



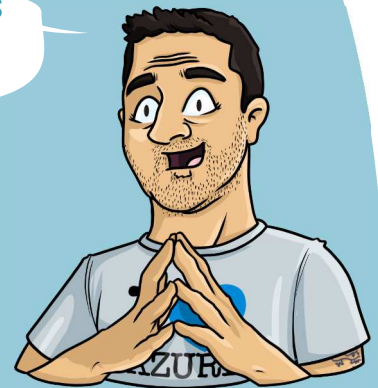
We talk about **virtual machines (VM)** on Azure, could you tell us a bit more?

Of course. A **VM** is a virtual server hosted on a hypervisor. On Azure, VMs run on the **Hyper-V** hypervisor.

VMs can be deployed on **Windows operating systems (OS)** or on different **Linux** distributions, as needed.

Currently Microsoft estimates that **60%** of VMs run on **Linux** OS and therefore **40%** on **Windows** OS.

I never thought that there are more Linux than Windows on Azure.



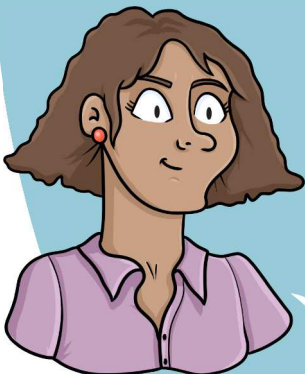
This is partly due to the fact that some Linux distributions are **license free** and therefore cheaper.

Another reason is the availability on the **marketplace** of turnkey solutions where you just have to deploy what you need. This may be a network appliance, a web server or even a firewall solution which are often based on Linux OS.

Small specificity, Azure offers 2 types of VM generations, **Gen1** and **Gen2**.

The generation of a VM defines the hardware on which it is executed. It offers **additional features**, such as support for booting UEFI instead of BIOS, but also SCSI disk controllers instead of IDE controllers.

Regarding the connection on the VMs, on **Linux**, it is done via the **SSH** protocol, and the connection on a **Windows** is done via the **RDP** protocol.





One of the many benefits of using VMs in Azure are the available **instance types**.

What exactly is an instance type?

It is simply an **allocation of vCPU and memory** resources. There are hundreds of them, for example Standard Dsv3, which includes 4vCPU, and 14GB of memory.

Instance types are categorized into **6 categories**: General Purpose, Compute Optimized, Memory Optimized, Storage Optimized, GPU, and High Performance Computing.

And I guess the more resources you allocate, the more it is expensive ?

Exactly !

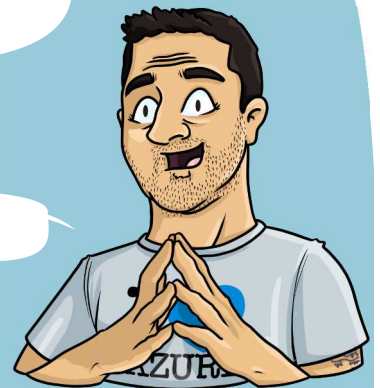
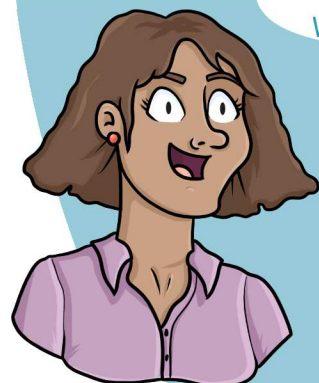
Another element that influences the price is its **version**. Newer versions run on newer hardware, so the prices are more attractive, but also the performance is better.

It is therefore necessary to prefer an instance Standard Dsv4 to a Standard Dsv3 instance.

But that's not all, the choice of instance type also influences other elements such as the **number of disks**, the **number of network cards (NICs)**, which you can associate with your instance, but also on the **IOPS** or even the **network throughput** of the VM.

So if I summarize, the more resources you have on your instance, the more configuration is customizable, and the better your performance will be !!

Absolutely. But beware, the idea is to have **performance in line with the workloads** running on the VM. It is therefore necessary to assess as closely as possible the quantity of resources required. Anyway, **you can change the instance type at any time**, it just requires a shutdown of the VM first.





Regarding the **disks**, they are now **managed** by Microsoft which manages them according to the configuration that you defined.

This avoids managing an additional element, which is rather practical.

Exactly !

Today, there are 2 types of disks: **HDD disks**, which are mechanical disks mainly used for archiving; And **SSD disks** that offer much better performance.

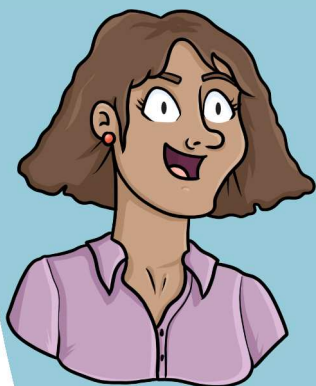
Another notion that is related to disks is the **replication type**. By default, data is replicated 3 times. **Locally Redundant Storage (LRS)**, data is replicated in the same Datacenter (DC) but on 3 different racks, and **Zone Redundant Storage (ZRS)**, data is replicated in 3 different DCs.



I love the principle of replication but I guess it affects the price of the disk?

Of course !

We will discuss this very interesting subject of storage in a future comic.



Back to our topic. On each VM deployed, Microsoft provides a **temporary SSD** disk free of charge. Its size will also depend on the **type of instance** configured.

But you have to be careful with this temporary disk. **Every time you restart the VM, the data stored there is deleted.** It can be used to host the Swap of a Linux OS, the pagefile of a Windows OS or non-critical logs.



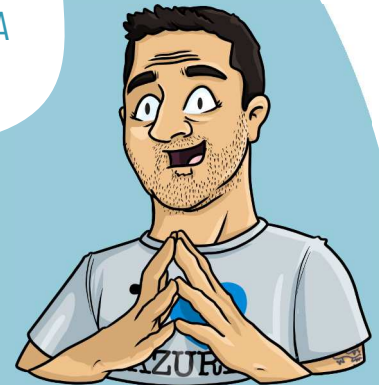
You do well to point out, I know someone who had installed an application on this disk, and during the 1st restart, everything was gone, and of course, it was a production environment !!



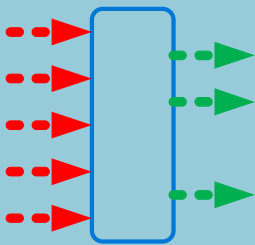
Once your **VM** is deployed, it needs to **communicate** with the other services deployed on Azure or On-Premise. This is where the **network** comes into the game.

As we have seen, a **VM** can have several **NICs**, which will be used for example to separate administration traffic from application traffic. A NIC is deployed in a **subnet**, which is itself deployed in a **virtual network (VNET)**.

Ah yes I remember, Stan mentioned the concept of the **Network Security Group (NSG)** that could be associated to a subnet!



Traffic filtering



Well done. An **NSG** allows you to **filter incoming and/or outgoing traffic** from your VM. When I talk about traffic, it concerns both internal traffic that passes through the **VNET**, but also internet traffic, if you have associated a **public IP** with your VM.

You can link a **NSG**, at the **subnet level**, or at the **NIC level**. You have the possibility of combining the 2 if you wish, but that makes management a little more complex.



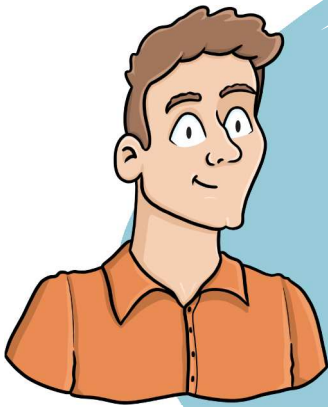
And can we associate other network components to a VM ?

Absolutely !



You can associate **Load Balancers**, which act on the transport layer (**LB4**), whether they are private with a private IP address, or whether they are public by being exposed on the Internet.

But also Application Gateways which intervene at the application layer (**LB7**), or even Traffic Managers which distribute traffic according to DNS requests. You can also consider network appliances, like NVA ...



This is where we realize that **VMs** on Azure offer a wide variety of opportunities.

It's true, and it's not over. Of course, you can configure a **backup and restore policy**.

This is **strongly recommended** for Production environments. Backup frequency and retention will depend on business needs and constraints.

Despite the fact that the data is replicated 3 times, do you think backups should be activated ?

It's a mandatory. Replication protects you against the unavailability of a rack that hosts your data, while the **backup and restore policy protects** you against **data loss or data corruption**.

Setting up backups is a good start, but you also need to be sure you can restore the data. It is therefore necessary to carry out **restoration tests**, to validate that the process works well, but also to validate that the data are indeed those expected.

Great point, I hadn't thought of that !!

Another cool feature is extensions. An **extension** is a small application (an agent, a script), which runs either when creating the VM or on demand when the VM is already installed.

Some features only work when an extension is installed such as **enablevmaccess** which allows to reset a user's password on a VM.

Moreover, some extensions are installed automatically depending on the features you activate on your VM, such as enabling the backup, or monitoring via Azure Monitor!

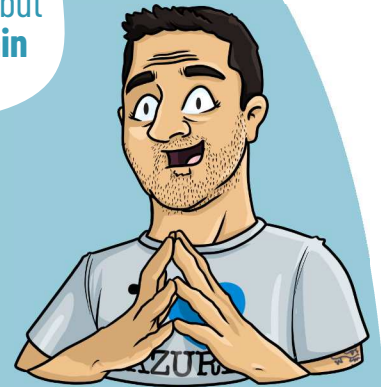




As we discussed in another comic, a VM can be integrated into an **Availability Set (AS)** in order to increase the **high availability** of an application.

Little reminder, by integrating VMs into an AS, they will be distributed between **Fault Domain (FD)**, but also between update domains or **Update Domain (UD)**.

Interesting, but whether the VMs are in an AS or not, is it possible **to monitor them** ?



Absolutely. The best way to do this is through **Azure Monitor**. Information can also be got through metrics or through Application Insight. Azure Monitor will be the subject of a dedicated comic in the coming weeks.

But that's not all, because monitoring a service is a good practice, but it's even better to be notified when there is a problem.

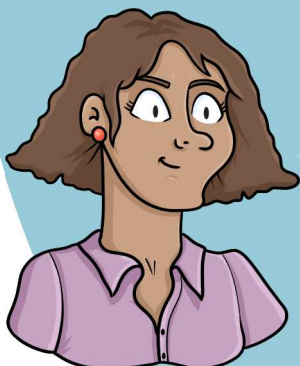


This is where **alerts** come in. We configure notification alert when a problem occurs or when a threshold that we have configured is reached. (Example: the CPU that exceeds 90% of utilization for a period of time).

There are also tools to troubleshoot in case of problems. Like **Boot Diagnostics**, **Serial Console** or even **Connection troubleshoot** to name a few.



VMs are usually the first service customers use when they start on Azure. This reassures them and step by step, they adopt new Azure services !



We realize that Azure provides a large number of tools that allow us to assist us on a daily basis for the management of VMs, and this is awesome

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 !

