Charpenay Côme Sio 1
19/11/25

B1 TP Compte Rendu

Cahier Des Charges

Partie 1

Sommaire :

Q1

Ordinateur portable Dell 15 -> respectant ces caractéristiques caméra HD intégré pour réunion.

Processeur :
min: intel i3 ou Ryzen 5
max: intel i5 ou Ryzen 5
RAM: 8Go

Processeur haute gamme mais d'entrée de marché pour avoir une stabilité du produit et un bon rapport qualité prix permettant des économies, une mémoire vive de 8 Go permettant plusieurs tâches en simultanés sur l'ordinateur. Du côté stockage il est favorable d'avoir 128Go minimum et 512Go max pour stocker plusieurs comptes-rendu, logiciels importants. L'autonomie de la batterie optimale serait ~7h pour les sessions de travail journalières. Le poids maximum serait inférieur à 2.5kg pour le confort de l'utilisateur.

Q2

Système chiffrement

Votre ordinateur peut prendre en charge le chiffrement de lecteur BitLocker (en anglais) ou le chiffrement de l'appareil (en anglais). Vous pouvez vérifier si votre appareil prend en charge le chiffrement BitLocker standard ou le chiffrement de l'appareil. Indisponible sur Windows 11 et 10 Famille.

Clé de Récupération

Normalement, votre clé de récupération est sauvegardée lorsque BitLocker est activé. Si vous activez le chiffrement de lecteur BitLocker, vous devez sélectionner manuellement l'emplacement de stockage de la clé de récupération pendant le processus d'activation. Si vous activez le chiffrement de l'appareil à l'aide d'un compte Microsoft, le chiffrement démarre automatiquement et la clé de récupération est sauvegardée sur votre compte Microsoft. Récupérez la clé de récupération et saisissez-la pour utiliser à nouveau votre ordinateur.

Windows permet d'ajouter plusieurs comptes d'utilisateur pour utiliser le même appareil, ce qui permet à chaque utilisateur d'avoir ses propres paramètres, documents et applications. Vous pouvez donc créer 2 utilisateurs sur votre poste informatique pour séparer un utilisateur professionnel et un personelle.

Perte et Vol

Localiser mon appareil est une fonctionnalité qui peut vous aider à localiser votre Windows 10 ou Windows 11 appareil s'il est perdu ou volé. Pour utiliser cette fonctionnalité, connectez-vous à votre appareil avec un compte Microsoft et assurez-vous d'en être l'administrateur. Cette fonctionnalité fonctionne lorsque la localisation de votre appareil est activée, et ce, même si d'autres utilisateurs de l'appareil ont désactivé les paramètres pour leurs applications. Chaque fois que vous essayez de localiser l'appareil, les utilisateurs verront une notification dans la zone de notification.

Pour configurer le blocage des applications potentiellement indésirables, accédez à Démarrer les paramètres > Mettre à jour & Sécurité > Sécurité Windows > contrôle de navigateur & > paramètres de protection basée sur la réputation.

Vous y trouverez un contrôle qui vous permet de désactiver le blocage des applications potentiellement indésirables et de sélectionner si vous souhaitez bloquer les applications, les téléchargements ou les deux.

Q3

Les services de déploiement Windows (WDS) sont la version révisée des services d'installation à distance (RIS). WDS permet le déploiement de systèmes d'exploitation Windows. Vous pouvez utiliser WDS pour configurer de nouveaux clients avec une installation basée sur le réseau sans nécessiter que les administrateurs visitent chaque ordinateur ou s'installent directement à partir d'un support CD ou DVD.

Fog Project est un logiciel sous Linux qui va vous permettre d'effectuer vos déploiements pour machines Windows, Linux, et Mac. Le déploiement sur les clients se fera par le biais d'un serveur PXE fourni par Fog Project. Un client est également disponible pour déployer des applications sur des systèmes en cours d'exécution.

Temps de déploiement :

WDS : 1 postes 10 min

Fog Project : 20 postes 45 min

OS Deployer est une solution complète qui automatise la création d'image disque et le déploiement de systèmes d'exploitation. En quelques étapes simples, les administrateurs peuvent enregistrer l'image disque de différentes versions de système d'exploitation, personnaliser les images selon les besoins des rôles d'utilisateur et des services d'une entreprise et les déployer sur plusieurs ordinateurs du réseau.

Image de machines en ligne

Créez une image d'une machine en ligne et fonctionnant dans le réseau sans nuire à la productivité de l'utilisateur final.

Migration des données des profils utilisateurs

Gagnez du temps et de l'énergie en migrant de manière transparente les profils d'utilisateurs au moment même où vous déployez le système d'exploitation.

Déploiement indépendant du matériel

Déployez une image de système d'exploitation normalisée sur n'importe quel ordinateur, de tout fournisseur ou modèle. OS Deployer configure automatiquement les paramètres concernés et installe les pilotes requis.

Déploiement personnalisé

Personnalisez l'image pour un déploiement selon les besoins de l'entreprise. Vous pouvez aussi configurer les activités post-déploiement et les applications à installer sur l'ordinateur cible après l'opération.

Déploiement de système d'exploitation partout

Déployez des systèmes d'exploitation sur tous les ordinateurs d'un site distant à partir d'une console centralisée.

Gestion automatisée des pilotes

Gestion fiable et pratique des pilotes pour collecter et distribuer automatiquement les pilotes sur n'importe quel ordinateur, n'importe où.

L'approvisionnement d'un ordinateur cible ou de test est le processus de configuration d'un ordinateur pour le déploiement, le test et le débogage automatiques des pilotes. Pour approvisionner un ordinateur, utilisez Microsoft Visual Studio.

Un environnement de test et de débogage comporte deux ordinateurs : l'ordinateur hôte et l'ordinateur cible. L'ordinateur cible est également appelé ordinateur de test. Vous développez et générez votre pilote dans Visual

Studio sur l'ordinateur hôte. Le débogueur s'exécute sur l'ordinateur hôte et est disponible dans l'interface utilisateur de Visual Studio. Lorsque vous testez et déboguer un pilote, le pilote s'exécute sur l'ordinateur cible.

Q4

VPN : NordVPN
Configurez accès Wifi: Se rendre dans les paramètres WiFi > connectez-vous à l'interface avec vos identifiants et sélectionnez l'option "WiFi". Modifier le mot de passe dans la section "Sécurité", entrez un nouveau mot de passe sécurisé.
Politiques Connexions Wifi publiques:
Les données suivantes peuvent être conservées pendant un délai de 3 mois maximum :

- **les données permettant d'identifier l'origine de la communication ;**
- **les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication ;**
- **les données techniques permettant d'identifier le ou les destinataires de la communication ;**
- **les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs.**

Garantir l'accès des ressources internes:
Acces zero Trust
Impact VPN sur les performances: En fonction de votre fournisseur de services, de l'appareil et d'autres aspects de votre configuration, un VPN peut effectivement ralentir votre débit Internet jusqu'à 50 %. Votre VPN est juste un logiciel qui chiffre et reroute votre trafic, en utilisant la connexion de votre FAI sur votre réseau.

Q5:

Données à sauvegarder automatiquement : fichiers importants, documents techniques..
Fréquence sauvegarde : Toutes les semaines
Où sont stockés les sauvegardes : Dans l'espace Cloud
Restaurer les données en cas de panne : Accédez au site web OneDrive. (Vérifiez que vous êtes connecté avec le compte approprié). > Options, puis sélectionnez Restaurer votre OneDrive dans le volet de navigation gauche. Remarque : Cette option est disponible uniquement avec un abonnement Microsoft 365.
Assurer la remonté des informations terrain :
Service Desk

Q6:

Quelle solution pour la saisie électronique des notes de frais : N2F (web), Cegid Notilus, Evoliz, Expensya (Web)
Comment intégrer avec le système comptable existant : Evoliz est accessible depuis n'importe quel navigateur (edge, chrome, safari...) et développé pour être responsive *(c'est à dire que ça rend bien)* sur tous les supports : ordinateur, smartphone, tablette...

Quelle procédure de validation des frais : Certifié NF203, NF525 et conforme Factur-X *(et ça, c'est plutôt classe)*, Evoliz s'occupe de l'ensemble des obligations liées à la facturation.factures de situation, récurrences, multi-devises, envoi sur Chorus Pro... Evoliz s'adapte à votre métier.

Comment gérer les différents types de frais (transport, repas, hébergement) :

Quels délais de remboursement cible :

Q7:

Quelles données RH doivent être accessibles: les données personnelles (téléphone, nom, prénom..)

Comment garantir la confidentialité des données:

SSO : OpenID Connect / SAML pour authentification centralisée (réduit les identifiants distribués).

Contrôle d'accès : RBAC (rôles pré-définis -> Admin RH, Manager, Paie, Recrutement, Lecture seule, External Partner) et, si besoin, ABAC pour règles fines (ex : accès selon site, service, contrat).

MFA : obligatoire pour tous les accès RH et pour les appels API à droits élevés.
Chiffrement : TLS 1.3 en transit ; chiffrement au repos (clé gérée KMS), chiffrement des champs sensibles (numéro SS, coordonnées bancaires).
Audit & SIEM : collecte des logs d'accès et d'API vers SIEM, alertes sur accès anormaux, conservation des logs conformes.
Hébergement : préférence pour environnements hébergés certifiés (ISO27001, SOC2) ou instance on-premises selon l'analyse de risque.

Exemple App: RH DEMAT

Quels niveaux d'accès différenciés mettre en place:

Voici quelques solutions à mettre en place.

Super-Admin (Sécurité/IT) : gestion comptes, audit — accès très restreint, supervisé.
Admin RH : gestion complète dossier (sauf données très sensibles si séparées).
Paie : accès uniquement aux champs nécessaires à la paie ; journalisation forte.
Manager : accès aux données professionnelles de son périmètre (coordonnées, contrat, évaluations), pas aux informations bancaires/santé.
Intervenant externe / lecture seule : accès limité à documents spécifiques (ex : contrats signés) via flux contrôlé ou espace sécurisé.
Principe du moindre privilège : attribution par défaut zéro, approbation manuelle pour montée en droit, revues trimestrielles.
Segmentation : séparer accès lecture/écriture (ex : équipe paie peut écrire dans paie mais pas modifier contrat).

Comment intégrer avec le système RH existant:

Vous pouvez cartographier les sources (HRIS, paie, annuaire, GED) et identifier la source de vérité pour chaque donnée. Vous pouvez également déployer SSO (Okta/Azure AD/Keycloak) + SCIM pour automatiser création/suppression de comptes. Grâce à API Gateway / Middleware il est possible de centraliser les appels API, appliquer sécurité (OAuth2, rate limiting, WAF). Il est important d'utiliser des fonctions de Mapping & transformation pour définir des contrats API (OpenAPI), tests d'intégration, et environnements préprod séparés. Il est conseillé de faire des tests via des pentests, revues conformités GDPR, tests de reprise et scénarios

offboarding (ensemble des procédures et pratiques mises en œuvre par une entreprise lors du départ d'un employé).

Quelle procédure pour les nouveaux arrivants:

Q8:

Quels outils de surveillance à distance recommandez-vous ?

Supervision réseau & serveurs : Zabbix, Centreon, Nagios, PRTG.
Supervision postes & usages : Microsoft Intune, GLPI + FusionInventory, Lansweeper.
Prise en main à distance : AnyDesk, TeamViewer, Microsoft Remote Desktop.
Journalisation & alertes : Graylog, ELK (Elastic Stack)

Outils Recommandés: pour Supervision -> Centreon/Zabbix pour prise en main à distance -> Anydesk

Comment diagnostiquer un problème à distance ?

Collecte des informations : demande à l'utilisateur le message d'erreur, le contexte, la dernière action effectuée.
Analyse via outils : vérifier alertes dans l'outil de supervision (CPU, RAM, réseau, disques...).

Tests rapides : **ping, vérification route réseau, test des services, redémarrage applicatif.**
Consultation des logs **(système, application)(Anydesk).**

Quelle procédure pour les pannes matérielles ?

Voici une listes de contraintes à suivre:

1.Diagnostic à distance pour confirmer qu'il s'agit bien d'un problème matériel.

2.Ouverture d'un ticket avec description, numéro de série et impact.

3.Vérification de la garantie (constructeur ou contrat entreprise).

4.Intervention locale ou échange standard (selon la criticité).

5.Remplacement ou envoi du matériel défectueux au fournisseur.

6.Re-test après réparation + mise à jour du parc informatique (inventaire).

Comment gérer le remplacement rapide d'un équipement ?

Voici une listes de contraintes à suivre:

1.Diagnostic à distance pour confirmer qu'il s'agit bien d'un problème matériel.

2.Ouverture d'un ticket avec description, numéro de série et impact.

3.Vérification de la garantie (constructeur ou contrat entreprise).

4.Intervention locale ou échange standard (selon la criticité).

5.Remplacement ou envoi du matériel défectueux au fournisseur.

6.Re-test après réparation + mise à jour du parc informatique (inventaire).

Quels indicateurs de suivi mettre en place ?

Avoir un stock supplémentaire de matériel prêt à l'emploi (PC, écrans, routeurs).
Utiliser des images système préconfigurées (Windows Autopilot, Clonezilla).
Automatiser les configurations via profils Intune / Active Directory. Récupération de l'ancien matériel pour réparation ou recyclage.