# Projet personnel encadré – SISR – 2e semestre

**Objectif :** Savoir définir une configuration en fonction d’un cahier des charges, savoir mettre en œuvre un scénario complet de configuration, savoir définir et réaliser des tests, savoir rendre-compte de l’avancement d’un projet, savoir compléter et faire aboutir le travail d’une autre équipe.

**Déroulement :**

**Etape 1.** Semaines du 16 et du 23 janvier 2024.

1.A. Description du projet, cahier des charges (voir modèle)

1.B. Architecture réseau (répartition des éléments actifs, plan d'adressage)

1.C. Planning détaillé

(à rendre le 23 janvier 2024, noté).

**Etape 2.** Phase technique

3 étapes intermédiaires, à définir dans le calendrier de chaque projet :

Du 23/01/2024 au 06/02/2024 : Réalisation 1er objectif technique (noté)

Du 06/02/2024 au 05/03/2024 : Réalisation 2e objectif technique (noté)

Du 05/03/2024 au 20/03/2024 : Réalisation 3e objectif technique (noté)

**Etape 3.** Présentation de projet

Préparation : Séance du 26/03/2024   
Présentation de votre projet + question à résoudre + revenir présenter la solution

Présentation : 03/04/2022

**Etape 4.** Héritage du projet d’un autre groupe (du 23/04/2022 au 07/05/2024)

3 semaines pour finaliser le projet hérité d’un autre groupe.

|  |  |
| --- | --- |
| A1.1.1 Analyse du cahier des charges d'un service à produire  A3.2.3 Élaboration de documents relatifs à la production et à la fourniture de service  A1.2.2 Rédaction des spécifications techniques de la solution  A1.2.4 Détermination des tests nécessaires à la validation  A1.2.5 Définition des niveaux d'habilitation  A1.3.1 Test d'intégration et d'acceptation d'un service  A1.3.2 Définition des éléments nécessaires à la continuité  A1.3.4 Déploiement d'un service  A1.4.1 Participation à un projet  A2.1.2 Évaluation et maintien de la qualité d'un service  A2.2.1 Suivi et résolution d'incidents | A2.2.3 Réponse à une interruption de service  A2.3.1 Identification, qualification et évaluation d'un problème  A3.1.1 Proposition d'une solution d'infrastructure  A3.1.2 Maquettage et prototypage d'une solution d'infrastructure  A5.2.4 Étude d‘une technologie, d'un composant, d'un outil  A3.2.1 Installation et configuration d'éléments d'infrastructure  A3.3.2 Planification des sauvegardes et gestion des restaurations  A3.3.3 Gestion des identités et des habilitations  A3.3.4 Automatisation des tâches d'administration  A3.3.5 Gestion des indicateurs et des fichiers d'activité  A4.1.8 Réalisation des tests nécessaires à la validation |

Contraintes techniques :

**Obligatoires :**

- Virtual box pour les machines virtuelles.

- Une machine (client ou serveur, physique ou VM) Windows, minimum

- Une machine (idem) Linux minimum

- Installation d’un service minimum au choix  
 - une base de données

- un site web

- un CMS  
 - un serveur d’impression

- un serveur de messagerie

- Une architecture réseau avec deux segments distincts interconnectés (soit sous-réseau, soit VLAN, soit WAN, ou cloud, au choix).

- Un script (Shell ou Powershell) automatisant une tâche d'administration (exemple : Création d'utilisateurs, déploiement d'un logiciel, sauvegarde, etc.)

- Un service DHCP avec deux plages séparées, et au minimum une adresse réservée (selon l'adresse MAC de la machine concernée)

- Une journalisation des accès à un service (access.log sur serveur HTTP, ou ouverture de session, ou journal d'événements sur un serveur d'impression, etc.) ou bien enregistrement d'incidents (GLPI ou autre solution) .

- Génération de statistiques sur cette journalisation (nombre d'accès par jour, etc.)

- Un système de sauvegarde et une démonstration d'une opération de reprise après incident

(par logiciel Cobian, FreeFileSync, etc., ou par script, par RAID logiciel, ou haute disponibilité avec redondance).

- Une authentification individualisée pour l'accès à un service (login propre à chaque utilisateur) ; une création d'un ou plusieurs utilisateurs ; une désactivation temporaire de compte utilisateur ; une suppression de compte utilisateur.

(Exemple : authentification sur un client, sur un service de messagerie, sur un site web / ftp ou autre, CMS type WordPress, etc.)

- Un rapport de test détaillé

**Options :**

- Relais DHCP

- Une authentification générique pour l'accès à un service (accès "public" avec néanmoins un mot de passe, FTP « anonymous », etc.)

- Une DMZ ou un proxy pour un service particulier

- Un système de diffusion de message aux utilisateurs pour l'administrateur.

- Serveur FTP

- VPN

- IP V6