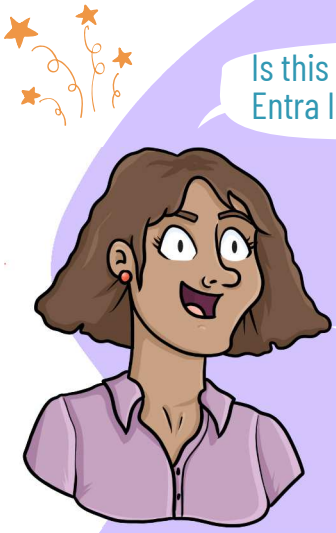
La Minute CLOUD de JULES & LÉA

Azure
Privileged Identity Management #1

Today we are going to talk security with **Privileged Identity Management (PIM)**

Is this a feature available in Microsoft Entra ID?



Yes exactly.

PIM allows you to **manage**, **control** and **supervise** access to critical resources through secure **privileged access**.

And this only applies to Azure?

No not at all !

You can obviously protect your Azure resources, but also Microsoft Entra ID, Microsoft 365, or even Microsoft Intune.

Alright.

And this is a basic functionality?

Nope. You need a Microsoft Entra ID P2 or Microsoft Entra ID Governance license.

Got it. But why use PIM?

It affords an additional layer of security, let me explain.

Today companies run many workloads in the Cloud, storing sensitive data.

The goal of PIM, is to reduce the risks associated to users with high privileges, such as Global Administrator

I understand better !

It also allows you to activate Just-in-time (JIT).

JIT allows you to authorize access to VMs for a period of time.

So you only allow access when you need it?!

Exactly!

Next

La Minute CLOUD de JULES & LÉA

Azure Privileged Identity Management #2

Come back to PIM. It allows you to elevate your privileges for a defined period.

That's great, but how do you check who's doing what?

Excellent question.

There are several mechanisms for this.

I guess!

First of all, there is an approval process which can be automatic or manual.

Then, you must provide a justification to carry out an elevation of privileges.

I assume all actions are traced?

Of course!

With the famous Who, When, What...

In addition, notifications are sent by email at each elevation.

The idea is therefore to have everything ready in the event of a security audit.

It's almost a turnkey audit!

You can also carry out **audit reviews** to check if any cleaning needs to be done in terms of permissions.

It's really awesome.

And how is this configured in practice?

Simply by enabling PIM, then it's basically configuration.

And obviously **multi-factor authentication (MFA)** is a key factor.

Obviously !!

Two notions are important in the configuration of PIM:

Active roles,

Eligible roles.

Next

La Minute CLOUD de JULES & LÉA

Azure
Privileged Identity Management #3

An **eligible role** is one that you can assign to yourself temporarily.

However an **active role** is either an eligible role that you have activated, or a permanent role that is assigned to you.

If I summarize, I can have a permanent Reader role, and an eligible Global Admin role, which I can activate on demand?

You have understood everything.

Knowing that it is better to have a permanent role with least privileges as possible, and elevate your permissions only when you need them.

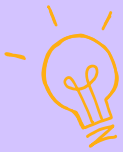
And creating an eligible role isn't too hard?

No not at all.

You select the role you wish to assign,

the duration or period during which the elevation will be active,

and the scope on which to apply it, for example an RG.



And an approver if I want to have validation process?

It looks like you've already used PIM.

Not yet, but I can clearly see the use cases in which it would be interesting.

And as always, the official documentation is perfect for answering any questions you have before getting started.

PIM is ideal for strengthening security with **least privilege** concept. We can elevate privileges on demand, without maintaining permanent access which is not always justified.

AMAZING

End

La Minute CLOUD de JULES & LÉA

Thank you!

If you want to continue **learning** in a fun way about the **Azure ecosystem**, and not miss any of our illustrations ...

... Feel free to subscribe at:

https://aka.ms/grow-una

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

If you like our work, please share it ;o)

See you soon!

GROW UNA