

Dossier

- Sommaire :
- 1) Partie Hardware
- 2) Partie Software
- 3) Partie Authentification
- 4) Choix de l'OS (Windows 10 / Windows 11)

Partie Hardware

Introduction :

Dans cette première partie nous allons vous présenter les deux machines (c'est-à-dire les postes de travail nomades) que nous avons retenu pour équiper chacun des employés afin de leur permettre d'exercer leurs missions professionnelles en télétravail.

Pour commencer, nous vous recommandons :

Le Laptop (pc portable) Dell Inspiron 15 3000

Partie Hardware

Dell Inspiron



15 3000

Caractéristiques Techniques :

Processeur Intel® Core™ i5-1135G7 de 11e génération (8 Mo de mémoire cache, jusqu'à 4,2 GHz)

Carte graphique Intel® Iris® Xe avec mémoire graphique partagée

8 Go de mémoire DDR4 à 2 666 MHz

Disque SSD M.2 PCIe NVMe de 256 Go

Partie Hardware

C'est un PC Portable adapté à une utilisation professionnelle avec un pavé numérique pour le confort des employés et un clavier en AZERTY. Il est livré de base avec Windows 10 édition Famille mais vous pouvez par la suite le passer en version Professionnel ou Entreprise lors de l'installation du master (image de l'OS).



Partie Hardware n°2

En deuxième choix nous vous proposons la virtualisation de machine :



La virtualisation de machines consiste à virtualiser un bureau informatique et permet d'émuler un environnement de travail, et ce depuis n'importe où du moment où vous possédez un ordinateur chez soi ou au bureau.

Partie Hardware n°3

Pour le travail physique en entreprise nous vous conseillons une station d'accueil qui sera compatible avec l'ordinateur portable précédent, c'est un dispositif qui permet de connecter tout les périphériques externes afin de ne pas perdre de temps a connecter / déconnecter sans cesse tous les supports sur le PC quand vous arrivez au travail.

C'est un gain de temps et une optimisation drastique pour travailler rapidement. Il suffit de brancher son PC à la station et tout est prêt (c'est du plug and Play).

Nous vous conseillons la Station d'accueil DELL USB 3.0 D3100

Partie Hardware n°3

Station d'accueil Dell USB 3.0 (D3100)



La station d'accueil Dell USB 3.0 connecte votre ordinateur portable à trois écrans supplémentaires, à divers périphériques externes et à Internet, via un câble unique. Elle fournit une charge USB aux périphériques, mais ne charge pas votre ordinateur.

Partie Hardware n°3

Nous avons optés pour le pack Clavier + Souris sans fil professionnel DELL KM5221W (AZERTY).



Quand les employés travailleront dans l'entreprise, ils auront besoin de deux écrans pour permettre de démultiplier les tâches, d'afficher plusieurs fenêtres de travail en même temps, cela leur fera gagner du temps et optimisera leur travail.

Nous vous recommandons également les moniteurs DELL 24 FHD SE2422HX

Partie Hardware n°3

DELL 24 FHD



SE2422HX

L'affichage de cet écran à bordures fines Full HD de 23,8" équipé de la technologie AMD FreeSync, d'un temps de réponse rapide et d'un taux d'actualisation de 75 Hz, idéal pour de la bureautique.

Partie Hardware (Serveurs et Switchs)

Afin de centraliser et stocker les données de l'entreprise, il vous faudra deux serveurs. Un pour l'usage quotidien, l'autre pour faire de la redondance, c'est-à-dire pour sauvegarder les données et prendre le relais du premier serveur si celui-ci tombe pour des raisons diverses. Il faudra également une licence serveur pour faire tourner ces serveurs.

Nous vous recommandons :

Un serveur avec la licence Windows server 2022

Même principe pour les Switchs.

Pour les câbles RJ45 qui serviront à connecter votre infrastructure, nous vous recommandons de prendre plusieurs sets de couleurs différentes afin de bien distinguer dans la baie informatique les types de connexions.

Partie Hardware (Serveurs et Switchs)

Nous vous recommandons ces références :

Serveur : Hewlett Packard Enterprise ProLiant DL380 Gen10 serveur 72 To 2,3 GHz 32 Go Rack (2 U) Intel® Xeon® Gold 800 W DDR4-SDRAM

Switch Entièrement Manageable Ethernet Plus L3, 48 Ports 10GBASE-T, 4 Uplinks QSFP+ 40Gb, S5850-48T4Q



Partie Software

Les Licences :

Pour les licences, il va vous falloir :

- 2 Des licences de bureautiques
- 2 Des licences de serveur
- 2 Une licence pour un VPN
- 2 Une licence pour un antivirus
- 2 Des licences professionnelles liés à votre travail d'assureur



Windows
Server
2022



TREND
MICRO™

SECURITY

The Ultimate Defense in a Connected World

Pour la bureautique, nous vous conseillons la licence Microsoft Office. Il faudra choisir le nombre total de licence suivant les besoins réels de vos employés. Par défaut nous vous conseillons d'en prendre une pour chaque collaborateur, soit 90 licences.

Pour vos serveurs, nous vous conseillons de prendre deux licences Windows Server 2022.

Pour le VPN, nous vous conseillons Stormshield VPN SSL. C'est un VPN sûr, professionnel, efficace et adapté à une grande entreprise.

Pour l'antivirus, nous vous conseillons Trend Micro Security Agent. Là encore c'est un antivirus adapté aux entreprises, capable de résister à tout les types de virus connus.

Pour les licences liés au travail d'assureur, nous vous conseillons Cleva. C'est un logiciel fournis par la société Inetum, qui est un fournisseur de solutions logicielles adaptées aux besoins des entreprises d'assurance, de mutuelles, les grands courtiers et les instituts de prévoyance.

Partie Authentification



Qu'est-ce que l'authentification en entreprise ?

MFA : C'est une méthode d'authentification qui exige de l'utilisateur qu'il fournisse plusieurs facteurs de vérification (au moins deux) pour accéder à une ressource (une application, un compte en ligne ou un VPN, par exemple). La MFA est un composant essentiel pour garantir une stricte politique de gestion des identités et des accès (IAM). La MFA ne se contente pas de demander un nom d'utilisateur et un mot de passe. Elle exige un ou plusieurs facteurs de vérification supplémentaires, ce qui diminue les chances de réussite d'une cyberattaque.

Comment ça marche ?

Schéma :

Etape 1 : Saisie du nom d'utilisateur et du mot de passe

Etape 2 : Saisie du code PIN qui apparaît sur l'application mobile.

Etape 3 : Vérification de l'empreinte digitale.



De manière générale, c'est une méthode d'authentification qui utilise le facteur de la connaissance, de la biométrie et de la possession et qui est donc sécurisée au maximum contre les problèmes de cybersécurité.

2FA : C'est une méthode d'authentification forte qui utilise deux preuves d'identification à un mécanisme d'identification.

Nous avons choisi le système **2FA RSA TOKEN** pour la 1 ère configuration qui est plus simple à mettre en place que du MFA. Le MFA demanderait une lourde procédure administrative et juridique à l'entreprise et serait probablement plus compliquée à mettre en place dans l'optique du télétravail et du nomadisme des employés.

Pour la 2^{ème} configuration, celle avec la virtualisation de machines, nous vous conseillons **l'authentification par MFA**, avec également l'implémentation de facteur d'authentification et de connexion forts.

Choix de l'OS (Windows 10 ou Windows 11 ?)

Windows 11 possède toutes les dernières mises à jour de sécurité et permet de mieux protéger l'entreprise face aux risques liés à la cybersécurité. Windows 11 est plus beau, plus fluide, plus ergonomique que Windows 10.

Vous n'aurez pas à l'acheter, il est plus préférable de directement faire la mise à jour vers Windows 11 une fois votre flotte de laptops en place.

Windows 10 sera quand même maintenu à jour jusqu'en 2025, ce qui laisse le temps à votre entreprise de choisir si jamais vous avez des doutes sur le déploiement de Windows 11. Dans le cas où Windows 11 vous décevrait pour diverses raisons, sachez qu'il est tout à fait possible de repasser à Windows 10 depuis Windows 11, et de manière légale.



FIN DE LA PRESENTATION

C'EST

LA FIN

Merci!