Azure

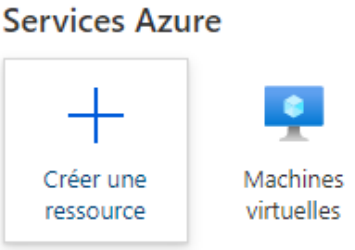
- Redimensionner disque sur VM Azure
- App Password (ADOC)
- Utilisateur Invité
- Powershell Azure : check IP disponible
- Renouvellement Certificat et Jeton Apple sur MDM
- MFA - Désactivation application Authenticator
- Accès Partenaires SSO

Redimensionner disque sur VM Azure

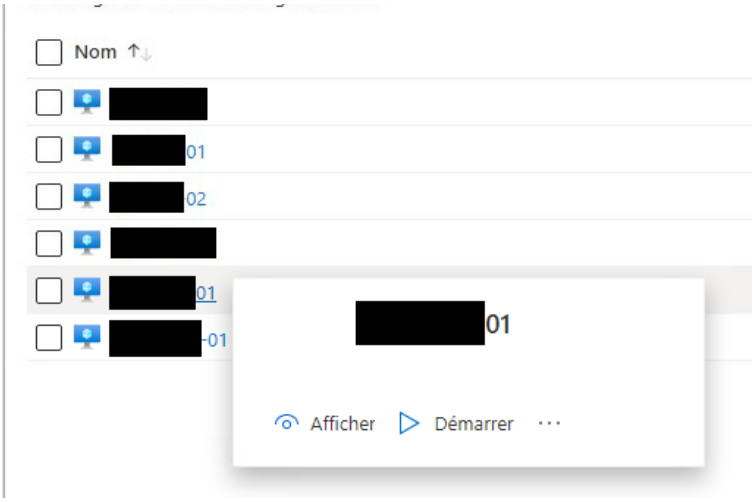
Procédure :

Se connecter au portail Azure du Tenant cible : https://portal.azure.com/#home
Avec un compte ayant les privilèges administrateur

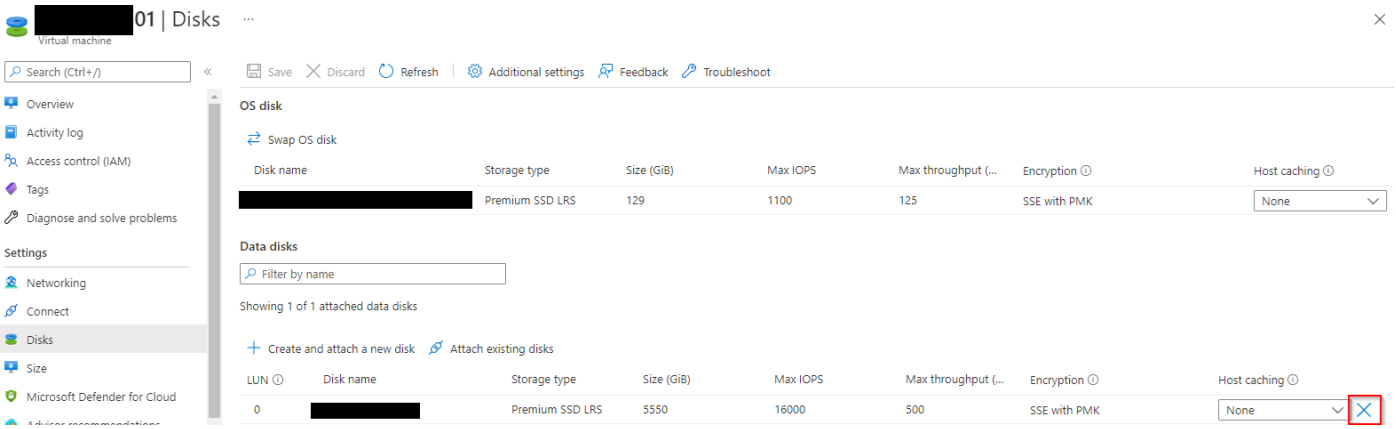
Se rendre sur le service Machines virtuelles :



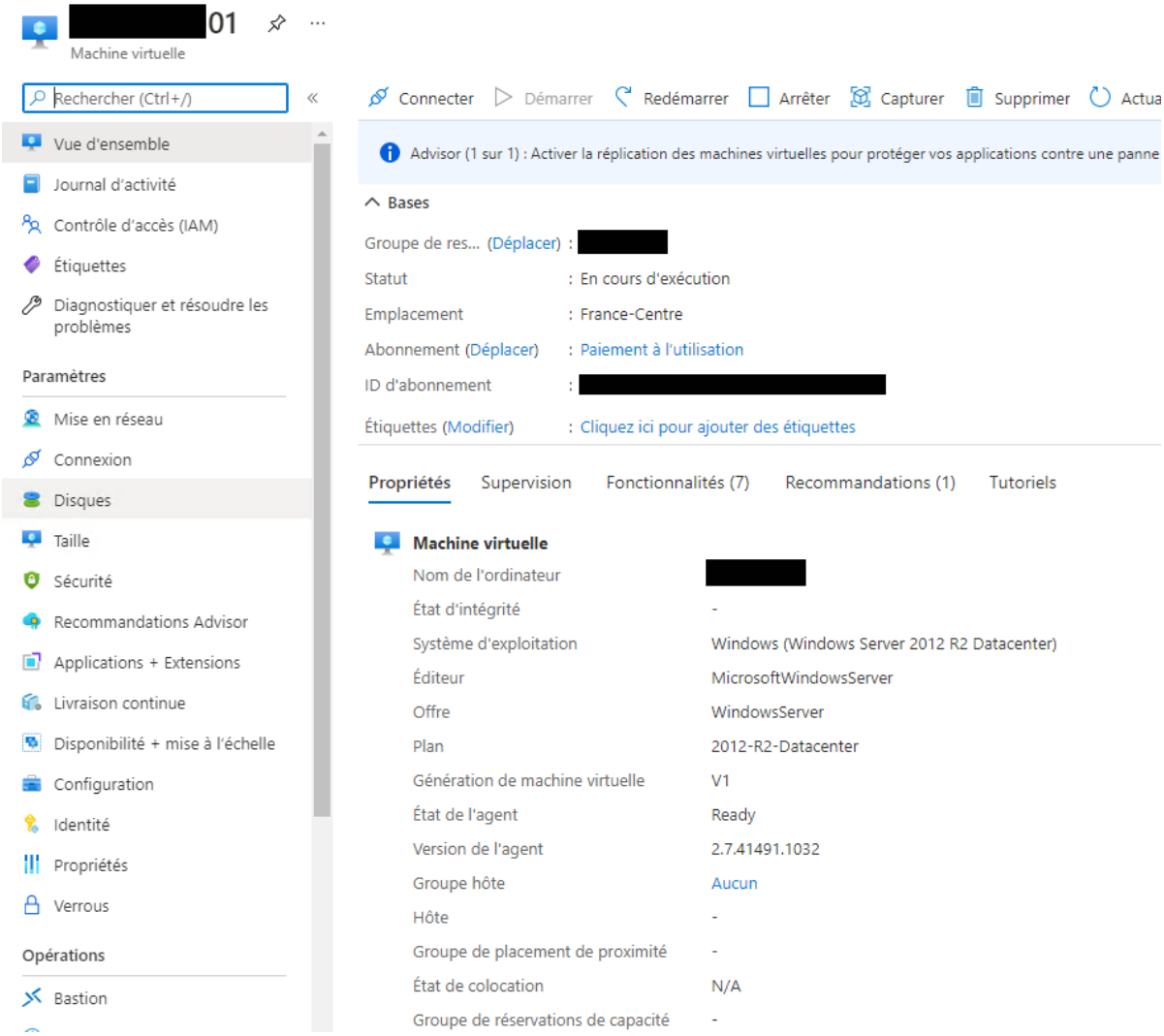
Ouvrir la VM souhaitée :



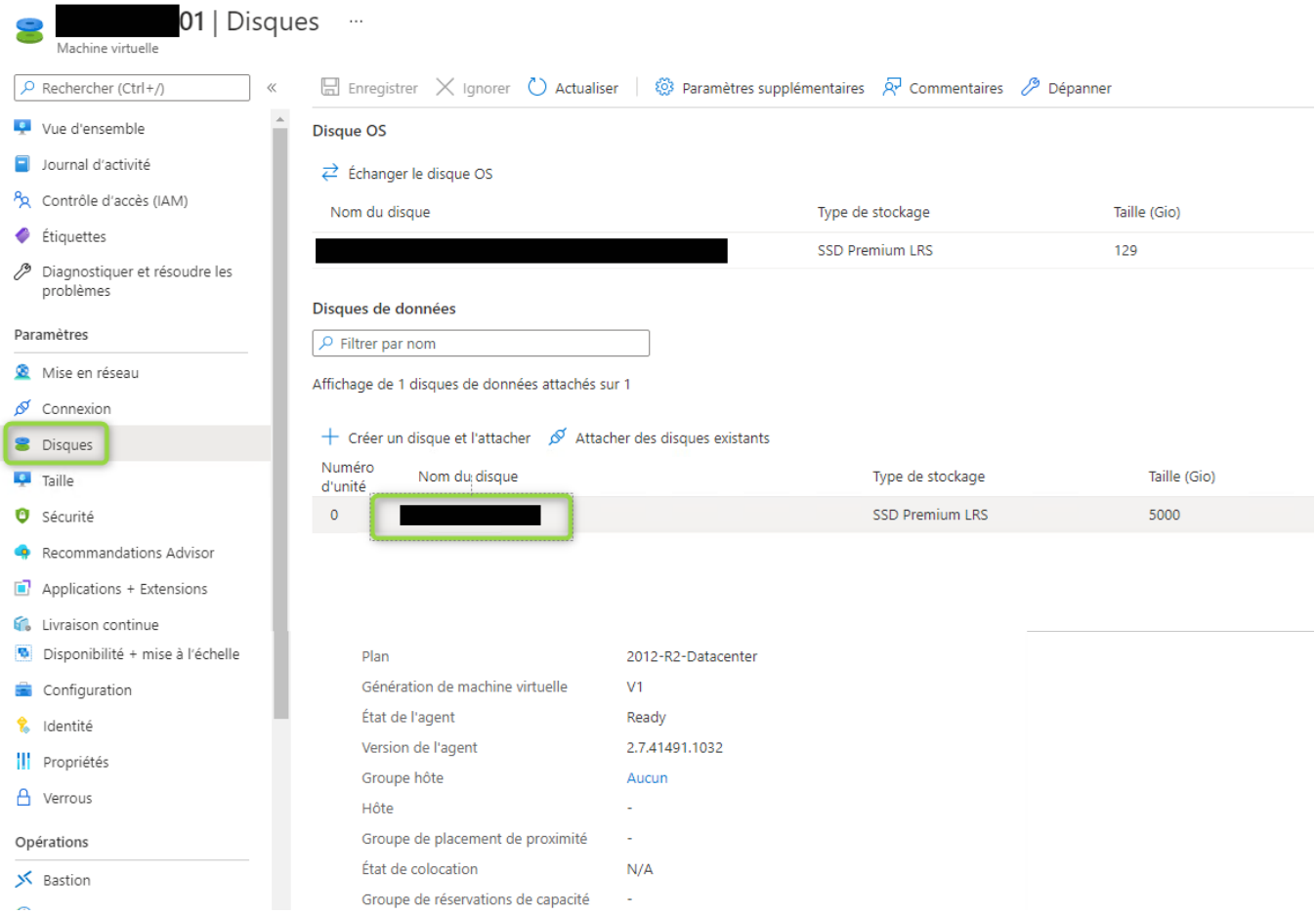
Une fois sur la fiche serveur > allez dans la section "Disks" puis appuyer sur la croix encadrée en rouge afin de désallouer le disque de la VM.



Une fois que l'on est certain d'avoir les accès pour démarrer la VM, procéder à son arrêt.

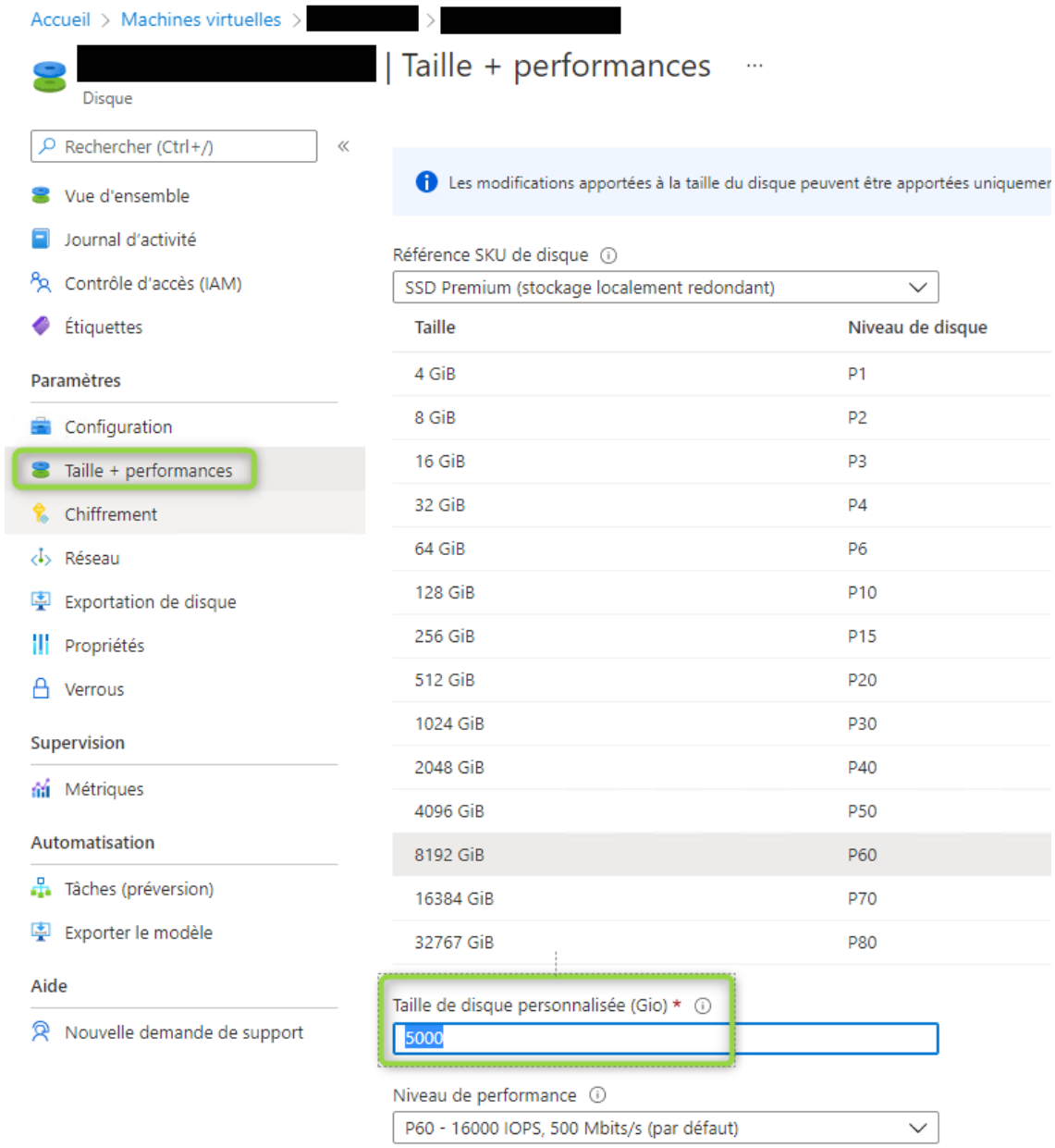


Dans le menu Disques, ouvrir le disque à modifier :

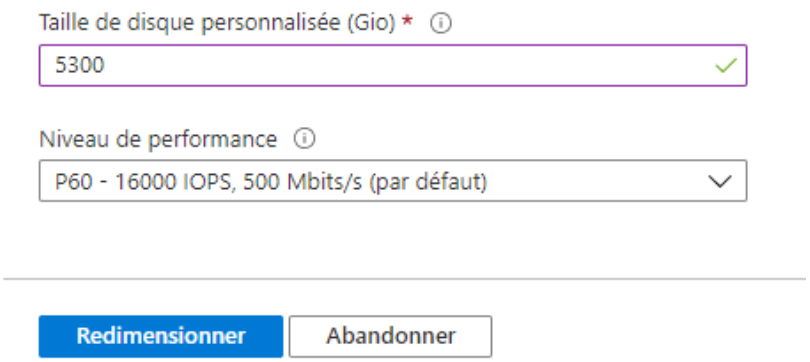


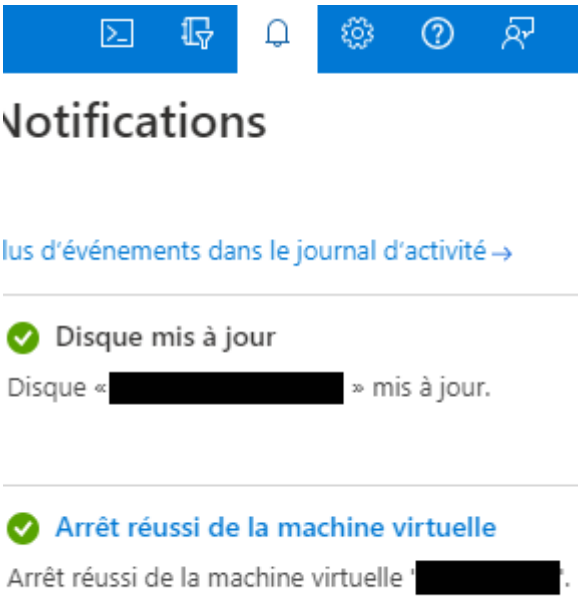
Dans Taille + performance, renseigner la taille du disque en Go
Entrez la taille du disque à créer. Vous êtes facturé le même prix, quel que soit l'espace disque utilisé sur le disque provisionné. Par exemple, si un disque de 200 Gio est provisionné sur un disque de 256 Gio, vous êtes facturé pour le disque de 256 Gio.

> Au préalable il est recommandé de vérifier dans quelle catégorie de taille se trouvera le disque après modifications, un changement de catégorie ou performance entraine une facturation différente pour le client.



Cliquer ensuite sur le bouton redimensionner.



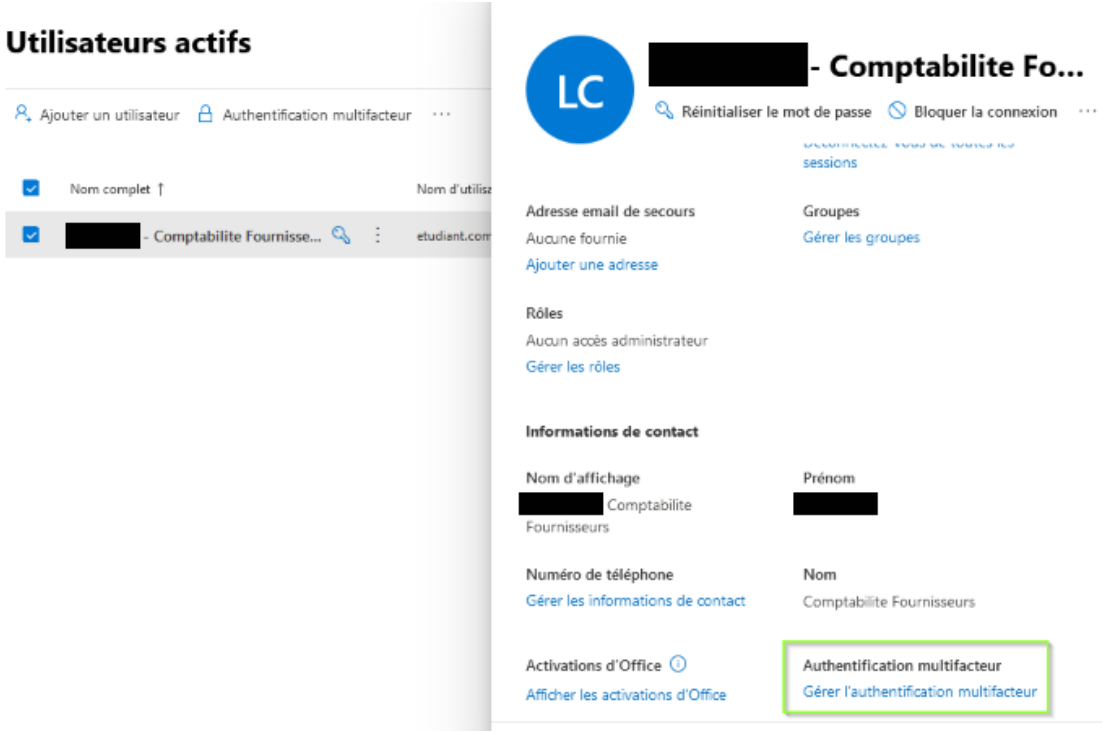


Attendre la fin du traitement dans les notifications
Vérifier que le disque est de nouveau alloué au serveur sinon le faire puis redémarrer la VM.
Vérifier ensuite que la taille du disque a bien été modifier dans le gestionnaire des disques, et augmenter la taille de la partition.

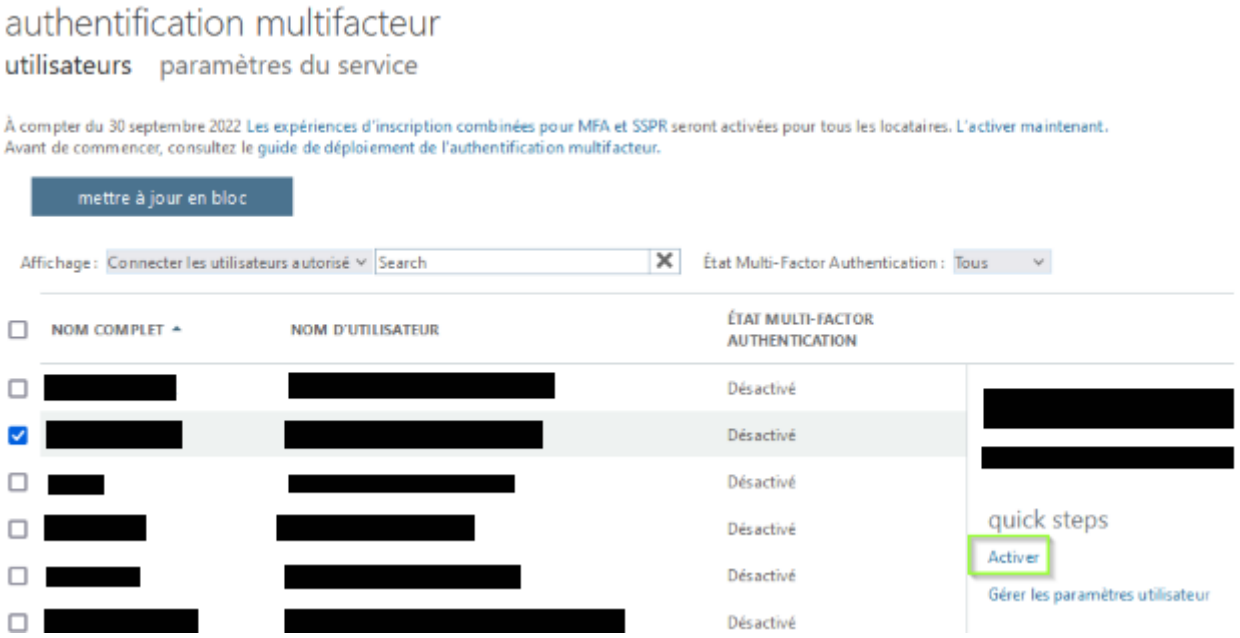
App Password (ADOC)

Il faut activer la MFA pour le compte souhaité en allant sur la fiche utilisateur

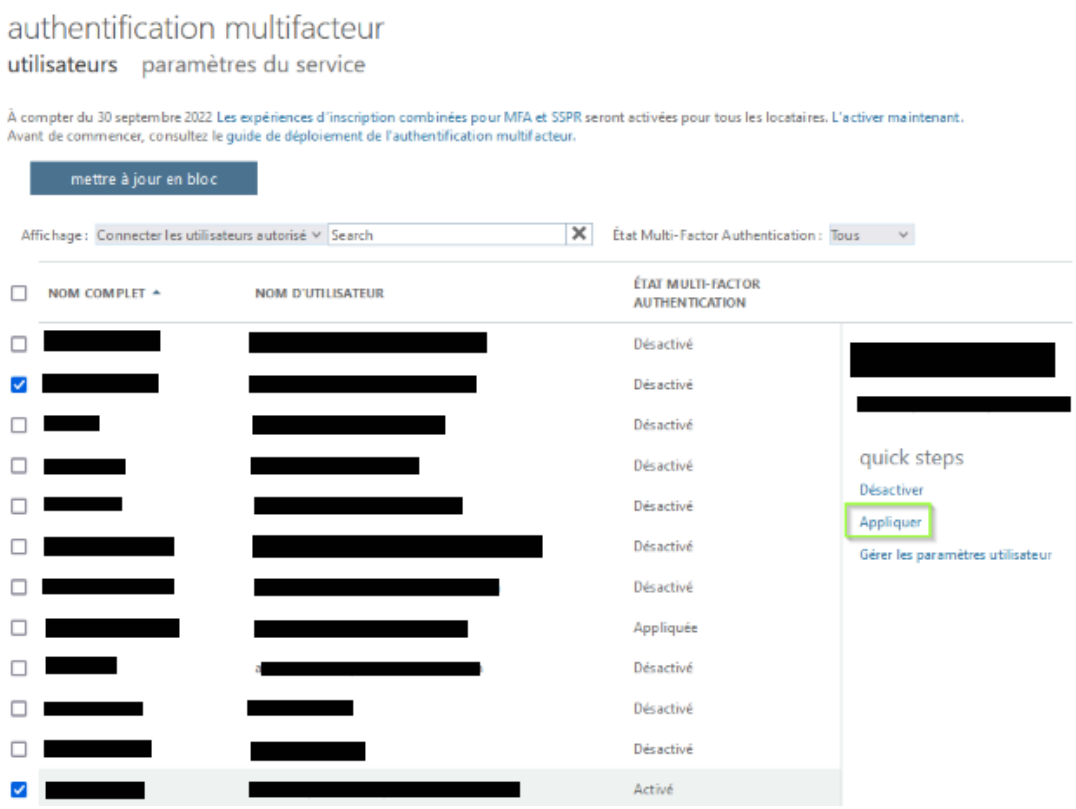
Dans le Centre d'Administartion MS 365 > Utilisateurs Actifs
Cliquer sur l'utilisateur puis Gérer l'authentification multifacteur



Activer sur l'utilisateur



Appliquer sur l'utilisateur

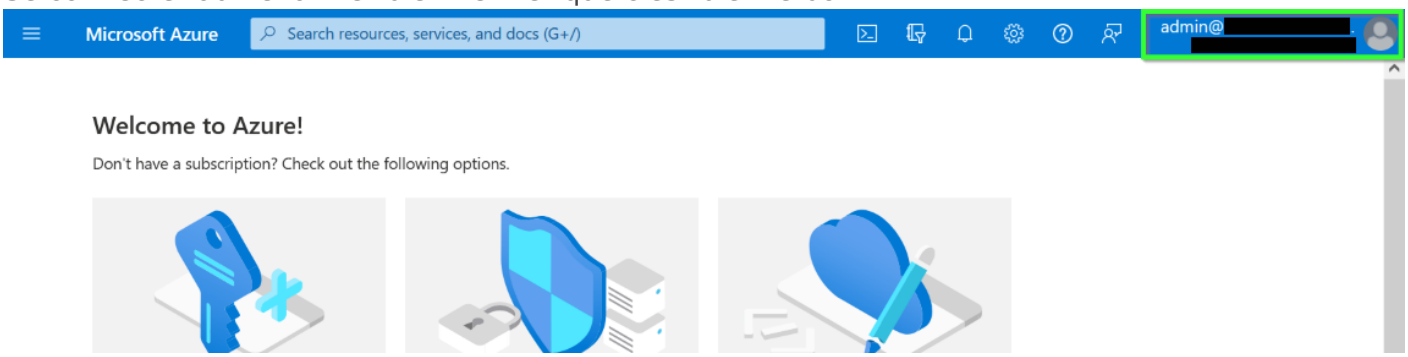


Se connecter au Webmail
Des infos supplémentaires sont demandé dès la première connexion

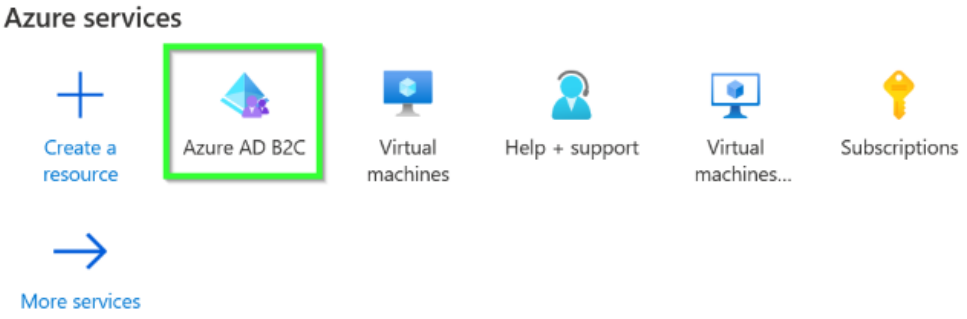
Entrer votre numéro de tél pour la MFA
Entré le code d'authentification reçu par SMS
Copier le App Password dans le KeePass

Utilisateur Invité

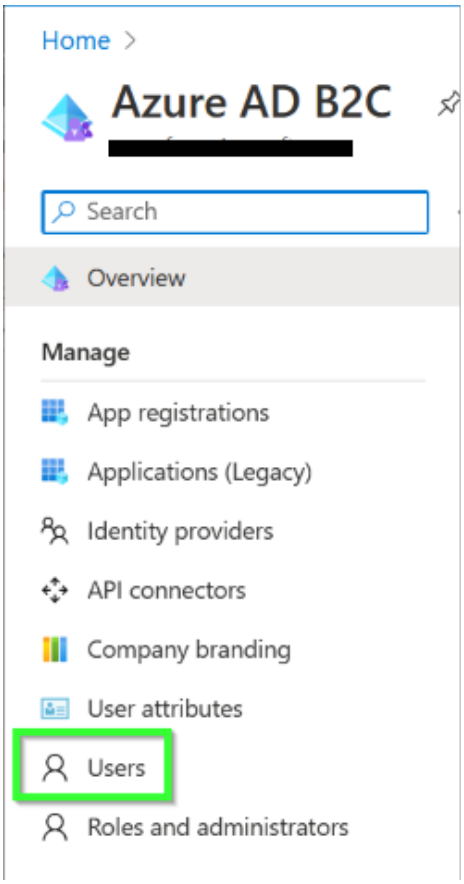
Se connecter au Tenant et bien vérifier que c'est bien le bon



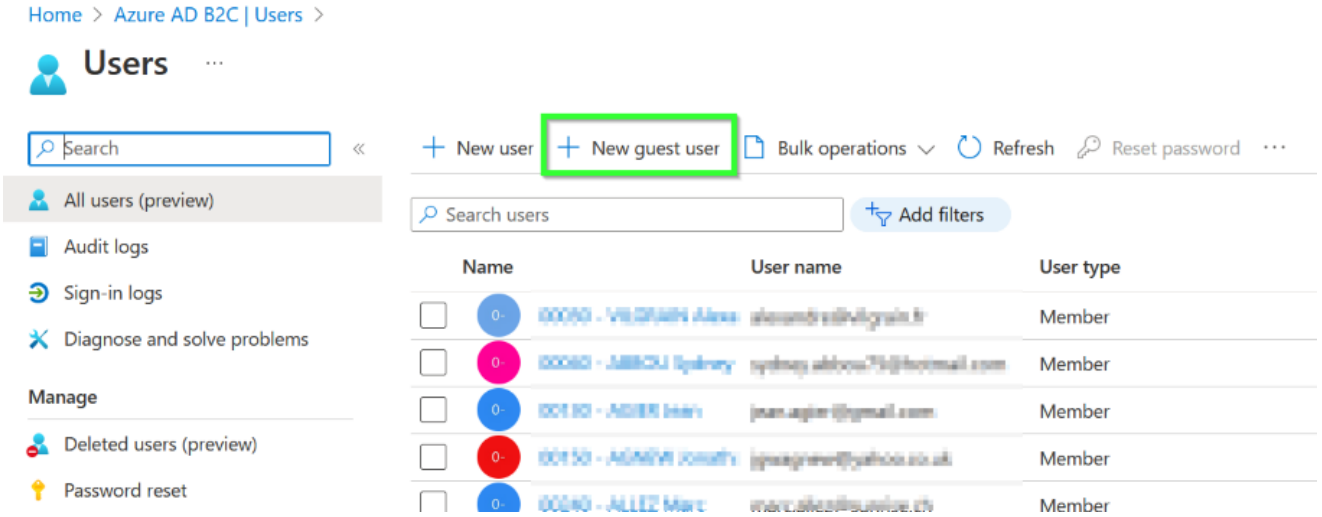
Aller dans Azure B2C



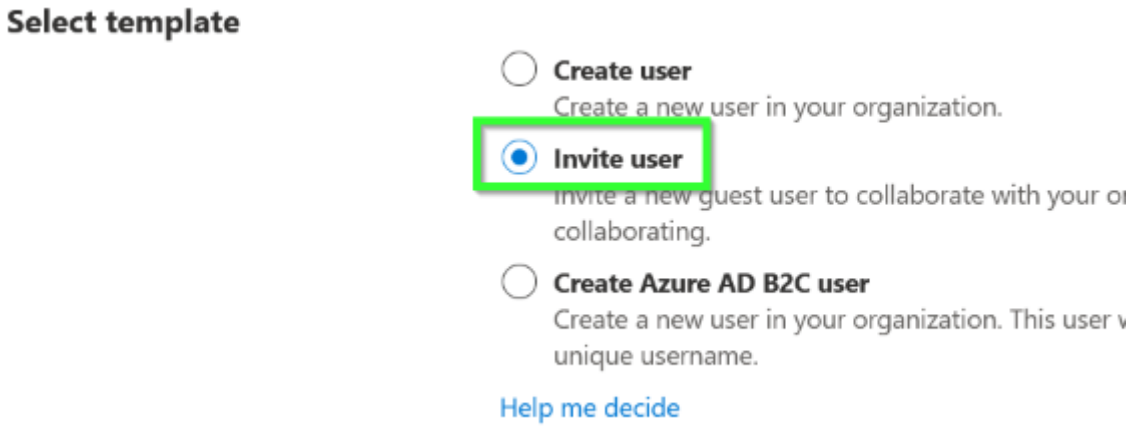
Puis User



Cliquer sur New Guest User



Remplir les champs encadrés



Dans Groups and Roles,
Bien sélectionner un groupe si besoin et/ou un Role si besoin
Dans cette exemple, l'utilisateur est un prestataire qui nous a confirmé qu'il a besoin de gérer les applications donc il est Application Admin.

> Si on vous demande Global Admin, faire confirmer les besoins réels et validé par le DSI (ou équivalent) en lui expliquant les impacts

Le reste des champs est optionnel

Block sign in bloquera la connexion au tenant.
Les autres infos, si vous les avez renseignez les.

Settings

Block sign in: Yes / No

Usage location:

Job info

Job title:

Department:

Company name:

Manager: No manager selected

Powershell Azure : check IP disponible

Au besoin, pour savoir si une ip est disponible sur Azure :

```
Connect-AzAccount
```

Puis

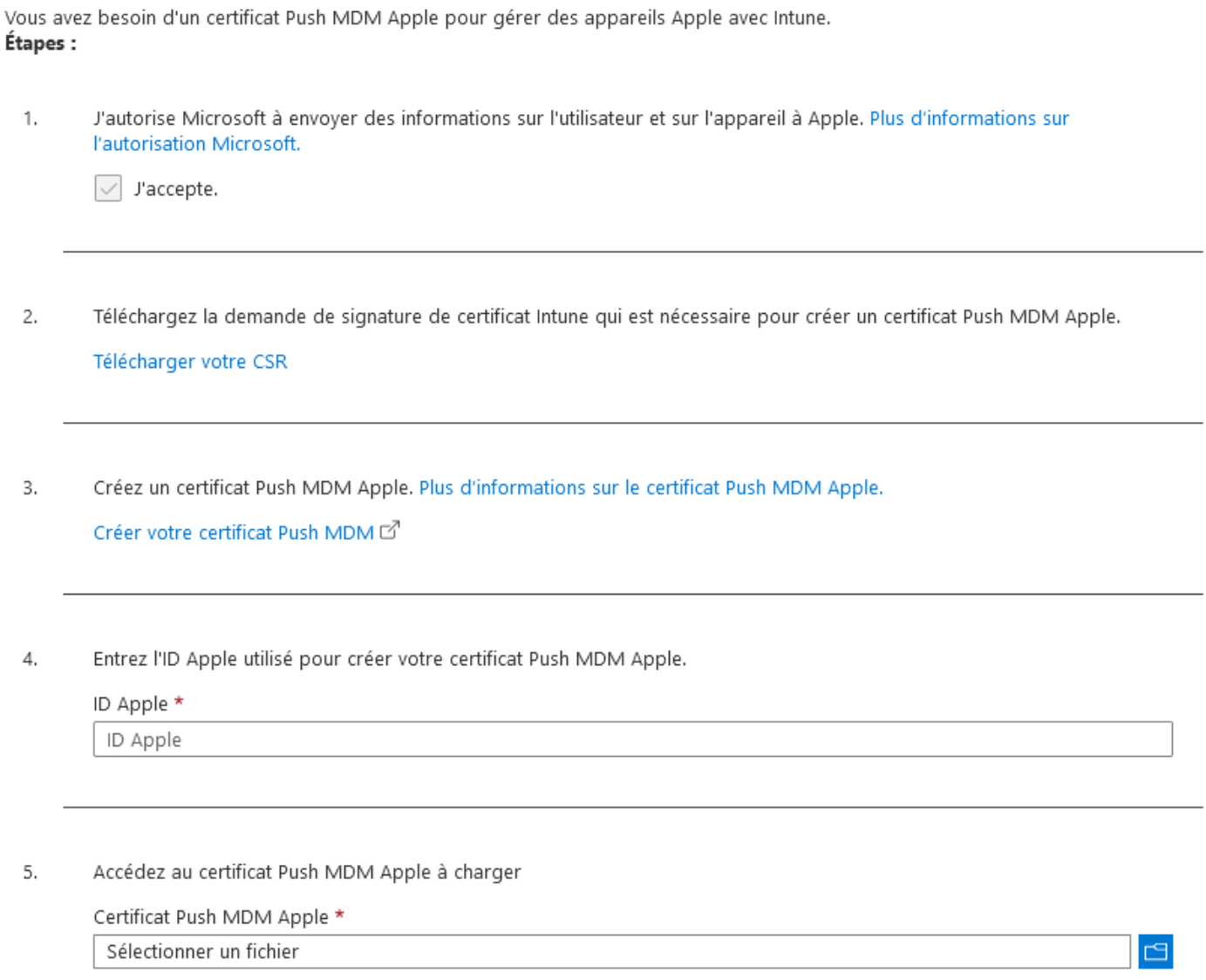
```
Get-AzVirtualNetwork -Name NOMduVNET -ResourceGroupName RESSOURCEGROUP| Test-AzPrivateIPAddressAvailability -IPAddress IPàTESTER
```

Renouvellement Certificat et Jeton Apple sur MDM

Certificat à renouveler tous les ans

1. Se connecter à https://endpoint.microsoft.com/
2. Allez dans "Appareils" > "Inscrire Appareils"
3. Allez dans "Inscription Apple" > "Certificat Push MDM Apple"

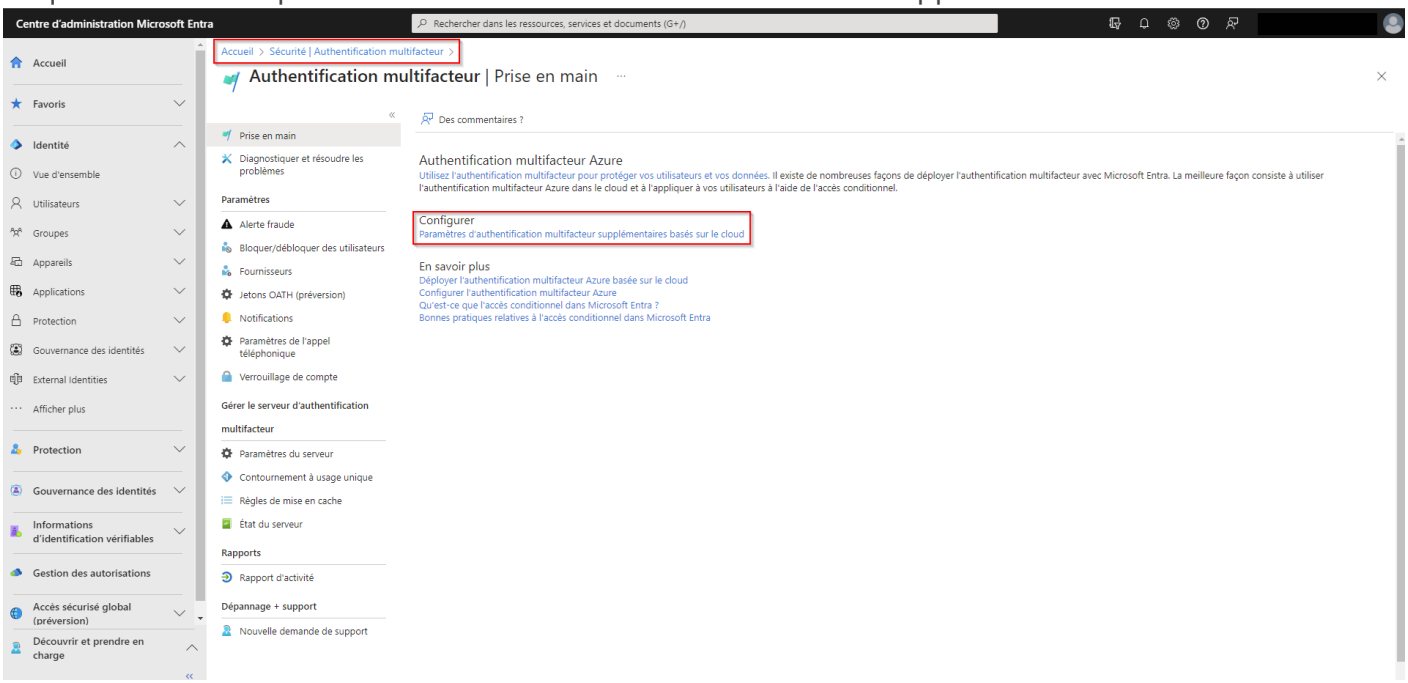
Suivez les étapes de configuration du certificat



MFA - Désactivation application Authenticator

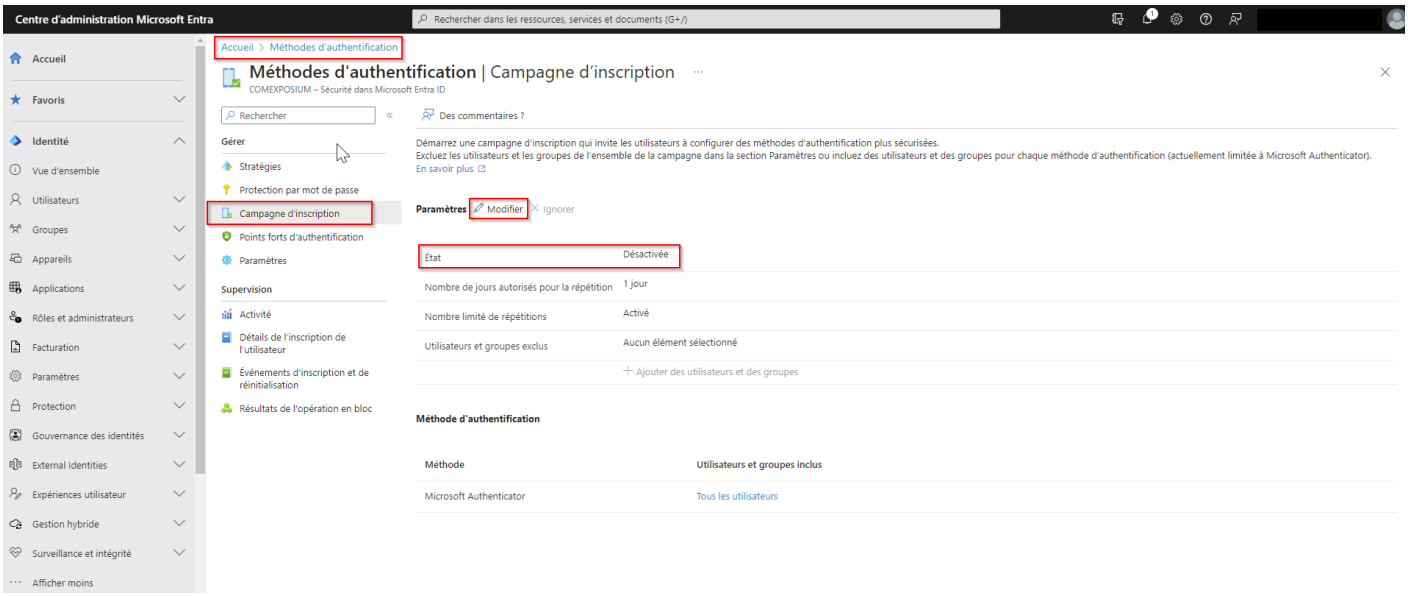
Microsoft force actuellement les utilisateurs à enregistrer l'application Authenticator comme méthode d'authentification via des campagnes.
Voici les étapes à suivre pour désactiver (temporairement) cette méthode :

Se connecter sur Azure et accéder à la page Accueil > Sécurité | Authentification multifacteur.
Cliquer ensuite sur paramètres d'authentification multifacteur supplémentaires basés sur le cloud.



Sur la page qui s'ouvre, décocher la "Notification via l'application mobile" et valider en enregistrant :

Ensuite, se rendre sur la page "Accueil > Méthodes d'authentification" puis cliquer sur "Campagne d'inscription" et modifier.
Changer l'état sur "Désactivée" puis valider.


Centre d'administration Microsoft Entra
Rechercher dans les ressources, services et documents (G+/)
Accueil
Favoris
Identité
Vue d'ensemble
Utilisateurs
Groupes
Appareils
Applications
Rôles et administrateurs
Facturation
Paramètres
Protection
Gouvernance des identités
External Identities
Expériences utilisateur
Gestion hybride
Surveillance et intégrité
Afficher moins
Accueil > Méthodes d'authentification
Méthodes d'authentification | Campagne d'inscription
COMEXPOSIUM – Sécurité dans Microsoft Entra ID
Rechercher
Gérer
Stratégies
Protection par mot de passe
Campagne d'inscription
Points forts d'authentification
Paramètres
Supervision
Activité
Détails de l'inscription de l'utilisateur
Événements d'inscription et de réinitialisation
Résultats de l'opération en bloc
Des commentaires ?
Démarrez une campagne d'inscription qui invite les utilisateurs à configurer des méthodes d'authentification plus sécurisées.
Excluez les utilisateurs et les groupes de l'ensemble de la campagne dans la section Paramètres ou incluez des utilisateurs et des groupes pour chaque méthode d'authentification (actuellement limitée à Microsoft Authenticator).
En savoir plus
Paramètres
Modifier
Ignorer
État
Désactivée
Nombre de jours autorisés pour la répétition
1 jour
Nombre limité de répétitions
Activé
Utilisateurs et groupes exclus
Aucun élément sélectionné
Ajouter des utilisateurs et des groupes
Méthode d'authentification
Méthode
Utilisateurs et groupes inclus
Microsoft Authenticator
Tous les utilisateurs

Accès Partenaires SSO

1. Contexte du Projet

Objectif : Permettre aux collaborateurs de sociétés partenaires d'accéder à un CMS via Single Sign-On (SSO).

Méthode : Azure B2B Collaboration via la Gestion des droits d'accès (Entitlement Management).

Domaines concernés :

- Région 1 : @partenaireA.com, @partenaireB.com

- Région 2 : @partenaireC.com, @partenaireB.com

2. Prérequis Azure (Microsoft Entra ID)

Avant la mise en service, les paramètres de collaboration externe ont été vérifiés dans le locataire cible :

- Inscription en libre-service : Activée.

- Restrictions d'accès : Accès limité aux propriétés et appartenances de leurs propres objets.

- Restrictions de collaboration : Invitations limitées aux domaines autorisés.

3. Configuration des Organisations Connectées

Pour établir la confiance avec les domaines externes, les organisations suivantes ont été créées dans Identity Governance :

- Partenaire A : domaine partenaireA.com

- Partenaire B : domaine partenaireB.com

- Partenaire C : domaine partenaireC.com

Ces organisations permettent à Microsoft Entra ID de reconnaître les annuaires sources des utilisateurs.

4. Création du Paquet d'Accès (Access Package)

Nom : Accès CMS Partenaires

Ressources incluses : Application Enterprise du CMS ou groupe de sécurité dédié.

Rôles assignés : Utilisateur / Membre.

Politique de demande :

- Type : Pour les utilisateurs externes non présents dans l'annuaire.

- Filtrage : Organisations connectées autorisées.

- Approbation : Requise par un sponsor interne.

5. Cycle de Vie et Sécurité

Révisions d'accès : Recommandées tous les 6 mois.

Expiration : Configurée automatiquement pour éviter les comptes inactifs.

Sécurité : Garantit la conformité et la protection des ressources de l'organisation.

Guide Utilisateur

1. Objectif

Ce guide explique comment les partenaires accèdent au CMS via le Single Sign-On (SSO).

2. Prérequis

Les utilisateurs doivent disposer :

- D'une adresse e-mail professionnelle appartenant à un domaine autorisé.

- D'un accès à l'URL du portail MyAccess fournie par l'organisation.

- D'une connexion Internet et d'un navigateur web moderne.

[Emplacement pour capture d'écran du portail Microsoft Entra ID]

3. Processus de Demande d'Accès

Étape 1 : Accéder au portail MyAccess via le lien fourni.

Étape 2 : Se connecter avec son adresse e-mail professionnelle.

Étape 3 : Sélectionner le paquet d'accès 'Accès CMS Partenaires'.

Étape 4 : Soumettre la demande pour approbation.

4. Connexion au CMS

Étape 1 : Accéder à la page de connexion du CMS.

Étape 2 : Cliquer sur 'Se connecter avec Microsoft'.

Étape 3 : S'authentifier avec son compte professionnel.

Étape 4 : Accéder au CMS sans avoir à saisir un nouveau mot de passe.