

# Installation de l'agent Azure AD Connect cloud sync

## Ressources

Lien pour l'installation de l'agent :

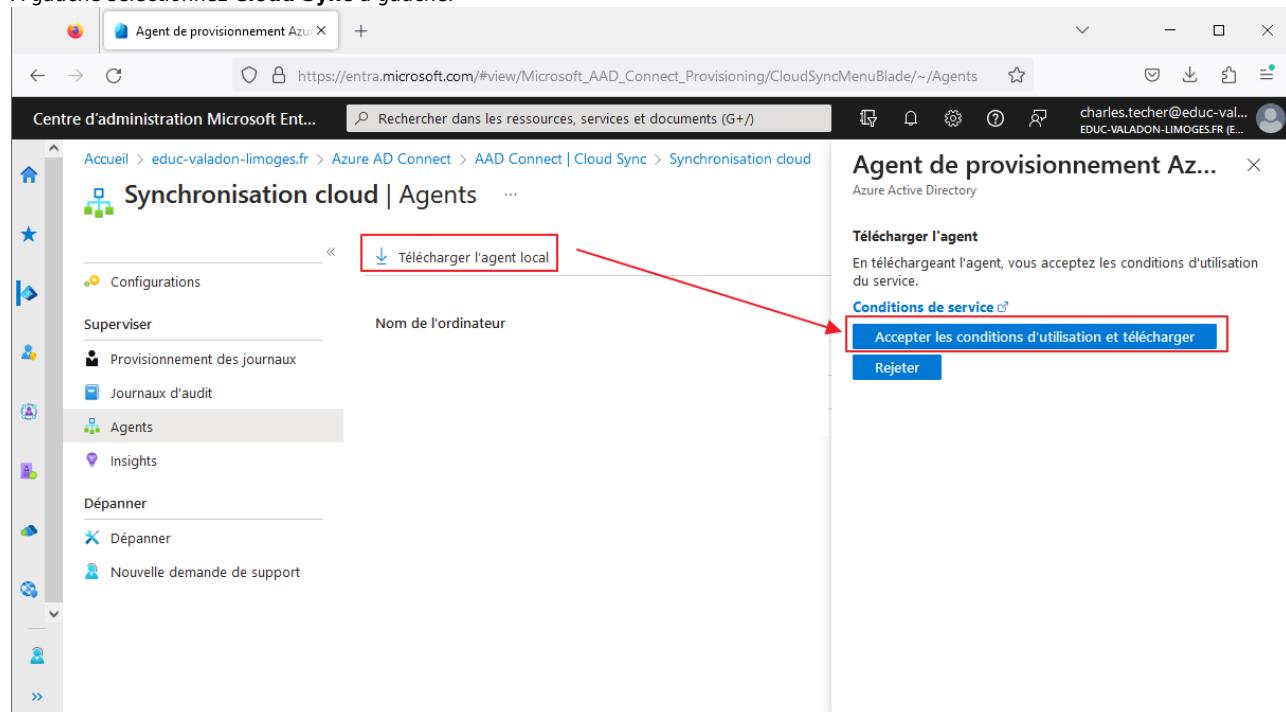
- <https://learn.microsoft.com/fr-fr/azure/active-directory/hybrid/cloud-sync/how-to-install>

## Téléchargement de l'agent que un Windows Server (minimum) 2016

Dans le **portail Azure** avec un **compte administrateur Azure** :

- Accédez à **Azure AD Connect**

- A gauche sélectionnez **Cloud Sync** à gauche.



- Sélectionnez **Agent** à gauche.
- Sélectionnez **Télécharger l'agent local**, puis **Accepter les conditions & télécharger**.
- Exécutez le fichier d'installation **AADConnectProvisioningAgentSetup.exe** situé dans le dossier de téléchargements.
- Dans l'écran de démarrage, sélectionnez **J'accepte la licence et les conditions**, puis cliquez sur **Installer**.

Après la fin de l'installation, l'**Assistant Configuration** démarre.

- Sélectionnez **Next** pour démarrer la configuration.

The screenshot shows the 'Welcome' screen of the Microsoft Entra Provisioning Agent Configuration wizard. On the left, a sidebar lists navigation options: 'Welcome' (selected), 'Connect Microsoft Entra ID', 'Configure Service Account', 'Connect Active Directory', and 'Confirm'. The main content area displays the following text:

Welcome to the Microsoft Entra provisioning agent configuration wizard

The Microsoft Entra provisioning agent supports the following provisioning scenarios:

- Provision identities from Active Directory to Microsoft Entra ID.
- Enable password writeback from Microsoft Entra ID for identities synchronized from Active Directory.
- Provision cloud security groups from Microsoft Entra ID to Active Directory.
- Provision identities from HR Systems (WorkDay and SuccessFactors) to Active Directory.
- Provision identities from HR systems to Active Directory using API-driven provisioning.
- Provision identities from Microsoft Entra ID to on-premises applications (SQL, LDAP, PowerShell, etc.).

Select the checkbox below for Entra Cloud Sync, HR-driven or API-driven provisioning scenarios

Connect to your Active Directory domain(s)

**Next**

- Sélectionner l'extension **Provisionnement piloté par les RH (Workday et SuccessFactors)/Synchronisation cloud Azure AD Connect**, puis cliquez sur **Next** :
- Se connectez-vous avec un **compte d'administrateur général Azure AD ou d'administrateur d'identité hybride**

Si vous avez la **sécurité renforcée d'Internet Explorer (ESC)** est **activée**, la connexion est bloquée.

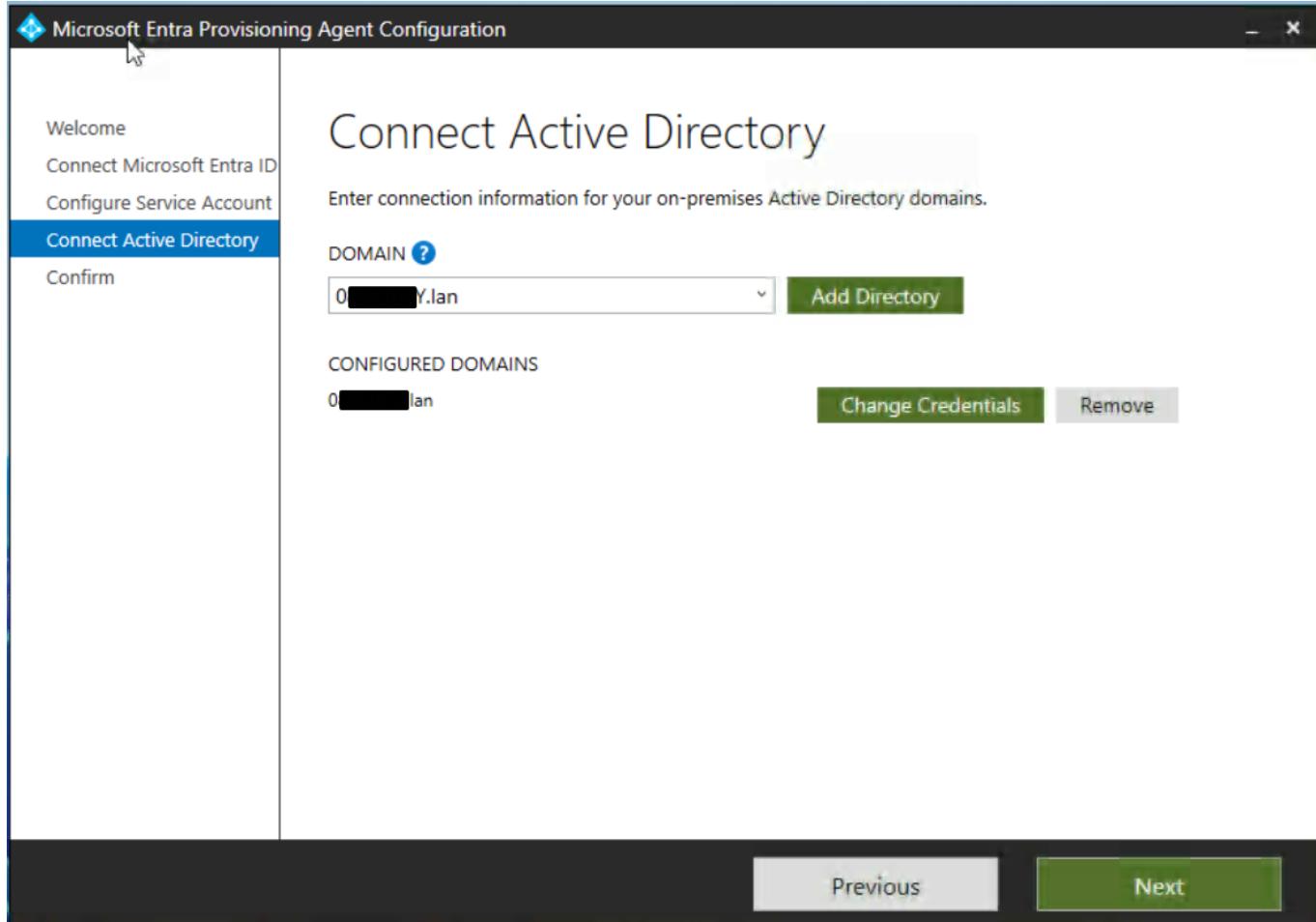
Dans ce cas :

- **fermez** l'installation,
- **désactivez** la sécurité renforcée d'Internet Explorer ([lien](#)),
- **redémarrez** l'installation du Package de l'agent de provisionnement Azure AD Connect.

Un **compte de service administré de groupe (gMSA)** doit être utilisé pour exécuter le service d'agent. Si un compte de service est déjà configuré dans le domaine par un agent installé sur un autre serveur, sélectionnez **Créer gMSA**, car le système détecte le compte existant et ajoute les autorisations requises pour que le nouvel agent utilise le même compte gMSA.

- **Créer un gMSA** permet à l'agent de créer le compte de service administré de groupe provAgentgMSA\$ dans le domaine Active Directory auquel est joint le serveur hôte. Pour utiliser cette option, entrez les informations d'identification de l'administrateur de domaine Active Directory (recommandé).

Dans l'écran **Connecter Active Directory** doit apparaître le nom de domaine AD local sous **Domaines configurés** :



## Retour au menu Synchronisation Cloud Azure AD Connect

- [Synchronisation Cloud Azure AD Connect](#)

