



Deliverable D300.2

Plan for Hosting and GE integration of Flspace

WP 300

Project Acronym & Number:	Flspace – 604 123
Project Title:	Flspace: 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:	Özgür Sönmezer, KOC; Bulent ERBAS, KOC; Philip Reimer, ATB
Contributors:	
Document Identifier:	Flspace-D300.2-Planning-Hosting-GE-Integration-V006.docx
Date:	30-10-2013
Revision:	006
Project website address:	http://www.Flspace.eu

The Flspace Project

As a use case project in Phase 2 of the FI PPP, Flspace 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. Flspace will focus on exploiting, incorporating and validating the Generic Enablers provided by the FI PPP FI-Ware project 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 work in the future. These 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.

The project will lay the foundation for realizing the vision and prepare for large-scale expansion, complying with the objectives and expected results of the Phase 2 use case projects. To achieve these outcomes the project will focus on the following four primary work areas, for which the main concepts and approach are outlined below:

1. **Implement the Flspace as an open and extensible Software-as-a-Service solution** along with an **initial set of cross-domain applications** for future B2B collaboration, **utilizing the Generic Enablers** provided by the FI-Ware
2. **Establish Experimentation Sites across Europe** where **pilot applications are tested in early trials** from the **Agri-Food and the Transport and Logistics** domains
3. **Provide a working Experimentation Environment** for conducting **early and large-scale trials** for Future Internet enabled B2B collaboration in several domains, and

Prepare for industrial uptake and innovation enablement by pro-active engagement of stakeholders and associations from relevant industry sectors and the IT industry.

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.Flspace.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)	

Change History

Version	Notes	Date
001	Initial Version (Özgür Sönmezer, KOC)	14-05-2013
003	Review (Bulent ERBAS, KOC)	07-07-2013
004	Review (Philip Reimer, ATB)	19-07-2013
005	Final version (Bulent ERBAS, KOC)	30-10-2013
006	Final document formatting of final version	30-10-2013

Document Summary

This document provides the Design of Hosting Infrastructure of FIspace- WP320 project to supply cloud platform in order to run the software developed WP200 (FIspace) and the use case trials defined in WP400. Hosting Infrastructure will be aligned to FI-WARE infrastructure to migrate modules in phase 3 and will also support to hosting and integration of necessary FI-WARE Generic Enablers.

Abbreviations

App	Software Application	i.e.	id est = that is to say
D	Deliverable	IP	Intellectual Property
DoW	Description of Work	IPR	Intellectual Property Rights
EC	European Commission	M	Month
e.g.	Exempli gratia = for example	RTD	Research and Technological Development
EU	European Union	SME	Small and Medium Sized Enterprise
FIA	Future Internet Assembly	ST	Sub-Task
FI PPP	Future Internet Public Private Partnership	T	Task
FP7	Framework Programme 7	WP	Work Package
GA	Grant Agreement		
ICT	Information and Communication Technology		

Table of Contents

1 Planning for Hosting environment and GE integration 6

2 Hosting Infrastructure 7

 2.1 Cloud Infrastructure 7

 2.2 Cloud Capacity 9

 2.3 Network & Security Infrastructure 9

 2.3.1 Secure Access Connection to the Infrastructure 11

 2.4 FI-WARE GEs Installations & Integrations 14

3 Support 16

List of Figures

Figure 1: FIspace Infrastructure – Hardware 7

Figure 2: FIspace Infrastructure – Software 8

Figure 3: Network & Security infrastructure. 10

1 Planning for Hosting environment and GE integration

This document provides the Design of Hosting Infrastructure of Flspace- WP320 project to supply cloud platform in order to run the software developed WP200 (Flspace) and the use case trials defined in WP400. Hosting Infrastructure will be aligned to FI-WARE infrastructure to migrate modules in phase 3 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 Hosting Infrastructure

KoçSistem will provide cloud hosting infrastructure for the development of FIspace. IBM Pureflex will be used as hardware with the following specs

Open Stack will be used for IaaS. Necessary operating systems and applications will be installed by KoçSistem.

2.1 Cloud Infrastructure

FIspace Infrastructure, Hardware:

- 8 Blade Server on IBM PureFlex Blade Chassis are used as Open Stack Processor and Memory hardware. All of them have 300 GB Raid 1 Hard Disks for Operating System (OS) installation.
 - 8 Node IBM Flex System x240
 - 6 IBM Flex System Enterprise Chassis 2500W Power Module.
 - 10 IBM Flex System Enterprise Chassis 80mm Fan Module.
- Two 10G Blade Switches are used to connect KoçSistem Network Infrastructure. Both switches are connected to Nexus 5000 with 2+2 cables for redundancy.
 - 2 IBM Flex System Fabric EN4093 10Gb Scalable Switch.
- Two SAN Switches are used for FC Storage connection. 2 Fiber cables are connected to KoçSistem SAN Distribution Switches for each server for redundancy.
 - 2 IBM Flex System FC3171 8Gb SAN Pass-thru.
- NetApp V6280, NetApp 6220, EMC VNX 7500, IBM XIV Storage Systems will be used for Virtual Machine Data stores.

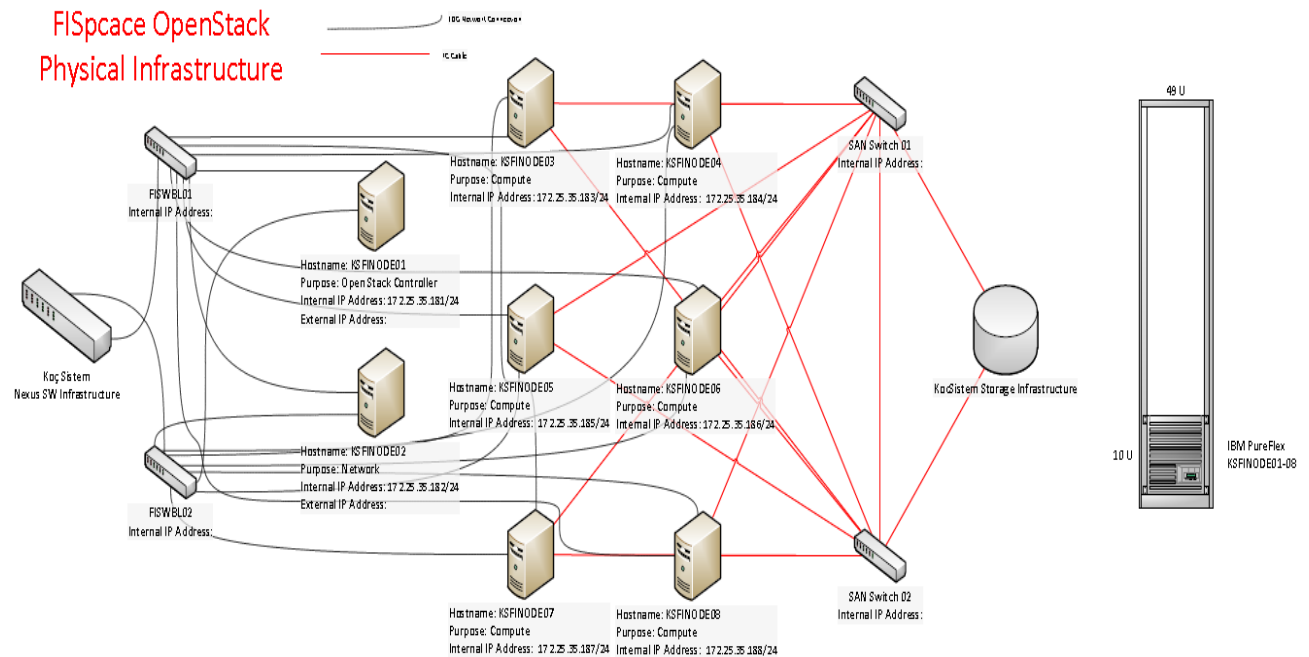


Figure 1: FIspace Infrastructure – Hardware

FIspace Infrastructure, Software:

- Ubuntu 12.04 LTS will be used for main OS.
- Controller Node; will be used for Open Stack Dashboard and Controller Node including MySQL database. This node is planned to be separated in the future as, MySQL Database, Open Stack Dashboard and Open Stack Controller Node.
 - MySQL Database.

- RabbitMQ.
- Quantum-Server.
- Nova-API.
- Nova-Scheduler.
- Keystone Identity Management.
- Network Node; will be used for Virtual Machine Network connection distribution for Open Stack. This node is planned to separate to multiple nodes in the future.
 - Quantum-Metadata-Agent.
 - Quantum-DHCP-Agent.
 - Quantum-I3-Agent.
 - Quantum-Plugin-Agent.
- Compute Nodes; will be used for Processor and Memory source for Open Stack. Compute Nodes can be removed or added in the future as needed. If resources are wasted, Compute nodes will be shut down or removed; if more resources are needed, more physical servers can be added as Compute Node to the Open Stack Cloud.
 - Nova-Compute.
 - Quantum-Plugin-Agent.
- There will be 3 main network VLANs on the Open Stack Environment:
 - Physical Maintenance Network. This network will be used to manage Server and Chassis console and control. This network is separated from other networks for security.
 - Open Stack Management and API Network. This network will be used to for Open Stack Controller-Compute-Network Node connection. This network is separated from other networks for security.
 - External Networks (Virtual Machine Data Network). These networks will be generated on KoçSistem Infrastructure and in Open Stack. They will be used by Client's Virtual Machines. This network can be connected to Internet if client wants to. Additionally, Open Stack Dashboard will be in one of these networks.

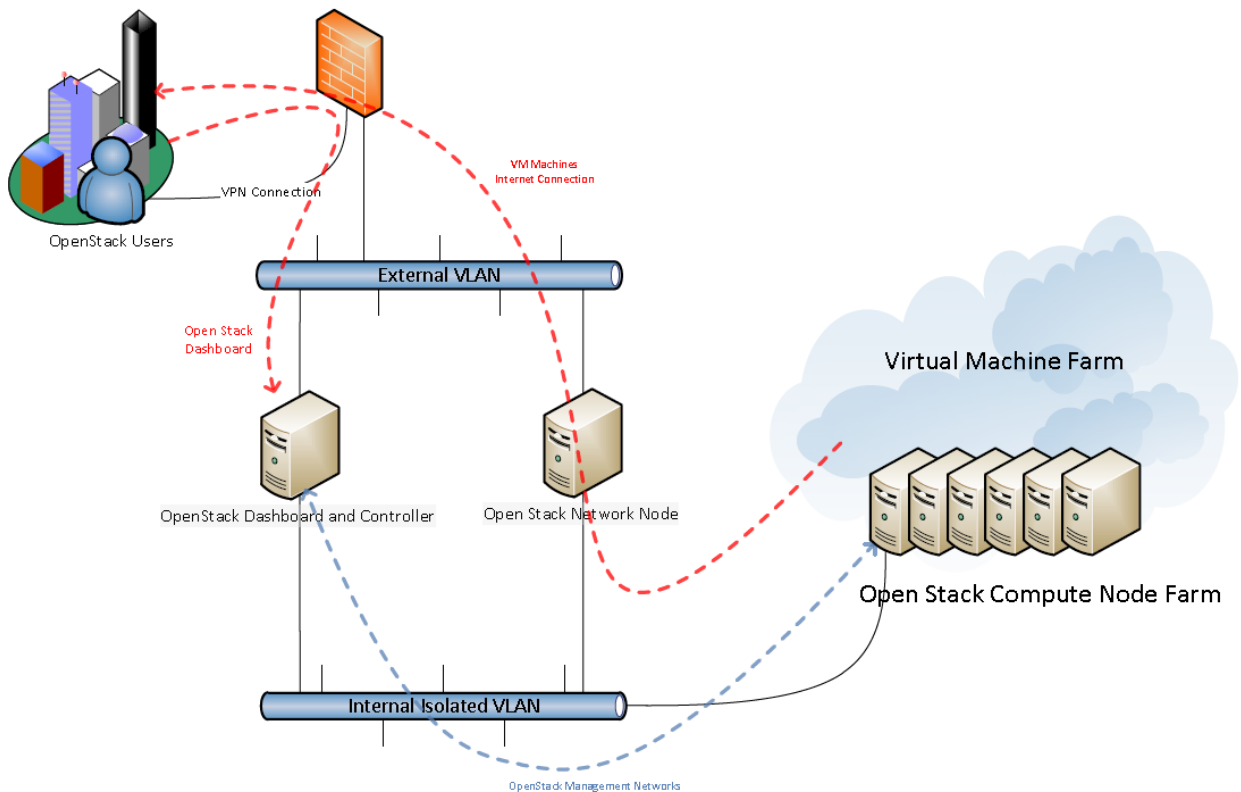


Figure 2: FIspace Infrastructure – Software

2.2 Cloud Capacity

IBM Pure Flex has 8 compute nodes. Specifications of each node as following;

- 16 cores total 8 cores of each socket, total 2 sockets Intel E5-2670
- 80 Up to VM per socket
- 128 Gbyte RAM, expandable up to 768 GB of each Node.

Each server has a capacity of 160 virtual machines up on required RAM, each node RAM capacity extendible up to 768 GB supported by IBM. 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.

2.3 Network & Security Infrastructure

KoçSistem will provide network and security infrastructure of FIspace project

Internal and real ip addresses are defined as below. These addresses can be extended in case of need.

Private Network	172.32.101 / 24
Public Network	37.131.251.1 / 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.

Vlan segmentations are planned for the servers segment like DMZ, database, test and prod environments. Traffic between the vlan segments will be inspected by firewall and IPS

FIspace development hosting infrastructure will use Security infrastructure inventory as below

- 2 redundant (Active – Standby) failover Virtual Firewall appliance with IPS features
- 2 redundant SSL VPN (Active Standby) failover appliance
- Backbone & Internet Switch with vlan segmentation for the project

In Figure 3, Network & Security infrastructure are shown.

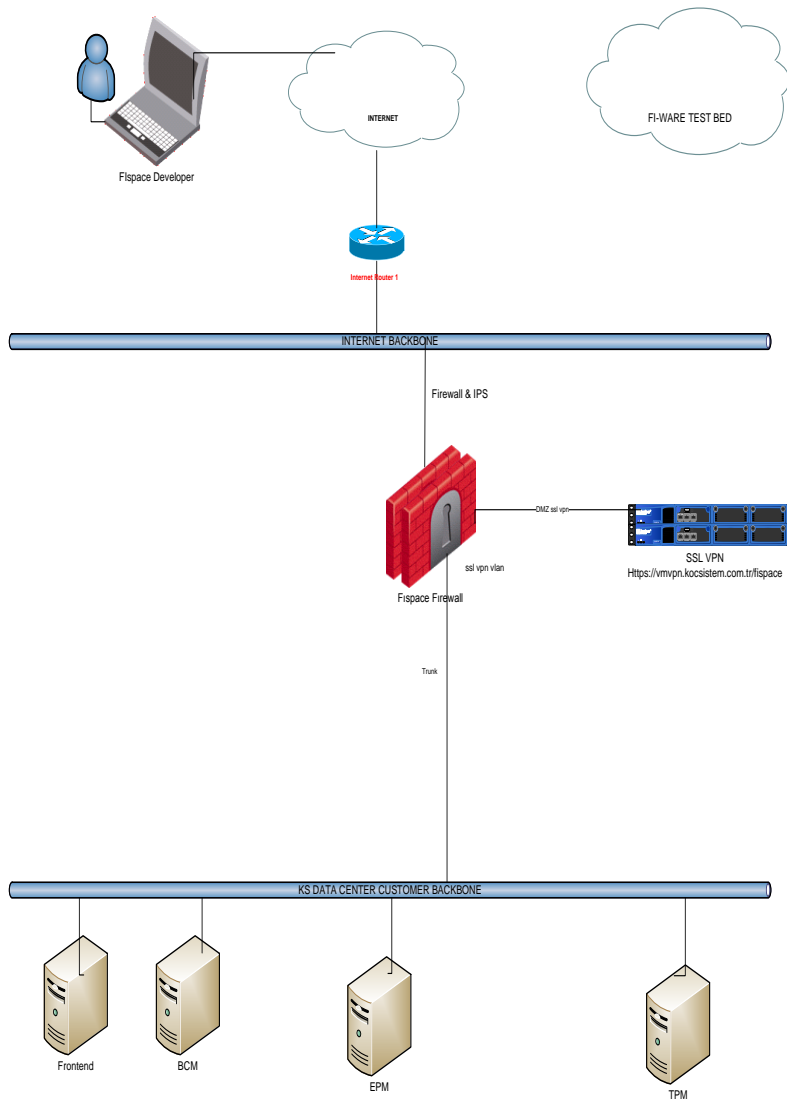


Figure 3: Network & Security infrastructure.

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/fispac>

For each project team members, users will be defined for secure access. Access and rights of the user will be defined according to the user needs.

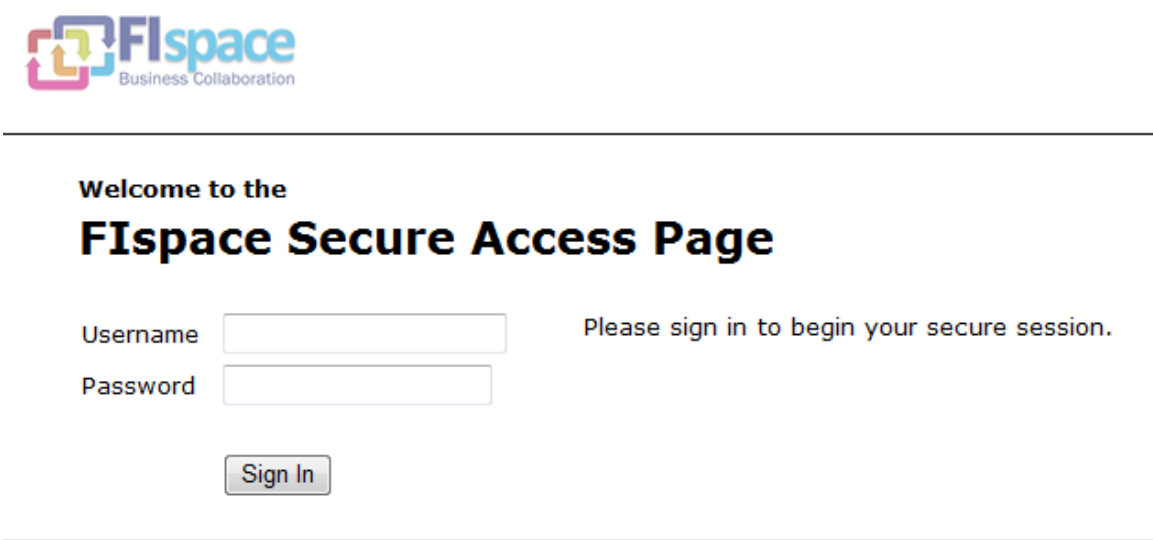
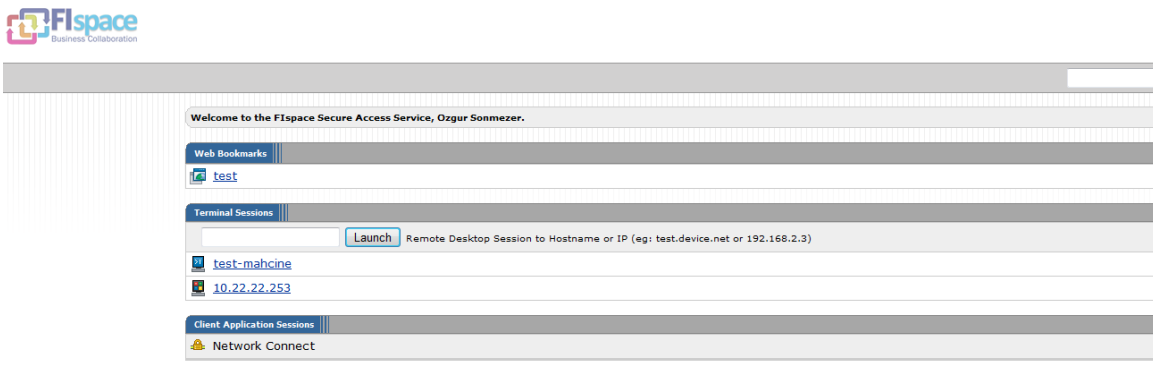
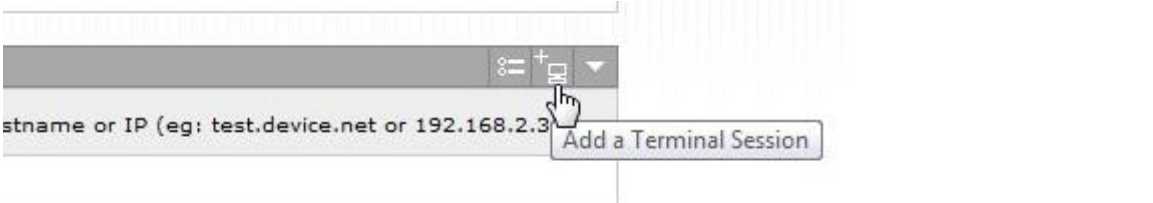
Module Inventory list contains the following Items;

- Module Name
- Operating System
- Network
- Need GE + Release
- 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

2.3.1 Secure Access Connection to the Infrastructure

Connection to the Virtual Machines will use Secure Access / SSL VPN technology
 Access and GUI Settings explained as below;

	<p>Login FIspace Secure Access page.</p> <p>After the first login, it will require a password change. Then access will be granted. There is a strict password policy...</p>
	<p>After Successful Login, it will be possible to make terminal session like remote desktop / ssh / Telnet. Basically on the terminal session window, windows remote desktop can be launched with the given ip address.</p>
	<p>Click "Add a Terminal Session" for adding ssh terminal session.</p>

Add Terminal Services Session

Session Type: SSH Secure Shell
Bookmark Name: Windows Terminal Services
Description: Citrix

SSH Secure Shell
Telnet
SSH Secure Shell

Settings

* Host: [] Name or IP address of the host
* Port: 22
* Screen Size: 80x25
* Screen Buffer: 100
* Font Size: Fixed Size of 12 pixels
 Resize to fit window

Session

Authentication:
Username: [] Username or <USER> for IVE session username

Add Terminal Services Session?

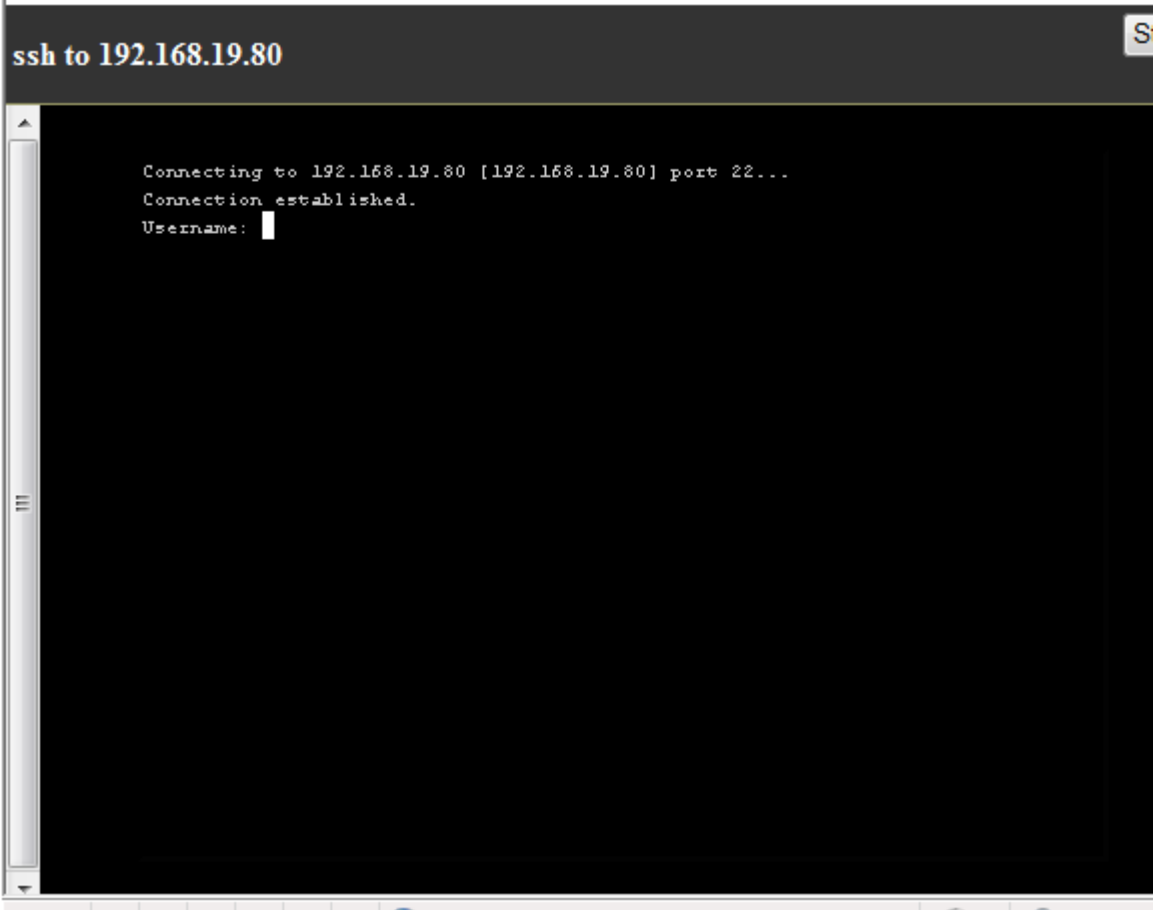



Choose “SSH Secure Shell” and select necessary settings for the ssh console

Terminal Sessions

[] **Launch** Remote Desktop Session to

<ssh://192.168.19.80:22>

SSH console can be added to the portal.
Console can be opened by clicking the link

	<p>Console will be opened on the browser</p>
	<p>Web pages can be added to web bookmarks.</p>
	<p>Alternatively, Web pages can be opened by "browse"</p>
	<p>IF IPsec vpn is necessary, click "network connect" Then, you can use any application like winscp, ssh terminal, putty, http and allowed other tcp/ udp applications needed.</p>

Developers list contains the user information that will use secure access to the Hosting infrastructure as below;

- Developer Name / Surname
- Developer mail address
- Developer WP / Task
- Developers Modules / GEs / Applications to connect
- Remote Access Applications
- Comments

2.4 FI-WARE GEs Installations & Integrations

Necessary operating systems and applications will be clarified by developers and KoçSistem will be responsible to supply that. Integration of the GEs which are used by FIspace modules will be handled by experts from responsible of FIspace modules. GEs, that are not provided by FIspace modules, to be directly used by baseline Apps will be integrated by baseline App owners. KoçSistem will install the necessary operating systems and platforms for the GEs that requested. FI-WARE GEs should be tested by GE owners before deployment process of the FIspace cloud environment. Integration and Installation of exploited GE process has been explained as 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 will be 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

GE inventory List with selected items shown in the table below;

GE name	Operating System	Applications Platform	Related WP/Task responsible	Estimated Time for installation and integration
Marketplace	Ubuntu 11.04	java 1.6	WP450 / Marketplace Operations Baseline App	2 weeks
Security Monitoring	Debian Based	N/A	WP200 / T270	2 weeks
IDM GE	N/A	N/A	WP200 / T270	2 weeks

GE name	Operating System	Applications Platform	Related WP/Task responsible	Estimated Time for installation and integration
Privacy Enabler	N/A	N/A	WP200 / T270	2 weeks
CEP	Linux	Java SE 6,Apache Tomcat 7	WP200/T240	2 weeks
Publish/Subscribe Context Broker - SAMSON Broker	CentOS 6.3	N/A	N/A	2 weeks
Gateway Data Handling	Windows(for the servlet release, others are outdated).	N/A	WP200/250	2 weeks
IoT Broker	N/A	N/A	WP200/250	2 weeks
Data Handling GE	N/A	MySQL 5.1.43,Apache HTTP web server, PHP,MySQL,phpMyAdmin	WP200/T270	2 weeks
Content Based Security	N/A	Tomcat 7,Maven	WP200/T270	2 weeks
Access Control GE	Linux i686	JDK 6 and 7, Glassfish Server 3.1.2 or later, OpenDJ 2.5-Xpress1 or later	WP200/T270	2 weeks
Repository GE	Ubuntu 11.04, 11.11, 12.04 LTS Microsoft Windows 7	MongoDB 2.x - mandatory Java 1.6.x - mandatory Application Server, Apache Tomcat 6.x - mandatory Repository Software - mandatory Mongo Shell - optional	WP450 / Marketplace Operations Baseline App	2 weeks
Object Storage GE	Ubuntu Server 10.04 LTS	OpenStack with Swift ,CDMI interface	WP450 / Product Information Service Baseline App	2 weeks
WireCloud GE	Ubuntu 12.04 LTS	Python 2.7 MySQL 5.x	WP200/T220	3 weeks

3 Support

First level support of Hosting environment, GE integrations and deployment will be done by KoçSistem experts. Second and third level support responsible will be GE owners from FI-WARE via escalation method.

Different mail address groups are planned to open a ticket directly to responsible engineer in the organization and/or his/her backup to make immediate response to support request.

SLA of support has been shown on table

SLA	Via	Level
5x8 and/or 7x12 availability best effort basis as standard. Service level upgrade requests will be fulfilled based on depends of Task Leader's requirements upon Project Management Board approval.	Mail / Phone	First Level -KoçSistem

