Deliverable D300.4

System and Support for V2 of the Hosting Environment & Advanced Integration of GEs

WP 300

Project Acronym & Number:	FIspace – 604 123
Project Title:	FIspace: Future Internet Business Collaboration Networks in Agri-Food, Transport and Logistics
Funding Scheme:	Collaborative Project - Large-scale Integrated Project (IP)
Date of latest version of Annex 1:	03.10.2013
Start date of the project:	01.04.2013
Duration:	24

Status:	Final
Authors:	Eliezer Dekel
Contributors:	WP 300
Document Identifier:	D300.4-HostingEnvironment-V2&GE-AdvIntegr-V008-Final.docx
Date:	20.03.2014
Revision:	008

Project website address:	http://www.FIspace.eu

The FIspace Project

Leveraging on outcomes of two complementary Phase 1 use case projects (FInest & SmartAgriFood), aim of FIspace is to pioneer towards fundamental changes on how collaborative business networks will work in future. FIspace will develop a multi-domain Business Collaboration Space (short: FIspace) that employs FI technologies for enabling seamless collaboration in open, cross-organizational business networks, establish eight working Experimentation Sites in Europe where Pilot Applications are tested in Early Trials for Agri-Food, Transport & Logistics and prepare for industrial uptake by engaging with players & associations from relevant industry sectors and IT industry.

Project Summary

As a use case project in Phase 2 of the FI PPP, FIspace aims at developing and validating novel Future-Internet-enabled solutions to address the pressing challenges arising in collaborative business networks, focussing on use cases from the Agri-Food, Transport and Logistics industries. FIspace will focus on exploiting, incorporating and validating the Generic Enablers provided by the FI PPP Core Platform with the aim of realising an extensible collaboration service for business networks together with a set of innovative test applications that allow for radical improvements in how networked businesses can work in the future. Those solutions will be demonstrated and tested through early trials on experimentation sites across Europe. The project results will be open to the FI PPP program and the general public, and the pro-active engagement of larger user communities and external solution providers will foster innovation and industrial uptake planned for Phase 3 of the FI PPP.

Project Consortium

- DLO; Netherlands
- ATB Bremen; Germany
- IBM; Israel
- KocSistem; Turkey
- Aston University; United Kingdom
- ENoLL; Belgium
- KTBL; Germany
- NKUA; Greece
- Wageningen University; Netherlands
- PlusFresc; Spain
- FloriCode; Netherlands
- Kverneland; Netherlands
- North Sea Container Line; Norway
- LimeTri; Netherlands
- Kühne + Nagel; Switzerland
- University Duisburg Essen; Germany
- ATOS; Spain
- The Open Group; United Kingdom
- CentMa; Germany
- iMinds; Belgium
- Marintek; Norway
- University Politecnica Madrid; Spain
- Arcelik; Turkey
- EuroPoolSystem; Germany
- GS1 Germany; Germany
- Mieloo & Alexander; Netherlands
- OPEKEPE; Greece
- Innovators; Greece

More Information

Dr. Sjaak Wolfert (coordinator)
LEI Wageningen UR
P.O. Box 35
6700 AA Wageningen

e-mail: sjaak.wolfert@wur.nl
phone: +31 317 485 939
mobile: +31 624 135 790
www.FIspace.eu

Dissemination Level

PU	Public	X
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Document Summary

This report describes the second version of the FIspace hosting environment. The Cloud architecture is based on OpenStack architecture used by FI-WARE. This Infrastructure as a Service (IaaS) is the platform where components developed in WP200 and Use cases (WP400) are deployed and executed. Each workpackage has different domain on the Infrastructure. The admin of the projects can create members to manage Virtual Machines. Upon a request, any developer can be added to the projects to manage their virtual machines. The document provides details on the architecture, security, login procedures, and operational support provided by KocSistem.

Abbreviations

API	application programming interface
FI PPP	Future Internet Public Private Partnership
GE	Generic Enablers
GUI	graphical user interface
http	Hypertext Transfer Protocol
IaaS	Infrastructure as a Service
ICT	Information and Communication Technology
IDM	Identity Management
IP	Intellectual Property
MOS	Market Operations Service
RAM	Random-Access Memory
RTD	Research and Technological Development
ssh	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VPN	Virtual Private Network
WP	Work Package

Table of Contents

1 Planning for Hosting environment and GE integration 5
2 FIspace Hosting Environment 5
2.1 Cloud Infrastructure 5
2.2 Access and Management of Cloud Platform 6
2.3 Network & Security Infrastructure 7
2.3.1 Secure Access Connection to the Infrastructure 9
2.4 Advanced Integration of FI-WARE GEs 9
3 Support 11
4 Conclusion and Outlook 11

List of Figures

Figure 1: FIspace OpenStack Physical Infrastructure. 5
Figure 2: Network & Security infrastructure 8

List of Tables

Table 1: GE inventory List 10
Table 2: SLA of support 11

1 Planning for Hosting environment and GE integration

This document provides the system and support of Hosting Infrastructure of FIspace and GE integration to supply cloud platform in order to run the software developed WP200 (FIspace Modules), as well as the Apps as developed as part of the use case trials defined in WP400. By using OpenStack architecture for the cloud infrastructure, module owners will have an option to deploy their virtual servers to new cloud environment in case of migration, and will also support to hosting and integration of necessary FI-WARE Generic Enablers

Architecture design and requirements of the cloud hosting environment is based on three major setups

1- Cloud Infrastructure Setup

2- Network and Security Infrastructure

3- Support

2 FIspace Hosting Environment

FIspace Hosting environment is running on openstack cloud platform. Firewall and SSL VPN appliances have been used to check access control mechanisms and provide network security for the development environment. All of the infrastructure details have been explained on D300.2 and user guide of the Cloud Platform.

2.1 Cloud Infrastructure

Each server has a capacity of 160 virtual machines up on required RAM, each node RAM capacity extendible up to 768 GB. 2x300GB internal storage of each node, external storage capacity is available via both NAS and SAN and will be provided upon request from module owners and deployed GE requirements.

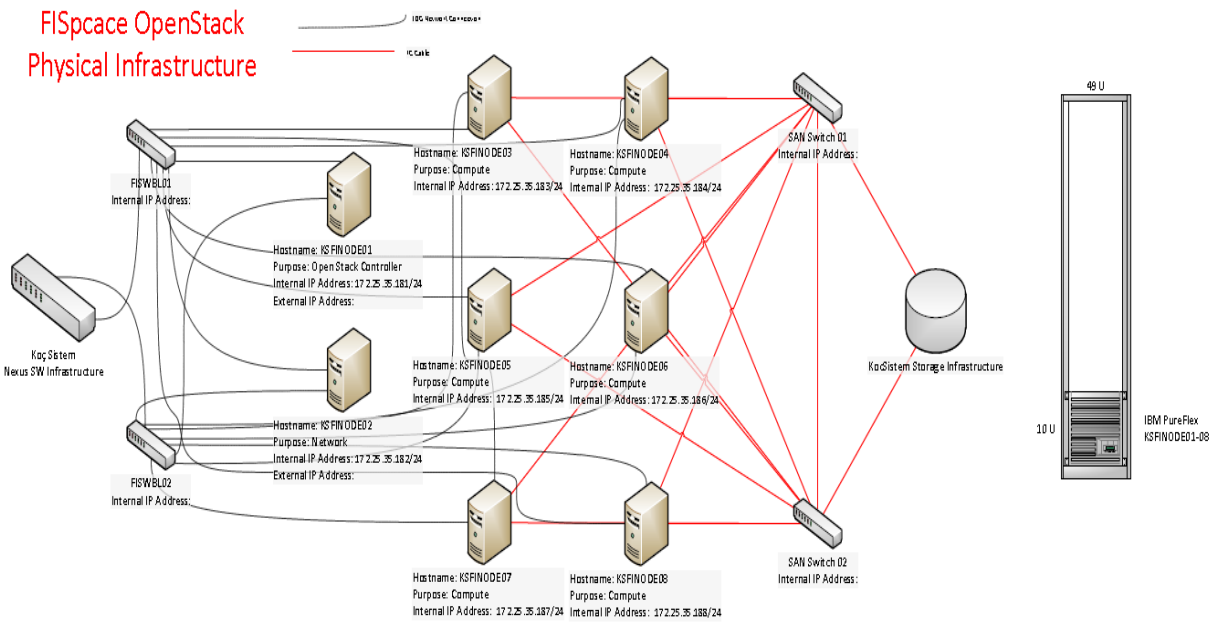
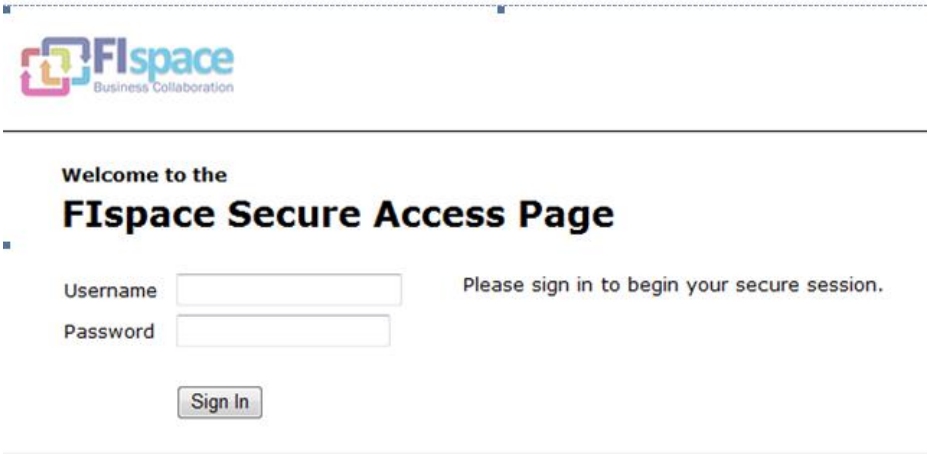


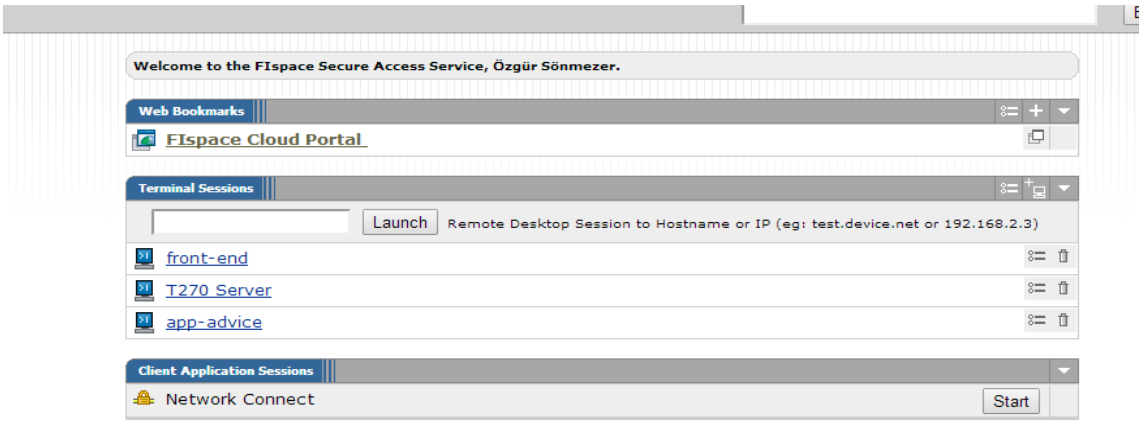
Figure 1: FIspace OpenStack Physical Infrastructure.

2.2 Access and Management of Cloud Platform

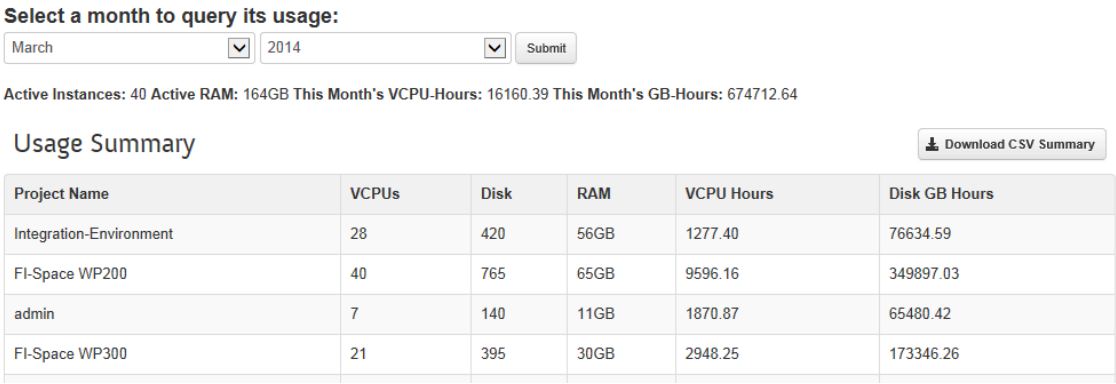


FIspace Developers logins to the secure access page of FIspace : https://37.131.248.22/fispace

After Successful login, develpers can acces to 'FIspace Cloud Portal' link on the access page to manage Cloud Platform



After successful Login, Project overview screen appears with given permission.

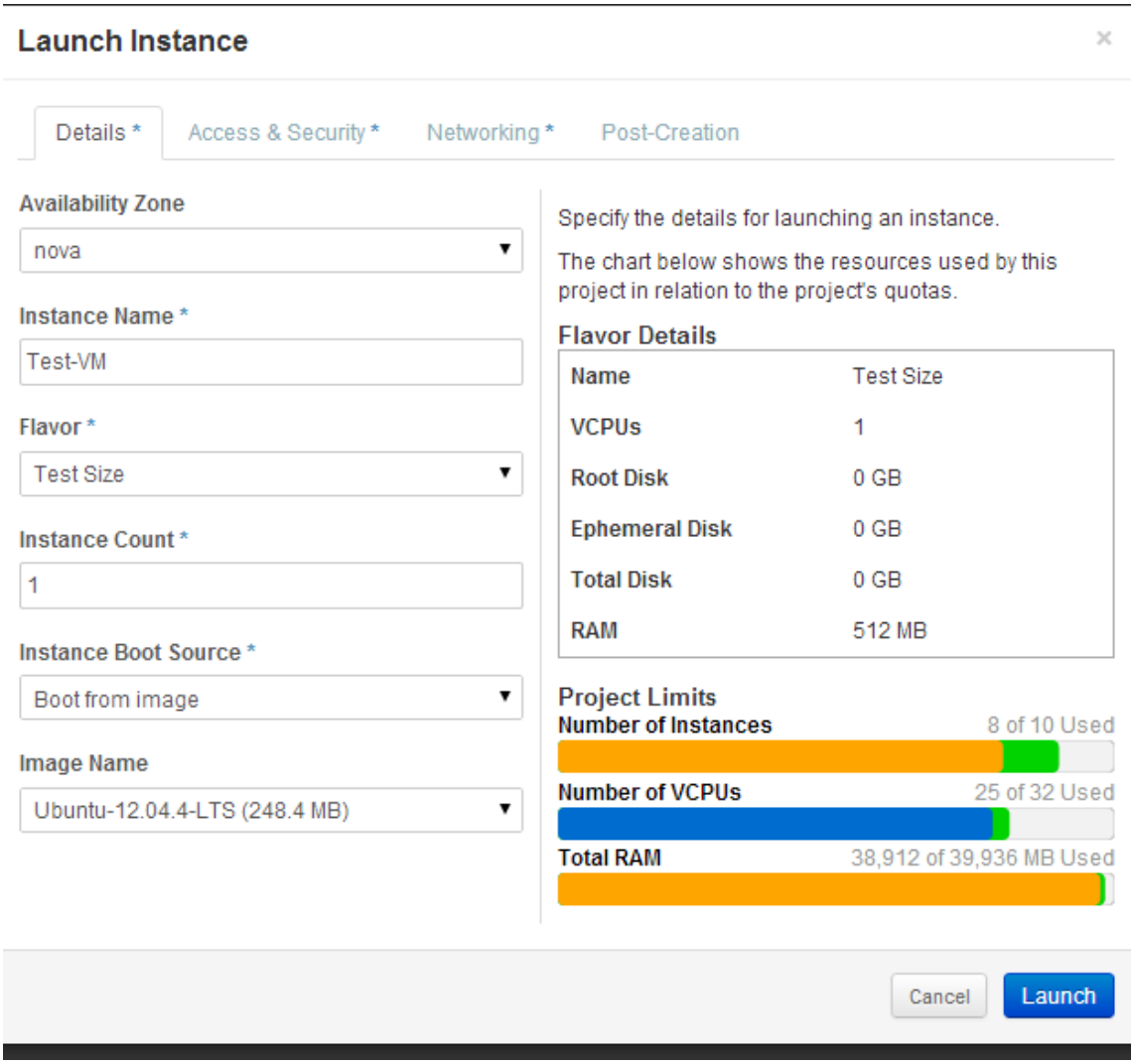


Project Name	VCPUs	Disk	RAM	VCPU Hours	Disk GB Hours
Integration-Environment	28	420	56GB	1277.40	76634.59
FI-Space WP200	40	765	65GB	9596.16	349897.03
admin	7	140	11GB	1870.87	65480.42
FI-Space WP300	21	395	30GB	2948.25	173346.26

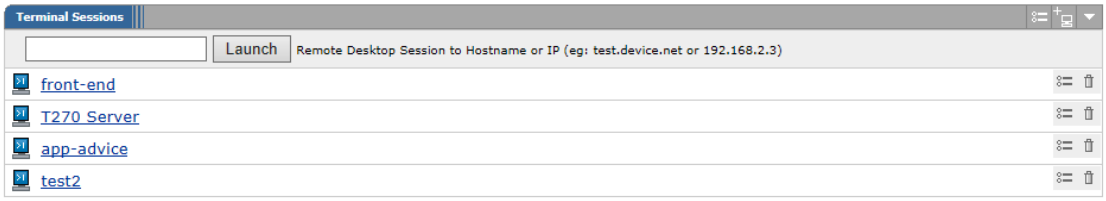
Currently FIspace Cloud Platform has 3 projects

- FIspace WP200: Current Software Development Project. Currently there are 21 Virtual Machines. Primary Integration Environment has been setup on this project.
- FIspace WP300: Experimental Environment Project. Currently there are 7 Virtual Machines
- Integration Environment: Integration Environment Project. Currently there are 7 Virtual Machines

Each project, members can be assign to create virtual machines and can be managed form secure access page. Most of the configurations has been predefined like ip subnet instance size, security groups and images of the operating systems and so on.



Finally, terminal session to the servers can be manually configured by the developer on the Secure Access Portal. For example, if a Linux virtual machine is created, ssh terminal service can be defined with given parameters.



2.3 Network & Security Infrastructure

Internal and real IP addresses are defined as below. Private Network has been used for the internal communication of the software's and virtual machines. Floating IP addresses has been used for internet connections to the firewall. Finally static real IP addresses have been used to reach to the servers directly form internet with the defined ports and services like http, https, ssh and so on.

Private Network	172.32.101.0 / 24
Public Network	37.131.251.0 / 24

SSL VPN technology provides secure access to the servers and modules. In case of need to reach servers & applications directly through internet, real IP addresses will be used to the servers from public network pool. Otherwise, private ip address will be used for the modules & servers.

In Figure 2, Network & Security infrastructure are shown.

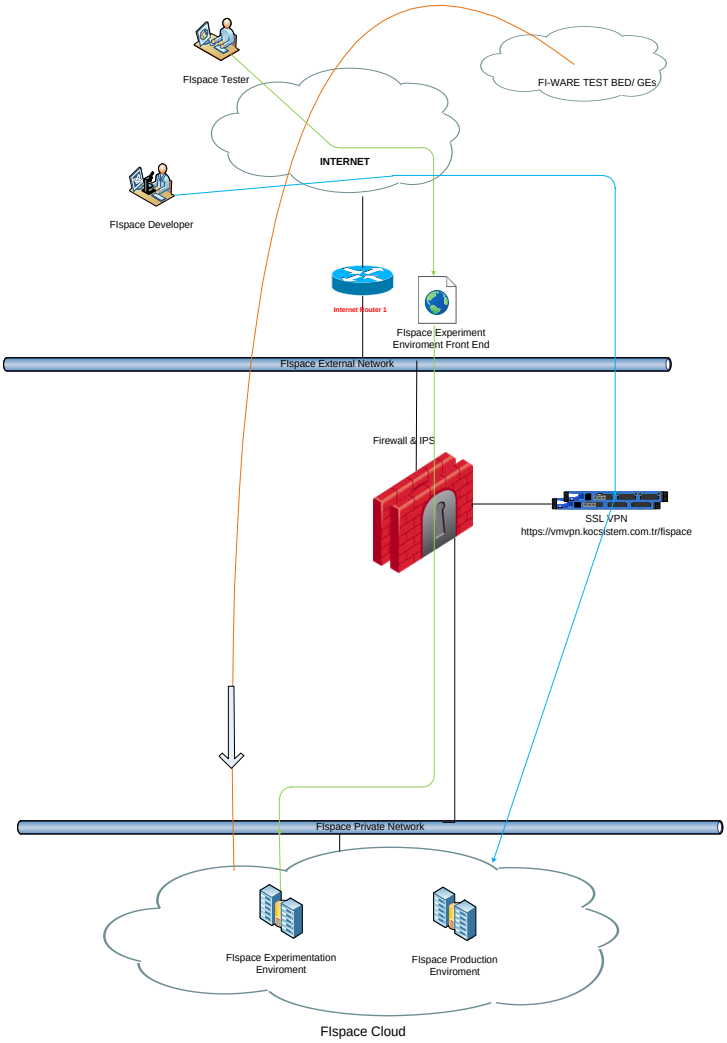


Figure 2: Network & Security infrastructure

Firewall and IPS will provide the secure infrastructure as well as access control to the systems. SSL VPN will provide to the secure access to the systems with user and role based. SSL VPN portal will be capable of to provide web bases access to the systems. In case of need of using IPsec vpn, it will be provided with a Java plugin to the client environment to provide TCP/UDP connections to the servers.

For secure access, SSL VPN will be used with address of https://vmvpn.kocsistem.com.tr/FIspace

For each project team, groups will be defined and for each team member user roles will be defined. Access policies will be defined based on user roles and groups.

Detailed information about FIspace Modules and planned to be used FI-WARE GEs in FIspace infrastructure needs to be collected by WP300 team for planning the hosting infrastructure and creating the FIspace instance with proper integration of modules and GEs. FIspace Modules and FI-WARE GEs inventory list is created by WP300 team in order to collect information including necessary hardware specs and operating environment for each FIspace modules and FI-WARE GEs.Inventory list is filled by WP200 and WP400 task leads and maintained by KocSistem.

FI-Space Modules and Applications inventory list contains the following items:

- Module or Application Name
- Operating System
- Network
- Considered as to be used GE and GE implementation
- Release/Version of the GE
- Tested / Contact person
- Important Links of GEs

- Applications / Platform
- Remote Access
- Internet Connection
- Resource Availability
- Acceptance Test of GE for the module
- Problems / Success with GEs

FI-WARE GEs inventory list with its items can be found in section “2.4 FI-WARE GEs Installations & Integrations”.

2.3.1 Secure Access Connection to the Infrastructure

Connection to the FIspace infrastructure based on Secure Access / SSL VPN technology Access and GUI Settings are explained as below;

FIspace Project member list contains the user information including work package and task information that drives to access policies to the FIspace infrastructure. For example, developer and a tester from WP200 will have different access rights to the same application or servers from FIspace platform. User and developer information for the secure access will be collected with the following items:

- User Name / Family Nane
- User full email address
- User WP / Task
- User Modules / GEs / Applications to connect
- User Role
- Remote Access Applications
- Comments

2.4 Advanced Integration of FI-WARE GEs

FIspace cloud infrastructure has been set up to provide running environment for FIpsace applications and FI-WARE GEs . Some of the GEs has been installed on cloud infrastructure and some FIspace applications has been integrated with FI-WARE GEs that has been installed out of the FIspace cloud. Necessary applications, operating systems and platform information have been collected and setup. Integration and Installation of exploited GE process is explained below:

Installation of GEs

- Assumed that setup files /codes from FI-WARE has been provided
- Installation of GE with GE expert from WP200 or WP400

Integration of GEs

- Assumed that integration information has been provided from FI-WARE
- Integration will be setup with FI-WARE GE developers, FIspace GE expert and KOC GE experts

FI-WARE GEs inventory list contains following the items and has been used for the GEs deployment and integrations

- GE name
- GE’s Release
- Operating System
- Applications / Platform
- Network
- GE Sources
- Remote Service Access
- API Specification
- GE’s FI-WARE test bed information
- Resource Availability
- GE/Server Location

- Integration
- Related WP / Task
- WP / Task lead
- FI-WARE Links
- Comments

The GE inventory List available at the time of writing (with selected items) is shown in the Table 1 below (this list will be continuously updated during the course of the project).

Table 1: GE inventory List

GE Name	Hosting Environment	Applications Platform	FIspace Integration
Marketplace	NKUA	java 1.6	Connected with Marketplace Operations Service(MOS)
IDM GE	FI-WARE	N/A	Integrated with LPA
Access Control GE	FI-WARE	JDK 6 and 7, Glassfish Server 3.1.2 or later, OpenDJ 2.5-Xpress1 or later	Integrated with IDM GE and LPA
Repository GE	NKUA	MongoDB 2.x - mandatory Java 1.6.x - mandatory Application Server, Apache Tomcat 6.x - mandatory Repository Software - mandatory Mongo Shell - optional	Connected with Marketplace Operations Service(MOS)
Store - WStore GE	FIspace Cloud	A Web Server (i.e Apache) MongoDB Python 2.5, 2.6 or 2.7. Python 3 and other versions are not supported. Django nonrel 1.3 or 1.4 djangotoolbox django_mongodb_engine lxml rdflib 3.2.0+ rdflib-jsonld Pymongo Pylucene paypalpy django-crontab wkpdf2html	Connected with Store component(T230), Marketplace GE,Repository GE
Wirecloud Application Mashup GE	FIspace Cloud	Python 2.7 pip 1.4.1 Apache 2.x MySQL 5.x	Integrated with Store and FIspace Front End

3 Support

First level support of Hosting environment, GE integrations and deployment will be done by KocSistem experts. Second and third level support responsible will be GE owners from FI-WARE via escalation method from FI-WARE Fusion Forge support and ticketing portal. Same holds for FIspace modules and Apps, the support for which is delegated to the respected product owners of the modules and Apps.

Wp320_support@kocsistem.com.tr mail address bas been used to open a ticket directly to responsible engineer in the organization and/or his/her backup to make immediate response to support request. IBM RTC, the developer tool of choice in the project, will be used to issue tickets

SLA of support has been shown on table:

Table 2: SLA of support

SLA	Via	Level
5x8 and/or 7x12 depend of Task Leader's requirements and Project Management Board approval.	Mail / Phone / Skype	First Level -KocSistem

4 Conclusion and Outlook

As D300.4 is concerned with providing an OpenStack based hosting environment and FI-WARE GE integration, this report describes the second version of the hosting Infrastructure, including cloud and network architecture. This infrastructure is designed to execute the software developed in WP200, the use case trials defined in WP400 and Experimental Environment from WP300. D300.4 has also presented integration planning of FI-WARE GEs to the software developed in WP200. The GEs integration mainly depends on the release of necessary GEs of FI-WARE planned to be used for the FIspace. In D300.4 Necessary GEs information has been collected. Each WP200 partner will be responsible for the availability and validation of the FIspace platform for their GE integration hence it is expected to be tested before the integration to the FIspace test environment. Successful GEs will be integrated with GEs owner and KocSistem WP300 allocated resources to the experimental environment.

The Cloud architecture is based on OpenStack architecture used by FI-WARE where OpenStack development has been supported by FIspace ICT project partners. Each workpackage has different domain on the Infrastructure. Admin of the projects can create members to manage Virtual Machines. Upon on a request, any developer can be added to the projects to manage their virtual machines.

Planned Network and Security Infrastructure of the Cloud Architecture is extendable in case of need of reel / private IP addresses and/or increase of internet connection bandwidth.

Developers, testers and/or users from each work packages will connect to the Cloud Architecture securely with appropriate rights by using SSL/VPN technologies. Firewall and IPS technologies will provided by the security of FIspace Cloud Architecture.

First level Support will be handled by KocSistem experts related with Cloud Architecture and GEs. Second and third level support of the GEs will be escalated to FI-WARE developers by using FI-WARE Fusion Forge support and ticketing portal.

FIspace

Business Collaboration