

# Sécurisation de l'Infrastructure de l'USS Entreprise avec Entra ID AzureAD

## 1. Création et Affectation des Groupes dans Entra ID

D'après les étapes documentées, voici comment recréer les groupes supprimés dans EntraID :

### Étape 1 : Accéder à Entra ID

1. Connectez-vous à votre portail Microsoft Entra ID ([lien vers le portail](#)).
2. Naviguez vers la section **Azure Active Directory** dans le menu principal.

### Étape 2 : Créer un Groupe

1. Dans le panneau de gauche, cliquez sur **Groupes** puis sur **+ Nouveau groupe**.
2. Configurez les paramètres :
  - **Type de groupe** : **Sécurité**.
  - **Nom du groupe** : Saisissez le nom du groupe (par exemple, "Amiral").
  - **Description** : Ajoutez une description pour identifier l'objectif du groupe.
  - **Propriétaire** : Ajoutez-vous comme propriétaire pour gérer le groupe.
3. Cliquez sur **Créer** pour valider.

### Étape 3 : Ajouter des Membres au Groupe

1. Une fois le groupe créé, cliquez dessus pour ouvrir ses paramètres.
2. Sous **Membres**, cliquez sur **Ajouter des membres**.
3. Sélectionnez les utilisateurs existants :
  - Pour le groupe **Amiral**, ajoutez **Jean-Luc Picard**.
  - Pour le groupe **Capitaine**, ajoutez **William Riker** et **Catherine Janeway**.
4. Enregistrez les modifications.

## 2. Configuration des Politiques de Sécurité dans Entra ID

### Étape 1 : Accéder à la Section des Politiques

1. Connectez-vous au portail [Microsoft Entra ID](#).
2. Naviguez vers **Azure Active Directory** > **Sécurité** > **Politiques d'accès conditionnel**.

## Étape 2 : Créer une Nouvelle Politique

1. Cliquez sur **+ Nouvelle politique**.
2. Donnez un nom descriptif à la politique, comme **"Restriction des accès non sécurisés"**.

## Étape 3 : Configurer les Conditions

1. **Utilisateurs et Groupes :**
  - Cliquez sur **Utilisateurs et groupes**.
  - Sélectionnez **Utilisateurs et groupes spécifiques**, puis ajoutez le groupe concerné (ex. "Capitaine").
2. **Applications Cloud ou Actions :**
  - Sélectionnez **Toutes les applications cloud** ou une application spécifique.
3. **Conditions :**
  - Cliquez sur **Emplacements**.
  - Activez la case **Configurer les emplacements**.
  - Ajoutez un **emplacement nommé** (ex. Réseau d'entreprise) et marquez les emplacements non définis comme **Bloquer l'accès**.

## Étape 4 : Configurer les Contrôles d'Accès

1. Sous **Accès accordé**, cochez **Exiger l'authentification multi-facteurs**.
2. Ajoutez d'autres contrôles si nécessaire (ex. exiger un appareil conforme).

## Étape 5 : Tester et Activer

1. Enregistrez la politique en mode **Activée : Non** pour tester.
2. Testez les connexions depuis différents emplacements (via VPN ou IP simulées).
3. Une fois validé, activez la politique.

## 3. Automatisation avec PowerShell : Création d'Utilisateurs et de Groupes dans Entra ID

Nous allons configurer des scripts PowerShell concrets pour automatiser la gestion des utilisateurs et des groupes

### *Script : Création Automatisée de Groupes*

1. Connecte-toi à <https://portal.azure.com> avec ton compte.
2. Clique sur l'icône du **Cloud Shell** (représentée par une fenêtre de terminal) dans la barre supérieure.
3. Si c'est la première fois :
  - Accepte la configuration d'un compte de stockage Azure (nécessaire pour le Cloud Shell).
  - Une fois configuré, le terminal s'ouvre.

4. Vérifie que tu es en mode **PowerShell** :
  - Si ce n'est pas le cas, sélectionne **PowerShell** dans le menu déroulant en haut du terminal.

## Étape 1 : Installer le Module AzureAD

Le module AzureAD est parfois déjà installé dans le Cloud Shell. Vérifie ou installe-le avec cette commande :

### Install-Module -Name AzureAD

```
PS /home/domenico_mandolino> Install-Module -Name AzureAD

Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository, change its InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to install the modules from 'PSGallery'?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"):
```

## Étape 2 : Se Connecter à Azure AD

Pour exécuter des commandes, connecte ton terminal à Azure AD :

### Connect-AzureAD

- Une fenêtre de connexion s'ouvre : entre tes identifiants administrateurs.

```
PS /home/domenico_mandolino> Connect-AzureAD
PS /home/domenico_mandolino> Connect-AzAccount
WARNING: Interactive authentication is not supported in this session, please run cmdlet 'Connect-AzAccount -UseDeviceAuthentication'.
PS /home/domenico_mandolino> Connect-AzAccount -UseDeviceAuthentication
WARNING: You may need to login again after updating "EnableLoginByIam".
Please select the account you want to login with.

[Login to Azure] To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the code DXBHDWHL to authenticate.
Retrieving subscriptions for the selection...

[Announcements]
With the new Azure PowerShell login experience, you can select the subscription you want to use more easily. Learn more about it and its configuration at https://go.microsoft.com/fwlink/?linkid=2271909.

If you encounter any problem, please open an issue at: https://aka.ms/azpsissue

Subscription name Tenant
-----
Abonnement Azure 1 Default Directory

PS /home/domenico_mandolino>
```

## Étape 3. Vérifier les Abonnements et le Contexte Actif

1. Vérifie que ton abonnement est actif en exécutant :  
powershell  
Copier le code

### Get-AzSubscription

```
PS /home/domenico_mandolino> Get-AzSubscription

TenantId: 5148f5aa-3e44-4f07-bc58-bdbec04d8262

Name                Id                                     State
----                -
Abonnement Azure 1 b012ecb6-f953-4052-bbc4-6fb76e73a3ce Enabled

PS /home/domenico_mandolino>
```

## Étape 4. Gestion des Groupes Azure AD

### Étape 5. Création de Groupes

Le script va pour créer des groupes de sécurité :

# Définir les noms des groupes à créer

```
$groupNames = @("Amiral", "Capitaine", "Équipage")
```

# Boucle pour créer les groupes

```
foreach ($groupName in $groupNames) {
```

```
    New-AzADGroup -DisplayName $groupName `
```

```
        -Description "Groupe $groupName pour l'USS Enterprise" `
```

```
        -MailEnabled:$false `
```

```
        -SecurityEnabled:$true `
```

```
        -MailNickname $groupName.ToLower() # Utilise le nom du groupe en minuscule  
comme alias
```

```
}
```

```
PS /home/domenico_mandolino> nano creation_groupes.ps1
PS /home/domenico_mandolino> ./creation_groupes.ps1
```

DisplayName	Id	MailNickname	Description
Amiral	a80b9660-9123-4a64-87c6-3c7a137eaaff	amiral	Groupe Amiral pour l'USS Enterprise
Capitaine	758e407b-d9df-4639-8cb6-f1f2a2677529	capitaine	Groupe Capitaine pour l'USS Enterprise
Équipage	b8e7c2a8-462d-49a9-a710-5b0683ca8818	équipage	Groupe Équipage pour l'USS Enterprise

```
PS /home/domenico_mandolino> █
```

### Étape 6. Vérification

Après exécution, vérifie que les groupes ont été créés avec leurs alias (**MailNickname**) correctement configurés :

```
Get-AzADGroup | Select-Object DisplayName, MailNickname
```

```
PS /home/domenico_mandolino> Get-AzADGroup | Select-Object DisplayName, MailNickname
```

DisplayName	MailNickname
Capitaine	capitaine
Amiral	amiral
Équipage	équipage

```
PS /home/domenico_mandolino> Disconnect-AzAccount -Scope {Scope} █
```

## **Script : Créer des Membres et les ajouter aux Groupes**

Une fois les groupes créés, assigner les utilisateurs aux groupes.

### **Étape 1 : Créer les Utilisateurs**

Azure AD dans PowerShell ne supporte pas directement la création d'utilisateurs avec le module Az. Utiliser plutôt l'interface web :

1. Accède au portail Azure (<https://portal.azure.com>).
2. Va dans **Azure Active Directory > Utilisateurs**.
3. Clique sur **+ Nouvel utilisateur** et crée les utilisateurs suivants :
  - **Nom** : Jean-Luc Picard, **UPN** : jeanluc.picard@vaisseau.com
  - **Nom** : Catherine Janeway, **UPN** : catherine.janeway@vaisseau.com
  - **Nom** : Geordi La Forge, **UPN** : geordi.laforge@vaisseau.com

### **Étape 2 : Ajouter les Utilisateurs aux Groupes**

Une fois les utilisateurs créés, utiliser le script suivant pour les ajouter à leurs groupes respectifs :

#### **# Récupérer les Groupes**

```
$amiralGroup = Get-AzureADGroup -Filter "DisplayName eq 'Amiral'"
```

```
$scapitaineGroup = Get-AzureADGroup -Filter "DisplayName eq  
'Capitaine'"
```

```
$sequipageGroup = Get-AzureADGroup -Filter "DisplayName eq  
'Équipage'"
```

#### **# Récupérer les Utilisateurs**

```
$picardUser = Get-AzureADUser -Filter "UserPrincipalName eq  
'jl.picard@domenicomandolinolaplatefor.onmicrosoft.com'"
```

```
$janewayUser = Get-AzureADUser -Filter "UserPrincipalName eq  
'c.janeway@domenicomandolinolaplatefor.onmicrosoft.com'"
```

```
$laforgeUser = Get-AzureADUser -Filter "UserPrincipalName eq  
'g.laforge@domenicomandolinolaplatefor.onmicrosoft.com'"
```

#### **# Ajouter les Membres aux Groupes**

```
Add-AzureADGroupMember -ObjectId $amiralGroup.ObjectId -RefObjectId  
$picardUser.ObjectId
```

```
Add-AzureADGroupMember -ObjectId $capitaineGroup.ObjectId  
-RefObjectId $janewayUser.ObjectId
```

```
Add-AzureADGroupMember -ObjectId $equipageGroup.ObjectId  
-RefObjectId $laforgeUser.ObjectId
```

### Étape 3. Vérifier les Membres des Groupes

Pour confirmer que les utilisateurs sont bien ajoutés dans les groupes, exécuter la commande suivante pour chaque groupe :

```
Get-AzADGroupMember -GroupObjectId $amiralGroup.Id
```

```
Get-AzADGroupMember -GroupObjectId $capitaineGroup.Id
```

```
Get-AzADGroupMember -GroupObjectId $equipageGroup.Id
```

```
PS /home/domenico_mandolino> Get-AzADGroupMember -GroupObjectId $amiralGroup.Id  
WARNING: This cmdlet is using a preview API version and is subject to breaking change in a future release.  
  
DisplayName      Id                                     Mail UserPrincipalName  
-----  
Jean-Luc Picard  37e2697b-6fff-4cae-acb4-739981824255  jl.picard@domenicomandolinolaplatefor.onmicrosoft.com  
  
PS /home/domenico_mandolino> Get-AzADGroupMember -GroupObjectId $equipageGroup.Id  
WARNING: This cmdlet is using a preview API version and is subject to breaking change in a future release.  
  
DisplayName      Id                                     Mail UserPrincipalName  
-----  
Geordi La forge  bbf1242c-6dcf-4857-bda0-d34e8bd6a87c  g.laforge@domenicomandolinolaplatefor.onmicrosoft.com  
  
PS /home/domenico_mandolino> Get-AzADGroupMember -GroupObjectId $capitaineGroup.Id  
WARNING: This cmdlet is using a preview API version and is subject to breaking change in a future release.  
  
DisplayName      Id                                     Mail UserPrincipalName  
-----  
Catherine Janeway 8959da4c-ac70-4eb1-a967-3c3252c331c8  c.janeway@domenicomandolinolaplatefor.onmicrosoft.com  
  
PS /home/domenico_mandolino> 
```

### Résultat Attendu

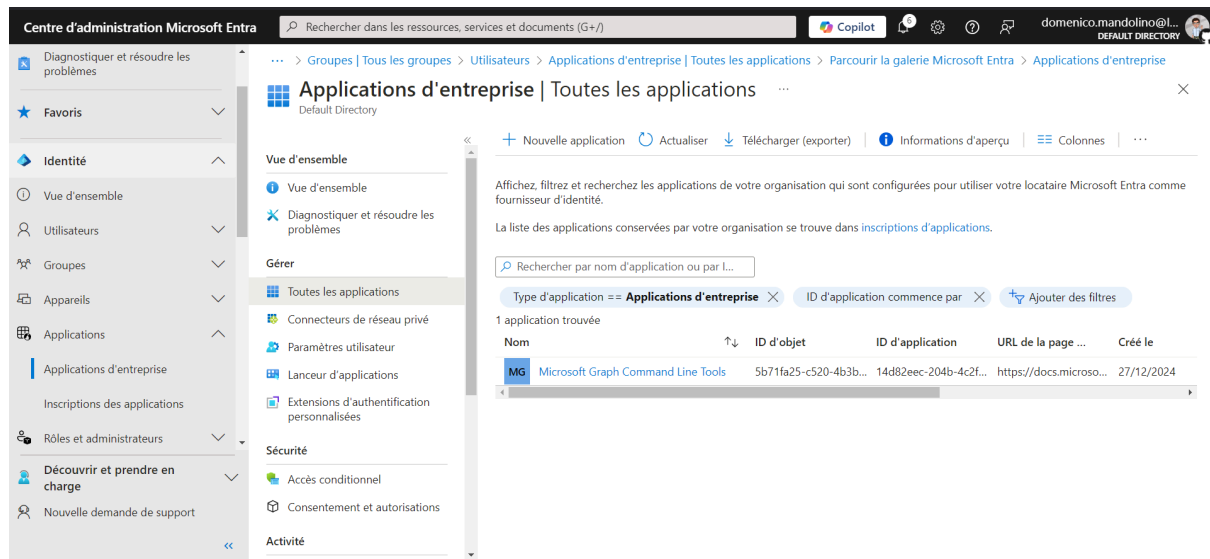
- **Jean-Luc Picard** est ajouté au groupe **Amiral**.
- **Catherine Janeway** est ajoutée au groupe **Capitaine**.
- **Geordi La Forge** est ajouté au groupe **Équipage**.

## 4.Intégration et Sécurisation des Applications

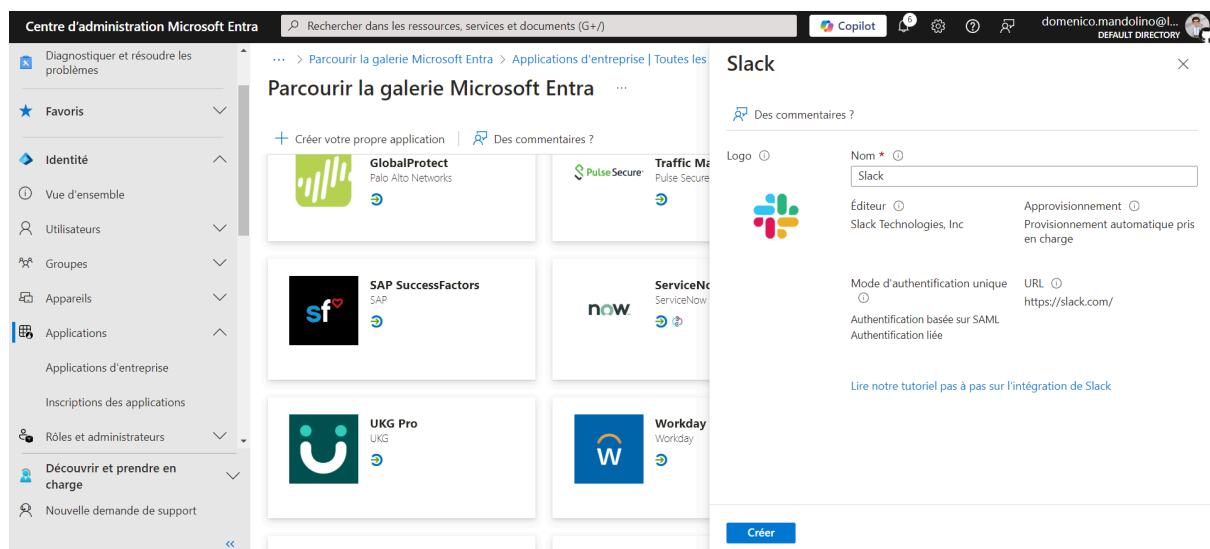
### 1. Intégrer une Application SaaS avec Azure AD

#### Étape 1 : Ajouter une Application SaaS

1. Connectez-vous au portail Azure : <https://portal.azure.com>.
2. Accédez à Azure Active Directory > Applications d'entreprise > + Nouvelle application.

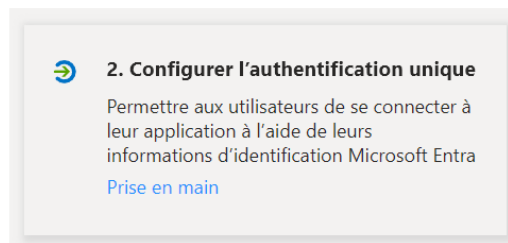


3. Cliquez sur Ajouter une application de la galerie.
4. Recherchez une application SaaS dans la galerie (par exemple, Zoom, Google Workspace, ou Slack).
5. Sélectionnez l'application et cliquez sur Créer.



## Étape 2 : Configurer l'Authentification

1. Une fois l'application ajoutée, va dans l'onglet **Authentification unique**.



2. Sélectionnez **SAML** comme méthode d'authentification.



3. Configurez les paramètres SAML :
  - **URL du service d'authentification (ACS)** : Renseignez l'URL fournie par le fournisseur SaaS.
  - **Identifiant (Entity ID)** : Fourni par l'application SaaS.
4. Téléchargez les métadonnées XML de l'Azure AD (fichier SAML) et importe-les dans l'application SaaS.
5. Testez la connexion en cliquant sur **Tester**.

1

Configuration SAML de base

Modifier

Identificateur (ID d'entité)	https://slack.com
URL de réponse (URL Assertion Consumer Service)	https://domenicomandolinolaplatefor.onmicrosoft.com.slack.com/sso/saml
URL de connexion	https://domenicomandolinolaplatefor.onmicrosoft.com.slack.com
État du relais (facultatif)	Facultatif
URL de déconnexion (facultatif)	https://login.microsoftonline.com/5148f5aa-3e44-4f07-bc58-bdbec04d8262/saml2



### Étape 3 : Attribuer les Utilisateurs ou Groupes

1. Dans l'onglet **Utilisateurs et groupes**, cliquez sur **+ Ajouter un utilisateur/groupe**.
2. Sélectionnez les utilisateurs ou groupes (par exemple, **Amiral**, **Capitaine**) qui ont besoin d'accéder à l'application.
3. Enregistrez les modifications.

## 2. Configurer le Single Sign-On (SSO) pour une Application

Le SSO permet aux utilisateurs de se connecter à toutes les applications avec leurs identifiants Azure AD.

### Étape 1 : Activer le SSO

1. Allez dans **Azure Active Directory > Applications d'entreprise**.
2. Sélectionnez l'application souhaitée.
3. Configurez les paramètres de SSO comme dans l'intégration SaaS.

### Étape 2 : Tester le SSO

1. Demandez à un utilisateur attribué de se connecter via le portail MyApps :  
<https://myapps.microsoft.com>.
2. Vérifiez qu'il est redirigé et authentifié avec succès.

## 3. Ajouter une Application Personnalisée

Si une application n'existe pas dans la galerie, vous pouvez l'ajouter comme une application personnalisée.

### Étape 1 : Ajouter l'Application

1. Dans **Azure Active Directory > Applications d'entreprise**, cliquez sur **+ Nouvelle application**.
2. Sélectionnez **Créer ma propre application**.
3. Choisissez d'intégrer **toute autre application que vous ne trouvez pas dans la galerie**.

### Étape 2 : Configurer l'Application

1. Configurez les paramètres généraux :
  - **Nom de l'application** : Gestion des Réparations.
  - **URL de connexion** : URL de l'application.
2. Configurez le SSO en suivant les étapes précédentes (SAML ou OpenID Connect).

### Étape 3 : Ajouter des Rôles et Permissions


1. Va dans l'onglet **Rôles et administrateurs** de l'application.
  2. Créez des rôles tels que :
    - **Ingénieurs** : Accès complet à l'application.
    - **Lecture seule** : Accès limité à la lecture des données.
  3. Attribuez ces rôles aux groupes ou utilisateurs.
- 

### 4. Tester et Valider l'Intégration

1. **Accès des utilisateurs** :
  - Connectez en tant qu'utilisateur pour vérifier que l'accès et les permissions fonctionnent.
2. **Logs et Surveillance** :
  - Allez dans **Surveillance** pour vérifier les journaux des connexions et identifier les erreurs.

Je n'ai pas pu terminer le job car je n'ai plus de crédit a disposition

#### Détails du crédit

Source :	Azure sign-up credit
Date d'effet :	07/12/2024
Date d'expiration :	06/01/2025
Montant d'origine :	200,00 \$US (190,80 €)
État :	 Expiré