

Projet Infrastructure E6

Une entreprise qui souhaite démarrer une nouvelle entité. A long terme, cette entité devrait devenir autonome et Vous intégrez le service informatique de cette nouvelle entité. Avec comme objectif l'indépendance, on vous demande de monter toute l'infrastructure pour le bon fonctionnement de l'entreprise. Mais afin d'accélérer malgré tout, vous pourrez vous appuyer sur l'infrastructure de l'entreprise et c'est à dire :

- Votre infrastructure sera un sous réseau qui vous sera donné par le responsable de l'entreprise.
- Votre routeur ne devra pas être en mode NAT (puisque en interne) mais en routage statique.
- Vous pouvez vous appuyer sur le DNS suivant : 192.168.10.120
- Vous utiliserez comme passerelle montante l'@ IP 10.21.3.1

Afin de préparer votre analyse théorique, on vous donne les informations suivantes :

l'entité est divisée en 3 services :

- Direction : le directeur, une assistante de direction, le DRH et un comptable.
- Commercial : un Directeur commercial et 2 commerciaux.
- Production : un directeur technique et 2 ingénieurs d'études.

l'entité a pour objectif de grossir très rapidement et vous demande de mettre en place tout de suite les bonnes pratiques même si pour le moment, il y a peu de personnes.

Pour les partages, la demande est :

- Commun : Tous les services ont le droit de lecture et écriture
- Direction : Le service de direction a le droit de lecture/écriture
- Commerces :
 - o L'équipe commerciale a le droit de lecture/écriture
 - o L'équipe de direction a le droit de lecture/écriture
- Production :
 - o L'équipe de production a le droit de lecture/écriture
 - o L'équipe de direction a le droit de lecture seulement
 - o L'équipe commerciale a le droit de lecture seulement

Dans l'entreprise, il y aura aussi 2 catégories de collaborateurs :

- Les VIP : le directeur, le DRH, le directeur commerciale et le directeur technique.
- Les employés : tous les autres collaborateurs.

Ces 2 catégories serviront pour la sécurité des postes. Nous avons en effet :

- o Les VIPS auront la possibilité d'utiliser les ports USB de leur PC
- o Message de bienvenue différents entre les PCs VIP et les autres

Vous avez à disposition :

- 1 serveur Lenovo pour l'hyperviseur
- 1 switch Cisco pour connecter vos périphériques
- 1 routeur cisco pour l'interconnexion
- 2 PC avec 2 cartes réseaux pour avoir 2 PC clients
- Le tout interconnecté dans une baie 15U accessible.

Objectif :

Il faudra une créer une infra complète :

- le routeur qui s'interfacera (WAN) avec le réseau SIO
 - o InterVLAN autorisé sauf « DMZ »
 - o Autorisation des flux Web (http et https) en provenance de l'extérieur sur le serveur Web de la DMZ
 - o Autorisation des flux Web et accès à distance en provenance du LAN sur le Serveur Web.
- 4 plages réseaux : 1 LAN + 3 VLANS:
 - o Serveurs : avec la présence des VM suivantes :
 - 1 x Serveur AD / DHCP / DNS / NTP / DFS
 - 1 x Serveur de supervision Zabbix
 - 1 ou plusieurs Serveurs optionnels (**cf paragraphes concernant les options**)
 - o PCs : avec la présence de PC physiques entrée dans le domaine mais avec 1 PC VPI et 1 PC utilisateur => règles de sécurité différentes.
 - o « DMZ » : avec la présence de la VM suivante :
 - 1 x Serveur Web sous Linux par personne présente dans l'équipe.
 - o 1 Vlan en attente

Demandes spécifiques liés au contexte :

- AD : construire une arborescence d'UO pour avoir des affectations spécifiques et hiérarchique des GPO (AGDLP)
- AD : GPO : 3 ou 4 différentes doivent être mise en place. De votre choix (à demander au prof) ou vous avez la liste :
 - o Montage de lecteur réseau au démarrage d'une session (obligatoire)
 - o Chargement d'un fond d'écran (bginfo pour les plus courageux)
 - o Modification du message d'accueil avant la connexion utilisateur (obligatoire)
 - o Désactivation des ports USB sur les PCs non-VIP (obligatoire)
 - o Installation en automatique d'un petit logiciel : ex 7zip ou un autre.
- Sauvegarde : sur le NAS, avoir une sauvegarde de vos configurations (switch , routeur, etc ...)
- Firewall : Autoriser l'accès depuis l'extérieur de l'entreprise (WAN) au port 80 et 443 vers votre serveur WEB (DMZ)
- Firewall : entre la DMZ(Interface DMZ IN) et les Vlan internes : interdire tout trafic sauf :
 - o L'accès au Web depuis l'extérieur (trafic retour) (80 et 443)
 - o Le fait de pouvoir administrer les serveurs web qui sont dans la DMZ
 - o Les protocoles nécessaires aux fonctionnements des serveurs de gestion de parcs (Ex : Zabbix).

Options : Le projet est ouvert aux propositions venant compléter l'infrastructure :

- Options pour le serveur de fichiers :
 - soit sous Windows Server mais il faudra compléter son offre.
 - soit sous TrueNas (avec un lien AD)
- Options disponibles pour compléter son offre :
 - Serveur de gestion de mise à jour : WSUS
 - Serveur de gestion de configuration et d'incidents : GLPI
 - N'hésitez pas à proposer une envie.

Trame à suivre :

1. Analyse théorique :
 - . Découpage de sa plage Réseau en 4 sous plages avec ses règles de gestions (passerelles, ID vlan etc ..).
 - . Elaboration d'un schéma réseau « cible »
 - . Elaboration des règles de nommage, du choix des OS et des capacités des VMs
 - . Validation des « productions » théorique par le professeur
2. Puis mise en Pratique (sans oublier screen, documentations, etc ...) :
 - . Installation du switch et du routeur avec une configuration basique permettant l'accès Internet
 - . Installation des PCs Clients afin de créer son environnement de travail
 - . Installation de l'hyperviseur avec gestion à distance.
 - . Mise en place des VLANs : on autorise tout (pas de filtrage pour le moment)
 - . Création de la VM AD, création du domaine, srv DNS, srv DHCP
 - . Insertion des PCs dans le domaine
 - . Installation du serveur de fichiers et des partages associés
 - . Mise en place des GPOs
 - . Mise en place de la DFS
 - . Installation de la VM serveur Web linux pour la DMZ
 - . Installation du serveur de gestion de parc (Zabbix)
 - . Installation du serveur optionnel
 - . Réglage firewall /sécurité