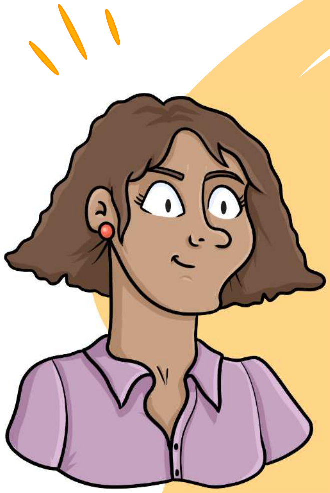
La Minute CLOUD de JULES & LÉA

Azure Key Vault #1



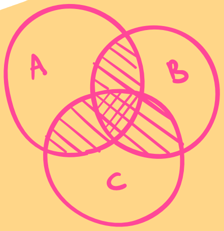
Philippe, I hear about vault on Azure, can you tell us more?

Of course ! This is **Azure Key Vault** (**KV**). This is the vault service **managed** by Microsoft. A **KV** can store different items.

The 1st item, are **encryption keys**, used to encrypt data stored on differents Azure services such as disks associated with VMs, or databases (DB)

The 2nd item, are the **secrets**. A secret can be a password, a token, an API key or a connection string used to connect to an application or a DB in a secure way.

And finally the last item, are the **SSL/TLS certificates**. In addition to being able to store your own certificates, it is also possible to generate a new one and even renew it automatically if you need.

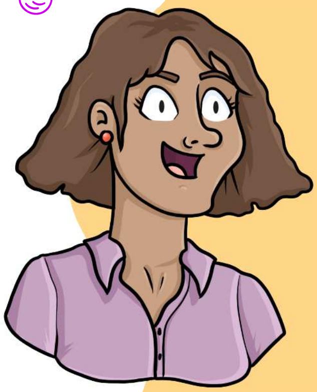


So rather than filling in this type of **sensitive information** in the code of our application, it is better to store them in a **KV**?

Absolutely. Each stored element provides a **URI** which is a link pointing to it, which can be directly called in your code. Thus, you avoid finding this sensitive information in public directories, such as GitHub.

next

Azure Key Vault #2



And I assume **KV** is natively integrated with other Azure services?

You guess right. It is strongly integrated with those that offer encryption with data **at rest**, on persistent storage, such as storage accounts, Azure SQL Database, Cosmos DB, or even Azure Data Lake.

KV is also used by the **Azure Disk Encryption** (**ADE**) service to encrypt VM disks. It uses **Bitlocker** for Windows and **DM-Crypt** for Linux.

Do you have other examples of Azure services that use **KV**?

We can also mention **WebApps**, which use it to store **SSL/TLS certificates**, or even **Azure Front Door**, if you want to use a personalized domain name with your own certificate.

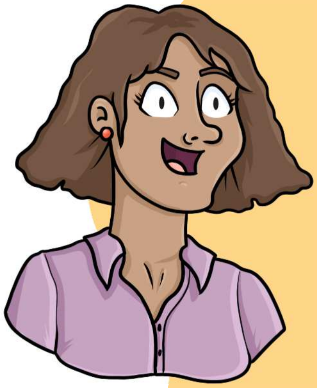
I see, but as **KV** is a PaaS service it is **natively exposed** on the Internet, isn't a problem?

Excellent question. With such a critical service, it is strongly recommended not to expose it on the Internet, and to achieve this, Microsoft offers 2 types of configurations.

The 1st is the implementation of a **firewall** (**FW**) that will allow you to **filter incoming traffic**, either by authorizing public IP addresses, or by filtering the Azure VNETs that can connect to it.

The 2nd, is the use of the **Private Endpoint**, which allows you to consume your **KV** directly from Microsoft's **private network**.

next



That's great ! In addition to the filtering that can be applied, is there another way to secure access to a **KV**?

Yes, through the **Access Policies** menu. We will be able to easily and very finely assign **permissions** on keys, secrets and certificates. For example, simply assign List access, on the secrets for Jules, which will allow him to simply list the secrets of a KV.

Permissions can be assigned as always, to a user, a usergroup, a SPN, or an Azure service.

So, the management of rights on the **KV** is done via **RBAC**, and the management of permissions on keys, secrets and certificates is done via the **Access Policies** menu?

Exactly ! But that's not all, Microsoft offers 2 other options:

The 1st one, is the **Soft Delete** which allows to restore a KV, or an object which has been deleted, during a predefined period during the creation of the **KV**.

The 2nd one, is the **Purge Protection**, which can be activated or not only when the **Soft Delete** is activated. It prevents the deletion of a KV altogether for a period that you define between **7 and 90 days**, just like the **Soft Delete**.

Despite all these protections, can we know who is accessing a KV?

Yes, via **Activity Log** which lets you know which identity is accessing the KV (a user, an application, etc.), by what, when and to which object. This information is stored in a storage account, and obviously only the members of the team in charge of security should have access to it!

And for the fun, we'll **encrypt** this **storage account** with a key that will be hosted on the KV ;)

La Minute CLOUD de JULES & LÉA

Thank you !

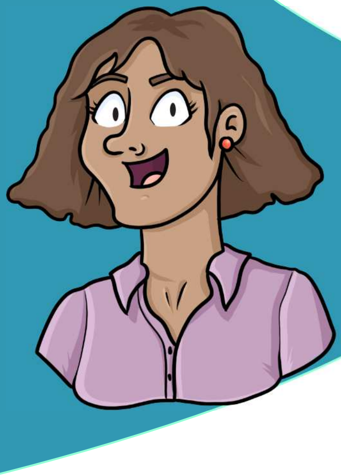
If you want to continue **learning** in a fun way about the **Azure ecosystem**, and not miss any of our illustrations ...

... Feel free to subscribe on Linkedin at:

https://aka.ms/grow-una

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

See you soon !



GROW UNA