PROJET EQUIPEMENTS
Choix d'équipement pour les visiteurs

(Michaël DANIEL, Julien ROLLAND)

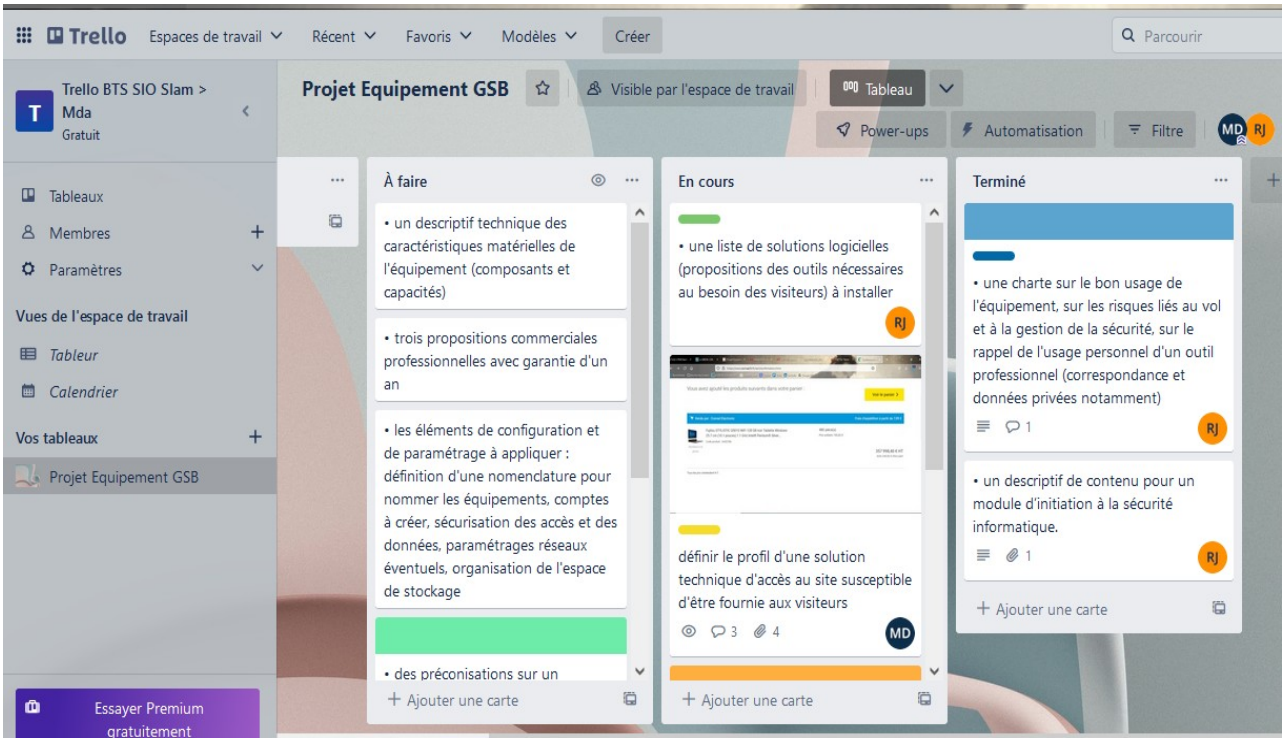
Table des matières

Contexte

Le laboratoire Galaxy Swiss Bourdin (GSB) est issu de la fusion entre le géant américain Galaxy (spécialisé dans le secteur des maladies virales dont le SIDA et les hépatites) et le conglomérat européen Swiss Bourdin (travaillant sur des médicaments plus conventionnels).
En 2015, les deux géants pharmaceutiques ont uni leurs forces pour créer un leader de ce secteur industriel. L'entité Galaxy Swiss Bourdin Europe a établi son siège administratif à Paris.
Le siège social de la multinationale est situé à Philadelphie, Pennsylvanie, aux Etats-Unis.
L'entreprise compte 480 visiteurs médicaux en France métropolitaine (Corse comprise), et 60 dans les départements et territoires d'outre-mer. Les territoires sont répartis en 6 secteurs géographiques (Paris-Centre, Sud, Nord, Ouest, Est, DTOM Caraïbes-Amériques, DTOM Asie-Afrique).
Les délégués médicaux disposaient d'un forfait pour s'équiper au niveau informatique.
Face à l'hétérogénéité des équipements choisis et utilisé, la DSI souhaite fournir un équipement homogène qui conviendrait aux besoins de ces utilisateurs. Seuls les visiteurs médicaux de métropole sont concernés par ce projet. Vous êtes chargé d'étudier le cahier des charges et de proposer des solutions qui le respectent.

Planification des tâches

Utilisation du site Trello avec la méthode Kanban pour l'organisation des tâches.



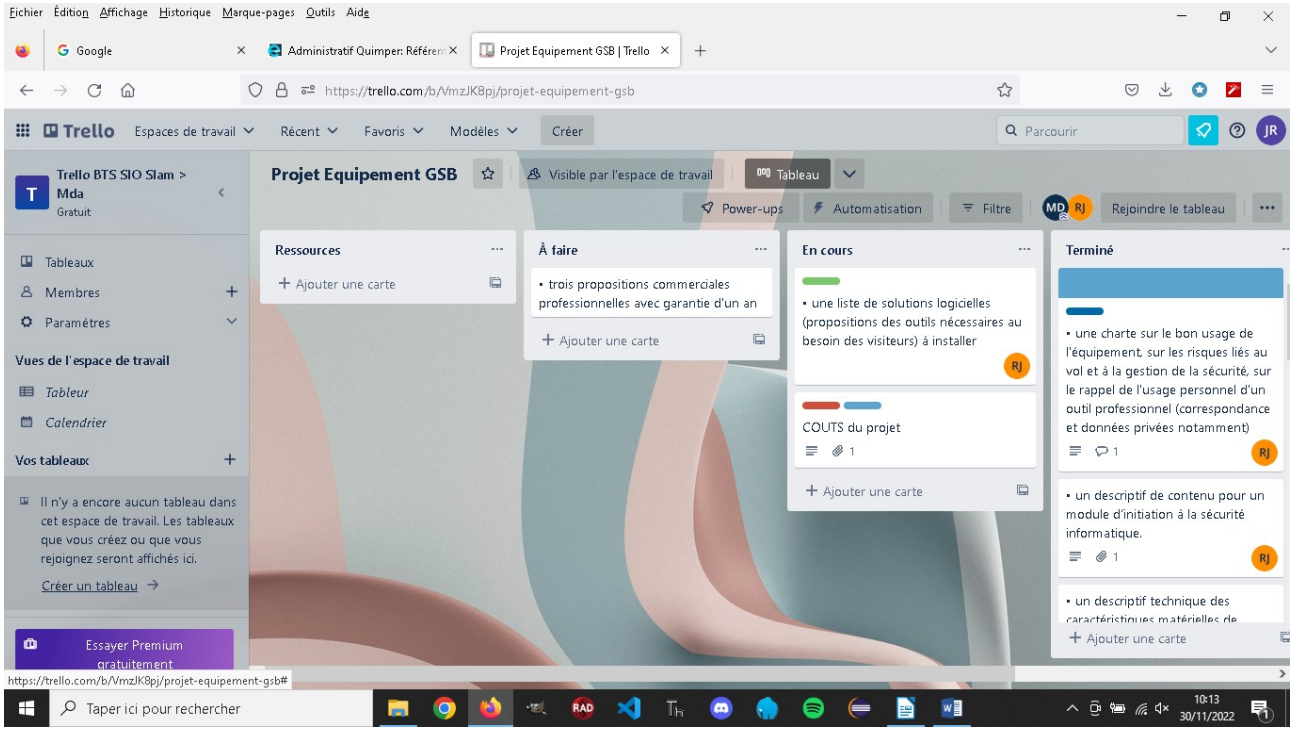
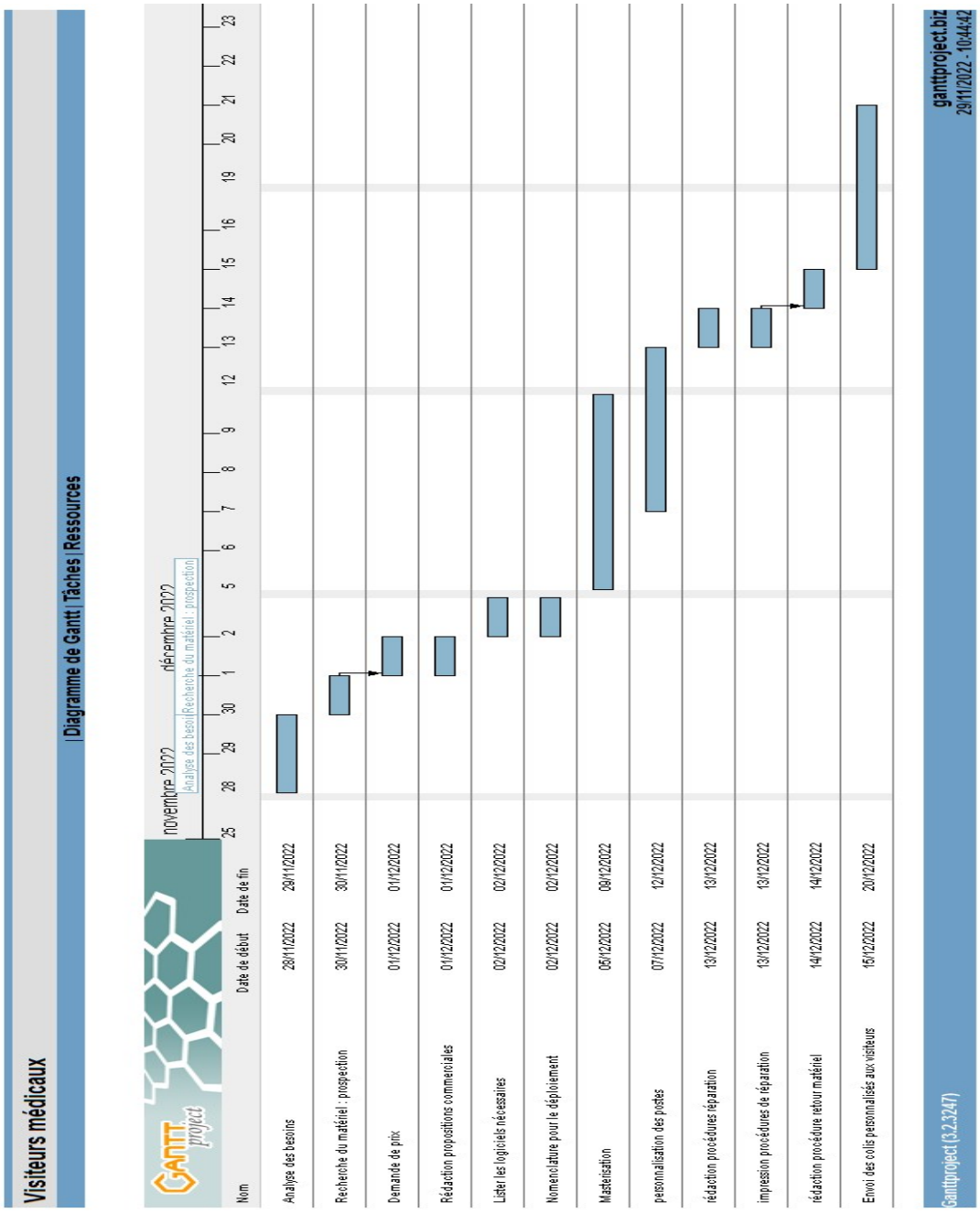


Diagramme de Gantt

Le diagramme de Gantt est un outil utilisé en ordonnancement et en gestion de projet et permettant de visualiser dans le temps les diverses tâches composant un projet. Il s'agit d'une représentation d'un graphe connexe, qui permet de représenter graphiquement l'avancement du projet.



Spécifications techniques

Environnement

Les visiteurs ont l'habitude des environnements Microsoft : Windows 10, Windows 11.

Utilisation

L'équipement doit être transportable (déplacements), connectable à un réseau filaire ou sans fil (hôtels). Il doit pouvoir être transporté lors des visites (utilisable en cas d'attente longue au cabinet médical). Il doit pouvoir être glissé dans la mallette du visiteur. Il est destiné à la saisie de comptes-rendus à partir d'un serveur Web, à la visualisation de la documentation technique (en ligne ou au format PDF) et à un usage professionnel (exploitation de données tableurs, messagerie électronique, rédaction de lettres diverses, gestion d'un budget d'activité, etc.).

L'usage personnel de l'équipement est fortement déconseillé. Le cloisonnement des usages, entre vie professionnelle et vie privée est atout important vis à vis de la protection des données médicales sensibles. Aucune garantie ou dépannage relatifs aux outils personnels installés sur le matériel ne seront proposés.

Coût

480 visiteurs étant susceptibles d'être équipés, on cherchera un tarif concurrentiel et le plus faible au regard du besoin. Seuls les besoins professionnels seront pris en compte pour choisir les capacités de l'équipement.

Les visiteurs souhaitant un matériel plus performant pourront bénéficier d'un financement à hauteur du prix de l'équipement retenu, le reste étant à leur charge.

- Windows 10, Windows 11 (pas de mention si version pro ou pas).
- L'équipement doit être facilement transportable.
- encombrement faible (malette du visiteur).
- la saisie de comptes-rendu : clavier indispensable.
- Applications de type bureautique : ça ne requiert pas une puissance phénoménale en terme de matériel
- (quantité de RAM / CPU / carte graphique).
- Perte ou vol de l'équipement : pas d'accès possible aux données par un tiers : capteur biométrique

Configuration matérielle minimum

- Processeur AMD ou Intel, 4 coeurs, 2,8Ghz

- Mémoire : 8Go DDR4-3200

- Disque : Sata ou SSD : 250Go

- Taille de l'écran : 10 pouces**- Port résau Ethernet + Wifi, 2 Ports USB, 1 webcam.**

Propositions matériels

Propositions basées sur les contraintes :

Marque Fujitsu-Siemens (partenaire historique de la SSI, possibilité d'avoir des prix négociés sur le volume d'achat …)

Le matériel d'occasion n'est pas envisageable : impossibilité de bénéficier de la garantie constructeur, obsolescence rapide du matériel, volume à commander trop important (340 unités).

Fujitsu-Siemens LifeBook U7411

ds-LIFEBOOK_U7411.pdf

Fujitsu-Siemens Stylistic Q5010

ds-STYLISTIC-Q7311.pdf

ASUS Vivobook S 14 Flip OLED (TP3402)

ds-STYLISTIC-Q5010-APAC.pdf

Société GSB – Direction des services Informatiques

Proposition commerciale n° 1 :

Matériel	Fournisseur	Commentaires	PU (HT)	QTE	TOTAL
Tablet PC Fujitsu-Siemens Stylistic Q5010	CONRAD.fr		745,83 €	480	357 998,40 €
Contrôleur de Domaine pour le déploiement		Appartient à la SSI	0,00 €	1	0,00 €

Conditions et tarification

Vous trouverez ci-dessous un résumé des coûts estimés associés au matériel ci-dessus. Nous demandons 50 % du paiement total à l'avance et les 50 % restants sont dus à la livraison de l'ordinateur. Les paiements doivent être effectués à temps et selon les conditions du contrat. Si les paiements ne sont pas reçus aux dates d'échéance convenues, La société GSB se réserve le droit d'interrompre tout travail jusqu'à ce que le solde impayé soit versé.

Tarification

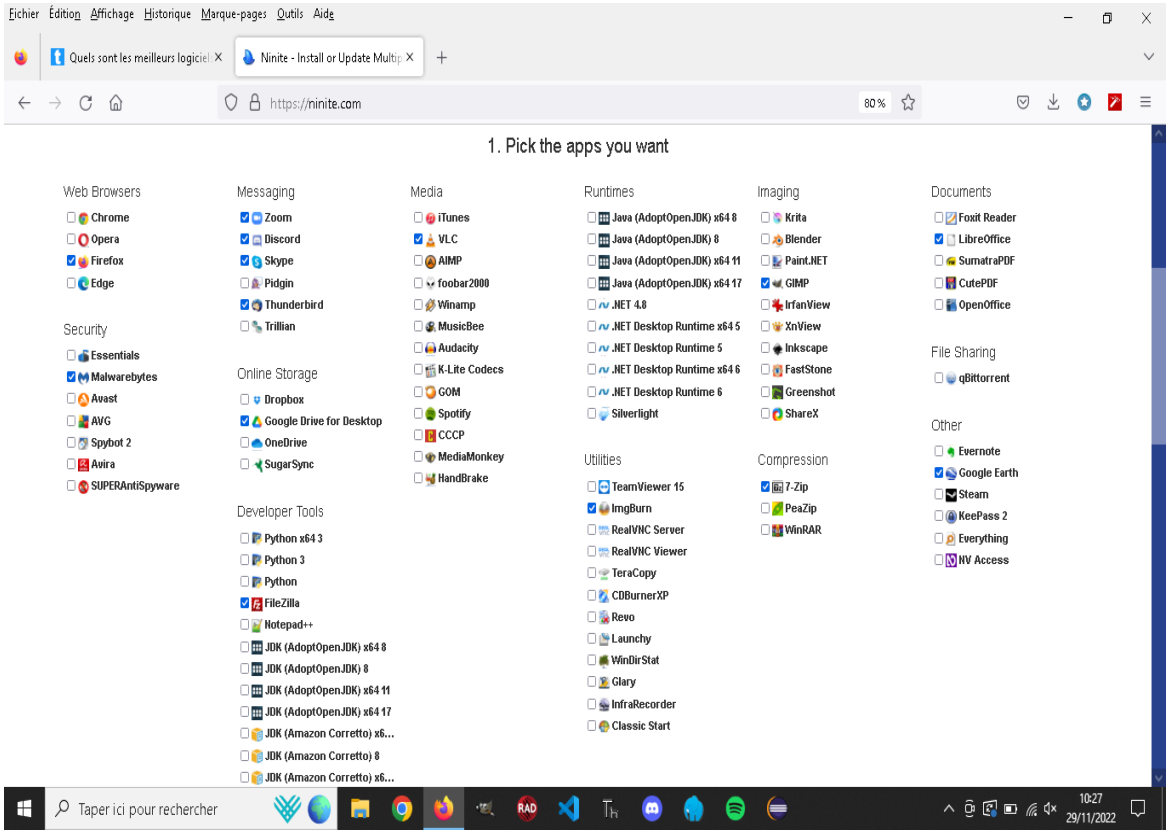
Nom	Prix	Quantité	Sous-total
Tablet PC Fujitsu-Siemens Stylistic Q5010	€745,83	480	€357 998,40
Frais de mise en service unique	€249,00	1	€249,00
Maintenance trimestrielle	€129,00	1	€129,00
Sous-total	€**877,00**		
Total	€877,00		

Calendrier de paiement

Date du paiement	Montant du paiement
Dès l'acceptation du contrat	50 % du solde total
Dès la livraison du [Product 1]	50 % du solde total

Propositions logiciels

Utilisation de ninite pour l'installation des logiciels.Le site Ninite est composé d'une page proposant diverses catégories, dans lesquelles se situent de nombreux logiciels, comme par exemple les navigateurs Web Google Chrome et Mozilla Firefox, le lecteur de média VLC, la suite bureautique OpenOffice, et bien d'autres encore. Le fonctionnement du siteest assez simple. Une fois sur le site internet vous devez tout d'abord sélectionner les logiciels que vous souhaitez installer. Pour l'exemple, nous allons choisir quelques logiciels en cochant la case comme sur l'image suivante. une fois que vous avez sélectionné tous les logiciels que vous souhaitez installer, il vous suffit de continuer vers le bas de la page de Ninite et vous trouverez le bouton « Get Your Ninite ».



- Libre Office
- Chrome, Firefox
- FileZilla
- 7-ZIP
- Pdf creator
- VLC
- Skype
- Windows defender
- Malwarebyte
- Ccleaner

Configuration

Déploiement :

WDS est le service de déploiement de systèmes d'exploitation Microsoft. Il permet de déployer dans un réseau d'entreprise des fichiers WIM, VHD et VHDX en démarrant depuis Windows PE, plus précisément depuis le fichier boot.wim. Ainsi, un administrateur n'a plus besoin de se déplacer pour installer Windows 10 depuis un support tel qu'un DVD-ROM ou un disque dur externe USB.

Il Faut :
- 1 contrôleur de domaine avec service DHCP.

Informations intéressantes pour la diffusion d'un "MASTER" avant d'automatiser l'installation de tous les postes, avec les logiciels adaptés, sans avoir à gérer la configuration poste par poste :

voir l'outil "sysprep"

Microsoft a un outil : "System Centre Configuration Manager" pour déployer des installations de postes en réseau, mais avec une licence payante :

System_Center_2022_licensing_datasheet_PW.pdf

==========

Suite au cours de Jean Georgelin sur l'automatisation et la personnalisation des installations de Windows sur un ensemble d'ordinateurs :
On peut utiliser des outils gratuits, comme :

Le Windows ADK (assessment deployment kit)

La multidiffusion en plaçant l'image maître de l'OS sur un serveur, et en l'installant à partir d' une connexion réseau.

Nomenclature de nommage des équipements :

Les 3 premiers caractères reprennent les initiales du nom de la société, en majuscule :

« GSB »

Suivi du n° de département du visiteur concerné – ex : 29

Enfin, le nom se termine par les 3 derniers chiffres du numéro de série de l'ordinateur : il y aura donc un lien fort entre le nom du PC et la matériel lui-même, qui devra changer changer en cas de remplacement du matériel.

Cela conduit à penser qu'il faut établir un tableau de suivi, une base de donnée mettant en relation le profil de l'utilisateur (Nom, adresse,…) et le nom de la machine qui lui a été attribuée.

Ce fichier sera alors mis à jour si le matériel devait changer (traçage du matériel suite à des opérations de maintenance)

- utilisation d'un caractère de séparation : trait d'union.

Exemple de nommage complet :

GSB-29-224

L'association département - numéro de série permet d'être assez sûr de disposer d'un nom unique.

Comptes à créer :

Administrateur :

Il ne sera pas nécessaire pour les utilisateurs de se connecter à un contrôleur de domaine.
Pour des opérations de maintenance, un compte administrateur Windows doit être créé avec un nom et un mot de passe connus du service informatique, valide pour l'ensemble des postes.

Exemple : **Administrateur / gs_ad*6791TT**

Utilisateur :

Compte utilisateur : **gsb / gsb**

Il sera demandé aux utilisateurs de modifier et personnaliser leur mot de passe, en prenant comme spécifications :

8 caractères minimum, au moins **1 majuscule**, au moins **1 caractère spécial** parmi cette liste : !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~

l'essentiel de la sécurité repose sur un accès matériel au PC contrôlé par un ou plusieurs capteurs biométriques qui empêcheront le démarrage matériel s'il n'est pas validé physiquement.

Problème : en cas de vol du PC portable ou de la tablette, le disque dur pourrait être extrait, ce qui contournerait le dispositif de protection biométrique.
Il faudrait alors aussi envisager de chiffrer le contenu du disque, en tout cas au minimum les données sensibles qui seront conservées sur une partition séparée.

Source Wikipedia :

Le chiffrement intégral du disque basé sur le matériel (en) dans l'appareil est appelés auto-chiffrement et n'a pas d'impact sur la performance du tout. En outre, la clé de chiffrement de support ne quitte jamais le dispositif et n'est donc pas accessible pour un virus dans le système d'exploitation.

Le chiffrement de la partition séparée pourra se faire à l'aide du logiciel Veracrypt, qu'il faudra installer sur tous les postes client.

Le mot de passe de protection de la partition ne sera pas défini par l'utilisateur, mais par la DSI, et communiquée à l'utilisateur de manière sécurisée (par téléphone ou par par mail avec échange de clefs publiques / privées PGP).

Déploiement d'une image personnalisée du système :

- Nous allons créer une installation de référence, capturez une image de l'installation et réexécutez « Windows programme d'installation » avec un fichier de réponses qui pointe vers notre image personnalisée. Le déploiement d'une image personnalisée à l'aide de « Windows configuration » offre plusieurs avantages par rapport à l'application d'une image à l'aide d'un outil de capture d'image.
- Le programme d'installation prend en charge les éléments suivants :
- Application d'un autre fichier de réponses pour des personnalisations supplémentaires pendant le déploiement.
- Reconfigurer la configuration du disque.
- Ajout de pilotes supplémentaires.
- Remplacement d'une clé de produit.
- Sélection d'une autre langue à installer.
- Sélection dans une liste d'images à installer, si votre fichier image contient plusieurs images.
- Installation sur un autre emplacement de lecteur.
- Mise à niveau d'une installation Windows existante.
- Configuration de l'ordinateur sur des systèmes d'exploitation à double démarrage.
- S'assurer que le matériel peut prendre en charge Windows.

Prérequis

Pour exécuter cette procédure pas à pas, vous devez disposer des éléments suivants :

Un ordinateur de technicien sur lequel les outils Windows Assessment and Deployment Kit (Windows ADK) sont installés.
ISO d'un produit Windows.

Un ordinateur de référence sur lequel vous allez installer et capturer votre image personnalisée.

Média PE de démarrage Windows. Il existe plusieurs types de Windows média PE que vous pouvez créer. Pour plus d'informations sur ces options, consultez la vue d'ensemble de WinPE.

Accédez à un partage réseau pour stocker votre image personnalisée et Windows configurer les fichiers sources.

Les étapes :

Étape 1 : Copier les fichiers sources d'installation Windows sur un partage réseau.

Étape 2 : Installer Windows sur votre ordinateur de référence.

Étape 3 : Capturer une image de l'installation.

Dans cette étape, nous allons capturer une image de l'installation de référence à l'aide de DISM, puis stocker l'image personnalisée sur un partage réseau.

Étape 4 : Créer un fichier de réponses personnalisé

> utilisation de « **Windows System Image Manager**. »

Étape 5 : Déployer l'image à l'aide du programme d'installation de Windows.

Récupération d'un poste client en vu de sa réparation :

On aurait pu inviter le client à créer un ticket d'incident à l'aide d'une solution logicielle de prise en charge du matériel (GMAO) comme glpi, mais si on considère justement que l'ordinateur n'est plus opérationnel et que c'est le seul outil informatique à sa disposition, il faudra plutôt traiter les demandes du client par téléphone, et utiliser glpi en interne, au niveau du service informatique.

Le client devra envoyer son matériel directement auprès d'un transporteur, qui se chargera de l'emballage et de l'expédition du colis. A réception, il sera enregistré informatiquement (glpi) pour avoir un suivi de la réparation.

Entre temps, un autre ordinateur, a destination du client aura été préparé, personnalisé au nom du client (avec ses codes, login, mots de passe…) et disposera des données issues de la la dernière sauvegarde réalisée avant le crash matériel.

Le visiteur médical n'aura ainsi pas à attendre le retour de son matériel après réparation, il sera ré-équipé au plus vite. Une fois réparé , le PC sera stocké dans un local, et pourra servir pour d'autres personnes.

Charte de bon usage des ressources informatiques du laboratoire de recherche

Règles générales :

L'utilisateur est responsable de l'usage qu'il fait de l'équipement informatique mis à disposition par GSB. Il doit en réserver l'usage au cadre de ses travaux.

Un usage personnel des moyens de communication est non admis. L'accès aux postes informatiques de l'Institut est strictement réservé aux visiteurs.

Les utilisateurs sont responsables, en tout lieu, de l'usage qu'ils font du système d'information du laboratoire de recherche.

Ils sont tenus à une obligation de réserve et de confidentialité à l'égard des informations et documents auxquels ils accèdent. Les utilisateurs sont soumis au respect des obligations résultant de son statut ou de son contrat. L'utilisation des ressources informatiques implique le respect des droits de propriété intellectuelle de l'institution ainsi que ceux de ses partenaires et, plus généralement, de tous tiers titulaires de tels droits.

Chaque utilisateur se doit d'utiliser les logiciels dans les conditions des licences souscrites et de ne pas reproduire, copier, diffuser, modifier ou utiliser les logiciels, bases de données, pages web, textes, images, photographies, sons, vidéos ou autres créations protégées par le droit d'auteur ou un droit privatif, sans avoir obtenu préalablement l'autorisation des titulaires de ces droits.

- La loi n°78-17 du 6 janvier 1978 modifiée en 2004 relative à l'informatique, aux fichiers et aux libertés définit les conditions dans lesquelles des traitements de données à caractère personnel peuvent être effectués. Elle ouvre aux personnes concernées par les traitements un droit d'accès et de rectification des données enregistrées sur leur compte. Le laboratoire de recherche a désigné un correspondant à la protection des données à caractère personnel. Ce dernier a pour mission de veiller au respect des dispositions de la loi n°78-17 du 6 janvier 1978 modifiée et il doit être consulté préalablement à la mise en oeuvre de tout fichier ou traitement.
- Toute communication de nature professionnelle, à diffusion interne ou externe, devra être effectuée au moyen de l'adresse institutionnelle de l'établissement ou de l'un de ses partenaires.
- Toute information est réputée professionnelle à l'exclusion des données désignées par l'utilisateur comme relevant de sa vie privée : dans ce cas, il lui appartient de procéder au stockage de ces données à caractère privé dans des répertoires explicitement prévus à cet effet et clairement identifiés comme privés. La protection et la sauvegarde de ces données sont de sa responsabilité. L'établissement ne peut être engagé à conserver cet espace

- L'utilisateur est responsable de son adresse électronique nominative délivrée par le laboratoire de recherche; tout message est réputé professionnel sauf s'il comporte une mention particulière et explicite indiquant son caractère privé ou s'il est stocké dans un espace privé de données. Sont interdits les messages comportant des contenus à caractère illicite quelle qu'en soit la nature. Il s'agit notamment des contenus contraires aux dispositions de la loi sur la liberté d'expression ou portant atteinte à la vie privée d'autrui.
- L'utilisateur doit s’assurer de l’identité et de l’exactitude des adresses des destinataires des messages. Il doit veiller à ce que la diffusion des messages soit limitée aux seuls destinataires concernés afin d’éviter les diffusions de messages en masse, l'encombrement inutile de la messagerie ainsi qu'une dégradation du service.
- Les communications syndicales, quel qu’en soit le canal de diffusion, doivent respecter les dispositions législatives et réglementaires en vigueur, en particulier celles du décret n°
  82- 447 du 28 mai 1982 relatif à l’exercice du droit syndical dans la fonction publique modifié.
- Responsabilités des parties
  Chaque utilisateur accède et utilise les moyens informatiques et le réseau auquel il a accès sous sa propre responsabilité. Il reconnaît que toute violation des dispositions de la présente charte, ainsi que, plus généralement, tout dommage créé à l'établissement ou à des tiers de son fait engagera sa responsabilité, tant sur le plan disciplinaire, que civil ou pénal. GSB déclare mettre en oeuvre - par le biais de la présente charte et des diverses mesures de sécurité physique et logique qui sont les siennes - tous les efforts nécessaires à un bon usage de ses systèmes et du réseau et n'assumer aucune responsabilité au titre des agissements fautifs ou délictueux des utilisateurs auxquels elle fournit un droit d'accès.

Descriptif de contenu pour un module d'initiation à la sécurité informatique

Module 1 : notions de base

1. Les enjeux de la sécurité des S.I.
2. Les besoins de sécurité
3. Notions de vulnérabilité, menace, attaque
4. Panorama de quelques menaces
5. Le droit des T.I.C. et l'organisation de la sécurité en France

Pour sensibiliser les visiteurs médicaux de l'entreprise GSB et les inciter à rester vigilants vis à vis de la sécurité informatique, il sera important d'insister sur des mesures concrètes afin de se protéger de potentiels dangers, en insistant sur les menaces auxquelles ils seront confrontés au quotidien.

4. Panorama de quelques menaces

a) Les sources potentielles de menaces

b) Panorama de quelques menaces

c) Hameçonnage & ingénierie sociale

d) Déroulement d'une attaque avancée

e) Violation d'accès non-autorisé

f) Fraude interne

g) Virus informatique

h) Déni de service Distribué (DdoS)

i) Illustration d'un réseau de botnets