

# Entra ID



projet réalisé par Youcef, Jordan

## Objectifs :

- Renforcer la sécurité via des politiques avancées.
- Automatiser la gestion des utilisateurs et des groupes grâce à PowerShell.
- Intégrer et sécuriser les applications essentielles.
- Détecter et répondre efficacement aux incidents de sécurité.

## Résumé-projet Entra ID :

### 1. Sécurité Avancée et Politiques de Sécurité :

#### 1.1 Détection et Blocage des Menaces :

Mise en place de politiques pour détecter et bloquer les attaques visant les identités des membres de Starfleet.

#### 1.2 Authentification Multi-Facteurs (MFA) :

Activation du MFA pour les officiers supérieurs afin de protéger les données sensibles.

#### 1.3 Politiques d'Accès Restrictives :

Création de politiques limitant les connexions depuis des emplacements non autorisés, tels que des planètes non sécurisées ou des vaisseaux inconnus.

#### 1.4 Tests de Politiques :

Simulation de connexions depuis divers secteurs galactiques pour évaluer l'efficacité des mesures de sécurité.

### 2. Automatisation avec PowerShell :

#### 2.1 Automatisation des Utilisateurs :

Développement de scripts pour ajouter de nouvelles recrues ou gérer les transferts entre vaisseaux.

#### 2.2 Gestion des Groupes :

Automatisation de l'ajout/suppression de membres dans des groupes tels que les équipes d'exploration et les équipes médicales.

#### 2.3 Application des Politiques de Sécurité :

Mise en œuvre automatique de politiques spécifiques pour les missions sensibles.

### 3. Intégration et Sécurisation des Applications

#### 3.1 Intégration SaaS avec Entra ID :

Intégration des applications essentielles de Starfleet (Journal de Bord, Centre de Commandement) avec Azure AD pour un accès sécurisé.

### 3.2 Single Sign-On (SSO) :

Configuration du SSO pour permettre aux membres d'utiliser leurs identifiants Starfleet.

### 3.3 Application Personnalisée :

Intégration de l'application de Gestion des Réparations pour l'ingénierie.

Configuration des rôles et permissions pour garantir l'accès exclusif aux ingénieurs pour certaines données.

Tests d'accès pour s'assurer du bon fonctionnement des permissions.

## 4. Surveillance et Réponse aux Incidents

### 4.1 Surveillance des Données Sensibles :

Observation des tentatives d'accès aux données critiques des missions.

### 4.2 Analyse des Logs :

Détection d'activités suspectes telles que des accès non autorisés aux plans des moteurs à distorsion.

### 4.3 Alertes en Temps Réel :

Configuration d'alertes pour les activités anormales, incluant les connexions suspectes depuis des zones inconnues.

### 4.4 Simulation et Tests de Réponse :

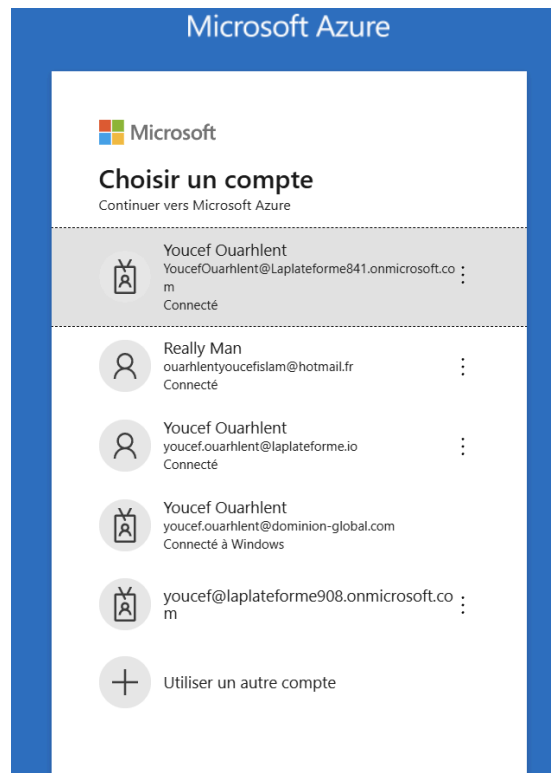
Simulation d'incidents (par exemple, tentative de piratage) pour tester les procédures, incluant la réinitialisation des accès et la mise en quarantaine des systèmes compromis.

## 1. Sécurité Avancée et Politiques de Sécurité :

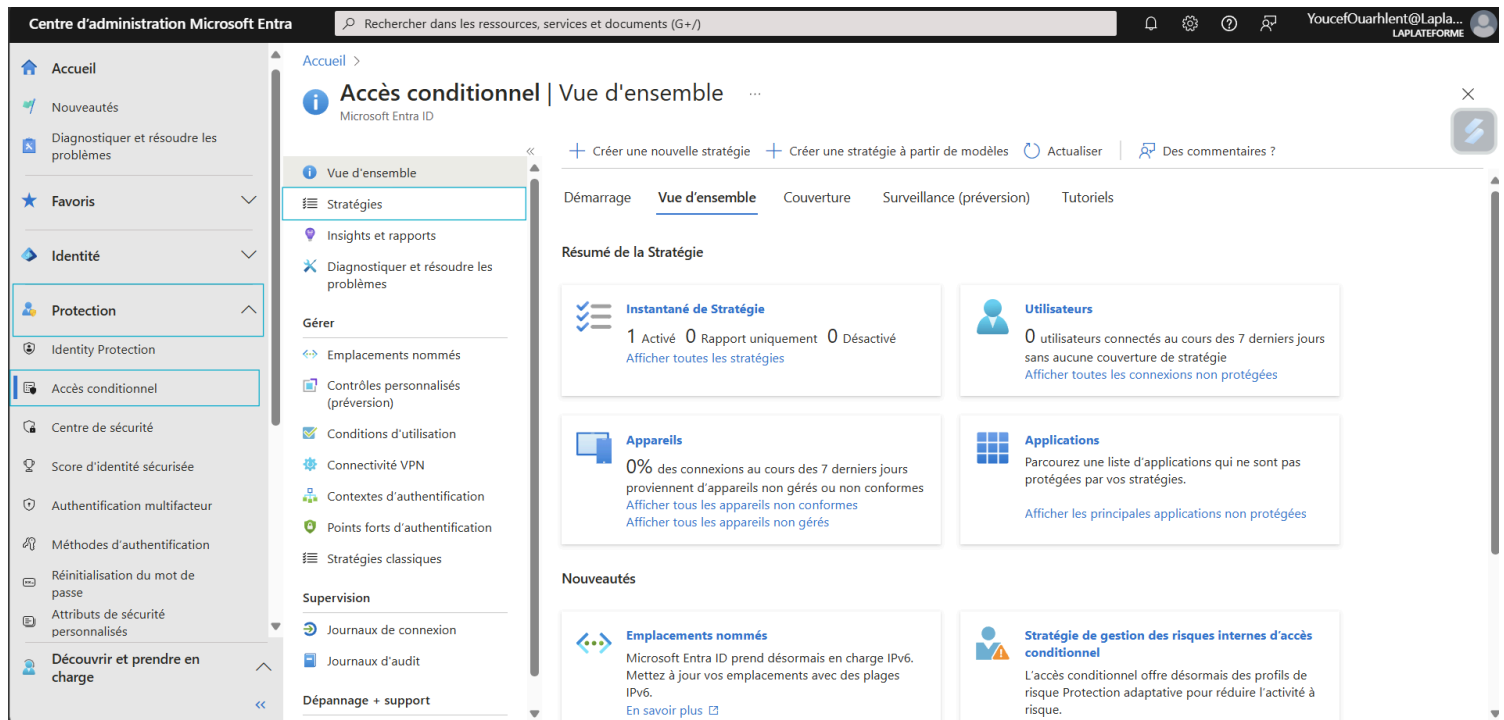
### 1.1 Détection et Blocage des Menaces :

Mise en place de politiques pour détecter et bloquer les attaques visant les identités des membres de Starfleet.

On commence par se rendre sur le portail <https://portal.azure.com/>



Une fois dessus on se rend sur “Microsoft Entra ID” > “Protection” > “Accès conditionnel”>”Créer une nouvelle stratégie”.



- **Créer une nouvelle stratégie d'accès conditionnel**

On crée “**Une nouvelle stratégie**” pour configurer la politique.

On donne un nom assez simple pour reconnaître la stratégie, comme “**Bloquer connexions suspectes**”.

- **Définir les utilisateurs et groupes concernés**

Dans **Affectations > Utilisateurs et groupes**, on sélectionne les membres d'équipage ou groupes auxquels cette politique s'appliquera.

Nom \*

Bloquer connexions suspectes

Affectations

Utilisateurs ⓘ

Utilisateurs spécifiques inclus

Ressources cibles ⓘ

Toutes les ressources (anciennement « Toutes les applications cloud »)

Réseau **NOUVEAUTÉ** ⓘ

N'importe quel réseau ou emplacement et 1 exclus

Conditions ⓘ

1 condition sélectionnée

Contrôles d'accès

Invités externes. [En savoir plus](#)

Inclure

Exclure

☐ Aucun

☐ Tous les utilisateurs

☒ Sélectionner des utilisateurs et des groupes


☐ Utilisateurs invités ou externes ⓘ

☐ Rôles d'annuaire ⓘ

☒ Utilisateurs et groupes

Sélectionner

1 utilisateur



Catherine Janeway  
Janeway@Laplateforme841.o...

...

Activer une stratégie

Rapport uniquement

Activé

Désactivé

## 1.2 Authentification Multi-Facteurs (MFA) :

Activation du MFA pour les officiers supérieurs afin de protéger les données sensibles.

Bulk update

Des commentaires ?

Users

Service settings

Utilisez l'authentification multifacteur (MFA) pour protéger vos utilisateurs et vos données. Notre approche recommandée pour appliquer l'authentification multifacteur consiste à utiliser des stratégies d'accès conditionnel adaptatives. [En savoir plus](#)

Avant de commencer, consultez le [guide de déploiement de l'authentification multifacteur](#).

✓ Activer MFA

⏏ Désactiver MFA

🛡 Appliquer MFA

⚙ Paramètres de MFA utilisateur

Rechercher

Statut : Tout

Afficher : Connecter les utilisateurs autorisés

🗑 Réinitialiser les filtres

<input type="checkbox"/>	Nom	UPN	Statut
<input type="checkbox"/>	Youcef Ouahrhlent	YoucefOuahrhlent@Laplateforme841.onmicrosoft.com	Enforced
<input type="checkbox"/>	Jean-Luc Picard	Picard@Laplateforme841.onmicrosoft.com	Enforced
<input type="checkbox"/>	Catherine Janeway	Janeway@Laplateforme841.onmicrosoft.com	Enforced
<input checked="" type="checkbox"/>	Geordi La forge	Laforge@Laplateforme841.onmicrosoft.com	Disabled
<input type="checkbox"/>	Deanna Troi	Troi@Laplateforme841.onmicrosoft.com	Disabled
<input type="checkbox"/>	William Riker	Riker@Laplateforme841.onmicrosoft.com	Disabled

Accueil > Laplateforme > Utilisateurs >

Authentification multifacteur par utilisateur

Bulk update

Des commentaires ?

Users

Service settings

Utilisez l'authentification multifacteur (MFA) pour protéger vos utilisateurs et vos données. Notre approche recommandée pour appliquer l'authentification multifacteur consiste à utiliser des stratégies d'accès conditionnel adaptatives. [En savoir plus](#)

Avant de commencer, consultez le [guide de déploiement de l'authentification multifacteur](#).

✓ Activer MFA

⏏ Désactiver MFA

🛡 Appliquer MFA

⚙ Paramètres de MFA utilisateur

Rechercher

Statut : Tout

Afficher : Connecter les utilisateurs autorisés

🗑 Réinitialiser les filtres

<input type="checkbox"/>	Nom	UPN	Statut
<input checked="" type="checkbox"/>	Youcef Ouahrhlent	YoucefOuahrhlent@Laplateforme841.onmicrosoft.com	Enforced
<input checked="" type="checkbox"/>	Jean-Luc Picard	Picard@Laplateforme841.onmicrosoft.com	Enforced
<input checked="" type="checkbox"/>	Catherine Janeway	Janeway@Laplateforme841.onmicrosoft.com	Enforced
<input type="checkbox"/>	Geordi La forge	Laforge@Laplateforme841.onmicrosoft.com	Disabled
<input type="checkbox"/>	Deanna Troi	Troi@Laplateforme841.onmicrosoft.com	Disabled
<input type="checkbox"/>	William Riker	Riker@Laplateforme841.onmicrosoft.com	Disabled

Activer l'authentification multifacteur

Si vos utilisateurs ne se connectent pas régulièrement via le navigateur, vous pouvez les rediriger vers ce lien pour qu'ils s'inscrivent à l'authentification multifacteur : <https://aka.ms/mfasetup>

Activer

Annuler

# Protéger votre compte

## Microsoft Authenticator



### Commencer par obtenir l'application

Sur votre téléphone, installez l'application Microsoft Authenticator. [Télécharger maintenant](#)

Après avoir installé l'application Microsoft Authenticator sur votre appareil, cliquez sur « Suivant ».

[Je souhaite utiliser une autre application d'authentification](#)

Suivant

## 1.3 Politiques d'Accès Restrictives :

Création de politiques limitant les connexions depuis des emplacements non autorisés, tels que des planètes non sécurisées ou des vaisseaux inconnus.

Pour ce faire, aller dans **Protection>Centre de sécurité>Emplacement des plages d'adresses IP**.

Centre d'administration Microsoft Entra

Rechercher dans les ressources, services et documents (G+/)

Accueil > Utilisateurs > Sécurité

Sécurité | Emplacements nommés

Rechercher

+ Emplacement des pays + Emplacement des plages d'adresses IP Configurer des adresses IP approuvées pour l'authentification multifactor

Les emplacements nommés sont utilisés par les rapports de sécurité Microsoft Entra pour réduire les faux positifs, et par les stratégies d'accès conditionnel Microsoft Entra. Les emplacements nommés marqués comme approuvés ou configurés dans les stratégies d'accès conditionnel ne peuvent pas être supprimés. [En savoir plus](#)

Rechercher par nom

Type d'emplacement : Tous les types Type approuvé : Tous les types Réinitialiser les filtres

1 emplacement nommé trouvé

Nom	Type d'emplacement	Approuvé	Stratégies d'accès conditionnel
Adresse IP Jordan	Plages d'adress...	Non	Bloquer connexions suspectes



## Nouvel emplacement (Plages d'adresses IP)



Charger Télécharger

Configurez les plages IPv4 et IPv6 de l'emplacement nommé. [En savoir plus](#)



Nom \*

Adresse IP Jordan



Marquer comme emplacement approuvé



1 plage d'adresses IP trouvée

10.10.137.214/16



jordi.laforge@laplateforme972.onmicrosoft.com

### Accès impossible pour le moment

Votre connexion a réussi mais ne respecte pas les critères pour accéder à cette ressource. Par exemple, vous vous connectez peut-être à partir d'un navigateur, d'une application ou d'un emplacement restreint(e) par votre administrateur.

[Se déconnecter et se connecter avec un autre compte](#)

[Plus de détails](#)



janeway@laplateforme841.onmicrosoft.com

## Action requise

Votre organisation requiert des informations de sécurité supplémentaires. Suivez les invites pour télécharger et configurer l'application Microsoft Authenticator.

[Utiliser un autre compte](#)

[En savoir plus sur l'application Microsoft Authenticator](#)

Suivant



picard@laplateforme841.onmicrosoft.com

## Action requise

Votre organisation requiert des informations de sécurité supplémentaires. Suivez les invites pour télécharger et configurer l'application Microsoft Authenticator.

[Utiliser un autre compte](#)


[En savoir plus sur l'application Microsoft Authenticator](#)

Suivant

## 2.1 Automatisation des Utilisateurs :

Développement de scripts pour ajouter de nouvelles recrues ou gérer les transferts entre vaisseaux.

Connectez-vous à votre compte



youcefouarhlent@laplateforme841.onmicrosoft.com

**Autorisations demandées**

Microsoft Graph Command Line Tools

Microsoft Corporation

Cette application souhaite :

- ✓ Lire les stratégies de votre organisation
- ✓ Accéder en lecture et en écriture aux stratégies d'accès conditionnel de votre organisation
- ✓ Afficher votre profil de base
- ✓ Conserver l'accès aux données auxquelles vous lui avez donné accès

☐ Consentement pour le compte de votre organisation

Accepter ces autorisations signifie que vous autorisez cette application à utiliser vos données comme indiqué dans les [conditions d'utilisation du service](#) et la [déclaration de confidentialité](#). Vous pouvez modifier ces autorisations à l'adresse <https://myapps.microsoft.com>. [Afficher les détails](#)

Cette application semble-t-elle suspecte ? [Signaler ici](#)

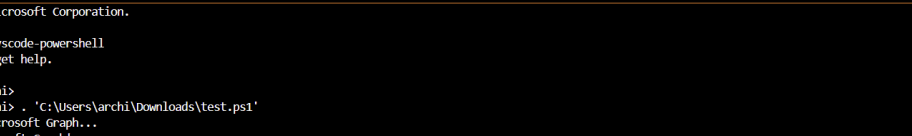
Annuler

Accepter

```

1 # Script pour ajouter un utilisateur à Starfleet via Microsoft Graph
2
3 # Vérifiez si le module Microsoft.Graph est installé
4 if (-not (Get-Module -ListAvailable -Name Microsoft.Graph)) {
5     Write-Host "Le module Microsoft.Graph n'est pas installé. Installation en cours..."
6     Install-Module -Name Microsoft.Graph -Scope CurrentUser -Force
7 }
8
9 # Connexion à Microsoft Graph
10 Write-Host "Connexion à Microsoft Graph..."
11 Connect-MgGraph -Scopes "User.ReadWrite.All GroupMember.ReadWrite.All"
12
13 # Collecte des informations utilisateur
14 Write-Host "Création d'un nouvel utilisateur pour Starfleet"
15
16 $Pseudo = Read-Host "Entrez le pseudo de l'utilisateur (ex : jl.picard)"
17 $SuffixeEmail = "@laplateforme841.onmicrosoft.com"
18 $UserPrincipalName = "$Pseudo$SuffixeEmail"
19 Write-Host "L'adresse email générée est : $UserPrincipalName"
20
21 $DisplayName = Read-Host "Entrez le nom complet de l'utilisateur (ex : Jean-Luc Picard)"
22 $Password = Read-Host "Entrez le mot de passe temporaire pour l'utilisateur"
23
24 # Création de l'objet PasswordProfile
25 $passwordProfile = @{
26     ForceChangePasswordNextSignIn = $true
27     Password = $Password
28 }
29
30 # Création de l'utilisateur
31 try {
32     New-MgUser -AccountEnabled:$true `
33         -DisplayName $DisplayName `
34         -MailNickname $Pseudo `
35         -UserPrincipalName $UserPrincipalName `
36         -PasswordProfile $passwordProfile `
37         -UsageLocation "FR"
38
39     Write-Host "Utilisateur $DisplayName créé avec succès !"
40 } catch {
41     Write-Host "Erreur lors de la création de l'utilisateur : $_" -ForegroundColor Red
42 }

```



```
Copyright (c) Microsoft Corporation.

https://aka.ms/vscode-powershell
Type 'help' to get help.

PS C:\Users\archi>
PS C:\Users\archi> . 'C:\Users\archi\Downloads\test.ps1'
Connexion à Microsoft Graph...
Welcome to Microsoft Graph!

Connected via delegated access using 14d82eec-204b-4c2f-b7e8-296a70dab67e
Readme: https://aka.ms/graph/sdk/powershell
SDK Docs: https://aka.ms/graph/sdk/powershell/docs
API Docs: https://aka.ms/graph/docs

NOTE: You can use the -Nowelcome parameter to suppress this message.

Création d'un nouvel utilisateur pour Starfleet
Entrez le pseudo de l'utilisateur (ex : jl.picard): Rija
L'adresse email de l'utilisateur est : Rija.laplateforme841@onmicrosoft.com
Entrez le nom complet de l'utilisateur (ex : Jean-Luc Picard): Rija
Entrez le mot de passe temporaire pour l'utilisateur: ZackS13012@

Utilisateur Rija créé avec succès !
Display Name Id Mail UserPrincipalName
-----
Rija 849ed593-1121-4010-ba68-2d9ba965d977 Rija.laplateforme841@onmicrosoft.com

PS C:\Users\archi>
```

## 1. Vérification du module `Microsoft.Graph`

Le script commence par vérifier si le module PowerShell `Microsoft.Graph` est installé.

- Si le module n'est pas disponible sur le système, il est automatiquement téléchargé et installé via la commande `Install-Module`.
  - Le paramètre `-Scope CurrentUser` garantit que l'installation est limitée à l'utilisateur courant et ne nécessite pas de droits administratifs.
  - L'installation est forcée (`-Force`) pour éviter toute demande de confirmation.
- 

## 2. Connexion à Microsoft Graph

Le script établit ensuite une connexion à Microsoft Graph.

- La commande `Connect-MgGraph` est utilisée pour authentifier l'utilisateur et établir une session.
  - Les scopes demandés (`User.ReadWrite.All` et `GroupMember.ReadWrite.All`) permettent de lire et modifier les informations des utilisateurs, ainsi que de gérer les membres des groupes (bien que cette fonctionnalité ne soit pas utilisée dans ce script).
- 

## 3. Collecte des informations utilisateur

Le script invite l'administrateur à entrer les informations nécessaires pour créer un utilisateur :

- Pseudo de l'utilisateur : Le pseudo est utilisé pour générer l'adresse email.
    - Un domaine fixe (`@Laplateforme841.onmicrosoft.com`) est ajouté au pseudo pour créer l'`UserPrincipalName` (adresse email principale).
    - Par exemple, si le pseudo est `j1.picard`, l'adresse email générée sera `j1.picard@Laplateforme841.onmicrosoft.com`.
  - L'adresse email générée est affichée pour confirmation.
  - Nom complet de l'utilisateur : Le nom complet (exemple : `Jean-Luc Picard`) sera utilisé comme `DisplayName` dans Azure Active Directory.
  - Mot de passe temporaire : L'administrateur doit entrer un mot de passe temporaire qui sera attribué au compte.
-

## 4. Création de l'objet PasswordProfile

Un objet **PasswordProfile** est créé pour stocker les paramètres liés au mot de passe utilisateur.

- **ForceChangePasswordNextSignIn = \$true** : Cette option oblige l'utilisateur à changer son mot de passe lors de sa première connexion.
  - **Password** : Définit le mot de passe temporaire saisi par l'administrateur.
- 

## 5. Création de l'utilisateur

Le script tente de créer un nouvel utilisateur dans Azure Active Directory en utilisant la commande **New-MgUser**.

- Les paramètres fournis à **New-MgUser** incluent :
  - **AccountEnabled = \$true** : Active immédiatement le compte utilisateur.
  - **DisplayName** : Définit le nom complet de l'utilisateur (exemple : **Jean-Luc Picard**).
  - **MailNickname** : Spécifie un alias pour l'utilisateur basé sur le pseudo (exemple : **jl.picard**).
  - **UserPrincipalName** : Définit l'adresse email principale générée (exemple : **jl.picard@Laplateforme841.onmicrosoft.com**).
  - **PasswordProfile** : Utilise l'objet créé précédemment pour appliquer les paramètres liés au mot de passe.
  - **UsageLocation = "FR"** : Définit la localisation de l'utilisateur (obligatoire pour certains services comme l'attribution des licences Office 365).

Si la création est réussie, un message de confirmation est affiché à l'écran.

---

## 6. Gestion des erreurs

Le script inclut un bloc **try-catch** pour gérer les éventuelles erreurs :

- Si une erreur survient lors de la création de l'utilisateur, elle est capturée par le bloc **catch**.
- Un message d'erreur détaillé est affiché en rouge pour alerter l'administrateur. Cela peut aider à diagnostiquer des problèmes comme des permissions insuffisantes ou un conflit avec un compte existant.

## 2.2 Gestion des Groupes :

Automatisation de l'ajout/suppression de membres dans des groupes tels que les équipes d'exploration et les équipes médicales.



```

1  # Script pour gérer les membres des groupes dans Azure Active Directory via Microsoft Graph
2
3  # Vérifiez si le module Microsoft.Graph est installé
4  if (-not (Get-Module -ListAvailable -Name Microsoft.Graph)) {
5      Write-Host "Le module Microsoft.Graph n'est pas installé. Installation en cours..."
6      Install-Module -Name Microsoft.Graph -Scope CurrentUser -Force
7  }
8
9  # Connexion à Microsoft Graph
10 Write-Host "Connexion à Microsoft Graph..."
11 Connect-MgGraph -Scopes "Group.ReadWrite.All User.Read.All"
12
13 # Fonction pour ajouter un utilisateur à un groupe
14 function Add-UserToGroup {
15     param (
16         [string]$GroupName,
17         [string]$UserPrincipalName
18     )
19     try {
20         # Récupérer l'ID du groupe
21         $Group = Get-MgGroup -Filter "displayName eq '$GroupName'"
22         if (-not $Group) {
23             Write-Host "Le groupe '$GroupName' n'existe pas." -ForegroundColor Yellow
24             return
25         }
26
27         # Récupérer l'ID de l'utilisateur
28         $User = Get-MgUser -Filter "userPrincipalName eq '$UserPrincipalName'"
29         if (-not $User) {
30             Write-Host "L'utilisateur '$UserPrincipalName' n'existe pas." -ForegroundColor Yellow
31             return
32         }
33
34         # Ajouter l'utilisateur au groupe
35         New-MgGroupMember -GroupId $Group.Id -DirectoryObjectId $User.Id
36         Write-Host "L'utilisateur '$UserPrincipalName' a été ajouté au groupe '$GroupName'."
37     } catch {
38         Write-Host "Erreur lors de l'ajout de l'utilisateur au groupe : $_" -ForegroundColor Red
39     }
40 }
41
42 # Fonction pour supprimer un utilisateur d'un groupe
43 function Remove-UserFromGroup {
44     param [
45         [string]$GroupName,
46         [string]$UserPrincipalName
47     ]
48     try {
49         # Récupérer l'ID du groupe
50         $Group = Get-MgGroup -Filter "displayName eq '$GroupName'"
51         if (-not $Group) {
52             Write-Host "Le groupe '$GroupName' n'existe pas." -ForegroundColor Yellow
53             return
54         }
55
56         # Récupérer l'ID de l'utilisateur
57         $User = Get-MgUser -Filter "userPrincipalName eq '$UserPrincipalName'"
58         if (-not $User) {
59             Write-Host "L'utilisateur '$UserPrincipalName' n'existe pas." -ForegroundColor Yellow
60             return
61         }
62
63         # Supprimer l'utilisateur du groupe
64         Remove-MgGroupMember -GroupId $Group.Id -DirectoryObjectId $User.Id
65         Write-Host "L'utilisateur '$UserPrincipalName' a été supprimé du groupe '$GroupName'."
66     } catch {
67         Write-Host "Erreur lors de la suppression de l'utilisateur du groupe : $_" -ForegroundColor Red
68     }
69 }
70

```

```

71 # Menu principal
72 do {
73     Write-Host "Gestion des Groupes Azure Active Directory" -ForegroundColor Cyan
74     Write-Host "1. Ajouter un utilisateur à un groupe"
75     Write-Host "2. Supprimer un utilisateur d'un groupe"
76     Write-Host "3. Quitter"
77
78     $Choice = Read-Host "Choisissez une option"
79
80     switch ($Choice) {
81         "1" {
82             $GroupName = Read-Host "Entrez le nom du groupe (ex : Exploration)"
83             $UserPrincipalName = Read-Host "Entrez l'email de l'utilisateur (UserPrincipalName, ex : user@domain.com)"
84             Add-UserToGroup -GroupName $GroupName -UserPrincipalName $UserPrincipalName
85         }
86         "2" {
87             $GroupName = Read-Host "Entrez le nom du groupe (ex : Exploration)"
88             $UserPrincipalName = Read-Host "Entrez l'email de l'utilisateur (UserPrincipalName, ex : user@domain.com)"
89             Remove-UserFromGroup -GroupName $GroupName -UserPrincipalName $UserPrincipalName
90         }
91         "3" {
92             Write-Host "Sortie du programme. À bientôt !" -ForegroundColor Green
93         }
94         default {
95             Write-Host "Option invalide. Veuillez réessayer." -ForegroundColor Yellow
96         }
97     }
98 } while ($Choice -ne "3")

```

```

Connected via delegated access using 14d82eec-204b-4c2f-b7e8-296a70dab67e
Readme: https://aka.ms/graph/sdk/powershell
SDK Docs: https://aka.ms/graph/sdk/powershell/docs
API Docs: https://aka.ms/graph/docs

NOTE: You can use the -Nowelcome parameter to suppress this message.

Gestion des Groupes Azure Active Directory
1. Ajouter un utilisateur à un groupe
2. Supprimer un utilisateur d'un groupe
3. Quitter
Choisissez une option: 1
Entrez le nom du groupe (ex : Exploration): Capitaine
Entrez l'email de l'utilisateur (UserPrincipalName, ex : user@domain.com): Riya@laplateforme841.onmicrosoft.com
L'utilisateur 'Riya@laplateforme841.onmicrosoft.com' a été ajouté au groupe 'Capitaine'.
Gestion des Groupes Azure Active Directory
1. Ajouter un utilisateur à un groupe
2. Supprimer un utilisateur d'un groupe
3. Quitter
Choisissez une option:

```

## 1. Vérification du module **Microsoft.Graph**

Le script commence par vérifier si le module PowerShell **Microsoft.Graph** est installé. Si le module n'est pas disponible sur le système, il est automatiquement téléchargé et installé.

- **Install-Module :**
    - Télécharge et installe le module nécessaire.
    - Le paramètre **-Scope CurrentUser** limite l'installation à l'utilisateur actuel sans nécessiter de droits administratifs.
    - Le paramètre **-Force** force l'installation sans demander confirmation.
-

## 2. Connexion à Microsoft Graph

Le script établit une connexion à Microsoft Graph via la commande **Connect-MgGraph**.

- **Authentification :**
    - La commande établit une session authentifiée pour effectuer des actions sur Azure Active Directory.
  - **Scopes requis :**
    - **Group.ReadWrite.All** : Gérer les groupes (ajouter, supprimer des membres, etc.).
    - **User.Read.All** : Lire les informations des utilisateurs nécessaires pour les opérations.
- 

## 3. Fonction **Add-UserToGroup**

Cette fonction est utilisée pour ajouter un utilisateur à un groupe spécifique.

- **Entrées :**
    - **\$GroupName** : Nom du groupe.
    - **\$UserPrincipalName** : Adresse email de l'utilisateur.
  - **Processus :**
    - Recherche le groupe avec **Get-MgGroup**.
    - Vérifie si l'utilisateur existe avec **Get-MgUser**.
    - Ajoute l'utilisateur au groupe avec **New-MgGroupMember**.
  - **Gestion des erreurs :**
    - Affiche un message si le groupe ou l'utilisateur est introuvable.
    - Utilise un bloc **try-catch** pour capturer les erreurs liées aux permissions ou conflits.
- 

## 4. Fonction **Remove-UserFromGroup**

Cette fonction est utilisée pour retirer un utilisateur d'un groupe.

- **Entrées :**
  - **\$GroupName** : Nom du groupe.
  - **\$UserPrincipalName** : Adresse email de l'utilisateur.
- **Processus :**
  - Recherche le groupe avec **Get-MgGroup**.
  - Vérifie si l'utilisateur existe avec **Get-MgUser**.
  - Supprime l'utilisateur du groupe avec **Remove-MgGroupMember**.
- **Gestion des erreurs :**

- Affiche un message si le groupe ou l'utilisateur est introuvable.
  - Utilise un bloc **try-catch** pour capturer les erreurs liées aux permissions ou conflits.
- 

## 5. Menu interactif

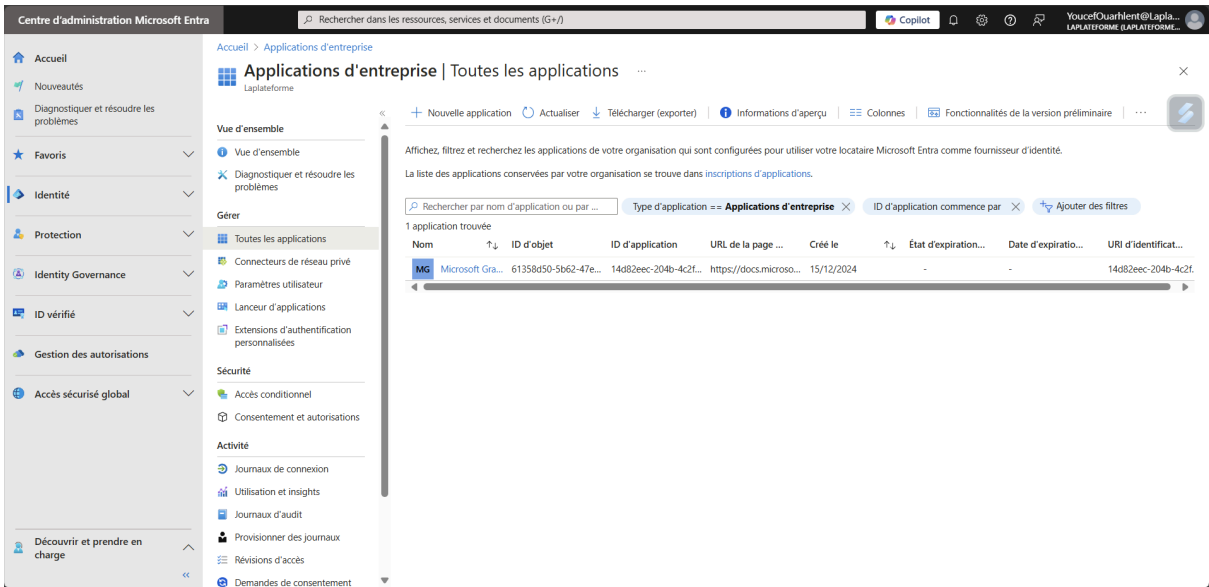
Le menu interactif permet à l'utilisateur de choisir entre trois options :

1. Ajouter un utilisateur à un groupe.
  2. Supprimer un utilisateur d'un groupe.
  3. Quitter le programme.
- Interaction utilisateur :
    - Le menu demande une option à l'utilisateur avec **Read-Host**.
  - Actions basées sur les choix :
    - **1** : Exécute la fonction **Add-UserToGroup**.
    - **2** : Exécute la fonction **Remove-UserFromGroup**.
    - **3** : Quitte le programme avec un message de sortie.
  - Validation des entrées :
    - Si une option invalide est choisie, un message d'erreur est affiché et le menu est réaffiché.

### 3. Intégration et Sécurisation des Applications

#### 3.1 Intégration SaaS avec Entra ID :

Intégration des applications essentielles de Starfleet (Journal de Bord, Centre de Commandement) avec Azure AD pour un accès sécurisé.



Accueil > Repair Management | Utilisateurs et groupes > Applications d'entreprise | Toutes les applications >

#### Parcourir la galerie Microsoft Entra

+ Créer votre propre application | Des commentaires ?

La galerie d'applications Microsoft Entra est un catalogue de milliers d'applications qui facilitent le déploiement et la configuration de l'authentification unique (SSO) et du provisionnement automatisé des utilisateurs. Lors du déploiement d'une application à partir de la galerie d'applications, vous tirez parti des modèles prédéfinis pour connecter vos utilisateurs de manière plus sécurisée à leurs applications. Parcourez ou créez votre propre application ici. Si vous voulez publier une application que vous avez développée dans la galerie Microsoft Entra pour que d'autres organisations puissent la découvrir et l'utiliser, vous pouvez créer une demande à l'aide du processus décrit dans [cet article](#).

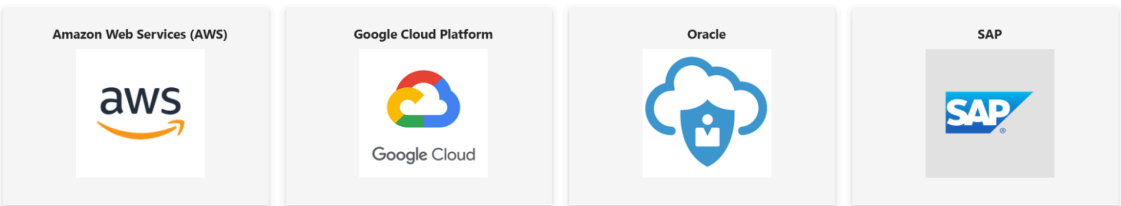
Rechercher dans l'application

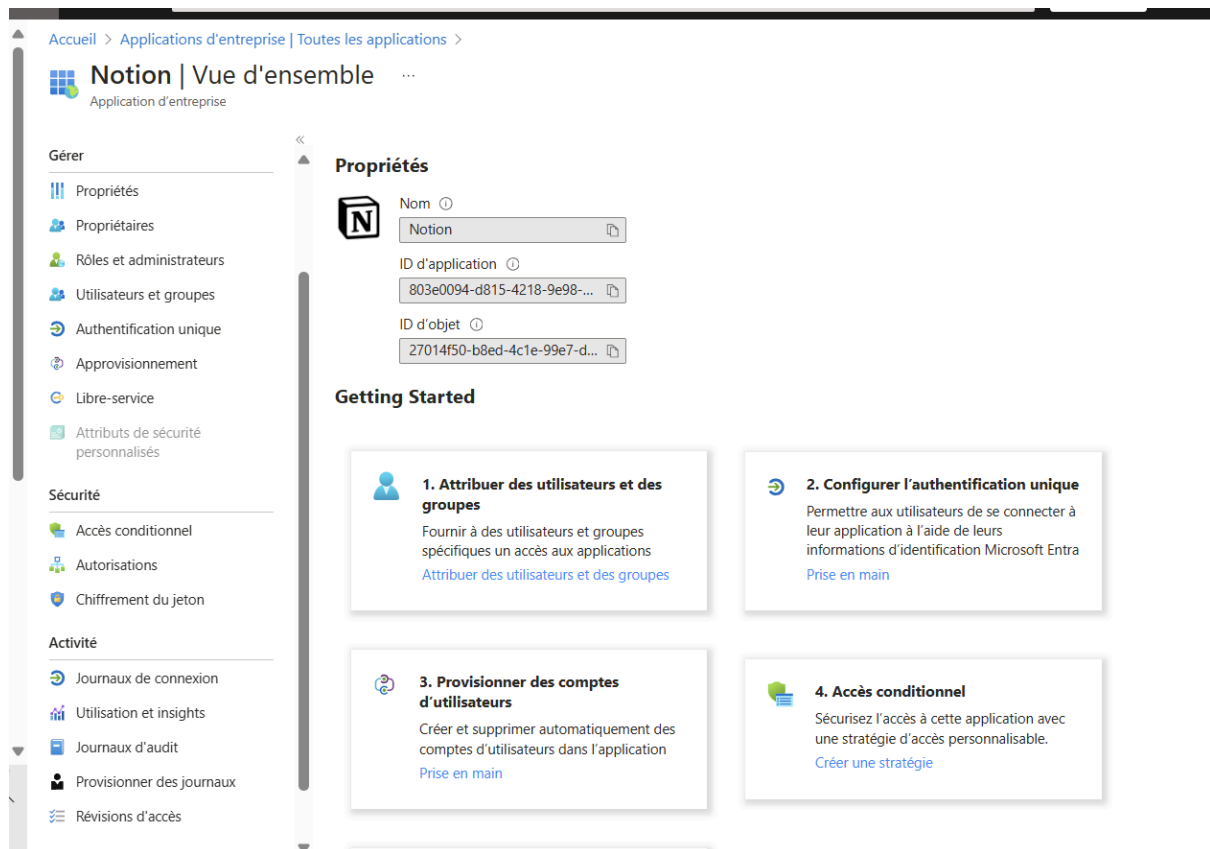
Authentification unique : **Tout**

Gestion du compte utilisateur : **All**

Catégories : **Tout**

#### Plateformes cloud





## Pourquoi Notion comme Journal de Bord ?

### 1. Centralisation de l'information

- **Organisation flexible** : Notion permet de structurer des journaux de bord en utilisant des pages hiérarchisées, des bases de données et des balises.
- **Un espace unique** : Centralisez toutes les informations importantes, notes de réunions, événements quotidiens, tâches, et projets dans un seul outil collaboratif.

### 2. Collaboration en temps réel

- **Mise à jour instantanée** : Les équipes peuvent travailler simultanément sur le journal de bord, ajoutant ou modifiant des entrées en temps réel.
- **Commentaires et mentions** : Facilitez les discussions avec la possibilité de commenter des sections spécifiques ou de mentionner des membres de l'équipe.

### 3. Suivi des activités et historique

- **Horodatage des modifications** : Notion garde une trace des modifications pour consulter l'historique des entrées.
- **Suivi des projets** : Ajoutez des champs personnalisés pour catégoriser et suivre l'état d'avancement des tâches ou des événements importants.

#### **4. Personnalisation et automatisation**

- **Modèles personnalisés** : Créez des modèles pour structurer les entrées de votre journal de bord (par exemple : une entrée journalière avec des sections pour les tâches, notes, et priorités).
- **Automatisation des rappels** : Ajoutez des deadlines ou configurez des intégrations avec d'autres outils pour recevoir des notifications.

#### **5. Recherche et accessibilité**

- **Moteur de recherche puissant** : Recherchez rapidement des mots-clés, des dates ou des sujets dans tout le journal.
- **Accessible partout** : Disponible sur le web, les applications mobiles et desktop, pour consulter ou mettre à jour votre journal à tout moment.

#### **6. Visualisation des données**

- **Bases de données dynamiques** : Ajoutez des tableaux ou des kanbans pour mieux visualiser vos tâches ou événements.
- **Liens entre pages** : Connectez facilement les entrées du journal à d'autres documents ou projets dans Notion.

### **Pourquoi Splunk comme Command Center ?**

- **Surveillance en temps réel** : Collecte des journaux système, des événements, et des métriques.
- **Tableaux de bord personnalisables** : Créez des vues centralisées pour superviser votre infrastructure IT.
- **Alertes et notifications** : Configurez des alertes pour des incidents critiques.
- **Analyse des données machine** : Idéal pour repérer les anomalies et diagnostiquer rapidement les problèmes.

### 3.2 Single Sign-On (SSO) :

Configuration du SSO pour permettre aux membres d'utiliser leurs identifiants Starfleet.

Accueil > Applications d'entreprise | Toutes les applications > Notion

## Notion | Authentification unique

Application d'entreprise

**Vue d'ensemble**

- Plan de déploiement
- Diagnostiquer et résoudre les problèmes

**Gérer**

- Propriétés
- Propriétaires
- Rôles et administrateurs
- Utilisateurs et groupes
- Authentification unique**
- Approvisionnement
- Libre-service
- Attributs de sécurité personnalisés

**Sécurité**


- Accès conditionnel
- Autorisations
- Chiffrement du jeton


**Activité**


- Journaux de connexion
- Utilisation et insights

L'authentification unique (SSO) apporte sécurité et confort aux utilisateurs qui se connectent à des applications dans Microsoft Entra ID. En effet, un utilisateur de votre organisation peut se connecter à toutes les applications qu'il utilise avec un seul compte. Une fois l'utilisateur connecté à une application, ces informations d'identification sont utilisées pour toutes les autres applications auxquelles il veut accéder. [En savoir plus.](#)

Sélectionner une méthode d'authentification unique [Aidez-moi à choisir](#)

 **Désactivé**  
L'authentification unique n'est pas activée. L'utilisateur ne pourra pas lancer l'application à partir de Mes applications.

 **SAML**  
Authentification enrichie et sécurisée aux applications à l'aide du protocole SAML (Security Assertion Markup Language).

 **Lié**  
Ajoutez un lien à une application dans Mes applications et/ou le lanceur d'applications Office 365.



# Configuration SAML de base



Enregistrer | Des commentaires ?

## Identificateur (ID d'entité) \* ⓘ

ID unique qui identifie votre application à Microsoft Entra ID. Cette valeur doit être unique dans toutes les applications de votre locataire Microsoft Entra. L'identificateur par défaut sera l'audience de la réponse SAML pour l'authentification unique initiée par IDP.

[Ajouter un identificateur](#)

## URL de réponse (URL Assertion Consumer Service) \* ⓘ

L'URL de réponse correspond à l'emplacement où l'application est supposée recevoir le jeton d'authentification. Cette URL est parfois appelée « Assertion Consumer Service » (ACS) dans SAML.

[Ajouter une URL de réponse](#)

## URL de connexion (facultatif)

L'URL d'authentification est utilisée si vous souhaitez effectuer une authentification unique initiée par le fournisseur de services. Cette valeur est l'URL de la page de connexion pour votre application. Ce champ n'est pas nécessaire si vous voulez effectuer une authentification unique initiée par le fournisseur d'identité.

Entrer une URL de connexion



## État du relais (facultatif) ⓘ

L'état de relais indique à l'application où rediriger les utilisateurs une fois l'authentification terminée, et la valeur est généralement une URL ou un chemin d'URL qui dirige les utilisateurs vers un emplacement spécifique au sein de l'application.

Entrer un état de relais

## URL de déconnexion (facultatif)

Accueil > Applications d'entreprise | Toutes les applications > Notion

Notion | Authentification basée sur SAML

Application d'entreprise

Vue d'ensemble

Plan de déploiement

Diagnostic et résolution des problèmes

Gérer

Propriétés

Propriétaires

Rôles et administrateurs

Utilisateurs et groupes

Authentification unique

Approvisionnement

Libre-service

Attributs de sécurité personnalisés

Sécurité

Accès conditionnel

Autorisations

Chiffrement du jeton

Activité

Journaux de connexion

Utilisation et insights

Charger le fichier de métadonnées

Modifier le mode d'authentification unique

Test cette application

Des commentaires ?

Configurer l'authentification unique avec SAML

Une implémentation SSO basée sur les protocoles de fédération améliore la sécurité, la fiabilité et l'expérience de l'utilisateur final. Elle est également plus facile à implémenter. Choisissez l'authentification unique SAML chaque fois que cela est possible pour les applications existantes qui n'utilisent pas OpenID Connect ou OAuth. [En savoir plus.](#)

Lire le [guide de configuration](#) pour l'intégration de Notion.

1

Configuration SAML de base

Modifier

Identificateur (ID d'entité)	https://www.notion.so/saml/metadata
URL de réponse (URL Assertion Consumer Service)	https://www.notion.so/saml/acs
URL de connexion	Facultatif
État du relais (facultatif)	Facultatif
URL de déconnexion (facultatif)	Facultatif

2

Attributs et revendications

Modifier

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
firstName	user.givenname
lastName	user.surname
email	user.mail
Identificateur unique de l'utilisateur	user.userprincipalname

3

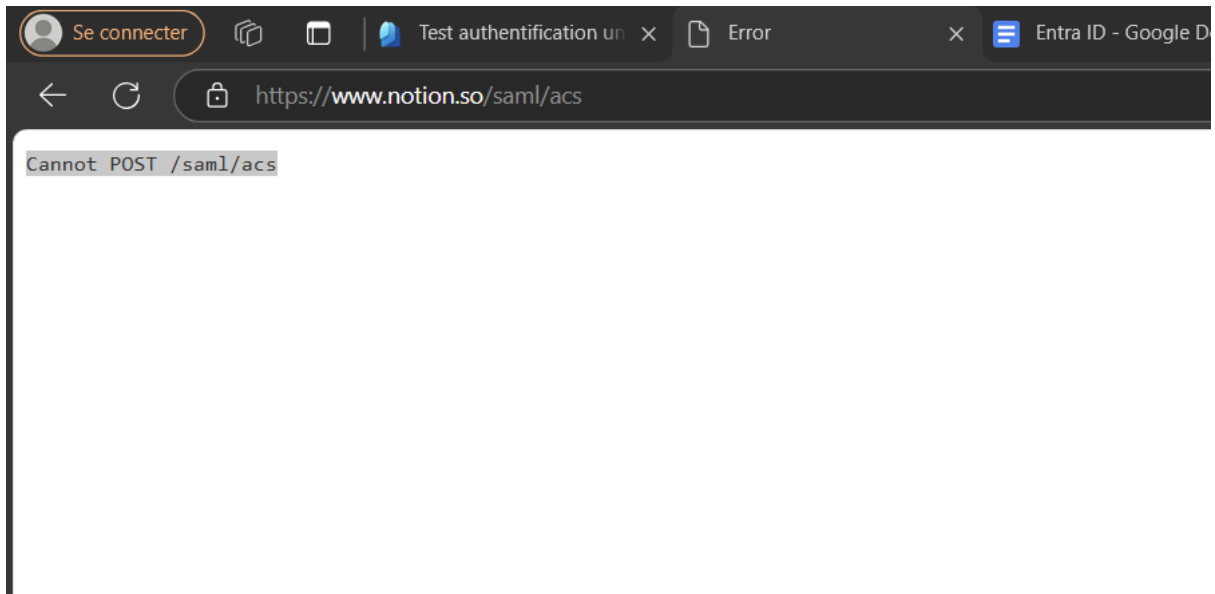
Certificats SAML



YoucefOuarhlent@Laplateforme841.onmicrosoft.com

## Test SAML Single Sign-On

Please wait...





Repair Management | Rôles et administrateurs

Application d'entreprise

Actualiser

Fonctionnalités de la version préliminaire

Des commentaires ?

Bénéficiez de l'accès juste-à-temps à un rôle lorsque vous en avez besoin à l'aide de PIM. En savoir plus sur PIM

Rôles d'administration

Les rôles d'administration sont utilisés pour accorder l'accès aux actions privilégiées dans Microsoft Entra ID. Nous vous recommandons d'utiliser ces rôles intégrés pour déléguer l'accès à la gestion des autorisations de configuration d'application étendue sans accorder d'accès pour gérer d'autres parties de Microsoft Entra ID, qui ne sont pas liées à la configuration de l'application.

[En savoir plus.](#)

Les rôles attribuables sont des rôles qui peuvent être attribués ici pour permettre la gestion de cette ressource. Les rôles au niveau du répertoire ont hérité de l'accès à cette ressource et ne peuvent être attribués qu'au niveau du répertoire [ici](#).

Rechercher par nom ou description

Attribuable : Oui

Ajouter des filtres

Rôle	Description	Privilegié	De...	Type
Administrateur d'application cloud	Peut créer et gérer tous les aspects des inscriptions d'applications et des applications d'entreprise, à l'exception du proxy d'application.	PRIVILÉGIÉ	0	Intégré
Ingé			0	Personnalisée
Lecteur de rapports	Peut lire les rapports d'audit et sur les connexions.		0	Intégré

## 4. Surveillance et Réponse aux Incidents

### 4.1 Surveillance des Données Sensibles :

Observation des tentatives d'accès aux données critiques des missions.

**Log Analytics est un service intégré à Azure Monitor qui permet de collecter, analyser et visualiser des données de journaux provenant de différentes sources, comme Microsoft Entra ID (Azure Active Directory), des machines virtuelles, des services cloud, et autres applications. Il est particulièrement utile pour :**

- Analyser les logs de manière centralisée.**
- Créer des requêtes avancées pour détecter des comportements anormaux.**
- Configurer des alertes personnalisées en fonction des données analysées.**
- Visualiser**

**Exemple d'utilisation avec Microsoft Entra ID** Supposons que vous souhaitiez détecter des tentatives de connexion suspectes dans Microsoft Entra ID.

**Étapes :**

- Configurer Log Analytics :** Allez dans le Portail Azure. Activez Log Analytics Workspace pour collecter les logs. Connecter les journaux d'Entra ID à Log Analytics :
- Dans Microsoft Entra ID,** configurez l'envoi des logs d'audit et des connexions vers votre Workspace Log Analytics.
- Écrire une requête KQL :** Exemple de requête pour identifier les connexions depuis un emplacement inhabituel : `kql Copier le code AuditLogs | where OperationName == "Sign-in" | where Location !in ("France", "USA") // Emplacements autorisés | project UserPrincipalName, IPAddress, Location, OperationName` Cette requête filtre les logs d'audit pour trouver des connexions depuis des pays non autorisés.
- Créer des alertes :** Allez dans Azure Monitor > Alertes. Configurez une règle d'alerte basée sur votre requête KQL. Spécifiez une action (par exemple, envoyer un e-mail, une notification, ou un webhook).
- Visualiser les résultats :** Créez un tableau de bord interactif pour afficher les logs et les alertes en temps réel.

Événements de connexion

Télécharger Exporter les paramètres de données Dépanner Actualiser Colonnes Des commentaires ?

Date : Dernières 24 heures Afficher les dates au format : Local Ajouter des filtres

Connexions utilisateur (interactives)										
Date	ID de requête	Utilisateur	Application	Statut	Adresse IP	Emplacement	Accès conditionnel	Exigence d'authen...		
16/12/2024 12:09:09	252c6c50-533e-4bfc-9...	Youcef Ouahrhent	Microsoft Graph Com...	Interrompu	37.26.187.6	Marseille, Bouches-Du...	Non appliqué	Authentification multif...		
16/12/2024 11:59:42	97a71300-d4ad-4ae9-...	Youcef Ouahrhent	Azure Portal	Opération réussie	37.26.187.6	Marseille, Bouches-Du...	Non appliqué	Authentification multif...		
16/12/2024 11:59:38	07102b09-98f9-45fc-9...	Youcef Ouahrhent	Azure Portal	Interrompu	37.26.187.6	Marseille, Bouches-Du...	Non appliqué	Authentification multif...		
16/12/2024 11:56:43	662d1276-f663-47e1-...	Youcef Ouahrhent	Azure Portal	Échec	37.26.187.6	Marseille, Bouches-Du...	Non appliqué	Authentification multif...		
15/12/2024 18:23:56	282623d8-0627-4f49-...	Youcef Ouahrhent	Notion	Opération réussie	2a01:e34:ec94:1520:d8...	Marseille, Bouches-Du...	Non appliqué	Authentification multif...		
15/12/2024 18:18:03	aa4f0526-d812-42d5-...	Youcef Ouahrhent	Notion	Opération réussie	2a01:e34:ec94:1520:d8...	Marseille, Bouches-Du...	Non appliqué	Authentification multif...		
15/12/2024 18:17:27	54d30791-5374-4ee2-...	Youcef Ouahrhent	Notion	Opération réussie	2a01:e34:ec94:1520:d8...	Marseille, Bouches-Du...	Non appliqué	Authentification multif...		
15/12/2024 18:14:34	2aed75eb-7884-418c-...	Youcef Ouahrhent	Notion	Échec	2a01:e34:ec94:1520:d8...	Marseille, Bouches-Du...	Non appliqué	Authentification multif...		
15/12/2024 18:07:40	8b116c8d-ee65-4f2e-...	Youcef Ouahrhent	Notion	Échec	2a01:e34:ec94:1520:d8...	Marseille, Bouches-Du...	Non appliqué	Authentification multif...		
15/12/2024 18:07:28	8b116c8d-ee65-4f2e-...	Youcef Ouahrhent	Notion	Échec	2a01:e34:ec94:1520:d8...	Marseille, Bouches-Du...	Non appliqué	Authentification multif...		
15/12/2024 18:07:24	06e4daf4-d586-47c3-...	Youcef Ouahrhent	My Apps	Opération réussie	2a01:e34:ec94:1520:d8...	Marseille, Bouches-Du...	Non appliqué	Authentification multif...		
15/12/2024 17:43:30	0431afc3-cb0f-44cd-9...	Youcef Ouahrhent	Azure Portal	Opération réussie	2a01:e34:ec94:1520:d8...	Marseille, Bouches-Du...	Non appliqué	Authentification multif...		
15/12/2024 17:18:51	0821b291-0dfe-4924-...	Youcef Ouahrhent	Microsoft Graph Com...	Opération réussie	2a01:e34:ec94:1520:19...	Marseille, Bouches-Du...	Non appliqué	Authentification multif...		
15/12/2024 17:18:24	911ef35f-28ec-4464-9...	Youcef Ouahrhent	Microsoft Graph Com...	Interrompu	2a01:e34:ec94:1520:19...	Marseille, Bouches-Du...	Non appliqué	Authentification multif...		
15/12/2024 16:43:12	82cb5eba-2459-4678-...	Youcef Ouahrhent	Microsoft Graph Com...	Opération réussie	2a01:e34:ec94:1520:19...	Marseille, Bouches-Du...	Non appliqué	Authentification multif...		
15/12/2024 16:43:06	82cb5eba-2459-4678-...	Youcef Ouahrhent	Microsoft Graph Com...	Interrompu	2a01:e34:ec94:1520:19...	Marseille, Bouches-Du...	Non appliqué	Authentification multif...		
15/12/2024 16:17:10	60d8f5cc-69c2-4f56-b...	Youcef Ouahrhent	Microsoft Graph Com...	Opération réussie	2a01:e34:ec94:1520:19...	Marseille, Bouches-Du...	Non appliqué	Authentification multif...		

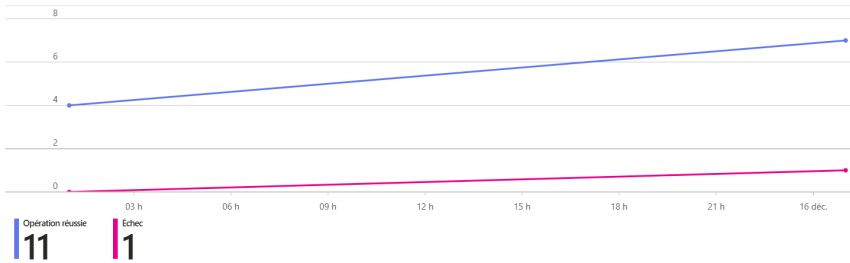
Utilisation et insights - Azure Portal

Des commentaires ?

Date 30 jours

- Passer en revue les utilisateurs inactifs
- Démarrer une nouvelle révision des accès

Activité de connexion



Échecs de connexion

Erreur	Code d'erreur	Occurrences	Dernière consultation
Authentication failed during strong authentication request.	500121	1	16/12/2024

Accueil / Applications d'entreprise / routes les applications / notion

Notion | Journaux de connexion

problèmes Télécharger Exporter les paramètres de données Dépanner Actualiser Colonnes Des commentaires ?

Date : 7 derniers jours Afficher les dates au format : Local Application contient 651d5427-ba6f-46e0-8fa2-e16beafd1e10 Ajouter des filtres

Connexions utilisateur (interactives)										
Date	ID de requête	Utilisateur	Application	Statut	Adresse IP	Emplacement	Accès condition...			
15/12/2024 18:23:56	282623d8-0627-4f49...	Youcef Ouahrhent	Notion	Opération réussie	2a01:e34:ec94:1520:...	Marseille, Bouches-D...	Non appliqué			
15/12/2024 18:18:03	aa4f0526-d812-42d5...	Youcef Ouahrhent	Notion	Opération réussie	2a01:e34:ec94:1520:...	Marseille, Bouches-D...	Non appliqué			
15/12/2024 18:17:27	54d30791-5374-4ee...	Youcef Ouahrhent	Notion	Opération réussie	2a01:e34:ec94:1520:...	Marseille, Bouches-D...	Non appliqué			
15/12/2024 18:14:34	2aed75eb-7884-418...	Youcef Ouahrhent	Notion	Échec	2a01:e34:ec94:1520:...	Marseille, Bouches-D...	Non appliqué			

Vous n'avez pas accès ...



Intégration Log Analytics non activée

Ce locataire Microsoft Entra n'est pas activé actuellement pour envoyer des journaux à Log Analytics. Cliquez sur le lien ci-dessous pour savoir comment activer cette fonctionnalité.

[En savoir plus sur l'intégration de Microsoft Entra ID à Log Analytics](#)

**Récapitulatif**

ID de session  
cb177577c12842fe9c1fe7a4f75c0078

Extension  
Microsoft\_AAD\_IAM

Code d'erreur  
403

ID de ressource  
Non disponible

Contenu  
NewLogAnalyticsBlade

4.2 Analyse des Logs :

Détection d'activités suspectes telles que des accès non autorisés aux plans des moteurs à distorsion.

Microsoft Azure

Rechercher dans les ressources, services et documents (G+)

Copilot

YoucefOuarhient@Lapla...

Accueil > Laplateforme > Utilisateurs > Utilisateurs

Utilisateurs | Journaux d'audit

Rechercher

Tous les utilisateurs

Journaux d'audit

Journaux de connexion

Diagnostiquer et résoudre les problèmes

Utilisateurs supprimés

Réinitialisation du mot de passe

Paramètres utilisateur

Résultats de l'opération en bloc

Nouvelle demande de support

Télécharger Actualiser Colonne Commentaires

Cette vue sera bientôt remplacée par une vue qui inclut des journaux d'attributs de sécurité personnalisés, un défilement infini et une réorganisation des colonnes. Essayez la nouvelle préversion des audits. →

Date : Dernier mois Afficher les dates au format : Local Service : Tout Catégorie : UserManagement Activité : Tout Ajouter des filtres

Date	Service	Catégorie	Activité	Statut	Motif d'état	Cible(s)	Initié par (acteur)
15/12/2024 18:16:58	Core Directory	UserManagement	Add app role assignment ...	Success		Notion, YoucefOuarhient@...	YoucefOuarhient@Laplatef...
15/12/2024 15:42:05	Core Directory	UserManagement	Add user	Success		Jojo@Laplateforme841.on...	Microsoft Graph Comman...
15/12/2024 15:40:23	Core Directory	UserManagement	Add user	Success		Rija@Laplateforme841.on...	Microsoft Graph Comman...
15/12/2024 15:38:46	Core Directory	UserManagement	Delete user	Success		96428748a15741d58ed3fe...	YoucefOuarhient@Laplatef...
15/12/2024 15:38:10	Core Directory	UserManagement	Add user	Success		raji@Laplateforme841.on...	Microsoft Graph Comman...
15/12/2024 15:08:41	Core Directory	UserManagement	Add app role assignment ...	Success		Microsoft Graph Comman...	YoucefOuarhient@Laplatef...
15/12/2024 15:08:26	Core Directory	UserManagement	Update user	Success		YoucefOuarhient@Laplatef...	Azure MFA StrongAuthenti...

4.3 Alertes en Temps Réel :

Configuration d'alertes pour les activités anormales, incluant les connexions suspectes depuis des zones inconnues.

Rechercher

En savoir plus Télécharger Actualiser Colonnes Des commentaires ?

Protéger

- Accès conditionnel
- Identity Protection
- Centre de sécurité

Gérer

- Score d'identité sécurisée
- Emplacements nommés
- Méthodes d'authentification
- Authentification multifacteur
- Autorités de certification (classiques)
- Infrastructure de clé publique (prévision)

Rapport

- Utilisateurs à risque
- Identités de charge de travail à risque
- Connexions à risque
- Détections de risques**

Want to allow automatic risk remediation? Set up risk policies in Conditional Access. Learn more →

Actualisation automatique : **Désactivé** Heure de la détection : **7 derniers jours** Afficher les dates au format : **Local** État à risque : **2 sélectionné(s)**

Type de détection : **Aucune sélection** Niveau de risque : **Haute, Moyen** Ajouter des filtres

**Type de détection**

- ☐ Accès en masse à des fichiers sensibles
- ☐ Activité anormale de l'utilisateur
- ☐ Activité depuis une adresse IP anonyme
- ☐ Adresse IP anonyme
- ☐ Adresse IP de l'acteur de menace vérifiée
- ☐ Adresse IP liée à un programme malveillant
- ☐ Adresse IP malveillante
- ☐ Anomalie de l'émetteur du jeton
- ☐ Attaquant au milieu
- ☐ Informations d'identification fuitées
- ☐ Jeton anormal

Appliquer

## Type de détection

- ☐ Informations d'identification fuitées
- ☐ Jeton anormal
- ☐ L'administrateur a confirmé que cet utilisateur est compromis
- ☐ L'utilisateur a signalé une activité suspecte
- ☐ Modèles d'envoi suspects
- ☐ Navigateur suspect
- ☒ Nouveau pays/nouvelle région
- ☐ Propriétés de connexion inhabituelles
- ☐ Pulvérisation de mot de passe
- ☒ Règles suspectes de manipulation de boîte de réception
- ☐ Tentative possible d'accès au jeton d'actualisation principal (PRT)

Appliquer

# Microsoft Azure



rija@laplateforme841.onmicrosoft.com

## Mettre à jour votre mot de passe

Vous devez mettre à jour votre mot de passe, car vous vous connectez pour la première fois ou votre mot de passe a expiré.

Mot de passe actuel

---

Nouveau mot de passe

---

Confirmer le mot de passe

---

[Se connecter](#)



# Microsoft Azure



rija@laplateforme841.onmicrosoft.com

## Accès impossible pour le moment

Votre connexion a réussi mais ne respecte pas les critères pour accéder à cette ressource. Par exemple, vous vous connectez peut-être à partir d'un navigateur, d'une application ou d'un emplacement restreint(e) par votre administrateur.

[Se déconnecter et se connecter avec un autre compte](#)

[Plus de détails](#)

Utilisateurs   Journaux de connexion								
Laplateforme								
Rechercher	«	Télécharger	Export	Paramètres	Dépanner	Actualiser	Colonnes	Des commentaires ?
Tous les utilisateurs	Date : 7 derniers jours   Afficher les dates au format : Local   Ajouter des filtres							
Journaux d'audit	Connexions utilisateur (interactives)   Connexions utilisateur (non interactives)							
Journaux de connexion								
Diagnostiquer et résoudre les problèmes								
Date	ID de requête	Utilisateur	Application	Statut	Adresse IP	Emplacement	Accès conditionnel	
16/12/2024 17:06:17	dc4ab7ef-abb9-48f3...	Rija	Azure Portal	Interrompu	2a0d:5600:1c4002:b...	Frankfurt Am Main, ...	Opération réussie	