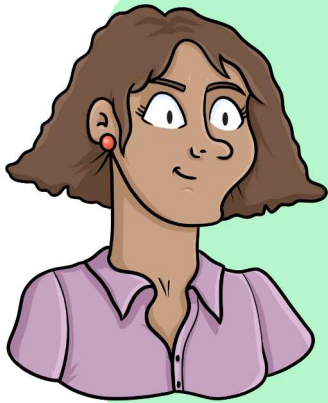Today we are going to discuss a service used by many customers, it is **Azure Monitor**.

I guess it is dedicated to monitoring?!

Yes, and even more than that.

It **collects**, **analyzes** and **exploits** telemetry data from services deployed on Azure or outside of Azure. These are the Azure platform metrics.

In addition to service metrics, Azure Monitor also allows you to collect activity logs of all operations performed in Azure, which can be found in the **Activity Logs** menu.

Now that you mention it, I think I know it.

Platform metrics **are enabled by default**, and can be viewed in near real time by browsing directly on supported services, such as CPU or memory usage for VMs.
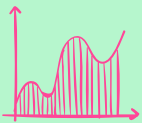
A question may be silly, but why should we monitor our resources?

This is not silly

Monitoring makes it possible to follow the **state of health** of the resources, its **behavior** and to take **preventive actions** to avoid incidents.

For example, adding more CPU resources, or expanding disk space.

In addition, it is possible to activate **alerts** when a threshold of a metric is reached, in order to be **notified** by **email**, **SMS** or by calling a **workbook** to analyze and correct if necessary.

next

I guess some services offer more information than others?

Indeed.

Some services offer an organized visualization called **Insights**

One example is **Application Insights**, which monitors the availability, performance, and usage of web applications that are hosted on Azure or locally.

There is also **Container Insights** which monitors the performance of workloads deployed in AKS containers.

Or even **VM Insights** which analyzes the performance and integrity of VMs.

Are other services supported?

Obviously!

We can mention Storage **Accounts**, many network services, Cosmos DB, Key Vault and others. In addition, new services are added regularly.

For supported services, there is a **Metrics** submenu that allows you to view all of the service's metrics, and the cherry on the cake, you can **pin** this information to a private **dashboard** or a shared dashboard.

Fantastic!

It's great, so you can have a dashboard per resource, or a dashboard per application with the metrics you want at a glance.
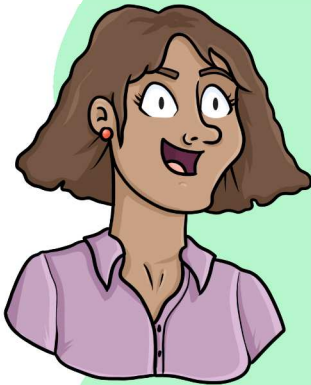
But, where is this information stored?
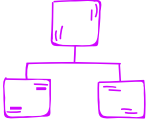
Excellent question!

Metrics and logs are stored in a **Log Analytics workspace**.

We can compare a workspace to a container in which data is stored and aggregated.

Data is organized into **tables**, where each, stores information based on its **property**.

What do you mean by property?

A property is a category that helps **classify data**.

There is for example the **Perf** property, which will group performance-related data, or the **AzureActivity** property, which will group data relating to actions performed in Azure.

Of course there are plenty of others.

That's great, but how do you access this data?

Via the Log Analytics services where the workspaces are created.

Log Analytics allows you to **execute queries** in the tables seen previously, hence their classification by properties in order to find them more easily. Queries are base on **Kusto Query Language** (KQL)
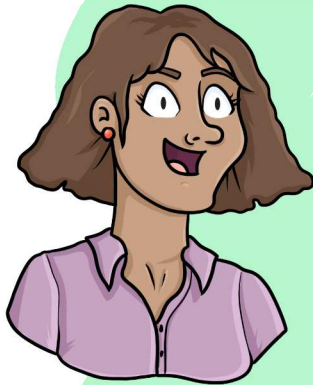
Wow, it sounds great!!

La Minute CLOUD de JULES & LÉA

And wait, it's not over.

Log Analytics offers you the possibility of installing an agent, in this case the **Microsoft Monitoring Agent** (MMA) which allows you to send specific logs according to your OS.

Like IIS logs?

Yes, among others.

For **Windows based-OS**, you can for example send system logs, application logs, or performance logs of your hardware.

For **Linux based-OS**, it's the same thing, with for example Apache logs, MySQL, without forgetting Syslog.

Well, that's powerful!

That's not all, since this agent also allows you to **send customized metrics** of your choice to your workspace.
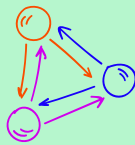
This is also the case with Application Insights, by installing the SDK, you can also do it by sending your metrics directly to the Azure Monitor Rest API.

What if my VMs don't have Internet access, am-I blocked?

Ahah, you can use **Log Analytics Gateway** (OMS Gateway), which will act as a gateway, a proxy by collecting information from different VMs and then sending it to Log Analytics.

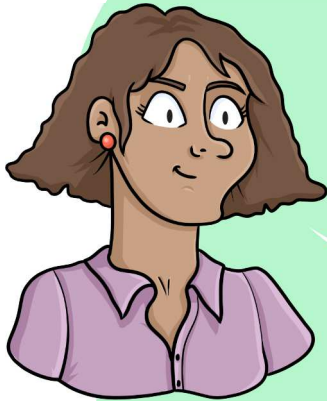Of course, this gateway **requires Internet access**.

Small specificity, it can only be installed on a Windows based-OS, but this does not prevent the transmission of data from VMs with a Linux based-OS.

It's good to know.

next

In addition to platform metrics, which are enabled by default as we saw previously, it is also possible to send **platform logs**.

They provide diagnostic and audit information for Azure resources and the platform on which they depend. Their name, **Diagnostic Settings**.

And it's up to us to activate them, if I understood correctly?!

Yes, they are activated on demand, because you have to send them to a destination to process or consult them.
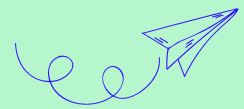
In addition to being able to be sent to a workspace, you can send them to a **Storage Account**, an **Event Hub**, which will allow you to then transmit them to a SIEM tool.

But it is also possible to send them **to external monitoring solutions** such as Apache Kafka, Datadog, the Elastic Stack or Logz.io to name a few.

Azure Monitor is a very complete tool, but what **about billing**?

It will depend.

For metrics enabled by default, there is no additional cost, as they are provided by Microsoft.

For data sent to a Log Analytics workspace, you will pay based on the amount of data ingested into the tool.

For data sent to a storage account, you will pay for the disk space used.

And finally to send it to an external solution, you will have the cost of outgoing data from Azure, to which you will have to add the cost of your external solution.

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://tinyurl.com/youtube-growuna

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

See you soon!

GROW UNA