La Minute CLOUD de JULES & LÉA

Azure
Privileged Identity Management #1

Aujourd'hui, nous allons parler sécurité avec **Privileged Identity Management (PIM)**

C'est une fonctionnalité disponible dans Microsoft Entra ID ?

Oui exactement.

PIM permet de **gérer**, **contrôler** et **superviser** l'accès aux ressources critiques au travers d'**accès privilégiés** sécurisés.

Et cela s'applique uniquement à Azure ?

Non pas du tout !

Tu peux évidemment protéger tes ressources Azure, mais aussi Microsoft Entra ID, Microsoft 365, ou encore Microsoft Intune.

Génial

Et c'est une fonctionnalité de base ?

Non il faut une licence M**icrosoft Entra ID P2** ou **Microsoft Entra ID Governance**.

Entendu. Mais qu'est ce que cela apporte d'utiliser PIM ?

Une couche de sécurité supplémentaire, je m'explique.

A notre époque où les entreprises exécutent de nombreuses charges de travail dans le Cloud, en stockant des données sensibles.

L'idée est de réduire les risques liés aux utilisateurs qui possédent des hauts privilèges, comme Administrateur Global.

Je comprend mieux !

Il permet aussi d'activer **Just-in-time (JIT)**.

JIT permet d'autoriser l'accès à des VMs pendant un temps donné.

Ainsi tu autorises l'accès uniquement lorsque tu en as besoin ?!

Exactement

Suivante

La Minute CLOUD de JULES & LÉA

Azure
Privileged Identity Management #2

Pour revenir à PIM, il permet d'élever ses privilèges, pendant une période définie.

C'est génial, mais comment vérifier qui fait quoi ?

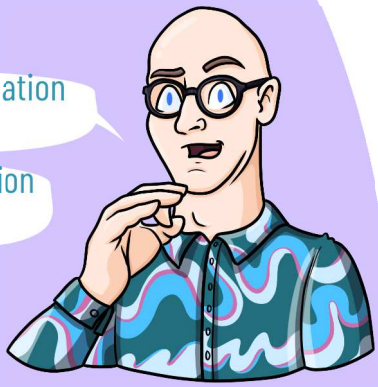
Excellente question.

Il existe plusieurs mécanismes pour cela.

Je m'en doutais !

Tout d'abord, il existe un process d'approbation qui peut être automatique ou manuel.

Ensuite, tu dois, renseigner une justification pour réaliser une élévation de privilèges.



Je suppose que toutes les actions sont tracées ?

Evidemment.

Avec le fameux Qui, Quand, Quoi ...

De plus, une notification est envoyée par mail à chaque élévation.

L'idée est donc que tout soit prêt en cas d'audit.

C'est presque un audit clé en main !

Tu peux aussi effectuer des **Review d'audit** pour vérifier si du ménage doit être réalisé au niveau des permissions.

C'est vraiment génial !

Et comment cela se configure concrètement ?

Simplement en activant PIM, ensuite c'est essentiellement de la configuration.

Et évidemment l'**authentification multi-facteur (MFA)** est forcément présente.

Evidemment !

Deux notions sont importantes dans la configuration de PIM :

Les **rôles actifs**,

Les **rôles éligibles**.

Suivante

La Minute CLOUD de JULES & LÉA

Azure
Privileged Identity Management #3

Un **rôle éligible**, est celui que tu peux t'attribuer temporairement.

Alors qu'un **rôle actif**, est soit un rôle éligible que tu as activé, soit un rôle permanent qui t'es affecté.

Si je résume, je peux avoir un rôle permanent **Reader**, et un rôle éligible **Global Admin**, que je peux activer à la demande ?

Tu as tout compris.

Il est conseillé d'avoir un rôle permanent avec **le moins de permissions possible**, et faire une élévation de privilèges uniquement quand c'est nécessaire.

Et la création d'un rôle éligible n'est pas trop complexe ?

Non pas du tout.

Tu sélectionnes le rôle que tu souhaites attribuer,

la durée ou la période pendant laquelle l'élévation sera active,

et le scope sur lequel l'appliquer, par exemple un RG.

Et un approbateur si je souhaite avoir une validation en amont ?

On croirait que tu as déjà utilisé PIM.

Pas encore, mais je vois très bien les cas d'usage.

Et comme toujours, la documentation officielle est parfait pour répondre aux questions que tu te poses avant de te lancer.

PIM est idéal pour renforcer la sécurité, car il est possible d'élever ses privilèges à la demande, sans pour autant conserver des accès permanents qui ne sont pas toujours justifiés.

AMAZING

Fin

La Minute CLOUD de JULES & LÉA

Merci à vous !

Si vous souhaitez continuer à **apprendre**, de façon ludique, sur **l'écosystème Azure**, et ne rater aucune de nos illustrations ...

... N'hésitez pas à vous abonner sur :

https://aka.ms/grow-una

https://www.youtube.com/@grow-una

Et si le contenu vous plaît, partagez-le ;o)

A très vite !

GROW UNA