La Minute CLOUD de JULES & LÉA

Azure RBAC #1

Hello Thomas, could you explain us, how the access rights are managed on Azure ?

It's based on the **Role Based access Control** (**RBAC**), that is a system of access control based on the roles of customers. However, it's not specific to Azure.

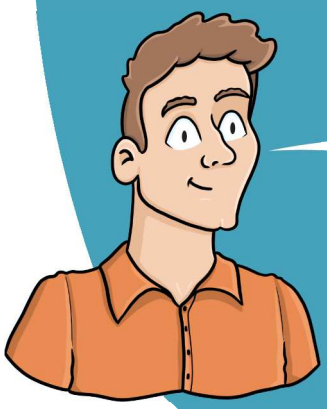
This mechanism, give to Azure administrators, the ability to manage access on Azure resources from identities hosted into **Azure AD**. This is called role assignment which is divided into **3 elements**.

It seems more complicated than I thought !

Not at all, you'll see. The 1st one is the **security principal**, that is to whom access is assigned. This can be a user, usergroup, SPN* or MSI**

The 2nd element corresponds to the **role definition**. It includes the permitted and/or prohibited actions that are assigned. Example, we authorize the creation of VMs but not the deletion.

And finally the last element is the **scope**, on which the rights are applied.



We could summarize:
To whom,
What,
On what !

Source : Microsoft

In fact, it is not more complicated than that.

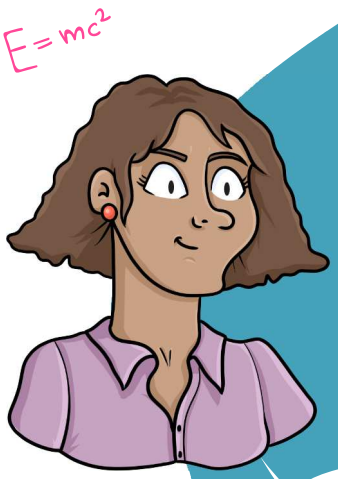
suivante

*SPN : Service Principal Name
**MSI : Managed System Identity

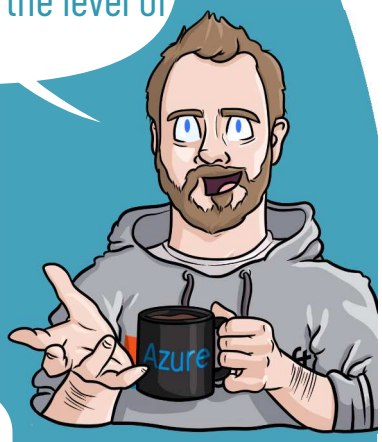
La Minute CLOUD de JULES & LÉA

Azure RBAC #2

It's even quite simple. And this only applies at the resource level ?



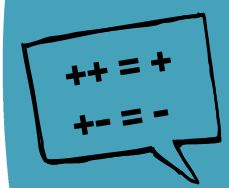
No. **RBAC** can be applied at the level of **Management Groups (MG)** which can group together other **MGs** or **subscriptions**, at the level of **subscriptions**, at the level of **Resource Groups (RG)** and finally at the level of the **resources** themselves.



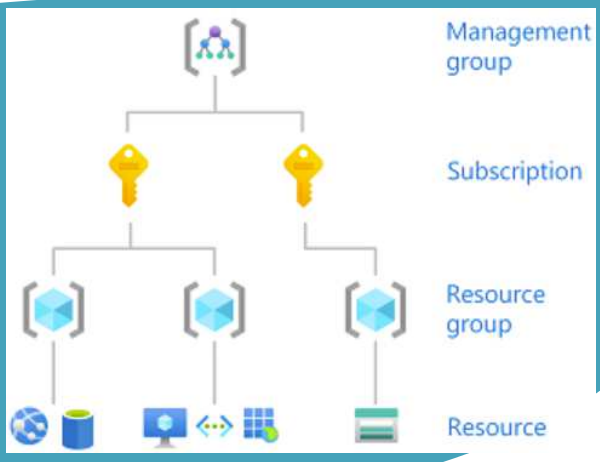
And what happens if a user is granted rights at different levels ?

It depends. By default, the rights are added together. Example, if you have the right to create VMs at the level of a **subscription**, but only the right to read on a **RG**, you will inherit the rights of the subscription and therefore be able to create VMs in this **RG**.

On the other hand, **an unauthorized action prevails over an authorized action**. Continuing the previous example, but this time you are not allowed to create VMs on this **RG**, so this one wins, even if you are allowed to create them at the **subscription** level.



Good to know, a prohibited action always prevails over an authorized action, whatever the level on which they apply!



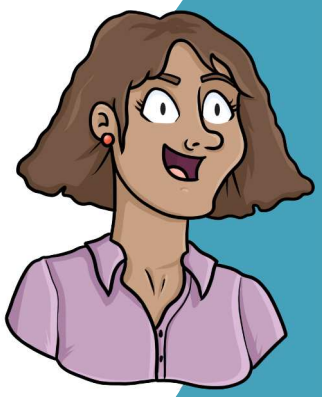
Source : Microsoft

suivante

La Minute CLOUD de JULES & LÉA

Azure RBAC #3

It must be long and tedious to select the rights to apply?!



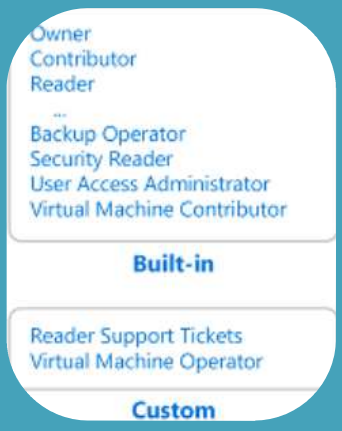
Again it's really simple. Microsoft has introduced the notion of **Built in roles** which are already preconfigured and which you can use.

We can mention the **Owner** role, which has all the rights. The **Contributor** role which has all the rights except managing access to resources. Or even the **Reader** role which allows read-only access.

Currently, there are more than **240 built in roles** !

Really interesting, but if we want specific access right ?

Source : Microsoft



Microsoft has thought of everything. It is possible to **create your own roles** by assigning or refusing the actions of your choice, in an extremely granular way. Within the same role, you can **combine authorized actions and prohibited actions**, without any problem.

Because **RBAC is a global service**, it can be used on resources in any region.

As you can have resources from different regions at the level of a **subscription** or an **RG**, the management of rights becomes very simple.

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 ...

GROW UNA

... Feel free to subscribe on Linkedin at:

https://aka.ms/grow-una

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

See you soon !