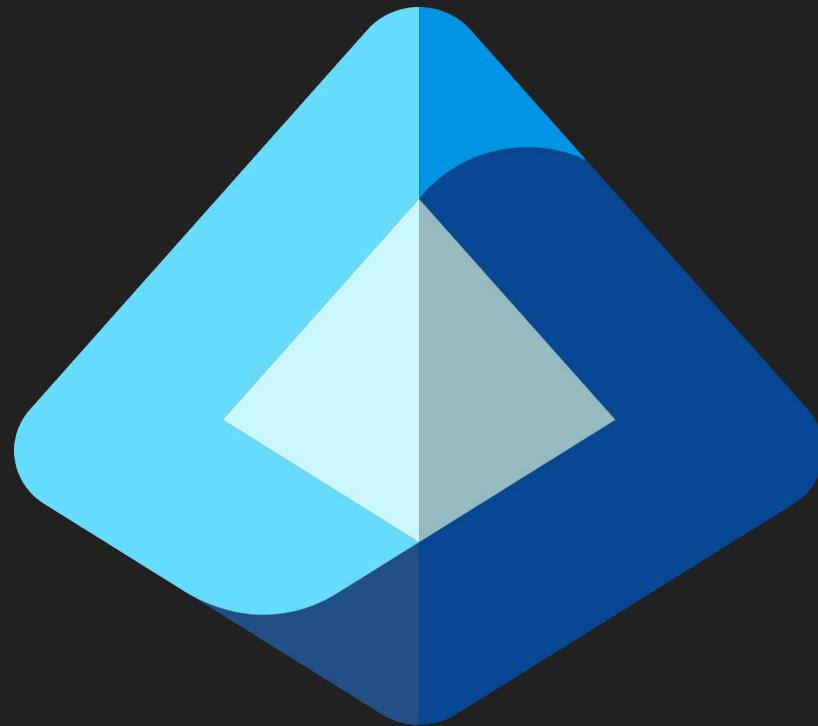




/ Entra ID



Jordan  
Yousef

### Microsoft Azure AD (Entra ID):

- Sécurité Avancée et Politiques de Sécurité
- Automatisation avec PowerShell
- Intégration et Sécurisation des Applications
- Surveillance et Réponse aux Incidents





# PROJET

/ Entra ID

## 1. Sécurité avancée et Politique de sécurité.

### 1.1. Détections et blocages des menaces :

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

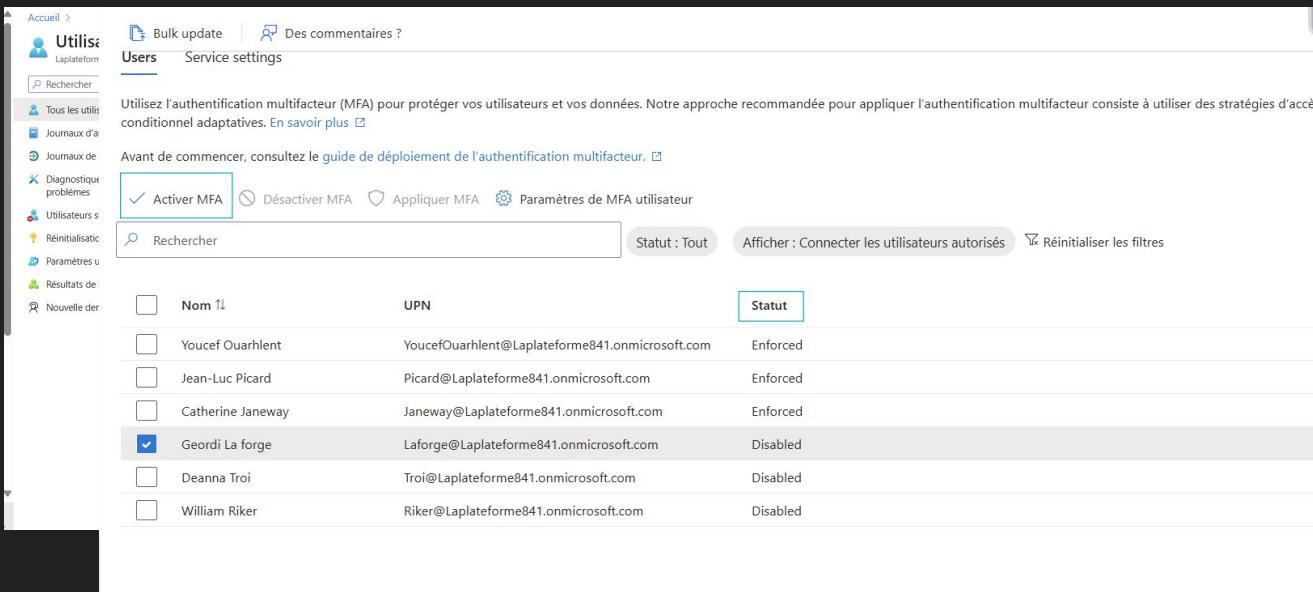
- On commence par se rendre sur le portail <https://portal.azure.com/>

The screenshot shows the Microsoft Azure login interface. At the top, it says "Microsoft Azure" and "Microsoft". Below that, a button says "Continuer vers Microsoft Azure". The main area lists several accounts:

- Youcef Ouarhlent (youcef.ouarhlent@laplateforme841.onmicrosoft.com) - connected
- Really Man (ouarhlenyoucefislam@hotmail.fr) - connected
- Youcef Ouarhlent (youcef.ouarhlent@laplateforme.io) - connected
- Youcef Ouarhlent (youcef.ouarhlent@dominion-global.com) - connected to Windows
- youcef@laplateforme908.onmicrosoft.com
- A plus sign icon with the text "Utiliser un autre compte" (Use another account).

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

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

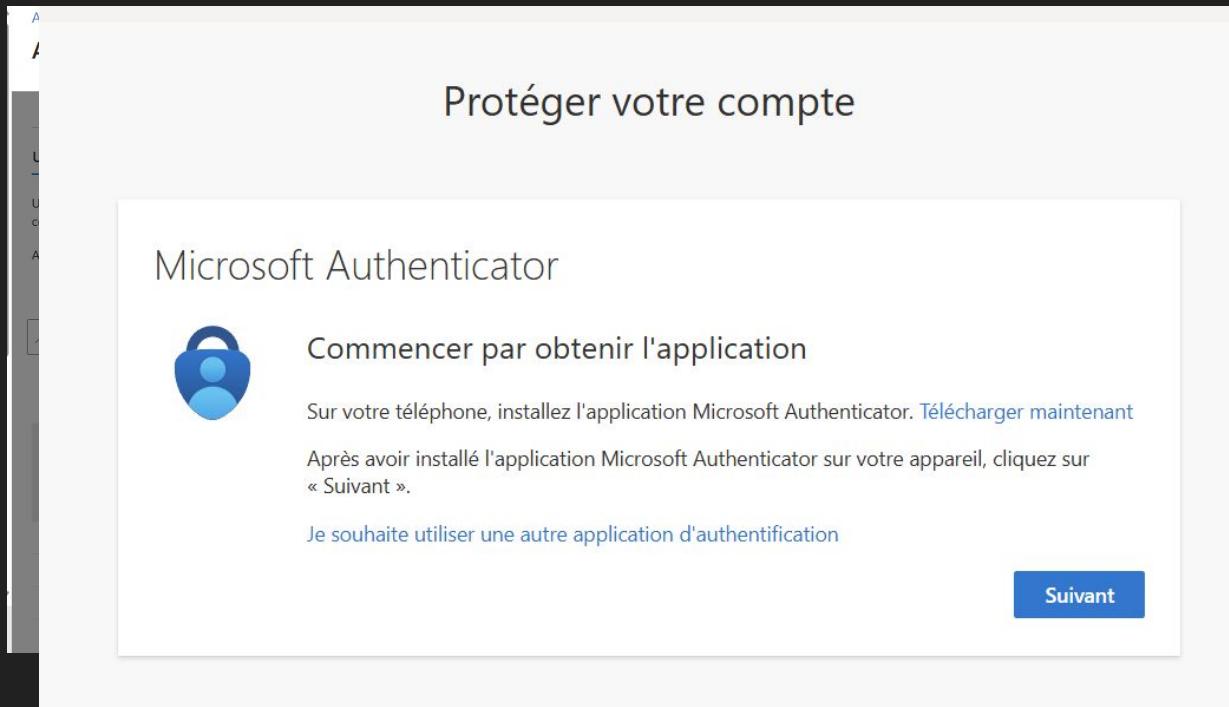


The screenshot shows the Microsoft Entra ID 'Users' page. On the left, there's a sidebar with various navigation links like Accueil, Utilisateurs, Journaux d'audit, Diagnostiquer les problèmes, Utilisateurs spéciaux, Réinitialiser les mots de passe, and Paramètres utilisateurs. The main content area has tabs for Bulk update and Des commentaires ?, with the 'Users' tab selected. A banner at the top encourages using MFA for user and data protection. Below it, a note about adaptive multi-factor authentication strategies is displayed. A section titled 'Avant de commencer...' provides deployment guides. At the bottom of this section, there are buttons for Activer MFA (selected), Désactiver MFA, Appliquer MFA, and Paramètres de MFA utilisateur. A search bar and filter buttons (Statut : Tout, Afficher : Connecter les utilisateurs autorisés, Réinitialiser les filtres) are also present. The main table lists users with columns for Nom, UPN, and Statut. The table shows six users: Youcef Ouarhlent (Enforced), Jean-Luc Picard (Enforced), Catherine Janeway (Enforced), Geordi La forge (Disabled), Deanna Troi (Disabled), and William Riker (Disabled). The row for Geordi La forge is highlighted with a grey background.

Nom	UPN	Statut
Youcef Ouarhlent	YousefOuarhlent@Laplateforme841.onmicrosoft.com	Enforced
Jean-Luc Picard	Picard@Laplateforme841.onmicrosoft.com	Enforced
Catherine Janeway	Janeway@Laplateforme841.onmicrosoft.com	Enforced
Geordi La forge	Laforge@Laplateforme841.onmicrosoft.com	Disabled
Deanna Troi	Troi@Laplateforme841.onmicrosoft.com	Disabled
William Riker	Riker@Laplateforme841.onmicrosoft.com	Disabled

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

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



The screenshot shows a step in the Microsoft Authenticator setup process titled "Protéger votre compte". It displays instructions for obtaining the app on a mobile device and provides an option to use a different authentication application. A "Suivant" button is visible at the bottom right.

Protéger votre compte

Microsoft Authenticator

Commencer par obtenir l'application

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

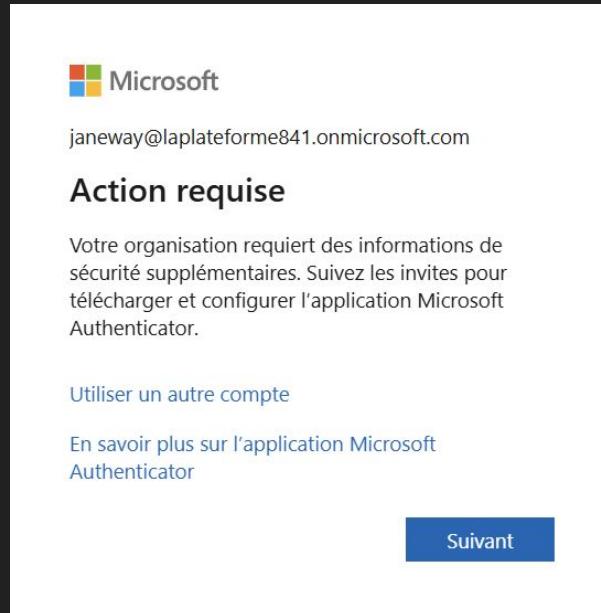
Après avoir installé l'application Microsoft Authenticator sur votre appareil, cliquez sur « Suivant ».

Je souhaite utiliser une autre application d'authentification

Suivant

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

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



# La Plateforme

/ Entra ID

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

The screenshot shows the Microsoft Entra ID Conditional Access overview page. The left sidebar navigation includes Accueil, Nouveautés, Diagnostiquer et résoudre les problèmes, Favoris, Identité, Protection (Identity Protection), and Accès conditionnel (selected). The main content area is titled "Accès conditionnel | Vue d'ensemble" and "Microsoft Entra ID". It features a navigation bar with "Créer une nouvelle stratégie", "Créer une stratégie à partir de modèles", "Actualiser", and "Des commentaires ?". Below this are tabs for Démarrage, Vue d'ensemble (selected), Couverture, Surveillance (préversion), and Tutoriels. A sidebar on the left lists "Stratégies" (selected), Insights et rapports, Diagnostiquer et résoudre les problèmes, Gérer (Emplacements nommés, Contrôles personnalisés (préversion), Conditions d'utilisation, Connectivité VPN, Contextes d'authentification, Points forts d'authentification, Stratégies classiques), Supervision (Journaux de connexion, Journaux d'audit), and Dépannage + support. The main content area displays a summary of the strategy, including an instantané section showing 1 activated strategy, 0 unique reports, and 0 deactivated strategies. It also shows sections for Utilisateurs (0 users connected in the last 7 days), Appareils (0% of connections from non-managed or non-compliant devices), and Applications (listing unprotected applications). A "Nouveautés" section highlights "Emplacements nommés" (IPv6 support) and "Stratégie de gestion des risques internes d'accès conditionnel" (adaptive risk protection profiles). The top right shows the user YoucefOuarhle@laplateforme.onmicrosoft.com.

# La Plateforme

/ Entra ID

- **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.

The screenshot shows the configuration interface for a new conditional access strategy. The strategy name is "Bloquer connexions suspectes". The "Affectations" section is set to "Utilisateurs spécifiques inclus". The "Ressources cibles" section lists "Toutes les ressources (anciennement « Toutes les applications cloud »)". The "Réseau" section is marked as "NOUVEAUTÉ" and specifies "N'importe quel réseau ou emplacement et 1 exclus". Under "Conditions", one condition is selected. In the "Contrôles d'accès" section, the "Activer une stratégie" button is active. The "Utilisateurs et groupes" checkbox is checked. A user named Catherine Janeway is listed under the "Selectionner" section. At the bottom, the "Rapport uniquement" button is active.

INVITES 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

**Selectionner**

1 utilisateur

C Catherine Janeway  
Janeway@Laplateforme841.o... \*\*\*

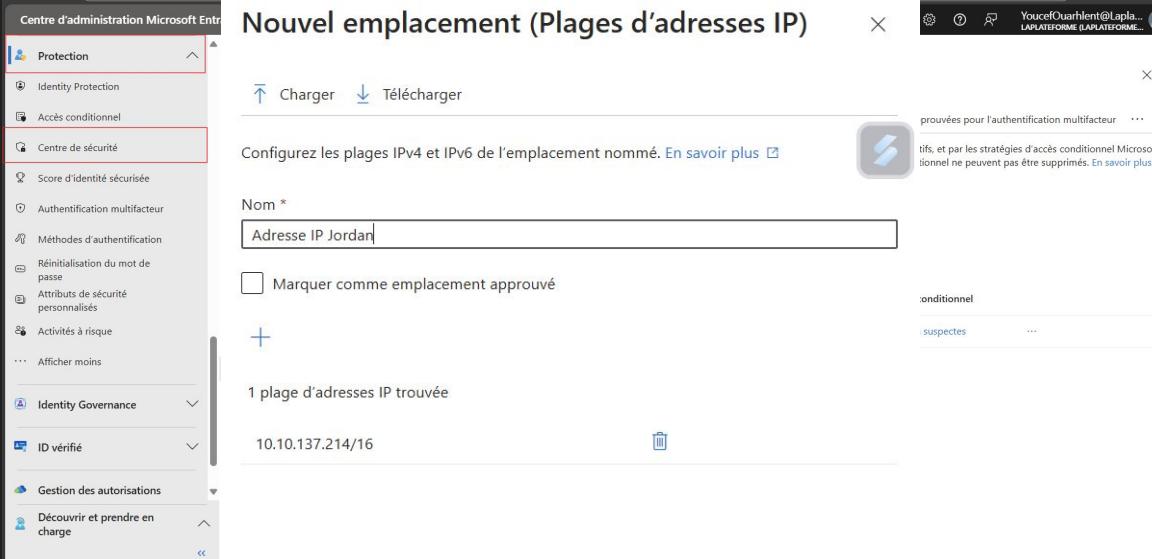
ACTIVER UNE STRATÉGIE

Rapport uniquement **Activé** Désactivé

### 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.



The screenshot shows the 'Nouvel emplacement (Plages d'adresses IP)' (New Location (IP Address Ranges)) configuration page in the Microsoft Entra ID interface. The left sidebar shows the navigation menu with 'Centre de sécurité' highlighted. The main form has the following fields:

- Nom \***: Adresse IP Jordan
- Marquer comme emplacement approuvé**: An unchecked checkbox.
- 1 plage d'adresses IP trouvée**: A table showing one found IP range: 10.10.137.214/16.

At the top right, there is a user profile for YoucefOuarhlent@laplateforme.onmicrosoft.com.

### 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.





## 2. Automatisation avec PowerShell :

```
C:\> Users> archi> Downloads > testps1 > testps1.ps1
File Edit Selection View Go Run Terminal Help ← → ⌘ Search
C:\> Users> archi> Downloads > testps1 > testps1.ps1 | script2.ps1 | script3.ps1
1 # Script pour ajouter un utilisateur à Starfleet via Microsoft Graph
2
3 # Vérifier 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 = $password
28 }
29
30 # Crédit de l'utilisateur
31 try {
32   New-MgUser -AccountEnabled:$true `-
33     -DisplayName $displayName `-
34     -MailNickname $pseudo `-
35     -UserPrincipalName $userPrincipalName `-
36     -PasswordProfile $passwordProfile `-
37     -UsageLocation "FR"
```

To learn more about how to use Git and source control in VS Code [read our docs](#).

Open Folder

Opening a folder will close all currently open editors. To keep them open, [add a folder instead](#).

You can clone a repository locally.

Clone Repository

< OUTLINE > TIMELINE

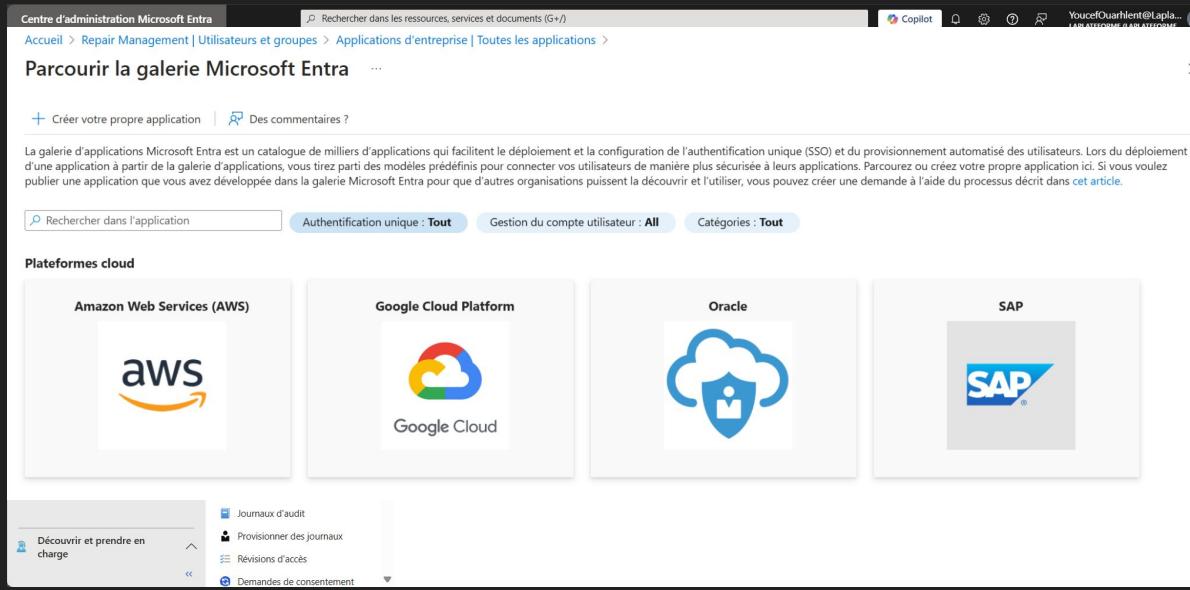
Ln 19, Col 62 Spaces:4 UTF-8 CRLF ⌘ PowerShell ⌘ Go Live ⌘

# Démonstration

### 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.

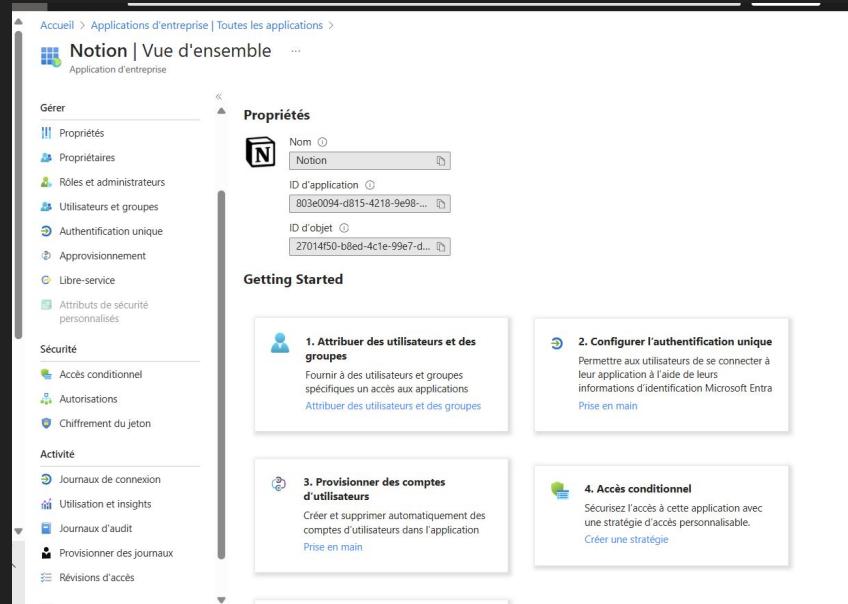


The screenshot shows the Microsoft Entra Admin Center interface. At the top, there's a navigation bar with links for 'Centre d'administration Microsoft Entra', 'Rechercher dans les ressources, services et documents (G+)', 'Copilot', and a user profile. Below the navigation, the page title is 'Accueil > Repair Management | Utilisateurs et groupes > Applications d'entreprise | Toutes les applications >'. A main heading 'Parcourir la galerie Microsoft Entra' is followed by a sub-section 'Plateformes cloud'. Under this section, four cards are displayed: 'Amazon Web Services (AWS)' with the AWS logo, 'Google Cloud Platform' with the Google Cloud logo, 'Oracle' with its logo, and 'SAP' with the SAP logo. At the bottom of the page, there's a sidebar with sections like 'Découvrir et prendre en charge', 'Journaux d'audit', 'Provisionner des journaux', 'Révisions d'accès', and 'Demandes de consentement'.

### 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.

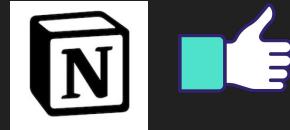


The screenshot shows the 'Properties' section of the Notion application in the Azure AD portal. The application name is 'Notion' (Vue d'ensemble). Key details shown include the application ID (803e0094-d815-4218-9e98-...) and object ID (27014f50-b8ed-4c1e-99e7-d...). The 'Getting Started' section provides four steps for configuration:

- 1. Attribuer des utilisateurs et des groupes**: Fournir à des utilisateurs et groupes spécifiques un accès aux applications. [Attribuer des utilisateurs et des groupes](#)
- 2. Configurer l'authentification unique**: Permettre aux utilisateurs de se connecter à leur application à l'aide de leurs informations d'identification Microsoft Entra. [Prise en main](#)
- 3. Provisionner des comptes d'utilisateurs**: Créez et supprimez automatiquement des comptes d'utilisateurs dans l'application. [Prise en main](#)
- 4. Accès conditionnel**: Sécurisez l'accès à cette application avec une stratégie d'accès personnalisable. [Créer une stratégie](#)

The left sidebar lists other management options like Propriétés, Propriétaires, Rôles et administrateurs, Utilisateurs et groupes, Authentication unique, Approvisionnement, Libre-service, Attributs de sécurité personnalisés, Accès conditionnel, Autorisations, Chiffrement du jeton, Journaux de connexion, Utilisation et insights, Journaux d'audit, Provisionner des journaux, and Révisions d'accès.

Pourquoi Notion comme Journal de Bord ? :



## 1. Centralisation de l'information :

- Organisation flexible : Pages hiérarchisées, bases de données et balises.
- Un espace unique : Regroupez notes, tâches, événements et projets dans un outil collaboratif.

## 2. Collaboration en temps réel :

- Mise à jour instantanée : Travail simultané et synchronisation automatique.
- Commentaires et mentions : Simplifiez les échanges au sein de l'équipe.

## 3. Suivi des activités et historique

- Horodatage des modifications : Suivez l'évolution des entrées.
- Suivi des projets : Catégorisez et gérez l'état d'avancement des tâches.

## 4. Personnalisation et automatisation

- Modèles : Structurez vos entrées avec des templates adaptés.
- Rappels : Configurez des notifications ou intégrez d'autres outils.



# La Plateforme

/ Entra ID

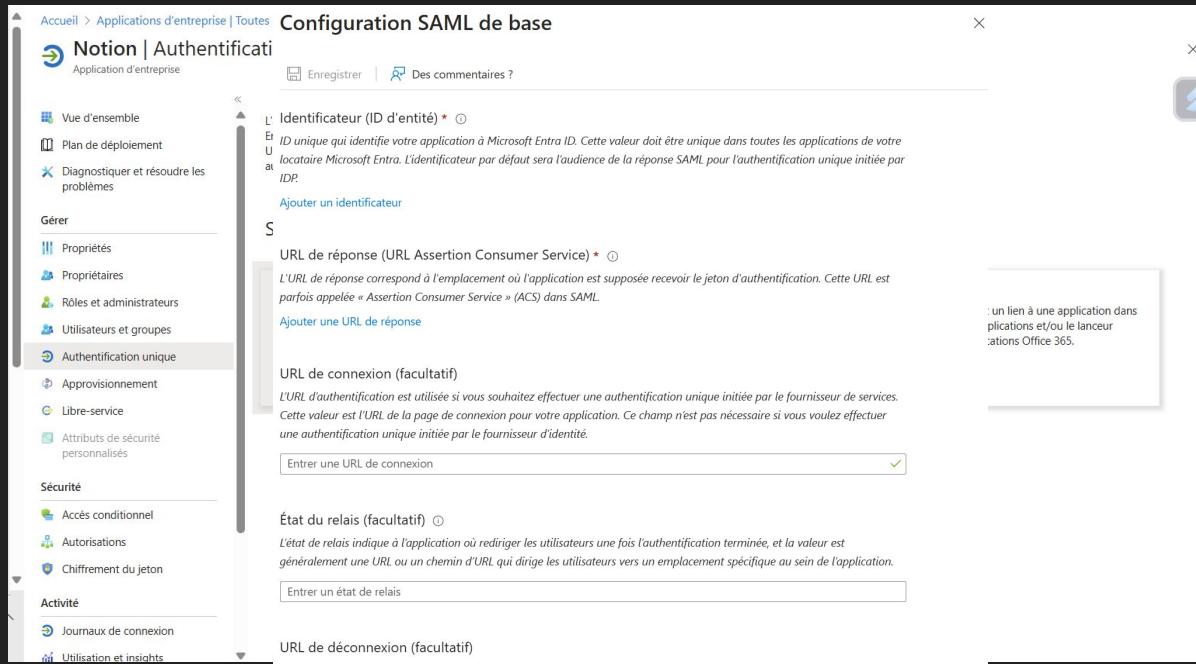
Pourquoi Splunk comme Command Center ? :



- **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) :

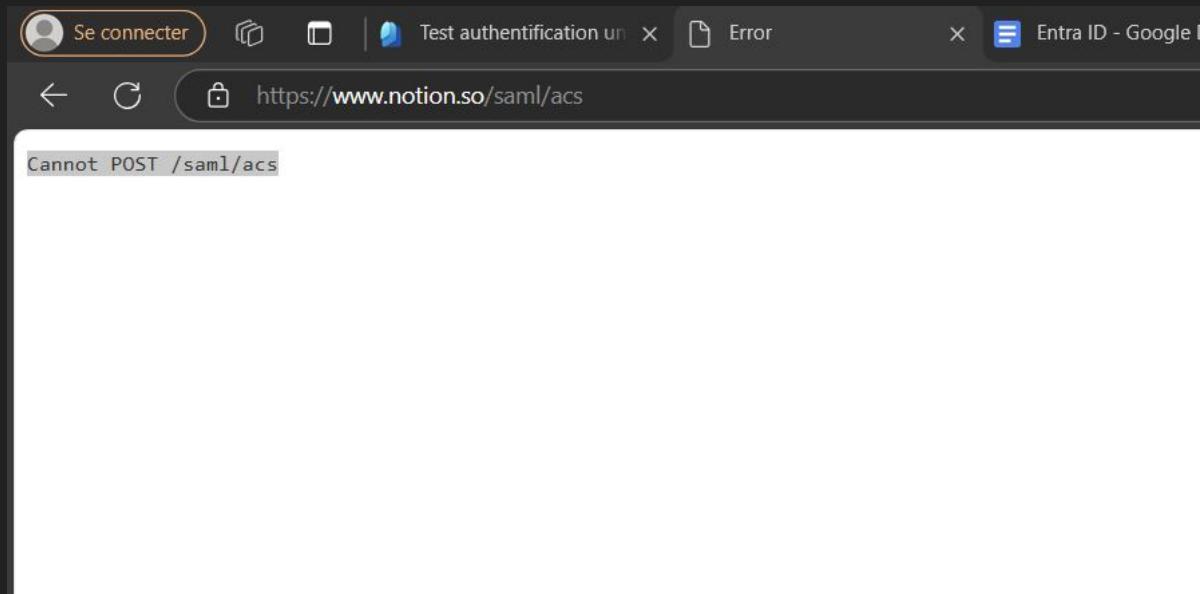
Configuration du SSO pour permettre aux membres d'utiliser leurs identifiants Starfleet.



The screenshot shows the 'Configuration SAML de base' (SAML Base Configuration) page for the 'Notion | Authentification' application in Microsoft Entra ID. The left sidebar lists various configuration sections: Vue d'ensemble, Plan de déploiement, Diagnostiquer et résoudre les problèmes, Gérer (Properties, Owners, Roles and Administrators, Users and groups, Authentication unique), Approvisionnement, Libre-service, Attributs de sécurité personnalisés, Sécurité (Accès conditionnel, Autorisations, Chiffrement du jeton), Activité (Journaux de connexion, Utilisation et insights), and finally Authentication unique (selected). The main content area displays fields for 'Identificateur (ID d'entité)' (Identifier (Entity ID)), 'URL de réponse (URL Assertion Consumer Service)' (Response URL (Assertion Consumer Service URL)), 'URL de connexion (facultatif)' (Optional Connection URL), 'État du relais (facultatif)' (Relay State (Optional)), and 'URL de déconnexion (facultatif)' (Optional Logout URL). A tooltip for 'URL de connexion' indicates it's for users to log in from the provider service. A note at the bottom states that the relay state is optional and typically used for redirecting users after authentication. A right-hand sidebar provides links to other applications and the Office 365 launcher.

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

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



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

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

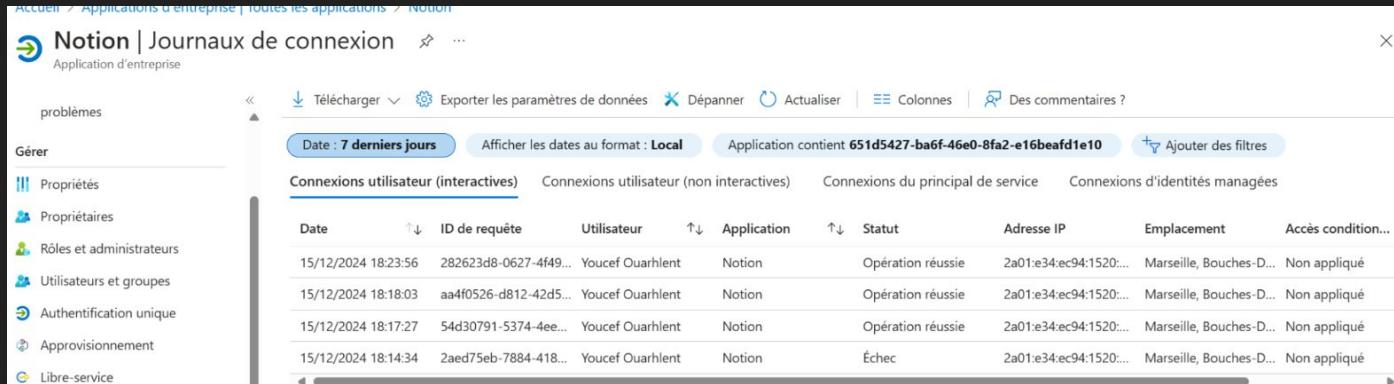


The screenshot shows the Microsoft Azure portal interface for managing enterprise applications. The top navigation bar includes 'Accueil', 'Applications d'entreprise | Toutes les applications', and 'Notion'. The main title is 'Notion | Authentification basée sur SAML'. Below the title, there's a Microsoft logo and the email address 'YoucefOuarhlent@laplateforme841.onmicrosoft.com'. A large button labeled 'Test SAML Single Sign-On' is prominently displayed. A cursor arrow is hovering over this button. Below the button, the text 'Please wait...' is visible. On the left side, there's a sidebar with several options: 'Chiffrement du jeton', 'Activité' (selected), 'Journaux de connexion', and 'Utilisation et insights'. On the right side, there are three columns of mapping details:

Attribut	Élément	Description
lastName	user.surname	
email	user.mail	
l'identificateur unique de l'utilisateur	user.userprincipalname	

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

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



The screenshot shows the Notion Connection Log interface. The top navigation bar includes links for Accueil, Applications d'entreprise, toutes les applications, and Notion. The main title is "Notion | Journaux de connexion". Below the title are various filter and export options. The left sidebar has sections for Gérer (Properties, Owners, Roles and Administrators, Users and Groups, Single Sign-On, Provisioning, and Libre-service). The main content area displays a table of connection logs. The table has columns for Date, ID de requête, Utilisateur, Application, Statut, Adresse IP, Emplacement, and Accès conditionnel. There are four tabs at the top of the table: Connexions utilisateur (interactives), Connexions utilisateur (non interactives), Connexions du principal de service, and Connexions d'identités managées. The first tab is selected. The table shows five rows of data, all of which are successful logins from the user "Youcef Ouarhlent" using the application "Notion".

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

### 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.

#### Créer votre propre application

Accueil > Repair Management

### Repair Management | Utilisateurs et groupes

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

Ajouter un utilisateur/groupe | Modifier l'affectation | Supprimer | Mettre à jour les informations d'identification | Colonnes | Des commentaires ?

L'application apparaît dans Mes applications pour les utilisateurs attribués. Définissez « Visible pour les utilisateurs ? » sur Non dans les propriétés pour empêcher ceci. →

Attribuez ici des utilisateurs et des groupes à des rôles d'application pour votre application. Pour créer des rôles d'application pour cette application, utilisez l'[inscription de l'application](#).

Nom d'affichage	Type d'objet	Rôle attribué
<input type="checkbox"/> Ingénierie	Groupe	User

Intégrer une autre application que vous ne trouvez pas dans la galerie (non galerie)

### 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.



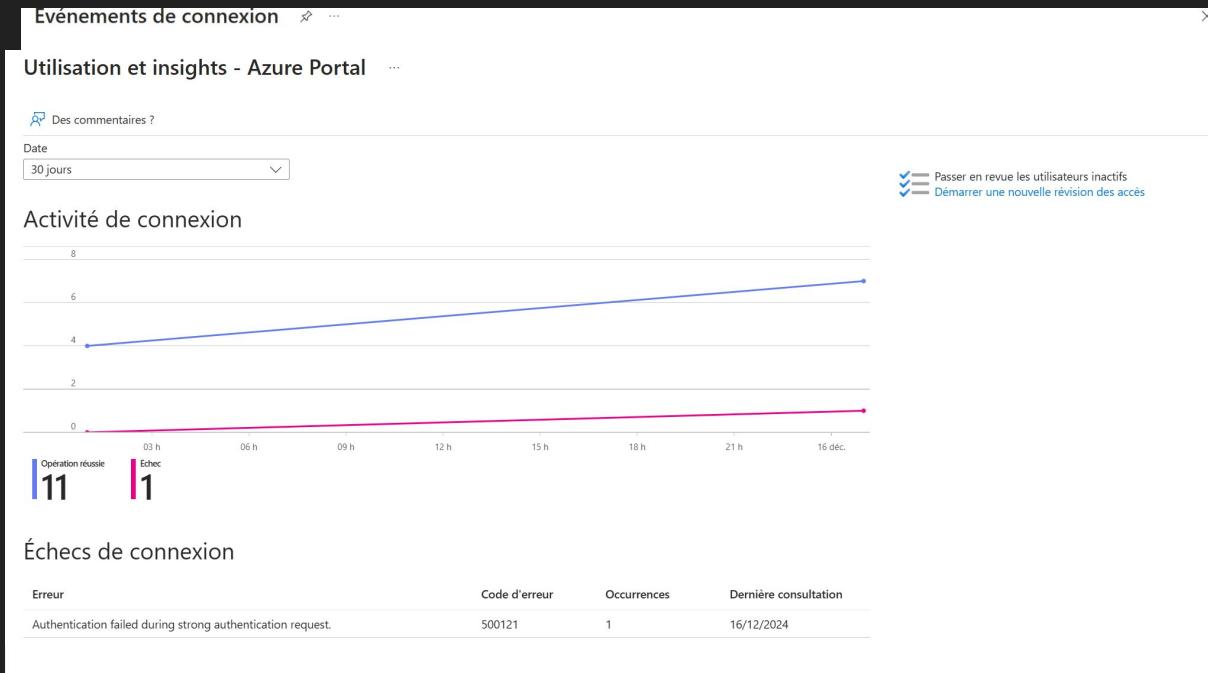
The screenshot shows the 'Repair Management | Rôles et administrateurs' page in the Microsoft Entra ID interface. The left sidebar lists various management options like 'Vue d'ensemble', 'Plan de déploiement', and 'Rôles et administrateurs'. The main content area displays a table of roles:

Rôle	Description	Privilégié	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	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 :

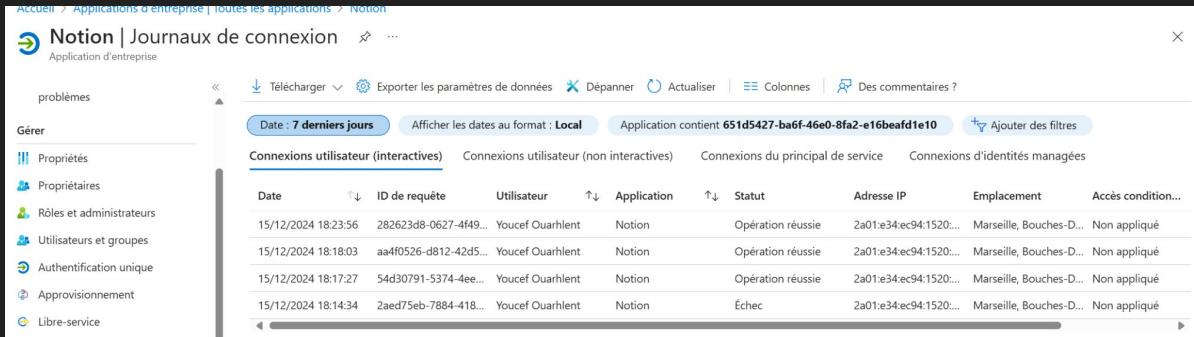
Observation des tentatives d'accès aux données critiques des missions.



## 4. Surveillance et Réponse aux Incidents

### 4.1 Surveillance des Données Sensibles :

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



The screenshot shows a Notion application interface titled "Notion | Journaux de connexion". The left sidebar has sections for "problèmes", "Gérer", and a list of items: Propriétaires, Rôles et administrateurs, Utilisateurs et groupes, Authentification unique, Approvisionnement, and Libre-service. The main area displays a table of connection logs with the following data:

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



/ Entra ID

## 4.2 Analyse des Logs :

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

The screenshot shows the Microsoft Azure Audit Logs interface. The top navigation bar includes 'Microsoft Azure', 'Rechercher dans les ressources, services et documents (G+ /)', 'Copilot', and a user profile 'YoucefOuarhle... LAPPLATEFORME (LAPPLATEFORME...)'. The main title is 'Utilisateurs | Journaux d'audit' under 'Laplateforme'. The left sidebar lists audit categories: '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', and 'Nouvelle demande de support'. The main content area displays a table of audit logs with the following data:

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, YoucefOuarhle...@...	YoucefOuarhle...@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		9f428748a15741d58ed3fe...	YoucefOuarhle...@Laplatef...
15/12/2024 15:38:10	Core Directory	UserManagement	Add user	Success		raj@Laplateforme841.on...	Microsoft Graph Comman...
15/12/2024 15:08:41	Core Directory	UserManagement	Add app role assignment ...	Success		Microsoft Graph Comman...	YoucefOuarhle...@Laplatef...
15/12/2024 15:08:26	Core Directory	UserManagement	Update user	Success		YoucefOuarhle...@Laplatef...	Azure MFA StrongAuthenti...



## 4.2 Analyse des Logs :

Log Analytics (dans Azure Monitor) permet de collecter, analyser et visualiser des journaux provenant de sources comme Microsoft Entra ID, machines virtuelles et services cloud.

Principales fonctionnalités :

- Analyse centralisée des journaux.
- Requêtes avancées pour détecter des anomalies.
- Alertes personnalisées.
- Tableaux de bord interactifs.

Vous n'avez pas accès ...



Intégration Log Analytics non activée

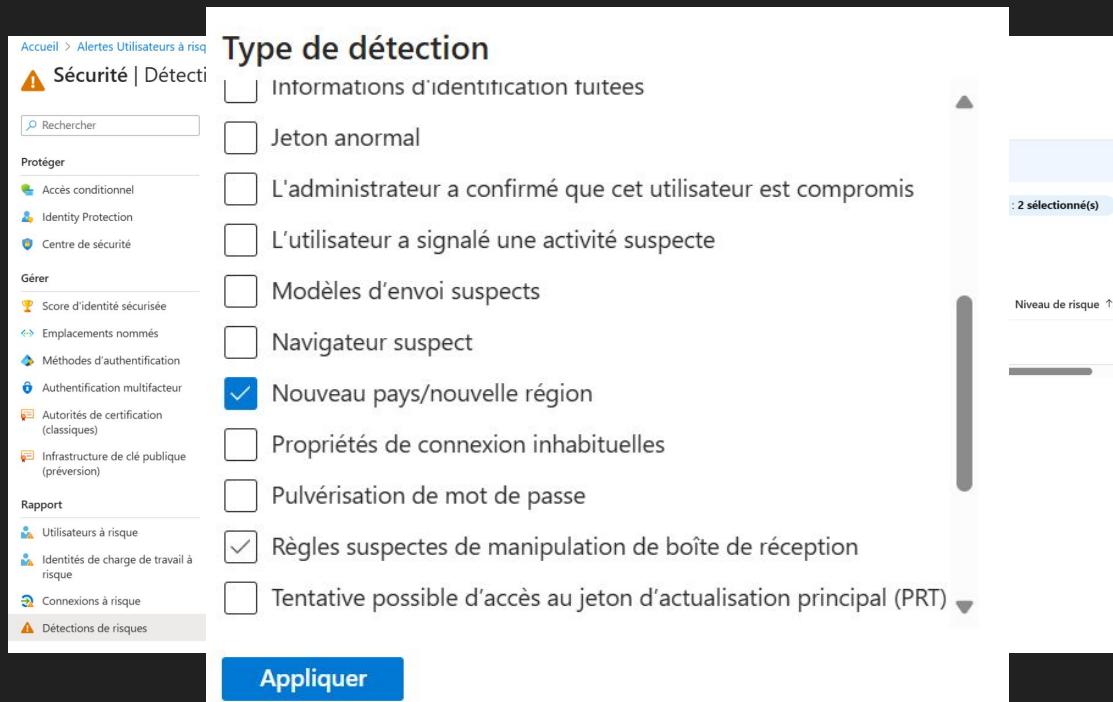
Ce locataire Microsoft Entra n'est pas activé actuellement pour envoyer des journaux à Log Analytics. Cliquez sur le lien ci-dessous pour savoir comment activer cette fonctionnalité.

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

Récapitulatif	Actions
ID de session cb177577c12842fe9c1fe7a4f75c0078	ID de ressource Non disponible
Extension Microsoft_AAD_JAM	Contenu NewLogAnalyticsBlade
Code d'erreur 403	

### 4.3 Alertes en Temps Réel :

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



The screenshot shows a configuration page for real-time alerts. On the left, a sidebar lists categories like Sécurité, Protéger, Gérer, and Rapport. The main area is titled "Type de détection" and lists various detection types with checkboxes. Two checkboxes are checked: "Nouveau pays/nouvelle région" and "Règles suspectes de manipulation de boîte de réception". A blue "Appliquer" button is at the bottom.

Accueil > Alertes Utilisateurs à risque

**Sécurité | Détection**

Rechercher

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 (préversion)

Rapport

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

Type de détection

- Informations d'identification tuitees
- 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)

2 sélectionné(s)

Niveau de risque ↑↓

Appliquer

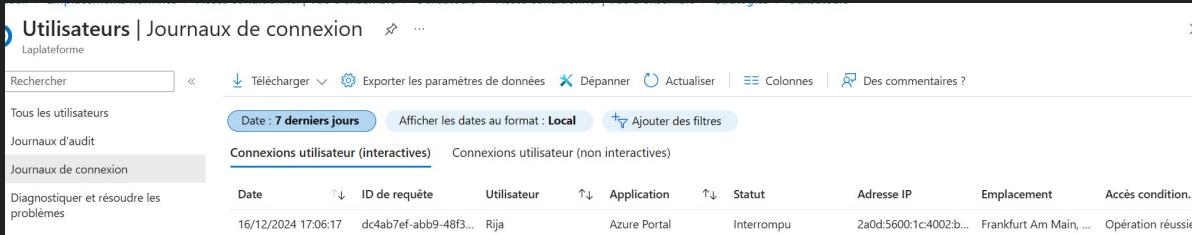
#### 4.3 Alertes en Temps Réel :

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



### 4.3 Alertes en Temps Réel :

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



The screenshot shows a table of connection logs. The columns are: Date, ID de requête, Utilisateur, Application, Statut, Adresse IP, Emplacement, and Accès condition... . The single visible row is: 16/12/2024 17:06:17, dc4ab7ef-abb9-48f3..., Rija, Azure Portal, Interrrompu, 2a0d:5600:1c:4002:b..., Frankfurt Am Main, ... Opération réussie.

Date	ID de requête	Utilisateur	Application	Statut	Adresse IP	Emplacement	Accès condition...
16/12/2024 17:06:17	dc4ab7ef-abb9-48f3...	Rija	Azure Portal	Interrrompu	2a0d:5600:1c:4002:b...	Frankfurt Am Main, ...	Opération réussie