La Minute CLOUD de JULES & LÉA

Azure RBAC #1

Hello Thomas, tu pourrais nous expliquer de quelle manière sont attribués les droits sur Azure ?

C'est basé sur le **Role Based access Control** (**RBAC**), qui est un système de contrôle d'accès en fonction du rôle. En revanche, il n'est pas spécifique à Azure.

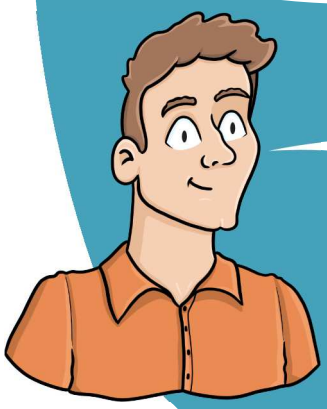
Ce mécanisme, permet de gérer les accès sur les ressources Azure, à partir des **identités** stockées dans **Azure AD**. On parle alors d'attribution de rôles qui se décompose en **3 éléments** distincts.

Cela semble plus compliqué que ce que je pensais !

Non pas du tout, tu vas voir. Le 1er est le **principal de sécurité**, c'est-à-dire à qui on attribue les accès. Cela peut être un utilisateur, un groupe d'utilisateurs, un SPN* ou une MSI**

Le 2ème élément correspond à la **définition du rôle.** Il englobe les actions autorisées et/ou interdites qui sont attribuées. Exemple, on autorise la création de VMs mais pas la suppression.

Et enfin le dernier élément, est l'**étendue**, c'est-à-dire le périmètre sur lequel sont appliqués les droits.



On pourrait donc résumer :
A qui,
Quoi,
Sur quoi !

Source : Microsoft

Effectivement, ce n'est pas plus compliqué que cela.

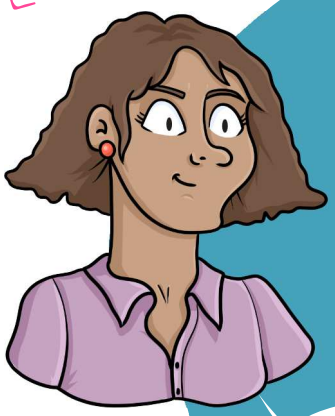
suivante

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

La Minute CLOUD de JULES & LÉA

Azure
RBAC #2

C'est même plutôt assez simple.
Et cela ne s'applique qu'à l'échelle des ressources?

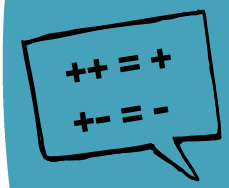


Non. Le **RBAC** peut s'appliquer au niveau des **Management Groups** (**MG**) qui peuvent regrouper d'autres **MG** ou bien des souscriptions, au niveau des **souscriptions**, au niveau des **Resource Groups** (**RG**) et enfin au niveau des **ressources** elles mêmes.

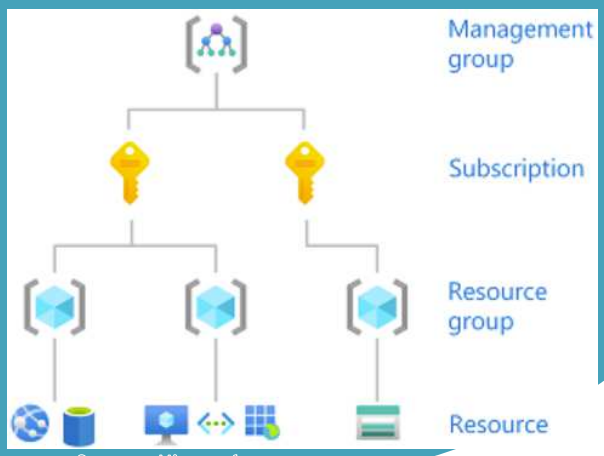
Et que se passe t'il, si on accorde à un utilisateur des droits à différents niveaux ?

Cela dépend. Par défaut, les droits s'additionnent entre eux. Exemple, si tu as le droit de créer des VMs au niveau d'une **souscription**, mais uniquement le droit en lecture sur un **RG**, tu vas hériter des droits de la souscription et donc pouvoir créer des VMs dans ce dit **RG**.

En revanche, **une action non autorisée, l'emporte sur une action autorisée**. En reprenant l'exemple précédent, mais cette fois-ci, tu n'es pas autorisé à créer de VMs sur ce **RG**, alors celui-ci l'emporte, même si tu es autorisé à en créer au niveau de la souscription.



Bon à savoir, une action interdite l'emporte toujours par rapport à une action autorisée, quelque soit le niveau sur lequel elles s'appliquent !



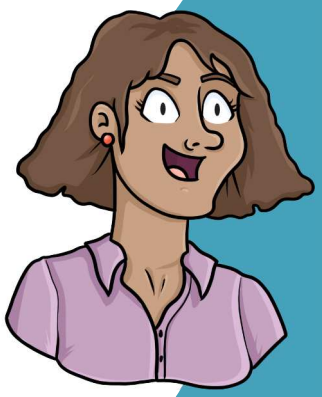
Source : Microsoft

suivante

La Minute CLOUD de JULES & LÉA

Azure
RBAC #3

Cela doit être long et fastidieux de sélectionner les droits à appliquer ?!



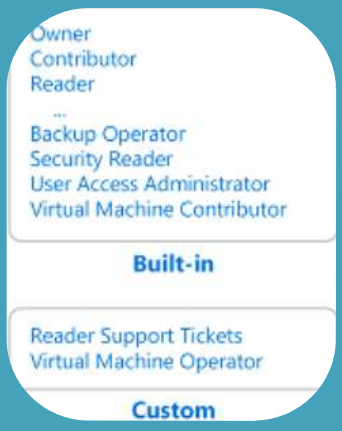
Encore une fois c'est ultra simple. On trouve des rôles intégrés appelés **Built in roles** qui sont déjà préconfigurés et à ta disposition.

On peut citer le rôle **Owner**, qui possède tous les droits. Le rôle **Contributor** qui a tous les droits à l'exception de la gestion des accès aux ressources. Ou bien encore le rôle **Reader** qui permet d'avoir des accès en lecture seule.

Aujourd'hui, il existe plus de 240 **Built in roles**.

Vraiment intéressant, mais si on veut quelque chose de personnalisé ?

Source : Microsoft



Microsoft a pensé à tout. Il est possible de **créer ses propres rôles** en attribuant ou refusant les actions de ton choix, de manière extrèmement granulaire. Au sein d'un même rôle, tu peux **combiner des actions autorisées et des actions interdites**, sans aucun problème.

Sachant que le **RBAC** est un **service global**, il peut être utilisé sur les ressources de n'importe quelle région.

Comme tu peux avoir des ressources de différentes région au niveau d'une **souscription** ou d'un **RG**, la gestion des droits devient alors une jeu d'enfant !

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 ...

GROW UNA

... N'hésitez pas à vous abonner sur Linkedin à l'adresse :

https://aka.ms/grow-una

Et si le contenu vous plait, partagez le ;o)

A très vite !