Aubrée Romain **Sotoca**
19/11/2025

Groupe 1

Atelier 9 TP 1

1)

Modèle recommandé : Lenovo ThinkPad X/T Series, Dell Latitude, ou HP EliteBook. Ces modèles offrent un bon indice de durabilité et des garanties professionnelles.

Configuration minimale : Intel Core i5 (dernière ou avant-dernière génération) ou AMD Ryzen 5 Pro. Ils ont un bon rapport qualité/prix/puissance.

RAM : 16Go ou 8Go selon l'utilisation du multitâche, l'idéal étant 16.

Stockage : SSD NVMe de 512 Go, avoir beaucoup de stockage est inutile étant donné le cloud, cela va juste servir à stocker et tourner les logiciels.

Autonomie Batterie : 8/10h, pour coller à la journée de travaille.

Poids : environ 1.4kg pour faciliter le transport.

2)

Système de chiffrement : Bitlocker est intégré à Windows Pro/Entreprise, il effectue une chiffrement du disque dur.

Gestion clé de récupération : Les clés doivent être centralisées dans l'AD (Active Directory) de l'entreprise.

Séparation Données Pro/Perso : Mise en place d'une charte informatique stricte interdisant l'usage personnel de la machine.

Procédure en cas de perte ou vol : Verrouillage et/ou d'effacement à distance (Remote Wipe) des données via la solution MDM (si le poste est connecté à Internet) ou/et révocation immédiate des accès (certificats VPN, mots de passe) de la machine.

Empêcher l'Installation de Logiciels Non Autorisés : Mise en place d'une politique de liste blanche (whitelist) via AppLocker (ou un équivalent d'Endpoint Protection). Seuls les .exe approuvés par l'entreprise peuvent être lancés.

3)

Solution de masterisation recommandée : Microsoft Endpoint Configuration Manager (MECM / SCCM), ou WDS (Windows Deployment Services) combiné à MDT (Microsoft Deployment Toolkit). Ces outils permettent de créer un master préconfiguré (OS, applications métier, VPN, paramètres de sécurité BitLocker, etc…).

Estimation du temps de déploiement : Il faut prévoir le déploiement d'environ 56 postes par semaine. La phase initiale de préparation du master (environ 2-3 semaines) doit être complétée avant le début du déploiement, donc environ 8 semaines.

Organisation du déploiement par régions : Déploiement par vague géographique, Pour faire en sorte que le support technique puisse rester “dans la zone” pour éviter les déplacements lointains.

Procédure de test après déploiement : Une checklist de validation et obligatoire incluant un test de connexion VPN/Wifi, lancement des applications métiers, vérification du chiffrement BitLocker, et test d'accès aux ressources partagées.

Mise à jour de l’image : Maintenir une image de référence, les mises à jour de sécurité et d'applications critiques doivent être intégrées à l'image tous les trimestres.

4)

Solution VPN recommandée : Un VPN SSL (Secure Sockets Layer). Les solutions basées sur SSL (comme Cisco AnyConnect ou les clients VPN intégrés aux pare-feu modernes) sont mieux car elles sont plus simples à configurer pour les utilisateurs, et sont moins susceptibles d'être bloquées par les réseaux Wi-Fi publics.

Configuration accès WiFi sécurisé : Authentification 802.1X pour l'accès aux réseaux internes du siège GSB ou/et configuration automatique de l'ordinateur pour établir le tunnel VPN dès la connexion à un réseau Wi-Fi public ou externe.

Politique pour les connexions Wi-Fi publiques : Connexion aux ressources internes de GSB OBLIGATOIREMENT via le tunnel VPN chiffré.

Garantir l'accès aux ressources internes : Le VPN doit donner accès uniquement aux VLANs “Serveurs” et “Sortie”.

Impact du VPN sur les performances : Il peut y avoir des décalage mais c’est au prix de la sécurité.

5)

Données à sauvegarder automatiquement : Documents de travail/rapports de visite, fichiers de présentation/notices (données sources du labo) et données de l'application de gestion des frais.

Fréquence de sauvegarde : Synchronisation des dossiers de travail vers le cloud dès que la connexion VPN est établie (ou client de synchronisation s’il y a internet)

Lieu de stockage des sauvegardes : Cloud d'entreprise sécurisé (Microsoft OneDrive Entreprise, SharePoint par exemple), le stockage local est une copie, la source principale doit être sur un serveur GSB.

Restauration des données : L'utilisateur peut récupérer ses fichiers via le Cloud.

Remontée des informations terrain : Développement d'une application métier centralisée pour l'enregistrement des informations, accessible via le VPN.

6)

Solution pour la saisie électronique : Mise en place d'un logiciel de gestion de notes de frais (Expensify, Concur, module intégré à l'ERP GSB par exemple), accessible via l'application métier ou une interface web sécurisée.

Intégration avec le système comptable : Utilisation d'une API ou d'un export automatique (CSV/XML) de la solution de frais vers le système comptable pour la gestion des remboursements.

Procédure de validation des frais : Mise en place d'un workflow de validation numérique, l'intégration des justificatifs (photos de reçus) est obligatoire pour remplacer la gestion forfaitaire.

Gestion des différents types de frais : Avec un plafond unique et règles

Délais de remboursement cible : Un délai maximal de 5 jours après validation finale par le responsable de secteur, rendu possible par l'automatisation du processus.

7)

Données RH accessibles : Visiteur médical (coordonnées professionnelles, affectation géographique, rattachement hiérarchique, historique de formation) et délégué/responsable (liste et coordonnées de leur équipe).

Garantir la confidentialité : L'accès doit se faire via une interface sécurisée (application métier ou portail RH).

Niveaux d'accès : Visiteur < Délégué régional < Responsable de secteur < Service RH/DSI.

Intégration avec le système RH : Utilisation de l'annuaire d'entreprise pour l'authentification et de l'API du SIRH (Système d'Information RH) pour récupérer les données vers l'interface sécurisée.

Procédure pour les nouveaux arrivants : Les informations de la nouvelle recrue doivent être renseignées dans le SIRH, ce qui déclenche automatiquement la création de son compte utilisateur AD.

8)

Outils de surveillance à distance : Microsoft Intune permet de surveiller l'état matériel (santé du disque, niveau de la batterie), vérifie la conformité des logiciels (antivirus, VPN), et effectue l'inventaire. TeamViewer (Version Entreprise) permet de visualiser et de prendre le contrôle du poste de travail pour résoudre un problème de logiciel ou de configuration après l'accord du visiteur et via le tunnel VPN sécurisé. GLPI ou Zendesk permet de centraliser toutes les demandes. Le visiteur peut soumettre un problème même à distance et suivre son statut.

Diagnostiquer un problème à distance : Grâce à Microsoft Intune et TeamViewer on pourra vérifier les performances/composants de l'ordinateur et TeamViewer permettra de prendre contrôle du pc pour simplifier la résolution du problème à distance.

Procédure pour les pannes matérielles : Envoi immédiat d'un poste de remplacement préconfiguré au visiteur, retour du poste défectueux au siège pour réparation/reconditionnement.

Gérer le remplacement rapide d'un équipement : Maintenir un stock tampon (environ 10-15 postes) de machines masterisé, prêtes à être envoyées.

Indicateurs de suivi : Envoie et comparaison des informations (température, vitesse ventilateur, santé des disques) journalière automatique grâce à Microsoft Intune.

9)

Intégration des nouveaux équipements dans la segmentation VLAN : Les visiteurs doivent rester dans le VLAN Visiteurs ou Visiteurs Internes, l'accès à leurs applications métier se fera via le tunnel VPN.

Politique d'accès Wi-Fi pour les visiteurs en déplacement : La connexion aux ressources internes doit toujours passer par le VPN.

Garantir la sécurité des connexions distantes : Les ordinateurs doivent être configurés pour bloquer l'accès aux ressources GSB si le VPN n'est pas établi (en cas d'oubli).

Bande passante nécessaire pour 450 utilisateurs mobiles : bande passante asymétrique de type FTTO (Fibre Optique Dédiée) avec un minimum de 500 Mbps en Upstream (émission), car c'est cette vitesse qui limite le nombre de connexions VPN simultanées.

Monitorer l'utilisation du réseau : Utilisation de ManageEngine sur les routeurs et le pare-feu pour suivre le trafic VPN.

10)

Format de formation recommandé : Un format Blended Learning.

Durée de formation par visiteur : 1 journée (4 à 6 heures) de formation initiale en groupe et accès illimité aux “cours”.

Points essentiels à couvrir : Sécurité, Utilisation de l’application métier, procédure de gestion des notes de frais, Bonnes pratiques d'utilisation (sauvegarde des données, charte informatique).

Évaluation de l'acquisition des compétences : Un quiz obligatoire à la fin de la session présentielle et un suivi des première utilisation de l'application métier.

Support post-formation : Mise en place d'un Service Desk avec un portail utilisateur, un numéro d'appel unique et un système de tickets pour le suivi des incidents.

Gestion de la formation des nouveaux arrivants : Le Délégué régional doit avoir l'outil pour former (kits d'accueil, accès rapide aux “cours”). Le Service RH (VLAN 30) envoie automatiquement les accès aux “cours” à la date d'embauche.

11)

Documents techniques à fournir : Procès-verbal d'acceptation (PV), manuel de masterisation/déploiement, schéma d'architecture réseau VPN, dossier d'architecture applicative, inventaire final du matériel.

Documentation utilisateur nécessaire : Guide de démarrage rapide du PC (instructions pour la première connexion, l'accès au VPN, et les étapes initiales de la connexion sécurisée), Manuel utilisateur de l'application métier (tutoriels détaillés pour l'enregistrement des visites et la saisie/validation des notes de frais), Support de formation (les kits “e-learning” et les présentations utilisés lors de la formation initiale), aide-mémoire sécurité (un document synthétique listant les bonnes pratiques (utilisation du VPN, gestion des mots de passe, procédure en cas de perte/vol)).

Procédures opérationnelles à décrire : Procédure de support (helpdesk), procédure de perte ou vol de matériel, procédure de gestion du cycle de vie (remplacement équipement défectueux), procédure d'arrivée/départ (gestion des accès et des équipements lors de l'arrivée d'un nouveau visiteurs ou de son départ.

Documentation de la configuration de sécurité : Charte d'utilisation des équipements nomades, politique d’accès sécurisé, rapport de conformité et de durcissement (hardening).

Indicateurs de suivi proposés : indicateur d'efficacité (délai moyen de traitement des notes de frais), indicateur de performance (taux d'adoption de l'application métier), indicateur de sécurité (taux de conformité BitLocker), indicateur de support (taux de résolution au premier contact ou temps moyen de réparation)

Mémento technique

Conclusion

Premier TP et introduction sur le réseau (SISR) et la gestion réseau entreprise.