D5.1 INFRASTRUCTURE DESIGN

29/06/2020

FUNDED BY NGI

This project has received funding from the European Union's H2020 research and innovation programme under Grant Agreement no 871498

Grant Agreement No.: 871498
Call: H2020-ICT-2018-2020

Topic: ICT-24-2018-2019
Type of action: RIA

D5.1 INFRASTRUCTURE DESIGN

Revision: v.2.0

WORK PACKAGE	5
TASK	5.1
DUE DATE	30/06/2020
SUBMISSION DATE	29/06/2020
DELIVERABLE LEAD	Engineering
VERSION	3.0
AUTHORS	Alfonso Pietropaolo (ENG)
REVIEWERS	Najmeh Mousavinezhad, Dr. Kathrin Knautz
ABSTRACT	Definition and description of the technical infrastructure provided by DAPSI (based on FIWARE Lab) to support users experimenting during the incubation process
KEYWORDS	Cloud infrastructure, virtual environment, FIWARE

Document Revision History

Version	Date	Description of change	List of contributor(s)
V1.0	08/06/2020	First Draft	Alfonso Pietropaolo (ENG)
V1.1	12/06/2020	Review of the First Draft Version	Fraunhofer IAIS
V2.0	16/06/2020	Finalization of the document	Alfonso Pietropaolo (ENG)
V.3	23/06/2020	Last review by the coordinator	Sara Mateo (Zabala)

DISCLAIMER

COPYRIGHT NOTICE

Project co-funded by the European Commission in the H2020 Programme		
Nature of the deliverable:	**R**	
Dissemination Level		
PU	Public, fully open, e.g. web	✓
CL	Classified, information as referred to in Commission Decision 2001/844/EC	
CO	Confidential to DAPSI project and Commission Services	

** R: Document, report (excluding the periodic and final reports)*

DEM: Demonstrator, pilot, prototype, plan designs

DEC: Websites, patents filing, press & media actions, videos, etc.

OTHER: Software, technical diagram, etc.

EXECUTIVE SUMMARY

This document provides a technical description about the design and architecture of the cloud infrastructure provided by the DAPSI project to all users belonging to the incubation process. Thanks to this infrastructure, DAPSI teams will benefit from an on-demand, ready-to-use virtual environment, so that they can focus on the business aspects of their solution. Startups, SMEs, and researchers will experience simplification of the setup and management of the technological infrastructure, at no cost.

Since the infrastructure is based on FIWARE[1] and FIWARE Lab technology, some background info about the FIWARE ecosystem are essential to better understand contents of this document:

FIWARE is a curated framework of open source platform components that can be assembled together and with other third-party platform components to build Smart Solutions faster, easier, and cheaper. A simple yet powerful API (FIWARE NGSI) enables the integration of components and provides the basis for the interoperability and replication (portability) of smart solutions. The main and only mandatory component of any "Powered by FIWARE" platform or solution is the FIWARE Context Broker Generic Enabler, bringing a cornerstone function in any smart solution. Built around the FIWARE Context Broker, a rich suite of complementary FIWARE Generic Enablers are available in the FIWARE catalogue[2], dealing with the following fields:

- Interfacing with the Internet of Things (IoT) Robots and third-party systems;
- Context Data/API management, publication, and monetization;
- Processing, analysis, and visualization of context information.

FIWARE Lab is a non-commercial sandbox environment where innovation and experimentation based on FIWARE technologies take place. Entrepreneurs and individuals can test the technology as well as their applications on FIWARE Lab, exploiting Open Data published by cities and other organizations. FIWARE Lab is deployed over a geographically distributed network of federated nodes leveraging on a wide range of experimental infrastructures. The DAPSI cloud infrastructure is one of those federated node, based on OpenStack[3] technologies and located precisely in an ENG's Data Center in Vicenza (Italy).

To maximize flexibility, sub-grantees are also allowed to adopt a hybrid deployment approach (distributed over DAPSI, own- and third-party infrastructures) for data, tools, and computation.

In order to guarantee a reasonable level of usability, a quota mechanism for computation, networking, and storage resources for each experiment will be established. Guidelines on how to configure containers will be also prepared, based on Docker[4], so that open call winners can prepare the business logic associated with their products.

After the finalization of the first call, a review of the infrastructure design will be performed for the benefit of subsequent calls. This process will take into account the feedback received from the participants of the program.

[1] https://www.fiware.org/
[2] https://www.fiware.org/developers/catalogue/
[3] https://www.openstack.org
[4] https://www.docker.com

This document does not describe the result of applying those technologies to the DAPSI project that will be part of the "D5.2 operation, support and update" but it is more a guide about the architecture of the infrastructure and procedures (inspired by common practices followed in the developer world, SCRUM and ITIL methodology) put in place for the management of the FIWARE Lab node.

This document represents a snapshot of the current use of the tools as of the date of the document. Procedures and tools may vary dynamically according to technology updates, users and business needs.

TABLE OF CONTENTS

1 ARCHITECTURE 8
2 HARDWARE RESOURCES 11
3 ACCOUNT MANAGEMENT 12
4 MONITORING 17
5 BASE-IMAGES MANAGEMENT 26
6 POLICIES DEFINITION 27
7 CONCLUSIONS 28

LIST OF FIGURES

FIGURE 1 FIWARE LAB ARCHITECTURE SCHEMA 9
FIGURE 2 FIWARE LAB CREATE NEW ACCOUNT FORM 16
FIGURE 3 FI-HEALT STATUS PAGE 18
FIGURE 4 FIWARE LAB INFOGRAPHIC MONITORING TOOL 20
FIGURE 5 FIWARE LAB STATUS PAGE 21
FIGURE 6 DEEP LOG INSPECTION TOOL 22
FIGURE 7 ENG CUSTOM MONITORING 23
FIGURE 8 USAGE OF RESOURCES 24
FIGURE 9 NETWORK TRAFFIC BY PROJECT 24
FIGURE 10 CPU UTILIZATION BY PROJECT 25
FIGURE 11 WARNINGS AND ERRORS 25

LIST OF TABLES

TABLE 1 FIWARE LAB NODE HARDWARE RESOURCES 11
TABLE 2 TOTAL AVAILABLE RESOURCES 12
TABLE 3 DEFAULT OPENSTACK FLAVOURS 13
TABLE 4 OPENSTACK NOVA DEFAULT QUOTA 13
TABLE 5 OPENSTACK NEUTRON DEFAULT QUOTA 14

1 ARCHITECTURE

The Application Infrastructure (FIWARE Lab) is freely available to all sub-grantees for experimenting purposes starting from the first phase of the three incubation interactions.

Selected sub-grantees can create a set of virtual machines with pre-determined features in terms of processing power and memory. These features could increase during the different phases of the project and according to users' needs.

The use of the Application Infrastructure is not mandatory and each participant can use his/her own infrastructure.

The Application Infrastructure tries to meet the following requirements:

- Virtual Machines provisioning. In order to host the developed applications and, if required, the application containers used to deploy them: a private network must be available to connect the internal services that interoperate to provide the final application;
- Public IP addresses. At least a public IP address for each sub-grantees must be provided in order to expose the deployed application on the internet: the possibility to have more than a single public IP address will depend on the availabilities of the infrastructure;
- Possibility to deploy different services supporting the final application. In particular, it could be necessary to deploy local databases, brokers and other services interoperating with the application container;
- Data and application security. Ensure privacy and security for the application developed by sub-grantees.

As one of the major FIWARE Foundation founders, Engineering has implemented the following FIWARE Lab node architecture in order to foster the wider adoption of FIWARE technologies in Italy and abroad:

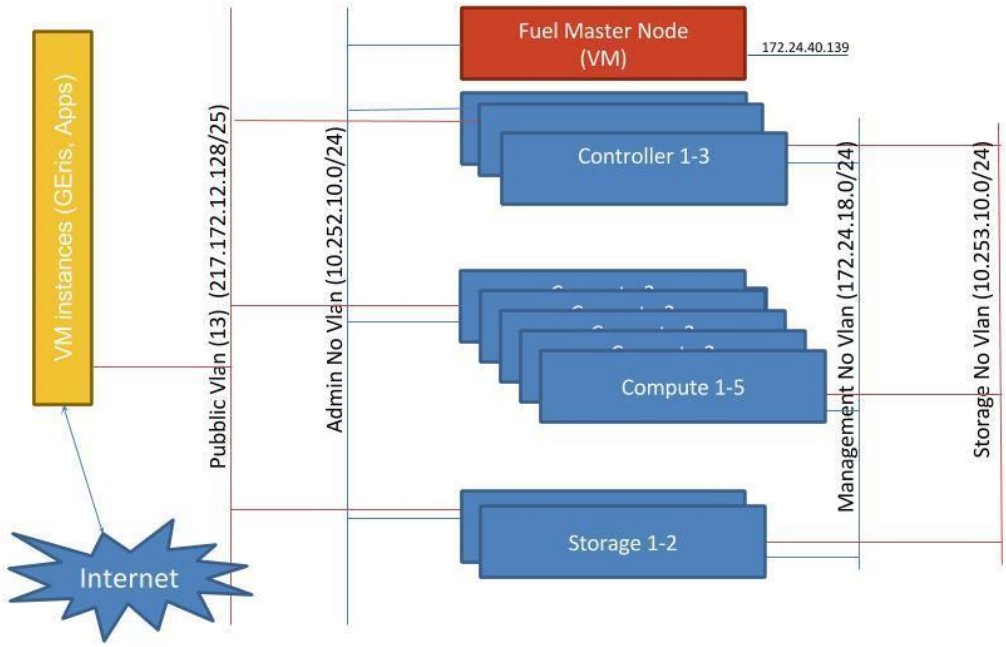


FIGURE 1 FIWARE LAB ARCHITECTURE SCHEMA

The Node is operated in a high secure Data Center located in Vicenza (Italy). For the protection of the entire FIWARE environment, Engineering uses the firewall and DDoS protection technology. The infrastructure is currently monitored under a 24X7 "gold" support contract, which ensures immediate action for any failure and is currently being defined a weekly backup policy.

As shown in the picture above (figure 1), the entire cluster is deployed through a "FUEL (Mirantis[5])" Master Node where the architecture is defined (number and characteristics of the nodes, compute nodes, controller nodes, networks, and storage).

In our case, we decided to have **3 controllers** deployed in High Availability (one always on), **5 compute** nodes for the execution of the different VMs, and **2 storage** nodes for volumes management.

The main role of the 3 controller node is to ensure that all OpenStack internal services are running and addressed to the proper VM (running on the compute node) and storage.

Namely, it manages the following services:

- **Neutron** for the network;
- **Cinder** for volumes;
- **Nova** for VMs;
- **Glance** for images;

[5] https://www.mirantis.com/software/mcp/openstack/fuel/

- **Ceilometer** for monitoring;
- **Horizon** for the Dashboard;
- **HA proxy** services;
- **Keystone** for Identity Management.

The role of the compute nodes is to actually run and host VMs, and last, the storage nodes provide disks, volumes, and virtual images to all VMs in a persistent way.

All physical servers (compute, provisioning and storage) are connected to a Data Center network with dual 10GE links to separate top-of-rack (ToR) switches. The complete Infrastructure runs on a 10 Gbit per second network. For the connection to the internet, there is a DDoS and a Firewall appliance running in a clustered mode. The bandwidth towards the internet is 1000 Mbit. A bandwidth of 100 Mbit per second is guaranteed for the use of FIWARE Lab. All components of the network are planned and built in a redundant and high available way.

All storage for instances, block volumes, and objects are provided by a Ceph cluster with 32 TB of raw storage across 2 servers with a replication factor of 2.

A full list of services, tools and components included within the aforementioned deployed architecture and part of the Openstack and FIWARE project are summarized here:

- Dedicated Management Network;
- Dedicated Management Firewall for security and filtering within the management environment and a connection towards the following components:
    - Management server zones
    - OOB/ILO network
    - Management of the Storage components.
- FIWARE Cloud Compute Service based on OpenStack Nova providing the ability to provision and manage VM and Linux Containers, as well as associated resources and artefacts. This is the most foundational part of the FIWARE Cloud, allowing to host arbitrary applications including FIWARE GEs and 'custom' applications;
- FIWARE Cloud Image Service based on OpenStack Glance, providing the ability to manage pre-built images that can be used to provision VMs (with operating system and a software stack pre-installed in the image) or Linux containers (typically comprising only the files of the application itself and its dependencies, rather than a full operating system);
- FIWARE Cloud Volume Service based on OpenStack Cinder providing the ability to provision and manage block storage (which can be attached to VMs and Linux Containers to keep the persistent state of the applications hosted on FIWARE Cloud);
- FIWARE Cloud Network Service based on OpenStack Neutron providing the ability to provision and manage virtual networks (connecting VMs and Linux Containers between them and to the external network);

- FIWARE Cloud Orchestration Service based on OpenStack Heat, providing the ability to orchestrate provisioning and ongoing management (e.g., auto-scaling) of collections of basic resources (VMs, networks, etc.), including inter-dependencies between them;
- FIWARE Cloud Object Storage Service based on OpenStack Swift providing a scalable, resilient and efficient facility to store and retrieve 'blob' objects and associated metadata, as well as to run computations (storlets) on objects;
- FIWARE Cloud Application Management Service based on OpenStack Murano providing the ability to manage provisioning and configuration of complex applications, including basic resources as well as software configuration within the VMs/containers;
- FIWARE Cloud Policy Service, providing the ability to define rules and apply actions in response to certain events associated with cloud resources and their state;
- FIWARE Cloud Monitoring Service, providing the ability to collect and distribute resource metrics associated with VMs or hosts.

2 HARDWARE RESOURCES

The following table (table 1) represents the summary of the hardware used for deploying the cluster:

node	CPU	RAM	HD	NETWORK
1x Master Node (virtual machine)	4 CORE	8 GB	80 GB	2 net. card 1.0 Gbps
3x Controller Node (DELL Inc PowerEdge M360)	48x 2.29 GHz	384 GB	0.3 TB	8 net. Card 10Gbps
5x Compute Node (DELL Inc PowerEdge M360)	48x 2.29 GHz	384 GB	0.3 TB	8 net. Card 10Gbps
2x Storage Node (DELL Inc PowerEdge R730xd)	24x 2.40 GHz	128 GB	1x 300GB + 5x 3.3 TB	4x net. Card 10Gbps + 2x net. Card 1.0 Gbps

TABLE 1 FIWARE LAB NODE HARDWARE RESOURCES

As a result of the hardware chosen for the deployment, the following table (table 2) shows the resources available for the end-users.

Note that the following resources are the total available and not the actual available at moment of writing this document.

CORES	RAM (GB)	BLOCK STORAGE	OBJECT STORAGE	BANDWIDTH	PUBLIC IPs
240 (x4)	1888	16.3 TB	16.3 TB	100Mbps	128

TABLE 2 TOTAL AVAILABLE RESOURCES

3 ACCOUNT MANAGEMENT

3.1 QUOTA DEFINITION

To prevent system capacities from being exhausted without notification, quotas are operational limited. For example, the number of gigabytes allowed per tenant can be controlled to ensure that a single tenant cannot consume all of the disk space. Quotas are currently enforced at the tenant (or project) level, rather than the user level.

Quotas are executed by making a claim, or reservation, on resources when a request is made, such as creating a new server. If the claim fails, the request is rejected. If the reservation succeeds then the operation progresses until such a point that the reservation is either converted into usage (the operation was successful) or rolled back (the operation failed).

Typically, the quota reservation is made in the nova-api service and the usage or rollback is performed in the nova-compute service, at least when dealing with a server creation or move operation.

As show in the tables below, Openstack comes with a set of default quota flavours (table 3), a set of default Nova quotas (table 4), and a set of Neutron quotas (table 5):

ID	Name	Memory (GB)	Disk (GB)	Ephemeral	Swap	vCPUs	RXTX factor	Public
1	M1.tiny	512	1	0		1	1.0	True
2	M1.small	2048	20	0		1	1.0	True
3	M1.medium	4096	40	0		2	1.0	True
4	M1.large	8192	80	0		4	1.0	True

TABLE 3 DEFAULT OPENSTACK FLAVOURS

Quota	Limit
Instances	2
Cores	4
RAM	4096
Floating IPs	1
Fixed IPs	-1
Metadata Item	1024
Injected files	5
Injected file content (bytes)	20240
Injected file path (bytes)	255
Key Pairs	10
Security Groups	10
Security Groups Rules	20

TABLE 4 OPENSTACK NOVA DEFAULT QUOTA

Field	Value
Floating IP	1
Network	5
Port	20
Router	1
Security Group	-1
Security Group Rule	-1
Subnet	5

TABLE 5 OPENSTACK NEUTRON DEFAULT QUOTA

3.2 ACCOUNT TYPES AND CREATION

FIWARE Lab Accounts can be categorized into two types: Trial and Community. Trial accounts provide limited resources for a reduced period.

A Trial account provides the following default quotas:

- 14 days of duration;
- 1 public IP address;
- 2 virtual machines instances, each of which has 2 virtual CPUs
- 40 GB of hard disk space;
- 4GB of RAM.

All the participants selected for the 1st phase will be provided (if asked) with a Trial account that will last for the whole phase.

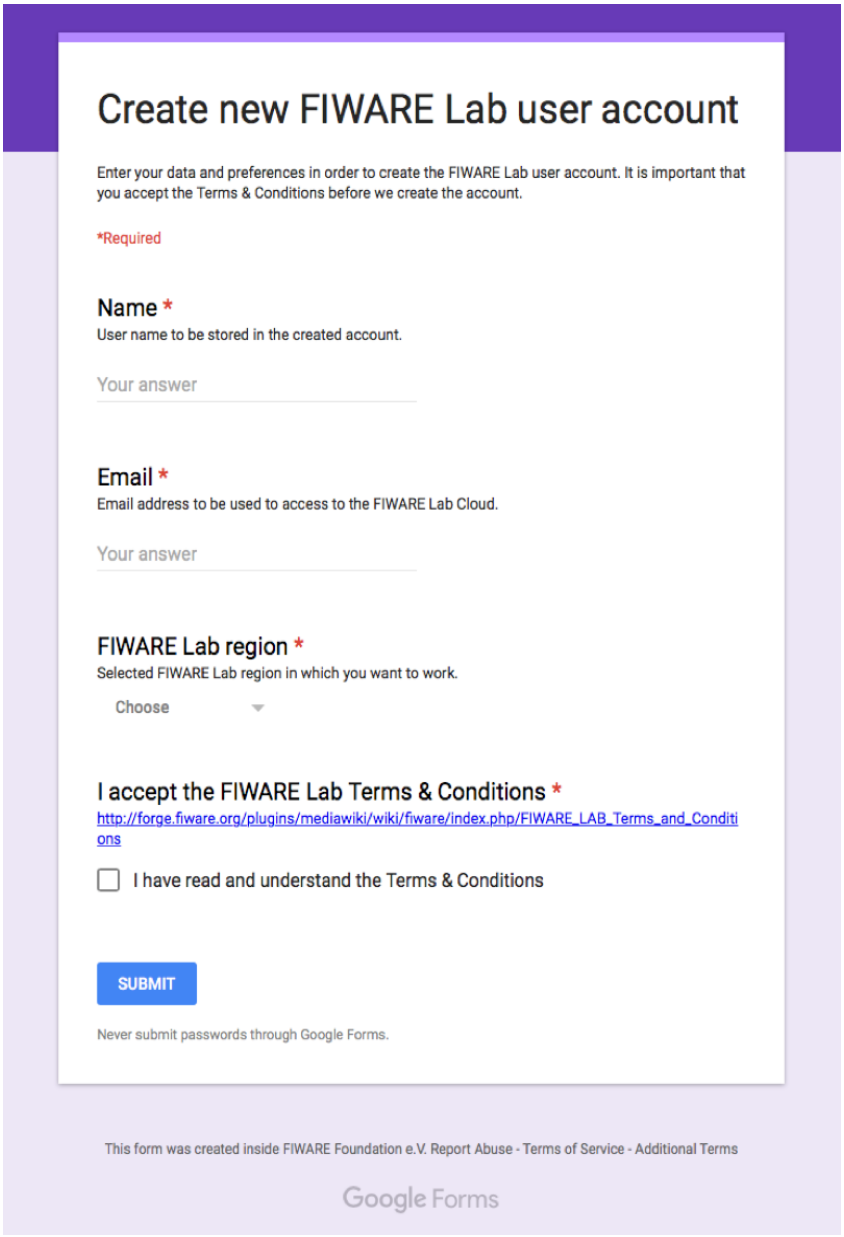
A Community Account that will last for 9 months will then be provided during the 2nd phase and the amount of resources will be defined according to users' needs.

In order to receive a new Trial Account it will be necessary to sign-in to the FIWARE Lab home page available at https://cloud.lab.fiware.org/ and clicking on CREATE ACCOUNT.

The process to create a new FIWARE Lab user account, includes also a procedure to check that the email introduced is a valid email. During this process, FIWARE requested the information from the user to be completed in a Google Form. This information includes a User Name to be kept in the database and a User Email to communicate any issue directly to the user.

In order to finalize the process, users will be also asked to select a FIWARE Lab region (Vicenza for DAPSI users) and to accept FIWARE Lab Terms & Conditions.

As shown in the picture below (figure 2) all data are mandatory to be filled. This form activates a specific procedure to manage the creation of the FIWARE Lab user account:



Create new FIWARE Lab user account

Enter your data and preferences in order to create the FIWARE Lab user account. It is important that you accept the Terms & Conditions before we create the account.

*Required

Name *
User name to be stored in the created account.

Your answer

Email *
Email address to be used to access to the FIWARE Lab Cloud.

Your answer

FIWARE Lab region *
Selected FIWARE Lab region in which you want to work.

Choose

I accept the FIWARE Lab Terms & Conditions *
http://forge.fiware.org/plugins/mediawiki/wiki/fiware/index.php/FIWARE_LAB_Terms_and_Conditions

I have read and understand the Terms & Conditions

SUBMIT

Never submit passwords through Google Forms.

This form was created inside FIWARE Foundation e.V. Report Abuse - Terms of Service - Additional Terms

Google Forms

FIGURE 2 FIWARE LAB CREATE NEW ACCOUNT FORM

4 MONITORING

In order to operate and administer the node, preventing any possible issue, and recover as soon as possible from fails, another very important aspect is how to monitor performance and availability. In this chapter, we will see tools and procedures put in place. In particular we will see 4 tools (FI-HEALTH, INFOGRAPHIC, STATUS CHECK and DEEP LOG) part of the centralized FIWARE LAB monitor architecture developed in collaboration with FIWARE, and 1 custom internal solution designed by ENG.

4.1 FI-HEALTH

FI-Health is an end-to-end testing tool that ensures that the OpenStack integrated components is working as expected.

Each of the FIWARE Lab nodes is tested in a real-world scenario using the OpenStack Rest API provided by the federated Keystone service endpoints. The idea behind these tests is to provide end-to-end testing of the FIWARE Cloud Portal to test whether the flow of the application is performing as designed from start to finish.

The purpose of carrying out these end-to-end tests is to identify OpenStack services problems before or at the same time that the users can observe those problems in the FIWARE Cloud Portal. Therefore, FI-Health is the key component to provide quality of service in the FIWARE Cloud environment. More information about the component is available by accessing the FIWARE Health GitHub repository[6].

[6] FIWARE Health GitHub repository

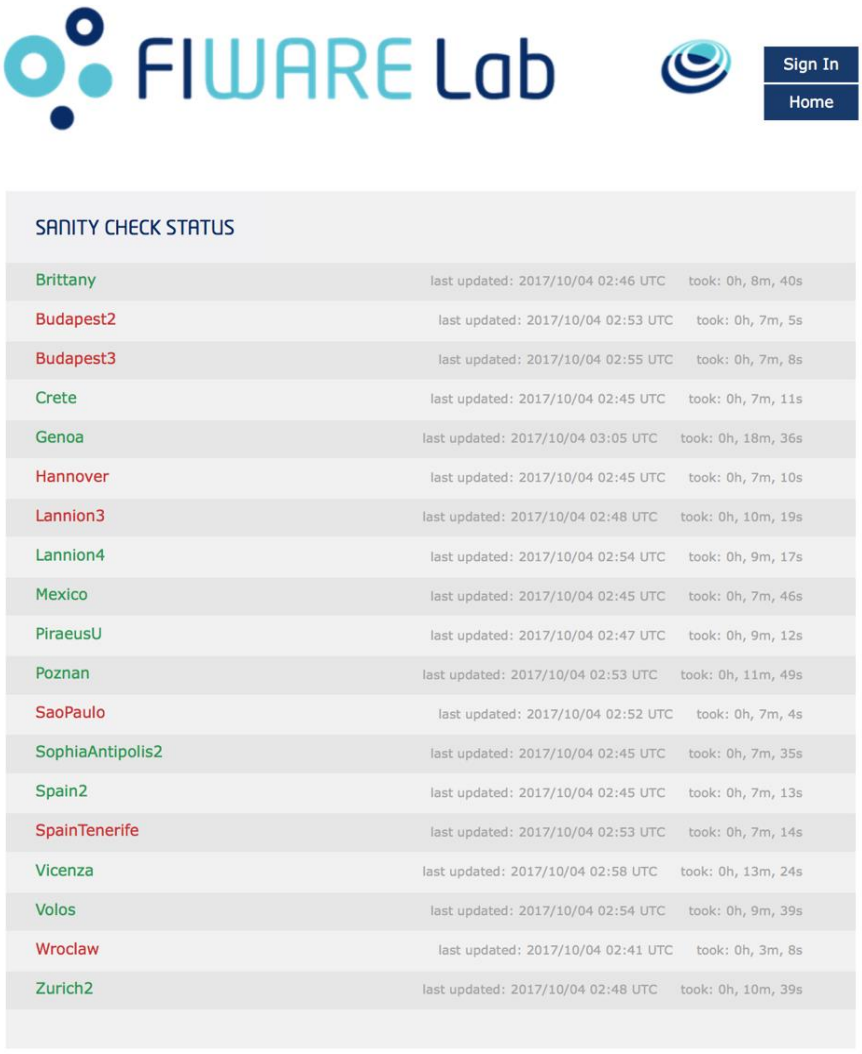


FIGURE 3 FI-HEALT STATUS PAGE

4.2 INFOGRAPHIC

FIWARE Lab Infographics and Status Pages are simple but important services to allow users to:

- Know in an intuitive way the infrastructure capacities made available by FIWARE Lab infrastructure;
- Monitor current status of infrastructure services and know about any issue.

While the information on infrastructure capacities is more related to marketing, the one on services status is extremely important to support Developers and Federation Managers operations.

The production URL of the Infographics is the following:

- http://infographic.lab.fiware.org/
- http://status.lab.fi-ware.org/

This component provides capacity information about the different OpenStack regions and status information of infrastructure services. The Federation Monitor component exposes data on the capacity and status of FIWARE Lab infrastructure through a set of RESTful API that Infographics and Status Pages calls in order to get that data.

For more details, it is recommended to refer to the main documentation included in the software repository[7].

Figure 4 shows the main page of the Infographics tool. It is comprised of:

- a user's section: it shows the total number of users as sum of Basic Users, Trial Users and Community Users;
- a map that shows all nodes;
- six interactive tabs that display different data;
- the list of FIWARE Lab Capacity supporters.

When data about a specific node are obsolete, the node in the map is grey and the user can check the timestamp of its last update by passing the cursor over it.

[7] https://github.com/SmartInfrastructures/fi-lab-infographics

FIGURE 4 FIWARE LAB INFOGRAPHIC MONITORING TOOL

The Status page (figure 5) depicted below is composed by:

- a big map that shows all the nodes and their overall status (green, yellow or red);
- a table showing the current status of all the FIWARE Lab nodes services together with the FIHealth Sanity Check status (FIHealth Sanity Check executes periodically a set of tests on the nodes in order to verify if the basic functionalities are guaranteed);
- a histogram that shows the average on the last selected months of the Sanity Check status for each node.

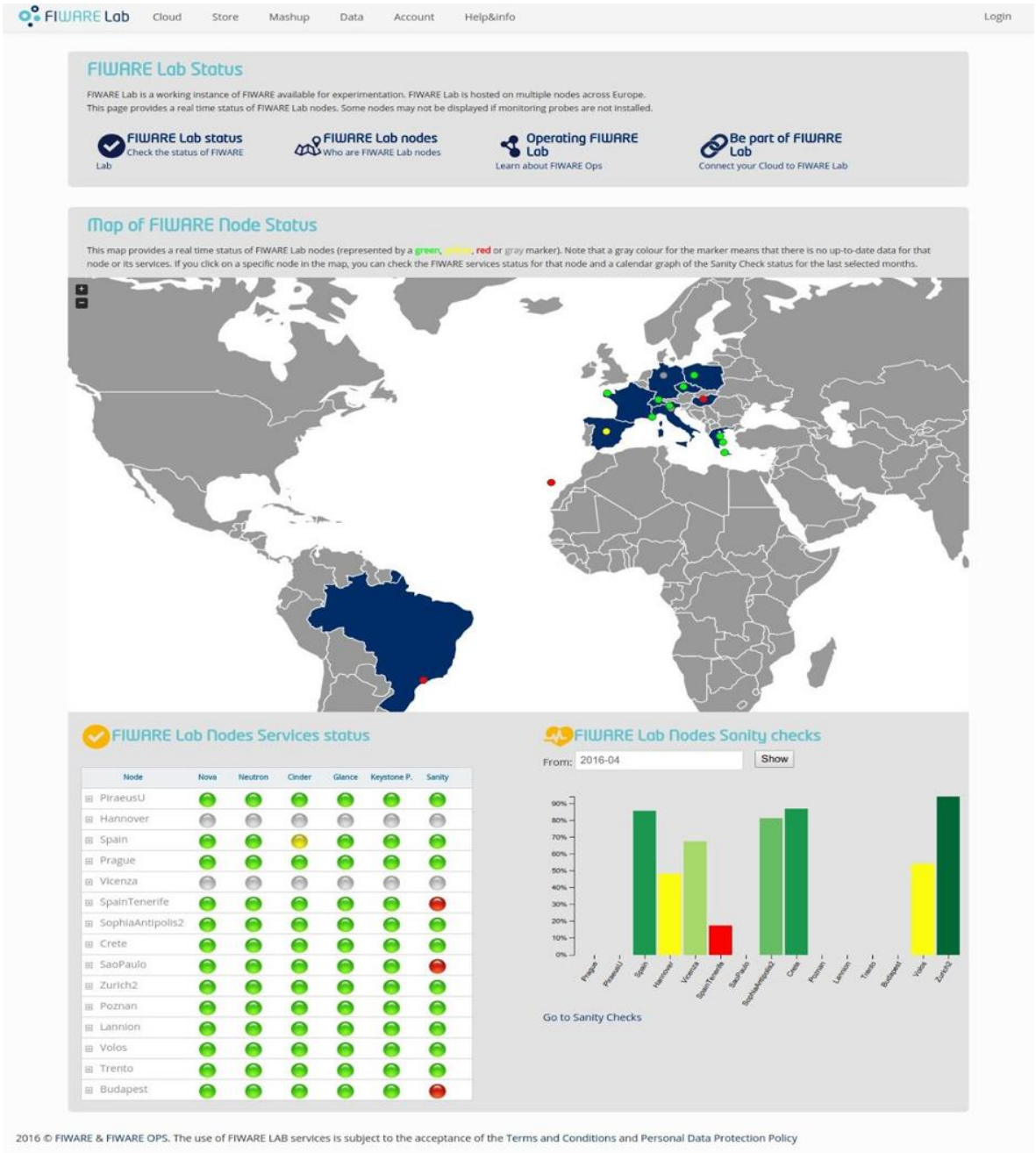


FIGURE 5 FIWARE LAB STATUS PAGE

4.3 DEEP LOG INSPECTION

Deep log inspection allows the node admin to analyse logs in a smart way, through a simply but powerful web interface (figure 6):

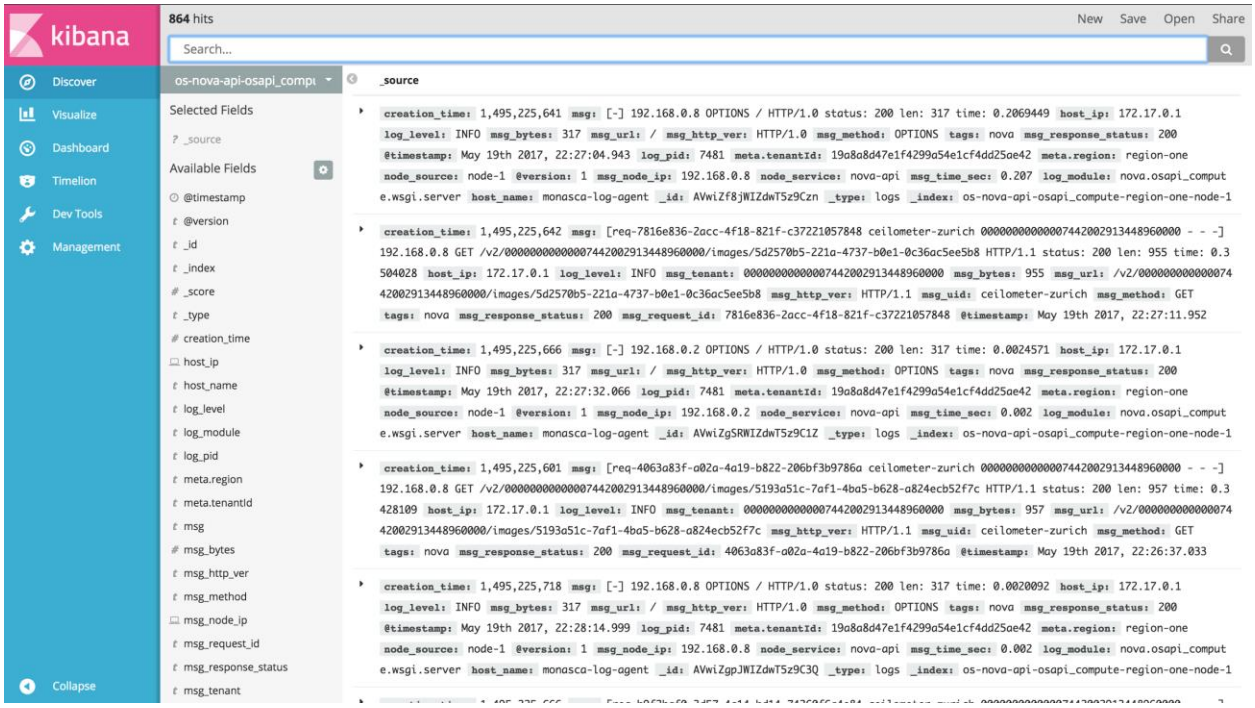


FIGURE 6 DEEP LOG INSPECTION TOOL

Different queries and visualizations are available to simplify admins routine analysis over the logs. More info are available at this link: http://deep-log-inspection.readthedocs.io/en/latest/

4.4 CUSTOM INTERNAL MONITORING

Alongside the centralized monitor architecture, ENG has developed a custom solution based on Grafana[8], to monitor its services and resources in order to optimize resource allocation among different projects and users.

Figure 7 shows the custom architecture developed by ENG:

[8] https://grafana.com

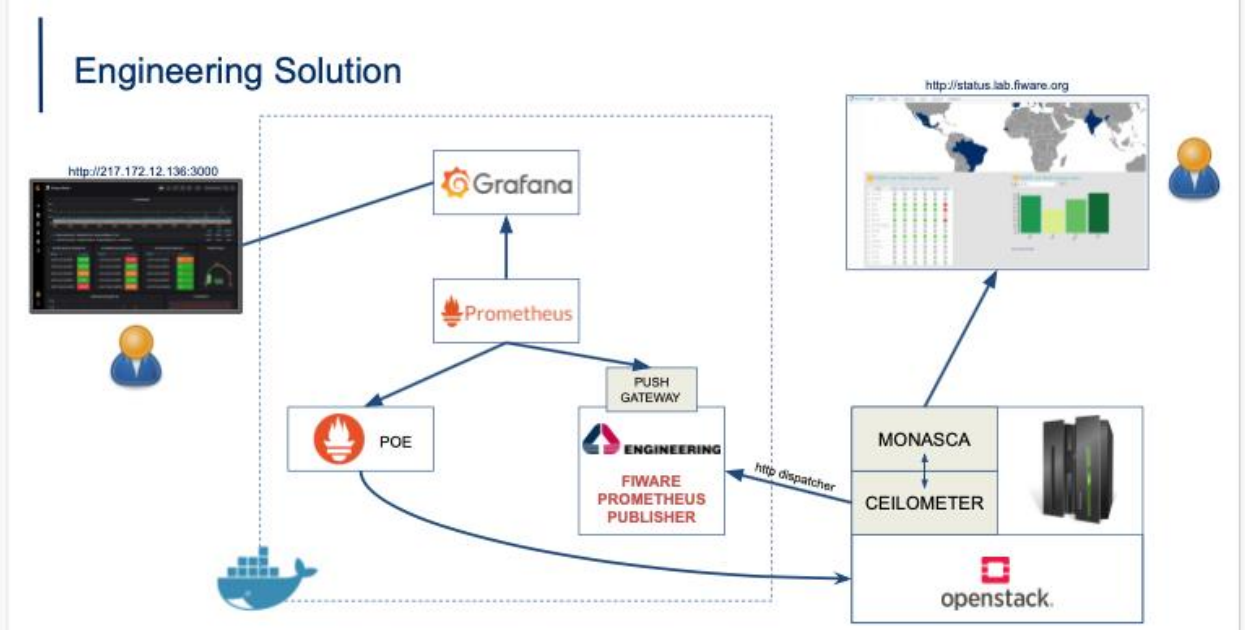


FIGURE 7 ENG CUSTOM MONITORING

Grafana represents the main tool used to visualize graphs and charts in a fashionable way (it exposes a customized dashboard available at http://vicenza.ddns.info/ - see the upper left side of the above picture). As it is shown, Grafana doesn't contain data, but it is fed by an Open Source Prometheus[9] database that takes data from OpenStack in either "get" or "push" way. For real-time information it is Prometheus that asks OpenStack to provide metrics through a POE plugin; while for historical data it is OpenStack Ceilometer that feeds the Prometheus database through a custom ENG plugin (FIWARE PROMETHEUS PUBLISHER – see the component at the centre-right of the picture) useful to convert Ceilometer metrics in Prometheus language. Moreover, as shown by the component at the upper left side, OpenStack sends information to the centralized monitor tool (see chapter 4.2 INFOGRAPHIC) by a Monasca[10] plugin.

[9] https://prometheus.io
[10] https://github.com/openstack/monasca-agent/blob/master/docs/Plugins.md

The following pictures (Figures 8 – 11) represent the final result of the custom monitoring architecture with some screenshot of the monitoring dashboard:

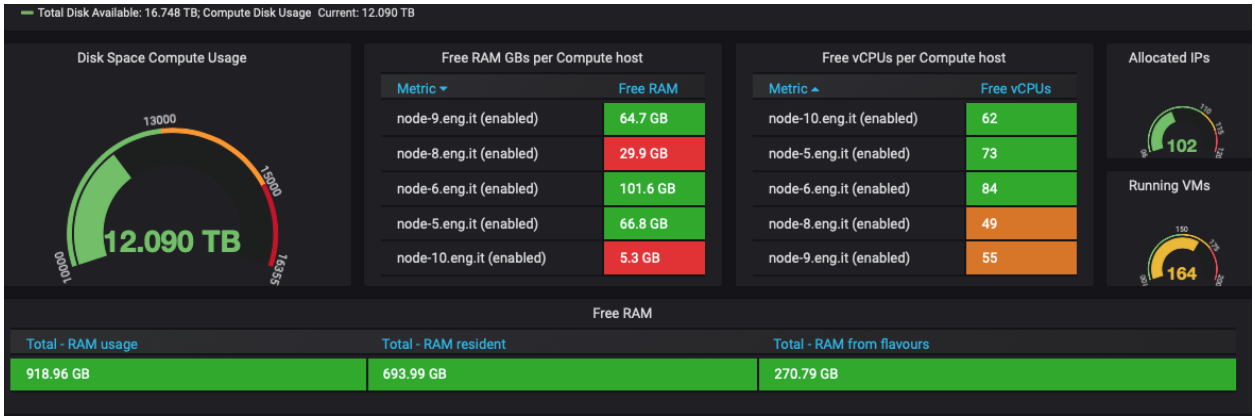


FIGURE 8 USAGE OF RESOURCES

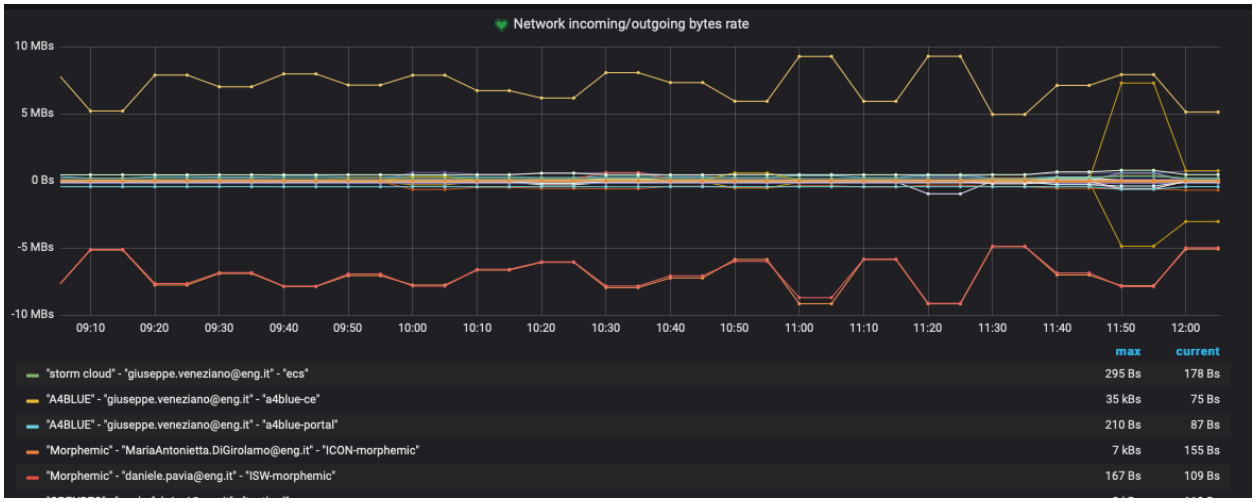


FIGURE 9 NETWORK TRAFFIC BY PROJECT

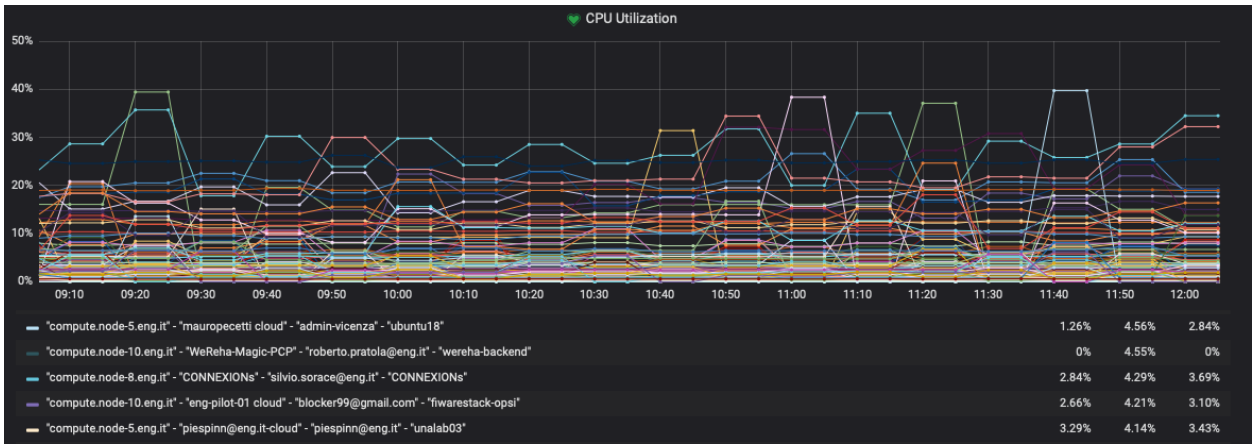


FIGURE 10 CPU UTILIZATION BY PROJECT

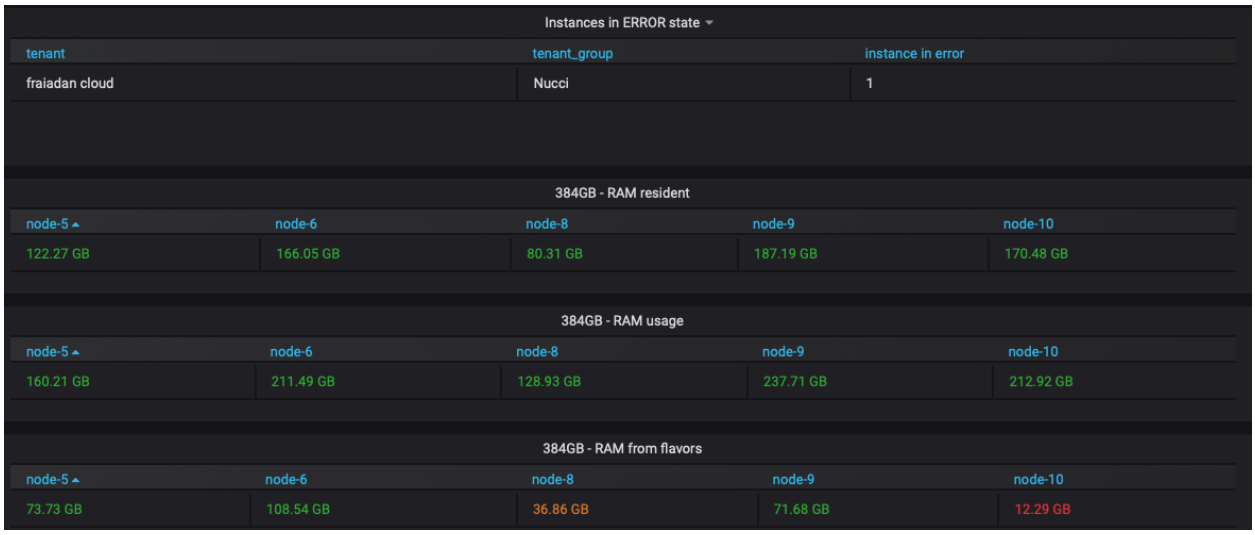


FIGURE 11 WARNINGS AND ERRORS

5 BASE-IMAGES MANAGEMENT

As part of the features offered by our application infrastructure, a set of pre-built virtual images are available to all users to easily deploy MVs with either Linux vanilla distribution or VMs with pre-configure FIWARE Generic Enablers.

The creation of base images is a very important operation mainly due to the security updates and configuration of them. We download the official images from the different OS supported in FIWARE Lab for OpenStack. There are three options that we can manage:

- CentOS 6 and 7;
- Ubuntu 14.04 and 16.04 (LTS releases);
- Debian 7 and 8.

However, we try to modify these images in order to make the default image a little more secure doing some operations on the Base Image. For this purpose, we follow the recommendations of the Centre for Internet Security (CIS[11]). CIS is a forward-thinking, non-profit entity that harnesses the power of a global IT community to safeguard private and public organizations against cyber threats

CIS Benchmarks is the global standard and recognized best practices for securing IT systems and data against the most pervasive attacks. It provides a very exhaustive guideline, continuously refined and verified, to configure Operating System in a secure way.

The recommendations that we adopt in the configuration of the virtual machines are the following:

- We remove the default password for the default user. Additionally, the only valid method to login on the Instances is through public-private key;
- Root user is disabled to be used to access to the Instance through SSH;
- We remove the less secure ciphers from the valid ciphers and the less secure Key exchange methods;
- We add a Warning banner explaining that an authorization is needed to access to these Instances;
- We add some IPTables rules to ensure that by default, only some ports (ssh, http and https can be used);
- By default, we enable only automatic security updates;
- The administrative access to the instances is using a specific user with both password and public-private key.

[11] https://www.cisecurity.org

6 POLICIES DEFINITION

As privacy policies definition, it is important to remark that ENG does not host any personal data in its Data Center. All personal information such username and email are stored within the centralized Identity Manager hosted by the FIWARE FOUNDATION.

ENG can only read these data for administration purposes (such as assign resources to a specific user).

Hereunder are reported privacy policy, terms and condition and cookies policies as described from the FIWARE FOUNDATION.

6.1 PRIVACY POLICY

The Privacy Policy is changed taking into account the change of ownership of the data from Telefónica I+D, S.A.U. to FIWARE Foundation, e.V.

Additionally, a depth revision of the content of this policy was made in order to update the content and provide a more detailed information about it. The result of this update can be seen in the corresponding "Annex A" Private Policy updated and it will be updated at the following URL:

http://forge.fiware.org/plugins/mediawiki/wiki/fiware/index.php/FIWARE_Privacy_Policy

6.2 TERMS & CONDITIONS

The Terms & Conditions is also updated following the last updated in the FIWARE ecosystem. This content makes reference to the use of the FIWARE Lab resources and the definition of the rights and obligations both in FIWARE Lab and user of these resources. The termination of these conditions and how to apply it besides with the intellectual property and proprietary rights. This content is reflected in the following URL:

http://forge.fiware.org/plugins/mediawiki/wiki/fiware/index.php/FIWARE_LAB_Terms_and_Conditions

The update of these Terms & Conditions will be notified to the users via email in order that they will be notified about the changes of them.

6.3 COOKIES POLICY

An update of the current Cookies Policy was driven in order to reflect the changes in the ownership of the data. The "Annex B" Cookies Policy updated reflects these changes and in the same way reflected in the following URL:

http://forge.fiware.org/plugins/mediawiki/wiki/fiware/index.php/Cookies_Policy_FIWARE

7 CONCLUSIONS

This document aims to give an overall overview of technologies and tools used to put in place the Cloud Infrastructure offered by the DAPSI project to all DAPSI users. It is also a sort of handbook manual of the design of such infrastructure and represents a snapshot of the situation as is at the moment of writing this document.

Results and achievement, as well as details about the operation and support provided for sub-grantees, will be objects of the "D5.2 Infrastructure Operation, Support and Update" (foreseen at M20, M30, M36). Since it is not expected a second version of the present deliverable, any update concerning design and architecture, and any other information included in this deliverable, will be then reported in the different editions of the D5.2.

ANNEX A

FIWARE Privacy Policy

This is the main privacy policy for fiware.org and for certain services provided through these and other FIWARE websites and applications ("our sites") by FIWARE Foundation, e.V. ("FIWARE").

At FIWARE we collect different types of information about our users for three main reasons:

1. To provide personalised services unique to individual users.
2. To help us to monitor and improve the services we offer.
3. If we have permission from the user, to market services, always in scope of the FIWARE Foundation mission, to them.

There may be other privacy policies that apply to certain services we provide. Please read these when you register or subscribe for these services on these sites.

Our principles

1. FIWARE adopts the necessary technical and organisational measures to avoid the loss, misuse, alteration, unauthorised access or theft of the personal data provided, taking into account the state of technology, the nature of the data and the risks to which they are exposed. This means:

- we make sure that we have appropriate security measures to protect your information; and
- we make sure that when we ask another organisation to provide a service for us, they have appropriate security measures.

2. We will respect your privacy. You should receive marketing emails only from us and, if you agree, from other organisations we have carefully chosen following the current European and German legislation. We will make sure it is clear when you can make these choices. However, we may email you occasionally with information or questions about your registration, your subscription account or postings, for example, with reminders, warnings, business opportunities or copyright requests.

3. We will collect and use individual user details only if we have your permission or we have sensible business reasons for doing so, such as collecting enough information to manage subscriptions.

4. We will be clear in our dealings with you as to what information about you we will collect and how we will use it.

5. We will use personal information only for the purposes for which it was originally collected, how they are defined at the beginning of this document, and we will make sure we delete it securely.

6. Our site is accessible via the internet. This means that people around the world who access our website can see anything you post on the website or twitter comments with the FIWARE hash.

7. If we or our service providers transfer any information out of the European Union (EU), it will only be done with the relevant protection (stated under German law) being in place.

The information that it is collected from you consist on:

- when you register or become a member of our portals
- when you use the website
- through cookies

Certain services that we provide may involve us collecting extra information (Membership, for example or subscription detail to the FIWARE Newsletter), such as where you are, therefore the service can be provided as designed.

Registration

The minimum information we need to register you is your name, email address and a password. We will ask you more questions for different services, including newsletter subscription. Unless we say otherwise, you have to answer all the registration questions.

All responsibility for the completion of forms with false, inaccurate, incomplete or outdated information shall vest on the Users.

To assist us in our marketing, in addition to the data that you provide to us if you register, we may also obtain data from trusted third parties to help us understand what you might be interested in. This 'profiling' information is produced from a variety of sources, including publicly available data or from sources such as surveys and polls where you have given your permission for your data to be shared. You can choose not to have such data shared with the FIWARE just informing us about it.

After you have registered, and with your permission, we may send you emails we think may interest you. At any time, you can decide not to receive these emails and will be able to 'unsubscribe'.

Who we share data with

We will not share your personal information with others for marketing purposes unless you have given us your permission. If we have your permission, we will share your information only with other organisations we have chosen carefully.

We can access and release personal information to keep to relevant laws and government requests, to operate our systems properly and to protect both us and our users.

Any other organisations who access your information in the course of providing services on our behalf will be governed by strict contractual restrictions to make sure that they protect your information and keep to data-protection and privacy laws which apply. We may also independently audit these service providers to make sure that they meet our standards. We may use service providers to help us run these sites (or services available on the sites), some of whom may be based outside the EU.

Google Analytics

We use Google Analytics on our sites for anonymous reporting of site usage and for advertising on the site. If you would like to opt-out of Google Analytics monitoring your behaviour on our sites please use this link (https://tools.google.com/dlpage/gaoptout/).

Legal information and how to contact us

FIWARE advises users of the FIWARE Open Source Community services ("the Users") that FIWARE complies with the current German legislation related to Personal Data Protection, Users' Privacy and the Secrecy And Security of Personal Data, as established in the Federal Data Protection Act in the version promulgated on 14 January 2003 (Federal Law Gazette I p. 66, BGBl. I S. 66 in German), as most recently amended by Article 7 of the Act of 30 June 2017 (Federal Law Gazette I p. 2097, BGBl. I S. 2097 in German). This Act serves to implement directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ EC no. L 281, p. 31 ff.). The data controller is the organisation responsible for protecting information and, in our case, is FIWARE Foundation, e.V., Franklinstrasse 13A, 10587 Berlin.

If you would like access to or a copy of the personal information we hold about you, to request a correction, or have any questions about how we may use it or to make a complaint, please contact the Data Protection Manager at the address shown above or just email to **fiware-personaldataprotection@lists.fiware.org**.

Complaints will be dealt with by the Data Protection Manager, and will be responded to within 30 days at the latest.

If you are not satisfied with the way your complaint was handled, you may be able to refer your complaint to your local data protection regulator.

Changes to the privacy policy

Should we elect to change our privacy policy we will post the changes here. Where the changes are significant, we may also choose to email all our registered users with the new details. Where required by law, will we obtain your consent to make these changes.

Changes to this policy by date

June 2016: Creation of the FIWARE Privacy Policy.

ANNEX B

Cookies Policy FIWARE

In accordance with the applicable law regarding the use of cookies in relation to the provision of electronic communication services, We, the FIWARE Foundation e.V., hereby inform you about the cookies used on the websites owned by Us (hereinafter, the "Websites") and why they are used. By browsing the Websites, you are giving your consent for them to be used. The cookies used on our Websites include both 'our own' and those of third parties and they enable us to store and access information in relation to the language, the type of browser used and other general characteristics predefined by the user, and also to track and analyse the activity carried out in order to introduce improvements and to provide our services in a more efficient, personalised manner. Websites does not use advertising or behavioural advertising cookies. The use of cookies offers numerous advantages in the provision of information technology services, because, among others: (i) they make it easier for the user to browse the Website and access the different services on offer; (ii) they mean that users do not have to set up the general, predefined characteristics each time they enter the Website; (iii) they enable us to improve the functioning and the services provided through the Website, after the corresponding analysis of the information obtained through the cookies installed. However, users can set up their browsers to accept or reject cookies, or select those allowed and those excluded by following one of the following procedures, depending on the browser used:

- Google Chrome (in the Tools Menu)

Settings > Show advanced options > Privacy (Content Settings) > Cookies

More information: https://support.google.com/chrome/answer/95647?hl=en

- Microsoft Internet Explorer (in the Tools Menu)

Internet > Privacy > Advanced

More information: http://windows.microsoft.com/en-us/internet-explorer/delete-manage-cookies#ie=ie-9

- Firefox

Options > Privacy > Cookies

More information: http://support.mozilla.org/en-US/kb/enable-and-disable-cookies-website-preferences

- Safari, iPad y iPhone

Preferences > Privacy

More information: http://www.apple.com/privacy/use-of-cookies/

- Opera

Settings > Preferences > Advanced > Cookies

More information: http://help.opera.com/Linux/10.60/en/cookies.html

Analytical cookies

These make it possible to track and analyse the behaviour of the users of the websites with which they are associated.