Monitorization Platform for a 5G Testbed (Plataforma de Monitorização de uma Testbed 5G)

Tutor: Rafael Direito (rdireito@av.it.pt) / Diogo gomes (dgomes@ua.pt)

Group Size: 4

Description: The main goal of this project is to create o toolset to monitor a 5G application testbed. Since these applications are deployed through VMs and containers, pragmatically, the main scope of the monitorization will rely onto these entities. Besides this, networking monitoring tools will also have to be addressed.

There are several tools that provide the mentioned features, for instance: Grafana, Prometheus, Netdata, and TICK Stack, thus an analysis of these tools is of utmost importance. Using the aforementioned tools, and similar ones, it is desired the students create a toolkit capable of monitoring the multiple aspects that influence the performance and security of a 5G testbed. This toolkit should present a uniform access interface, like an API or/and UI, that transparently provides all the data collected by its underlying monitoring tools.

Requirements:
- The following parameters will have to be monitored:
  - VM-level metrics – CPU, RAM, Disk, Network
  - Hypervisor-level metrics - CPU, RAM, Disk, Network, etc
  - Testbed-level metrics – Network, VNF instantiation times, etc
- The monitoring toolkit should:
  - Offer uniform access interfaces
  - Allow transparency regarding the underlying tools used for monitoring metrics
  - Be implemented through a micro-service architecture, being extremely modular
  - Easily allow the addition of new backend monitoring tools
  - Implement mechanisms to manage the authentication and authorization of the users who will use this tool
  - Provide alarmistic based on pre-defined thresholds. For instance, an e-mail should be sent to the testbed's admin when certain events take place
- The toolkit should rely on free/open-source tools
- The toolkit should be able to generate a weekly/monthly report regarding the testbed status

Possible challenges:
- Non-invasive monitoring of the testbed's applications. The applications should be seen as black boxes and no access to their internal logic will be provided
- Implementation of a security monitoring toolkit that should detect whenever a 5G application is trying to attack the testbed's infrastructure and take the necessary actions
- Implementation of mechanisms that enable the integration of the developed monitoring toolkit with other toolkits used in different testbeds and present a uniform access interface to the collected data. For instance, if a company has several testbeds, in several locations, it should be possible to present the monitoring information of all the company's testbeds through a unified interface

Expected Results:
- User-friendly platform
- The toolkit should be developed taking into consideration aspects like decoupling, modularity, extendibility, and security
- The addition of new tools to this toolkit should be as simple as possible