

# Azure AD

- [Les différents types de jointure](#)
- [Administrateur local de l'appareil joint Microsoft Entra](#)
- [Configurer un alias en environnement hybride](#)
- [Synchronisation AD connect](#)

# Les différents types de jointure

<https://jlou.eu/re-joignez-la-force-dazure-ad/>

	Registration Options		
Name	Azure AD Join	Device Registration	Domain Join + Device Registration
Primary Audience	<ul style="list-style-type: none"> <li>Choose your own device (CYOD) for: <ul style="list-style-type: none"> <li>Long term employees</li> <li>Seasonal workers and Students</li> <li>Cloud-only users</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>Bring your own device (BYOD) for all users</li> </ul>	<ul style="list-style-type: none"> <li>Long term employees</li> </ul>
Device Ownership	Organization	Personal	Organization
Device Types	PCs, Tablets, and Phones running Windows 10	PCs, Tablets, and Phones running Windows (8.1-10), Android, and IOS	PCs running Windows (7-10)
Provisioning	<ul style="list-style-type: none"> <li>Self configure using Out of box experience (OOBE)</li> </ul>	<ul style="list-style-type: none"> <li>Windows 8.1-10: Self configure in Settings</li> <li>IOS 8.3: via Over-the-Air Profile</li> <li>Android 4.0+: via Azure Authenticator App</li> </ul>	<ul style="list-style-type: none"> <li>Domain Join <ul style="list-style-type: none"> <li>Provisioned by IT</li> </ul> </li> <li>Workplace Join <ul style="list-style-type: none"> <li>Windows 8.1-10: Self configure in Settings and via GPO</li> <li>Windows 7: via GPO</li> </ul> </li> </ul>
Device Login	Organizational accounts (Authenticated against AAD)	End-user local authentication (PIN, Passcode, Pattern)	Organizational accounts (Authenticated against AD)
Management	<ul style="list-style-type: none"> <li>MDM (seamless Intune auto enrollment)</li> </ul>	<ul style="list-style-type: none"> <li>MDM</li> </ul>	<ul style="list-style-type: none"> <li>SCCM + GPOs</li> </ul>
Resources	<ul style="list-style-type: none"> <li>All users <ul style="list-style-type: none"> <li>Cloud and Single Sign On (SSO) to enterprise resources in the cloud with reduced logins</li> <li>Conditional access to resources applications when using Intune</li> </ul> </li> <li>On premises users <ul style="list-style-type: none"> <li>SSO to enterprise resources on-premises exposed via Web Application Proxy (WAP) using Azure AD Connect Device Writeback with reduced logins</li> </ul> </li> </ul>		<ul style="list-style-type: none"> <li>Single Sign On (SSO) to on premises and cloud hosted enterprise resources with reduced logins</li> </ul>
Additional functionality	<ul style="list-style-type: none"> <li>Azure AD cloud Bitlocker Key Storage</li> <li>Microsoft Passport Sign In</li> <li>Phone and PIN Sign In</li> <li>Enterprise State Roaming (Public Preview)</li> </ul>	<ul style="list-style-type: none"> <li>Microsoft Passport Sign In (Windows 10)</li> </ul>	<ul style="list-style-type: none"> <li>Microsoft Passport Sign In (Windows 10)</li> </ul>

# Administrateur local de l'appareil joint Microsoft Entra

## Procédure pour ajouter un utilisateur au rôle "Administrateur local de l'appareil joint Microsoft Entra"

### 1. Accéder au Centre d'administration 365

- Connectez-vous à l'interface d'administration Microsoft 365 via le lien suivant : [Centre d'administration 365](#).

### 2. Vérifier les privilèges administratifs de l'utilisateur

- Dans le centre d'administration, vérifiez que l'utilisateur **n'a pas** d'autres privilèges administrateurs.

### 3. Accéder à la gestion des rôles d'administrateurs

- Allez dans **Centre d'administration Identité > Rôles et administrateurs**.

### 4. Trouver et attribuer le rôle

- Cherchez le rôle intitulé **"Administrateur local de l'appareil joint Microsoft Entra"**.
- Ajoutez l'utilisateur dans ce groupe.

### 5. Conséquences

- Une fois l'utilisateur ajouté, il pourra se connecter en tant qu'administrateur local sur les postes et effectuer des élévations de privilèges.

# Configurer un alias en environnement hybride

## Étapes pour configurer un alias dans un environnement hybride :

1. **Accédez à Active Directory (AD) :**
    - Connectez-vous à un serveur qui dispose des outils de gestion d'Active Directory ou utilisez les outils PowerShell à distance pour gérer Active Directory.
  2. **Ouvrir l'éditeur d'attributs pour l'utilisateur :**
    - Ouvrez **Active Directory Users and Computers**.
    - Faites un clic droit sur l'utilisateur pour lequel vous souhaitez ajouter un alias, puis sélectionnez **Propriétés**.
  3. **Modifier l'attribut `proxyAddresses` :**
    - Dans la fenêtre des propriétés de l'utilisateur, accédez à l'onglet **Attributs**.
    - Cherchez l'attribut **`proxyAddresses`**.
  4. **Ajouter l'alias :**
    - Sous l'attribut **`proxyAddresses`**, vous devez ajouter deux adresses :
      - **`SMTP:adresseprincipale@domaine.com`** (en majuscule `SMTP` pour l'adresse principale).
      - **`smtp:alias@domaine.com`** (en minuscule `smtp` pour l'alias).
    - Exemple :
      - `SMTP:adresseprincipale@domaine.com`
      - `smtp:alias@domaine.com`
  5. **Valider les changements :**
    - Cliquez sur **OK** pour valider et appliquer les modifications.
  6. **Vérifier la synchronisation hybride :**
    - Si vous êtes dans un environnement hybride (Exchange local avec Exchange Online), assurez-vous que les modifications sont synchronisées entre vos environnements local et cloud.
    - Si vous utilisez **Azure AD Connect**, il faut attendre que la synchronisation se produise automatiquement, ou vous pouvez forcer la synchronisation via PowerShell avec la commande `Start-ADSyncSyncCycle -PolicyType Delta`.
  7. **Vérifier le résultat :**
    - Vous pouvez vérifier que l'alias a bien été configuré en envoyant un e-mail à l'adresse alias pour voir s'il est bien reçu sur la boîte de l'utilisateur principal.
-

Cela permet de configurer un alias correctement pour un utilisateur, tout en respectant la structure d'un environnement hybride où vous avez à la fois un serveur local et une configuration cloud.

# Synchronisation AD connect

## Types de Synchronisation avec Azure AD Connect

### 1. Synchronisation Delta

La **synchronisation Delta** est la plus courante. Elle permet de synchroniser uniquement les objets qui ont changé depuis la dernière synchronisation, comme l'ajout d'un utilisateur, d'un groupe, ou des modifications d'attributs.

Commande :

powershell

```
Start-ADSyncSyncCycle -PolicyType Delta
```

- **Utilisation** : Lorsqu'un utilisateur ou un groupe est ajouté ou modifié dans Active Directory (par exemple, après avoir ajouté un alias ou modifié un attribut).
- **Fréquence** : Utilisée régulièrement (automatiquement par défaut toutes les 30 minutes).

### 2. Synchronisation Complète (Initiale)

La **synchronisation complète** effectue une synchronisation complète de tous les objets dans Active Directory, quel que soit leur état. Elle est utilisée principalement lors de changements structurels dans la configuration de Azure AD Connect (par exemple, modifications des règles ou des filtres).

Commande :

powershell

```
Start-ADSyncSyncCycle -PolicyType Initial
```

- **Utilisation** : Après des modifications majeures dans Azure AD Connect, comme des changements de règles de synchronisation, des filtres de connexion ou lors de la première installation d'Azure AD Connect.
- **Fréquence** : Effectuée rarement, généralement lors des mises à jour ou modifications majeures.

### 3. Synchronisation Complète (Force)

La **synchronisation complète (force)** est similaire à la synchronisation complète mais forcée immédiatement. Cela peut être utile dans des scénarios où la synchronisation ne se lance pas correctement ou pour garantir que les objets sont bien synchronisés.

Commande :

powershell

```
Start-ADSyncSyncCycle -PolicyType Full
```

- **Utilisation** : Quand vous devez forcer une synchronisation complète après une interruption, un changement de configuration important ou une erreur dans la synchronisation précédente.
- **Fréquence** : Moins courante, utilisée principalement pour résoudre des problèmes ou forcer une synchronisation après un changement important.

## 4. Synchronisation des Staging Mode (Mode de préproduction)

Le **mode de préproduction** permet de tester la synchronisation des objets sans affecter réellement les utilisateurs finaux. Cela permet de valider les configurations sans risquer de modifier l'environnement de production.

Commande :

powershell

```
Start-ADSyncSyncCycle -PolicyType Staging
```

- **Utilisation** : Lors des tests dans un environnement de préproduction avant la mise en production réelle.
- **Fréquence** : À utiliser uniquement en environnement de préproduction, avant de passer les modifications en production.

## 5. Synchronisation de l'annuaire "Tiers" (Interim Synchronization)

Il s'agit d'une synchronisation qui permet de faire une synchronisation d'un autre environnement ou d'une autre partition d'annuaire dans un scénario multi-annuaire. Ce n'est pas couramment utilisé sauf dans des environnements complexes.

Commande :

powershell

```
Start-ADSyncSyncCycle -PolicyType Interim
```

- **Utilisation** : Synchroniser des annuaires ou des partitions supplémentaires dans des environnements multi-annuaire.

- **Fréquence** : Utilisé uniquement dans des configurations d'annuaire complexes avec plusieurs sources d'annuaire.

## Résumé des Types de Synchronisation et Commandes :

Type de Synchronisation	Commande PowerShell	Description
<b>Synchronisation Delta</b>	<code>Start-ADSyncSyncCycle -PolicyType Delta</code>	Synchronise les objets modifiés depuis la dernière synchronisation. Utilisé pour des changements courants dans l'AD.
<b>Synchronisation Complète (Initiale)</b>	<code>Start-ADSyncSyncCycle -PolicyType Initial</code>	Synchronisation complète de tous les objets. Utilisé après des changements dans la configuration ou la première installation.
<b>Synchronisation Complète (Force)</b>	<code>Start-ADSyncSyncCycle -PolicyType Full</code>	Forcer une synchronisation complète. Utilisé pour résoudre les problèmes ou forcer la synchronisation d'objets.
<b>Synchronisation Staging Mode</b>	<code>Start-ADSyncSyncCycle -PolicyType Staging</code>	Mode de préproduction pour tester la synchronisation sans affecter l'environnement de production.
<b>Synchronisation d'annuaire Tiers</b>	<code>Start-ADSyncSyncCycle -PolicyType Interim</code>	Utilisé pour synchroniser un autre annuaire ou une autre partition d'annuaire dans des configurations complexes.

## Quand utiliser chaque type de synchronisation :

- **Delta** : Utilisé pour les changements réguliers dans les objets, comme l'ajout ou la modification de groupes ou utilisateurs.
- **Complète (Initiale)** : Utilisé pour des changements importants dans Azure AD Connect, comme les modifications de configuration.
- **Complète (Force)** : Utilisé pour forcer une synchronisation complète lorsqu'il y a un problème ou pour assurer que tout est bien synchronisé.
- **Staging Mode** : Utilisé pour tester les configurations avant la mise en production.
- **Annuaire Tiers** : Utilisé dans les environnements multi-annuaire pour synchroniser des sources d'annuaire supplémentaires.