UNIVERSITAT POLITÈCNICA DE VALÈNCIA

atmosphere-eubrazil.eu

@AtmosphereEUBR

ATMOSPHERE

Adaptive, Trustworthy, Manageable, Orchestrated, Secure Privacy-assuring Hybrid, Ecosystem for REsilient Cloud Computing

To Trust or not to Trust,

That is the question

Co-funded by the European Commission
Horizon 2020 - Grant #777154

European Commission

Open questions

Do you **trust** Cloud Services?

Do you **trust** the provider, the VMI, the PaaS services and the applications?

What do you need to **trust** in Cloud Computing?

Will you upload **sensitive data** to the Cloud?

ATMOSPHERE
Adaptive, Trustworthy, Manageable, Orchestrated, Secure Privacy-assuring Hybrid, Ecosystem for REsilient Cloud Computing

ATMOSPHERE goals & partners

- ATMOSPHERE is a 24-month project aiming at the design and development of a **framework** and a **platform** to implement **trustworthy cloud services** on top of an intercontinental hybrid and **federated** resource pool.
  - Supporting the development, build, deployment, measurement and evolution of trustworthy cloud resources, data management services and data processing services,
  - A pilot use case on **Medical Imaging Processing**.
- Expected results:
  - A Hybrid federated VM and container platform
  - A development framework with three sets of services
    - Trustworthy evaluation and monitoring framework.
    - Trustworthy Distributed Data Management
    - Trustworthy Distributed Data Processing

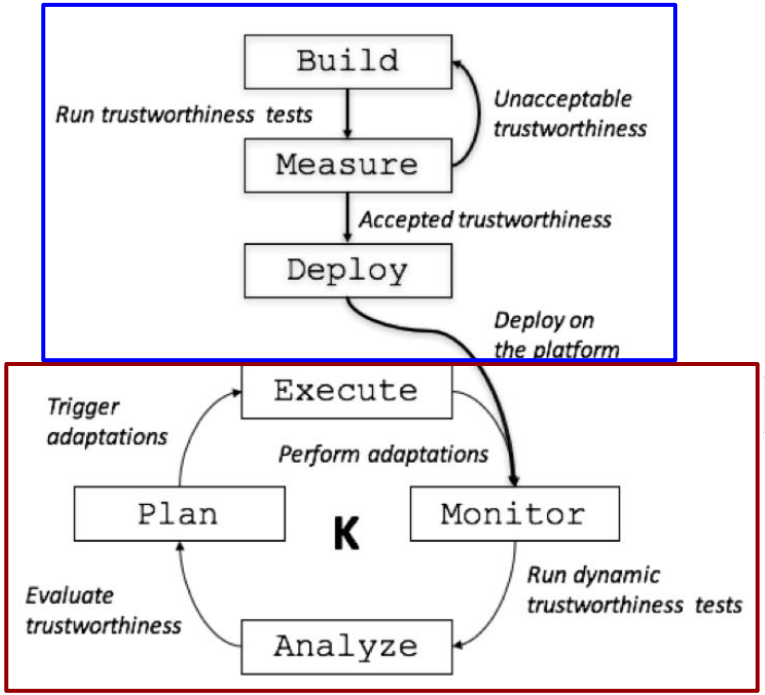
UNIVERSITAT POLITÈCNICA DE VALÈNCIA
Universidade Federal de Campina Grande
Trust-IT Services Communicating ICT to markets
UNIVERSIDADE FEDERAL DE MINAS GERAIS
UNIVERSIDADE DE COIMBRA
UFAM
POLITECNICO DI MILANO
Universidade de Brasília Departamento de Ciência da Computação
TECHNISCHE UNIVERSITÄT DRESDEN
UNICAMP UNIVERSIDADE ESTADUAL DE CAMPINAS
UNIVERSITY OF PIRAEUS RESEARCH CENTER
KUNUMI
quibim
DELL EMC

Trustworthiness properties

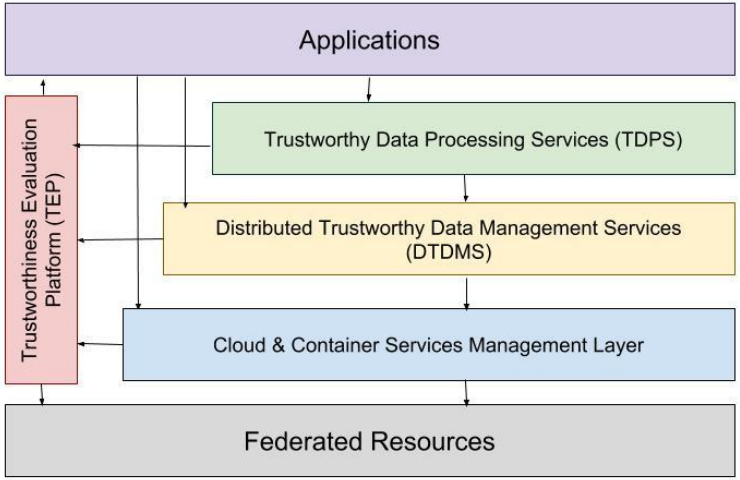
Trust. property	Explanation
Security	Covering **Integrity, Availability, Confidentiality**, we define it as the attack resistance and fault tolerance against malicious attacks.
Privacy assurance	Guarantee of an entity to be secure from unauthorized disclosure of sensible info.
Coherence	Consistency of the information regardless of the location.
Isolation	The effects of a service do not impact the trustworthiness of other data & services (e.g. crashes, starvation or privacy issues of a service do not compromise others).
Stability	The service produces equivalent outcomes and QoS for equivalent inputs and resources used.
Fairness	The assurance of ethical and legal rights.
Transparency	Involves multiple sub-dimensions, such as **Awareness, Access, Redress** (capability of rectifying), **Explanation, Provenance, Auditability, Traceability** and **Accountability** (assign responsibility to services and their outcomes).
Dependability	Includes multiple sub-dimensions, such as **Integrity** (absence of improper system alterations), **Availability** (readiness for correct service), **Reliability** (continuity of correct service), **Maintainability** (ability to undergo modifications and repairs), **Safety** (absence of catastrophic consequences on the user(s) and the environment), and **Performance stability** over time (in terms of applications execution time or throughput).

Trustworthiness life-cycle

- Trustworthiness metrics define the properties that can be evaluated in each one of these dimensions:
  - A priori and a posteriori evaluation of vulnerability, performance, integrity, scalability, resource consumption, fairness, isolation, etc.
  - Enabling creating self-adaptive applications
  - Tracing the degree of compliance of regulations such as the EU-GDPR.
  - Privacy protection, traceability, confidentiality warning, etc.
- ATMOSPHERE will provide a continuous, global score of trust for an application, that can be used to readjust some parameters to increase trust.



Layers of the project

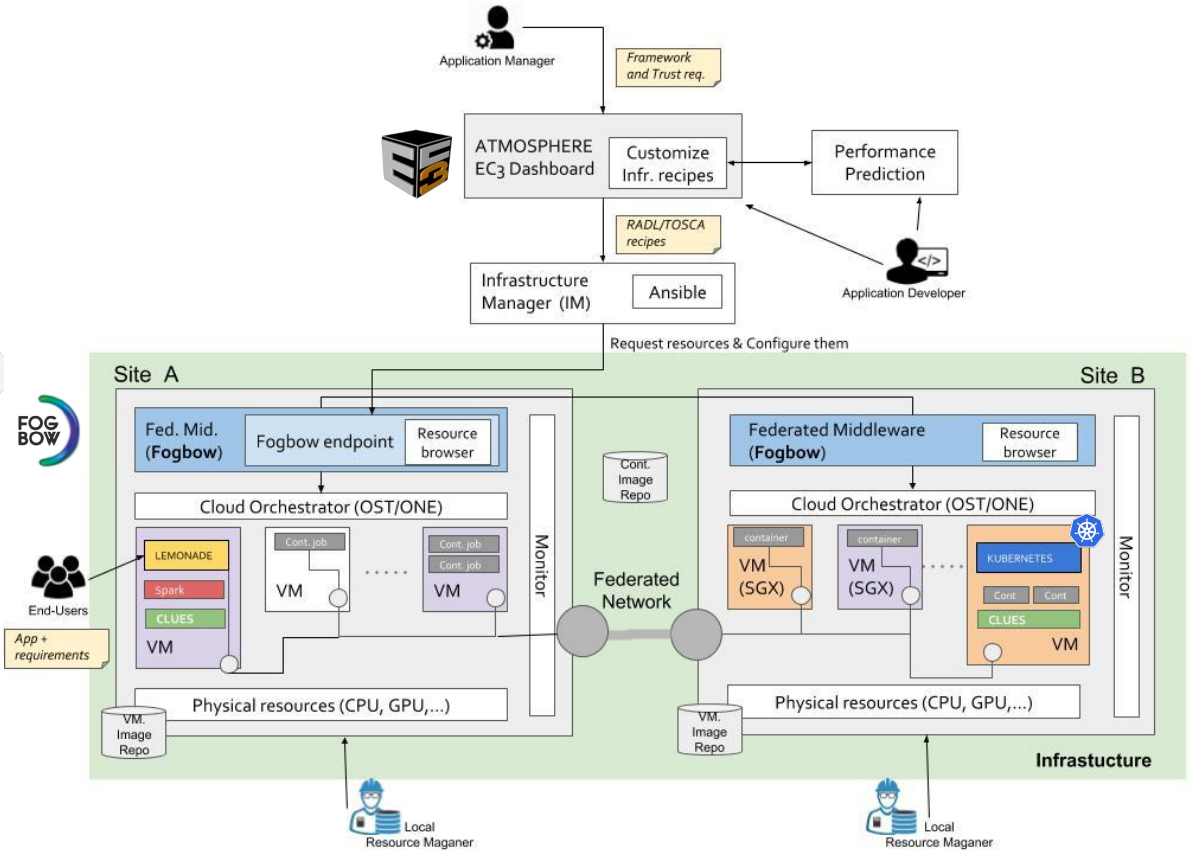


- Three main layers:
  - Cloud resources
  - Data management services
  - Data processing services
- A transversal layer to manage trustworthiness for the entire cloud platform

- Four different user profiles:
  - **Application developer**: codes and registers applications.
  - **Application manager**: deploys applications and resources.
  - **Final users** (i.e doctors): use applications.
  - **Resource Manager**: maintains the underlying infrastructure.

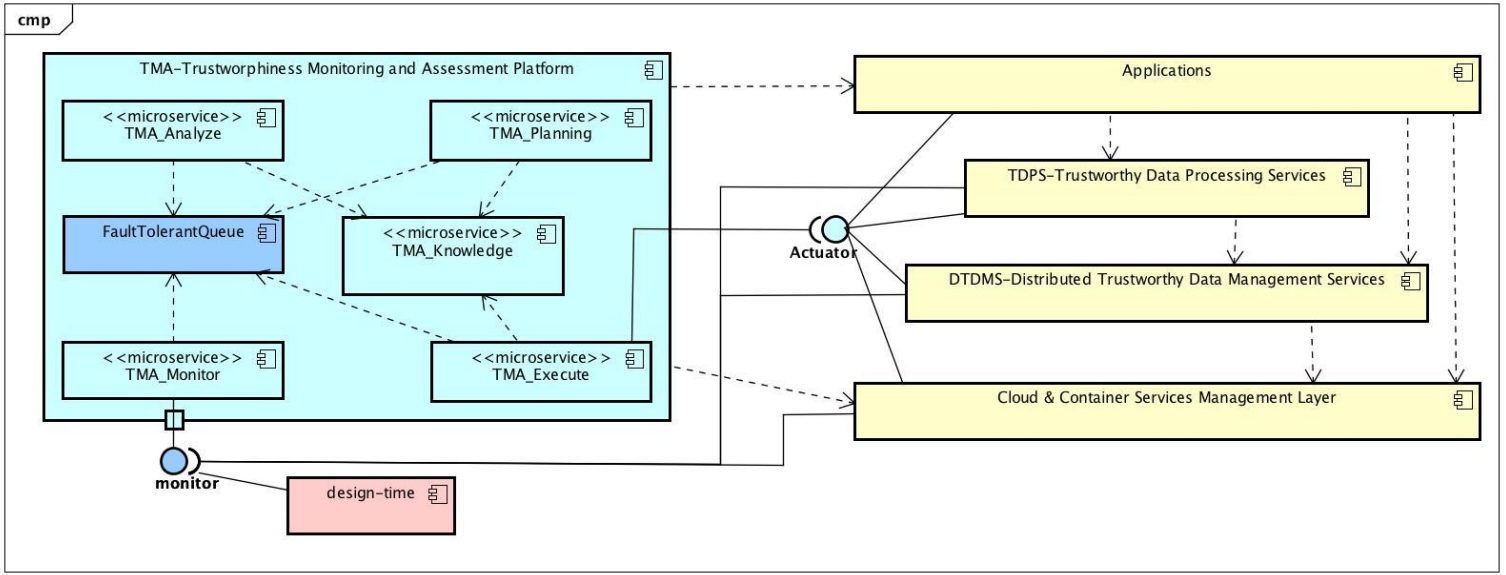
ATMOSPHERE
Adaptive, Trustworthy, Manageable, Orchestrated, Secure Privacy-assuring Hybrid, Ecosystem for REsilient Cloud Computing

Cloud & Container Services Management Platform



- Federated network powered by OpenVSwitch, ONOS (inter-datacenters) and VLANs (intra-datacenters).
- Federated Cloud managed by Fogbow.
- Dashboard based on the EC3 web service.
- Automatic management and configuration of virtual elastic clusters.
- Support for heterogeneous resources.
- Critical applications dealing with sensitive data running on SGX enclaves.

Trustworthiness Monitoring & Assessment Framework



- In every layer of the ATMOSPHERE platform, the deployed probes are responsible for the active monitoring tasks. The TMA_Monitor follows a passive strategy.
- Everything is delivered as Kubernetes services, to easily deploy the microservices that compose the monitoring layer.

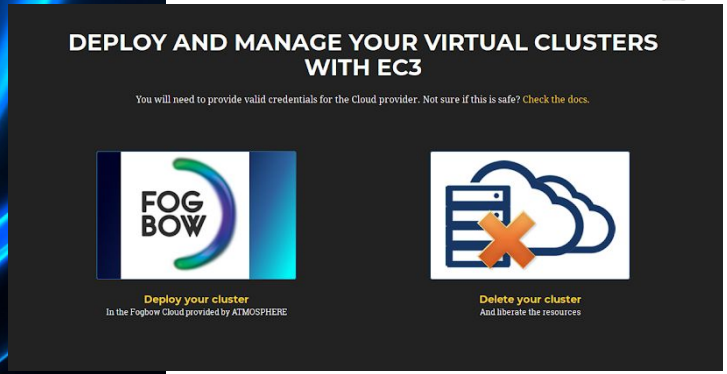
Available on github: https://github.com/eubr-atmosphere/tma-framework

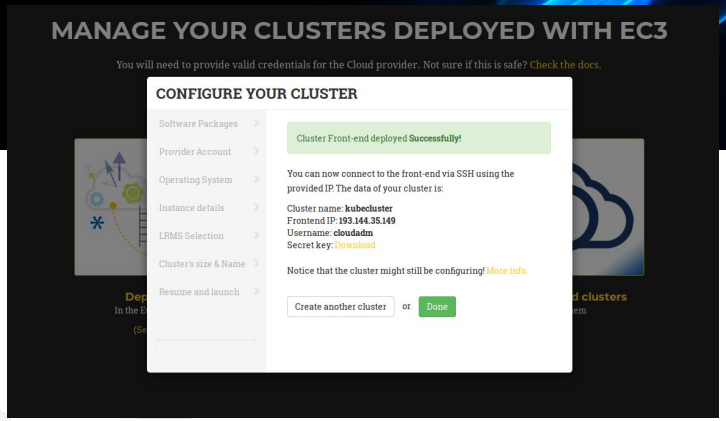
Trustworthiness Monitoring & Assessment Framework

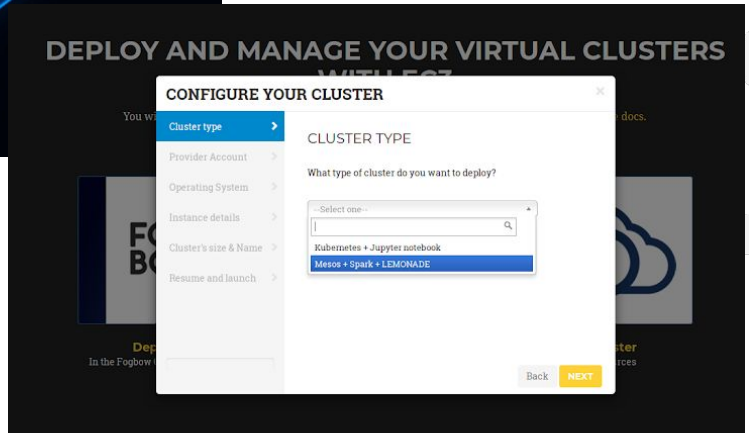
- Five main components:
  - **TMA_Monitor**: provides a generic interface in which the other layers (through probes) provide trustworthiness-related information through the RESTful interface.
  - **TMA_Analyze**: is responsible for continuously listening to the Knowledge microservice, calculate the trustworthiness scores and, if such scores fall below a threshold, activates the TMA_Planning microservice.
    - The trustworthiness scores imply merging several metrics. E.g. Privacy can be computed as the maximum of the privacy risk and the data loss scores for each dataset.
  - **TMA_Planning**: exposes an interface that allow the TMA_Analyze component to notify it about the need for adaptations to achieve the required goals, or to recover the desired levels of trustworthiness.
  - **TMA_Execute**: provides an interface through which the TMA_Planning component can submit an adaptation plan to be performed.
  - **TMA_Knowledge**: stores the collected monitoring data and also stores and manages information about the application architecture, resources and assets available and their possible adaptations.

ATMOSPHERE
Adaptive, Trustworthy, Manageable, Orchestrated, Secure Privacy-assuring Hybrid, Ecosystem for REsilient Cloud Computing

Dashboard

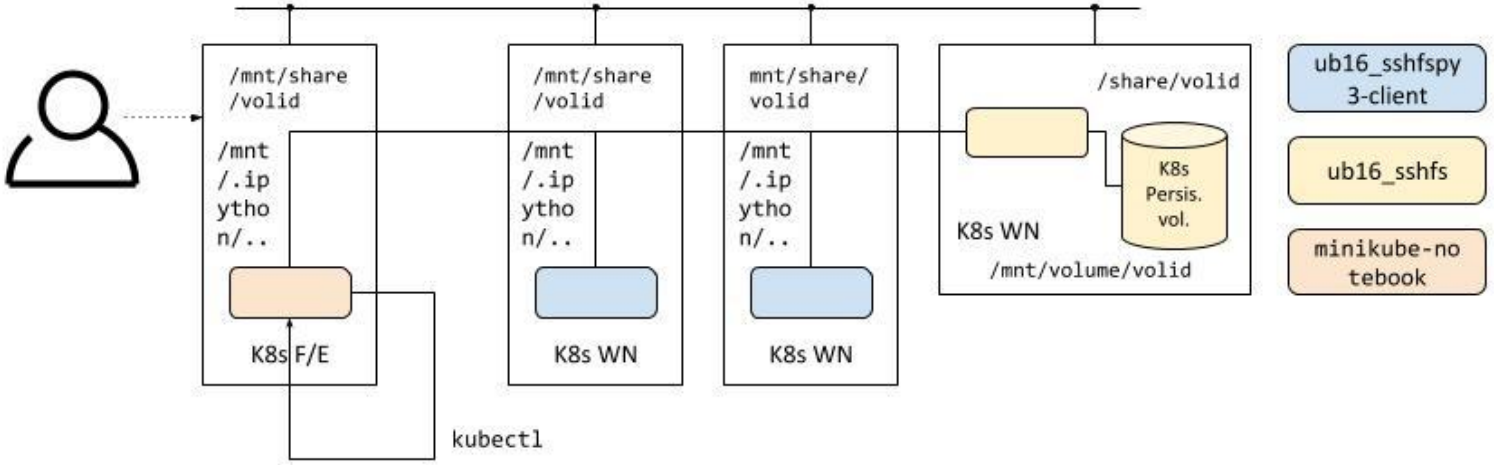






Available at: https://servproject.i3m.upv.es/ec3-atmosphere/

Application deployment (example)



- Three steps:
  1. Deploy the Kubernetes cluster through EC3.
  2. Deploy the shared space and copy data.
  3. Run the processing application and check the results.
- This gives the possibility of deploying services, running functions and scaling-up the cluster directly from the Jupyter notebook.

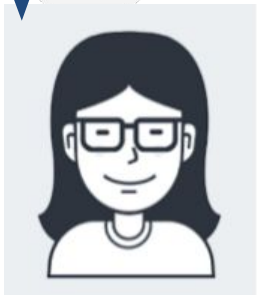
Conclusions: What could you expect from ATMOSPHERE?

ATMOSPHERE

- A quantitative trustworthiness score on the isolation, reliability, performance, privacy risks and stability,.
- Both at design time (virtuous cycle) and at runtime.
- A set of trustworthy services for data processing

Application Developers *(Code & Register Application)*

- A Federated hybrid cloud infrastructure.
- A convenient and interoperable cloud orchestrator to deploy complex applications.
- A broker and a monitoring service for dynamically assessing and adjusting the applications.



Application Managers *(Deploy Application and Resources)*

- A Data analysis framework with high-level trustworthiness scores such as fairness and explainability.
- An environment to safely process data and expose processing algorithms with IPR restrictions.

Data scientists *(Use Applications)*

ATMOSPHERE
Adaptive, Trustworthy, Manageable, Orchestrated, Secure Privacy-assuring Hybrid, Ecosystem for REsilient Cloud Computing

Don’t miss a beat!

Follow on Twitter
@AtmosphereEUBR

Connect on LinkedIn
linkedin.com/in/atmosphere/

Check our official website
http://www.atmosphere-eubrazil.eu/

Official Github organization
https://github.com/eubr-atmosphere

REGISTER FOR THE NEWSLETTER:

www.atmosphere-eubrazil.eu/user/register

Thanks for your attention!

Contact
Amanda Calatrava (@amcaar)
Instituto de Instrumentación para Imagen Molecular
Universitat Politècnica de València (UPV)


amcaar@i3m.upv.es


https://amcaar.github.io/

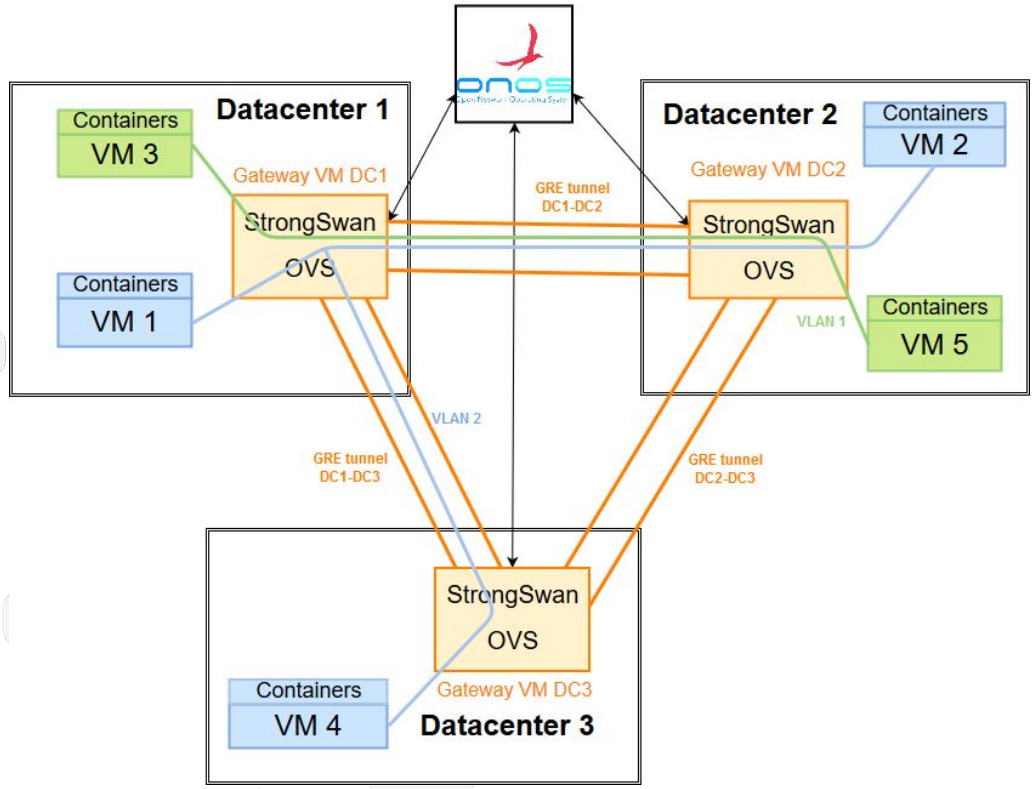
Improving Trustworthiness of Data Analytics

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

ATMOSPHERE
Adaptive, Trustworthy, Manageable, Orchestrated, Secure Privacy-assuring Hybrid, Ecosystem for Resilient Cloud Computing

atmosphere-eubrazil.eu

Network configuration



- The gateway VM is the interface between the intra-datacentre network and the inter-datacentres network.
  - Each gateway VM runs open vSwitch.
  - Managed by ONOS
- The edges the L2oL3 tunnels established between these nodes.
  - An IPsec VPN solution like StrongSwan is used to encrypt these L2oL3 tunnels
- ONOS is distributed across datacenters
  - Each datacenter instantiates a single ONOS VM and all the instances share a common state of the network.