La Minute CLOUD de JULES & LÉA

Azure Key Vault #1

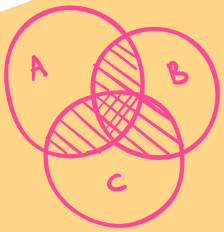
Philippe, j'entends souvent parler de coffre fort sur Azure, tu peux nous en dire plus ?

Oui sans problème. Il s'agit de **Azure Key Vault** (**KV**). C'est le service de **coffre fort managé** par Microsoft. A l'intérieur, on peut y stocker différents éléments.

Le 1er, sont les **clés** de chiffrement, utilisées pour chiffrer les données stockées sur des supports comme des disques associés à des VMs, ou des bases de données (DB)

Le 2ème élément, sont les **secrets**. Un secret peut être un mot de passe (MDP), un jeton, une clé API ou une chaine de connexion permettant de se connecter à une application ou à une DB de manière sécurisée.

Et enfin le dernier élément, sont les **certificats SSL/TLS**. En plus de pouvoir stocker ses propres certificats, il est aussi possible d'en générer et même de les renouveler automatiquement.



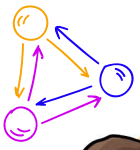
Donc plutôt que de renseigner ce type d'informations sensibles dans le code de notre application, il vaut mieux utiliser un **KV** ?

Tout à fait. Chaque élément stocké, fournit une **URI** qui est un lien pointant dessus, qui peut être directement appelée dans ton code. Ainsi, tu évites de retrouver ces informations plus que sensibles dans des répertoires publics, type GitHub.

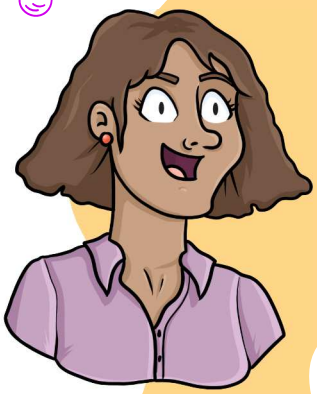
suivante

La Minute CLOUD de JULES & LÉA

Azure
Key Vault #2



Et je suppose que **KV** est intégré nativement avec d'autres services Azure ?



Tu supposes bien. Il est fortement intégré à ceux qui proposent du chiffrement avec des données au repos (**at rest**), c'est-à-dire hébergées sur un stockage persistant, comme les comptes de stockage, Azure SQL Database, Cosmos DB, ou bien encore Azure Data Lake.

KV est aussi utilisé par le service **Azure Disk Encryption** (**ADE**) pour chiffrer les disques des VMs. Il utilise **Bitlocker** pour Windows et **DM-Crypt** pour Linux..

Tu as d'autres exemples de services Azure qui l'utilisent ?

On peut citer également les **WebApp**, qui l'utilisent pour stocker des certificats SSL/TLS, ou bien encore **Azure Front Door**, si tu souhaites utiliser un nom de domaine personnalisé avec ton propre certificat.

Je vois, mais comme **KV** est un service PaaS il est exposé nativement sur Internet, ce n'est pas problématique ?

Excellente question. Avec un service aussi critique, il est fortement recommandé de ne pas l'exposer sur Internet, et pour y parvenir, Microsoft propose 2 type de configurations.

La 1ère, est la mise en place d'un **firewall** (**FW**) qui va te permettre de **filtrer le trafic entrant**, soit en autorisant des adresses IP publiques, soit en filtrant les VNET Azure qui peuvent s'y connecter.

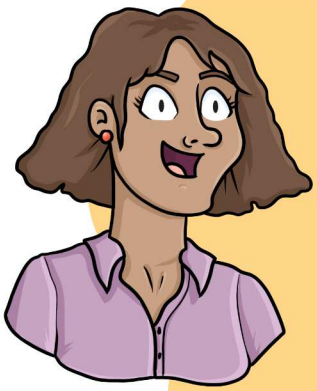
La 2nde, est l'utilisation du **Private Endpoint**, qui permet de consommer ton **KV** directement depuis le réseau privé de Microsoft.

suivante

La Minute CLOUD de JULES & LÉA

Azure
Key Vault #3

C'est super ! En plus du filtrage que l'on peut appliquer, existe t-il un autre moyen pour sécuriser l'accès aux données ?



Oui, au travers du menu **Access Policies**. On va pouvoir attribuer facilement et très finement des **permissions** sur les clés, secrets et certificats. Par exemple, attribuer simplement un accès List, sur les secrets pour Jules, ce qui lui permettra simplement de lister les secrets d'un **KV**.

Les permissions peuvent être affectées comme toujours, à un utilisateur, un groupe d'utilisateurs, un SPN, ou à un service Azure.

Donc, la gestion des droits sur le **KV** s'effectue via le **RBAC**, et la gestion des permissions sur les clés, secrets et certificats s'effectue via le menu **Access Policies** ?

Exactement ! Mais ce n'est pas tout, Microsoft propose 2 autres options :

La 1ère, est le **Soft Delete** qui permet de restaurer un **KV**, ou un objet qui a été supprimé, pendant une période prédéfinie lors de la création du **KV**.

La 2nde, est le **Purge Protection**, que l'on peut activer ou non uniquement lorsque le **Soft Delete** est activé. Il empêche carrément la suppression d'un **KV** pendant une période que tu définis entre 7 et 90 jours, tout comme le **Soft Delete**.

Malgré toutes ces protections, peut on savoir qui accède à un **KV** ?

Oui, via la **journalisation** qui permet de savoir quelle identité accède au **KV** (un utilisateur, une application, ...), par quel moyen, quand et à quel objet. Ces informations sont stockées dans un compte de stockage, et évidemment seuls les membres de l'équipe en charge de la sécurité devront y avoir accès !

Et tant qu'on y est, on chiffrera ce compte de stockage avec une clé qui sera hébergée sur le **KV** ;)

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 plaît, partagez-le ;o)

A très vite !