PPE 3- Séance 4,5,6 ….

Objectifs :

- ☐ Disposer d'une infrastructure GSB (specimen) en production.

Synoptique des étapes (cochées si réalisées: ✅)

Architecture par défaut.

1. Appréhender l'infrastructure sur laquelle nous allons installer le contexte GSB
   1. Étude de l'architecture du Réseau SIO. CF Annexe 1
2. Appréhender l'infrastructure du contexte GSB (CF. Annexes). ✅
3. Accéder et prendre en main les hyperviseurs . ✅
   1. Identifier la carte d'administration POD (sur le serveur Physique) accès PORT18
   2. Installer configurer un poste MMC individuel (serveur W12),
   3. Créer un VLAN **Hvx** pour que chacun puisse manager l'hyperviseur.
   4. Connecter les MMC au serveur. (Accès : administrateur , P@ssW0rd)
   5. Créer les comptes de chaque administrateur de pod (4 comptes par POD)
   6. Identifier les cartes :
      1. D'administration prof
      2. D'administration Etudiants (POD)
      3. De réseau à dédier à GSB.
4. Structurer votre infrastructure. (Visio des Vlans et des actifs nécessaires)
   1. Définir les réseaux de GSB en lien direct avec les cartes des hyperviseurs
5. Configurer **ProxyLAB** pour l'accès au Wan (NAT) et le filtrage ✅
6. Configurer les Vlans:
7. Configurer le routeur intervlans (Hors services du réseau DHCP)
   - Actifs de votre choix (routeur physique , switch de niveau 3)
8. Installer votre contrôleur de domaine gsb (CDLAB) (CF. Annexe Contraintes)
   1. Domaine et rôle (AD)
   2. DNS
   3. DHCP (pour les clients des différents services)
   4. Annuaire
   5. Groupes
   6. Utilisateurs
   7. GPO

Vers une architecture améliorée. [Evolution du contexte]

Mission : service web

- Ouvrir un service web au public (gérer ou non le site WordPress de présentation de l'entreprise)
- Isoler le nouveau service web Réflexion proposition mise en œuvre)
  - ☐ Sécuriser les échanges, Authentifier les accès.

Mission : supervision

- Mettre en œuvre une solution de supervision des services, des serveurs et actifs

Mission : DOS (disponibilité de services):

- ☐ Mener une réflexion sur la disponibilité de services et la redondance.
  - Critique de l'existant.
  - Proposition de solutions pour les
    - Services : (AD, web)
    - Actifs : serveurs, switch routeurs.
- ☐ Mise en œuvre des propositions.

Mission : Recouvrement des données (sauvegarde / Backup). ◦ Prévoir un plan de sauvegarde des données (choix matériel / logiciel / fréquence / support / …) ◦ Mettre en œuvre et automatiser les sauvegardes .
Mission : Sécurisation des accès : ▯ Authentification RADIUS. ▯ Authentifier les machines connues et les autoriser à se connecter au VLAN autres services) ▯ Pour les machines inconnues seront assocées au VLAN visiteur. ▪ Portail captif :Simplifier et Améliorer le service d'accès internet aux visiteurs, en proposant un portail captif aux machines inconnues (l'utilisateur disposera d'un identifiant pour pouvoir se connecter).
Mission : ▪ Automatisation des taches d'administration : ▯ Prévoir une « batterie d'outils scripts ou autres » afin de faciliter : ◦ L'ajout / suppression modification d'utilisateurs dans le système ◦ La configuration ou reconfiguration de services 'souffrants'
Mission : ▪ Configuration d'un NAS avec migration des données des serveurs FTP vers le NAS et ajout de partages pour la documentation.

Travail à Faire :

1. RAPPEL SEANCE 1: Étude du contexte GSB

A l'aide de l'annexe et des documents du réseau CERTA fournis dans l'archive ;

- ▯ analysez le contexte (Annexe + contexte/GSB-1-Organisation.pdf) ,
- ▯ et présentez un schéma *visio* de la configuration envisagée du contexte GSB sur votre POD (@ IP, machine physique et VM qui endosseront le rôle des serveurs du contexte)
- ▯ Donnez l'ordre dans lequel vous comptez les installer (justifiez votre choix)

- Attention on ne vous demande pas encore de les implanter, mais juste de les représenter.

2. RAPPEL séance 2 et 3: Préparation du contexte GCB.

Remarque : On distinguera les serveurs de POD (Machines situées sur vos bureau) et serveur Rack de POD (Machine située dans le local technique)

◦ Réinitialisation des switch :
- ▪ Rechercher dans la doc le moyen de réinitialiser les switch. (Testez physiquement le bouton reset et trouver une solution alternative au cas où).

◦ Installation des 4 Serveurs Windows_2012R2 ou 16 sur les serveurs physiques du POD (SP1-g SP2-g SP3-G et SP4-g) et ce pour chaque groupe.

◦ Serveurs de Virtualisation :
- ▪ ~~Configurer le serveur hyperV du rack physique dans le local technique SP-HV-12R2-PODg. CF. Cours : datacenter.sio~~ (Pour des raisons de délais et d'ordre technique, ces serveurs sont déjà installés et prêts à être configurés pour héberger les VM de contexte GSB)
- ▪ Configurer les 4 serveurs (SPn-g) 2012 physique du POD
  - ▯ Configurer le serveur en HYPER V pour qui puisse **aussi** héberger des Vms (par exemple les clients)
  - ▯ Dédiez ces 4 serveurs 2012 R2 à la gestion des HyperV (Installer les outils MMC)
    - ◦ Ajouter les serveurs suivants dans le gestionnaire de serveur

- **Rack SP-HV*g*-16-CD1**
- **Physique SP-HV-12R2-POD*g* ou SP-HVn-16-PODg**

Plus de détail dans le cours datacentersio

3. Sécurité et accès internet :

- A partir des travaux effectués en TP, rédiger une note sur le NAT contenant les éléments suivants :
  - Le Principe
  - Les entrées de la table -t nat d'iptables
  - Les commandes iptables
    - pour : configurer la translation d'adresses depuis votre réseau interne (**adresses des VMs GSB**) vers le réseau **10.10*NumGroupe.0.0 /16 (rappel adresse du routeur : 10.10NumGroupe.0.1*** relié à la prise 18 du bandeau.
  - La persistence d'iptables
    - paquet
    - commande de sauvegardes
    - commande de restauration
    - fichier lu par défaut lors du lancement de debian (rules.v4)

- Installer un serveur physique station DELL pour accueillir le NAT. (MUTLAB)
  - Debian serveur
  - Routage actif avec configuration d'une passerelle NAT.

- Configurer sur ce même serveur, les règles de filtrage (MUTLAB).
  - Dressez un plan des règles à mettre en œuvre à l'aide du TP :
    - Partir du principe que rien n'est autorisé,
    - Puis n'autoriser que les connexions entrantes lorsqu'elles font suite de connexions établies ou relatives (établies depuis l'intérieur du réseau)

4. Implémentez les services minimum

- Référez vous à l'annexe pour installer les services minimum et configurer les différents VLAN correspondant avec pour l'instant un routage par défaut pour que chaque service chaque vlan (sauf le vlan Visiteurs) peut uniquement accéder (quel que soit le protocole) aux vlans "Serveurs" et "Sortie";

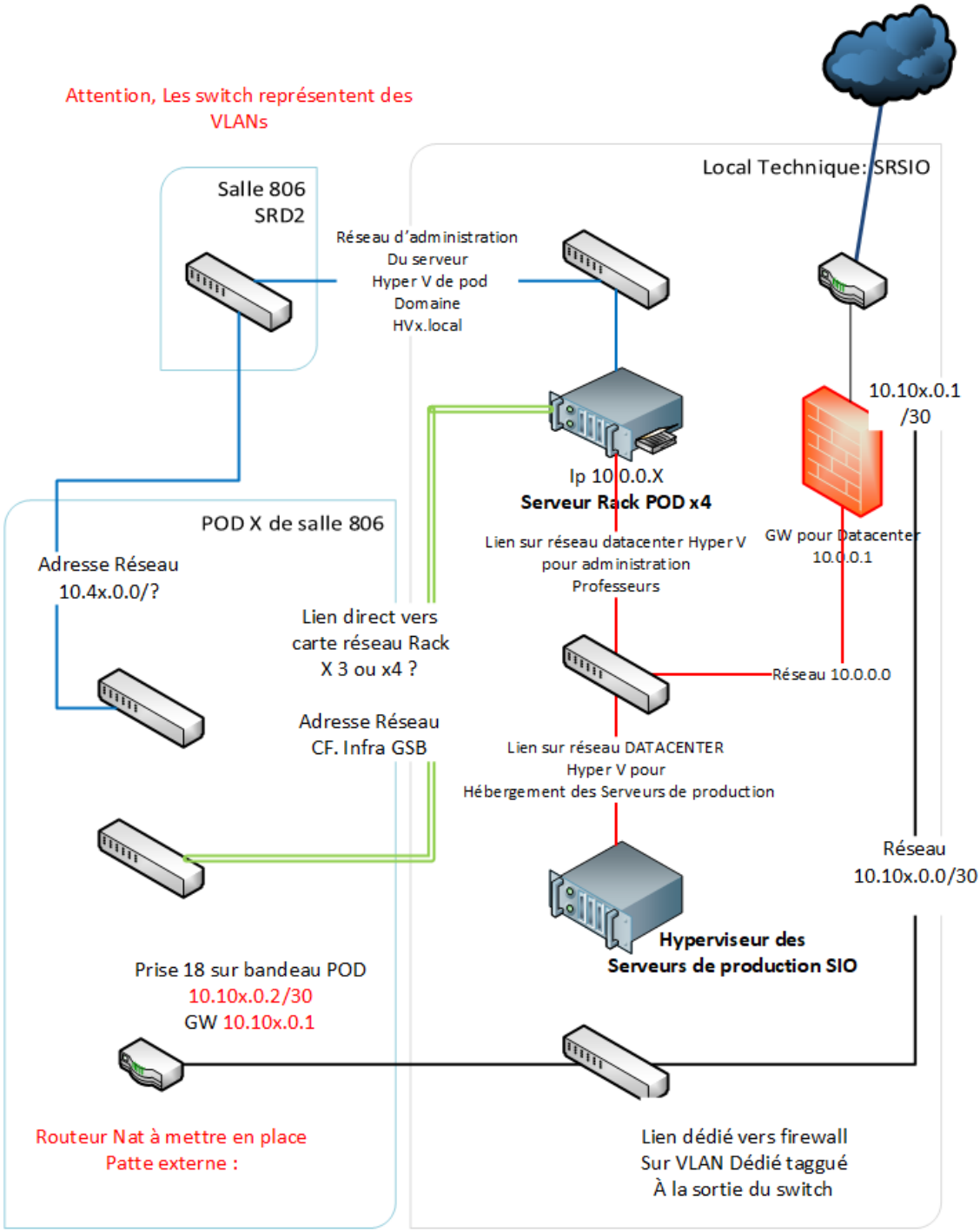
- le vlan "Visiteurs" peut uniquement interroger les serveurs DNS et DHCP et sortir sur internet. Aucun accès aux visiteurs aux ressources partagés ni aux serveurs.

5. Configurer Les groupes , utilisateurs et GPO.

- A l'aide du cours sur les droits, la méthode AGDLP et les GPO et le OU, configurer dans un premier temps les groupes GG, DL et les partages pour les utilisateurs de la liste en annexe.

- Dans un deuxième temps vous automatiserez au travers d'un script l'ajout en masse d'utilisateurs avec la possibilité d'associer automatiquement ces derniers a une OU et a un global.

Annexe 1: Infrastructure d'accueil Hvx.local



Annexe 2 : Réseau GSB simplifié.

Segmentation

L'organisation (simplifiée) des VLANs et de l'adressage IP est la suivante :

Simplification. (On considère Que tous les autres Services de l'entreprises Seront associés à ce Vlan

N° VLAN	Service(s)	Adressage IP
10	Réseau & Système	192.168.10.0/24
20	Direction / DSI	192.168.20.0/24
30	RH/Compta/Juridique/Secrétariat Administratif	192.168.30.0/24
40	Autres Services	192.168.40.0/24
~~40~~	~~Communication / Rédaction~~	~~192.168.40.0/24~~
~~50~~	~~Développement~~	~~192.168.50.0/24~~
~~60~~	~~Commercial~~	~~192.168.60.0/24~~
~~70~~	~~Labo-Recherche~~	~~192.168.70.0/24~~
~~100~~	~~Accueil~~	~~192.168.100.0/24~~
150	Visiteurs	192.168.150.0/24
~~200~~	~~Démonstration~~	~~192.168.200.0/24~~
300	Serveurs	172.x.x.0/24
400	Sortie	172.31.x.0/30

Rappel des contraintes :

Les règles actuelles concernant les vlans sont les suivantes :

- chaque vlan (sauf le vlan Visiteurs) peut uniquement accéder (quel que soit le protocole) aux vlans "Serveurs" et "Sortie";
- le vlan "Visiteurs" peut uniquement interroger les serveurs DNS et DHCP et sortir sur internet.

Les points d'accès wifi :

- Toutes les salles de réunion sont équipées d'un point d'accès Wifi positionné par défaut dans le VLAN "Visiteurs" qui autorise uniquement un accès Internet.
- Les portables connectés en wifi à ce point d'accès reçoivent ainsi une adresse IP et n'ont, par conséquent accès qu'aux services DHCP et DNS.
- [Mission] Le point d'accès peut être configuré à la demande pour être raccordé à un VLAN présent au niveau de l'étage.

Les Unités organisationnelles :

- Chaque service « utilisateur » disposera de son OU (Cf. document des utilisateurs ci-dessous).

Les GPO

- Dressez votre liste de restriction et ou configuration imposée.
  - Cortana, télémétrie, quotas (100 Mo), navigateur par défaut (chrome) et fond d'écran correspondant au logo du service dans lequel est installé l'ordinateur, la politique de mots de passe etc.
- Centralisez les profils sur le serveur AD (Disque SCSI distinct de label : userdocs)

Les partages :

- Administration
- RessourcesTechniques
- Administratif.

Les utilisateurs :

OU	Sous OU	GG	Utilisateurs
Direction (Direction + DSI)		GG_Dir	Paul Hochon Jean Pierre Detaille
Administratifs		GG-ADM	
	RH	GG_RH	Annie Cheduchien Helene Debrebis
	Compta	GG_Compta	Jacques Umul Aude Alajoie
	Juridique	GG_Juridique	Alba Lance Ced Lex
	Secrétariat	GG_Secretariat	Geraldine Dehors Nadeje EnaveK
invite		GG_invite	Alphonse Dansletas

Les droits pour Domaines locaux :

Administration	
◦ CT	RH, Direction
◦ L	Secrétariat
◦ L_E	Juridique
Contrats	
◦ CT	Direction
◦ L	Secrétariat, Compta
◦ L_E	Juridique. RH
Administratif.	
◦ CT	Direction
◦ L	RH, Juridique
◦ L_E	Compta, secretariat
Informatique	
◦ CT ◦ L	DSI STAGIAIRE

Schéma simplifié de l'infrastructure à produire…