LIVRE BLANC METSYS - OFFICE 365

Metsys
La Grande Arche Paroi Nord
Paris La défense
92044 Cedex

Tel - 01 40 903 341
Fax – 01 40 903 101
www.Metsys.fr

Version 1.0 – 04/10/2016

Guillaume MATHIEU (guillaume.mathieu@metsys.fr)

TABLE DES MATIERES

1 Présentation générale d'Office 365 6

1.1 Présentation de la solution Exchange Online 7

1.2 Présentation d'Exchange Online Protection 8

1.3 Présentation de la solution Skype for Business Online 10

1.4 Présentation de la solution SharePoint Online 11

1.5 Présentation de la solution OneDrive for Business 12

1.6 Présentation de la solution Office Web App 13

1.7 Présentation d'Office 365 ProPlus (Office 2016 Professionnel) 15

1.8 Présentation de Microsoft Azure Rights Management 16

1.9 Office 365 et les terminaux mobiles 16

1.10 Les différents plans (contrats) de licence Office 365 17

2 Créer son environnement de test Office 365 en moins d'une heure 18

2.1 Objectifs 18

2.2 Créer un nouveau tenant Office 365 (version d'évaluation de 30 jours) 18

2.3 Ajouter un domaine personnalisé au niveau de son tenant Office 365 20

3 Les outils d'administration Office 365 22

3.1 L'interface web d'administration et les modules PowerShell 22

3.2 Comment exécuter un script PowerShell qui se connecte aux services Office 365 sans saisir son login / mot de passe 23

3.3 Assigner automatiquement une licence à un compte Azure Active Directory 24

3.3.1 Présentation générale de la solution 24

3.3.2 Déploiement de la solution 24

3.3.3 Code source de la solution 28

4 Déployer Office 365 ProPlus (en version 2013 ou 2016) 35

4.1 Présentation d'Office ProPlus 2016 35

4.2 OneDrive For Business, un composant à déployer de manière spécifique 36

4.3 Installer Office 365 ProPlus 43

4.4 Désinstaller Office ProPlus 49

5 Le provisionning des comptes Office 365 50

5.1 Présentation générale 50

5.2 Les choix d'architecture 52

5.2.1 Choix 1 : choix de l'outil de synchronisation 52

5.2.2 Choix 2 : activer la synchronisation des mots de passe avec Azure Active Directory Connect 52

5.2.3 Choix 2 : préparation du schéma Active Directory 53

5.2.4 Choix 4 : déployer un serveur de secours Azure Active Directory Connect 54
5.2.5 Choix 5 : déterminer l'attribut qui est utilisé pour générer le login Office 365 55
5.2.6 Choix 6 : déterminer l'attribut qui est utilisé pour associer le compte Azure Active Directory et le compte Active Directory 55
5.2.7 Choix 7 : base de données pour Azure AD Connect 55
5.2.8 Choix 8 : mode d'installation d'Azure Active Directory Connect 57
5.2.9 Choix 9 : configurer Azure Active Directory Connect pour répliquer les mots de passe avec des domaines Office 365 fédérés 58
5.2.10 Choix 10 : les options de synchronisation d'Azure Active Directory Connect 59
5.3 Installation d'Azure Active Directory Connect 60
5.3.1 Choisir son architecture cible 60
5.3.2 Préparer l'annuaire pour Exchange 2016 et Skype for Business 2015 60
5.3.3 Ajouter les suffixes UPN correspondant aux domaines Office 365 62
5.3.4 Activer la synchronisation au niveau du tenant Office 365 63
5.3.5 Télécharger la dernière version d'Azure Active Directory Connect 63
5.3.6 Vérifier les prérequis logiciels et matériels d'Azure Active Directory Connect 63
5.3.7 Créer les comptes de services 64
5.3.8 Installation et configuration Azure Active Directory Connect 67
5.3.9 Configuration d'Azure Active Directory Connect (après déploiement) 70
5.3.10 Renforcement de la sécurité du serveur Azure Active Directory Connect 72
5.4 Recette du déploiement d'Azure Active Directory 72
6 Mise en œuvre de la fédération d'identité avec Office 365 74
6.1 Les différentes méthodes d'authentification avec Office 365 74
6.2 Office 365 et la fédération d'identité 75
6.2.1 Présentation générale 75
6.2.2 Les clients passifs (web) 78
6.2.3 Le scénario client actif 80
6.2.4 Les clients MEX (Office 365 ProPlus / Office) 82
6.2.5 Le client Skype for Business (anciennement Lync) 84
6.2.6 Office 365 Modern Authentication 86
6.3 Présentation d'ADFS 3.0 88
6.4 Déploiement d'ADFS et de Web Application Proxy (WAP) 91
6.4.1 Présentation générale 91
6.4.2 Validation des prérequis 91
6.4.3 Génération du certificat ADFS.LABMETSYS.FR 92
6.4.4 Créer le compte de service MSEXP\SVC-ADFS 96
6.4.5 Installation du serveur Microsoft ADFS 3.0 96
6.4.6 Installation du serveur Web Application Proxy 98
6.4.7 Configuration du Tenant Office 365. 101
6.4.8 Activer le protocole ADAL au niveau de son tenant Office 365 101
6.4.9 Recette 103
6.5 Paramètres avancés Microsoft ADFS 106

6.5.1 ADFS 3.0 et les mots de passe expirés 106
6.5.2 Sécurisation ADFS : Activer les logs d'authentification 106
6.5.3 Sécurisation ADFS : Extranet Lockout 107
6.5.4 Personnalisation du portail ADFS 3.0 107
7 Déploiement et configuration d'Azure Active Directory Connect et ADFS dans une architecture d'annuaire complexe ou en cours de migration 108
7.1 Les scénarios 108
7.2 La problématique du routage des suffixe UPN 109
7.3 Configuration du serveur Azure Active Directory Connect 110
7.4 Configuration du ou des serveurs ADFS et Web Application Proxy 114
7.5 Configuration du Tenant Office 365 et du serveur ADFS 3.0 119
8 Préparer son réseau et ses pare-feu / proxy pour Office 365 122
8.1 Dimensionner ses liens réseaux pour Office 365 122
8.2 Configurer les pare-feu / proxy pour Office 365 124
9 Configurer son navigateur pour Office 365 125
9.1 Les paramètres à prendre en compte pour Office 365 125
9.2 Paramétrage d'Internet Explorer 11 pour Office 365 127
9.3 Paramétrage de Firefox pour Office 365 131
10 L'authentification multi-facteurs et Office 365 132
11 La délégation d'administration et Office 365 136
11.1 Synthèse du besoin 136
11.2 Comment déléguer l'administration d'Office 365 avec les outils natifs Microsoft 137
11.3 La solution Metsys 140
12 La sauvegarde des données Office 365 141
12.1 Les scénarios de panne 141
12.2 Les solutions natives Office 365 141
12.3 Les solutions tierces 144
13 Migrer vers Office 365 145
13.1 Migrer d'Exchange On-Premise vers Exchange Online 145
13.2 Migrer de Google Apps vers Office 365 146
14 Le mode hybride Office 365 148
14.1 Le mode hybride Exchange 148
14.2 Le mode hybride Skype for Business 149
15 Trucs et astuces et dépannage Office 365 150
15.1 Les principaux outils à connaître pour faire du dépannage Office 365 150

15.2 Lancer une synchronisation Azure Active Directory Connect manuellement 150

15.3 Reconfiguration d'Azure Active Directory Connect suite à une mise à jour du schéma Active Directory 151

15.4 Supprimer un utilisateur Azure Active Directory (synchronisé avec Azure Active Directory Connect)..... 151

15.5 Modifier l'attribut ImmutableID 152

15.6 Forcer la conversion d'un domaine de messagerie fédéré en domaine Managed..... 152

15.7 Migrer un utilisateur vers un nouveau de domaine de messagerie fédéré..... 153

15.8 Utilisateurs avec un compte Live et compte Azure Active Directory identiques..... 154

1 Présentation générale d'Office 365

Microsoft Office 365 est une suite commerciale qui inclut les produits Microsoft suivants :

- Exchange Online : messagerie traditionnelle (MAPI, SMTP, POP, IMAP, Webmail).
- Skype for Business : messagerie instantanée, téléphonie sur IP, audioconférence et vidéoconférence.
- SharePoint Online : bibliothèque de document, site web collaboratif, intranet et extranet.
- Yammer : réseau social d'entreprise (sur le principe de Facebook).
- One drive : une sous entité de Sharepoint permettant le stockage et le partage de fichier par utilisateur
- Azure RMS : sécurisation et chiffrement des données d'entreprise
- Office 365 Pro Plus : suite Office lourde entière en mode click to run (amélioration continue)

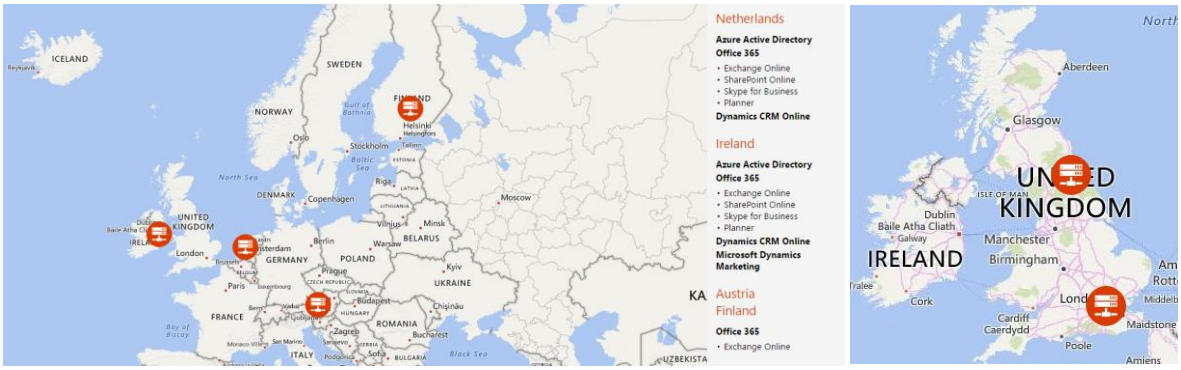
Tous ces produits s'appuient sur un annuaire Azure Active Directory qui permet aux clients de s'authentifier.

Tous les services de la suite Office 365 sont accessibles depuis les clients lourds Microsoft (Outlook, Skype for Business), une interface web (Outlook Web App) ou des terminaux mobiles (IPhone, Android, Windows Phone, BlackBerry).

Tous les serveurs Office 365 sont hébergés dans les centre de données Microsoft.

Le site web http://o365datacentermap.azurewebsites.net montre la carte des centres de données Office 365 (au 12/09/2016). Pour l'union européenne, ces centres de données se trouvent en Autriche, Ireland, Finlande et au Pays Bas (centre de données de secours). On notera l'ouverture d'un nouveau centre de données en Angleterre (https://blogs.office.com/2016/09/07/office-365-local-datacenters-now-available-in-the-united-kingdom/).

Un centre de données en France devrait ouvrir en 2017 (annonce Microsoft - octobre 2016).



Microsoft s'engage à garantir la confidentialité de ces données via le Trust center

https://products.office.com/en-us/business/office-365-trust-center-welcome

La solution Office 365 évolue très rapidement **(un changement majeur tous les 3 mois).** Il est donc nécessaire de consulter régulièrement les sites web suivants :

http://blogs.office.com/

https://community.office365.com/en-us/

Les points fort d'Office 365 :

- L'administration de l'infrastructure de messagerie est effectuée par Microsoft. Le client final garde uniquement à sa charge l'administration des comptes utilisateurs.
- Les administrateurs peuvent paramétrer la solution de manière avancée et automatiser la gestion des comptes utilisateurs à l'aide de script PowerShell.
- Boîtes aux lettres avec une taille maximum est de 50 Go.

- 1 To de données avec *OneDrive For Business*
- Le coût de la solution Online est moindre (investissement sur 5 ans) par rapport à l'achat des solutions équivalentes hébergées On-Premise.
- Logiciels / services toujours à jour (génération 2013 / 2016/…)

Les points faibles d'Office 365 :

- SSO complexe à mettre en place (ADFS). En cas de panne du SSO, plus d'accès aux services Office 365.
- Reconfiguration requise des serveurs Proxy.
- Prérequis Active Directory (modification attribut *UserPrincipalName*).
- Forte sollicitation du réseau WAN / LAN

1.1 Présentation de la solution Exchange Online

Exchange Online reprend l'ensemble des fonctionnalités d'Exchange On-Premise (soit Exchange 2016 au 12/09/2016). Les principales limites de la solution sont au niveau de l'interface d'administration qui ne permet pas toutes les options d'un serveur Exchange 2016 (pas de stratégie d'adresses de messagerie par exemple). Le tableau ci-dessous présente les caractéristiques de la solution.

Eléments	Détails
Nombre d'emails envoyés sur une plage horaire	30 messages à la minute par personne.
Nombre maximum de destinataires dans un email	500 destinataires.
Taille maximum des emails	150 Mo.
Taille maximum des boîtes aux lettres	50 Go (illimité en E3 / E5)
Limites sur les formats des pièces jointes	Aucune.
Gestion des adresses de messagerie	Exchange Online ne supporte pas les stratégies d'adresses de messagerie. Pour définir les adresses email dans Exchange Online, vous pouvez modifier les attributs *Mail*, *MailNickName* et *ProxyAddresses* au niveau de l'annuaire Active Directory et utiliser l'outil *Azure Active Directory Connect* pour répliquer ces valeurs dans l'annuaire Azure Active Directory d'Office 365.
Prise en charge du protocole POP3, IMAP, SMTP	Exchange Online prend en charge ces protocoles mais nécessite un accès chiffré via le protocole TLS (non supporté par Outlook 2003)
Boîtes aux lettres de salles / de ressources	Exchange Online prend en charge gratuitement la création de ce type de boîte aux lettres.
Boîtes aux lettres partagées	Ce type de boîte aux lettres est gratuit et permet de créer des boîtes aux lettres communes par services par exemple.
Relais anonyme	Exchange Online ne supporte pas le relais anonyme ou non authentifié. Si vous souhaitez disposer de relais anonymes, METSYS vous préconise de déployer un serveur Exchange interne (qui servira uniquement pour le relais email). **MAJ 2016: Il est possible de définir des IPS publiques fixes autorisées au relaying mail**

Pour plus d'informations, voir http://technet.microsoft.com/en-us/library/exchange-online-limits.aspx.

Office 365 prend en charge uniquement les protocoles suivants :

- IMAPS
- POP3S
- SMTPS ou SMTP authentifié
- RPC Over HTTPS.

Office 2003 ne fonctionne pas correctement avec Office 365 (Outlook 2003 ne peut pas se connecter à un serveur Exchange 2013 et versions ultérieures). Office 2007 et 2010 fonctionnent mais avec des limitations.

https://products.office.com/en-us/office-system-requirements/#Office365forBEG

Office 365 permet de chiffrer et signer les emails à l'aide du protocole *S/MIME* ou de la nouvelle fonctionnalité *Office 365 Message Encryption*. Cette solution permet d'envoyer des pièces jointes chiffrées vers des services de messagerie externes comme *Gmail*, *Yahoo*, *Lotus Notes*.

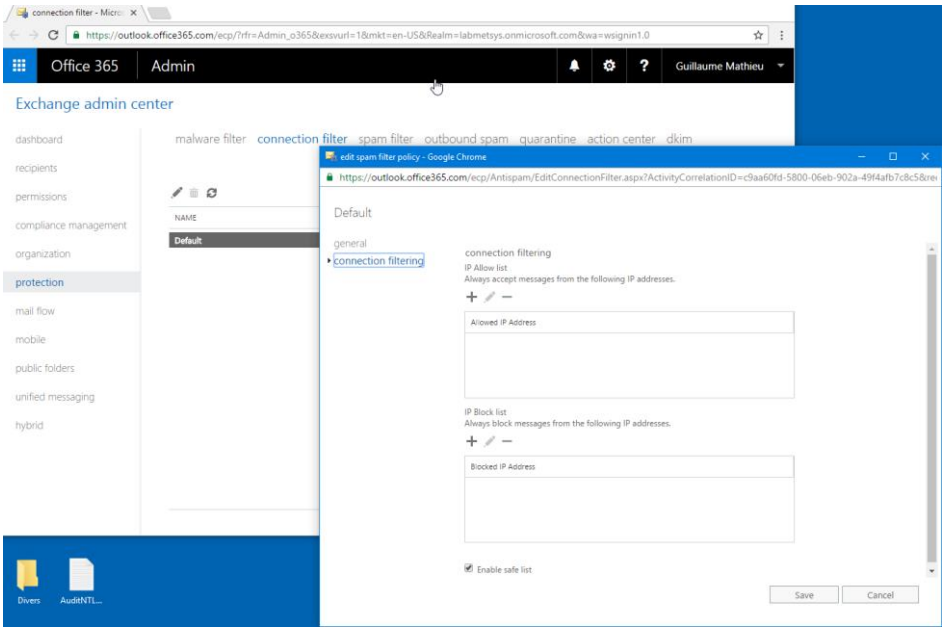
Ce service est accessible pour 2€ par utilisateur par mois pour les licences Office 365 Plan E1 et est inclus avec les licences Office 365 Plan E3 et Plan E5. Pour plus d'informations, voir :

https://products.office.com/en-us/exchange/office-365-message-encryption

1.2 Présentation d'Exchange Online Protection

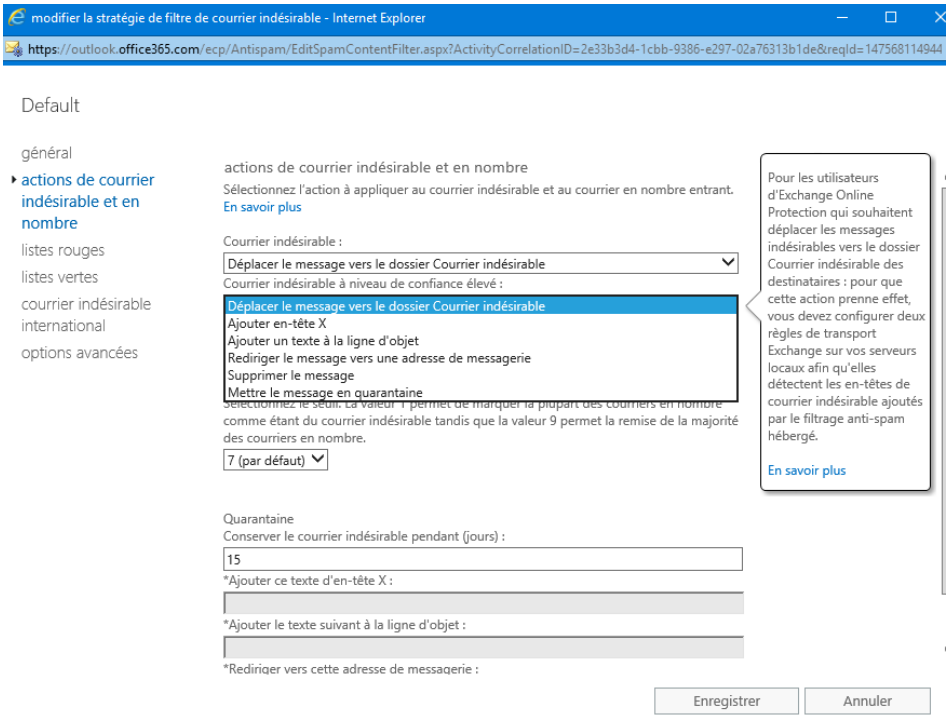
Office 365 dispose d'une solution antispam / antivirus appelée Exchange Online Protection. Cette solution peut être utilisée pour sécuriser une messagerie Exchange On-Premise, Exchange Online (activée par défaut) ou une organisation Exchange hybride (Exchange Online / On-Premise).

Exchange Online Protection permet de bloquer / autoriser (liste blanche) des ensembles d'adresses IP. Il est recommandé de cocher la case *Enable Safe List*. Ce service permet en effet de télécharger automatiquement une liste blanche d'adresses IP publiques (pour éviter les faux positifs).



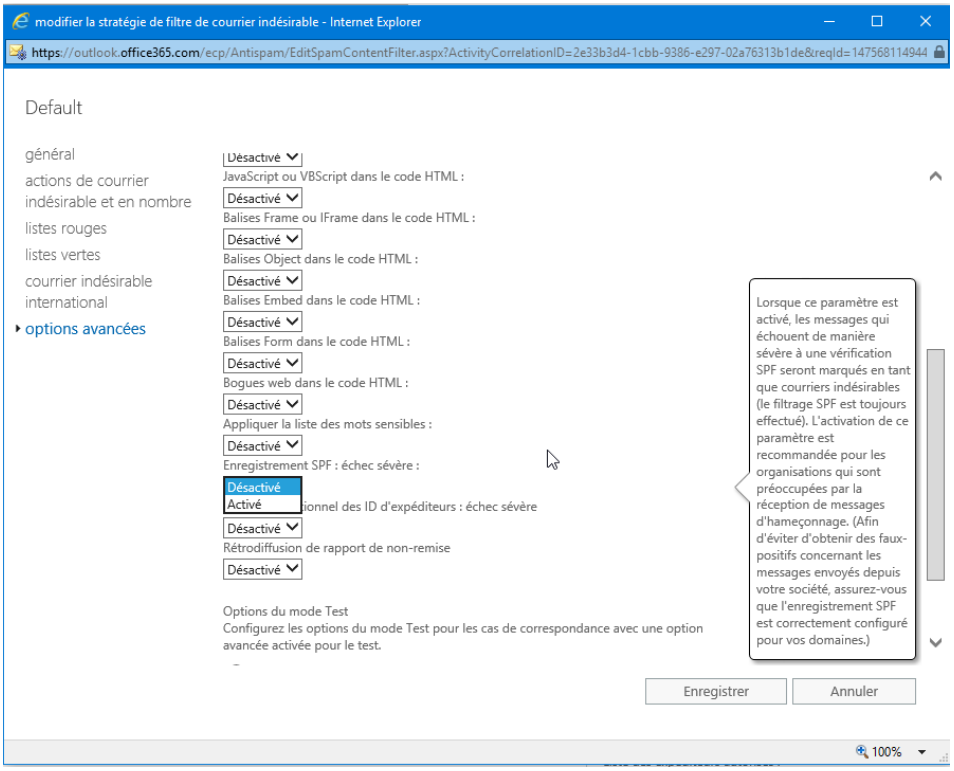
Exchange Online dispose d'une fonctionnalité de filtrage du contenu des emails. Il est possible de choisir une action pour les courriers indésirables / courriers indésirables très probables. Cette action peut être de déplacer le message vers le dossier Courrier indésirable, ajouter un en-tête pour un traitement ultérieur (règle de transport), rediriger le message vers une autre boîte aux lettres, supprimer purement le message ou le mettre en quarantaine. Il est possible de définir la durée pendant laquelle le courrier indésirable est conservé en quarantaine (15 jours).

Exchange Online Protection permet aussi de définir que les courriers provenant d'un expéditeur ou d'un domaine de messagerie spécifique seront traités comme courriers indésirables (ou l'inverse).



Exchange Online inclut aussi un mécanisme de quarantaine qui permet stocker les spams potentiels pendant une durée maximum configurable (15 jours). L'administrateur peut ensuite libérer les messages et déclarer à Microsoft les faux positifs. Il peut aussi permettre aux utilisateurs de recevoir la liste de tous les emails bloqués en quarantaine. Les utilisateurs peuvent alors débloquer un email et signaler à Microsoft un faux positif.

Les options avancées d'Exchange Online Protection permettent de définir par exemple qu'un email est un spam si l'enregistrement DNS SPF au niveau du domaine de messagerie de l'expéditeur n'existe pas.



Je vous invite à consulter l'article ci-dessous qui présente le fonctionnement des entrées DNS SPF :

https://technet.microsoft.com/en-us/library/dn789058(v=exchg.150).aspx

Microsoft propose des vidéos et des guides de configuration pour Exchange Online Protection.

https://technet.microsoft.com/en-us/library/dn750855(v=exchg.150).aspx

https://technet.microsoft.com/en-us/library/jj723137(v=exchg.150).aspx

1.3 Présentation de la solution Skype for Business Online

Skype for Business Online est la version dans le cloud de Skype for Business 2015 (anciennement appelée Lync, OCS et LCS). Elle inclut les fonctionnalités suivantes :

- Messagerie instantanée
- Partage d'écran / application.
- Conférence audio / vidéo.
- Téléphonie sur IP (prochainement en France avec la licence E5).

Office 365 Plan E5 va permettre très prochainement maintenant de relier la téléphonie sur IP Skype For Business avec le réseau GSM / RTC en France (déjà disponible aux Etats Unis).

Pour plus d'informations sur Office 365 Plan E5 : https://products.office.com/fr-fr/business/office-365-enterprise-e5-business-software

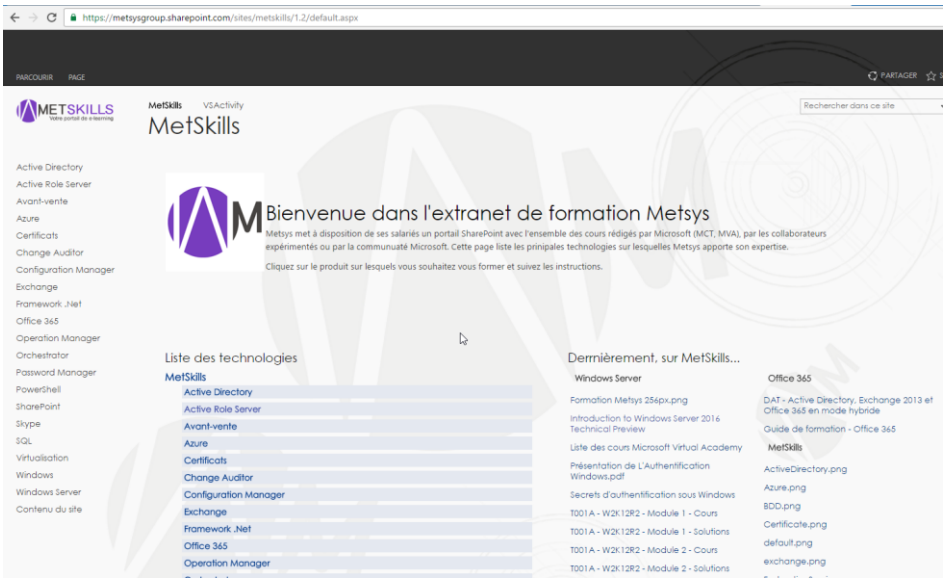
Si vous souhaitez utiliser un système de téléphonie interne, il est nécessaire de garder des serveurs Skype For Business On Premise, les lier avec la téléphonie et de configurer un mode hybride avec Skype Online.

1.4 Présentation de la solution SharePoint Online

La partie collaborative d'Office 365 est gérée par le produit SharePoint Online, un équivalent Online de SharePoint Server. SharePoint Online permet de créer entre autres des sites web d'entreprise, des Intranet et des sites web pour partager des données entre utilisateurs.

Le portail de formation interne de Metsys (capture ci-dessous) est basé sur SharePoint Online et permet de mettre à disposition des collaborateurs Metsys l'ensemble des documents de formation.

Quand un collaborateur publie un document, une notification est envoyée à notre responsable formation.

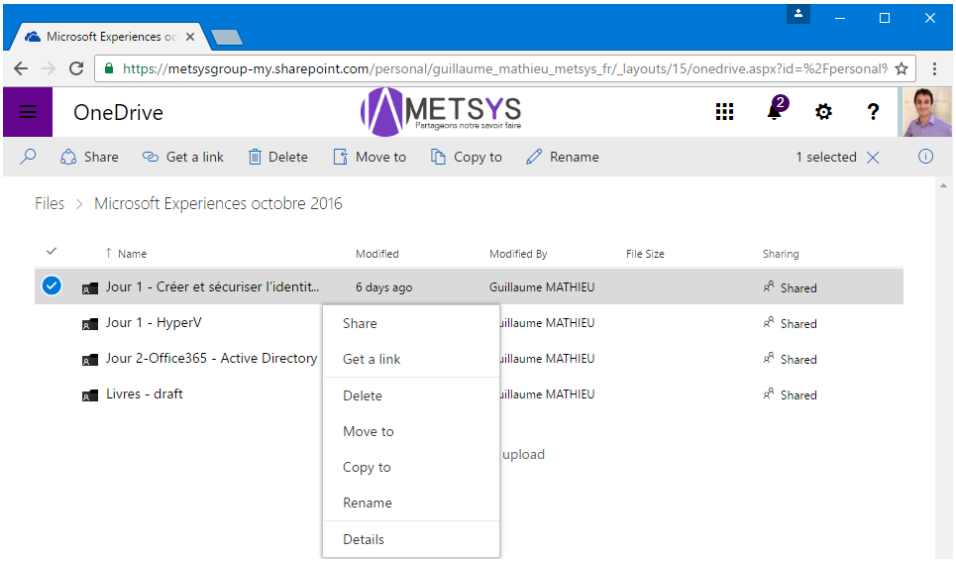


On notera que SharePoint Online n'inclut pas toutes les fonctionnalités de personnalisation de son équivalent On-Premise. Le lien ci-dessous liste les limitations de SharePoint Online.

https://support.office.com/en-us/article/SharePoint-Online-and-OneDrive-for-Business-software-boundaries-and-limits-8f34ff47-b749-408b-abc0-b605e1f6d498?CorrelationId=f8936b64-0fc3-4f17-99b6-a56087a354b3&ui=en-US&rs=en-US&ad=US

1.5 Présentation de la solution OneDrive for Business

Microsoft propose avec OneDrive for Business (anciennement *SkyDrive Pro*) un espace de stockage de 1 To pour stocker les données personnelles de chaque utilisateur. Cette solution s'appuie sur SharePoint Online contrairement à la version grand public du produit *OneDrive*. Il est possible de partager ces données aux autres utilisateurs de l'entreprise ou à des personnes externes (génération d'un lien) depuis l'interface web de l'outil *OneDrive for Business*.

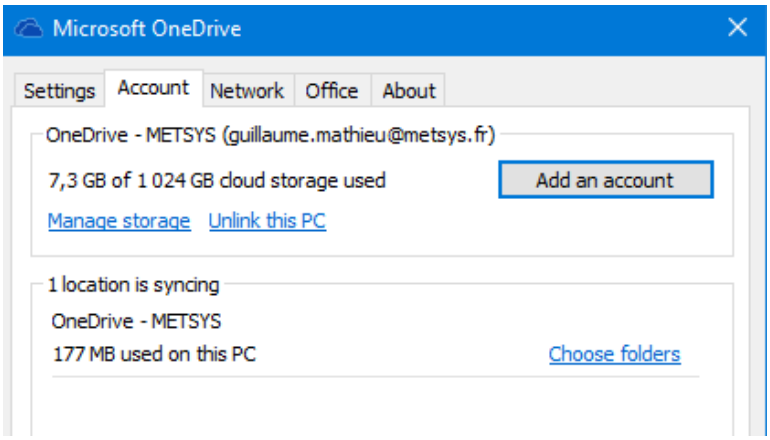


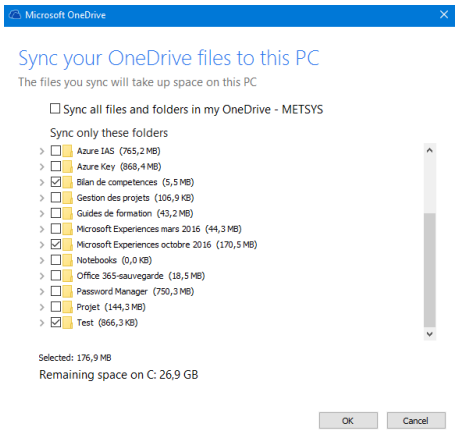
Microsoft met à disposition un client de synchronisation pour synchroniser les données OneDrive for Business sur ses périphériques (téléphone portable, ordinateurs, tablettes). Il est nécessaire d'utiliser la dernière version du client de synchronisation comme expliquée dans les articles ci-dessous :

https://support.microsoft.com/en-us/kb/2903984

https://support.microsoft.com/en-us/kb/3175950

Il est possible de synchroniser l'ensemble des données hébergées sur OneDrive for Business ou uniquement une partie. L'outil de synchronisation intègre un gestionnaire de conflits (en cas de changement sur le poste de travail et directement sur le serveur OneDrive pendant une période de temps où aucune synchronisation n'a eu lieu).





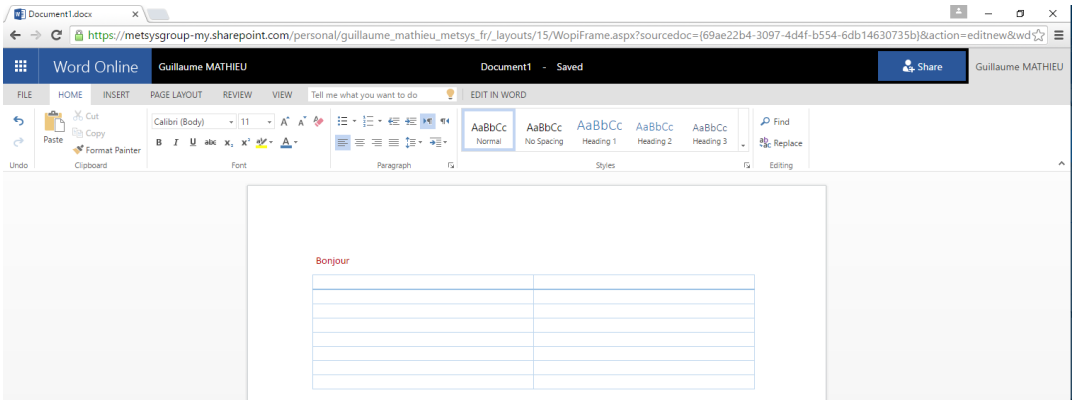
Il est possible de configurer le dossier Mes Documents pour rediriger vers l'espace de stockage de OneDrive for Business comme expliqué dans cet article : https://community.spiceworks.com/how_to/88394-redirect-my-documents-to-onedrive-for-business

L'article ci-dessous présente les 5 points à bien comprendre pour déployer la solution OneDrive For Business :
http://blog.recordlion.com/sharepoint/onedrive-for-business-things-to-know/

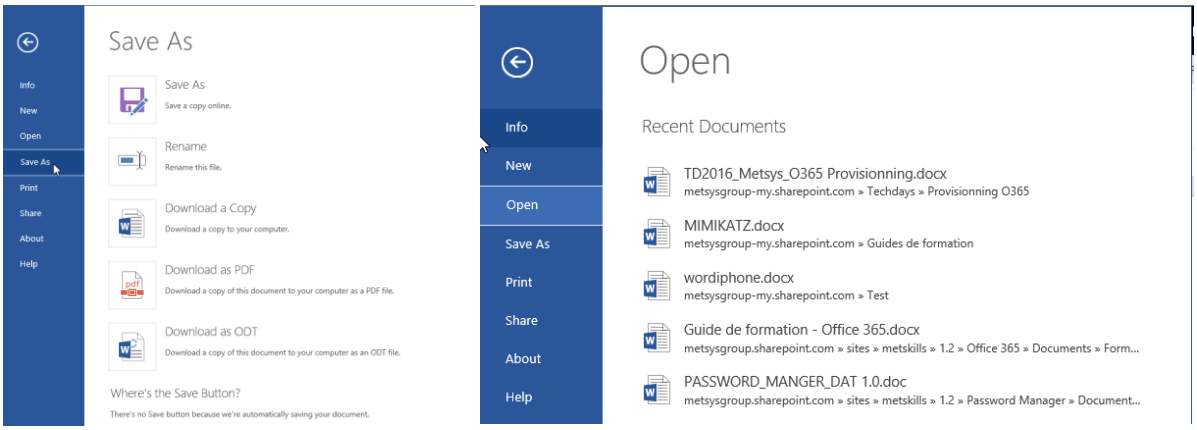
Le MVA ci-dessous présente dans le détail OneDrive for Business (bibliothèque de document SharePoint) :
https://mva.microsoft.com/en-us/training-courses/collaborating-office-365-with-onedrive-for-business-8466?l=sJ3Zr8Wz_9704984382

1.6 Présentation de la solution Office Web App

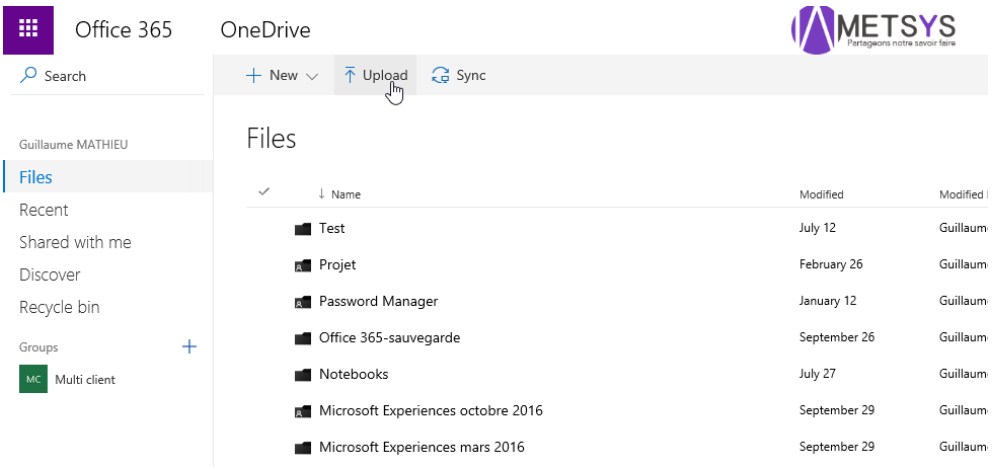
Office 365 dispose d'une version web de la suite Office 365 ProPlus appelée *Office Web App*. Word Online, Excel Online, PowerPoint Online, One Note Online permettent de lire, créer et modifier des documents Office depuis un navigateur web.



Les changements sont sauvegardés automatiquement (pas de bouton *Save*). Les fichiers de travail sont obligatoirement stockés sur *OneDrive For Business* ou sur un site *SharePoint Online*. Il est cependant possible de télécharger une copie d'un document vers un disque local.



Pour éditer un fichier local, il est donc nécessaire de le copier au préalable le fichier sur OneDrive for Business à l'aide du client web OneDrive For Business (bouton *Upload*).



Word Online ne permet pas (entre autres) de créer des nouveaux styles ou d'ouvrir un fichier protégé par un mot de passe.

https://support.office.com/en-us/article/Differences-between-using-a-document-in-the-browser-and-in-Word-3e863ce3-e82c-4211-8f97-5b33c36c55f8

https://technet.microsoft.com/en-us/library/word-online-service-description.aspx

Excel Online intègre aussi de nombreuses limitations (au niveau de la prise en charge des formules). Dans certains cas, Excel Online propose d'ouvrir un fichier en lecture seule ou de convertir un fichier pour pouvoir l'ouvrir en lecture / écriture.

https://support.office.com/en-us/article/Comparing-Excel-Services-and-Excel-Web-App-SharePoint-2013-855ee1a3-9263-425d-bccd-4070d2413aa7

https://technet.microsoft.com/en-us/library/excel-online-service-description.aspx

La version Online d'Office 365 ProPlus est optimisée pour la coédition.

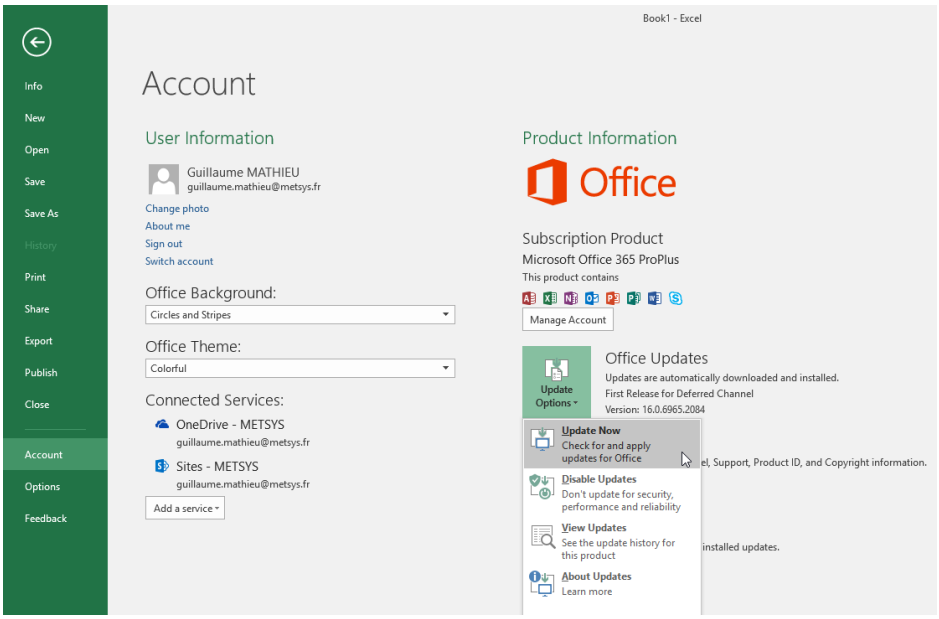
1.7 Présentation d'Office 365 ProPlus (Office 2016 Professionnel)

Office 365 ProPlus est un équivalent d'Office 2013 ou 2016 Professionnel. Office 365 ProPlus peut être installé sur une station de travail Windows ou Apple (Mac).

Il est nécessaire de disposer d'une licence Office 365 **Plan E3** ou **Plan E5** pour activer Office 365 ProPlus.

La solution Office 365 ProPlus ne peut pas être activée avec un numéro de série.

Le format de l'installation n'est pas du MSI mais du *Click to Run*.



Office 365 ProPlus est configuré pour se mettre à jour automatiquement. Microsoft propose pour cela plusieurs méthodes de mise à jour comme expliqué dans l'article https://technet.microsoft.com/fr-fr/library/mt455210.aspx :

- **Deferred channel** : une mise à jour des fonctionnalités est proposée tous les 4 mois par Microsoft (option par défaut).
- **Current channel :** une mise à jour des fonctionnalités est proposée tous les mois.
- **First Deferred channel :** permet à des utilisateurs pilotes de tester la prochaine version *Deferred*.

Le déploiement et la configuration d'Office 365 ProPlus 2016 sont présentés plus loin dans ce document.

Le produit existe en version 32 bits et 64 bits. Il est recommandé d'utiliser une version 32 bits d'Office ProPlus (compatibilité avec les macros). La grosse nouveauté d'Office ProPlus (en version 2016) est la prise en charge améliorée de la coédition.

Le MVA ci-dessous présente les nouvelles fonctionnalités d'Office 365 Pro Plus (version 2016) : https://mva.microsoft.com/en-us/training-courses/office-365-proplus-whats-new-in-2016-and-beyond-14065?l=6k9rJAomB_9800115881

1.8 Présentation de Microsoft Azure Rights Management

Azure Rights Management est l'équivalent Online de la solution *Active Directory Rights Management* dans le cloud. Cette fonctionnalité est incluse avec Office 365 Plan E3 et Plan E5 et peut être achetée (louée) séparément pour 1,70 € par mois par utilisateur (https://products.office.com/fr-fr/business/microsoft-azure-rights-management). Elle permet de gérer les droits d'accès sur les données de la suite Office 365 (un email, un fichier Word). Il est par exemple possible d'empêcher un utilisateur de transférer un email ou définir des droits personnalisés au niveau d'un fichier Word (bloquer la modification, l'impression, le copier / coller…).

Un chapitre sera consacré à *Azure Rights Management* dans une prochaine version de ce guide.

1.9 Office 365 et les terminaux mobiles

Microsoft a développé une version mobile de ces principaux logiciels : *Word*, *Excel*, *Outlook*, *PowerPoint*, *OneNote* et *Delve*. Ces applications peuvent être téléchargées au niveau des magasins d'application (Store) Android, IOS ou Windows Phone. Elles sont gratuites et permettent par défaut de lire tous les fichiers de la suite Office (*docx*, *xlsx*, *pptx*…). Pour accéder à l'ensemble des fonctionnalités de ces logiciels (édition des fichiers Office), il est nécessaire de s'authentifier avec son login / mot de passe Office 365 (compte Azure Active Directory).

On notera que les versions mobiles intègrent uniquement les fonctionnalités les plus basiques / adaptées à l'utilisation sur un terminal mobile et que ces dernières s'adaptent à la taille de l'écran (téléphone, tablette…).

http://office.microsoft.com/en-us/mobile/

L'application OneDrive permet d'accéder et de synchroniser les données hébergées sur OneDrive For Business sur son terminal mobile. Elle s'avère par exemple très pratique pour copier des données entre un terminal mobile IOS et une station de travail de Windows.

L'application OME Viewer permet de visualiser les emails chiffrés à l'aide de la fonctionnalité *Message Encryptions*.

L'application Office 365 Admin permet d'accéder aux fonctionnalités d'administration (de base) d'un Tenant Office 365. Il est par exemple possible d'assigner une licence Office 365 à un utilisateur avec cette application.

Exchange Online prend en charge le protocole ActiveSync. Il est donc possible de synchroniser ces emails sans déployer l'application mobile Outlook. Mais dans ce cas-là le terminal doit répondre aux conformités de sécurité définies par l'administrateur Exchange : code pin activé ou mot de passe fort, auto effacement du terminal… Le terminal est enrôlé.

Office 365 prend en charge les terminaux mobiles BlackBerry (antérieur à la version 10). Les nouveaux BlackBerry utilisent quant à eux la technologie ActiveSync.

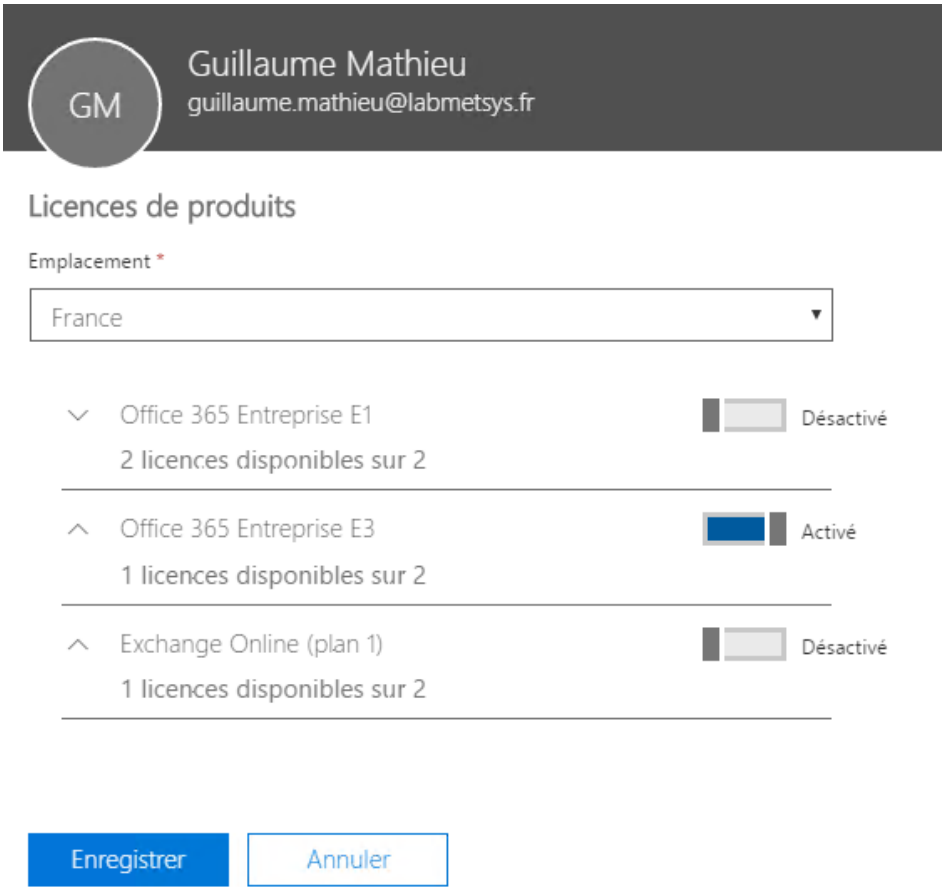
https://technet.microsoft.com/fr-fr/library/office-365-blackberry.aspx

1.10 Les différents plans (contrats) de licence Office 365

Pour disposer d'Office 365, il faut souscrire à un abonnement. Le client n'est pas propriétaire des licences avec Office 365. Il achète uniquement un droit d'usage du service Office 365 (location).

Il existe de très nombreux plans de licences Office 365 (*Enterprise*, *Business*, *Education*…). Chaque plan dispose de composants qui correspondent à un logiciel intégré dans la suite Office 365 comme Exchange Online, Skype for Business Online ou SharePoint Online.

On assigne un plan Office 365 à un compte utilisateur *Azure Active Directory*. Il est possible d'activer un plan de licences et de désactiver certains de ces composants sans que cela affecte le coût de la licence.



Si vous effectuez un déploiement pour une entreprise, il est recommandé d'acheter uniquement des plans *Enterprise* ou *Business*. Le lien ci-dessous présente les principaux plans Entreprise Office 365 (E1, E3 et E5) :

https://products.office.com/en-us/business/compare-more-office-365-for-business-plans

Le plan Business est limité à 300 comptes utilisateurs, là où l'entreprise n'a pas de limite.

On notera que le plan Office 365 E4 a été remplacé par le plan E5.

https://products.office.com/fr-fr/business/office-365-enterprise-e5-business-software

Il est possible dans certains cas de mixer différents plans Office 365 sur le même Tenant Office 365. Il est par exemple possible de disposer de licences Office 365 Plan E1 et de licences Office 365 Plan E3 sur un même Tenant Office 365.

2 Créer son environnement de test Office 365 en moins d'une heure

2.1 Objectifs

Le but est de déployer une maquette Office 365 fonctionnelle. L'environnement de tests doit permettre :

- De créer un Tenant Office 365 avec 20 licences d'évaluation Office 365 Plan E3 ou E5.
- D'utiliser toutes les fonctionnalités d'Office 365 Plan E3 ou E5. Les utilisateurs doivent pouvoir envoyer et recevoir leur email (domaine de messagerie publique) depuis et vers Internet.
- D'installer Office 365 ProPlus (Office 2016) sur une station de travail Windows 7 fraîchement installée membre d'un groupe de travail ou d'un domaine.

Je vous invite à consulter le MVA suivant pour découvrir Office 365 (en français) :

https://mva.microsoft.com/fr-fr/training-courses/comment-dployer-et-grer-office-365-pour-les-pme-fr-15938?l=NnrSTLs9B_705192797

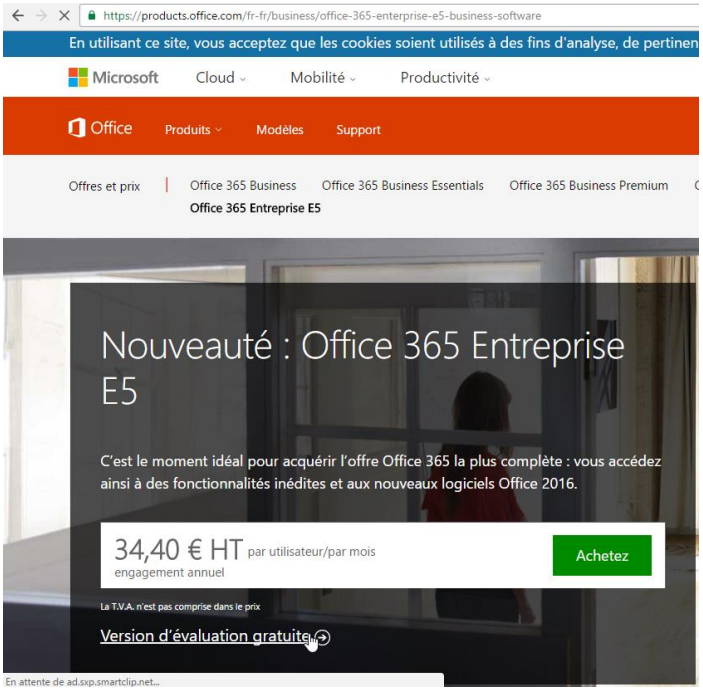
2.2 Créer un nouveau tenant Office 365 (version d'évaluation de 30 jours)

Pour déployer cet environnement de test, il n'est pas nécessaire d'acheter de serveurs ou des licences Office 365. Une station de travail Windows 7 SP1 (ou versions ultérieures) et un navigateur web récent (Internet Explorer 11, Chrome, Firefox ou Edge) sont cependant requis. En effet les clients web d'Office 365 ne sont plus compatibles avec Internet Explorer 8 ou 9. Office 365 ProPlus (Office 2013 / 2016 Professionnel) ne peut pas être déployé sur une station de travail Windows XP Pro : http://office.microsoft.com/en-us/office365-suite-help/software-requirements-for-office-365-for-business-HA102817357.aspx)

Microsoft permet de créer un Tenant Office 365 avec des licences d'évaluation (Plan E3 ou Plan E5) :

https://products.office.com/fr-fr/business/office-365-enterprise-e3-business-software

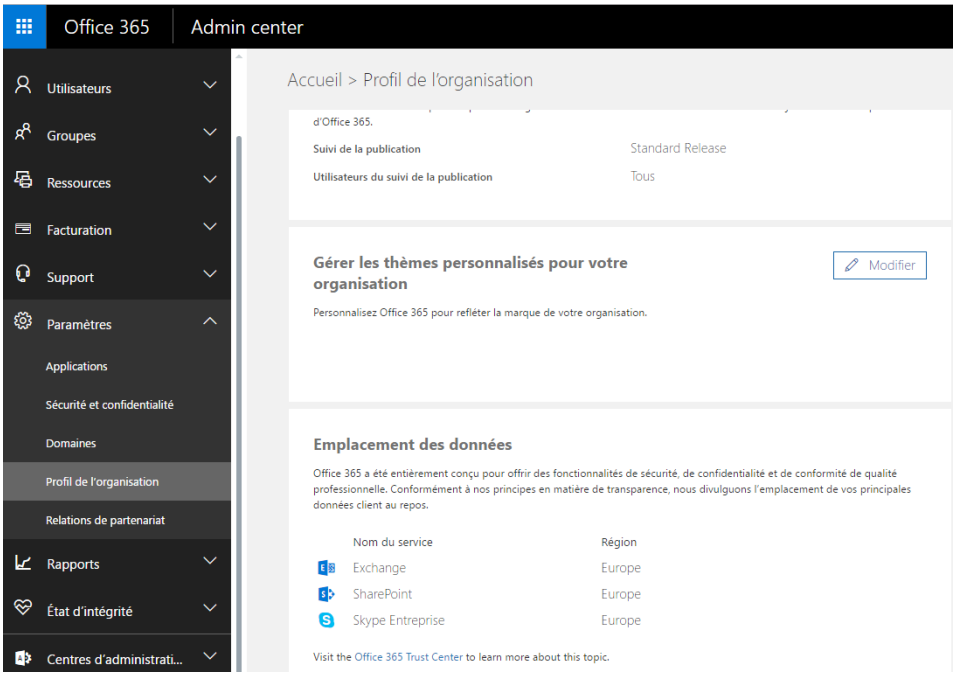
https://products.office.com/fr-fr/business/office-365-enterprise-e5-business-software



Un Tenant Office 365 dispose d'un nom DNS sous le format *XXXX.ONMICROSOFT.COM* où *XXXX* est le nom du Tenant. Ce nom doit être choisi judicieusement car il ne peut pas être changé par la suite.

Dans notre cas, nous allons créer un tenant appelé *LABMETSYS.ONMICROSOFT.COM*.

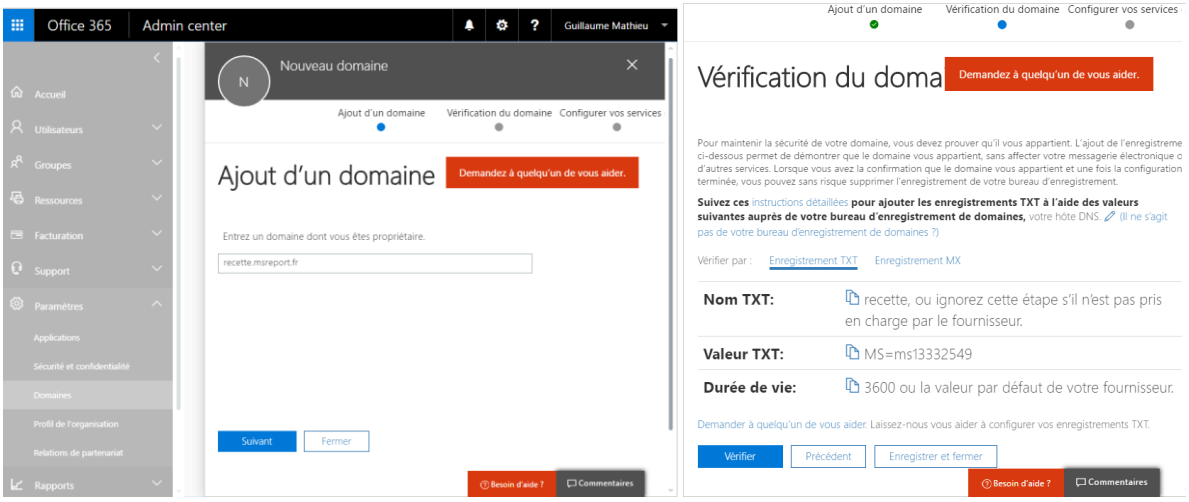
Avant de créer son Tenant Office 365, il est nécessaire de valider dans quel centre de données le Tenant Office 365 sera créé. Ce choix doit être mûrement réfléchi surtout pour les grandes sociétés. Il est possible de retrouver cette information dans la section Profil de mon *Organisation | Emplacement des données*. Dans l'exemple ci-dessous, le Tenant Office 365 a été créé en Europe dans le centre de données de Dublin.



2.3 Ajouter un domaine personnalisé au niveau de son tenant Office 365

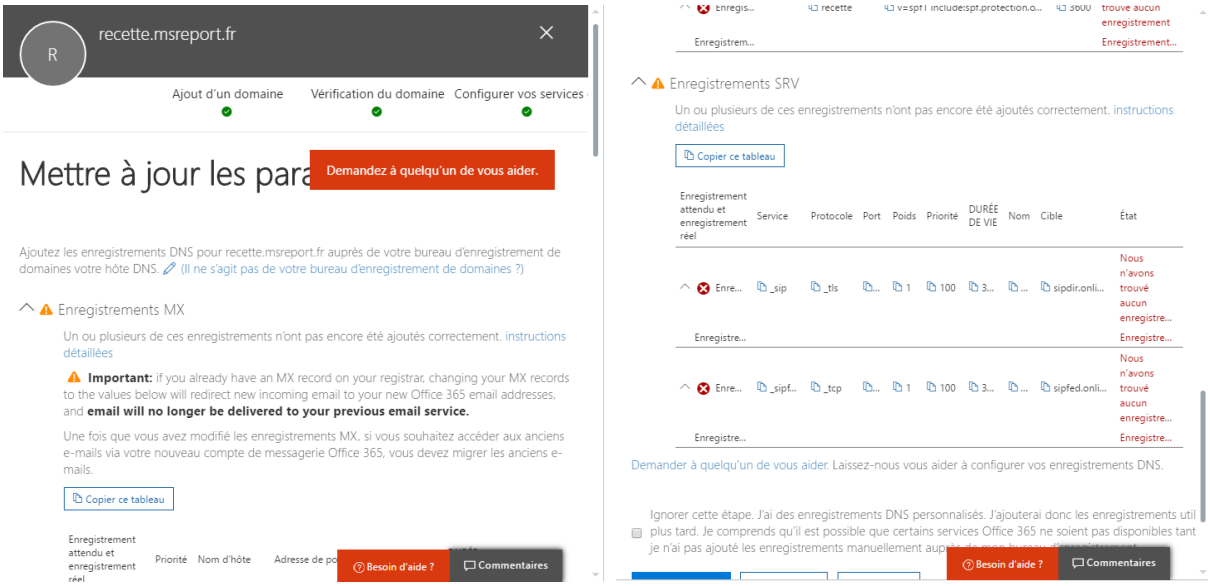
Pour ajouter votre domaine de messagerie, il faut aller ouvrir une session en tant qu'administrateur global Office 365 et aller dans la section *Paramètres | Domaines* puis cliquer sur *Ajouter un domaine*.

Dans l'exemple ci-dessous, on ajoute le domaine *RECETTE.MSREPORT.FR*.

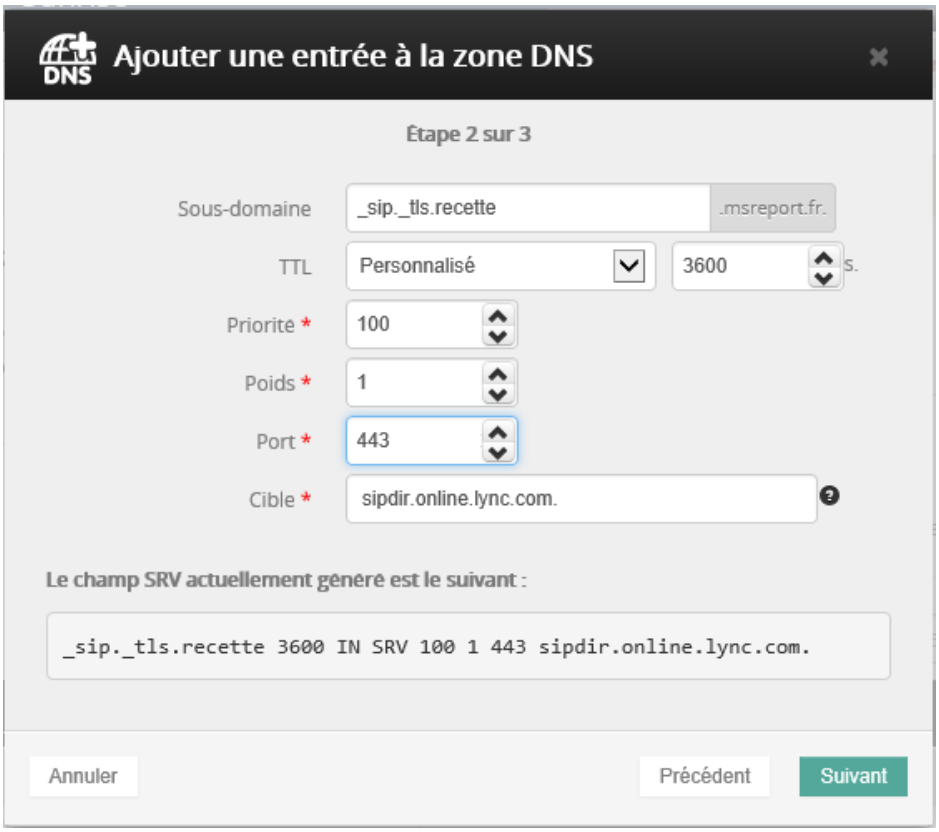


Dans mon cas, le domaine *MSREPORT.FR* est géré par OVH. Je dois donc me connecter à l'interface d'administration OVH et créer l'entrée DNS de type *TXT* pour prouver que je suis bien le propriétaire du domaine *MSREPORT.FR*.

Une fois cette étape effectuée, il faut créer l'ensemble des entrées DNS pour le domaine *RECETTE.MSREPORT.FR*.



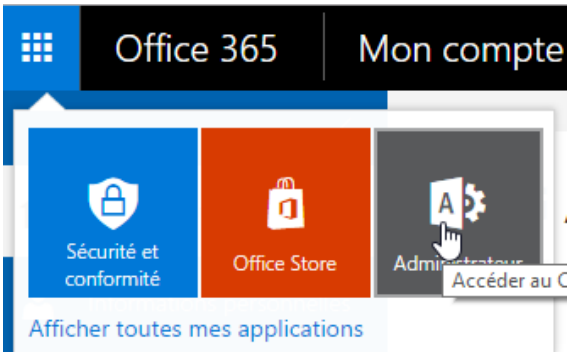
La création des entrées SRV est un peu délicate (surtout si comme dans l'exemple vous créez une entrée pour un sous-domaine).

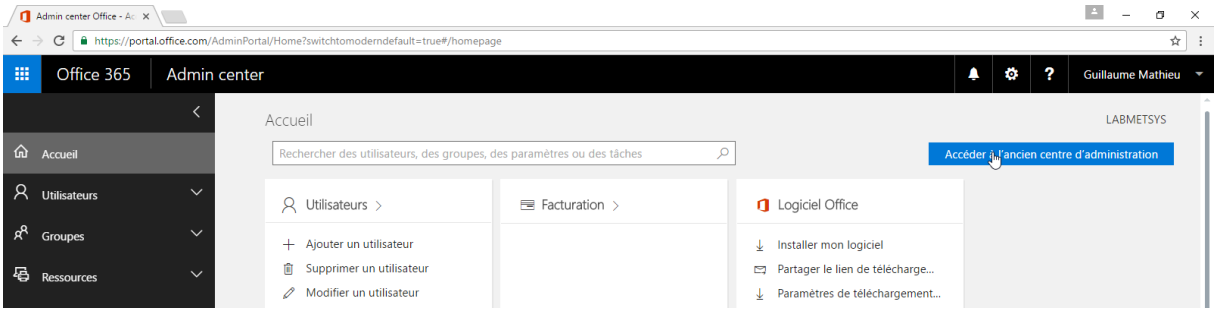


3 Les outils d'administration Office 365

3.1 L'interface web d'administration et les modules PowerShell

La solution Office 365 dispose une interface d'administration web et de nombreux modules PowerShell. L'interface d'administration web est disponible à l'adresse suivante : https://portal.office.com. Il est aussi possible d'accéder à l'interface d'administration avec le bouton Administrateur.





On notera que Microsoft est en cours de migration vers une nouvelle interface. Pour cette raison, certaines fonctionnalités sont encore présentes uniquement dans l'ancienne interface. Cette dernière est accessible via l'URL https://portal.office.com/Admin/Default.aspx?switchtoclassic=true ou via le bouton *Accéder à l'ancien centre d'administration* au niveau de la page d'accueil.

Il existe un module PowerShell pour toutes les solutions de la gamme Office 365 :

- Module PowerShell pour Azure Active Directory (version actuelle 1.1.166.0 au 22/09/2016) : http://social.technet.microsoft.com/wiki/contents/articles/28552.microsoft-azure-active-directory-powershell-module-version-release-history.aspx
- Module Exchange Online : https://technet.microsoft.com/fr-fr/library/jj984289(v=exchg.160).aspx
- Module SharePoint Online : https://www.microsoft.com/fr-FR/download/details.aspx?id=35588
- Module Skype for Business Online (Lync Online) : https://www.microsoft.com/en-us/download/details.aspx?id=39366
- Module Azure RMS : https://technet.microsoft.com/fr-fr/library/jj585012.aspx

Pour Exchange Online, aucun module n'est nécessaire. On se connecte en *Remote PowerShell* et les commandes sont directement lancées sur les serveurs Exchange Online.

3.2 Comment exécuter un script PowerShell qui se connecte aux services Office 365 sans saisir son login / mot de passe

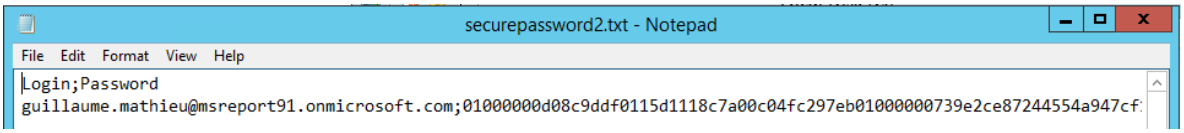
La première étape consiste à générer un fichier chiffré où l'on va stocker le login / mot de passe utilisé pour se connecter aux services Office 365. Cette procédure est présentée en détail dans l'article ci-dessous :

http://www.adminarsenal.com/admin-arsenal-blog/secure-password-with-powershell-encrypting-credentials-part-1

Les commandes PowerShell ci-dessous permettent de générer le fichier chiffré :

```
$FileInfo = "c:\securepassword2.txt"
$User = "guillaume.mathieu@msreport91.onmicrosoft.com"
$Password = "P@sswordvachette"
$secure = ConvertTo-SecureString $password -force -asPlainText
$EncryptedPassword = ConvertFrom-SecureString $secure
echo "Login;Password" | Out-File $FileInfo -Encoding UTF8 -Force
echo "$User;$EncryptedPassword" | Out-File $FileInfo -Encoding UTF8 –Append
```

On obtient le résultat suivant :



Les commandes PowerShell ci-dessous permettent de générer le crédential *$cred2* à partir du fichier contenant le login et le mot de passe chiffré.

```
$FileInfo = "c:\securepassword2.txt"
$Info = Import-Csv -Path $FileInfo -Delimiter ";" -Encoding UTF8
$User2 = $Info.Login
$Password2 = ConvertTo-SecureString -string $Info.Password
$cred2 = New-Object -TypeName System.Management.Automation.PSCredential -argumentList
$User2,$Password2
```

La commande ci-dessous permet de se connecter à Exchange Online avec *$Cred2*.

```
# Connect to Exchange Online
try {Import-PSSession (New-PSSession -ConfigurationName "Microsoft.Exchange" -ConnectionUri
"https://outlook.office365.com/powershell-liveid/" -Credential $cred -Authentication "Basic" -AllowRedirection
-Name "ExchangeOnline" -SessionOption $Option) -AllowClobber:$True}
catch {$ConnectFailure = $_.Exception.Message}
```

3.3 Assigner automatiquement une licence à un compte Azure Active Directory

3.3.1 Présentation générale de la solution

Les commandes *New-Mailbox* et *Enable-Mailbox* n'existent pas avec Exchange Online.

Pour créer une nouvelle boîte aux lettres Exchange Online et l'assigner à un compte Office 365 (Azure Active Directory), il faut assigner un plan de licence Office 365 intégrant le composant *Exchange Online* comme le plan E1, E3 ou E5. Ce fonctionnement est identique pour toutes les autres applications Office 365 (Skype for Business, OneDrive For Business…).

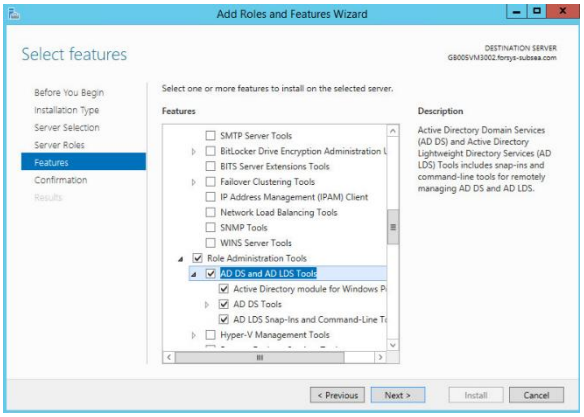
La solution ci-dessous permet à l'aide d'un script PowerShell Azure Active Directory d'assigner une licence à un utilisateur qui est membre d'un groupe spécifique.

Le script vérifie que le compte Azure Active Directory existe et qu'il ne dispose pas déjà d'une licence Office 365. Il assigne ensuite une licence puis vérifie par exemple que la boîte aux lettres Exchange Online est créée. Une fois le bon fonctionnement de la boîte Exchange Online validée, le script supprime l'utilisateur du groupe.

3.3.2 Déploiement de la solution

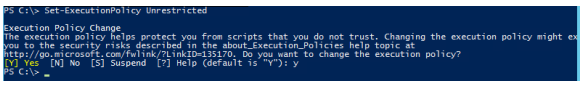
Dans cet exemple, on va déployer cette solution sur le serveur Azure Active Directory Connect. Ouvrir une session en tant qu'administrateur.

Installer les outils d'administration Active Directory dont le module PowerShell sur le serveur qui exécute le script PowerShell.



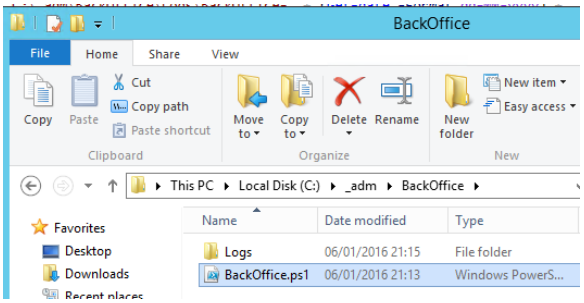
Entrer la commande suivante pour autoriser l'exécution des scripts non signés :

Set-ExecutionPolicy Unrestricted



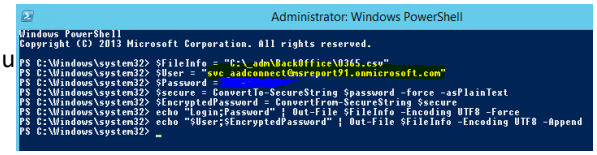
Créer le dossier *C:_adm\BackOffice\Logs*

Créer le fichier *C:_adm\BackOffice\BackOffice.ps1*



Le script a besoin d'un fichier CSV qui contient le login et mot de passe d'un compte Azure Active Directory qui dispose du droit d'assigner des licences Office 365.

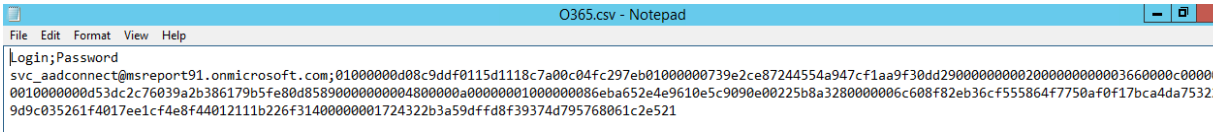
Pour plus de sécurité, le mot de passe sera stocké au format chiffré dans le fichier à l'aide d'une clé DPAPI.



Pour cela exécuter le script ci-dessous en remplaçant le nom de l'utilisateur et le mot de passe dans le script.

```
$FileInfo = "C:\_adm\BackOffice\O365.csv"
$User = "XXXX@XXXX.onmicrosoft.com"
$Password = "XXXXX"
$secure = ConvertTo-SecureString $password -force -asPlainText
$EncryptedPassword = ConvertFrom-SecureString $secure
echo "Login;Password" | Out-File $FileInfo -Encoding UTF8 -Force
echo "$User;$EncryptedPassword" | Out-File $FileInfo -Encoding UTF8 -Append
```

On obtient alors le résultat suivant :



Copier le code source du BackOffice disponible dans les annexes de ce document dans le fichier *C:_adm\BackOffice\BackOffice.ps1*

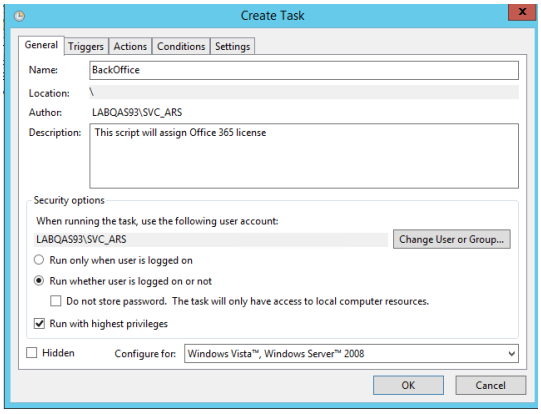
Penser à modifier les variables globales du script avec les informations de votre Tenant Office 365.

```
$global:MessagingSuffix = @("@msreport93.intra")
$Global:LogAction = "C:\_adm\BackOffice\Logs\BackOffice-" + (Get-date -Format dd-MM-yyyy) + ".txt"
$Global:O365AccountSkuID = "MSREPORT93:ENTERPRISEPACK"
$Global:o365ManagementGroup = "O365-E3-License-Management"
$Global:FileInfo = "C:\_adm\BackOffice\O365.csv"
```

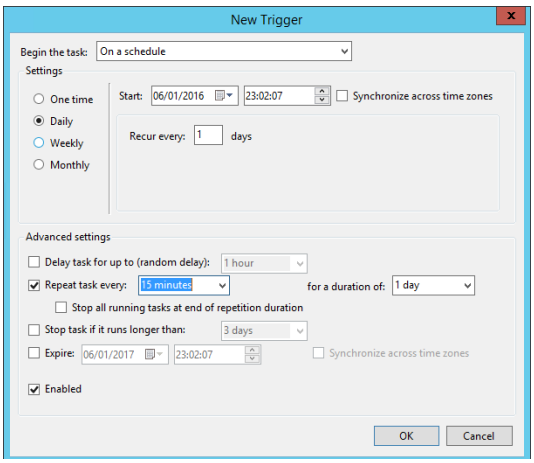
Créer une tâche planifiée.

Entrer *BackOffice* comme nom.

Cocher la case *Run with High privileges*.

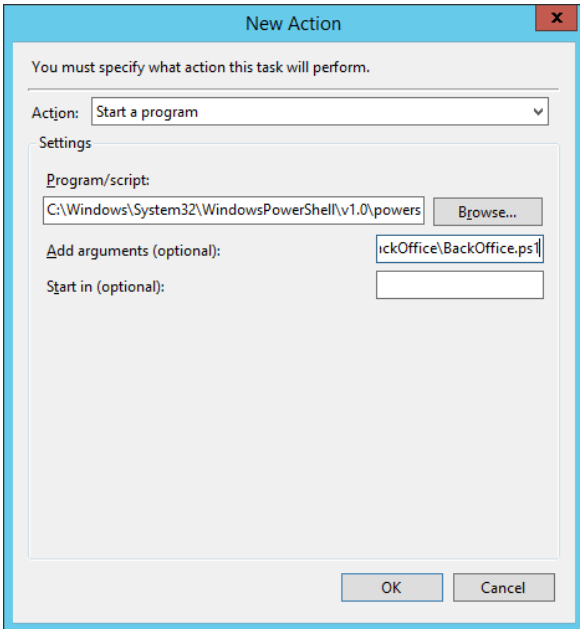


Configurer la tâche pour s'exécuter toutes les 15 minutes en cochant la case *Repeat the task every: 15 minutes.*

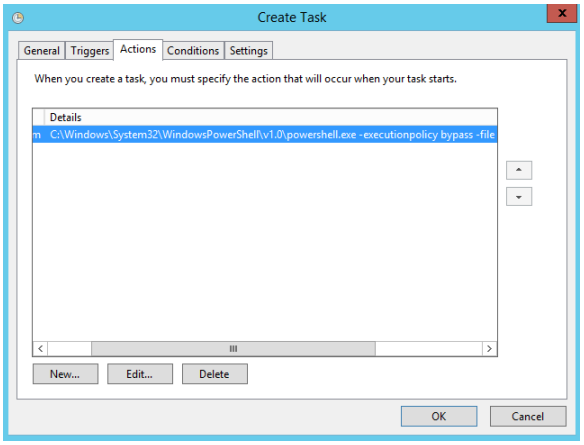


Spécifier comme programme à exécuter :

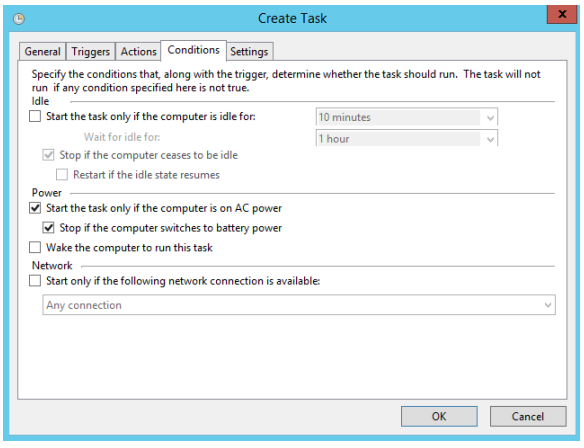
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -executionpolicy bypass -file C:_adm\BackOffice\BackOffice.ps1



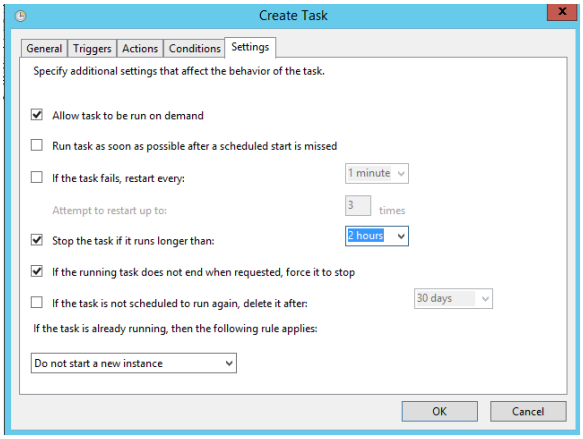
Vous devez obtenir le résultat de droite.



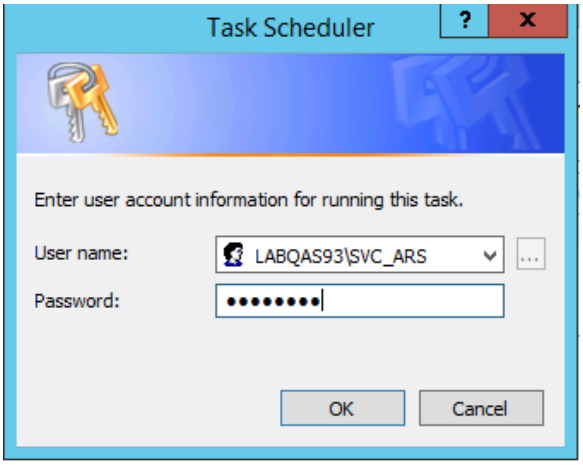
Laisser les options par défaut dans l'onglet *Conditions*.



Cocher la case *Stop the task if it runs longer than: 2 hours*



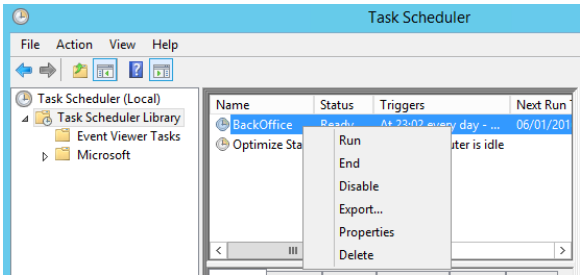
Entrer le mot de passe du compte qui exécutera cette tâche (administrateur du serveur Azure Active Directory Sync).



Créer un utilisateur appelé Mathieu BERTRAND avec les attributs suivants renseignés :

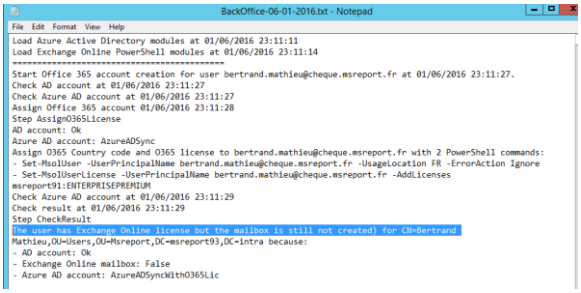
- UserPrincipalName: *mathieu.bertrand@cheque.msreport.fr*
- Mail: *mathieu.bertrand@cheque.msreport.fr*
- MailNickName: *mathieu.bertrand*
- ProxyAddresses: *SMTP:mathieu.bertrand@cheque.msreport.fr*

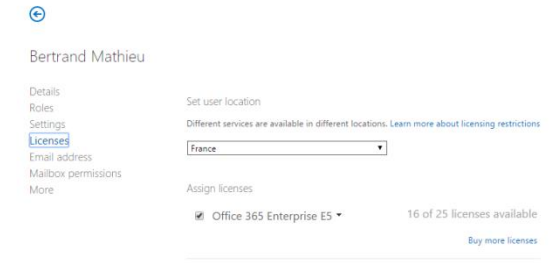
Exécuter la tâche.

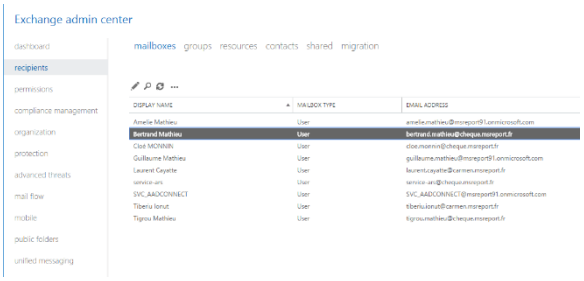


Contrôler le résultat à l'aide du fichier de log *C:_adm\BackOffice\Logs\BackOffice-XXXX.txt.*

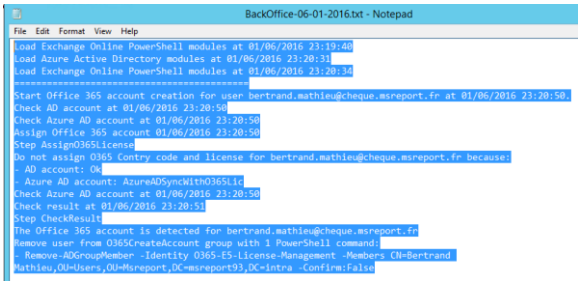
Dans cet exemple, le script a assigné une licence Office 365 correctement mais la boîte aux lettres Exchange Online n'a pas encore été créée.







Lors la seconde exécution du BackOffice (15 minutes après), la boîte aux lettres Exchange est détectée et l'utilisateur est alors supprimé du groupe utilisé par cette solution.



3.3.3 Code source de la solution

```
## ============================================================================= ##
# Writen by Guillaume MATHIEU V2.0 the 01/06/2016
# This script allow to assign Office 365 license if the user is member of a group.
## ============================================================================= ##

# Global Variables
# Replace global variables by your information.
$global:MessagingSuffix = @("@carmen.msreport.fr","@cheque.msreport.fr")
$Global:LogAction = "C:\_adm\BackOffice\Logs\BackOffice-" + (Get-date -Format dd-MM-yyyy) + ".txt"
$Global:O365AccountSkuID = "msreport91:ENTERPRISEPREMIUM"
$Global:o365ManagementGroup = "O365-E5-License-Management"
$Global:FileInfo = "C:\_adm\BackOffice\O365.csv"

# ---------------------------------------------------- #
# This function allows to check the user account
# UserPrincipalName and email msut not contains * character.
# C attribute (country code) must not be empty.
# ---------------------------------------------------- #
Function AnalyseADAccount($User)
{
```

```
echo "Check AD account at $([string](Get-Date))" | Out-File -FilePath $LogAction -Append -Encoding UTF8
# Check UserPrincipalName
$MailDomFound = $False
Foreach ($MailDom in $MessagingSuffix)
{if ($User.UserPrincipalName -match $MailDom -and $User.UserPrincipalName -ne "*"){$MailDomFound = $True}}
If ($MailDomFound -eq $False){$UserPrincipalNameError = "UserPrincipalName is invalid. "}

# Check Email
$MailDomFound = $False
Foreach ($MailDom in $MessagingSuffix)
{if ($User.Mail -match $MailDom -and $User.Mail -ne "*"){$MailDomFound = $True}}
If ($MailDomFound -eq $False){$EmailError = "Email is invalid. "}

# Check country code
If (!($User.Country))
{$User.CheckADAccount = $CountryCodeError = "Country code is invalid. "}

# Generate result
if ($SamAccountNameError -ne $Null -or $UserPrincipalNameError -ne $Null -or $EmailError -ne $Null -or $CountryCodeError -ne $Null)
{$User.CheckADAccount = $SamAccountNameError + $UserPrincipalNameError + $EmailError + $CountryCodeError}
else
{$User.CheckADAccount = "Ok"}
Return
}

# ------------------------------------------------------ #
# This function allows to check the Azure Active Directory
# account (Msoluser)
# The script will only assign a Office 365 license if the
# MsolUser is synchronised and has not Office 365 license
# ------------------------------------------------------ #
Function CheckAzureADAccount($User)
{
echo "Check Azure AD account at $([string](Get-Date))" | Out-File -FilePath $LogAction -Append -Encoding UTF8
# Check if Azure AD account is synchronised
$TestMsolUser = Get-MsolUser -UserPrincipalName $User.UserPrincipalName -ErrorAction Ignore
if ($TestMsolUser.LastDirSyncTime -ne $Null -and $TestMsolUser.IsLicensed -eq $False){$User.CheckAzureADAccount = "AzureADSync"}
elseif ($TestMsolUser.LastDirSyncTime -eq $Null -and $TestMsolUser.IsLicensed -eq $False){$User.CheckAzureADAccount = "AzureADNoSync"}
```

```
 elseif ($TestMsolUser.LastDirSyncTime -ne $Null -and $TestMsolUser.IsLicensed -eq
$True){$User.CheckAzureADAccount = "AzureADSyncWithO365Lic"}
 elseif ($TestMsolUser.LastDirSyncTime -eq $Null -and $TestMsolUser.IsLicensed -eq
$True){$User.CheckAzureADAccount = "AzureADNoSyncWithO365Lic"}
 else {$User.CheckAzureADAccount = "NoAzureADAccount"}
 Return
}

# ----------------------------------------------------- #
# This function allows to assign the Office 365 license.
# Only if MsolUser is synchronized.
# Only if the Msoluser has no Office 365 license.
# ----------------------------------------------------- #
Function AssignO365License($User)
{
 echo "Assign Office 365 account $([string](Get-Date))" | Out-File -FilePath $LogAction -Append -Encoding UTF8
 # Assign Office 365 country code and license if user is valided and is synchronized to Azure Active Directory and
has no Office 365 license
 if ($User.CheckADAccount -eq "Ok" -and $User.CheckAzureADAccount -eq "AzureADSync")
 {

  # Build O365 license
  $O365LicenseBuild = (Get-MsolAccountSku | where {$_.AccountSkuId -eq $O365AccountSkuID}).AccountSkuId

  # Write PowerShell commands executed to log file
  echo "Step AssignO365License" | Out-File -FilePath $LogAction -Append -Encoding UTF8
  echo "AD account: $($User.CheckADAccount)" | Out-File -FilePath $LogAction -Append -Encoding UTF8
  echo "Azure AD account: $($User.CheckAzureADAccount)" | Out-File -FilePath $LogAction -Append -Encoding
UTF8
  echo "Assign O365 Country code and O365 license to $($User.UserPrincipalName) with 2 PowerShell
commands:" | Out-File -FilePath $LogAction -Append -Encoding UTF8
  echo "- Set-MsolUser -UserPrincipalName $($User.UserPrincipalName) -UsageLocation $($User.Country) -
ErrorAction Ignore" | Out-File -FilePath $LogAction -Append -Encoding UTF8
  echo "- Set-MsolUserLicense -UserPrincipalName $($User.UserPrincipalName) -AddLicenses
$O365LicenseBuild" | Out-File -FilePath $LogAction -Append -Encoding UTF8

  # Assign Office 365 country code
  Try {Set-MsolUser -UserPrincipalName $user.UserPrincipalName -UsageLocation $User.Country -ErrorAction
Ignore}
  Catch{Echo "The Error $($_.Exception.Message) occurs during assigning Country code to MsolUser for
$($User.UserPrincipalName) at $([string](Get-Date))" | Out-File -FilePath $LogAction -Append -Encoding UTF8}

  # Assign a Office 365 Plan E1 license
  Try {Set-MsolUserLicense -UserPrincipalName $User.UserPrincipalName -AddLicenses $O365LicenseBuild}
  Catch{Echo "The Error $($_.Exception.Message) occurs during assigning Office 365 license to MsolUser for
$($User.UserPrincipalName) at $([string](Get-Date))" | Out-File -FilePath $LogAction -Append -Encoding UTF8}
```

```
 }
 else
 {
  echo "Step AssignO365License" | Out-File -FilePath $LogAction -Append -Encoding UTF8
  echo "Do not assign O365 Contry code and license for $($User.UserPrincipalName) because:" | Out-File -
FilePath $LogAction -Append -Encoding UTF8
  echo "- AD account: $($User.CheckADAccount)" | Out-File -FilePath $LogAction -Append -Encoding UTF8
  echo "- Azure AD account: $($User.CheckAzureADAccount)" | Out-File -FilePath $LogAction -Append -Encoding
UTF8
 }
}

# ---------------------------------------------------------------- #
# This function will check if the license is properly assigned.
# Check Exchange Online mailbox, license assignment and User account
# Remove the user from the group $o365ManagementGroup if the license
# is properly assigned
# ---------------------------------------------------------------- #
Function CheckResult($User)
{
 echo "Check result at $([string](Get-Date))" | Out-File -FilePath $LogAction -Append -Encoding UTF8
 $CheckExchangeOnlineMailbox = $False
 # If user has Office 365 licenses, remove the user from the group.
 if ($User.CheckADAccount -eq "Ok" -and $User.CheckAzureADAccount -eq "AzureADSyncWithO365Lic")
 {
  # If user has Exchange Online Mailbox
  if ((Get-O365Mailbox -Identity $User.UserPrincipalName) -ne $null -and $o365ManagementGroup)
  {
   $CheckExchangeOnlineMailbox = $True
   # Write log file
   echo "Step CheckResult" | Out-File -FilePath $LogAction -Append -Encoding UTF8
   echo "The Office 365 account is detected for $($User.UserPrincipalName)" | Out-File -FilePath $LogAction -
Append -Encoding UTF8
   echo "Remove user from O365CreateAccount group with 1 PowerShell command:" | Out-File -FilePath
$LogAction -Append -Encoding UTF8
   echo "- Remove-ADGroupMember -Identity $o365ManagementGroup -Members $($User.DistinguishedName)
-Confirm:$False" | Out-File -FilePath $LogAction -Append -Encoding UTF8

   # Run Command: remove from $o365ManagementGroup
   Try{Remove-ADGroupMember -Identity $o365ManagementGroup -Member $user.DistinguishedName -
Confirm:$False}
   Catch{Echo "The Error $($_.Exception.Message) occurs during removing the user $($User.DistinguishedName)
from the group $o365ManagementGroup at $([string](Get-Date))" | Out-File -FilePath $LogAction -Append -
Encoding UTF8}
  }
  else
```

```
 {
  echo "Step CheckResult" | Out-File -FilePath $LogAction -Append -Encoding UTF8
  echo "The user has Exchange Online license but the mailbox is still not created) for
$($User.DistinguishedName) because:" | Out-File -FilePath $LogAction -Append -Encoding UTF8
  echo "- AD account: $($User.CheckADAccount)" | Out-File -FilePath $LogAction -Append -Encoding UTF8
  echo "- Exchange Online mailbox: $CheckExchangeOnlineMailbox" | Out-File -FilePath $LogAction -Append -
Encoding UTF8
  echo "- Azure AD account: $($User.CheckAzureADAccount)" | Out-File -FilePath $LogAction -Append -Encoding
UTF8
 }
}
else
{
 echo "Step CheckResult" | Out-File -FilePath $LogAction -Append -Encoding UTF8
 echo "The Office 365 account is not created properly (perhaps Dirsync synchronization is required...) for
$($User.DistinguishedName) because:" | Out-File -FilePath $LogAction -Append -Encoding UTF8
 echo "- AD account: $($User.CheckADAccount)" | Out-File -FilePath $LogAction -Append -Encoding UTF8
 echo "- Exchange Online mailbox: $CheckExchangeOnlineMailbox" | Out-File -FilePath $LogAction -Append -
Encoding UTF8
 echo "- Azure AD account: $($User.CheckAzureADAccount)" | Out-File -FilePath $LogAction -Append -Encoding
UTF8
}
}

# Generate Credentail based on CSV file
$Info = Import-Csv -Path $FileInfo -Delimiter ";" -Encoding UTF8
try{$Cred = New-Object -TypeName System.Management.Automation.PSCredential -argumentList
$Info.Login,(ConvertTo-SecureString -string $Info.Password)}
catch
{
 echo "Exit. Unable to generate $Credential at $([string](Get-Date))" | Out-File -FilePath $LogAction -Append -
Encoding UTF8
 Exit
}

# Load Azure Active Directory module
echo "Load Azure Active Directory modules at $([string](Get-Date))" | Out-File -FilePath $LogAction -Append -
Encoding UTF8
$Info = Import-Csv -Path $FileInfo -Delimiter ";"
Import-Module MsOnline
Try{Connect-MsolService -Credential $Cred -ErrorAction Ignore}
Catch
{
 echo "Exit. Unable to connect to Azure Active Directory at $([string](Get-Date))" | Out-File -FilePath $LogAction
-Append -Encoding UTF8
 Exit
```

```
}

# Load Active Directory module
Try{Import-Module ActiveDirectory}
Catch
{
 echo "Exit. Unable to load Active Directory PowerShell module at $([string](Get-Date))" | Out-File -FilePath $LogAction -Append -Encoding UTF8
 Exit
}

# Connect to Exchange Online (configure Prefix Office365)
echo "Load Exchange Online PowerShell modules at $([string](Get-Date))" | Out-File -FilePath $LogAction -Append -Encoding UTF8
$Option3 = New-PSSessionOption -IdleTimeout 36000000
Try
{Import-PSSession (New-PSSession -ConfigurationName "Microsoft.Exchange" -ConnectionUri "https://outlook.office365.com/powershell-liveid/" -Credential $cred -Authentication "Basic" -AllowRedirection -Name "ExchangeOnlineBackOffice" -SessionOption $Option3) -AllowClobber:$True -Prefix O365}
Catch
{
 Catch
{
 echo "Exit. Unable to connect to Exchange Online at $([string](Get-Date))" | Out-File -FilePath $LogAction -Append -Encoding UTF8
 Exit
}

 Exit
}

## Create Office 365 account
$base = Get-ADGroup -Identity $o365ManagementGroup | Get-ADGroupMember | Get-ADUser -Properties *
$base | Add-Member -MemberType Noteproperty -Name "CheckADAccount" -value "Ok" -Force
$base | Add-Member -MemberType Noteproperty -Name "CheckAzureADAccount" -value "NoAzureADSync" -Force

foreach ($user in $Base)
{
 echo "==========================================" | Out-File -FilePath $LogAction -Append -Encoding UTF8
 echo "Start Office 365 account creation for user $($User.UserPrincipalName) at $([string](Get-Date))." | Out-File -FilePath $LogAction -Append -Encoding UTF8

 # Check AD account
 AnalyseADAccount($User)
```

```
# Check Azure AD account
CheckAzureADAccount($User)

# Assign Office 365 license and remove user from the group
AssignO365License($User)

# Check Azure AD account
CheckAzureADAccount($User)

# Check result
CheckResult($User)

# Create empty line in log file.
echo "" | Out-File -FilePath $LogAction -Append -Encoding UTF8
echo "" | Out-File -FilePath $LogAction -Append -Encoding UTF8
echo "" | Out-File -FilePath $LogAction -Append -Encoding UTF8
}

## Disconnect Exchange Online and Exchange On-Premise Remote PowerShell sessions
Get-PSSession -Name ExchangeOnlineBackOffice -ErrorAction Ignore | Remove-PSSession
```

4 Déployer Office 365 ProPlus (en version 2013 ou 2016)

4.1 Présentation d'Office ProPlus 2016

Office 365 ProPlus est une version spéciale d'Office Professionnel. Microsoft met à disposition sur le Tenant Office 365 (à la date du 1 septembre 2016) 2 versions :

- Une version basée sur Office 2013.
- Une version basée sur Office 2016.

Il est très fortement recommandé de déployer Office 2016. Office 365 ProPlus en génération 2016 contient les programmes suivants : *Access*, *Excel*, *OneDrive For Business*, *OneNote*, *Outlook*, *PowerPoint*, *Publisher*, *Skype for Buisines* et *Word*.

Elle se déploie aussi via une nouvelle méthode appelée *Click to Run* qui permet d'utiliser les applications Office alors que la solution est en cours de déploiement.

Office 365 ProPlus 2016 peut être installé sur une station de travail Windows ou Apple (Mac).

Overview

Resources for Click-to-Run for Office 365 products are packaged similarly to the way standard Office 2013 Windows Installer (MSI) resources are organized. Language-neutral product resources are packaged into a single file that contains all the neutral resources. Language-specific resources are packaged into language-specific files such as en-us for English (United States) resources.

If you purchased an Office 365 subscription, you can use it to install Office in multiple languages. You do not have to buy a Language Pack. If your organization allows it, users can install Office 365 ProPlus languages directly from the Office 365 portal. When users install Office from the **software** page, they select a language from the **Language** drop-down box.

In managed enterprise environments, end-users may not have permission to install software from the Office 365 portal. If you are configuring an on-premises deployment of Office 365 Click-to-Run applications for users in your organization, you can use the Office Deployment Tool and a custom Configuration.xml file to install Click-to-Run in multiple languages.

Note:

The Language elements that you specify in the Config.xml file for Click-to-Run determine which languages will be installed. Administrators must specify the languages they want to install. The first language determines the Shell UI language. The Shell UI is the language that is used to display shortcuts, right-click context menus, and tooltips.
If you decide that you want to change the Shell UI language after an initial installation, you have to uninstall Click-to-Run and reinstall it. Add the language that you want to set for the Shell UI as the first language in the custom Configuration.xml file.

Une licence Office 365 Plan E3 ou Office 365 Plan E5 est requise pour activer Office 365 ProPlus. Il n'est pas possible d'activer cette version avec un numéro de série.

https://support.office.com/en-us/article/Unlicensed-Product-errors-in-Office-0d23d3c0-c19c-4b2f-9845-5344fedc4380?ui=en-US&rs=en-US&ad=US

Office 365 ProPlus doit s'activer au moins tous les 30 jours comme expliqué dans l'article https://technet.microsoft.com/en-us/library/gg982959.aspx. Dans le cas contraire, Office 365 passe en mode fonctionnalité réduit. Il n'est alors plus possible de modifier ou créer un document (uniquement lire et imprimer).

Activating Office 365 ProPlus

As part of the installation process, Office 365 ProPlus communicates with the Office Licensing Service and the Activation and Validation Service to obtain and activate a product key. Each day, or each time the user logs on to their computer, the computer connects to the Activation and Validation Service to verify the license status and extend the product key. As long as the computer can connect to the Internet at least once every 30 days, Office remains fully functional. If the computer goes offline for more than 30 days, Office enters reduced functionality mode until the next time a connection can be made. To get Office fully functional again, usually a user can simply connect to the Internet and let the Activation and Validation Service reactivate the installation.

Office 365 ProPlus peut être installé sur 5 périphériques avec la même licence.
https://technet.microsoft.com/en-us/library/gg702619.aspx

Licensing differences

- Office 365 ProPlus is offered as a monthly subscription. If you cancel your subscription, Office 365 ProPlus goes into reduced functionality mode. In reduced functionality mode, users can open and view existing Office files, but users can't use most of the other features of Office 365 ProPlus. For more information, see Overview of licensing and activation in Office 365 ProPlus.
- To use Office 365 ProPlus, a user must have an Office 365 account and have been assigned a license. If you, as the Office 365 administrator for your organization, remove a user's license or account, the user's installations of Office 365 ProPlus go into reduced functionality mode.
- Even though users don't need to be connected to the Internet all the time to use Office 365 ProPlus, users must connect to the Internet at least once every 30 days. This is so that the status of their Office 365 subscriptions can be checked. If users don't connect within 30 days, Office 365 ProPlus goes into reduced functionality mode. After users connect to the Internet and their subscription status is verified, all the features of Office 365 ProPlus are available again.
- Users can install Office 365 ProPlus on up to five different computers with a single Office 365 license. For example, a user can have Office 365 ProPlus installed on a computer in the office, on a laptop to use when traveling, and on a home computer.

Office 365 ProPlus peut être déployé pour supporter plusieurs langues d'installation. La première langue est celle du package d'installation.

Il est impossible d'installer une version d'Office ProPlus 32 bits si vous disposez d'un composant Office 64 bits (Visio, Project…) comme expliqué dans cet article https://support.microsoft.com/en-us/kb/2745026

Il est parfois impossible de désinstaller Office ProPlus. Une procédure pas à pas est fournie par Microsoft :
https://support.office.com/en-us/article/Uninstall-Office-2013-Office-2016-or-Office-365-from-a-Windows-computer-9dd49b83-264a-477a-8fcc-2fdf5dbf61d8?ui=en-US&rs=en-US&ad=US

4.2 OneDrive For Business, un composant à déployer de manière spécifique

Il existe deux versions du produit *OneDrive* :

- La version orientée « grand public » qui se base sur un compte Microsoft Live.
- La version intégrée dans Office 365 (orientée pour les entreprises) qui s'appuie sur un compte Azure Active Directory et la technologie SharePoint.

Comme expliquée dans l'article ci-dessous, le client OneDrive (dernière version) fonctionne maintenant avec la solution « *grand public*» et la solution orientée entreprise.

https://support.office.com/en-us/article/Get-started-with-the-new-OneDrive-sync-client-in-Windows-615391c4-2bd3-4aae-a42a-858262e42a49?ui=en-US&rs=en-US&ad=US

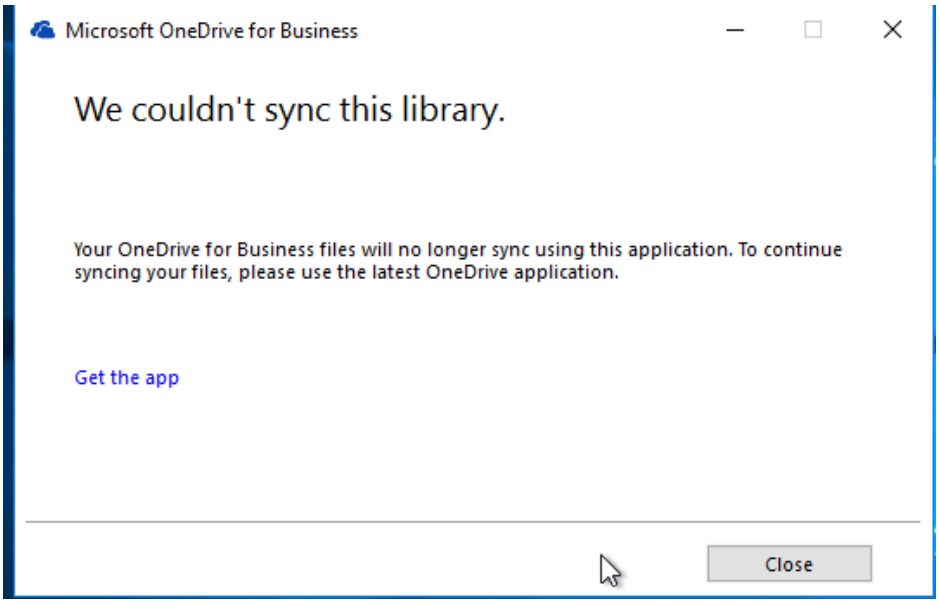
The new OneDrive sync client lets you connect and sync files from your OneDrive for Business. You can add a work or school account to the new OneDrive sync client and sync all your files to your computer.

NOTES:

- The new OneDrive sync client now supports Windows 10, Windows 8.1, Windows 8, and Windows 7. The new OneDrive sync client doesn't yet support syncing site libraries or on-premises instances of OneDrive for Business (when your organization doesn't subscribe to an Office 365 business plan).
- The new OneDrive sync client also supports real-time co-authoring and sharing documents from Office apps when you're using Office 2016 (Click-to-Run version 16.0.6741.2027 or later). Integration with the downloadable MSI version of Office 2016 is coming later this year. For more information about installing Office 365, see Install Office on your PC or Mac.

Windows 10 dispose de base du client OneDrive. Il est recommandé de le mettre à jour à la dernière version : https://support.office.com/en-US/article/Turn-off-or-uninstall-OneDrive-f32a17ce-3336-40fe-9c38-6efb09f944b0?ui=en-US&rs=en-US&ad=US

Office 365 ProPlus (version 2013 ou 2016) intègre toujours pour le moment l'ancien client de synchronisation OneDrive For Business qui va être déprécié prochainement. Le client de synchronisation ne fonctionne déjà plus pour le Tenant Office 365 de moins de 250 personnes). Si on essaie de synchroniser son espace OneDrive For Business, l'application *OneDrive for Business* déployée avec Office 2016 va afficher ce message : *Your OneDrive for Business files will no longer sync using this application. To continue syncing your files, please use the latest OneDrive application.*



Ce client n'est en effet plus utilisable pour les sociétés de moins de 250 utilisateurs et sera prochainement déprécié pour tous les clients. Il est donc nécessaire de déployer un package Office ProPlus sans ce client et de déployer manuellement le nouveau client appelé *OneDrive For Business Next Generation Sync Client.*

Extrait de l'article https://support.office.com/en-us/article/Transition-from-the-previous-OneDrive-for-Business-sync-client-4100df3a-0c96-464f-b0a8-c20de34da6fa

Beginning in May 2016, Office 365 customers with fewer than 250 Office 365 licenses will be required to use the OneDrive for Business Next Generation Sync Client to sync OneDrive for Business files. This requirement will be rolled out between May 2016 and July 31, 2016 and will not apply to on-premises customers or customers with more than 250 Office 365 licenses.

Le nouveau client de synchronisation OneDrive est beaucoup plus stable que l'ancien client *OneDrive for Business*. On notera que le nouveau client dispose d'une option qui permet de configurer Office 2016 pour enregistrer les données dans le cache *OneDrive For Business* de la station de travail et non plus directement sur les serveurs de Microsoft :

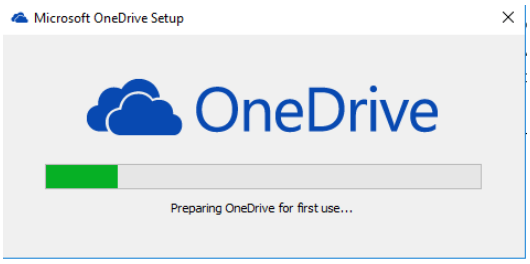
https://support.office.com/en-us/article/Use-Office-2016-to-sync-Office-files-that-I-open-8a409b0c-ebe1-4bfa-a08e-998389a9d823?ui=en-US&rs=en-US&ad=US

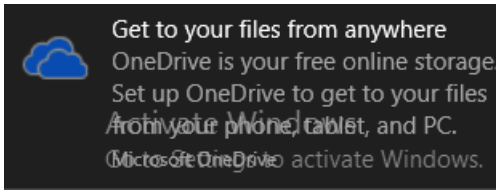
Les prochaines versions d'Office 365 ProPlus 2016 intégreront uniquement le nouveau client.

La procédure ci-dessous montre comment configurer le client *OneDrive For Business Next Generation Sync Client.*

Télécharger le nouveau client *OneDrive For Business Next Generation Sync Client*.

https://onedrive.live.com/about/fr-fr/update/

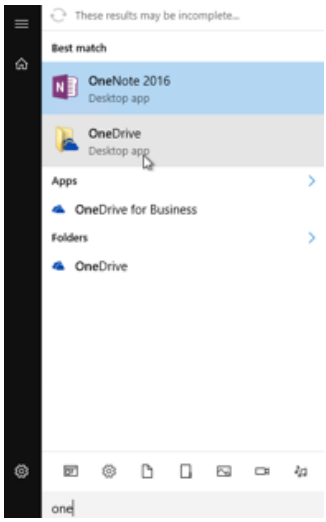


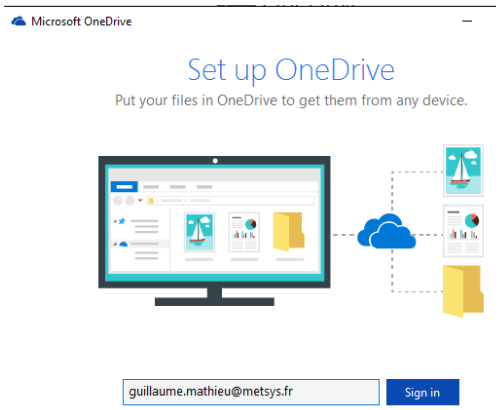


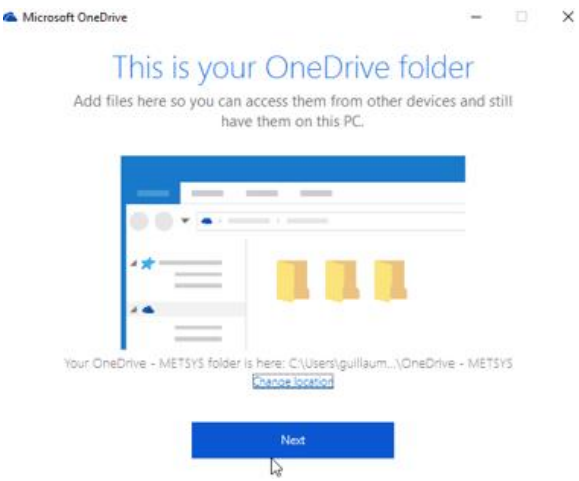
Le processus correspondant à l'ancien OneDrive for Business s'appelle *Groove.exe*. Le nouveau s'appelle *OneDrive.exe*.

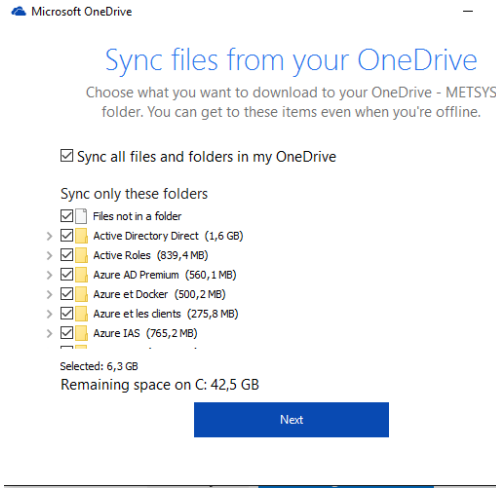
En configuration par défaut, on se retrouve avec 2 clients OneDrive différents sur la machine Windows 10 :

Il ne faut plus utiliser le lien *OneDrive for Business* (groove.exe). Pour cela, il sera nécessaire de personnaliser le package *Office 365 ProPLus 2016* pour ne pas inclure l'ancien client OneDrive For Business.

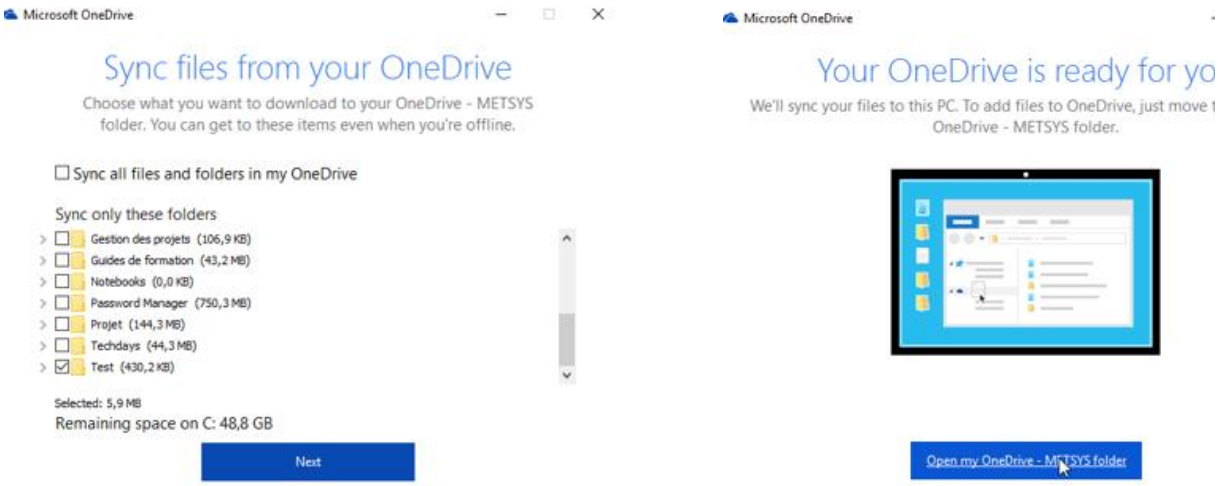




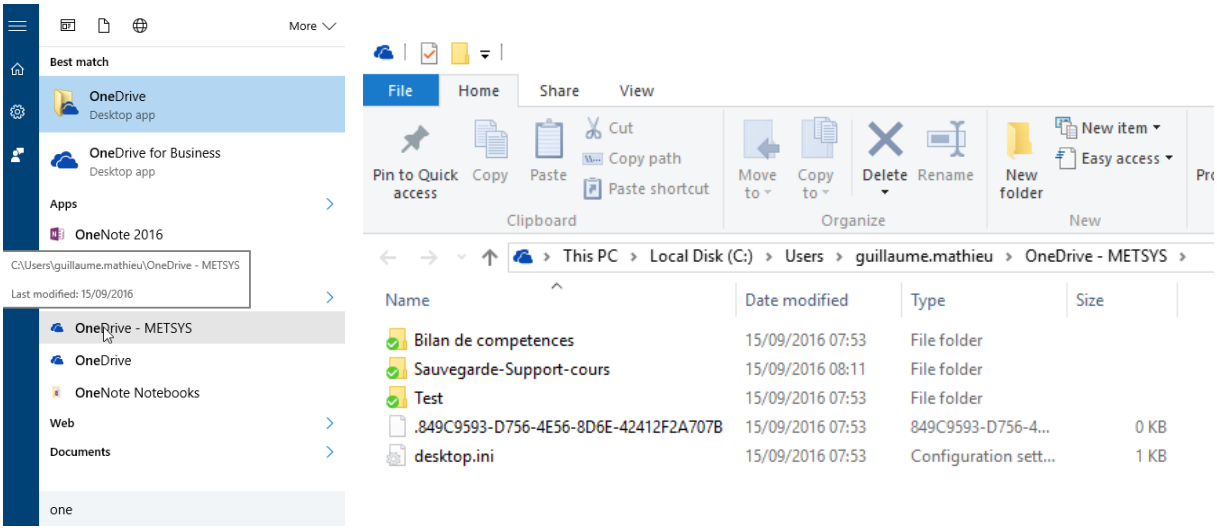




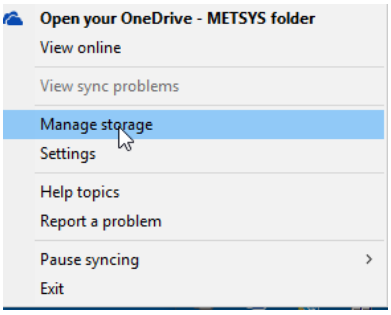
On peut choisir quel dossier on va synchroniser.

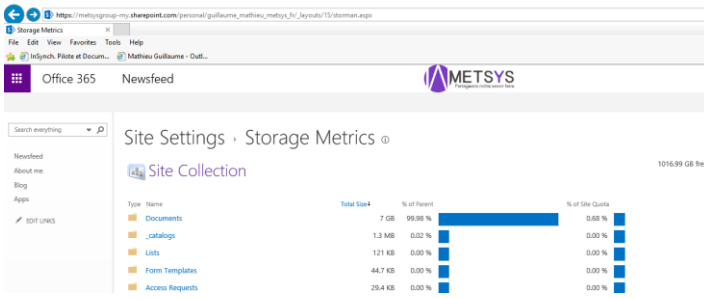


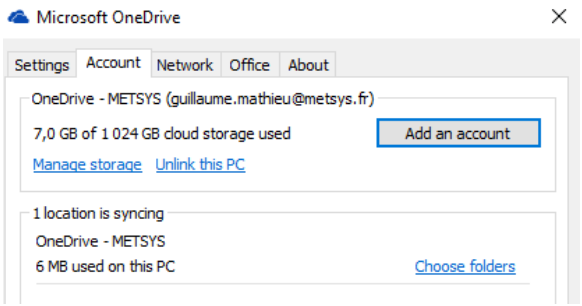
L'icône OneDrive – *LE-NOM-DU-TENANT* s'affiche ensuite.

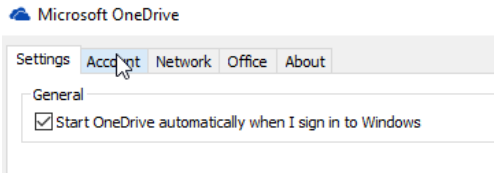


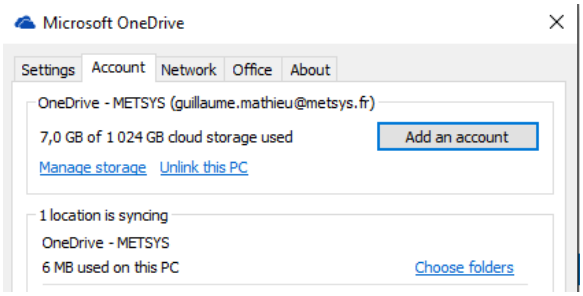
Il est possible d'accéder à la configuration avancée du client *OneDrive for Business Next Generation* depuis la barre des tâches (en bas à droite).

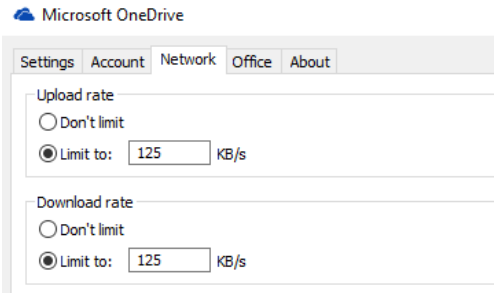


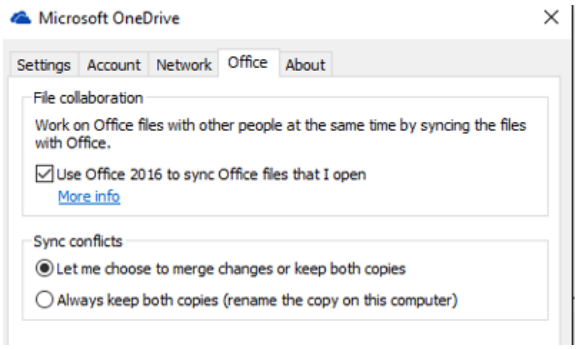




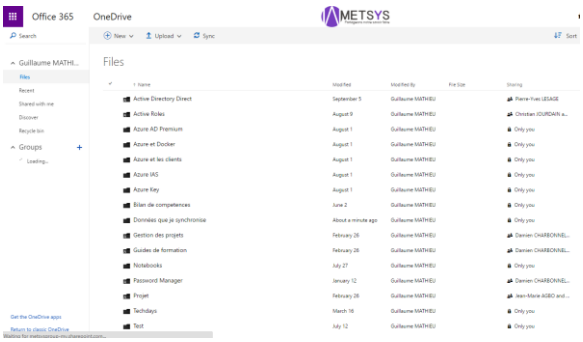


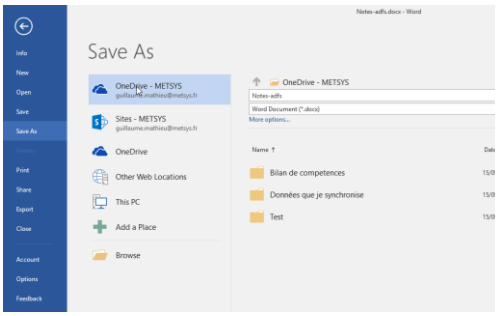






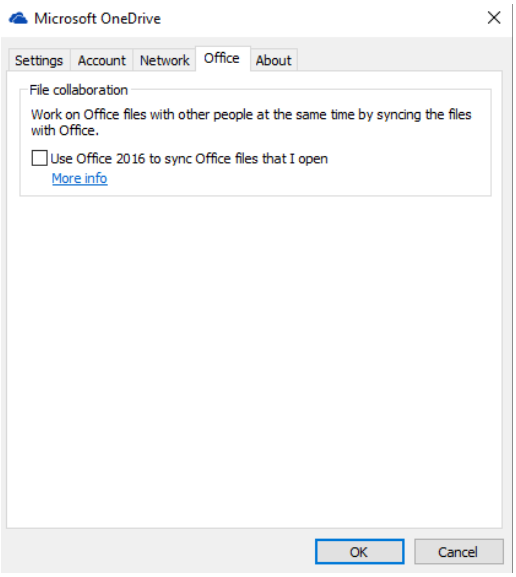
Avec les réglages par défaut, les clients lourds comme *Word*, *Excel* enregistrent les données dans le cache du client OneDrive par défaut. Seuls les dossiers synchronisés sont alors visibles.

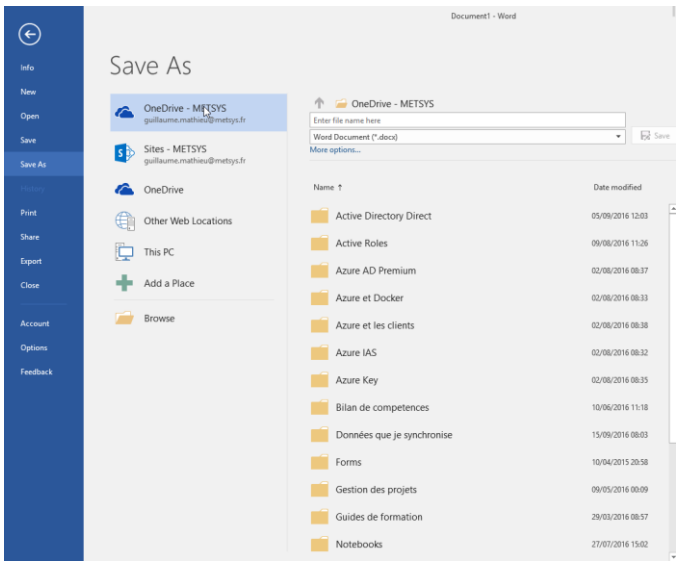




Par défaut le lien vers le cache hors connexion est *C:\Users\%username%\OneDrive – METSYS.*

Si je désactive l'option *Use Office 2016 to sync Office files that I have open*, je me connecte directement au site web OneDrive For Business en ligne et non à mon cache OneDrive For Business locale.

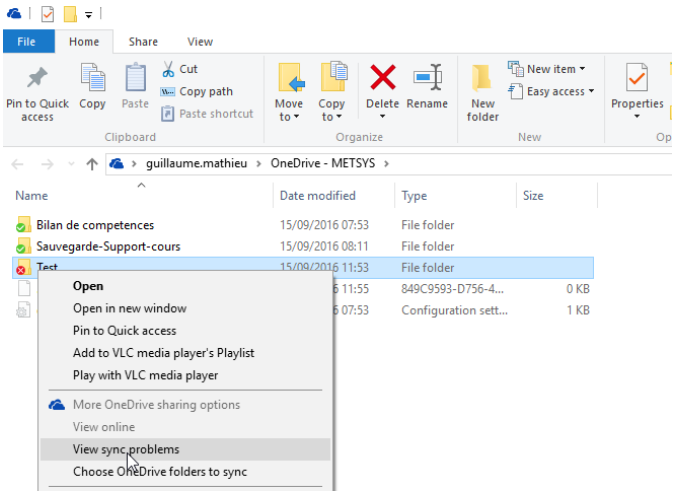


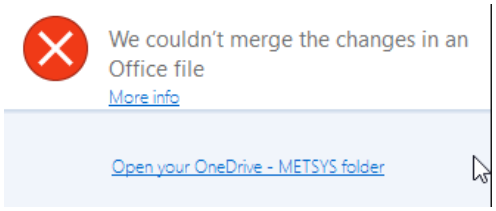


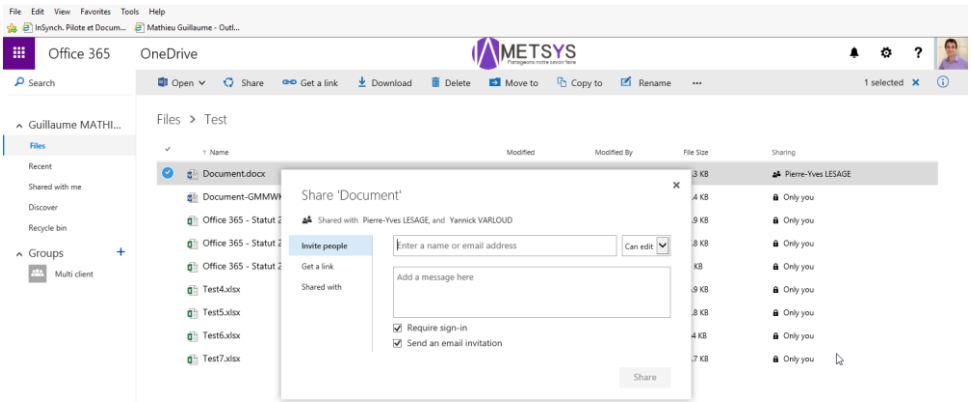
Gestion des conflits dans OneDrive

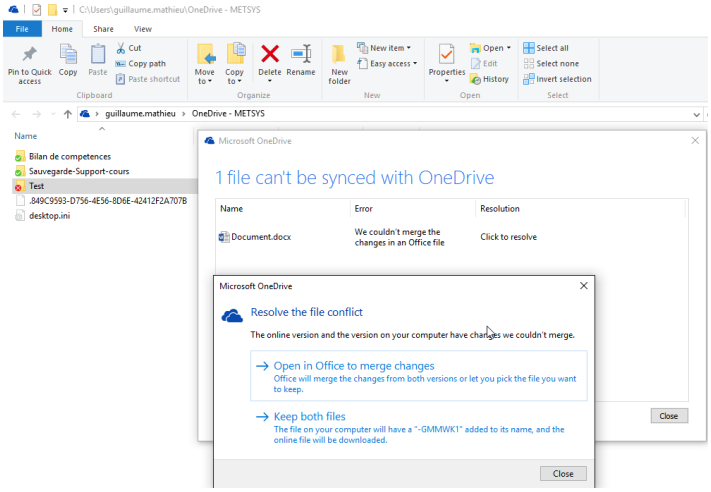
Pour générer un conflit, il suffit d'arrêter le synchronisation *OneDrive For Business Next Generation Sync Client* puis modifier la version en ligne. Désactiver la carte réseau et modifier ensuite la version du cache local. Cet incident peut se produire :

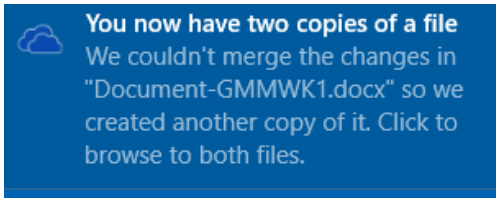
- Si un utilisateur travaille dans le train et a un problème avec son client *OneDrive For Business Next Generation Sync Client.*
- Si l'utilisateur a partagé son document avec l'utilisateur B. A modifie le document hors connexion. B le modifie en ligne. Quand A se reconnecte au réseau, il y a conflit.

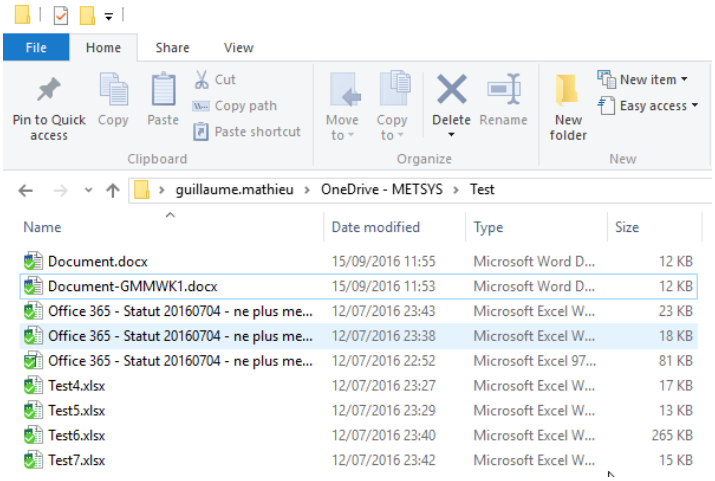


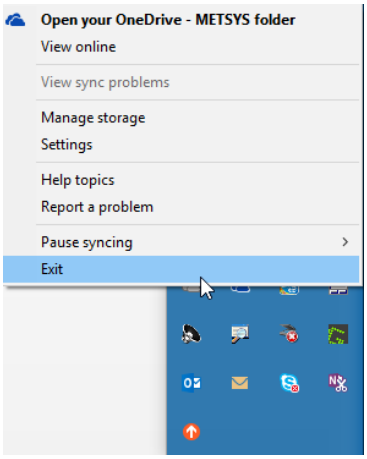


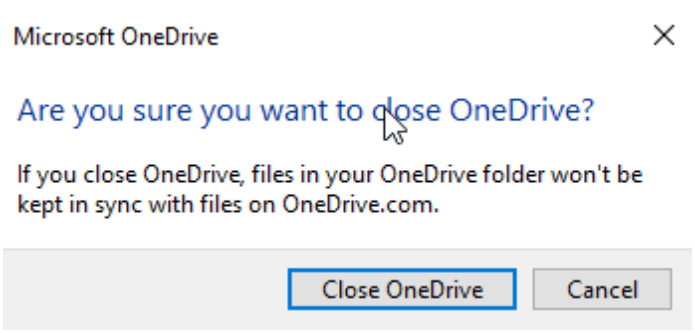


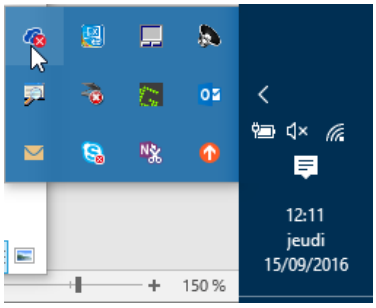




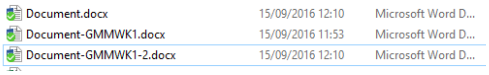








Si on avait déjà 2 fichiers (premier conflit), un troisième fichier est créé



Configuration par GPO du client One drive for business

Il est possible de configurer le client par GPO, il faut récupérer la dernière version à cette adresse :

https://support.office.com/en-us/article/Administrative-settings-for-the-new-OneDrive-sync-client-0ecb2cf5-8882-42b3-a6e9-be6bda30899c?ui=en-US&rs=en-US&ad=US

4.3 Installer Office 365 ProPlus

La procédure ci-dessous est basée sur les articles suivants :

http://technet.microsoft.com/en-us/library/jj219422.aspx

https://technet.microsoft.com/en-us/library/jj219426.aspx

http://aka.ms/ODT

https://support.microsoft.com/en-us/kb/2842297

https://technet.microsoft.com/en-us/library/mt455210.aspx

Les MVA ci-dessous traitent aussi du déploiement d'Office 365 ProPlus

https://mva.microsoft.com/fr-fr/training-courses/office-365-comment-dployer-le-client-office-fr-12617

https://mva.microsoft.com/en-us/training-courses/office-365-proplus-deployment-for-it-pros-8278?l=NWCZLZWy_2704984382

La première étape est de déterminer :

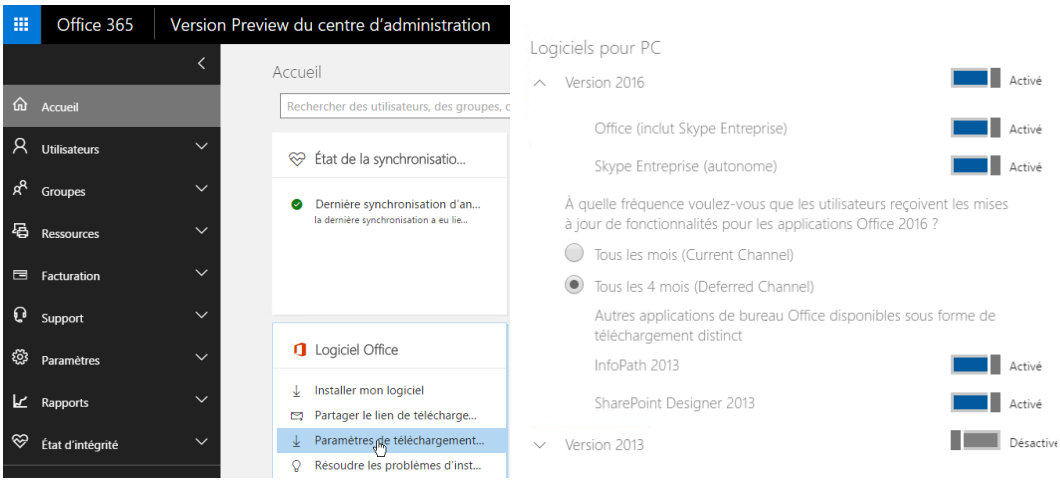
- Si on déploie Office 365 ProPlus en version 2011 (Mac uniquement), 2013 (PC uniquement) ou 2016 (recommandée).
- Si on déploie une version 32 bits (recommandée) ou 64 bits.
- La langue de déploiement.
- Les composants de la suite Office 365 ProPlus à déployer. Une société peut souhaiter ne pas déployer le client OneDrive For Business.
- Si on masque ou pas OneDrive (version grand public).

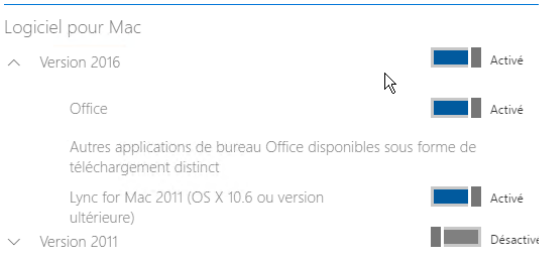
Il sera nécessaire de créer un package séparé pour chaque combinaison de ces 3 facteurs.

La seconde étape est de configurer le package Office 365 ProPlus depuis le tenant Office 365. Il faut aller dans *Accueil | Paramètres de téléchargement*.

Il est possible via cet emplacement de définir :

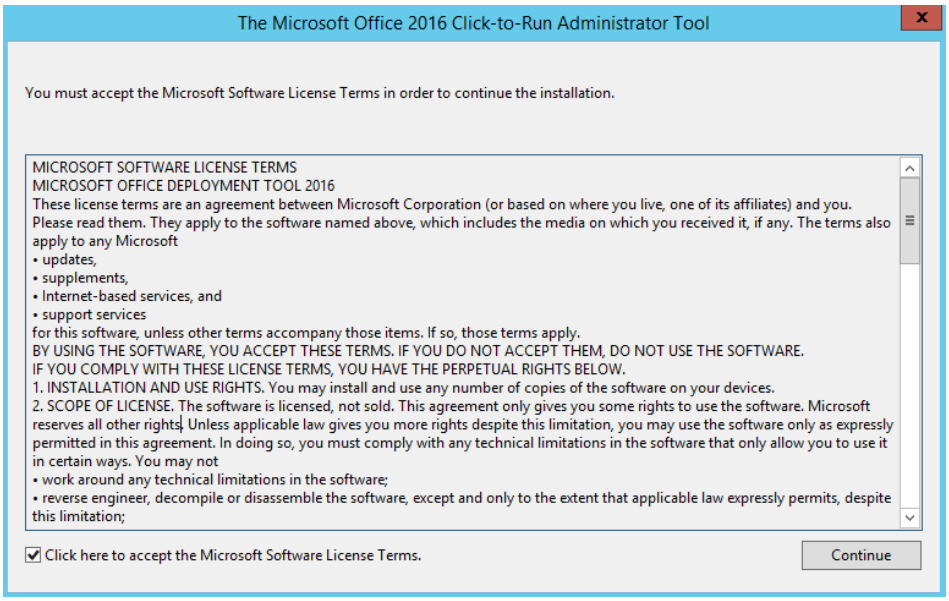
- Si l'on peut télécharger Office 2016 ou Office 2013 sur PC.
- Si l'on peut télécharger et installer Office 2016 ou Office 2011 pour station de travail Apple (Mac).
- Si l'on souhaite mettre à disposition de l'utilisateur le client Skype Entreprise uniquement (PC et Mac). Cette option permet aux utilisateurs disposant de licence Office 365 plan E1 de télécharger le client Skype for Business. En effet le client web Skype for Business permet uniquement de faire de la messagerie instantanée. C'est pour cette raison que le client lourd Skype for Business est disponible pour les personnes qui disposent d'une licence Office 365 Plan E1.



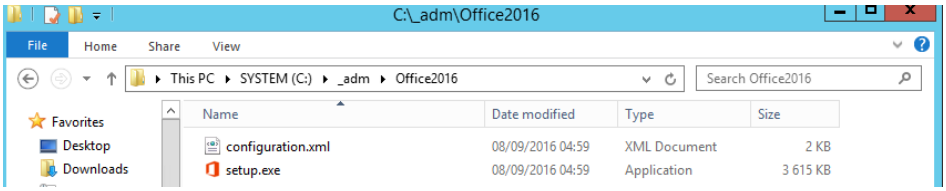


L'étape suivante va consister à télécharger et installer *Microsoft Office 2016 Click to Run Administrator Tool*.

https://www.microsoft.com/en-us/download/confirmation.aspx?id=49117



On obtient alors les fichiers suivants :



On va créer 2 fichiers de configuration :

- Un pour le téléchargement des sources.
- Un pour le paramétrage par défaut du client Office 365 ProPlus. On notera que les options par défaut du client Office 365 ProPlus pourront être surchargées par la suite à l'aide des GPO Office 2016. Les fichiers ADMX et ADML peuvent être téléchargés à l'adresse suivante : https://www.microsoft.com/en-us/download/details.aspx?id=49030

Créer et partager le dossier *C:_adm\OfficeProPlus2016US*. Le compte avec lequel on va générer le package complet doit disposer d'un accès en lecture / écriture à ce partage. Le groupe *Authenticated Users* doit disposer d'un accès en lecture à ce partage.

Créer le fichier *DowloadOfficeProPlus.xml* avec le contenu ci-dessous. Cela va permettre de télécharger la dernière version d'Office 365 ProPlus 2016 à la dernière version vers un dossier partagé en version 32 bits. La package d'installation sera disponible en anglais et en français. On télécharge la dernière version car on a spécifié *Channel="Current"*. Si on souhaitait la dernière version d'il y a 4 mois, il faudrait mettre Channel="*Deferred*".

```
<Configuration>
 <Add SourcePath="\\msexpdc1\Office2016-Deploy" OfficeClientEdition="32" Channel="Current" >
  <Product ID="O365ProPlusRetail" >
   <Language ID="fr-fr"/>
   <Language ID="en-us"/>
  </Product>
 </Add>
</Configuration>
```

Lancer la commande suivante pour télécharger les sources d'Office 2016.

```
Cd c:\_adm\DeployOffice2016
setup.exe /download C:\_adm\DeployOffice2016\DowloadOfficeProPlus.xml
```

Si on télécharge la version *Current*, le numéro de version (à la date du 15/09/2016) est le *16.0.7167.2060* (1,51 Go). Si on télécharge la version *Deferred*, le numéro de version est le *16.0.6741.2063* (1,44 Go).

Il faut ensuite créer un fichier de configuration *Install-OfficeProPlus2016-X32-US.xml qui* va nous permettre de déployer Office 365 ProPlus (version 2016) avec les réglages et les composants que l'on souhaite.

Dans l'exemple ci-dessous, on va déployer la dernière version disponible d'Office 365 ProPlus 2016 (*Channel="Current"*) en version 32 bits en anglais avec une mise à jour des fonctionnalités tous les mois (*Channel="Current")* et avec une interaction complète. L'installation va télécharger les sources d'installation depuis le partage \\serveur1\OfficeProPlus2016US.

On a la possibilité d'exclure certains composants de l'installation : *ID="Access", ID="Excel", ID="Groove", ID="InfoPath", ID="Lync", ID="OneDrive", ID="OneNote", ID="Outlook", ID="PowerPoint", ID="Publisher", ID="SharePointDesigner", ID="Visio"*).

Dans notre exemple, on va exclure *Publisher*, *Access* et *Groove* (ancien client OneDrive for Business) et *OneDrive*.

Les mises à jour seront effectuées via la source d'installation sur le partage *\\msexpdc1\Office2016-Deploy*.

```
<Configuration>
 <Add SourcePath="\\msexpdc1\Office2016-Deploy\" OfficeClientEdition="32" Channel="Current">
  <Product ID="O365ProPlusRetail">
   <Language ID="en-us" />
   <ExcludeApp ID="Publisher" />
   <ExcludeApp ID="Access" />
   <ExcludeApp ID="Groove" />
   <ExcludeApp ID="OneDrive" />
  </Product>
```

```
</Add>
<Updates Enabled="TRUE" UpdatePath="\\msexpdc1\Office2016-Deploy\" Channel="Current" />
<Display Level="Full" AcceptEULA="TRUE" />
<Property Name="AUTOACTIVATE" Value="1" />
<Logging Level="Standard" Path="%temp%" />
<Property Name="PinIconsToTaskbar" Value="TRUE"/>
<Property Name="AUTOACTIVATE" Value="1"/>
</Configuration>
```

Value	Description
SourcePath="\\Server\Share"	Office will be downloaded to "\\server\share" on your network and deployed using installation files at that location.
OfficeClientEdition="32"	Downloads and installs the 32 bit edition of Office.
Channel="Deferred"	After installation, Office will be updated using the Deferred channel.
Product ID="O365ProPlusRetail"	Downloads and installs Office 365 ProPlus.
Language ID="en-us" Language ID="ja-jp"	Downloads and installs English and Japanese versions of Office.
Updates Enabled="TRUE" UpdatePath="\\Server\Share "	After installation, Office checks for updates at "\\server\share" on your network.
Display Level="None" AcceptEULA="TRUE"	When installing Office, no user interface is displayed.
Logging Level="Standard" Path="%temp%"	Log files are stored in the %temp% folder.

Microsoft permet de déployer les produits suivants avec des plans de licence Office 365. La licence Plan E3 / E5 d'Office 365 donne par exemple le droit de déployer l'application avec l'ID *O365ProPlus*.

Il est possible d'acheter des licences Office 365 Visio, Share Point Designer et Project (avec les ID respectifs *VisioProRetail, SPDRetail ProjectProRetail*).

ID attribute (part of Product element)	Defines the ID of the product to download or install.
	
	Required.
		Office 365 Product IDs:
		
		`ID="O365ProPlus"`
		
		`ID="VisioProRetail"`
		
		`ID="ProjectProRetail"`
		
		`ID="SPDRetail"`
		
		For a list of all supported product IDs, see Product IDs that are supported by the Office Deployment Tool for Click-to-Run

On notera que l'*Office Deployement Tool (ODT)* permet aussi de déployer d'autres solutions de la gamme Office (autres qu'Office 365). Extrait de l'article https://support.microsoft.com/en-us/kb/2842297

In addition to these product IDs, the following non-Office 365 product IDs are supported by this tool:

Note For Lync or Skype for Business, see the table that's listed later in this article.

- AccessRetail
- ExcelRetail
- HomeBusinessRetail
- HomeStudentRetail
- InfoPathRetail
- ProfessionalRetail
- O365HomePremRetail
- O365SmallBusPremRetail
- OneNoteRetail
- OutlookRetail
- PowerPointRetail
- ProjectProXVolume
- ProjectStdRetail
- ProjectStdXVolume
- PublisherRetail
- VisioProXVolume
- VisioStdRetail
- VisioStdXVolume
- WordRetail

For managing the Lync or Skype for Business clients, the following table lists the tool version and the correct product ID

La liste des ID ci-dessous correspond aux composants des produits sous licence Office 365 soit Office 365 ProPlus (*O365ProPlus*), Visio (*VisioProRetail*), Project (*ProjectProRetail*) et SharePoint Designer (*SPDRetail*).

ID attribute (part of ExcludeApp element)	Defines the ID of the product that should not be installed.
	
	Required.
		`ID="Access"`
		`ID="Excel"`
		`ID="Groove"`
		`ID="InfoPath"`
		`ID="Lync"`
		`ID="OneDrive"`
		`ID="OneNote"`
		`ID="Outlook"`
		`ID="PowerPoint"`
		`ID="Publisher"`
		`ID="SharePointDesigner"`
		`ID="Visio"`
		`ID="Word"`
		
		For OneDrive for Business, use **Groove**. For Skype for Business, use **Lync**.

L'option C*hannel* est très importante car c'est cette option qui va contrôler comment Office ProPlus va se mettre à jour : https://technet.microsoft.com/en-us/library/mt455210.aspx

Elle va de pair avec l'option *Updates Enabled* que l'on peut positionner à *True* ou *False*. Pour désactiver complètement les mises à jour, il est nécessaire de spécifier la ligne *Updates Enabled="False"*. Dans ce cas l'instruction *Channel* est ignorée. Si cette option n'est pas spécifiée, les mises à jour sont actives par défaut en mode *Deferred* (mise à jour des fonctionnalités tous les 4 mois).

L'option recommandée est de mettre à jour les fonctionnalités d'Office ProPlus (autres que les correctifs de sécurité) tous les 4 mois. Pour cela, il faut sélectionner l'option *Deferred* (option par défaut).

Update channel	Feature updates	Security updates	Non-security updates
Current Channel	Monthly	Monthly	Monthly
Deferred Channel	Every four months	Monthly	Every four months
First Release for Deferred Channel	Every four months	Monthly	Monthly

The first Deferred Channel release will be available approximately four months after the release of Office 2016. After a Deferred Channel release is available, it only gets security updates, if there are any, in the following months. After it's been released, no new features are added to Deferred Channel. The next time you'll receive new features, if there are any, is when the next Deferred Channel release is made available.

A Deferred Channel release is supported for eight months. When a new Deferred Channel release is made available, you can continue to use the Deferred Channel release that you've deployed. But four months later, when another Deferred Channel is released, your original Deferred Channel release is no longer supported and won't get any more security updates.

Pour déployer le package, il faut ensuite lancer la commande suivante (sur une seule ligne) :

\\192.168.1.2\c$_adm\OfficeProPlus2016US\setup.exe /configure
\\192.168.1.2\c$_adm\OfficeProPlus2016US\Install-OfficeProPlus2016-X32-US.xml

L'installation s'exécute alors.

4.4 Désinstaller Office ProPlus

La procédure ci-dessous est basée sur les articles suivants :

http://technet.microsoft.com/en-us/library/jj219422.aspx

https://technet.microsoft.com/en-us/library/jj219426.aspx

http://aka.ms/ODT

https://support.microsoft.com/en-us/kb/2842297

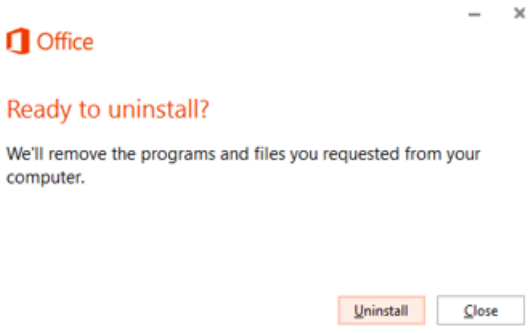
Le principe est identique à la procédure d'installation d'Office ProPlus 2016 sauf que l'on va spécifier dans le fichier XML le paramètre *Remove*.

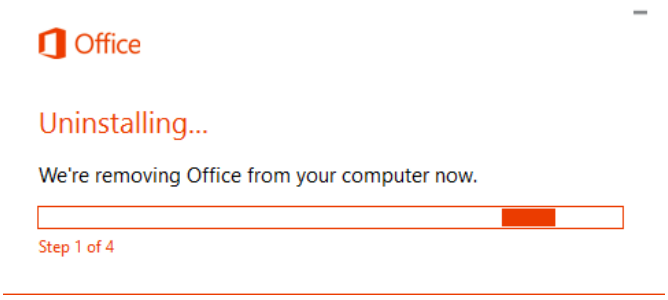
```
<Configuration>
  <Remove SourcePath="\\192.168.1.2\OfficeProPlus2016US" OfficeClientEdition="32">
    <Product ID="O365ProPlusRetail"/>
  </Remove>
</Configuration>
```

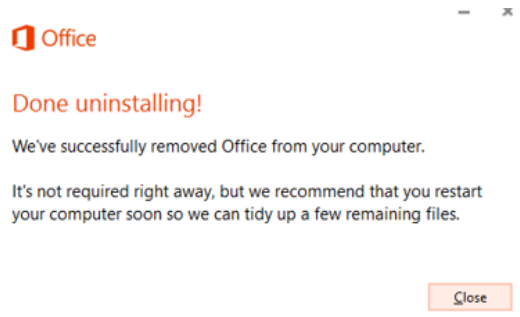
On notera aussi que selon la version d'Office 2016, la suppression par *Ajout / suppression* de logiciels dans le panneau de configuration échoue.

Pour supprimer le package sur une station de travail, il faut lancer la commande suivante (sur une seule ligne) :

\\192.168.1.2\c$_adm\OfficeProPlus2016US\setup.exe /configure
\\192.168.1.2\c$_adm\OfficeProPlus2016US\Uninstall-OfficeProPlus2016-X32-US.xml







5 Le provisionning des comptes Office 365

Les commandes *Enable-Mailbox* et *New-Mailbox* n'existent pas avec Exchange Online (contrairement à Exchange On-Premise). Pour créer une nouvelle boîte aux lettres Exchange Online, on affecte une licence Exchange Online à un utilisateur Azure Active Directory. Tous les plans de licences Office 365 incluent donc de base une licence Azure Active Directory. Le tableau ci-dessous liste les différentes éditions d'Azure Active Directory :

https://azure.microsoft.com/en-us/documentation/articles/active-directory-editions

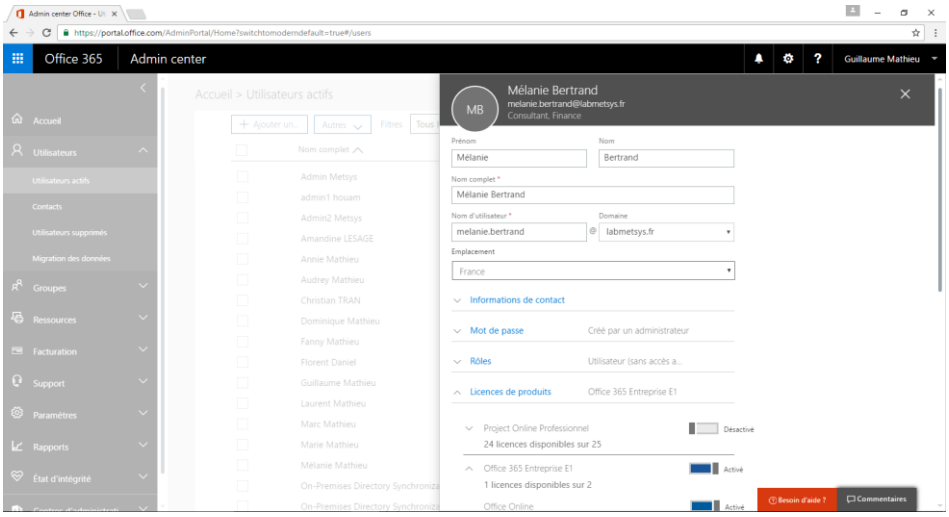
Les éditions d'Azure Active Directory

Fonctionnalités	Free	Basic	Premium P1	Premium P2	Office 365
Commun					
Objets Active Directory	500 000	Illimité	Illimité	Illimité	Illimité
SSO avec les applications SaaS	10 / utilisateur	10 / utilisateur	Illimité	Illimité	10 / utilisateur
Gestion des utilisateurs, provisionning, enregistrement d'appareils	✓	✓	✓	✓	✓
Synchronisation d'annuaire	✓	✓	✓	✓	✓
Modification du mot de passe en self-service pour les utilisateurs cloud	✓	✓	✓	✓	✓
Rapports de sécurité / d'utilisation	3 rapports	3 rapports	Avancés	Avancés	3 rapports
Basic					
Gestion / provisionning des accès basée sur les groupes		✓	✓	✓	
Réinitialisation du mot de passe en self-service pour les utilisateurs cloud		✓	✓	✓	✓
Personnalisation des pages et portails		✓	✓	✓	✓
Azure App Proxy		✓	✓	✓	
SLA 99,9%		✓	✓	✓	✓
Premium					
Réinitialisation / modification du mot de passe en self-service pour les utilisateurs AD			✓	✓	
Gestion des groupes en self-service pour les utilisateurs cloud / groupes dynamiques			✓	✓	
Multi-Factor Authentication cloud (Azure MFA) & on-premises (MFA Server)			✓	✓	Cloud uniquement
Connect Health			✓	✓	
Cloud App Discovery			✓	✓	
Azure AD Identity Protection / Azure AD Privileged Identity Management				✓	

Ce chapitre présente comment créer, gérer et supprimer les comptes Azure Active Directory.

5.1 Présentation générale

Le provisionning des comptes Office 365 (Azure Active Directory) peut être effectué manuellement ou automatiquement. Pour créer manuellement un compte Azure Active Directory, vous pouvez utiliser le portail d'administration Office 365 (https://login.microsoftonline.com) ou la commande *New-MsolUser* du module PowerShell Azure Active Directory.



Il est aussi possible d'utiliser un outil comme *Azure Active Directory Connect* pour automatiser cette action.

Cet outil permet de répliquer le contenu (ou une partie seulement) de l'annuaire Active Directory de la société dans l'annuaire Azure Active Directory d'Office 365.

Pour utiliser la synchronisation d'annuaire, il est nécessaire d'activer une option au niveau du Tenant Office 365.

Quand cet outil est utilisé, vous ne pouvez plus modifier les objets synchronisés directement depuis l'interface d'administration d'Office 365 ou depuis le PowerShell Azure Active Directory. Tous les changements (création, modification et suppression d'un compte Azure Active Directory) doivent être effectués depuis l'annuaire Active Directory puis répliqués dans l'annuaire Azure Active Directory à l'aide du serveur *Azure Active Directory Connect*. Certains attributs utilisés par Exchange, Skype for Business, SharePoint, RMS restent cependant éditables.

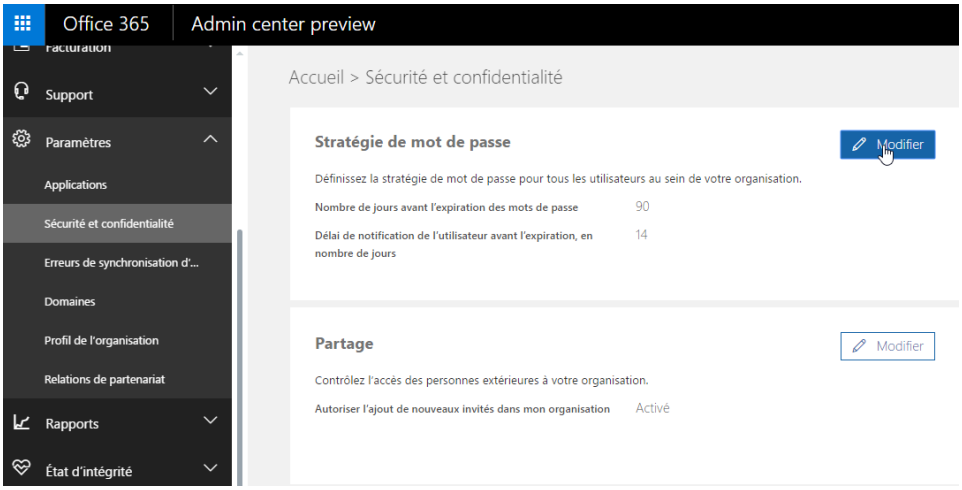
Un message d'erreur apparaît en cas de tentative et explique que ce compte est synchronisé et doit donc être géré depuis l'annuaire Active Directory de l'entreprise.

On notera que les outils *DirSync* et *Azure Active Directory Sync* sont dépréciés et vont être arrêtés prochainement (13 avril 2017). L'outil à déployer est donc *Azure Active Directory Connect* pour synchroniser les comptes utilisateurs Active Directory vers l'annuaire Azure Active Directory (utilisé par Office 365).

https://azure.microsoft.com/fr-fr/documentation/articles/active-directory-aadconnect-dirsync-deprecated/

On notera que Microsoft Azure Active Directory Connect s'appuie sur le moteur de synchronisation de *Microsoft Identity Manager* (anciennement *Forefront Identity Manager*).

Par défaut, le mot de passe du compte Azure Active Directory dispose d'une durée de vie de 90 jours. Ce paramètre est configurable au niveau du Tenant Office 365. Quand un compte utilisateur Azure Active Directory est synchronisé (avec un outil comme Azure Active Directory Connect), c'est alors la stratégie de mots de passe du domaine Active Directory qui s'applique et non la stratégie de mots de passe de l'annuaire Azure Active Directory.



Il est aussi possible de définir que le mot de passe d'un compte Azure Active Directory (objet de type *MsolUser*) n'expire jamais avec la commande *Set-MsolUser* et le paramètre *-PasswordNeverExpires*.

Set-MsolUser -UserPrincipalName admin-gmathieu@labmetsys.onmicrosoft.com -PasswordNeverExpires $True

Ce paramètre n'est cependant pas recommandé pour des raisons de sécurité et doit être réservé uniquement aux comptes de services Azure Active Directory.

Les articles suivants présentent l'outil Azure Active Directory Connect en détails :

https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnectsync-understanding-default-configuration/

https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnectsync-best-practices-changing-default-configuration/

Je vous invite aussi à suivre le MVA suivant pour plus d'informations sur Azure Active Directory Connect :

https://mva.microsoft.com/en-us/training-courses/provisioning-and-configuring-office-365-10569?l=mxq2EgB8_8800115881

Nous allons maintenant voir les choix d'architecture à effectuer pour déployer votre solution de synchronisation d'annuaire.

5.2 Les choix d'architecture

5.2.1 Choix 1 : choix de l'outil de synchronisation

Azure Active Directory Connect (gratuit) permet de prendre en charge la synchronisation de plusieurs domaines / forêts vers un unique Tenant Office 365 contrairement à un outil comme *Dirsync*.

Comme vu précédemment, vous ne devez plus utilisez les outils *DirSync* et *Azure Active Directory Sync* qui sont dépréciés. Il est aussi possible d'utiliser *Microsoft Identity Manager* / *Forefront Identity Manager* (payant, licence par utilisateur).

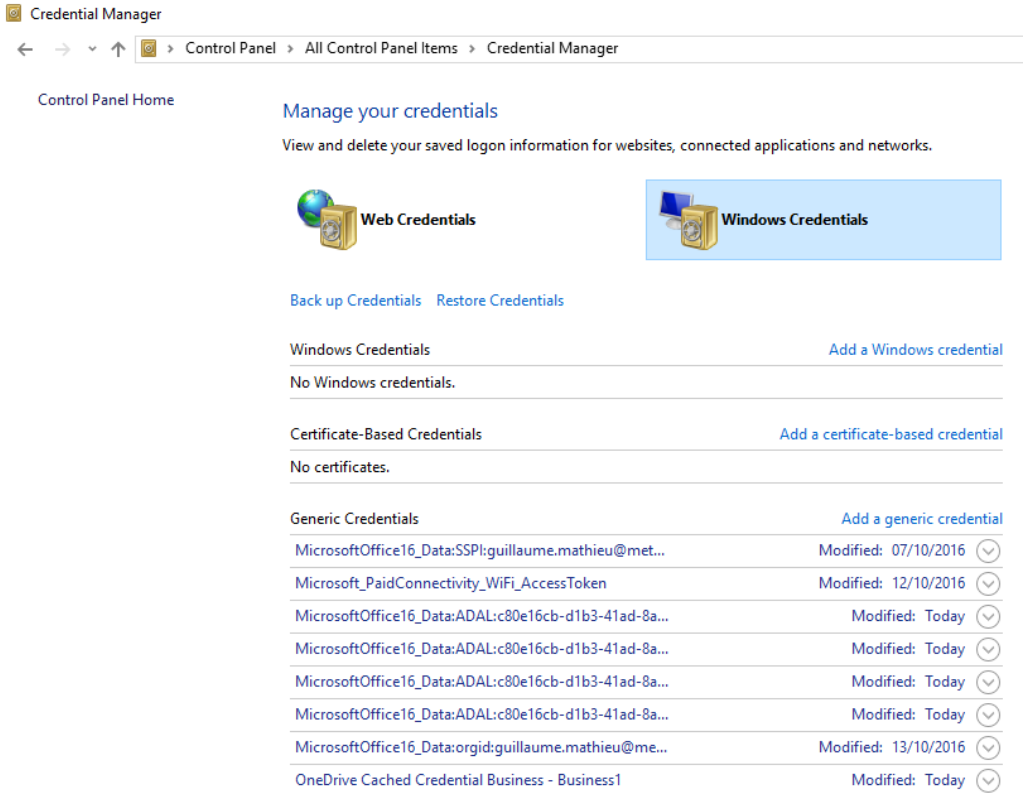
5.2.2 Choix 2 : activer la synchronisation des mots de passe avec Azure Active Directory Connect

Azure Active Directory Connect permet maintenant de synchroniser le mot de passe du compte Active Directory dans l'annuaire Azure Active Directory d'Office 365. Le mot de passe d'un compte utilisateur Active Directory est stocké dans l'attribut *UnicodePwd* sous forme d'un Hash *MD4* (*NTHASH*). Le serveur *Azure Active Directory Connect* récupère le *NTHASH* et génère un hash *SHA-256* à partir de ce dernier. Le résultat devient la valeur du mot de passe du compte utilisateur de l'annuaire Azure Active Directory.

En cas de panne du serveur *Azure Active Directory Connect*, les utilisateurs existants Office 365 peuvent toujours se connecter. Si ces derniers ont changé de mot de passe pendant la panne du serveur *Azure Active Directory Connect*, ils doivent utiliser leur ancien mot de passe pour se connecter à Office 365.

Cette méthode permet de disposer du même login / mot de passe que son compte Active Directory pour accéder à Office 365. Il est cependant nécessaire de saisir ce mot de passe à chaque accès aux services ou de mémoriser ce mot de passe dans le coffre-fort de Windows.

Si l'on veut disposer d'un véritable SSO, il est nécessaire d'utiliser une solution de fédération d'identité comme *ADFS 3.0* (ou *Ping Identity*). La mise en œuvre de ce type de solution est présentée dans le chapitre fédération d'identité de ce document.



5.2.3 Choix 2 : préparation du schéma Active Directory

Azure Active Directory est un outil de synchronisation d'annuaire.

Pour pouvoir modifier l'attribut *TargetAddress* (adresse email de redirection) de l'annuaire Azure Active Directory, il est recommandé de disposer de cet attribut au niveau de son annuaire Active Directory ce qui n'est pas le cas par défaut.

Microsoft recommande donc de préparer le schéma Active Directory pour Exchange 2016 et Skype for Business 2015 afin de disposer entre autre des attributs *TargetAddress*, *MailNickName, msrtcsip-primaryuseraddress* et *msExchHideFromAddressLists*.

Cette action est requise si l'on souhaite définir une adresse SIP spécifique pour Skype For Business qui ne correspond pas à l'adresse email Exchange. Dans l'exemple ci-dessous, on va créer le compte utilisateur suivant dans son annuaire Active Directory et le répliquer avec *Azure Active Directory Connect*.

Attribut Active Directory	Valeur	Explication
UserPrincipalName	melanie.bertrando@labmetsys.fr	Correspond par défaut au login Office 365 (attribut *UserPrincipalName* de l'annuaire Azure Active Directory). Pour simplifier la vie à l'utilisateur, il est recommandé de définir la même valeur que l'adresse email.
SamAccountName	melanie.bertrando	Attribut obligatoire
Mail	melanie.bertrando@labmetsys.fr	Adresse email principale
msrtcsip-primaryuseraddress	mbertrando@labmetsys.fr	Adresse SIP principale. Dans cet exemple, l'utilisateur devra saisir dans Skype for Business une adresse SIP qui est différente de son adresse email (complexe).
ProxyAddresses	SMTP: melanie.bertrando@labmetsys.fr smtp:mbertrando@labmetsys.fr sip:mbertrando@labmetsys.fr	Il s'agit d'un attribut tableau qui contient toutes les adresses emails et SIP de l'utilisateur. L'entrée qui commence par *SMTP:* correspond à l'adresse email principale de l'utilisateur.
MailNickName	Melanie.bertrando	Cet attribut correspond au champ alias dans Exchange Online. Il ne doit pas contenir d'espace.
Targetaddress		Cet attribut doit être vide car on souhaite créer un utilisateur avec boîte aux lettres Exchange. Il est à saisir quand on souhaite créer un contact de messagerie (utilisateur avec adresse de messagerie externe).
msExchHideFromAddressLists	False	Cet attribut permet de masquer / afficher un utilisateur dans la liste d'adresse globale.

Une fois l'objet synchronisé dans Azure Active Directory, il faut lui assigner une licence Office 365 (Plan E1 par exemple) pour lui permettre de disposer d'Exchange Online et de Skype for Business Online.

Pour plus d'informations :

http://social.technet.microsoft.com/wiki/contents/articles/19901.dirsync-list-of-attributes-that-are-synced-by-the-azure-active-directory-sync-tool.aspx

http://www.resdevops.com/2013/02/13/extend-ad-schema-to-allow-greater-office-365-management/

5.2.4 Choix 4 : déployer un serveur de secours Azure Active Directory Connect

Azure Active Directory Connect peut maintenant être déployé sur 2 serveurs. Une option appelée *Staging Mode* permet de déployer le second serveur Azure Active Directory comme serveur de secours. En cas de défaillance du premier serveur *Azure Active Directory Connect*, il est possible de relancer l'assistant de configuration Azure *Active Directory Connect* et de désactiver le *Staging Mode* sur le second serveur.

Les 2 serveurs *Azure Active Directory Connect* doivent cependant disposer de la même configuration.

https://dirteam.com/sander/2015/10/19/ten-things-you-should-know-about-azure-ad-connect-and-azure-ad-sync/

5.2.5 Choix 5 : déterminer l'attribut qui est utilisé pour générer le login Office 365

Par défaut, le login Office 365 est généré à partir de la valeur de l'attribut *UserPrincipalName* de l'annuaire Active Directory. Cette configuration peut être modifiée lors de l'installation d'Azure Active Directory (*Alternate Login ID*). Cette option est décrite dans le chapitre « *Déploiement et configuration d'Azure Active Directory Connect et ADFS dans une architecture d'annuaire complexe ou en cours de migration* » de ce document.

5.2.6 Choix 6 : déterminer l'attribut qui est utilisé pour associer le compte Azure Active Directory et le compte Active Directory

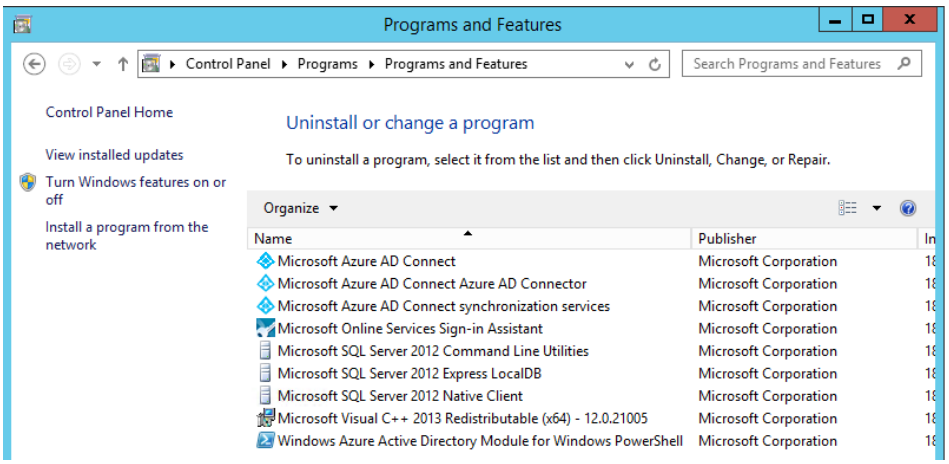
La mise en œuvre de la fédération d'identité avec Office 365 nécessite de disposer d'un attribut qui permet d'associer le compte Azure Active Directory et le compte Active Directory. Cet attribut ne doit jamais changer de valeur (dans la mesure du possible).

Cet attribut s'appelle *ImmutableID* au niveau de l'annuaire Azure Active Directory et est généré par défaut par le serveur Azure Active Directory à partir de l'attribut *ObjectGuid*.

Cette configuration peut être modifiée lors de l'installation d'Azure Active Directory. Cette option est décrite dans le chapitre « *Déploiement et configuration d'Azure Active Directory Connect et ADFS dans une architecture d'annuaire complexe ou en cours de migration* » de ce document.

5.2.7 Choix 7 : base de données pour Azure AD Connect

Par défaut *Azure Active Directory Connect* déploie une base de données *SQL Server 2012 Express LocalDB* pour stocker sa configuration. Il est cependant possible d'utiliser une autre édition de SQL Server (Express, Standard).



Quelques informations sur *SQL Server Express LocalDB* :

SQL Server Express LocalDB ne démarre pas comme un service et prend uniquement 33 Mo d'espace disque (en version 64 bits).

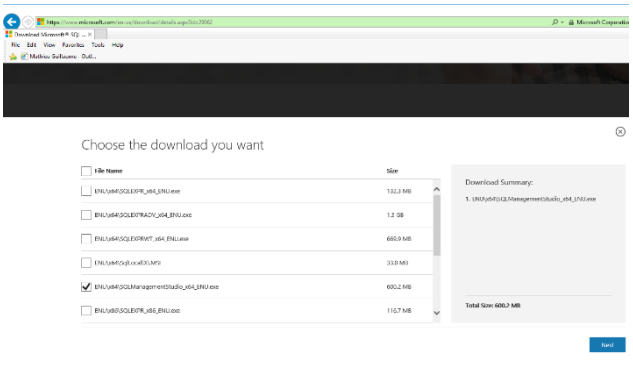
Pour administrer la base *SQL Server Express LocalDB*, il faut télécharger SQL Server Management Studio Express 2012 ou SQL Server Management Studio Express 2014 :

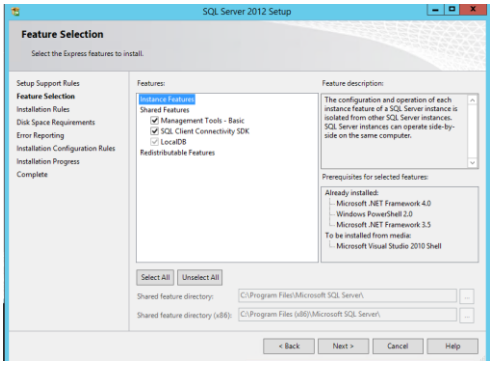
https://www.microsoft.com/en-us/download/details.aspx?id=29062

https://www.microsoft.com/en-US/download/details.aspx?id=42299

Il n'y a pas de service SQL Server Agent donc il est impossible de planifier des sauvegardes (jobs).

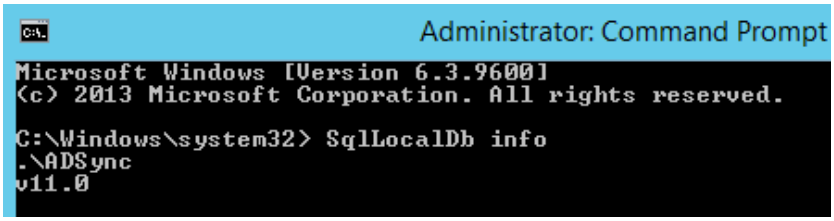
En cas de crash du serveur *Azure Active Directory Connect*, Microsoft recommande tout simplement de réinstaller le serveur, reconfigurer les règles personnalisées et relancer une synchronisation complète. Il n'est donc pas nécessaire de sauvegarder la base de données SQL Server utilisée par *Azure Active Directory Connect*.

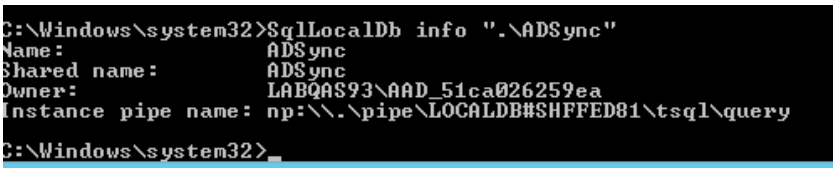




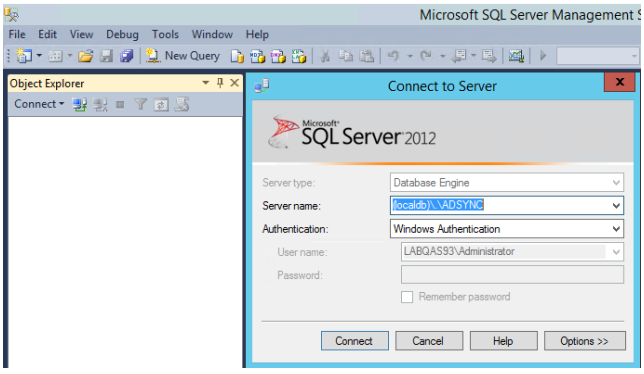
Ce type de base peut être géré localement avec l'outil *SqlLocalDB*.

Lancer la commande *SqlLocalDb info* pour obtenir le nom de l'instance *SQL Server Express LocalDB*.

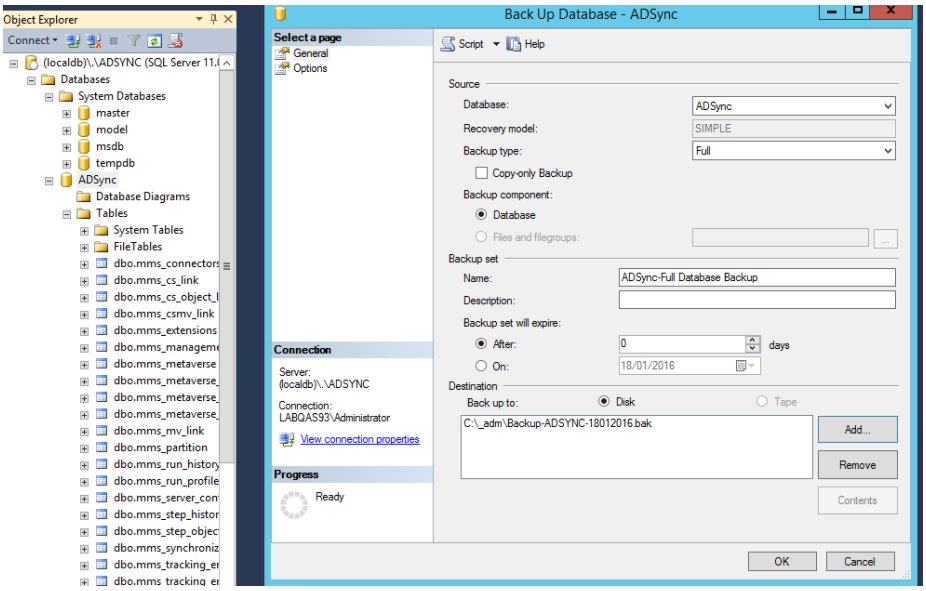




Pour se connecter avec SQL Server Management Studio à l'instance « *.\AdSync* » taper la valeur suivante : Server name : *(localdb)\.\ADSYNC*



On peut alors lancer un backup de la base de données *ADSYNC* créé par l'outil *Azure Active Directory Connect*.



Pour plus d'informations

https://www.mssqltips.com/sqlservertip/2694/getting-started-with-sql-server-2012-express-localdb/

https://blogs.msdn.microsoft.com/sqlexpress/2011/07/12/introducing-localdb-an-improved-sql-express/

5.2.8 Choix 8 : mode d'installation d'Azure Active Directory Connect

Il existe 2 modes d'installation avec *Azure Active Directory Connect*.

Une installation par défaut permet de déployer automatiquement la solution *SQL Server Express LocalDB*. Lors de l'installation, il vous est demandé de spécifier un compte utilisateur Active Directory membre du groupe *Enterprise Admins* et un compte Azure Active Directory *Global Administrator* sur le Tenant Office 365. Ces 2 comptes servent uniquement à créer automatiquement les comptes de service qui seront utilisés par Azure Active Directory. L'inconvénient est que mot de passe de ces comptes est généré automatiquement et ne peut pas être connu. Les paramètres appliqués avec la configuration par défaut sont présentés dans cet article :

https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnectsync-understanding-default-configuration/

Une installation avancée permet d'utiliser un serveur SQL Server Standard, de spécifier le nom des groupes d'administration, le login / mot de passe des comptes de service. Le compte de service spécifié pour le connecteur Active Directory doit être configuré à l'avance et doit disposer du minimum de droits requis. Eviter par exemple de le mettre membre du groupe *Enterprise Admins*.

L'installation d'Azure *Active Directory Connect* sur un contrôleur de domaine est supportée mais doit être évitée car les groupes d'administration d'*Azure Active Directory Connect* sont alors créés dans le domaine et non dans la base SAM locale du serveur (qui n'existe pas sur un contrôleur de domaine). Le compte de service qui démarre le service *Azure Active Directory Connect* est aussi créé dans le domaine et non dans la base SAM locale.

5.2.9 Choix 9 : configurer Azure Active Directory Connect pour répliquer les mots de passe avec des domaines Office 365 fédérés

Quand on configure un domaine Office 365 en mode *Managed* (configuration par défaut), c'est le serveur d'Azure Active Directory qui authentifie l'utilisateur.

Quand on configure un domaine Office 365 en mode *Federated*, le serveur Azure Active Directory transfère la demande d'authentification auprès d'un serveur de fédération d'identité (*ADFS*, *Ping Identity,…*) qui fait alors la demande d'authentification au niveau de l'annuaire de l'entreprise (Active Directory).

Répliquer les mots de passe Active Directory dans l'annuaire Azure Active Directory n'a donc en pratique aucun intérêt si tous les domaines Office 365 sont en mode *Federated*. Cette option permet cependant de disposer d'une solution de repli en cas de défaillance prolongée de la solution de fédération d'identité. En effet, si l'architecture de fédération d'identité est hors service, les utilisateurs dont le domaine de messagerie Office 365 est en mode fédéré ne peuvent plus se connecter au service Office 365.

L'administrateur peut alors utiliser la commande *Set-MsolDomainAuthentication* pour forcer ce domaine de messagerie en mode *Managed*. Exemple :

Set-MsolDomainAuthentication -DomainName msexperiences.msreport.fr -Authentication Managed

Cette solution de tolérance de panne est officiellement supportée depuis 2014 mais ne doit être utilisée qu'en dernier recours. Il est très fortement recommandé de déployer une solution de fédération d'identité hautement disponible avec Office 365 :

http://social.technet.microsoft.com/wiki/contents/articles/17857.dirsync-how-to-switch-from-single-sign-on-to-password-sync.aspx

At General Availability, the Password Synchronization feature did not support the synchronization of passwords for users in a Federated namespace.

We have recently updated the service code to allow this.

This enables the added possibility of running Password Sync while using Single Sign-On, and **temporarily switching** over to use synchronized passwords for login if you experience availability issues with your SSO infrastructure!

5.2.10 Choix 10 : les options de synchronisation d'Azure Active Directory Connect

Le tableau ci-dessous décrit les principales options de synchronisation d'Azure Active Directory Connect.

Option	Description
Exchange hybrid deployment	Permet de configurer attributs de l'annuaire Azure Active Directory qui réplique vers l'annuaire Active Directory. En effet certains changements effectués côté Exchange Online doivent être répliqués côté Exchange On-Premise : https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnectsync-attributes-synchronized/#exchange-hybrid-writeback
Azure AD app and attribute filtering	Cette option permet de définir la liste des attributs répliqués par le serveur Azure Active Directory Connect : https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnect-get-started-custom/#azure-ad-app-and-attribute-filtering
Password synchronization	Cette option permet de répliquer le mot de passe des comptes utilisateurs Active Directory dans l'annuaire Azure Active Directory.
Password writeback	Cette option permet de réinitialiser son mot de passe Active Directory quand on réinitialise son mot de passe Azure Active Directory.
Group writeback	Cette option permet de répliquer les groupes Office 365 au niveau de l'organisation Exchange On-Premise (Exchange 2013 U8 et versions ultérieures). https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnect-feature-preview/#group-writeback
Device writeback	Cette option permet de créer au niveau du *Relying Party Trust* d'ADFS des règles de filtrage conditionnel basés sur des terminaux. https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnect-feature-device-writeback/
Directory extension attribute sync	Cette option permet d'ajouter des attributs à synchroniser au niveau de l'annuaire Azure Active Directory (comme *EmployeeID* ou *Division*). https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnectsync-feature-directory-extensions/

5.3 Installation d'Azure Active Directory Connect

L'installation d'*Azure Active Directory Connect* nécessite 10 étapes :

- Choisir son architecture cible.
- Préparer le schéma Active Directory pour Exchange 2016 et Skype for Business 2015.
- Ajouter les suffixes UPN correspondant aux domaines de messagerie.
- Activer la synchronisation au niveau du tenant Office 365.
- Télécharger la dernière version d'Azure Active Directory Connect.
- Vérifier les prérequis logiciels et matériels pour le déploiement d'Azure Active Directory Connect.
- Créer les comptes de services.
- Installer et configurer Azure Active Directory Connect.
- Lancer une synchronisation complète pour prendre en charge les nouveaux paramètres de configuration.
- Faire la Recette de la solution.

5.3.1 Choisir son architecture cible

Dans cet exemple nous ferons une installation avancée. L'outil Azure Active Directory Connect sera configuré pour installer une base *SQL Server Express Local DB*. On créera un compte de service appelé *MSEXP\SVC-ADDSYNC* pour la synchronisation entre la *Métaverse* (base de données interne d'*Azure Active Directory Connect)* et l'annuaire Active Directory. On utilisera l'attribut *UserPrincipalName* Active Directory comme login Azure Active Directory (attribut *UserPrincipalName* Azure Active Directory). On utilisera l'attribut *ObjectGUID* comme identifiant unique Office 365. Seule la fonctionnalité de réplication des mots de passe sera activée (pas de mode hybride Exchange, …). Le schéma Active Directory sera préparé pour Exchange 2016 et Skype for Business 2015.

5.3.2 Préparer l'annuaire pour Exchange 2016 et Skype for Business 2015

L'annuaire local doit être préparé pour Exchange 2016 et Skype for Business 2015 pour pouvoir bénéficier des attributs comme *TargetAddress, MailNickName, ms-rtc-sip-primaryuseraddress* qui n'existent pas dans le schéma Active Directory de base. La procédure de mise à jour du schéma Active Directory est complexe et peut avoir un impact catastrophique en cas d'échec. Il est donc nécessaire d'effectuer les actions suivantes en prérequis :

- Faire au minimum une sauvegarde de l'*Etat du Système* d'au moins un contrôleur de chaque domaine. Si possible, faire une sauvegarde complète vers un partage externe d'au moins un contrôleur par domaine avec *Windows Server Backup* avant d'exécuter la mise à jour du schéma.

- Valider la procédure de restauration complète de l'annuaire. Vous pouvez consulter la procédure *Forest Recovery* de Microsoft à cette adresse :
  https://technet.microsoft.com/fr-fr/library/cc757662(v=ws.10).aspx
  http://msreport.free.fr/?p=349

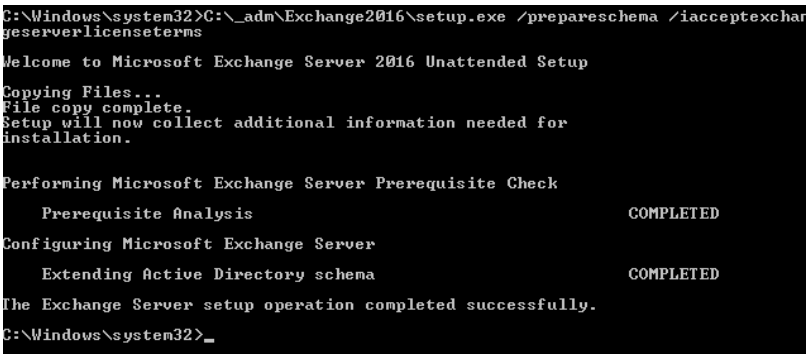
- Désactiver la réplication entrante et sortante entre le contrôleur de domaine maître de schéma et les autres contrôleurs de domaine pendant la mise à jour du schéma. La réplication sera réactivée une fois la mise à jour du schéma effectuée (statut : *COMPLETED*). Cette opération est décrite dans les articles https://support.microsoft.com/en-us/kb/321153
  Pour désactiver la réplication :
  repadmin /options +DISABLE_OUTBOUND_REPL
  repadmin /options +DISABLE_INBOUND_REPL
  Pour réactiver la réplication :
  repadmin /options -DISABLE_OUTBOUND_REPL

repadmin /options -DISABLE_INBOUND_REPL

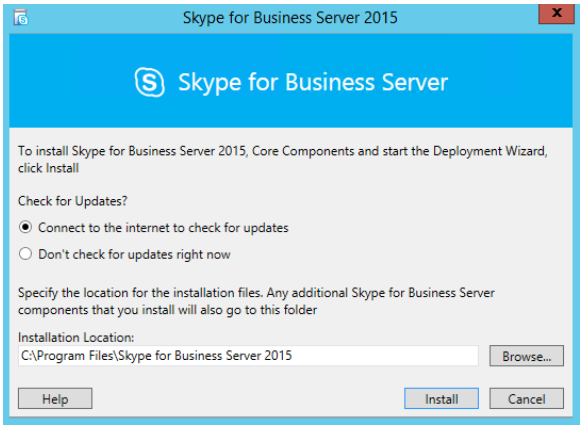
- Effectuer cette action sur le maître de schéma avec un compte membre des groupes *Schema Admins* et *Enterprise Admins*. Lire les préconisations de l'article http://blogs.technet.com/b/askpfeplat/archive/2012/05/28/best-practices-for-implementing-schema-updates-or-how-i-learned-to-stop-worrying-and-love-the-forest-recovery.aspx

- Télécharger les sources d'installation d'Exchange 2016 et de Skype for Business 2015 :
  https://www.microsoft.com/en-us/download/details.aspx?id=49161
  https://www.microsoft.com/fr-fr/evalcenter/evaluate-skype-for-business-server

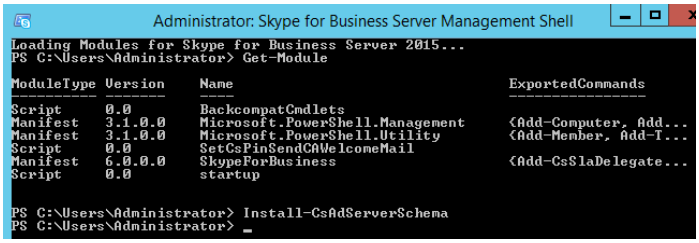
Extraire les sources d'installation dans un dossier comme C:_adm. Entrer la commande suivante pour préparer le schéma pour Exchange 2016 : *setup.exe /prepareschema /iacceptexchangeserverlicenseterms*

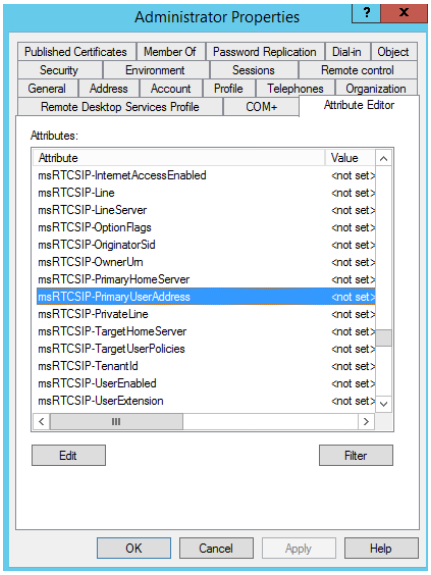


La préparation du schéma avec les extensions Skype for Business nécessite de déployer les outils d'administration Skype for Business comme expliqué dans l'article https://technet.microsoft.com/en-us/library/dn951386.aspx.



Saisir la commande *Install-CSAdServerSchema*.

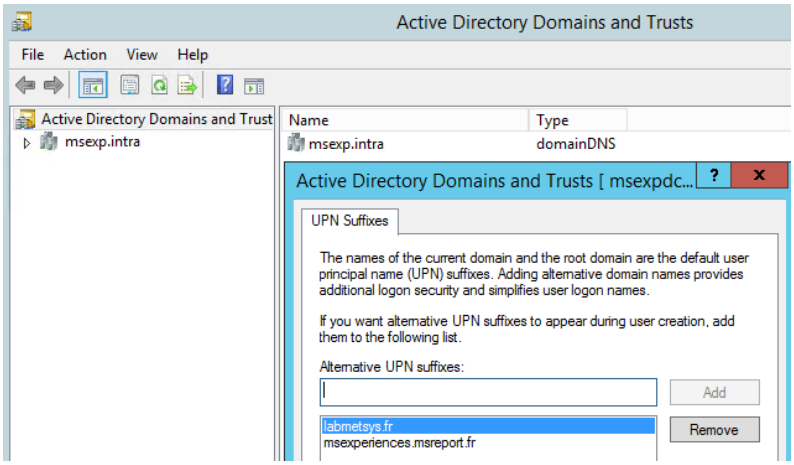




Lancer ensuite la commande *Get-CsAdServerSchema* pour vérifier que l'extension de schéma a été effectuée correctement.

5.3.3 Ajouter les suffixes UPN correspondant aux domaines Office 365

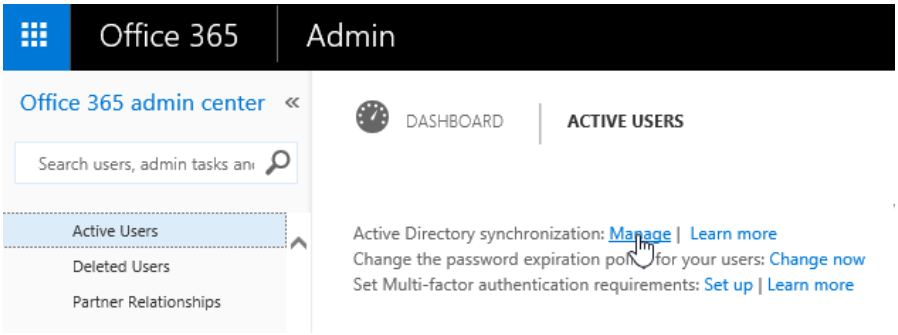
Si vous devez configurer Azure Active Directory Connect pour synchroniser l'attribut *UserPrincipalName* d'Active Directory avec l'attribut *UserPrincipalName* d'Azure Active Directory (annuaire d'Office 365), il est nécessaire d'ajouter les domaines de messagerie en tant que suffixes UPN. Cette action se fait depuis la console *Active Directory Domain and Trusts*.



5.3.4 Activer la synchronisation au niveau du tenant Office 365

La synchronisation entre l'annuaire Active Directory et l'annuaire Azure Active Directory doit être activée au niveau du Tenant Office 365. Cette action peut être effectuée via l'interface graphique (ancien portail Office 365) ou en PowerShell.

Pour l'activer via l'interface graphique, il faut afficher l'ancienne interface et aller dans la section *Utilisateurs | Utilisateurs actifs | Manage*.



Pour faire cette action en PowerShell :

$Cred = Get-Credential

Connect-MsolService -Credential $Cred

Set-MsolDirSyncEnabled -EnableDirSync $True

```
PS C:\Users\Administrator> Connect-MsolService -Credential $Cred
PS C:\Users\Administrator> Set-MsolDirSyncEnabled -EnableDirSync $True

Confirm
Continue with this operation?
[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): y
PS C:\Users\Administrator> _
```

5.3.5 Télécharger la dernière version d'Azure Active Directory Connect

Vous pouvez télécharger la dernière version d'Azure Active Directory Connect (1.1.281.0 – version du 7 septembre 2016) à cette adresse : http://www.microsoft.com/en-us/download/details.aspx?id=47594

5.3.6 Vérifier les prérequis logiciels et matériels d'Azure Active Directory Connect

La solution Azure Active Directory évolue très rapidement. Les 2 articles ci-dessous décrivent les prérequis pour l'installation d'Azure Active Directory Connect et les personnalisations qui sont supportées :

https://azure.microsoft.com/fr-fr/documentation/articles/active-directory-aadconnect-get-started-custom/

https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnectsync-best-practices-changing-default-configuration/

Le nom DNS du domaine ne doit pas être de type *SINGLE LABEL* (*METSYS.* au lieu de *METSYS.INTRA* par exemple). Le nom NETBIOS du domaine ne doit pas contenir le caractère *Point*.

https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnect-faq/

Q: Are SLDs (Single Label Domains) supported?
No, Azure AD Connect does not support on-premises forests/domains using SLDs.

Q: Are "dotted" NetBios named supported?
No, Azure AD Connect does not support on-premises forests/domains where the NetBios name contains a period "." in the name.

Depuis février 2016, le logiciel *Azure Active Directory Connect* peut être configuré avec un compte d'administration qui est activé pour l'authentification multi-facteurs.

Q: Will installation work if the Azure AD Global Admin has 2FA enabled?
With the builds from February 2016, this is supported.

Depuis février 2016, il est possible de déployer *Azure Active Directory Connect* avec une forêt dont tous les domaines ne sont pas joignables.

Q: I have a forest where one domain cannot be contacted. How do I install Azure AD Connect?
With the builds from February 2016, this is supported.

Il n'est pas supporté de renommer un serveur *Azure Active Directory Connect*.

Environment

Q: Is it supported to rename the server after Azure AD Connect has been installed?
No. Changing the server name will cause the sync engine to not be able to connect to the SQL database and the service will not be able to start.

Il n'est pas supporté de changer le mot de passe du compte de service Azure Active Directory généré par l'installateur.

Changes to the service account

Azure AD Connect sync is running under a service account created by the installation wizard. This service account holds the encryption keys to the database used by sync. It is created with a 127 characters long password and the password is set to not expire.

- It is **unsupported** to change or reset the password of the service account. Doing so destroys the encryption keys and the service is not able to access the database and is not able to start.

5.3.7 Créer les comptes de services

Pour installer *Azure Active Directory Connect* en mode avancé, on a besoin :

- D'un compte administrateur local pour lancer l'installation d'Azure Active Directory Connect.
- D'un compte de service Active Directory.
- D'un compte *Global Administrator* sur le Tenant Office 365 (annuaire Azure Active Directory).

L'installateur va utiliser le compte spécifié à l'installation comme compte de service pour le connecteur Active Directory correspondant au domaine spécifié. Des scripts PowerShell sont disponibles sur ce site pour vous aider à définir les droits requis pour ce compte :

https://blog.kloud.com.au/2014/12/18/aadsync-ad-service-account-delegated-permissions/

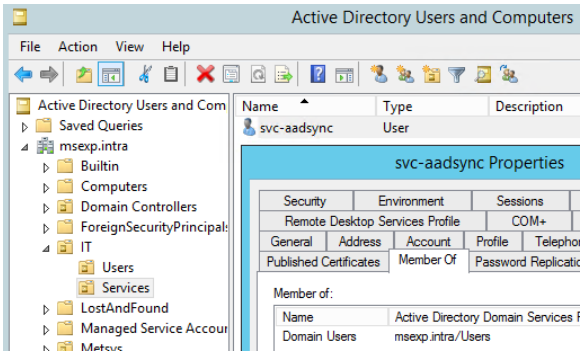
https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnect-accounts-permissions/

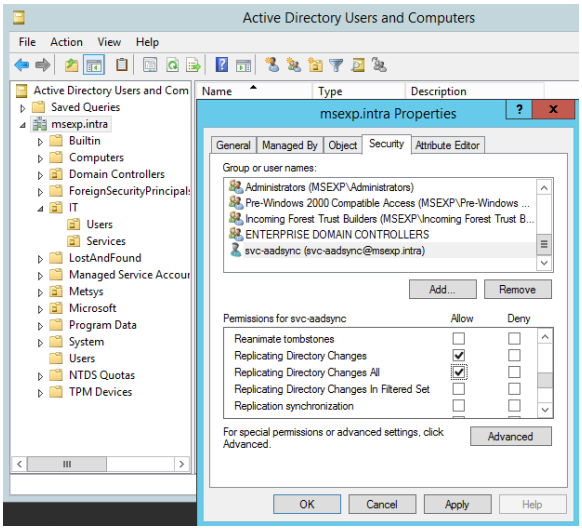
https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnect-accounts-permissions/#create-the-ad-ds-account

Créer et configurer le compte utilisateur Active Directory *MSEXP\SVC-AADSYNC* pour prendre en charge la synchronisation entre l'annuaire Active Directory et la *Métaverse* (base de données de l'outil d'Azure Active Directory Connect). Ce compte doit disposer des droits *Replicate Directory Changes* et *Replicating Directory Changes All* dans tous les domaines de la forêt à synchroniser.

Custom settings installation

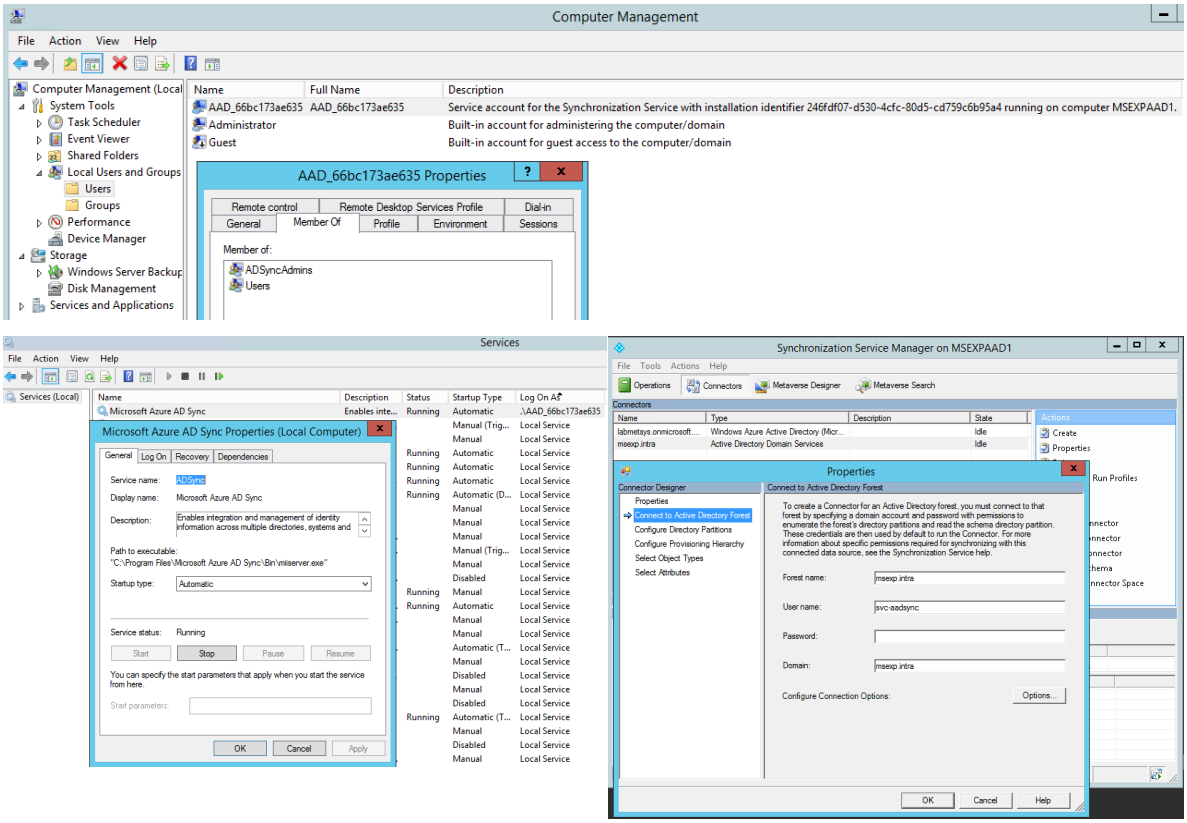
When using custom settings, the account used to connect to Active Directory must be created before the installation. The permissions you must grant this account can be found in create the AD DS account.





Feature	Permissions
Password sync	• Replicate Directory Changes • Replicate Directory Changes All
Exchange hybrid deployment	Write permissions to the attributes documented in Excha writeback for users, groups, and contacts.
Password writeback	Write permissions to the attributes documented in Gettir with password management for users.
Device writeback	Permissions granted with a PowerShell script as describe writeback.
Group writeback	Read, Create, Update, and Delete group objects in the OU distributions groups should be located.

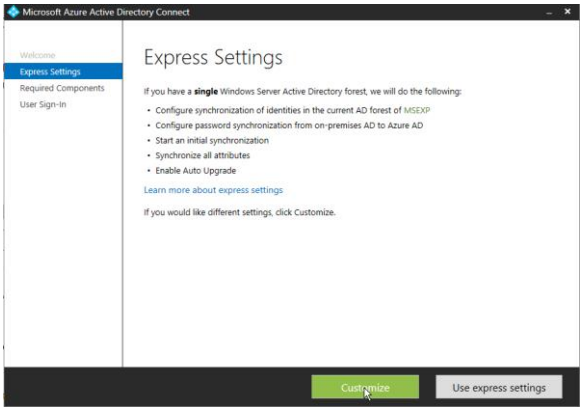
Une fois l'installation terminée, un compte utilisateur appelé *AAD_66BC173AE635* est créé automatiquement dans la base SAM si Azure Active Directory Connect est installé sur un serveur membre. Ce compte permet de démarrer le service *Azure Active Directory Connect*. Il n'est pas supporté de modifier son mot de passe.

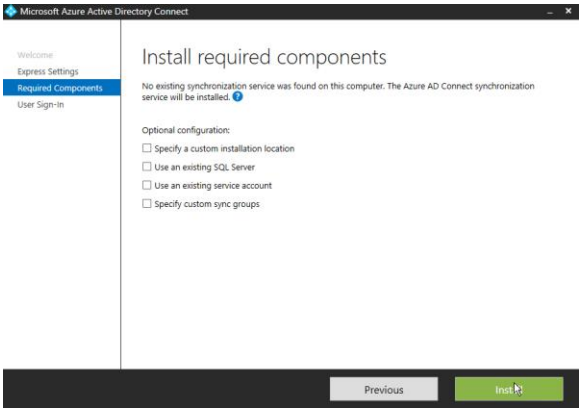


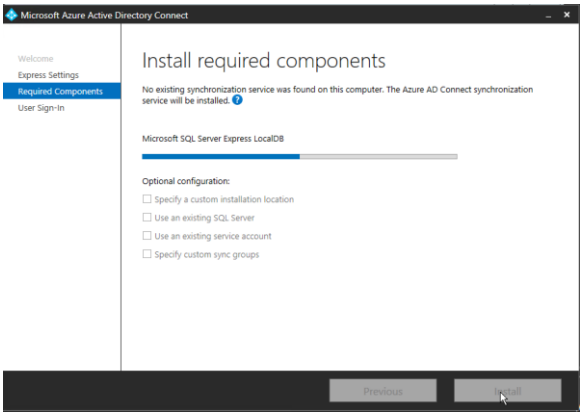
Un compte d'administration appelé Sync_MSEXPAAD1_66bc173ae635@labmetsys.onmicrosoft.com est créé automatiquement. Ce compte dispose du rôle *Directory Synchronisation Accounts* au niveau du tenant Office 365 et permet de créer les comptes dans l'annuaire Azure Active Directory. Une fois *Azure Active Directory Connect* déployé, il est donc possible de désactiver le compte Azure Active Directory avec le privilège *Global Administrator* Office 365 spécifié pendant l'installation.

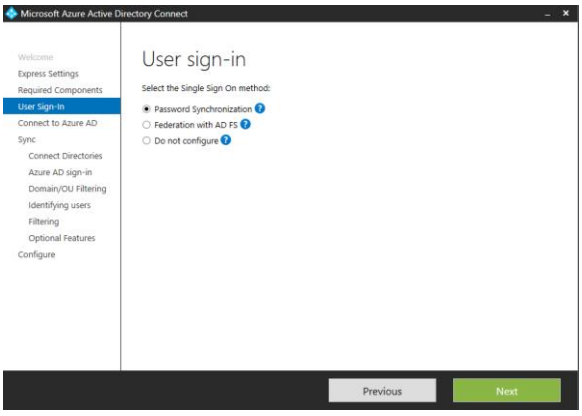
5.3.8 Installation et configuration Azure Active Directory Connect

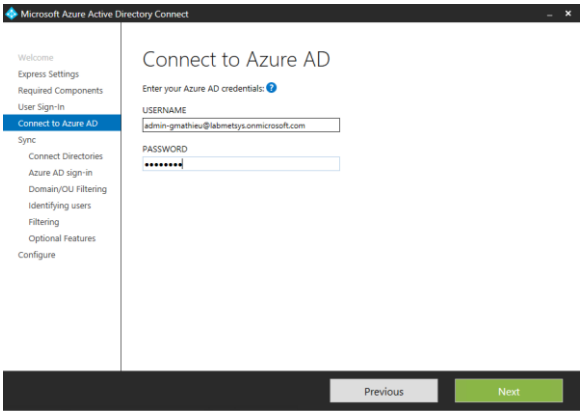
Il est recommandé d'installer Azure Active Directory Connect en mode avancé.

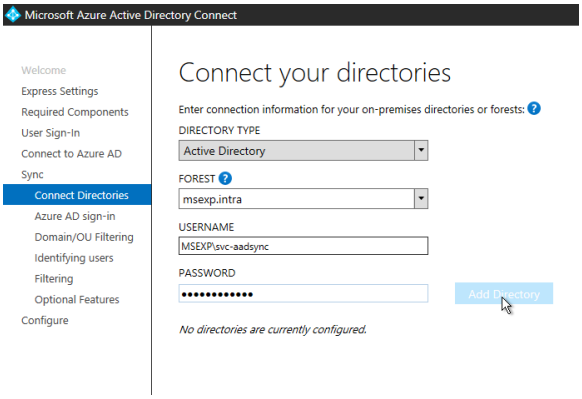


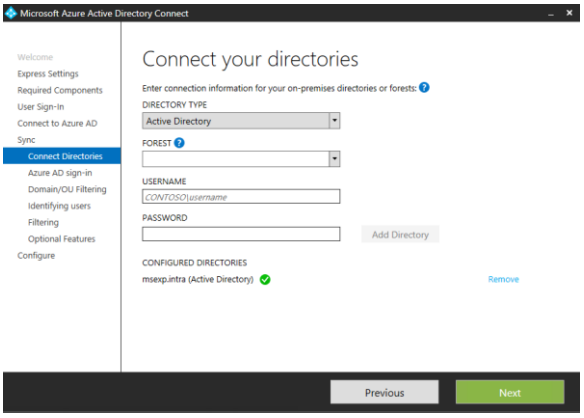


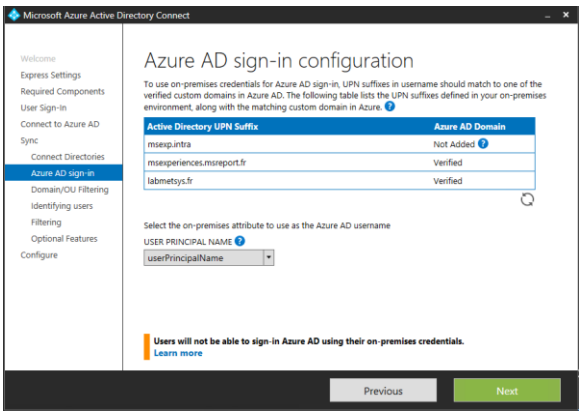


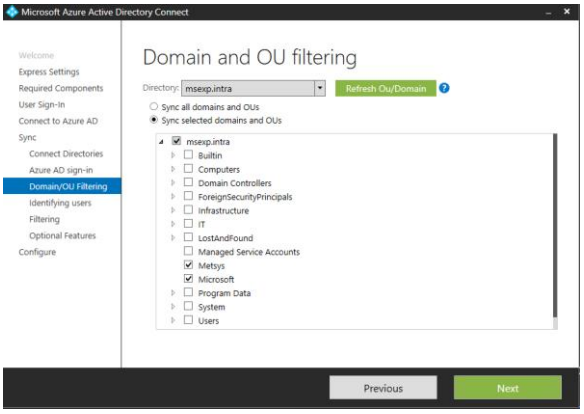


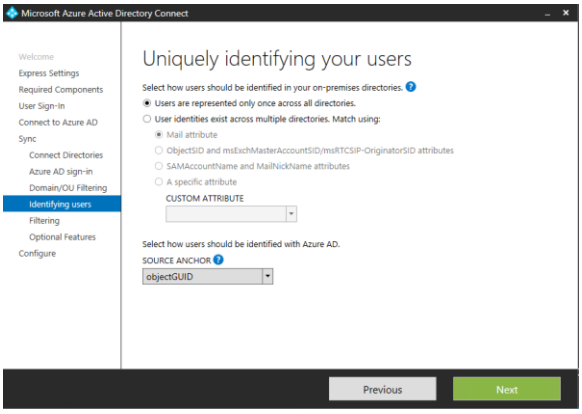


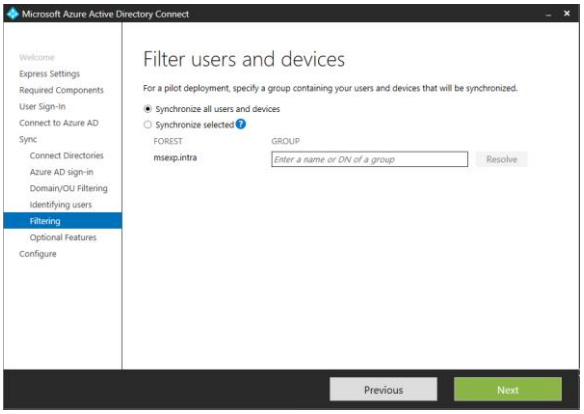


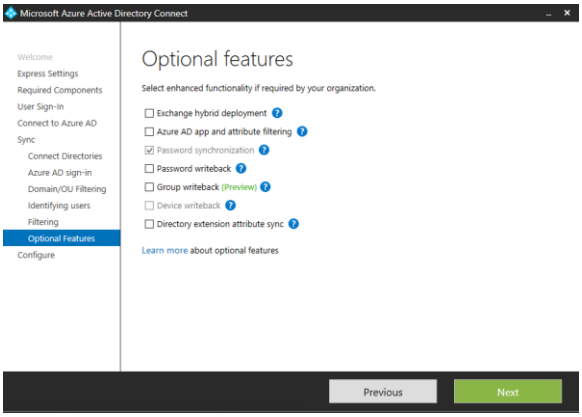

Microsoft Azure Active Directory Connect
Connect your directories
Enter connection information for your on-premises directories or forests:
DIRECTORY TYPE
Active Directory
FOREST
USERNAME
CONTOSO\username
PASSWORD
Add Directory
CONFIGURED DIRECTORIES
msexp.intra (Active Directory)
Remove
Previous
Next

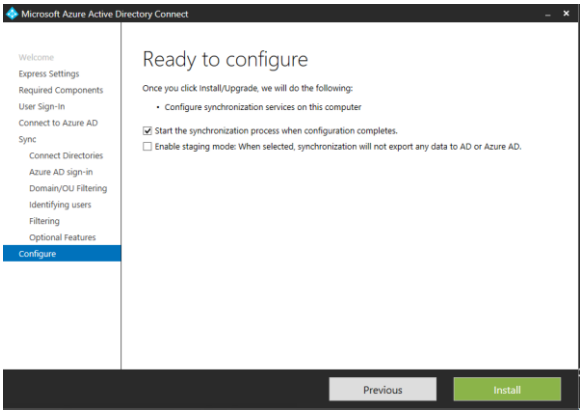

Microsoft Azure Active Directory Connect
Azure AD sign-in configuration
To use on-premises credentials for Azure AD sign-in, UPN suffixes in username should match to one of the verified custom domains in Azure AD. The following table lists the UPN suffixes defined in your on-premises environment, along with the matching custom domain in Azure.
Active Directory UPN Suffix
Azure AD Domain
msexp.intra
Not Added
msexperiences.msreport.fr
Verified
labmetsys.fr
Verified
Select the on-premises attribute to use as the Azure AD username
USER PRINCIPAL NAME
userPrincipalName
Users will not be able to sign-in Azure AD using their on-premises credentials.
Learn more
Previous
Next

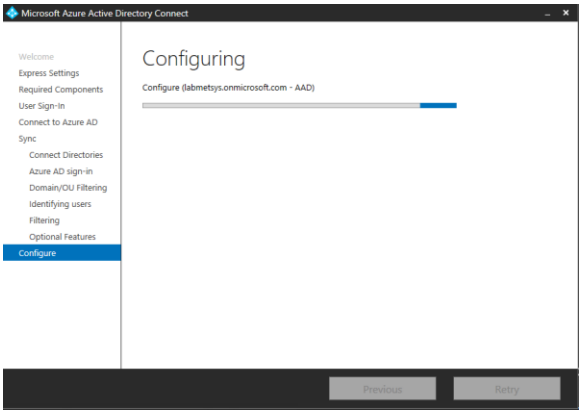

Microsoft Azure Active Directory Connect
Domain and OU filtering
Directory:
msexp.intra
Refresh Ou/Domain
Sync all domains and OUs
Sync selected domains and OUs
msexp.intra
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Infrastructure
IT
LostAndFound
Managed Service Accounts
Metsys
Microsoft
Program Data
System
Users
Previous
Next

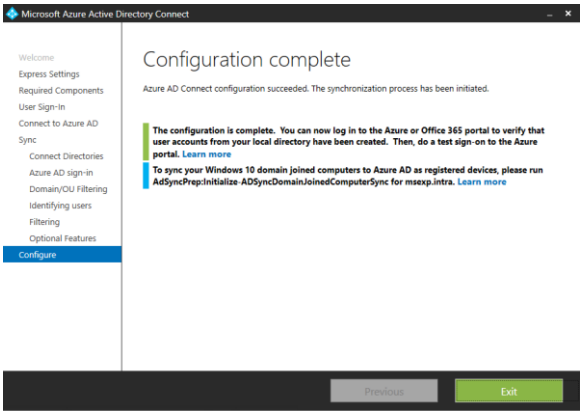

Microsoft Azure Active Directory Connect
Uniquely identifying your users
Select how users should be identified in your on-premises directories.
Users are represented only once across all directories.
User identities exist across multiple directories. Match using:
Mail attribute
ObjectSID and msExchMasterAccountSID/msRTCSIP-OriginatorSID attributes
SAMAccountName and MailNickName attributes
A specific attribute
CUSTOM ATTRIBUTE
Select how users should be identified with Azure AD.
SOURCE ANCHOR
objectGUID
Previous
Next


Microsoft Azure Active Directory Connect
Filter users and devices
For a pilot deployment, specify a group containing your users and devices that will be synchronized.
Synchronize all users and devices
Synchronize selected
FOREST
GROUP
msexp.intra
Enter a name or DN of a group
Resolve
Previous
Next


Microsoft Azure Active Directory Connect
Optional features
Select enhanced functionality if required by your organization.
Exchange hybrid deployment
Azure AD app and attribute filtering
Password synchronization
Password writeback
Group writeback (Preview)
Device writeback
Directory extension attribute sync
Learn more about optional features
Previous
Next


Microsoft Azure Active Directory Connect
Ready to configure
Once you click Install/Upgrade, we will do the following:
Configure synchronization services on this computer
Start the synchronization process when configuration completes.
Enable staging mode: When selected, synchronization will not export any data to AD or Azure AD.
Previous
Install

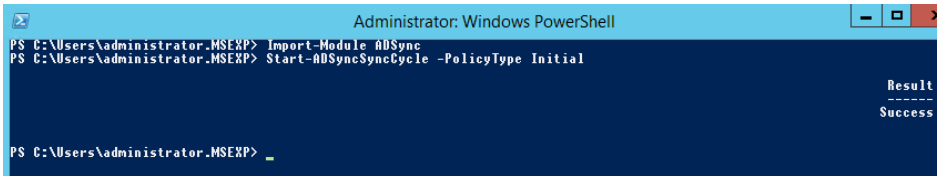

Microsoft Azure Active Directory Connect
Configuring
Configure (labmetsys.onmicrosoft.com - AAD)
Previous
Retry



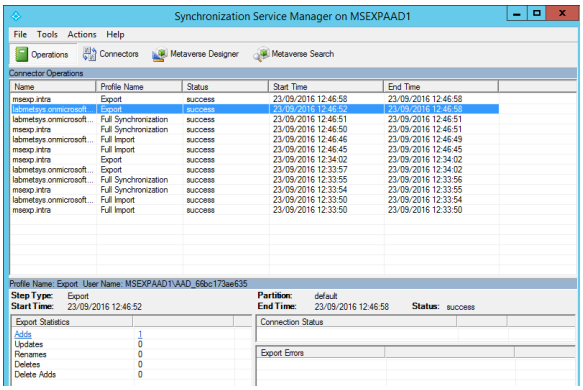
Pour lancer la synchronisation initiale, exécuter les commandes :

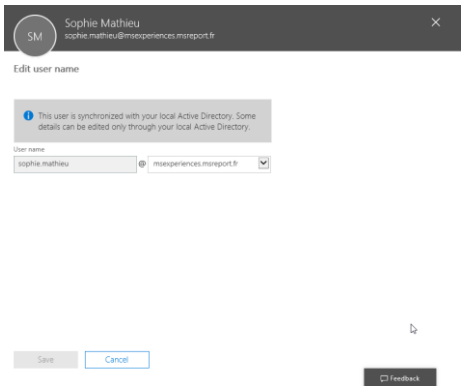
Import-Module ADSync

Start-ADSyncSyncCycle -PolicyType Initial



Dans mon exemple, un compte dans l'OU Metsys (*sophie.mathieu@msreperiences.msreport.fr*) a été synchronisé. Ce compte ne peut donc plus être modifié directement depuis l'annuaire Azure Active Directory.

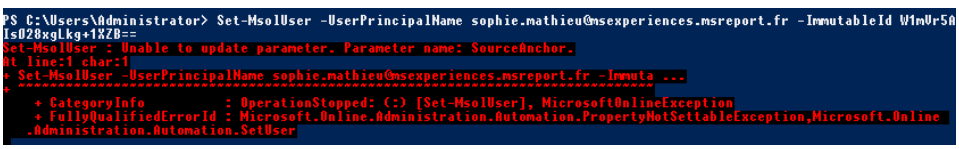




Taper la commande suivante pour afficher l'attribut *ImmutableID* du compte Sophie MATHIEU (W1mVr5AIs028xgLkg+1XZA==) :

Get-MsolUser -UserPrincipalName sophie.mathieu@msexperiences.msreport.fr | Select-Object UserPrincipalName,Islicenced,ImmutableID

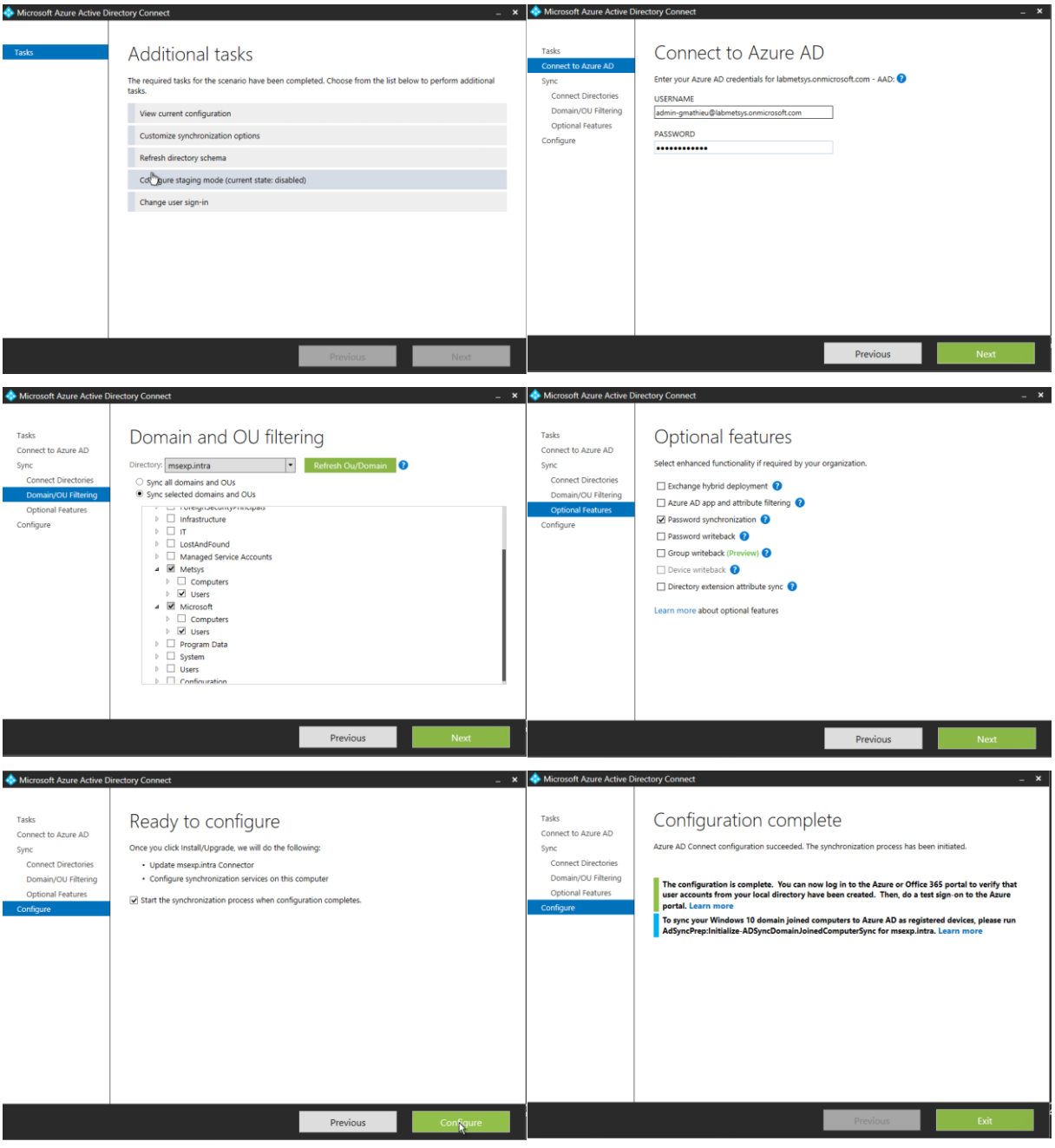
On notera que l'on ne peut pas modifier la valeur de l'attribut *ImmutableId* quand un compte est synchronisé



5.3.9 Configuration d'Azure Active Directory Connect (après déploiement)

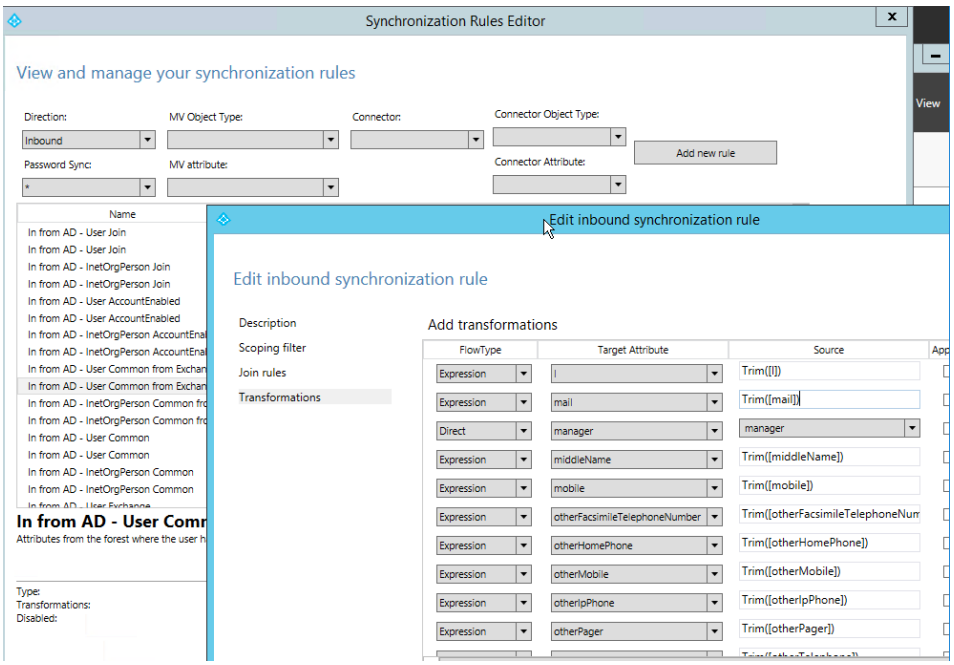
Il est possible de reconfigurer l'outil Azure Active Directory Connect après installation en exécutant le programme *C:\Program Files\Microsoft Azure Active Directory Connect\AzureADConnect.exe*.

Cette console permet d'afficher et/ou de modifier la configuration de l'outil. On peut par exemple activer ou non la synchronisation des mots de passe et/ou modifier les règles de filtrage des containeurs à synchroniser (unités d'organisation). Attention, cela écrase tous les réglages définis manuellement dans les autres consoles.

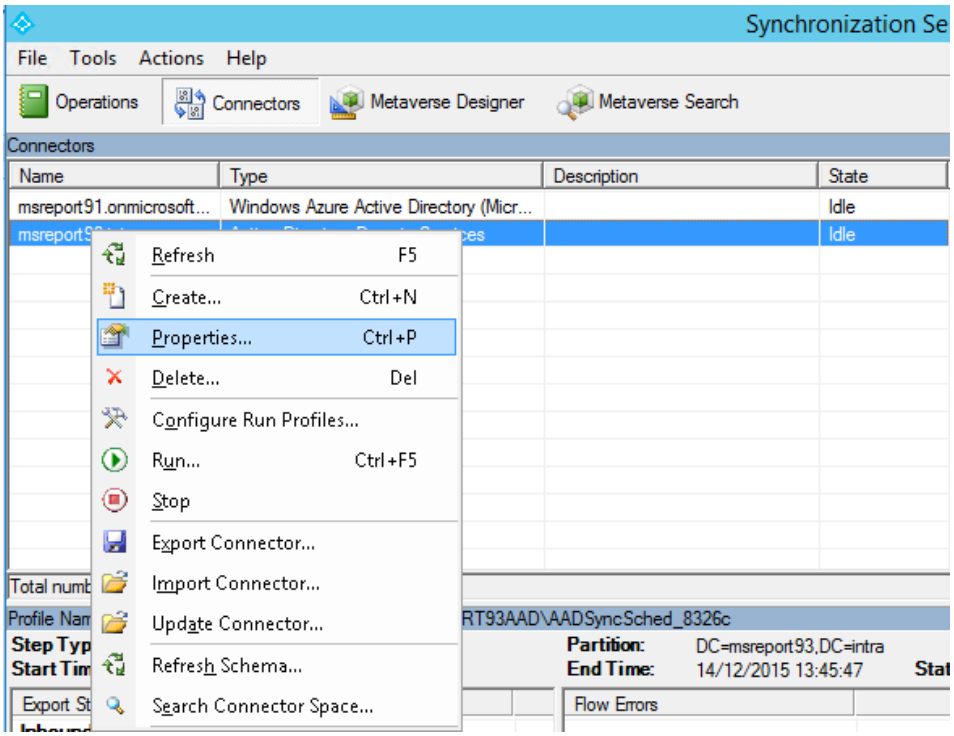


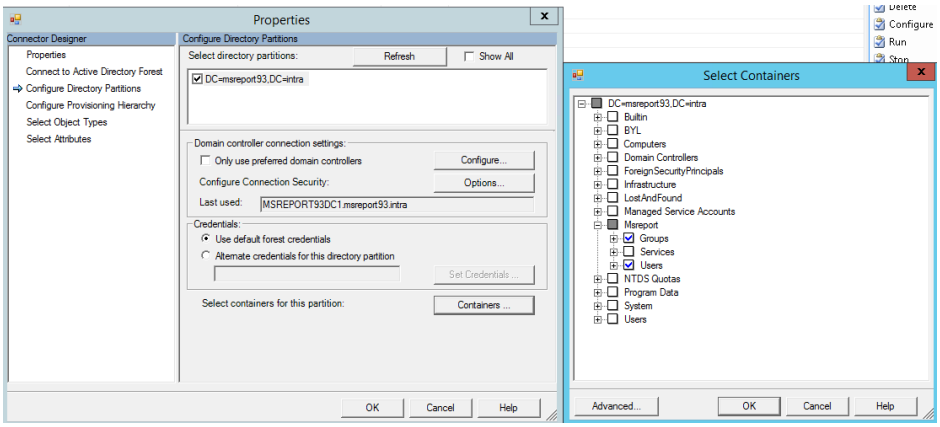
Contrairement à l'outil *DirSync*, il n'est plus possible de modifier les règles de synchronisation directement depuis la console *MIIS.EXE* (console *Forefront Identity Manager*). Ces règles peuvent être éditées depuis l'outil *C:\Program Files\Microsoft Azure AD Sync\UIShell\SyncRulesEditor.exe*.

On notera qu'il existe des règles *Inbound* et *Outbound* (point de vue de la *Métaverse*).



Le filtrage par OU peut se faire via la console *Azure Active Directory Connect* (*C:\Program Files\Microsoft Azure Active Directory Connect\AzureADConnect.exe*) ou via la console *Synchronisation Service*.





On doit lancer une synchronisation complète si on a modifié les règles de synchronisation (ajout d'une OU à synchroniser ou modification des règles de synchronisation d'attributs…) :

Import-Module ADSync

Start-ADSyncSyncCycle -PolicyType Initial

https://msdn.microsoft.com/en-us/library/azure/dn801051.aspx

5.3.10 Renforcement de la sécurité du serveur Azure Active Directory Connect

Par défaut, les transferts entre *Azure AD Connect* et Office 365 sont effectués en TLS 1.0. On peut activer le mode TLS 1.2 afin de garantir une sécurité supérieure lors des transferts d'informations. Le seul prérequis est que la machine soit Windows 2008 R2 ou supérieur et que le TLS 1.2 soit activé dans le registre Windows.

Activation de TLS 1.2 pour tout le serveur :

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client] "DisabledByDefault"=dword:00000000 "Enabled"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server] "DisabledByDefault"=dword:00000000 "Enabled"=dword:00000001

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319

"SchUseStrongCrypto"=dword:00000001

Redémarrer le serveur Azure AD Connect et lancer une nouvelle synchronisation.

5.4 Recette du déploiement d'Azure Active Directory

Créer le compte *annie.mathieu*. Ce compte doit disposer de tous les attributs requis :

Attribut	Valeur
Mail	annie.mathieu@msexperiences.msreport.fr
MailNickName	annie.mathieu
ProxyAddresses	SMTP:annie.mathieu@msexperiences.msreport.fr
UserPrincipalName	annie.mathieu@msexperiences.msreport.fr
SamAccountName	annie.mathieu
Mot de passe	**********

Lancer une synchronisation *Azure Active Directory Connect* avec la commande suivante :

Import-Module ADSync

Start-ADSyncSyncCycle -PolicyType initial

On pourra lancer d'autres synchronisations manuelles différentielles avec cette commande :

Import-Module ADSync

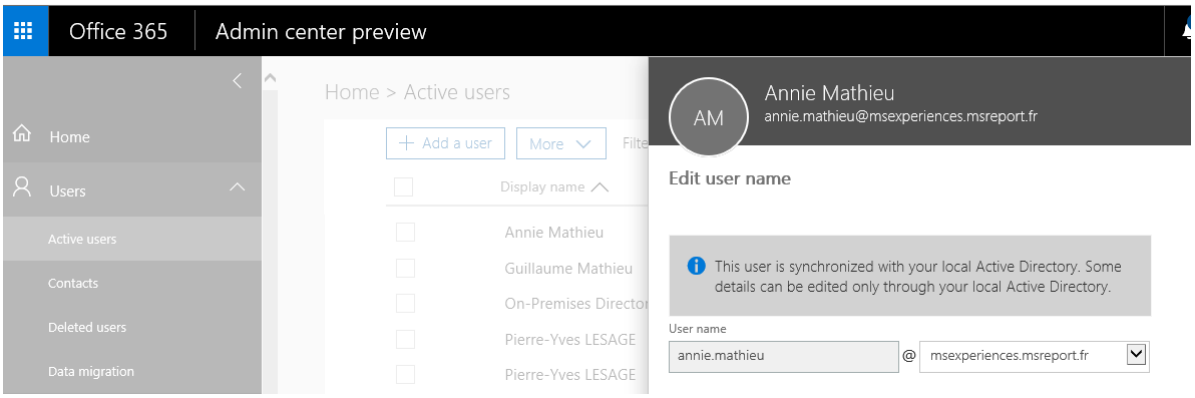
Start-ADSyncSyncCycle -PolicyType Initial

Le compte doit ensuite apparaître au niveau du Tenant Office 365. Les comptes synchronisés ne sont plus éditables. Les attributs utilisés par Exchange Online, Skype for Business Online et autres applications Office 365 restent éditables. L'attribut *ImmutableId* de l'annuaire Office 365 (Azure Active Directory) correspond au GUID de l'annuaire Active Directory. C'est cet attribut qui permet de faire la correspondance entre les 2 comptes.

Ce lien est requis lors de la mise en œuvre de la fédération d'identité avec une solution comme ADFS 3.0.

Le script en pièce jointe permet de convertir l'*ImmutableID* en GUID :

https://gallery.technet.microsoft.com/office/Covert-DirSyncMS-Online-5f3563b1/view/Discussions



6 Mise en œuvre de la fédération d'identité avec Office 365

6.1 Les différentes méthodes d'authentification avec Office 365

Il existe 3 solutions pour s'authentifier avec Office 365 comme expliqué dans le MVA (en français) suivant : https://mva.microsoft.com/fr-fr/training-courses/fdration-didentit-avec-microsoft-azure-active-directory-fr-8961

Solution 1 : utiliser un compte Azure Active Directory sans l'option synchronisation de mots de passe

Il s'agit de la solution activée par défaut au niveau du Tenant Office 365. Cette méthode est recommandée uniquement pour les petites sociétés.

Chaque utilisateur s'authentifie avec son compte Azure Active Directory et son mot de passe associé.

L'utilisateur peut mémoriser ce login / mot de passe dans le coffre-fort de Windows. L'utilisateur devra changer son mot de passe tous les 90 jours (paramètre configurable au niveau des stratégies de mots de passe Azure Active Directory). Cette solution ne nécessite aucune configuration mais nécessite que l'utilisateur mémorise un login / mot de passe supplémentaire. Ce mode est utilisé pour les comptes de secours et / ou les comptes de services Office 365.

Solution 2 : utiliser un compte Azure Active Directory avec l'option synchronisation de mots de passe :

Il s'agit de la solution obtenue après avoir déployé un serveur *Azure Active Directory Connect* avec l'option réplication de mots de passe.

L'utilisateur s'authentifie toujours avec son compte Azure Active Directory et son mot de passe associé mais ce dernier est identique au login / mot de passe du compte utilisateur du domaine Active Directory.

L'utilisateur doit cependant toujours saisir ce login / mot de passe pour s'authentifier avec Office 365.

L'utilisateur peut mémoriser ce login / mot de passe dans le coffre-fort de Windows. Il devra le saisir de nouveau uniquement quand il changera son mot de passe de compte utilisateur Active Directory.

Solution 3 : utiliser une solution de fédération d'identité

Cette solution est totalement différente des 2 autres solutions. Elle permet à l'utilisateur de s'authentifier à Office 365 avec son login / mot de passe Active Directory (et non Azure Active Directory).

Pour des raisons de sécurité, Office 365 ne doit pas pouvoir accéder directement à l'annuaire Active Directory de l'entreprise. On va donc utiliser un tiers de confiance qui sera accessible par les serveurs Office 365 et qui lui disposera d'un accès à l'annuaire Active Directory de l'entreprise. Ce tiers de confiance est la solution de fédération d'identité.

Exemple de fonctionnement :

Un utilisateur se connecte à Outlook Web App (https://outlook.office.com/) avec son navigateur web.

Exchange Online redirige le navigateur vers un serveur d'authentification Azure Active Directory (https://login.microsoftonline.com).

Le serveur d'authentification Azure Active Directory analyse le suffixe DNS du login de l'utilisateur. Si ce dernier correspond à un domaine Office 365 de type *Federated*, le serveur Azure Active Directory redirige le navigateur vers le serveur de fédération d'identité de la société de l'utilisateur (ADFS 3.0 dans notre cas).

Le serveur de fédération d'identité authentifie l'utilisateur à l'aide de son login / mot de passe Active Directory et génère un jeton SAML 1.1 pour l'utilisateur.

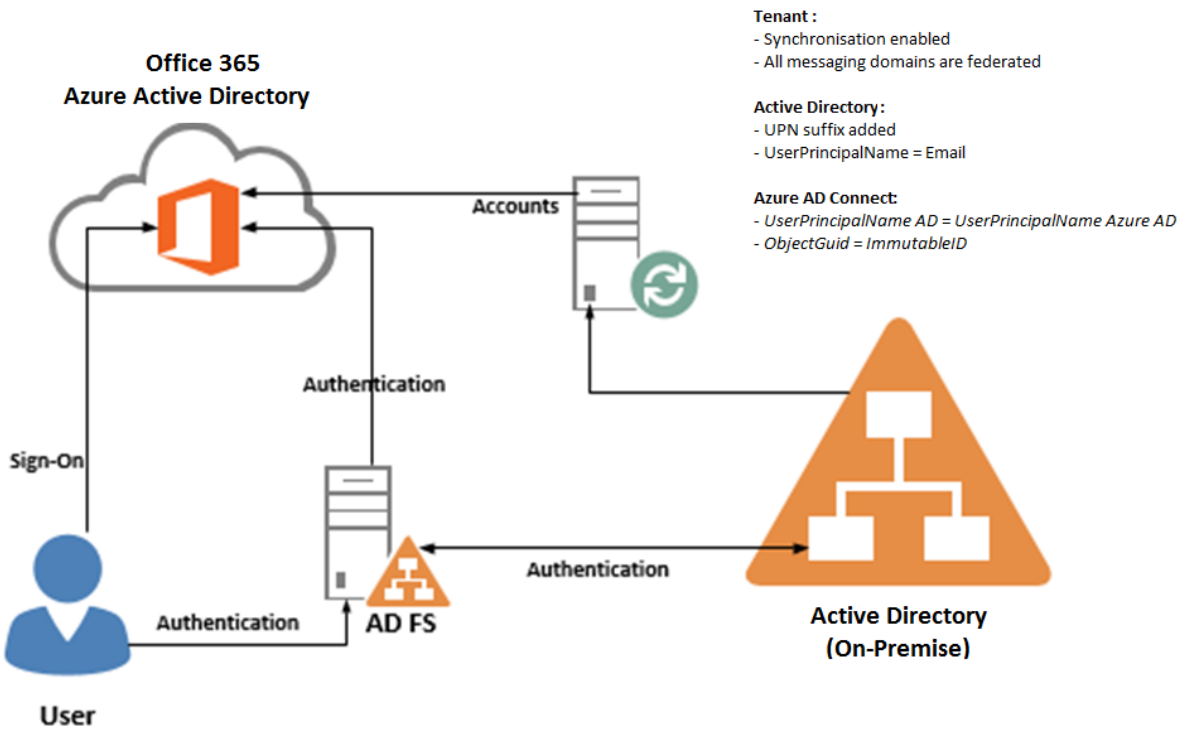
Le navigateur présente ce jeton SAML au serveur Azure Active Directory qui génère à son tour un jeton d'authentification et le renvoie au navigateur.

Le navigateur présente ce jeton d'authentification au serveur Exchange Online et l'utilisateur peut accéder à Outlook Web App.

6.2 Office 365 et la fédération d'identité

6.2.1 Présentation générale

Le schéma ci-dessous présente l'architecture type pour mettre en œuvre la fédération d'identité.



Le Tenant Office 365 doit être activé pour la synchronisation d'annuaire. En effet, il est nécessaire de disposer d'un attribut (*ImmutableID*) pour faire le mappage entre le compte Active Directory et le compte Azure Active Directory. Cet attribut est généré par le serveur Azure Active Directory en se basant sur l'attribut *ObjectGuid* du compte utilisateur de l'annuaire Active Directory : https://gallery.technet.microsoft.com/office/Covert-DirSyncMS-Online-5f3563b1?stoAI=10&wa=wsignin1.0&stoAI=10

En cas de panne de la solution de fédération d'identité, l'accès aux applications et aux services Office 365 n'est plus possible. Il est donc nécessaire de déployer une architecture de fédération d'identité hautement disponible soit un minimum de 7 serveurs :

- 2 serveurs Windows 2012 R2 membres du domaine, hébergés dans le réseau local de l'entreprise avec le rôle *Active Directory Federation Services* (*ADFS 3.0).*
- 2 serveurs Windows 2012 R2 en groupe de travail, hébergés dans une DMZ avec le rôle *Remote Access* et le service de rôle *Web Application Proxy.* Ces serveurs jouent le rôle de reverse proxy.
- 1 serveur *Azure Active Directory Connect pour la synchronisation des annuaires Active Directory et Azure Active Directory*.
- 2 répartiteurs de charges (des *Kemp Load Master VLM 2000*) pour répartir les connexions clientes sur les serveurs ADFS 3.0 et les serveurs *Web Application Proxy*. Ces équipements doivent être capable de détecter et isoler un serveur ADFS 3.0 ou WAP défaillant.

L'article Microsoft https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnect-federation-compatibility/ présente les différences solutions de fédération d'identité compatibles avec Office 365. On notera que certaines solutions ne sont que partiellement prises en charge comme la solution *BIG-IP*.

Il est fortement recommandé de toujours rester dans une architecture supportée à 100 %. En effet la solution Office 365 évolue très vite (un changement majeur en moyenne tous les 3 mois). Ce qui fonctionne aujourd'hui mais qui est non supporté ne fonctionnera peut-être plus demain.

BIG-IP with Access Policy Manager BIG-IP ver. 11.3x – 11.6x

The BIG-IP with Access Policy Manager, (APM) BIG-IP ver. 11.3x – 11.6x implements the widely used SAML identity standard to provide a single sign-on experience and attribute exchange framework.

The following is the scenario support matrix for this single sign-on experience:

Client	Support	Exceptions
Web-based clients such as Exchange Web Access and SharePoint Online	Supported	None
Rich client applications such as Lync, Office Subscription, CRM	Not Supported	Not Supported
Email-rich clients such as Outlook and ActiveSync	Supported	None

For more information about BIG-IP Access Policy Manager, see BIG-IP Access Policy Manager.

L'activation et le paramétrage de la fédération d'identité avec Office 365 se fait au niveau de chaque domaine Office 365 à l'aide des commandes *Convert-MsolDomainToFederated*, *Set-MsolDomainAuthentication* et *Set-MsolDomainFederationSettings*.

Il est possible de disposer sur un même Tenant Office 365 de domaines en mode *Federated* et en mode *Managed*.

On notera que la commande *Convert-MsolDomainToFederated* permet à la fois de configurer le domaine Office 365 et le serveur ADFS 3.0.

Les commandes *Set-MsolDomainAuthentication* et *Set-MsolDomainFederationSettings* servent principalement quand on fédère un domaine de messagerie Office 365 avec une solution de fédération d'identité tierce comme *Ping Identity*.

Les versions antérieures à Office 2013 ne prenaient pas en charge nativement l'authentification avec un annuaire Azure Active Directory et l'utilisation de protocoles de fédérations d'identité comme *SAML* ou *OAUTH*. Microsoft a donc développé dans un premier temps, un client autonome appelé *Microsoft Online Sign In Assistant* pour ajouter ces fonctionnalités à ses logiciels. Le *Microsoft Online Sign In Assistant* se présente sous la forme d'un service Windows appelé *MSOIDSVC* et peut être téléchargé à cette adresse :

https://www.microsoft.com/fr-fr/download/details.aspx?id=41950

Le *Microsoft Online Sign In Assistant* a ensuite été intégré dans Office 2013 / 2016 sous forme d'une DLL et se trouve avec le package Office 365 ProPlus à l'emplacement suivant : *C:\Program Files\Common Files\Microsoft Shared\ OFFICE15\MSO.DLL.*

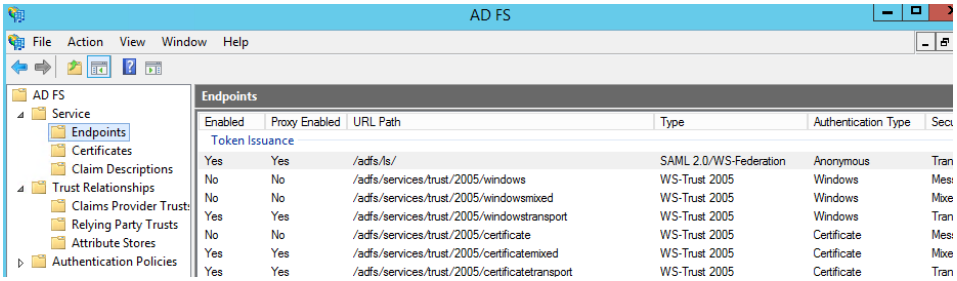
Jusqu'à mai 2016 et la sortie officielle de *Modern Authentication* (ADAL), Microsoft s'appuyait sur plusieurs flux / protocoles de signalisation de fédération d'identité (*Ws-Federation*, *WS-MEX*, *WS-Trust*) selon le type de clients.

La commande *Get-MsolFederationProperty* permet d'afficher la configuration d'un domaine Office 365 en mode *Federated*. Or cette commande dispose des attributs : *PassiveClientSignOutUrl*, *FederationMetadataUrl* et *ActiveClientSignInUrl*. Dans l'exemple ci-dessous, chacun de ces attributs est en fait un point de terminaison ADFS différent.

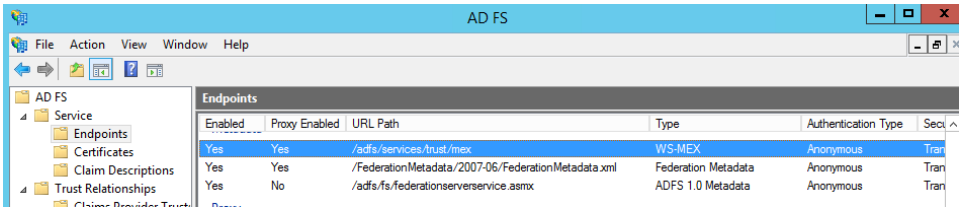
```
PS C:\> Get-MsolFederationProperty -DomainName labmetsys.fr | where {$_.Source -eq "Microsoft Office 365"} | Select-Obje
ct PassiveClientSignOutUrl,FederationMetadataUrl,ActiveClientSignInUrl | fl

PassiveClientSignOutUrl : https://adfs.labmetsys.fr/adfs/ls/
FederationMetadataUrl   : https://adfs.labmetsys.fr/adfs/services/trust/mex
ActiveClientSignInUrl   : https://adfs.labmetsys.fr/adfs/services/trust/2005/usernamemixed
```

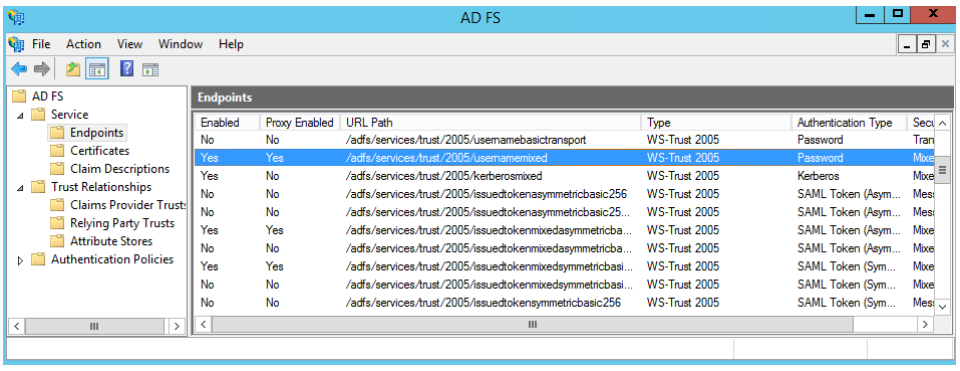
L'attribut *PassiveClientSignOutUrl* (*https://adfs.labmetsys.fr/adfs/ls*) renvoie vers le point de terminaison ADFS utilisé par les navigateurs web qui se connectent à Outlook Web App ou à Office Online.



L'attribut *FederationMetadataUrl* (*https://adfs.labmetsys.fr/adfs/services/trust/mex*) renvoie vers le point de terminaison ADFS utilisé par les clients *MEX* (clients Office 365 ProPlus / Office).



L'attribut *ActiveClientSignInUrl* (*https://adfs.labmetsys.fr/adfs/services/trust/2005/usernamemixed*) renvoie vers le point de terminaison ADFS utilisé par les serveurs Exchange Online. Nous verrons dans les paragraphes suivants que le client Outlook ne se comporte pas comme un client *MEX*.



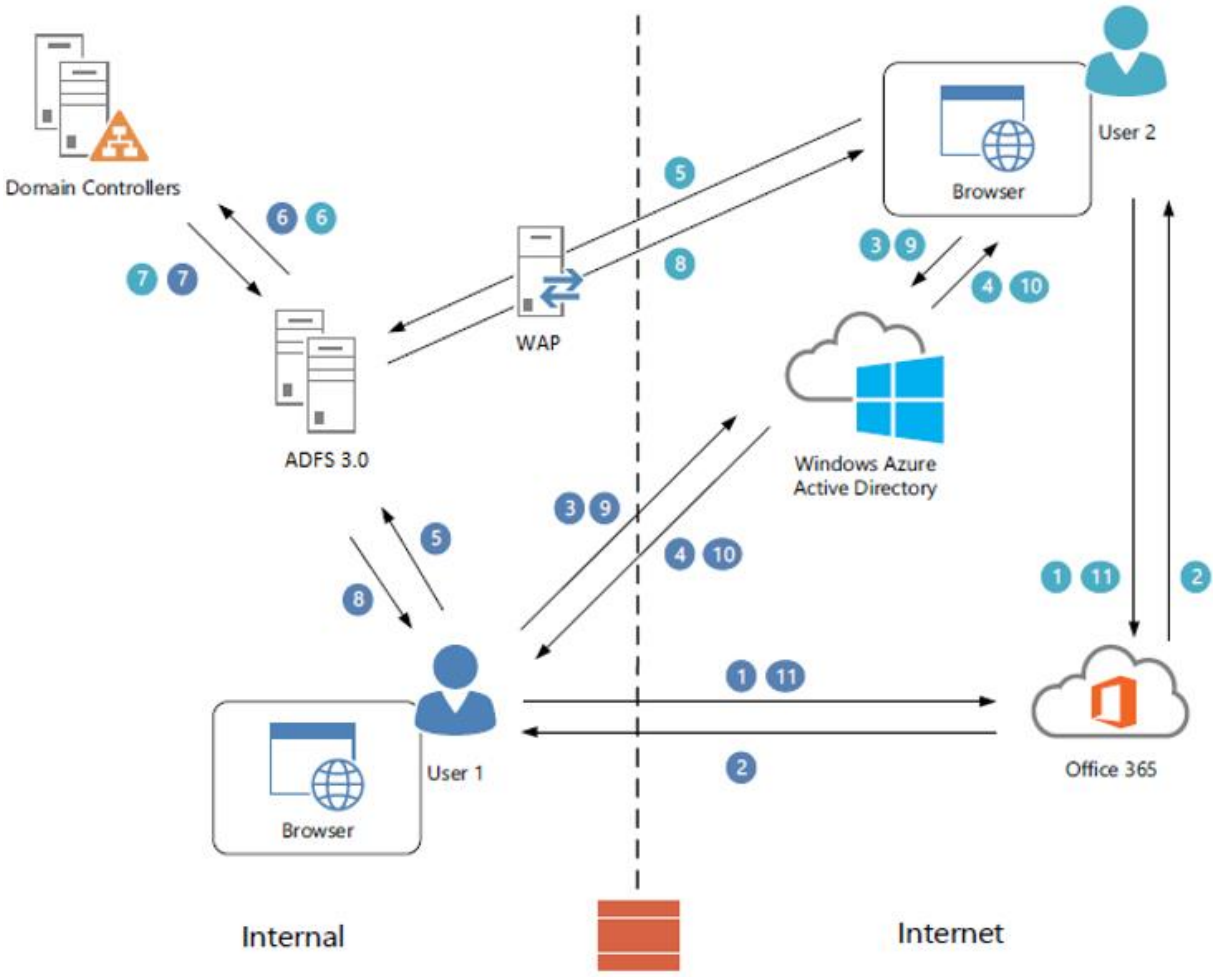
L'article Microsoft permet de connaître la durée de vie des jetons d'accès Office 365 :

https://support.office.com/en-US/article/Session-timeouts-for-Office-365-37a5c116-5b07-4f70-8333-5b86fd2c3c40

L'article http://www.msexchange.org/articles-tutorials/office-365/exchange-online/exchange-online-identity-models-and-authentication-demystified-part1.html permet d'en savoir plus sur le fonctionnement de la fédération d'identité avec Exchange Online.

6.2.2 Les clients passifs (web)

Le scénario d'authentification fédéré « passif » s'applique quand un utilisateur (dans cet exemple : *melanie.mathieu@msexperiences.msreport.fr*) se connecte à Outlook Web App, à un site web SharePoint Online, à son espace OneDrive For Busines ou accède à des documents hébergés sur SharePoint Online depuis un client Office ProPlus.

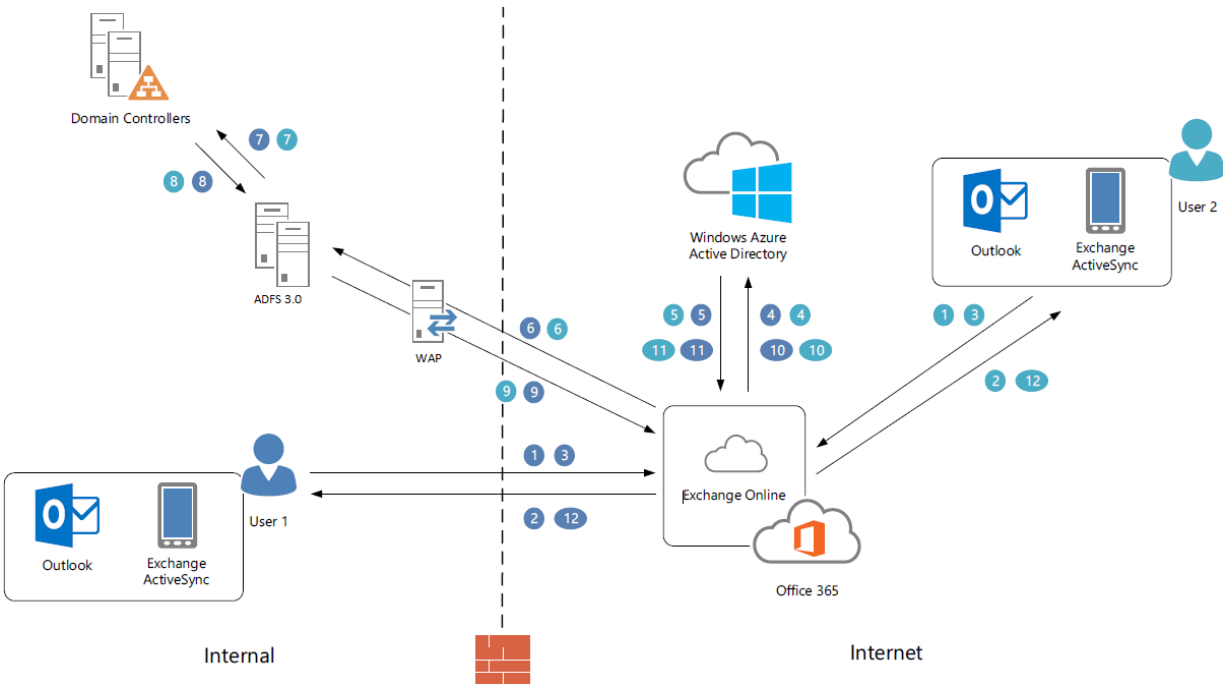


#	Flux
1	L'utilisateur *melanie.mathieu@msexperiences.msreport.fr* se contacte au site web Outlook Online (*Outlook Web App*, https://outlook.office.com).
2	Outlook Online indique qu'il a besoin d'un jeton d'authentification et renvoie l'URL du service d'authentification d'Office 365 https://login.microsoftonline.cxom à l'aide d'une redirection HTTP.
3	Le navigateur se connecte sur le service d'authentification d'Office 365 et saisit son adresse email.
4	Le service d'authentification d'Office 365 analyse le suffixe DNS de cette adresse email. Le service d'authentification d'Office 365 détecte que ce suffixe DNS (*@msexperiences.msreport.fr*) correspond à un domaine Office 365 de type *Federated* déclaré sur le Tenant Office 365 *LABMETSYS* et renvoie au navigateur web l'URL du serveur ADFS correspondant au client passif soit : *https://adfs.labmetsys.fr/adfs/ls/*
5	Si l'utilisateur se connecte depuis le réseau interne de l'entreprise, il s'authentifie en Kerberos ou NTLM auprès du serveur ADFS. Si l'URL adfs.lebametsys.fr a été ajouté dans la zone Intranet *Local d'Internet* Explorer 11, alors l'authentification se fait de manière transparente (authentification intégrée). Si l'utilisateur se connecte depuis un réseau extérieur, un formulaire web s'affiche (configuration par défaut du serveur ADFS 3.0).
6	Le serveur ADFS 3.0 interroge l'annuaire Active Directory (envoie du login / mot de passe de l'utilisateur). Le domaine Active Directory est en effet déclaré en tant que *Claims Provider Trust* et *Attributes Stores* dans la console ADFS 3.0.
7	Le contrôleur de domaine authentifie l'utilisateur.
8	Le serveur ADFS 3.0 construit un *jeton SAML 1.1* (*logon token*) qui contient les claims suivants : ➢ *UserPrincipalName :* la valeur de cet attribut doit correspondre à l'attribut UserPrincipalName du compte Azure Active Directory (annuaire Office 365). Le mappage *UserPrincipalName* Active Directory -> *UserPrincipalName* Azure Active Directory peut être modifié au niveau du serveur Azure Active Directory Connect. ➢ *ImmutableID :* c'est l'identifiant unique du compte utilisateur dans l'annuaire Azure Active Directory. Il correspond par défaut à l'attribut *ObjectGUID* convertit en base 64. Le mappage *ObjectGuid* -> *ImmutableID* peut être modifié au niveau du serveur Azure Active Directory Connect.
9	Le navigateur envoie le jeton SAML 1.1 (*logon token*) à l'aide d'une requête HTTP POST au service d'authentification d'Office 365.
10	Le service d'authentification d'Office 365 génère et renvoie au navigateur un jeton SAML d'authentification (*authentication token*) qui contient les claims suivants : ➢ *UserPrincipalName :* la valeur de cet attribut doit correspondre à l'attribut UserPrincipalName du compte Azure Active Directory (annuaire Office 365). ➢ *ImmutableID :* c'est l'identifiant unique du compte utilisateur dans l'annuaire Azure Active Directory.
11	Le navigateur web envoie ce jeton SAML d'authentification à *Outlook Online* (*Outlook Web App*). Ce dernier utilise la valeur des claims pour déterminer les droits de l'utilisateur au niveau du service puis autorise ou non l'accès au service.

6.2.3 Le scénario client actif

Le scénario d'authentification fédéré « *client actif* » s'applique quand un utilisateur (dans cet exemple : *melanie.mathieu@msexperiences.msreport.fr*) se connecte avec son client Outlook ou avec un client ActiveSync au serveur Exchange Online.

Le client Outlook ne sait pas nativement récupérer un jeton d'authentification. Cette tâche est donc réalisée par le serveur Exchange Online qui fait office de proxy. C'est pour cette raison, qu'un POPUP d'authentification s'affiche au démarrage d'Outlook même quand on utilise une solution de fédération d'identité avec Office 365. En pratique, le client Outlook fait une authentification de base auprès du serveur Exchange Online (login / mot de passe envoyé en clair via une connexion HTTPS).

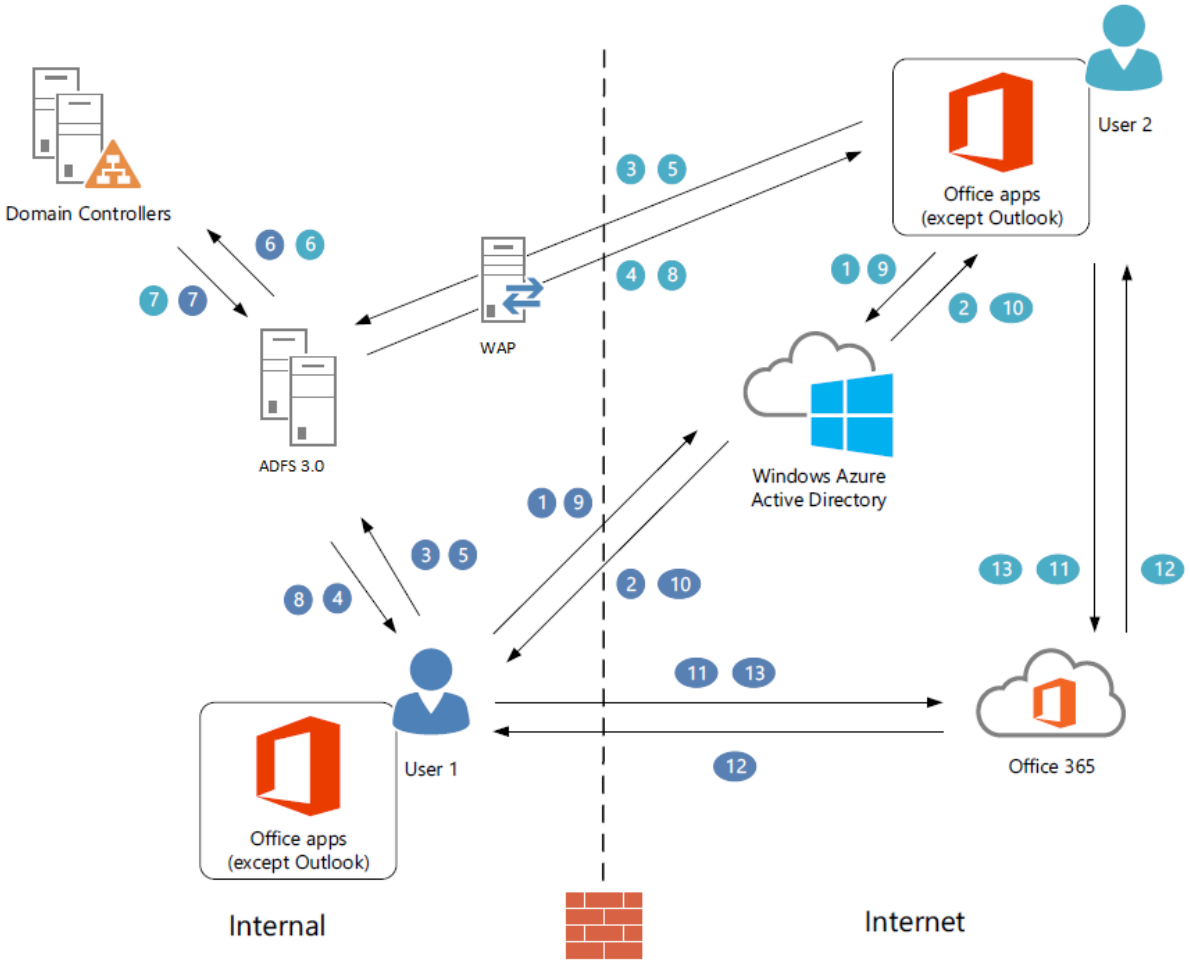


#	Flux
1	L'utilisateur *User 1* ouvre une session sur son ordinateur depuis le réseau de l'entreprise. L'utilisateur *User 2* ouvre une session sur son ordinateur depuis l'extérieur de l'entreprise (machine dans le domaine ou en groupe de travail). Les 2 utilisateurs démarrent Outlook 2013.
2	Exchange Online demande une authentification basique. L'utilisateur obtient une fenêtre de login / mot de passe et saisit alors son login (*UserPrincipalName* Active Directory, configuration par défaut) et son mot de passe. La fenêtre de login / mot de passe n'apparaît pas si l'utilisateur a mémorisé le mot de passe dans le coffre-fort de Windows.
3	Le login / mot de passe est envoyé au serveur Exchange Online.
4	Le serveur Exchange Online reprend ce login / mot de passe et l'utilise pour s'authentifier auprès d'un serveur Azure Active Directory. Le serveur Exchange Online se comporte dans le scénario *client actif* comme une sorte de proxy d'authentification.
5	Azure Active Directory analyse le suffixe de l'attribut *UserPrincipalName* et détermine alors que le domaine de messagerie Office 365 correspondant est un domaine de messagerie fédéré. Le serveur Azure Active Directory retourne alors l'URL du serveur de fédération d'identité associé à ce domaine de messagerie, dans notre cas le serveur ADFS 3.0 appelé *adfs.labmetsys.fr*.
6	Exchange Online envoie le login / mot de passe de l'utilisateur au serveur ADFS 3.0 et demande un jeton SAML 1.1.
7	Le serveur ADFS 3.0 contacte le contrôleur de domaine pour authentifier l'utilisateur.
8	Le contrôleur de domaine authentifie l'utilisateur.
9	Le serveur ADFS 3.0 génère un jeton SAML 1.1 (*logon token*) contenant les claims suivants : ➢ *UserPrincipalName :* la valeur de cet attribut doit correspondre à l'attribut *UserPrincipalName* du compte Azure Active Directory (annuaire Office 365). ➢ *ImmutableID :* c'est l'identifiant unique du compte utilisateur dans l'annuaire Azure Active Directory. Le jeton SAML est signé par le serveur ADFS 3.0.
10	Le serveur Exchange Online envoie le jeton d'authentification au serveur Azure Active Directory et le convertit en un jeton d'authentification (*authentication token*) qui contient : ➢ *UserPrincipalName :* la valeur de cet attribut doit correspondre à l'attribut *UserPrincipalName* du compte Azure Active Directory (annuaire Office 365). ➢ *ImmutableID :* c'est l'identifiant unique du compte utilisateur dans l'annuaire Azure Active Directory.
11	Le serveur Azure Active Directory valide l'accès de l'utilisateur.

6.2.4 Les clients MEX (Office 365 ProPlus / Office)

Le scénario d'authentification fédéré « *MEX* » s'applique quand les clients Office 365 ProPlus (Word, Excel…) s'activent (tous les 30 jours au minimum) ou quand les clients Office 2013 / 2016 (dont Office 365 ProPlus) se connectent à un site SharePoint Online ou OneDrive for Business (ouverture / sauvegarde d'un fichier).

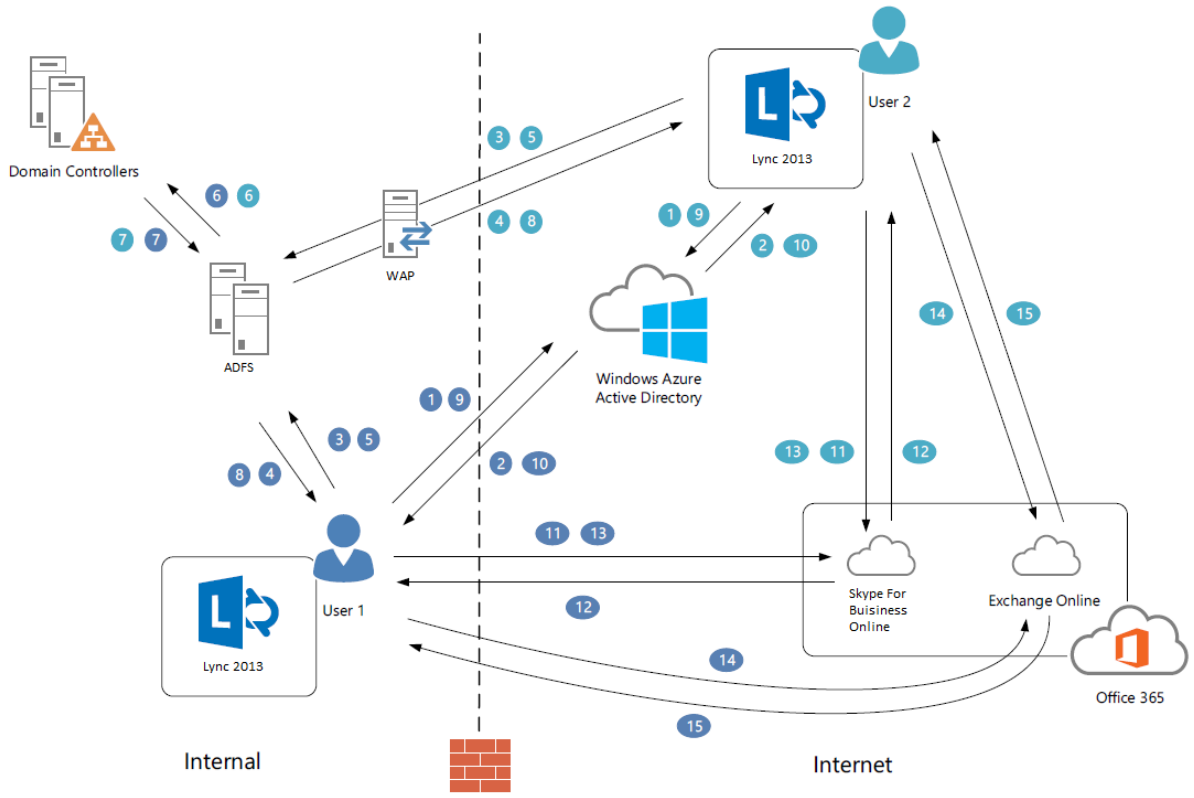
Les clients MEX s'appuient en fait sur le service *MSOIDSVC* soit le *Microsoft Online Sign Assistant*.



#	Flux
1	L'utilisateur *User 1* ouvre une session sur son ordinateur depuis le réseau de l'entreprise. L'utilisateur *User 2* ouvre une session sur son ordinateur depuis l'extérieur de l'entreprise (machine dans le domaine ou en groupe de travail). Les 2 utilisateurs démarrent le Word 2013. Le service *MSOIDSVC* (DLL d'Office 2013) s'authentifie avec le serveur Azure Active Directory. Le service *MSOIDSVC* copie le suffixe de messagerie de l'attribut *UserPrincipalName* du compte de l'utilisateur Active Directory et l'envoie au serveur Azure Active Directory. C'est pour cela que par défaut le suffixe DNS de l'attribut *UserPrincipalName* doit correspondre à un domaine de messagerie Office 365.
2	Le serveur Azure Active Directory vérifie si le suffixe DNS de l'utilisateur correspond à un domaine de messagerie Office 365 et si ce domaine est fédéré. Si le domaine de messagerie est fédéré, le serveur Azure Active Directory utilise la valeur de l'attribut *FederationMetadataUrl* de ce domaine de messagerie (commande *Get-MsolFederationProperty*). Dans notre cas, le serveur Azure Active Directory renvoie donc l'URL suivante au service MSOIDSVC. https://adfs.labmetsys.fr/adfs/services/trust/mex
3	Si une URL est retournée, le service MSOIDSVC contacte le serveur ADFS à cette adresse : https://adfs.labmetsys.fr/adfs/services/trust/mex.
4	Le serveur ADFS 3.0 renvoie la liste de tous les points de terminaison *Ws-Trust*.
5	Le service MSOIDSVC choisit le point de terminaison *Ws-Trust* et demande un jeton SAML 1.1 au serveur ADFS 3.0. Le service MSOIDSVC s'authentifie (Kerberos, NTLM) auprès du serveur ADFS 3.0 dans le contexte du compte de l'utilisateur.
6	Le serveur ADFS 3.0 contacte un contrôleur de domaine.
7	Le contrôleur de domaine valide le login / mot de passe de l'utilisateur.
8	Le serveur ADFS génère un jeton SAML 1.1 qui inclut les claims suivant : ➢ *UserPrincipalName :* la valeur de cet attribut doit correspondre à l'attribut UserPrincipalName du compte Azure Active Directory (annuaire Office 365). ➢ *ImmutableID :* c'est l'identifiant unique du compte utilisateur dans l'annuaire Azure Active Directory. Un jeton SAML (*logon token*) est renvoyé au service MSOIDSVC.
9	Le service *MSOIDSVC* renvoie le jeton SAML au serveur Azure Active Directory.
10	Le serveur Azure Active Directory vérifie le jeton et le convertit en un jeton d'authentification (*authentication token*) et le renvoie au service *MSOIDSVC*.
11	Le serveur MSOIDSVC se connecte au serveur Office 365.
12	Le serveur Office 365 demande un jeton SAML s'authentification.
13	Le client envoie le jeton SAML (*authentication token*) au serveur Office 365.

6.2.5 Le client Skype for Business (anciennement Lync)

Le scénario d'authentification fédéré « *client Skype for Business* » s'applique quand un utilisateur (dans cet exemple : *melanie.mathieu@msexperiences.msreport.fr*) se connecte avec son client Lync 2013 (Skype For Business). Ce scénario est une variante des scénarios *MEX* / *clients actifs* car Skype for Business Online s'appuie sur la liste de contact d'Exchange Online (*Unified contact store*).



#	Flux
1	L'utilisateur *User 1* ouvre une session sur son ordinateur depuis le réseau de l'entreprise. L'utilisateur *User 2* ouvre une session sur son ordinateur depuis l'extérieur de l'entreprise (machine dans le domaine ou en groupe de travail). Les 2 utilisateurs démarrent le client *Lync 2013*. Le service *MSOIDSVC* (installé avec Office 2013) s'authentifie avec le serveur Azure Active Directory. Le service *MSOIDSVC* envoie l'adresse SIP saisie par l'utilisateur dans son client Skype for Business au serveur Azure Active Directory.
2	Le serveur Azure Active Directory vérifie si le suffixe DNS de l'utilisateur correspond à un domaine de messagerie Office 365 et si ce domaine est fédéré. Si le domaine de messagerie est fédéré, le serveur Azure Active Directory utilise la valeur de l'attribut *FederationMetadataUrl* de ce domaine de messagerie (commande *Get-MsolFederationProperty*). Dans notre cas, le serveur Azure Active Directory renvoie donc l'URL suivante au service MSOIDSVC. https://adfs.labmetsys.fr/adfs/services/trust/mex
3	Si une URL est retournée, le service MSOIDSVC contacte le serveur ADFS à cette adresse : https://adfs.labmetsys.fr/adfs/services/trust/mex.
4	Le serveur ADFS 3.0 renvoie la liste de tous les points de terminaison *Ws-Trust*.
5	Le service *MSOIDSVC* choisit le point de terminaison *Ws-Trust* et demande un jeton SAML 1.1 au serveur ADFS 3.0. Le service *MSOIDSVC* s'authentifie (Kerberos, NTLM) auprès du serveur ADFS 3.0 dans le contexte du compte de l'utilisateur.
6	Le serveur ADFS 3.0 contacte un contrôleur de domaine.
7	Le contrôleur de domaine valide le login / mot de passe de l'utilisateur.
8	Le serveur ADFS génère un jeton SAML 1.1 qui inclut les claims suivant : ➢ *UserPrincipalName :* la valeur de cet attribut doit correspondre à l'attribut *UserPrincipalName* du compte Azure Active Directory (annuaire Office 365). ➢ *ImmutableID :* c'est l'identifiant unique du compte utilisateur dans l'annuaire Azure Active Directory. Un jeton SAML (*logon token*) est renvoyé au service *MSOIDSVC*.
9	Le service *MSOIDSVC* renvoie le jeton SAML au serveur Azure Active Directory.
10	Le serveur Azure Active Directory vérifie le jeton et le convertit en un jeton d'authentification (*authentication token*) et le renvoie au service *MSOIDSVC*.
11	Le serveur *MSOIDSVC* se connecte au serveur Skype For Business Online.
12	Le serveur Skype for Business Online demande un jeton SAML s'authentification.
13	Le client envoie le jeton SAML (*authentication token*) au serveur Skype For Business Online.
14	Le client envoie le jeton SAML (*authentication token*) à Exchange Web Services (car Skype For Business Online s'appuie sur la liste de contact Exchange Online ; *Unified contact store*).
15	Le service Exchange Web Services authentifie l'utilisateur et renvoie les informations demandées.

6.2.6 Office 365 Modern Authentication

Microsoft travaille depuis plusieurs années pour permettre à l'ensemble des services Office 365 de prendre en charge le protocole de fédération *OAUTH* (pour *Open Authentication*). Ce protocole de fédération d'identité est une norme standard et ouverte qui date de 2006 et qui est utilisée entre autres par Facebook et Google.

Le protocole *OAUTH* est activé de base au niveau de SharePoint Online. Il doit être activé manuellement au niveau d'Exchange Online et de Skype for Business Online avec les commandes PowerShell suivantes.

- *Set-OrganizationConfig -OAuth2ClientProfileEnabled:$true*
- *Set-CsOAuthConfiguration -ClientAdalAuthOverride Allowed*

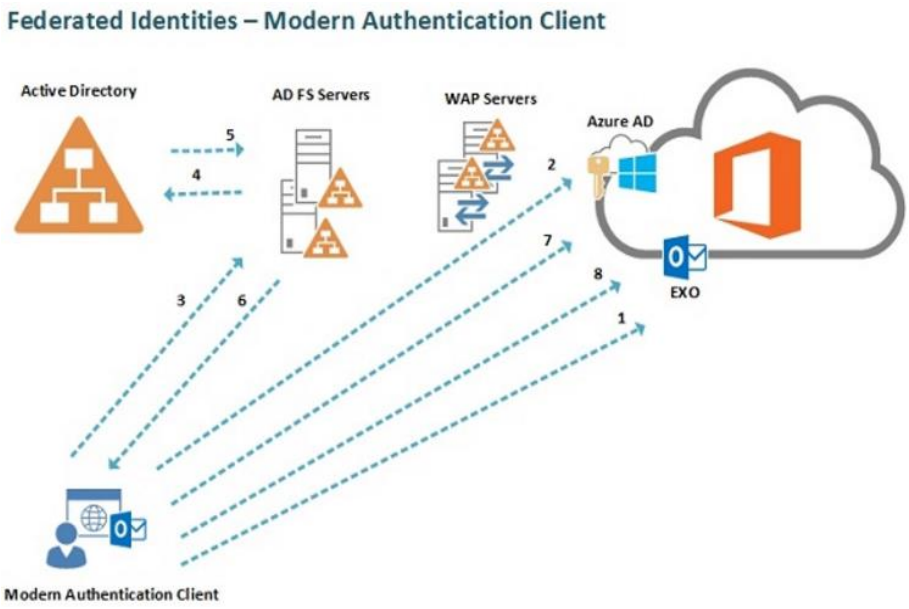
Microsoft a créé la librairie *Azure AD Authentication Library ou ADAL*. Cette librairie est déployée avec Office 2013 (depuis la version de mars 2015) et avec Office 2016 (fichier *C:\Program Files\Microsoft Office\root\VFS\ProgramFilesCommonX64\Microsoft Shared\OFFICE16 ADAL.DLL*). Elle remplace le composant *Microsoft Online Sign In Assistant* (fichier *MSO.DLL*). Toutes les applications Office 2013 / 2016 prennent donc en charge le protocole *OAUTH*. Avec le protocole *OAuth*, deux jetons d'authentification (*authentication token*) sont fournis au client quand il s'est authentifié avec succès au niveau du serveur Azure Active Directory :

- Un jeton d'accès qui est un *JSON Web Token* (*JWT*) et qui est valide pendant 1 heure.
- Un jeton de rafraîchissement qui est valable de 14 à 90 jours. Ce jeton permet de générer un nouveau jeton d'accès. Si l'utilisateur change de mot de passe, ce jeton de rafraîchissement devient invalide.

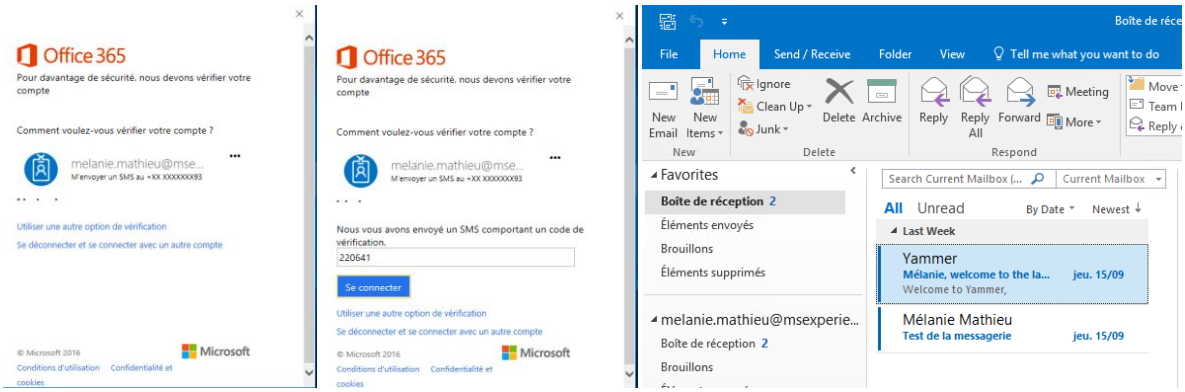
On notera que le protocole *OAUTH* est utilisé avec les domaines de type *Managed* et les domaines de type *Federated*. Les jetons *OAUTH* ne doivent pas être confondus avec les jetons *SAML.*

Quand un utilisateur se connecte avec son navigateur sur *Word Online* (ou *Outlook Web App*…) et qu'il appartient à un domaine Office 365 fédéré, le serveur Azure Active Directory (online) redirige toujours le navigateur vers un serveur de fédération d'identité (ADFS 3.0 dans notre exemple). Ce dernier authentifie toujours l'utilisateur et génère toujours un jeton *SAML 1.1*. Le navigateur présente ce jeton SAML 1.1 au serveur Azure Active Directory qui lui génère alors un jeton d'accès (JWT) et un jeton de rafraîchissement.

Tous les logiciels de la suite Office 2013 / 2016 intègrent maintenant un composant web qui permet à ces derniers de se comporter comme des clients web (*Ws-Federation*). Pour cette raison, Office 365 ne dispose plus que d'un seul scénario de fédération d'identité.



Le protocole ADAL permet aussi maintenant de prendre en charge l'authentification à 2 facteurs (ou plus) au niveau des clients Office 365 ProPlus (Word, Excel, Outlook).



Pour plus d'informations sur le protocole ADAL :

https://blogs.office.com/2014/11/12/office-2013-updated-authentication-enabling-multi-factor-authentication-saml-identity-providers

https://blogs.office.com/2015/11/19/updated-office-365-modern-authentication-public-preview/

https://blogs.office.com/2015/03/23/office-2013-modern-authentication-public-preview-announced/

https://blogs.office.com/2014/11/12/office-2013-updated-authentication-enabling-multi-factor-authentication-saml-identity-providers/

http://social.technet.microsoft.com/wiki/contents/articles/30214.office-2013-and-office-365-proplus-modern-authentication-things-to-know-before-onboarding.aspx

http://www.msexchange.org/articles-tutorials/office-365/exchange-online/exchange-online-identity-models-authentication-demystified-part5.html

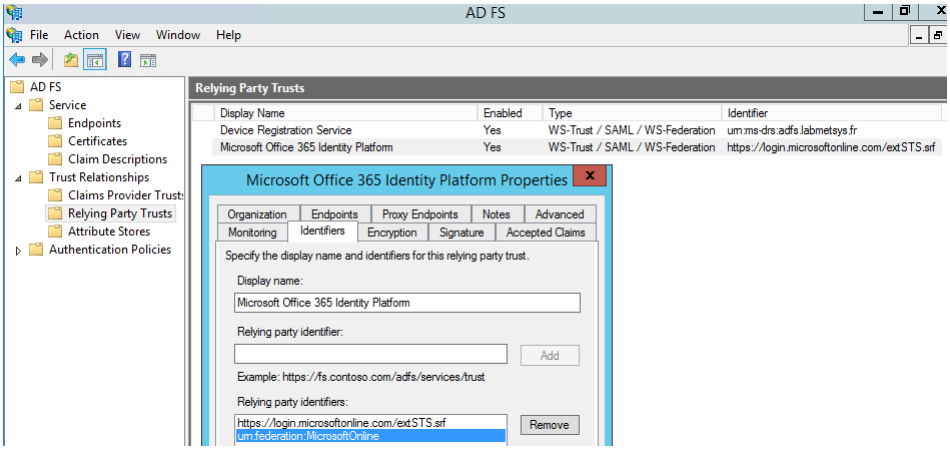
Nous vous conseillons d'activer ADAL pour améliorer l'expérience utilisateur que ce soit sur téléphone ou PC.

6.3 Présentation d'ADFS 3.0

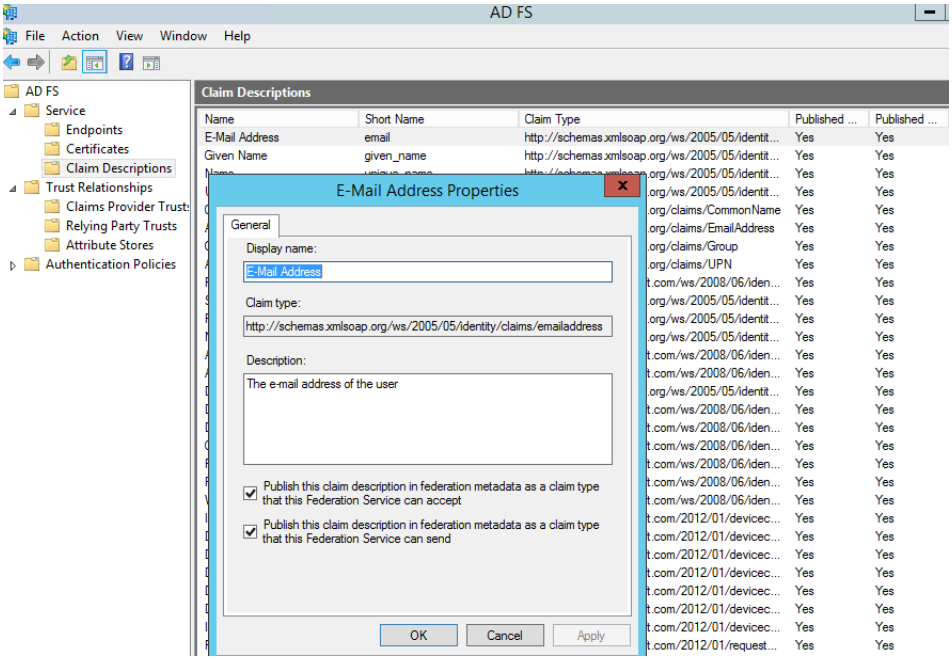
ADFS 3.0 est la solution de fédération d'identité de Microsoft. Cette solution joue le rôle d'intermédiaire de confiance entre 2 entités. Dans le cas d'Office 365, ADFS établit un lien de confiance entre l'annuaire Active Directory et l'annuaire Azure Active Directory d'Office 365. On notera que le serveur Azure Active Directory n'a pas d'accès direct à l'annuaire Active Directory (pas d'ouverture du port LDAP 389).

On peut voir ces deux relations de confiance au niveau des onglets :

- Le *Claim Provider Trust*
- Le *Relying Party Trust*.

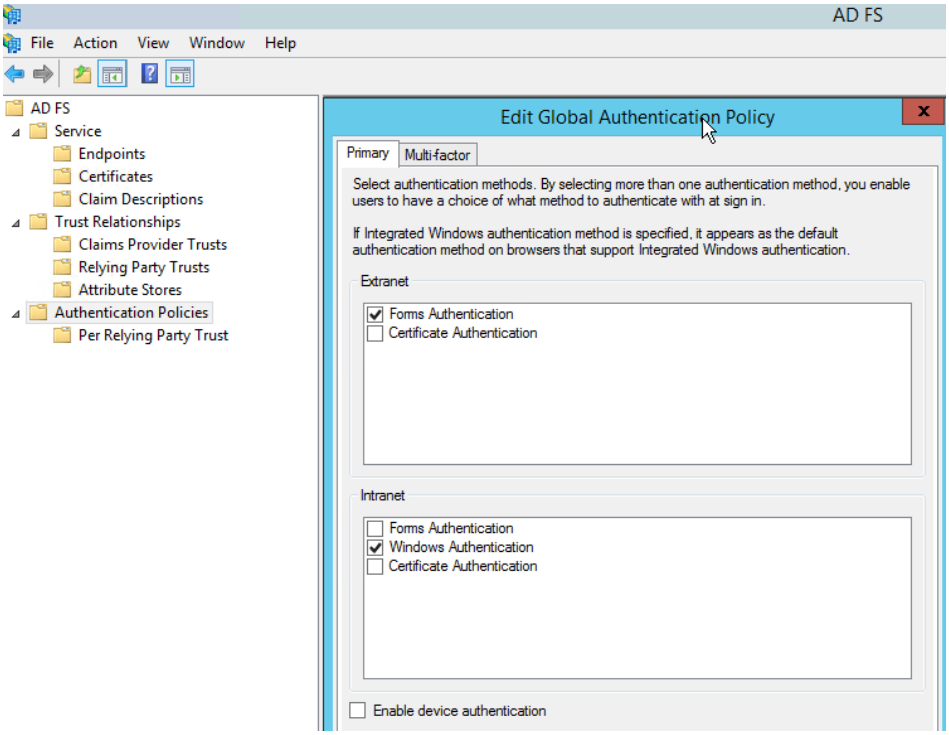


Microsoft ADFS 3.0 prend en charge les protocoles de fédération d'identité *WS-Federation*, *WS-Trust*, *OAUTH* et *SAML 2.0*. Le but d'un serveur ADFS est de générer un jeton de logon, généralement un jeton SAML 1.1 ou SAML 2.0. Un jeton SAML contient un ensemble des claims. Une fois le jeton SAML de logon généré, ce dernier est renvoyé au serveur Azure Active Directory qui permettra de générer le jeton d'authentification pour accéder aux services Office 365. Exemple de claims : *GivenName*, *LastName*, *SamAccountName.*

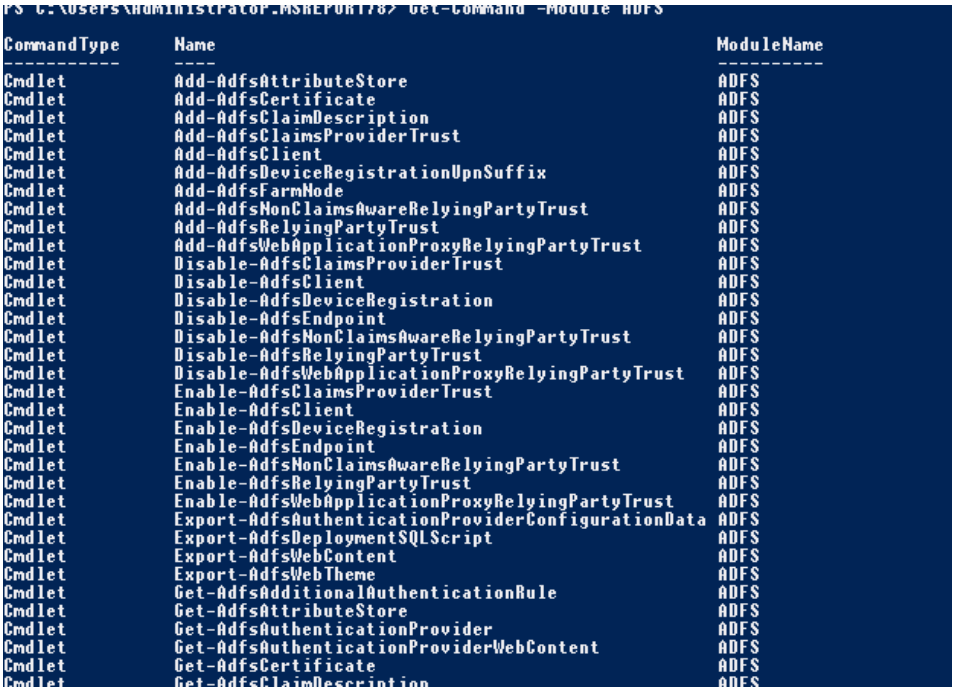


ADFS 3.0 prend en charge 3 méthodes d'authentification :

- Authentification par certificat
- Authentification intégrée
- Authentification par formulaire



Microsoft ADFS 3.0 peut être administré via une console MMC et un module PowerShell.



```
PS C:\Users\Administrator.MSREPUN178> Get-Command -Module ADFS

CommandType     Name                                               ModuleName
-----------     ----                                               ----------
Cmdlet          Add-AdfsAttributeStore                             ADFS
Cmdlet          Add-AdfsCertificate                                ADFS
Cmdlet          Add-AdfsClaimDescription                           ADFS
Cmdlet          Add-AdfsClaimsProviderTrust                        ADFS
Cmdlet          Add-AdfsClient                                     ADFS
Cmdlet          Add-AdfsDeviceRegistrationUpnSuffix                ADFS
Cmdlet          Add-AdfsFarmNode                                   ADFS
Cmdlet          Add-AdfsNonClaimsAwareRelyingPartyTrust            ADFS
Cmdlet          Add-AdfsRelyingPartyTrust                          ADFS
Cmdlet          Add-AdfsWebApplicationProxyRelyingPartyTrust       ADFS
Cmdlet          Disable-AdfsClaimsProviderTrust                    ADFS
Cmdlet          Disable-AdfsClient                                 ADFS
Cmdlet          Disable-AdfsDeviceRegistration                     ADFS
Cmdlet          Disable-AdfsEndpoint                               ADFS
Cmdlet          Disable-AdfsNonClaimsAwareRelyingPartyTrust        ADFS
Cmdlet          Disable-AdfsRelyingPartyTrust                      ADFS
Cmdlet          Disable-AdfsWebApplicationProxyRelyingPartyTrust   ADFS
Cmdlet          Enable-AdfsClaimsProviderTrust                     ADFS
Cmdlet          Enable-AdfsClient                                  ADFS
Cmdlet          Enable-AdfsDeviceRegistration                      ADFS
Cmdlet          Enable-AdfsEndpoint                                ADFS
Cmdlet          Enable-AdfsNonClaimsAwareRelyingPartyTrust         ADFS
Cmdlet          Enable-AdfsRelyingPartyTrust                       ADFS
Cmdlet          Enable-AdfsWebApplicationProxyRelyingPartyTrust    ADFS
Cmdlet          Export-AdfsAuthenticationProviderConfigurationData ADFS
Cmdlet          Export-AdfsDeploymentSQLScript                     ADFS
Cmdlet          Export-AdfsWebContent                              ADFS
Cmdlet          Export-AdfsWebTheme                                ADFS
Cmdlet          Get-AdfsAdditionalAuthenticationRule               ADFS
Cmdlet          Get-AdfsAttributeStore                             ADFS
Cmdlet          Get-AdfsAuthenticationProvider                     ADFS
Cmdlet          Get-AdfsAuthenticationProviderWebContent           ADFS
Cmdlet          Get-AdfsCertificate                                ADFS
Cmdlet          Get-AdfsClaimDescription                           ADFS
```

Je vous invite à lire les 6 articles ci-dessous qui expliquent en détail le fonctionnement d'un serveur ADFS :

https://blogs.technet.microsoft.com/askpfeplat/2014/08/24/adfs-deep-dive-primer/

https://blogs.technet.microsoft.com/askpfeplat/2014/11/02/adfs-deep-dive-comparing-ws-fed-saml-and-oauth/

https://blogs.technet.microsoft.com/askpfeplat/2014/11/23/adfs-deep-dive-planning-and-design-considerations/

https://blogs.technet.microsoft.com/askpfeplat/2015/01/26/adfs-deep-dive-certificate-planning/

https://blogs.technet.microsoft.com/askpfeplat/2015/03/01/adfs-deep-dive-onboarding-applications/

https://blogs.technet.microsoft.com/askpfeplat/2015/06/14/adfs-deep-dive-troubleshooting/

6.4 Déploiement d'ADFS et de Web Application Proxy (WAP)

6.4.1 Présentation générale

Nous allons déployer l'architecture suivante :

- 1 domaine Active Directory *LABMETSYS.INTRA* géré par 1 contrôleur de domaine Windows 2012 R2.
- 1 serveur ADFS 3.0 Windows 2012 R2 membre du domaine *LABMETSYS.INTRA*.
- 1 serveur Web Application Proxy (WAP) en MDZ membre d'un groupe de travail.

Le Tenant Office 365 sera configuré pour prendre en charge *Modern Authentication* (ADAL) pour Exchange Online et Skype for Business Online.

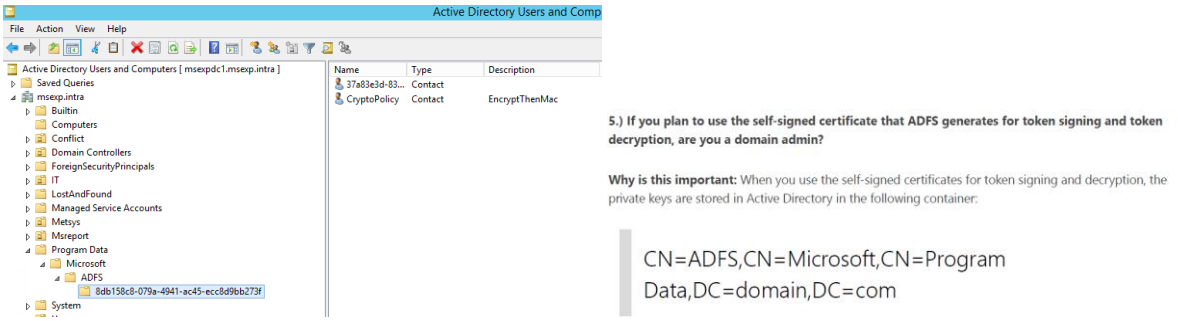
Pour déployer une solution hautement disponible, il est nécessaire de déployer un second serveur ADFS et un second serveur WAP et un cluster de 2 répartiteurs de charge. Je vous invite pour cela à lire le livre blanc de Kemp https://support.kemptechnologies.com/hc/en-us/articles/204250925-AD-FS-v3.

Le déploiement de cette solution se fera en 8 étapes :

- Validation des prérequis.
- Génération d'un certificat public *adfs.labmetsys.fr* auprès de l'autorité de certification en ligne *STARTSSL*. La génération de ce type de certificats est gratuite pour un usage non professionnel (pas d'utilisation en production).
- Création du compte de service *MSEXP\SVC-ADFS.*
- Installation du serveur Microsoft ADFS 3.0.
- L'installation du serveur WAP (Web Application Proxy).
- Configuration du Tenant Office 365.
- Activation de *Modern Authentication* (*ADAL*) au niveau du Tenant Office 365.
- Recette.

6.4.2 Validation des prérequis

Il faut disposer d'un compte membre du groupe *Domain Admins* pour déployer ADFS 3.0 car les clés privées pour le certificat de signature et de chiffrement du serveur ADFS sont stockées dans le conteneur *CN=ADFS,CN=Microsoft,CN=Program, Data,DC=domain,DC=COM.*



Vous devez disposer d'une adresse IP publique et rediriger le port 443 de cette IP vers l'adresse IP privée du serveur Web Application Proxy.

Le serveur Web Application Proxy et ADFS doivent aussi disposer d'un accès web restreint pour télécharger la CRL pour chaque certificat défini au niveau des *Relying Party Trust*.

15.) Do all your ADFS servers and ADFS Proxy/WAP servers have outbound TCP 80 open to the internet to perform certificate revocation checking?

Why is this important: To perform certificate revocation checking, all ADFS and ADFS Proxy/WAP servers must have TCP 80 outbound access.

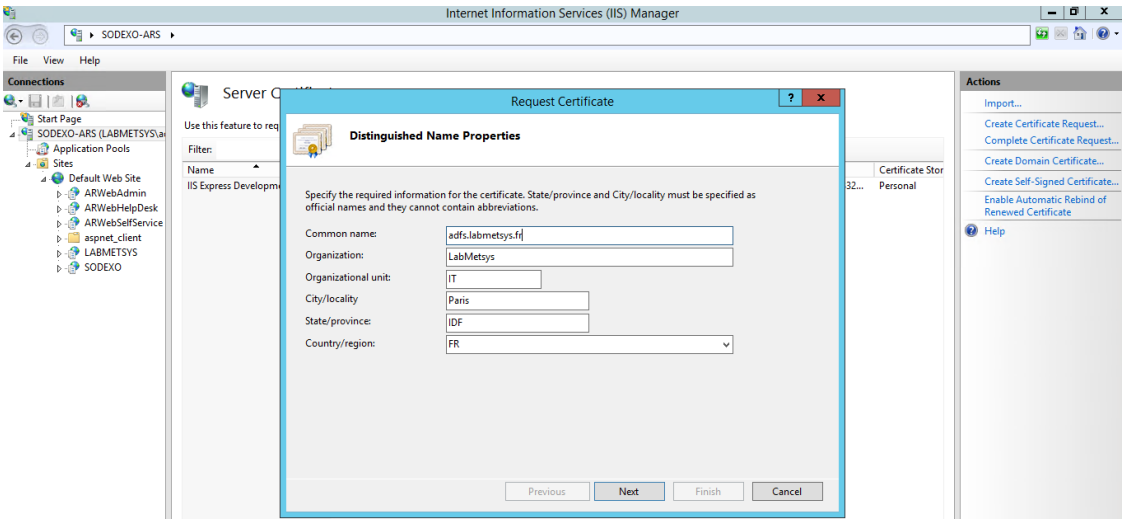
Il est recommandé que les certificats sur les serveurs WAP ne permettent pas l'exportation de la clé privée (protection contre le vol du certificat).

Mark the SSL Certificate Private Keys as Non-Exportable

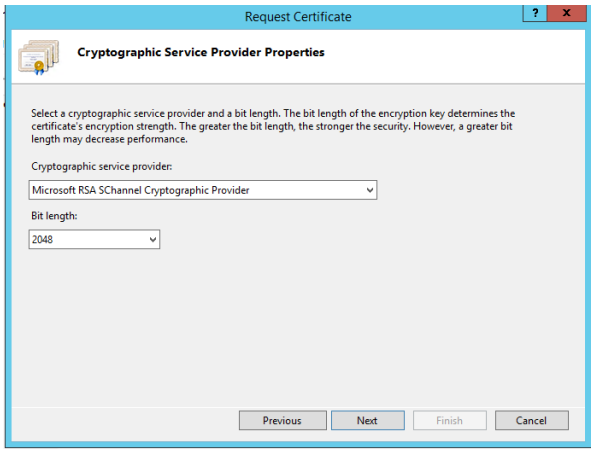
Being that the ADFS Proxy/WAP servers are public facing, I typically recommend that the SSL certificates private keys are marked as non-exportable.

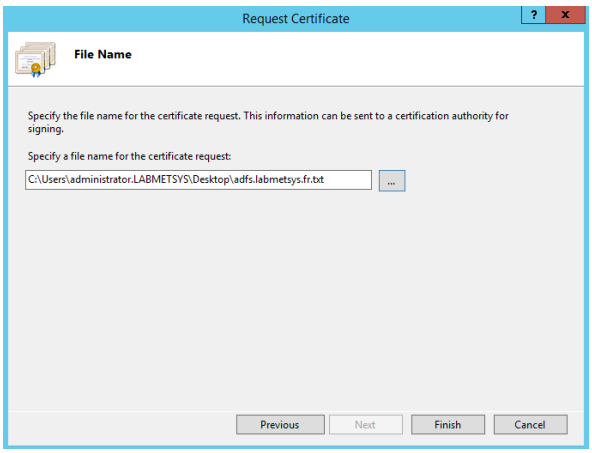
6.4.3 Génération du certificat ADFS.LABMETSYS.FR

Installer sur le serveur Web Application Proxy (WAP) le composant IIS (installation par défaut). Lancer la console IIS. Sélectionner le nom du serveur puis cliquer sur *Server Certificates*. Cliquer sur *Create Certificate Request*. Entrer comme *Common Name* la valeur *adfs.labmetsys.fr*.

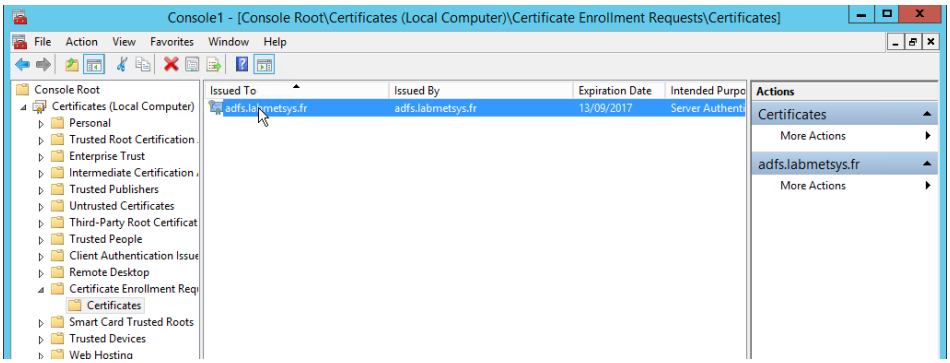


Sélectionner une taille de clé de 2048 bits (prérequis avec l'autorité de certification StartSSL). Sauvegarder la demande de certificats vers un fichier texte.





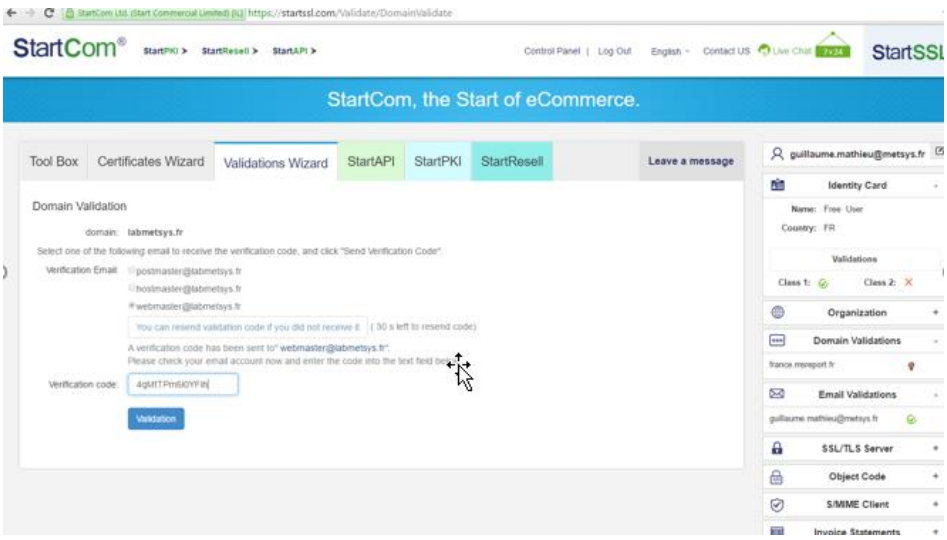
Si on se connecte au magasin de certificat ordinateur de la machine, on peut voir la demande de certificat dans le conteneur *Certificate Enrollment Requests*.



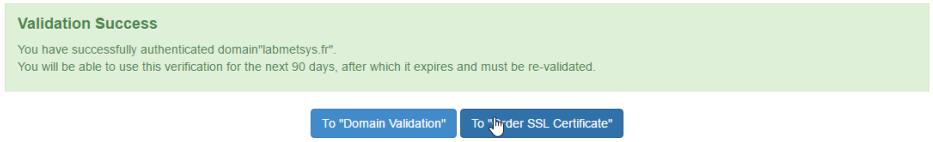
Lancer Internet Explorer et se connecter sur le site https://startssl.com.

Il est nécessaire de se créer un compte utilisateur client pour cela. On obtient alors un certificat utilisateur qui nous permettra de nous authentifier ensuite sur le site de *StartSSL*.

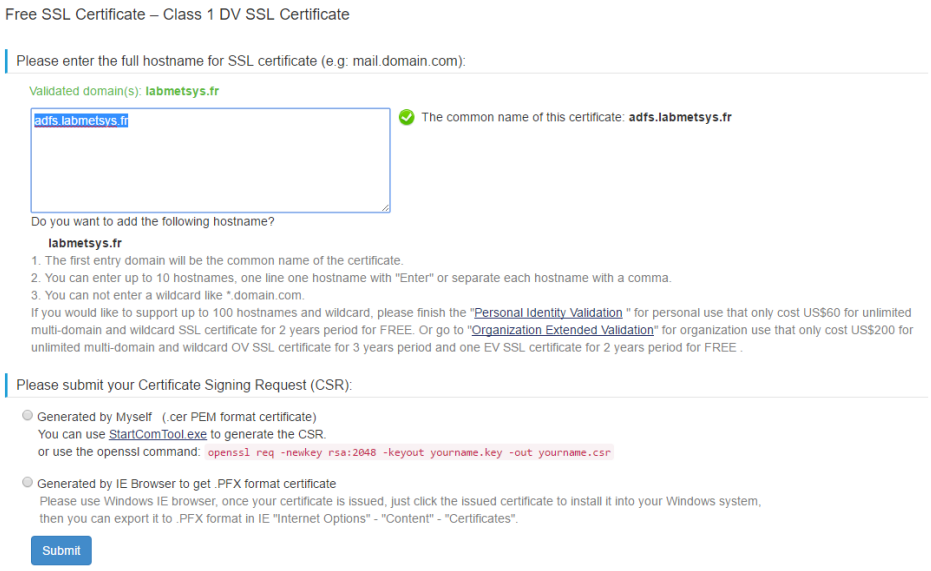
On va ensuite demander un certificat web. La première étape va consister à valider que l'on est bien le propriétaire du domaine DNS *LABMETSYS.FR*. Pour cela, il est nécessaire de configurer un compte Office 365 pour disposer d'une adresse de messagerie webmaster@labmetsys.fr. Un email avec un code de vérification est alors envoyé à cette adresse. Saisir ce code et cliquer sur le bouton *Validation*.



Une fois la validation effectuée, cliquer sur le bouton *To order SSL certificate*.

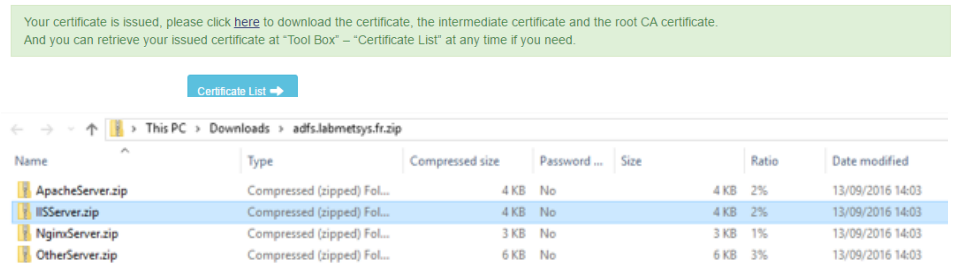


Entrer le nom du certificat, dans notre cas *ADFS.LABMETSYS.FR* et sélectionner *Generated by myself*.



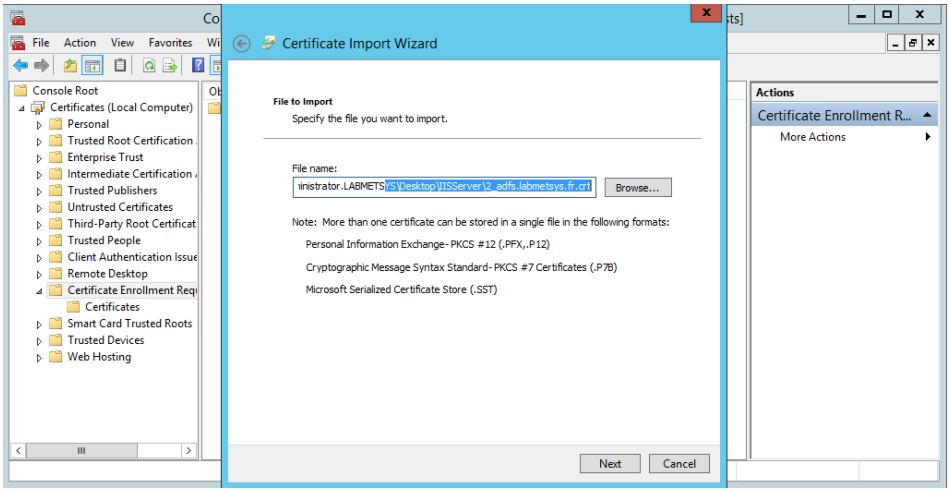
Il faut ensuite copier le contenu du fichier de demande de certificat généré précédemment. On notera qu'il faut supprimer la dernière ligne vide avec l'autorité de certification STARTSSL. Cliquer ensuite sur le bouton *Submit*.

Cliquer sur le bouton *here* pour télécharger le certificat. Dans notre cas, on utilisera le certificat au format *IIS*.

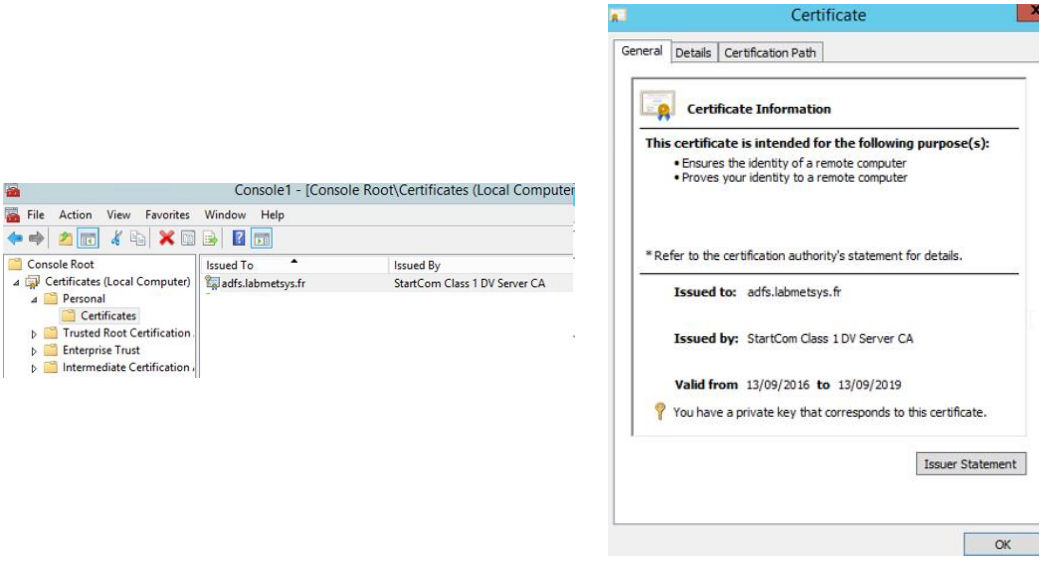


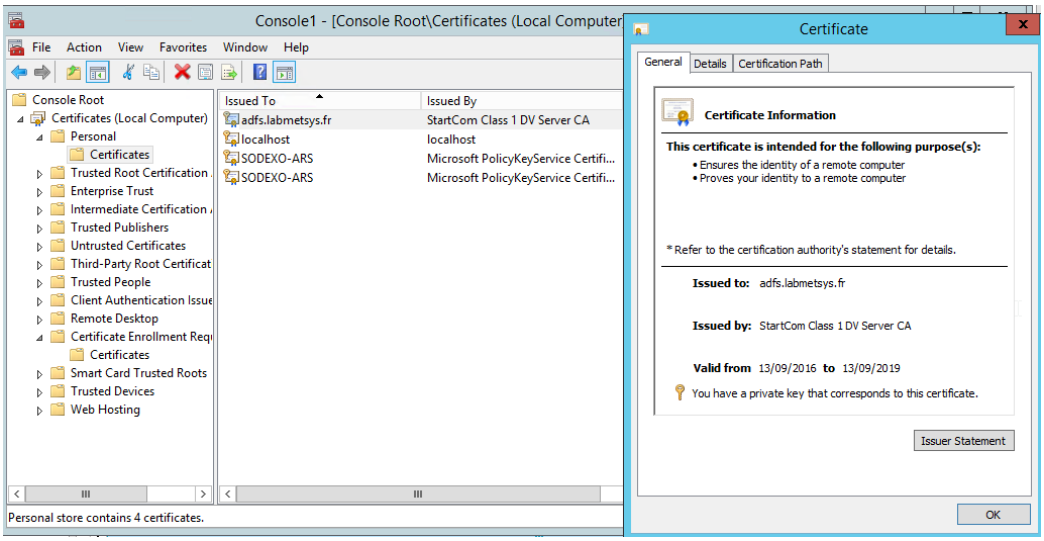
Ouvrir de nouveau le magasin de certificat ordinateur sur le serveur Web Application Proxy.

Faire un clic droit sur *Certificates Enrollment Request* puis cliquer sur *Certificate Import Wizard*.



On obtient alors le certificat *ADFS.LABMETSYS.FR*.

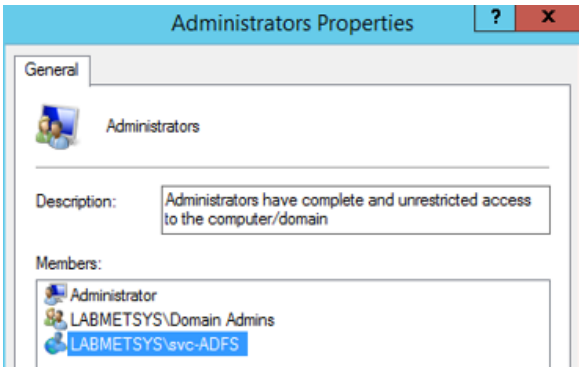




Exporter ensuite le certificat au format PFX (avec sa clé privée) et la copier sur le serveur ADFS.

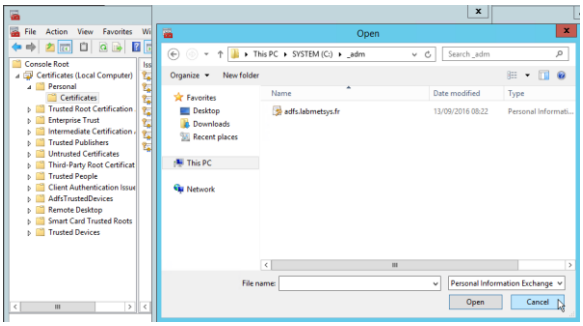
6.4.4 Créer le compte de service MSEXP\SVC-ADFS

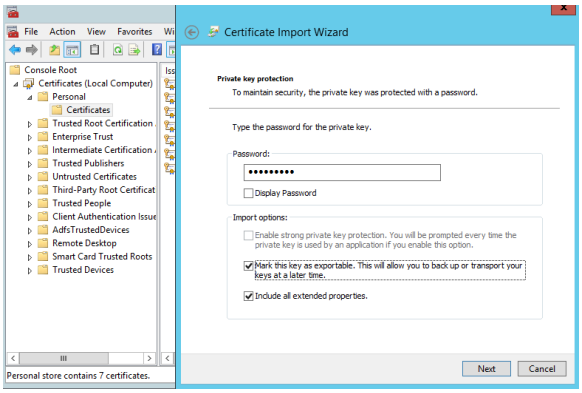
Créer le compte de service *svc-adfs* avec mot de passe qui n'expire jamais dans le domaine *MSEXP.INTRA*. Ce compte doit être configuré en tant qu'administrateur local sur le serveur ADFS 3.0 et le serveur *Web Application Proxy* (WAP).

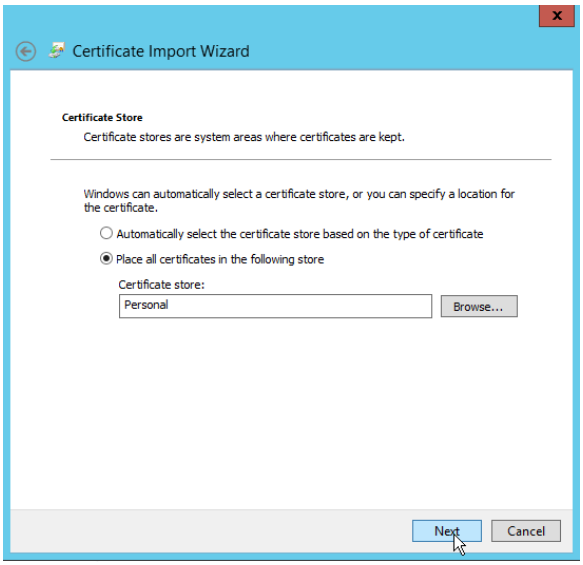


6.4.5 Installation du serveur Microsoft ADFS 3.0

Installer le rôle Active Directory federation Services sur le premier serveur. Une fois le rôle déployé, lancer l'assistant de configuration. Se connecter au magasin de certificat ordinateur et importer le certificat généré à l'étape précédente





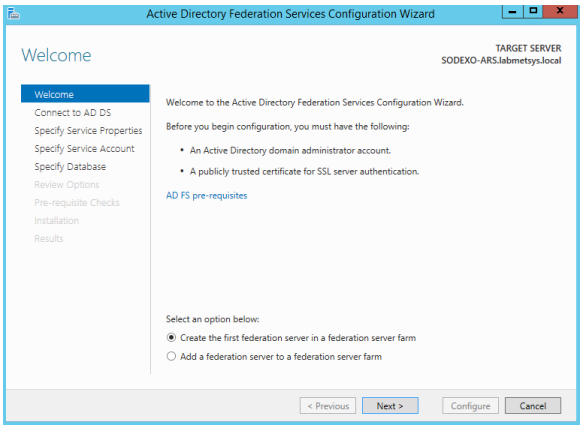


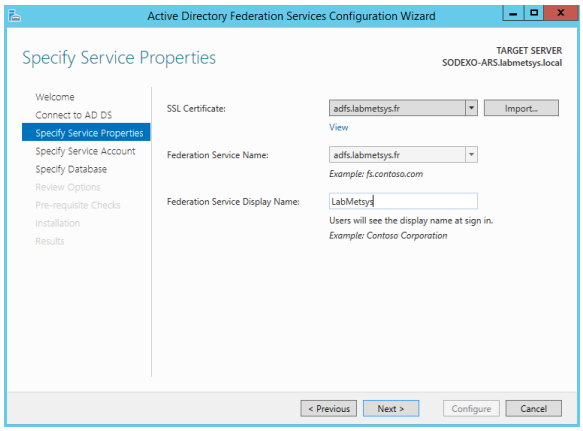
Sélectionner *Create the first federation server in a federation server farm* puis cliquer sur *Next*.

Sélectionner le certificat généré précédemment. Entrer les valeurs suivantes :

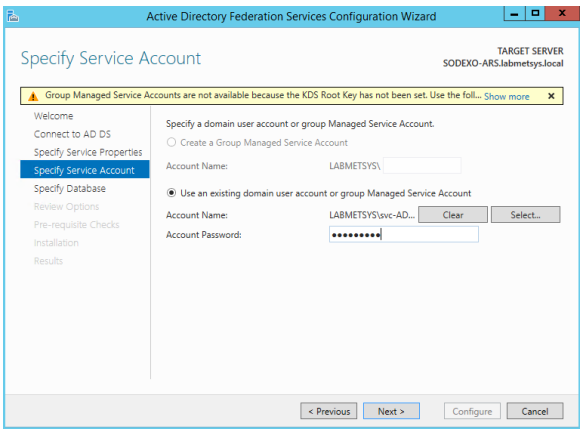
Federation Service Name : *adfs.labmetsys.fr*

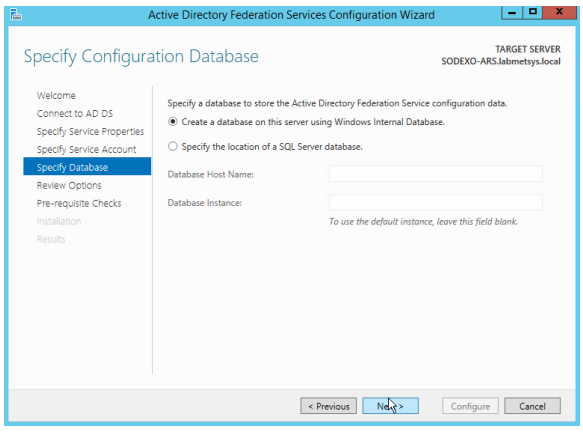
Federation Service Display Name : *LabMetsys*

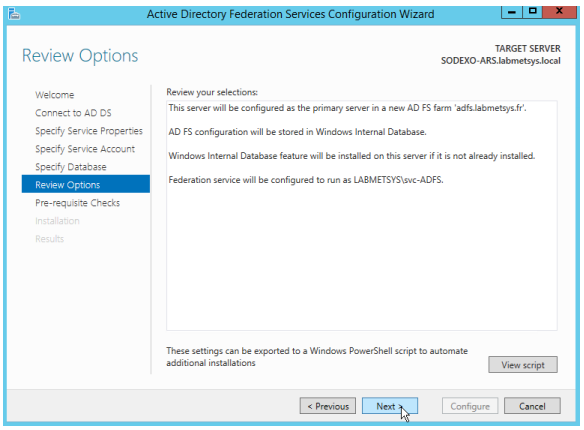


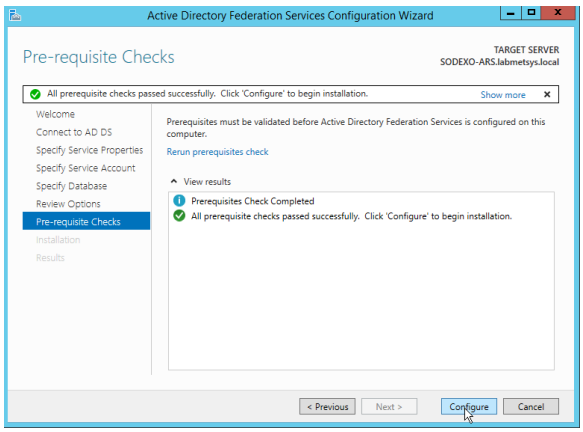


Sélectionner ensuite le compteb *labmetsys\svc-adfs*. Créer une base de données Windows Internal Database.



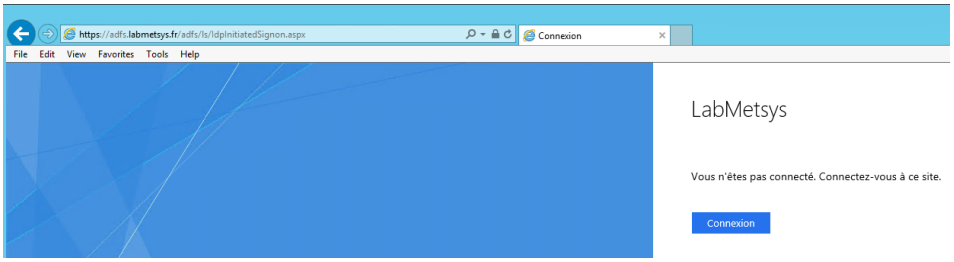






Il est ensuite nécessaire de valider le bon fonctionnement du serveur ADFS 3.0 en se connectant à l'adresse suivante : https://adfs.labmetsys.fr/adfs/ls/IdpInitiatedSignon.aspx

On notera qu'il est impératif de se connecter avec le nom DNS *ADFS.LABMETSYS.FR*.

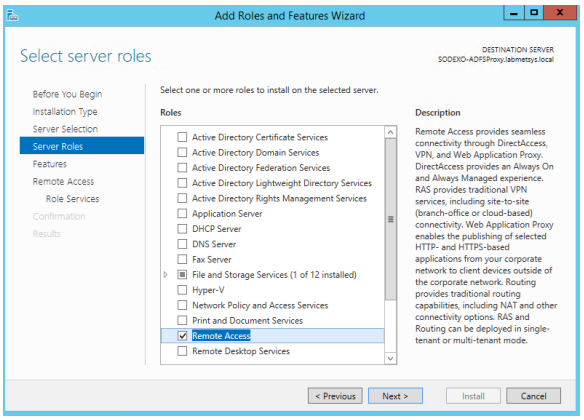


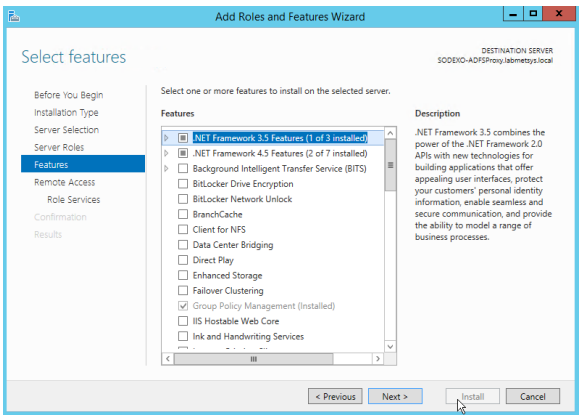
6.4.6 Installation du serveur Web Application Proxy

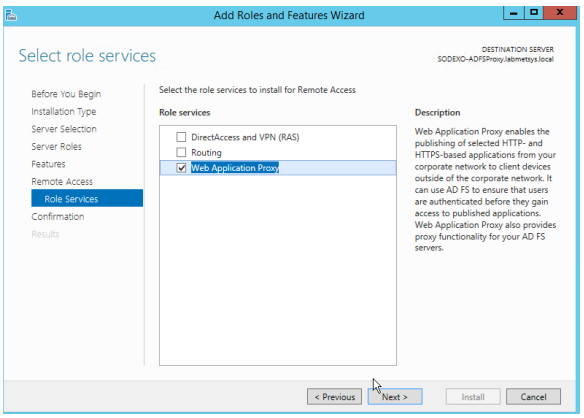
Le serveur WAP (*Web Application Proxy*) doit être en DMZ et installé sur une machine membre d'un groupe de travail. Cette machine doit être accessible depuis Internet au niveau du port TCP 443.

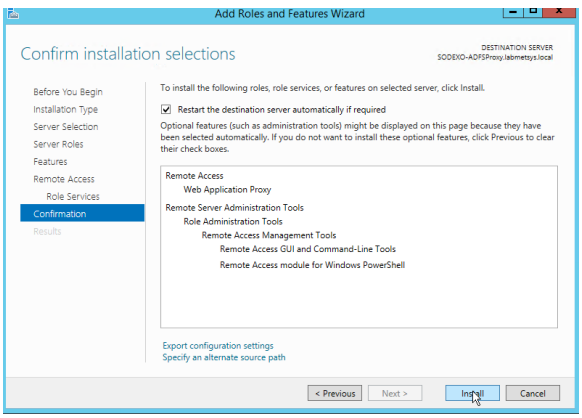
Importer le certificat *ADFS.LABMETSYS.FR* sur cette machine.

Installer ensuite le rôle *Remote Access* et sélectionner le rôle de service *Web Application Proxy*. Cette procédure est basée sur l'article Microsoft https://msdn.microsoft.com/en-us/library/azure/dn528859.aspx



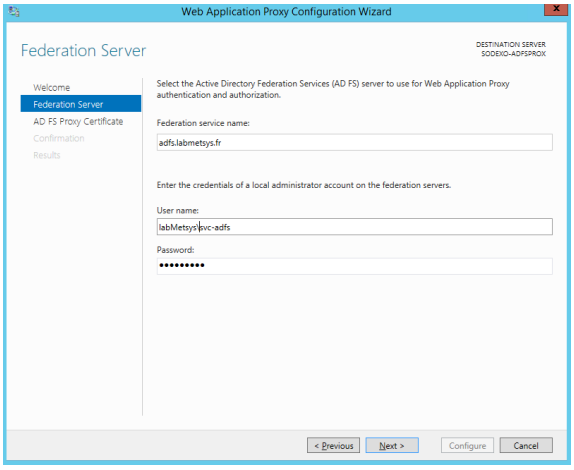


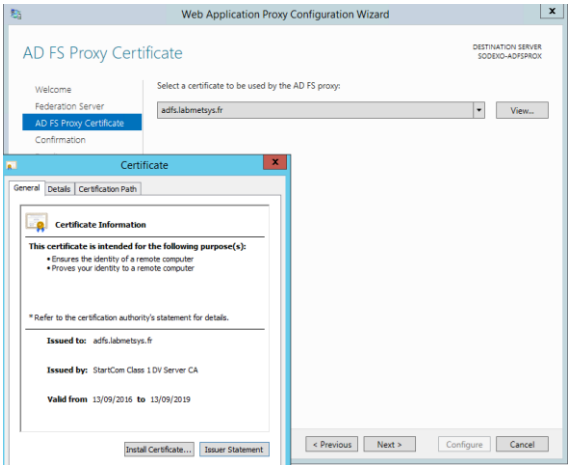




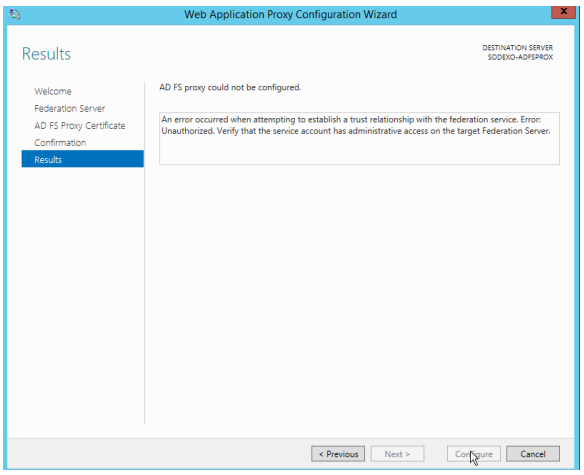
Une fois l'installation terminée, exécuter l'assistant de configuration de *Web Application Proxy* depuis la console *Remote Access Management* (*RAMgmtUI.exe*).

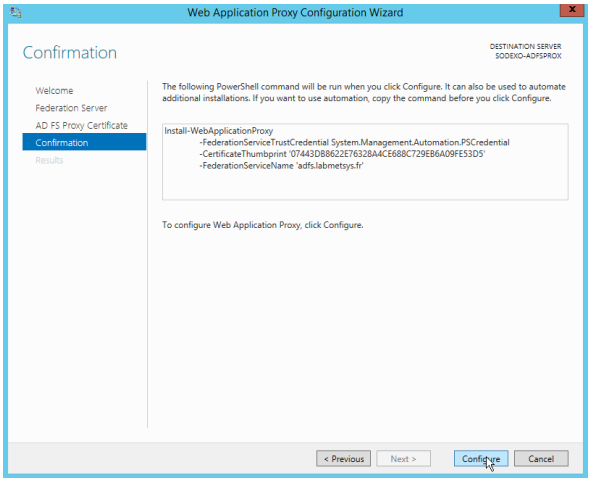
Entrer le nom de la ferme ADFS Proxy. On notera que dans notre cas, il est nécessaire de saisir *ADFS.LABMETSYS.FR*. Sur le serveur DNS interne (réseau local), cette entrée DNS doit résoudre l'IP interne du WAP. Depuis Internet, cette entrée DNS doit résoudre l'IP publique qui permet de publier le serveur WAP sur Internet.

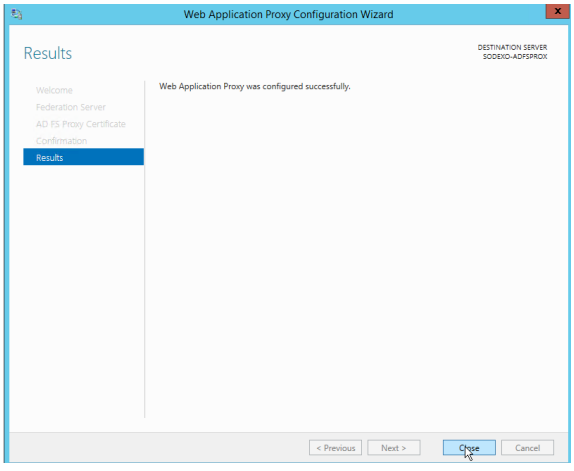




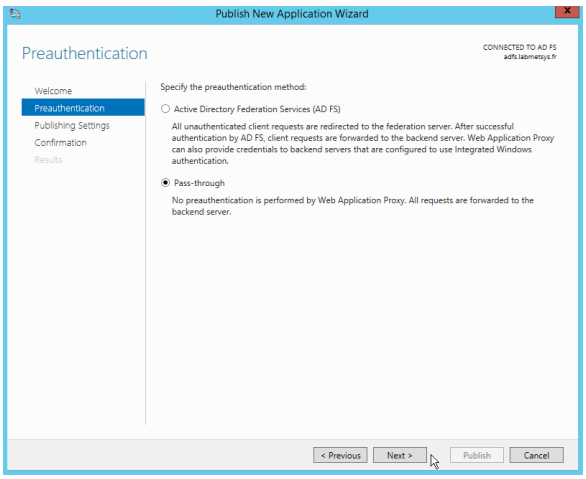
Cliquer ensuite sur *Install*.

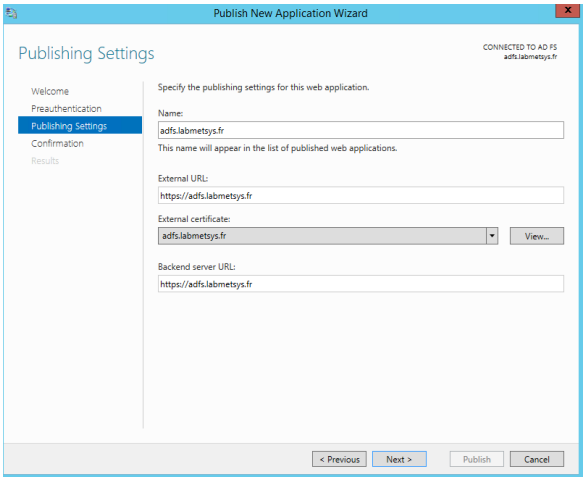


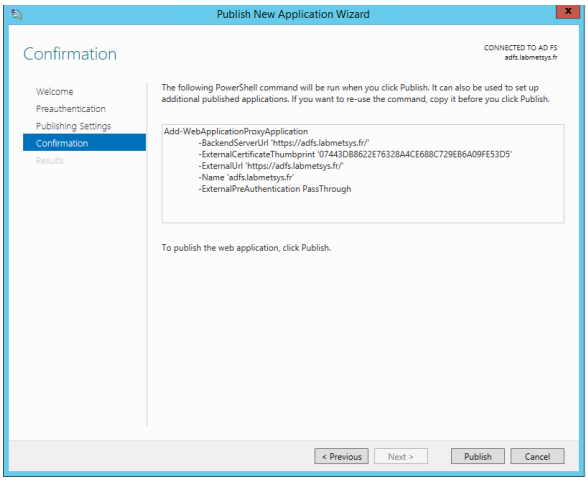


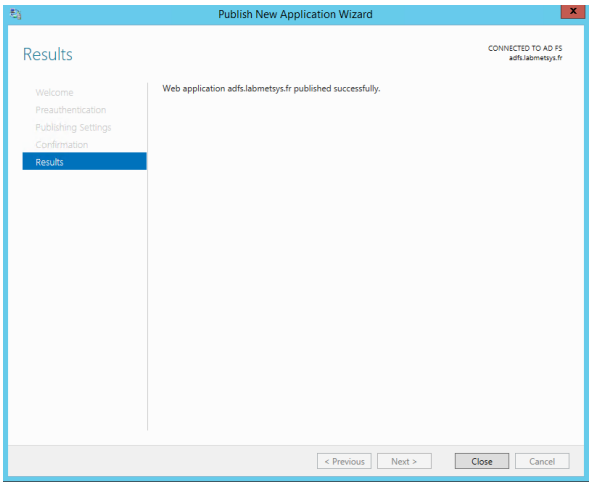


Il faut ensuite créer la publication. Cliquer sur *General | Publish*.

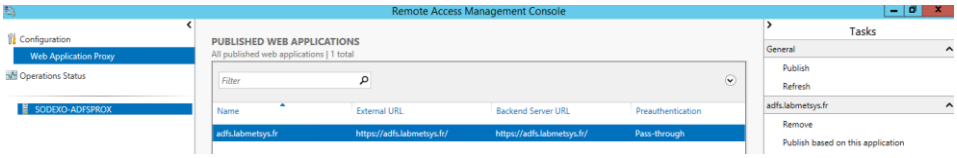






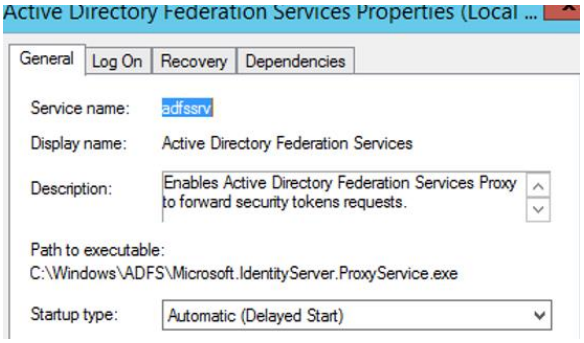


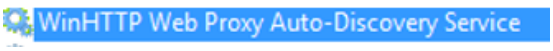
On obtient le résultat suivant

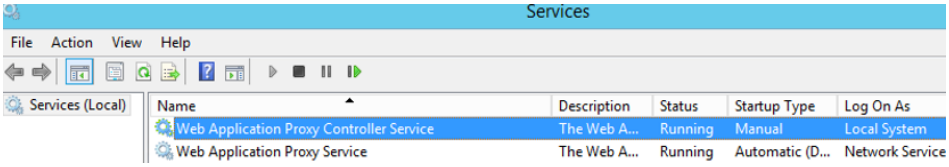


Il est maintenant nécessaire de valider si on peut accéder depuis une machine sur Internet à la page suivante : https://adfs.labmetsys.fr/adfs/ls/IdpInitiatedSignon.aspx

On notera que 4 services ont été créés sur le serveur Web Application Proxy.



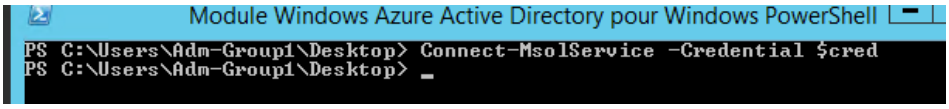




6.4.7 Configuration du Tenant Office 365.

Se connecter sur le serveur Microsoft ADFS 3.0. Installer le module PowerShell pour Azure Active Directory.

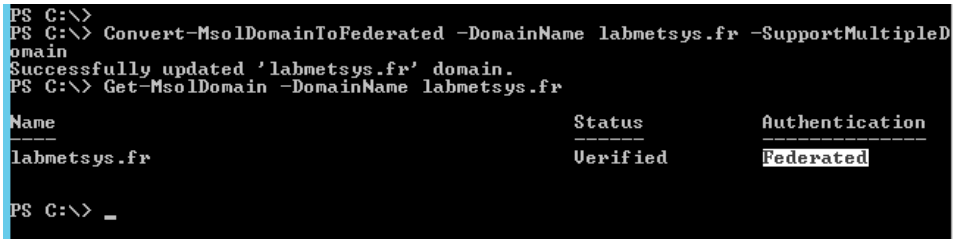
Lancer le module Power Shell Azure Active Directory en tant qu'administrateur (UAC) et exécuter les commandes suivantes : *Connect-MsolService –Credential $cred*



Vérifier l'état actuel des domaines avec la commande *Get-MsolDomain*.

Dans l'exemple ci-dessous, on va convertir le domaine *LABMETSYS.FR* en domaine *Federated* avec la commande :

Convert-MsolDomainToFederated -DomainName labmetsys.fr -SupportMultipleDomain



6.4.8 Activer le protocole ADAL au niveau de son tenant Office 365

La procédure ci-dessous est basée sur les articles Microsoft suivant :

http://social.technet.microsoft.com/wiki/contents/articles/32711.exchange-online-how-to-enable-your-tenant-for-modern-authentication.aspx

https://support.office.com/en-us/article/How-modern-authentication-works-for-Office-2013-and-Office-2016-client-apps-e4c45989-4b1a-462e-a81b-2a13191cf517?ui=en-US&rs=en-US&ad=US

Le nouveau protocole de fédération d'identité ADAL est activé par défaut pour SharePoint Online uniquement.

Il est nécessaire de l'activer manuellement pour Exchange Online puis pour Skype for Business Online.

Extrait de l'article http://social.technet.microsoft.com/wiki/contents/articles/32711.exchange-online-how-to-enable-your-tenant-for-modern-authentication.aspx :

We recommend that you enable your Exchange Online tenant for modern authentication prior to enabling Skype for Business Online for modern authentication.

La commande ci-dessous permet de voir si ADAL est activé au niveau de votre organisation Exchange Online :

*Get-OrganizationConfig | ft name, *OAuth**

```
PS C:\> Get-OrganizationConfig | ft name, *OAuth*

Name                                               OAuth2ClientProfileEnabled
----                                               --------------------------
labmetsys.onmicrosoft.com                                              False
```

La commande ci-dessous permet d'activer ADAL au niveau de l'organisation Exchange Online :

Set-OrganizationConfig -OAuth2ClientProfileEnabled:$true

Télécharger et installer ensuite le module PowerShell pour Skype for Business Online à l'adresse suivante :

https://www.microsoft.com/en-us/download/details.aspx?id=39366

Il faut ensuite se connecter à Skype For Business Online

$session = New-CsOnlineSession -Credential $credential

Import-PSSession $session

Taper la commande suivante pour valider si ADAL est activé pour Skype for Business Online :

Get-CsOAuthConfiguration

```
PS C:\Users\administrator.LABMETSYS> Get-CsOAuthConfiguration

Identity                                : Global
PartnerApplications                     : {Name=microsoft.exchange;ApplicationIdentifier=00000002-0000-0ff1-ce00-000000000000;Realm=;ApplicationTrustLevel=Full;AcceptSecurityIdentifierInformation=False;Enabled=True, Name=microsoft.sharepoint;ApplicationIdentifier=00000003-0000-0ff1-ce00-000000000000;Realm=;ApplicationTrustLevel=Full;AcceptSecurityIdentifierInformation=False;Enabled=True, Name=microsoft.skype.platformmonitoringservice;ApplicationIdentifier=44ff763b-5d1f-40ab-95bf-f31a18757998;Realm=;ApplicationTrustLevel=Full;AcceptSecurityIdentifierInformation=False;Enabled=True, Name=microsoft.skype;ApplicationIdentifier=00000004-0000-0ff1-ce00-000000000000;Realm=;ApplicationTrustLevel=Full;AcceptSecurityIdentifierInformation=False;Enabled=True}
OAuthServers                            : {Name=microsoft.sts;IssuerIdentifier=00000001-0000-0000-c000-000000000000;Realm=;MetadataUrl=https://accounts.accesscontrol.windows.net/metadata/json/1;AuthorizationUriOverride=;Type=Acs;AcceptSecurityIdentifierInformation=False, Name=evosts;IssuerIdentifier=sts.windows.net;Realm=;MetadataUrl=https://login.windows.net/common/FederationMetadata/2007-06/FederationMetadata.xml;AuthorizationUriOverride=;Type=AzureAd;AcceptSecurityIdentifierInformation=False}
Realm                                   :
ServiceName                             : 00000004-0000-0ff1-ce00-000000000000
ClientAuthorizationOAuthServerIdentity  : evosts
ExchangeAutodiscoverUrl                 : https://pilot.outlook.com/autodiscover/autodiscover.svc
ExchangeAutodiscoverAllowedDomains      : *.outlook.com;*.microsoft.com
ClientAdalAuthOverride                  : Disallowed
AlternateAudienceUrl                    :
```

Exécuter la commande ci-dessous pour activer le protocole ADAL :

Set-CsOAuthConfiguration -ClientAdalAuthOverride Allowed

```
PS C:\Users\administrator.LABMETSYS> Set-CsOAuthConfiguration -ClientAdalAuthOverride Allowed
PS C:\Users\administrator.LABMETSYS> Get-CsOAuthConfiguration

Identity                                : Global
PartnerApplications                     : {Name=microsoft.exchange;ApplicationIdentifier=00000002-0000-0ff1-ce00-000000000000;Realm=;ApplicationTrustLevel=Full;AcceptSecurityIdentifierInformation=False;Enabled=True, Name=microsoft.sharepoint;ApplicationIdentifier=00000003-0000-0ff1-ce00-000000000000;Realm=;ApplicationTrustLevel=Full;AcceptSecurityIdentifierInformation=False;Enabled=True, Name=microsoft.skype.platformmonitoringservice;ApplicationIdentifier=44ff763b-5d1f-40ab-95bf-f31a18757998;Realm=;ApplicationTrustLevel=Full;AcceptSecurityIdentifierInformation=False;Enabled=True, Name=microsoft.skype;ApplicationIdentifier=00000004-0000-0ff1-ce00-000000000000;Realm=;ApplicationTrustLevel=Full;AcceptSecurityIdentifierInformation=False;Enabled=True}
OAuthServers                            : {Name=microsoft.sts;IssuerIdentifier=00000001-0000-0000-c000-000000000000;Realm=;MetadataUrl=https://accounts.accesscontrol.windows.net/metadata/json/1;AuthorizationUriOverride=;Type=Acs;AcceptSecurityIdentifierInformation=False, Name=evosts;IssuerIdentifier=sts.windows.net;Realm=;MetadataUrl=https://login.windows.net/common/FederationMetadata/2007-06/FederationMetadata.xml;AuthorizationUriOverride=;Type=AzureAd;AcceptSecurityIdentifierInformation=False}
Realm                                   :
ServiceName                             : 00000004-0000-0ff1-ce00-000000000000
ClientAuthorizationOAuthServerIdentity  : evosts
ExchangeAutodiscoverUrl                 : https://pilot.outlook.com/autodiscover/autodiscover.svc
ExchangeAutodiscoverAllowedDomains      : *.outlook.com;*.microsoft.com
ClientAdalAuthOverride                  : Allowed
AlternateAudienceUrl                    :


PS C:\Users\administrator.LABMETSYS> _
```

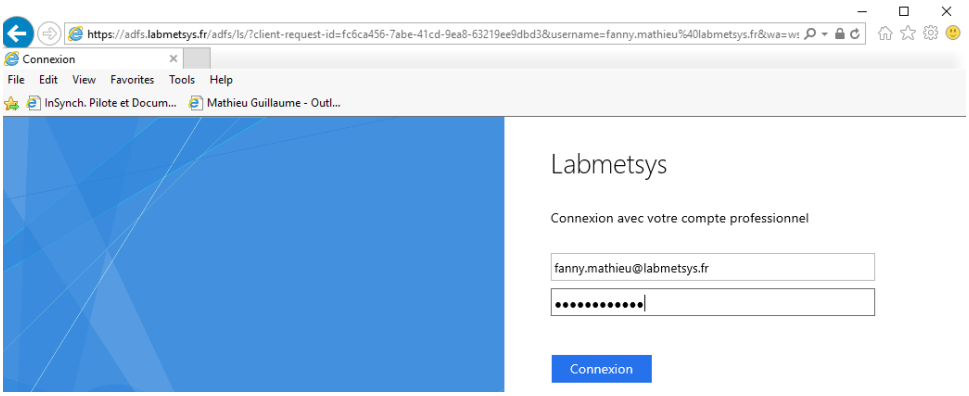
Si vous disposez de client Office 2013, il faut créer les deux entrées de registre suivantes. Avec Office 2016, ADAL est utilisé par défaut.

https://support.office.com/en-us/article/How-modern-authentication-works-for-Office-2013-and-Office-2016-client-apps-e4c45989-4b1a-462e-a81b-2a13191cf517?ui=en-US&rs=en-US&ad=US

Entrée	Type	Valeur
HKCU\SOFTWARE\Microsoft\Office\15.0\Common\Identity\EnableADAL	REG_DWORD	1
HKCU\SOFTWARE\Microsoft\Office\15.0\Common\Identity\Version	REG_DWORD	1

6.4.9 Recette

Se connecter sur https://outlook.office365.com depuis une machine sur Internet (non connectée au réseau de l'entreprise). Le formulaire ci-dessous s'affiche.

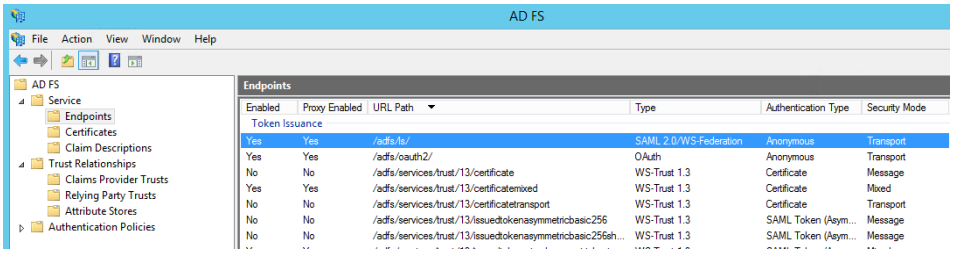


Copier / coller l'URL du navigateur et analyser son contenu :

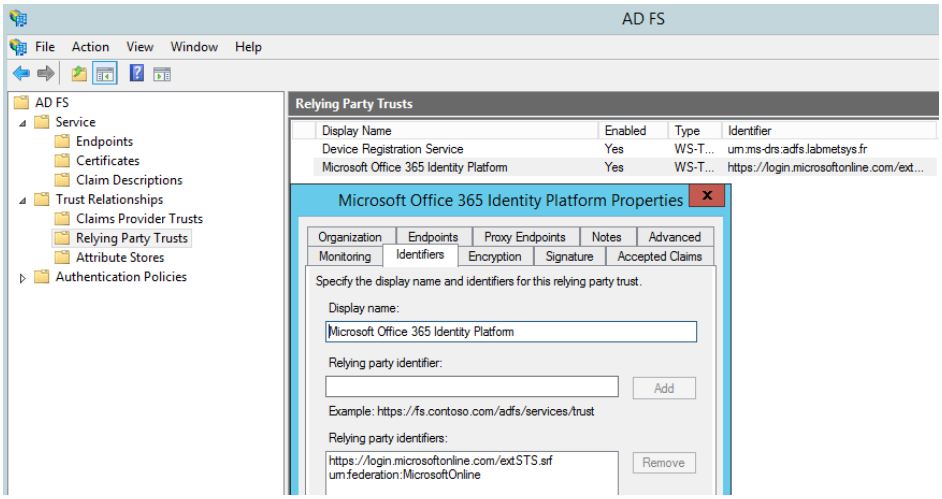
https://adfs.labmetsys.fr/adfs/ls/?client-request-id=fc6ca456-7abe-41cd-9ea8-63219ee9dbd3&username=fanny.mathieu%40labmetsys.fr&wa=wsignin1.0&wtrealm=urn%3afederation%3aMicrosoftOnline&wctx=estsredirect%3d2%26estsrequest%3drQIIAeNisNLJKCkpKLbS1y_ILypJzNHLzUwuyi_OTyvJz8vJzEvVS87P1csvSs9MAbGKhLgEwpbk_NlXddZx3opkxXkvb19exahM2Aj9C4yMLxgZbzEJ-hele6aEF7ulpqQWJZZk5uc9YuINLU4t8s_LqQzJz07Nm8TMl5OfnpkXX1yUFp-Wk18OFACaUJCYXBJfkpmcnVqyi1nFwjTJ3NQyyVA3KSUtTdck2TJVNynVPFnXKNHYzNw40cA82dLgAovADxbGRaxANx9XX5FUPN_XZeq0o-IvGiPenmLVd3H0Top0TMwKCigNs8yuSvMtjww3yfcLcnLOscg1zPLLycx0DPZ28y6pLLY1tTI8wMkIAA2&popupui=

Comme on se connecte via un client web, c'est le protocole de signalisation Ws-Federation qui est utilisé.

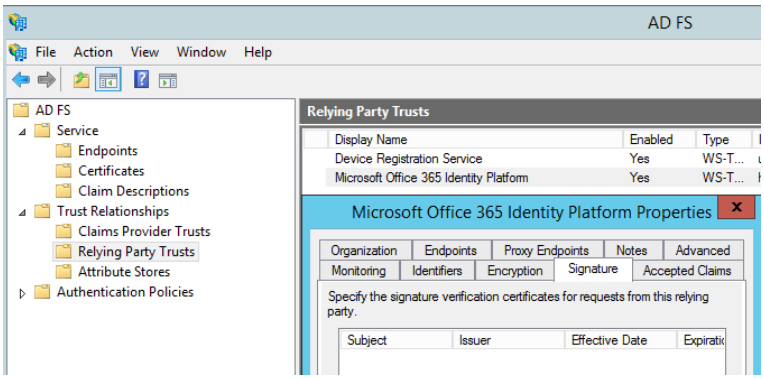
Se connecter sur le serveur ADFS et valider que l'URL https://adfs.labmetsys.fr/adfs/ls/ correspond au point de terminaison *Ws-Federation* ou *SAML V2*.



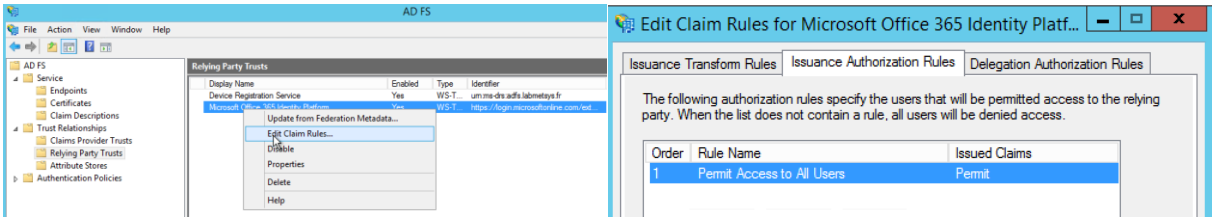
Comme on dispose de la balise *wtrealm* au niveau de l'URL (*wtrealm=urn%3afederation%3aMicrosoftOnline*) on sait que l'on va faire du *WS-Federation*. Ce champ correspond en fait à l'identifiant du *Relying Party Trust* d'Office 365 (*urn :federation :MicrosoftOnline*).



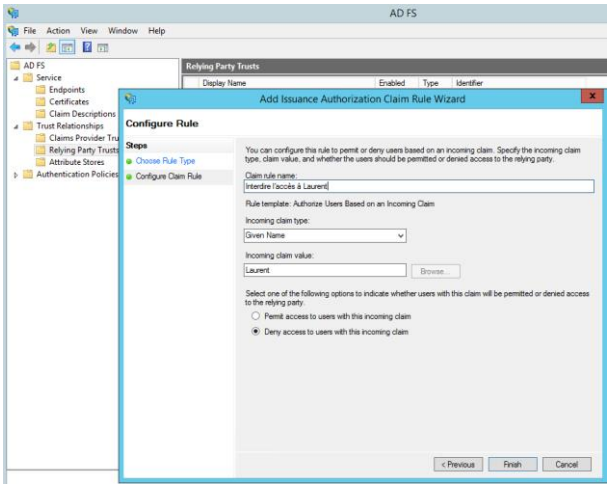
Si on va dans la partie Signature, on voit que le trafic vers ce *Relying Party Trust* n'a pas besoin d'être signé. Pour rappel, on signe avec sa clé privée (*Microsoft Office 365 Identity Plateform*) et ce dernier a besoin de connaître votre clé publique pour lire la signature. Avec le *Relying Party Trust* Office 365, cela n'est pas implémenté.

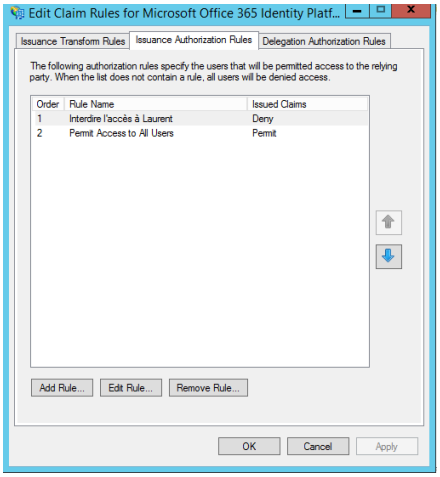


Par défaut, il n'y a aucune *Issuance Authorization* définie au niveau du serveur ADFS 3.0. Cela indique que tous les utilisateurs authentifiés peuvent se connecter au service. Cette configuration se trouve au niveau des *Claims rules*. En pratique le filtrage des accès est effectué au niveau des serveurs Office 365 et non au niveau du serveur ADFS 3.0.



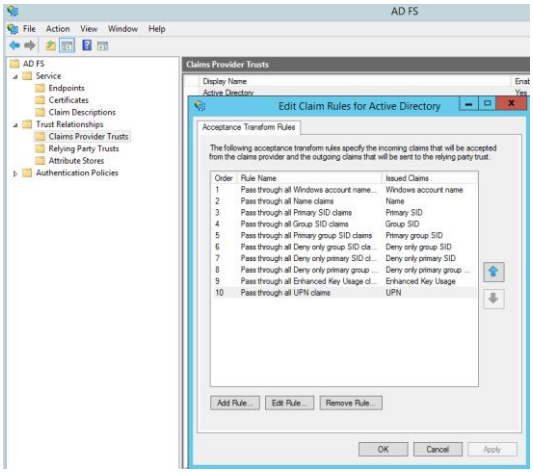
On peut cependant faire du filtrage au niveau du serveur ADFS (exemple avec le compte *laurent.mathieu*)

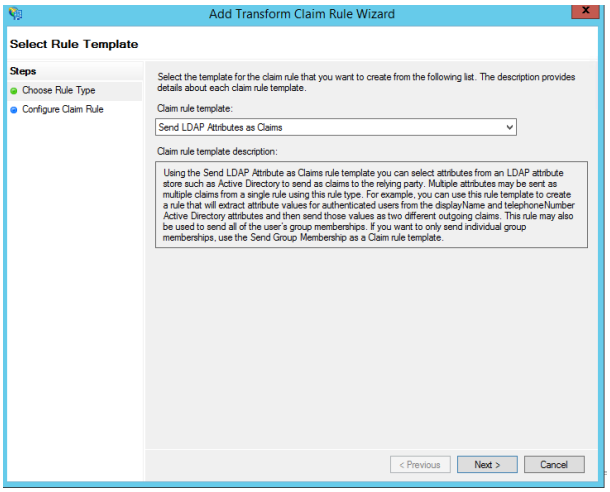




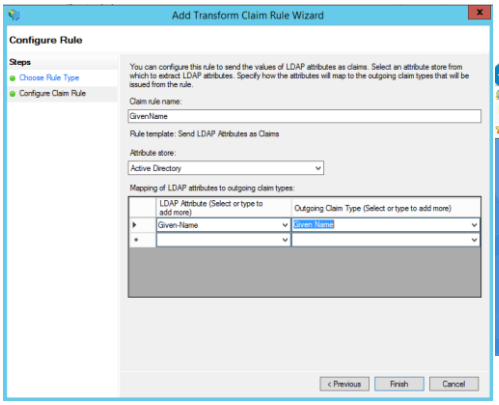
Pour que cela fonctionne, il faut ajouter le Claim description *GivenName* au niveau des règles *Acceptance Transform Rules*. Dans notre cas, on dispose d'un claim description appelé *GivenName*.

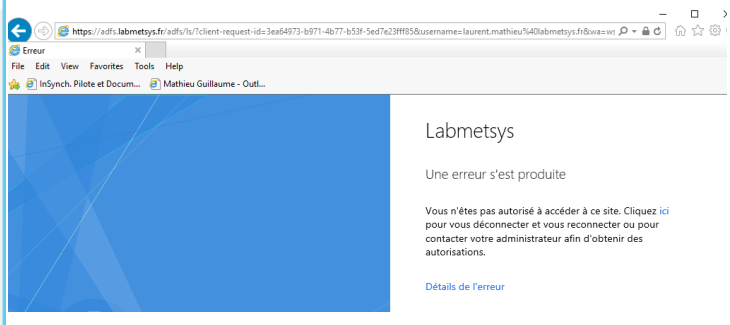
On déclare dans la règle que ce claim contient l'attribut *GivenName* de l'annuaire AD.





L'utilisateur obtient alors ce message.

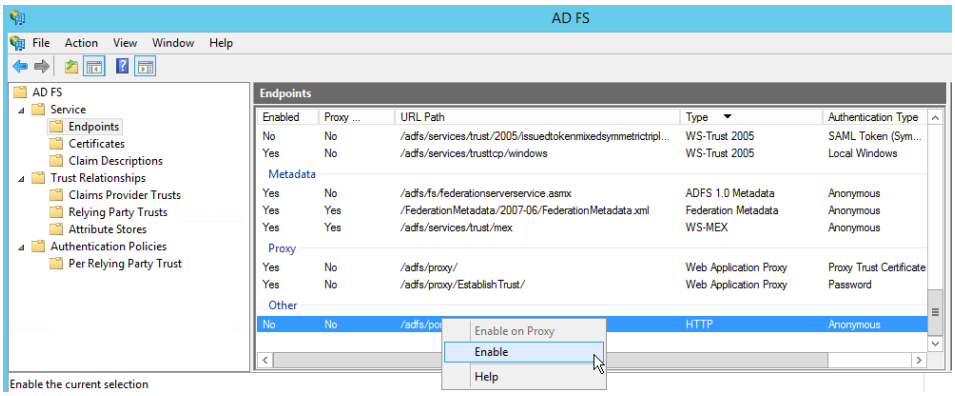




6.5 Paramètres avancés Microsoft ADFS

6.5.1 ADFS 3.0 et les mots de passe expirés

ADFS permet à un utilisateur dont le mot de passe a expiré de le changer. Pour activer cette fonctionnalité, lancer la console *AD FS Management* puis aller dans *ADFS | Service | Endpoints*. Faire un clic droit sur la ligne avec l'URL *ADFS/portal/updatepassword/* (la dernière ligne) et cliquer sur *Enable*. Cliquer sur *OK*.



Faire ensuite un clic droit sur la ligne avec l'URL *ADFS/portal/updatepassword/* (la dernière ligne) et cliquer sur *Enable On Proxy*. Cliquer sur *OK*. Il est nécessaire de redémarrer le service ADFS.

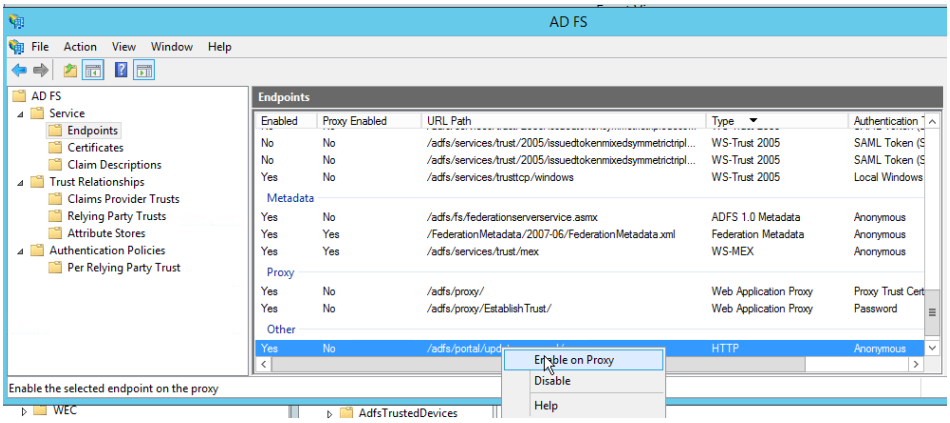
Cette action peut aussi être effectuée en PowerShell à l'aide des commandes ci-dessous :

Enable-AdfsEndpoint "/adfs/portal/updatepassword/"

Set-AdfsEndpoint "/adfs/portal/updatepassword/" -Proxy:$true

Restart-Service AdfsSrv -Force

Redémarrer les services ADFS sur tous les serveurs ADFS comme proxy.



6.5.2 Sécurisation ADFS : Activer les logs d'authentification

Par défaut les évènements de logins ratés ou réussis ne sont pas logués sur les serveurs ADFS. On peut les activer avec ces commandes (sur le premier serveur ADFS) :

Set-ADFSProperties -LogLevel Information,Errors,Verbose,Warnings,FailureAudits,SuccessAudits

auditpol.exe /set /subcategory:"Application Generated" /failure:enable /success:enable

Redémarrer le service ADFS.

Toutes les connexions apparaissent maintenant dans le journal *Security* du serveur ADFS 3.0.

6.5.3 Sécurisation ADFS : Extranet Lockout

Il est possible de bloquer un utilisateur temporairement quand celui-ci se trompe de mot de passe plusieurs fois à partir d'internet. Il faut pour cela exécuter cette commande :

Set-AdfsProperties -EnableExtranetLockout:$true -ExtranetLockoutThreshold 5 -ExtranetObservationWindow (New-TimeSpan -Minutes 10)

Redémarrer le serveur ADFS. L'utilisateur sera bloqué 10 min s'il se trompe 5 fois de suite.

https://technet.microsoft.com/en-us/library/dn486806.aspx

https://flamingkeys.com/2015/06/ad-fs-3-best-practices/

6.5.4 Personnalisation du portail ADFS 3.0

La personnalisation du site web ADFS 3.0 va permettre d'ajouter par exemple un lien vers l'outil de réinitialisation des mots de passe de l'entreprise. Avec ADFS 3.0, il est possible de personnaliser l'interface web d'ADFS à l'aide des commandes PowerShell comme *Set-AdfsWebTheme* et *Set-AdfsGlobalWebContent*.

Nous allons pour cela nous appuyer sur la procédure Microsoft ci-dessous :

https://technet.microsoft.com/en-us/library/dn280950(v=ws.11).aspx.

La commande ci-dessous permet de changer le nom de la société :

Set-AdfsGlobalWebContent –CompanyName "Contoso Corp"

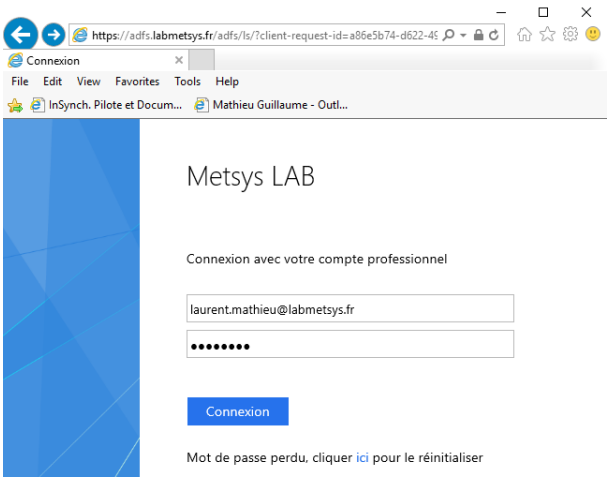
La commande ci-dessous permet d'ajouter un lien vers le site Helpdesk :

Set-AdfsGlobalWebContent -HelpDeskLink http://www.metsys.fr/support -HelpDeskLinkText Support

La commande ci-dessous permet d'ajouter un lien vers le site de réinitialisation de mot de passe (interface anglaise et française) :

Set-AdfsGlobalWebContent -SignInPageDescriptionText " Mot de passe perdu, cliquer <A href='https://aka.ms/sspr'>ici</A> pour le réinitialiser " -Locale FR-FR

Set-AdfsGlobalWebContent -SignInPageDescriptionText " Missing your password, click <A href='https://aka.ms/sspr'>here</A> to reset it " -Locale EN-US



7 Déploiement et configuration d'Azure Active Directory Connect et ADFS dans une architecture d'annuaire complexe ou en cours de migration

7.1 Les scénarios

Quand l'on souhaite déployer une architecture Office 365 fédérée, il est nécessaire de déployer *Azure Active Directory Connect* pour entre autre stocker dans l'attribut *ImmutableID* de l'annuaire d'Office 365 (Azure Active Directory), une valeur qui permet de référencer l'objet dans l'annuaire Active Directory de l'entreprise.

Azure Active Directory Connect est configuré par défaut pour générer cette valeur (*ImmutableID)* à partir de l'attribut *ObjectGuid* du compte utilisateur du domaine Active Directory de l'entreprise.

Azure Active Directory Connect est aussi configuré par défaut pour générer le login Office 365 (attribut *UserPrincipalName* de l'annuaire Azure Active Directory) en se basant sur la valeur de l'attribut *UserPrincipalName* de l'annuaire Azure Active Directory.

La configuration par défaut est très fortement recommandée si l'on souhaite activer le mode hybride ou si l'on ne souhaite pas activer l'authentification ADAL sur le Tenant Office 365 (*Modern Authentication*). Cette configuration présente cependant les inconvénients suivants :

- Lorsque l'on migre un compte utilisateur Active Directory, d'une forêt A vers une forêt B, l'attribut *ObjectGUID* du compte change. Cela va générer une erreur de synchronisation au niveau du serveur Azure Active Directory Connect. Pour rappel, il n'est pas possible de modifier l'attribut *ImmutableID* même en PowerShell (voir paragraphe astuce pour le contournement possible).
- Il n'est pas possible de définir le même suffixe UPN (le même domaine de messagerie) dans 2 forêts Active Directory différentes sous peine de problème de routage de suffixe UPN soit sous peine de problèmes d'authentification Kerberos.
- Il est nécessaire de changer la valeur de l'attribut *UserPrincipalName* du compte Active Directory. Le suffixe UPN de l'attribut *UserPrincipalName* doit en effet correspondre à un domaine DNS enregistré sur Office 365.

Pour supprimer ces contraintes, il est possible de modifier cette configuration par défaut. La bonne pratique est de changer l'attribut *UserPrincipalName* par l'attribut *Mail* et l'attribut *objectGUID* par l'attribut *ms-DS-consistencyGUID* au niveau des règles de synchronisation de l'outil *Azure Active Directory Connect*. Cette solution présente cependant les inconvénients suivants :

- Elle est plus difficile à maintenir et demande des modifications manuelles sur les serveurs Microsoft ADFS et sur le serveur *Azure Active Directory Connect*.
- Elle n'est pas recommandée si l'on dispose du mode hybride Exchange. On notera que cette contrainte va évoluer prochainement.
- Elle nécessite l'activation de l'authentification moderne (ADAL) au niveau d'Exchange Online et Skype for Business Online.

Les articles suivants présentent les limites pour d'utilisation l'*Alternate Login ID* :

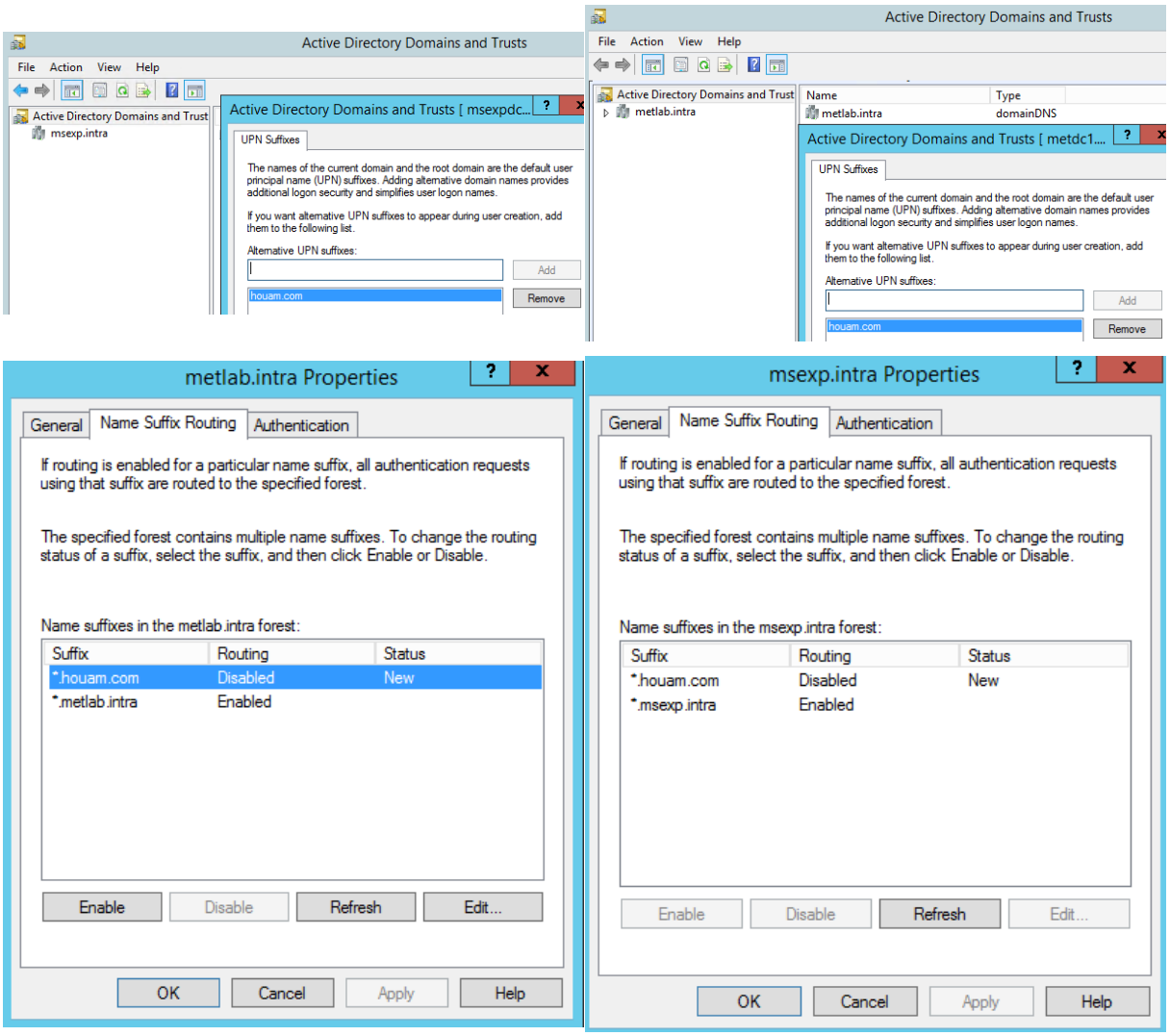
https://technet.microsoft.com/en-us/library/dn659436.aspx

https://azure.microsoft.com/fr-fr/documentation/articles/active-directory-aadconnect-get-started-custom/

"*We have recently changed our support statement on using Alternate ID with Exchange Hybrid. For the best user experience in an Exchange Hybrid environment, we recommend using the same set of credentials for on-premises and Exchange Online.*"

7.2 La problématique du routage des suffixe UPN

Dans l'exemple ci-dessous une relation d'approbation inter-forêts existait entre *MSEXP.INTRA* et *METLAB.INTRA*. Si on respecte les prérequis de la configuration de base, on est obligé d'ajouter les suffixe DNS de messagerie en tant que suffixes DNS au niveau de la console *Active Directory Domains and Trusts*. Dans l'exemple ci-dessous, on ajoute le suffixe UPN *Houam.com* dans les 2 forêts. Cela génère un conflit. Pour cette raison, le routage du suffixe UPN dans les 2 forêts est désactivé. L'authentification Kerberos échouera donc quand un utilisateur de la forêt A essaiera d'accéder à une ressource de la forêt B en utilisant un *ServicePrincipalName* contenant le domaine de messagerie *HOUAM.COM*. Par défaut Active Directory désactive le routage pour les suffixes UPN en conflits.



Il n'est donc pas possible en configuration par défaut de disposer d'un utilisateur de la forêt A et de la forêt B avec le même login Office 365 sous peine de très gros problèmes d'authentification avec le protocole Kerberos.

7.3 Configuration du serveur Azure Active Directory Connect

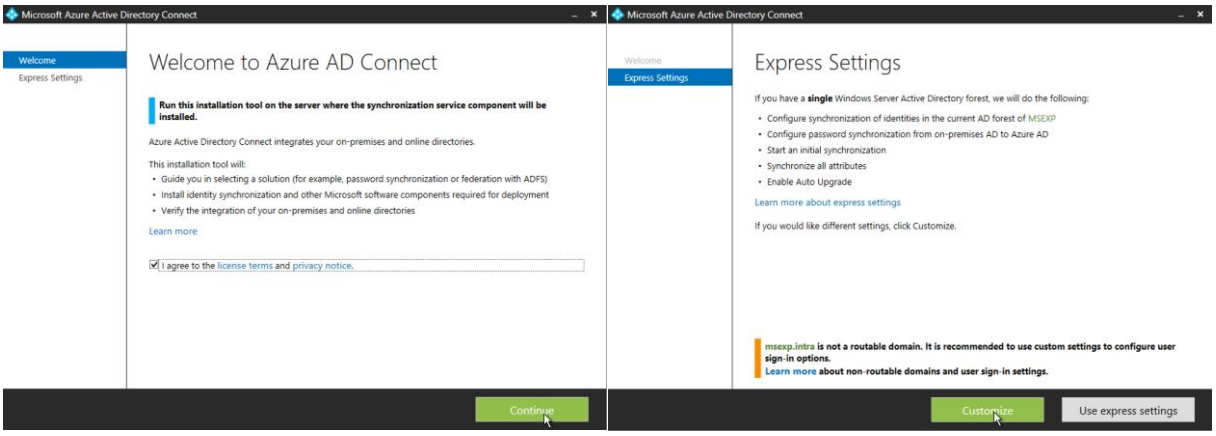
Cette procédure décrit comment activer l'*Alternate Login ID* (ou ID secondaire) lors de l'installation de l'outil de synchronisation *Azure Active Directory Connect*. Dans notre cas, c'est l'attribut *Mail* qui va permettre de générer le login Office 365 (attribut *UserPrincipalName* de l'annuaire Azure Active Directory).

Elle explique aussi comment utiliser l'attribut *ms-ds-consistencyguid* au lieu de l'attribut *ObjectGuid* pour générer la valeur de l'*ImmutableID*. Si le compte utilisateur est migré dans une nouvelle forêt, on peut garder la valeur de l'attribut *ms-ds-consistencyguid* du compte de l'ancienne forêt Active Directory car cet attribut est éditable. Pour rappel, il est impossible de modifier manuellement l'attribut *ObjectGuid*.

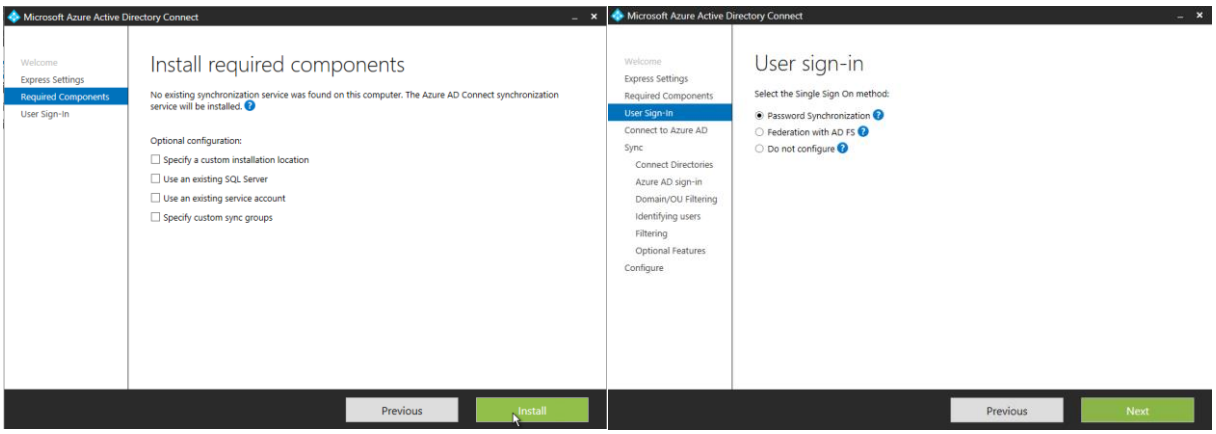
Dans notre cas, on laisse la synchronisation de mots de passe actif comme méthode de secours. Elle est basée sur l'article https://technet.microsoft.com/library/dn659436.aspx

ADFS sera activé plus loin dans la procédure.

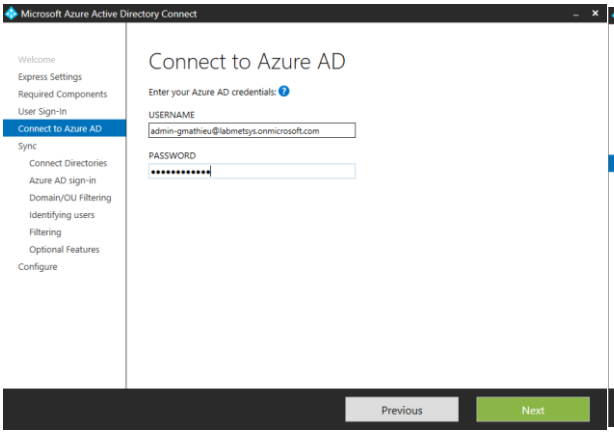
Il est nécessaire d'effectuer cette configuration dès l'installation d'Azure Active Directory Connect.

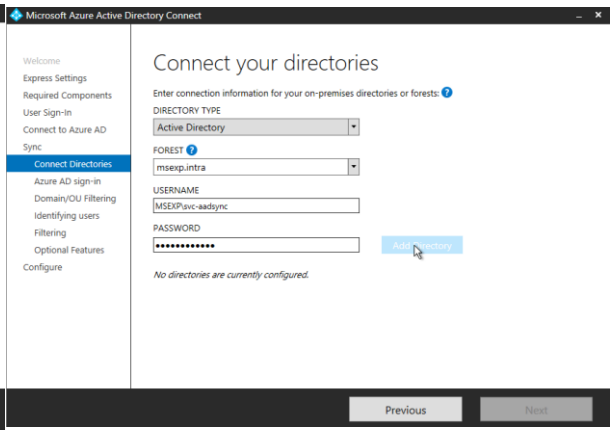


Nous souhaitons disposer de la synchronisation de mots de passe comme mécanisme de tolérance de panne. En cas de défaillance de l'architecture ADFS, il est possible temporairement de convertir le domaine en *Managed*. Les mots seront déjà répliqués.

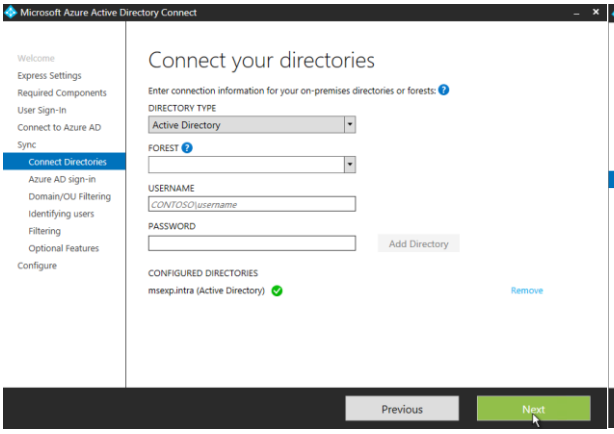


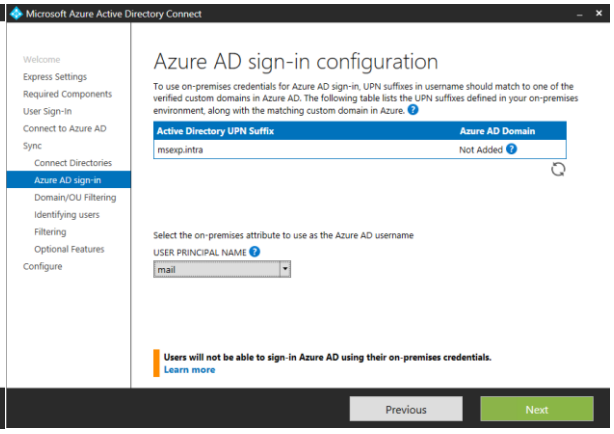
Il est nécessaire de spécifier le compte de service (*AADSYNC* dans cet exemple).





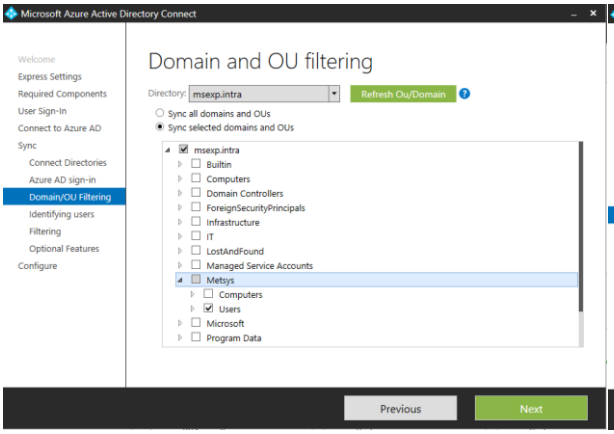
Aucun suffixe UPN dans cette forêt n'est routable. Il est donc nécessaire de choisir l'attribut *mail* comme login Office 365 (attribut *UserPrincipalName* dans l'annuaire Azure Active Directory).

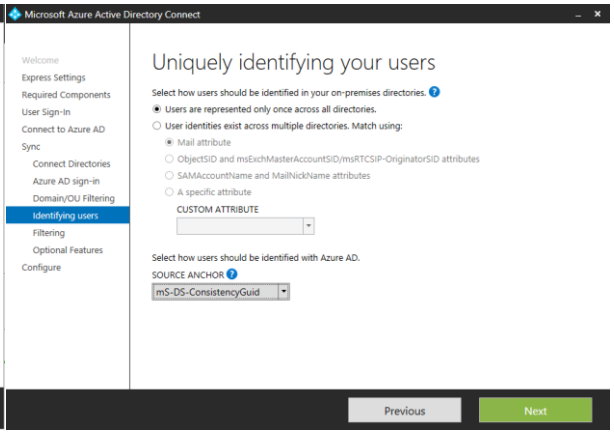


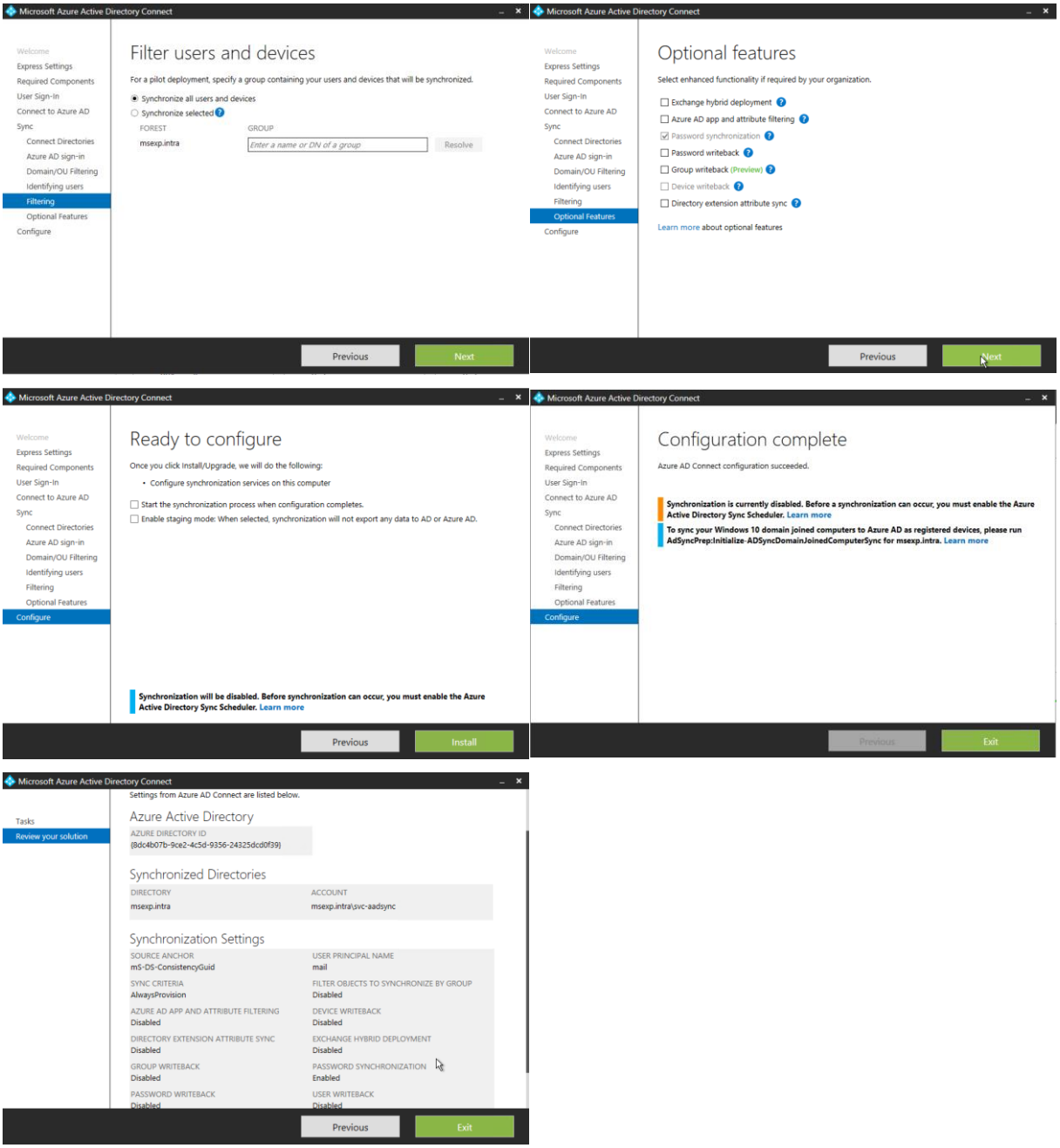


Filtrer les OU à synchroniser (uniquement l'OU User).

Sélectionner l'attribut *ms-DS-ConsistencyGuid* comme attribut pour générer la valeur de l'*ImmutableID*.

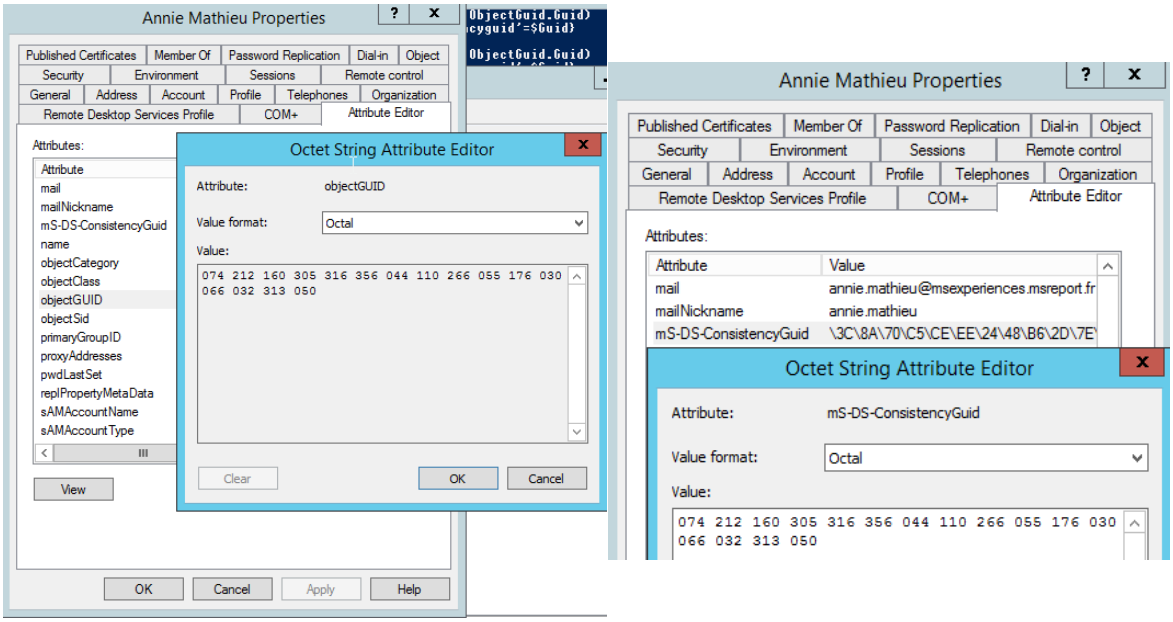






Avant de lancer la synchronisation, il faut valider que tous les objets à synchroniser disposent d'une valeur dans l'attribut *ms-ds-consistencyguid*. Si ce n'est pas le cas, Azure Active Directory Connect ne réplique pas l'objet dans l'annuaire *Azure Active Directory*. Il l'ajoute cependant dans la *Metaverse*.

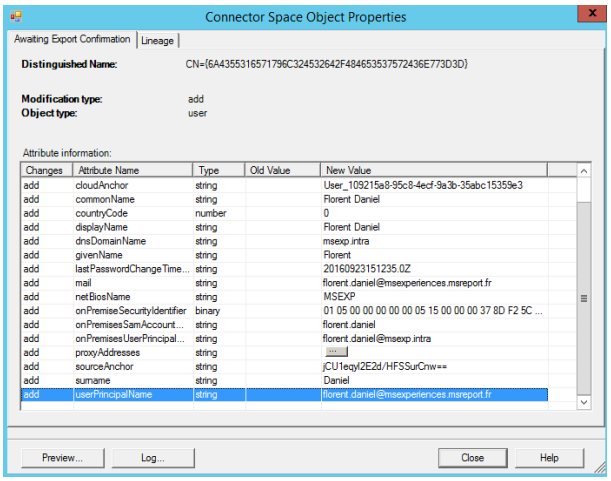
```
$User = "florent.daniel"
$Guid = [GUID]((Get-ADUser -Identity $User).ObjectGuid.Guid)
Set-Aduser $User –replace @{'ms-ds-consistencyguid'=$Guid}
```



Lancer manuellement la synchronisation à l'aide des commandes PowerShell :

Import-Module ADSync

Start-ADSyncSyncCycle -PolicyType Initial



On notera qu'il est aussi possible de modifier les règles dans Azure Active Directory Connect pour éviter d'avoir à utiliser un script PowerShell. Cette méthode est présentée dans les articles suivants :

http://studioblog.azurewebsites.net/immutableid-ms-ds-consistencyguid-adConnect

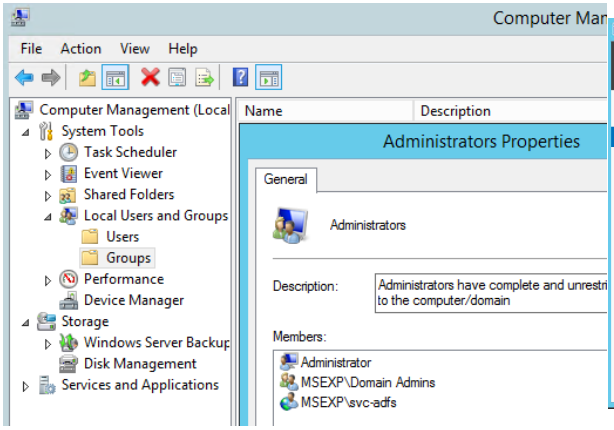
http://studioblog.azurewebsites.net/immutableid-ms-ds-consistencyguid-aadsync/

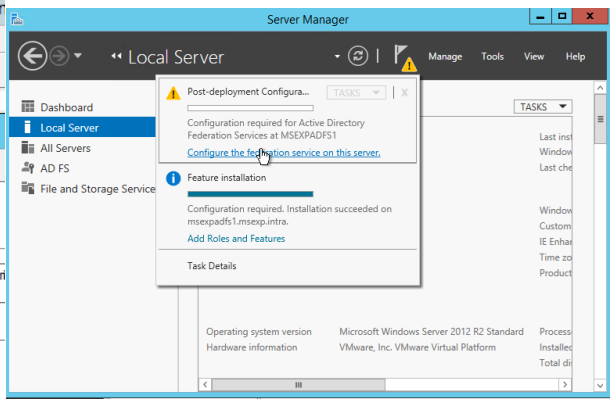
7.4 Configuration du ou des serveurs ADFS et Web Application Proxy

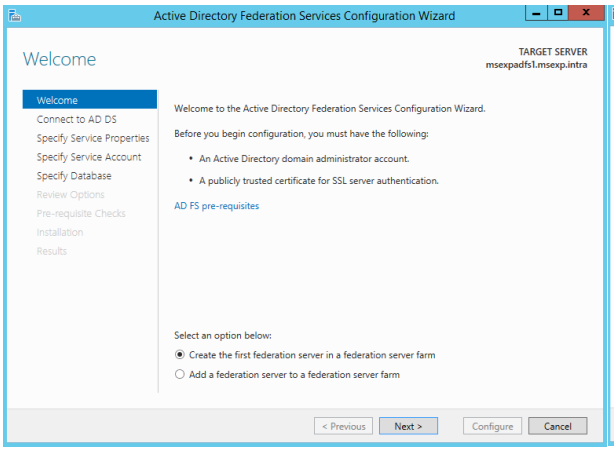
On va réutiliser le certificat précédemment généré (*ADFS.LABMETSYS.FR*). Dans cette maquette, on ne déploiera qu'un seul serveur ADFS et WAP. Vous pouvez vous reporter au paragraphe sur la fédération d'identité pour plus de détails sur la procédure d'installation d'ADFS / WAP.

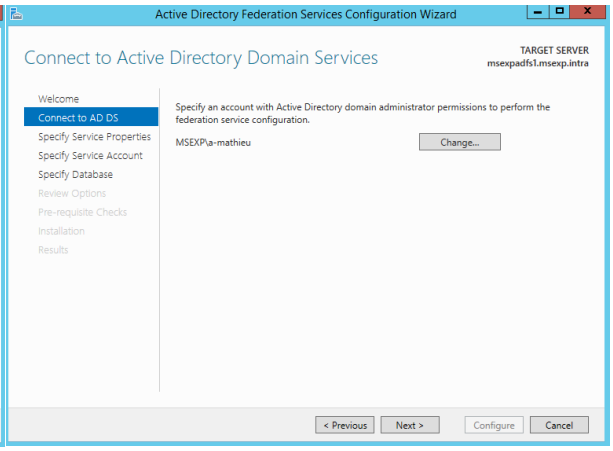
La mise en œuvre de l'*Alternate Login ID* nécessite que le correctif Installer le correctif 2919355 soit installé sur le serveur Windows 2012 R2 (https://support.microsoft.com/en-us/kb/2919355). Ce correctif peut être très complexe à installer. En cas de problème, le plus simple est de réinstaller un système en partant d'une image qui intègre les derniers correctifs Microsoft.

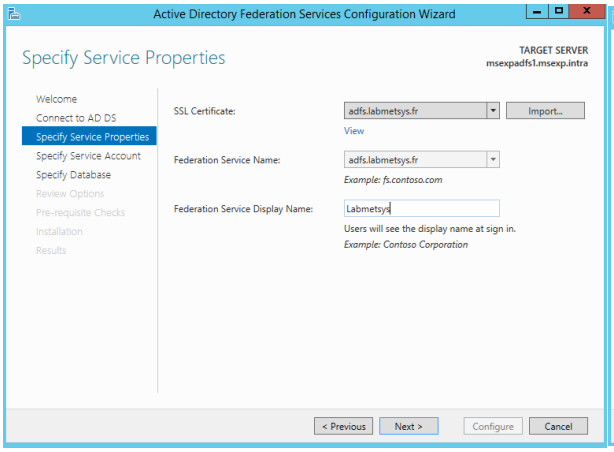
Se connecter sur le serveur ADFS 3.0 et ajouter l'utilisateur *MSEXP\SVC-ADFS* en tant qu'administrateur local.

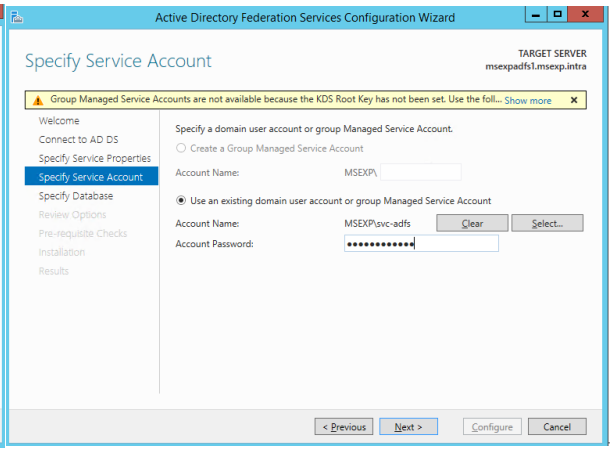


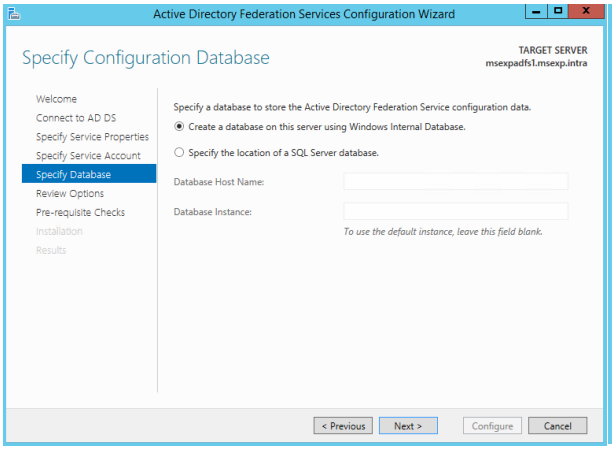


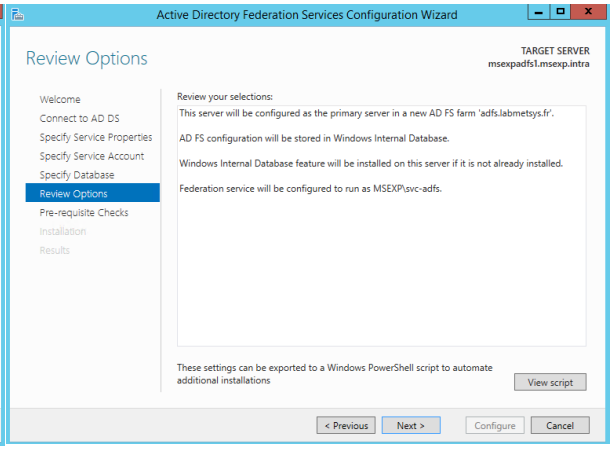






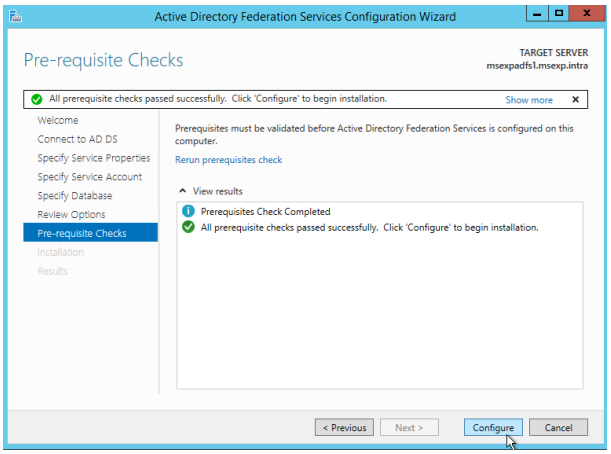






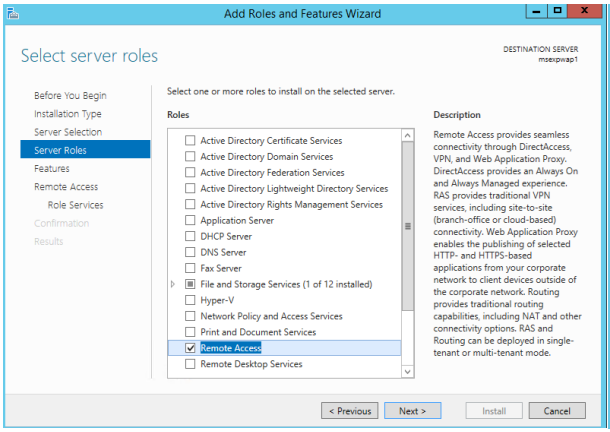
On peut visualiser le code PowerShell généré par Server Manager.

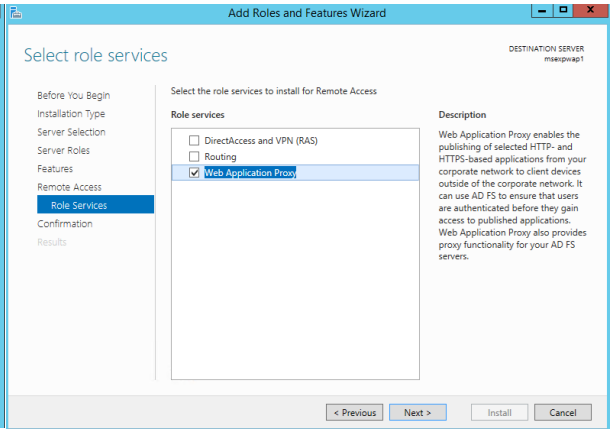
```
Import-Module ADFS
# Get the credential used for performaing installation/configuration of ADFS
$installationCredential = Get-Credential -Message "Enter the credential for the account used to perform the configuration."
# Get the credential used for the federation service account
$serviceAccountCredential = Get-Credential -Message "Enter the credential for the Federation Service Account."
Install-AdfsFarm `
-CertificateThumbprint:"07443DB8622E76328A4CE688C729EB6A09FE53D5" `
-Credential:$installationCredential `
-FederationServiceDisplayName:"Labmetsys" `
-FederationServiceName:"adfs.labmetsys.fr" `
-ServiceAccountCredential:$serviceAccountCredential
```

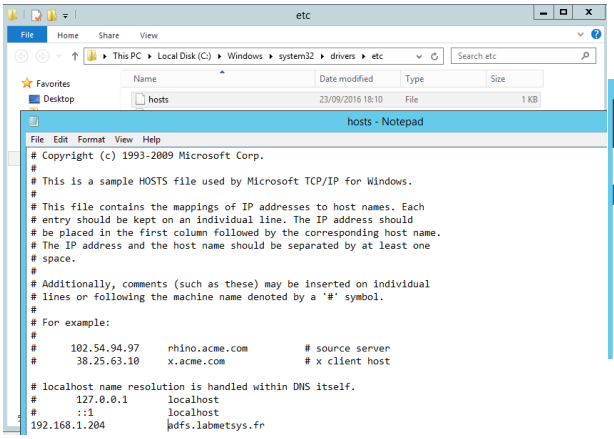


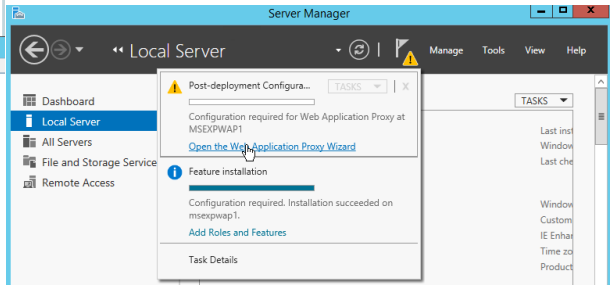
Il faut créer l'entrée *ADFS.LABMETSYS.FR* au niveau du service DNS interne. Cette entrée doit pointer vers le serveur Web Application Proxy qui en production et qui doit être en DMZ.

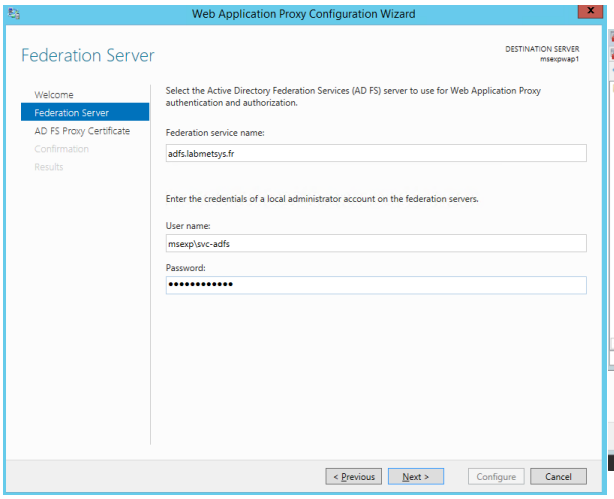
Installer le serveur Web Application Proxy (installation par défaut).

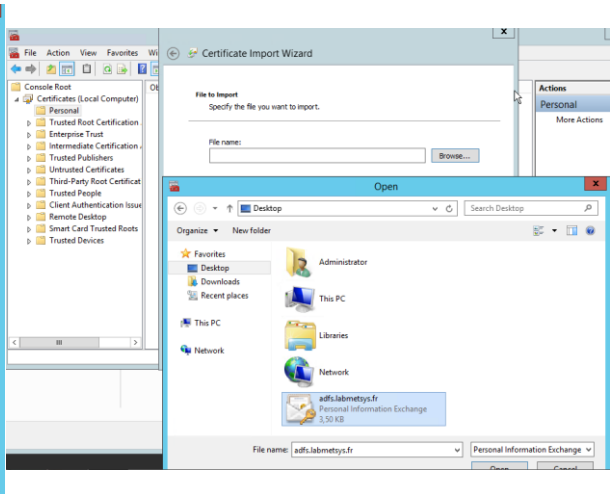

Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
msexpwap1
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Remote Access
Role Services
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Active Directory Certificate Services
Active Directory Domain Services
Active Directory Federation Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
Application Server
DHCP Server
DNS Server
Fax Server
File and Storage Services (1 of 12 installed)
Hyper-V
Network Policy and Access Services
Print and Document Services
Remote Access
Remote Desktop Services
Description
Remote Access provides seamless connectivity through DirectAccess, VPN, and Web Application Proxy. DirectAccess provides an Always On and Always Managed experience. RAS provides traditional VPN services, including site-to-site (branch-office or cloud-based) connectivity. Web Application Proxy enables the publishing of selected HTTP- and HTTPS-based applications from your corporate network to client devices outside of the corporate network. Routing provides traditional routing capabilities, including NAT and other connectivity options. RAS and Routing can be deployed in single-tenant or multi-tenant mode.
< Previous
Next >
Install
Cancel

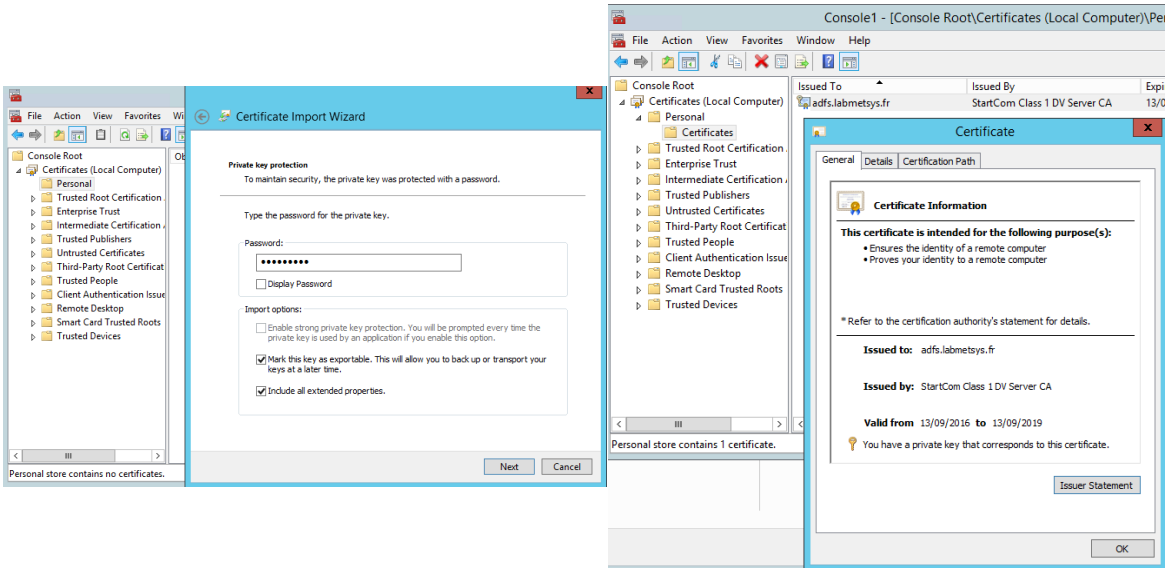

Add Roles and Features Wizard
Select role services
DESTINATION SERVER
msexpwap1
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Remote Access
Role Services
Confirmation
Results
Select the role services to install for Remote Access
Role services
DirectAccess and VPN (RAS)
Routing
Web Application Proxy
Description
Web Application Proxy enables the publishing of selected HTTP- and HTTPS-based applications from your corporate network to client devices outside of the corporate network. It can use AD FS to ensure that users are authenticated before they gain access to published applications. Web Application Proxy also provides proxy functionality for your AD FS servers.
< Previous
Next >
Install
Cancel

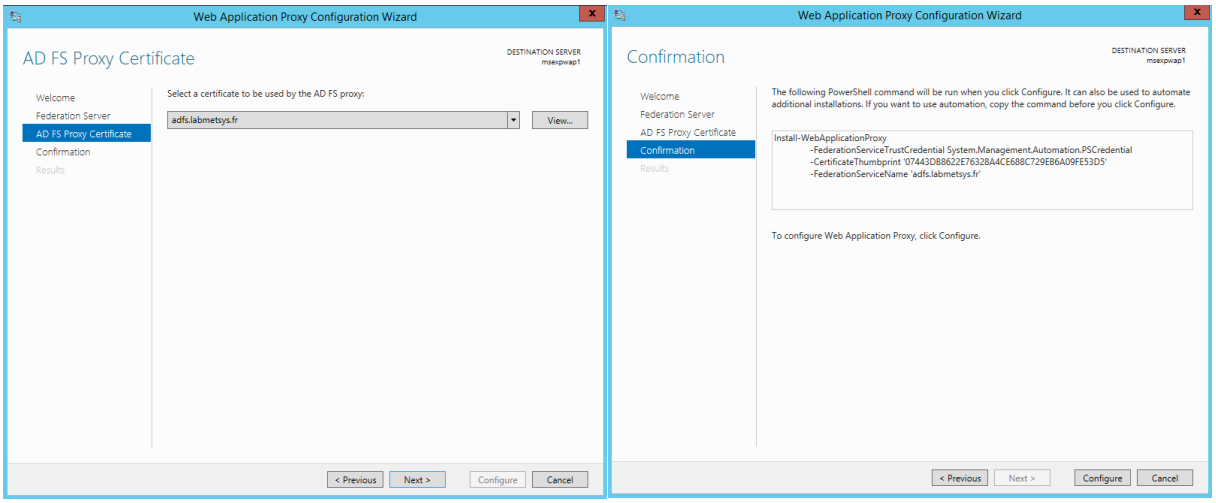

etc
File
Home
Share
View
This PC
Local Disk (C:)
Windows
system32
drivers
etc
Search etc
Favorites
Desktop
Name
Date modified
Type
Size
hosts
23/09/2016 18:10
File
1 KB
hosts - Notepad
File Edit Format View Help
Copyright (c) 1993-2009 Microsoft Corp.
#
This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
This file contains the mappings of IP addresses to host names. Each
entry should be kept on an individual line. The IP address should
be placed in the first column followed by the corresponding host name.
The IP address and the host name should be separated by at least one
space.
#
Additionally, comments (such as these) may be inserted on individual
lines or following the machine name denoted by a '#' symbol.
#
For example:
#
102.54.94.97   rhino.acme.com   # source server
38.25.63.10   x.acme.com   # x client host
localhost name resolution is handled within DNS itself.
127.0.0.1   localhost
::1   localhost
192.168.1.204   adfs.labmetsys.fr


Server Manager
Local Server
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Service
Remote Access
Post-deployment Configura...
TASKS
Configuration required for Web Application Proxy at MSEXPWAP1
Open the Web Application Proxy Wizard
Feature installation
Configuration required. Installation succeeded on msexpwap1.
Add Roles and Features
Task Details

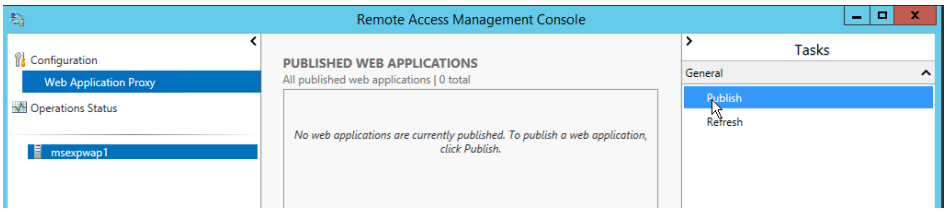

Web Application Proxy Configuration Wizard
Federation Server
DESTINATION SERVER
msexpwap1
Welcome
Federation Server
AD FS Proxy Certificate
Confirmation
Results
Select the Active Directory Federation Services (AD FS) server to use for Web Application Proxy authentication and authorization.
Federation service name:
adfs.labmetsys.fr
Enter the credentials of a local administrator account on the federation servers.
User name:
msexp\svc-adfs
Password:
••••••••••••
< Previous
Next >
Configure
Cancel

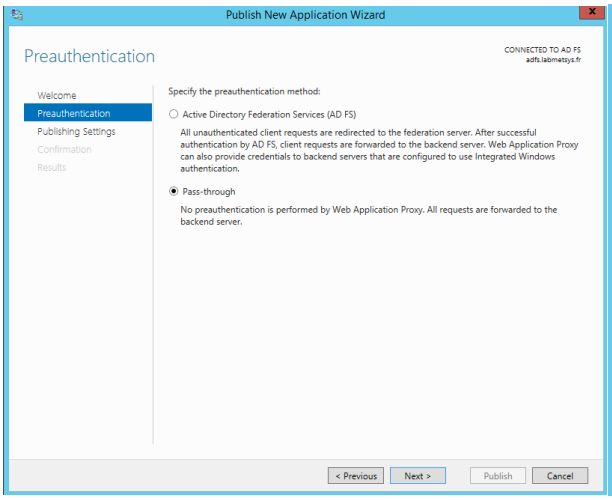

Certificate Import Wizard
File to Import
Specify the file you want to import.
File name:
Browse...
Open
Desktop
Search Desktop
Organize
New folder
Favorites
Desktop
Downloads
Recent places
This PC
Network
Administrator
This PC
Libraries
Network
adfs.labmetsys.fr
Personal Information Exchange
3,50 KB
File name: adfs.labmetsys.fr
Personal Information Exchange
Actions
Personal
More Actions

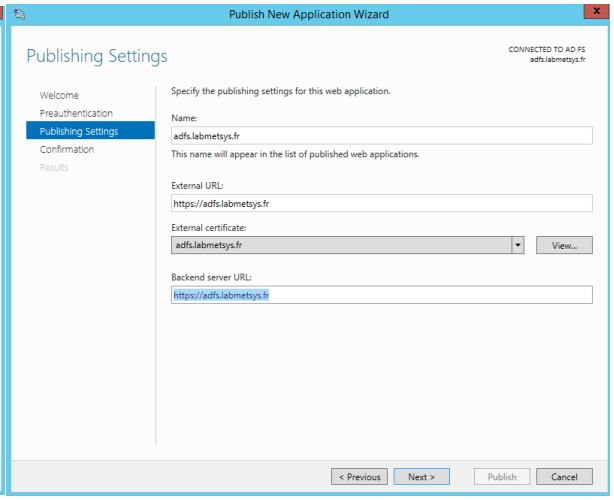


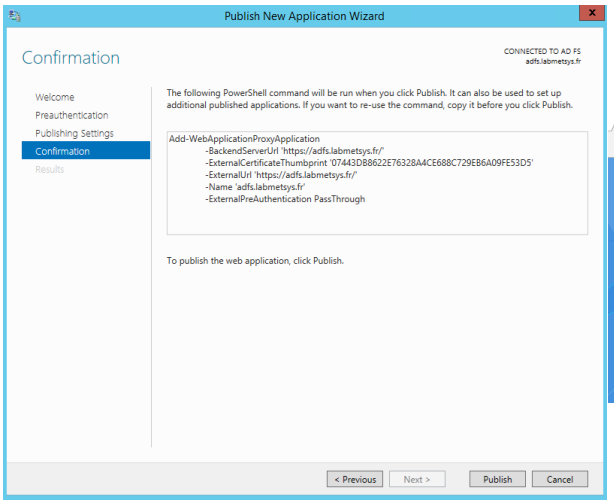


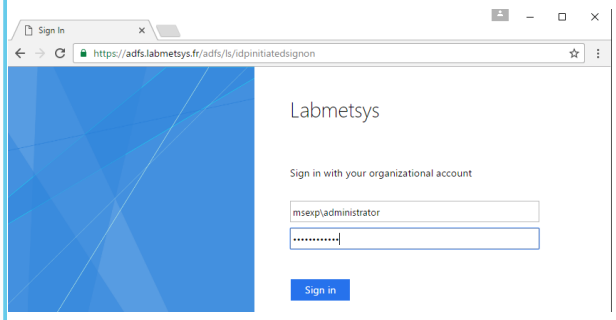
Il faut ouvrir sur votre pare-feu d'entreprise le port 443 et le rediriger vers le serveur Web Application Proxy.

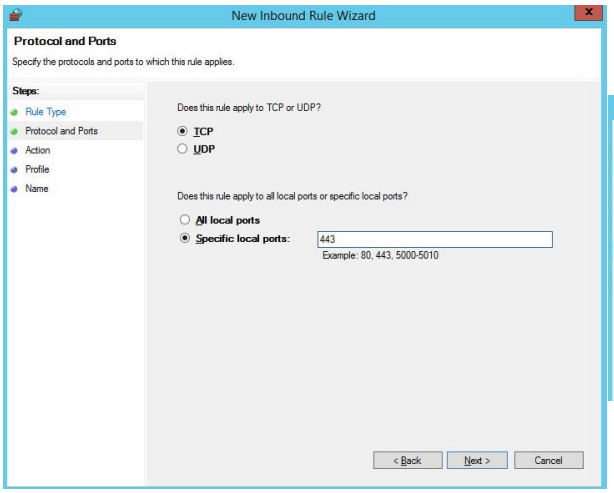


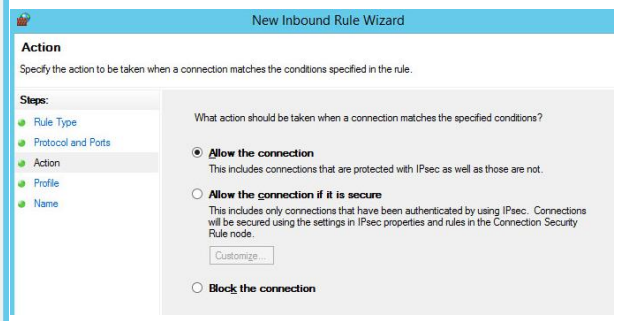

Publish New Application Wizard
Preauthentication
CONNECTED TO AD FS
adfs.labmetsys.fr
Welcome
Preauthentication
Publishing Settings
Confirmation
Results
Specify the preauthentication method:
Active Directory Federation Services (AD FS)
All unauthenticated client requests are redirected to the federation server. After successful authentication by AD FS, client requests are forwarded to the backend server. Web Application Proxy can also provide credentials to backend servers that are configured to use Integrated Windows authentication.
Pass-through
No preauthentication is performed by Web Application Proxy. All requests are forwarded to the backend server.
< Previous
Next >
Publish
Cancel

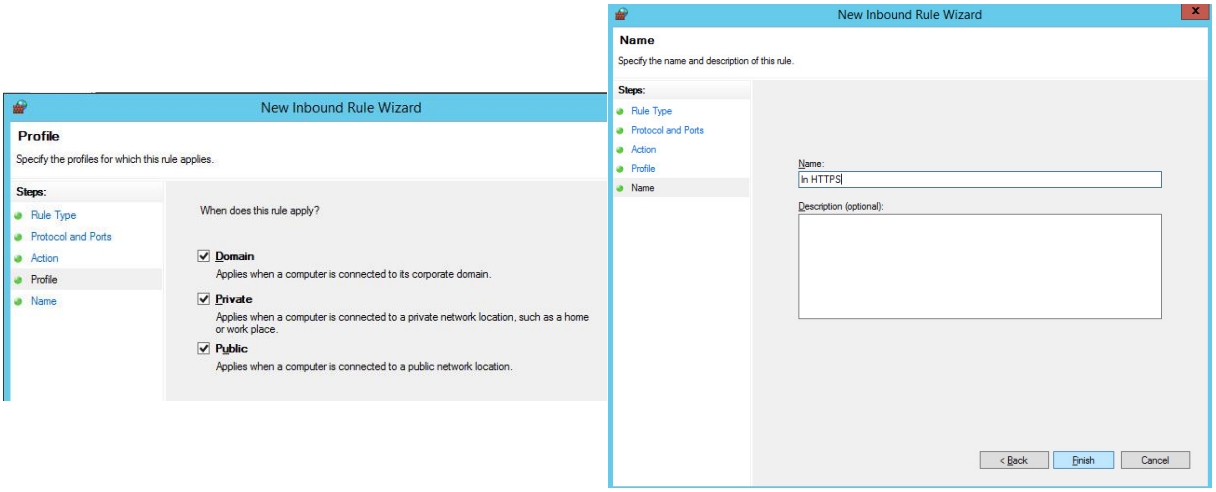

Publish New Application Wizard
Publishing Settings
CONNECTED TO AD FS
adfs.labmetsys.fr
Welcome
Preauthentication
Publishing Settings
Confirmation
Results
Specify the publishing settings for this web application.
Name:
adfs.labmetsys.fr
This name will appear in the list of published web applications.
External URL:
https://adfs.labmetsys.fr
External certificate:
adfs.labmetsys.fr
View...
Backend server URL:
https://adfs.labmetsys.fr
< Previous
Next >
Publish
Cancel


Publish New Application Wizard
Confirmation
CONNECTED TO AD FS
adfs.labmetsys.fr
Welcome
Preauthentication
Publishing Settings
Confirmation
Results
The following PowerShell command will be run when you click Publish. It can also be used to set up additional published applications. If you want to re-use the command, copy it before you click Publish.
Add-WebApplicationProxyApplication
-BackendServerUrl 'https://adfs.labmetsys.fr/'
-ExternalCertificateThumbprint '07443D88622E76328A4CE688C729EB6A09FE53D5'
-ExternalUrl 'https://adfs.labmetsys.fr/'
-Name 'adfs.labmetsys.fr'
-ExternalPreAuthentication PassThrough
To publish the web application, click Publish.
< Previous
Next >
Publish
Cancel


Sign In
https://adfs.labmetsys.fr/adfs/ls/idpinitiatedsignon
Labmetsys
Sign in with your organizational account
msexp\administrator
Sign in


New Inbound Rule Wizard
Protocol and Ports
Specify the protocols and ports to which this rule applies.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
Does this rule apply to TCP or UDP?
TCP
UDP
Does this rule apply to all local ports or specific local ports?
All local ports
Specific local ports:
443
Example: 80, 443, 5000-5010
< Back
Next >
Cancel


New Inbound Rule Wizard
Action
Specify the action to be taken when a connection matches the conditions specified in the rule.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
What action should be taken when a connection matches the specified conditions?
Allow the connection
This includes connections that are protected with IPsec as well as those are not.
Allow the connection if it is secure
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.
Customize...
Block the connection



Vérifier le bon fonctionnement de l'URL : https://adfs.labmetsys.fr/adfs/ls/idpinitiatedsignon

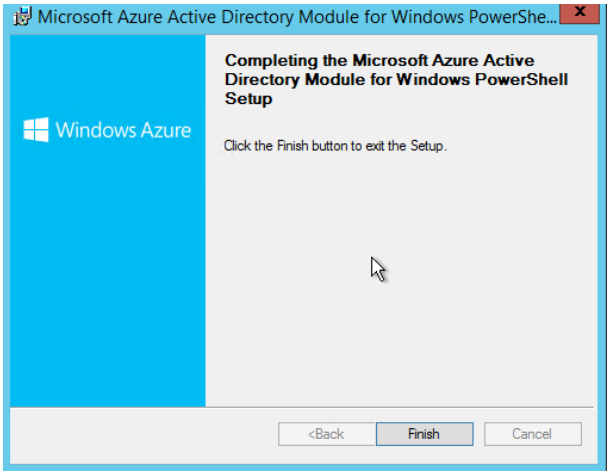
On doit pouvoir s'authentifier sur le serveur ADFS.

7.5 Configuration du Tenant Office 365 et du serveur ADFS 3.0

Cette procédure est basée sur l'article Microsoft https://technet.microsoft.com/en-us/library/dn659436.aspx.

La première va consister à convertir les domaines *LABMETSYS.FR* et *MSEXPERIENCES.MSREPORT.FR* en domaines fédérés. Installer le module PowerShell Azure Active Directory sur le serveur ADFS.

http://social.technet.microsoft.com/wiki/contents/articles/28552.microsoft-azure-active-directory-powershell-module-version-release-history.aspx



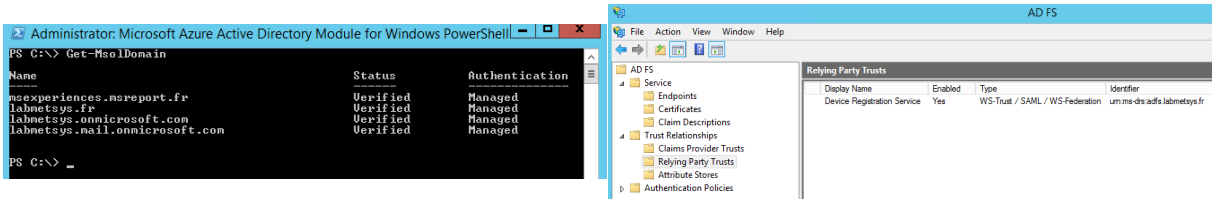
Se connecter ensuite au tenant Office 365 :

$cred = Get-Credential

Connect-MsolService -Credential $cred

Taper la commande *Get-MsolDomain* pour valider le statut des domaines de messagerie Office 365.

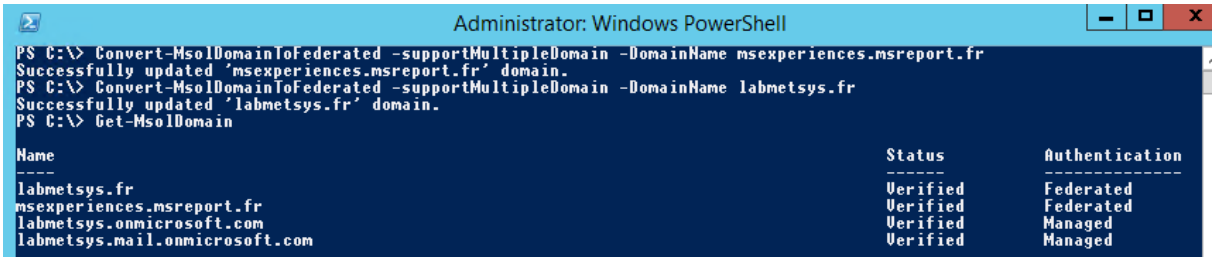
La commande *Convert-MsolDomain -domain msexperiences.msreport.fr* va à la fois configurer le serveur ADFS 3.0 (création d'un *Relying Party Trust* ou RP) et le domaine Office 365 (passage en mode *Federated* avec la configuration des URL de redirection).



Saisir la commande pour activer la fédération sur les 2 domaines de messagerie. Comme on fait cette action en local, il n'y a pas besoin de spécifier le serveur ADFS.

Convert-MsolDomainToFederated -supportMultipleDomain -DomainName msexperiences.msreport.fr

Convert-MsolDomainToFederated -supportMultipleDomain -DomainName labmetsys.fr

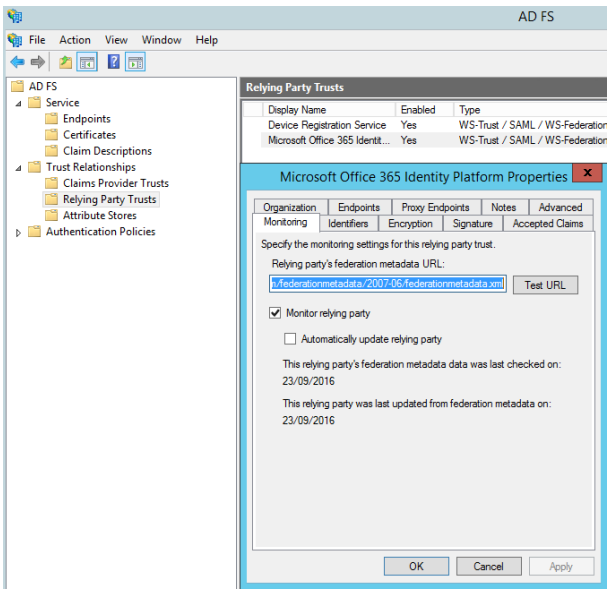


Il est ensuite nécessaire de valider le bon fonctionnement du serveur ADFS 3.0 depuis le réseau interne et externe en se connectant à l'adresse suivante : https://adfs.labmetsys.fr/adfs/ls/IdpInitiatedSignon.aspx

On notera qu'il est impératif de se connecter avec le nom DNS *ADFS.LABMETSYS.FR.*

Le correctif Windows https://support.microsoft.com/en-us/kb/2919355 doit être installé ou la dernière mise à jour cumulative pour Windows 2012 R2 doit être installée. Windows 2012 R2 dispose en effet de mise à jour cumulative qui apporte de nouvelles fonctionnalités au système :

https://blogs.technet.microsoft.com/chad/2015/01/21/current-windows-server-2012-r2-windows-8-8-1-update-rollups/



Windows Server 2012 R2 & Windows 8.1

General Availability Update Rollup – http://support2.microsoft.com/kb/2883200

October 2013 – http://support2.microsoft.com/kb/2884846

November 2013 – http://support2.microsoft.com/kb/2887595

December 2013 – http://support2.microsoft.com/kb/2903939

January 2014 – http://support2.microsoft.com/kb/2911106

February 2014 – http://support2.microsoft.com/kb/2919394

March 2014 – http://support2.microsoft.com/kb/2928680

April 2014 – http://support2.microsoft.com/kb/2919355 *See Note

May 2014 – http://support2.microsoft.com/kb/2955164 **See Note

June 2014 – http://support2.microsoft.com/kb/2962409 **See Note

July 2014 – http://support2.microsoft.com/kb/2967917 **See Note

August 2014 – http://support2.microsoft.com/kb/2975719 **See Note

September 2014 – http://support2.microsoft.com/kb/2984006 **See Note

October 2014 – http://support2.microsoft.com/kb/2995388 **See Note

November 2014 – http://support2.microsoft.com/kb/3000850 **See Note

December 2014 – http://support2.microsoft.com/kb/3013769 **See Note

May 2016 – https://support.microsoft.com/en-us/kb/3156418 **See Note

```
PS C:\Users\administrator.MSEXP> Get-MsolDomainFederationSettings -DomainName msexperiences.msreport.fr

ActiveLogOnUri                      : https://adfs.labmetsys.fr/adfs/services/trust/2005/usernamemixed
DefaultInteractiveAuthenticationMethod :
FederationBrandName                 : LabMetsys
IssuerUri                           : http://msexperiences.msreport.fr/adfs/services/trust/
LogOffUri                           : https://adfs.labmetsys.fr/adfs/ls/
MetadataExchangeUri                 : https://adfs.labmetsys.fr/adfs/services/trust/mex
NextSigningCertificate              :
OpenIdConnectDiscoveryEndpoint      :
PassiveLogOnUri                     : https://adfs.labmetsys.fr/adfs/ls/
SigningCertificate                  : MIIC3jCCAcagAwIBAgIQfzUqaBqOro1DZ3Uq2KTbHzANBgkqhkiG9w0BAQsFADArMSkwJwYDVQQDEy
                                      BBREZTIFMpZ25pbmcgLSBhZGZzLmxhYm1ldHN5cy5mcjAeFw0xNjA5MjMyMzM2NDRaFw0xNzA5MjMy
                                      MzM2NDRaMCsxKTAnBgNVBAMTIEFERlMgU21nbmluZyAtIGFkZnMub2FibWUOc3lzLmZyMIIBIjANBg
                                      kqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAyF8wAMwOPj1UOH2xFwF+II+X7tH3iMfmyBehIiive9ef
                                      ewQDkPdEUMQbCohFXGt/zqMuOXE2e4OayAE422jMHqU+aaOVYxvmK9DNJAsXKyqEaKuUrAr693niFd
                                      DilcakhIEXCZU9+6JZ9M5R8kKc3zgUa8GJHmm169v5MWDJjKCpkz4R3NjV989gIx9yFQYnKVTocfi+
                                      WYsQpeKG3/m78UMthPy9vQXDMFPdOlW1Wm4uxRSrR+Q21rKO3OozUr4Jo3F9LhK8Y5OtwChd2LLPyJ
                                      NmiVaYqGQ6yu+1ROYAiLEJI/3bG9qOOciCc19vDAJc68JAUQW359+JMM9bF8L4dQIDAQABMA0GCSqG
                                      SIb3DQEBCwUAA4IBAQBwbnF2AMhwvnJUUVffS2bOAhZW91TpOOhAQNJ4lGEMD2bEN2X3c8zUMh22NI
                                      ghDHqFQxdfQOkrJqjyZR1tIXfZmrYd4aa7UK4YvXWpSL8NVGv65UEheYxVjNP1XRby511jGD6Ffp+z
                                      rbrDaEsI9i4CPToZTh9MUaH/ragjx1B+05SrRZNkc+FQz/jje+eqdqPcb8RAsbFW+Xskrx7Be9OED8
                                      A3qeRCFGOCm56411T5uHbkhh3FAvROeeb+9MMjfyBQUG3BsXPWWBNx+yHx8s89PbVH+ubZX3HW1sBe
                                      2xxFrXLZhd5UeA16bOC7eizestxRboH1BXvjA1RVr/liYTjb
SupportsMfa                          : False


PS C:\Users\administrator.MSEXP> _
```

Il faut activer l'*Alternate Login ID* au niveau du serveur ADFS et du Tenant Office 365. Attention si les correctifs du KB 2919355 ou une mise à jour cumulative plus récente n'ont pas été déployés, le paramètre *-AlternateLoginID* n'est pas disponible. Cela s'effectue avec la commande ci-dessous :

Set-ADFSClaimsProviderTrust -TargetIdentifier "AD AUTHORITY" -AlternateLoginID mail -LookupForests msexp.intra,metlab.intra

```
PS C:\> Set-ADFSClaimsProviderTrust -TargetIdentifier "AD AUTHORITY" -AlternateL
oginID mail -LookupForests msexp.intra
PS C:\> _
```

La dernière partie correspond à la modification des Claims ADFS. Lancer la console ADFS de management. Dans le menu *ADFS / Trust Relationships / Microsoft Office 365 Identity Platform* cliquer sur *Edit Claim Rules*.

Au niveau de l'onglet *Issuance Transform Rules*, éditer la règle 1. Sauvegarder son contenu et le remplacer par :

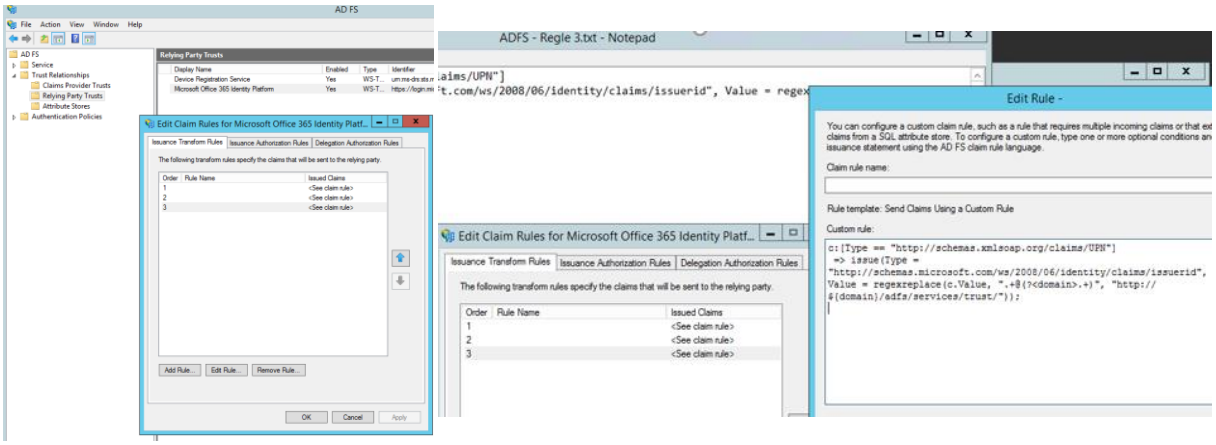
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]

=> issue(store = "Active Directory", types = ("http://schemas.xmlsoap.org/claims/UPN", "http://schemas.microsoft.com/LiveID/Federation/2008/05/ImmutableID"), query = "samAccountName={0};mail,mS-DS-ConsistencyGuid;{1}", param = regexreplace(c.Value, "(?<domain>[^\\]+)\\(?<user>.+)", "${user}"), param = c.Value);

Au niveau de l'onglet *Issuance Transform Rules*, éditer la règle 3. Sauvegarder son contenu et le remplacer par :

c:[Type == "http://schemas.xmlsoap.org/claims/UPN"]

=> issue(Type = "http://schemas.microsoft.com/ws/2008/06/identity/claims/issuerid", Value = regexreplace(c.Value, "^((.)([.|@]))?(?<domain>[^.]*[.].*)$", "http://${domain}/ADFS/services/trust/"));*



Redémarrer les serveurs *ADFS* / *WAP*. La configuration est maintenant terminée.

8 Préparer son réseau et ses pare-feu / proxy pour Office 365

8.1 Dimensionner ses liens réseaux pour Office 365

La première étape est de consulter les 2 articles ci-dessous :

https://support.office.com/en-us/article/Network-planning-and-performance-tuning-for-Office-365-e5f1228c-da3c-4654-bf16-d163daee8848

https://blogs.technet.microsoft.com/onthewire/2014/06/18/top-10-tips-for-optimising-troubleshooting-your-office-365-network-connectivity/

Pour fonctionner de manière optimale, il est nécessaire de configurer Office 365 selon les capacités des liens WAN de l'entreprise et des équipements de sécurité (proxy / pare feu). Pour évaluer son besoin en bandes passantes, latence, Microsoft met à disposition des feuilles de calcul :

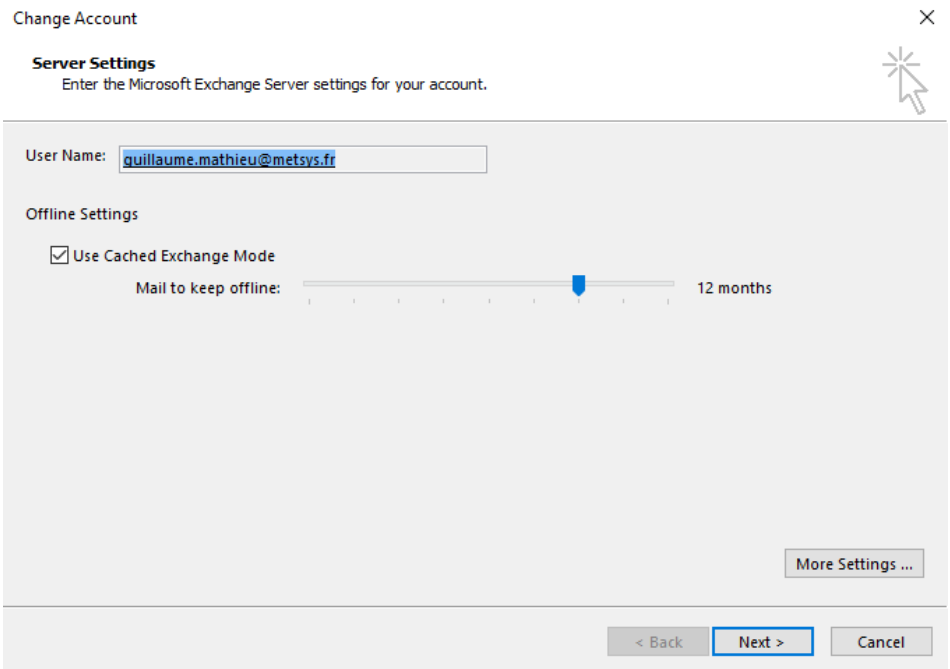
https://gallery.technet.microsoft.com/Exchange-Client-Network-8af1bf00

http://go.microsoft.com/fwlink/p/?LinkId=321551

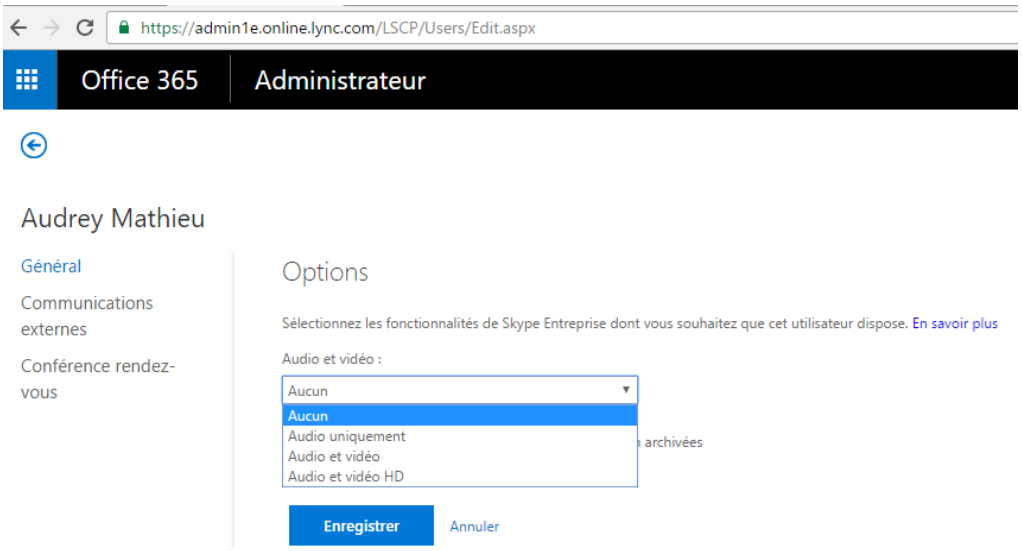
Les migrations de données (Exchange Online, OneDrive for Business) doivent être programmées hors des heures de travail. Si les liens réseaux sont trop lents ou coûteux pour migrer les données existantes vers Office 365, il est possible de les transférer à l'aide de disques que l'on envoie chez Microsoft.

https://support.office.com/en-us/article/Use-drive-shipping-to-import-PST-files-to-Office-365-40829b57-793c-4d41-b171-e9270129173d

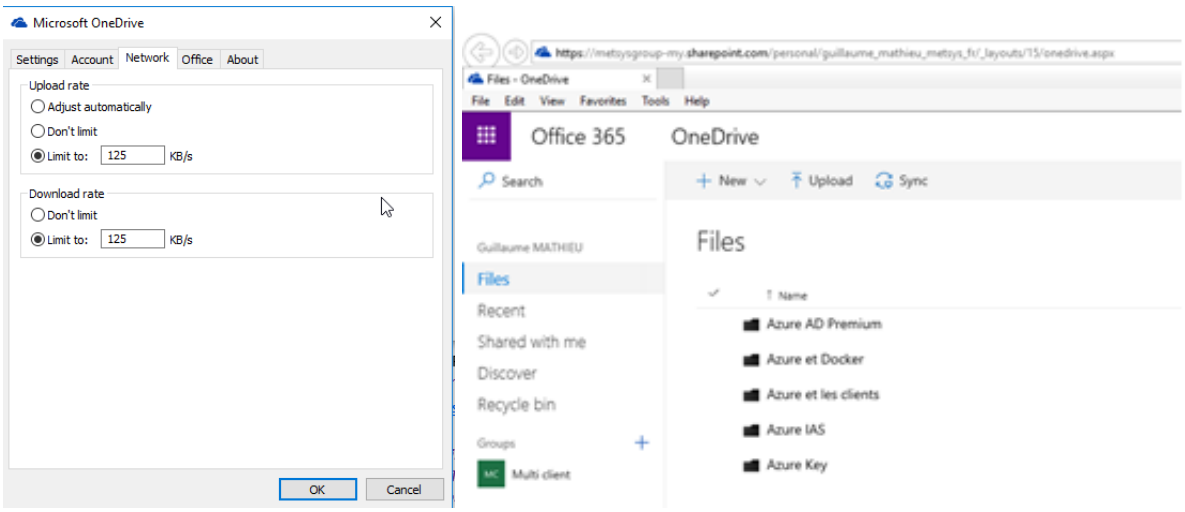
Il est recommandé de déployer Outlook 2013 / 2016 pour ne pas télécharger l'intégralité de la boîte aux lettres quand le mode cache est activé (permet de diminuer la taille du fichier OST).



Il est aussi recommandé de configurer les options vidéo de Skype for Business (désactiver la vidéo haute définition).



Le client de synchronisation *OneDrive for Business* peut aussi générer un trafic réseau très important. Ce dernier peut être configuré pour limiter la bande passante utilisée. Dans certains cas, il peut être nécessaire de bloquer l'utilisation de ce client de synchronisation. Les utilisateurs doivent alors se connecter au client web OneDrive for Business. Pour rappel, les fonctionnalités de coédition sont uniquement disponibles si les données sont hébergées sur un espace SharePoint Online ou sur OneDrive for Business. Pour cette raison, il est déconseillé de bloquer l'utilisation de OneDrive / SharePoint avec Office 365.



De nombreux éditeurs comme *Riverbed* proposent des solutions pour compresser / optimiser le trafic réseau requis par la solution Office 365 : http://www.riverbed.com/fr/solutions/solutions-by-application/office-365.html

8.2 Configurer les pare-feu / proxy pour Office 365

Le déploiement d'Office 365 est très impactant pour les proxys / pare-feu.

En moyenne, un utilisateur sous Office 365 (qui utilise tous les produits de la suite) maintient environ 20 à 40 connexions TCP en permanence contre une dizaine pour un utilisateur standard qui navigue uniquement sur Internet. Pour cette raison, Microsoft recommande de disposer d'une adresse IP publique pour 1625 utilisateurs. On obtient ce chiffre en divisant le nombre de ports disponibles 65535 (pour une IP publique) par 40.

Office 365 nécessite aussi que les proxys soient configurés pour ne pas authentifier le trafic Office 365. Microsoft fournit une liste d'URL à définir en exception :

https://support.office.com/en-us/article/Office-365-URLs-and-IP-address-ranges-8548a211-3fe7-47cb-abb1-355ea5aa88a2

En effet quand l'authentification est requise, le client essaie tout d'abord d'accéder à la ressource en anonyme. Le proxy renvoie alors un message 407 (authentification requise) au navigateur web. Cela peut générer des ralentissements ou l'affichage de fenêtre d'authentification comme expliqué dans l'article suivant :

https://blogs.technet.microsoft.com/onthewire/2014/06/18/top-10-tips-for-optimising-troubleshooting-your-office-365-network-connectivity/

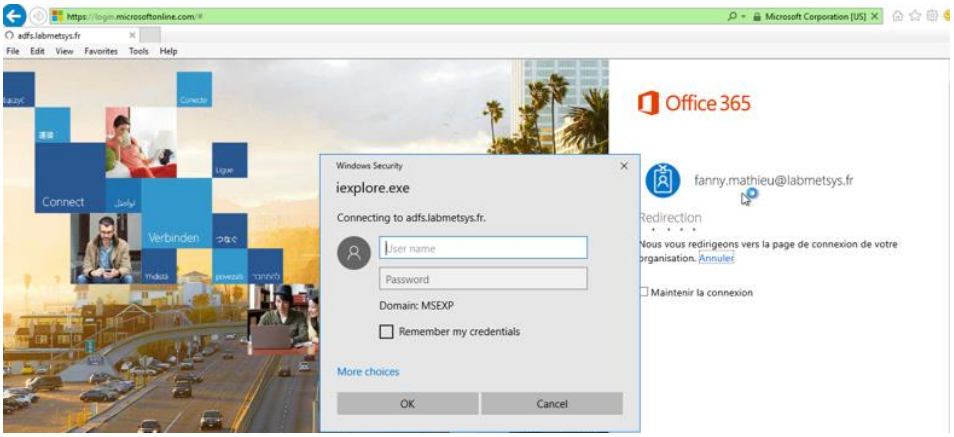
9 Configurer son navigateur pour Office 365

9.1 Les paramètres à prendre en compte pour Office 365

Dans l'exemple ci-dessous, l'utilisatrice *MSEXP\FANNY.MATHIEU* (*fanny.mathieu@labmetsys.fr*) se connecte sur son poste de travail depuis le réseau interne de la société *LABMETSYS*. Elle lance Internet Explorer 11 et accède à Outlook on the Web (Outlook Web App) via l'URL https://outlook.office365.com.

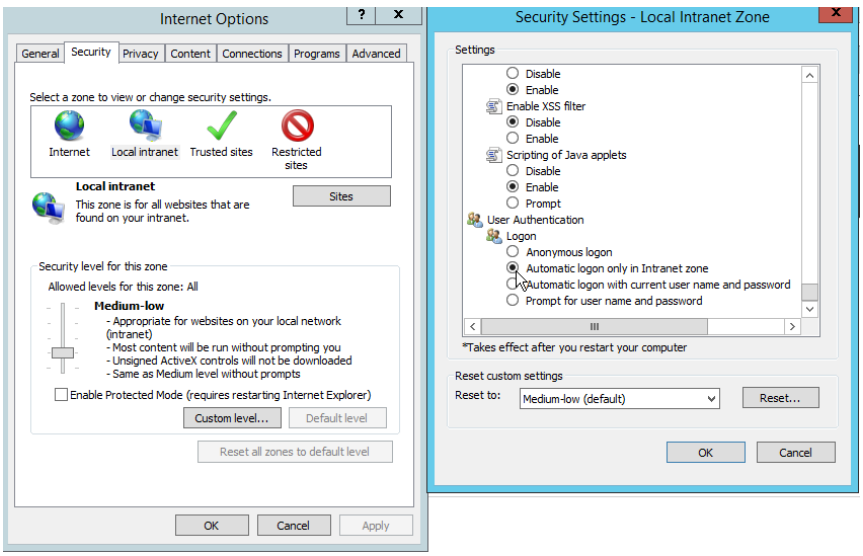
Le domaine de messagerie *LABMETSYS.FR* est fédéré.

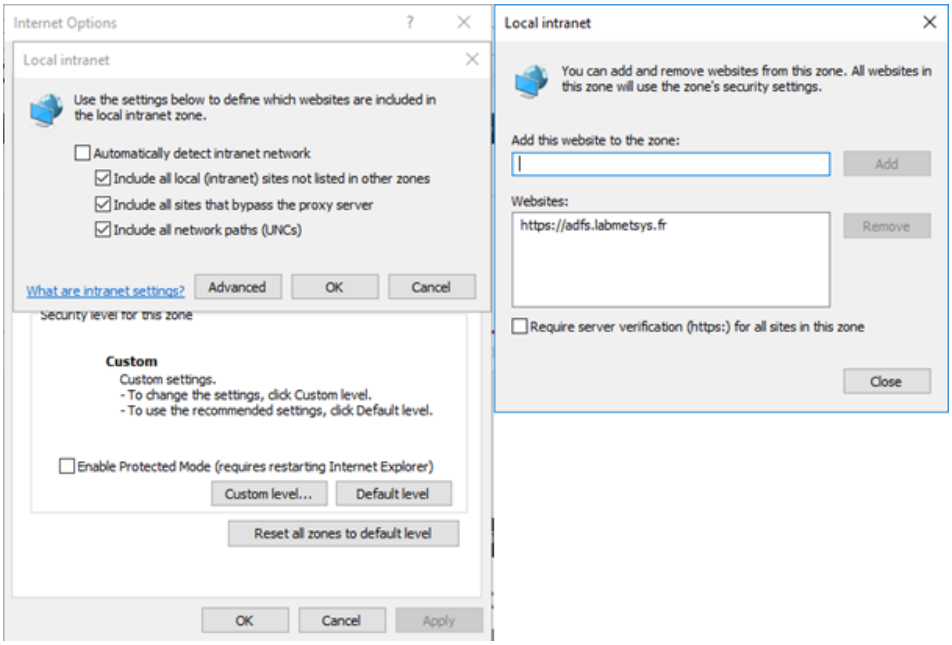
Le serveur d'authentification *Azure Active Directory* redirige donc le navigateur vers l'URL du serveur ADFS 3.0 de l'entreprise (*adfs.labmetsys.fr*). Le navigateur doit ensuite s'authentifier auprès du serveur ADFS 3.0. Par défaut, une fenêtre d'authentification apparaît et l'utilisateur est obligé de saisir de nouveau son login / mot de passe.



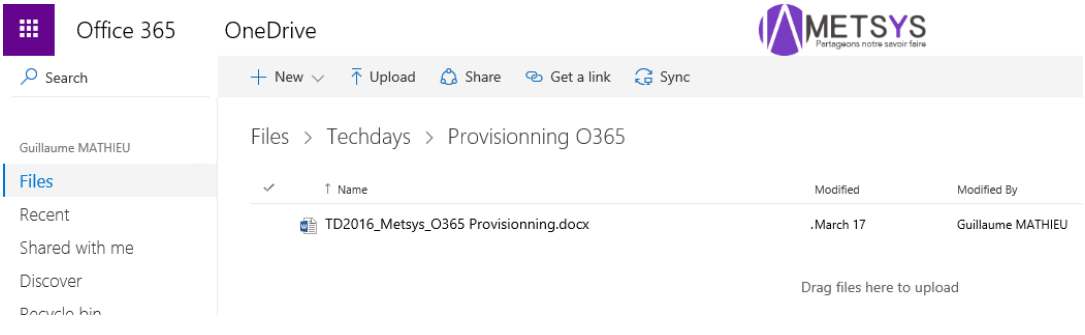
Une fois l'authentification faite, le serveur ADFS 3.0 génère un jeton SAML 1.1 et redirige le navigateur vers https://outlook.office365.com (l'authentification se fait via le jeton SAML 1.1)

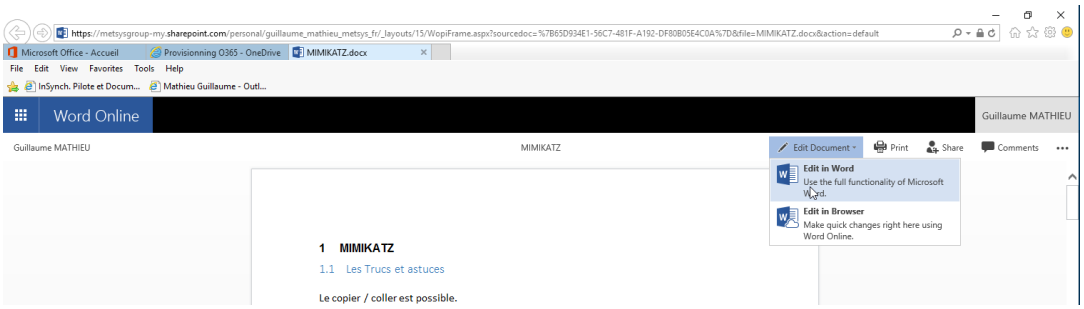
Pour éviter ce POPUP, il est nécessaire d'ajouter le site web *https://adfs.labmetsys.fr* qui correspond au serveur ADFS dans la zone *Intranet Local* d'Internet Explorer. En effet, Internet Explorer est configuré pour envoyer le login / mot de passe automatiquement au site web qui est dans la zone *Intranet Local*. Ce mécanisme est appelé authentification intégrée.

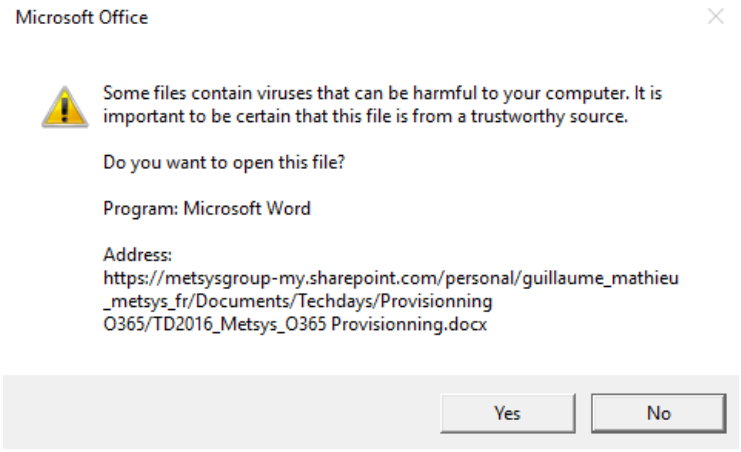




On notera aussi que par défaut, un POPUP apparaît quand un utilisateur ouvre un fichier depuis son OneDrive for Business (le site web en ligne).







Ce message se produit car le site web https://metsysgroup-my.sharepoint.com doit être ajouté dans la zone *Site web de confiance* d'Internet Explorer. On notera qu'il est recommandé d'ajouter aussi tous les URL SharePoint Online décrit dans l'article https://support.office.com/fr-fr/article/URL-et-plages-d-adresses-IP-Office-365-8548a211-3fe7-47cb-abb1-355ea5aa88a2 en tant que site web de confiance.

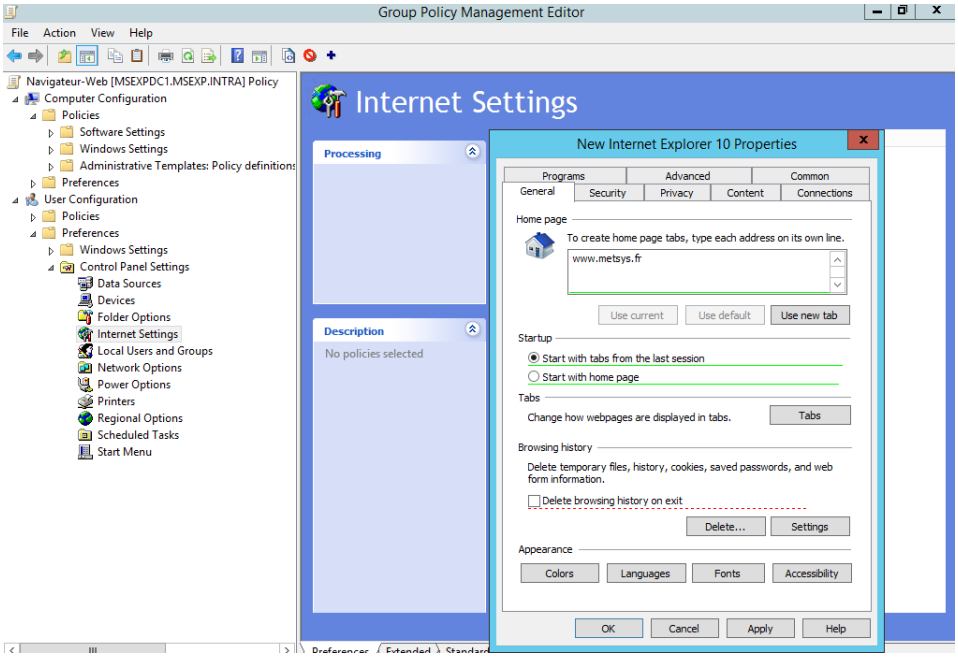
9.2 Paramétrage d'Internet Explorer 11 pour Office 365

Internet Explorer Maintenance Mode est déprécié depuis Internet Explorer 10 et ne peut pas être utilisé pour le paramétrage d'Internet Explorer 11.

Le paramétrage avancé du proxy et des options de sécurité se fait maintenant depuis la section *Préférences* sous : *User Configuration | Preferences | Control Panel Settings*

https://blogs.msdn.microsoft.com/askie/2015/10/12/how-to-configure-proxy-settings-for-ie10-and-ie11-as-iem-is-not-available/

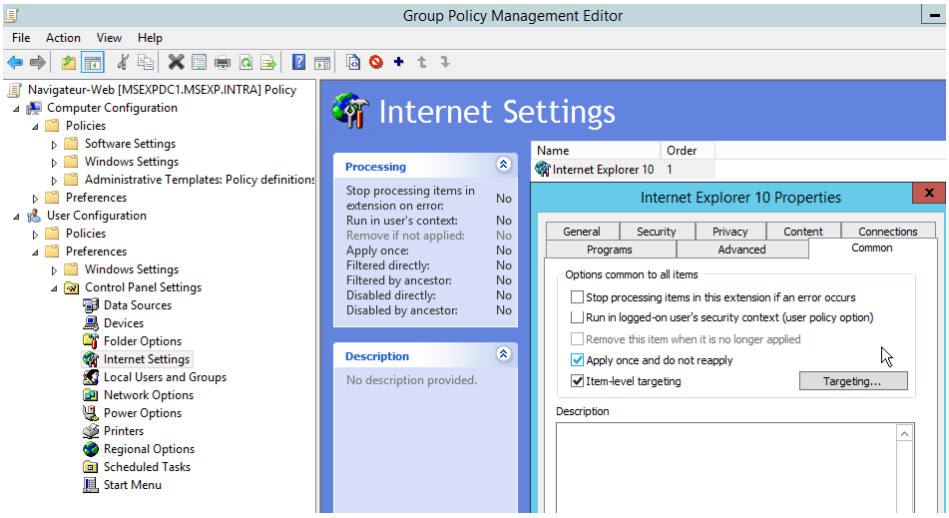
Les paramètres Internet Explorer 10 fonctionnent aussi avec Internet Explorer 11.

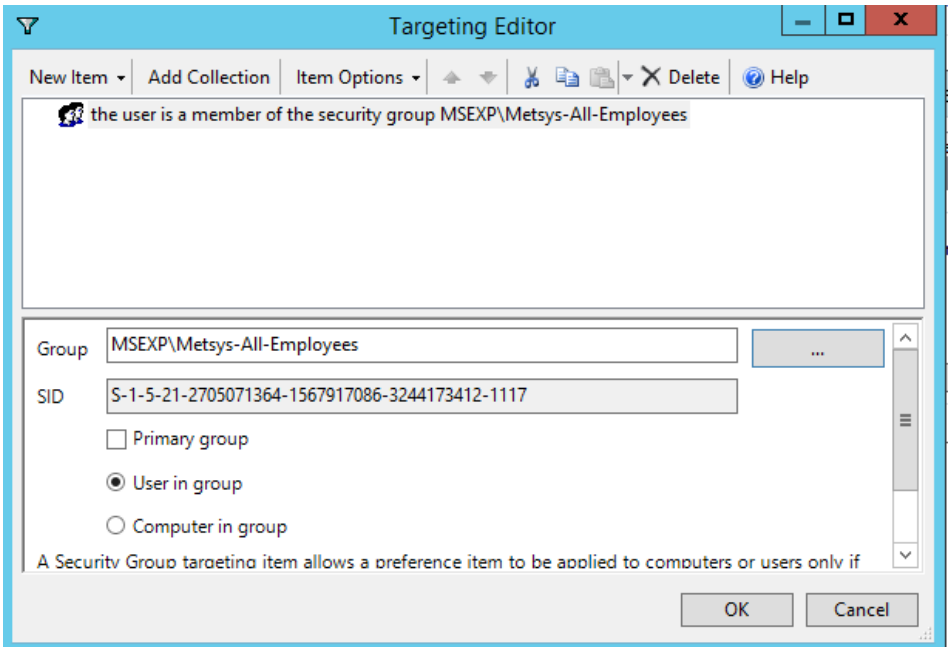


Il est possible de ne pas configurer (en rouge) ou de laisser par défaut (code vert) certains paramètres. Pour cela il faut utiliser les touches du clavier *F5*, *F6*, *F7*, *F8*. Attention, cela ne fonctionne pas correctement parfois en RDP. Il est alors nécessaire d'utiliser le clavier virtuel : https://msitpros.com/?p=1014

Il est aussi possible d'appliquer la configuration Internet Explorer qu'une seule fois. Les utilisateurs peuvent ensuite modifier les paramètres. Ces derniers ne sont pas écrasés quand les GPO se réappliquent sur la station de travail (toutes les 90 minutes).

Il est aussi possible de créer des règles pour cibler à qui s'appliquent la configuration (machines membres d'un groupe, utilisateur spécifique).



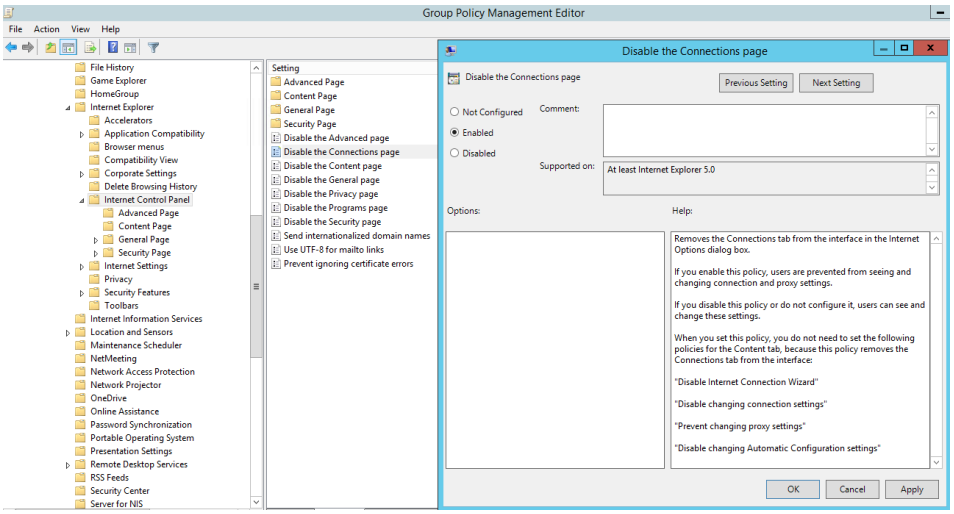


Tous les autres paramètres de configuration d'Internet Explorer 11 (masquer certains onglets comme *Connexion*, définir la liste des sites web de confiance, Intranet Local…) sont au niveau de :

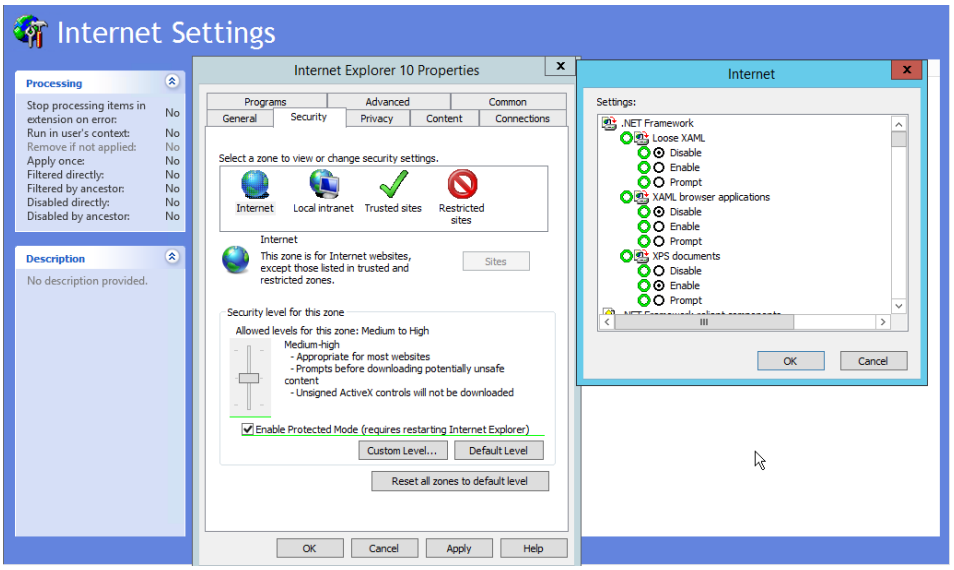
Computer Configuration\Administrative Templates\Windows Components

User Configuration\Administrative Templates\Windows Components

https://technet.microsoft.com/en-us/itpro/internet-explorer/ie11-deploy-guide/group-policy-objects-and-ie11.



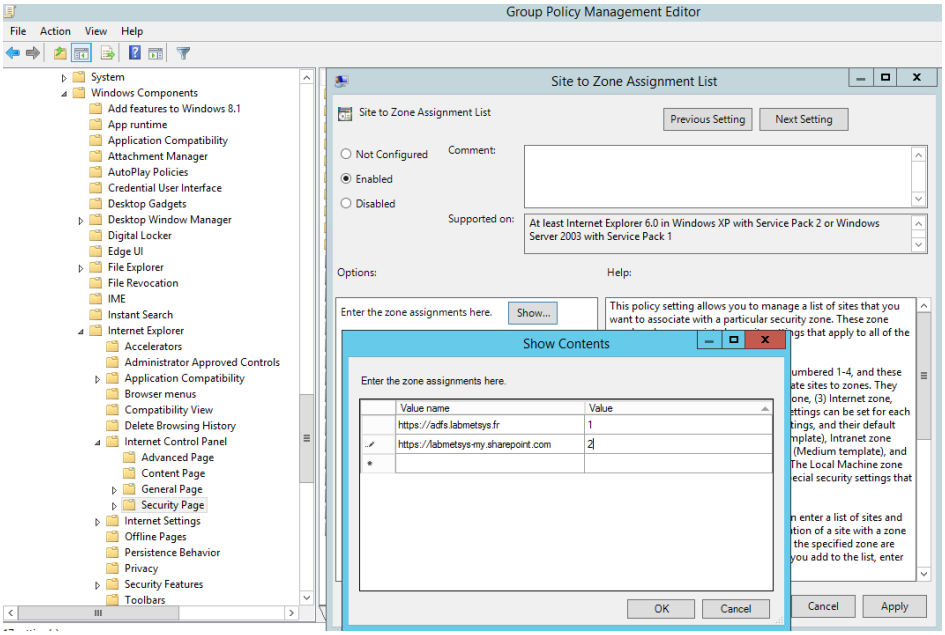
Internet Explorer dispose de 4 zones pour les sites web avec des configurations de sécurité différentes : *Internet*, *Local Intranet*, *Trusted Sites* et *Restricted sites*. Les paramètres de ces zones se configurent à l'aide du nœud *Préférences*.



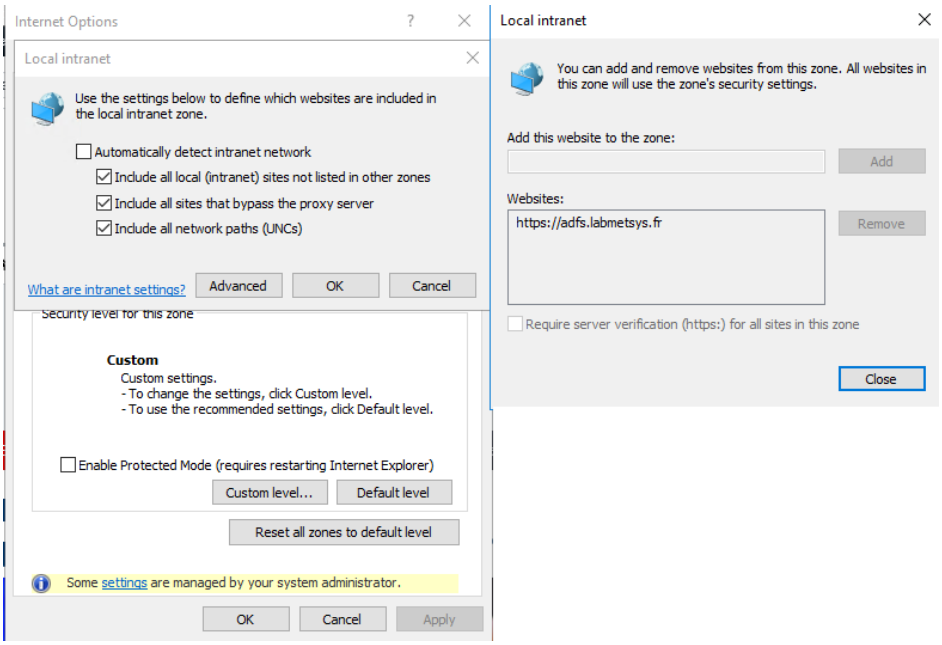
Il est cependant nécessaire d'aller au niveau de *Site to Zone Assignment List* dans la section *User Configuration | Administrative Tools | Windows Components | Internet Explorer | Internet Control Panel | Security Page* pour définir les sites web qui sont dans chacune de ces zones.

- Valeur 1 : sites web Intranet local
- Valeur 2 : sites web de confiance
- Valeur 3 : sites web Internet
- Valeur 4 : sites web restreints

Dans l'exemple ci-dessous, https://adfs.labmetsys.fr a été ajouté dans la zone *Intranet local* d'Internet Explorer.



Une fois cette GPO appliquée, l'utilisateur ne peut plus ajouter un site web en tant que site web de confiance.



Si vous souhaitez permettre aux utilisateurs de modifier les propriétés de leur navigateur, il est possible de déployer directement les entrées de registre correspondantes comme expliqué dans l'article https://blog.thesysadmins.co.uk/group-policy-internet-explorer-security-zones.html.

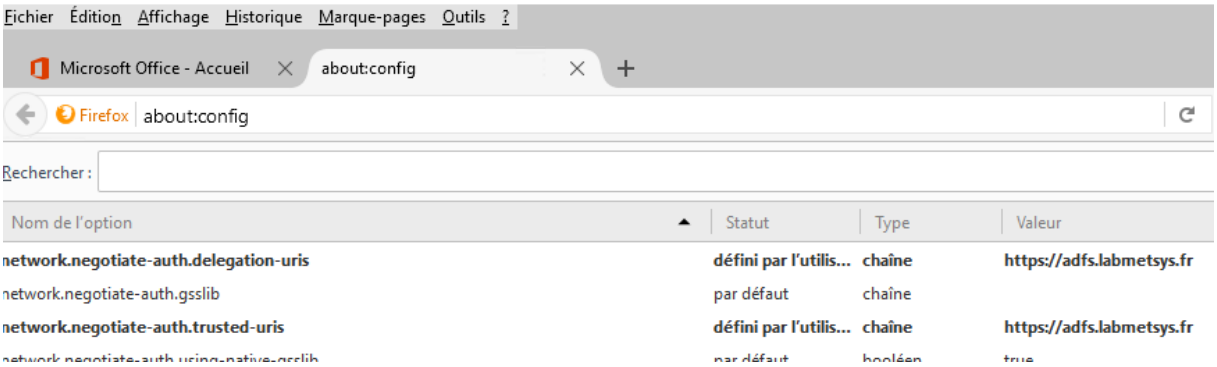
Pour connaître la zone d'un site web, se connecter sur ce site avec Internet Explorer et aller dans le menu *File | Properties*.

9.3 Paramétrage de Firefox pour Office 365

Firefox peut être configuré de manière avancée en tapant *about:config* dans la barre d'adresse.

Pour permettre le bon fonctionnement de Firefox avec ADFS 3.0 et Office 365, il est nécessaire d'appliquer la procédure suivante : https://jorgequestforknowledge.wordpress.com/2015/05/15/configuring-windows-integrated-authn-for-firefox-against-adfs-v3-0-and-higher/

Il faut pour cela activer les 2 paramètres suivants et saisir l'entrée *LABMETSYS.FR* au niveau des paramètres de configuration *network.negotiate-auth.trusted-uris* et *network.negotiate-auth.delegation-uris*.



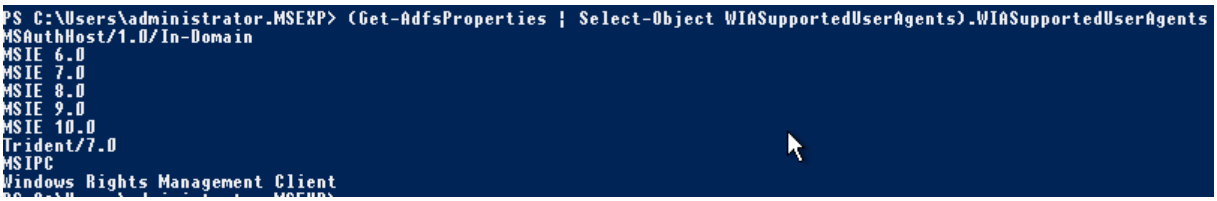
Il faut aussi configurer ADFS pour autoriser Firefox pour faire de l'authentification intégrée en appliquant les procédures ci-dessous :

https://social.msdn.microsoft.com/Forums/fr-FR/3834f6b8-7078-4169-81e0-8f4fbdc08490/ad-fs-30-firefox-and-chrome-no-integrated-windows-authentification?forum=Geneva

http://www.isaacoben.com/2014/03/27/adfs-3-0-iwa-browser-clients-support-for-firefox-and-safari/

Pour voir la configuration actuelle :

Get-AdfsProperties | Select-Object WIASupportedUserAgents



Pour ajouter Firefox dans la configuration WIA :

Set-ADFSProperties -WIASupportedUserAgents ("MSAuthHost/1.0/In-Domain","MSIE 6.0","MSIE 7.0","MSIE 8.0","MSIE 9.0","MSIE 10.0","Trident/7.0","MSIPC","Windows Rights Management Client","Mozilla/5.0")

Il faut aussi saisir cette seconde commande sur le serveur ADFS 3.0 :

Set-ADFSProperties -ExtendedProtectionTokenCheck None

10 L'authentification multi-facteurs et Office 365

L'authentification multi-facteurs Office 365 permet à un utilisateur Office 365 de s'authentifier avec plusieurs facteurs / paramètres. L'utilisateur saisit pour commencer son login Office 365 et le mot de passe associé puis doit ensuite utiliser un ou plusieurs autres facteurs parmi la liste suivante :

- Un mot de passe unique : l'utilisateur saisit un code (reçu par SMS ou généré via l'application *Authenticator*) pour valider son identité.
- Un appel téléphonique : l'utilisateur reçoit un appel téléphonique et doit appuyer sur une touche (# par défaut) pour valider son identité
- Validation : l'utilisateur doit valider la demande d'authentification dans l'application *Authenticator*.

Office 365 permet de disposer gratuitement de la solution *Multi-Factor Authentication for Office 365*. Cette dernière est une version simplifiée d'*Azure Multifactor Authentication* qui est le nouveau de la solution *Phone Factor* rachetée par Microsoft.

https://azure.microsoft.com/en-us/documentation/articles/multi-factor-authentication-how-it-works/#feature-comparison-of-versions

Version	Description
Multi-Factor Authentication for Office 365	This version works exclusively with Office 365 applications and is managed from the Office 365 portal. So administrators can now help secure their Office 365 resources by using multi-factor authentication. This version comes with an Office 365 subscription.
Multi-Factor Authentication for Azure Administrators	The same subset of Multi-Factor Authentication capabilities for Office 365 will be available at no cost to all Azure administrators. Every administrative account of a Azure subscription can now get additional protection by enabling this core multi-factor authentication functionality. So an administrator that wants to access Azure portal to create a VM, a web site, manage storage, mobile services or any other Azure Service can add multi-factor authentication to his administrator account.
Azure Multi-Factor Authentication	Azure Multi-Factor Authentication offers the richest set of capabilities. It provides additional configuration options via the Azure Management portal, advanced reporting, and support for a range of on-premises and cloud applications. Azure Multi-Factor Authentication can be purchased as a stand-alone license and is bundled within Azure Active Directory Premium and Enterprise Mobility Suite. It can also be purchased on a consumption basis by creating an Azure Multi-Factor Authentication Provider in an Azure subscription.

Le paramétrage de la solution est très simple et est décrit dans les articles suivants :

https://support.office.com/en-us/article/Set-up-multi-factor-authentication-for-Office-365-users-8f0454b2-f51a-4d9c-bcde-2c48e41621c6?ui=en-US&rs=en-US&ad=US

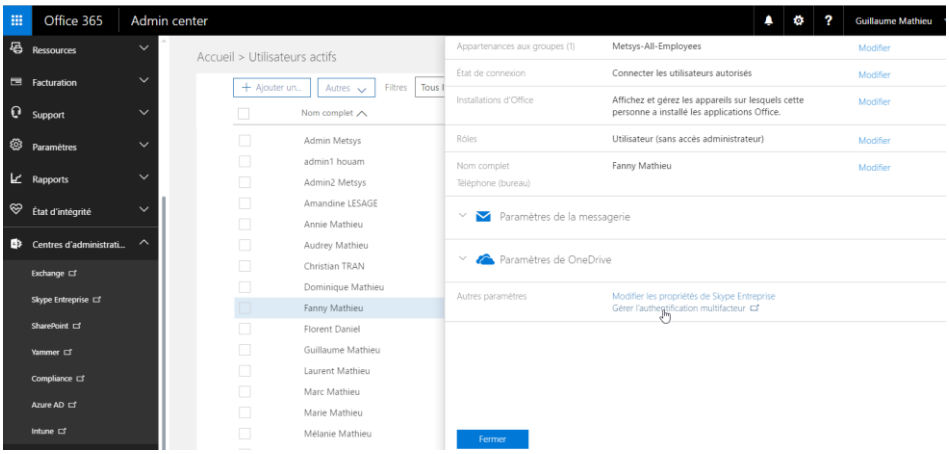
https://support.office.com/en-us/article/Plan-for-multi-factor-authentication-for-Office-365-Deployments-043807b2-21db-4d5c-b430-c8a6dee0e6ba?ui=en-US&rs=en-US&ad=US

Pour permettre le bon fonctionnement de l'authentification multi-factor avec Office 365 ProPlus (Word, Excel, PowerPoint, Outlook, Skype for Business), il est nécessaire d'activer Modern Authentication (ADAL) au niveau d'Exchange Online et Skype for Business (voir paragraphe sur la fédération d'identité de ce document). Si *ADAL* (*Modern Authentication)* n'est pas activé, il est nécessaire d'utiliser des mots de passe d'application qui ne permettent pas une expérience utilisateur satisfaisante.

The following figure shows how the updated Office 2013 device apps (on Windows) enable users to sign in with MFA. TheOffice 2013 device apps support multi-factor authentication through the use of the Active Directory Authentication Library (ADAL). Azure AD hosts a webpage where users can sign in. The identity provider can be Azure AD or a federated identity provider like AD FS. The authentication for federated users follows these steps:

1. Azure AD redirects the user to the sign-in web page hosted by the identity provider of record for the Office 365 tenant. The identity provider is determined by the domain specified in the user's sign in name.
2. The user signs in on the sign in web page on his or her device.
3. The identity provider returns a token to Azure AD when the user is successfully signed in.
4. Azure AD returns a JSON Web Token (JWT) to the Office device app, and the device app is authenticated by using a JWT with Office 365.

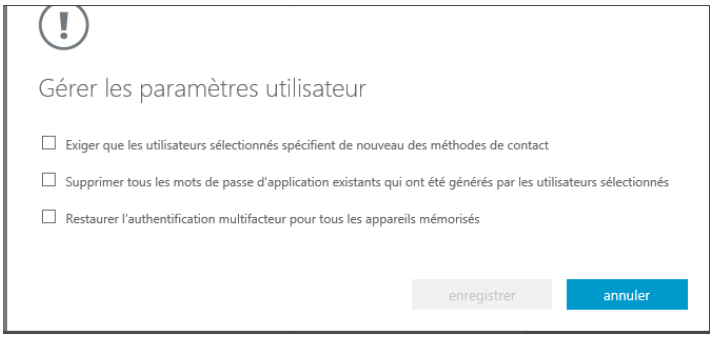
Une fois cette action effectuée, il suffit de cliquer sur le lien *Gérer l'authentification multifacteur* au niveau des propriétés d'un compte utilisateur.



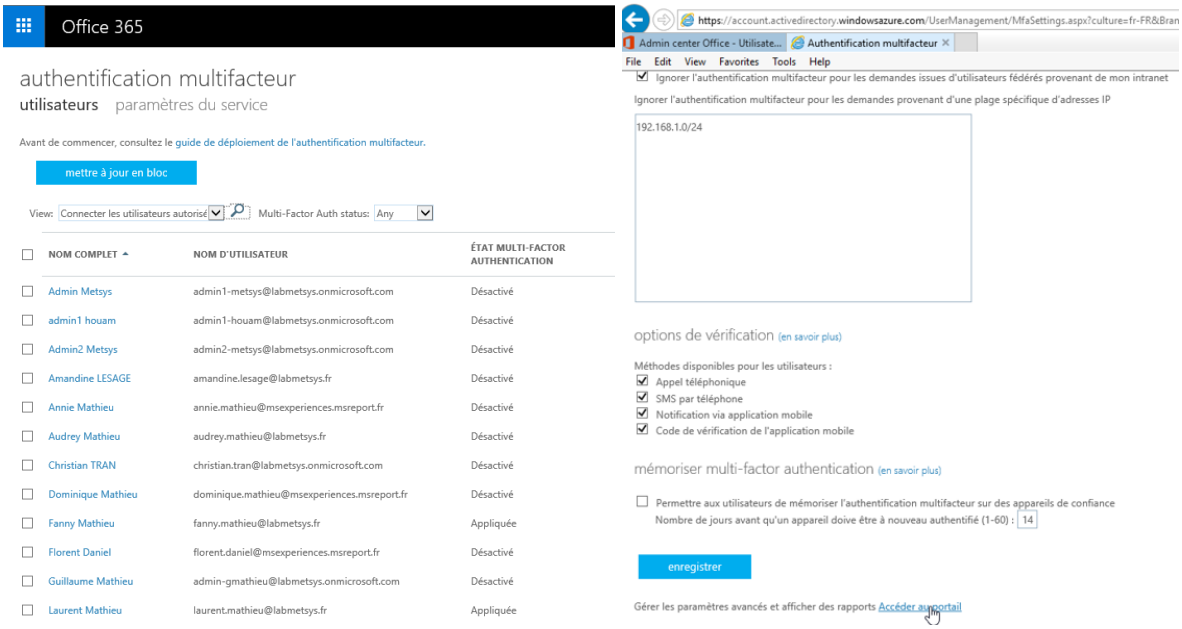
On est alors redirigé vers le site web :

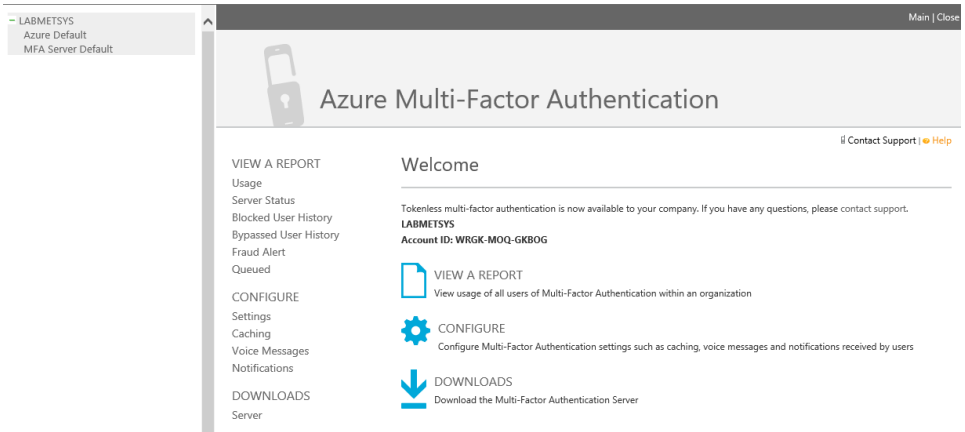
https://account.activedirectory.windowsazure.com/UserManagement/MultifactorVerification.aspx?culture=fr-FR&BrandContextID=O365

L'onglet *Utilisateurs* permet d'activer la solution pour un utilisateur et d'exiger entre autre que ce dernier se réenregistre.

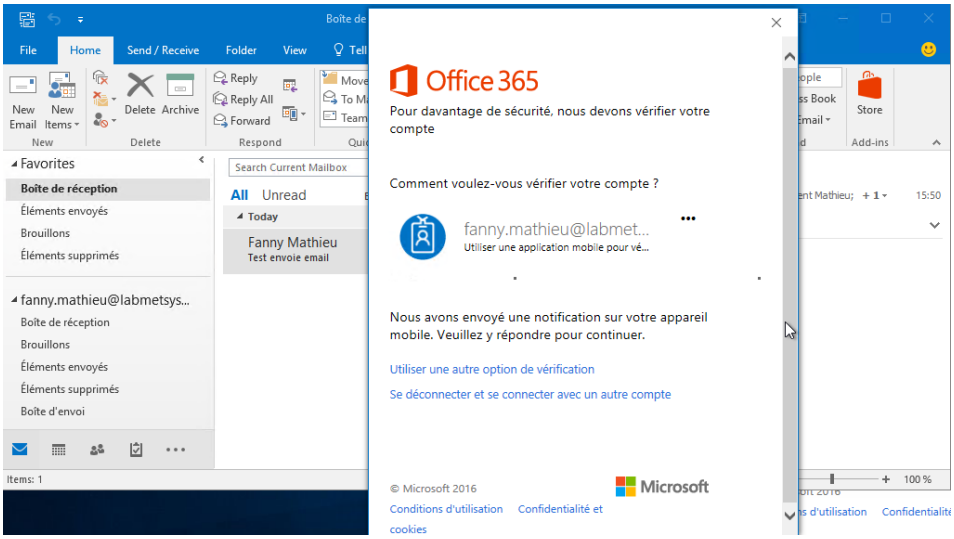


L'onglet *Paramètres du service* permet de configurer la solution (les facteurs d'authentification, les plages d'exclusion). Il est possible d'accéder à l'interface d'administration avancée avec le lien *Accéder au portail* en bas de page. On arrive alors à une nouvelle page https://pfweb.phonefactor.net/framefactory. On notera que Microsoft n'a pas modifié la page d'administration qui garde l'ancien nom de la solution (Phone Factor).





L'utilisateur doit ensuite s'enregistrer et choisir une des méthodes d'authentification. Il peut le faire depuis l'interface web ou Office 365 ProPlus (Word, Excel, PowerPoint…). La capture ci-dessous montre la solution une fois qu'un utilisateur s'est enregistré.



11 La délégation d'administration et Office 365

11.1 Synthèse du besoin

Dans l'exemple ci-dessous, le groupe Metsys souhaite dispose de 2 entités *Houam* et *Metsys*.

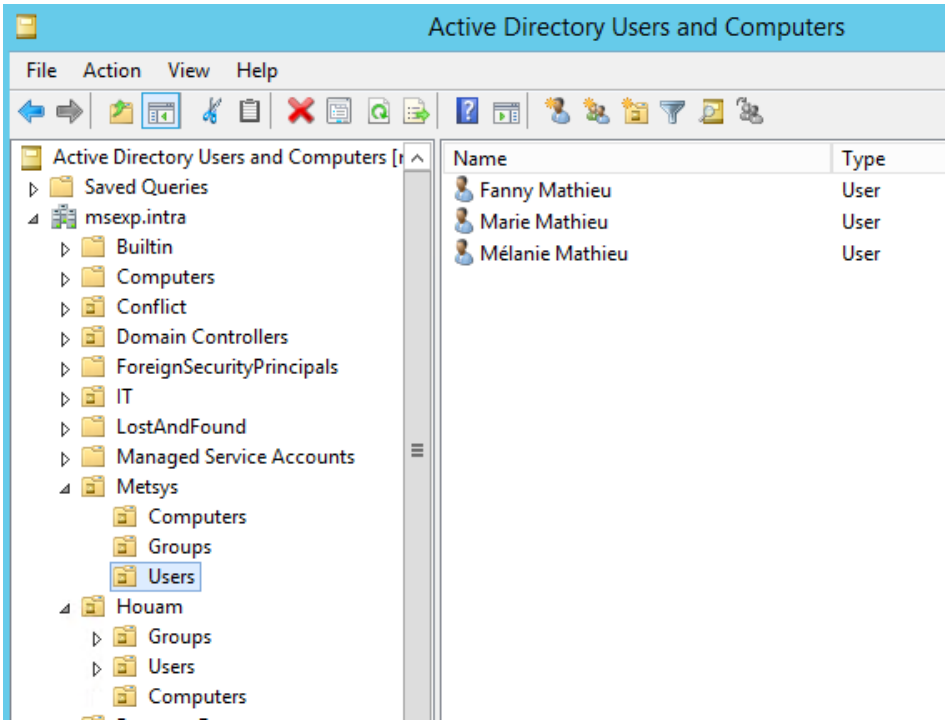
Le groupe Metsys dispose de contacts informatiques pour chacune de ces 2 sociétés. Ces personnes sont en charge des tâches quotidiennes comme la création des comptes utilisateurs et le paramétrage des machines et la gestion des licences Office 365. Elles peuvent être amenées à configurer aussi les comptes Office 365 (ajout d'un alias email) ou d'une option.

La direction du groupe Metsys souhaite que chaque contact informatique puisse uniquement gérer les utilisateurs de son entité et dispose des droits les plus réduits possibles au niveau du Tenant Office 365.

Pour cela, les comptes Azure Active Directory suivants ont été créés :

admin1-metsys@labmetsys.onmicrosoft.com : ce compte pour gérer tous les utilisateurs de l'entité *Metsys.*

admin1-houam@labmetsys.onmicrosoft.com : ce compte pourra gérer tous les utilisateurs de l'entité *Houam.*



Une délégation d'administration fine a déjà été mise en place de manière similaire dans l'annuaire Active Directory. Azure Active Directory et ADFS ont été déployés afin de permettre aux utilisateurs d'accéder de manière transparente à leur messagerie (SSO).

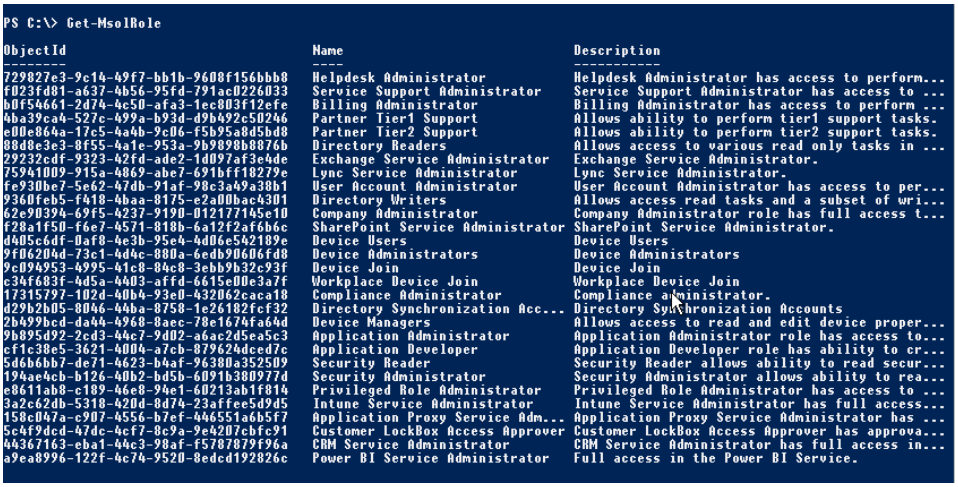
11.2 Comment déléguer l'administration d'Office 365 avec les outils natifs Microsoft

Azure Active Directory dispose de rôles d'administration prédéfinis qui permettent de déléguer l'administration de l'annuaire Azure Active Directory et de tous les services qui s'appuient sur Azure Active Directory comme *Exchange Online*, Skype for Business (anciennement Lync Online). Il est possible de lister ces rôles à l'aide de la commande *Get-MsolRole*.

On notera que certaines applications Office 365 disposent de leur propre système de délégation d'administration. Exchange Online permet par exemple de déléguer l'accès à des commandes PowerShell Exchange Online spécifiques pour certains utilisateurs (*RBAC*). De plus Exchange Online permet aussi de restreindre l'étendue de cette délégation avec les *Management Scopes*.

Skype for Business Online dispose de RBAC tout comme Exchange Online mais ne dispose pas encore d'équivalent des *Management Scope* d'Exchange Online.

SharePoint Online dispose de son propre mécanisme pour la délégation d'administration des sites web.



```
PS C:\> Get-MsolRole

ObjectId                             Name                                Description
--------                             ----                                -----------
729827e3-9c14-49f7-bb1b-9608f156bbb8 Helpdesk Administrator              Helpdesk Administrator has access to perform...
f023fd81-a637-4b56-95fd-791ac0226033 Service Support Administrator       Service Support Administrator has access to ...
b0f54661-2d74-4c50-afa3-1ec803f12efe Billing Administrator               Billing Administrator has access to perform ...
4ba39ca4-527c-499a-b93d-d9b492c50246 Partner Tier1 Support               Allows ability to perform tier1 support tasks.
e00e864a-17c5-4a4b-9c06-f5b95a8d5bd8 Partner Tier2 Support               Allows ability to perform tier2 support tasks.
88d8e3e3-8f55-4a1e-953a-9b9898b8876b Directory Readers                   Allows access to various read only tasks in ...
29232cdf-9323-42fd-ade2-1d097af3e4de Exchange Service Administrator      Exchange Service Administrator.
75941009-915a-4869-abe7-691bff18279e Lync Service Administrator          Lync Service Administrator.
fe930be7-5e62-47db-91af-98c3a49a38b1 User Account Administrator          User Account Administrator has access to per...
9360feb5-f418-4baa-8175-e2a00bac4301 Directory Writers                   Allows access read tasks and a subset of wri...
62e90394-69f5-4237-9190-012177145e10 Company Administrator               Company Administrator role has full access t...
f28a1f50-f6e7-4571-818b-6a12f2af6b6c SharePoint Service Administrator    SharePoint Service Administrator.
d405c6df-0af8-4e3b-95e4-4d06e542189e Device Users                        Device Users
9f062d4d-73c1-4dec-880a-6edb905606fd8 Device Administrators              Device Administrators
9c094953-4995-41c8-84c8-3ebb9b32c93f Device Join                         Device Join
c34f683f-4d5a-4403-affd-6615e00e3a7f Workplace Device Join               Workplace Device Join
17315797-102d-40b4-93e0-432062caca18 Compliance Administrator            Compliance administrator.
d29b2b05-8046-44ba-8758-1e26182fcf32 Directory Synchronization Acc...    Directory Synchronization Accounts
2b499bcd-da44-4968-8aec-78e1674fa64d Device Managers                     Allows access to read and edit device proper...
9b895d92-2cd3-44c7-9d02-a6ac2d5ea5c3 Application Administrator           Application Administrator role has access to...
cf1c38e5-3621-4004-a7cb-879624dced7c Application Developer               Application Developer role has ability to cr...
5d6b6bb7-de71-4623-b4af-96380a352509 Security Reader                     Security Reader allows ability to read secur...
194ae4cb-b126-40b2-bd5b-6091b380977d Security Administrator              Security Administrator allows ability to rea...
e8611ab8-c189-46e8-94e1-60213ab1f814 Privileged Role Administrator       Privileged Role Administrator has access to ...
3a2c62db-5318-420d-8d74-23affee5d9d5 Intune Service Administrator        Intune Service Administrator has full access...
158c047a-c907-4556-b7ef-446551a6b5f7 Application Proxy Service Adm...    Application Proxy Service Administrator has ...
5c4f9dcd-47dc-4cf7-8c9a-9e4207cbfc91 Customer LockBox Access Approver    Customer LockBox Access Approver has approva...
44367163-eba1-44c3-98af-f5787879f96a CRM Service Administrator           CRM Service Administrator has full access in...
a9ea8996-122f-4c74-9520-8edcd192826c Power BI Service Administrator      Full access in the Power BI Service.
```

La nouvelle fonctionnalité appelée *Administrative Unit* d'Azure Active Directory Premium va nous permettre de limiter l'étendue d'un rôle Azure Active Directory à un ensemble d'utilisateurs.

Les *Administrative Units* fonctionnent sur le même principe que les unités d'organisation Active Directory.

Les *Administrative Units* nécessitent une licence Azure Active Directory Premium pour les administrateurs uniquement.

https://azure.microsoft.com/en-us/documentation/articles/active-directory-administrative-units-management/

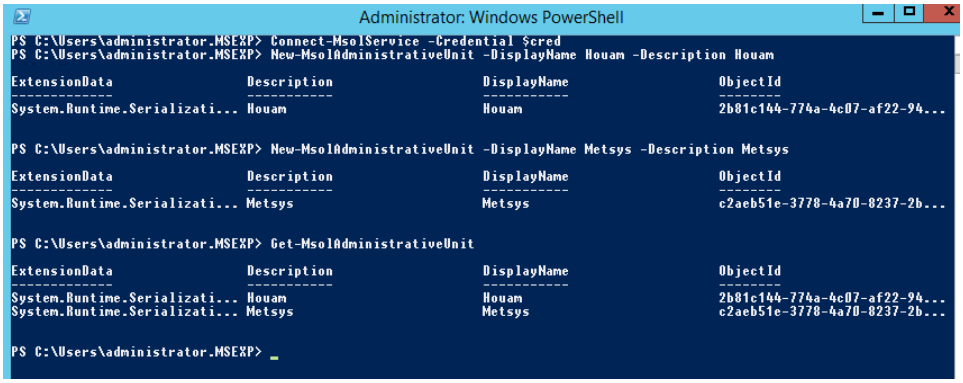
> **Important:**
>
> You can create and use administrative units only if you enable Azure Active Directory Premium. For more information, see Getting started with Azure AD Premium.

La procédure ci-dessous est basée sur l'article https://www.petri.com/create-manage-azure-active-directory-administrative-units

Dans l'exemple ci-dessous on va créer 2 *Administrative Units*.

On va ensuite assigner des utilisateurs Azure Active Directory à cette *Administrative Unit*.

On va enfin assigner un ou plusieurs rôles à cette *Administrative Unit*.



Trouver l'Object ID de l'utilisateur :

Get-MsolUser -UserPrincipalName laurent.mathieu@labmetsys.fr | Select-Object UserPrincipalName,ObjectId

Trouver l'*ObjectID* de la *Managed Unit*

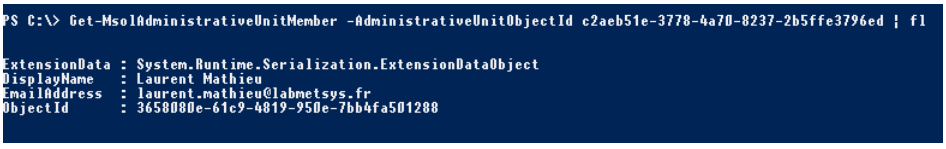
Get-MsolAdministrativeUnit | Select-Object DisplayName,ObjectID

Il faut ensuite ajouter l'utilisateur dans la *Managed Unit*. Il faut ajouter les utilisateurs 1 à 1.

Add-MsolAdministrativeUnitMember -AdministrativeUnitMemberObjectId 3658080e-61c9-4819-950e-7bb4fa501288 -AdministrativeUnitObjectId c2aeb51e-3778-4a70-8237-2b5ffe3796ed

Il est possible de lister les membres d'une *Managed Unit* à l'aide de la commande :

Get-MsolAdministrativeUnitMember –AdministrativeUnitObjectId c2aeb51e-3778-4a70-8237-2b5ffe3796ed



Dans l'exemple ci-dessous on assigne à l'utilisateur *admin1-metsys@onmicrosoft.com* le rôle *User Account Administrator* avec le scope correspondant à la *Managed Unit* Metsys.

Add-MsolScopedRoleMember -RoleObjectId fe930be7-5e62-47db-91af-98c3a49a38b1 -AdministrativeUnitObjectId c2aeb51e-3778-4a70-8237-2b5ffe3796ed -RoleMemberUserPrincipalName admin1-metsys@labmetsys.onmicrosoft.com

Il est possible de contrôler les assignations avec la commande *Get-MsolScopedRoleMember -RoleObjectId fe930be7-5e62-47db-91af-98c3a49a38b1*.

```
PS C:\> Get-MsolScopedRoleMember  -RoleObjectId fe930be7-5e62-47db-91af-98c3a49a38b1

ExtensionData             : System.Runtime.Serialization.ExtensionDataObject
AdministrativeUnitObjectId : c2aeb51e-3778-4a70-8237-2b5ffe3796ed
DisplayName               : Admin Metsys
ObjectId                  : f69c82b3-c7bb-4529-8ced-60e688df174a
RoleMemberType            : User
UserPrincipalName         : admin1-metsys@labmetsys.onmicrosoft.com
```

Dans l'exemple ci-dessous, Marie, Audrey, Laurent et Marc Mathieu ne disposent pas de licences *Azure Active Directory Premium*. Ces 4 comptes sont membres d'une Administrative Unit appelée Metsys.

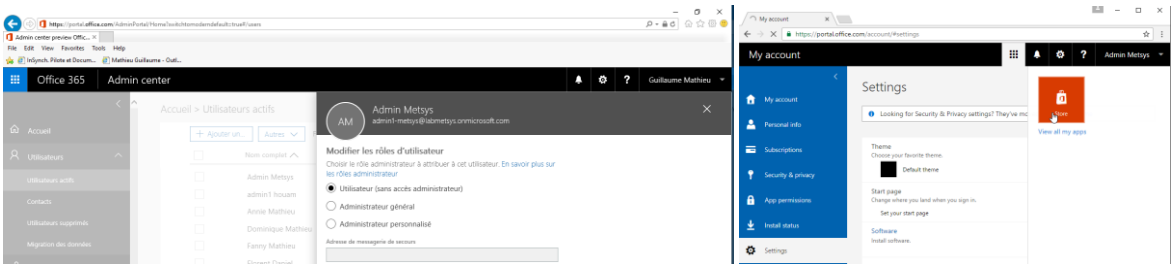
Le compte *admin1-metsys@labmetsys.onmicrosoft* dispose du rôle *User Account Administrator* au niveau de l'annuaire Azure Active Directory.

```
PS C:\> Get-MsolAdministrativeUnitMember -AdministrativeUnitObjectId c2aeb51e-3778-4a70-8237-2b5ffe3796ed

ExtensionData                    DisplayName          EmailAddress                 ObjectId
-------------                    -----------          ------------                 --------
System.Runtime.Serializati... Laurent Mathieu      laurent.mathieu@labmetsys.fr 3658080e-61c9-4819-950e-7b...
System.Runtime.Serializati... Marie Mathieu        marie.mathieu@labmetsys.fr   497f0440-20a4-4ac6-bcc0-a2...
System.Runtime.Serializati... Audrey Mathieu       audrey.mathieu@labmetsys.fr  7deaa9fc-7531-41bc-8929-25...
System.Runtime.Serializati... Marc Mathieu         marc.mathieu@labmetsys.fr    72dfa8e7-a969-4847-b3bf-cb...
```

On notera que l'interface web Office 365 ne prend pas encore en charge les Administrative Unit.

L'administrateur admin1-metsys@lametsus.onmicrosoft.com devra donc gérer les comptes Azures Active Directory à l'aide de PowerShell.



On notera que l'utilisateur admin1-metsys@labmetsys.onmicrosoft.com peut modifier des paramètres comme *Usage Location* mais étrangement ne peut pas assigner de licences Office 365 alors que son rôle le permet.

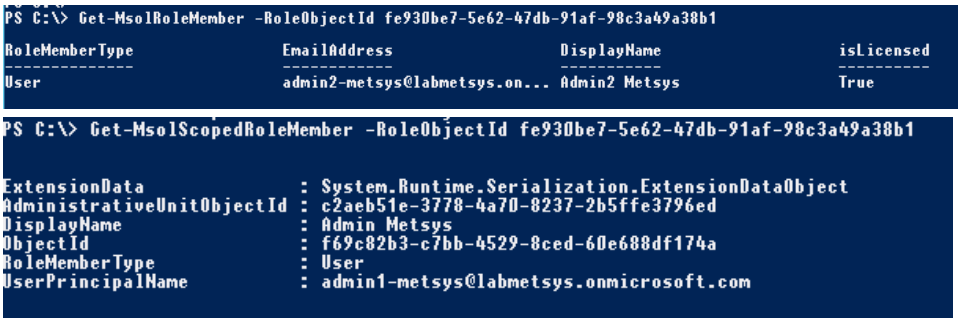
```
PS C:\> Set-MsolUserLicense -UserPrincipalName marc.mathieu@labmetsys.fr -AddLic
enses "labmetsys:STANDARDPACK"
Set-MsolUserLicense : Access Denied. You do not have permissions to call this
cmdlet.
At line:1 char:1
+ Set-MsolUserLicense -UserPrincipalName marc.mathieu@labmetsys.fr
-AddLicenses "l ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
www
    + CategoryInfo          : OperationStopped: (:) [Set-MsolUserLicense], Mic
   rosoftOnlineException
    + FullyQualifiedErrorId : Microsoft.Online.Administration.Automation.Acces
   sDeniedException,Microsoft.Online.Administration.Automation.SetUserLicense
```

```
PS C:\> Set-MsolUser -UserPrincipalName marc.mathieu@labmetsys.fr -UsageLocation FR
PS C:\> Set-MsolUser -UserPrincipalName marc.mathieu@labmetsys.fr -UsageLocation FR
PS C:\> Get-MsolUser -UserPrincipalName marc.mathieu@labmetsys.fr | fl -Property UserPrincipalName,UsageLocation


UserPrincipalName : marc.mathieu@labmetsys.fr
UsageLocation     : FR
```

On ne rencontre pas le problème avec un compte qui dispose du même rôle (admin2) mais qui n'a pas un

scope réduit.



11.3 La solution Metsys

Metsys a développé un module pour déléguer l'administration de la solution Office 365 aux différentes équipes d'administration. Ce module s'appuie sur la solution *Dell Active Roles 7*.

Cette solution est présentée en détail dans la vidéo suivante :

https://experiences.microsoft.fr/channel/metsys-organise-ladministration-des-comptes-office-365-de-technip/7744f48d-7044-4470-b9fc-90935db4d0c7

12 La sauvegarde des données Office 365

12.1 Les scénarios de panne

Il existe au minimum 5 scénarios de pannes nécessitant une restauration des données Office 365 (une boîte aux lettres, un email, un document sous OneDrive) :

- Panne des serveurs hébergeant les données (panne des serveurs Exchange Online, SharePoint Online).
- Suppression accidentelle des données par l'utilisateur (suppression d'un email).
- Suppression accidentelle des données par l'administrateur (suppression de la licence Office 365 ou suppression du compte Azure Active Directory).
- Une corruption des données (fichiers Word, Excel qui refuse de s'ouvrir sur son OneDrive).
- Changement de configuration (modification du site SharePoint que l'on ne souhaite pas conserver).

12.2 Les solutions natives Office 365

Les données de votre Tenant Office 365 sont répliquées dans 2 centres de données différents. Une base de données Exchange Online est par exemple répliquer 4 fois dans 2 centres de données différents. Microsoft propose donc une solution pour le scénario 1 (panne des serveurs).

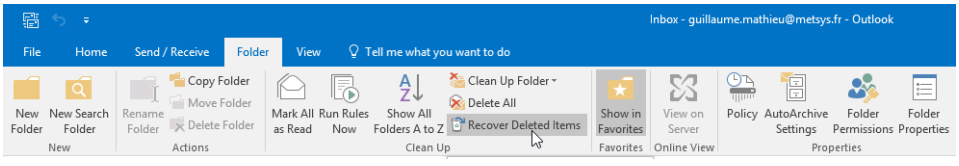
Pour les autres scénarios, Microsoft propose d'utiliser les corbeilles applicatives (Exchange, SharePoint), l'activation de fonctionnalité d'archivage légale (Exchange Online) et propose un service de sauvegarde limité uniquement pour SharePoint Online.

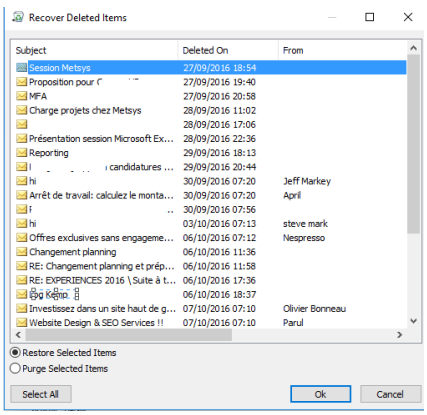
Exchange Online :

Microsoft propose plusieurs options pour la récupération des éléments supprimés.

Un utilisateur peut récupérer les éléments qu'il a supprimés dans Outlook ou Outlook Web App. En effet, les éléments supprimés sont conservés pendant une durée de 14 jours par défaut au niveau des bases Exchange Online. Il est possible de définir cette durée de rétention à 30 jours au niveau de chaque boîte aux lettres à l'aide de la commande PowerShell suivante : *Get-Mailbox -ResultSize unlimited -Filter {(RecipientTypeDetails -eq 'UserMailbox')} | Set-Mailbox -RetainDeletedItemsFor 30*

On notera que les données supprimées sont déplacées dans un conteneur appelé *Recoverable Items folder*. Ce dernier a un quota de 30 Go (warning à 20 Go). Les données supprimées ne sont donc plus comptabilisées dans le quota de 50 Go de la boîte aux lettres Exchange Online.





Une autre option est d'utiliser la fonctionnalité *Mailbox Litigation Hold*. Cette dernière permet d'empêcher un utilisateur de supprimer réellement du contenu de sa boîte aux lettres Exchange Online. Les données Exchange Online supprimées sont toujours déplacées dans le conteneur *Recoverable Items folder* mais le quota de ce dossier passe à 100 Go quand cette fonctionnalité est activée. Si le conteneur *Recoverable Items folder* atteint la limite de 100 Go, l'utilisateur ne peut plus supprimer d'éléments au niveau de sa boîte aux lettres. Cette option se configure au niveau de chaque boîte aux lettres avec la commande PowerShell suivante :

Set-Mailbox Office365UPN -LitigationHoldEnabled $true

Pour activer cette fonctionnalité, il faut être membre du groupe *Discovery Management*.

https://technet.microsoft.com/en-us/library/dn440734(v=exchg.150).aspx

http://blogs.office.com/2013/10/28/office-365-compliance-controls-data-loss-prevention/

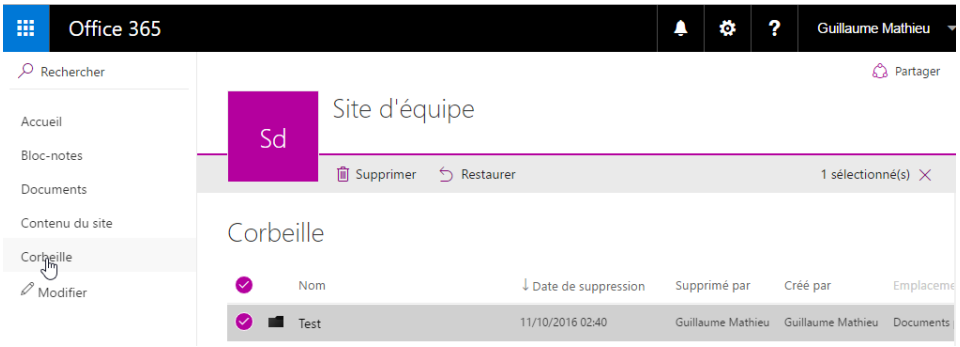
http://windowsitpro.com/exchange-server/no-backups-o365-exchange-online-alternative-recovery-options

SharePoint Online :

Microsoft propose plusieurs solutions pour sauvegarder les sites SharePoint Online.

Une corbeille est disponible au niveau de chaque collection de site SharePoint Online. Elle permet de restaurer les documents pendant 90 jours.

https://itsolutionsblog.net/the-backup-options-in-sharepoint-online/



Si vous supprimez entièrement une collection de site, cette dernière sera visible dans la corbeille SharePoint Online pendant 30 jours.

Il est aussi possible d'Utiliser la fonctionnalité *Version History*.

Cette fonctionnalité est présentée en détail dans l'article https://support.office.com/en-us/article/Enable-and-configure-versioning-for-a-list-or-library-1555d642-23ee-446a-990a-bcab618c7a37

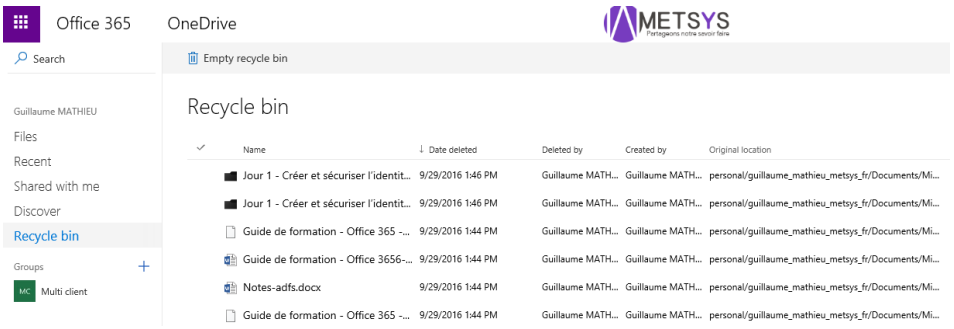
Si aucune des 2 solutions n'est fonctionnelles (l'administrateur a supprimé les éléments depuis la corbeille), il est possible de faire une demande de restauration au support Office 365. Microsoft fait en effet des sauvegardes toutes les 12 heures des sites SharePoint Online et les conserve pendant un maximum de 14 jours.

Le niveau de granularité est le site ou la collection de sites. Les sites / collections de sites sont restaurés à l'emplacement d'origine ! Vous perdrez donc toutes les données depuis la dernière sauvegarde.

http://www.jasperoosterveld.com/2016/08/sharepoint-online-backup-restore/

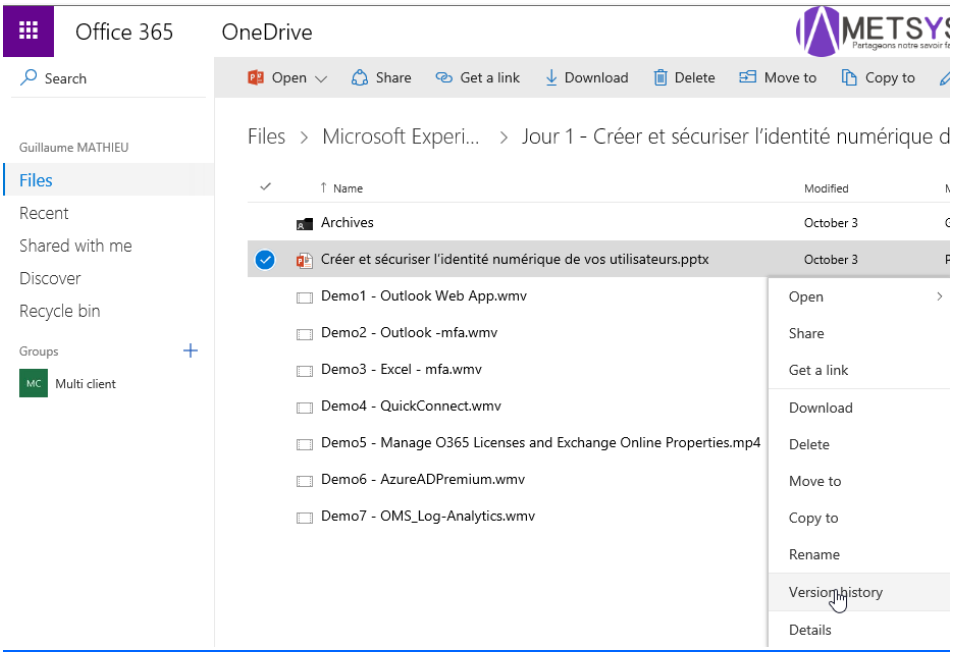
OneDrive for Business :

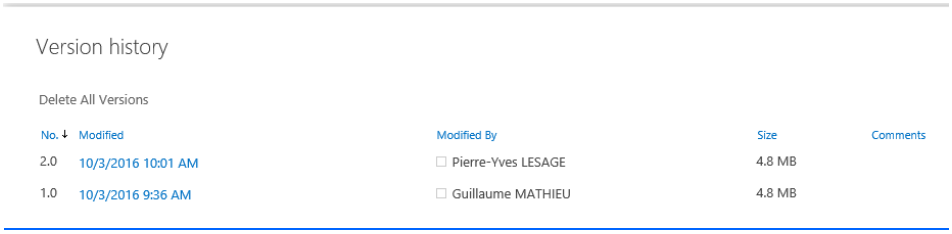
Les utilisateurs peuvent restaurer les données supprimées depuis moins de 90 jours directement depuis l'onglet *Recycle bin* du client web OneDrive for Business. Dans l'exemple ci-dessous, je peux visualiser tous les fichiers supprimés.



Les utilisateurs peuvent restaurer une version précédente d'un fichier à l'aide de la fonctionnalité *Version History*.

https://support.office.com/en-us/article/Restore-a-previous-version-of-a-document-in-OneDrive-for-Business-159cad6d-d76e-4981-88ef-de6e96c93893





En cas de suppression du compte utilisateur Azure Active Directory ou de suppression de la licence SharePoint Online, les données sont supprimées dans les 30 jours par défaut. Cette durée peut être modifiée à l'aide de la commande *Set-SPOTenant -OrphanedPersonalSitesRetentionPeriod*

https://support.microsoft.com/en-us/kb/3042522.

12.3 Les solutions tierces

Des éditeurs comme *CLOUDALLY* (http://www.cloudally.com) proposent des solutions tierces pour réellement sauvegarder les données de votre tenant Office 365 (Exchange Online, SharePoint Online, OneDrive for Business). Ce type de solution est recommandé si vous hébergez des données critiques pour votre société.

13 Migrer vers Office 365

13.1 Migrer d'Exchange On-Premise vers Exchange Online

Il existe principalement 5 solutions :

Solution 1 : effectuer une migration à l'aide du mode hybride Exchange.

Cette procédure est présentée dans le chapitre suivant et permet une migration progressive et partielle des ressources vers Exchange Online.

Solution 2 : effectuer une migration de type *Staged* :

Cette procédure est détaillée dans l'article Microsoft :

https://support.office.com/en-us/article/Perform-a-staged-migration-of-email-to-Office-365-83bc0b69-de47-4cc4-a57d-47e478e4894e?ui=en-US&rs=en-US&ad=US

Cette procédure permet de migrer une organisation Exchange 2003 ou 2007 vers Exchange Online.

Solution 3 : effectuer une migration par basculement (*CutOver*) :

Cette procédure permet de migrer une organisation Exchange 2003, 2007, 2010 ou Exchange 2013 vers Exchange Online. Elle est détaillée dans les articles Microsoft ci-dessous :

https://support.office.com/fr-fr/article/Effectuer-une-migration-%c3%a0-basculement-de-la-messagerie-vers-Office-365-9496e93c-1e59-41a8-9bb3-6e8df0cd81b4?ui=fr-FR&rs=fr-FR&ad=FR

https://support.office.com/fr-fr/article/Ce-que-vous-devez-savoir-sur-une-migration-de-messagerie-%c3%a0-basculement-vers-Office-365-961978ef-f434-472d-a811-1801733869da?ui=fr-FR&rs=fr-FR&ad=FR

On notera que ce type de migration est incompatible avec Azure Active Directory Connect (le serveur de synchronisation) comme expliqué dans les articles ci-dessous :

La désactivation de la synchronisation sur un tenant Office 365 en production n'est pas sans impact sur les utilisateurs France déjà synchronisés.

La synchronisation d'annuaire est un prérequis à ADFS (fédération d'identité) et permet de générer automatiquement la valeur de l'attribut *ImmutableID*.

On perd aussi le provisionning automatique des comptes pendant toute la phase de migration.

On notera enfin qu'il faut jusqu'à 72 heures pour la prise en compte de la désactivation de la synchronisation sur le Tenant Office 365.

Exemple d'impact (tenant configuré avec Azure Active Directory Connect et la synchronisation de mots de passe) :

Si un utilisateur change son mot de passe au niveau de son compte Active Directory pendant la migration, son mot de passe Office 365 ne sera plus le même.

Contournements :

- On peut bloquer le changement de mot de passe temporairement pour tous les utilisateurs.
- On peut aussi lister les comptes dont le mot de passe va changer prochainement et les configurer avec l'option *Password Never expires*.

Pour cette raison, on peut conclure que la procédure de migration par basculement (*CutOver*) n'est pas adaptée à la complexité d'un grand groupe ou un Tenant Office 365 déjà en production et configurée avec des outils de synchronisation ou de fédération d'identité.

De plus, une reconfiguration du profil de messagerie est obligatoire.

Solution 4 : effectuer une migration IMAP :

Cette procédure ne permet pas de migrer les éléments Calendrier ou Contact comme expliqué ci-dessous :

https://support.office.com/en-us/article/What-you-need-to-know-about-migrating-your-IMAP-mailboxes-to-Office-365-3fe19996-29bc-4879-aab9-5a622b2f1481?ui=en-US&rs=en-US&ad=US

Elle ne doit donc pas être utilisée avec Exchange sauf si tous les clients Exchange sont configurés en IMAP (peu probable). On notera que cette procédure est simple mais manuelle. Une reconfiguration du profil de messagerie est obligatoire.

Solution 5 : migration par exportation des boîtes aux lettres sous forme de PST / importation des PST à l'aide de l'outil Office 365

Exchange On-Premise (toutes versions) permet d'exporter les boîtes aux lettres sous forme de PST (outil tiers ou commande PowerShell). Pour importer les fichiers PST, il existe 2 solutions :

https://support.office.com/en-us/article/Use-network-upload-to-import-PST-files-to-Office-365-103f940c-0468-4e1a-b527-cc8ad13a5ea6 (payant).

https://technet.microsoft.com/en-us/library/hh781035(v=exchg.141).aspx (gratuit)

On notera que cette procédure est simple mais manuelle. Une reconfiguration du profil de messagerie est obligatoire.

13.2 Migrer de Google Apps vers Office 365

Il est possible d'utiliser un outil comme *Cloudiway* pour permettre la migration des données Google Gmail ou Google Drive vers leur équivalent Office 365.

Quand Google est utilisé comme source de données, il n'est possible que de migrer 2,5 Go de données par jour (limitation Google). Cloudiway permet de faire de la synchronisation différentielle pour contourner ce problème. Ce point est expliqué dans l'article : http://kb.cloudiway.com/migration-pending-status/

Le chemin d'accès d'un fichier dans *OneDrive For Business* ne doit pas dépasser 260 caractères (pas de limite dans Google Drive). Un dossier appelé _TRUNCATED est créé dans OneDrive for Business pour l'outil de migration si un fichier a un chemin d'accès de plus de 260 caractères dans Google Drive. Ce point est expliqué dans l'article Cloudiway suivant : http://kb.cloudiway.com/folders-created-during-file-migration/

1. _TRUNCATED folder

In One Drive, folders and files url length are limited to 260 characters. In google drive, they can have unlimited length.

In order to migrate the Google Drive folders with url characters length up to 260 to One Drive, a folder _TRUNCATED is created by the migration tool. All the long url folders contents will be migrated to this folder.

Le dossier *Shared with me* dans Google Drive permet de voir les fichiers partagés par les autres utilisateurs comme expliqué dans l'article : https://support.google.com/drive/answer/2375057?hl=en

"Shared with me" lists only files and folders that include your email address in their share settings. You won't see files with share settings set to "Anyone with the link" or "Public."

L'outil *Cloudiway* migre uniquement les données Google Drive de l'utilisateur, pas les données que d'autres utilisateurs Google Drive lui partagent. Cette contrainte doit être prise en compte dans la conception des lots de migration. Il sera nécessaire en effet de migrer ensemble les utilisateurs Google Drive qui partagent des données. Cette limitation est expliquée dans l'article http://kb.cloudiway.com/google-drive-migration :

The main benefit of Cloudiway Migration for migrating your data from Google Drive to OneDrive and Sharepoint Online is that it migrates and maintains the permissions.
To achieve this, Cloudiway Migration is using the following logic:
During the migration of a Google drive, only files that the user owns are migrated.
For example, if you migrate a Google Drive that has 2 files (one file created by the user and one file shared with the user), only the file created by the user will be migrated.

14 Le mode hybride Office 365

14.1 Le mode hybride Exchange

Le mode hybride Exchange permet de disposer de boîte aux lettres sur des serveurs Exchange On-Premise et Online en même temps. Ce mode de fonctionnement est souvent utilisé par des sociétés de taille importante qui sont en cours de migration ou qui souhaitent conserver certaines boîtes aux lettres sensibles sur des serveurs internes (contraintes légales).

Le mode hybride Exchange permet de faire une migration progressive des ressources Exchange 2007, 2010 et Exchange 2013 On-Premise vers Exchange Online. Il est possible par exemple de déplacer la boîte aux lettres d'un utilisateur Exchange 2007 vers Exchange Online avec une commande PowerShell.

Les utilisateurs qui sont migrés sous Exchange Online (Office 365) sont vus comme des *Remote Mailbox* (type *Office 365*) par les serveurs Exchange On-Premise.

Le mode hybride nécessite un certificat SSL. Il est possible de générer gratuitement ce certificat avec l'autorité de certification STARTSSL (environnement de qualification uniquement, voir procédure pour la génération du certificat pour le serveur ADFS).

Il est recommandé de disposer d'Outlook 2013 / 2016 sur les postes de travail ou d'utiliser Outlook Web App.

Le mode hybride ne prend pas en charge tous les scénarios de partage d'éléments entre utilisateurs Exchange Online et utilisateurs Exchange On-Premise comme expliqué dans l'article https://technet.microsoft.com/en-us/library/jj200581(v=exchg.150).aspx#considerations

- **Mailbox permissions migration** On-premises mailbox permissions such as Send As, Receive As, and Full Access that are explicitly applied on the mailbox are migrated to Exchange Online. Inherited (non-explicit) mailbox permissions and any permissions on non-mailbox objects—such as distribution lists or a mail-enabled user—are not migrated. Therefore, you have to plan for configuring these permissions in Office 365 if applicable for your organization. For example, you can use the Add-RecipientPermission and Add-MailboxPermission Windows PowerShell cmdlets to set the permissions in Office 365.

- **Support for cross-premises mailbox permissions** Exchange hybrid deployments support the use of the **Full Access** mailbox permission between mailboxes located in an on-premises Exchange organization and mailboxes located in Office 365. A mailbox on an on-premises Exchange server can be granted the **Full Access** permission to an Office 365 mailbox, and vice versa. For example, an Office 365 mailbox can be granted the **Full Access** permission to an on-premises shared mailbox. Users need to open the mailbox using the Outlook desktop client; cross-premises mailbox permissions aren't supported in Outlook on the web.

> **Note:**
>
> Users might receive additional credential prompts when they first access a mailbox that's in the other organization and add it to their Outlook profile.

We don't, however, support the use of the Send-As, Receive-As, or Send on behalf of mailbox permissions in hybrid deployments between on-premises Exchange and Office 365 organizations. We also don't support delegating permissions to a mailbox or individual folders using the Outlook client. These permissions are only available when both the mailbox granting the permissions, and the mailbox receiving the permissions, are in the same organization. Any mailboxes that receive these permissions from another mailbox need to be moved at the same time as that mailbox. If a mailbox receives permissions from multiple mailboxes, that mailbox, and all of the mailboxes granting permissions to it, need to be moved at the same time. In addition to these permissions, the Auto Mapping feature is also unsupported when used between mailboxes in the on-premises Exchange and Office 365 organizations.

Le mode hybride Exchange n'est pas recommandé si le Tenant Office 365 est configuré avec un *Alternate Login ID.* Les fonctionnalités de partage de boîtes aux lettres entre utilisateurs Exchange Online et Exchange On-Premise ne sont pas disponibles dans ce mode par exemple.

Le mode hybride Exchange nécessite le déploiement d'un serveur Exchange 2010, 2013 pour activer l'hybridation si on dispose d'Exchange 2007. On notera aussi que le partage d'éléments de messagerie entre boîtes aux lettres Exchange 2007 et boîtes aux lettres Exchange Online ne fonctionne pas. Cette fonctionnalité est en effet uniquement disponible à partir d'Exchange 2010 / 2013. Pour cette raison, il est recommandé de migrer toutes les ressources vers Exchange 2013 ou Exchange 2016 avant d'activer le mode hybride.

http://blog.enowsoftware.com/solutions-engine/advanced-sharing-scenarios-with-exchange-hybrid-deployments

L'article de la base de connaissance https://support.microsoft.com/en-us/kb/3064053 s'applique uniquement à *Exchange Online vNext* qui est le nouveau nom de l'offre Office 365 dédié (tenant non mutualisé). Il peut donc être ignoré.

Les procédures ci-dessous expliquent comment déployer le mode hybride.

https://technet.microsoft.com/en-us/library/jj200581(v=exchg.150).aspx

https://technet.microsoft.com/en-us/library/hh534377(v=exchg.150).aspx

https://technet.microsoft.com/en-us/library/jj200581(EXCHG.150).aspx#feat

http://www.msexchange.org/articles-tutorials/office-365/exchange-online/configuring-exchange-2013-hybrid-deployment-and-migrating-office-365-exchange-online-part11.html

https://technet.microsoft.com/fr-fr/library/jj200581(v=exchg.150).aspx

http://blogs.technet.com/b/shahnawaz/archive/2015/06/24/one-stop-for-hybrid-deployment-with-office-365.aspx

https://technet.microsoft.com/en-us/library/jj200581(v=exchg.150).aspx#considerations

14.2 Le mode hybride Skype for Business

Le mode hybride Skype for Business permet d'hybrider des serveurs Lync 2010, Lync 2013 et Skype for Business 2015 avec Skype for Business Online.

https://technet.microsoft.com/en-us/library/jj204805(v=ocs.15).aspx

https://support.office.com/en-us/article/Configure-Skype-for-Business-Server-2015-Hybrid-for-Office-365-operated-by-21Vianet-b06ee805-4349-4519-82fb-b06ed57c0bd0?ui=en-US&rs=en-US&ad=US

15 Trucs et astuces et dépannage Office 365

15.1 Les principaux outils à connaître pour faire du dépannage Office 365

L'outil *Microsoft Remote Connectivity Analyzer* (https://testexchangeconnectivity.com) permet de valider le bon fonctionnement des services Office 365 comme la configuration automatique des clients Outlook et Skype for Business.

En cas de problèmes pour s'authentifier auprès des services Office 365, appliquer la procédure suivante :

https://blogs.technet.microsoft.com/abizerh/2015/06/01/possible-causes-of-authentications-failures-for-federated-users-in-office-365/

Les MVA ci-dessous présentent les différents outils et la méthodologie pour dépanner Office 365 :

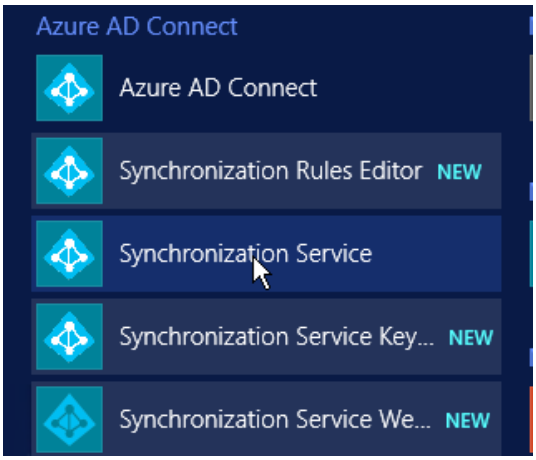
https://mva.microsoft.com/en-us/training-courses/office-365-troubleshooting-8467?l=xIHkqAXz_7504984382

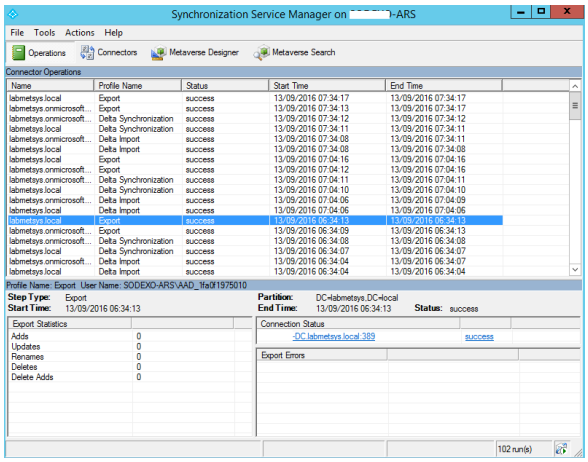
https://mva.microsoft.com/en-us/training-courses/office-365-performance-management-8416?l=webmRJKz_7104984382

https://mva.microsoft.com/en-us/training-courses/understanding-and-troubleshooting-office-365-end-user-performance-issues-14084?l=s3f3rAvmB_6100115881

15.2 Lancer une synchronisation Azure Active Directory Connect manuellement

Par défaut *Azure Active Directory Connect* effectue une synchronisation différentielle toutes les 30 minutes. On peut le voir en lançant la console *Synchronization Services* dans l'onglet *Operations*.





Il est possible de lancer une synchronisation manuelle complète (*initial*) ou incrémentale (*delta*) avec PowerShell. Pour cela, taper les commandes suivantes :

Import-Module ADSync

Start-ADSyncSyncCycle -PolicyType delta

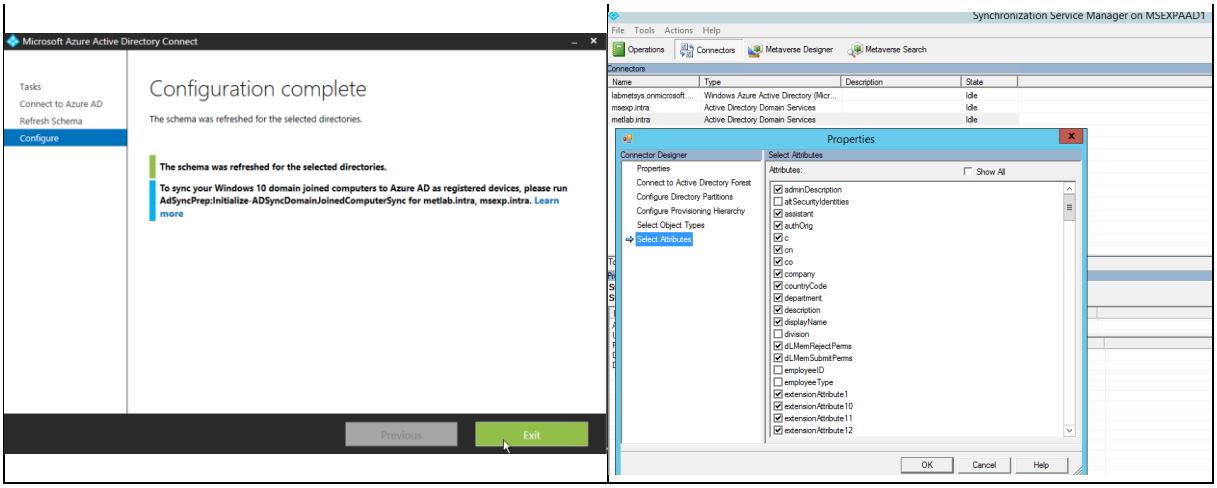
Une synchronisation complète (initiale) est requise en cas de changement dans les règles de synchronisation comme l'ajout d'une nouvelle unité d'organisation. Pour cela, taper les commandes suivantes :

Import-Module ADSync

Start-ADSyncSyncCycle -PolicyType Initial

15.3 Reconfiguration d'Azure Active Directory Connect suite à une mise à jour du schéma Active Directory

Dans l'exemple ci-dessous, le schéma Active Directory du domaine *METLAB.INTRA* a été préparé pour Exchange 2016 après l'installation *d'Azure Active Directory Connect*. Pour mettre à jour la liste des attributs synchronisés par défaut avec un schéma étendu pour Exchange 2016, il est possible d'utiliser l'option *Refresh Schema* de la console *Microsoft Azure Active Directory Connect*. Cela évite d'aller manuellement configurer les règles dans la console *Synchronization Services* d'*Azure Active Directory Connect*.



15.4 Supprimer un utilisateur Azure Active Directory (synchronisé avec Azure Active Directory Connect)

Il n'est pas possible de supprimer un utilisateur Azure Active Directory qui a été créé / synchronisé avec *Azure Active Directory Connect*. Le fonctionnement normal est de supprimer le compte utilisateur dans l'annuaire Active Directory (source). Si cet annuaire n'existe plus, la procédure officielle est de désactiver la synchronisation d'annuaire. La désactivation puis réactivation de la synchronisation d'annuaire va nécessiter environ 72 heures.

https://support.microsoft.com/en-us/kb/2619062

Attention la désactivation de la synchronisation peut réellement nécessiter 72 heures même sur un tenant qui contient très peu d'utilisateurs. Dans mon cas, cette procédure a nécessité 12 heures alors que je disposais que 10 comptes sur mon Tenant Office 365.

Même si on force la commande en PowerShell, cela échoue avec le message ci-dessous car la synchronisation est en *pending disabled*. On notera que l'on peut immédiatement supprimer les comptes qui sont repassés en *InCloud*.

```
[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): y
Set-MsolDirSyncEnabled : You cannot turn off Active Directory synchronization.
At line:1 char:1
+ Set-MsolDirSyncEnabled -EnableDirSync $True
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : OperationStopped: (:) [Set-MsolDirSyncEnabled], MicrosoftOnlineException
    + FullyQualifiedErrorId : Microsoft.Online.Administration.Automation.DirSyncStatusChangeNotAllowedException,Micros
   oft.Online.Administration.Automation.SetDirSyncEnabled
```

On notera que l'on ne peut pas supprimer l'ancien compte de synchronisation via l'interface graphique. C'est uniquement possible en PowerShell.

```
PS C:\> Get-MsolUser | Select-Object UserPrincipalName

UserPrincipalName
-----------------
pylesage_me.com#EXT#@labmetsys.onmicrosoft.com
Sync_SODEXO-ARS_1fa0f1975010@labmetsys.onmicrosoft.com
admin-gmathieu@labmetsys.onmicrosoft.com
sa-ars-o365@labmetsys.onmicrosoft.com
pierre-yves.lesage@labmetsys.onmicrosoft.com


PS C:\> Remove-MsolUser -UserPrincipalName Sync_SODEXO-ARS_1fa0f1975010@labmetsys.onmicrosoft.com

Confirm
Continue with this operation?
[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): y
```

```
PS C:\> Remove-MsolUser -UserPrincipalName Sync_SODEXO-ARS_1fa0f1975010@labmetsys.onmicrosoft.com

Confirm
Continue with this operation?
[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): y
PS C:\> Get-MsolUser | Select-Object UserPrincipalName

UserPrincipalName
-----------------
pylesage_me.com#EXT#@labmetsys.onmicrosoft.com
admin-gmathieu@labmetsys.onmicrosoft.com
sa-ars-o365@labmetsys.onmicrosoft.com
pierre-yves.lesage@labmetsys.onmicrosoft.com
```

15.5 Modifier l'attribut ImmutableID

Quand un compte est synchronisé depuis Active Directory, changer l'attribut *ImmutableID* n'est pas possible (officiellement). Il faut pour faire cette action désactiver la synchronisation d'annuaire au niveau du Tenant Office 365 (application de la procédure https://support.microsoft.com/en-us/kb/2619062).

```
PS C:\Users\Administrator> Set-MsolUser -UserPrincipalName sophie.mathieu@msexperiences.msreport.fr -ImmutableId W1mVr5A
IsO28xgLkg+1XZB==
Set-MsolUser : Unable to update parameter. Parameter name: SourceAnchor.
At line:1 char:1
+ Set-MsolUser -UserPrincipalName sophie.mathieu@msexperiences.msreport.fr -Immuta ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : OperationStopped: (:) [Set-MsolUser], MicrosoftOnlineException
    + FullyQualifiedErrorId : Microsoft.Online.Administration.Automation.PropertyNotSettableException,Microsoft.Online
   .Administration.Automation.SetUser
```

En pratique, il existe une solution de contournement décrite dans cet article :

http://mstechtalk.com/understand-and-modify-office365-users-immutableid/

Il faut déplacer le compte utilisateur dans une unité d'organisation non synchronisée avec Azure Active Directory Connect et lancer une synchronisation. Le compte est alors supprimé au niveau d'*Azure Active Directory*. En pratique, le compte est uniquement marqué comme supprimé. On peut utiliser la commande PowerShell *Restore-MsolUser* pour le restaurer. Une fois l'objet restauré, le compte utilisateur apparaît comme *In Cloud* et non comme un compte synchronisé. Il est donc possible de modifier la valeur de l'attribut *ImmutableID* à l'aide du script https://gallery.technet.microsoft.com/Change-ImmutableID-using-59e3e955.

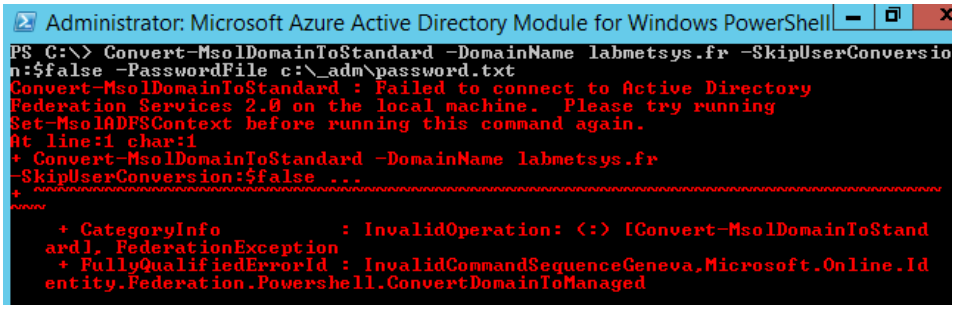
15.6 Forcer la conversion d'un domaine de messagerie fédéré en domaine Managed

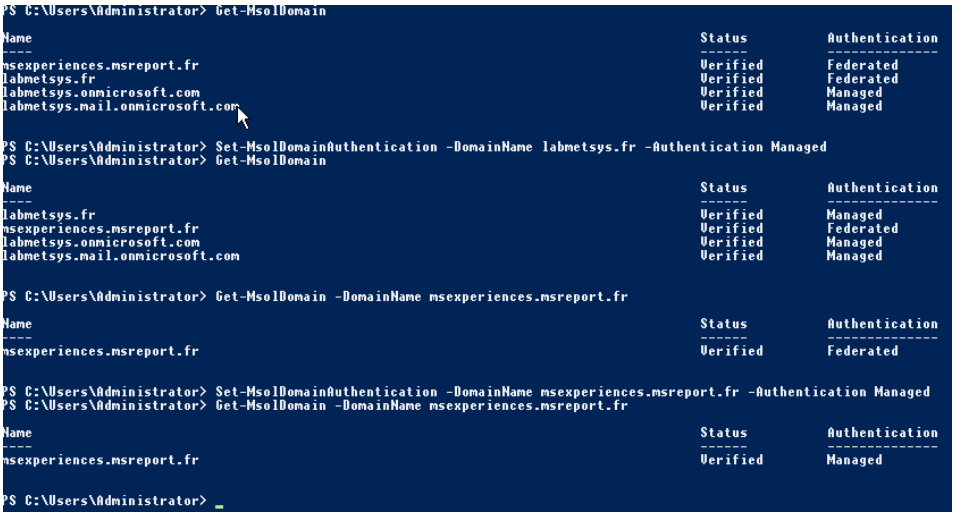
La commande PowerShell *Convert-MsolDomainToStandard* permet de convertir un domaine *Federated* (authentification avec un serveur ADFS / annuaire Active Directory) en un domaine *Managed* (authentification via l'annuaire *Azure Active Directory*).

Cette commande change la configuration du domaine au niveau du Tenant Office 365 et supprime le *Relying Party Trust* d'Office 365 au niveau du serveur ADFS. **Pour que cette commande s'exécute correctement, il faut donc être connecté au serveur ADFS.**

Si le serveur ADFS n'est plus disponible (hors service ou éteint) et que vous souhaitez convertir le domaine *Federated* en domaine *Managed*, il faut exécuter une autre commande PowerShell appelée *Set-MsolDomainAuthentication*.

Exemple : *Set-MsolDomainAuthentication -DomainName msexperiences.msreport.fr -Authentication Managed*





Remarque :

La commande *Set-MsolDomainFederationSettings* permet de changer les paramètres du domaine de messagerie fédéré : https://msdn.microsoft.com/en-us/library/azure/dn194088(v=azure.98).aspx

15.7 Migrer un utilisateur vers un nouveau de domaine de messagerie fédéré

La procédure suivante explique comment modifier le login Office 365 d'un utilisateur (attribut *UserPrincipalName* Azure Active Directory) d'un domaine fédéré A (*@MSREPORT.FR*) vers un domaine fédéré B (*@METSYS.FR*). Ce type de changement génère en effet une erreur de synchronisation.

La migration doit se faire en 2 étapes :

- Configuration du login Office 365 avec domaine A vers le domaine de messagerie par défaut du Tenant Office 365 (exemple : @*LABMETSYS.ONMICROSOFT.COM*). Lancer une synchronisation.
- Configuration du login Office 365 avec le domaine de messagerie par défaut du Tenant vers le domaine de messagerie B. Lancer une synchronisation.

https://support.microsoft.com/en-us/kb/2669550

Remarque :

Lorsque l'outil *Azure Active Directory Connect* réplique un compte dans l'annuaire Azure Active Directory, il vérifie que le suffixe UPN (*@METSYS.FR* par exemple) existe dans le Tenant Office 365. Si ce n'est pas le cas, il

affecte alors au compte utilisateur Azure Active Directory le domaine de messagerie par défaut du Tenant Office 365 (exemple : *@LABMETSYS.ONMICROSOFT.COM*).

15.8 Utilisateurs avec un compte Live et compte Azure Active Directory identiques

Si un utilisateur dispose d'un compte Live (OneDrive, Skype, Outlook, Live…) et d'un compte Azure Active Directory avec le même login, le message ci-dessous apparaît (non bloquant). Pour se connecter avec son compte Azure Active Directory, il faut cliquer sur *Compte professionnel ou scolaire*.

Pour corriger ce problème, il faut appliquer la procédure suivante :

https://support.microsoft.com/fr-fr/help/11545/microsoft-account-rename-your-personal-account