
Mise en place ADSync

Introduction

ADSync va nous permettre de synchroniser les objets Active Directory « On Premise » vers notre tenant Azure

Dans notre cas pcs.local vers premium-computer.fr

Installation

Alias UPN

Il faut configurer un suffixe UPN en l'occurrence ici premium-computer.fr sur notre AD dans la documentation d'échange accessible sur mon site nous avons déjà observé comment l'installer.

Installation Azure AD connect

Il faut se rendre sur ce lien <https://www.microsoft.com/en-us/download/details.aspx?id=47594>

Azure AD Connect V2

Azure AD Connect allows you to quickly onboard to Azure AD and Office 365

Important! Selecting a language below will dynamically change the complete page content to that language.

Select language

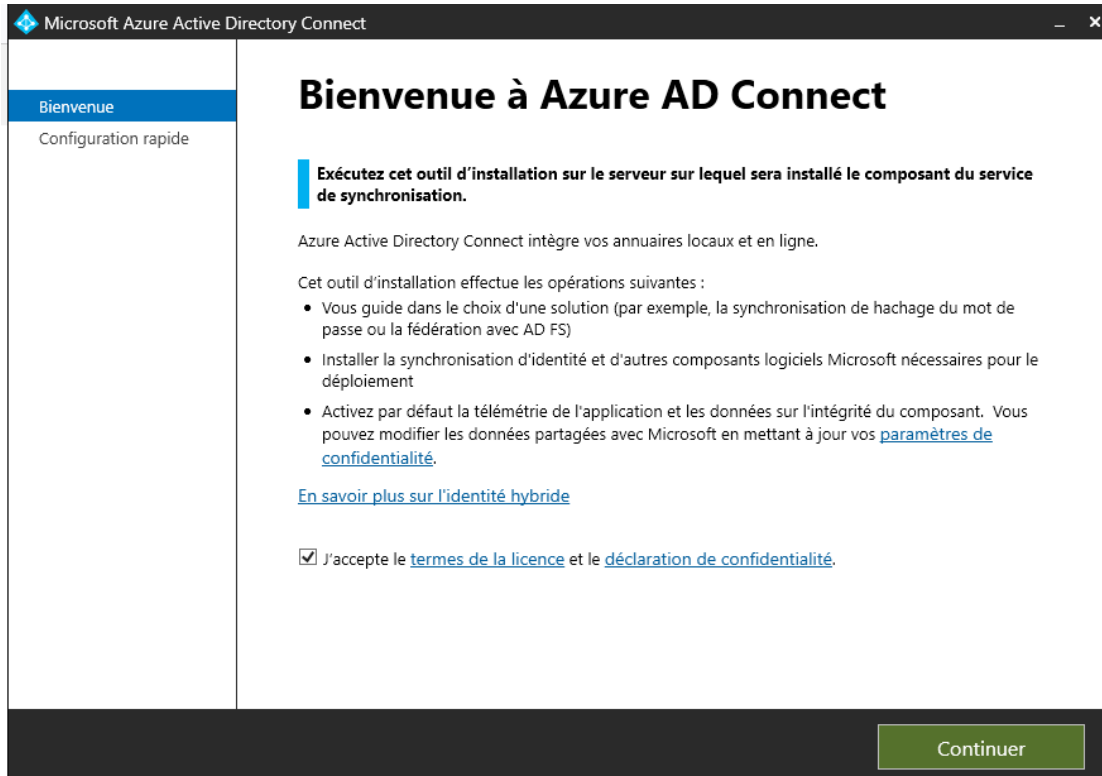
English

Download

Lancez le « .msi »

En cas de problème d'installation car agent introuvable exécuter ces actions

1. Supprimez la clé avec le nom de produit "Microsoft Azure AD Connect" dans HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Products et redémarrez l'installateur.



Ensuite continuer

Après personnaliser

Microsoft Azure Active Directory Connect

Bienvenue

Configuration rapide

Configuration rapide

Si vous disposez d'une forêt Windows Server Active Directory **unique**, nous effectuerons les opérations suivantes :

- Configuration de la synchronisation des identités dans la forêt AD actuelle de PCS
- Configurer la synchronisation de hachage du mot de passe à partir d'AD local vers Azure AD
- Lancement d'une synchronisation initiale
- Synchronisation de tous les attributs
- Activer la mise à niveau automatique

[En savoir plus sur la configuration rapide](#)

Sélectionnez Personnaliser pour choisir des options de déploiement avancées ou importer des paramètres à partir d'un serveur existant.

pcs.local n'est pas un domaine routable. Il est recommandé d'utiliser des paramètres personnalisés pour configurer des options de connexion utilisateur.
[En savoir plus](#) à propos des domaines non routables et des paramètres de connexion utilisateur.

Personnaliser Utiliser la configuration rapide

Je laisse par défaut

Vu qu'une ancienne installation fut trouvée je crée un nouveau dossier pour « ADSync »

Installer les composants nécessaires

Aucun service de synchronisation existant n'a été trouvé sur cet ordinateur. Le service de synchronisation Azure AD Connect sera installé. ?

Spécifier un emplacement d'installation personnalisé

EMPLACEMENT D'INSTALLATION

C:\ADSYNC

Parcourir

- Utiliser un SQL Server existant
- Utiliser un compte de service existant
- Spécifier des groupes de synchronisation personnalisés
- Importer les paramètres de synchronisation ?

L'annuaire de données de moteur de synchronisation C:\Program Files\Microsoft Azure AD Sync\Data contient des fichiers. Cet annuaire doit être vide pour que l'installation puisse continuer.

Précédent

Installer

Ensuite l'installation s'effectue

Installer les composants nécessaires

Aucun service de synchronisation existant n'a été trouvé sur cet ordinateur. Le service de synchronisation Azure AD Connect sera installé. ?

Azure ADConnect Agent Updater Installer



Spécifier un emplacement d'installation personnalisé

EMPLACEMENT D'INSTALLATION

C:\ADSYNC

Parcourir

Utiliser un SQL Server existant

Utiliser un compte de service existant

Spécifier des groupes de synchronisation personnalisés

Importer les paramètres de synchronisation ?

Ensuite on synchronise le hachage du mot de passe

Connexion utilisateur

Sélectionnez la méthode d'authentification. ?

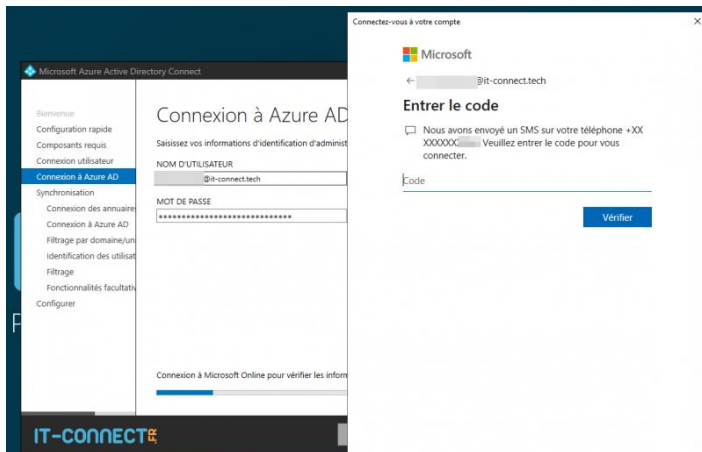
- Synchronisation de hachage du mot de passe ?
- Authentification directe ?
- Fédération avec AD FS ?
- Fédération avec PingFederate ?
- Ne pas configurer ?

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

Activer l'authentification unique ?

Sa veut dire que le hachage sera répliqué vers le tenant pour que le même mot de passe soit valide des deux côtés.

Ensuite on nous demande de nous authentifier avec le compte 365



Ensuite le domaine dans lequel est notre PC s'affiche automatiquement il faut l'ajouter ensuite on nous demande si on veut créer un compte pour ADsync ou on a déjà un compte réservé à cet effet.

Le plus simple est de créer un compte pour cela il faudra renseigner un compte admin du domaine qui créera l'utilisateur voulu.

Connexion de vos annuaires

Saisissez les informations d'identification pour les annuaires ou les batteries de serveurs locaux. [?](#)

TYPE D'ANNUAIRE

Active Directory

FORÊT [?](#)

Ajout d'un annuaire

RÉPERTOIRES CONFIGURÉS

pcs.local (Active Directory)

Supprimer

Le domaine maintenant est correctement ajouté je peux faire suivant.

On vérifie bien que notre suffixe UPN apparait correctement en état « VERIFIE » et on coche la petite case en bas puis « suivant »

Et on coche ici

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](#)

Je synchronise tout ce qu'il y'a dans le domaine « pcs.local »

Filtrage par domaine ou unité d'organisation

Annuaire : pcs.local

Actualiser les domaines ?

- Synchroniser tous les domaines et toutes les unités d'organisation
- Synchroniser les domaines et les unités d'organisation sélectionnés

▲ pcs.local

- ▶ Builtin
- ▶ Computers
- ▶ Domain Controllers
- ▶ ForeignSecurityPrincipals
- ▶ Infrastructure
- ▶ LostAndFound
- ▶ Managed Service Accounts
- ▶ PremiumCS
- ▶ Program Data
- ▶ System
- ▶ Users

Ici on laisse tout par défaut c'est pour l'identification unique

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 est actuellement synchronisé à l'aide de mS-DS-ConsistencyGuid et réécrira l'ancre source pour vos utilisateurs locaux. [En savoir plus](#)

Ici on synchronise tout

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

pcs.local

Résolution

Ensuite on coche que la synchronisation du mot de passe car nous ne faisons pas co-habiter des BAL exchange online et on-premise, pareils pour les dossiers public à priori, je n'active pas la réécriture du mot de passe pour réduire la surface d'attaque.

Fonctionnalités facultatives

Sélectionnez la fonctionnalité améliorée si votre organisation le demande.

- Déploiement Exchange hybride ?
- Dossiers publics de la messagerie Exchange ?
- Filtrage des applications et des attributs Azure AD ?
- 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.

Ensuite je fais suivant et je démarre le processus de synchronisation en appuyant sur suivant.

Configuration terminée

Configuration d'Azure AD Connect réussie. Le processus de synchronisation a été lancé.

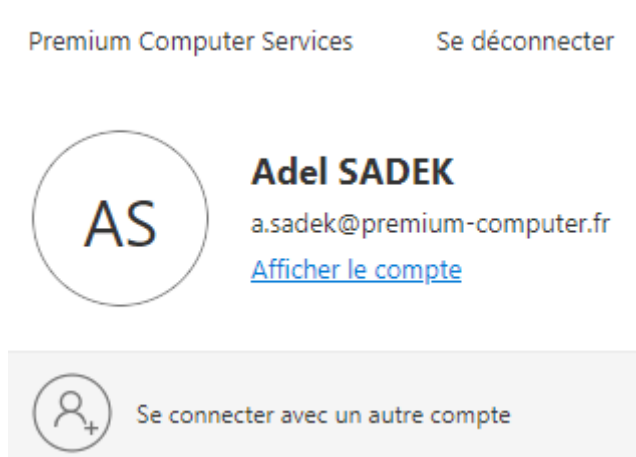
La configuration est terminée. Vous pouvez à présent vous connecter au portail Azure ou Office 365 pour vérifier que les comptes utilisateurs de votre répertoire local ont été créés. Effectuez ensuite un essai d'authentification sur le portail Azure. [En savoir plus sur les étapes suivantes et la gestion d'Azure AD Connect](#)

Azure Active Directory est configuré pour utiliser l'attribut AD `mS-DS-ConsistencyGuid` comme attribut d'ancre source. [En savoir plus sur la configuration de l'attribut d'ancrage source](#)

Échec de l'inscription de votre agent Azure AD Connect Health pour la synchronisation. [En savoir plus sur l'agent Azure AD Connect Health](#)

Je ne sais pas pourquoi AD connect health est fail.


J'essaye de me connecter sur office ça a l'air de fonctionner



Je crée cet user



Ensuite j'exécute cette commande pour lancer une synchro manuelle et rapide car par défaut

```
PS C:\Windows\system32> Start-ADSyncSyncCycle  
  
Result  
-----  
Success  
  
PS C:\Windows\system32> 
```

<http://go.microsoft.com/fwlink>