

# PROJET FINAL

Département SYSTÈME



Hiver 2013

Cahier de charge

420-B61 Implantation d'une infrastructure réseau sous TCP/IP v4

420-B64 Implantation d'un réseau corporatif sous Active Directory

# Table des matières

<b>INTRODUCTION.....</b>	<b>5</b>
Objectif général du projet .....	5
Objectifs du cours B61 .....	5
Objectifs du cours B64 .....	6
<b>FONCTIONNEMENT GÉNÉRAL .....</b>	<b>8</b>
Étape préliminaire .....	8
Évaluation .....	9
Étape de réalisation .....	9
Sous-étape d'implantation.....	9
Sous-étape de validation .....	10
Rapports et programmation.....	11
Rédaction des rapports .....	11
Rédaction du code .....	11
<b>RÉPARTITION DES TÂCHES D'ÉQUIPE.....</b>	<b>12</b>
Équipes à trois membres.....	12
Équipes à deux membres.....	13
<b>LA CORPORATION .....</b>	<b>15</b>
<b>LES ORDINATEURS .....</b>	<b>16</b>
Description.....	16
Particularités pour la journée de projet .....	17
<b>INFRASTRUCTURE DU RESEAU .....</b>	<b>18</b>
Le domaine .....	18
Les cartes réseaux .....	19
Le plan d'adressage du domaine.....	19
Le plan d'adressage du réseau public.....	19

<b>LES SERVEURS .....</b>	<b>20</b>
Description.....	20
Particularités des serveurs personnels .....	20
Bureau à distance .....	21
Hyper-V sur les serveurs personnels.....	21
Particularités des postes clients .....	22
<b>LES SERVEURS DE FICHIERS .....</b>	<b>22</b>
Le diagramme de l'infrastructure .....	23
<b>LE ROUTEUR .....</b>	<b>24</b>
NAT et le pare-feu .....	24
VPN .....	25
Hyper-V sur le routeur.....	26
<b>L'AUTORITÉ DE CERTIFICATION .....</b>	<b>26</b>
<b>LE SERVEUR SMTP .....</b>	<b>26</b>
<b>LES SERVEURS DNS .....</b>	<b>27</b>
DNS privé.....	27
DNS public .....	27
<b>LE SERVEUR IIS CORPORATIF .....</b>	<b>28</b>
Site WEB corporatif .....	28
Site WEB sécurisé corporatif .....	29
Site FTP corporatif .....	30
<b>STRATÉGIES DE GROUPE CORPO .....</b>	<b>31</b>
<b>VOTRE «ADMINISTRATEUR».....</b>	<b>33</b>
<b>LE DÉPARTEMENT SYSTÈME .....</b>	<b>34</b>
<b>LES UNITÉS D'ORGANISATION.....</b>	<b>35</b>
<b>LES UTILISATEURS ET LES GROUPES .....</b>	<b>36</b>
Généralités sur les utilisateurs.....	36
Les groupes.....	37
La programmation .....	37

<b>LES SERVEURS DE FICHIERS .....</b>	<b>38</b>
Les dossiers personnels.....	38
Les dossiers de profils.....	38
Les dossiers du département.....	39
Autorisations sur les dossiers .....	39
Emplacement des dossiers .....	40
Les espaces de noms .....	40
Les autorisations NTFS .....	40
Les partages .....	41
Programmation .....	41
<b>LES QUOTAS DE DOSSIERS.....</b>	<b>42</b>
Description des quotas .....	42
Les rapports de quotas .....	42
<b>LES STRATÉGIES DE GROUPE.....</b>	<b>43</b>
Stratégie pour les postes client .....	43
Votre département.....	44
Section «Analystes».....	44
Section «Supports».....	45
Section «Architectes».....	45
Section «Déploiements» .....	46
<b>GESTIONNAIRES DU DEPARTEMENT .....</b>	<b>46</b>
Stratégies de groupe .....	46
Délégation de pouvoir .....	46
<b>LE SERVEUR IIS.....</b>	<b>47</b>
Site WEB départemental .....	47
Site WEB sécurisé départemental .....	48
Site FTP départemental.....	49

<b>ANNEXES –ÉLÈVES-ÉQUIPE .....</b>	<b>50</b>
Listes des numéros de postes.....	50
Localisation des «Routeurs» local 4:07 .....	51
Localisation des «Routeurs» local 4:08.....	52
Plan d'adressage privé – corporatif .....	53
Plan d'adressage public .....	54
Attribution des départements .....	55
<b>ANNEXE – STRATEGIES DE GROUPE .....</b>	<b>57</b>
Stratégies .....	57
Préférences .....	58
<b>ANNEXE – ÉVALUATION DE STRUCTURE.....</b>	<b>58</b>
<b>ANNEXE – SYSTEME .....</b>	<b>59</b>
Procédure d'activation des S.E.....	59

---

# INTRODUCTION

---

## Objectif général du projet

Ce projet constitue l'épreuve certificative des cours 420-B61 et 420-B64. Ce projet vérifie aussi toutes les compétences en lien avec les ordinateurs, les systèmes d'exploitation et les réseaux.

L'objectif poursuivi est de mettre en place une structure de réseau corporatif.

Les dernières semaines de cours sont réservées à la préparation et l'exécution de ce projet. Certaines parties devront être faites en équipe, selon un plan d'allocation des responsabilités personnel à chaque membre de l'équipe. La grande majorité du projet est le résultat d'un travail individuel.

## Objectifs du cours B61

Il s'agit pour vous, en équipe et individuellement, d'installer un réseau Intranet pour une entreprise œuvrant dans le domaine des jeux vidéo sous l'Active Directory. Le réseau de l'entreprise devra être relié à Internet.

Le réseau que vous installerez supportera uniquement le protocole TCP/IP v4. Vous devrez vérifier le câblage et tester la communication.

Votre réseau devra lier deux plans d'adressage:

- ▣ Un plan d'adressage corporatif privé, implanté par adresses statiques ;
- ▣ Un plan d'adressage pour le réseau public, implanté sur le routeur.

Les fonctions «serveur DNS» seront implantées sur deux serveurs :

- ▣ Un dans la corporation et un sur le réseau public.

Les fonctions de «routeur» seront implantées sur un serveur avec 2 cartes réseau actives

- ▣ Il permettra la circulation des paquets de et vers Internet;
- ▣ Il servira de serveur VPN et de serveur NAT;
- ▣ Il servira de pare-feu, avec redirection d'adresse du public au privé.

Les fonctions d'une autorité de certification seront implantées sur le contrôleur de domaine.

Les fonctions «serveur IIS» seront implantées afin de permettre

- ▣ L'existence de plusieurs sites WEB, http et https ;
- ▣ L'existence de sites FTP ;
- ▣ Pour tous les sites les accès seront possibles de l'interne ;
- ▣ Pour certains sites les accès seront possibles de l'externe.

Le rôle Hyper-V sera fonctionnel sur votre serveur personnel

- ▣ Il permettra l'implantation d'un poste de travail Windows 8.

Tous les serveurs devront accepter la gestion via le bureau à distance.

## Objectifs du cours B64

Il s'agit pour vous, en équipe et individuellement, d'installer une gestion des ressources d'un réseau corporatif sous l'Active Directory.

Au sein de votre équipe chacun d'entre vous serez responsable d'un département. En annexe vous trouverez le département qui vous est assigné. Voici les principaux objectifs techniques du projet :

Configurer un serveur en tant que contrôleur de domaine.

Créer une structure d'unités d'organisation pour le département qui vous est assigné qui contiendra tous les objets de votre département.

- ▣ par programmation en PowerShell.

Créer plusieurs dizaines d'utilisateurs dans votre département, ayant chacun des propriétés particulières

- ▣ par programmation en PowerShell.

Mettre en place des structures pour faciliter la gestion

- ▣ Créer des groupes par programmation PowerShell ;
- ▣ Planifier et créer des stratégies de groupes ;

- ▣ Effectuer des délégations de contrôle.

#### Gérer les serveurs de fichiers

- ▣ Planifier et implanter des droits de partage et NTFS afin d'offrir un environnement sécurisé ;
- ▣ Implanter des structures de dossiers personnels ;
- ▣ Implanter des structures de dossiers de profil ;
- ▣ Implanter des espaces de noms DFS afin de faciliter les accès aux partages ;
- ▣ Implanter des quotas de volume et de dossiers, ainsi qu'une structure SMTP pour avertir des dépassements.
- ▣ Implanter des redirections de dossiers



---

# FONCTIONNEMENT GÉNÉRAL

---

Tous les élèves sont regroupés en équipe de deux ou trois personnes. Le projet s'étale sur quatre semaines. Le temps de projet est divisé en deux grandes étapes. La première étape consiste à faire l'analyse préliminaire et d'émettre des rapports. Cette étape durera environ trois semaines. La deuxième étape est celle de l'implantation et de la validation, et durera une journée complète, soit le 29 mai. La validation se fera à la fin de la journée d'implantation.

La majorité du travail est individuel. Pour ce qui est du travail d'équipe, une répartition équitable des responsabilités sera imposée et sera prise en compte lors de l'évaluation.

L'évaluation du projet sera calculé sur plusieurs éléments, entre autres les rapports préliminaires, l'évaluation de structure, les fichiers de réalisation et l'évaluation fonctionnelle. Une liste des détails de la pondération accordée à chaque élément vous sera fournie lors de la première semaine de projet.

## Étape préliminaire

Les semaines précédant le projet sont dédiées à la préparation du projet et à la rédaction de plusieurs rapports d'analyse. Durant ces périodes nous répondons à toutes les questions de précisions sur le projet et sur la matière qui s'y rattache. Durant ces périodes seront annoncés les rectificatifs ou les mises en contexte, s'il y a lieu. Une version écrite de chaque correctif sera aussi disponible sur «Léa».

Suite à la présentation officielle du projet, chaque élève devra choisir, en collaboration avec son équipe, une tâche d'équipe dont il sera le seul responsable. Ces tâches se greffent à la liste des tâches personnelles que chacun devra réaliser.

Chaque élève se voit aussi confier la charge de développer l'environnement réseautique d'un département particulier (voir les annexes).

De plus, dès le 6 mai vous pourrez installer sur la partition deux des postes de travail que vous avez utilisé durant la session des images système similaires à ce que vous aurez lors du projet. Vous pourrez y faire tous les tests, en relation avec le projet qui vous sembleront nécessaires.

# Évaluation

Il y aura plusieurs rapports à compléter. Ces documents devront être remis aux dates prescrites. Chaque rapport devra être remis sur Léa. Certaines sections de rapports devront en plus être remises en format imprimé.

Tout retard dans la remise entraîne des pénalités de 10% par jour, incluant les jours de fins de semaine. Dans les cas où un élève a effectué plusieurs remises, seules la dernière version sera considérée. Pour les rares rapports d'équipe qui sont remis en un seul exemplaire, il est de la responsabilité de tous de s'assurer du contenu et du respect des délais.

Les corrections seront rapidement disponibles à même le système de remise sur Léa. Dès que les corrections sont publiées plus aucun retard ne sera accepté.

Tous les rapports devront être faits avec les outils appropriés (Word, Visio, Excel, ..). Aucune version manuscrite ne sera acceptée.

Le travail d'équipe a été minimisé dans la mesure du possible. Cependant au début du projet certaines décisions d'équipe doivent obligatoirement être prises. Nous évaluons que les deux premières journées du projet, soit les 8 et 9 mai seront principalement dédiés au travail en équipe. Aussi durant ces journées tout élève absent ou en retard se verra pénalisé dans son évaluation. Tout élève absent lors de ces journées se verra automatiquement attribuer la note 0 pour l'évaluation du rapport d'équipe. Une pénalité de 15% sera attribuée par heure de retard.

## Étape de réalisation

### Sous-étape d'implantation

L'implantation du projet se tient sur une journée complète, le 29 mai. L'accès au local est possible à partir de 7h45 et ce jusqu'à 18h00. Durant cette journée vous devez gérer votre temps à votre convenance.

#### RÈGLES DE COMPORTEMENT

Lors des heures de réalisation vous pouvez discuter avec les membres de votre équipe. Cela doit se faire à voix basse, sinon vous devez sortir du local. Vous pouvez sortir du local pour prendre des pauses à volonté, mais rappelez-vous que le temps total qui vous est alloué est fixe. Petit rappel : Il est interdit de manger et boire dans le local.

Vous avez accès à tout votre matériel du cours. Une fois votre réseau mis en place, il n'y a aucune restriction pour l'accès à Internet. Aucun soutien technique n'est donné durant cette journée, sauf en cas de bris de matériel.

Tout élève transgressant une des règles précédentes recevra un premier avertissement, puis sera expulsé du local.

## ÉVALUATION DE STRUCTURE

A partir de 8h00 votre équipe a une première échéance à respecter, soit l'implantation du domaine. Vous avez un maximum de trois heures pour effectuer cette étape. À partir de 11h00, chaque équipe se verra retirer l'usage du compte «Administrateur», et fera l'objet d'une première évaluation. Vous trouverez en annexe le détail des éléments qui seront considérés pour cette évaluation.

Cette échéance a deux objectifs, s'assurer que le travail d'équipe est en grande partie terminé au tout début du projet, et apporter les correctifs nécessaires pour que le développement subséquent se fasse sur une plate-forme «saine».

## ÉVALUATION

À la fin de la journée chaque élève aura à remettre divers fichiers. Deux dépôts devront être effectués, un sur Léa et un autre dans le partage Netlogon. Un dossier au nom de chaque élève devra être créé dans le partage Netlogon afin d'y déposer le travail demandé. Le contenu du dossier de chaque élève constitue une partie de l'évaluation de réalisation.

## Sous-étape de validation

La validation se tient à la fin de la journée à partir de 16:00, la dernière évaluation se tiendra à 18:30. Votre équipe se verra attribuer une heure de validation. Les heures sont attribuées par tirage au sort au début de la journée du projet. Les équipes ayant terminés avant leur temps pourront être évaluées immédiatement s'ils le désirent.

À votre heure, votre réseau doit être fonctionnel et tous les membres de l'équipe doivent être à leur serveur personnel, prêt pour l'évaluation. L'évaluation se termine après 30 minutes, même si tous les points de contrôle n'ont pas été effectués.

Les élèves absents à ce moment se verront attribués la note 0 pour la section de l'évaluation fonctionnelle.

# Rapports et programmation

## Rédaction des rapports

Pour chaque rapport à remettre un fichier gabarit vous sera fourni. Vous devrez obligatoirement utiliser ces fichiers. Dans les rapports d'équipe sur la première page vous retrouvez un champ dans lequel vous devrez indiquer votre nom de domaine.

Dans les rapports personnels sur la première page vous trouverez un champ dans lequel vous devrez indiquer votre nom.

Dans tous les rapports, la qualité du français ainsi que la qualité de la présentation représente une évaluation négative pouvant aller jusqu'à un maximum de 10% de chaque rapport.

## Rédaction du code

Dans les fichiers de script à remettre les premières lignes devront être des commentaires dans lesquelles vous devrez clairement identifier les informations suivantes :

- Votre nom
- La date
- L'objectif du code
- Le serveur à partir duquel le code doit être exécuté
- Les serveurs qui seront modifiés par l'exécution du code

Votre code devra contenir des commentaires pertinents. La présentation du code devra être structurée.

Aucun nom de domaine ou d'ordinateur ne devra être présent dans aucun script, vous devez obligatoirement récupérer l'information à l'aide de cmdlet ou de variables d'environnement disponible.

Quand un nom doit être utilisé à plusieurs reprises vous devez mettre cette valeur dans une variable.

---

# RÉPARTITION DES TÂCHES D'ÉQUIPE

---

## Équipes à trois membres

### TACHE 1

- ▣ Renommer le contrôleur de domaine selon les décisions d'équipe
- ▣ Configuration IP principale du contrôleur
- ▣ Paramétrage du bureau à distance du contrôleur
- ▣ Création du domaine
  - Installation du rôle DNS
- ▣ Configuration d'une autorité de certification
- ▣ Installation du rôle IIS sur le contrôleur (Web et FTP)
- ▣ Installation et configuration du rôle SMTP
- ▣ Création du site Web sécurisé
- ▣ Création de la GPO corporative, du backup et de l'importation

### TACHE 2

- ▣ Renommer le routeur selon les décisions d'équipe
- ▣ Joindre le routeur au domaine
- ▣ Configuration IP principale du routeur
- ▣ Paramétrage du bureau à distance du routeur
- ▣ Installation du rôle routage (Nat et VPN)
- ▣ Paramétrage du pare-feu du routeur concernant la corporation
- ▣ Configuration du serveur DNS «privé» concernant la corporation
- ▣ Création du site FTP corporatif sur le contrôleur
- ▣ Création de la GPO corporative, du backup et de l'importation

## TACHE 3

- ▣ Renommer le client externe selon les décisions d'équipe
- ▣ Configuration IP principale du client externe
- ▣ Paramétrage du bureau à distance du client externe
- ▣ Installation d'Hyper-V sur le routeur (pour les besoins «Client externe»)
  - Renommer correctement la carte réseau d'Hyper-V
- ▣ Installation du rôle DNS sur le client externe
- ▣ Configuration du serveur DNS «public» concernant la corporation
- ▣ Création de la connexion VPN sur le «poste externe»
- ▣ Création du site Web corporatif sur le contrôleur
- ▣ Création de la GPO corporative, du backup et de l'importation

## Équipes à deux membres

## TACHE 1

- ▣ Renommer le contrôleur de domaine selon les décisions d'équipe
- ▣ Configuration IP principale du contrôleur
- ▣ Paramétrage du bureau à distance du contrôleur
- ▣ Création du domaine
- ▣ Configuration d'une autorité de certification
- ▣ Installation du rôle IIS sur le contrôleur (Web et FTP)
- ▣ Installation et configuration du rôle SMTP
- ▣ Création du site Web sécurisé
- ▣ Création du site Web corporatif sur le contrôleur
- ▣ Configuration du serveur DNS «privé» concernant la corporation

- ▣ Configuration du serveur DNS «public» concernant la corporation
- ▣ Création des GPO corporatives, de leur backup et importation

## TACHE 2

- ▣ Renommer le routeur selon les décisions d'équipe
- ▣ Joindre le routeur au domaine
- ▣ Configuration IP principale du routeur
- ▣ Paramétrage du bureau à distance du routeur
- ▣ Installation du rôle routage (Nat et VPN)
- ▣ Paramétrage du pare-feu du routeur concernant la corporation
- ▣ Création du site FTP corporatif sur le contrôleur
- ▣ Renommer le client externe selon les décisions d'équipe
- ▣ Configuration IP principale du client externe
- ▣ Paramétrage du bureau à distance du client externe
- ▣ Installation du rôle DNS sur le client externe
- ▣ Création de la connexion VPN sur le «poste externe»

---

# LA CORPORATION

---

La compagnie Sega, dont le slogan est «Sega, c'est plus fort que toi !», après avoir retiré du marché sa console de jeu en 2001, a décidé de se relancer dans le monde du jeu et de mettre sur le marché une nouvelle console et plusieurs séries de jeux.

Votre firme de consultant doit implanter une structure informatique complète, matérielle et logicielle, convenant à tous les types d'employés de l'entreprise.

Vous devez satisfaire les besoins corporatifs pour des accès à toutes les ressources à l'interne de la compagnie, mais aussi certains accès de l'externe.

Au sein de l'entreprise voici les trois départements auxquels vous aurez affaire : «Système», «Programmation» et «Artistique». Chacun des départements a un ensemble de besoins assez similaires, mais qui s'appliquent à des niveaux différents.

Dans le département «système» vous retrouverez les employés qui s'occupent entre-autres du support on-line, du support à la clientèle, les architectes d'infrastructure, les responsables des déploiements, les analystes en sécurité et finalement les analystes en stockage.

Dans le département «programmation» vous retrouverez les employés qui s'occupent entre-autres du développement 3D, du développement .NET, des modélisateurs, des Web designer, des testeurs d'outils et des testeurs de jeux.

Dans le département «artistique» vous retrouverez les employés qui s'occupent entre-autres de gérer la production, de gérer le graphique, des spécialistes des effets spéciaux, des responsables de la scénarisation, des designers de texture et finalement des designers audio.

En équipe vous aurez à mettre en place tout ce qui est nécessaire pour la corporation. Puis au sein de votre équipe chacun d'entre vous serez responsable d'un département.

Dans les équipes constituées seulement de deux élèves, un des départements sera «fermé».



---

# LES ORDINATEURS

---

## Description

Chaque équipe de trois membres aura à sa disposition 5 ordinateurs. Les équipes de deux membres auront 6 ordinateurs. Le système d'exploitation Serveur 2012 sera déjà installé sur chacun de ces ordinateurs. Chaque ordinateur, à l'exception du routeur aura un fichier VHDX contenant le système d'exploitation Windows 8. Le routeur aura un fichier VHDX contenant le système d'exploitation Serveur 2012. Toutes les mises à jour auront été faites.

Voici l'état dans lequel les serveurs vous seront remis.

- Le système ne sera pas nécessairement activé
- La fonctionnalité «Expérience utilisateur» aura été installée
- Toutes les mises à jour disponibles auront été faites
- Pour PowerShell le niveau d'exécution sera à «Unrestricted»
- La suite Office de Microsoft (version 2010), ce qui inclus Word, Excel, Visio
- NotePad++
- Adobe reader,
- Filezilla version installée et non portable, dans le dossier «C:\Program Files (x86)\FileZilla FTP Client»
- EasyBCD
- Le dossier C:\\_Outils
- Le dossier C:\\_VirDisque, pour le fichier VHDX
- Aucun rôle, ni fonctionnalité supplémentaire ne sera préinstallé.

Le dossier C:\\_Outils contiendra

- Les exécutables de certains produits installés
- La documentation supplémentaire des cours

Le dossier C:\\_VirDisque contiendra

- Un VHDX pour le rôle Hyper contenant Windows 8 ou un serveur 2012
- Un sysprep aura été fait sur ce système
- Sera déjà installé
  - RSAT (seulement sur le Windows 8)
  - Filezilla dans le dossier «C:\Program Files (x86)\FileZilla FTP Client»

# Particularités pour la journée de projet

Votre système sera installé sur la partition 4 et portera la lettre C:\. Cette partition servira d'espace pour les fonctions de serveur de fichiers pour tous les membres de l'équipe.

Au début de la journée de production les mots de passe seront fournis.

Les noms d'ordinateurs auront été générés aléatoirement (15 caractères aléatoires). Vous devez obligatoirement les modifier selon vos décisions d'équipe. La modification du nom de l'ordinateur jouant le rôle de contrôleur de domaine doit se faire obligatoirement avant de créer le domaine.

Chaque équipe recevra ses ordinateurs avec les deux cartes réseaux câblées. La carte réseau sur la plaque maitresse est reliée au réseau du département (OnBoard), la carte réseau supplémentaire sera reliée à un commutateur (PCI). Malgré le fait que tout le matériel est vérifié, vous êtes responsable de vérifier la connectivité. Du matériel supplémentaire sera disponible au besoin.

Dans l'image officielle du projet des fonctionnalités d'audit sont mises en place. Il est formellement défendu de faire un montage des autres partitions, sous peine de se voir attribuer la note 0 pour le projet.

# INFRASTRUCTURE DU RESEAU

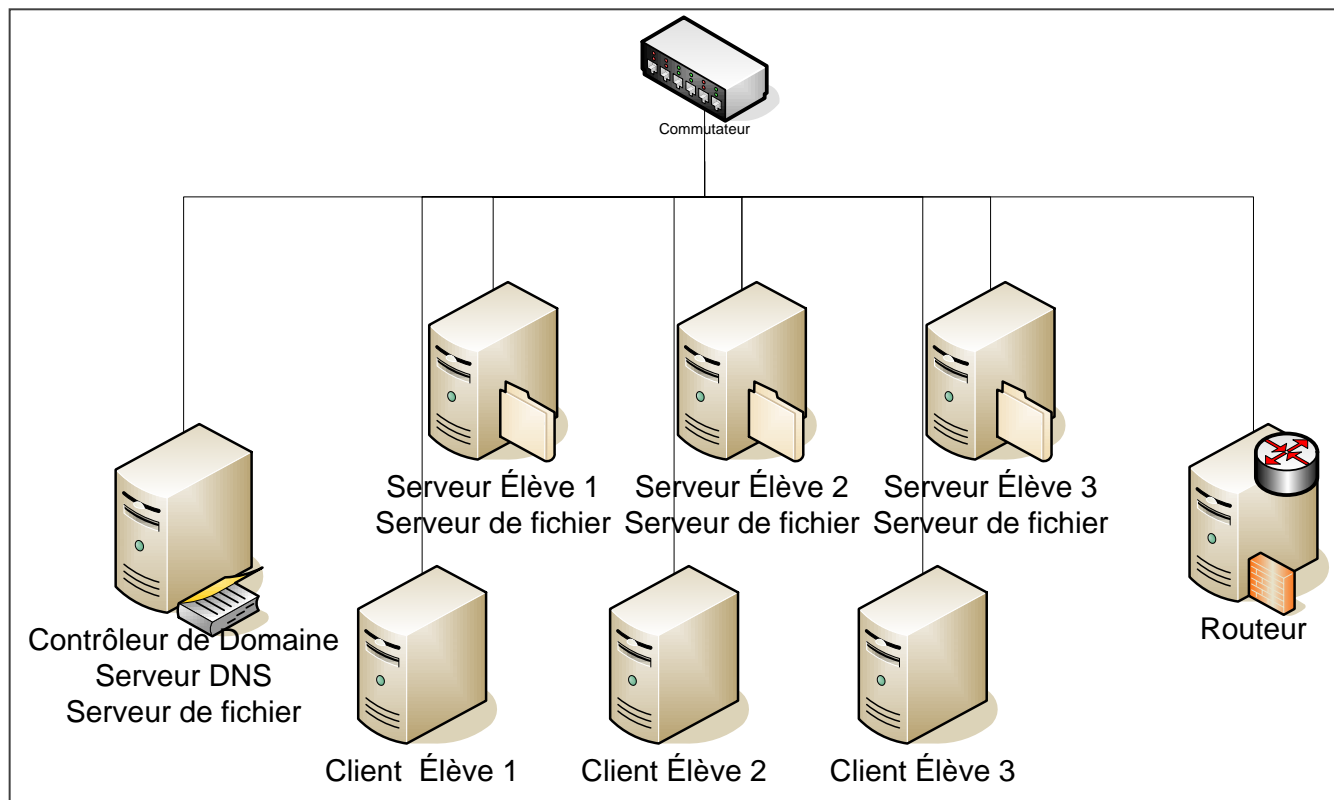
## Le domaine

Vous devez installer un réseau corporatif sous Active Directory. Le nom du domaine est laissé à votre choix, mais doit obligatoirement se terminer par le TLD «.PRO».

Le niveau fonctionnel du domaine sera le plus élevé possible. Un serveur DNS sera présent sur ce serveur et contiendra tous les enregistrements relatifs à l'Active Directory.

En plus du contrôleur de domaine, quatre serveurs et trois «Windows 8» seront membre du domaine.

L'utilisateur «Administrateur» est disponible pour les trois premières heures du projet. Par la suite vous devrez utiliser votre propre utilisateur administrateur. (Voir la section des utilisateurs)



# Les cartes réseaux

Tous les serveurs auront deux cartes réseau, mais seules les cartes utilisées devront être activées. Sur les cartes actives, seule la pile IPv4 devra être fonctionnelle. Attention sur les serveurs où sera installé le rôle Hyper-V, selon le type de commutateur virtuel créé vous devrez modifier le nom de la carte virtuelle afin de respecter les configurations.

## Le plan d'adressage du domaine

Votre réseau privé (corporatif) devra utiliser un plan d'adressage privé de classe B. La classe d'adresse qui vous est attribuée se trouve dans l'annexe «Plan d'adressage privé». À l'intérieur du plan d'adressage de l'équipe, chaque équipier devra s'attribuer des adresses dont il sera le seul mandataire. À part l'adresse principale, toutes les adresses supplémentaires devront être attribuées par programmation.

Tous les serveurs auront une ou plusieurs adresses statiques, selon leur rôle. Vous devez optimiser le nombre d'adresses IP nécessaire. Le nom de la carte réseau desservant votre réseau corporatif doit obligatoirement se nommer «SEGA». Nom de la carte contenant la configuration IP avant l'installation d'Hyper-V.

## Le plan d'adressage du réseau public

Pour ce qui est de votre réseau public la plage d'adresses qui vous est attribuée se trouve dans l'annexe «Plage d'adresses publiques». À l'intérieur de la plage d'adresses publiques, chaque équipier devra s'attribuer des adresses dont il sera le seul mandataire. Toutes les adresses supplémentaires dont vous êtes le mandataire devront être attribuées par programmation.

Vous avez la responsabilité de deux ordinateurs du réseau public, votre routeur et un client externe. Le serveur ayant le rôle du routeur aura deux cartes réseau à configurer. Sur votre routeur, le nom de la carte réseau publique sera «WAN». Pour les équipes de trois, ce nom sera modifié lors de l'installation du rôle Hyper-V.

Pour ce qui est des adresses de votre fournisseur Internet, voici les adresses importantes à connaître :

- Routeur : 10.57.1.1
- Serveurs DNS : 10.57.4.28, 10.57.4.29

---

# LES SERVEURS

---

## Description

Les ordinateurs que vous aurez à votre disposition tiendront des rôles très précis. Sur tous ces ordinateurs sera installée une version de Serveur 2012.

Un ordinateur sera le contrôleur de domaine. De plus il sera le serveur DNS corporatif et le serveur web corporatif.

Trois serveurs seront les postes de travail personnels de chaque élève de l'équipe. Ces serveurs seront aussi serveur web pour chaque département. Ils hébergeront un système Windows 8, sous Hyper-V, afin de faire les tests sur vos implantations.

Un ordinateur sera le routeur.

Sur le routeur pour les équipes de trois membres, on trouvera un système Serveur 2012 sous Hyper-V, afin de jouer le rôle de serveur DNS public et de poste client pour les tests de l'extérieur de la corporation.

Pour les équipes de deux membres un sixième ordinateur tiendra le rôle de serveur DNS public et de poste client pour les tests de l'extérieur de la corporation. Aucune installation Hyper-V ne sera nécessaire sur le routeur.

Sur les serveurs vous ne devez installer que les rôles et fonctionnalités qui sont nécessaires. Tous ce qui est superflu sera en évaluation négative.

## Particularités des serveurs personnels

Chaque serveur personnel devra avoir toutes les consoles nécessaires afin de permettre la gestion de toutes les fonctionnalités du domaine. Sur le bureau de votre utilisateur personnel une console MMC devra être sauvegardé sous le nom «GESTION» et contenir toutes les consoles appropriées.

## Bureau à distance

Chaque serveur, serveurs personnels, routeur et contrôleur de domaine, devra avoir la fonctionnalité «Bureau à distance» d'activée. Il ne faudra autoriser que les connexions avec authentification NLA.

Sur tous les serveurs les membres du groupe «Administrateurs» pourront bénéficier de l'accès bureau à distance. Sur votre serveur personnel vous devrez aussi permettre à vos «gestionnaires» de département de bénéficier de cet outil. Prenez note qu'il n'est pas question d'un groupe commun de gestionnaire pour l'équipe, mais bien de groupe de département.

Les accès seront possibles à l'interne de la corporation, mais pour les serveurs personnels, il devra aussi être possible de faire des accès de l'externe. Les noms utilisés pour l'accès à l'externe seront le prénom de l'élève ayant la responsabilité du serveur. Vous devrez utiliser la zone externe spécifiée dans la section DNS.

Vous pouvez utiliser le bureau à distance lors de vos accès sur les autres serveurs, comme le contrôleur de domaine et le routeur. Souvenez-vous que vous ne disposez que de deux licences. Dans toutes les équipes, la règle sera de fermer sa session dès que le travail est effectué de façon à éviter les conflits.

## Hyper-V sur les serveurs personnels

Chaque serveur personnel devra avoir le rôle Hyper-V d'installé. Un fichier VHDX contenant «Windows 8» est mis à votre disposition pour agir comme poste client.

Une fois le rôle installé les noms de la nouvelle carte réseau devra être «SEGA\_CONFIG». Le type de carte réseau virtuelle devra permettre la communication avec votre serveur.

Le fichier de l'ordinateur virtuel se trouve dans le dossier C:\\_VirDisque. La création de l'ordinateur virtuel devra être localisée dans le dossier C:\\_VirOrdi.

La création de l'ordinateur virtuel devra se faire par script. Ce qui inclut la création du commutateur virtuel approprié, la mémoire dynamique devra être activée, 1024 mo de départ jusqu'à un maximum de 2048 mo. La touche «NumLock» devra être active. Aucun chemin de dossier ne pourra être explicitement présent dans la programmation.

# Particularités des postes clients

Une fois l'installation du Windows terminée vous devrez joindre ce poste à votre domaine, et y faire toutes les installations requises pour respecter les spécifications du cahier de charge. L'objet ordinateur représentant votre poste client devra être déplacé dans l'unité d'organisation «Ordinateurs» sous l'unité de votre département.

Sur chaque client Chrome et Filezilla devront être installés.

Comme pour les serveurs le nom de la carte réseau donnant accès à votre réseau corporatif doit obligatoirement se nommer «SEGA».

---

## LES SERVEURS DE FICHIERS

---

Les cinq ordinateurs de votre corporation seront utilisés comme serveurs de fichiers. Tous les dossiers créés sur les serveurs de fichiers devront l'être sous des dossiers précis, sous le «C:\». Voici la liste des dossiers racines que vous devez obligatoirement utiliser :

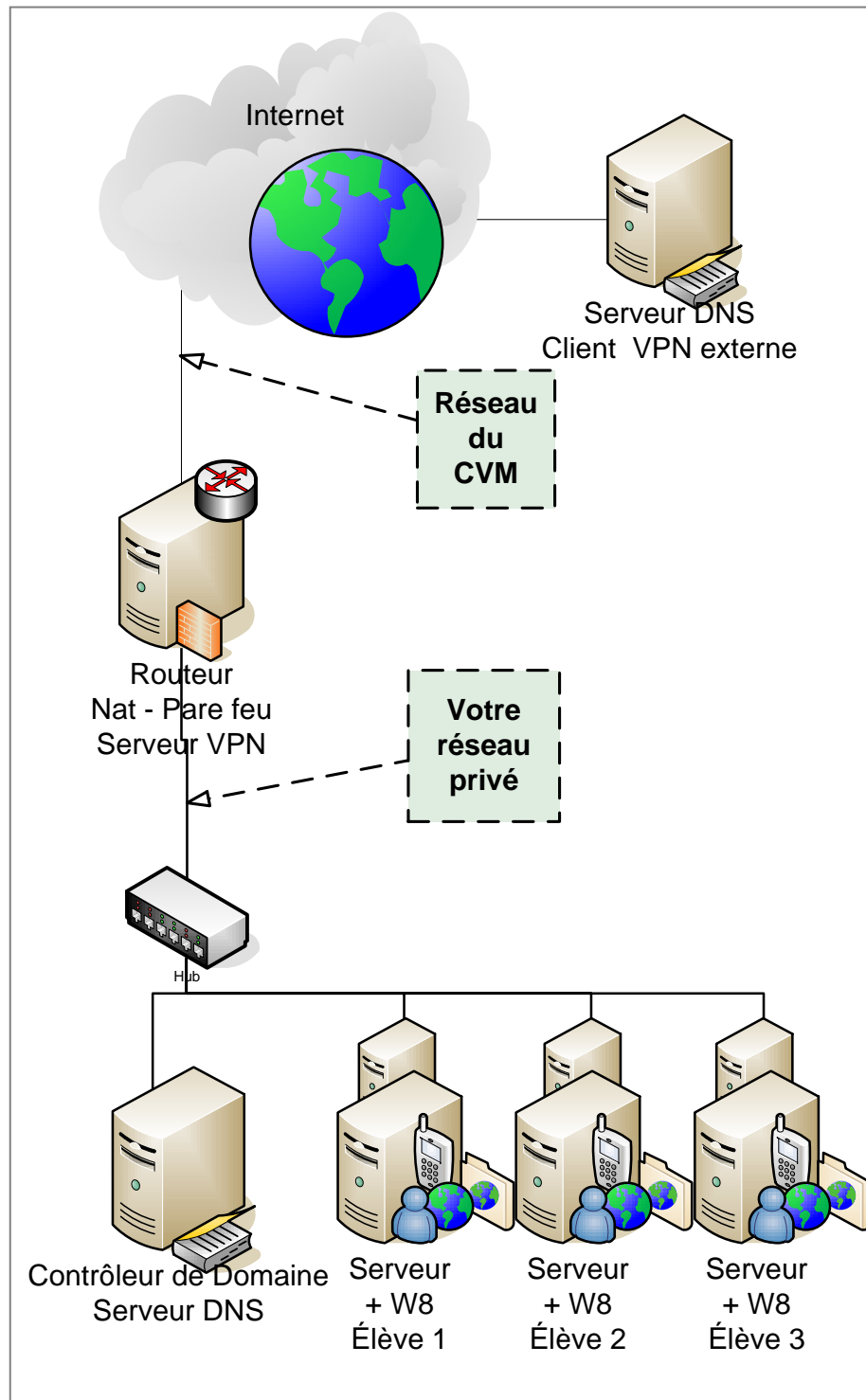
- «\_SEGA», pour les dossiers qui sont à l'équipe ;
- «\_SEGA\_ART», pour les dossiers de l'élève qui est responsable du département artistique ;
- «\_SEGA\_PROG», pour les dossiers de l'élève qui est responsable du département de programmation ;
- «\_SEGA\_SYS», pour les dossiers de l'élève qui est responsable du département système.

Chacun des dossiers ajoutés sous ses dossiers racines devra porter un nom significatif et être documenté dans les rapports du projet.

Aucun des dossiers racines ne devra être partagé. Lors de la correction seuls ces dossiers seront vérifiés.

Vous trouverez plus de détails sur les dossiers à créer dans la section se rapportant aux utilisateurs de votre département.

# Le diagramme de l'infrastructure





---

# LE ROUTEUR

---

Ce serveur sera membre de votre domaine, et fera le lien entre votre réseau et Internet via ses deux cartes réseau. Le routeur cumulera plusieurs fonctions, il sera :

- Serveur NAT pour l'accès des postes à l'intérieur de votre réseau vers Internet;
- Pare-feu;
- Serveur VPN, afin de permettre l'accès de l'extérieur vers votre réseau corporatif.
- Pour les équipes de trois personnes il hébergera le client externe (voir la section «Client externe»)

L'installation du routeur est un travail d'équipe, sauf pour certains paramétrages du pare-feu.

Vous devez modifier le mode de démarrage du service routeur. Par défaut ce mode est à «Automatique différé» vous devez le mettre à «automatique».

## NAT et le pare-feu

La carte réseau connectée au collège jouera le rôle de carte publique (fournisseur Internet). Les fonctionnalités de pare-feu devront être activées sur la carte publique. Mais une certaine «ouverture» devra être présente. Vous devrez laisser passer:

- Les requêtes WEB pour certains sites ;
- Les requêtes FTP pour certains sites ;
- Les fonctionnalités de VPN.

En équipe vous devez créer un pool d'adresses publiques suffisant pour satisfaire tous les besoins spécifiés dans le cahier de charge. Vous devez aussi paramétrer le pare-feu pour les besoins corporatif.

Individuellement vous devez faire les redirections de port pour les besoins de votre département.

# VPN

Le serveur VPN ne supportera que le nombre de ports spécifiés pour chaque type de connexions

- «WAN Miniport (IKEv2)» à 3 ports
- «WAN Miniport (SSTP)» à 3 ports
- «WAN Miniport (PPTP)» à 3 ports
- «WAN Miniport (L2TP)» à 3 ports

L'accès au VPN pourra se faire autant par adresse que par nom. L'accès par nom se fera à l'aide du nom «VPN» dans la zone externe spécifiée dans la section DNS.

Tous les membres du groupe «administrateurs», ainsi que vos utilisateurs de type «gestionnaires» de votre département auront le droit d'utiliser l'accès VPN. Ce droit devra être établi par stratégie de groupe.

Votre utilisateur «administrateur» aura une adresse qui lui sera spécifiquement réservée, via les propriétés des utilisateurs.

Vos utilisateurs de type «gestionnaires» auront une adresse distribuée par un pool d'adresses commun sur le routeur. Prévoir assez d'adresses client pour le maximum de connexions possibles.

Une connexion VPN portant le nom de votre domaine devra être créée sur le «client externe».

## Hyper-V sur le routeur

Dans les équipes de trois personnes le routeur devra avoir le rôle Hyper V d'installé. Un fichier VHDX contenant un «Serveur 2012» est mis à votre disposition pour agir comme poste client externe.

Une fois le rôle installé les noms de la nouvelle carte réseau devra être «WAN\_CONFIG». Le type de carte réseau virtuelle devra permettre la communication avec l'adresse publique de votre routeur.

Le fichier de l'ordinateur virtuel se trouve dans le dossier C:\\_VirDisque. La création de l'ordinateur virtuel devra être localisée dans le dossier C:\\_VirOrdi.

La création de l'ordinateur virtuel devra se faire par script. Ce qui inclut la création du commutateur virtuel approprié, la mémoire dynamique devra être activée, 1024 mo de départ jusqu'à un maximum de 2048 mo. La touche «NumLock» devra être active. Aucun chemin de dossier ne pourra être explicitement présent dans la programmation.

---

## L'AUTORITÉ DE CERTIFICATION

---

Sur votre contrôleur de domaine, vous devrez installer une autorité de certification. Cette autorité servira à émettre les certificats pour tous les accès web sécurisés.

Vous devez paramétrer l'autorité en respectant les caractéristiques suivantes:

- L'autorité ne doit pas porter le nom du serveur qui l'héberge
- Le nom de l'autorité de certification doit commencer par les lettres «GOV» et ne doit pas dépasser 10 caractères
- L'autorité sera de type «Entreprise»
- La durée de validité du certificat sera d'un mois
- Redémarrer le contrôleur de domaine après l'installation de ce rôle

---

## LE SERVEUR SMTP

---

Un serveur SMTP devra être installé sur le contrôleur de domaine. Ce serveur sera utilisé pour toute la corporation quand des messages devront être envoyés pour des dépassements de quotas

---

# LES SERVEURS DNS

---

Deux serveurs DNS devront être implantés pour le projet. Un serveur interne à la corporation que nous nommerons «serveur DNS Privé», et un serveur externe que nous nommerons «serveur DNS Public». Le nom des zones hébergées sur chaque serveur sera différent.

## DNS privé

Ce serveur DNS sera localisé sur le contrôleur de domaine. Il doit être installé avant que le domaine soit créé. Il aura deux fonctions, la première sera de supporter toutes les informations relatives à l'Active Directory comme le demande Microsoft dans ses spécifications. Sa deuxième fonction sera de contenir toutes les zones et les enregistrements nécessaires à l'intérieur de la corporation.

La zone directe principale pour le domaine, sera automatiquement créée lors de la création du domaine (NomDomaine.**PRO**). Vous devrez vérifier sa présence et valider ses enregistrements.

Ce serveur DNS devra avoir un redirecteur vers votre DNS public.

## DNS public

Ce serveur DNS sera installé sur votre «Client externe». Vous devrez le paramétrer afin de permettre l'accès aux ressources de votre réseau corporatif à partir de postes partout à travers le monde.

Toutes les ressources où l'on vous demande des accès de l'extérieur devront pouvoir l'être à l'aide d'un nom pleinement qualifié. Pour différencier les accès de l'extérieur une zone «NomDomaine.**PRE**» devra être créée.

Vous devrez configurer ce serveur DNS de façon similaire à celui d'un fournisseur d'accès Internet. Ce serveur DNS devra avoir des redirecteurs vers les DNS du collègue

Vous devrez y mettre les enregistrements pertinents pour faire les accès publics spécifiés Par exemple: Web, VPN, Bureau à distance.

---

# LE SERVEUR IIS CORPORATIF

---

Le serveur IIS corporatif sera localisé sur le contrôleur de domaine. Les services de rôles nécessaires devront être installés en fonction des spécifications des sites Web et des sites FTP corporatif que le serveur doit héberger.

## Site WEB corporatif

Un site WEB corporatif devra être configuré. Voici les caractéristiques auxquelles ce site doit répondre :

- Type de site
  - Par adresse
  - Utiliser l'adresse privée principale du contrôleur de domaine
  - Port 80
- Authentification
  - Site en accès anonyme
- Référence privée
  - Le nom du site sera «www»
  - Ce site sera dans la zone DNS de votre domaine de l'Active Directory
- Référence publique
  - L'adresse publique principale du routeur
  - Le nom du site sera «www»
  - Ce site sera dans une zone publique (voir section DNS public)
- Hébergement
  - La localisation physique du répertoire de ce site se trouve sur le contrôleur de domaine dans le dossier C:\\_SEGA\WEB.
- Contenu
  - La page «Index» qui sera affichée doit contenir
    - Le nom de votre compagnie
    - Le nom de chaque membre de l'équipe

Ce site devra être accessible de l'intérieur et de l'extérieur de la corporation.

# Site WEB sécurisé corporatif

Un site WEB sécurisé devra être configuré. Voici les caractéristiques auxquelles ce site doit répondre :

- Type de site
  - Par adresse
  - Port 80, 443
  - Exiger le SSL pour la connexion
- Authentification
  - Site en accès anonyme
- Référence privée
  - Le nom du site sera SSS
  - Ce site sera dans la zone DNS de votre domaine de l'Active Directory
- Hébergement
  - La localisation physique du répertoire de ce site se trouve sur le contrôleur de domaine dans le dossier C:\\_SEGA\WEBSEC.
- Contenu
  - La page «Index» qui sera affichée doit contenir
    - La mention de site sécurisé
    - Le nom de la corporation
    - L'adresse du site
    - Le nom de l'élève responsable

Ce site devra être accessible seulement de l'intérieur de la corporation.

# Site FTP corporatif

Un site FTP corporatif devra être configuré. Voici les caractéristiques auxquelles ce site doit répondre :

- Type de site
  - Par adresse
  - Utiliser l'adresse privée principale du contrôleur de domaine
  - Port 21
- Authentification
  - Anonyme en lecture seulement, pour l'accès anonyme vous devez utiliser l'utilisateur «WEB» au niveau du domaine.
  - En authentification de base pour les membres des groupes «administrateurs» en lecture écriture
- Référence privée
  - Le nom du site sera «CORPO»
  - Ce site sera dans la zone DNS de votre domaine de l'Active Directory
- Référence publique
  - L'adresse publique principale du routeur
  - Le nom du site sera «EXTRANET»
  - Ce site sera dans une zone publique (voir section DNS public)
- Contenu
  - Au moins un fichier portant un nom significatif
  - La localisation physique du répertoire se trouve sur le contrôleur de domaine dans le dossier C:\\_SEGA\FTP.

Ce site FTP devra être accessible de l'intérieur et de l'extérieur de la corporation.

Note: pour tester votre site FTP de l'extérieur vous devez forcer FileZilla à utiliser le mode ACTIF.

# STRATÉGIES DE GROUPE CORPO

Au niveau de la corporation vous devrez implanter plusieurs stratégies. Chaque élève de l'équipe est responsable d'implanter une stratégie selon sa tâche. Les noms de stratégies devront être respectés. Lors de la préparation du projet chaque élève doit préparer sa stratégie, en faire une copie de sécurité. Lors de la production chaque élève est responsable d'importer sa stratégie et de s'assurer de son exécution.

Équipe à 3 (TRIO):

1. Sécurité
2. Accès
3. Employé

Équipe à 2 (DUO):

1. Sécurité
2. Accès

Le tableau suivant cible les éléments de stratégies qui doivent être programmés. Il est formellement interdit d'ajouter d'autres éléments dans ces stratégies. De plus il est interdit de modifier les stratégies de domaine implantées par défaut.

Élément de stratégie	TRIO	DUO
Conserver l'historique des mots de passe pour les 10 derniers	1	1
Longueur minimale du mot de passe de 9 lettres	1	1
Durée de vie minimale du mot de passe à 0	1	1
Durée de vie maximale du mot de passe à 10	1	1
Ouverture de session interactive: prévenir l'utilisateur qu'il doit changer son mot de passe 2 jours avant qu'il n'expire	1	1
Activer la clé de registre «EnableLinkedConnections» à 1	1	1



Ouverture de session interactive : Ne pas afficher le dernier nom d'utilisateur	2	2
Ouverture de session interactive : Ne pas demander la combinaison de touches Ctrl+Alt+Suppr	2	2
Ouvertures de sessions interactives : nombre d'ouverture de sessions précédentes réalisées en utilisant la cache, mettre ce paramètre à 0 ouverture de session.	2	2
Afficher les informations sur les ouvertures de session précédentes au cours d'une ouverture de session utilisateur	2	2
Toujours attendre le réseau lors du démarrage de l'ordinateur et de l'ouverture de session	2	2
Fixer les options de dossiers qui permettront ■ de voir les extensions des fichiers dont le type est connu	2	2
Désactiver le paramètre : Afficher le moniteur d'évènements de mise hors tension	3	1
Arrêt: Permet au système d'être arrêté sans avoir à se connecter	3	1
Activer l'exécution des scripts et sélectionner "Autoriser tous les scripts"	3	1
Lier la lettre N: au partage Netlogon	3	2
Activer «Accès réseau : ne pas autoriser le stockage de mots de passe et d'informations d'identification pour l'authentification du réseau»	3	2
Activer «Supprimer au redémarrage du système les profils utilisateur plus anciens que 2 jours »	3	2

---

## VOTRE «ADMINISTRATEUR»

---

Vous devez vous créer un utilisateur de type «administrateur». Il portera votre prénom et fera partie des mêmes groupes que l'utilisateur Administrateur. Il devra être créé dans le conteneur USERS. Après la première évaluation vous devrez obligatoirement utiliser votre propre utilisateur.

Cet utilisateur devra être créé par script.

Cet utilisateur devra avoir une console de gestion contenant toutes les consoles nécessaires pour faire le travail du projet sur tous les serveurs.

---

# LE DÉPARTEMENT SYSTÈME

---

Tout ce qui suit concerne votre département et se trouve à être sous votre entière responsabilité.

Comme nous l'avons mentionné dans l'introduction dans le département «système» vous retrouverez les employés suivants:

- ▣ Les responsables du support
  - On-line, 10 utilisateurs
  - À la clientèle, 15 utilisateurs
- ▣ Les architectes d'infrastructure, 8 utilisateurs
- ▣ Les responsables des déploiements, 17 utilisateurs
- ▣ Les analystes
  - En sécurité, 12 utilisateurs
  - En stockage, 13 utilisateurs.

Les soixante-quinze employés du département «Système» devront être regroupés dans des unités d'organisation définissant chaque type de métiers. Il y aura donc six unités d'organisation de métier. De plus vous devrez regrouper les deux types d'employés de structure sous une même unité globale. Vous devrez faire de même pour les différents analystes. Toutes ces unités seront sous une unité représentant votre département et se nommant «SYSTEME».

À partir de l'analyse des stratégies de groupe que vous aurez à implanter vous pouvez ajouter des unités d'organisation si vous le jugez nécessaire. Votre structure d'unités et votre implantation de stratégies devront être intimement liées et devront être justifiées lors de la rencontre d'évaluation du 16 mai.

Lors de cette rencontre vous devrez présenter et expliquer votre fichier Visio schématisant votre structure d'unités d'organisation et les liens vers vos objets de stratégies de groupe. Ce fichier devra être aussi remis électroniquement.

---

# LES UNITÉS D'ORGANISATION

---

En plus des unités servant à rassembler vos utilisateurs, vous devrez avoir une unité dédiée à contenir vos postes clients. Cette unité se trouvera directement sous l'unité de votre département, et portera le nom «Ordinateurs». Dans le cadre du projet cette unité ne contiendra qu'un seul objet ordinateur, votre Windows 8 virtuel.

Tous les noms de vos unités d'organisation ne devront comporter aucun espace, ni caractère accentué.

La création de votre structure d'unité d'organisation doit se faire via un script Power Shell qui lira le nom de vos unités dans un fichier CSV. Ce fichier CSV que vous devez créer doit représenter la structure des unités qui a été approuvée.

La création de votre fichier de données devra répondre aux restrictions suivantes :

- Le nom du domaine ne doit pas être présent
- Une ligne de titre
- Une ligne par unité d'organisation à créer.
  - Les descriptions ne sont pas nécessaires
  - Mettre les champs que vous jugez nécessaires

---

# LES UTILISATEURS ET LES GROUPES

---

## Généralités sur les utilisateurs

Tous vos utilisateurs auront

- Le même mot de passe.
- Un profil qui sera errant et modifiable.
- Un répertoire personnel

Tous vos utilisateurs devront obligatoirement avoir les propriétés suivantes :

- un prénom, un nom et un nom affiché
- les propriétés UserPrincipalName et SamAccountName
- une description, se rapportant à votre département et qui peut être la même pour tous
- une adresse complète, avec code postal
- des options de compte (compte actif, le mot de passe doit pouvoir être changé)
- un chemin du profil
- un dossier personnel
- Trois numéros de radio messagerie

Tous les noms de vos utilisateurs devront répondre aux règles de nomenclature suivantes :

- Commenceront par la même lettre,
- Suivi des six premiers caractères du nom, ou moins si le nom ne contient pas le nombre suffisant
- Suivi des trois premiers caractères du prénom, ou moins si le prénom ne contient pas le nombre suffisant

Tous les utilisateurs de votre département seront soumis aux spécifications suivantes, quel que soit l'ordinateur sur lequel ils se connectent:

- Ajouter la variable d'environnement «\_DEPT» avec la valeur «SYSTEME»

# Les groupes

La création de groupes est fortement recommandée pour éviter de donner des droits aux utilisateurs à la pièce. Mais pour chaque groupe créé, il devra y avoir au moins

- une description (onglet général) description
- un nom de groupe antérieur à Windows 2000 (onglet général)

Tous les groupes devront être de type «Domaine Local». Tous vos noms de groupe devront débiter par la même lettre que vos utilisateurs.

L'emplacement des objets «groupe» dans votre Active Directory est laissé à votre discrétion, mais je vous recommande fortement de tous les mettre directement sous l'unité d'organisation de votre département.

# La programmation

Tous les utilisateurs et groupes de votre département devront être créé par programmation en PowerShell.

Pour vos utilisateurs de département un fichier CSV contenant les informations obligatoires est mis à votre disposition. Vous n'avez pas le droit de modifier ce fichier.

Les noms doivent être utilisés séquentiellement et vous devez vous assurez de l'unicité de vos noms de login.

Pour vos groupes vous devrez créer votre propre fichier csv.

Que la création soit une réussite ou un échec vous devez créer un fichier de log permettant d'avoir un suivi de votre exécution. Un seul fichier de log doit être utilisé pour vos créations d'utilisateurs et de groupes.

**N.B. Recréer les utilisateurs et les groupes durant le projet, a un impact direct sur les attributions des droits NTFS. Même si les utilisateurs portent les mêmes noms, leur SID est différent. Les droits NTFS font toujours référence aux SID.**

---

# LES SERVEURS DE FICHIERS

---

Tous les dossiers créés sur les serveurs de fichiers devront l'être sous un dossier précis, sous le «C:\». Dans votre cas ce dossier portera le nom «\_SEGA\_SYS». Ce dossier ne devra pas, en aucun cas, être partagé. Lors de la correction seul le contenu de ce dossier sera vérifié.

Chacun des dossiers ajoutés sous ce dossier devra porter un nom significatif et être documenté dans les rapports appropriés.

## Les dossiers personnels

Tous vos utilisateurs devront avoir un répertoire personnel, auquel aucun autre utilisateur du domaine n'aura accès à part eux-mêmes. Des droits appropriés devront être donnés sur ces répertoires. Les administrateurs devront conserver leur droit sur ces répertoires. Afin de vous faciliter votre gestion il est permis de donner l'autorisation «Contrôle total» à votre utilisateur personnel sur ces dossiers.

Le partage du dossier racine de vos dossiers personnels sera un partage non publié. L'énumération basée sur l'accès devra être activé.

Lors de leur login vos utilisateurs, grâce à leurs propriétés, auront accès à leur répertoire personnel via la lettre S:

## Les dossiers de profils

Les dossiers de profil de vos utilisateurs seront sur votre serveur personnel.

Le partage du dossier racine de vos profils sera un partage non publié. L'énumération basée sur l'accès devra être activé.

Les administrateurs devront conserver leur droit sur ces répertoires. Afin de vous faciliter votre gestion il est permis de donner l'autorisation «Contrôle total» à votre utilisateur personnel sur ces dossiers.

# Les dossiers du département

Des dossiers communs sont mis à la disposition des utilisateurs de votre département. Ces dossiers sont :

- La documentation pour le support
- La documentation pour les déploiements
- Les copies de sécurité
- La documentation de l'architecture

## Autorisations sur les dossiers

Tous vos gestionnaires auront le droit de modifier sur tous ces dossiers.

Pour le dossier de documentation pour le support

- Tous vos utilisateurs auront le droit de lecture-exécution
- Tous les responsables du support auront le droit de modifier.

Pour le dossier de documentation pour les déploiements

- Tous les responsables du déploiement auront le droit de modifier.
- Tous les responsables du support auront le droit de lecture-exécution.
- Tous les architectes d'infrastructure et tous les analystes n'auront aucun droit.

Pour le dossier des copies de sécurité

- Tous les responsables du déploiement et tous les responsables du support auront le droit de modifier.
- Tous les architectes d'infrastructure n'auront aucun droit.
- Tous les analystes auront le droit de lecture-exécution.

Pour le dossier de documentation de l'architecture

- Tous les architectes d'infrastructure auront le droit de modifier.
- Tous les responsables du déploiement n'auront aucun droit.
- Tous les responsables du support et tous les analystes auront le droit de lecture-exécution.

L'énumération basée sur l'accès devra être activé sur le partage de chacun de ces dossiers.



## Emplacement des dossiers

La documentation pour le support sera sur le «contrôleur de domaine»

La documentation pour les déploiements sera sur le serveur «Artistique»

Les copies de sécurité sera sur le serveur «Programmation» et sera répliqué sur le «routeur» à l'aide d'une DFS.

La documentation de l'architecture sera sur votre serveur personnel

## Les espaces de noms

Vous devez créer un espace de noms DFS de type « Domaine » contenant des liens vers vos quatre dossiers de «département». L'espace nom DFS sera emmagasinée sur votre serveur personnel. L'énumération basée sur l'accès devra être activé sur la structure DFS.

Le dossier DFSROOT devra être utilisé, mais devra être relocalisé sous votre dossier «\_SEGA\_SYS».

Par stratégie, pour tous vos utilisateurs du département la lettre T: sera un lien vers cet espace de noms.

Les répertoires personnels ne doivent pas apparaître dans l'espace de noms DFS.

Le dossier de téléchargement nécessaire pour la redirection devra être présent dans votre espace de noms.

## Les autorisations NTFS

L'attribution des autorisations devront être optimisée en fonction des usages de chaque dossier. Quand vous devez créer une structure de dossier, vous devez contrôler l'héritage des autorisations. Les dossiers racines seront créés par programmation.

Lors de la correction, section exécution, si les accès aux dossiers fonctionnent parce que les autorisations NTFS sont excessives (Modification ou Contrôle total aux utilisateurs du domaine) la note 0 sera attribuée.

## Les partages

Tous les partages devront être créés avec des noms significatifs. L'attribution des droits de partage devra être faite selon des normes facilitant l'administration. Pour chaque partage qui contient une série de sous-dossiers, pour lesquels les autorisations NTFS sont limitées, l'énumération basée sur l'accès devra être activée.

Je vous recommande de bien vérifier avec vos coéquipiers les noms qu'ils utiliseront pour leur partage afin de ne pas créer de duplicata de nom dans votre domaine.

Les partages seront créés par programmation.

## Programmation

Tous les partages, autorisations de partage, les propriétés de partage, les dossiers racine et les autorisations NTFS seront créés par script Power Shell.

Les sous-dossiers relatifs aux utilisateurs seront créés en même temps que la création des utilisateurs.

Toutes les créations de dossiers, de partages et l'attribution des autorisations doivent se faire à partir de votre serveur personnel.

---

# LES QUOTAS DE DOSSIERS

---

## Description des quotas

Vous devez créer différents quotas de dossier pour votre division. Tous les quotas devront obligatoirement être faits à partir de modèle.

Grâce au serveur SMTP, tous les messages d'avertissement des utilisateurs de votre division devront être envoyés par courriel à votre utilisateur administrateur. Vous devez utiliser l'adresse «ProjetReseauH13@hotmail.com».

Tous vos quotas devront générer un avertissement par courriel quand l'occupation des dossiers atteints 10%.

Tous les répertoires personnels seront soumis à un quota automatique inconditionnel de 400 mo avec un avertissement à 390 mo.

Tous les répertoires de profil seront soumis à un quota automatique inconditionnel de 500 mo avec un avertissement à 490 mo.

Tous les dossiers de département devront avoir un quota de dossier de 200 mo, conditionnel, avec un avertissement à 190 mo.

Si vous désirez vous pouvez programmer d'avance vos modèles et quotas. Tous les cmdlets sont disponibles dans le module «FileServerResourceManagen».

## Les rapports de quotas

Un rapport sur l'utilisation de tous vos quotas de dossiers de tous les serveurs de fichiers où vous en avez devra être généré au maximum trente minutes avant votre évaluation finale.

Les rapports devront être en format html.

Si vous désirez vous pouvez programmer d'avance vos rapports. Tous les cmdlets sont disponibles dans le module «FileServerResourceManagen».

---

# LES STRATÉGIES DE GROUPE

---

Dans votre département l'utilisation des stratégies de groupe, section stratégie et section préférence, pour gérer l'environnement du domaine et des utilisateurs de votre département est obligatoire.

Le choix de l'implantation doit être fait selon des critères qui minimiseront le travail des administrateurs du réseau. Plus précisément on cherche à éviter le filtrage de sécurité si possible. De plus pour une même «unité» on ne désire pas retrouver les mêmes paramètres dans deux stratégies différentes.

Les sections non utilisées des stratégies devront être désactivées. Vous devrez être en mesure de justifier les liaisons, le filtrage et toute autre propriété activée pour chacun des objets de stratégie.

**N.B. Si vous décidez d'utiliser le ciblage ou le filtrage de sécurité dans vos stratégies lors des importations de vos GPO vous devrez refaire vos liens. Même si les utilisateurs ou groupes portent les mêmes noms, leur SID est différent.**

## Stratégie pour les postes client

Tous les ordinateurs clients de votre département devront être soumis aux paramètres suivants

- Ouverture de session interactive : contenu du message pour les utilisateurs essayant de se connecter
- Ouverture de session interactive : titre du message pour les utilisateurs essayant de se connecter
- Désactiver «Afficher l'animation à la première connexion»
- Activer «Ne pas ouvrir de session pour les utilisateurs avec des profils temporaires»
- Activer «Ne pas vérifier les utilisateurs propriétaires des dossiers Profils itinérants»
- Activer «Supprimer les copies mises en cache des profils itinérants»

Il s'agit ici bien entendu, de votre poste Windows 8 virtuel. Il est considéré comme un poste client spécifique à votre département.

# Votre département

Tous les utilisateurs de votre département devront bénéficier des paramètres suivants :

- Ne pas afficher le bouton «Affichage du mot de passe»
- Créer un raccourci sur le bureau vers une invite de commande
- Forcer un écran de veille spécifique «Rubans»

## Section «Analystes»

Dans ces utilisateurs il y aura 3 utilisateurs que vous choisirez qui seront gestionnaires. Tous les gestionnaires seront dans la sous-section «sécurité».

Tous les utilisateurs de cette section devront bénéficier des paramètres suivants :

- Attribuer un papier peint spécifique pour le bureau, une image des forces de l'ordre
- Forcer un écran de veille spécifique «Bulles»
- «Démarrer l'Explorateur de fichiers avec le ruban réduit», avec l'option «Toujours ouvrir de nouvelles fenêtres de l'Explorateur de fichiers avec le ruban réduit»
- Créer une redirection pour le dossier «Documents» vers leurs répertoires personnels

Seulement les utilisateurs de la sous-section «sécurité» devront bénéficier des paramètres suivants :

- Ne pas déplacer les fichiers supprimés vers la Corbeille

Seulement les utilisateurs de la sous-section «stockage» devront bénéficier des paramètres suivants :

- Empêcher l'accès aux outils de modifications du Registre et désactiver l'exécution silencieuse de regedit.exe
- Créer une variable d'environnement DOSSIER contenant le mot «Stockage»
- Les options de dossiers ne permettront de voir les extensions

## Section «Supports»

Dans ces utilisateurs il y aura 6 utilisateurs que vous choisirez qui seront gestionnaires. Il y aura 3 gestionnaires dans la sous-section «on-line» et 3 gestionnaires pour la sous-section «clientèle».

Tous les utilisateurs de cette section devront bénéficier des paramètres suivants :

- Attribuer un papier peint spécifique pour le bureau, une image d'un téléphone
- Ne pas déplacer les fichiers supprimés vers la Corbeille
- Créer une tâche planifiée à l'ouverture de session qui fera démarrer la calculatrice

Seulement les utilisateurs de la sous-section «on-line» devront bénéficier des paramètres suivants :

- Empêcher l'accès aux outils de modifications du Registre et désactiver l'exécution silencieuse de regedit.exe
- Créer une redirection pour le dossier «Favoris» vers leurs répertoires personnels

Seulement les utilisateurs de la sous-section «clientèle» devront bénéficier des paramètres suivants :

- Aucun accès au panneau de configuration
- «Démarrer l'Explorateur de fichiers avec le ruban réduit», avec l'option «Ne jamais ouvrir de nouvelles fenêtres de l'Explorateur de fichiers avec le ruban réduit»

## Section «Architectes»

Tous les utilisateurs de cette section devront bénéficier des paramètres suivants :

- Attribuer un papier peint spécifique pour le bureau, une image d'un plan
- Forcer un écran de veille spécifique «Bulles»
- Créer un raccourci sur le bureau vers FileZilla
- Les options de dossiers n'auront pas le paramètre «Utiliser l'assistant Partage»

## Section «Déploiements»

Dans ces utilisateurs il y aura 4 utilisateurs que vous choisirez qui seront gestionnaires.

Tous les utilisateurs de cette section devront bénéficier des paramètres suivants :

- Attribuer un papier peint spécifique pour le bureau, une image d'un diagramme de procédure
- «Démarrer l'Explorateur de fichiers avec le ruban réduit», avec l'option «Ne jamais ouvrir de nouvelles fenêtres de l'Explorateur de fichiers avec le ruban réduit»

---

## GESTIONNAIRES DU DÉPARTEMENT

---

### Stratégies de groupe

Les gestionnaires auront les caractéristiques suivantes :

- Activer «Toujours afficher tous les éléments du Panneau de configuration»
- Créer une redirection pour le dossier «Téléchargements» vers un partage commun.
- Le bouton «Affichage du mot de passe» devra être présent
- Créer un raccourci dans la barre des tâches vers une invite de commande
- Les options de dossiers ne permettront de voir les extensions
- Créer une tâche planifiée à l'ouverture de session qui fera démarrer la console de gestion «Utilisateurs et ordinateurs Active Directory»

Pour la redirection le dossier «TELE» sera situé sur votre serveur personnel sous «C:\\_SEGA\_SYS». Ce dossier devra être partagé et l'énumération basée sur l'accès devra être activé. De plus ce dossier devra être présent dans votre espace de nom. Seuls les gestionnaires de votre département auront les autorisations sur ce dossier.

### Délégation de pouvoir

Tous les gestionnaires présents dans la section «Supports» auront le pouvoir de modifier les mots de passes des utilisateurs de leur section

Les gestionnaires présents dans la sous-section «Sécurité» auront le pouvoir de modifier les mots de passes des utilisateurs de leur sous-section

Les gestionnaires présents dans la section «Déploiements» auront le pouvoir de modifier les mots de passe de tous les utilisateurs de votre département.

---

# LE SERVEUR IIS

---

Vous devez installer un serveur IIS sur votre serveur personnel. Les services de rôles nécessaires devront être installés en fonction des spécifications des sites Web et des sites FTP.

## Site WEB départemental

Un site WEB de département devra être configuré. Voici les caractéristiques auxquelles ce site doit répondre :

- Type de site
  - Par adresse
  - Utiliser l'adresse privée principale de votre serveur
  - Port 80
- Authentification
  - Site en accès anonyme
- Référence privée
  - Le nom du site sera «SYSTEME»
  - Ce site sera dans la zone DNS de votre domaine de l'Active Directory
- Référence publique
  - Une adresse publique du routeur
  - Le nom du site sera «SYSTEME»
  - Ce site sera dans une zone publique (voir section DNS public)
- Hébergement
  - La localisation physique du répertoire de ce site sera C:\\_SEGA\_SYS\WEB sur votre serveur personnel.
- Contenu
  - La page «Index» qui sera affichée doit contenir
    - Le nom de votre département
    - Votre nom

Ce site devra être accessible de l'intérieur et de l'extérieur de la corporation.



# Site WEB sécurisé départemental

Un site WEB sécurisé de département devra être configuré. Voici les caractéristiques auxquelles ce site doit répondre :

- Type de site
  - Par adresse
  - Port 80, 443
  - Exiger le SSL pour la connexion
- Authentification
  - Site en accès anonyme
- Référence privée
  - Le nom du site sera «SECSYS»
  - Ce site sera dans la zone DNS de votre domaine de l'Active Directory
- Hébergement
  - La localisation physique du répertoire de ce site sera C:\\_SEGA\_SYS\WEBSEC sur votre serveur personnel.
- Contenu
  - La page «Index» qui sera affichée doit contenir
    - La mention de site sécurisé
    - Le nom du département
    - L'adresse du site
    - Votre nom

Ce site devra être accessible seulement de l'intérieur de la corporation.

# Site FTP départemental

Un site FTP de département devra être configuré. Nous désirons avoir un site pour chaque utilisateur qui remplit la fonction de responsable de déploiement. Voici les autres caractéristiques auxquelles ce site doit répondre :

- Type de site
  - Par adresse
  - Utiliser l'adresse privée principale du contrôleur de domaine
  - Port 21
  - Isolé dans l'Active Directory
- Authentification
  - En authentification de base pour les utilisateurs responsables du déploiement
- Référence privée
  - Le nom du site sera «FSYS»
  - Ce site sera dans la zone DNS de votre domaine de l'Active Directory
- Localisation
  - La localisation physique dans IIS sera le répertoire C:\\_SEGA sur votre serveur personnel.
  - La localisation réelle des dossiers FTP sera le répertoire C:\\_SEGA\_SYS\FTP sur votre serveur personnel.
- Autorisations NTFS
  - En authentification de base pour les membres des groupes «administrateurs» en lecture écriture
  - Chaque utilisateur ne pourra voir que son propre dossier dans lequel il aura le droit de modification

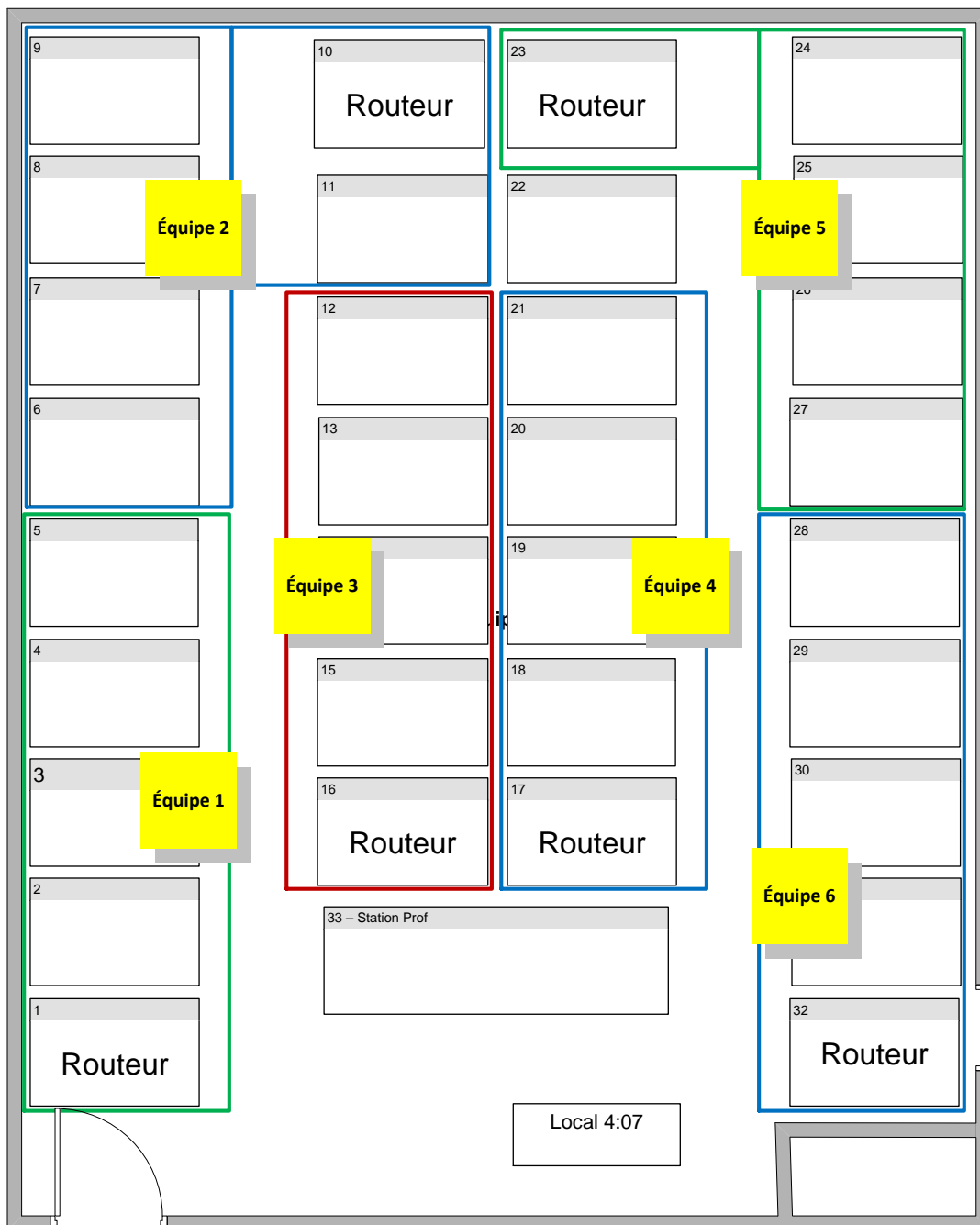
Ce site FTP devra être accessible seulement de l'intérieur de la corporation.

# ANNEXES –ÉLÈVES-ÉQUIPE

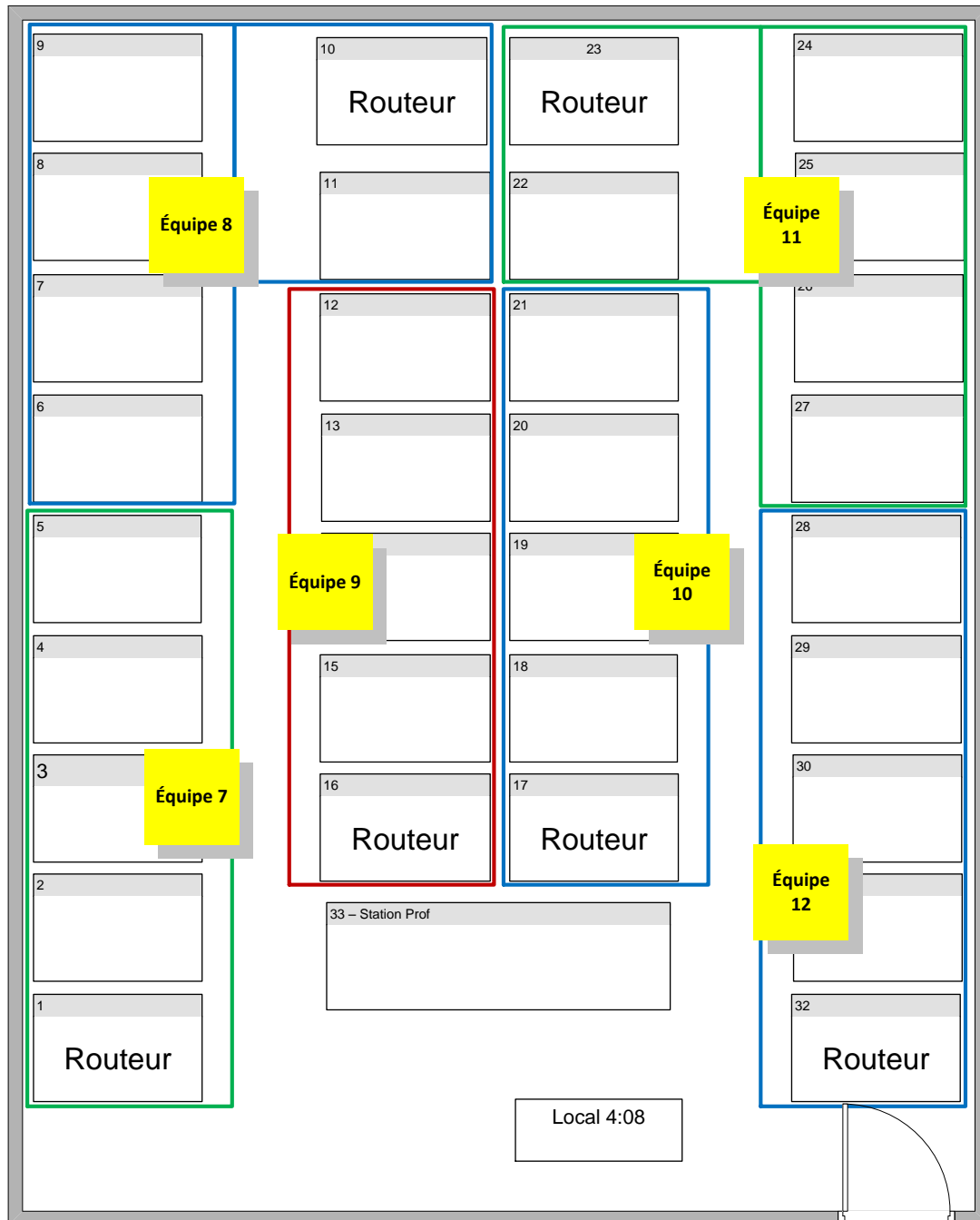
## Listes des numéros de postes

Équipe	Noms	Emplacement
1	Duplan,Chelny; Palanque,Erwan; Tran,Shi-Hui	407 – Postes 1 à 5
2	Charbonneau-Fortin,Michael; Tremblay,François;	407 – Postes 6 à 11
3	DeGagné,Marc-André; Mané,Aboubacar; Païement,Augustin	407 – Postes 12 à 16
4	Boisvert,Carl; Distaulo,Justin; Goudreau,Nathael	407 – Postes 17 à 21
5	Décary,Reno; Paquin,Marc; Waucheul,Nicolas	407 – Postes 23 à 27
6	Côté,Maxime; Majeau,Marc-André; R.parent,Jean-Philippe	407 – Postes 28 à 32
7	Caya,Etienne; Massabot,Raphaël; Olivier,Maxime	408 – Postes 1 à 5
8	Fauteux,Jean-Sébastien; Grenier,Marc;	408 – Postes 6 à 11
9	Martinez,Olivier; Michel,Pierrick; Sidibe,Fatou	408 – Postes 12 à 16
10	Lebrun,David; Massey,Jeff; Singirankabo,CharlesEmmanuel	408 – Postes 17 à 21
11	Bergeron,MarcOlivier; Ryc,Samuel;	408 – Postes 22 à 27
12	Izquierdo,Gonzalo; Martin,Antoine; St-Onge,Francis	408 – Postes 28 à 32

# Localisation des «Routeurs» local 4:07



# Localisation des «Routeurs» local 4:08



# Plan d'adressage privé – corporatif

Les directives sont en fonction de la classe d'adresses privées B

Équipe	No Classe	No sous-réseau	Nb sous-réseau souhaités	Nb hôtes souhaités
1	9	4	<b>12</b>	<b>3200</b>
2	12	5	<b>22</b>	<b>1200</b>
3	7	6	<b>35</b>	<b>800</b>
4	15	4	<b>70</b>	<b>400</b>
5	11	5	<b>14</b>	<b>2400</b>
6	10	6	<b>28</b>	<b>1800</b>
7	4	4	<b>42</b>	<b>600</b>
8	13	5	<b>92</b>	<b>500</b>
9	6	6	<b>15</b>	<b>3500</b>
10	5	4	<b>19</b>	<b>1900</b>
11	14	5	<b>52</b>	<b>700</b>
12	8	6	<b>110</b>	<b>300</b>

## Plan d'adressage public

Equipe	Plage
1	10.57.61.0/16
2	10.57.62.0/16
3	10.57.63.0/16
4	10.57.64.0/16
5	10.57.65.0/16
6	10.57.66.0/16
7	10.57.67.0/16
8	10.57.68.0/16
9	10.57.69.0/16
10	10.57.70.0/16
11	10.57.71.0/16
12	10.57.72.0/16

# Attribution des départements

Équipe	Nom		Département
1	Duplan	Chelny	Programmation
	Palanque	Erwan	Artistique
	Tran	Shi-Hui	Système
2	Charbonneau-Fortin	Michael	Artistique
	Tremblay	François	Programmation
3	De Gagné	Marc-André	Programmation
	Mané	Aboubacar	Artistique
	Païement	Augustin	Système
4	Boisvert	Carl	Programmation
	Distaulo	Justin	Artistique
	Goudreau	Nathaël	Système
5	Décarie	Reno	Programmation
	Paquin	Marc	Système
	Waucheul	Nicolas	Artistique
6	Côté	Maxime	Artistique
	Majeau	Marc-André	Système
	Parent	Jean-Philippe	Programmation
7	Caya	Etienne	Programmation
	Massabot	Raphaël	Artistique
	Olivier	Maxime	Système
8	Fauteux	Jean-Sébastien	Artistique
	Grenier	Marc	Programmation
9	Martinez	Olivier	Système
	Michel	Pierrick	Artistique
	Sidibe	Fatou	Programmation



10	Lebrun	David	Programmation
	Massey	Jeff	Artistique
	Singirankabo	Charles Emmanuel	Système
11	Bergeron	Marc Olivier	Programmation
	Ryc	Samuel	Système
12	Izquierdo	Gonzalo	Système
	Martin	Antoine	Programmation
	St-Onge	Francis	Artistique

---

# ANNEXE – STRATEGIES DE GROUPE

---

## Stratégies

1. Attribuer un papier peint spécifique pour le bureau
2. Ne pas déplacer les fichiers supprimés vers la Corbeille
3. Activer «Toujours afficher tous les éléments du Panneau de configuration»
4. Aucun accès au panneau de configuration
5. Forcer un écran de veille spécifique, avec une des options suivantes
  - a) Ballet de lignes = Mystify.scr
  - b) Bulles = Bubbles.scr
  - c) Rubans = Ribbons.scr
6. «Démarrer l'Explorateur de fichiers avec le ruban réduit», avec une des options suivantes
  1. Toujours ouvrir de nouvelles fenêtres de l'Explorateur de fichiers avec le ruban réduit
  2. Ne jamais ouvrir de nouvelles fenêtres de l'Explorateur de fichiers avec le ruban réduit
7. Empêcher l'accès aux outils de modifications du Registre et désactiver l'exécution silencieuse de regedit.exe
8. Créer une redirection pour le dossier «Documents» vers leurs répertoires personnels
9. Créer une redirection pour le dossier «Favoris» vers leurs répertoires personnels.
10. Créer une redirection pour le dossier «Téléchargements» vers un partage commun. Ce partage sera situé sur votre serveur personnel et devra être présent dans votre espace de nom
11. Ne pas afficher le bouton «Affichage du mot de passe»

## Préférences

12. L'espace de nom devra être présent dans l'explorateur de fichiers, lié à la lettre appropriée
13. Créer des variables d'environnement selon les demandes
14. Créer un raccourci sur le bureau vers FileZilla
15. Créer un raccourci sur le bureau vers une invite de commande
16. Créer un raccourci dans la barre des tâches vers une invite de commande
17. Les options de dossiers ne permettront de voir les extensions
18. Les options de dossiers n'auront pas le paramètre «Utiliser l'assistant Partage»
19. Créer une tâche planifiée à l'ouverture de session qui fera démarrer la calculatrice
20. Créer une tâche planifiée à l'ouverture de session qui fera démarrer la console de gestion «Utilisateurs et ordinateurs Active Directory»

---

## ANNEXE – ÉVALUATION DE STRUCTURE

---

Voici la liste des éléments qui devront être terminés pour l'évaluation de structure :

- Configurations de base des serveurs personnels (nom, rôles, fonctionnalités)
- Implantation du plan d'adressage
- Installation du domaine et joindre les quatre serveurs au domaine
- Installation et configuration du routeur (nat, vpn )
- Installation de l'autorité de certification
- Installation du serveur SMTP
- Création des stratégies de groupe du domaine
- Création des utilisateurs personnels «administrateurs»

---

# ANNEXE – SYSTEME

---

## Procédure d'activation des S.E.

Quand la carte réseau «OnBoard» est activé le serveur DHCP du département lui fournit une adresse et votre système d'exploitation est automatiquement activé auprès de notre serveur KMS.

Si jamais ce n'était pas le cas voici la procédure d'activation

- Activer temporairement votre carte réseau OnBoard et paramétrez là en client DHCP
- Vérifier si elle obtient une adresse ip dans le réseau 10.57.0.0/16
- Démarrer une invite de commande en tant qu'administrateur
- Changer le répertoire pour C:\Windows\System32
- Donner la commande

---

```
slmgr /skms 10.57.4.29
```

---

- Donner la commande

---

```
slmgr /ato
```

---

- Un message devrait vous dire si l'activation s'est bien passée

Pour vérifier si l'activation est bien faite:

---

```
slmgr /dlv
```

---