Proposition infrastructure



Partie Active Directory & messagerie

Une image contenant texte

Description générée automatiquement

Table des matières

[Introduction 2](#_Toc107065961)

[Active Directory : 3](#_Toc107065962)

[Introduction 3](#_Toc107065963)

[Présentation détaillée de la solution 3](#_Toc107065964)

[Azure AD 3](#_Toc107065965)

[DNS 17](#_Toc107065966)

[DHCP 19](#_Toc107065967)

[Messagerie : 21](#_Toc107065968)

[Introduction 21](#_Toc107065969)

[Présentation détaillée de la solution 21](#_Toc107065970)

[Attribution de licence 21](#_Toc107065971)

[Migration vers Microsoft 365 23](#_Toc107065972)

[Backup Microsoft 365 25](#_Toc107065973)

[Téléphonie Teams 32](#_Toc107065974)

[Tarification Microsoft 365 34](#_Toc107065975)

[Tarification totale 34](#_Toc107065976)

[Schéma Global 35](#_Toc107065977)

[Planning 35](#_Toc107065978)

# Introduction

La partie Active Directory & Messagerie de la nouvelle infrastructure de la société MALO se découpe de la manière suivante :

* Active Directory : Elles constituent les fonctions essentielles pour gérer les utilisateurs et les ordinateurs et pour permettre aux administrateurs système d’organiser les données en hiérarchies logiques.
* Messagerie : C’est un logiciel dont le but est de recevoir, classer et d'envoyer des courriers électroniques.

C’est deux parties sont obligatoires au sein d’une infrascture d’entreprise.

Le but à travers cette rédaction est d’expliquer comment remettre à niveau l’existant et prévoir l’évolution futur de l’entreprise.

# Active Directory :

## Introduction

Pour gérer l’Active Directory, nous avons fait le choix de passer par Azure AD pour des raisons d’homogénéités, de disponibilités et de performances.

La convention de nommage se fera ainsi :

* Serveur : SRV-<nom du serveur ou utilité>
* PC : PAR-TC001 | BRU-LP001

## Présentation détaillée de la solution

Actuellement, l’entreprise Malo possède un service AD, DNS ainsi que DHCP sur une machine de type Windows Server hébergé sur hyperviseur « On Premise ».

Le principe de cette présentation détaillée va être de vous montrer comment migrer l’entièreté de ces services sur le Cloud Azure et développer quelques points intéressants.

### Azure AD

#### Introduction

Azure Active Directory (Azure AD) est un service de gestion des identités et des accès basés sur le cloud. Ce service permet aux collaborateurs d’accéder à des ressources externes telles que Microsoft 365, le portail Azure et des milliers d’autres applications SaaS. Azure Active Directory aide également à accéder aux ressources internes, notamment les applications situées sur votre réseau intranet d’entreprise et les applications cloud développées pour votre organisation.

#### Création d’un tenant sous Azure

Tout d’abord, il faut posséder un compte Azure, si vous n’en possédez pas, rendez-vous sur « <https://azure.microsoft.com/free/> ».

Après être connecté au portail Azure, vous pouvez créer un nouveau tenant qui représentera votre organisation, pour cela, rendez-vous dans « Gérer les locataires » depuis la vue d’ensemble d’Azure Active Directory, puis « Créer ».

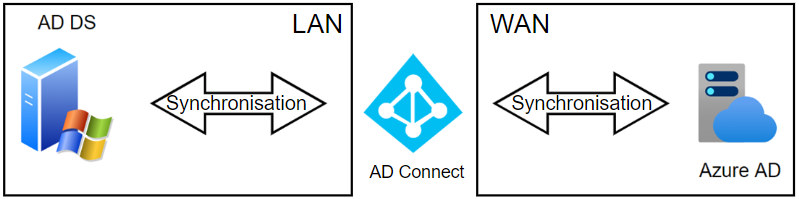
 Partie « Configuration » :

Et enfin, valider pour créer.

Pour des raisons de qualité, nous supprimons le répertoire par défaut.

#### Migration AD DS vers Azure AD

Une fois votre tenant Azure créer et configurer, nous allons migrer l’existant dans Azure AD, pour cela, nous aurons besoin des loggings administrateur de la machine hébergeant les services AD déjà existant.

 Il sera nécessaire d’installer « AD Connect » sur la machine maitre du domaine et effectuer ensuite la synchronisation pour que l’entièreté de l’AD soit répliquée sur Azure AD :

Pour commencer, nous allons installer l’AD Connect sur l’existant au sein de l’entreprise MALO, pour cela, télécharger [ici](https://www.microsoft.com/en-us/download/details.aspx?id=47594) Azure AD Connect et exécuter le sur la machine principale.

Je sélectionne ensuite « Personnaliser » et procède à son installation :

Une image contenant texte

Description générée automatiquement

Une fois l’installation effectuée, sélectionner en « Connexion utilisateur » « Synchronisation de hachage du mot de passe ».

Entrez les identifiants de l’admin général d’Azure AD. Sélectionner en « Type d’annuaire », « Active Directory » et prendre la foret voulu « malo.priv » dans notre cas et l’ajouter. Créer un utilisateur qui va permettre la synchronisation avec Azure, « malo.priv\azure.sync » dans notre cas et attribuer lui un mot de passe.

Une image contenant texte

Description générée automatiquement

Ensuite, sélectionner « userPrincipalName » et continuer **sans faire correspondre tous les suffixes UPN des domaines vérifiés**.

Sélectionner les domaines et unités d’organisation à synchroniser. Laisser par défaut les sections non abordés et valider avec « Suivant ».

Laisser suffisamment de temps pour qu’Azure AD et le domaine contrôleur échange les données et assurez-vous ensuite que les utilisateurs soient bien remontés dans la section « Utilisateurs » d’Azure AD :

Une image contenant texte

Description générée automatiquement

Après avoir vérifié que la copie des utilisateurs a bien été faites, nous allons pouvoir arrêter la synchronisation entre la machine qui héberge l’AD On Premise et Azure AD, pour cela, commencer par ouvrir un PowerShell sur la machine existante (ou a été installé Azure AD) en administrateur et faites les commandes suivantes :

PS C:\> Import-Module ADSync *Elle servira à importer le module « ADSync »*

PS C:\> Set-ADSyncScheduler -SyncCycleEnabled $false *Elle servira à arrêter le cycle de synchronisation côté AD DS.*

PS C:\> Connect-MsolService *Elle servira à vous connecter à votre Azure AD en admin*

PS C:\> Set-MsolDirSyncEnabled -EnableDirSync $false *Elle servira à arrêter le cycle de synchronisation côté Azure AD.*

Une fois les lignes de PowerShell exécutées, il nous restera qu’a supprimer depuis le panneau de configuration (Panneau de configuration\Programmes\Programmes et fonctionnalités) « Microsoft Azure AD Connect » ainsi que l’entièreté de c’est « supporting components ».

Pour des raisons de qualité, le dossier « Microsoft Azure AD Sync » depuis C:\Program Files a été supprimé ainsi que l’utilisateur créer pour la synchronisation depuis « C:\Users ».

#### Création d’utilisateur sous Azure AD

Pour la création d’utilisateur sous Azure AD, rendez-vous dans la section « Utilisateur » depuis votre « Azure Active Directory » présent sur la [page principal d’Azure](https://portal.azure.com/#home).

 Puis sélectionner « Nouvel utilisateur » :

#### Tarification

L’entièreté des licences nécessaire sont présente dans le pack « Microsoft 365 E3 » que nous évoquerons dans la partie « Messagerie ».

#### Domain Publique

Il est important de déclarer le domaine Azure pour des questions de certification, de redirection et pour éviter les usurpations.

Et y ajouter 3 entrés :

* La valeur TXT permettant de certifier que tu es le propriétaire du domaine
* La valeur MX pour rediriger les mails vers le tenant o365
* L'enregistrement SPF permettant d'éviter les usurpations

Il est nécessaire pour commencer d’ajouter un domaine depuis le panneau administrateur de Microsoft 365, pour le créer, rendez-vous [ici](https://admin.microsoft.com/Adminportal/Home?source=applauncher#/Domains/Wizard) et sélectionner « Ajouter un enregistrement TXT au enregistrements DNS du domaine ».

Pour la valeur TXT, les 3 données sont disponibles lors de la création du domaine sur Microsoft365.

Comme nous prenons le filtrage mail Microsoft, pour la valeur MX, elle est disponible après la création du domaine sous « Enregistrements DNS » :



Et la valeur SPF, qui est disponible à la création du domaine.

Ces trois données doivent être ajoutée depuis « Ajouter une entrée » :



##### Tarification

Le seul achat que nous faisons dans cette partie est le nom de domaine :



#### Création de GPO sous Intune (Endpoint)

Nous allons voir dans cette section comment effectuer la création de GPO sous Intune (Endpoint) qui visera à permettre la gestion des ordinateurs (utilisateurs)et des utilisateurs dans l’environnement Azure.

Il ne sera pas nécessaire d’introduire les serveurs dans la boucle car elles seront déjà gérées du fait que la machine soit hébergée sur Azure.

Une image contenant flèche

Description générée automatiquement

##### Création de groupe dynamique

Tout d’abord, nous avons besoin de créer deux groupes [ici](https://endpoint.microsoft.com/#blade/Microsoft_AAD_IAM/GroupsManagementMenuBlade/AllGroups), un groupe « GS\_Computers » qui sera dynamique (syntaxe règle : device.DeviceOSType -startsWith "Windows") pour les ordinateurs et l’autre pour les utilisateurs (syntaxe règle : (user.userType -eq "Member")).

Les servers sont gérés via un agent installé sur les machines et expliqués sur la partie d’Hadrien « Gouvernance ».

##### Création de profil de configuration

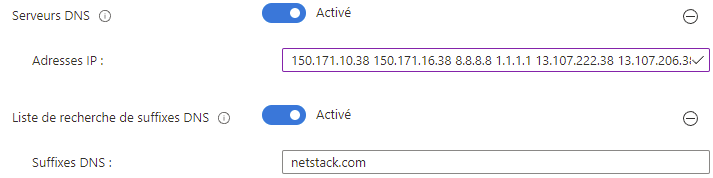
Une fois les groupes créer, nous allons pouvoir créer un **profil de configuration** qui sont les stratégies que nous allons poussez sur les machines, pour cela, rendez-vous dans « Appareil » puis « Profil de configuration » et enfin, « Créer un profil ».

 Nous allons commencer par sélectionner « Modèle » puis « Modèle d’administration », nous allons la nommer « Synchronisation OneDrive », sélectionner « OneDrive » et enfin « Connecter silencieusement les utilisateurs à l’application de synchronisation OneDrive avec leurs informations d’identification Windows », cela permettra de connecter automatiquement les utilisateurs à leur OneDrive :

Il ne reste plus qu’à l’affecter au groupe ordinateur créer précédemment et de valider la création.

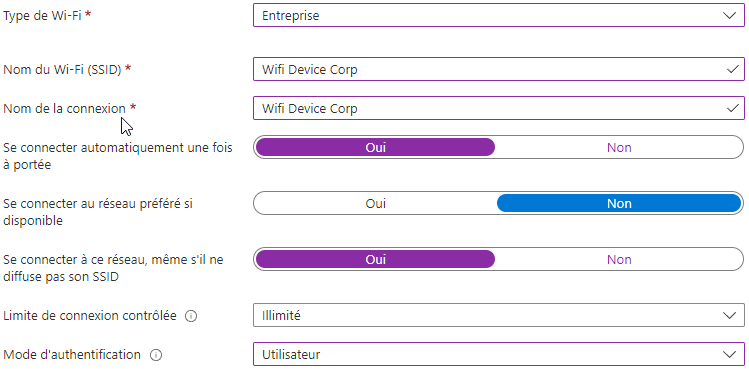
Nous allons de plus, personnaliser les configurations DNS des postes, pour cela, créer un deuxième profil et sélectionner « Catalogue des paramètres » en type de profil.

Choisissez un nom et ajouter des paramètres, rechercher « DNS » et sélectionner « Modèles d’administration\Réseau\Client DNS » puis, sur la colonne d’en bas, « DNS servers ». Activer et entrer les adresses IP des DNS Zone :



Attribuer votre stratégie au groupe d’ordinateur dynamique créer au paravent.

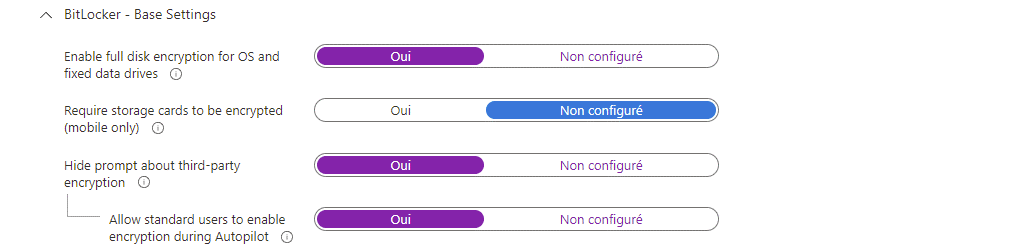
Nous allons par la même occasion créer un profil permettant la connexion automatique à un réseau WiFi. Pour cela, création d’un profil, Modèle puis « Wi-Fi » :



L’authentification se fera automatiquement grâce à l’utilisateur authentifier sur l’ordinateur.

Et attribuer au groupe d’ordinateur précédemment configuré.

##### Configuration des points de terminaison

 Nous allons ensuite créer depuis « Sécurité du point de terminaison », « Chiffrement de disque » une stratégie pour que Windows 10 force l’activation de BitLocker et nous monte la clef dans la section « Chiffre disque » sous « Appareil Windows » :

Plus qu’à l’affecter sur le groupe ordinateur créer au départ.

##### Installation d’application

###### .MSI

Pour pousser des applications sur le poste, rendez-vous dans la section « Applications » puis « Windows » et enfin « Ajouter » :

Une image contenant texte

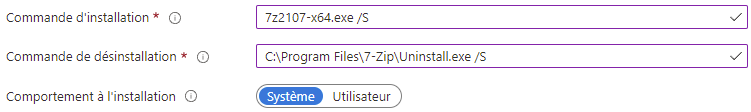
Description générée automatiquement

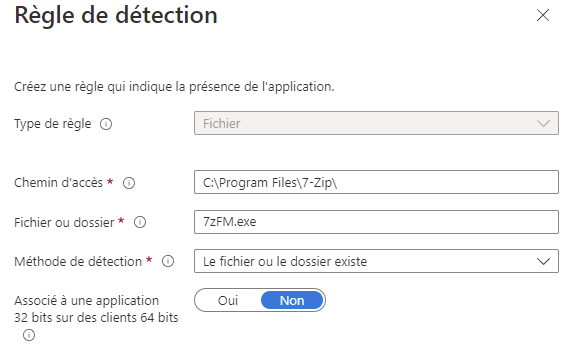
Et l’affilier au bon groupe ordinateur.

###### .EXE

Pour ajouter un « .exe » sur le poste, il suffit d’aller dans la rubrique « Application Windows (Win32) », d’ajouter le « .intunewin » qui aura été « pacqué » en amont grâce à [cet outil](https://github.com/microsoft/Microsoft-Win32-Content-Prep-Tool/archive/refs/heads/master.zip).

Sur la section suivante entrez les informations suivantes (adaptation nécessaire en fonction des logiciels) :





Puis, les règles de détection :

Et enfin, l’affecter sur le groupe ordinateur.

###### Portail d’entreprise via le Microsoft Store Privé

Il sera nécessaire pour la synchronisation entre le poste et le tenant d’installer l’application « Portail Entreprise ». Pour des raisons de simplicité, nous allons le pousser via stratégie, mais avant toute chose, il va falloir configurer les prérequis.

Pour commencer, rendez-vous dans « Administration du locataire » puis « Connecteurs et jetons » et enfin « Microsoft Store pour Entreprises » Sélectionner « Activer » puis « Ouvrir le Microsoft Store pour Entreprises ».

Rendez-vous dans « Gérer » puis « Paramètres de distributions » et « Activer » Microsoft Intune.

Ensuite, rendez-vous dans « Magasin Privée » et l’activer.

Rechercher ensuite via la barre de recherche en haut à droite « Portail d’entreprise » et « Obtenir l’application ».

Rendez-vous ensuite dans « Gérer » puis « Gérer les applications », cliquer sur « Portail d’entreprise » et enfin dans la section « Disponibilité du magasin privé » cocher « Tout le monde ».

Retourner ensuite sur la page Intune et sélectionner « Synchroniser » pour synchroniser le magasin privé du tenant.

Une image contenant texte

Description générée automatiquement

Il nous reste plus qu’à affecter cette application à notre groupe dynamique, Application -> Windows -> Portail d’entreprise -> Propriétés -> « Affectations » Modifier.

###### Applications Microsoft 365

Il peut être aussi intéressant pour Malo de déployer les outils Microsoft 365, pour cela, rendez-vous dans « Application, Windows, ajouter et sélectionner « Applications Microsoft 365 ».

Sélectionner les applications Office, Excel, Outlook, PowerPoint, Teams ainsi que Word pour notre part.

Entrer les informations sur la suite d’applications :

Une image contenant texte

Description générée automatiquement

Et sélectionner la langue sur la dernière ligne en bas de la page.

Il ne reste plus qu’a l’affecter au groupe d’ordinateur.

###### Profil de déploiement

Une image contenant texte

Description générée automatiquement Pour les inscriptions d’appareil et pour automatiser le nommage des postes, nous allons créer un profil de déploiement, pour cela rendez-vous dans Appareils -> Inscrire des appareils -> Profils de déploiement.

Créer ensuite votre profil comme ci-contre :

La valeur « %RAND:3% » va permettre de générer aléatoirement 3 chiffres à la suite de « PAR-LAP »

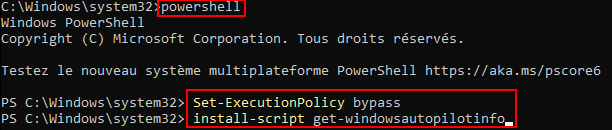
Il sera possible depuis l’interface Azure de modifier à distance le nom du poste si besoin.

Attribuer le profil au groupe ordinateur.

#### Test

Pour le test, nous avons montez un Windows 10 Professionnel qui nous servira de test.

Pour introduire un poste dans Azure, il existe plusieurs possibilités, dans notre cas, nous allons utiliser la méthode full géré, pour cela, il suffit d’installer Windows 10 sur le stockage, de le connecter à internet une fois que l’assistance Windows vous le demande et à partir de là, ouvrir une fenêtre CMD (Shift + F10) et de rentrer les commandes suivantes :



Dites « O » aux trois questions qui suivent (pour l’installation des prérequis).

Exécuter ensuite le script officiel de Microsoft précédemment installé grâce à la commande suivante :

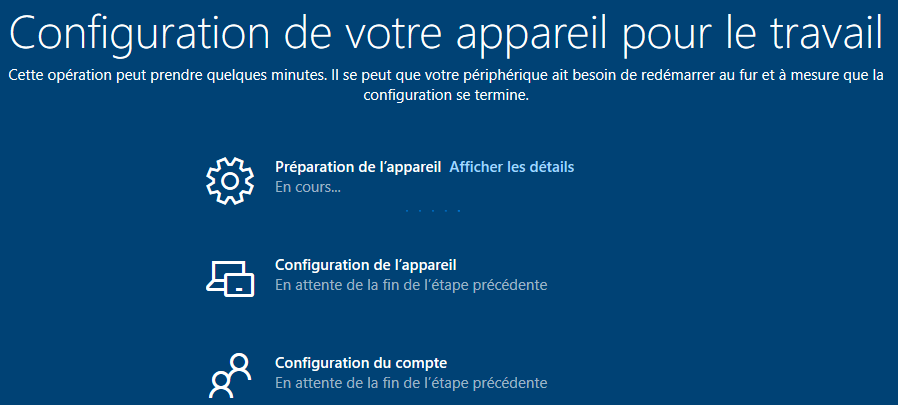


Connectez-vous ensuite avec un compte administrateur du domaine et laisser le poste faire ces pré-installations pendant au moins 5 minutes.

Il est possible de faire préconfigurer cette partie par votre fournisseur en suivant [ce tutoriel](https://youtu.be/l2q99uGa1gg).

Une fois les 5 minutes passées, redémarrer le poste et connecter vous avec le compte utilisateur qui utilisera le poste.

Après avoir entre les identifiants, le poste va se configurer automatiquement via plusieurs étapes que nous avons configurées auparavant :



##### Profil de configuration :

Le poste à bien connecté automatiquement le OneDrive sur le poste de l’utilisateur :

Le poste à bien ajouté les Serveurs DNS renseigner :

Une image contenant texte

Description générée automatiquement

Nous pouvons en conclure que nos stratégies créer précédemment dans le « Profil de configuration » sont fonctionnelles.

##### Points de terminaison :

Nous pouvons constater que le poste à bien été chiffré avec BitLocker et que la clef de récupération remonte bien sous « Clés de récupération » :

Une image contenant texte

Description générée automatiquement

##### Installation d’application :

Les logiciels « Mozilla.msi » et « 7-Zip.exe » ont bien été installer :

Une image contenant texte

Description générée automatiquement

Nous remarquons de plus que le portail d’entreprise c’est bien installé automatiquement :

Une image contenant texte

Description générée automatiquement

Le pack Office est bien installé avec les applications mentionner depuis l’interface Azure :



A noter que la connexion aux applications Microsoft se fait automatiquement via le compte connecter sur le poste.

Nous pouvons donc en conclure que notre stratégie de déploiement créer précédemment fonctionne correctement.

##### Sortir du tenant Intune

Nous avons vu dans la première partie plusieurs façon d’introduire un ordinateur dans le tenant Azure de malo, nous allons maintenant grâce à cette partie vous montrer comment en sortir.

Pour notre cas, il suffit de changer d’utilisateur et se connecter avec un administrateur du tenante, une fois cela fait, rendez vous dans les paramètres Windows puis « Compte » et enfin « Accès Professionnel ou Scolaire ». Cliquer ensuite sur « Déconnecté » et valider :

Une image contenant texte

Description générée automatiquement

Entrez le compte administrateur local du poste et redémarrer pour appliquer les changements.

### DNS

#### Introduction

Le Domain Name System ou DNS est un service informatique distribué utilisé qui traduit les noms de domaine Internet en adresse IP ou autres enregistrements.

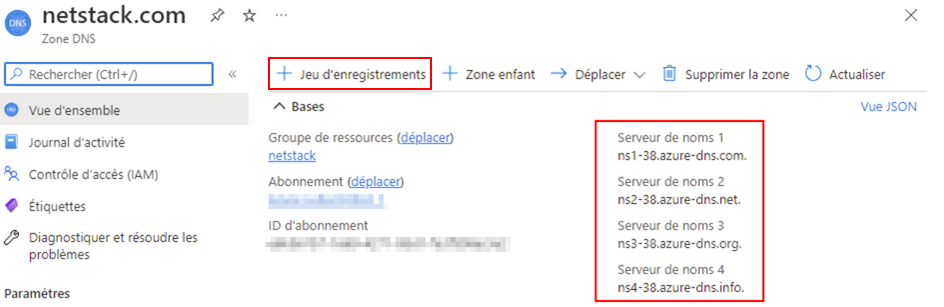
Une image contenant flèche

Description générée automatiquement

#### Mise en place

Pour mettre en place le DNS sur Azure, rendez-vous sur le [Portail Azure](https://portal.azure.com/#home) et chercher « Zones DNS » créer une zone avec un groupe de ressources et un nom.

Plusieurs serveurs DNS nous sont alors données que nous pouvons apercevoir depuis la section de droite :



Une fois votre Zone DNS créée, sélectionner la et cliquer sur « Jeu d’enregistrement », de là, vous pourrez ajouter un hôte A mais encore un CNAME, …

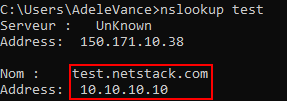
#### Test

Pour effectuer ce test, nous reprenons notre machine test (de la section « Création de GPO sous Intune (Endpoint) »).

Dans le cadre du « test », nous avons créé un hôte A nommé « test » resolutionnant l’IP « 10.10.10.10 » :



Pour savoir si le test est correct, nous allons utiliser l’outil « nslookup » depuis la machine test :



Nous pouvons en conclure que le DNS effectue bien son rôle de DNS.

#### Tarification :

Une image contenant texte

Description générée automatiquement

### DHCP

#### Introduction

« Dynamic Host Configuration Protocol » est un protocole réseau dont le rôle est d’assurer la configuration automatique des paramètres IP d’une station ou d'une machine, notamment en lui attribuant automatiquement une adresse IP et un masque de sous-réseau.

Une image contenant flèche

Description générée automatiquement

#### Mise en place

##### Création d’une machine sous Azure

Pour créer une machine sur Azure, rendez-vous sur le [Portail Azure](https://portal.azure.com/#home), puis dans « Machine Virtuelles » et enfin « Créer » en haut à gauche, de là, vous pouvez configurer votre machine à votre souhait.

Dans notre cas, nous sélectionnons « DRV-DHCP » en nom de machine virtuelle, sur Windows Server 2019 avec une taille de 1 vCPU et 3.5Go de mémoire et un SSD Premium pour la redondance.

Après avoir créé la machine en sélectionnant « Vérifier + créer », nous pouvons la démarrer et commencer l’installation des rôles nécessaire au bon fonctionnement.

##### Installation des rôles nécessaire

Il est important d’installer le rôle « DHCP » pour assurer le bon fonctionnement du service, pour cela, rendez-vous dans la gestion du serveur, puis « Gérer » et enfin, « Ajouter rôles et fonctionnalités », une page s’affiche alors, cocher la case « Serveur DHCP » et laisser l’installation se faire.

##### Configuration DHCP

Pour la configuration DHCP, il est nécessaire d’ouvrir depuis les « outils » présent dans la « Gestion de serveur » « DHCP ».

Nous pouvons ensuite, depuis la section de gauche, créer une nouvelle étendue qui permettra l’obtention d’IP dynamiquement :

Une image contenant texte

Description générée automatiquement

Chaque étendu représente un VLAN sur les sites de Paris et Belgique.

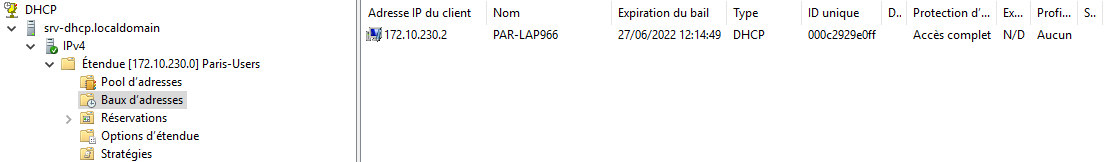
L’entièreté des VLANs et leurs fonctions sont précisées dans la partie de Paul « Réseau ».

Les options détendues sont configurées en fonction des stratégies délivrées par Paul sur la partie « Réseau ».

##### Test

Pour le test du DHCP, nous reprenons la même machine que créer dans la section « Endpoint », nous reconstituons l’architecture au plus semblable et nous essayons d’obtenir une adresse IP sur le poste client.

Nous pouvons apercevoir sur le poste que l’obtention d’une adresse est bien effectuée et que depuis le panneau de gestion DHCP, nous retrouvons bien notre client :



Nous pouvons aussi nous apercevoir que sur la poste client, l’obtention de la passerelle est bien effective.

Les DNS ne sont pas configurés depuis le serveur DHCP car nous avons poussé les DNS directement depuis Endpoint.

#### Tarification



Soit environ 85,91€/mois.

# Messagerie :

## Introduction

Pour assurer un service de messagerie, nous avons fait le choix d’opter la solution de Microsoft, Microsoft 365.

Les différentes applications Microsoft (Outlook, OneDrive, …) seront disponibles depuis les catalogues d’applications classiques sur Android et IOS.

Microsoft 365 sera accessible via le Cloud Public de Microsoft, la volumétrie sera de 100Go par utilisateur, la performance sera celle de Microsoft et de la disponibilité, d’Exchange.

La haute disponibilité, la messagerie instantanée, la sauvegarde et la rétention… est présente grâce au SaaS Microsoft.

Une fois le tenant configuré, il sera possible d’attribuer des licences aux différents utilisateurs pour leur donner ainsi accès à un panel d’application Microsoft (Word, Excel, PowerPoint, …).

## Présentation détaillée de la solution

Actuellement, le service de messagerie est assuré sur une machine stockée au sein de l’entreprise Malo, le but de cette partie va être de montrer, comment migrer l’entièreté des données (mail, contact, calendrier, …) sur le cloud Microsoft 365 puis de montrer comment s’effectue la mise en place des sauvegardes et enfin l’intégration des numéros sur Team.

### Attribution de licence

#### Introduction

Dans cette partie, nous allons voir ensemble ou acquérir les licences et comment les attribuer.

Il est très important de savoir car pour tout nouvelle arrivant dans l’entreprise, il faudra lui créer un compte et lui ajouter une licence acheter au préalable.

#### Mise en place

##### Achat de licences

Pour commencer nous allons procéder à l’achat de licence, pour cela, rendez-vous dans votre portal admin Microsoft 365 et allez dans la section « Facturation » puis « Acheter des services ».

Depuis ce menu, vous pourrez aisément acheter votre licence et ad dons nécessaire au bon fonctionnement des outils mis à disposition.

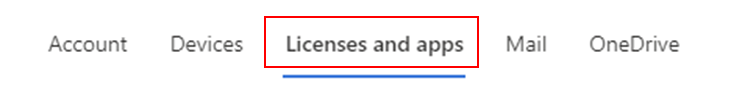
Dans notre cas, nous aurons 4 licences à acheter, don 3 à prendre pour nouvelle utilisateurs :

* Microsoft 365 E3 (Licences pour bénéficier des applications de productivité et des fonctionnalités clés en matière de sécurité et de conformité)
* Microsoft Teams Phone Standard (Nécessaire pour l’activation de la téléphonie par Teams)
* Communications Credits (Cette licence permet à l’utilisateur d’avoir accès a un pool mensuel de minutes si toutes les minutes de votre forfait d'appels sont utilisées avant le début du mois suivant)
* Microsoft 365 Domestic Calling Plan (120min) (Forfait par utilisateurs permettant d’avoir accès à 120min /mois d’appelle)

##### Attribution de licence

Pour attribuer les licences précédemment acheter, rendez-vous sur votre portal d’administration Microsoft 365 et aller dans la section « Users » puis « Active users ».

Sélectionner ensuite l’utilisateur voulu pour l’attribution de licence et rendez-vous dans la section « Licenses and apps » :

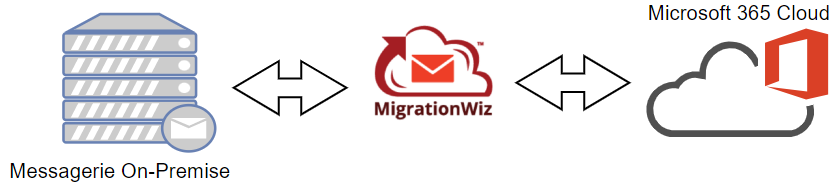


De là, vous pourrez aisément sélectionner en cochant les différentes licences, soit « Microsoft 365 E3, Microsoft Teams Phone Standard, Communications Credits et Microsoft 365 Domestic Calling Plan (120min) ».

### Migration vers Microsoft 365

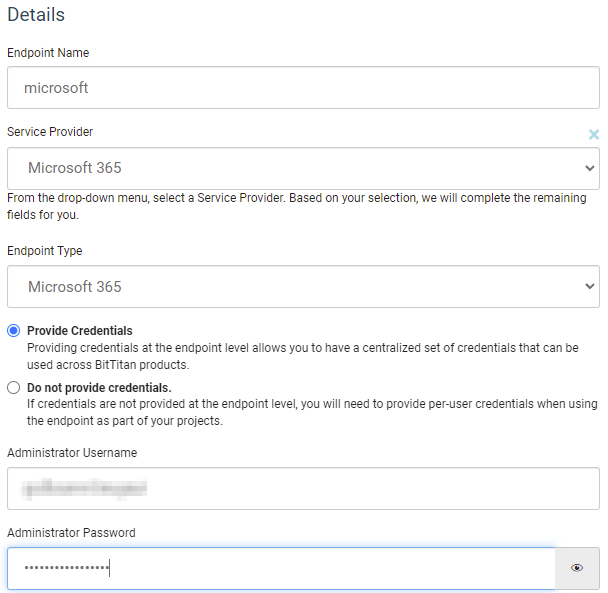
#### Introduction

Cette partie vise à traiter la migration des boites aux lettres vers le tenant Microsoft 365 précédemment créée. Pour se faire, nous avons choisi d’utiliser « MigrationWiz » qui est un outil nous permettant de migrer des BALs.



#### Mise en place

Après avoir créé un compte depuis [le site officiel de MigrationWiz](https://www.bittitan.com/account/register), nous pouvons créer un nouveau projet de boite aux lettres depuis le tableau de bord.



Une fois cela fait, nous allons pouvoir configurer les « paramètres source » soit la boite aux lettres visant à être migrée et en « destination settings », configurer la partie qui va recevoir la boite aux lettres, soit pour nous, notre Microsoft 365 :

Nous pouvons ensuite sauvegarder le projet et ajouter les informations des comptes depuis le bouton « Bulk Add » et ainsi, importer le csv (constituer à partir du template) qui va permettre à MigrationWiz de faire la liaison entre l’adresse actuel et la future :

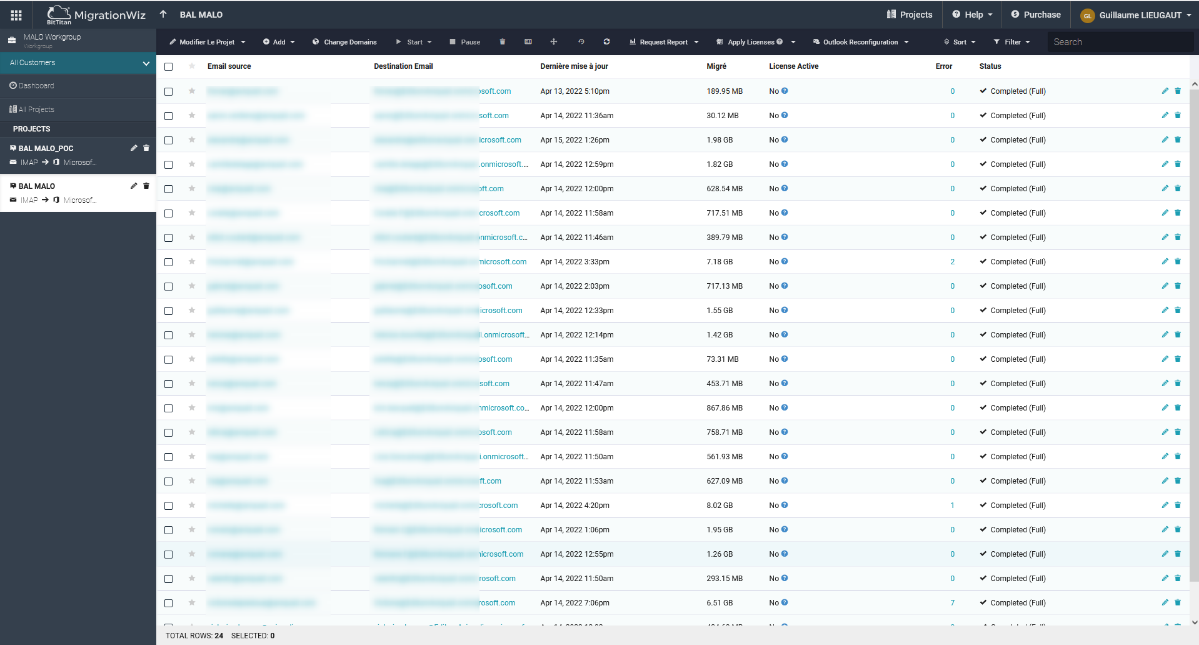
Une image contenant table

Description générée automatiquement

Nous pouvons ensuite attribuer les licences à la liste des utilisateurs à migrer puis lancer la migration depuis la section situer sur la partie haute de la page :



Nous pouvons apercevoir que la migration c’est bien déroulé car la colonne « Status » présente « Completed (Full) » :



#### Tarification

Comment expliquer dans le déroulement de la migration, nous avons besoin de licence, cette licence coute 15$/utilisateurs.

Ce qui nous ramène à 15$\*200⁓=279,44€

### Backup Microsoft 365

#### Introduction

Cette partie a été réalisé avec la coopération de Stéphane sur la partie « Infrastructure ».

Cette partie va traiter toute la partie « sauvegarde » de l’entièreté du tenant Microsoft 365. Elle est très importante car elle permet d’assurer une sauvegarde.

 Elle va se décomposer en deux grandes parties qui représentera les deux solutions utilisées pour assurer la sauvegarde, Veeam Backup for Microsoft 365 dans un premier temps, puis Backblaze.

*Cette partie est en collaboration avec Stéphane sur la partie infrastructure.*

#### Veeam Backup for Microsoft 365

##### Introduction

Veeam Software est une société privée du secteur des technologies de l’information, proposant des solutions de sauvegarde pour la gestion des données dans le cloud. Il nous permettra grâce à la solution « Sauvegarde des données Microsoft 365 » de sauvegarde l’entièreté du tenant Microsoft 365.

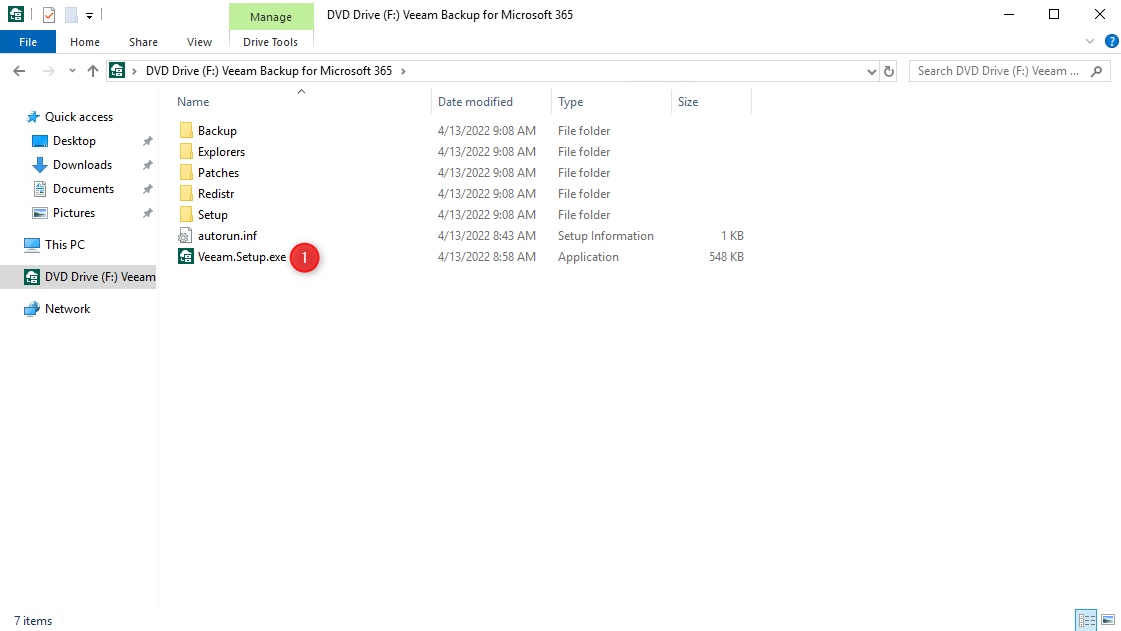
##### Mise en place

Mise en place la VM Windows Server 2019 sur Azure (c’est elle qui héberge VB365) :

Une image contenant texte

Description générée automatiquement

Chargement de l’ISO puis installation :



Double-cliquer sur 1 puis exécuter en mode Administrateur.

Une image contenant texte

Description générée automatiquement

Sélectionner 1 puis l’installation démarre en mode automatique et quasi silencieuse :

Une image contenant table

Description générée automatiquement

Sélectionner 1 « Add Org » puis indiquer le type de déploiement en 2 (ici MS365), cocher les cases correspondant au besoin en 3 puis cliquer sur 4, « Next » :

Une image contenant texte

Description générée automatiquement

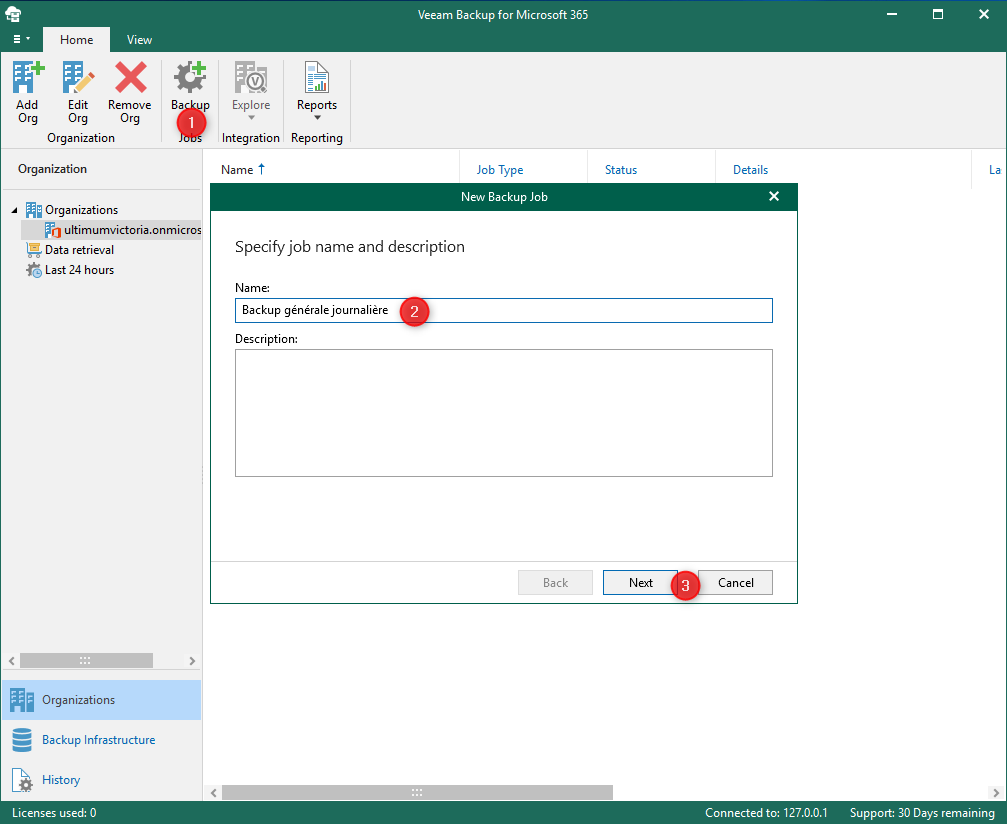
Cocher l’option en 1 puis cliquer sur Next en 2. Cette option nous permettra de nous connecter au tenant MS365 en enrollant l’application, VB365 dans Azure et de manière automatisée :

Une image contenant table

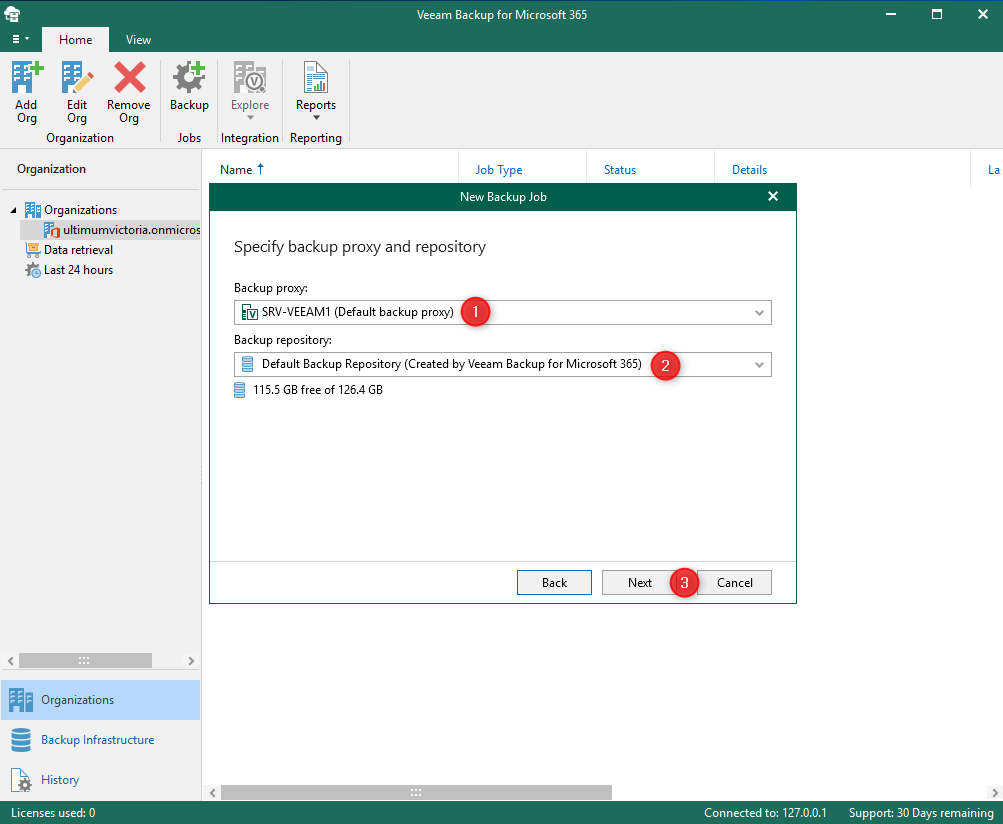
Description générée automatiquement

Laissez l’utilitaire réaliser la connexion aux différents services puis cliquer sur 1, « finish » :

Il est à noter que l’utilitaire demandera de s’enrôler avec un compte MS365 disposant de suffisamment de droits. Il est recommandé de créer un compte spécialement dédié à cet usage et de seulement lui attribuer les droits de sauvegarde et d’accès à EWS, AAD. Les droits d’administrateur global n’ont pas à lui être attribué.



Pour créer une nouvelle stratégie de sauvegarde, il faut se rendre en 1, « backup » puis indiquer un nom en 2 et « next » en 3 :



Nous indiquerons en 1 l’adresse du proxy de sauvegarde (ici en local pour le POC mais sera sur les serveurs de Backblaze à la mise en prod) puis le Repository correspondant en 2 :

Pour le repository, nous avons plusieurs choix :

* En local
* Sur un stockage en ligne compatible S3 (Bucket AWS, Backblaze)
* Sur Azure Files

Cliquer ensuite sur « Next » en 3.

Une image contenant texte

Description générée automatiquement

Nous traitons la sauvegarde générale totale, nous allons donc la programmer pour qu’elle s’exécute tous les jours à 22h, elle devra réessayer jusqu’à 3 fois si elle rencontre des objets récalcitrants.

Une image contenant texte, table

Description générée automatiquement Nous lui demandons ensuite de débuter le travail dès le clic sur « Save ». La sauvegarde se lance immédiatement.

Voici le résultat de cette sauvegarde :

##### Tarification

Pour la tarification, Veeam possède une calculatrice pour calculer les coups ([Princing-Calculator](https://www.veeam.com/pricing-calculator?ad=onpage)).

Nous pouvons nous apercevoir, que pour 200 utilisateurs Microsoft 365, nous en avons pour 3550€/an, soit environ 3550/12= 295,8€/mois.

#### Backblaze

Backblaze est un fournisseur de stockage de données. Il nous permettra le stockage de l’entièreté du tenant Microsoft 365 que Veeam à extrait.

L’avantage indéniable de ce type de produit, c’est que la volumétrie est parfaitement évolutive : Nous savons que les 45To de Malo ne seront pas utilisé à 100% dès le départ. Ce qui implique que nous n’ayons pas besoin de provisionner 45To côté Backblaze. Ainsi nous ne provisionnerons dans l’immédiat que le quart soit 11To pour un coût brut de 155€ par mois. L’évolutivité, à la baisse ou à la hausse se fera automatiquement en fonction de ce qui est envoyé par les logiciels de sauvegarde tels que Veeam.

### Téléphonie Teams

#### Introduction

Comme évoque dans l’introduction général de la partie « Messagerie », nous allons effectuer l’intégration de numéro de téléphone dans Teams pour tout appel vers l’extérieur du cycle « Teams ».

Cette partie se déroulera en deux grandes sections, la première pour l’acquisition de numéro et la deuxième pour l’attribution.

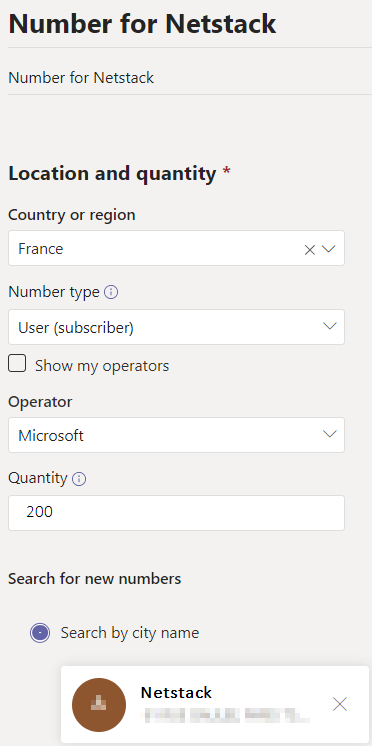
Une image contenant flèche

Description générée automatiquement

#### Mise en place

##### Acquisition de numéro

Pour commencer, rendez-vous sur votre « Admin Portal » puis « Teams » et enfin « Locations » « Emergency addresses » ([ICI](https://admin.teams.microsoft.com/locations)) et créer en deux, une pour la France et l’autre pour la Belgique :



Une fois les adresses créées, rendez-vous dans « Voice » puis « Phone Number » et enfin « Add ».

Remplissez les différentes sections et faites de même avec la Belgique.

Après avoir émis la demande de numéro de téléphone, nous allons être mis en contact avec un commercial pour la confirmation de la commande (numéro, prix, …).

##### Attribution de numéro

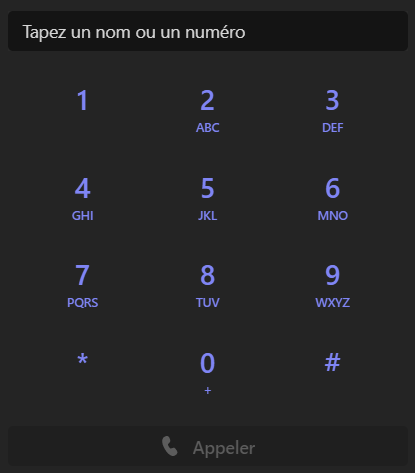
Après avoir confirmé la commande, nous allons pouvoir attribuer les numéros de téléphone aux utilisateurs.

Dans un premier temps, il faut s’assurer que les licences en rapport avec la téléphonie on bien été attribué à l’utilisateur souhaité (Microsoft Teams Phone Standard, Microsoft 365 Domestic Calling Plan (120min) et « Communications Credits ».

Rendez-vous ensuite dans « Admin Portal » puis « Teams » et enfin « Manage users » sous « Users » ([ICI](https://admin.teams.microsoft.com/users)).

Sélectionner un des utilisateurs à attribuer le numéro et faite « Edit » dans la section « General information ».

Une nouvelle fenêtre sur la partie de droite va alors s’ouvrir et vous n’aurez plus qu’à sélectionner un des numéros depuis la section « Assigned phone number ».



Après quelques minutes de synchronisation, l’utilisateur va pouvoir depuis Teams sous « Appel », appeler des numéros de téléphone :

Il sera aussi possible depuis l’application mobile de passer des appels avec son numéro attribué sur Teams.

### Tarification Microsoft 365

Pour assurer l’entièreté des services mis en place, nous avons choisi des licences « Microsoft 365 E3 », chaque utilisateur en possèdera une.

La licence coute 35,40€/utilisateurs/mois, soit 200utilisateurs\*35,40€ = 7 080€/mois.

Il y aura de plus, les add-ons téléphonique à prendre en compte soit 200utilisateurs\*11,80€ = 2 360€/mois.

# Tarification totale

|  |  |  |  |
| --- | --- | --- | --- |
| **Produit** | **Quantité** | **Période de payement** | **Prix TTC** |
| **Service Domain Publique** | x1 | /an | 6,99 € |
| **Service DNS** | x25 | Ponctuel | 11,68 € |
| **Machine DHCP** | x1 | /mois | 85,91 € |
| **Licence Microsoft 365 E3** | x200 | /mois | 7 080,00 € |
| **Licence Add-ons Téléphonie** | x200 | /mois | 2 360,00 € |
|  |  | Total le premier mois | 9 544,58 € |

# Schéma Global

# Une image contenant table Description générée automatiquementPlanning