune possède un domaine, le premier gouybues-group.local et le second gouybues-telecom.local. Lors de l’installation du contrôleur de domaine, Active Directory crée également le service DNS, Il nous a donc fallu créer la zone de recherche inverse.

Le second service à installer pour rendre l’annuaire opérationnel est le serveur DHCP, et la création d’une plage d’adresse dynamique qui attribuera une adresse IP aux futurs hôtes du réseau.

Une fois le contrôleur de domaine créé, nous avons pu commencer la création des utilisateurs. Pour cela nous avons créé une unité d’organisation portant le nom de notre domaine, et créé dans celle-ci des groupes portant le nom des services de l’entreprise. Nous avons terminé par la création des utilisateurs et leurs rattachements à leur groupe respectif. Nous avons créé un groupe qui englobe tous les autres groupes pour représenter tous les membres du domaine.

### Group Policy Object (GPO)

Pour la configuration des services d’annuaire, tel que le partage de fichiers Active Directory, les GPO apportent la solution qui permet de définir des droits aux utilisateurs sur les services créés dans Active Directory.

* Répertoire de partage Commun

Le premier GPO que nous avons créé est un mappage d’un lecteur qui représentera un répertoire de notre Windows Server sur les poste clients. Pour la filiales Telecom celui-ci se nommera T : (Telecom) et pour la maison mère ce sera G : (Group). Ses 2 lecteurs seront disponibles à tous les utilisateurs membre du domaine.

* Répertoire de partage par Service

Les prochains GPO sont responsables du partage par service. Nous avons créé un GPO par service qui mappera un dossier du nom du service sur le poste client et est nommé S : (Share). Seul les utilisateurs membre du groupe du service sont autorisés à accéder au lecteur, les autres ne le visualiseront pas. Seul le service Direction aura les autorisations d’accès à tous les dossiers.

Nous avons créé un dernier GPO qui redirigera le dossier « Mes Documents » de chaque utilisateur sur le serveur Windows. Il prendra le nom de l’utilisateur dans l’arborescence Windows Server. Le GPO est configuré de manière à ce que la réplication soit automatique et en temps réel. Ce GPO permet à un utilisateur d’accéder à son « Mes Documents » sur tous les postes du domaine.

* Déploiement d’application

L’entreprise souhaite que 7zip soit installé automatiquement sur tous les postes du domaine. Nous avons donc créé un GPO à qui on a indiqué que l’installateur du logiciel (d’extension .msi) serait à installer. Nous lui demandons de lancer automatiquement l’installation (en arrière-plan) sur tous les poste du domaine lors de l’ouverture d’une session.

* Partage des imprimantes

Le partage des imprimantes sur le contrôleur domaine s’effectue également grâce à un GPO. On lie une imprimante présente sur le réseau au GPO et on peut configurer les droits d’accès des groupes et/ou utilisateurs à celle-ci. Dans notre cas, tous les membres du domaine ont accès aux imprimantes du réseau.

* Déploiement des fonds d’écran

Nous configurons le GPO pour qu’il change automatique le fond d’écran du bureau de l’utilisateur par rapport au groupe auquel il appartient.

* Password Settings Object

Pour la politique de sécurité des mots de passe, nous avons créé un PSO qui s’appliquera à tous les utilisateurs du domaine. Celui-ci est configuré de manière à ce que les nouveaux mots de passe comporte au minimum 8 caractère, que le système demande à l’utilisateur une modification de celui-ci tous les 90 jours, et qu’en cas de 3 échecs la session soit verrouillée et ne peut être que déverrouiller que par un administrateur. Le PSO n’est pas un GPO mais un Objet à part entière.

### Service de déploiements de postes

Pour pouvoir installer des postes clients à distance, on utilise un service de déploiement d’image. Ce service est séparé en 2 entités :

* WDS
* MDT

Le WDS (Windows Deployment System) permet d’envoyer des images à des machines connectées au réseau via PxE. Il permet à la machine de télécharger une image d’installation et une image de démarrage.

Ensuite, nous utilisons le MDT (Microsoft Deployment Toolkit) pour configurer l’installation et créer une image de démarrage personnalisée. En effet, grâce au MDT, on peut passer les étapes de l’installation et avoir certains paramètres comme la connexion automatique au domaine dès l’installation.

Une fois tout ceci fait, nous mettons à jour le service, ce qui va nous générer une image de démarrage personnalisée. Il suffit d’importer cette image de démarrage dans le WDS aux côtés de l’image d’installation. Quand on lancera le client et qu’il se connectera via PxE, le service MDT lancera notre installation de Windows personnalisée et automatisée.

## Linux Serveur

### Samba 4

Samba est un logiciel d’interopérabilité qui permet à des ordinateurs Unix de mettre à disposition des imprimantes et des fichiers dans des réseaux Windows. De plus, la quatrième version de ce logiciel permet de créer un Active Directory ainsi que toutes ses fonctionnalités. En effet, Samba4 permettra de répliquer les objets créés dans l’Active Directory de Windows Server (notamment ceux de l’annuaire LDAP). Pour compléter Samba, nous copierons et synchroniserons le dossier SYSVOL afin de pouvoir récupérer l’ensemble des GPO.

3.3.1 : Active Directory

Active Directory est un annuaire qui va nous permettre une authentification centralisée des utilisateurs et l’applications des règles de groupe.

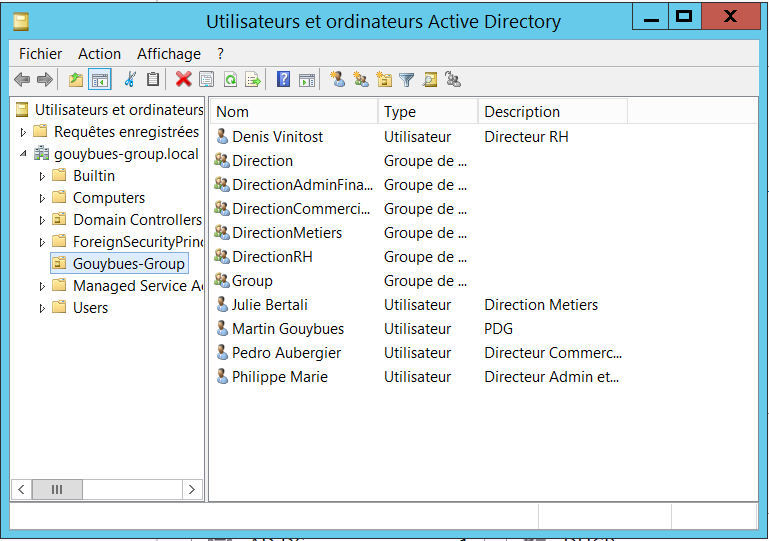
Pour mettre en place cet annuaire, il a fallu commencer par installer le rôle active directory dans le gestionnaire de serveur et créer le contrôleur de domaine.

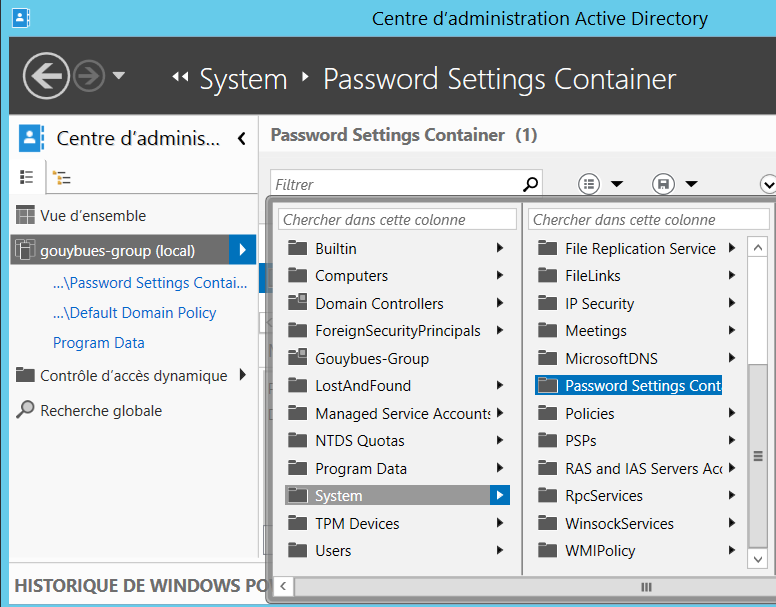
On a ensuite exécuté un script powershell pour créer la forêt et le DNS.

Il convient ensuite d’ajouter le rôle de DHCP que l’on configure pour distribuer jusqu’à 40 adresses IP.

On peut passer à la création des groupes et utilisateurs

Quant à la sécurité des mots de passes :



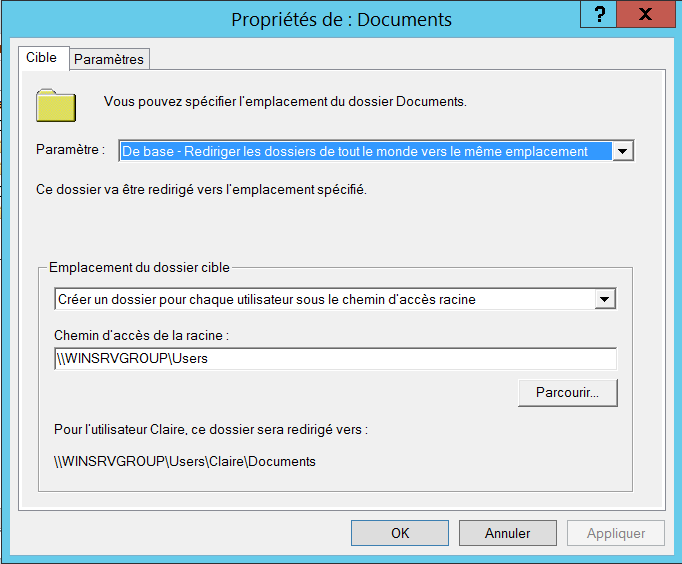


Nous avons activé une longueur minimale de 8 caractères. Nous avons désactivé l’exigence de complexité. Nous demandons à l’utilisateur de modifier son mot de passe tous les 90j. Et en cas de 3 tentatives de connexion échouées, seul un administrateur peut déverrouiller le compte qui est alors verrouillé par sécurité. Ce PSO s’applique à tous les utilisateurs des domaines Telecom et Group.

3.3.2 : partage de répertoire :

Il était attendu que chaque service ait accès à son répertoire partagé et que chaque utilisateur ait accès à son répertoire personnel sur tous les postes clients.

Nous avons pour cela créés une stratégie de groupe par service redirigeant un répertoire share présent dans le serveur et correspondant au service du client vers son poste et une autre s’occupant de rediriger le répertoire Documents de chaque utilisateur sur un dossier dédié portant le nom de l’utilisateur sur Share. Il actualise le répertoire de l’utilisateur en temps réel, l’utilisateur aura accès à ses données automatiquement sur n’importe quel poste client du domaine.



3.5 : Supervision

Afin d’assurer la supervision de notre serveur Windows (Telecom), nous allons utiliser un fork de centOS avec un superviseur Nagios embarqué.



Celui-ci embarque aussi un serveur apache et une application web joignable par le biais de l’IP du serveur.

Tout commence donc par l’installation de la distribution et la configuration IP du poste.