

Compte rendu Atelier 9

Louis Ludovic HERZOG

19 Novembre 2025

Sommaire

1	Analyse du problème	2
2	Conception de la solution	2
3	Réalisation	3
4	Memento Technique	10
5	Retour d'expérience	11

1 Analyse du problème

Il faut remplir de cahier des charges du directeur technique de GSB

2 Conception de la solution

J'ai du d'abord répondre à un QCM afin de se préparer à répondre au cahier des charges : J'ai obtenu 19/20.

Q Question 20 sur 20

Quelle est la principale raison du turn-over important des visiteurs ?

A. Les salaires trop bas

B. Les fusions récentes et réorganisations

C. Le manque de formation

D. Les conditions de travail difficiles

Question précédente

Soumettre le QCM

Quitter

Résultats du QCM

Votre score : 19/20

Réponses correctes : 19

Réponses incorrectes : 1

Recommencer le QCM

Télécharger le corrigé

3 Réalisation

Question 1

Le choix de l'équipement doit se baser sur la mobilité, la robustesse et la performance pour un usage intensif sur le terrain.

Caractéristique	Recommandation	Justification
Modèle / Gamme	Ordinateur portable professionnel	Robustesse, support à long terme
Processeur (CPU) minimal	Intel Core i5 ou équivalent AMD Ryzen 5	Performance suffisante pour les applications métier.
Mémoire Vive (RAM)	16 Go minimum	Indispensable pour la fluidité avec VPN et applications métier.
Stockage (SSD) / Capacité	SSD de 512 Go minimum	Rapidité du système et résistance aux chocs.
Autonomie Batterie	12 heures minimum	Couvrir une journée de travail complète sans recharge.
Poids maximum	1,5 kg maximum	Optimiser l'ergonomie et le confort en déplacement.

Question 2

Étant donné que les données de l'entreprise sont stratégiques et ne peuvent tolérer ni fuite, ni destruction, la sécurité doit être maximale.

1. Système de chiffrement :

- Recommandation : Utilisation de BitLocker (intégré à Windows Professionnel) ou d'un équivalent pour le chiffrement intégral du disque dur (Full Disk Encryption). * Justification : En cas de perte ou de vol du portable, les données restent illisibles sans la clé de déchiffrement, garantissant la protection des informations stratégiques.

2. Gestion des clés de récupération :

- La clé de récupération BitLocker doit être automatiquement sauvegardée dans l'Active Directory (Annuaire) centralisé de GSB.
- Seuls les administrateurs du Service Réseau et Système doivent avoir accès à cette clé pour pouvoir déverrouiller le disque en cas d'oubli de mot de passe ou de panne.

3. Séparation données Pro/Perso :

- Mise en place de profils utilisateur distincts : un profil Administrateur (limité au Service Réseau) et un profil Utilisateur Standard pour le visiteur.
- L'utilisation de solutions de Cloud personnel sécurisé (ex. : OneDrive Entreprise) pour les documents professionnels permet de les synchroniser et de les séparer des données personnelles (qui ne devraient pas être stockées sur l'équipement de l'entreprise si possible).

4. Procédure en cas de perte ou vol :

- Déclaration immédiate par le visiteur (Hotline DSI).
- Suppression des données à distance (Wipe Data) via un outil de gestion des appareils mobiles (MDM) si possible.
- Désactivation immédiate du compte utilisateur dans l'Annuaire (empêche toute connexion VPN ou accès réseau).
- Remplacement rapide de l'équipement par le Service Réseau et Système.

5. Prévention des logiciels non autorisés :

- Le profil utilisateur standard ne doit pas avoir de droits Administrateur, empêchant l'installation de tout logiciel non autorisé sans l'intervention de la DSI

Question 3

Le déploiement de 450 postes dans une période courte (objectif de 8 semaines) nécessite une solution de masterisation efficace.

1. Solution de masterisation :

- **Recommandation** : Utilisation de WDS (Windows Deployment Services) ou de SCCM (System Center Configuration Manager) si déjà en place, ou une solution libre comme FOG Project.
- **Justification** : Ces solutions permettent de créer une image système (Master) unique, comprenant le système d'exploitation, les applications métier, le client VPN et les paramètres de sécurité. Cette image est clonée massivement, garantissant l'uniformisation des machines et du mode de fonctionnement.

2. Durée du déploiement :

- L'étape de masterisation initiale (création et tests) prend environ 1 à 2 semaines.
- Le déploiement des 450 postes peut être réalisé en 4 à 6 semaines, en travaillant par lots (ex. : 100 machines par semaine) et en coordination avec la logistique.
-

3. Organisation du déploiement par régions :

- Le déploiement doit suivre l'organisation géographique de GSB (6 secteurs : Paris-Centre, Sud, Nord, Ouest, Est, DTOM).
- **Planification par vagues** : Déploiement par secteur géographique (ex. : 1 secteur par semaine), en priorisant les régions avec le plus grand nombre de visiteurs (France métropolitaine 480 visiteurs).

4. Logistique :

- Utiliser les délégués régionaux comme points de contact pour la distribution et la collecte des anciens équipements.

5. Procédure de test après déploiement

- Vérification fonctionnelle de la connectivité (VPN, WiFi, Messagerie).
 - Test d'accès aux applications métier (Intranet, base d'information pharmaceutique).
 - Validation par le visiteur de la bonne exécution des tâches critiques (saisie de rapport de visite, gestion des frais).
6. Mise à jour de l'image :
- L'image maître doit être mise à jour trimestriellement (patches de sécurité, nouvelles versions d'applications) et redéployée sur les postes non encore livrés ou pour les nouveaux arrivants.

Question 4

Les visiteurs médicaux étant des acteurs mobiles autonomes, le VPN est la solution clé.

1. Solution VPN :
 - **Recommandation** : Utilisation d'un VPN SSL (Secure Sockets Layer) ou IPsec (Internet Protocol Security), comme ceux fournis par des équipements de pare-feu professionnels (ex. : Fortinet, Cisco).
 - **Justification** : Le VPN crée un tunnel sécurisé entre l'ordinateur du visiteur et le réseau interne de GSB, garantissant la confidentialité des données échangées (même sur un WiFi public). Le VPN est indispensable pour l'accès aux ressources internes non externalisées (comme les serveurs métier au siège parisien).
2. Configuration de l'accès WiFi sécurisé :
 - Utilisation du VLAN Visiteurs au siège : Lors des passages au siège , le visiteur peut se connecter au WiFi des salles de réunion qui est par défaut dans le VLAN "Visiteurs" (192.168.150.0/24) avec un accès limité à Internet, DNS et DHCP.
 - Pour les ressources internes, la connexion au VPN doit être systématique même au siège afin de garantir une uniformisation de la connexion sécurisée, en plus de l'accès au réseau filaire si nécessaire.
3. Politique pour les connexions WiFi publiques :
 - Interdiction d'accéder aux données stratégiques sans VPN. item[•] Configuration du poste pour une connexion VPN automatique dès la détection d'une connexion Internet.
 - Sensibilisation des utilisateurs aux risques des hotspots publics.
4. Garantir l'accès aux ressources internes :
 - Toutes les applications métier, l'Annuaire, et l'Intranet doivent être accessibles uniquement via le tunnel VPN sécurisé. item[•] Les services externalisés (Messagerie, Intranet Lite) continuent d'assurer une continuité de service minimal sans VPN.
5. Impact du VPN sur les performances :
 - Impact minime, mais mesurable, dû au chiffrement/déchiffrement des données. Nécessité d'un tunnel VPN bien configuré et de serveurs VPN au siège avec une capacité de bande passante suffisante (lien dédié vers les États-Unis et lien Internet du siège).

Question 5

La remontée régulière et directe des informations terrain et la protection contre la destruction sont les priorités.

1. Données à sauvegarder automatiquement :
 - Rapports de visite et informations terrain.
 - Documents de travail des visiteurs (notes, présentations, etc.).
 - Données personnelles des utilisateurs (profil, paramètres) pour faciliter la restauration en cas de remplacement du poste.
2. Fréquence de sauvegarde :
 - Synchronisation en temps réel et/ou automatique (via le client Cloud/VPN) à chaque enregistrement d'un document ou d'un rapport.
3. Localisation des sauvegardes :
 - Stockage Cloud sécurisé (ex. : OneDrive/SharePoint Entreprise) : permet une synchronisation permanente même en mobilité et facilite l'accès aux données.
 - Réplication des serveurs métier aux États-Unis : pour les bases de données centrales (BDMED, BDPHARMA), la réplication quotidienne assure la continuité et la sécurité de l'information stratégique.
4. Restauration des données :
 - Restauration immédiate par l'utilisateur via le client Cloud (synchronisation rapide sur le nouveau poste).
 - Restauration par la DSI à partir des sauvegardes serveurs ou Cloud pour les pannes graves.
5. Assurer la remontée des informations terrain :
 - Développement d'une application métier centralisée (mobile ou web) permettant la saisie directe des informations terrain (confiance, lisibilité des notices) et leur enregistrement dans une base de données au siège (gérée par le Service Développement).

Question 6

L'objectif est d'assurer une gestion unique et uniformisée en intégrant les données à l'application métier RH/GRC (Progiciel de Gestion Intégré - PGI).

1. Solution pour la saisie électronique des notes de frais :
 - **Recommandation** : Module dédié du PGI (PGILAB) ou solution SaaS spécialisée (ex. : Expensify, Concur), accessible via le poste portable et le VPN.
 - **Fonctionnalité** : Utilisation de l'appareil photo du portable pour scanner les justificatifs. Saisie automatique des frais et rattachement au compte visiteur.
2. Intégration avec le système comptable existant :

- Le module de gestion des frais doit être totalement interfacé avec le module Comptabilité du PGI (PGILAB). Les dépenses validées doivent être exportées automatiquement vers le module comptable pour traitement.
- 3. Procédure de validation des frais :
 - **Visiteur** : Saisie et envoi de la note de frais électronique.
 - **Délégué Régional / Responsable de Secteur** : Validation hiérarchique via l'application (consultation des dépenses et des justificatifs).
 - **Comptabilité** : Validation finale et déclenchement du remboursement.
- 4. Gestion des différents types de frais :
 - L'application doit supporter à la fois la gestion des cartes bancaires de l'entreprise (Galaxy) et le système de gestion forfaitaire (Swiss-Bourdin) en attente de l'uniformisation définitive.
- 5. Délais de remboursement cible :
 - 5 jours ouvrés maximum après la validation finale par la Comptabilité, pour améliorer la satisfaction et la fidélité des visiteurs.

Question 7

Un accès plus direct aux données de personnel est nécessaire pour les responsables de secteur et délégués régionaux afin de gérer le turn-over.

1. Données RH à rendre accessibles :
 - Coordonnées de contact (téléphone, email) des équipes (Visiteurs et Délégués régionaux).
 - Statut (nouveau, départ, mutation).
 - Historique des formations (nécessaire pour former les recrues).
 - Date d'arrivée/départ.
2. Garantir la confidentialité des données :
 - Les données doivent être limitées au strict nécessaire pour la fonction (principe du moindre privilège).
 - Accès uniquement via une application sécurisée, authentifiée (mot de passe/certificat), et accessible uniquement via le VPN.
 - Le RGPD impose de masquer les informations sensibles (salaire, données médicales) au personnel non RH/Comptabilité.
3. Niveaux d'accès différenciés :
 - Responsable de Secteur : Accès aux données RH de tous ses Délégués et Visiteurs.
 - Délégué Régional : Accès aux données RH des Visiteurs sous sa responsabilité.
 - Visiteur : Accès uniquement à ses propres données.
 - Service RH (PGILAB) : Accès complet.
4. Intégration avec le système RH existant :

- Développement d'une interface (via API) entre l'application métier des visiteurs (développée par le Service Développement) et le module RH du PGI (PGILAB).
5. Procédure pour les nouveaux arrivants :
- L'arrivée d'un nouveau personnel déclenche automatiquement la création de son compte utilisateur dans l'Annuaire (LABANNU) et l'accès à l'application de suivi des équipes.

Question 8

Le support doit être efficace et rapide, notamment pour ces postes mobiles, afin de minimiser l'impact sur l'activité.

1. Outils de surveillance à distance :
 - **Recommandation** : Solutions de RMM (Remote Monitoring and Management) comme Team-Viewer, LogMeIn ou l'outil intégré de SCCM (si utilisé).
 - **Fonctionnalité** : Permet à l'équipe Réseau et Système de prendre le contrôle de l'ordinateur portable du visiteur (après accord) pour diagnostiquer et résoudre les problèmes logiciels.
2. Diagnostiquer un problème à distance :
 - Utilisation du RMM pour consulter l'état du système (journaux d'événements, utilisation CPU/RAM/Disque, état du VPN).
 - Mise en place d'un système de Helpdesk (via l'Intranet) pour la gestion des tickets d'incidents (catégorisation, priorité, suivi).
3. Procédure pour les pannes matérielles :
 - **Niveau 1 (Support DSI)** : Tentative de résolution à distance.
 - **Niveau 2 (Remplacement)** : Si la panne est confirmée, la procédure de remplacement rapide est déclenchée
4. Gérer le remplacement rapide d'un équipement :
 - Mise en place d'un stock tampon de 5% à 10% des équipements pré-configurés et prêts à être expédiés dans les 24h suivant le diagnostic.
 - Envoi du nouvel équipement, récupération de l'équipement défectueux et transfert des données de sauvegarde.
5. Indicateurs de suivi (KPI) à mettre en place :
 - Taux de disponibilité du VPN.
 - Délai moyen de résolution (DMR/MTTR) des incidents (objectif : < 8h).
 - Taux de satisfaction des visiteurs suite à une intervention (enquête rapide).

Question 9

L'intégration doit se faire principalement via le VPN pour les utilisateurs mobiles.

1. Intégration des nouveaux équipements dans la segmentation VLAN :

- Les ordinateurs portables des visiteurs ne font pas partie d'un VLAN fixe interne (sauf temporairement en VLAN 150 - Visiteurs ou via filaire).
 - L'accès aux ressources est géré par le routage inter-VLAN (MUTLAB, niveau 3 avec ACL) et le Pare-feu/Proxy (ProxSILAB) uniquement après l'établissement du tunnel VPN vers le réseau interne du siège.
 - Seuls les services externalisés (Messagerie, Intranet Lite) seront accessibles sans VPN.
2. Politique d'accès WiFi pour les visiteurs en déplacement :
- Connexion au VPN obligatoire sur tout réseau WiFi externe (y compris domicile, client ou public).
 - Trafic de données des applications métier chiffré par le VPN avant de transiter par Internet.
3. Garantir la sécurité des connexions distantes :
- Authentification forte (ex. : 2FA - Double Facteur d'Authentification) pour l'accès VPN.
 - Le Pare-feu (ProxSILAB) doit disposer de règles d'ACL très strictes, n'autorisant que le trafic VPN authentifié à traverser le réseau.
4. Bande passante nécessaire pour 450 utilisateurs mobiles :
- La bande passante dépend de l'usage. En estimant un usage léger (envoi de rapports, emails, navigation) et non intensif, un lien Internet d'au moins 100 Mbps symétrique pour le siège (pour le service VPN) est un minimum (en plus des 100 Mbps du lien dédié US). La majorité des besoins en bande passante se fera sur le lien Internet du visiteur (fibre/ADSL/4G).
5. Monitorer l'utilisation du réseau :
- Utilisation d'outils de supervision réseau (ex. : Nagios, Zabbix) pour surveiller l'état du tunnel VPN, la charge CPU/mémoire des serveurs VPN/ProxSILAB et la latence du réseau.

Question 10

Le programme de formation est crucial pour gérer le turn-over important et l'uniformisation du mode de fonctionnement.

Axe de formation	Contenu essentiel	Format recommandé
Sécurité et usage	Procédures de sécurité (VPN obligatoire, gestion du mot de passe, perte/vol)	E-learning (rapide, traçable) et Module de test.
Nouveaux outils métier	Utilisation de l'application de rapport de visite et de gestion des frais.	Ateliers présentiels ou Visio (par groupe de secteur).
Réseau et connectivité	Fonctionnement du VPN, connexion au WiFi sécurisé du siège.	Guide papier et tutoriels vidéo.
Logiciels bureautiques	Présentation des logiciels standardisés.	E-learning et Foire aux Questions (FAQ).

Question 11

Les livrables doivent être complets et concerner à la fois le Service Développement et le Service Réseau et Système.

Catégorie de Livrable	Documents et Éléments attendus	Responsable(s) Principal(aux)
Technique/Système	Dossier d'Architecture Technique, Schéma d'infrastructure.	Service Réseau et Système
Déploiement	Image Master et procédures de masterisation, Inventaire détaillé des équipements.	Service Réseau et Système
Applicatif/Logiciel	Spécifications fonctionnelles et techniques des applications, Code Source.	Service Développement
Sécurité	Charte de Sécurité, Matrice des flux réseau (ACL sur MUTLAB).	Service Réseau et Système
Utilisateur/Support	Manuel Utilisateur du nouvel équipement et des applications métier, Procédures de support.	Services Développement, Rédaction
Gestion de Projet	Indicateurs de Suivi (KPI) : Taux d'équipement, Taux d'utilisation du VPN, DMR des incidents.	DSI / Chefs de Projet

4 Memento Technique

Cette section a été entièrement faite par IA, afin de pouvoir terminer le compte rendu à temps.

Terme technique	Catégorie	Définition	Contexte d'utilisation dans GSB
VLAN (Virtual LAN)	Réseau	Technique permettant de segmenter un réseau physique en plusieurs réseaux logiques.	Utilisé pour séparer les services (Développement, Visiteurs, Serveurs).
VPN (Virtual Private Network)	Sécurité/Réseau	Tunnel chiffré sur un réseau public pour connecter un utilisateur distant au réseau privé de l'entreprise.	Indispensable pour l'accès sécurisé des visiteurs mobiles aux ressources internes.
ACL (Access Control List)	Sécurité/Réseau	Liste de règles pour filtrer les flux et déterminer quel trafic est autorisé ou bloqué.	Utilisé sur le commutateur MUTLAB pour le routage inter-VLAN.
Masterisation	Déploiement/Logiciel	Processus de création d'une image système standardisée qui sera clonée sur plusieurs postes.	Recommandé pour l'uniformisation des 450 ordinateurs portables.
Chiffrement	Sécurité	Rendre illisible une information à l'aide d'une clé, sauf pour le destinataire.	Mesure de sécurité pour protéger les données stratégiques sur le disque dur.
DHCP	Réseau	Protocole attribuant automatiquement les adresses IP aux clients.	Assure la distribution des adresses IP, notamment le VLAN Visiteurs.
Annuaire	Logiciel/Système	Base de données centralisée qui stocke les informations des utilisateurs (comptes, mots de passe).	Utilisé pour la gestion centralisée des environnements et l'authentification (LABANNU).
PGI	Logiciel/Système	Système d'information qui intègre toutes les fonctions de gestion (RH, Comptabilité, GRC).	Le PGI de GSB (PGILAB) est le système central à interfacer.
Turn-over	RH/Gestion	Taux de renouvellement du personnel d'une entreprise.	Jugé important chez les visiteurs, rendant le suivi et la formation complexes.
Routage Inter-VLAN	Réseau	Mécanisme permettant aux différents VLAN de communiquer entre eux via un équipement de niveau 3.	Réalisé par le commutateur MUTLAB chez GSB
Virtualisation	Système	Technologie permettant de créer une version virtuelle d'une ressource physique pour consolider les services.	Utilisée pour un nombre croissant de serveurs chez GSB

5 Retour d'expérience

Ce tp a pris beaucoup trop de temps. Je trouve que réduire la quantité de question ou le couper en 2 aurait donné lieu à un meilleur rendu final.