

PROJET GPOPU



Définition du besoin

GSB souhaite migrer leur ancien serveur LABANNU sous Windows 2012 vers Windows Server 2016 et redimensionner le service de résolution de noms. Vous devez mettre en place une maquette afin de valider les outils de migration et le bon fonctionnement du nouveau système, avant d le déployer en production.

Mission

La mission de votre équipe sera de :

- Préparer le nouveau contrôleur de domaine sous Windows serveur 2016 ;
- Concevoir la structure optimale d'un ensemble de restrictions sur les comptes utilisateurs des différents services, les implanter et les valider (Windows 10) ;
- Préparer les scripts de migration des utilisateurs et des groupes ;
- Déployer les services NTP, DHCP et DNS centralisés et relayés, et un service DNS secondaire ;
- Offrir une connexion sans-fil sécurisée aux utilisateurs munis d'un laptop.

Projet : AP 3.1	Contexte : GSB	Mode : projet	Équipe : 4 étudiants	Durée : 20 heures (5 séances)
-----------------	----------------	---------------	----------------------	-------------------------------

Cahier des charges

Serveurs, services, passerelles, contraintes de Labo

- Labannu<eq> (Win2016) est **PDC** sur le domaine gsb.local, avec UO, groupes, utilisateurs et ordinateurs du contexte utiles à la validation de la solution.
- Labannu<eq> fournit les services **DNS** primaire pour le domaine et **DHCP** pour l'ensemble des sous-réseaux d'utilisateurs.
- *Les fichiers de configuration seront sauvegardés et commentés (ex. exclusions DHCP).*
- La zone gsb.local permet de résoudre les noms de tous les serveurs et passerelles maquettés (5) mais aussi des STA obtenant une configuration DHCP. Une résolution inverse et la fonction cache pour les redirections au DNS du FAI sont aussi fournies.
- Les sous-réseaux d'utilisateurs inclus dans ce maquettage seront { RS ; RH ; Dev ; Redac ; Com }.
- Labsecdns<eq> (Debian12 ; .0.40) est un serveur DNS secondaire de délestage (LB) dans le sous-réseau Serveurs. Il sera DNS principal pour toutes les machines sauf les serveurs, passerelles, STA Admins et Dev. Il sera DNS de secours (FT) pour toutes les autres machines, à l'inverse de Labannu.
- Sortlab<eq> (pfSense) est passerelle entre les réseaux Sortie (.2) et le WAN, et fournit côté Sortie les services **NTP** pour toutes les machines du parc, et **DNS Forwarder** pour les serveurs DNS.
- ComLab<eq> (pfSense) est passerelle entre les réseaux RS (.2) et Com (.1). Le réseau Com ne touche donc pas directement Mutlab, pour lequel le switch 3 de l'armoire de plot sera utilisé.
- Les numéros de VLAN et l'adressage des sous-réseaux correspondants correspondent au contexte de production.
- Pour des raisons de contraintes de laboratoire, la STA Redac sera dans le sous-réseau RH.
- Dans cette maquette, les commerciaux seront connectés exclusivement en sans-fil au domaine diffusé sfCom<eq>. Des téléphones portables seront utilisés comme STA Com pour les tests.
- Les admins RS pourront être connectés en filaire mais aussi en sans-fil au domaine non-diffusé sfRS<eq>.
- Les développeurs pourront être connectés en filaire mais aussi en sans-fil au domaine non-diffusé sfDev<eq>.
- Toutes les connexions sans-fil seront en WPA3 (ou WPA2 si le WAP est ancien). Pour les admins et les développeurs, le SSID devra être déployé par GPO.
- Les utilisateurs de RH et de Redac seront connectés en filaire uniquement.

Restrictions à mettre en place pour les différents services

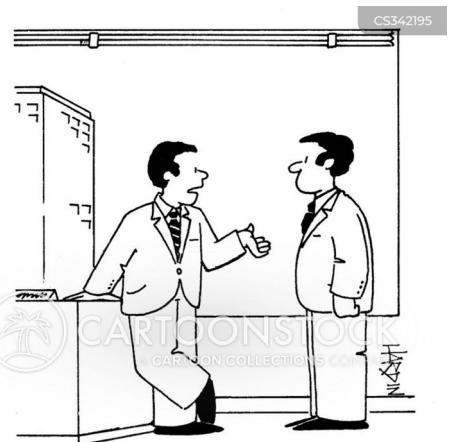
Dans une phase de conception par matrice d'analyse des restrictions, vous optimiserez la structure des stratégies de groupes pour obtenir un minimum de GPO.

- **Réseau & Système**
 - ne pas déplacer les fichiers vers la corbeille quand ils sont supprimés
 - assistant de nettoyage
 - pas d'écran de bienvenue à l'ouverture de session
 - autorisé à modifier les paramètres de carte réseau
 - accès au panneau de configuration du poste
 - barre des tâches non verrouillée
 - présence du menu exécuter dans le menu « démarrer »
- **RH**
 - cacher le gestionnaire de tâches
 - ne pas avoir accès au panneau de configuration du poste
 - verrouiller la barre des tâches
 - taille max de la corbeille : 5% de l'espace disque
 - pas d'assistant de nettoyage
- **Développement**
 - assistant de nettoyage
 - ne pas déplacer les fichiers vers la corbeille quand ils sont supprimés
 - présence du menu exécuter dans le menu « démarrer »
 - pas d'écran de bienvenue à l'ouverture de session
 - autorisé à modifier les paramètres de carte réseau
 - accès au panneau de configuration du poste
 - barre des tâches non verrouillée
- **Rédaction**
 - cacher le gestionnaire de tâches
 - taille max de la corbeille : 5% de l'espace disque
 - ne pas avoir accès au panneau de configuration du poste
 - verrouiller la barre des tâches
 - pas d'assistant de nettoyage
 - dossier de travail permettant l'accès aux catalogues des produits et plaquettes de GSB
- **Commercial**
 - taille max de la corbeille : 5% de l'espace disque
 - ne pas avoir accès au panneau de configuration du poste
 - verrouiller la barre des tâches
 - cacher le gestionnaire de tâches
 - dossier de travail permettant l'accès aux catalogues des produits et plaquettes de GSB
 - pas d'assistant de nettoyage
 - connexion autorisée aux horaires de bureau uniquement

Automatisation d'une partie de la migration

Afin d'optimiser certaines opérations de migration fastidieuses (tâches répétitives, longues et fortement sujettes aux erreurs de saisie), un ou plusieurs scripts en PowerShell devront permettre la création automatique d'utilisateurs et de groupes sur le nouveau PDC. Un fichier CSV contient l'ensemble des informations nécessaires.

Les directeurs techniques de la DSI sont à votre disposition dans les locaux de GSB pour toute clarification concernant votre projet.



Tâches et livrables

Afin de réaliser ce projet, vous devrez, au sein de l'équipe, planifier et distribuer les tâches telles que, par exemple :

- la spécification de l'infrastructure de maquettage dans le

"The organizational structure is pretty simple; We do the work; they take the credit."

- cadre de votre plot de Labo SISR, sous formes d'un schéma réseau logique et d'un schéma réseau physique ;
- l'identification et la validation des US auprès du directeur de projet ;
 - le découpage des US en tâches d'une durée de 1h max chacune (méthode agile) ;
 - l'utilisation de Trello comme outil de gestion agile du projet ;
 - la spécification des plans de tests pour chaque tâche (unitaire et d'intégration – approche d'analyse top-down) ;
 - la configuration du réseau ;
 - la configuration des systèmes et des services ;
 - la validation des briques fonctionnelles de la maquette (tests de validation de chaque US – approche d'analyse bottom-up).

Les livrables attendus par le client sont :

PARTIE GESTION DE PROJET

- vos 5 screenshots Trello de fin de chaque séance (les tests d'intégration et de validation donnent lieu à une tâche chacun) ;
- vos journaux de bord ;
- vos fiches de réalisation professionnelle ;
- votre onglet d'équipe du fichier en ligne Livraison par équipe ap3.1 ;
- **une fiche recette** sous forme de grille synthétique, recensant :
 - pour chaque US du projet si la solution apportée est totalement fonctionnelle (vert), partiellement fonctionnelle (orange) ou non livrée (rouge) ;
 - pour chaque US orange ou rouge (**réserves**), les problèmes rencontrés (techniques, humains, temporels, organisationnels) et les solutions tentées ou envisagées.
- un bilan d'équipe avec 1 à 5 points clés sur ce que vous avez appris et ce que vous feriez différemment si c'était à refaire.

PARTIE TECHNOLOGIQUE

- votre plan de tests (unitaires, d'intégrations) basé sur les tâches de votre Trello ;
- votre plan de tests de validation, basé sur vos US et cas d'utilisations ;
- un dossier technique de conception réseau avec : { la table des systèmes ; le schéma logique complété pour correspondre à votre équipe ; le schéma réseau physique (avec numéros de ports et de VLAN en formalisme U/T) correspondant à votre équipe et votre plot ; les tables de routage prévues pour Comlab, Mutlab et Sortlab } → cf. ressource *Conception initiale - infos.txt* ;
- une documentation technique de configuration de mutlab avec les commandes : { show vlan 1/50/300/400 ; show ip ; show ip route ; show dhcp-relay ; show ip helper-address } ;
- les fichiers de configuration effectifs des 2 switches NG, de la borne wifi NG, et du switch MUTLAB ;
- une documentation technique de configuration de Comlab avec les screenshots de : { dashboard services status.interfaces firewall.rules routing-table } ;
- une documentation technique de configuration de Sortlab avec les screenshots de : { dashboard services status.interfaces firewall.rules routing-table dns-forwarder ntp-server } ;
- les fichiers de configuration de Sortlab et de Comlab ;
- une documentation technique du service DHCP de Labannu permettant de refaire la configuration à partir de zéro si nécessaire ;
- une documentation technique du service DNS de Labannu et de Labsecdns permettant de refaire la configuration à partir de zéro si nécessaire ;
- la structure de l'annuaire et des GPO (schéma de conception AD + tableau d'analyse GPO + copies d'écran de l' AD) ;
- une documentation sur la mise en œuvre de toutes vos restrictions/GPO ;
- une sauvegarde de vos GPO (Fichiers + Tutoriel de sauvegarde) ;
- vos scripts PowerShell (code source commenté + copies d'écran avant/après l'exécution du script).

Ressources

Vous avez à votre disposition des ressources partielles relative au projet, dans le dossier Commun :

- Documentations techniques de l'infrastructure de Labo ;
- OVA orgKali, orgWin10 ;
- OVA orgDeb12, orgWin2016, orgpfSense272 ;
- Fichier CSV des utilisateurs ;
- Conception initiale - infos.txt

