**Sécurisation de l'Infrastructure de l'USS**

**Enterprise avec EntraID AD**

**Objectifs :**

* Renforcer la sécurité avec des politiques avancées.
* Automatiser la gestion des utilisateurs et des groupes via PowerShell.
* Intégrer et sécuriser des applications.
* Détecter et répondre aux incidents de sécurité.

1. **Sécurité Avancée et Politiques de Sécurité**
2. **Mettre en place des politiques pour détecter et bloquer les attaques**

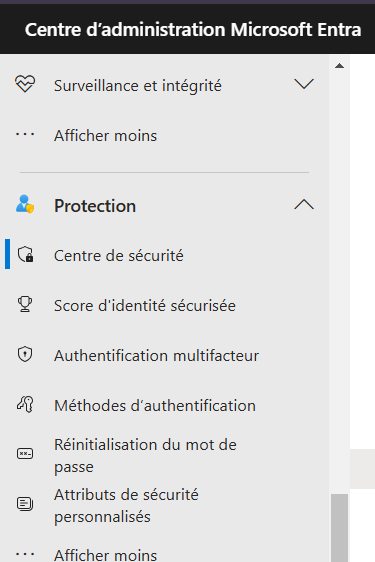
**contre les identités des membres d'équipage.**

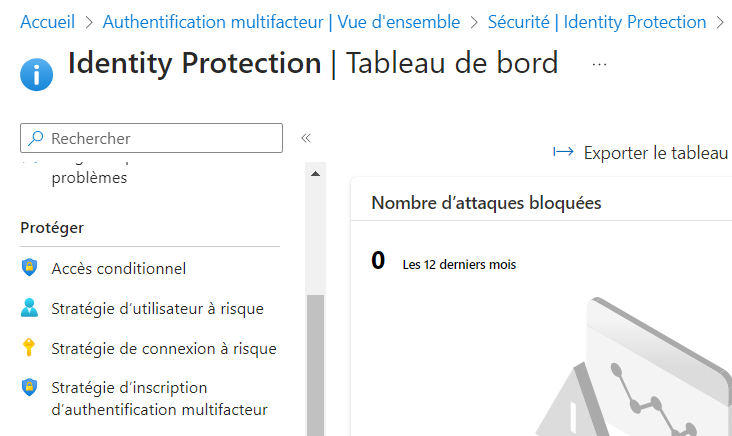
Pour mettre en place une politique de détection et de blocage des attaques contre identités des membres d'équipage dans **Microsoft Entra ID**, il faut créer une **politique d’accès conditionnel** et utiliser les **stratégies de protection des identités** pour détecter et réagir face aux tentatives de connexion suspectes.

### **Étapes à suivre :**

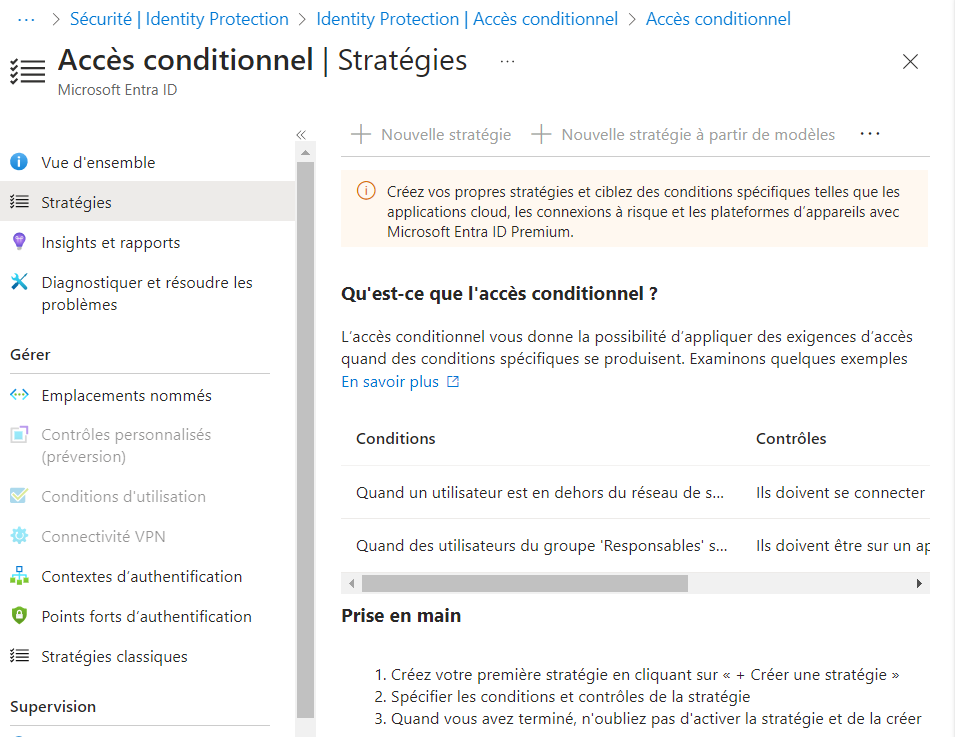
1. **Accéder à Microsoft Entra ID et au menu Accès Conditionnel**
   * On commence par se connecter au **Portail Azure** (<https://portal.azure.com>).
   * Ensuite, on va dans **Microsoft Entra ID** > **Sécurité** > **Accès conditionnel** pour lancer la création d'une nouvelle stratégie.

Chemin pour la Nouvelle version Centre administration entra ID, on se rend sur la gauche Protection > afficher plus … > centre de sécurité

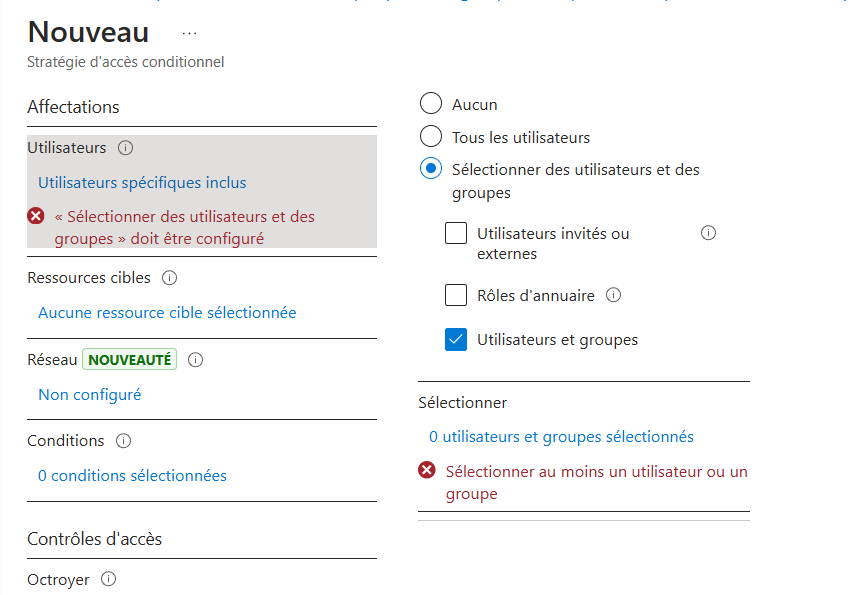


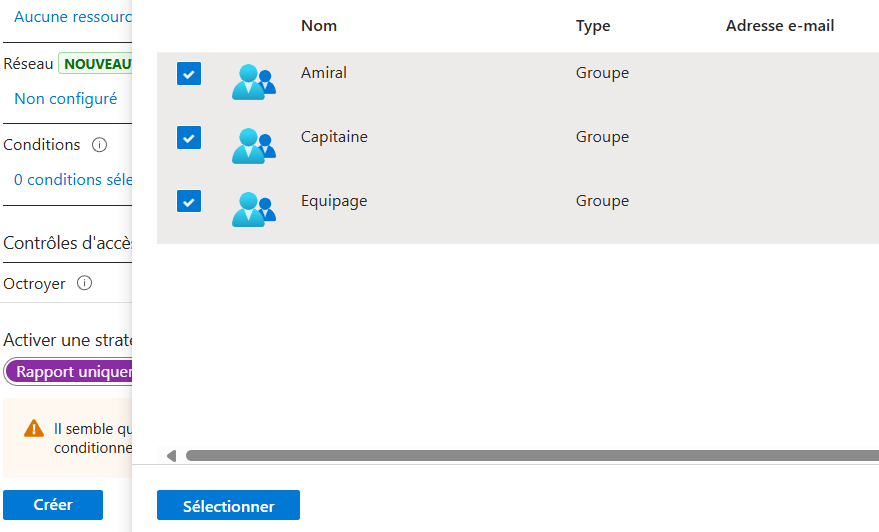


1. **Créer une nouvelle stratégie d’accès conditionnel**
   * Dans **Accès conditionnel**, on clique sur **Nouvelle stratégie** pour configurer la politique.
   * On donne un nom clair et descriptif, comme "Détection et blocage des attaques sur les identités des membres d’équipage".

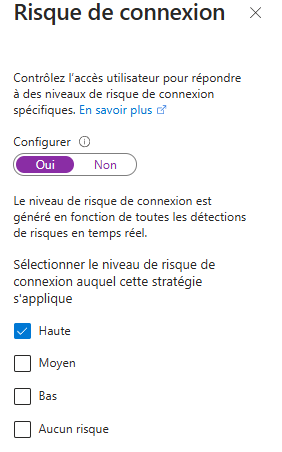
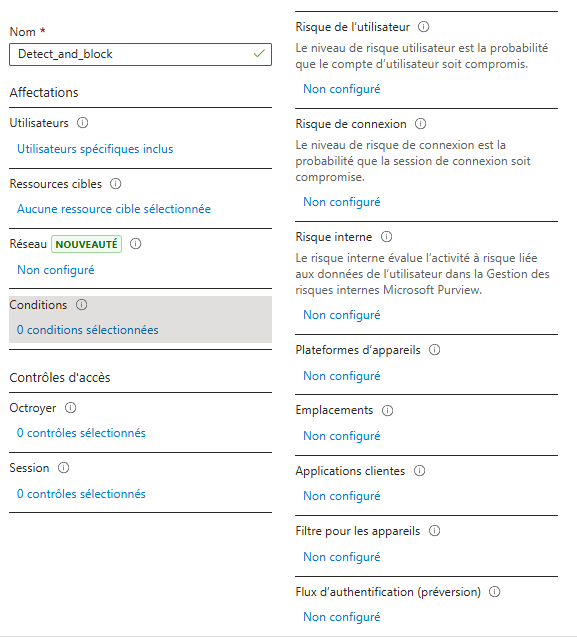


1. **Définir les utilisateurs et groupes concernés**
   * Dans **Affectations** > **Utilisateurs et groupes**, on sélectionne les membres d'équipage ou groupes auxquels cette politique s’appliquera.

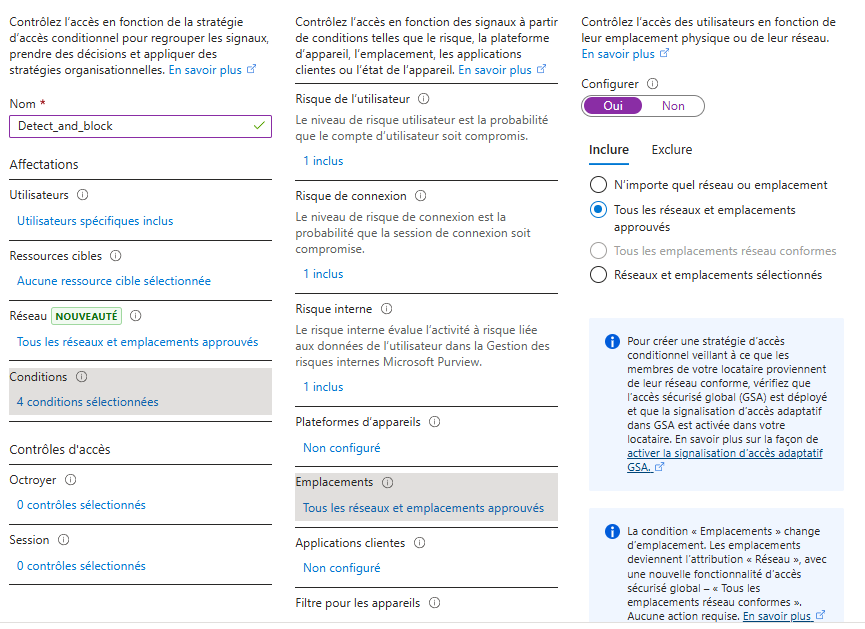




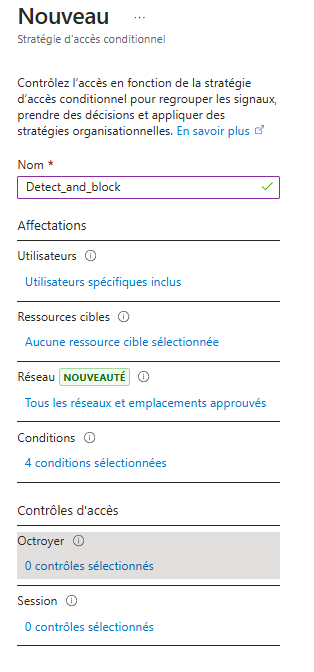
1. **Configurer les conditions de détection des risques**
   * **Signaux de risque** : Dans **Risque d’utilisateur** et **Risque de connexion**, on sélectionne des niveaux de risque (Moyen ou Élevé) pour que la politique se déclenche selon des critères de sécurité spécifiques.



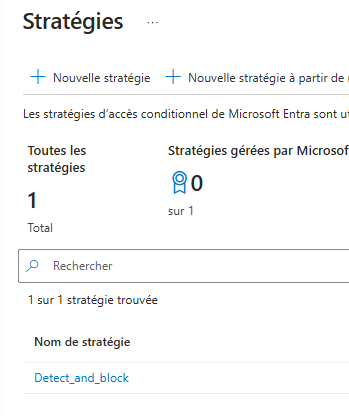
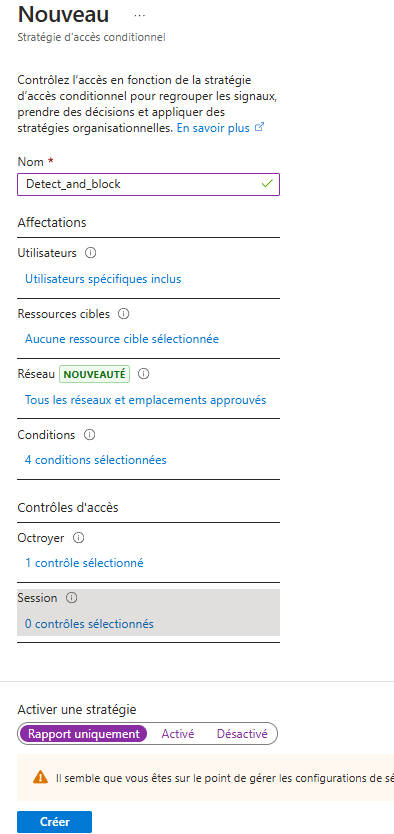
* + **Emplacements** : On peut restreindre les connexions aux **emplacements approuvés**, ce qui bloque l'accès depuis des zones non sécurisées.



1. **Définir les contrôles d’accès**
   * On peut choisir de **bloquer l’accès** ou de **demander une authentification multifacteur (MFA)** en fonction du niveau de risque détecté.



1. **Activer et tester la politique**
   * Avant le déploiement, on recommande d’activer la politique en **Mode d’audit** ou **Report Only** pour observer les résultats sans bloquer les accès. Si le test est concluant, on active pleinement la politique.



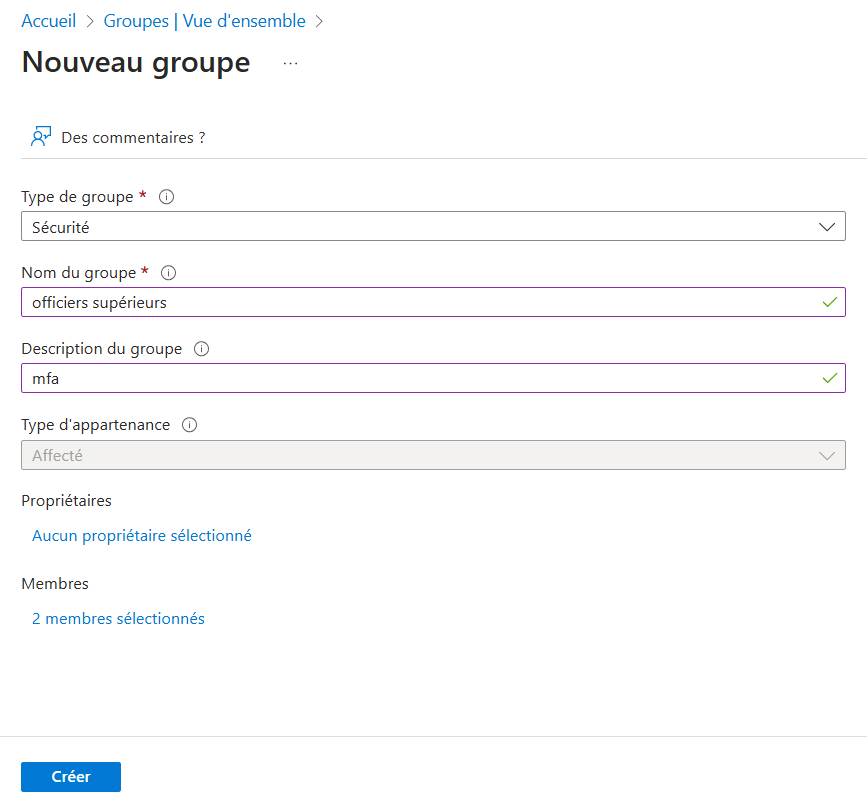
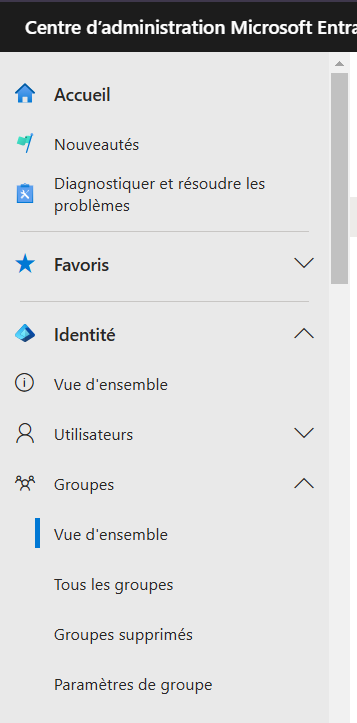
Cette configuration dans **Microsoft Entra ID** permet de renforcer la sécurité des identités des membres d’équipage et de bloquer proactivement les tentatives de connexion suspectes.

1. **Activez MFA pour tous les officiers supérieurs afin de sécuriser l'accès**

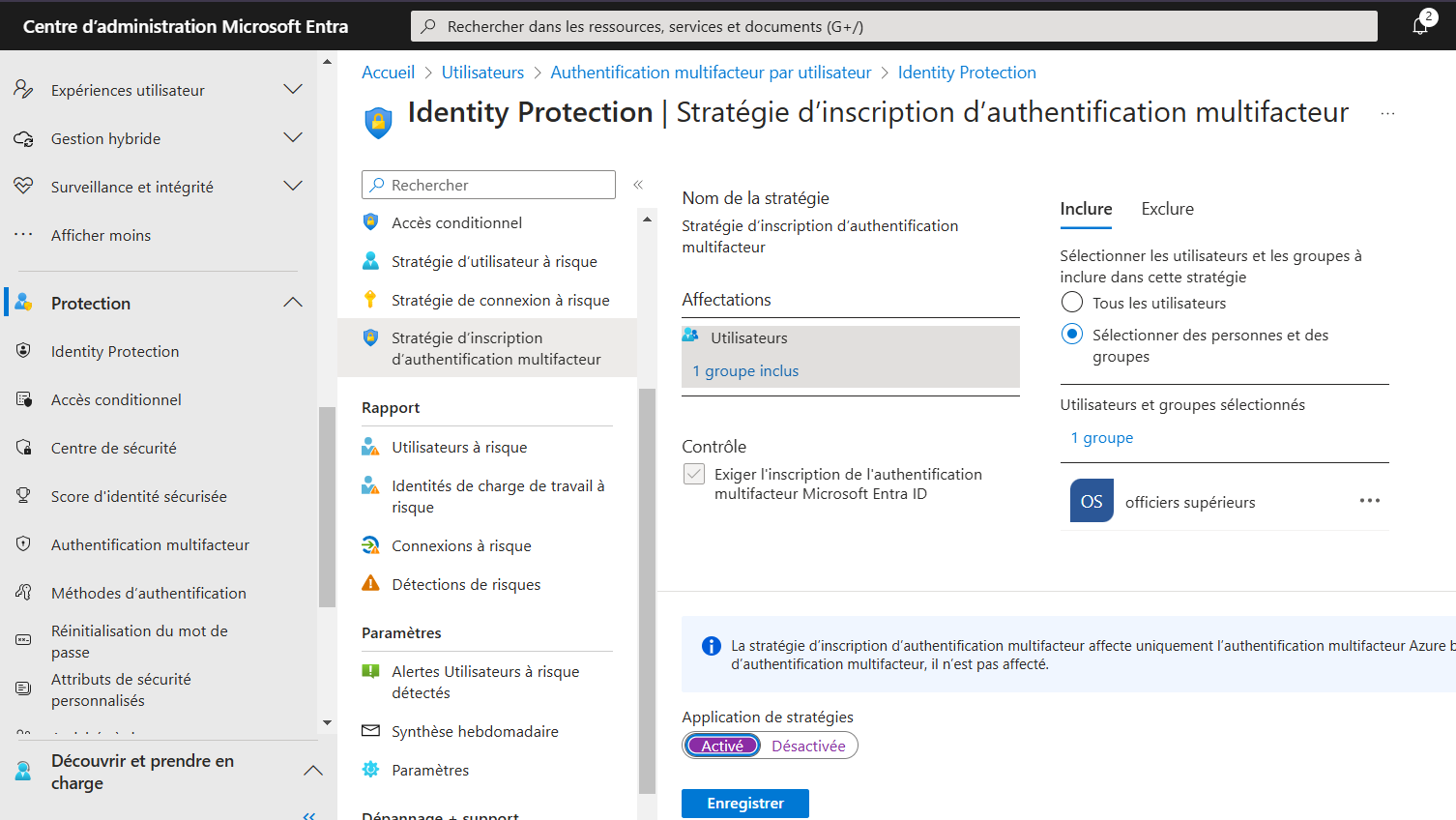
**aux données sensibles de Starfleet.**

Pour activer l’authentification multifacteur (MFA) pour tous les officiers supérieurs, voici les étapes à suivre.

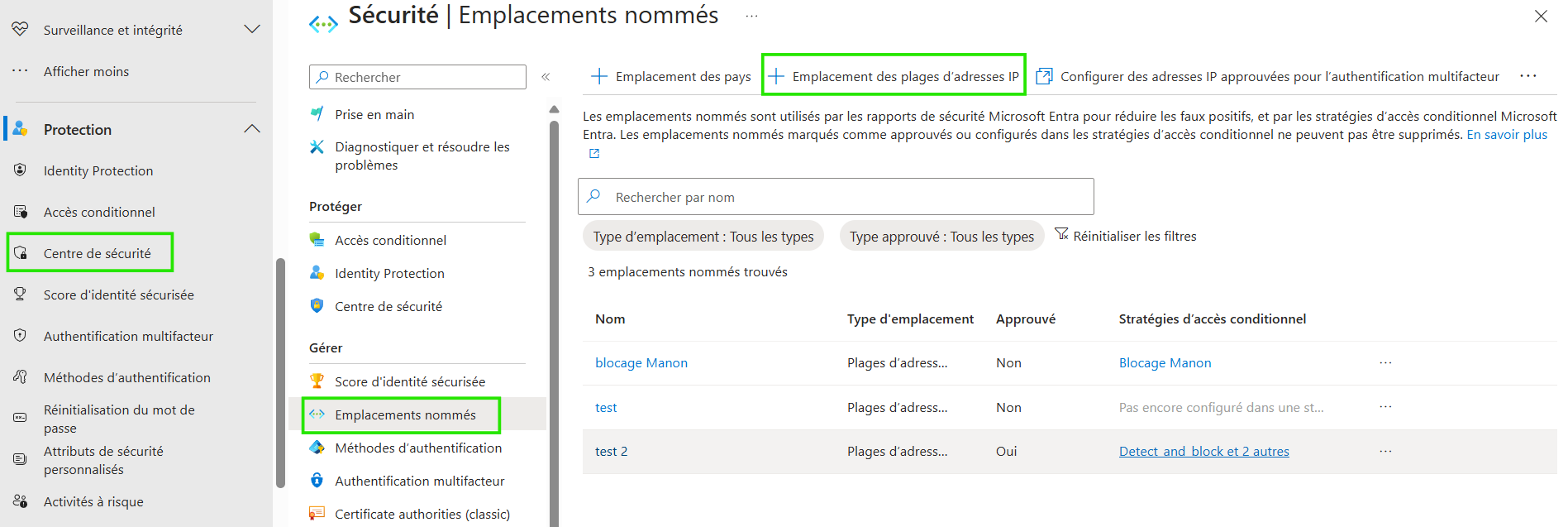
On commence par créer un groupe pour “ les officiers supérieurs” donc on se rend sur **microsoft entra id > groupes> vue d’ensemble** puis **créer un nouveau groupe**

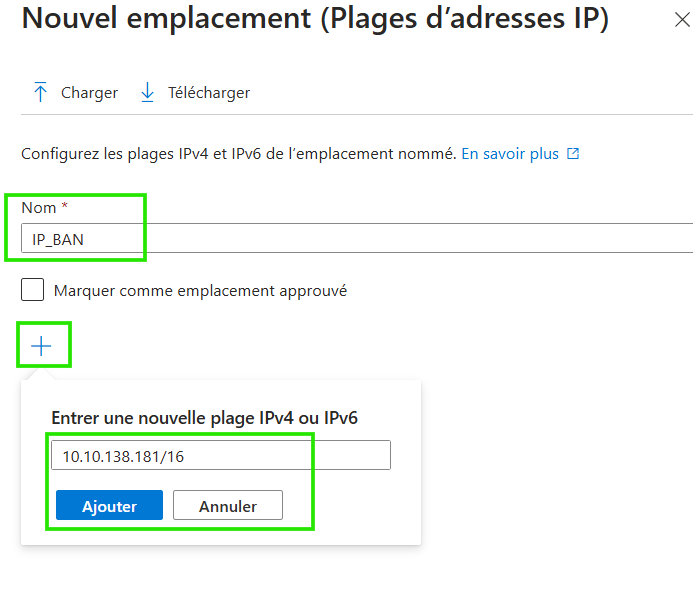


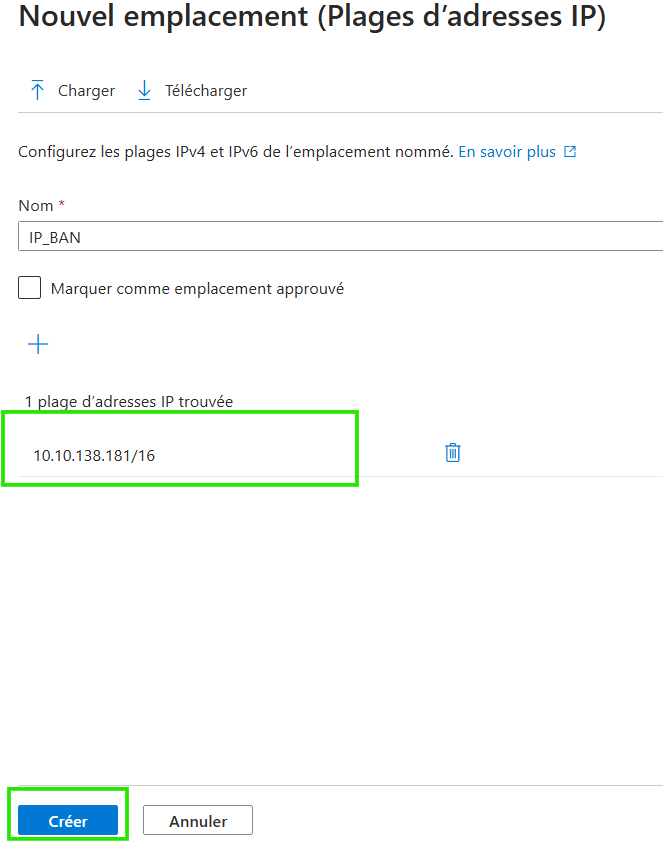
Maintenant que notre groupes est créé avec les utilisateurs correspondants, on se rend dans l’onglet **Protection > Identity Protection > stratégie d’inscription d’authentification multifacteur**



1. **Créez des politiques d'accès pour restreindre les connexions depuis des emplacements non autorisés comme des planètes non sécurisées ou des vaisseaux inconnus.**

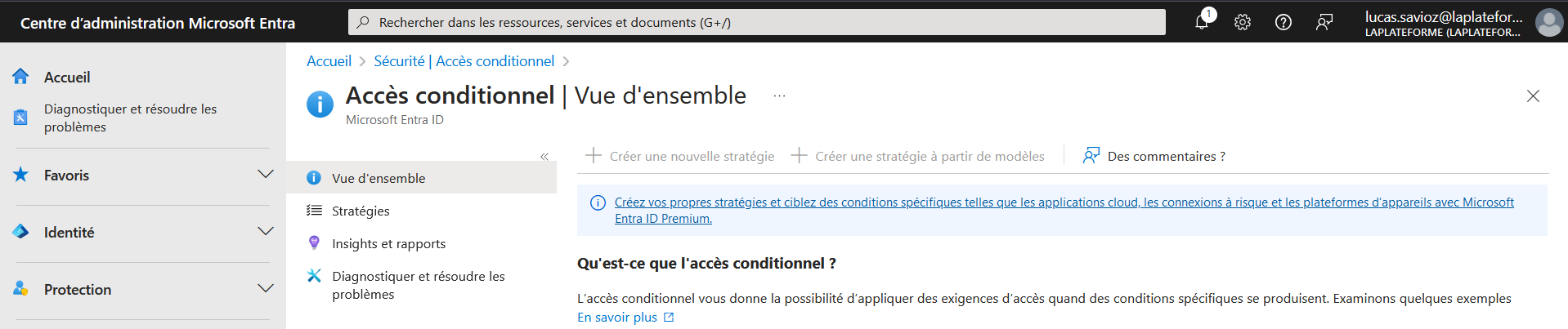
Pour cet exercice, nous allons restreindre l’accès via une adresse IP. Mais avant de créer cette stratégie, on va ajouter une plage d’adresse IP.  
Pour ce faire, aller dans **Protection>Centre de sécurité>Emplacement des plages d’adresses IP.**  


Ajoutez votre plage d’adresse IP et le nom de la plage.  


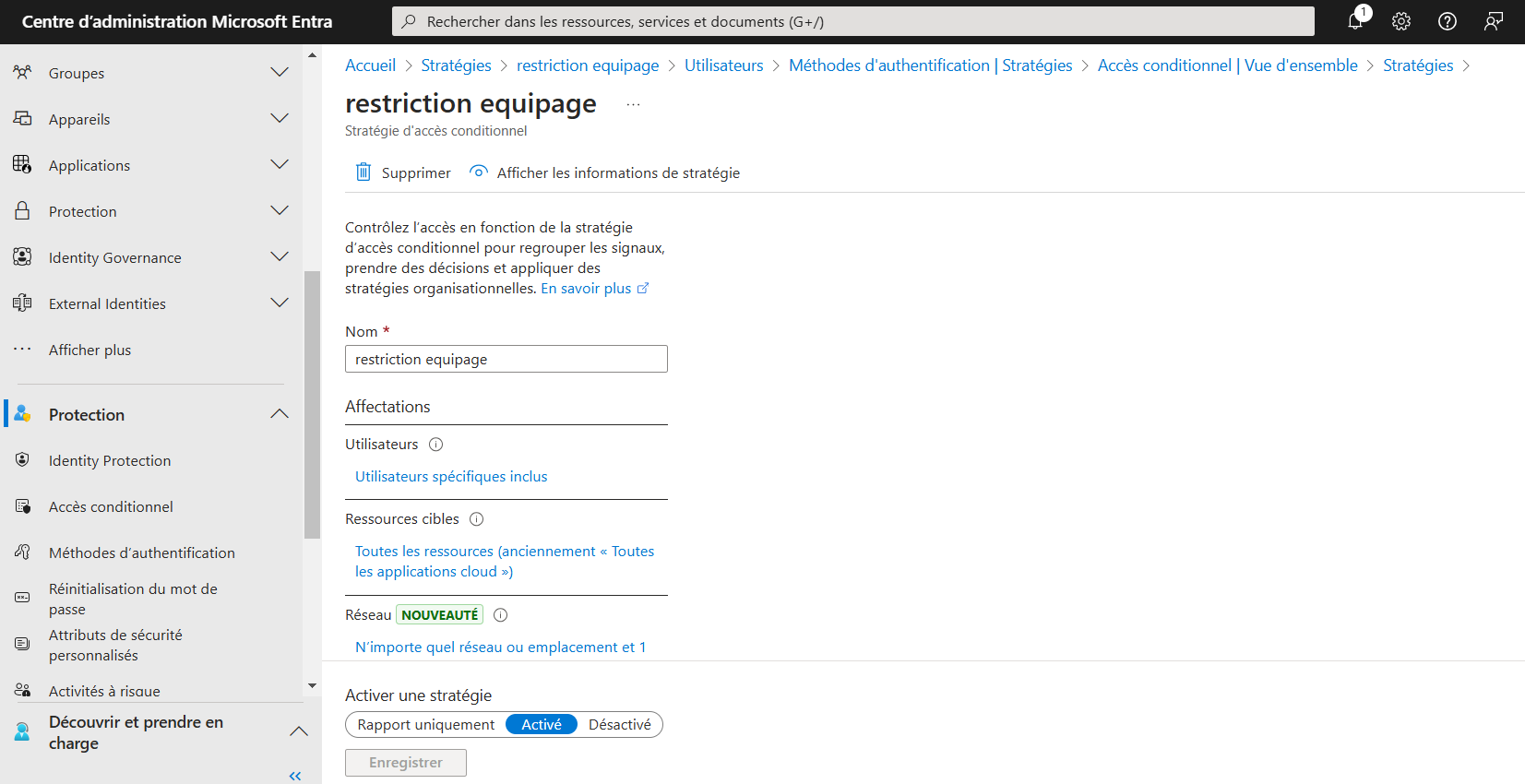
Puis créer.  


Pour restreindre les connexions, on a besoin de créer une nouvelle stratégie restrictive.

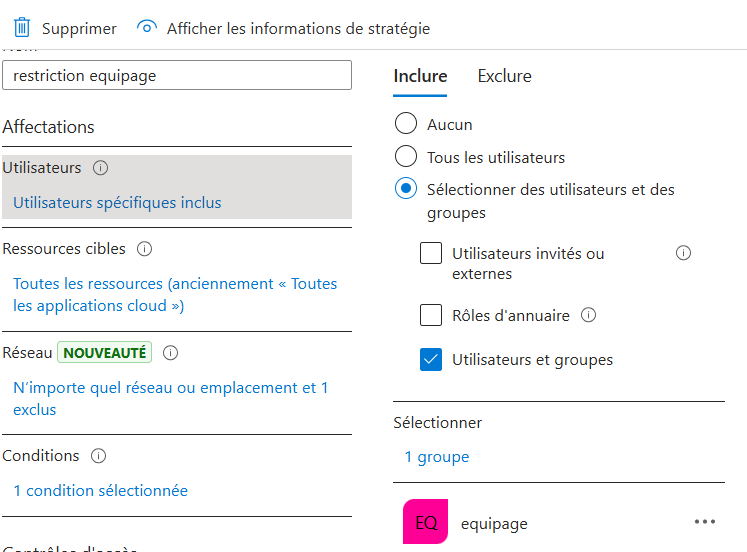
Aller dans : **Microsoft Entra ID > Sécurité > Accès conditionnel > Créer une nouvelle stratégie.**



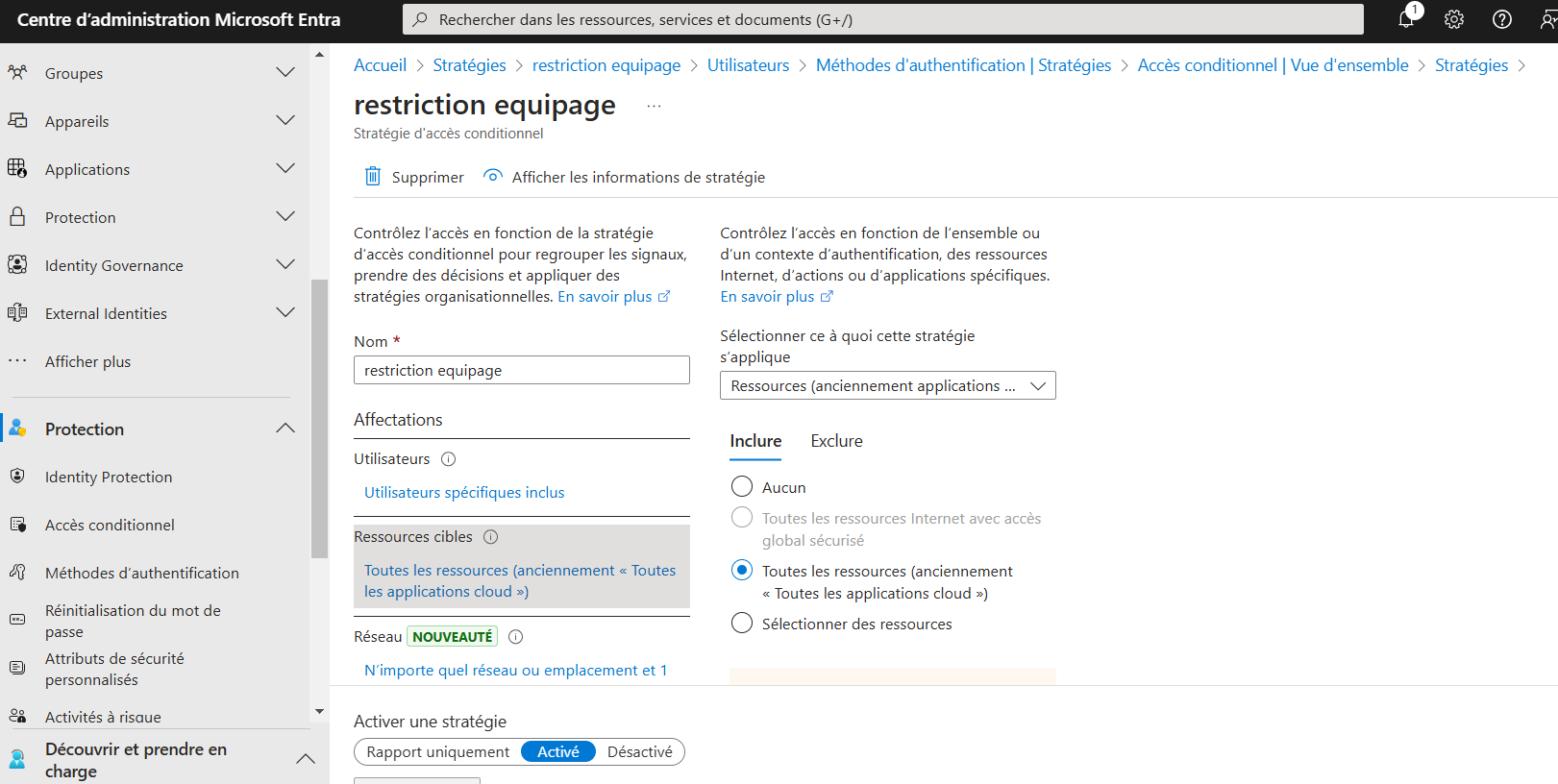
Donnez un nom descriptif à la stratégie : "Restreindre Connexions Equipages."



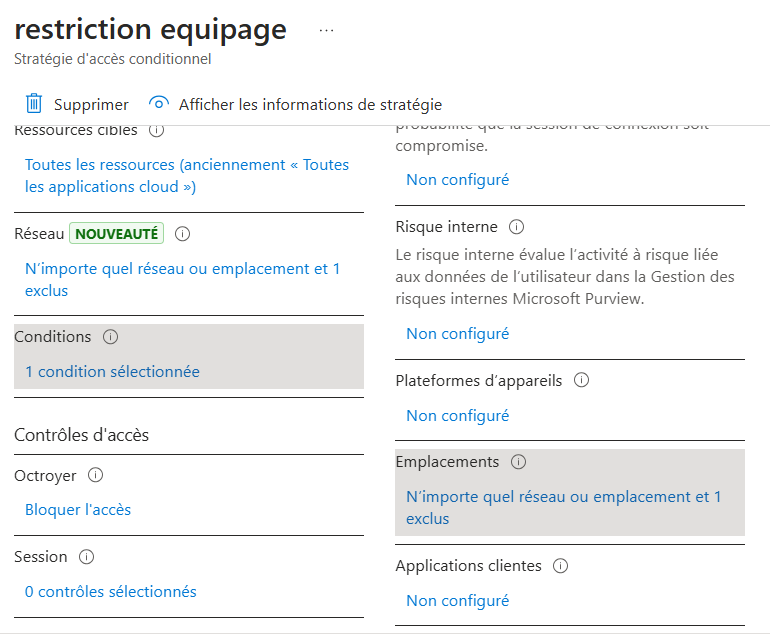
Ensuite, on s’occupe des affectations. On commence par les utilisateurs, nous allons inclure les utilisateurs concernés par notre restriction dans cet exemple nous avons créer le groupe équipage pour restreindre la connexion comprenant Deanna, jordi



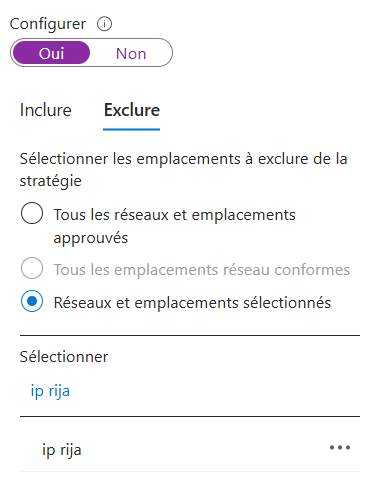
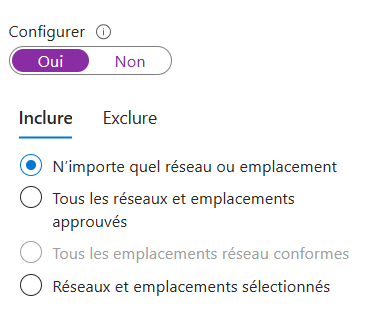
Après On s’occupe d’affecter les ressources cibles,



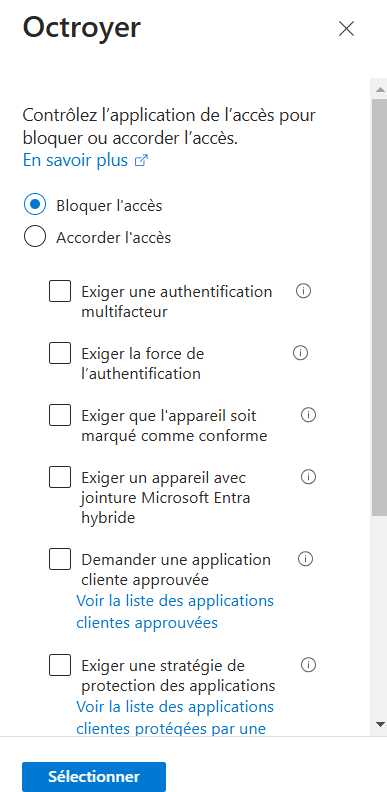
Puis les conditions, on se rend dans “emplacement”



on configure inclure et exclure de la manière suivante:



et on termine sur octroyer ou l’on bloque l’accès.



Résultat de la restriction de connexion avec l’un des utilisateurs



**2. Automatisation avec PowerShell**

**● Créez des scripts pour automatiser la gestion des utilisateurs, , ajouter**

**des nouvelles recrues de Starfleet ou des transferts d'autres vaisseaux.**

Pour automatiser la gestion des utilisateurs dans Microsoft Entra ID avec PowerShell, nous allons utiliser le module **Microsoft Graph PowerShell** (anciennement Azure AD PowerShell) pour créer des scripts qui ajoutent des utilisateurs, gèrent leurs informations, et facilitent le transfert ou l’ajout de nouvelles recrues.

Commande pour installer le module Microsoft Graph PowerShell :

**Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope CurrentUser**

* **Objectif** : Cette commande définit la politique d'exécution de PowerShell pour permettre l'exécution de scripts téléchargés depuis des sources distantes s'ils sont signés par un éditeur de confiance.
* **Options** :
  + **-ExecutionPolicy RemoteSigned** : Autorise l'exécution de scripts locaux non signés, mais exige que les scripts téléchargés à distance soient signés.
  + **-Scope CurrentUser** : Applique cette politique uniquement à l'utilisateur actuel, sans affecter les autres utilisateurs sur la machine.

**Install-Module Microsoft.Graph -Scope CurrentUser -Repository PSGallery -Force**

* **Objectif** : Installe le module Microsoft.Graph pour PowerShell, qui permet d'interagir avec l'API Microsoft Graph.
* **Options** :
  + **-Scope CurrentUser** : Installe le module uniquement pour l'utilisateur actuel.
  + **-Repository PSGallery** : Indique que le module doit être installé depuis le dépôt PowerShell Gallery, qui est le référentiel officiel pour les modules PowerShell.
  + **-Force** : Force la réinstallation du module si une version est déjà présente, sans demander de confirmation.

**Get-InstalledModule Microsoft.Graph**

* **Objectif** : Vérifie si le module Microsoft.Graph est installé sur le système et affiche ses détails.
* **Utilisation** : Cette commande est utile pour confirmer que l’installation du module s’est bien déroulée et pour vérifier la version installée ainsi que son emplacement.

**Connect-MgGraph -Scopes "Group.ReadWrite.All"**

* **Objectif** : Établit une connexion avec l'API Microsoft Graph en utilisant le module Microsoft.Graph et demande des autorisations spécifiques.
* **Options** :
  + **-Scopes "Group.ReadWrite.All"** : Spécifie les autorisations pour cette session. Ici, Group.ReadWrite.All permet de lire et de modifier tous les groupes au sein de l'organisation. Tu devras fournir tes informations d'authentification, et si ton compte a les autorisations nécessaires, tu pourras accéder aux groupes et les modifier.

Script PowerShell pour ajouter un utilisateur :



**● Gérez les groupes, comme les équipes d'exploration et les équipes**

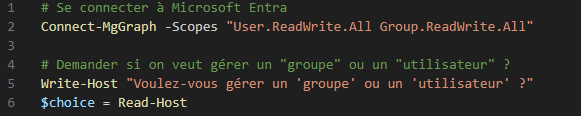
**médicales, en automatisant l'ajout et la suppression des membres.**

### **Connexion à Microsoft Entra**

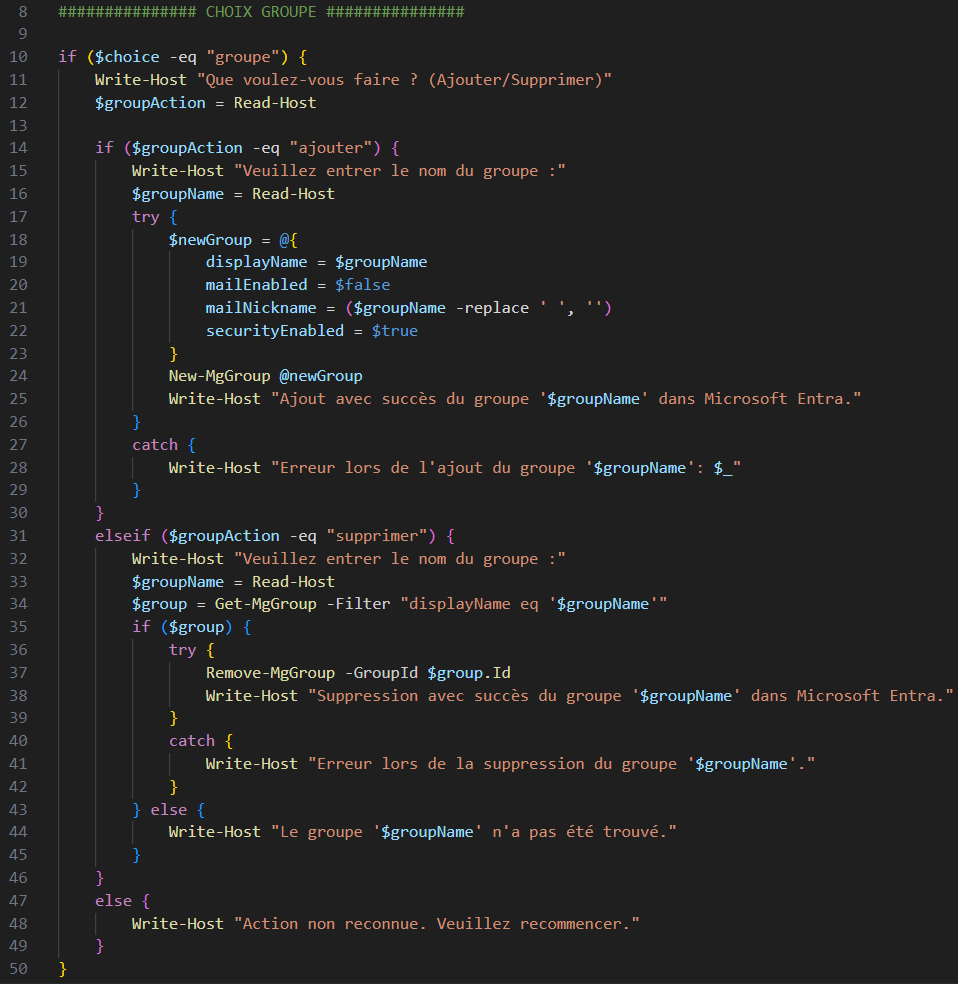
Se connecter à Microsoft Entra pour avoir les permissions nécessaires pour lire et écrire des informations sur les groupes.

Utiliser les permissions spécifiques pour accéder aux données des groupes.

**Demander l'action à réaliser pour les groupes** :

****

**Demande de choix entre Groupes et Utilisateurs**



**Write-Host** : Affiche le message pour demander à l'utilisateur s'il veut gérer un groupe ou un utilisateur.

**$choice = Read-Host** : Lit la réponse de l'utilisateur et la stocke dans la variable $choice.

**Gestion des Groupes** :

**if ($choice -eq "groupe")** : Vérifie si l'utilisateur a choisi de gérer un groupe.

**Write-Host "Que voulez-vous faire ? (Ajouter/Supprimer)"** : Demande à l'utilisateur ce qu'il veut faire (ajouter ou supprimer un groupe).

**$groupAction = Read-Host** : Lit la réponse de l'utilisateur et la stocke dans la variable $groupAction.

**Ajout d’un groupe :**

**if ($groupAction -eq "Ajouter")** : Vérifie si l'utilisateur a choisi d'ajouter un groupe.

**Write-Host "Veuillez entrer le nom du groupe :"** : Demande à l'utilisateur d'entrer le nom du groupe.

**$groupName = Read-Host** : Lit la réponse de l'utilisateur et la stocke dans la variable $groupName.

**Supprimer un groupe :**

**elseif ($groupAction -eq "Supprimer")** : Vérifie si l'utilisateur a choisi de supprimer un groupe.

**Write-Host "Veuillez entrer le nom du groupe :"** : Demande à l'utilisateur d'entrer le nom du groupe.

**$groupName = Read-Host** : Lit la réponse de l'utilisateur et la stocke dans la variable $groupName.

**$group = Get-MgGroup -Filter "displayName eq '$groupName'"** : Récupère les détails du groupe avec le nom spécifié.

**if ($group)** : Vérifie si le groupe existe.

**try { ... } catch { ... }** : Bloc de code pour gérer les erreurs. Essaye d'exécuter le code dans try et, en cas d'erreur, exécute le code dans catch.

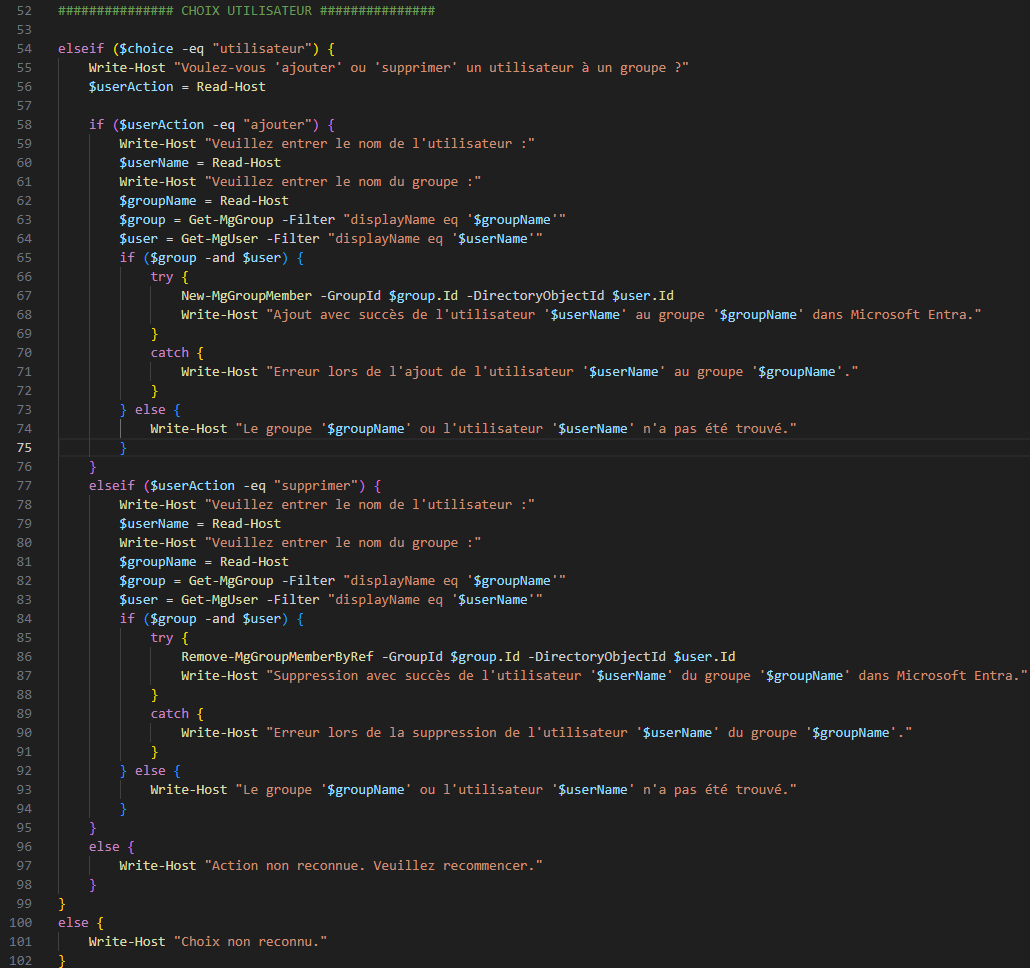
**Remove-MgGroup -GroupId $group.Id** : Supprime le groupe spécifié par l'ID.

**Write-Host "Suppression avec succès du groupe '$groupName' dans Microsoft Entra."** : Affiche un message indiquant que le groupe a été supprimé avec succès.

**catch { Write-Host "Erreur lors de la suppression du groupe '$groupName'." }** : Affiche un message d'erreur en cas de problème lors de la suppression du groupe.

**else { Write-Host "Le groupe '$groupName' n'a pas été trouvé." }** : Affiche un message indiquant que le groupe n'a pas été trouvé.

**Gestion des utilisateurs :**



**Choix utilisateur sélectionné :**

**elseif ($choice -eq "utilisateur")** : Vérifie si l'utilisateur a choisi de gérer un utilisateur.

**Write-Host "Voulez-vous 'ajouter' ou 'supprimer' un utilisateur à un groupe ?"** : Demande à l'utilisateur ce qu'il veut faire entre ajouter ou supprimer un utilisateur à un groupe.

**$userAction = Read-Host** : Lit la réponse de l'utilisateur et la stocke dans la variable $userAction.

**Ajout d’un utilisateur à un groupe :**

**if ($userAction -eq "ajouter")** : Vérifie si l'utilisateur a choisi d'ajouter un utilisateur à un groupe.

**Write-Host "Veuillez entrer le nom de l'utilisateur :"** : Demande à l'utilisateur d'entrer le nom de l'utilisateur.

**$userName = Read-Host** : Lit la réponse de l'utilisateur et la stocke dans la variable $userName.

**Write-Host "Veuillez entrer le nom du groupe :"** : Demande à l'utilisateur d'entrer le nom du groupe.

**$groupName = Read-Host** : Lit la réponse de l'utilisateur et la stocke dans la variable $groupName.

**$group = Get-MgGroup -Filter "displayName eq '$groupName'"** :

Requête pour trouver le groupe dans Microsoft Entra correspondant au displayName $groupName.

**$user = Get-MgUser -Filter "displayName eq '$userName'"** : Requête pour trouver l'utilisateur dans Microsoft Entra correspondant au displayName $userName.

**if ($group -and $user) {** : Vérifie si le groupe et l'utilisateur existent (si les deux requêtes ont renvoyé un résultat).

**try { Remove-MgGroupMemberByRef -GroupId $group.Id -DirectoryObjectId $user.Id** : Essaie de supprimer l'utilisateur du groupe en utilisant l'ID du groupe ($group.Id) et l'ID de l'utilisateur ($user.Id).

**Write-Host "Suppression avec succès de l'utilisateur '$userName' du groupe '$groupName' dans Microsoft Entra."** : Affiche un message de succès si l'utilisateur a été supprimé du groupe.

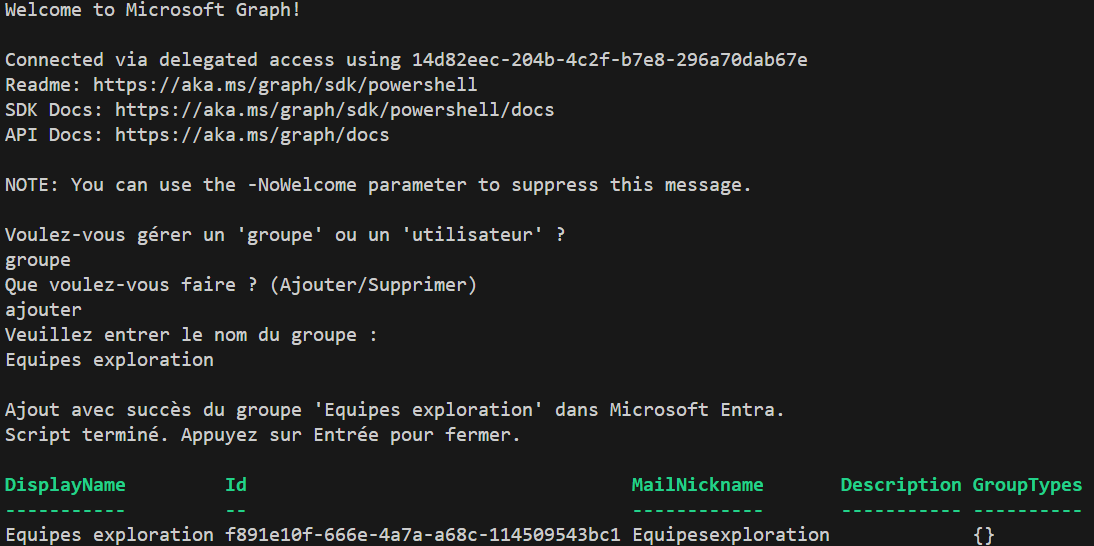
**} catch { Write-Host "Erreur lors de la suppression de l'utilisateur '$userName' du groupe '$groupName'." }** : Capture et affiche un message en cas d'échec de la suppression.

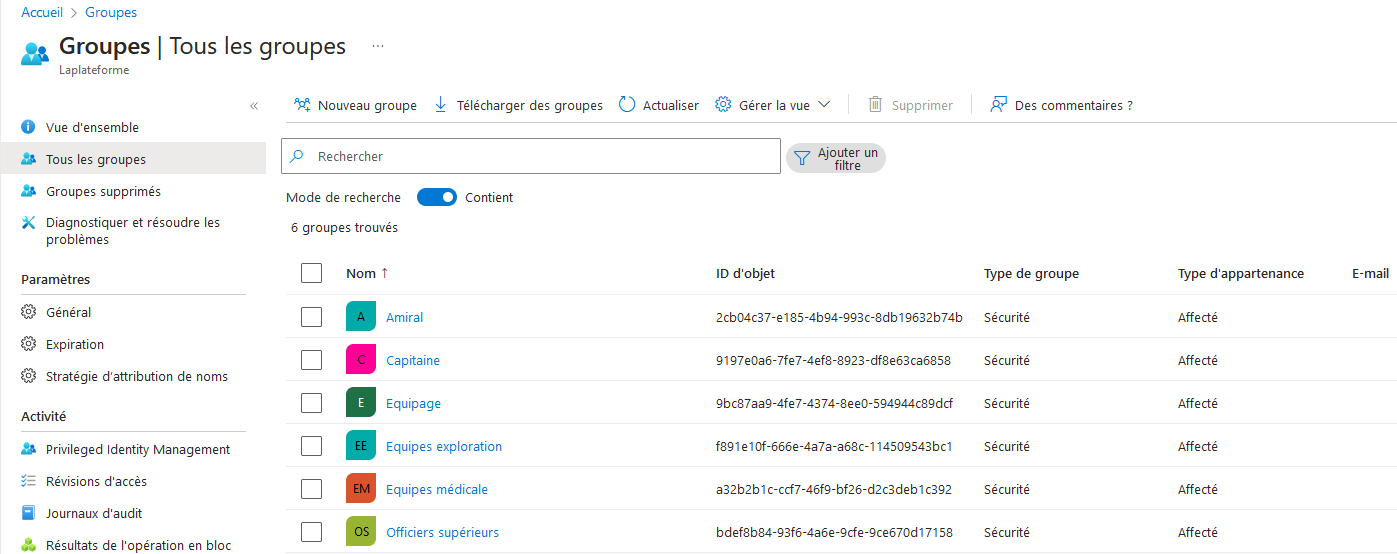
**} else { Write-Host "Le groupe '$groupName' ou l'utilisateur '$userName' n'a pas été trouvé." }** : Affiche un message si le groupe ou l'utilisateur n'a pas été trouvé.

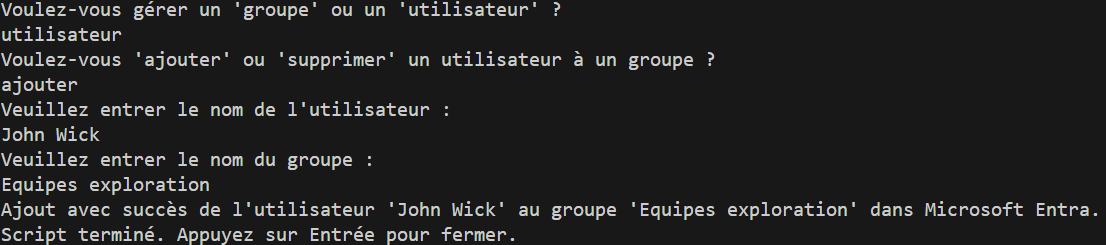
Et si l'action n'est ni ajouter ni supprimer : **else { Write-Host "Action non reconnue. Veuillez recommencer."}**

Cela affichera un message d'erreur si l'utilisateur a saisi une action non valide.

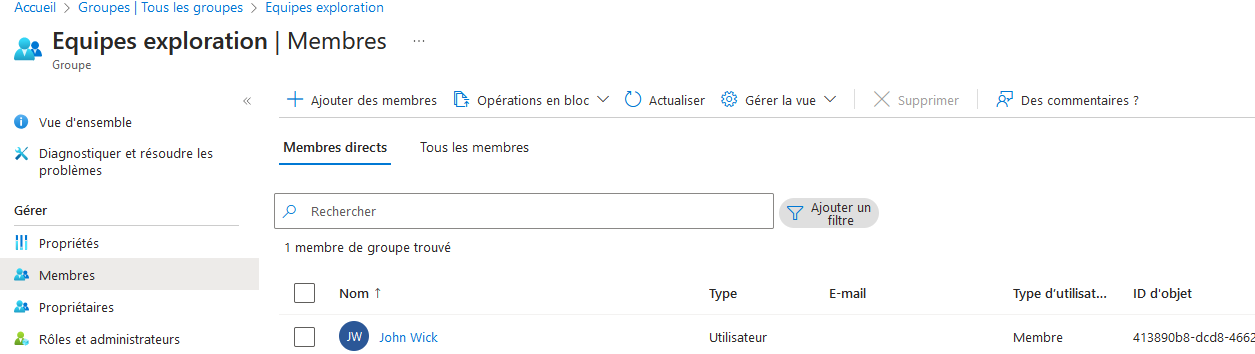
**Exécution du script :**



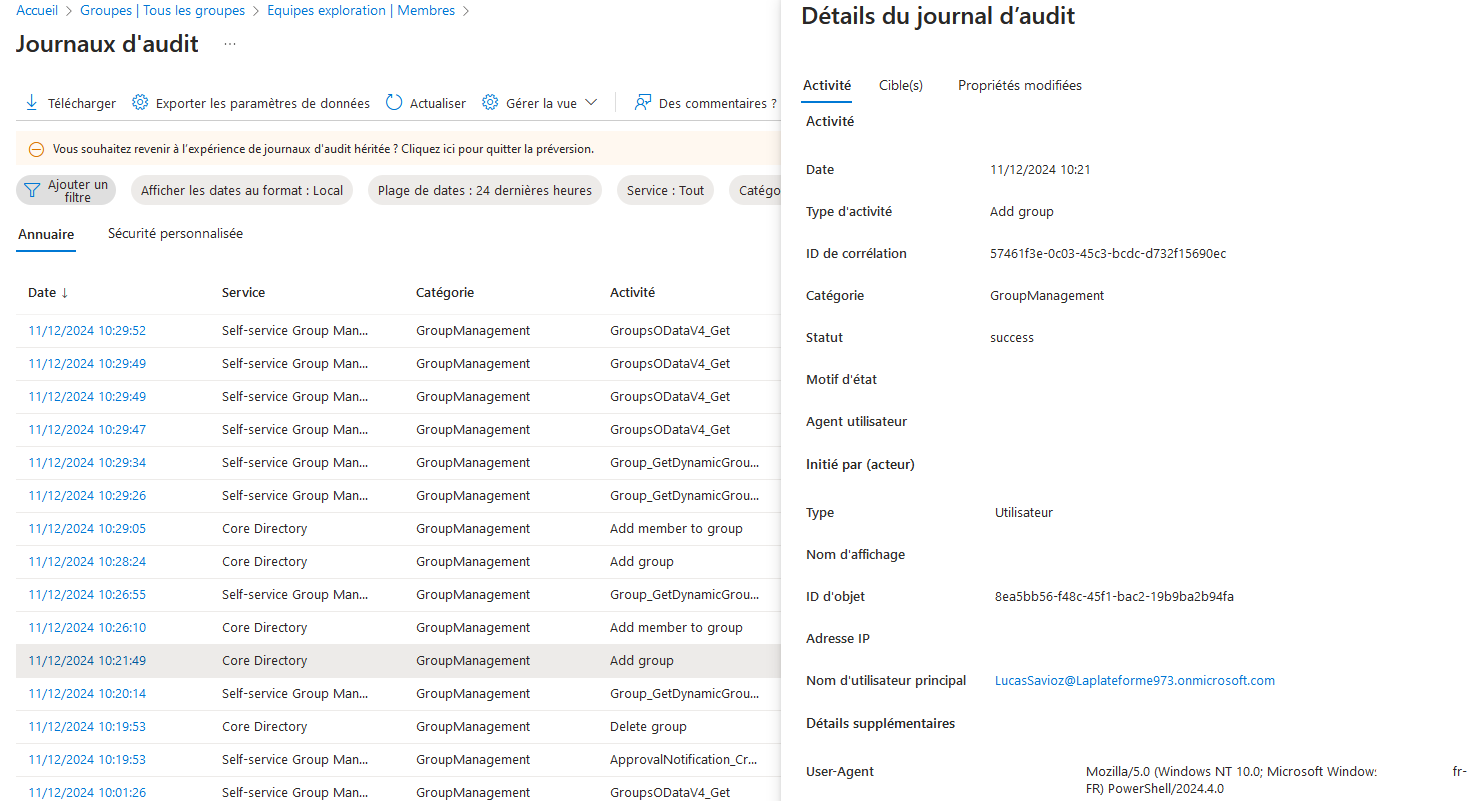




Vérification dans Microsoft Entra : 

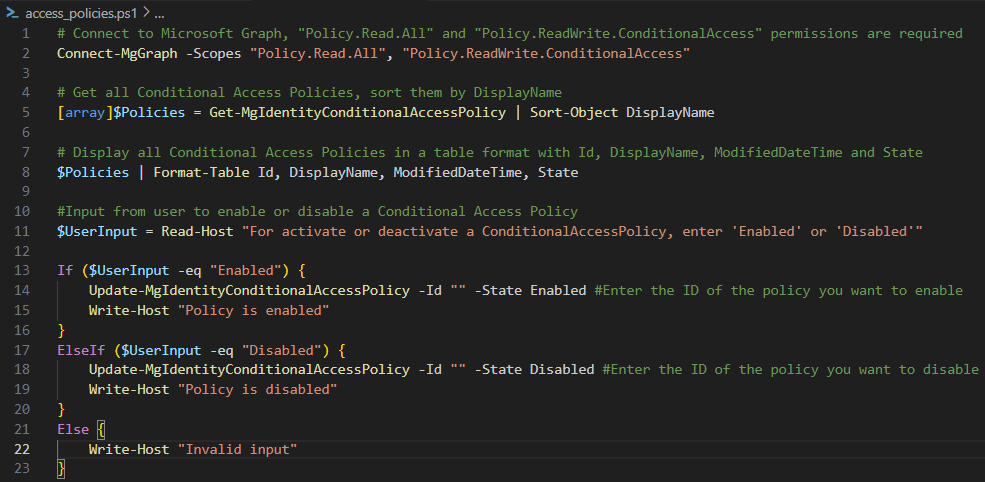


**Vérification des journaux d’audit :**

****

**● Appliquez automatiquement les politiques de sécurité pour les missions**

**sensibles.**

****

**[array]$Policies = Get-MgIdentityConditionalAccessPolicy | Sort-Object DisplayName**

**Objectif :** Récupérer toutes les politiques d'accès conditionnel disponibles dans l'annuaire Azure AD et les trier par leur nom.

**Explication :**

* Get-MgIdentityConditionalAccessPolicy interroge l'API pour obtenir les politiques.
* La méthode Sort-Object DisplayName trie ces politiques par leur nom pour une meilleure lisibilité.

**[array]$Policies = Get-MgIdentityConditionalAccessPolicy | Sort-Object DisplayName**

**Objectif :** Récupérer toutes les politiques d'accès conditionnel disponibles et les trier par nom pour une meilleure organisation.  
**Explication :**

* Get-MgIdentityConditionalAccessPolicy appelle l'API Microsoft Graph pour récupérer une liste de toutes les politiques d'accès conditionnel.
* | Sort-Object DisplayName trie les politiques par leur nom (propriété DisplayName) pour les afficher de manière ordonnée.
* [array] convertit le résultat en tableau pour permettre un traitement ultérieur.

**$Policies | Format-Table Id, DisplayName, ModifiedDateTime, State**

**Objectif :** Afficher les politiques d'accès conditionnel dans un tableau lisible contenant des informations clés.  
**Explication :**

* $Policies contient les politiques récupérées.
* | Format-Table Id, DisplayName, ModifiedDateTime, State organise les colonnes pour afficher :
  + Id : l'identifiant unique de la politique.
  + DisplayName : le nom de la politique.
  + ModifiedDateTime : la dernière date de modification.
  + State : l'état actuel de la politique (par exemple, Enabled ou Disabled).

**$UserInput = Read-Host "For activate or deactivate a ConditionalAccessPolicy, enter 'Enabled' or 'Disabled'"**

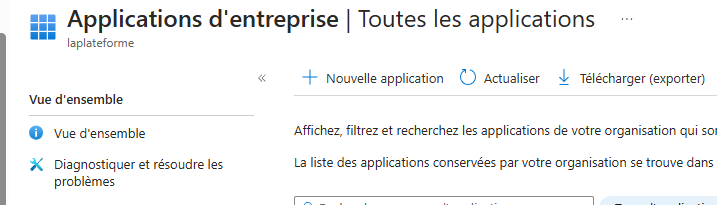
**Objectif :** Demander à l'utilisateur s'il veut activer ou désactiver une politique d'accès conditionnel.  
**Explication :**

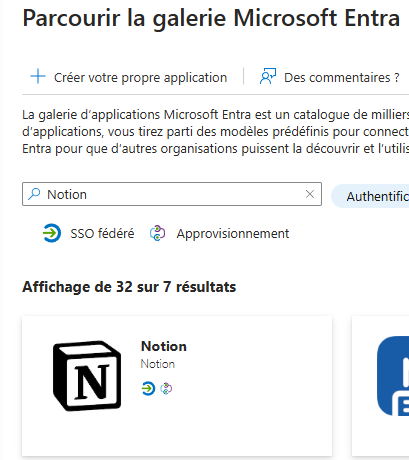
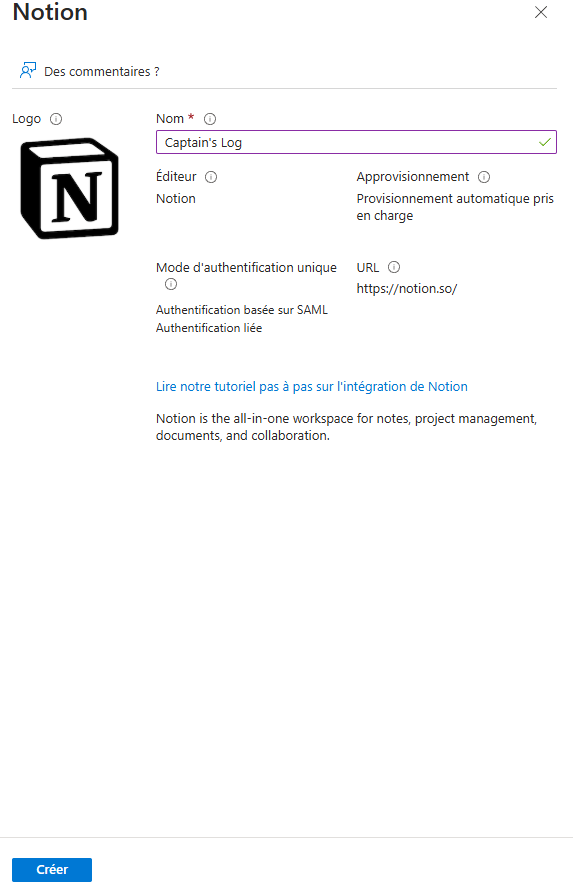
* Read-Hostaffiche une invite de commande à l'utilisateur.
* L'utilisateur doit entrer soitEnabled(pour activer une politique)soitDisabled(pour la désactiver).
* La valeur saisie est stockée dans$UserInput.

**3. Intégration et Sécurisation des Applications**

**Intégrer une application SaaS avec Entra ID :**

* **Intégrez des applications essentielles de Starfleet, comme le Journal de Bord (Captain's Log) et le Centre de Commandement (CommandCenter), avec Azure AD pour un accès sécurisé.**

Cliquez sur “Nouvelle application” dans l’onglet Applications>Application d’entreprises.  


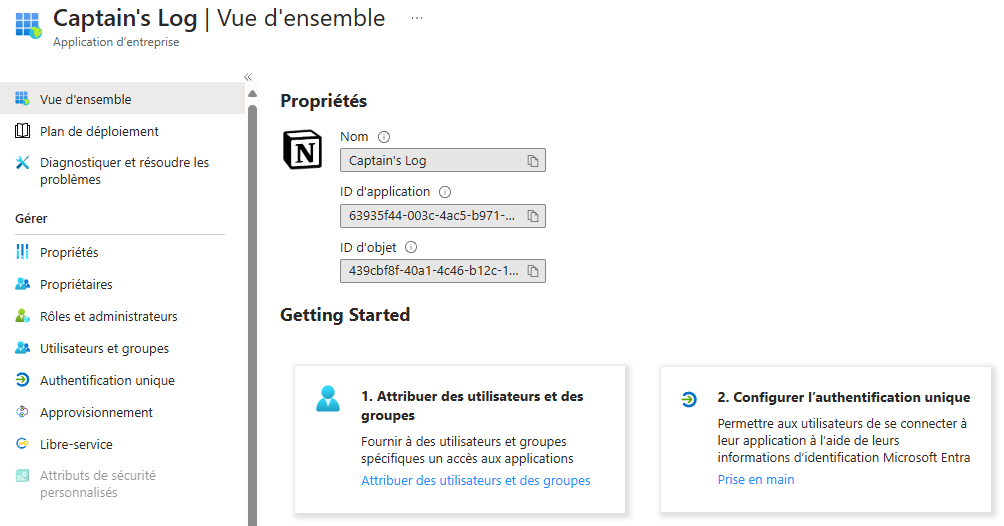
Pour le journal de bord, on va utiliser l’application **Notion** que l’on va renommer **Captain’s Log**.  
  


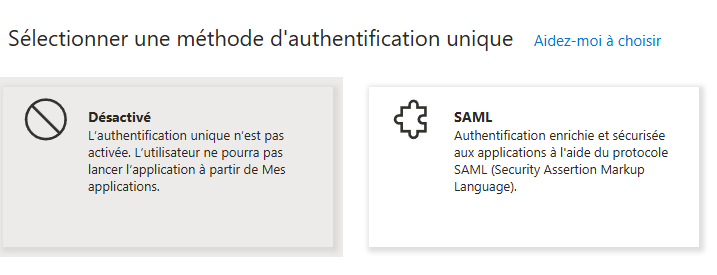
* **Configurez le Single Sign-On (SSO) pour ces applications afin que**

**les membres d'équipage puissent y accéder avec leurs**

**identifiants Starfleet .**

**Captain’s Log** est maintenant créé cliquez sur **“Configurer l’authentification unique”** pour mettre en place le SSO.





L’activation du SSO coté app nécessite un abonnement, il n’est donc pas possible de le tester. Cependant, nous verrons dans la partie suivante comment tester le SSO.

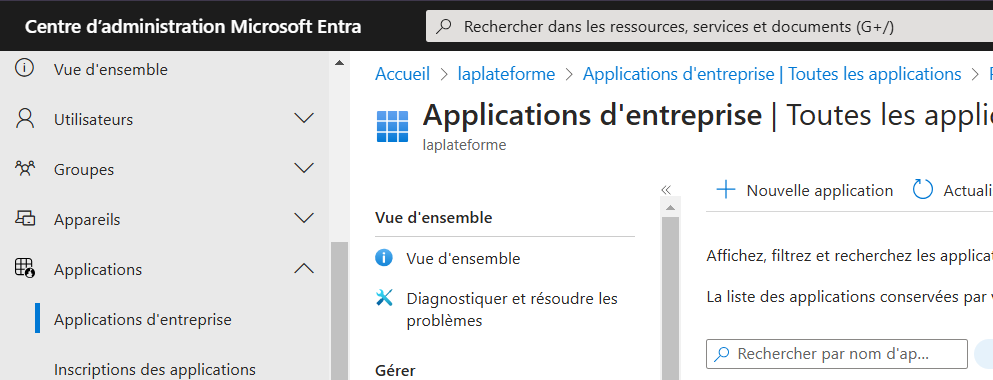
**Ajouter une application personnalisée :**

* **Ajoutez l'application de Gestion des Réparations (Repair Management) utilisée par l'ingénierie.**

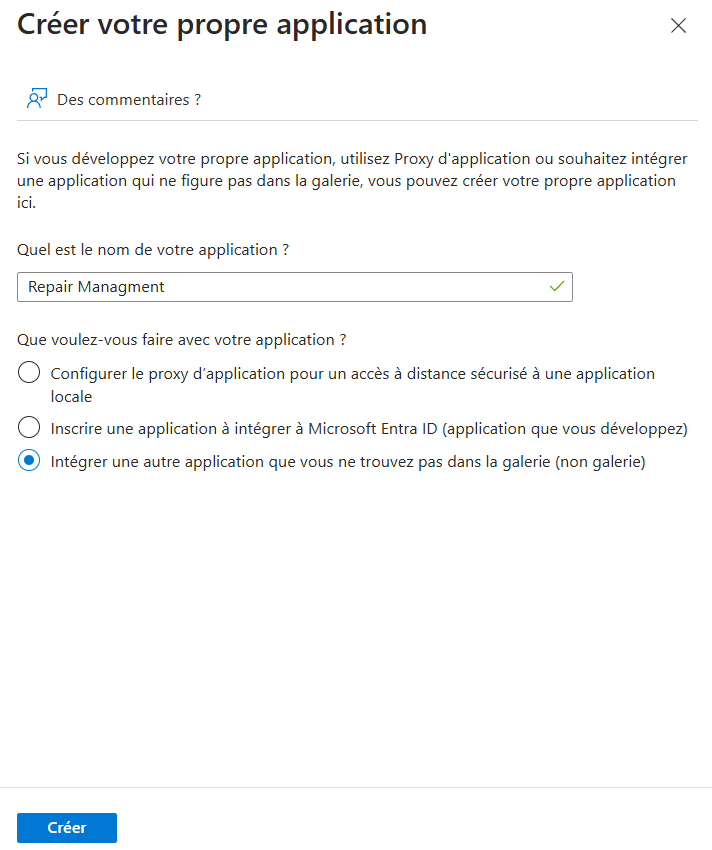
Pour intégrer l’application “Repair Management” avec azure AD pour un accès sécurisée, nous avons suivi les étapes suivantes:

Etape 1 :

On se rend **Entra ID > Applications > Application d’entreprise > Nouvelle application**

On rentre le nom de notre application dans la zone de texte dédiée. puis on sélectionne **“ Intégrer une autre application que vous ne trouvez pas dans la galerie (non galerie)”** qui est idéale lorsque l'application n'est pas listée, mais que vous voulez profiter des fonctionnalités Entra ID comme le SSO, la gestion des utilisateurs, et la sécurité avancée.

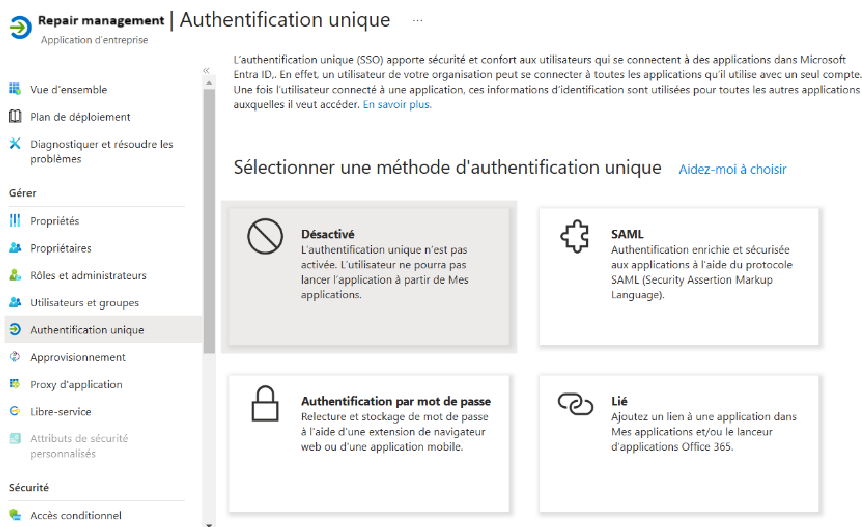
  


Notre Application Captain’s Log est créée. Maintenant nous allons mettre en place **l'authentification Unique.**

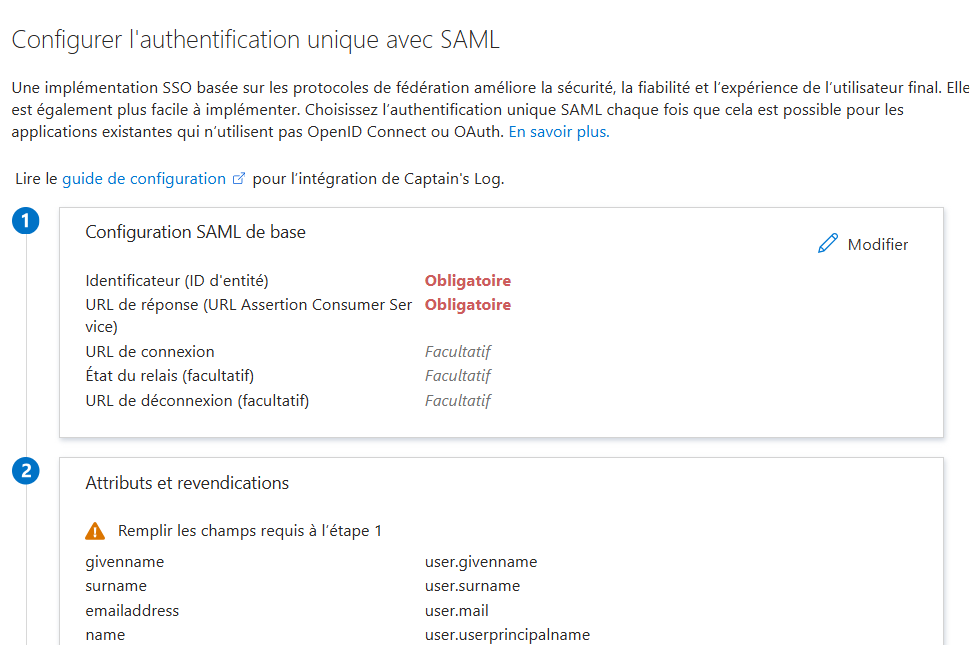
C’est quoi ?

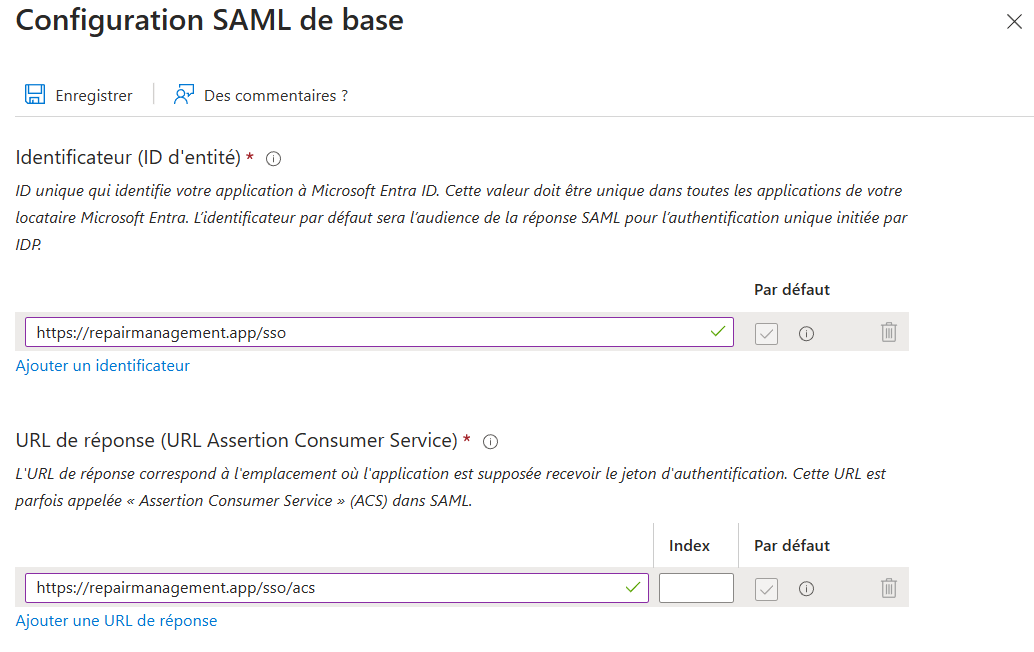
C'est une méthode d'authentification qui permet aux utilisateurs de se connecter avec un ensemble d'informations d'identification à plusieurs systèmes logiciels indépendants. Avec l'authentification unique, un utilisateur n'a pas besoin de se connecter à chaque application dont il se sert.

On se rend dans **Gérer** > **Authentification unique** de l’application que nous venons de créer



On choisit le protocole **SAMSL**  qui permet aux utilisateurs de s'authentifier une seule fois **(SSO**) et d'accéder à plusieurs applications en échangeant des informations d'authentification sous forme de jetons XML sécurisés entre un fournisseur d'identité (IdP) et un fournisseur de service (SP).

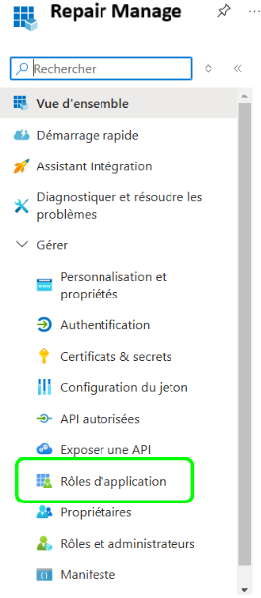
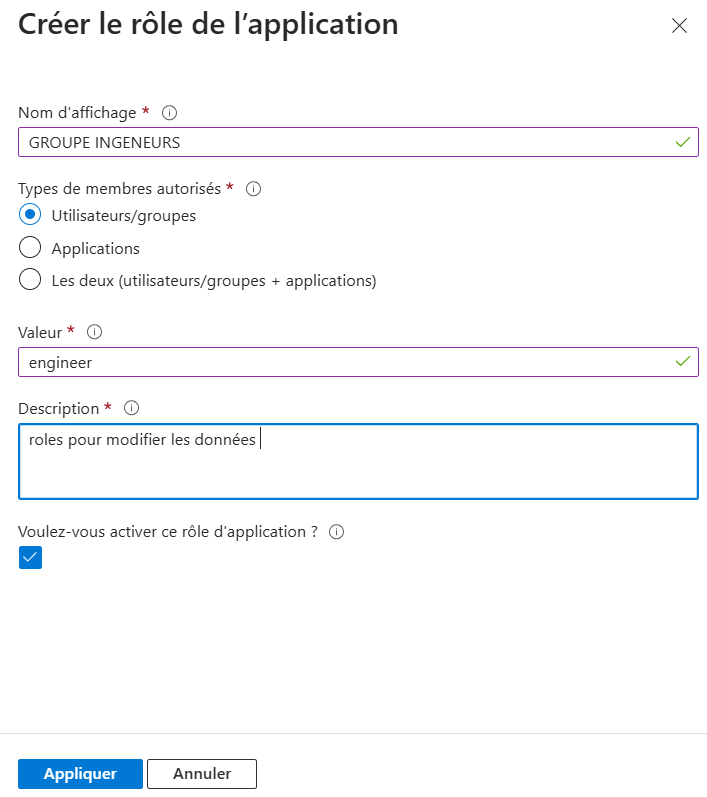




* **Configurez les rôles et permissions pour l'application, permettant par exemple seulement aux ingénieurs de modifier les données.**

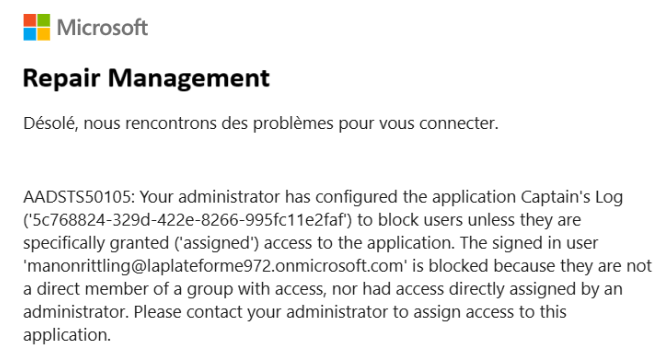
Pour configurer les rôles et permissions pour l’application permettant seulement aux ingénieurs de modifier les données.

Il suffit de se rendre dans Microsoft Entra ID > Inscription d’application , on clique sur l’application en question

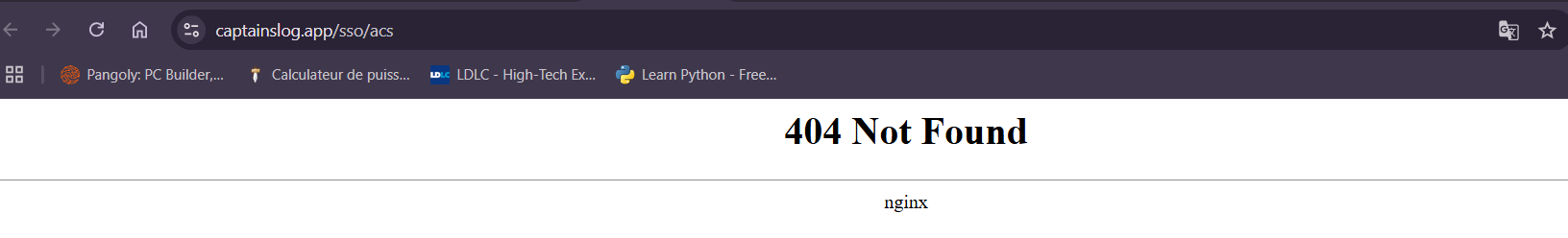
****

* **Testez les accès pour vérifier que les permissions sont correctement appliquées.**



On peut observer ci-dessous que nous n’avons pas accès à l’application car l’utilisateur n’a pas été ajouté à la liste des utilisateurs autorisés à utiliser l’application.

Pour que notre utilisateur puisse utiliser l’application, il faut donc l’ajouter à la liste en cliquant sur “Ajouter un utilisateur/groupe” via l’onglet “utilisateurs et groupes”.  
Ci-dessous le résultat.

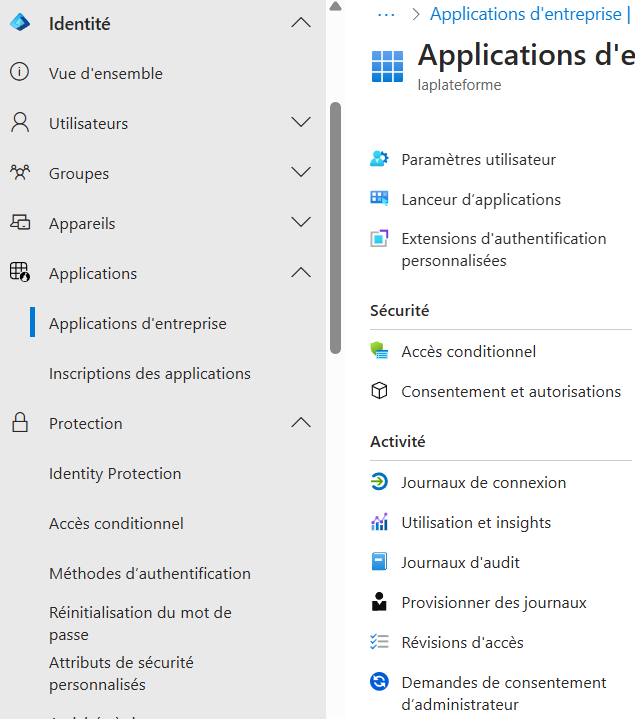


**Surveillance et Réponse aux Incidents**

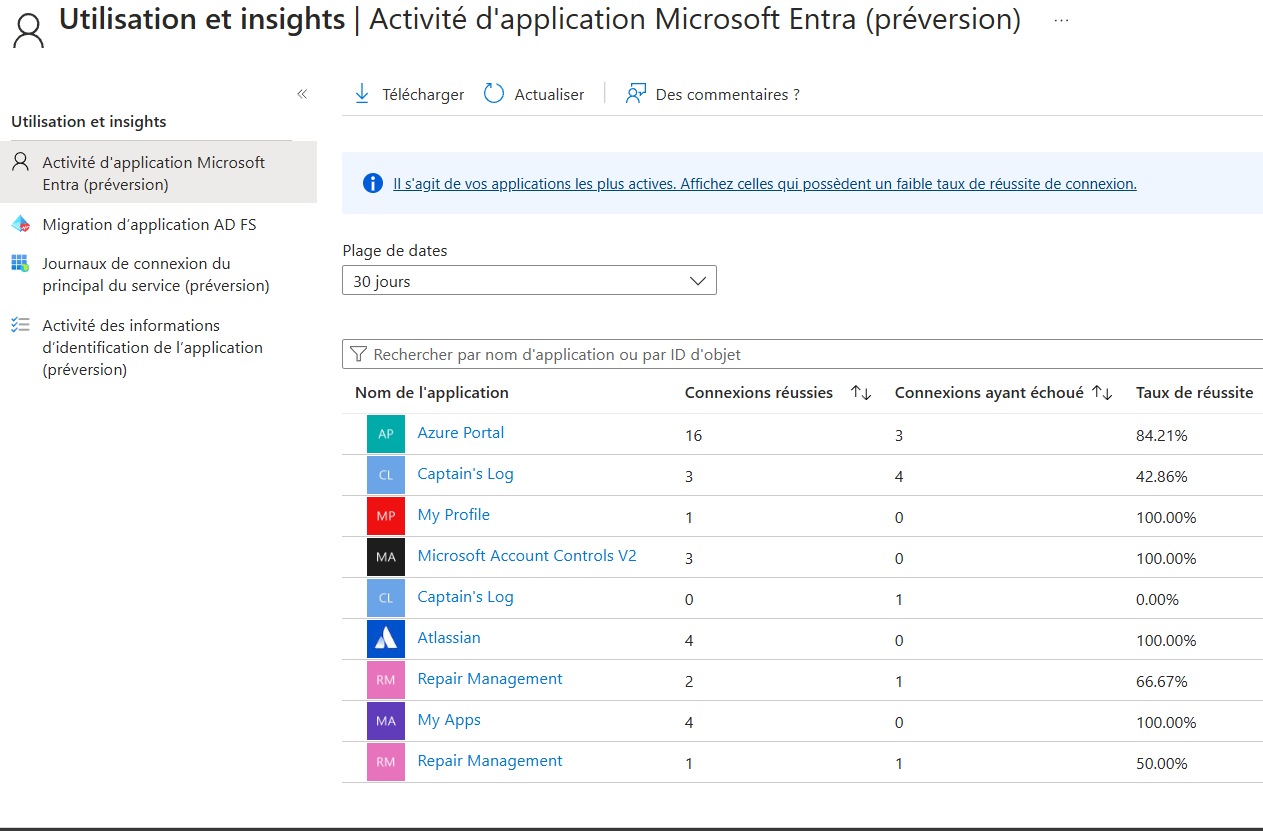
* **Surveillez les tentatives d'accès aux données confidentielles des**

**missions de Starfleet.**

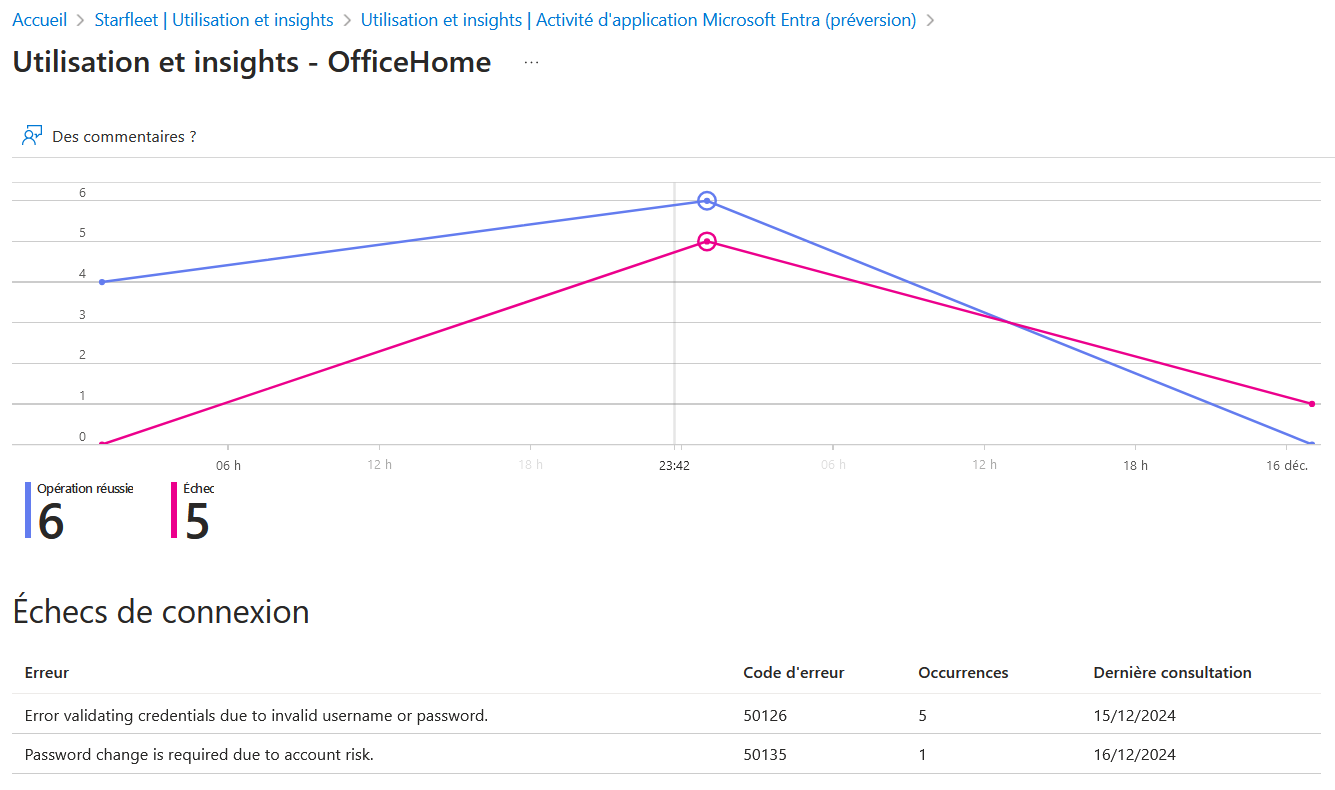
On peut observer les activités de connexions sur nos applications dans Entra ID dans **Application>Applications d’entreprise>Utilisation et Insights**.

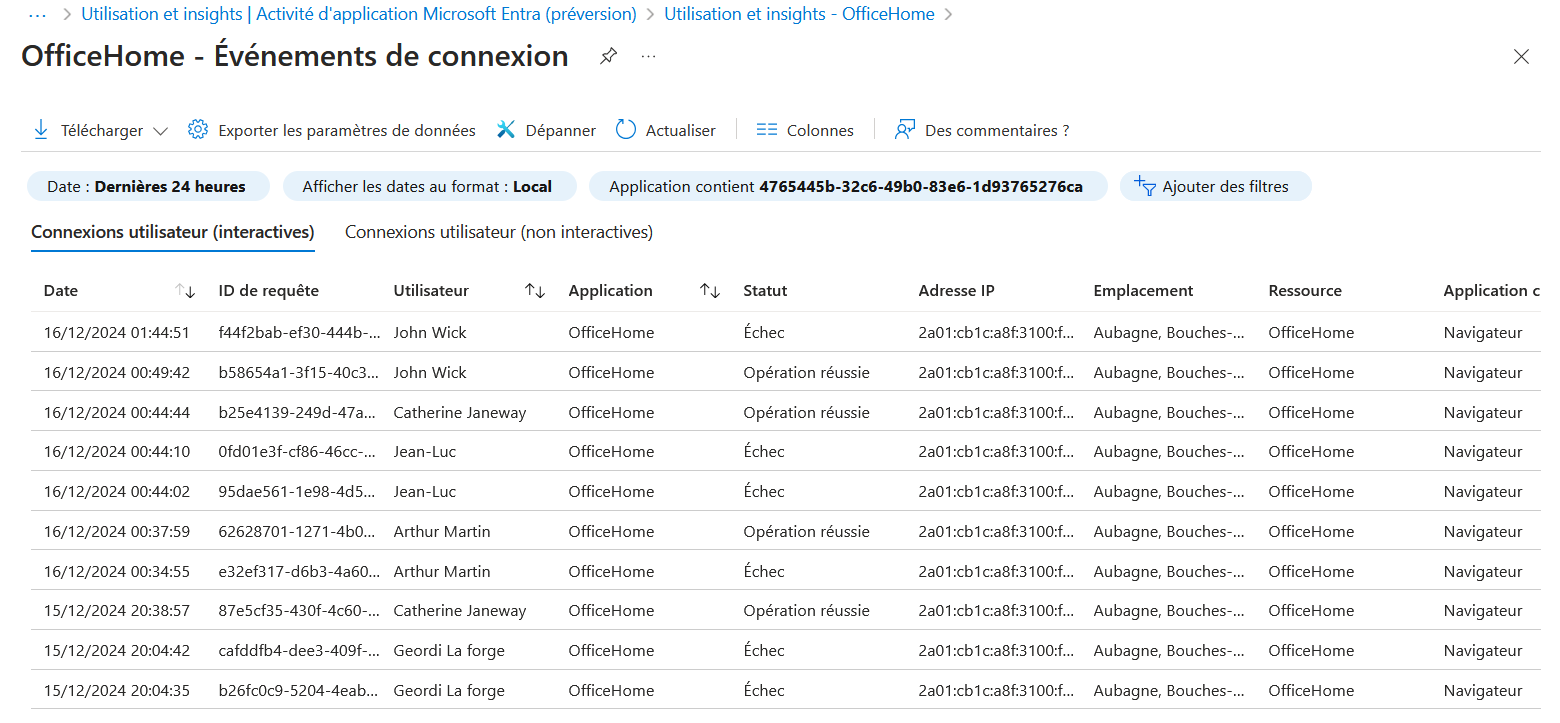
 

Dans cette partie on peut observer toutes nos applications créées, avec le nombre de connexions réussi et le nombre de connexions échoué.



En cliquant sur unze des applications on peut observer en détail la date et l’heure des tentatives. On peut aussi cliquer sur un des pics de graph pour voir en détails les utilisateurs.

****

**Ci-dessous le détail sur les écénements de connexion.**

* **Analysez les logs pour identifier les activités suspectes, comme des**

**accès non autorisés aux plans des moteurs à distorsion.**

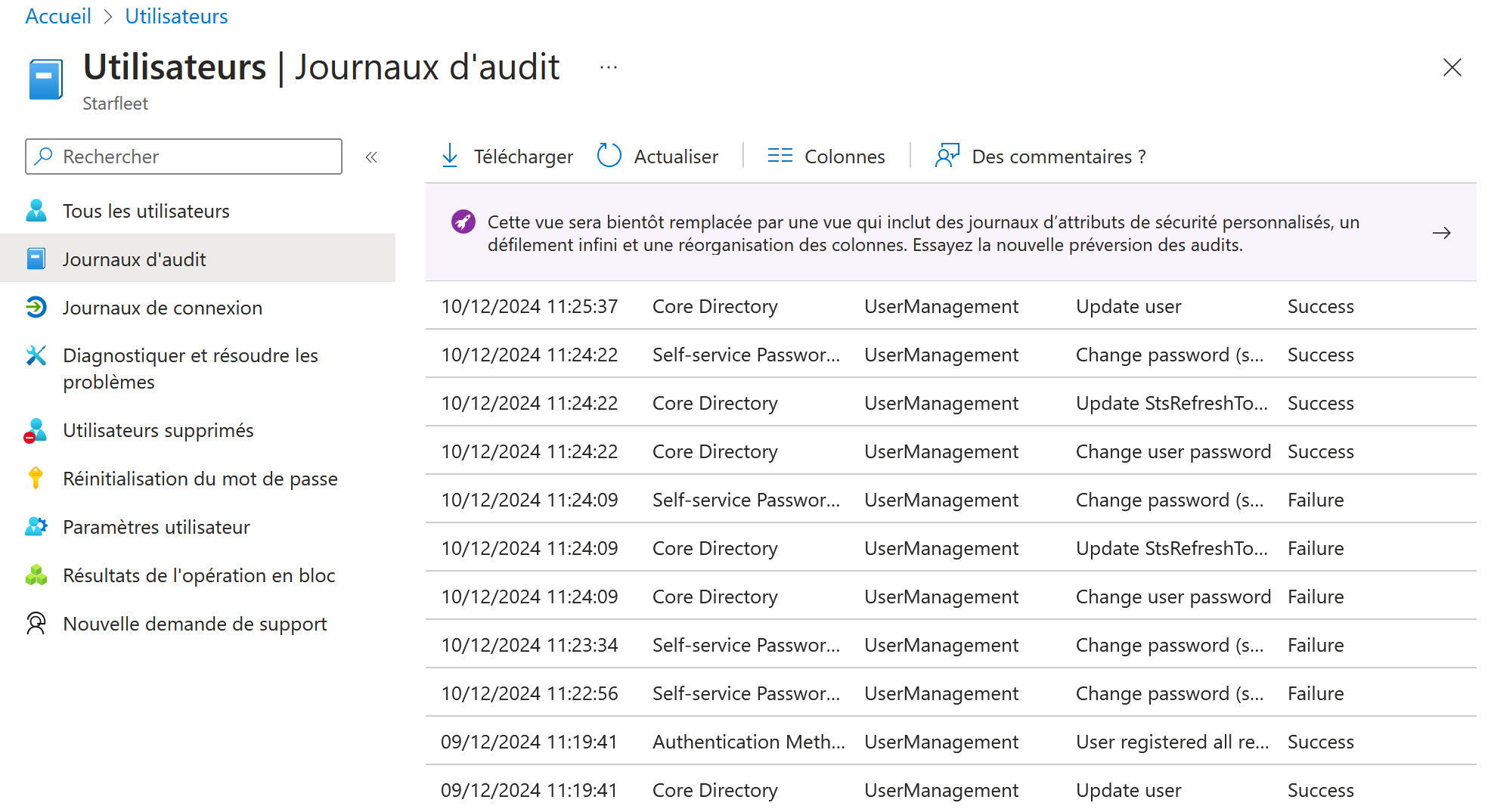
Pour analyser les logs et identifier les activités suspectes.

On commence par les journaux d’audit

Les **journaux d'audit** servent à enregistrer et tracer toutes les actions significatives dans un système informatique. Ils permettent :

1. **Traçabilité** : Savoir qui a fait quoi, quand et où.
2. **Sécurité** : Détecter les anomalies et activités suspectes.
3. **Enquête** : Analyser les incidents de sécurité et identifier les causes.
4. **Conformité** : Répondre aux exigences réglementaires (RGPD, ISO 27001, etc.).
5. **Maintenance** : Optimiser les performances et surveiller l’état du système.

C’est un outil qui garantit la **sécurité**, la **conformité** et la **stabilité** des infrastructures informatiques.

****

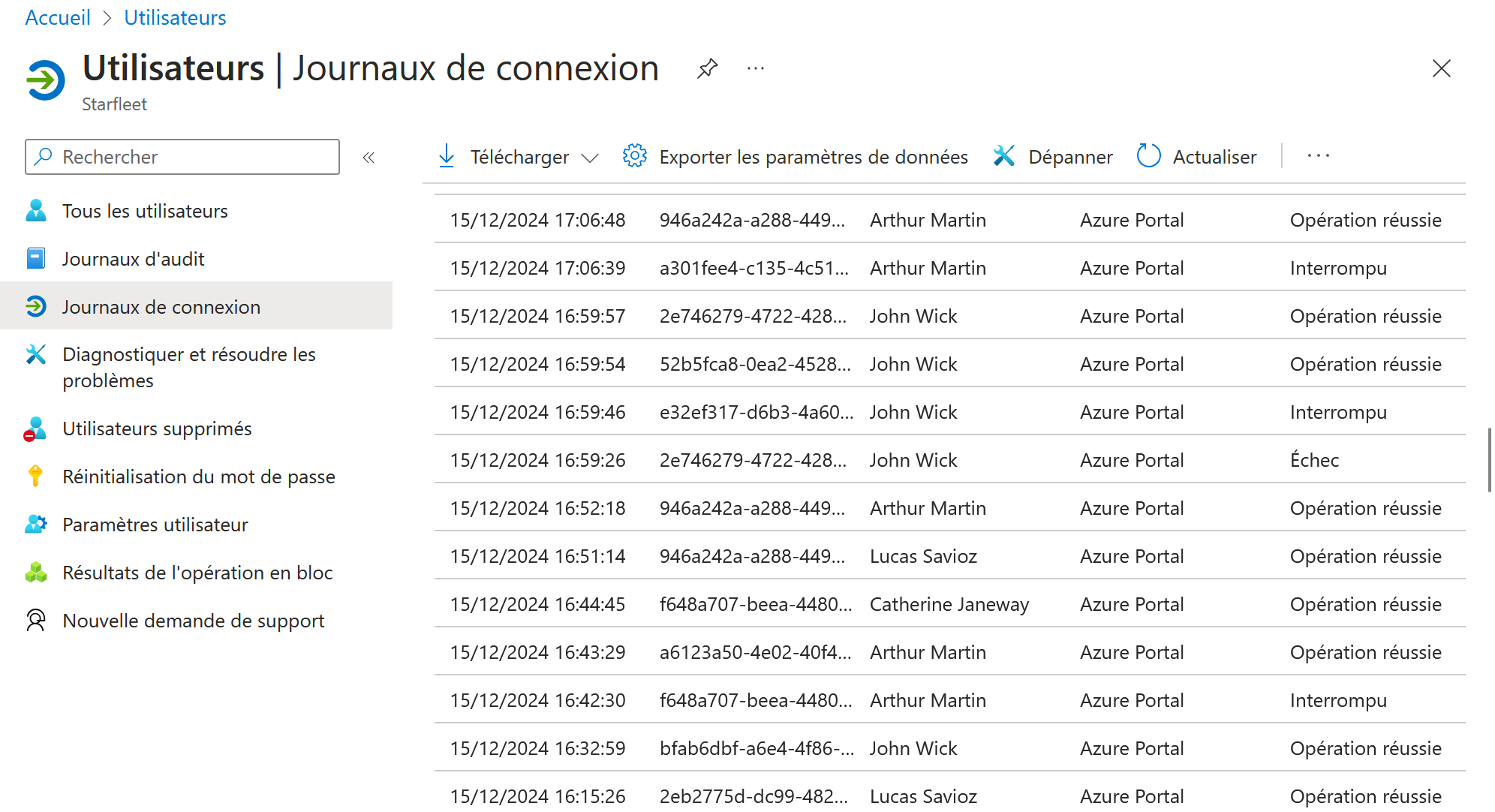
Les **journaux de connexions** enregistrent les tentatives de connexion et de déconnexion sur un système informatique. Ils sont essentiels pour suivre l’activité des utilisateurs et assurer la sécurité du système. Voici ce qu'ils incluent généralement :

1. **Informations sur l'utilisateur : Nom d'utilisateur, adresse IP, nom de la machine, etc.**
2. **Type de connexion : Connexion réussie ou échouée.**
3. **Horodatage : Date et heure de chaque tentative.**
4. **Protocole utilisé : SSH, RDP, FTP, etc.**
5. **Durée de la session : Temps écoulé pendant la connexion.**

Les **journaux de connexions** sont utilisés pour :

* **Surveiller les accès et détecter des tentatives non autorisées.**
* **Analyser les attaques par force brute ou autres comportements suspects.**
* **Assurer la conformité aux exigences de sécurité et réglementations.**

Ils sont essentiels pour garantir une gestion rigoureuse des accès et la traçabilité des utilisateurs.

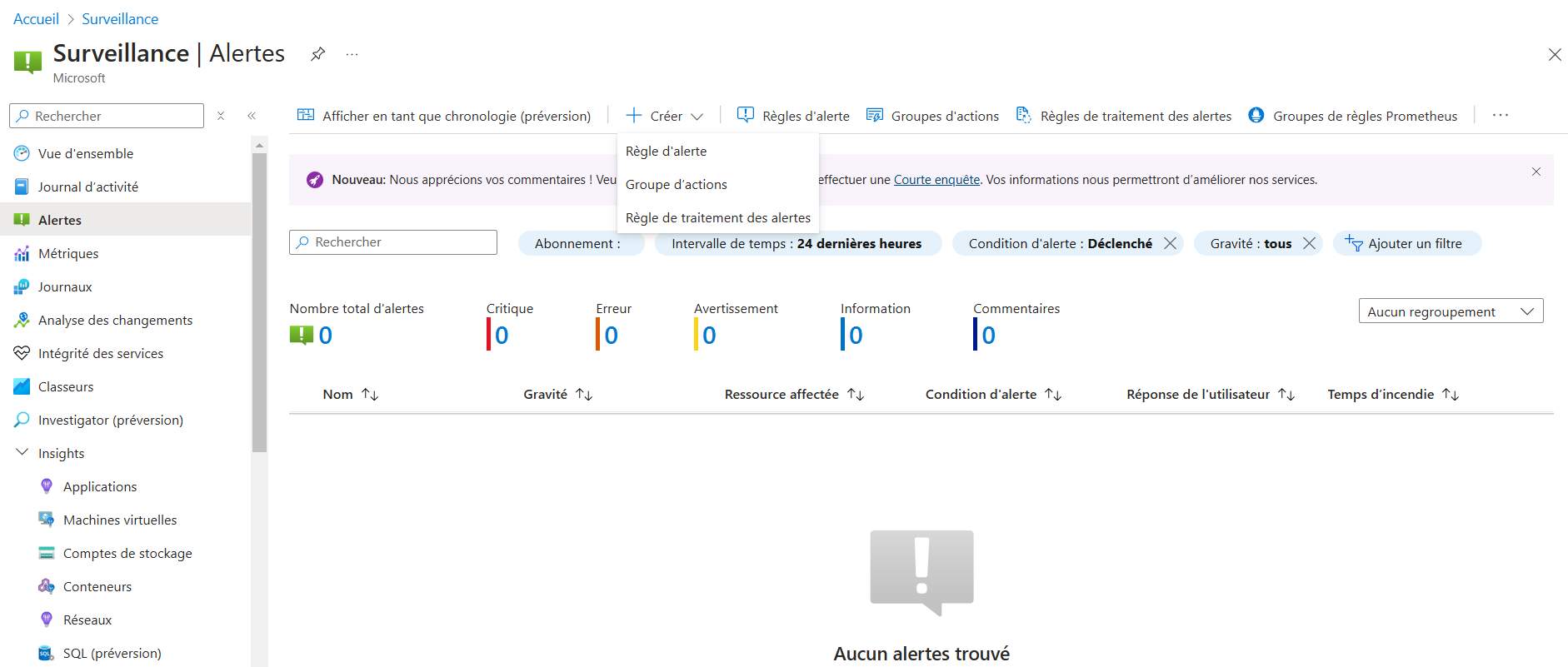
****

* **Configurez des alertes pour être informé en temps réel des activités**

**anormales, comme des connexions depuis des zones de l'espace non**

**reconnues.**

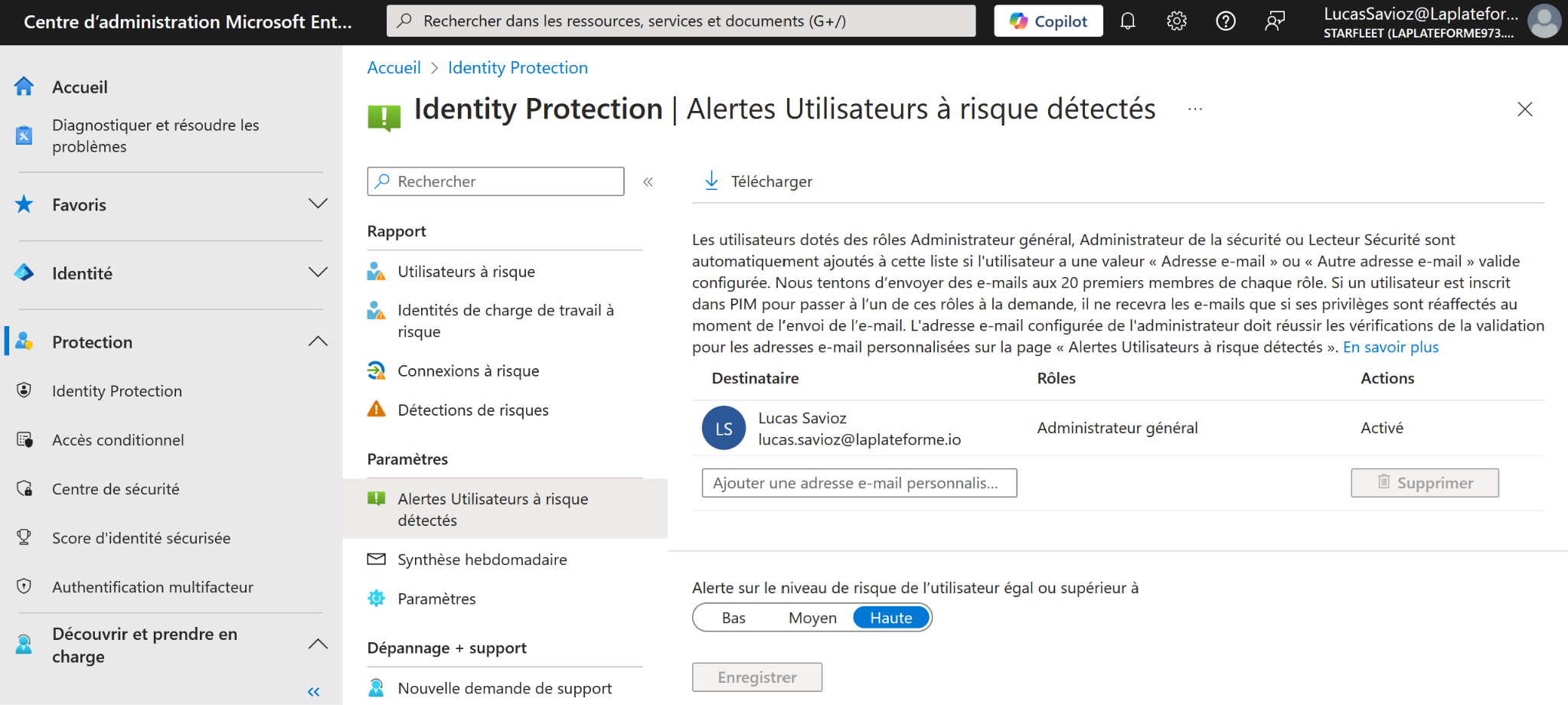
Créer une **règle d'alerte dans la surveillance sur Azure** est une pratique essentielle pour garantir la disponibilité, la performance et la sécurité de vos services et ressources dans le cloud.

****

Pour cela vérifier que les utilisateurs à privilège soient bien notifiés de toute modification au sein de l’organisation.

Aller dans Protection > Identity Protection > Alertes Utilisateurs à risque détectés.

Vérifier qu’un ou plusieurs ajouts de mail soient renseigner avec une alerte de niveau “Haute”



**Création d’une stratégie d’accès conditionnel pour limiter les accès des planètes inconnues.**

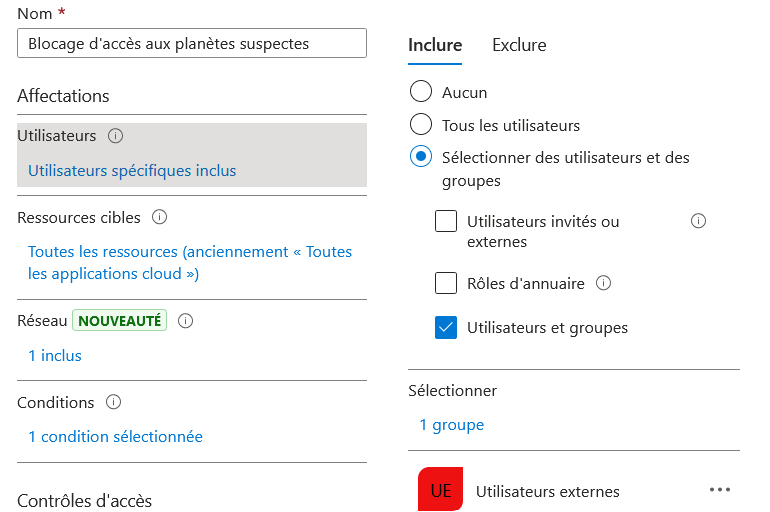
Pour cela on se rend dans Protection > Accès Conditionnel > Emplacements nommés > + Emplacement des pays.

On va créer notre emplacement “Planètes suspectes”. On sélectionne tous les pays sauf la France. Laisser bien les adresses IPv4 du pays, puis faire “Enregistrer”.



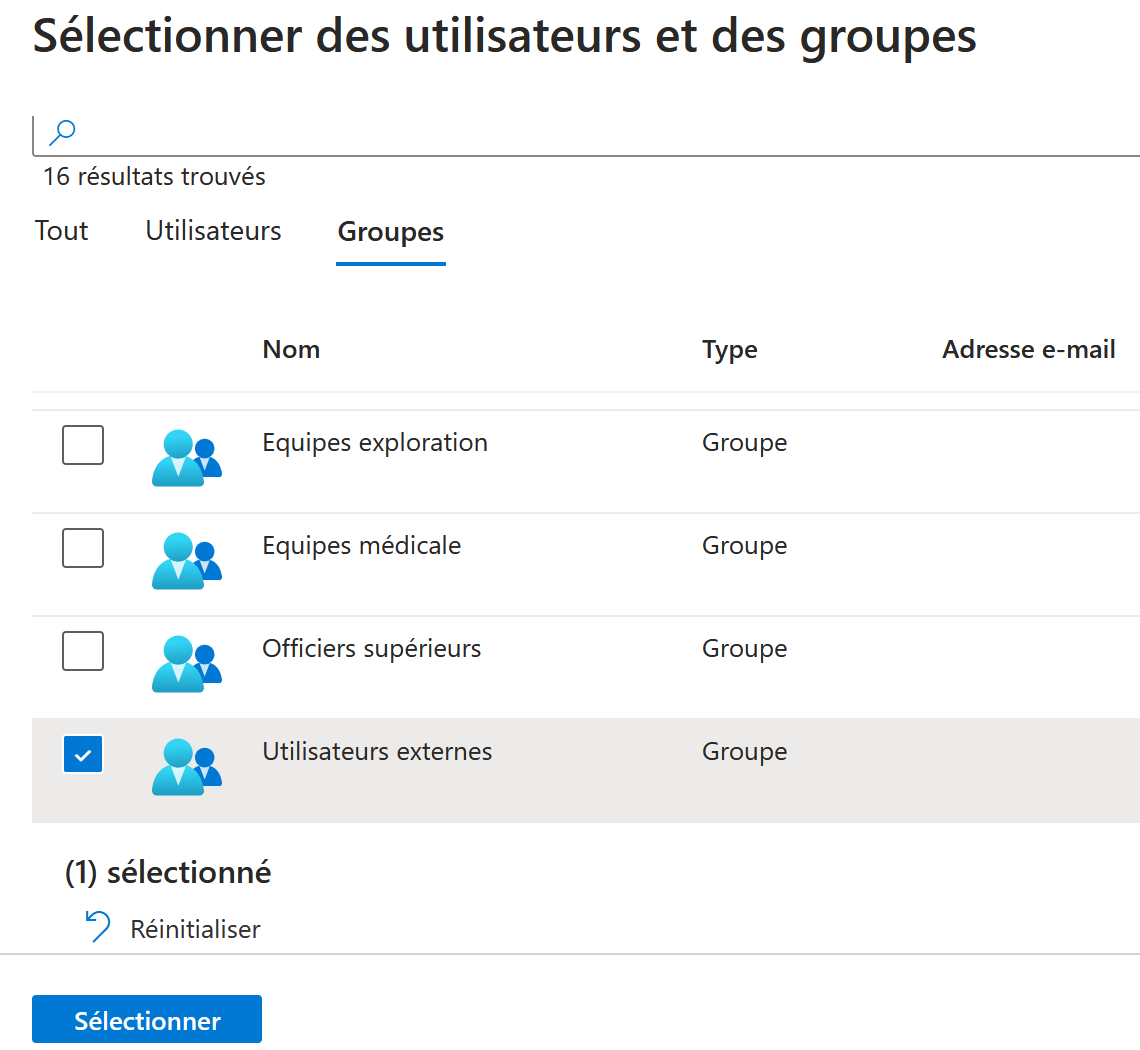
Une fois l’emplacement créé, on crée la stratégie.

On sélectionne le groupe “Utilisateurs externes” qui utilisent des connexions sur des planètes suspectes avec des adresses IP inconnues.

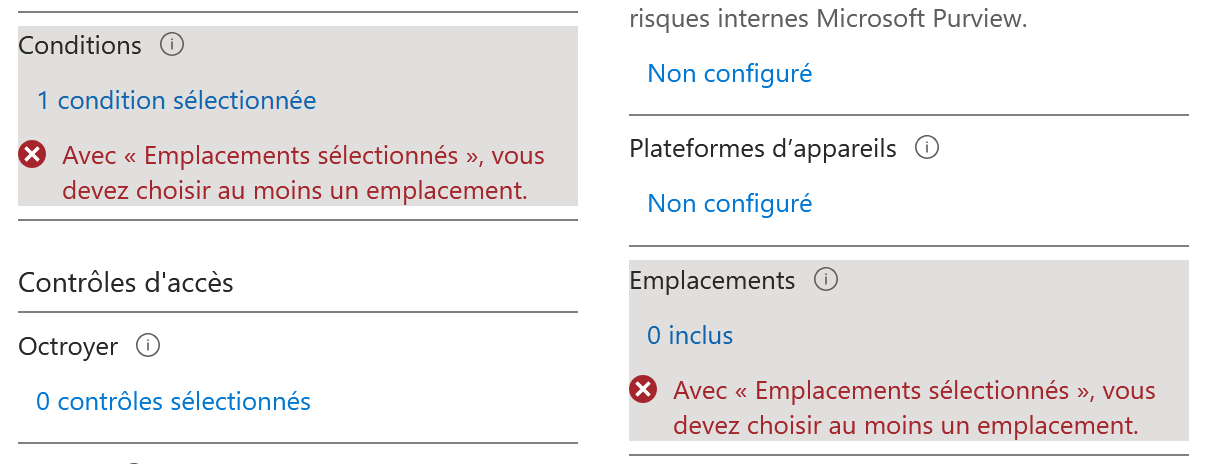


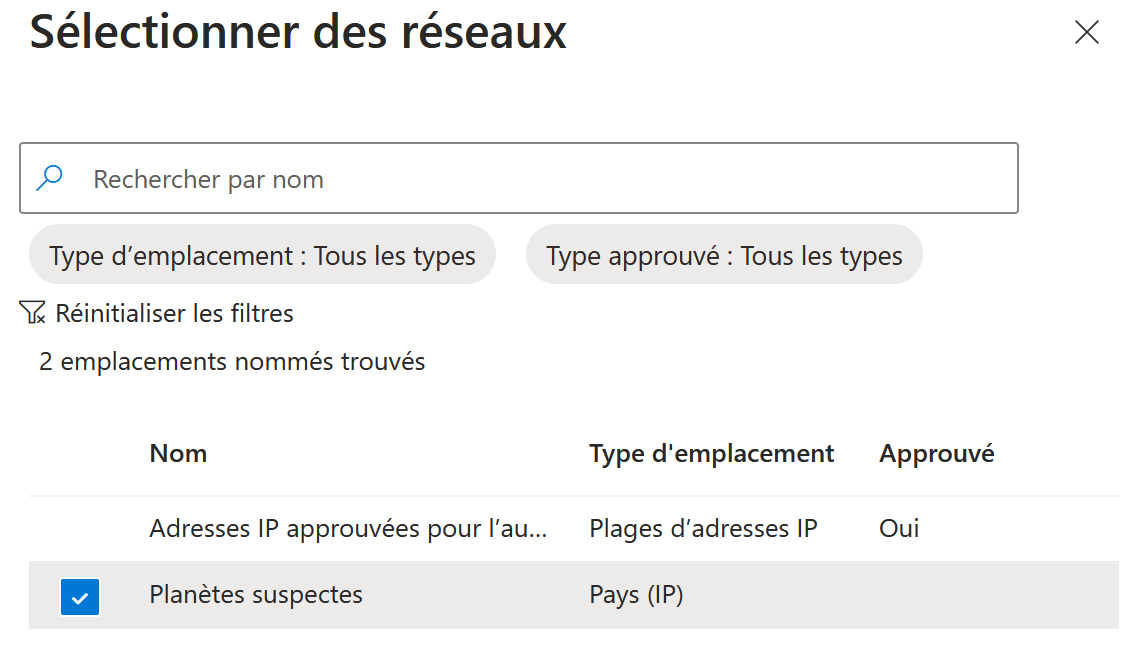
Ce groupe se compose de :

John Wick et Arthur Martin, deux utilisateurs clandestins suspectés par les officiers supérieurs.

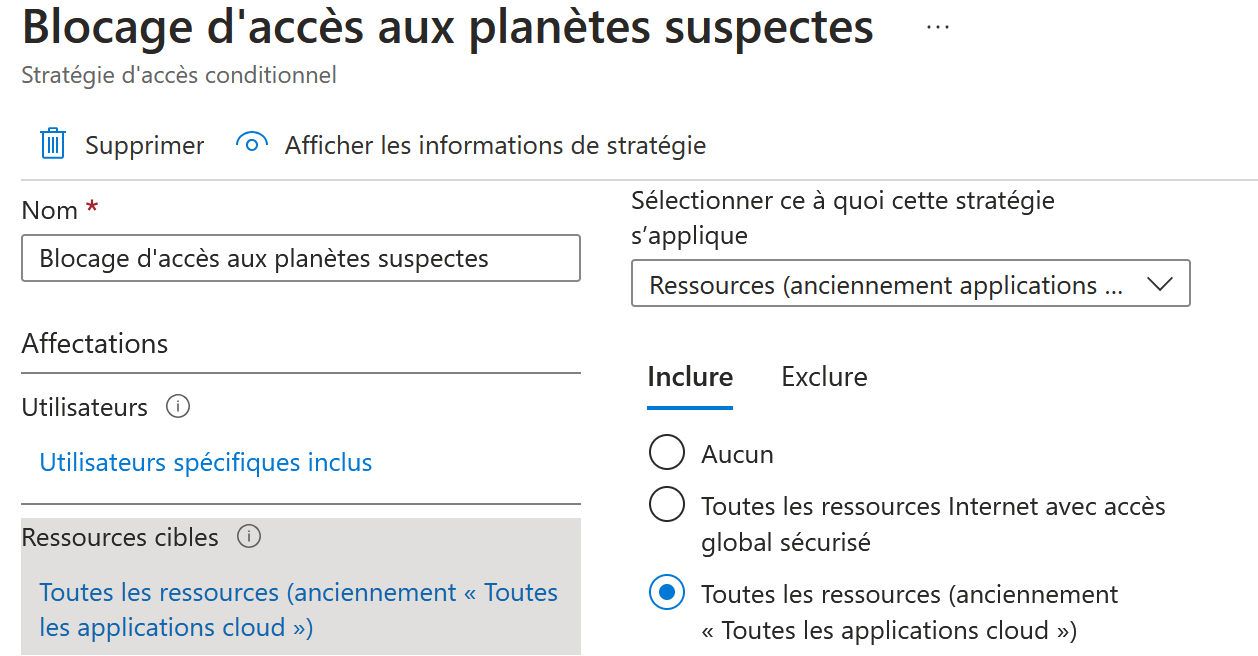


Paramétrer sur “OUI” les conditions d’emplacements avec “Planètes suspectes” :

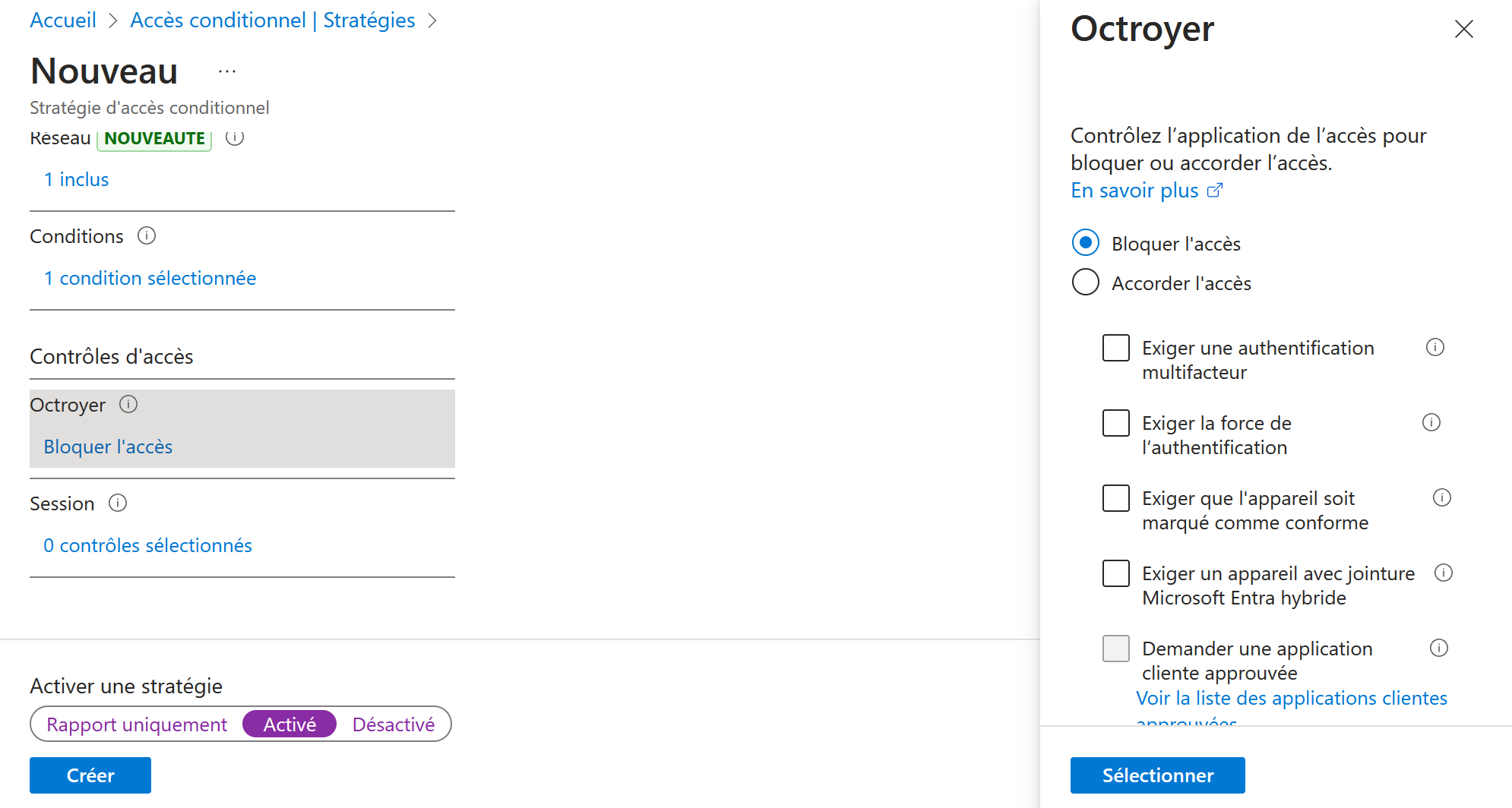
****

****

Sélectionner >Ressources cibles puis ajouter toutes les ressources “toutes les applications cloud”



Pour finir, création de la stratégie pour “ Octroyer puis bloquer l’accès”.

****

* **Simulez des incidents de sécurité, par exemple une tentative de**

**piratage des systèmes du vaisseau, et testez vos procédures de**

**réponse, incluant la réinitialisation des accès et la mise en quarantaine**

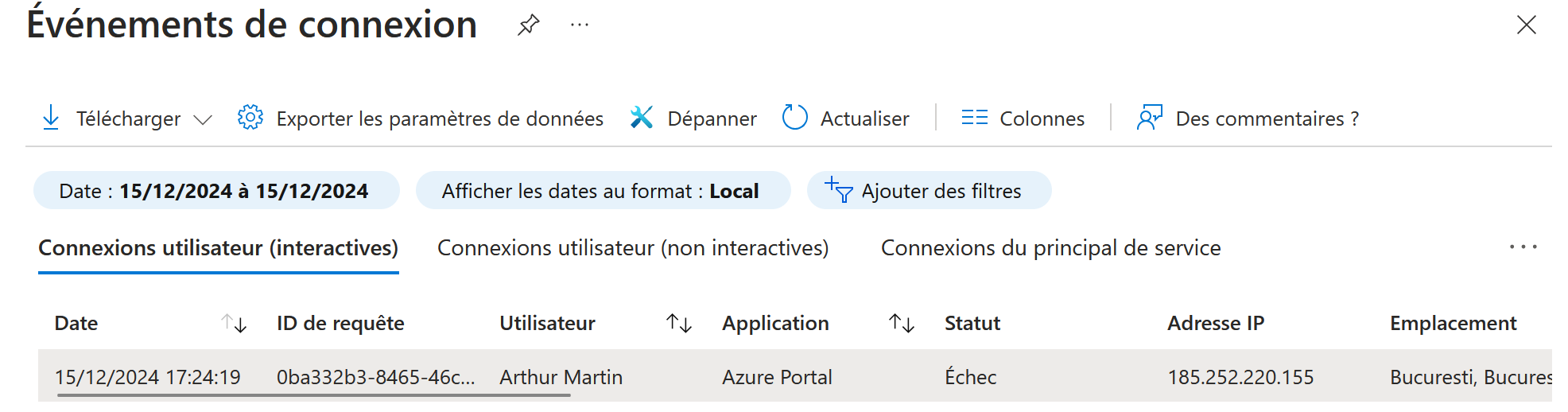
**des systèmes compromis.**

Test de la stratégie avec une connexion depuis une adresse IP inconnus :

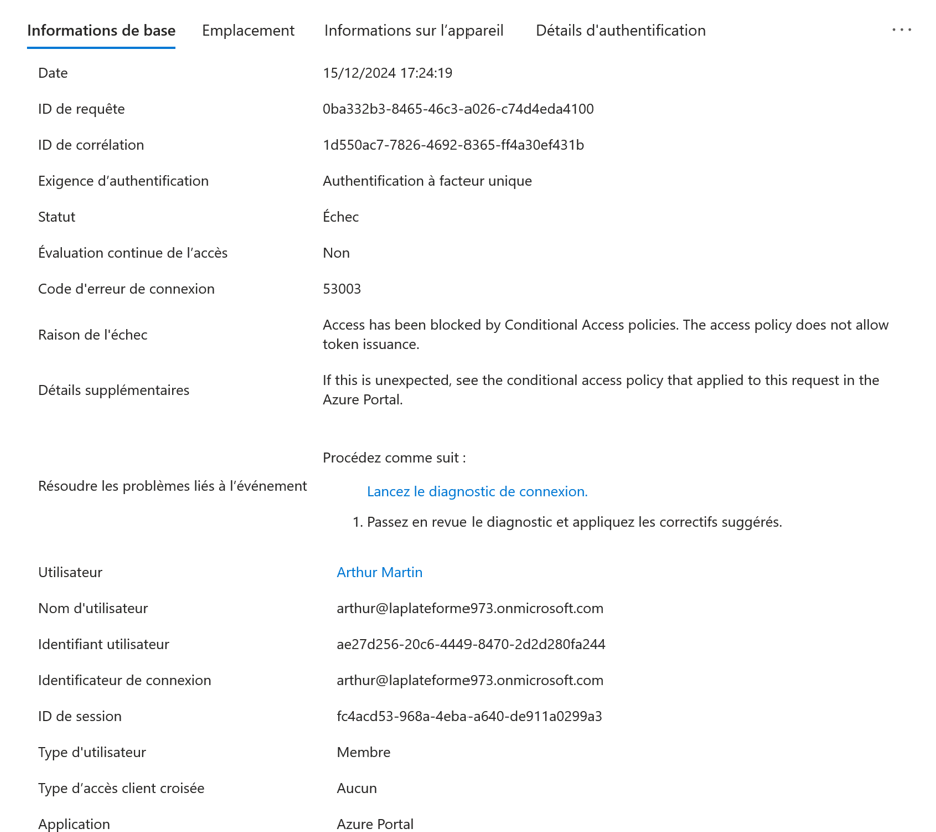


Vérifier les événements de connexion. Pour cela on se rend sur le journal de connexion des utilisateurs puis on vérifie la connexion suspecte.

Identité > Surveillance et Intégrité > Journaux de connexion

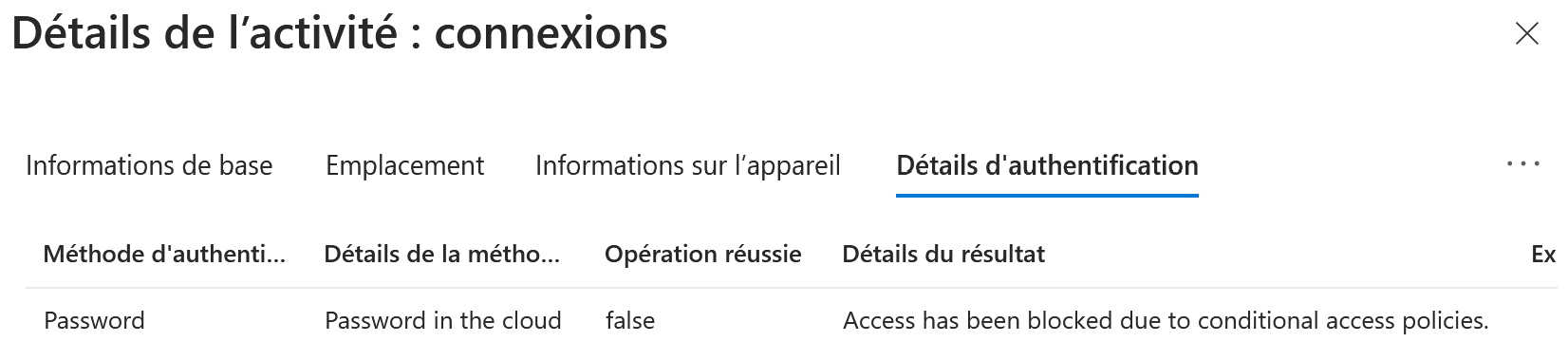


Identifier la menace avec les informations de la requête.



On constate une connexion suspecte et refusée depuis la planète Roumanie.





On constate que notre stratégie d’accès conditionnel à bien fonctionner et à intercepter la connexion inconnue depuis la planète suspecte.