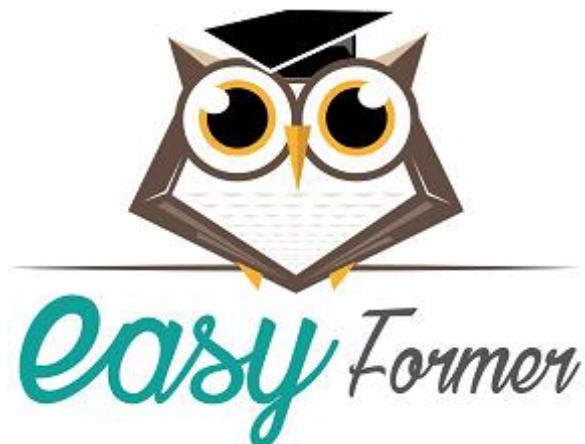


Découvrir le cloud hybride

**Mise en place d'une infrastructure en cloud hybride
avec Microsoft Azure et Windows Server**



Référence : TP-CLOUD-HYBRIDE-2522

Auteur :

Nicolas

Destinataires :

Formateurs

Apprenants

Sommaire

	page
1 INTRODUCTION.....	3
1.1 CONSIGNE.....	3
2 DECOUVRIR AZURE ACTIVE DIRECTORY	4
2.1 INTRODUCTION A AZURE ACTIVE DIRECTORY	4
2.1.1 Qu'est-ce qu'un annuaire (directory) ?.....	4
2.1.2 Qu'est-ce qu'un service d'annuaire (directory service) ?.....	4
2.1.3 Qu'est-ce que le protocole LDAP ?	5
2.1.4 Qu'est-ce qu'AD DS ?	5
2.1.5 Qu'est-ce qu'Active Directory ?.....	5
2.1.6 Qu'est-ce qu'un contrôleur de domaine ?	5
<i>Créez un Active Directory « on-premises ».....</i>	6
<i>Créez quelques utilisateurs dans l'AD local.....</i>	7
2.1.7 Qu'est-ce qu'Azure Active Directory ?	7
2.1.8 Quelles sont les différences entre ADDS et Azure Active Directory ?.....	8
2.2 LES UTILISATEURS ET GROUPES DANS AZURE	9
2.2.1 Les utilisateurs dans Azure.....	9
<i>Créez quelques utilisateurs depuis Azure AD.....</i>	9
<i>Créez des utilisateurs en PowerShell avec le Cloud Shell.....</i>	10
2.2.1 Les types de groupe.....	12
<i>Créez un groupe depuis Azure AD</i>	13
<i>Ajoutez un utilisateur à un groupe</i>	13
2.2.2 Personnalisation des portails de connexion Azure	15
<i>Configurez la marque de société</i>	15
3 DECOUVRIR AZURE ACTIVE DIRECTORY CONNECT.....	16
3.1 INTRODUCTION A AZURE AD CONNECT	16
3.1.1 Qu'est-ce qu'Azure AD Connect ?.....	17
3.1.2 Qu'est-ce qu'un UPN ?.....	17
3.2 PREREQUIS POUR SYNCHRONISER UN AD LOCAL AU CLOUD AVEC AZURE AD CONNECT .	18
<i>Ajoutez un suffixe UPN à votre Active Directory.....</i>	18
<i>Maîtrisez votre synchronisation</i>	19
<i>Créez un compte de service qui sera utilisé par l'outil Azure AD Connect</i>	20
<i>Changez l'UPN des utilisateurs à synchroniser</i>	23
<i>Intégrez vos utilisateurs à synchroniser dans votre groupe de synchro</i>	23
<i>Installez l'outil Azure AD Connect.....</i>	23
3.3 LA SYNCHRONISATION AVEC AZURE AD CONNECT.....	24
3.4 LA JONCTION DES MACHINES A AZURE AD	32
3.4.1 Joindre une machine Windows 10 à Azure AD.....	33



1 Introduction

1.1 Consigne

Si vous êtes un ou une stagiaire en formation et que votre organisme de formation me demande de vous évaluer vous devrez me prouver que vous avez bien participé aux exercices. Dans ce but, je vous demanderai d'effectuer des captures d'écran démontrant votre investissement.

Vous devrez m'envoyer vos captures **en fin de module** par mail à l'adresse que je vous communiquerai ou via un lien de partage *cloud* (OneDrive, Google Drive, etc.) si vous savez le faire **en respectant bien les consignes suivantes** sous peine de pénalités :

- Il faudra coller vos captures dans un document texte (.doc, .docx) que vous m'enverrez. Cette solution est celle que je vous recommande de faire car ça vous permettra de revenir à votre document plus tard quand vous aurez besoin de vous souvenir de ce que vous avez appris.
- Vous pouvez aussi choisir de ne pas faire de document, dans ce cas il faudra :
 - renommer chaque image (.png, .jpg) de capture d'écran obtenue par votre prénom ou vos initiales suivi d'un numéro, par ex. « **prénom01** » ou « **pn02** »
 - m'envoyer vos captures **en une seule fois** dans une archive (.zip, .rar, .7zip) **renomée avec votre prénom** et **contenant toutes vos captures** (= ne pas envoyer les captures une à une dans un mail)

Merci de respecter ces consignes ça me permettra de gérer plus efficacement la partie correction et notation.





L'outil Greenshot : <https://getgreenshot.org/downloads/>

Je vous conseille d'utiliser Greenshot (un logiciel libre & open source) pour les prises de capture d'écran (il est plus pratique que « Outil capture d'écran » de Windows). Une fois installé et lancé en arrière-plan, utilisez la touche « *Impr écran* » de votre clavier pour prendre une capture d'écran rapide puis choisissez « Enregistrer directement » pour qu'elle arrive immédiatement sur votre bureau ou « Enregistrer sous » pour la renommer avant de l'enregistrer où vous voulez. Il propose aussi d'autres actions rapides comme envoyer la capture directement dans un éditeur d'image (pour faire des cadres, des flèches, du floutage) ou dans le presse-papier (pour pouvoir coller la capture d'écran quelque part sans avoir besoin de l'enregistrer en tant que fichier au préalable) :

- Enregistrer directement (utilise les préférences de sortie)
- Enregistrer sous (afficher la boîte de dialogue)
- Ouvrir dans l'éditeur d'image
- Vers l'imprimante
- Vers le presse-papier
- Microsoft Outlook
- Microsoft OneNote
- Microsoft Powerpoint
- Microsoft Word
- Microsoft Excel
- Téléverser vers Imgur
- Fermer

2 Découvrir Azure Active Directory

2.1 Introduction à Azure Active Directory

2.1.1 Qu'est-ce qu'un annuaire (directory) ?

Un annuaire est **une base de données structurée hiérarchiquement, optimisée pour la lecture, consultable à travers un réseau et stockant des informations sur les objets du réseau**.

Ces objets (= les données de l'annuaire) peuvent être de diverses natures et incluent généralement des ressources partagées telles que des ordinateurs, des serveurs, des contrôleurs de domaine, des volumes, des imprimantes, des comptes d'utilisateur et des groupes d'utilisateurs.

L'annuaire met ces objets à la disposition des utilisateurs et des administrateurs réseau afin qu'ils puissent les trouver et les utiliser rapidement.

L'objectif de l'annuaire est de centraliser les données d'une organisation, évitant ainsi la redondance, garantissant la mise à jour des données, et réduisant les coûts d'administration.

2.1.2 Qu'est-ce qu'un service d'annuaire (directory service) ?



Un service d'annuaire est associé à un annuaire et **permet de rendre accessible les informations de l'annuaire aux utilisateurs de cet annuaire** (en faisant correspondre les noms des ressources réseau à leurs adresses réseau respectives).

Par exemple, il stocke des informations sur les comptes d'utilisateurs, comme les noms, les mots de passe, les numéros de téléphone et permet aux utilisateurs autorisés du même réseau d'accéder à ces informations.

Autrement dit : le service fournit les méthodes de stockage des données d'annuaire et de mise à disposition de ces données aux utilisateurs et administrateurs du réseau.

Plus d'infos sur : <https://learn.microsoft.com/fr-fr/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview> et https://en.wikipedia.org/wiki/Directory_service

2.1.3 Qu'est-ce que le protocole LDAP ?

Le protocole LDAP (Lightweight Directory Access Protocol, signifiant « protocole léger d'accès à l'annuaire ») est **un protocole d'application pour l'utilisation de divers services d'annuaire**. Il permet donc d'accéder à des bases d'informations sur les utilisateurs d'un réseau, via l'interrogation d'annuaires.

Autrement dit : le protocole LDAP est **un protocole qui permet de gérer des annuaires grâce à des requêtes d'interrogations et de modification de la base d'informations**.

Plus d'infos sur : <https://www.it-connect.fr/chapitres/les-protocoles-ldap-dns-et-kerberos/> et https://fr.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol

2.1.4 Qu'est-ce qu'AD DS ?

Active Directory Domain Services, « les Services de Domaine Active Directory » ou plus simplement AD DS, est la solution de service d'annuaire développée par l'entreprise Microsoft. AD DS est donc **un service d'annuaire**.

Plus d'infos sur : <https://learn.microsoft.com/fr-fr/training/modules/introduction-to-ad-ds/2-define-ad-ds>

2.1.5 Qu'est-ce qu'Active Directory ?

Active Directory (signifiant en français « annuaire actif ») est la solution d'annuaire développée par l'entreprise Microsoft. Il utilise le protocole LDAP. Active Directory est donc **un annuaire LDAP**. L'objectif principal d'Active Directory est de fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateurs utilisant le système Windows, macOS et encore Linux. Un utilisateur peut ainsi facilement trouver des ressources partagées, et les administrateurs peuvent contrôler leur utilisation grâce à des fonctionnalités de distribution, de duplication, de partitionnement et de sécurisation de l'accès aux ressources répertoriées.

Si les administrateurs ont indiqué les attributs convenables, il sera possible d'interroger l'annuaire pour obtenir, par exemple, « toutes les imprimantes couleur à cet étage du bâtiment ».

Plus d'infos sur : https://fr.wikipedia.org/wiki/Active_Directory

2.1.6 Qu'est-ce qu'un contrôleur de domaine ?

Un contrôleur de domaine (DC) est **un serveur qui répond aux demandes d'authentification de sécurité au sein d'un domaine de réseau informatique**.



Il est chargé d'autoriser l'accès de l'hôte aux ressources du domaine. Il authentifie les utilisateurs, stocke les informations de compte d'utilisateur et applique la politique de sécurité pour un domaine. Lorsque l'on crée un domaine, le serveur depuis lequel on effectue cette création est promu au rôle de « contrôleur de domaine » du domaine créé.

Il devient contrôleur du domaine créé, ce qui implique qu'il sera au cœur des requêtes à destination de ce domaine. De ce fait, il devra vérifier les identifications des objets, traiter les demandes d'authentification, veiller à l'application des stratégies de groupe ou encore stocker une copie de l'annuaire Active Directory.

Un contrôleur de domaine est indispensable au bon fonctionnement du domaine, si l'on éteint le contrôleur de domaine ou qu'il est corrompu, le domaine devient inutilisable.

De plus, lorsque vous créez le premier contrôleur de domaine dans votre organisation, vous créez également le premier domaine, la première forêt, ainsi que le premier site.

Le rôle du serveur de contrôleur de domaine est l'un des rôles les plus importants à sécuriser dans n'importe quel environnement d'ordinateurs fonctionnant avec Windows Server et le service d'annuaire Active Directory. Toute atteinte à l'intégrité d'un contrôleur de domaine ou la perte de ce dernier dans ce type d'environnement pourrait entraîner des conséquences graves pour les ordinateurs clients, serveurs et applications s'appuyant sur les contrôleurs de domaine pour l'authentification, la stratégie de groupe et un annuaire LDAP central.

Plus d'infos sur : <https://www.it-connect.fr/chapitres/controleur-de-domaine-et-domaine/> et https://en.wikipedia.org/wiki/Domain_controller

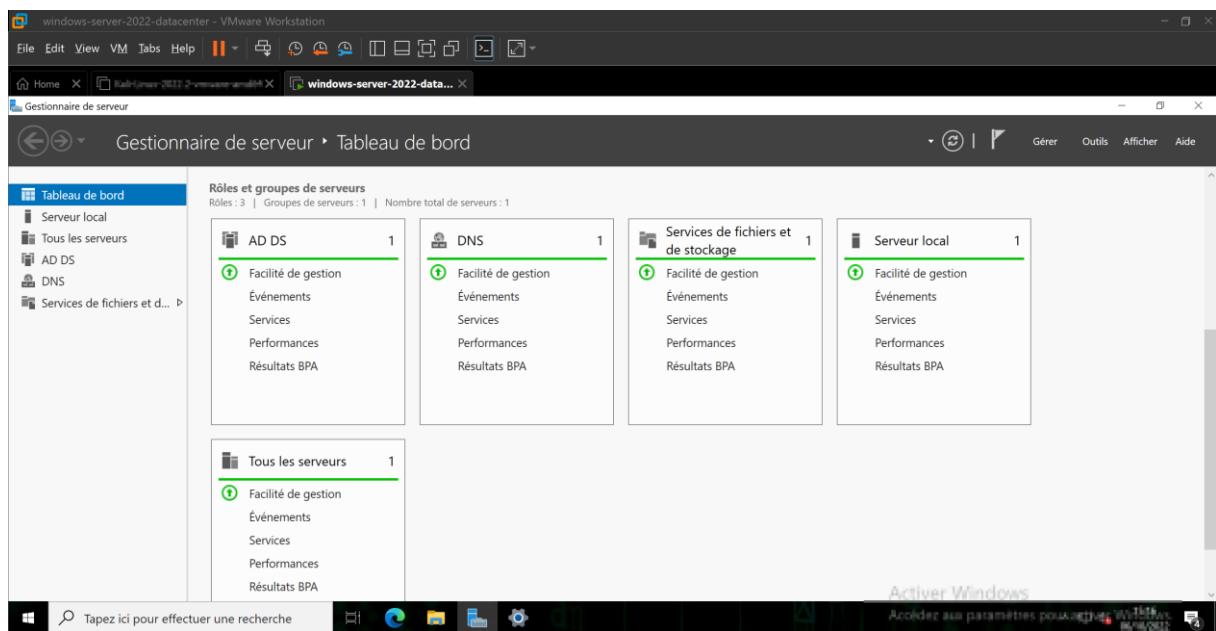
Créez un Active Directory « on-premises »

Pour la réalisation de travaux pratiques de cloud hybride vous allez devoir créer un serveur virtuel sous l'hyperviseur VMware WorkStation qui tiendra le rôle de serveur Active Directory physique. Vous connecterez son interface réseau (Network Adapter) en « bridged » (sur le VMnet0) ou en NAT (sur le VMnet8) pour bénéficier d'un accès internet, vous y installerez un système Windows Server 2019 ou 2022, fixerez son adresse IP (astuce « ncpa.cpl ») et installerez les services DNS et AD DS puis il vous restera à promouvoir le serveur en contrôleur de domaine.

Vous pouvez choisir le nom de domaine de votre choix. Par exemple « monorganisation.local », « tp-azure.lab » ou « monentreprise.onmicrosoft.com ». Moi lors de la création de ce document j'ai choisi de mettre directement le nom de domaine qui est dans le cloud Azure pour m'éviter de faire une petite étape (que je décrirai quand-même ci-dessous). Je vous conseille de ne pas faire comme moi et de choisir un nom de domaine différent car on apprend mieux par la pratique.

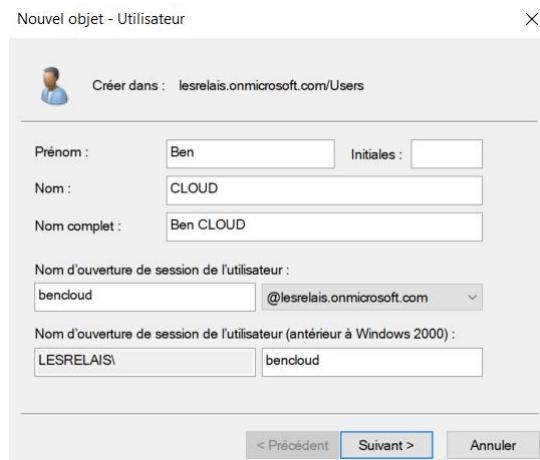
Ensuite prenez une capture d'écran (selon la [consigne](#) précédemment donnée) prouvant que vous avez bien accompli l'exercice. Vous devez faire cela en autonomie car vous êtes censés maîtriser cette partie.





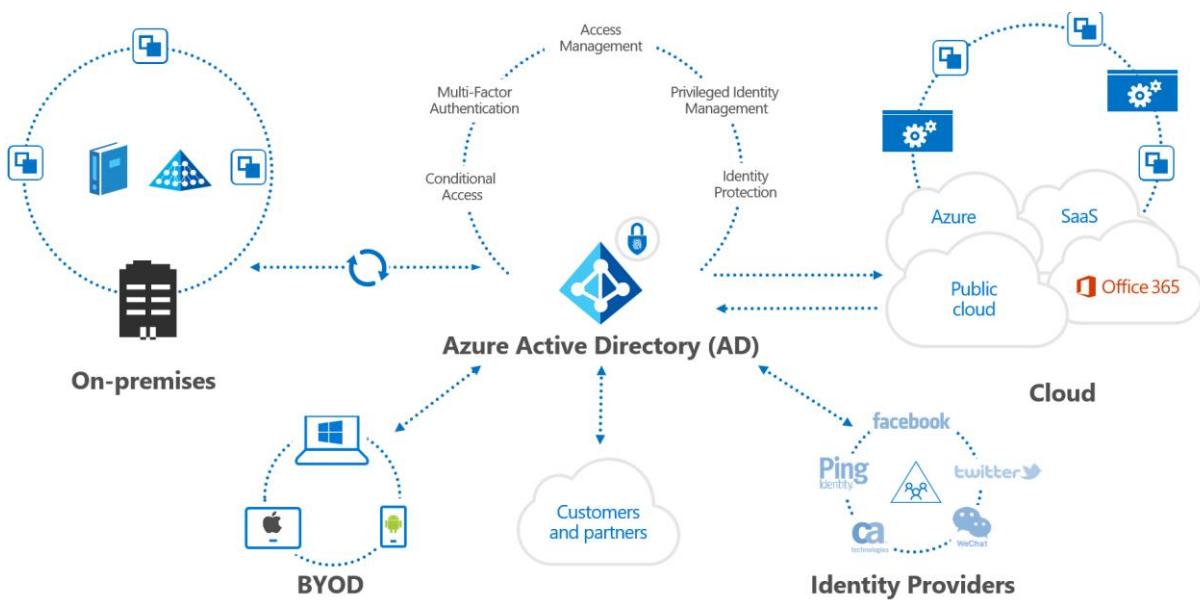
Créez quelques utilisateurs dans l'AD local

Créez quelques utilisateurs dans votre Active Directory local. Faites cela en autonomie. Ensuite prenez une capture d'écran (selon la [consigne](#) précédemment donnée) prouvant que vous avez bien accompli l'exercice.



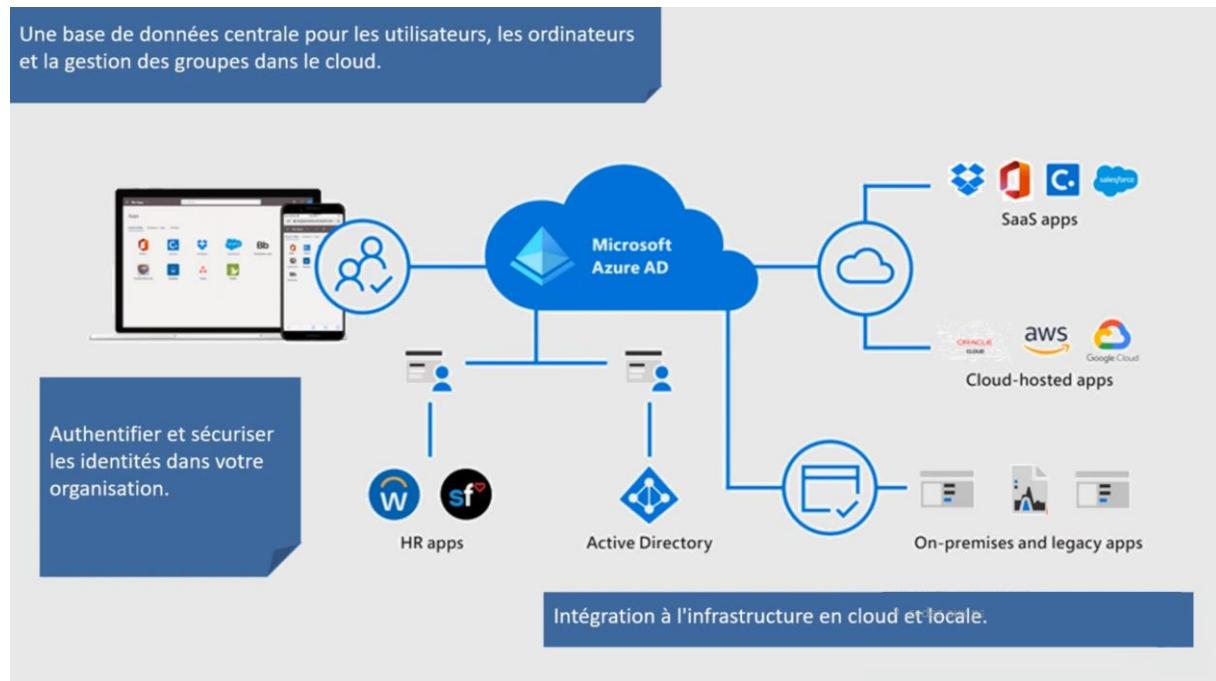
2.1.7 Qu'est-ce qu'Azure Active Directory ?





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

En d'autres termes, Azure Active Directory (Azure AD) est **une solution IDaaS (Identity as a Service) complète qui couvre tous les aspects de l'identité, la gestion des accès et la sécurité**.



Plus d'infos sur : <https://learn.microsoft.com/fr-fr/azure/active-directory/fundamentals/active-directory-whatis>

2.1.8 Quelles sont les différences entre ADDS et Azure Active Directory ?



AD DS vs Azure Active Directory

Fonctionnalité	AD DS	Azure AD
Localisation	Sur site	Azure
Cryptage par défaut	Non	Oui
Protocole de requête	LDAP	REST
Authentification	Kerberos	SAML, WS-Federation, OpenID Connect
Autorisation	Kerberos	OAuth2
Service de fédération avec des services tiers comme Facebook	Non	Oui
Groupes dynamiques	Non	Oui
Utilisateurs et groupes Azure AD	Hiérarchique	Plat
Unités Organisationnelles	Oui	Non
GPOs	Oui	Non

Pour mieux connaître les différences entre Active Directory et Azure Active Directory, consultez : <https://learn.microsoft.com/fr-fr/azure/active-directory/fundamentals/active-directory-compare-azure-ad-to-ad>

2.2 Les utilisateurs et groupes dans Azure

2.2.1 Les utilisateurs dans Azure

Il est à noter que des utilisateurs que j'avais précédemment ajoutés via l'interface d'administration web de Microsoft 365/Office 365 apparaissent dans la liste des utilisateurs Azure. C'est normal car derrière mon *tenant*¹ M365 il y a le même Azure AD que pour mon compte Azure. Je suis dans l'écosystème Microsoft et je constate que ses services cloud sont liés les uns aux autres.

Créez quelques utilisateurs depuis Azure AD

Créez quelques utilisateurs depuis Azure AD puis prenez une capture d'écran (selon la consigne précédemment donnée) prouvant que vous avez bien accompli l'exercice.

¹ Dans l'univers du cloud de Microsoft 365 et Azure, le terme *tenant*, traduit par « locataire » **désigne l'instance dédiée qui est attribuée au client et dans laquelle vont être stockées ses données (objets du système d'information de l'entreprise tels que des groupes, des utilisateurs, des applications)**. Chaque client possède sa propre bulle, son propre *tenant* qui est indépendant des *tenants* des autres entreprises.



Nom d'affichage	Nom d'utilisateur principal	Type d'utilisateur	Synchronisatio...	Identités	Nom de l'entreprise	Type de création
AC	accueil@lesrelais.onmicrosoft.com	Membre	Non	lesrelais.onmicrosoft.com		
BB	benbod@lesrelais.onmicrosoft.com	Membre	Non	lesrelais.onmicrosoft.com		
BL	bob.leponge@lesrelais.onmicrosoft.com	Membre	Non	lesrelais.onmicrosoft.com		
HP	helga.pataki@lesrelais.onmicrosoft.com	Membre	Non	lesrelais.onmicrosoft.com		
LR	contact@lesrelais.onmicrosoft.com	Membre	Non	lesrelais.onmicrosoft.com		

Il est à noter que des utilisateurs que j'avais précédemment ajoutés via l'interface d'administration web de Microsoft 365/Office 365 apparaissent dans la liste des utilisateurs Azure. C'est normal car derrière mon *tenant* M365 il y a le même Azure AD que pour mon compte Azure. Je suis dans l'écosystème Microsoft et je constate que ses services cloud sont liés les uns aux autres.

Créez des utilisateurs en PowerShell avec le Cloud Shell

Il est aussi possible de créer des utilisateurs Azure en PowerShell. Le moyen le plus simple est d'utiliser Azure Cloud Shell qui est un terminal en client léger accessible directement depuis le portail Azure.

Cliquez sur cette icône pour accéder au Cloud Shell d'Azure.

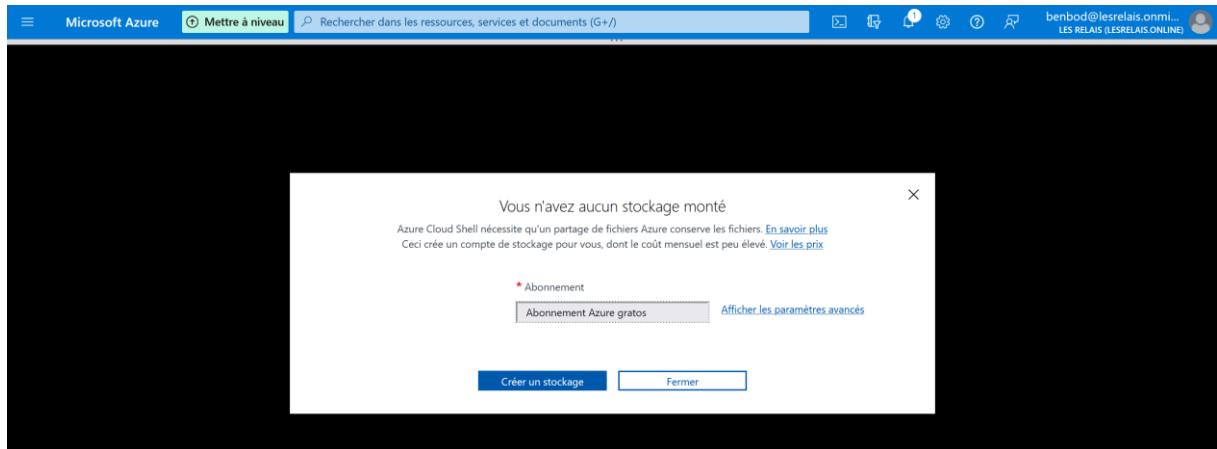
Si vous avez le lien pour y accéder directement : <https://shell.azure.com/>
Vous arriverez sur une page vous demandant de choisir votre shell. Choisissez « PowerShell ».

Mise en place d'une infrastructure en cloud hybride avec Microsoft Azure et Windows Server

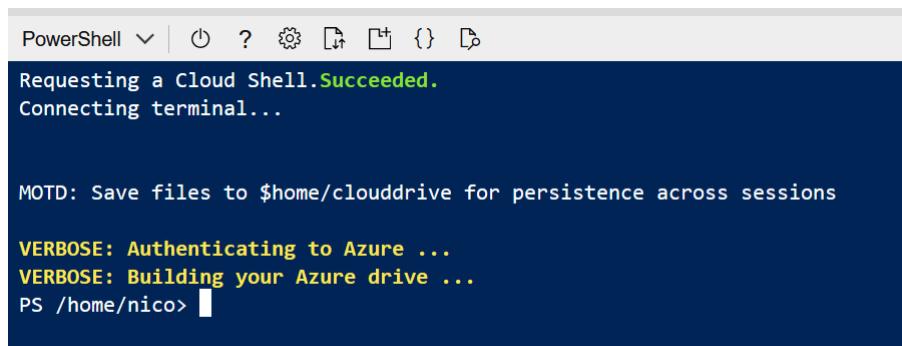
Page 10 sur 37



Azure va vous demander la première fois de créer un compte de stockage.



Votre Shell démarre.



Premièrement il faut lancer la commande pour se connecter à Azure AD :

```
Connect-AzureAD
```

Ensuite, avant de lancer la commande pour créer l'utilisateur, il faudra créer une variable dans PowerShell pour spécifier le profil de mot de passe de l'utilisateur (la commande ci-dessous est sur une seule ligne) :

```
$PasswordProfile = New-Object -TypeName Microsoft.Open.AzureAD.Model.PasswordProfile
```

Puis définissez la valeur du mot de passe dans cette variable, par exemple « 123-Poi !!! » :

```
$PasswordProfile.Password = "123-Poi!!!"
```

Enfin, transmettez cette variable à l'applet de commande :



```
New-AzureADUser -DisplayName "Bob ONION" -PasswordProfile $PasswordProfile -UserPrincipalName "bob.onion@easycloudformer.onmicrosoft.com" -AccountEnabled $true -MailNickname "Bob"
```

L'utilisateur « Bob ONION » est automatiquement créé.

```
PS /home/nico> Connect-AzureAD
PS /home/nico> $PasswordProfile = New-Object -TypeName Microsoft.Open.AzureAD.Model.PasswordProfile
PS /home/nico> $PasswordProfile.Password = "123-Poiii"
PS /home/nico> New-AzureADUser -DisplayName "Bob ONION" -PasswordProfile $PasswordProfile -UserPrincipalName "bob.onion@easycloudformer.onmicrosoft.com" -AccountEnabled $true -MailNickname "Bob"
ObjectID DisplayName UserPrincipalName UserType
----- ----- -----
131c5d0f-7824-41e6-8e95-689435b3cc31 Bob ONION bob.onion@easycloudformer.onmicrosoft.com Member
```

Plus d'infos sur la création d'utilisateurs en PowerShell dans Azure : <https://learn.microsoft.com/fr-fr/powershell/module/azuread/new-azureaduser?view=azureadps-2.0> et <https://learn.microsoft.com/fr-fr/powershell/module/azuread/connect-azuread?view=azureadps-2.0>

2.2.1 Les types de groupe

Il existe des groupes statiques et des groupes dynamiques.

Un groupe statique est un groupe où vous allez devoir vous-même ajouter les objets (ordinateurs, utilisateurs) que vous souhaitez dans ce groupe.

Un groupe dynamique (d'utilisateurs ou d'ordinateurs) permet de faciliter la gestion des groupes car vous pouvez définir une « requête dynamique », une règle d'appartenance basée sur un attribut (par ex. : si le nom de l'utilisateur contient tel caractère ou telle expression, si l'ordinateur est sous tel système d'exploitation) et automatiser l'ajout (ou la suppression) du groupe sur la base de ce critère.

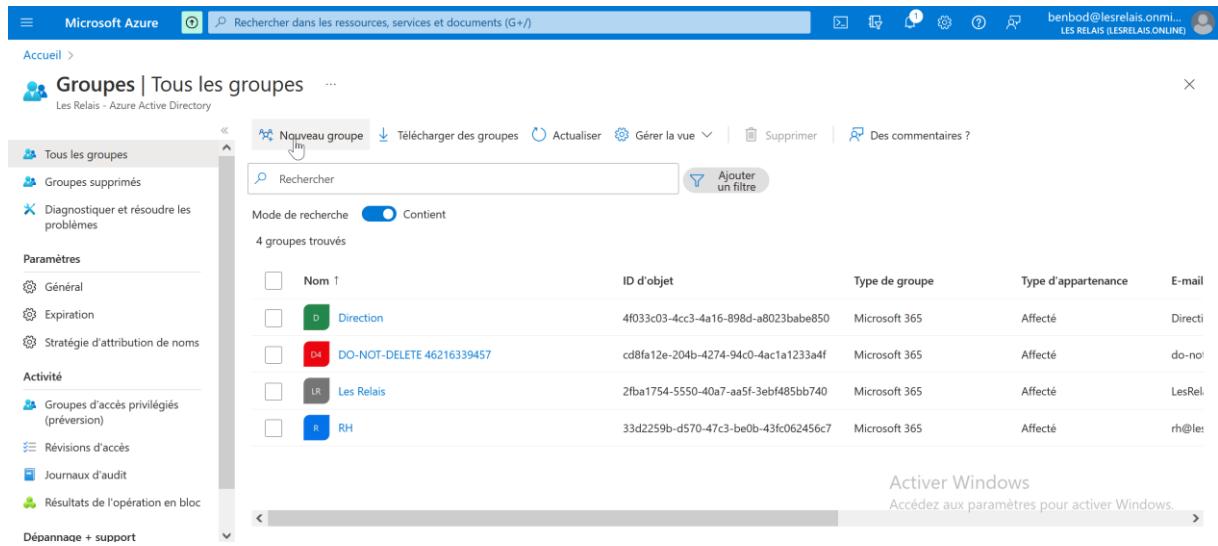
L'utilisation des groupes dynamiques nécessitent une licence Azure AD P1.



Plus d'infos sur : <https://learn.microsoft.com/fr-fr/azure/active-directory/enterprise-users/groups-create-rule>

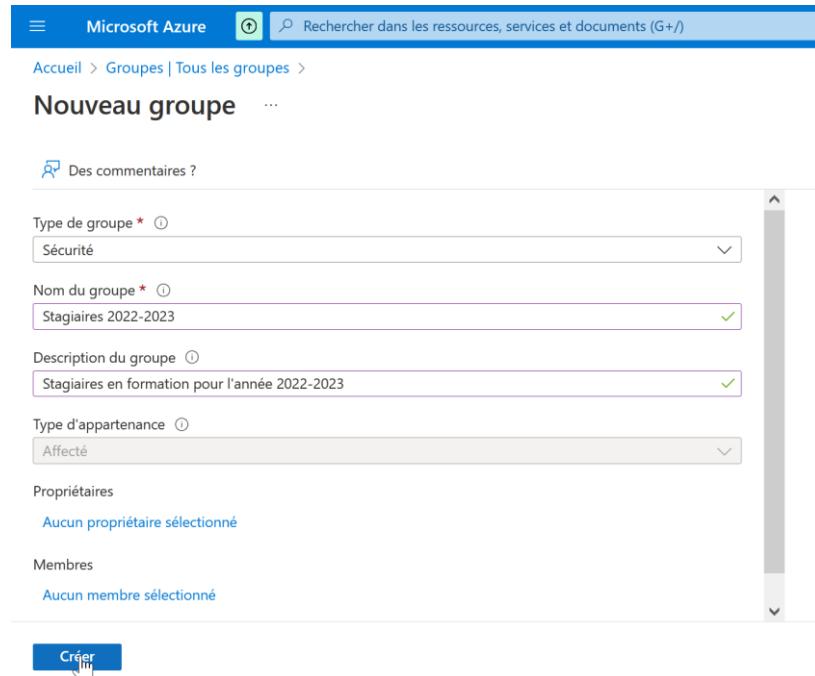
Créez un groupe depuis Azure AD

Cliquez sur « Nouveau groupe »



The screenshot shows the 'Groups | Todos los grupos' page in the Azure Active Directory. The page lists four existing groups: 'Direction', 'DO-NOT-DELETE 46216339457', 'Les Relais', and 'RH'. A 'Nouveau groupe' (New group) button is highlighted with a cursor. The page includes a search bar, filter options, and a table with columns for Nom, ID d'objet, Type de groupe, Type d'appartenance, and E-mail.

En type de groupe choisissez un groupe de « Sécurité » qui va vous permettre d'octroyer des droits par exemple sur une application. Pour avoir plus d'infos sur chaque type de groupe vous pouvez passer votre curseur sur le « i ». Entrez le nom, la description et cliquez sur « Créer ».



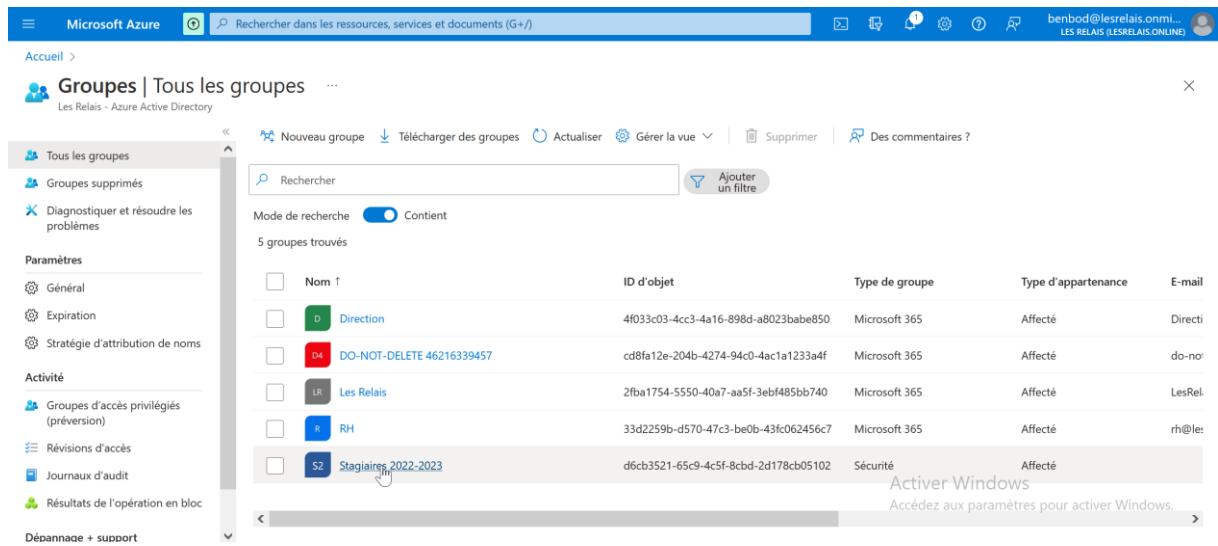
The screenshot shows the 'Nouveau groupe' (New group) creation form. The 'Type de groupe' (Group type) is set to 'Sécurité'. The 'Nom du groupe' (Group name) is 'Stagiaires 2022-2023'. The 'Description du groupe' (Group description) is 'Stagiaires en formation pour l'année 2022-2023'. The 'Type d'appartenance' (Membership type) is 'Affecté'. The 'Créer' (Create) button is highlighted with a cursor.

Ensuite prenez une capture d'écran (selon la consigne précédemment donnée) prouvant que vous avez bien accompli l'exercice.

Ajoutez un utilisateur à un groupe

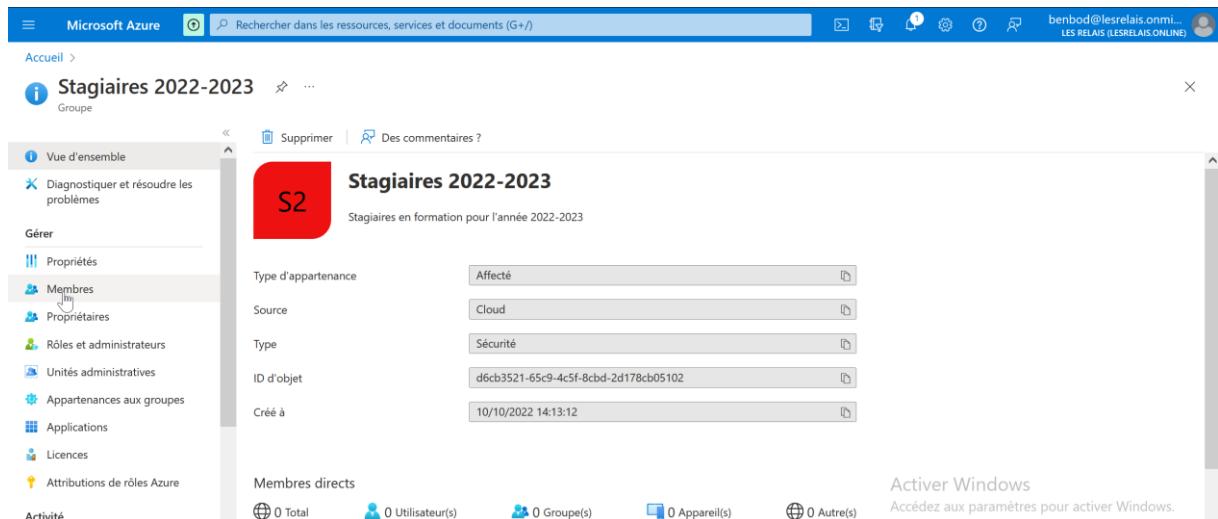


Cliquez sur le nouveau groupe créé (actualisez la page si vous ne le voyez pas arriver).



The screenshot shows the Microsoft Azure Groups page. The left sidebar shows navigation options like 'Tous les groupes', 'Groupes supprimés', and 'Diagnostiquer et résoudre les problèmes'. The main area displays a list of groups with columns for 'Nom', 'ID d'objet', 'Type de groupe', 'Type d'appartenance', and 'E-mail'. A new group, 'Stagiaires 2022-2023', is listed with an 'S2' icon. A tooltip 'Activer Windows' is visible at the bottom right.

Cliquez sur « membres » pour ajouter un ou plusieurs membres à ce groupe.



The screenshot shows the 'Stagiaires 2022-2023' group settings page. The left sidebar shows 'Membres' is selected. The main area displays group details like 'Type d'appartenance' (Affecté), 'Source' (Cloud), 'Type' (Sécurité), 'ID d'objet' (d6cb3521-65c9-4c5f-8cbd-2d178cb05102), and 'Créé à' (10/10/2022 14:13:12). Below this, 'Membres directs' are listed with a total of 0. A tooltip 'Activer Windows' is visible at the bottom right.

Cliquez sur « Ajoutez des membres » et recherchez un membre avec la barre de recherche. Cliquez sur son nom puis sur le bouton « Sélectionner ». Ensuite prenez une capture d'écran (en respectant la consigne précédemment donnée) prouvant que vous avez bien accompli l'exercice.



2.2.2 Personnalisation des portails de connexion Azure

Il est possible de personnaliser les portails web avec la marque de l'entreprise.

Configurez la marque de société

Ajoutez une image d'arrière-plan à votre portail de connexion, ainsi qu'une bannière et un texte personnalisé. Pour cela il vous faut une licence Azure AD Premium ou Microsoft 365. Vous pouvez prendre la version d'essai d'Azure AD Premium si besoin.

Plus d'infos sur : <https://learn.microsoft.com/fr-fr/azure/active-directory/fundamentals/customize-branding>

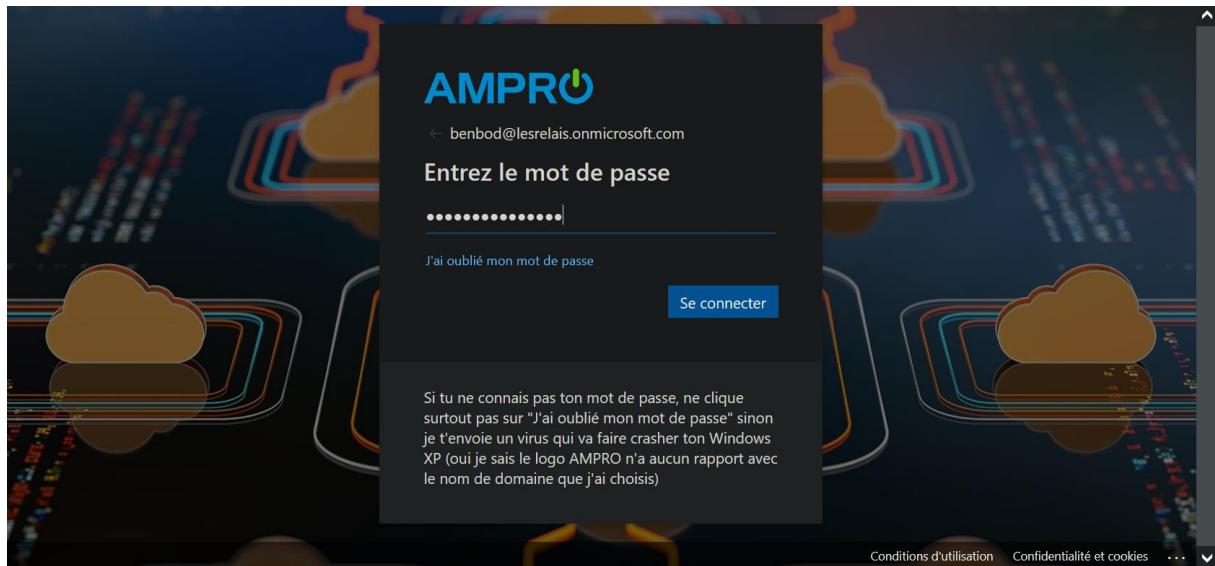


Utilisez un opérateur Google :

Téléchargez des images respectant les tailles requises en allant sur Google Image (et non pas Google) : <https://www.google.fr/imghp?hl=fr&qobl> puis en entrant un mot de votre choix suivi de l'opérateur Google permettant de rechercher une image avec une taille précise, par ex. : *computing imagesize:1920x1080*



Ensuite accédez à un portail de connexion tel que myapps.microsoft.com ou office.com qui sont des portails web qu'Azure AD va utiliser. Authentifiez-vous avec un utilisateur qui est dans votre base Azure AD et admirez votre belle page de connexion. Ensuite prenez une capture d'écran (en respectant la [consigne](#) précédemment donnée) prouvant que vous avez bien accompli l'exercice.



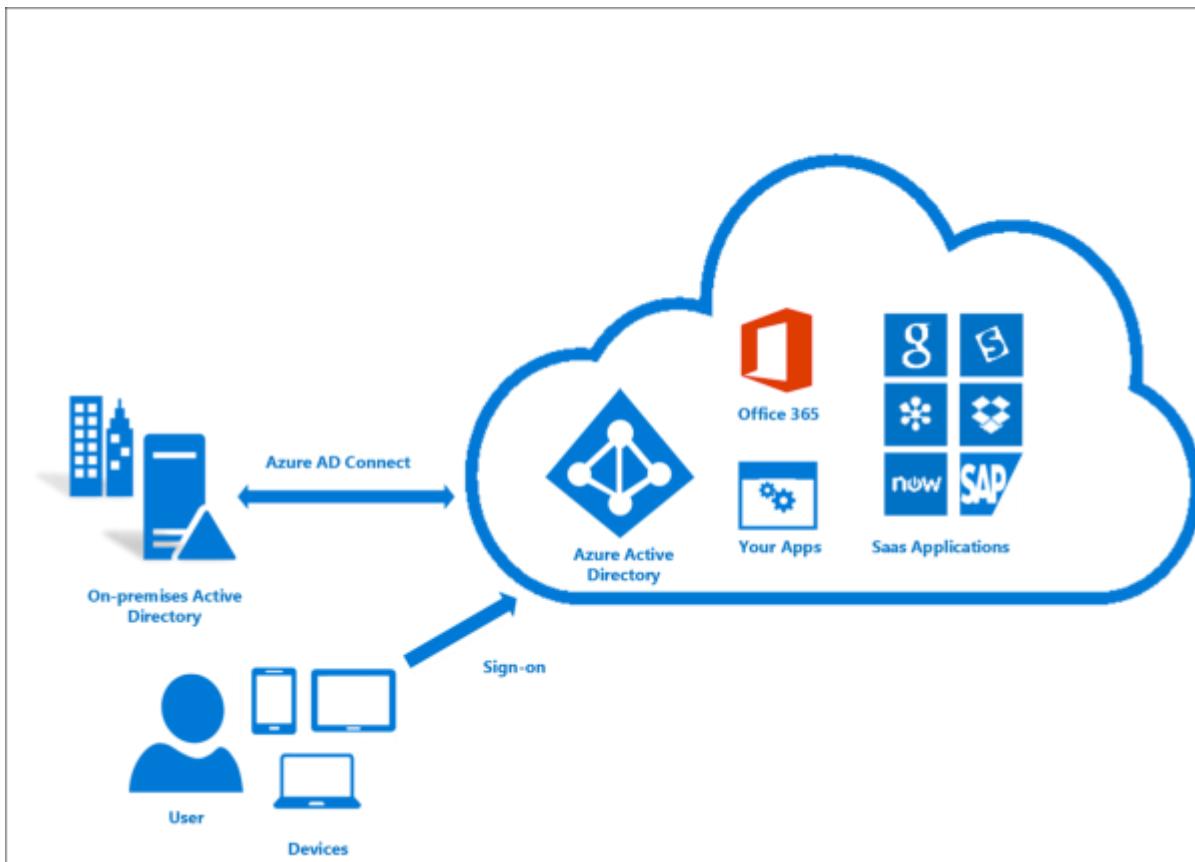
3 Découvrir Azure Active Directory Connect

Les entreprises et les organisations utilisent aujourd'hui de plus en plus souvent une combinaison d'applications locales et cloud. Les utilisateurs doivent avoir accès à ces applications en local et dans le cloud.

3.1 Introduction à Azure AD Connect



3.1.1 Qu'est-ce qu'Azure AD Connect ?



Azure AD Connect est **un outil permettant de connecter l'infrastructure d'identité locale à Microsoft Azure AD**. L'assistant déploie et configure les prérequis et les composants requis pour la connexion, y compris la planification de la synchronisation et les méthodes d'authentification. Azure AD Connect synchronise les objets locaux présents dans Active Directory avec un service Azure AD correspondant au sein d'un locataire (« *tenant* ») Microsoft 365 ou Azure.

Le logiciel Azure AD Connect Sync est le successeur de DirSync.

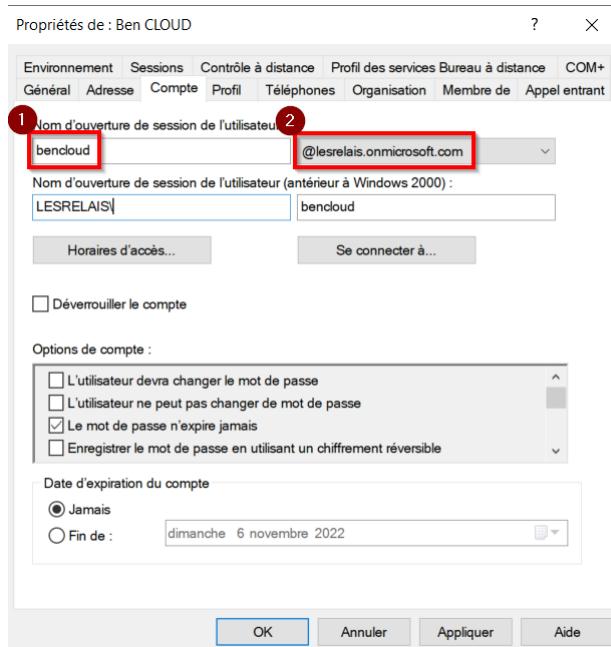
Plus d'infos sur : https://en.wikipedia.org/wiki/Azure_AD_Connect

3.1.2 Qu'est-ce qu'un UPN ?

Un UPN (User Principal Name, « nom d'utilisateur principal ») est **un attribut constituant une norme de communication Internet pour les comptes d'utilisateur**.

Un UPN se compose d'un préfixe UPN (nom de compte d'utilisateur) et d'un suffixe UPN (nom de domaine DNS). Le préfixe et le suffixe sont accolés par le symbole « @ » (prononcé « arobase » en français). Par ex. dans la capture d'écran ci-dessous « bencloud » est mon identifiant de compte et le suffixe est « @lesrelais.onmicrosoft.com »





Les pages de connexion invitent souvent les utilisateurs à entrer leur adresse e-mail alors que la valeur demandée est en réalité leur UPN.

Un UPN doit être unique parmi tous les objets principaux de sécurité d'une forêt de répertoires. Un compte utilisateur ne peut avoir qu'un seul suffixe UPN, il n'est pas possible de créer des alias comme pour une adresse e-mail.

Le suffixe par défaut est le nom de domaine de l'environnement Active Directory mais pour des raisons pratiques, il est possible d'ajouter un suffixe qui correspond par exemple au domaine de messagerie de l'entreprise, ce qui permet aux utilisateurs de s'identifier avec leur adresse e-mail.

Plus d'infos sur : <https://learn.microsoft.com/fr-fr/azure/active-directory/hybrid/howto-troubleshoot-upn-changes>

3.2 Prérequis pour synchroniser un AD local au cloud avec Azure AD Connect

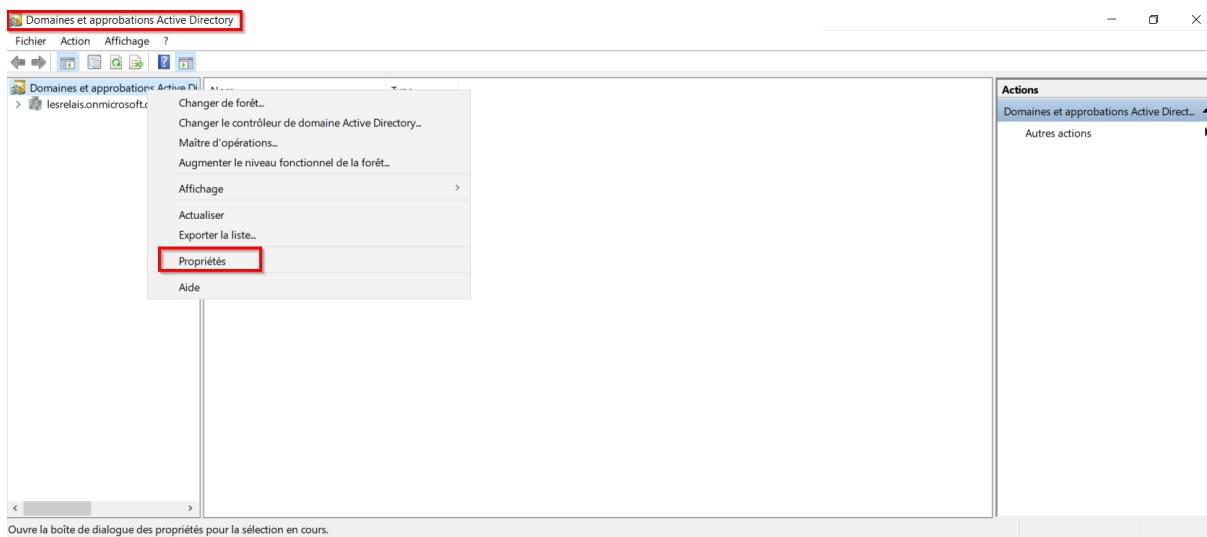
Pour la synchronisation AD local-Azure AD, il est nécessaire que l'UPN soit identique au domaine Azure AD. Moi c'est déjà le cas car j'ai mis le nom de domaine « lesrelais.onmicrosoft.com » à mon contrôleur de domaine dès le début mais si vous, vous avez choisi un nom de domaine différent il faut faire les étapes suivantes.

Pour en savoir plus sur les prérequis : <https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-prerequisites>

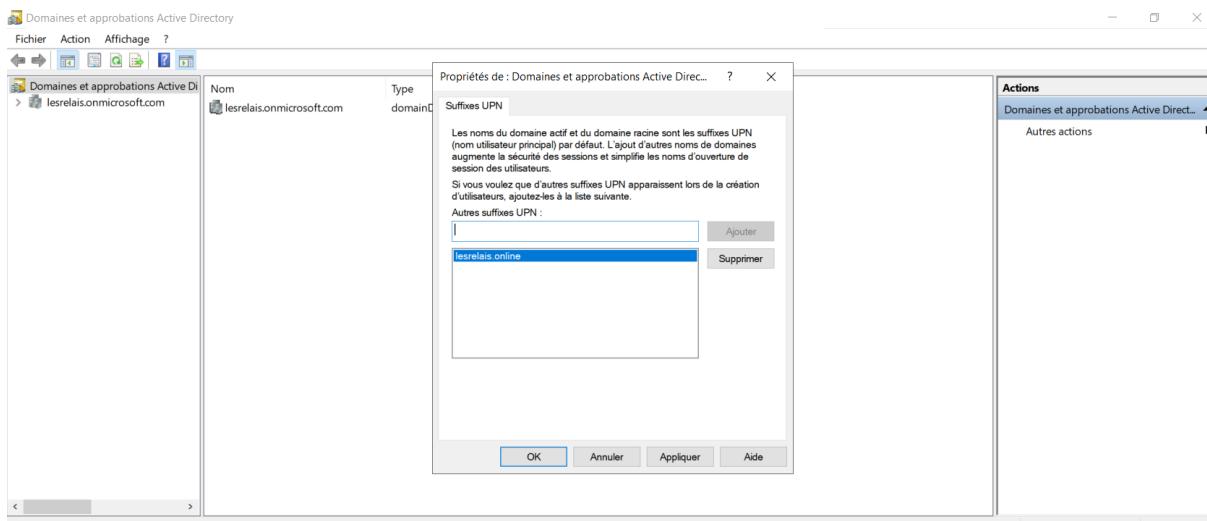
Ajoutez un suffixe UPN à votre Active Directory

Allez dans « Domaines et approbations Active Directory ».





Puis ajoutez le suffixe UPN obtenu lors de la création de votre compte Azure et qui ressemble à « monentreprise.onmicrosoft.com » (moi pour l'exemple dans la capture ci-dessous j'ai ajouté « lesrelais.online »). Ensuite prenez une capture d'écran (en respectant la consigne précédemment donnée) prouvant que vous avez bien accompli l'exercice.



UTILE

Attention :

Le fait d'ajouter un suffixe d'UPN ne le configure pas sur les utilisateurs. Pour changer le suffixe UPN d'un utilisateur il faut le faire sur l'utilisateur en question.

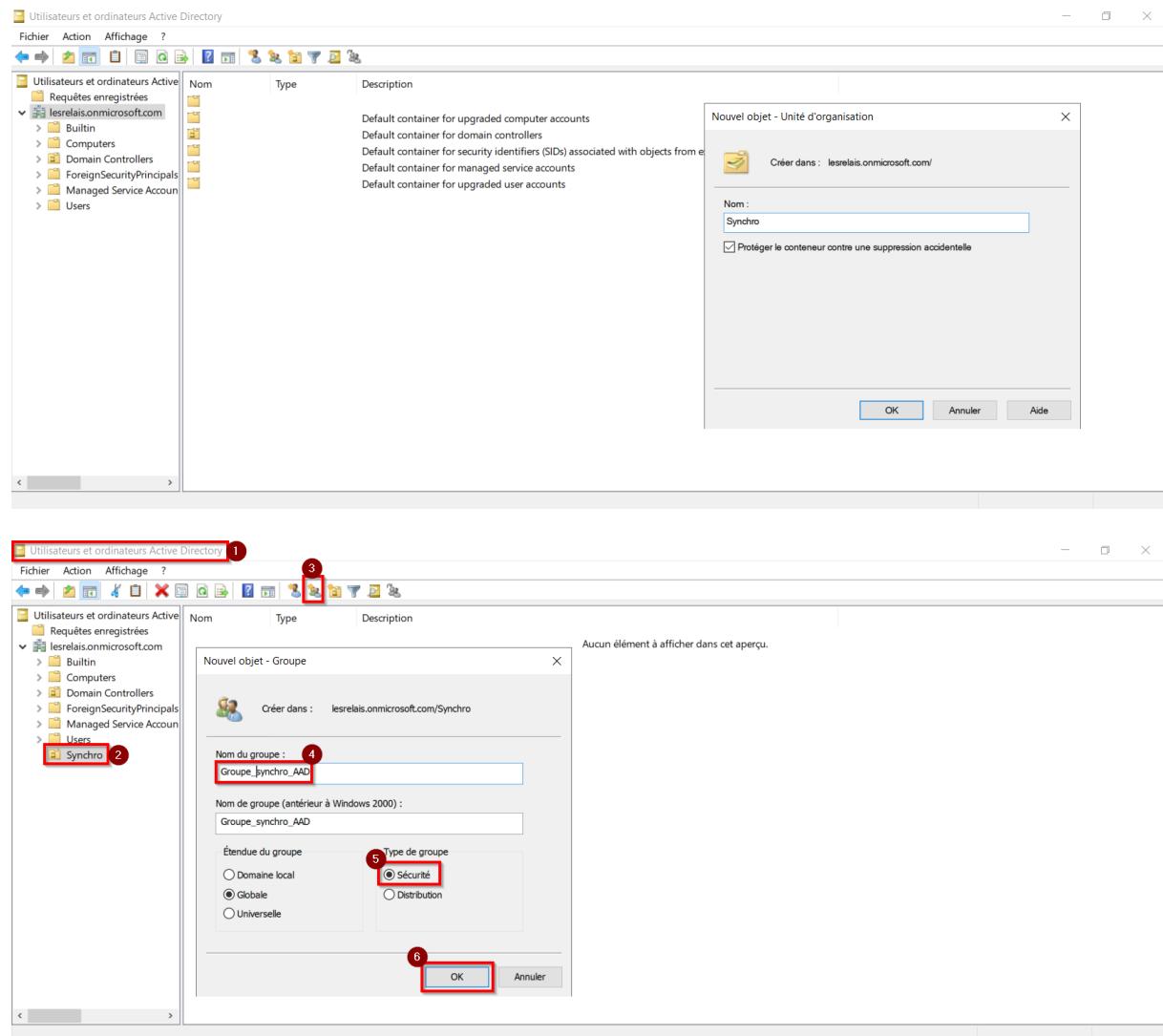
Maîtrisez votre synchronisation

Ensuite je vais créer une nouvelle OU (Unité d'Organisation) puis y créer un groupe. Tout simplement car je veux filtrer les éléments à synchroniser (= je ne veux pas synchroniser l'ensemble de mon annuaire Active Directory).



Je vais donc mettre dans ce groupe les utilisateurs, les groupes et les ordinateurs que je veux synchroniser. Puis je dirais à l'outil Azure AD Connect : « Si l'objet est membre du groupe alors synchronise-le ».

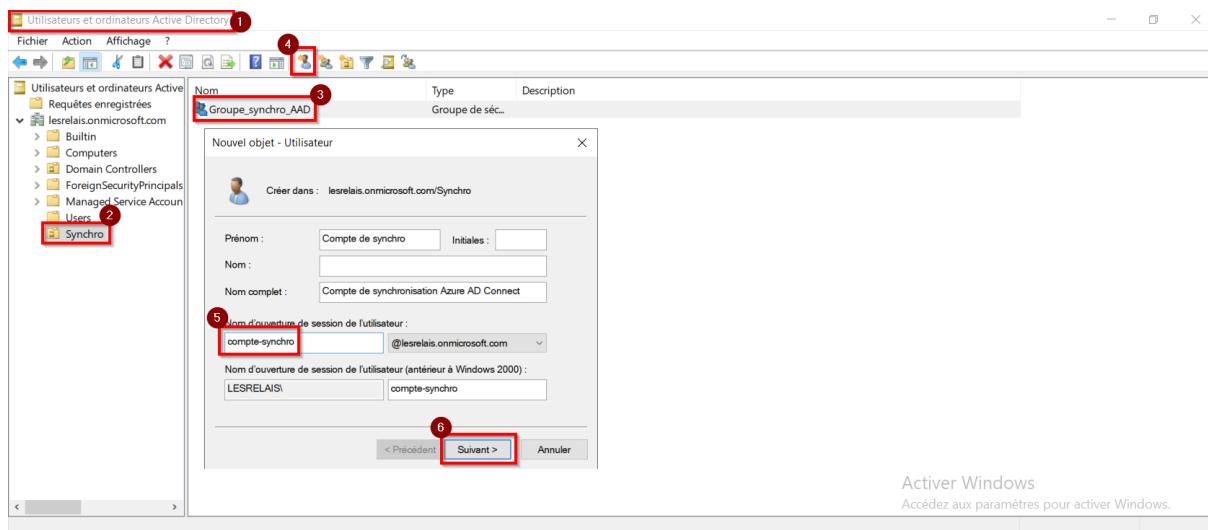
Pour faire cela ça vous devrez aller dans « Utilisateurs et ordinateurs Active Directory » et suivre les étapes ci-dessous. Ensuite prenez une capture d'écran (en respectant la [consigne](#) précédemment donnée) prouvant que vous avez bien accompli l'exercice.



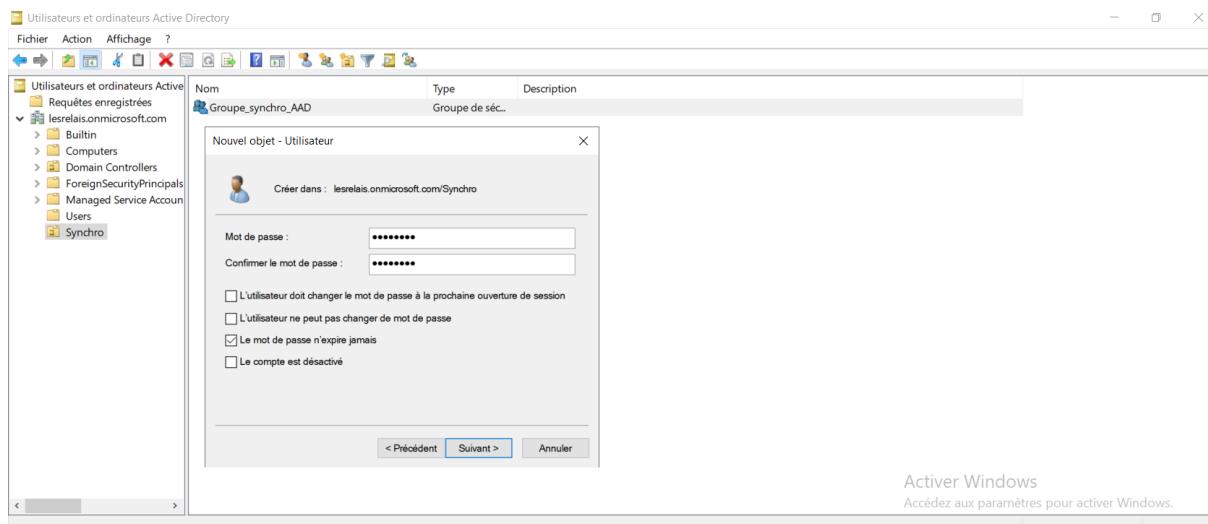
Créez un compte de service qui sera utilisé par l'outil Azure AD Connect

Suivez les étapes ci-dessous pour créer un compte utilisateur de service qui sera utilisé par l'outil Azure AD Connect pour se connecter à Azure AD.



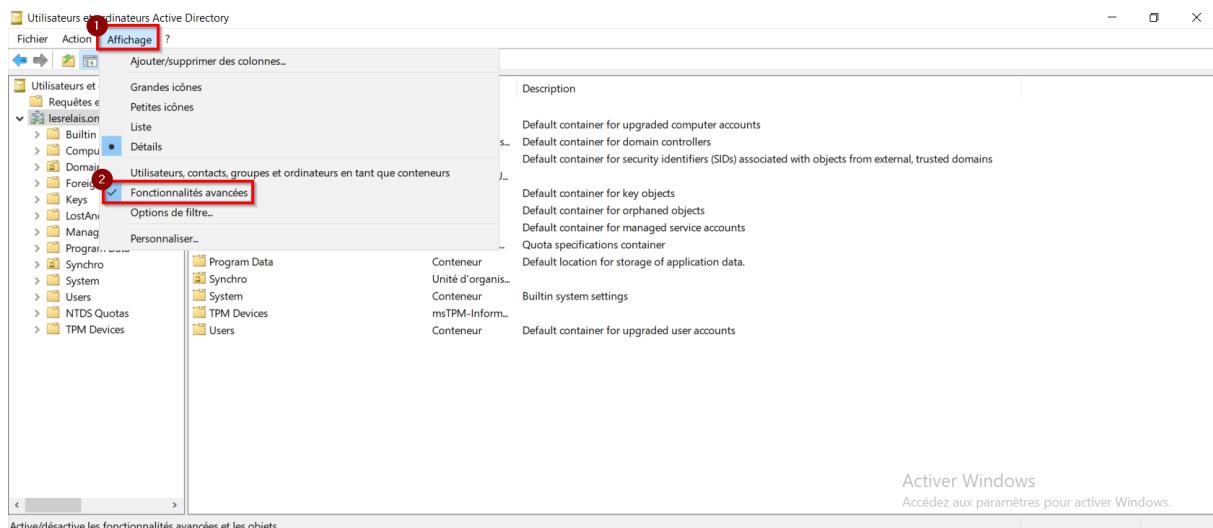


Ce compte n'a pas besoin d'avoir le suffixe UPN de votre Azure AD (= vous pouvez lui mettre le suffixe par défaut de l'AD local qui est peut-être chez vous « monorganisation.local » ou « tp-azure.lab »). Cochez évidemment la case « Le mot de passe n'expire jamais » sinon le mot de passe expirera (après X jours selon la politique de sécurité mise en place) et il faudra reconfigurer l'outil régulièrement. Vous pouvez le nommer comme bon vous semble mais c'est une bonne chose de le nommer de manière à ce qu'il ne soit jamais supprimé par erreur comme par ex. « ne-pas-supprimer-AADC ».

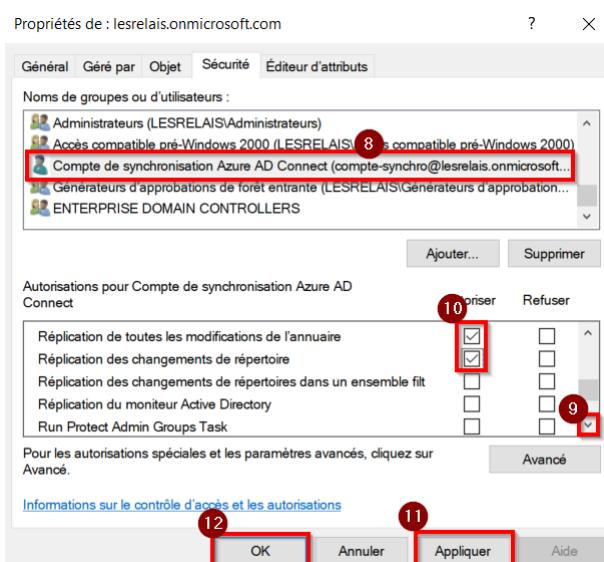
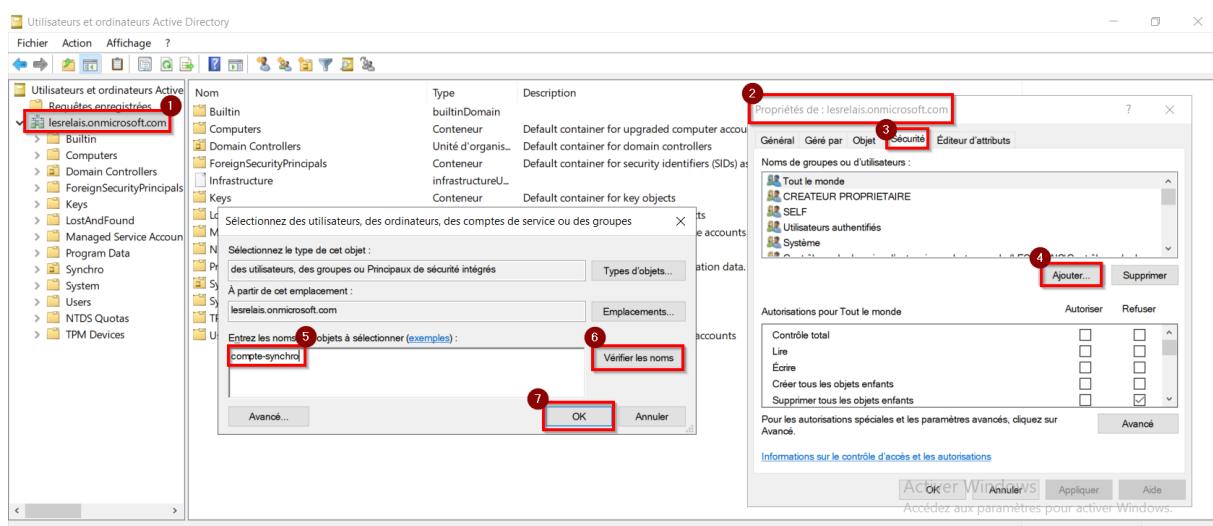


Il n'a pas besoin non plus d'avoir des droits d'administration. Il faudra néanmoins lui attribuer des droits spécifiques à la raison de sa création : les droits de réplication. Pour cela il faut tout d'abord activer l'affichage des fonctionnalités avancées pour déverrouiller plus d'options de paramétrage.





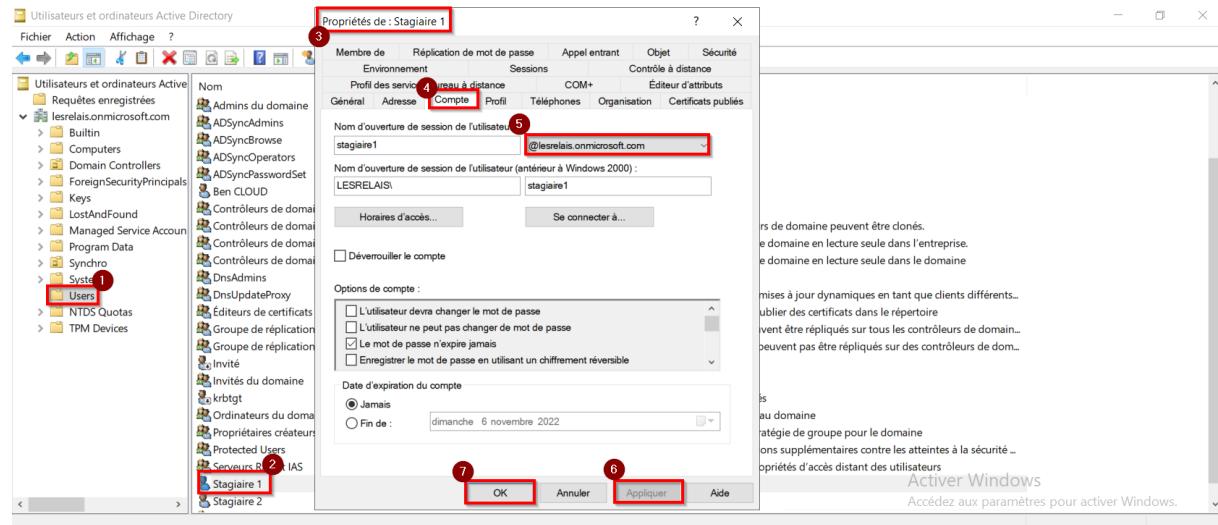
Puis on va se rendre dans les propriétés de la racine de notre domaine, puis dans l'onglet « Sécurité » on va ajouter l'utilisateur créé précédemment et lui attribuer les droits de réplication.



Une fois cela fait, prenez une capture d'écran (en respectant la [consigne](#) précédemment donnée) prouvant que vous avez bien accompli l'exercice.

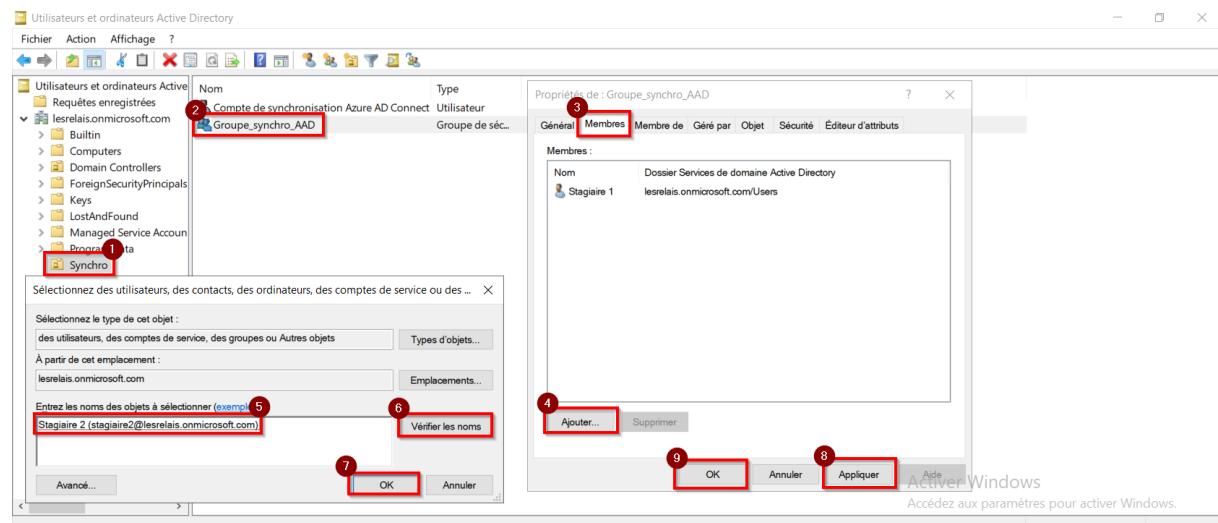
Changez l'UPN des utilisateurs à synchroniser

Pour la suite vous pouvez créer de nouveaux utilisateurs dans votre AD local ou utiliser ceux créés précédemment mais il va falloir changer leur suffixe d'UPN par celui du cloud Azure. Faites cela puis prenez une capture d'écran (en respectant la [consigne](#) précédemment donnée).



Intégrez vos utilisateurs à synchroniser dans votre groupe de synchro

Intégrez vos utilisateurs à synchroniser dans votre groupe de synchro. Ensuite prenez une capture d'écran (en respectant la [consigne](#) précédemment donnée) prouvant que vous avez bien accompli l'exercice.



Installez l'outil Azure AD Connect

Téléchargez l'outil Azure AD Connect via ce lien :



<https://www.microsoft.com/en-us/download/details.aspx?id=47594>

Installez-le sur votre serveur puis lancez-le une fois l'installation terminée.

3.3 La synchronisation avec Azure AD Connect

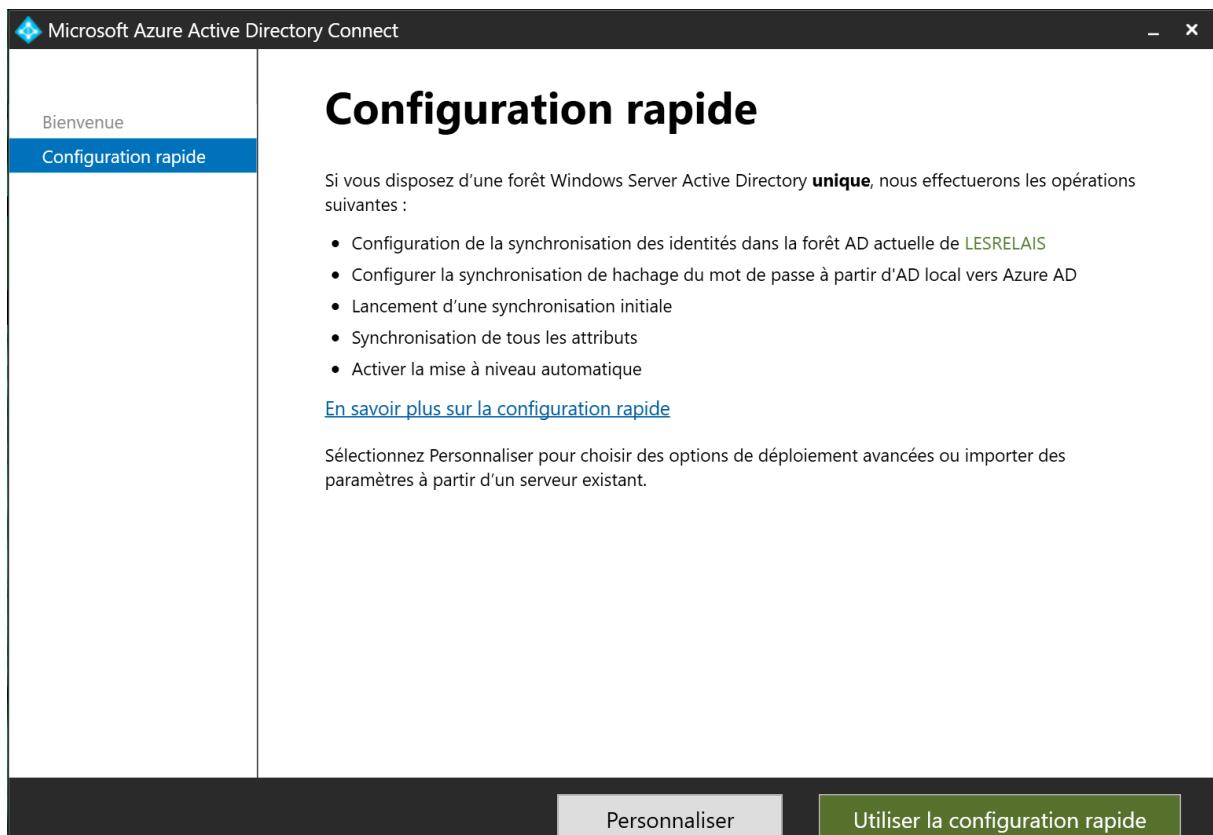
Vous allez lancer la synchronisation avec Azure AD Connect.



Tutoriels d'installation :

<https://www.it-connect.fr/installation-et-configuration-dazure-ad-connect/> et
<https://learn.microsoft.com/fr-fr/azure/active-directory/hybrid/how-to-connect-install-roadmap>
(puis regardez les autres chapitres dans le sommaire sur la gauche)

Choisissez l'installation personnalisée plutôt que la configuration rapide.



Ensuite ne cochez aucune case et cliquez sur « Installer ».

Pour la partie « Connexion utilisateur », choisissez « Synchronisation de hachage de mot de passe ». Grâce à cette option, l'utilisateur pourra se connecter au cloud grâce au même mot de passe que dans l'Active Directory local.



Microsoft Azure Active Directory Connect

Connexion utilisateur

Sélectionnez la méthode d'authentification. [?](#)

Synchronisation de hachage du mot de passe [?](#)

Authentification directe [?](#)

Fédération avec AD FS [?](#)

Fédération avec PingFederate [?](#)

Ne pas configurer [?](#)

Sélectionnez cette option pour activer l'authentification unique pour les utilisateurs d'ordinateurs de bureau d'entreprise :

Activer l'authentification unique [?](#)

Précédent Suivant

Pour l'étape « Connexion à Azure AD », vous devez vous authentifier avec le compte qui est administrateur général de votre *tenant*.

Microsoft Azure Active Directory Connect

Connexion à Azure AD

Entrez vos informations d'identification Azure AD d'administrateur général ou d'administrateur d'identité hybride. [?](#)

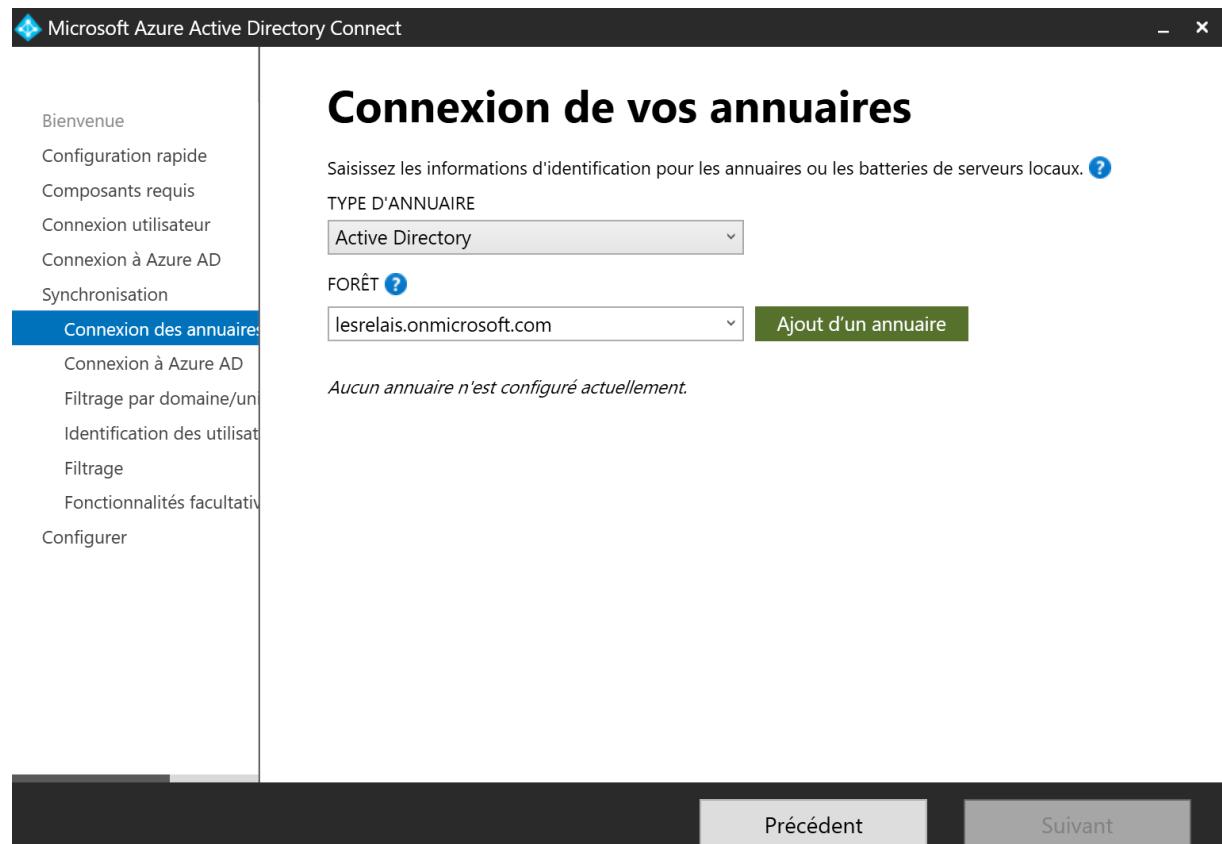
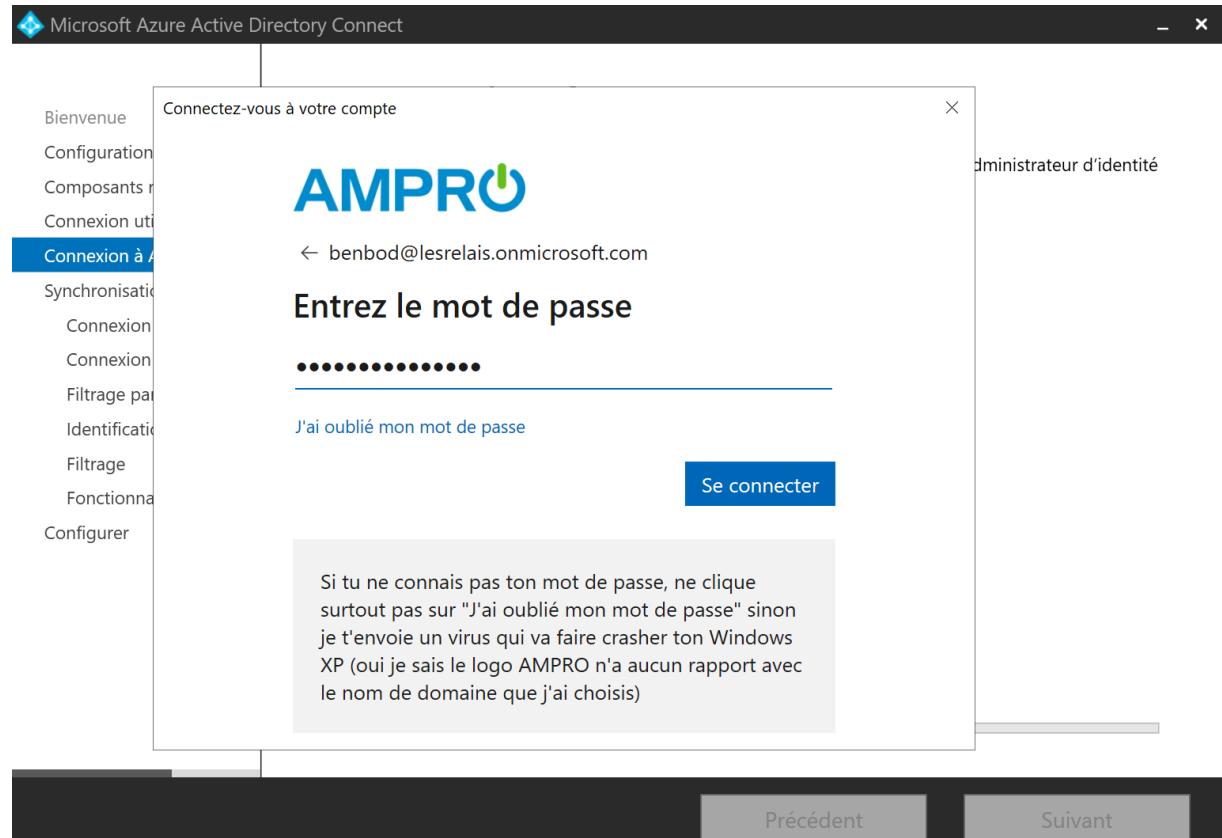
NOM D'UTILISATEUR

MOT DE PASSE

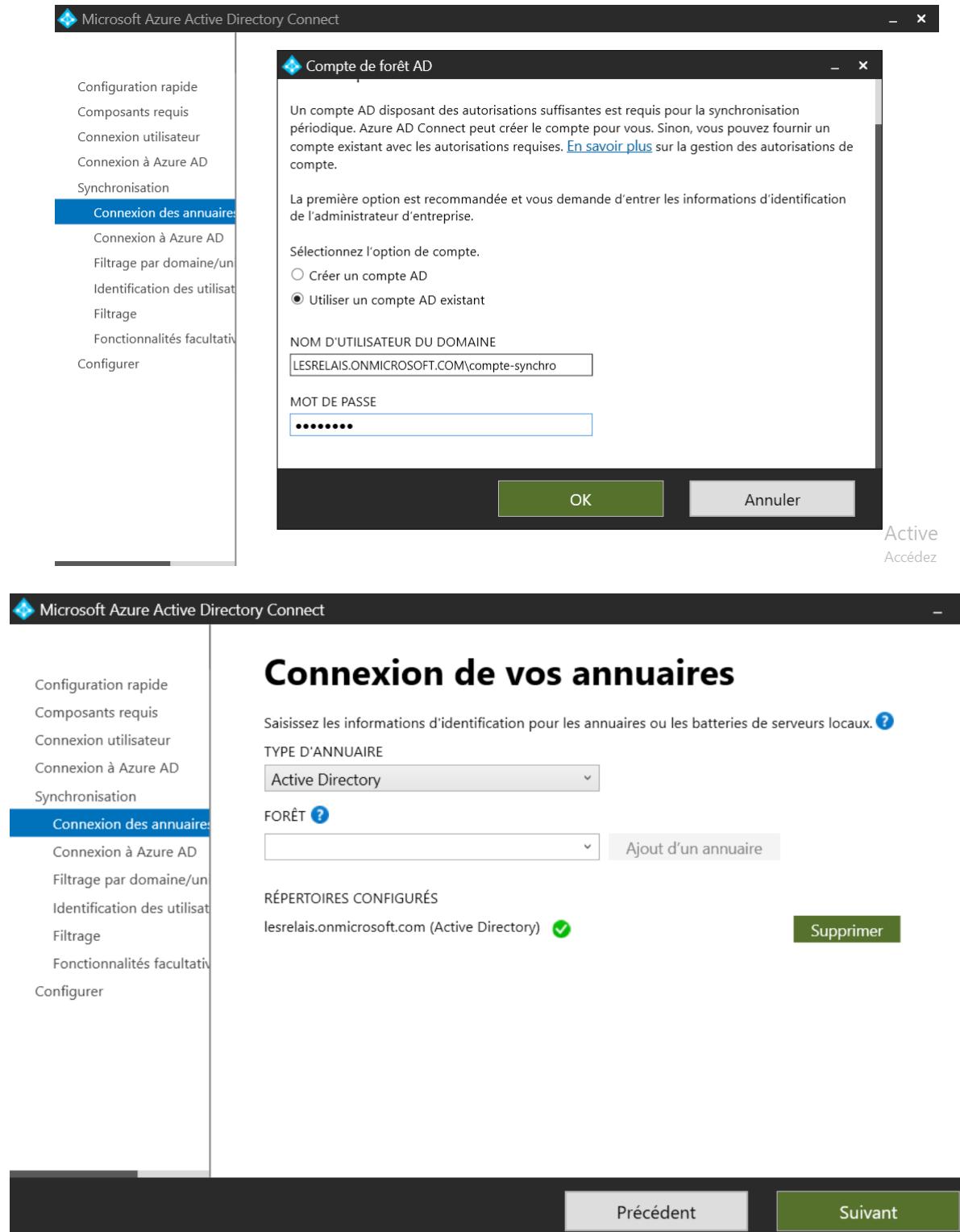
Précédent Suivant



Un portail de connexion s'ouvre, il faudra retaper le mot de passe (et entrer le code MFA si configuré).



A cette étape il faut renseigner le compte de service spécialement créé pour la synchronisation, le mien est « compte-synchro ».



Jusqu'ici tout va bien, je clique sur « Suivant ». Je coche ensuite la petite case « Continuer sans faire correspondre tous les suffixes à des domaines vérifiés » et je clique sur « Suivant ».



Microsoft Azure Active Directory Connect

Configuration de la connexion à Azure AD

Pour se connecter à Azure avec les mêmes informations d'identification que votre annuaire local, un domaine Azure AD correspondant est requis. Le tableau suivant liste les suffixes UPN de votre environnement local et l'état du domaine AD Azure associé. [?](#)

Suffixe UPN Active Directory	Domaine Azure AD
lesrelais.onmicrosoft.com	Non ajouté ?
lesrelais.online	Non ajouté ?

Sélectionnez l'attribut local à utiliser comme nom d'utilisateur Azure AD

NOM D'UTILISATEUR PRINCIPAL [?](#)

userPrincipalName

Continuer sans faire correspondre tous les suffixes UPN à des domaines vérifiés

Les utilisateurs ne pourront pas se connecter à Azure AD à l'aide d'informations d'identification locales si le suffixe UPN ne correspond pas à un domaine vérifié. [En savoir plus](#)

Précédent Suivant

Microsoft Azure Active Directory Connect

Filtrage par domaine ou unité d'organisation

Annuaire : Actualiser les domaines [?](#)

Synchroniser tous les domaines et toutes les unités d'organisation

Synchroniser les domaines et les unités d'organisation sélectionnés

lesrelais.onmicrosoft.com

Précédent Suivant



Microsoft Azure Active Directory Connect

Identification de manière unique de vos utilisateurs

Sélectionnez la manière dont les utilisateurs doivent être identifiés dans vos annuaires locaux. [?](#)

Les utilisateurs ne sont représentés qu'une fois sur tous les annuaires.

Les identités utilisateurs existent sur plusieurs annuaires. Correspondance à l'aide de :

- Attribut de messagerie
- Attributs ObjectSID et msExchMasterAccountSID/msRTCSIP-OriginatorSID
- Attributs SAMAccountName et MailNickName
- Un attribut spécifique

Sélectionnez la manière dont les utilisateurs doivent être identifiés auprès d'Azure AD. [?](#)

Laisser Azure gérer l'ancre source

Choisir un attribut spécifique

Azure réécrira les ancrées sources uniques dans votre annuaire local si mS-DS-ConsistencyGuid n'est pas actuellement utilisé par votre organisation. [En savoir plus](#)

Précédent **Suivant**

Ensuite au niveau du filtrage, on va préciser qu'on ne veut synchroniser que le groupe « Groupe_synchro_AAD » selon notre volonté de ne pas synchroniser tous les objets de l'annuaire.

Microsoft Azure Active Directory Connect

Filtrer les utilisateurs et appareils

Pour un déploiement pilote, spécifiez un groupe contenant les utilisateurs et appareils à synchroniser. Les groupes imbriqués ne sont pas pris en charge et sont ignorés.

Synchroniser tous les utilisateurs et les appareils

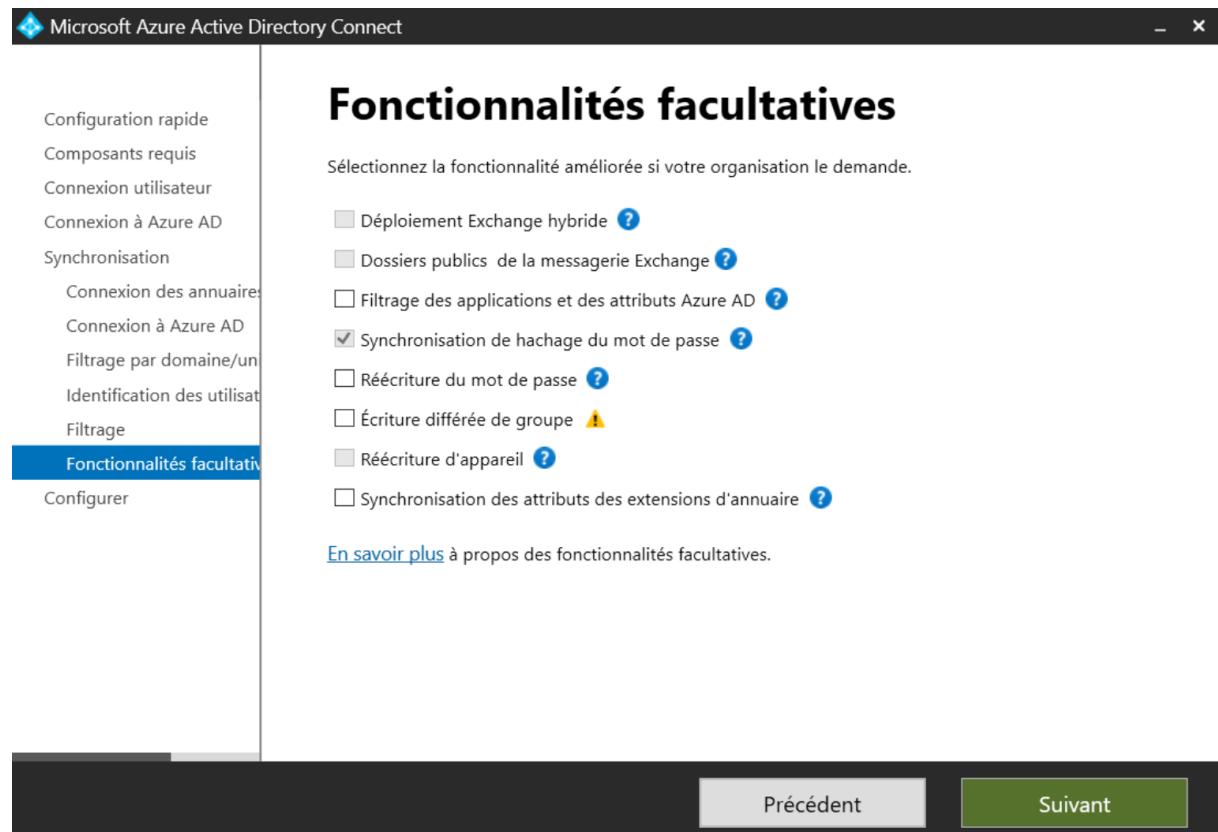
Synchronisation choisie [?](#)

FORÊT	GROUPE
esrelais.onmicrosoft.com	<input type="text" value="Groupe_synchro_AAD"/> Résolution

Précédent **Suivant**



Je peux choisir ici d'activer des fonctionnalités facultatives comme par exemple la réécriture du mot de passe. Je clique sur « Suivant ».



Microsoft Azure Active Directory Connect

Fonctionnalités facultatives

Sélectionnez la fonctionnalité améliorée si votre organisation le demande.

Déploiement Exchange hybride ?

Dossiers publics de la messagerie Exchange ?

Synchronisation de hachage du mot de passe ?

Réécriture du mot de passe ?

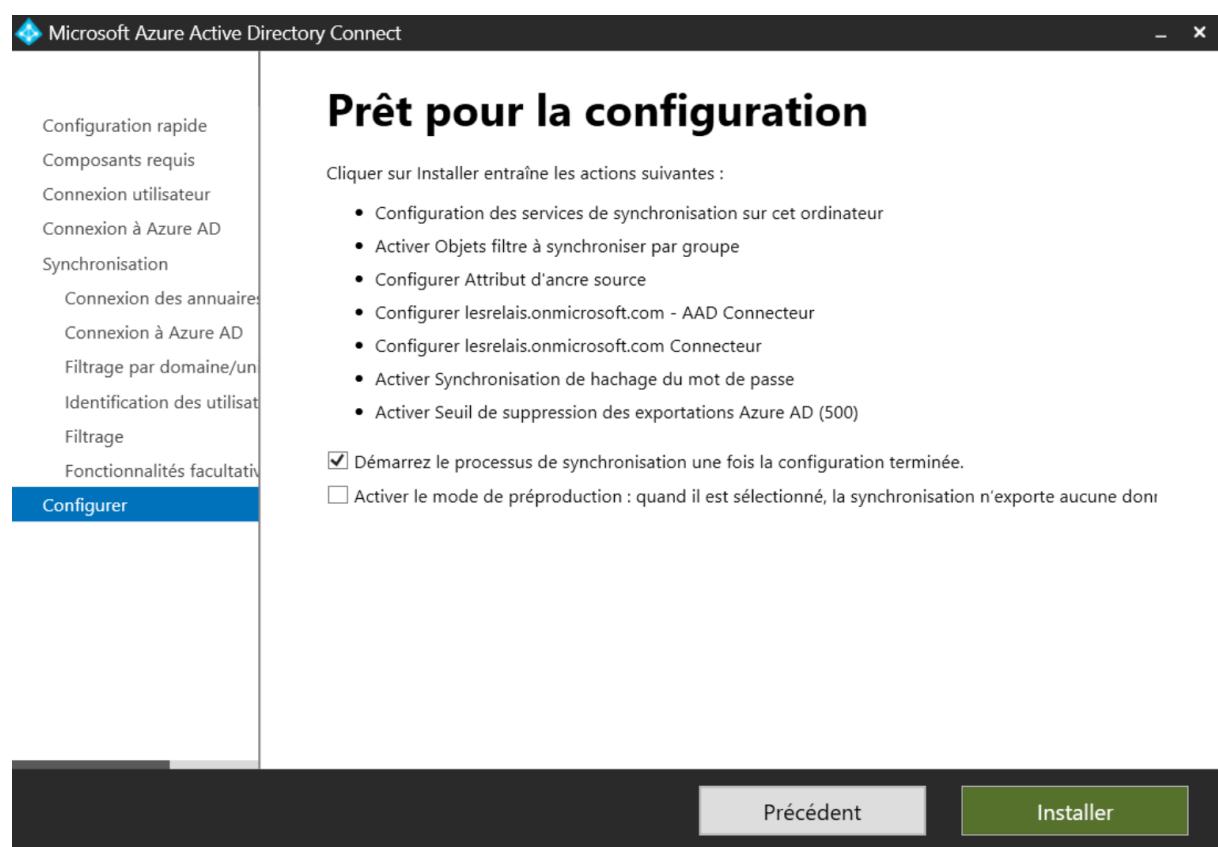
Écriture différée de groupe ⚠

Réécriture d'appareil ?

Synchronisation des attributs des extensions d'annuaire ?

[En savoir plus](#) à propos des fonctionnalités facultatives.

Précédent Suivant



Microsoft Azure Active Directory Connect

Prêt pour la configuration

Cliquez sur Installer entraîne les actions suivantes :

- Configuration des services de synchronisation sur cet ordinateur
- Activer Objets filtre à synchroniser par groupe
- Configurer Attribut d'ancêtre source
- Configurer lesrelais.onmicrosoft.com - AAD Connecteur
- Configurer lesrelais.onmicrosoft.com Connecteur
- Activer Synchronisation de hachage du mot de passe
- Activer Seuil de suppression des exportations Azure AD (500)

Démarrez le processus de synchronisation une fois la configuration terminée.

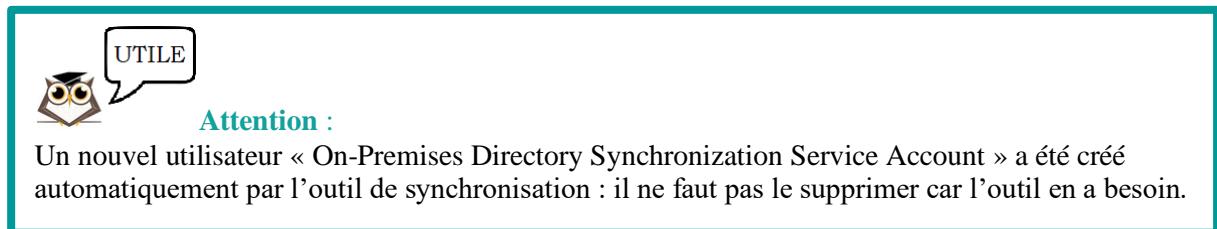
Activer le mode de préproduction : quand il est sélectionné, la synchronisation n'exporte aucune don

Précédent Installer



Je clique sur « Installer ».

Si je vérifie mes utilisateurs dans Azure AD avant la fin de l'installation et je constate que mes utilisateurs de l'AD local ne sont pas présents.



Nom d'affichage	Nom d'utilisateur principal	Type d'utilisateur	Synchronisatio...	Identités	Nom de l'entreprise
AC Accueil	accueil@lesrelais.onmicro...	Membre	Non	lesrelais.onmicrosoft.com	
AZ azurereadconnect	azurereadconnect@lesrelais...	Membre	Non	lesrelais.onmicrosoft.com	
BB Ben Bod	benbod@lesrelais.onm...	Membre	Non	lesrelais.onmicrosoft.com	
BL Bob LEPONGE	bob.lepong@lesrelais.on...	Membre	Non	lesrelais.onmicrosoft.com	
HP Helga PATAKI	helga.pataki@lesrelais.on...	Membre	Non	lesrelais.onmicrosoft.com	
LA Les Relais	contact@lesrelais.onm...	Membre	Non	lesrelais.onmicrosoft.com	
OD On-Premises Directory Syncro...	Synt_WIN-FNUAUHBV81T...	Membre	Oui	lesrelais.onmicrosoft.com	
TE test1	test1@lesrelais.onmicrosoft...	Membre	Non	lesrelais.onmicrosoft.com	Activez Windows
TE test2	test2@lesrelais.onmicrosoft...	Membre	Non	lesrelais.onmicrosoft.com	Accédez aux paramètres pour activer Windows.

J'attends la fin de l'installation...

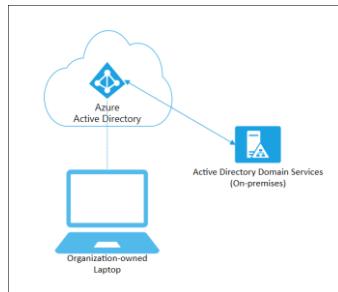


Je réactualise ma page de navigateur sur Azure AD et je constate que les utilisateurs que j'ai voulu synchroniser (et seulement eux) sont bien là désormais ! Je peux facilement les différencier des autres utilisateurs créés depuis le cloud par le « Oui » dans la colonne « Synchronisation locale activée ».

Prenez des captures d'écran (en respectant la consigne précédemment donnée) prouvant que vous avez bien accompli l'exercice.

3.4 La jonction des machines à Azure AD





Tous les appareils Windows 11 et Windows 10 sauf les éditions Famille peuvent être joints à un annuaire Azure Active Directory.

Les administrateurs peuvent utiliser la jonction à Azure AD pour sécuriser et mieux contrôler les appareils joints à l'aide d'outils de gestion des périphériques mobiles (MDM, « Mobile Device Management »), tels que Microsoft Intune ou dans des scénarios de cogestion à l'aide de Microsoft Endpoint Configuration Manager.

Ces outils offrent un moyen d'appliquer les configurations requises par l'organisation, comme :

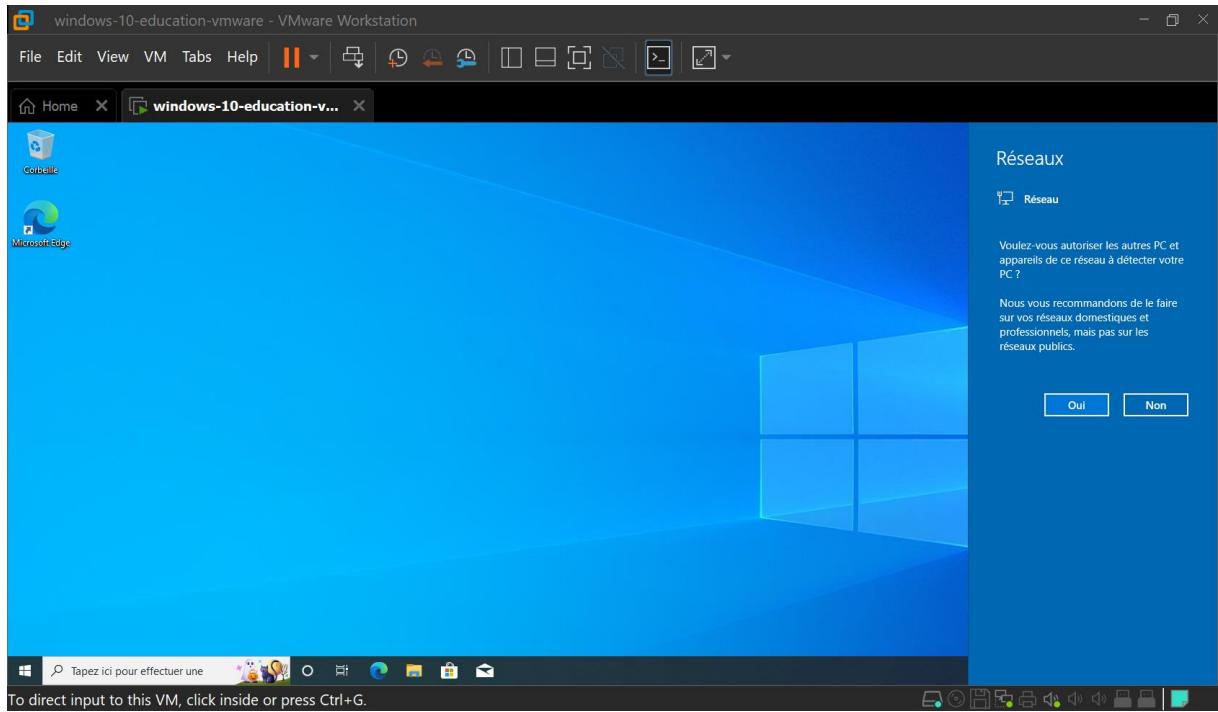
- Exiger le chiffrement du stockage
- Complexité du mot de passe
- Installation de logiciels
- Mises à jour logicielles

Plus d'infos sur Azure AD Join : <https://learn.microsoft.com/fr-fr/azure/active-directory/devices/concept-azure-ad-join>

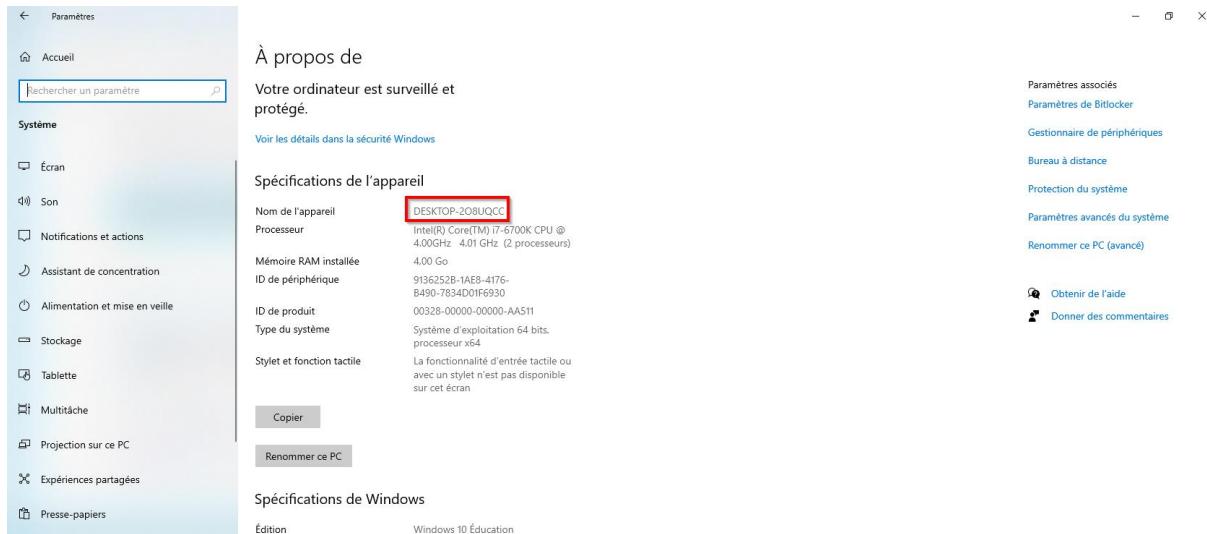
3.4.1 Joindre une machine Windows 10 à Azure AD

Nous allons joindre une machine Windows 10 Education à notre annuaire Azure Active Directory. Pour cela créez une nouvelle VM avec votre hyperviseur VMware. Choisir l'ISO de la version Education vous permettra d'éviter des étapes de configuration lors de l'installation de Windows (= ça va plus vite et ça demande moins d'interactions). Une fois la machine créée vous arrivez sur le bureau Windows :



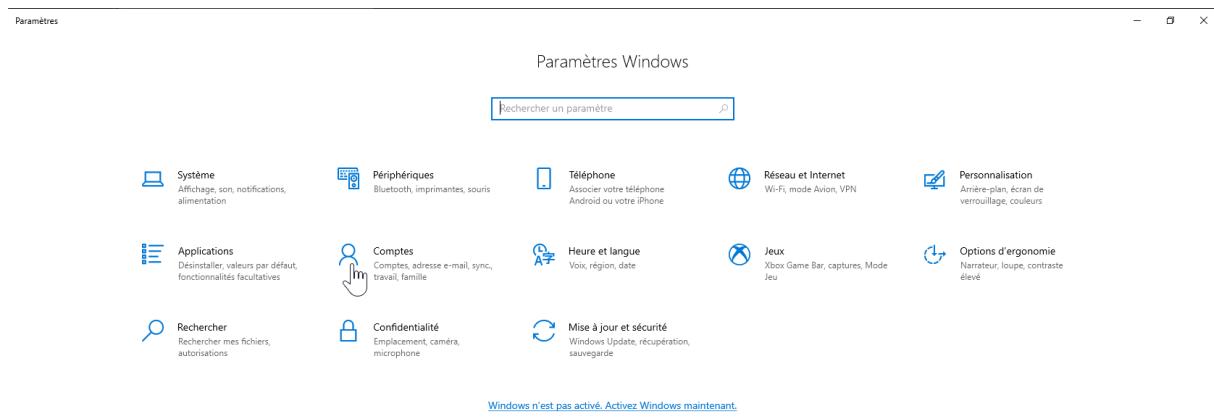


Vous pouvez regarder le nom de votre machine attribué automatiquement lors de l'installation de Windows 10 Education. Ma machine s'appelle « DESKTOP-2O8UQCC ».

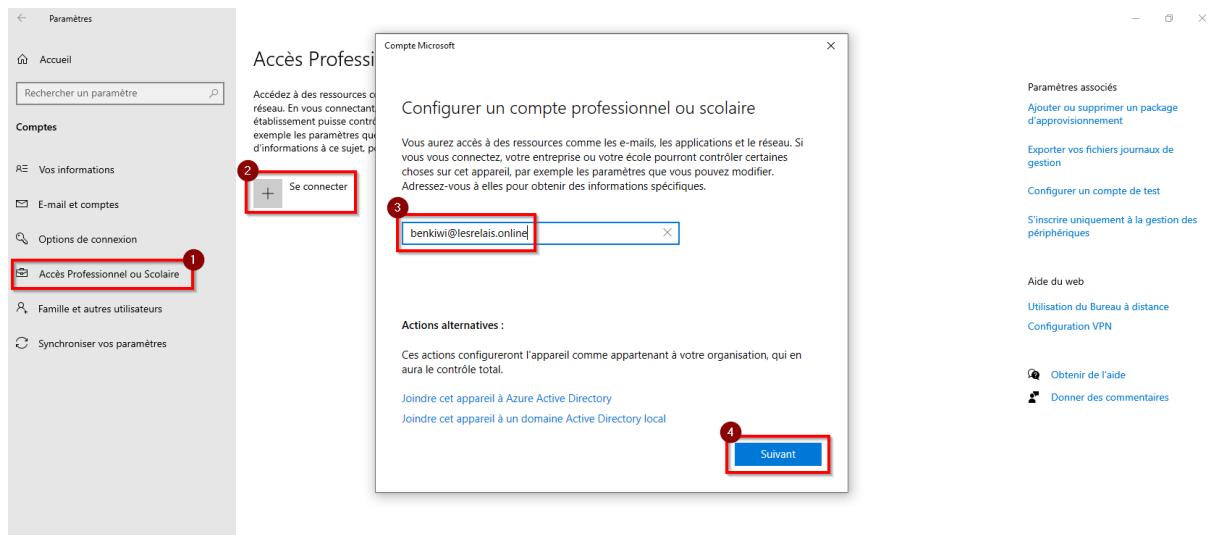


Ensuite ouvrez les paramètres de Windows et cliquez sur « Comptes » :



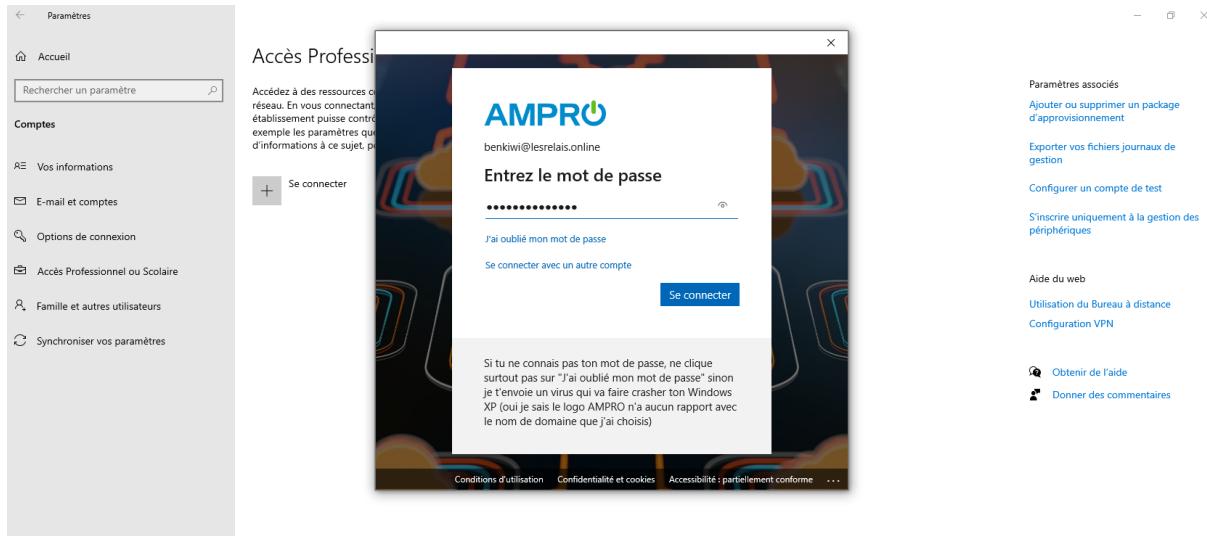


Puis sur « Accès Professionnel ou Scolaire » puis « Se connecter ». Entrez le compte utilisateur Azure Active Directory de la personne qui est censée utiliser ce poste puis cliquez sur « Suivant ».

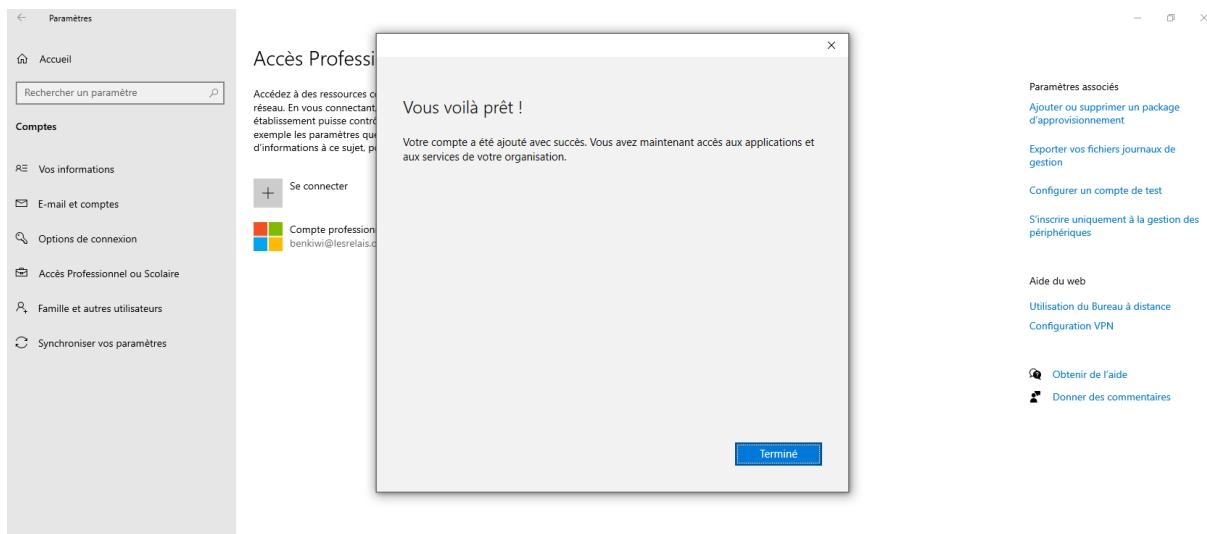


Une fenêtre s'ouvre sur le portail de connexion de votre entreprise, entrez le mot de passe puis cliquez sur « Se connecter ».





Patientez un peu et vous obtiendrez ce message :



On voit désormais que la machine est jointe à Azure AD avec le compte utilisateur benkiwi@lesrelais.online .

Maintenant retournez sur Azure AD avec votre compte administrateur et vérifiez que la machine est bien jointe au domaine. Pour cela retrouvez l'utilisateur et cliquez sur « Appareils »



Vous souhaitez revenir à l'expérience de liste des appareils hérités ? Cliquez ici pour désactiver la préversion, puis actualisez votre navigateur. Vous devrez peut-être le désactiver une seconde fois.

Nom	Activé	Système d'e...	Version	Type de connexion	GPM	Conforme	Inscrit	Activité
DESKTOP-208UQCC	Oui	Windows	10.0.19045.2006	Azure AD registered	None	N/A	31/10/2022 12:25	31/10/2022 12:25

Vous constatez que la machine « DESKTOP- 208UQCC » est bien présente. En cliquant dessus vous avez accès à certaines informations et actions possibles.

Propriétés	Nom	DESKTOP-208UQCC
Rôles et administrateurs (préversion)	ID de l'appareil	a561d662-6312-4712-866b-e59038f24c5
Unités administratives (préversion)	ID de l'objet	1eb68926-7c9d-4ae3-8d4a-fb07b5277506
Activé	Actif	Oui
Système d'exploitation	Windows	
Version	10.0.19045.2006	
Type de connexion	Azure AD registered	
Propriétaire	Ben KIWI	
Nom d'utilisateur principal	benkwi@lesrelais.online	
GPM	Aucun	
Conforme	N/A	
Inscrit	31/10/2022 12:25:18	
Activité	31/10/2022 12:25:18	
Groupes	Aucun	

Prenez des captures d'écran (en respectant la consigne précédemment donnée) prouvant que vous avez bien accompli l'exercice.

