# MISE EN PLACE DU TELETRAVAIL

23 FEVRIER 2021

**Créé par : Bryan CHELVANAIGUM, Lyssandre BARRILLET et Antony ONGANI**

ASSURMER

# SOMMAIRE

# Introduction

## Contexte

Suite à la situation sanitaire actuelle, la COVID-19 a impacté notre quotidien, que ce soit dans notre sphère privée mais aussi d'un point de vue professionnel. Pour faire face à cette pandémie, il apparait nécessaire de protéger ses collaborateurs tout en maintenant l'activité de l'entreprise. C'est ainsi que la meilleure solution, permettant d'allier survie de l'entreprise et sécurité de collaborateurs s'est massivement développée : le télétravail (activité professionnelle effectuée en tout ou partie à distance du lieu où le résultat du travail est attendu).

Nous avons pris en compte les caractéristiques spécifiques de votre entreprise. Votre PME spécialisée dans le secteur des assurances, comptant 111 collaborateurs répartis sur 15 agences ainsi qu'un siège social, a été minutieusement analysée dans le but de vous offrir une offre personnalisée adaptée à vos besoins. L'objectif étant de maintenir la crédibilité et la confiance que vous avez développées auprès des particuliers et des professionnels faisant notamment d'ASSURMER le 1er assureur des professionnels du sport nautique en France.

Nous allons donc vous présenter nos solutions pour mettre en place le télétravail le plus optimal possible en adéquation avec les besoins de votre entreprise tout en répondant à plusieurs problématiques qu'imposent le travail à distance.

Dans un premier temps, nous nous concentrerons sur la gestion des actifs (matériels, applicatifs et sécurité), puis nous vous présenterons les outils et le processus de déploiement des postes de travail, pour enfin, vous expliquer la mise en place de l'assistance et du support aux utilisateurs. Une procédure de prise en main de cette assistance et du support utilisateurs vous sera fournie en annexe de ce dossier.

# La gestion des actifs liés au télétravail

## Les postes informatiques

### Les postes informatiques pour les collaborateurs du siège social

Pour les collaborateurs au sein du siège social (dont le DSI et les équipes IT font partis), notre choix s'est porté vers l'ordinateur portable Dell Inspiron 15 3501. Nous préconisons l'achat de 22 postes (10% de marge d'appareils supplémentaires selon l'effectif actuel de 20 collaborateurs au siège social). Il s'agit d'une machine dont les caractéristiques principales sont :

- Ecran LED antireflet Full HD de 15,6 pouces (pour un confort visuel optimisé)
- Processeur Intel Core i5-1135G7 (modèle de 11ème génération, fréquence de 2,40 GHz jusqu'à 4,20 GHz, 4 cœurs, 8 threads, 8 Mo de mémoire cache)
- Carte graphique Intel Iris Xe
- Mémoire de 8 Go de RAM (1 x 8 Go DDR4 à 2666MHz)
- 256 Go de stockage SSD (M.2 PCIe NVMe)
- Lecteur d'empreintes digitales
- Un port USB-C 3.2 Gen 1 (débit jusqu'à 5 Gb/s)
- Deux ports USB-A 3.2 Gen 1 (débit jusqu'à 5 Gb/s)
- Port HDMI 1.4
- Port RJ45
- Prise jack audio 3,5 mm
- Bluetooth
- WIFI 802.11ac 1x1
- Poids : 1,83 kg.

## Les postes informatiques pour les collaborateurs en agence


Pour les collaborateurs en agences, nous privilégions l'ordinateur portable Dell Inspiron 15 3505. Nous préconisons l'achat de 100 postes (+10% de marge d'appareils selon l'effectif actuel de 91 collaborateurs en agences). Nous avons ici affaire à une machine dont les caractéristiques principales sont :

- Ecran LED antireflet Full HD de 15,6 pouces (pour un confort visuel optimisé)
- Processeur AMD Ryzen 3 3250U (fréquence de 2,6 GHz jusqu'à 3,5 GHz, 2 cœurs, 4 threads, 4 Mo de mémoire cache)
- Carte graphique AMD Radeon
- Mémoire de 8 Go de RAM (2 x 4 Go DDR4 à 2400 MHz)
- 256 Go de stockage SSD (M.2 PCIe NVMe)
- Un port USB-A 2.0
- Deux ports USB-A 3.2 Gen 1 (débit jusqu'à 5 Gb/s)
- Port HDMI1.4
- Port RJ45
- Prise jack audio 3,5 mm
- Bluetooth
- WIFI 802.11ac 1x1
- Poids : 1,83 kg.

# Accessoires

Souris

Pour un confort optimal de navigation, nous avons choisis la souris optique sans-fil Dell WM126. Elle possède 3 boutons, une molette de défilement et possède une résolution de 1000 dpi pour un poids de 57,6 g. Un récepteur USB devra être branché à l'ordinateur.

Sacoche de transport

Pour faciliter le nomadisme des collaborateurs d'ASSURMER, notre choix s'est orienté vers la sacoche Activ' Bag 15,6" de chez Urban Factory. Légère et ergonomique grâce à ses poches situées à l'avant et à l'arrière de la sacoche, celle-ci vous permettra de d'emporter avec vous, l'ordinateur accompagné de son chargeur et de la souris présentée précédemment ainsi que vos documents papiers.

# Les licences

## Le système d'exploitation : Windows 10 Professionnel

Les 122 postes de travail seront équipés nativement du système d'exploitation Windows 10 Professionnel. Cette version de Windows a pour principales fonctionnalités supplémentaires :

- Windows Hello Entreprise (authentification biométrique grâce au lecteur d'empreintes digitales pour les postes des collaborateurs du siège social)
- La compatibilité avec la Protection des données Microsoft
- Le chiffrement du contenu des disques durs par le biais de BitLocker et BitLocker To Go
- La possibilité de déployer les dernières mises à jour de produit Microsoft grâce à Windows Server Update Services (WSUS)
- Windows Update pour Entreprise
- Le programme Windows Insider pour Entreprises (permet d'explorer de nouvelles fonctionnalités, de déployer Windows plus rapidement et d'avoir un aperçu de Windows Server)
- Le navigateur web Microsoft Edge
- Le tableau blanc collaboratif Windows (zone de dessin numérique libre où regrouper les personnes, les idées et le contenu)
- La possibilité d'intégrer la machine à un réseau professionnel
- La gestion de stratégies de groupes en matière de déploiement.

## Les logiciels de bureautique : Microsoft Office 365

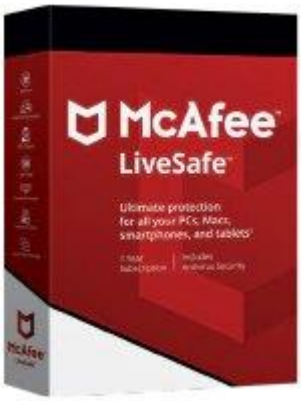
Les outils de productivité que nous vous préconisons sont inclus dans l'abonnement à la suite Microsoft Office 365. D'après les besoins de votre entreprise, la formule Microsoft 365 Business Standard nous paraît être la solution la plus adaptée. Il s'agit d'un abonnement annuel (126€ par appareil) permettant l'accès aux logiciels Microsoft :

- Word (logiciel de traitement de texte)
- Excel (logiciel tableur)
- PowerPoint (logiciel de présentation)
- Outlook (gestionnaire d'informations personnelles et client de courrier électronique)
- Access (base de données relationnelle)
- Publisher (logiciel de publication assistée par ordinateur)

- SharePoint (série de logiciels pour applications Web et portails)
- OneDrive (espace de stockage en ligne sécurisé et partagé par les utilisateurs d'une entreprise)
- Yammer (outil de micro blogage proposant la mise en place gratuite d'un réseau social interne)
- Teams (application de communication collaborative propriétaire)
- Exchange (solution de courrier et de calendrier de classe Entreprise)

Un domaine personnalisé gratuit pendant 1 an est inclus avec cette suite bureautique.
De plus, 1 To de stockage cloud et les versions en ligne de Microsoft Office sont également inclus.
Les 122 postes que nous vous livrerons auront une licence d'un an à Microsoft 365 Business Standard.

## Le logiciel antivirus : McAfee LiveSafe




Un abonnement de 12 mois au logiciel antivirus McAfee LiveSafe.
« Le logiciel McAfee LiveSafe vous protège, vous ainsi que vos données, votre identité et tous vos appareils. Quoi que vous fassiez, où que vous alliez, McAfee LiveSafe vous permet de rester en ligne en toute confiance. »
Les principales fonctionnalités de ce logiciel sont :

- La protection de votre poste informatique
- Un gestionnaire de mots de passe (crée des mots de passes forts et uniques, les enregistre et les mémorise)
- Une console web simple d'utilisation vous permettant de suivre la protection de votre appareil en temps réel
- La protection du réseau domestique de vos collaborateurs nomades. Vos appareils seront sécurisés contre tout accès non autorisé. Vous pourrez ainsi naviguer en toute sécurité et protéger vos informations personnelles
- 1 Go de stockage personnel par appareil

# La gestion des techniques d'authentification et de sécurité

Lorsqu'un utilisateur veut accéder à un système d'information il doit dans un premier temps effectuer une procédure d'identification et d'authentification. Nous allons ainsi, brièvement vous rappeler les spécificités de l'identification et de l'authentification, puis vous familiariser avec les notions de 2FA et MFA pour finalement vous présenter notre choix.

## L'identification

L'identification est une phase qui consiste à établir l'identité de l'utilisateur. Elle permet de répondre à la question : « Qui êtes-vous ? ». L'utilisateur utilise un identifiant (que l'on nomme « compte d'accès », « nom d'utilisateur » ou encore « login » en anglais) qui l'identifie et qui lui est attribué individuellement. Cet identifiant est unique.

## L'authentification

L'authentification est une phase qui permet à l'utilisateur d'apporter la preuve de son identité. Elle intervient après la phase dite d'identification. Elle permet de répondre à la question : "Êtes-vous réellement cette personne ?". L'utilisateur utilise un « authentifiant » ou « code secret » que lui seul connait. Le code secret d'un utilisateur est une information personnelle qui ne doit en aucun cas être divulguée. Il est aussi communément appelé "mot de passe".

Les principaux risques liés au mot de passe sont sa divulgation et sa faiblesse. La divulgation d'un mot de passe est causée soit par négligence des règles ("prêt" de son identifiant et authentifiant à un collègue ou à sa hiérarchie), soit par un acte de malveillance (craquage de mot de passe, cheval de Troie, hameçonnage, etc…). Dans les deux cas, la responsabilité de l'utilisateur, propriétaire de l'identité usurpée, peut se voir engagée.
La faiblesse d'un mot de passe constitue une faille sérieuse. Les techniques utilisées pour "découvrir" les mots de passe (craquage, ingénierie sociale) sont toujours efficaces lorsque ces derniers sont trop simplistes ou lorsqu'ils se rapportent à des éléments de la vie privée ou publique de la personne (prénom d'un enfant, marque de sa voiture, etc.).

Or, cette sécurité permet de garantir la confidentialité : un des principes fondamentaux en termes de cybersécurité. Celle-ci permet de garantir la propriété selon laquelle l'information n'est pas diffusée, ni divulguée à des personnes, des entités ou des processus non autorisés.

Il existe trois techniques d'authentification de l'utilisateur :

- L'authentification dématérialisée (« ce que l'on sait ») : par exemple un mot de passe qui a pour avantage la simplicité de connexion de l'utilisateur au quotidien mais qui a pour faille d'être potentiellement divulguée par mégarde ou d'être intercepté par les nombreux actes de malveillances venues de n'importe où dans le monde.
- L'authentification matérialisée (« ce que l'on a ») : par exemple une carte à puce qui a pour avantage l'impossibilité pour une personnes non autorisée d'avoir accès au compte utilisateur d'un collaborateur possédant toujours activement sa carte à puce. Cependant, l'inconvénient pour le collaborateur sera d'être dans l'impossibilité de pouvoir accéder à son compte utilisateur en cas d'oubli de cet outil de sécurité.

- L'authentification biométrique (une caractéristique propre à la personne) : par exemple la reconnaissance faciale ou l'empreinte digitale qui a pour avantage d'être indissociable du collaborateur concerné mais qui a pour inconvénient la stricte nécessité de se mettre en conformité avec le RGPD (Règlement Général sur la Protection des Données).
  Dans le cas du système de contrôle d'accès aux ordinateurs portables professionnels avec biométrie par empreinte digitale, celle-ci n'a plus besoin d'être déclarée à la CNIL (Commission Nationale de l'Informatique et des Libertés) depuis le 25 mai 2018 (date d'entrée en application du RGPD).

## L'authentification double-facteur (2FA) et multi-facteur (MFA)

La vérification en deux étapes (double-facteur ou encore 2FA) contribue à votre protection en rendant plus difficile la connexion d'autres personnes à votre compte. Elle utilise deux formes d'identité différentes : votre mot de passe et une méthode de contact (ou informations de sécurité). Même si quelqu'un découvre votre mot de passe, il ne pourra pas aller plus loin s'il n'a pas accès à vos informations de sécurité. C'est également la raison pour laquelle il est important d'utiliser des mots de passe différents pour vos comptes.

Si vous activez la vérification en deux étapes, vous recevez un code de sécurité dans votre messagerie, sur votre téléphone ou dans votre application d'authentification à chaque fois que vous vous connectez à un périphérique qui n'est pas reconnu comme périphérique de confiance.

Quelques exemples d'authentification à double facteur :

- La génération d'une question secrète dont seul l'utilisateur connaît la réponse
- L'envoi d'un code unique par sms ou email
- L'envoi d'un code utilisable pendant une période limitée
- L'utilisation d'un code tournant avec validation sur un autre appareil (appairage sur smartphone ou via une calculette token)
- L'utilisation d'un logiciel ou d'une application d'authentification
  - Microsoft Authenticator (application sur smartphone)
  - Windows Hello Entreprise
- Le recours à la reconnaissance faciale, détection de l'iris ou par empreinte digitale
- L'utilisation d'une clé cryptographique :
  - Symétrique
    La même clé sert à chiffrer et à déchiffrer
  - Asymétrique
    On utilise deux clés différentes, la clé de chiffrement est publique alors que celle servant au déchiffrement est gardée secrète (la clé secrète, ou clé privée, ne peut pas se déduire de la clé publique)

L'authentification multi-facteur (aussi appelée MFA) consiste en l'utilisation de plusieurs formes de vérification pour démontrer l'identité de l'utilisateur lors de la connexion à une application ou un logiciel. Cette authentification utilise les mêmes méthodes d'authentification que l'authentification à double-facteur mais utilise plus de deux facteurs.

Par exemple, l'utilisation du mot de passe du compte utilisateur, Windows Hello Entreprise ainsi que Microsoft Authenticator. Ou encore, l'utilisation du mot de passe du compte

utilisateur, l'application mobile Gmail ainsi que l'authentification biométrique du smartphone de l'utilisateur.

## Notre préconisation : Microsoft Authenticator

Afin de sécuriser au mieux l'authentification de vos collaborateurs, nous vous préconisons l'authentification multi-facteur par le biais de l'application mobile Authenticator (disponible sur Android et iOS). Celle-ci approuve la connexion de l'utilisateur à partir de l'application mobile grâce à une notification push (instantanée). Tout d'abord, vous devez vous authentifier avec votre identifiant et votre mot de passe traditionnel, ensuite l'application Authenticator enverra sur le smartphone de l'utilisateur une demande d'approbation d'accès, l'utilisateur devra alors accepter cet accès. Afin de valider la connexion, l'application mobile utilisera alors la méthode de déverrouillage biométrique utilisée sur le smartphone de l'utilisateur (reconnaissance faciale, empreinte digitale, etc…). Nous avons ainsi, une authentification à 3 facteurs (mot de passe, application Authenticator et déverrouillage biométrique du smartphone).

Cependant, pour les utilisateurs ne disposant pas de déverrouillage biométrique sur leur smartphone, l'application Authenticator n'utilisera aucun outil d'authentification afin de valider la connexion. Il s'agira alors, simplement, d'une authentification à double facteur (mot de passe et application Authenticator). Dans les deux cas, il est important d'activer dans les paramètres de l'application, le « verrou d'application » qui exigera une authentification biométrique (si c'est possible) ou un code secret lors de l'ouverture de l'application et pour l'approbation de connexion. Il serait, dans le cas de l'utilisation d'un code secret, important de sensibiliser ces utilisateurs sur l'importance d'utiliser un outil de déverrouillage du smartphone (code secret, schéma de déverrouillage, etc…).

# Sécurisation du réseau d'entreprise grâce à un VPN

En informatique, un réseau privé virtuel ou réseau virtuel privé, plus communément abrégé en VPN (Virtual Private Network en anglais), est un système permettant de créer un lien direct entre des ordinateurs distants, qui isole leurs échanges du reste du flux de données se déroulant sur les réseaux de télécommunication.

Cette solution d'utilisation d'un réseau sécurisé permet de répondre aux trois principes fondamentaux en termes de cybersécurité, à savoir, la disponibilité (propriété d'accessibilité et d'utilisabilité à la demande par une entité autorisée), l'intégrité (propriété d'exactitude et de complétude, propriété assurant que des données n'ont pas été modifiées ou détruites de façon non autorisée) ainsi que la confidentialité (propriété selon laquelle l'information n'est pas diffusée ni divulguée à des personnes, des entités ou des processus non autorisés).

Il sera donc nécessaire de créer un réseau VPN sur lequel l'ensemble des collaborateurs de l'entreprise puisse se connecter pour ainsi avoir accès à la ferme de serveurs hébergée chez l'ESN ITCLOUD.

# Environnement de travail

Le télétravail requiert quelques prérequis que nous recommandons pour permettre d'optimiser le bien-être des collaborateurs :

- S'installer dans un environnement :
  - Calme (permettant de se concentrer ou de téléphoner sans être dérangé)
  - Illuminé (si possible par la lumière du jour)
  - Adapté (un bureau suffisamment spacieux, un fauteuil de bureau confortable)
- Instaurer des temps de pause (l'isolement qu'induit le télétravail peut, chez certaines personnes, leurs faire perdre la notion du temps, il est alors important de profiter de ce temps de pause pour s'aérer l'esprit, marcher, discuter avec leur entourage, etc…)
- Maintenir un lien social entre collègues
- Organiser des réunions hebdomadaires pour suivre l'état moral des collaborateurs mais aussi l'avancement de la productivité (par le biais de l'application de communication collaborative Teams)
- De posséder une box internet : prérequis indispensable, des solutions alternatives existent pour les personnes mal desservies par les réseaux filaires (partage de connexion, box 4G, internet via satellite, etc…)

# Tableau récapitulatif des coûts

| Equipements ou licences | Tarif unitaire HT | Quantité | PRIX TOTAL HT |
|---|---|---|---|
| PC Portable siège social | 579,3 | 22 | 12744,6 |
| PC Portable agence | 479,3 | 100 | 47930 |
| Souris sans-fil | 14,32 | 122 | 1747,04 |
| Sacoche | 15,92 | 122 | 1942,24 |
| Système d'exploitation | 0 | 122 | 0 |
| Logiciel antivirus (1 an) | 0 | 122 | 0 |
| Logiciels Microsoft Office (1 an) | 126 | 122 | 15372 |
| | | | |
| **Tarif total Hors-Taxes (en euros)** | | | **79735,88** |

# Déploiement des postes de travail

## Windows Deployment Service

Windows Deployment service permet de déployer un poste client via le réseau, et de lui envoyer un système d'exploitation personnalisé, ainsi que diverses applications. Particulièrement utile dans le cas du télétravail ou d'un déploiement massif de poste, il va permettre une administration centralisée de la gestion des OS et application nécessaire à une entreprise.

### Le choix de WDS

WDS présente divers avantages :

- Diminution de la complexité, du temps nécessaire ainsi que des coûts engendrés par rapport à des installations manuelles postes par postes.
- Il permettra de créer une image à partir d'un OS de référence que l'on pourra dupliquer.
- Il centralise les images et la gestion de celle-ci sur le même serveur.
- Nous pourrons déployer les postes via le réseau une fois celui-ci configuré.
- Cet outil sera « relativement » simple d'utilisation une fois configuré

### Installation et configuration du rôle

Windows Service Deployment regroupe un ensemble de composants :

Nous retrouverons :

## Des composants Serveur

Incluent un amorçage PXE, permettant à une machine d'aller chercher une image sur un serveur de fichier prévu à cet effet.

Un serveur DHCP permettant de fournir un adresse IP à chaque machine se connectant sur le réseau.

Un serveur de fichier permettant de stocker les images voulus.

Un serveur DNS permettant d'appartenir à un domaine.

Un protocole FTPT permettant le transfert de l'image.

## Des composants Client

Demandant l'exécution du service WDS à travers une requête lors du démarrage du poste, permettant de booter une image préalablement installée sur notre serveur.

## Des composants de gestion

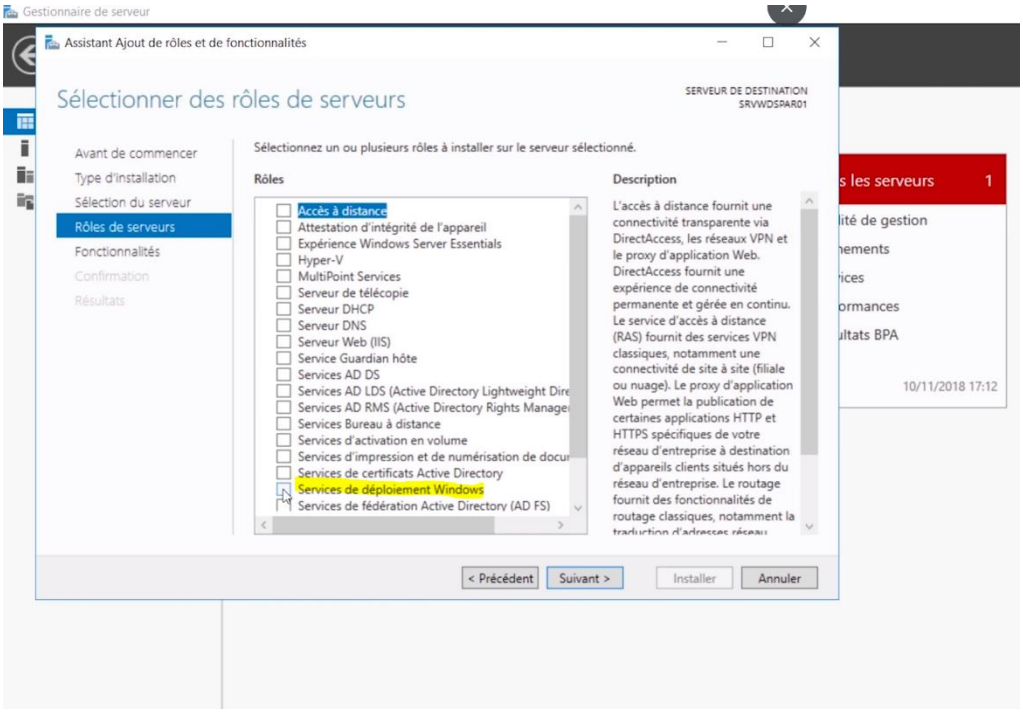
Regroupant l'ensemble des outils permettant l'administration du serveur, des images, des applications.

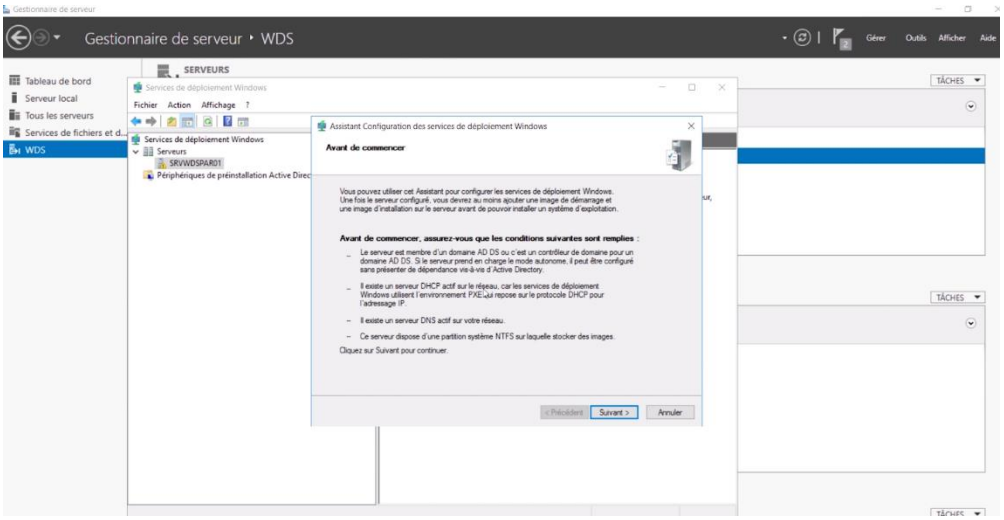
## Prérequis :

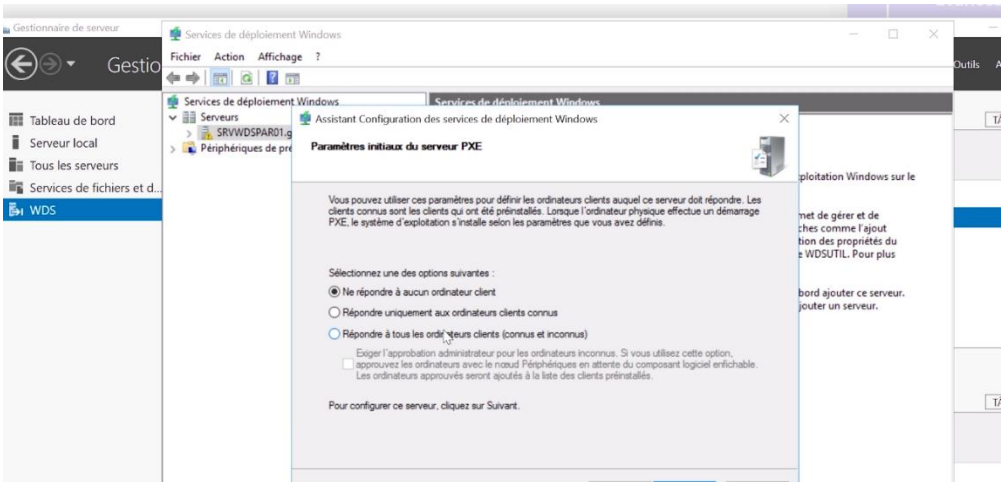
Afin de configurer Windows Deployment Service sur notre réseau, nous devons disposer de plusieurs prérequis :

- Nous devons disposer d'un Active Directory.
- Un serveur DHCP doit être configuré pour que les clients s'identifient au réseau et obtiennent une adresse IP afin que le client puisse recevoir l'image Windows dès son démarrage car nous allons utiliser l'environnement PXE.
- Un DNS doit exister sur le réseau.
- Une partition NTFS doit être disponible pour stocker les images.
- Configurer l'identification : pour installer le rôle WDS, nous devrons être administrateur sur le serveur

Nous allons mettre en place le rôle « Service de Déploiement Windows » via le gestionnaire de serveur Windows Server 2019

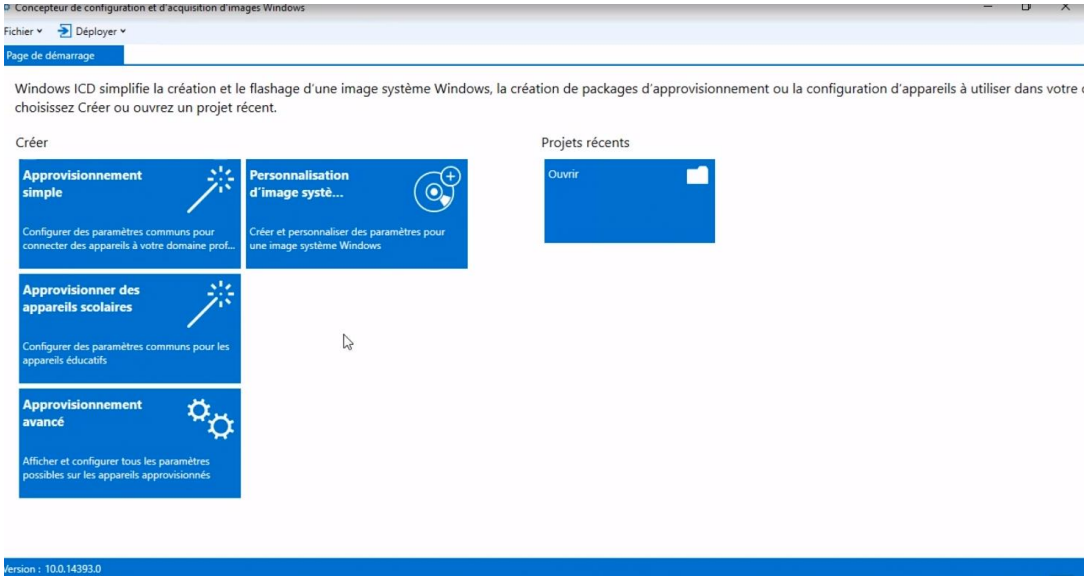


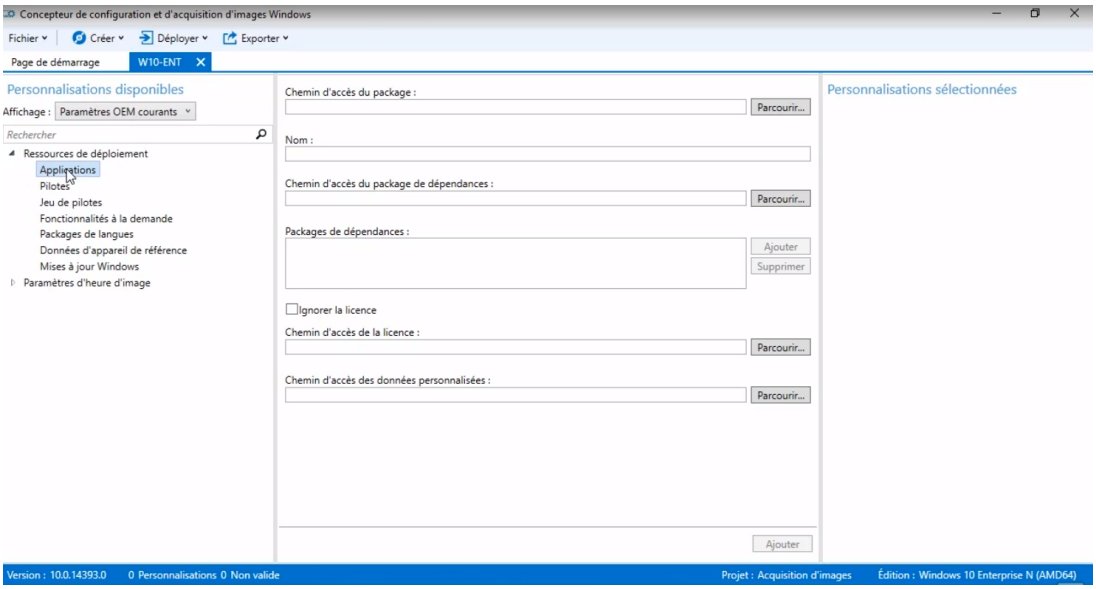



# Windows ADK

Nous allons utiliser Windows ADK afin de mettre en place notre image sur notre poste de référence. Une fois installé, nous pourront configurer notre image grâce au « concepteur de configuration et d'acquisition d'image Windows » en personnalisant notre image.




Nous allons ensuite configurer notre image en y ajoutant des applications. Puis nous allons générer l'image au format de fichier image Windows (WIM).




## L'ajout de différentes images nécessaires au déploiement d'un poste

Il existe différents types d'image, les images mince, hybride, et volumique.

### Image mince

- Image ne contenant que le système d'exploitation.
- Image capturée ou utilisation de l'ISO.
- Nécessite peu de maintenance (pas de problème d'application, de pilote car l'image ne contient rien).
- Les applications vont devoir être déployées par un autre biais : (GPO, script, etc…).

### Image hybride

- Image contenant système d'exploitation, pilotes et applications communes.
- Image capturée.
- Maintenance nécessaire lors de la mise à jour d'une application.

### Image volumique

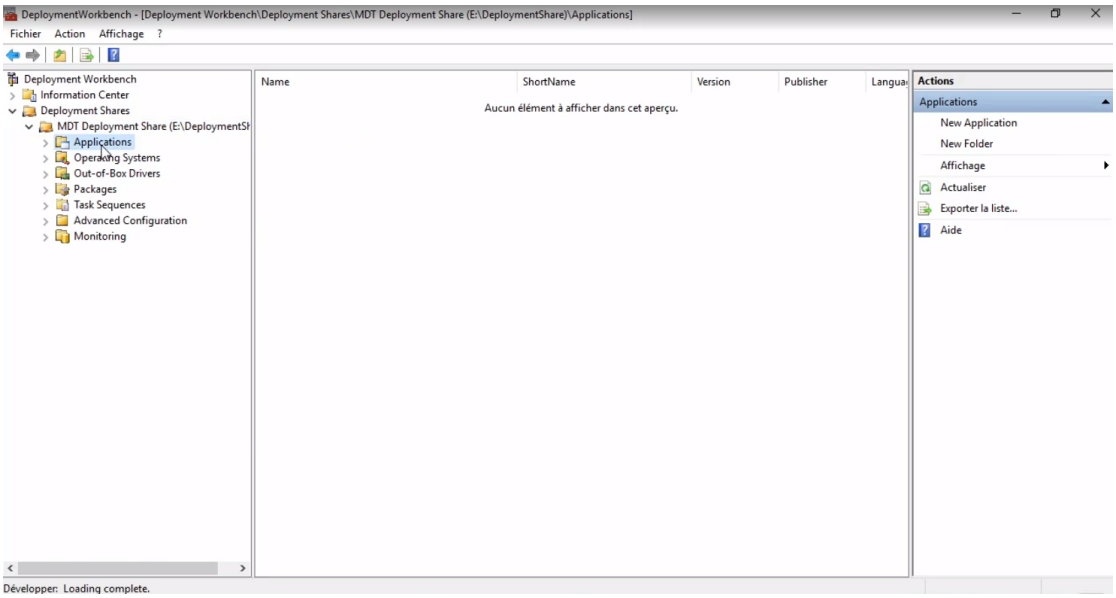
- Image contenant système d'exploitation et applications.
- Image capturée.
- Maintenance assez lourde, une image par poste.

Dans notre cas nous voulons que nos ordinateurs contiennent tous le même OS ainsi que les mêmes applications, nous allons utiliser une image hybride.

# Microsoft Deployment Toolkit (MDT)

Ce service de Windows permet de générer plusieurs scénarios d'installation comme de la migration, ou le déploiement d'un parc informatique conséquent. C'est une solution téléchargeable gratuitement qui nous permettra d'installer des applications lors de notre déploiement Windows.

Le but de MDT est de pousser nos images à travers le réseau pour ne pas avoir à les installer manuellement.
Le client va démarrer via un boot PXE, sur le réseau, la machine va récupérer via le serveur DHCP configuré précédemment, une adresse IP. Cela va permettre de déterminer le serveur WDS ainsi que le fichier de démarrage « bootstrap » qui va permettre de nous indiquer où se trouve le serveur MDT.
Enfin, grâce au protocole TFTP le fichier bootstrap va être « poussé », permettant le déploiement des applications.
Nous allons alors créer un nouvel environnement dans l'outils MDT Deployment Workbench.



# Autre outil de déploiement

## Présentation de CloneZilla


CloneZillaLive est un programme libre, basé sur Linux aidant au déploiement, à la sauvegarde. Il permet de faire des images de disques de plusieurs systèmes. L'inconvénient est qu'il est nécessaire de déployer chaque poste à la main avec une clé bootable composé d'une image. Il nécessite ainsi une mise en place longue et couteuse, ne le rendant pas adéquat dans un contexte d'entreprise.
Il existe une version Server Edition permettant de gérer tout un réseau pour une restauration plus simple et rapide.