**D7.2: XIFI Training Strategy and Material (v1)**

Revision: v.1.0

<table>
<thead>
<tr>
<th>Work package</th>
<th>WP 7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task</td>
<td>Task 7.1, Task 7.2</td>
</tr>
<tr>
<td>Due date</td>
<td>30/04/2014</td>
</tr>
<tr>
<td>Submission date</td>
<td>07/05/2014</td>
</tr>
<tr>
<td>Deliverable lead</td>
<td>Eamonn Power (WIT)</td>
</tr>
<tr>
<td>Authors</td>
<td>Eamonn Power (WIT), Mark Roddy (WIT), Jacques Magen (InterInnov), Giulia Pastor (InterInnov), Laura Pucci (ENG), Davide Dalle Carbonare (ENG), Federico Facca (CREATE-NET), Alessandro Martellone (CREATE-NET), Panos Trakadas (SYNELIXIS), Andreas Papadakis (SYNELIXIS)</td>
</tr>
<tr>
<td>Reviewers</td>
<td>Uwe Herzog (Eurescom)</td>
</tr>
</tbody>
</table>

**Abstract**

This deliverable defines the first version of the training strategy and materials production processes. It includes details of the planning and organisation of training sessions. There are details on the use of tools to support the community in the production of training materials. Finally, it also includes a first version of the infrastructure owners training manual.

**Keywords**

Training, Community, Manual
Document Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Description of change</th>
<th>List of contributor(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>V0.1</td>
<td>19.12.2013</td>
<td>First Outline and draft material</td>
<td>Eamonn Power</td>
</tr>
<tr>
<td>V0.2</td>
<td>13.01.2014</td>
<td>Module Template revision</td>
<td>Eamonn Power</td>
</tr>
<tr>
<td>V0.3</td>
<td>22.01.2014</td>
<td>Training Session Information</td>
<td>Giulia Pastor, Jacques Magen</td>
</tr>
<tr>
<td>V0.4</td>
<td>03.03.2014</td>
<td>Stakeholder Updates</td>
<td>Eamonn Power, Giulia Pastor</td>
</tr>
<tr>
<td>V0.5</td>
<td>17.03.2014</td>
<td>Webinar Updates</td>
<td>Laura Pucci</td>
</tr>
<tr>
<td>V0.6</td>
<td>24.03.2014</td>
<td>Requirements</td>
<td>Eamonn Power</td>
</tr>
<tr>
<td>V0.7</td>
<td>03.04.2014</td>
<td>Material Production Updates</td>
<td>Mark Roddy, Eamonn Power</td>
</tr>
<tr>
<td>V0.8</td>
<td>08.04.2014</td>
<td>Training Sessions Revision</td>
<td>Giulia Pastor</td>
</tr>
<tr>
<td>V0.9</td>
<td>14.04.2014</td>
<td>Stakeholder Revision</td>
<td>Eamonn Power</td>
</tr>
<tr>
<td>V0.9.1</td>
<td>26.04.2014</td>
<td>Process Diagram Updates</td>
<td>Eamonn Power</td>
</tr>
<tr>
<td>V1.0</td>
<td>06.05.2014</td>
<td>Training Manual Annex, Completed Sections</td>
<td>Eamonn Power</td>
</tr>
</tbody>
</table>

Disclaimer

This report contains material which is the copyright of certain XIFI Consortium Parties and may only be reproduced or copied with permission in accordance with the XIFI consortium agreement.

All XIFI Consortium Parties have agreed to publication of this report, the content of which is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Unported License¹.

Neither the XIFI Consortium Parties nor the European Union warrant that the information contained in the report is capable of use, or that use of the information is free from risk, and accept no liability for loss or damage suffered by any person using the information.

Copyright notice

© 2013 - 2015 XIFI Consortium Parties

---

¹ http://creativecommons.org/licenses/by-nc-nd/3.0/deed.en_US
EXECUTIVE SUMMARY

XIFI Training Strategy and Material (v1): This deliverable documents the strategy for XIFI training and the suite of training material that will be produced for the different levels of training i.e. Basic, Intermediate and Advanced, and describes the processes that will be followed with respect to training and knowledge transfer. The Deliverable will also describe the “XIFI Recognition & Reward Programme”. A Training Manual is issued as an appendix to the deliverable. This document is aimed at anyone who wants to contribute to the training community being built by XIFI. The manual is aimed at infrastructure owners and operators.
# TABLE OF CONTENTS

**EXECUTIVE SUMMARY** ....................................................................................................................... 3  
**TABLE OF CONTENTS** ......................................................................................................................... 4  
**LIST OF FIGURES** ................................................................................................................................. 7  
**LIST OF TABLES** ................................................................................................................................. 8  
**ABBREVIATIONS** ................................................................................................................................. 9  

1. **INTRODUCTION** ................................................................................................................................. 10  
2. **CORE CONCEPTS** ............................................................................................................................ 11  
2.1 Communication Plan .......................................................................................................................... 11  
3. **STAKEHOLDERS** .............................................................................................................................. 12  
3.1 Source Stakeholders ............................................................................................................................ 12  
3.2 Target Stakeholders ............................................................................................................................. 12  
3.3 Trainer Stakeholders ........................................................................................................................... 13  
4. **REQUIREMENTS FOR TRAINING PROGRAMME** ........................................................................... 14  
5. **ORGANISATION OF THE TRAINING SESSIONS** ......................................................................... 17  
5.1 Workplan ............................................................................................................................................. 17  
5.2 Beta Training Sessions ....................................................................................................................... 17  
5.3 Specific Training and awareness sessions for Public Authorities .................................................... 18  
5.3.1 Training Sessions ............................................................................................................................ 18  
5.3.2 Webinars ....................................................................................................................................... 19  
5.4 Organisation of training sessions ....................................................................................................... 20  
5.5 Organisation of the webinars ............................................................................................................. 22  
5.6 Organisation of training sessions for Public Authorities ................................................................. 24  
6. **CONTENT OF THE SESSIONS** ......................................................................................................... 25  
6.1 Internal training courses for the teachers ........................................................................................... 25  
6.2 Basic training session .......................................................................................................................... 25  
6.2.1 For all stakeholders ......................................................................................................................... 25  
6.2.2 For FI-Developers ........................................................................................................................... 25  
6.2.3 For Infrastructure Owners ............................................................................................................ 25  
6.3 Intermediate training session ............................................................................................................. 26  
6.3.1 For Infrastructure Owners ............................................................................................................ 26  
6.4 Advanced training session .................................................................................................................. 26  
6.5 Other training session ......................................................................................................................... 26  
7. **TRAINING MATERIAL DEVELOPMENT** ....................................................................................... 27  
7.1 Community Portal .............................................................................................................................. 32
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A5.1.1</td>
<td>Installation Manual</td>
<td>58</td>
</tr>
<tr>
<td>A5.1.2</td>
<td>User Manual</td>
<td>59</td>
</tr>
<tr>
<td>A5.2</td>
<td>DCA</td>
<td>72</td>
</tr>
<tr>
<td>A5.2.1</td>
<td>Installation Manual</td>
<td>73</td>
</tr>
<tr>
<td>A5.2.2</td>
<td>User Manual</td>
<td>74</td>
</tr>
<tr>
<td>REFERENCES</td>
<td></td>
<td>84</td>
</tr>
</tbody>
</table>
LIST OF FIGURES

Figure 1 - Planned Training Sessions........................................................................................................19
Figure 2 - Planned Webinars..........................................................................................................................19
Figure 3 - XIFI Website Linking to the Training Portal ................................................................................22
Figure 4 - Schedule of Deliverable Release ..................................................................................................28
Figure 5 - Graph of initial training content topics from analysis ....................................................................31
Figure 6 - Template title slide .........................................................................................................................33
Figure 7 - Template content slide ...................................................................................................................34
Figure 8 - Video production processes ...........................................................................................................35
Figure 9 - Course creation process for manuals ...............................................................................................36
Figure 10 - OpenStack Networking Architecture ............................................................................................45
Figure 11 - The Multi Domain VPN ................................................................................................................46
Figure 12 - Basic Physical Deployment ............................................................................................................51
Figure 13 - High availability physical deployment ..........................................................................................54
Figure 14 - Service per node in the basic architecture deployment model .........................................................57
Figure 15 - Service per node in HA architecture deployment model .................................................................58
Figure 16 - The ITBox homepage .....................................................................................................................60
Figure 17 - Creation of a new environment .......................................................................................................60
Figure 18 - DCRM install options ....................................................................................................................61
Figure 19 - Final creation step ..........................................................................................................................61
Figure 20 - The page of the created environment ............................................................................................62
Figure 21 - Environment definition ................................................................................................................63
Figure 22 - List of available servers ................................................................................................................64
Figure 23 - Network interface configurations ..................................................................................................65
Figure 24 - Hard disk configuration ...............................................................................................................65
Figure 25 - Detailed information about the selected server .............................................................................66
Figure 26 - Infrastructure network settings ....................................................................................................67
Figure 27 - L2/L3 Neutron Configuration .........................................................................................................68
Figure 28 - Infrastructure settings (monitoring, admin account, common) .......................................................69
Figure 29 - Infrastructure settings (scheduler drivers, syslog, storage) ...........................................................70
Figure 30 - Health check result .......................................................................................................................71
Figure 31 - Installation in progress ..................................................................................................................72
Figure 32: The architecture of the DCA persistency layer ................................................................................81
# LIST OF TABLES

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Processes and Tools</td>
<td>11</td>
</tr>
<tr>
<td>2</td>
<td>Training Stakeholder Requirements</td>
<td>15</td>
</tr>
<tr>
<td>3</td>
<td>Beta Training Session</td>
<td>18</td>
</tr>
<tr>
<td>4</td>
<td>First Training Session for Public Authorities</td>
<td>18</td>
</tr>
<tr>
<td>5</td>
<td>First Training Session</td>
<td>18</td>
</tr>
<tr>
<td>6</td>
<td>Second Training Session</td>
<td>19</td>
</tr>
<tr>
<td>7</td>
<td>Third Training Session</td>
<td>19</td>
</tr>
<tr>
<td>8</td>
<td>Actions related to the first training session</td>
<td>21</td>
</tr>
<tr>
<td>9</td>
<td>Actions related to the second training session</td>
<td>21</td>
</tr>
<tr>
<td>10</td>
<td>Actions related to the third training session</td>
<td>21</td>
</tr>
<tr>
<td>11</td>
<td>First Training Session for Public Authorities</td>
<td>24</td>
</tr>
<tr>
<td>12</td>
<td>Training Content Sections from Deliverable Analysis</td>
<td>31</td>
</tr>
<tr>
<td>13</td>
<td>Public List of Software Components</td>
<td>32</td>
</tr>
<tr>
<td>14</td>
<td>Hardware Recommendation for basic physical deployment</td>
<td>52</td>
</tr>
<tr>
<td>15</td>
<td>Hardware recommendations for High Availability physical deployments</td>
<td>55</td>
</tr>
</tbody>
</table>
## ABBREVIATIONS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>API</td>
<td>Application Programmer Interface</td>
</tr>
<tr>
<td>ATOS</td>
<td>ATOS SPAIN SA</td>
</tr>
<tr>
<td>DT</td>
<td>DEUTSCHE TELEKOM AG</td>
</tr>
<tr>
<td>DoW</td>
<td>Description of Work</td>
</tr>
<tr>
<td>EC</td>
<td>European Commission</td>
</tr>
<tr>
<td>EIT ICT Labs</td>
<td>The European Institute for Innovation and Technology’s Information and Communication Technology Labs</td>
</tr>
<tr>
<td>FI</td>
<td>Future Internet</td>
</tr>
<tr>
<td>FI-Lab</td>
<td>Future Internet Lab</td>
</tr>
<tr>
<td>FI-Ops</td>
<td>Future Internet Operations Support tools</td>
</tr>
<tr>
<td>FI-PPP</td>
<td>Future Internet Public Private Partnership</td>
</tr>
<tr>
<td>FIA</td>
<td>Future Internet Assembly</td>
</tr>
<tr>
<td>FIF</td>
<td>Future Internet Forum</td>
</tr>
<tr>
<td>FIRE</td>
<td>Future Internet Research and Experimentation</td>
</tr>
<tr>
<td>GE</td>
<td>Generic Enabler</td>
</tr>
<tr>
<td>Generic Enabler</td>
<td>A specification of an API and core functionality expected behind the API</td>
</tr>
<tr>
<td>OSS</td>
<td>Open source software</td>
</tr>
<tr>
<td>RED.ES</td>
<td>ENTIDAD PUBLICA EMPRESARIAL RED.ES</td>
</tr>
<tr>
<td>SE</td>
<td>Specific Enabler</td>
</tr>
<tr>
<td>SME</td>
<td>Small to Medium Enterprise</td>
</tr>
<tr>
<td>TUB</td>
<td>TECHNISCHE UNIVERSITAT BERLIN</td>
</tr>
<tr>
<td>Telefonica</td>
<td>TELEFONICA INVESTIGACION Y DESARROLLO SA</td>
</tr>
<tr>
<td>UPM</td>
<td>UNIVERSIDAD POLITECNICA DE MADRID</td>
</tr>
<tr>
<td>WP</td>
<td>Work Package</td>
</tr>
<tr>
<td>XIFI Adapters</td>
<td>Software components in charge of supporting the integration of infrastructure into the XIFI framework and federation</td>
</tr>
<tr>
<td>XiPi</td>
<td>XiPi is an on-line catalogue of Future Internet infrastructures</td>
</tr>
</tbody>
</table>
1 INTRODUCTION

The main aim of the Training and Knowledge Transfer work package is to educate, inform and train the stakeholder groups in how to use and interact with the XIFI Federation effectively, whilst understanding the varying needs, interests and abilities of each stakeholder group.

Engagement and uptake from the different stakeholders is of utmost importance. The community approach being taken in the FI-PPP could be likened to an open-source community. The public access to repositories, the documentation published and the access to OSS reference implementations of Generic Enablers point now just to OSS but to open communities. Bangerth and Heister\(^1\) found that the top three reasons for success with open source computational libraries were:

- Quality and Utility
- Documentation
- Building a Community

Work Package 7 is responsible for Training and Knowledge Transfer. This includes documentation and the building of a community around it for training and knowledge transfer.
## 2  CORE CONCEPTS

When considering training and knowledge transfer, the following concepts are required to be understood:

**Federated Infrastructures:** The core of the federated infrastructure is community cloud for Future Internet technologies. "A community cloud serves a group of Cloud Consumers which have shared concerns such as mission objectives, security, privacy and compliance policy, rather than serving a single organisation as does a private cloud."\(^2\) The federated infrastructure leverages the capacity of the whole federation for individual applications - while the ownership remains either with organisations in the community, or with third parties.

**XIFI:** XIFI is a federation of resources offered to the FI-PPP developer community by FI infrastructures. FI-PPP developers themselves may contribute to the community cloud by offering additional hardware capacity (under their own control or open to other PPP participants) and their own services (the so called Specific Enablers).

**FI-Lab:** is the virtual marketplace where users can browse through, configure and access available infrastructure - all necessary for development and experimentation.

**FI-Ops:** a dedicated toolset, which eases the deployment, setup and operation of FI-Lab Instances.

**Stakeholders:** the different stakeholder groups targeted by the XIFI project as documented in the Stakeholder Glossary.

### 2.1  Communication Plan

The planned high-level process and supports for communication and cooperation was outlined as follows:

<table>
<thead>
<tr>
<th>Process</th>
<th>Support Tool</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workpackage Lifecycle Management</td>
<td>Agile-style – proposed a review of tasks on a 2-week basis with a call once a month with an increase in call frequency to every week near deliverable deadlines. Use of the Redmine Roadmap module (<a href="http://redmine.fi-xifi.eu/projects/xifi-wp7/roadmap">http://redmine.fi-xifi.eu/projects/xifi-wp7/roadmap</a>)</td>
</tr>
<tr>
<td>Task assignment and monitoring tool</td>
<td>XIFI Redmine – for task management, also a good integration point with technical WPs (<a href="http://redmine.fi-xifi.eu/projects/xifi">http://redmine.fi-xifi.eu/projects/xifi</a>)</td>
</tr>
<tr>
<td>Knowledge Capture - notice board, meeting notes and draft docs</td>
<td>XIFI Wiki – for knowledge capture and document drafting (<a href="http://wiki.fi-xifi.eu/Xifi:Wp7">http://wiki.fi-xifi.eu/Xifi:Wp7</a>)</td>
</tr>
<tr>
<td>Content creation and collaboration</td>
<td>XIFI Subversion server - storage of content being produced (source material, etc.) (<a href="https://xifisvn.res.eng.it/wp7">https://xifisvn.res.eng.it/wp7</a>)</td>
</tr>
<tr>
<td>Content publishing and archival</td>
<td>XIFI BSCW server – publishing/archive of completed deliverables, slides and training content (<a href="https://bscw.fi-xifi.eu/bscw/cgi/14046">https://bscw.fi-xifi.eu/bscw/cgi/14046</a>)</td>
</tr>
<tr>
<td>Group Discussion</td>
<td>WP7 Mailing List – group notifications and general discussion, we anticipate that many items will be discussed in Redmine</td>
</tr>
</tbody>
</table>

*Table 1 - Processes and Tools*
3 STAKEHOLDERS

The first step in the WP7 Stakeholders analysis was the identification of the stakeholders we want to train and inform.

In order to do this, we analysed the work carried out in the WP9 Task T9.2 “Promotion towards Stakeholders Groups”, in which we identified the relevant target communities with potential interest to the XIFI project (for more details, please see https://www.fi-xifi.eu/about-xifi/stakeholders.html), and we adapted it according to the WP7 needs.

Starting from this point, we defined two concepts of stakeholders:

- **Source stakeholders**
- **Target stakeholders**

The *source stakeholders* are the stakeholders who shall participate in the training sessions. The *target stakeholders* are the stakeholders we would like to see emerge as a result of training (i.e. what we want to achieve with the source stakeholders at the end of the session). For example, we organize a Training session for National Authorities (source stakeholders). Thanks to the XIFI training, these National Authorities will become Intermediaries (target stakeholders), which will mobilize the FI Experimenters in their countries to use XIFI Infrastructures and services for their experimentations. The aim of the training programme is to progress these source stakeholders into a number of target stakeholders.

Initially, the following *source and target stakeholders* are identified:

### 3.1 Source Stakeholders

The Source stakeholders are mainly the stakeholders identified in these categories:

- National Authorities (Smart Cities, Local, Regional, National, European and International Authorities);
- Intermediaries (FI-PPP Phase III)
- Developers (Phase III Developers, Content providers and app.developers, Industry, Web entrepreneurs)
- Infrastructures owners and operators (XiPi Infrastructures, FIRE Facilities, Use case platforms, EIT ICT Lab nodes)

### 3.2 Target Stakeholders

The Target stakeholders are mainly the stakeholders identified in these categories:

- Developer (Experimenters, FI-Ops User)
- Sponsor and/or investors (FI App Sponsor)
- Intermediaries (Others)
- Infrastructures owners and operators (XIFI additional nodes owners/operators; FI-Ops owners/operators; FI-Lab Instance Providers)
- Technology providers (GE- Developers and SE- Developers)
### 3.3 Trainer Stakeholders

In addition, as part of the requirements gathering process, a number of stakeholders specifically related to the creation of training content have been identified. These roles are:

- **Training Activity Lead** - This is the WP7 lead but the role will have to be able to exist in a community outside of XIFI for sustainability.
- **Course Editor** - a role and a group responsible for producing coherent courses related to the training programme.
- **Module Editor** - a role and a group responsible for producing the module that make up the courses.
- **Content Contributor** - any person who contributes content for courses and modules.
- **Training Community Coordinator** - a role responsible for liaising with training event coordinators to ensure that training events are appropriately resourced and providing feedback to the training activity lead, course editors, module editors and content contributors after data has been gathered and analysed.
- **Training Event Coordinator** - a role responsible for the organisation of individual training events. They organise logistics (facilities, etc.), line up trainers and training event participants.
- **Trainer** - they train event participants on topics using material produced for the courses that have been organised.
- **Training Event Analyst** - they gather data on training events and courses using methodologies for training evaluation.

Since the project is still on-going and other stakeholders may be targeted, we plan to update the list of the *source and target* stakeholders during the project lifetime according to the project needs.
# REQUIREMENTS FOR TRAINING PROGRAMME

The requirements for the training programme started with initial discussions at WP7 meetings. These requirements were captured and discussed internally and finally refined.

<table>
<thead>
<tr>
<th>As a/an</th>
<th>I want to..</th>
<th>so that..</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical Manager</td>
<td>have input on the production of the training material roadmap</td>
<td>the release of technical components matches the training programmes</td>
</tr>
<tr>
<td>Training Lead Activity</td>
<td>have a training strategy</td>
<td>other training stakeholders can collaborate effectively</td>
</tr>
<tr>
<td>Training Lead Activity</td>
<td>have training manuals for components</td>
<td>source stakeholders of training can become target stakeholders</td>
</tr>
<tr>
<td>Training Lead Activity</td>
<td>have tutorial material</td>
<td>trainers have content for training sessions and webinars</td>
</tr>
<tr>
<td>Training Lead Activity</td>
<td>have a collection of slide sets</td>
<td>trainers have content for training sessions and webinars</td>
</tr>
<tr>
<td>Training Lead Activity</td>
<td>ensure training events can be organised</td>
<td>our source stakeholders can make effective use of the resources being provided in XIFI and the FIPPP</td>
</tr>
<tr>
<td>Training Lead Activity</td>
<td>have a collection of training videos</td>
<td>source stakeholders can learn asynchronously and effectively</td>
</tr>
<tr>
<td>Training Lead Activity</td>
<td>produce hard-copy training manuals</td>
<td>source stakeholders have good reference material</td>
</tr>
<tr>
<td>Training Lead Activity</td>
<td>ensure a training portal is deployed</td>
<td>source stakeholders can learn asynchronously</td>
</tr>
<tr>
<td>Infrastructure Manager</td>
<td>recognise the efforts of new federation members</td>
<td>other new federation members will be encouraged to engage with the federation</td>
</tr>
<tr>
<td>Course Editor</td>
<td>create course requirements and monitor their fulfilment</td>
<td>I can plan new course development work</td>
</tr>
<tr>
<td>Course Editor</td>
<td>receive completed modules</td>
<td>I can provide them to trainers</td>
</tr>
<tr>
<td>Module Editor</td>
<td>create module requirements and monitor their fulfilment</td>
<td>I can plan new module development work and provide completed modules to the course editor</td>
</tr>
<tr>
<td>Module Editor</td>
<td>store completed modules</td>
<td>I can provide them to the course editor</td>
</tr>
<tr>
<td>Content Contributor</td>
<td>get module requirements and update their progress</td>
<td>the module editor is aware of module production progress</td>
</tr>
<tr>
<td>Content Contributor</td>
<td>store completed content</td>
<td>the module editor can add it to modules</td>
</tr>
<tr>
<td>Training Community Coordinator</td>
<td>leverage of existing tools of the FIPPP</td>
<td>the training community can be fully aware of the greater activities of the FIPPP</td>
</tr>
<tr>
<td>Training Community Coordinator</td>
<td>create a forum for community contributions</td>
<td>the training community is capable of responding to community needs</td>
</tr>
<tr>
<td>Training Community Coordinator</td>
<td>hold 3 basic training sessions</td>
<td>source stakeholders can become target stakeholders</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-------------------------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>Training Community Coordinator</td>
<td>2 intermediate training sessions</td>
<td>source stakeholders can become target stakeholders</td>
</tr>
<tr>
<td>Training Community Coordinator</td>
<td>2 advanced training sessions</td>
<td>source stakeholders can become target stakeholders</td>
</tr>
<tr>
<td>Training Community Coordinator</td>
<td>3-5 awareness sessions</td>
<td>source stakeholders can become target stakeholders</td>
</tr>
<tr>
<td>Training Community Coordinator</td>
<td>3-5 webinars</td>
<td>source stakeholders can become target stakeholders</td>
</tr>
<tr>
<td>Training Event Coordinator</td>
<td>have a listing training event requirements and track associated tasks</td>
<td>training events can be carried out appropriately</td>
</tr>
<tr>
<td>Training Event Coordinator</td>
<td>to promote the training event and gather registrations</td>
<td>logistics for training events can be planned appropriately</td>
</tr>
<tr>
<td>Trainer</td>
<td>to get access to training material for a given course</td>
<td>I can train stakeholders</td>
</tr>
<tr>
<td>Trainer</td>
<td>to submit trainer feedback from course</td>
<td>the course and modules can improve based on experience</td>
</tr>
<tr>
<td>Trainer</td>
<td>to discuss course material with other trainers and course editors</td>
<td>feedback presented to course and module editors is coherent</td>
</tr>
<tr>
<td>Training Analyst Event Coordinator</td>
<td>have a set of training event evaluation methodologies</td>
<td>I know which data to gather at training events</td>
</tr>
<tr>
<td>Training Analyst Event Coordinator</td>
<td>a set of metrics to evaluate training sessions</td>
<td>data gathering can be completed effectively</td>
</tr>
<tr>
<td>Training Analyst Event Coordinator</td>
<td>store the data gathered from training sessions</td>
<td>I can evaluate the training session and programme</td>
</tr>
<tr>
<td>Training Analyst Event Coordinator</td>
<td>produce feedback to the other training stakeholders</td>
<td>training courses and events can be improved incrementally</td>
</tr>
</tbody>
</table>

Table 2 - Training Stakeholder Requirements

In order to produce a plan for the training process, materials and a complimentary recognition programme, a guiding strategy is required.

The mission is the efficient production of training programmes and materials to support the training and assessment of candidates from all the identified stakeholder groups in order of priority from group 1 to group 3. A core component of these programmes is the recognition of effort by stakeholders in these programmes.

The time span for the work package is fixed and the budget is also fixed. In this case, the only flexibility we have is in scope. As such, we start developing training material with a very narrow scope. In addition, we start by identifying the highest priority items.
As the high priority items are developed, the scope is gradually expanded. This allows us to deliver functional training material from the very start and improve it incrementally. This ensures that a quality deliverable is created first and then extended.

To allow us to go from source material to training module ready for teaching, it is necessary to describe the process for transformation.

As part of this process, some guidelines for Deliverable Writers have been created to ensure the source material is of a reasonable minimum quality:

- Structure instructional material into learning objectives with:
  o A target user in mind for the objective
  o A list of the tasks that the user needs to do for the objective
- Skills and knowledge for those tasks
- Those learning objectives will be combined into training modules so keeping them atomic makes this easy to do.
- Use examples and illustrations where appropriate - provide source material to enable amendments and reformatting.
- Field test instructional material before contribution

Finally, through work package discussion, a number of general requirements have emerged.

Ideally, material should be presented online first.

Use of the wiki to capture technical documentation should ensure that cutting edge documentation is available at all times.

The eLearning portal provides higher quality structured learning which can be engaged in at the learners own pace and time schedule. This should be able to provide an effective baseline of knowledge for any stakeholder wishing to engage with the community.

Webinars should be scheduled to engage with community demand. Ultimately, if a topic is repeated for a webinar, this points out a topic for eLearning portal content creation.

We should always aim to ‘train the trainer’ while maintaining trainer quality:

- It is good if a component creator can be a trainer
- It is better if someone trained by the component creator can be a trainer
- It is best if someone can be trained using documentation having never met the component creator

Physical session allows for not just mono-directional lecturing by trainers but also for structured discussion and conversation within the attendee groups. Physical training sessions can be used where there is a high value on the target stakeholders gaining access to the material and the community.
ORGANISATION OF THE TRAINING SESSIONS

Task T7.2 **Community building and training** will address the actual delivery of the training material and the creation of an online community, which will support the training and knowledge transfer. It will organize the training events, ensure that the appropriate trainers are available and execute the training.

As already mentioned in section 4 “Stakeholders”, the approach to training will support the different source stakeholders in their progression into a number of “target stakeholders”. The training will also endorse the stakeholders in their advancement through the “Levels of Achievement” specified in the XIFI Recognition and Reward Programme defined as a part of the strategy in task T7.1 “Training Strategy and Materials”.

The following training sessions are planned at this stage: 3 sessions of basic training; 2 sessions of intermediate training, 2 sessions of advanced training. These sessions will be co-located at 4 different dates:

- 1 basic session;
- 1 basic session + 1 intermediate session;
- 1 basic session + 1 intermediate session + 1 advanced session;
- 1 advanced session.

In addition to these training sessions, 5 additional webinars will be planned according to the outcomes of the training sessions and 5 estimated additional specific training and awareness sessions organized with WP9 for representatives from Public Authorities, taking advantage of existing events at European, national, regional and local level.

In order to organize the training sessions in the most efficient way, we started to collect some inputs from the XIFI partners. In detail, we asked partners to indicate if their organisation is able to host the training sessions (i.e. availability for: room for 20-30 persons, internet connection and sockets for all the participants, screens, projector, coffee-breaks and lunches) and if they are interested in teaching during these training sessions.

In addition, we have prepared an indicative calendar, according to the outcomes of the project, and we identified the “source” and the “target” stakeholders for the first planned training sessions.

**5.1 Workplan**

In this deliverable we show the plan for the organization of the β training session, the training sessions, webinars and additional specific training and awareness sessions, from Month 6 to Month 18 (the D7.3 “XIFI Training Strategy and Material (v2)” will be delivered at Month 18 and it will cover the organization of the training from Month 18 to Month 24).

**5.2 Beta Training Sessions**

We plan organising an initial β Training session for the new partners that will run alongside the XIFI General Meeting in Zurich, in order to “test” the training material we have prepared. The new partners will receive basic training on the infrastructure tools and network configuration options.
Below we summarise the source and target stakeholders and the objective of the training.

<table>
<thead>
<tr>
<th>Source Stakeholders</th>
<th>Target Stakeholders</th>
<th>Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>National research and education networks, Industry association, Industry, SMEs</td>
<td>Infrastructure owners/operators – XIFI additional nodes</td>
<td>Train the new partners in order to expand the XIFI federation to several new countries.</td>
</tr>
</tbody>
</table>

Table 3 - Beta Training Session

### 5.3 Specific Training and awareness sessions for Public Authorities

The first specific training and awareness session for public Authorities will be co-located at the FIF-FIA Athens and it will be organised in collaboration with Work package 9. This training session is “specific training and awareness sessions” and are dedicated to the Public Authorities.

We have summarised below the source and target stakeholders and the objective of the training.

<table>
<thead>
<tr>
<th>Source Stakeholders</th>
<th>Target Stakeholders</th>
<th>Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public Authorities-National Authorities</td>
<td>Intermediaries-others</td>
<td>Mobilise FI experimenters in their countries</td>
</tr>
</tbody>
</table>

Table 4 - First Training Session for Public Authorities

We plan to organize a second training and awareness session using the workshop with the Chambers of Commerce initiated by FI-WARE.

### 5.3.1 Training Sessions

Since we have planned 2 sessions in March and April, we are organising the 1st Training session in May 2014 and the 2nd and 3rd training sessions in June 2014.

These first training sessions shall follow the outcomes of the first year of the project and the issue of the Training Manual (Month 12, March 2014).

Below we summarise the source and target stakeholders and the objectives of the training for the 1st, 2nd and 3rd sessions.

<table>
<thead>
<tr>
<th>Source Stakeholders</th>
<th>Target Stakeholders</th>
<th>Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Developers, students from TUB (in the course of regular lectures and projects) as well as start-ups, SMEs and developers from the DT Developer Gaden</td>
<td>Developers-Fi-Ops users</td>
<td>Use XIFI Infrastructures + services for experimentations</td>
</tr>
</tbody>
</table>

Table 5 - First Training Session
2nd Training session: Basic level – organised at UPM

<table>
<thead>
<tr>
<th>Source Stakeholders</th>
<th>Target Stakeholders</th>
<th>Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infrastructure owners/operators - XiPi IOs; XIFI new partners</td>
<td>Infrastructure owners/operators</td>
<td>Expand the XIFI federation to several new countries</td>
</tr>
</tbody>
</table>

*Table 6 - Second Training Session*

3rd Training session: Intermediate level – organised at UPM

<table>
<thead>
<tr>
<th>Source Stakeholders</th>
<th>Target Stakeholders</th>
<th>Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infrastructure owners/operators - XiPi IOs; XIFI new partners</td>
<td>Infrastructure owners/operators</td>
<td>To offer, powered by Fi-Ops, the FI-PPP technologies (Enablers) to 3rd parties and join the infrastructure federation and therefore FI-LAB</td>
</tr>
</tbody>
</table>

*Table 7 - Third Training Session*

We plan to organize the 4th training session in September 2014 (training session for Phase III projects), when the starting date of the Phase III projects is confirmed. The 5th and 6th training sessions could be co-located in November/December 2014, because we feel September (Month 18) seems to be a turning point of the project. At M18 some key milestones will be achieved: MS24; MS32; MS42; MS54; MS83, MS94. Moreover, 8 deliverables will be deliver to the EC: D1.5; D2.4; D2.5; D3.5; D4.5; D6.3; D7.3; D8.4; D11.2.3.

As the project ends in March 2015, we shall try to host the 7th training session in February 2015. This training session shall follow the project results from September 2014 to February 2015.

The table below summarises the planned training sessions.

<table>
<thead>
<tr>
<th>Session</th>
<th>May</th>
<th>June</th>
<th>July</th>
<th>August</th>
<th>September</th>
<th>October</th>
<th>November</th>
<th>December</th>
<th>January</th>
<th>February</th>
<th>March</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2nd</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3rd</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4th</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5th</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6th</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7th</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Figure 1 - Planned Training Sessions*

5.3.2 Webinars

We plan to organise 5 additional webinars, which are aligned with the outcomes of the training sessions.

Below we summarise the scheduling of the webinars.

<table>
<thead>
<tr>
<th>Session</th>
<th>June</th>
<th>July</th>
<th>August</th>
<th>September</th>
<th>October</th>
<th>November</th>
<th>December</th>
<th>January</th>
<th>February</th>
<th>March</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2nd</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3rd</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4th</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5th</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6th</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7th</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Figure 2 - Planned Webinars*
5.4 **Organisation of training sessions**

As indicated in the DoW, 7 training sessions at 4 different dates are planned: 3 sessions of basic training; 2 sessions of intermediate training, 2 sessions of advanced training.

To organize these training sessions as effectively as possible, we adopted the following procedure:

- We asked the XIFI partners if they were interested in teaching and if their organization would be able to host a training session for 30 people;
- We identified the teachers and the location;
- We identified the source and target stakeholders;
- We prepared the content of these training sessions;
- We prepared the training material;
- We will promote the training sessions.

These training sessions would be promoted on a large scale in the Future Internet community via the Future Internet portal and mailing list, to all the FI PPP participants, including new entrants from Phase III. For the 1st, 2nd and 3rd training session, we will invite students from TUB and UPM, some of the open source communities associated with our partners, some developer user communities from the XIFI partners and new partners, the developers interested in the FI-WARE challenge and the new XIFI partners. We will reuse the contacts of Infrastructures owners and operators which participated in the webinars organized by the INFINITY project, using the XiPi mailing list. In addition, we will ask the XIFI partners to promote these training sessions through their channels and contacts. Advertisement and promotion will be made on various websites (eg. XIFI website, FI-WARE website etc…) through specific e-mailing with all mailing lists available and through social media, in particular Twitter and LinkedIn, as well as Facebook whenever relevant.

The table below summarises the actions to be done in order to organise the training sessions (Month 6-18):

<table>
<thead>
<tr>
<th>1ST TRAINING SESSION – BASIC TRAINING SESSION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Source Stakeholders</strong></td>
</tr>
<tr>
<td>Developers</td>
</tr>
<tr>
<td>Students from TUB,</td>
</tr>
<tr>
<td>some of the open source communities associated with Fraunhofer,</td>
</tr>
<tr>
<td>DT Developer Garden</td>
</tr>
<tr>
<td>Start-ups; SMEs</td>
</tr>
<tr>
<td>developer user communities from new partners</td>
</tr>
<tr>
<td><strong>Target Stakeholders</strong></td>
</tr>
<tr>
<td>Developers - FI-Ops users</td>
</tr>
<tr>
<td><strong>Location and Date</strong></td>
</tr>
<tr>
<td>Fraunhofer Fokus, Berlin, Germany. 15th May 2014</td>
</tr>
<tr>
<td><strong>Support Material</strong></td>
</tr>
<tr>
<td>Slides, training manual, training video, Guided tour/hands-on experiments</td>
</tr>
<tr>
<td><strong>Teachers</strong></td>
</tr>
<tr>
<td>Fokus Fraunhofer, DT, TUB</td>
</tr>
<tr>
<td><strong>Content of the training session</strong></td>
</tr>
<tr>
<td>Basic</td>
</tr>
<tr>
<td>Presentation - XIFI Architecture and capacities</td>
</tr>
<tr>
<td>Demonstration and case studies</td>
</tr>
</tbody>
</table>
Practical examples potentially including practice/tutorials
( XIFI Core Concepts; Summary of XIFI Node Features; Setup and Use of Experimentation/Developer Environment; Resource Catalogue and Recommendation Tool)

| Audience expected | ~25 people |

### Table 8 - Actions related to the first training session

<table>
<thead>
<tr>
<th>2nd TRAINING SESSION – BASIC TRAINING SESSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Stakeholders</td>
</tr>
<tr>
<td>Target Stakeholders</td>
</tr>
<tr>
<td>Location and Date</td>
</tr>
<tr>
<td>Support Material</td>
</tr>
<tr>
<td>Teachers</td>
</tr>
</tbody>
</table>
| Content of the training session | Basic
XIFI Core Concepts
Summary of XIFI Node Features
Process for infrastructure joining the federation
Architecture of Federated Platform
Components Function Overview
Management of an Infrastructure (Data Centre and Network)
XIFI Monitoring Support
XIFI Support Procedures |
| Audience expected | ~20 people |

### Table 9 - Actions related to the second training session

<table>
<thead>
<tr>
<th>3rd TRAINING SESSION – INTERMEDIATE TRAINING SESSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Stakeholders</td>
</tr>
<tr>
<td>Target Stakeholders</td>
</tr>
<tr>
<td>Location and Date</td>
</tr>
<tr>
<td>Support Material</td>
</tr>
<tr>
<td>Teachers</td>
</tr>
</tbody>
</table>
| Content of the training session | Intermediate:
Hands-on session with the FI-Ops developers (in 2 groups): configuring and deep understanding on adapting your infrastructure to the FI-PPP offer |
| Audience expected | ~20 people |

### Table 10 - Actions related to the third training session
5.5 Organisation of the webinars

The XIFI project plans to publish five webinars (Web Seminars) based on the outcomes of the training sessions and on the needs that will be gathered from the stakeholder groups. This training material will be hosted in the eLearning platform available at http://edu.fi-xifi.eu (also accessible through XIFI website at http://fi-xifi.eu/training.html).

These webinars are conceived to have an asynchronous nature, this kind of publication, indeed, allows the end users to access the training material, constituting the webinars, whenever and as many times as they want, can and need.

This “asynchronous nature” allows overcoming a typical issue of the webinars organization, which actually is scheduling the proper timing when all interested attendees are available. This way it’s even easier to reach a higher number of people, compared to the traditional webinar modality.

In addition, the training material of each asynchronous webinar held this way, can be always updated and enriched allowing users to always have at their disposal new and up-to-date contents. This would not be so easy holding traditional webinars, since it should require to schedule a new timing involving again the same attendees of the previous webinar in order to transfer them new content.

For sure the interaction between the teacher and the attendees, that can happen during a traditional webinar, is not so effective in this asynchronous modality. In order to balance the two modalities and reach the most effective results in terms of knowledge transfer, the webinars are provided with a dedicated forum, where all attendees can ask for questions and more details, can actively participate to discussions and get answers on possible problems or interested topics. The forum is also a valid tool, useful to the author of the webinar, in order to gather feedback from the users and properly react to improve the webinar itself, by enriching the related training material. Moreover, when publishing a webinar, the author is also asked to publish, following a “best practice”, the contacts of at least one or two reference persons able to give needed information and details on the topic dealt with by the webinar. These contact persons play an “off-line teacher” role, whom the users can anytime refer to get information they possibly didn’t get elsewhere on that topic.
The eLearning Platform aggregates different kinds of available training material, which can be hosted by different locations (i.e. stored internally or external to the platform).

Each webinar can be created as easily as any other training course published to the Platform, by organizing different available resources structured in a logical path. Any course can aggregate different kinds of training material, such as:

- seminars
- videos
- files – .pdf and .ppt
- links to any kind of web resources (wiki, blogs, services, etc.)

An asynchronous web seminar published to the Platform is organized with a number of seminars related to a (need) number of topics affecting the webinar. Once a training course is published, the entire course can be split by topics in order to produce one seminar per topic. Thus, the training path, linked to that webinar, can be rebuilt, as sequence of seminars, directly in the structure of the course. As stated above, a number of different resources can be referenced, published, embedded, uploaded and, thus, included and logically organized in a course in order to set-up a webinar.

**Seminars**

In the eLearning Platform a seminar is defined as a set of slides simultaneously accompanied by an audio presenting and explaining the content of those slides (needed information on how to create and publish a seminar is available in the FI-WARE wiki at [http://forge.fi-ware.eu/plugins/mediawiki/wiki/fiware/index.php/How_to_create_a_SCORM_course](http://forge.fi-ware.eu/plugins/mediawiki/wiki/fiware/index.php/How_to_create_a_SCORM_course)). The seminar, which is actually one – and usually the most important – of the elements composing the webinar, can be prepared in the same manner as if preparing a lesson to be held live: a number of slides and a speech text. For each slide must be recorded the audio introducing its content.

**Videos**

Videos can be referenced within the webinar as a valid and effective resource to transfer knowledge, particularly when practical examples are needed (e.g. how to use a service or steps to be followed to perform a given process). A video can be uploaded (.mp4 format recommended) to the Platform, referenced/ embedded with an external link (YouTube). It’s worth to mention that should be avoided to upload videos longer than 10 minutes to the Platform, to be included in a webinar. For example, any video consisting of a recorded session, taken from a live webinar (though not recommended, being usually of a low quality), could be split in topics no longer than 10 minutes each, and, after that, rebuild the entire session using the structure of the course. In general, it’s better to structure the webinar with one video per topic that could actually be auto-consistent and no longer than 10 minutes. Subtitles to the video should be added in post production and include in the structure of the course a file that contains the transcript audio of the videos.

**Files**

Files can be uploaded and enclosed in the webinar as documentation to give details on any topic of the session. User manuals, forms, installations steps, etc. can be accessed by the users in the meanwhile listening to the learning course, so to have a valid support to better follow the exact content that is being dealt with during the webinar.

**External resources**

Links to any kind of external resource can be incorporated in the learning course. This turns out to be very useful mainly for two reasons:

When the topic of a webinar (or one of its sessions) is dealing, for example, with specific on-line services, the users can access, through the given link, to that service and verify and check at the same moment the indications given in the course on that service.
Links to blogs, forums, communities and any kind of documentation are fundamental for a in-depth analysis and a deeper understanding of the topic dealt with by the webinar.

5.6   Organisation of training sessions for Public Authorities

Five indicative specific training and awareness training sessions for Public Authorities will be organised, taking advantage of the existing events at European, national, regional and local level. The main purpose of these training sessions will be to provide basic information about XIFI and to create awareness about the FI-PPP world in order to support the PAs in their progression into a number of target stakeholders (e.g. Intermediaries).

So far, we have planned the following training session:

<table>
<thead>
<tr>
<th>1st Training session for Public Authorities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Stakeholders</td>
</tr>
<tr>
<td>Target Stakeholders</td>
</tr>
<tr>
<td>Type of Session</td>
</tr>
<tr>
<td>Location and Date</td>
</tr>
<tr>
<td>Support Material</td>
</tr>
<tr>
<td>Teachers</td>
</tr>
<tr>
<td>Content of the training session</td>
</tr>
<tr>
<td>Audience expected</td>
</tr>
</tbody>
</table>

Table 11 - First Training Session for Public Authorities

Four additional sessions will be organised.
6 CONTENT OF THE SESSIONS

In creating content for the training sessions, the following considerations were taken.

6.1 Internal training courses for the teachers

We should always aim to ‘train the trainer’ while maintaining trainer quality:

- It is good if a component creator can be a trainer
- It is better if someone trained by the component creator can be a trainer
- It is best if someone can be trained using documentation having never met the component creator to be a trainer

In practical terms, this is related to the development roadmap of the components and initiatives being worked on as part of the technical and operational work packages (WP1 - WP5).

The versioning of material related to components used in the system must align with the release and roll out of those components (so education matches the situation on the ground). For this to be completed, there must be reasonable demos in place for the trainers along with the documentation of the component. This is a core focus for WP6 and happens in coordination with the Technical Manager at each technical meeting.

6.2 Basic training session

These sessions are designed to be broad in content scope but provide some basic skills needed to carry out common tasks.

6.2.1 For all stakeholders

Core Concepts

- Summary of support procedures
- Summary of FI-Lab service features

6.2.2 For FI-Developers

- Architecture and capacities demonstration
- Case studies
- Practical examples potentially including practice/tutorials
- Summary of FI-Lab/FI-Ops Features
- Setup and Use of Experimentation/Developer Environment
- Resource Catalogue and Recommendation Tool

6.2.3 For Infrastructure Owners

- XIFI Core Concepts
- Summary of FI-Lab/FI-Ops Features
- Process for infrastructure joining the federation
- Architecture of Federated Platform
- Components Function Overview
- Management of an Infrastructure (Data Centre and Network)
- FI-Ops Monitoring Support
- Support Procedures

### 6.3 Intermediate training session

These sessions are designed to provide more focus over the basic sessions. In addition, they'll also equip the attendee with newer skills for complex tasks.

#### 6.3.1 For Infrastructure Owners

Hands-on session with the FI-Ops developers (in 2 groups): configuring and deep understanding on adapting your infrastructure to the FI-PPP offer

### 6.4 Advanced training session

These sessions provide attendees with advanced, leading edge skills related to a narrow set of topics.

### 6.5 Other training session

It was identified that while technical training is absolutely necessary, there is also a need to support technical and non-technical managers and leaders associated with the source stakeholders. For this reason, training and awareness session will provide a mix of basic technical content with additional strategic content for these groups.
7 TRAINING MATERIAL DEVELOPMENT

Training material is created from the following streams:

- Identification of reference material from deliverables, papers, workshop posters, etc.
- Technical documentation from component development.

The procedure for development of reference material is as follows:

- At specified periods in the project, batches of deliverables are taken and reviewed.
- Modular topics of interest are noted. Additionally, preceding reference topics are also identified and marked as dependencies.
- The information is tabulated centrally.
- A graph of the dependencies is generated.
- Topic clusters can be identified and high priority topics can be picked easily based on topic precedence.
The initial review produced the following information:

<table>
<thead>
<tr>
<th>Id</th>
<th>Name</th>
<th>Source</th>
<th>Difficulty</th>
<th>Length</th>
<th>Prerequisite</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Core Concepts</td>
<td>D1.1</td>
<td>Basic</td>
<td>Short</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>5.6 Summary of XIFI Nodes Features</td>
<td>D1.1</td>
<td>Basic</td>
<td>Short</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>6.1 An infrastructure owner wants to join the XIFI Federation</td>
<td>D1.1</td>
<td>Basic</td>
<td>Short</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>6.2 A UC project wants to setup and use an experimentation environment</td>
<td>D1.1</td>
<td>Basic</td>
<td>Short</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>6.4 An end-user of the Federation requests support and help</td>
<td>D1.1</td>
<td>Intermediate</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>6.5 Management of an Infrastructure (Network and Data Centre)</td>
<td>D1.1</td>
<td>Intermediate</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>7 DRAFT OF THE ARCHITECTURE OF XIFI FEDERATED PLATFORM</td>
<td>D1.1</td>
<td>Intermediate</td>
<td>Long</td>
<td>2</td>
</tr>
<tr>
<td>8</td>
<td>APPENDIX A: FI-WARE GE HW/SW REQUIREMENTS</td>
<td>D1.2</td>
<td>Intermediate</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>APPENDIX B HIGH AVAILABILITY GUIDELINES</td>
<td>D1.2</td>
<td>Intermediate</td>
<td>Long</td>
<td>8</td>
</tr>
<tr>
<td>10</td>
<td>1.3 Introduction to XIFI Adapters</td>
<td>D3.1</td>
<td>Basic</td>
<td>Short</td>
<td>6</td>
</tr>
<tr>
<td>11</td>
<td>2.1 XIFI Network-based Services Adapters</td>
<td>D3.1</td>
<td>Intermediate</td>
<td>Short</td>
<td>10</td>
</tr>
<tr>
<td>12</td>
<td>2.2 XIFI Infrastructure Monitoring Adapters</td>
<td>D3.1</td>
<td>Intermediate</td>
<td>Short</td>
<td>11</td>
</tr>
<tr>
<td>13</td>
<td>2.4 Software-Defined Networking (SDN)</td>
<td>D3.1</td>
<td>Intermediate</td>
<td>Short</td>
<td>10</td>
</tr>
<tr>
<td>14</td>
<td>2.5 Bandwidth on Demand (BoD)</td>
<td>D3.1</td>
<td>Intermediate</td>
<td>Short</td>
<td>10</td>
</tr>
<tr>
<td>15</td>
<td>2.6 Network as a Service (NaaS)</td>
<td>D3.1</td>
<td>Intermediate</td>
<td>Short</td>
<td>10</td>
</tr>
<tr>
<td>16</td>
<td>2.7 Infrastructure as a Service (IaaS)</td>
<td>D3.1</td>
<td>Intermediate</td>
<td>Short</td>
<td>10</td>
</tr>
<tr>
<td>17</td>
<td>2.8 Platform as a Service (PaaS)</td>
<td>D3.1</td>
<td>Intermediate</td>
<td>Short</td>
<td>10</td>
</tr>
<tr>
<td>18</td>
<td>4.1 Network-based Services Management Systems</td>
<td>D3.1</td>
<td>Intermediate</td>
<td>Short</td>
<td>11</td>
</tr>
<tr>
<td>19</td>
<td>4.1.1 Traditional Management</td>
<td>D3.1</td>
<td>Intermediate</td>
<td>Short</td>
<td>11</td>
</tr>
<tr>
<td>20</td>
<td>4.1.2 Open Access Management</td>
<td>D3.1</td>
<td>Intermediate</td>
<td>Short</td>
<td>11</td>
</tr>
<tr>
<td>21</td>
<td>4.1.3 SDN-based Network Management</td>
<td>D3.1</td>
<td>Intermediate</td>
<td>Short</td>
<td>11</td>
</tr>
<tr>
<td>22</td>
<td>4.1.4 OpenNaaS</td>
<td>D3.1</td>
<td>Intermediate</td>
<td>Short</td>
<td>11</td>
</tr>
<tr>
<td>23</td>
<td>4.2 Network Monitoring Tools</td>
<td>D3.1</td>
<td>Intermediate</td>
<td>Short</td>
<td>11</td>
</tr>
<tr>
<td>24</td>
<td>4.2.1 PerfSONAR</td>
<td>D3.1</td>
<td>Intermediate</td>
<td>Short</td>
<td>11</td>
</tr>
<tr>
<td>25</td>
<td>4.3 Datacenter Monitoring Tools</td>
<td>D3.1</td>
<td>Intermediate</td>
<td>Short</td>
<td>11</td>
</tr>
<tr>
<td>26</td>
<td>4.3.1 Collectd</td>
<td>D3.1</td>
<td>Intermediate</td>
<td>Short</td>
<td>11</td>
</tr>
<tr>
<td>27</td>
<td>4.3.2 Nagios</td>
<td>D3.1</td>
<td>Intermediate</td>
<td>Short</td>
<td>11</td>
</tr>
<tr>
<td>28</td>
<td>4.3.3 OpenNMS</td>
<td>D3.1</td>
<td>Intermediate</td>
<td>Short</td>
<td>11</td>
</tr>
<tr>
<td>No.</td>
<td>Section Title</td>
<td>Module</td>
<td>Complexity</td>
<td>Duration</td>
<td>Page</td>
</tr>
<tr>
<td>-----</td>
<td>-------------------------------------------------------------------------------</td>
<td>--------</td>
<td>------------</td>
<td>----------</td>
<td>------</td>
</tr>
<tr>
<td>29</td>
<td>4.4 FI-WARE GEs Management Tools</td>
<td>D3.1</td>
<td>Intermediate</td>
<td>Short</td>
<td>11</td>
</tr>
<tr>
<td>30</td>
<td>4.4.1 Cloud IaaS Deployment tools</td>
<td>D3.1</td>
<td>Intermediate</td>
<td>Short</td>
<td>11</td>
</tr>
<tr>
<td>31</td>
<td>5 NETWORK-BASED SERVICES ADAPTERS</td>
<td>D3.1</td>
<td>Advanced</td>
<td>Long</td>
<td>11</td>
</tr>
<tr>
<td>32</td>
<td>6 XIFI INFRASTRUCTURE MONITORING MIDDLEWARE</td>
<td>D3.1</td>
<td>Advanced</td>
<td>Long</td>
<td>12</td>
</tr>
<tr>
<td>33</td>
<td>7 GE DEPLOYMENT AND CONFIGURATION ADAPTER</td>
<td>D3.1</td>
<td>Advanced</td>
<td>Long</td>
<td>29</td>
</tr>
<tr>
<td>34</td>
<td>8 INFRASTRUCTURE TOOLBOX</td>
<td>D3.1</td>
<td>Advanced</td>
<td>Long</td>
<td>30</td>
</tr>
<tr>
<td>35</td>
<td>9 APIS SPECIFICATION</td>
<td>D3.1</td>
<td>Advanced</td>
<td>Long</td>
<td>18</td>
</tr>
<tr>
<td>36</td>
<td>2.2 Components functionality overview</td>
<td>D4.1</td>
<td>Basic</td>
<td>Short</td>
<td>3</td>
</tr>
<tr>
<td>37</td>
<td>3.1 Identity Federation and Single Sign On</td>
<td>D4.1</td>
<td>Basic</td>
<td>Long</td>
<td>36</td>
</tr>
<tr>
<td>38</td>
<td>3.2 XIFI Portal</td>
<td>D4.1</td>
<td>Basic</td>
<td>Long</td>
<td>36</td>
</tr>
<tr>
<td>39</td>
<td>3.3 Resources Catalogue and Recommendation tool</td>
<td>D4.1</td>
<td>Basic</td>
<td>Long</td>
<td>36</td>
</tr>
<tr>
<td>40</td>
<td>3.4 SLA Management</td>
<td>D4.1</td>
<td>Basic</td>
<td>Long</td>
<td>36</td>
</tr>
<tr>
<td>41</td>
<td>3.5 Interoperability tools</td>
<td>D4.1</td>
<td>Basic</td>
<td>Long</td>
<td>36</td>
</tr>
<tr>
<td>42</td>
<td>3.6 Security and Privacy Dashboard</td>
<td>D4.1</td>
<td>Basic</td>
<td>Long</td>
<td>36</td>
</tr>
<tr>
<td>43</td>
<td>APPENDIX A: WIRECLOUD MASHUP PLATFORM</td>
<td>D4.1</td>
<td>Advanced</td>
<td>Long</td>
<td>38</td>
</tr>
<tr>
<td>44</td>
<td>APPENDIX B: RESOURCE CATALOGUE, API OPERATIONS</td>
<td>D4.1</td>
<td>Advanced</td>
<td>Long</td>
<td>38</td>
</tr>
<tr>
<td>45</td>
<td>APPENDIX C: SLA MANAGEMENT, API OPERATIONS</td>
<td>D4.1</td>
<td>Advanced</td>
<td>Long</td>
<td>40</td>
</tr>
<tr>
<td>46</td>
<td>APPENDIX D: INTEROPERABILITY TOOL, API OPERATIONS</td>
<td>D4.1</td>
<td>Advanced</td>
<td>Long</td>
<td>41</td>
</tr>
<tr>
<td>47</td>
<td>APPENDIX E: CLOUD4SOA</td>
<td>D4.1</td>
<td>Advanced</td>
<td>Long</td>
<td>45</td>
</tr>
<tr>
<td>48</td>
<td>1.3 XIFI Federation Policies</td>
<td>D5.1</td>
<td>Intermediate</td>
<td>Short</td>
<td>3</td>
</tr>
<tr>
<td>49</td>
<td>1.4 XIFI Federation, Federation Extension, and Evolution of Procedures</td>
<td>D5.1</td>
<td>Intermediate</td>
<td>Short</td>
<td>3</td>
</tr>
<tr>
<td>50</td>
<td>1.5 Infrastructures versus Nodes</td>
<td>D5.1</td>
<td>Intermediate</td>
<td>Short</td>
<td>3</td>
</tr>
<tr>
<td>51</td>
<td>1.6 Lessons Learned From Previous/Other Research Projects</td>
<td>D5.1</td>
<td>Intermediate</td>
<td>Short</td>
<td>3</td>
</tr>
<tr>
<td>52</td>
<td>2.1 General Procedures For the Management of Nodes</td>
<td>D5.1</td>
<td>Intermediate</td>
<td>Short</td>
<td>6</td>
</tr>
<tr>
<td>53</td>
<td>2.2 General Procedures For the Developer Support</td>
<td>D5.1</td>
<td>Intermediate</td>
<td>Short</td>
<td>5</td>
</tr>
<tr>
<td>54</td>
<td>2.3 General Procedures For the Infrastructure Support</td>
<td>D5.1</td>
<td>Intermediate</td>
<td>Short</td>
<td>52</td>
</tr>
</tbody>
</table>
This information was further constrained to a first set of clustered information and represented on a graph as follows:

**Figure 5 - Graph of initial training content topics from analysis**

Technical Documentation is treated as a special type of reference documentation. While the requirements and descriptions of component may not be subject to change making their deliverable-based descriptions accurate and fit for training material, their installation, usage and maintenance guides may be subject to change based on new developments, changes in the environment (upstream software increments, operating systems upgrade or hardware improves). As such, the following should be true when including technical components documentation in training:

The component version that the training material refers to must be clearly labelled on the documentation

- A URL to the online version of that documentation must be present in the provided training material
- A URL to the latest version of that component and associated document should be provided

Currently, the Technical Manager maintains a list of components and associated documentation on the XIFI Wiki [3]
7.1 Community Portal

The details of the eLearning portal can be found in D7.1 - XIFI online community portal[4]. The following is the executive summary providing an overview for reader here.

Specific activities to educate, inform and train the stakeholders groups in how to effectively use and interact with the XIFI Federation have been planned in the XIFI Workpackage in charge of Training. Deliverable D7.1 has built the XIFI online community portal. This is the main online interface from XIFI to external stakeholders that are interested or have already decided to join the XIFI federation. Adding to the various information that is already available on the XIFI web, e.g. a Wiki, downloadable XIFI material or summary information on FI-Ops, D7.1 focuses on enabling concrete training and educating activities. The core element is an e-learning platform where the various XIFI training material will be provided. It is accessible from the Training page of the XIFI web or directly at http://edu.fi-xifi.eu.

The most important benefit that the eLearning platform offers is that all content and all courses are

<table>
<thead>
<tr>
<th>Name</th>
<th>Architecture Layer</th>
<th>Redmine Backlog</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Federated Identity Management</td>
<td>Security</td>
<td>Backlog</td>
<td></td>
</tr>
<tr>
<td>Federation Monitoring</td>
<td>Monitoring</td>
<td>Backlog</td>
<td></td>
</tr>
<tr>
<td>OpenStack Data Collector</td>
<td>Monitoring</td>
<td>Backlog</td>
<td></td>
</tr>
<tr>
<td>Cloud Portal</td>
<td>User Oriented</td>
<td>Backlog</td>
<td></td>
</tr>
<tr>
<td>Resource Catalogue&amp;Recommender</td>
<td>GUI</td>
<td>Backlog</td>
<td></td>
</tr>
<tr>
<td>SLA_Manager</td>
<td>User Oriented</td>
<td>Backlog</td>
<td></td>
</tr>
<tr>
<td>Federation Manager</td>
<td>User Oriented</td>
<td>Backlog</td>
<td></td>
</tr>
<tr>
<td>Infographics and Status Pages</td>
<td>User Oriented</td>
<td>Backlog</td>
<td></td>
</tr>
<tr>
<td>Access Control GE</td>
<td>Security</td>
<td>Backlog</td>
<td></td>
</tr>
<tr>
<td>Infrastructure Toolbox</td>
<td>Deployment &amp; Operations</td>
<td>Backlog</td>
<td></td>
</tr>
<tr>
<td>Deployment and Configuration Adapter</td>
<td>Deployment &amp; Operations</td>
<td>Backlog</td>
<td></td>
</tr>
<tr>
<td>Interoperability Tool</td>
<td>User Oriented</td>
<td>Backlog</td>
<td></td>
</tr>
<tr>
<td>Network Active Monitoring</td>
<td>Monitoring</td>
<td>Backlog</td>
<td></td>
</tr>
<tr>
<td>FI-Lab App Template</td>
<td>User Oriented</td>
<td>Backlog</td>
<td></td>
</tr>
<tr>
<td>NGSIAdapter</td>
<td>Monitoring</td>
<td>Backlog Adapter</td>
<td></td>
</tr>
<tr>
<td>DEM</td>
<td>Monitoring</td>
<td>Backlog</td>
<td></td>
</tr>
<tr>
<td>NPM</td>
<td>Monitoring</td>
<td>Backlog</td>
<td></td>
</tr>
<tr>
<td>Security Proxy</td>
<td>Security</td>
<td>Backlog</td>
<td></td>
</tr>
<tr>
<td>Security Dashboard</td>
<td>Security</td>
<td>Backlog</td>
<td></td>
</tr>
<tr>
<td>Security Monitoring</td>
<td>Security</td>
<td>Backlog</td>
<td></td>
</tr>
</tbody>
</table>

Table 13 - Public List of Software Components
available at any time, ready for use as often as the user wants and needs. Students can access the courses on their own, and in case of questions they can directly contact the teacher via the available channels.

### 7.2 Online Training Content

Every course can include various types of contents. The ones probably most interesting are:

- **Web seminar**: This format is represented by a list of slides (directly accessible from a menu) and a synchronised audio track.
- **Video**: This format is particularly useful when a recorded session is already available (e.g. webinar, presentation).
- **Document**: It is possible to use this format for publishing manuals, guides, or other kind of documents, e.g. in pdf format.
- **Web link**: A web link can provide a reference to an external (web) resource.

Users may start using the platform, i.e. taking a training course, in guest mode without registration. However, for using some of the training material formats e.g. participating in a poll a prior registration at the portal is necessary. Registration is always required for anybody who wants to create a new training course or upload training material. In addition to that, these users also need to send an email to the platform operator to request getting Author status for their registered account.

Creating a training course then is rather straightforward. As a first step, a new course needs to be created and a number of parameters can be filled to configure the course, e.g. defining the date from which the course becomes available in the portal or the number of elements the course contains. In a second step, the course that so far has no content can be filled with material in one of the various possible formats. Detailed help information is available for each of the parameters that can be filled or course material formats that can be included.

In conclusion it can be said that the portal that has been setup is a powerful tool that enables the provision of all required information related to training and community building, and offers specific functionality to create and provide online training courses which can well support and complement the other e.g. physical training activities planned by XIFI.

### 7.3 Presentations

The presentations should use the agreed XIFI presentation template.

---

**Figure 6 - Template title slide**
The template ensures that content appears to follow the branding guidelines and other design features created in WP9 - Federation Promotion & Dissemination.

7.4 Training Videos

7.4.1 Overview

As already stated, the overall aims are to educate, inform and train the stakeholders groups in how to use and interact with the XIFI Federation effectively, whilst understanding the varying needs, interests and abilities of each stakeholder group.

The XIFI project has planned to develop a series of training videos on the outcomes of the XIFI project results and has decided to use professional help to produce a series of online knowledge transfer videos. Work-package 7 will liaise in close cooperation with the technical coordination to produce Request for Proposals for each of these videos.

7.4.2 Objective of the training videos

The XIFI project wants to produce training videos, which for example will explain the core concepts of the XIFI project in a very clear and comprehensive way. The videos will be used as supporting tools during the training sessions and also will be published in the on-line learning platform and social media channels.

7.4.3 Target audience

The purpose of the videos will be to explain various aspects of the project to a diversified audience: ICT specialists, such as developers, infrastructure owners, engineers, researchers, etc who are not familiar with the XIFI project but, with an appropriate training, could use the services offered by XIFI; Public Authorities, such as Smart Cities, Local, Regional, National, European and International Authorities which are not familiar with XIFI but, with an appropriate training, could mobilize the Future Internet experimenters in their own countries.
7.4.4  Context for usage of the videos

The videos will be:
- Used as a support during the training sessions;
- Published on the XIFI e-learning platform (Moodle based tool);
- Published on YouTube;
- Used during events and webinars

7.4.5  Production Process

In producing the videos, the following processes were used when engaging with professional video production organisations.

![Video production processes](link)

7.5  Training Manuals

The training manuals are assembled from a number of diverse sources both within and outside of XIFI as a project. Those materials are then reviewed, assessed for suitability and appropriate parts added to the final manuals. Where necessary, additional materials will be sought from suitable content contributors.

7.5.1  Source Materials

In the course of producing the first manuals, the following were identified as sources of material:
- XIFI Deliverables - periodic review of deliverables is needed to ensure that manuals are up to
date on a global level. Those reviews co-inside with releases of banks of deliverables.

- FI-WARE Deliverables - Where it is necessary to reference material from FI-WARE, publicly available information is used.
- Third-party components - Where it is necessary to reference material for third party components, publicly available information is used.

7.5.2  Manual Assembly

As was referenced in the training programme requirements, a process for producing learning material is needed. The initial process used is described below:

![Learning Material Production Process Diagram]

*Figure 9 - Course creation process for manuals*

In this model, high-level courses are outlined to fit the needs of the training community. These course outlines are broken down into modules with defined learning outcomes. Those learning outcomes are then satisfied by contributions from specialist sources (XIFI deliverables, component authors or identified third party sources).

This model requires that material release match the technical roadmap of the overall project. It further requires a 'pull-model' of content collection and assembly. The content is gathered from deliverables and component documentation and added to the modules that make up the course manuals.
8 XIFI RECOGNITION & REWARD PROGRAMME

8.1 Overview

The Recognition and Reward Programme has been designed to encourage the infrastructures joining XIFI to perform a real engagement and participation in the XIFI federation and FI-LAB. This task is part of the work package dealing with training activities, since passing the training phase is a precondition for the recognition or reward.

8.2 Objective

The XIFI Recognition and Reward Programme should be used to encourage the participation of different stakeholders in the training and recognised the willingness and effective XIFI federation participation as a new node. These infrastructures that are receiving direct funding from the European Commission are therefore excluded for the participation in the (it shouldn’t be oriented to any party receiving funding directly or indirectly from XIFI) economic rewards but they can receive the recognition. The target stakeholders are the infrastructure owners (although in rare exceptions facilitators may receive a reward, this shouldn’t be the case), and it should be discussed who receives the reward, being the reward focused on the infrastructure itself and the infrastructure person in charge. Since the Recognition and Reward Programme has been designed to attract more infrastructures, the recognition and reward can only happen when the infrastructure effectively joined the XIFI federation under a certain conditions defined in the commitment levels.

8.3 How to recognise and reward by commitment levels

The Reward and Recognition programme should be based on 3 levels starting from the training completion with the sufficient commitment level:

BRONZE: this level includes the engagement and partial integration, forming part of the federation but with caveats and pre-conditions for the experimentation. The training should have been completed and the understanding of the processes done.

SILVER: this level will be reached after the BRONZE level, when the achievement of joining the XIFI federation and offering openly the same services (with a similar service level) as the other infrastructures already in XIFI is reached.

GOLD: this level will be reached after the SILVER level when the infrastructure in addition to being federated and openly offering services, is contributing with a number of users / developers which is increasing the use of the XIFI federation and the objectives of the FI-PPP.

The next step will be to define the economic compensation when reaching those levels and when to consider the level achieved. For this purpose a committee will be formed by different partners, from the technical and business sides of XIFI to determine the achievement and the maximum number of infrastructures that can be awarded with an economic prize. It is planned to offer the compensation to the first infrastructures joining the first 2 levels and keep some budget for the GOLD level to be given at the end of the project.

8.4 Coherence with the training

It is indispensable to match the timing with the training to encourage those infrastructures that are successfully passing the training (to be evaluated with a questionnaire) to take part in the federation and receive the recognition.
8.5 Publicity

The publicity of the Recognition and Reward Programme should be done along with the rest of publicity to join the federation and participate in the training for infrastructure owners. Evident channels are the XiPi portal, infrastructure programmes, list of infrastructures in Europe collected by the project INFINITY, etc. In addition the Recognition and Reward Programme will be publicised in every XIFI event to attract infrastructures to the federation. The infrastructures receiving a reward (economic reward) should indicate clearly the recognition obtained in their infrastructure website. The rest of infrastructures receiving recognition are encouraged but not obliged to. For that purpose a seal and XIFI logo will be prepared for that purpose.
9 CONCLUSION

For effective development of the XIFI federation and use of FI technologies, a training programme must be created. For this programme to be sustainable, we must also create an associated community. Creating communities has been made possible in recent years through the use of collaboration tools and technologies. In the case of the "Training and Knowledge Transfer" work package of XIFI, we leverage as many of the tools of the project and the FIPPP to ensure integration with existing efforts.

In developing the training material, a set of source stakeholders have been identified and progression path toward target stakeholders outlined. This provides the initial training needs of those source stakeholders. Existing information was analysed to provide material that enables the knowledge necessary for those source stakeholders to develop the skills required to progress.

In order to incentivise the progression of high-value stakeholders, a recognition and reward programme is to be instantiated. This will follow the progression of stakeholders through the training programmes, their application of those skills and the delivery of value to the federation as a result.

Finally, a production process for training material has been created and the resulting material is being used in the training sessions being organised as part of the overall training programme. As the technical of XIFI progresses, the training programme will follow in close proximity to provide the next communities of FI technology users.
10 REFERENCES


APPENDIX A: FI-OPS INFRASTRUCTURE PROVIDER MANUAL

A.1 Introduction

This manual aims to cover topics relevant to an infrastructure owner and infrastructure operators looking to deploy, setup and integrate a new infrastructure into the XIFI federation and by extension provide services on FI-Lab.

Please note that the topics discussed in this manual are subject to change. It is recommended that you also reference the cited source documents online. A future point release will remove this message.

A.2 Core Concepts

In this section the authors highlight some of the main guidelines that should be taken into consideration to drive the building of XIFI.

XIFI as a community cloud: XIFI is a federation of resources offered to the FI-PPP developer community by FI infrastructures. FI-PPP developers themselves may contribute to the community cloud by offering additional hardware capacity (under their own control or open to other PPP participants) and their own services (the so called Specific Enablers).

XIFI as showcase for promotion of FI-PPP technologies for developers: XIFI is the natural showcase to promote FI-PPP results by hosting Generic Enablers, Specific Enablers and end user applications build on top of them, by interconnecting data and advanced services offered by FI infrastructures.

XIFI as opportunity for FI infrastructures to attract new communities of developers through FI-PPP services: XIFI aims at identifying, within the project lifetime, ways to ensure its sustainability. The natural way is to proof to infrastructure owners that, keeping alive the community cloud, will allow them to attract communities of developers beyond what they achieved so far. Of course this has several implications related to FI-PPP IPR handling that will be analysed within the XIFI project.

XIFI as validation and test of FI-WARE technologies in the field of Cloud Computing: XIFI can be regarded as an horizontal use case project that leverage on FI-WARE Generic Enablers to show how to build a largely distributed and federated cloud platform that offer FI-PPP technologies to developers. In this sense, it is very important to collaborate with FI-WARE (and the upcoming Technical Foundation project) to define our fine-grained architecture and to provide requirements back to FI-WARE.

XIFI as a flexible platform: the need to integrate and federate different existing infrastructures, demands for ability to tackle different needs raised by infrastructures for their integration, both at technical level, operational level and business level. The flexibility regards also the capacity: for example at the moment it is very difficult to forecast the needed resources (e.g. CPU cores, RAM, storage, network bandwidth) and XIFI should be ready to scale-up (this means also that software and hardware architecture should support that) with the growth of resource demands.

A.2.1 What is an infrastructure according to XIFI?

The authors used and will use the term infrastructure (and node as synonym) in different parts of this document and of XIFI documentation. Thus it is important to define what an infrastructure in our context is. In XIFI an infrastructure is any infrastructure that:

- offers capacity to host FI-WARE GE for building FI applications (compulsory). To offer capacity to host FI-WARE GE, the infrastructure should be able to host the Cloud Hosting GE offered by FI-WARE through which the other GE are provisioned. This means, in concrete terms, that the infrastructure should be equipped with a data center
• offers connectivity to Internet and GEANT network (compulsory). Connectivity to Internet allows developers and application end-users to access the services hosted on the infrastructure. This connectivity can be provided through different means (GEANT or other providers). XIFI, to leverage on EU FI facilities and to reduce the cost of connectivity, decided that the backbone network to allow XIFI nodes intra-communication is provided through GEANT

• offers additional capacities such as: sensing environment, advanced wireless connectivity, smart city datasets (would like). Future Internet developers may use such capacities to experiment GEs in real environments and on real data

• offers services to developers: support, backup, ... (would like). Infrastructure may offer additional operational services to enrich their offer. The absence of these services should not be conflicting with operation of XIFI federation[1]

• offers access to end-user communities (would like). Infrastructures may be well connected to communities of end-users that developers can leverage on to test and validate their applications

A.2.2 XIFI and stakeholders

The above discussion revolves around the two main stakeholders of XIFI:

Future Internet Developers (intended as IT professionals involved in the development of FI applications): application developers that want to leverage on FI-PPP technology platforms to develop innovative applications for so called Future Internet scenarios (e.g. smart mobility, smart energy, smart healthcare).

Future Internet Infrastructures: infrastructures offering capacity to host Future Internet applications and advanced hardware/services that can be used to support Future Internet application developers. As such Future Internet infrastructures are service hosting providers.

The two stakeholders have different objectives and needs that XIFI should be able to balance in building its offer. Nevertheless, the main objective of FI-PPP programme is to foster large adoption (and validation) of FI-PPP technologies. This requires a critical mass of developers (beyond FI-PPP Large Trials projects) to adopt GEs and SEs to build Future Internet applications. Thus it is crucial for the success of FI-PPP (and of XIFI) to attract as much as possible developers willing to use FI-PPP tools. This clearly gives to FI Developers a privileged position among stakeholders. XIFI should balance these two perspectives (the one of FI Infrastructures and the one of FI Developers) keeping into account as well FI-PPP general objectives.

Other relevant stakeholders in the picture are:

Future Internet Core Platform developers – which correspond to FIWARE (and the upcoming Technical Foundation project) developers, and that aim to offer the services (Generic Enablers) part of their platform to the Future Internet Developers.

Future Internet application sponsors and data providers – that support Future Internet Developers through financial and in-kind resources.

XIFI Consortium – that is in charge of the different operational and administrative activities to enable the provisioning of XIFI platform.

The stakeholders mentioned above may correspond to one or more role XIFI will take into consideration in the requirements analysis.

A.2.3 XIFI offer to developers and infrastructure owners

In this section the authors summarize some of the key elements of XIFI offer to developers and
infrastructures.

XIFI will offer to developers: a single entry point to access FI-PPP technologies and underlying advanced Future Internet infrastructures. Through this entry point:

The developer will be able to access GEs and SEs deployed on different infrastructures in a transparent way.

The developer will be able to manage shared and private resources under her/his control.

The developer will be able to transparently deploy FI-WAREGEs and her/his own SEs.

The developer will be able to acquire information on the different characteristics of the infrastructures, such as: advanced experimental services (e.g. sensor networks, smart energy grids), SLAs, usage term and conditions.

The developer will be able to create projects/experiments "encompassing" more than one site (infrastructure) in a transparent way.

The developer will have a single access point to monitor services he/she is using and platforms he/she deployed.

The developer will be supported in moving platforms he/she deployed from a location to another.

The developer will have access to tutorials for deploying FI-WARE GEs and its own SEs.

The developer will have access to the help desk granting Level 1 and Level 2 support.

XIFI will offer to infrastructure owners: a single entry point to publish their offer and access services meant for them. Through the single entry point:

The infrastructure owners will advertise: advanced experimental services (e.g. sensor networks, smart energy grids), SLAs, usage term and conditions.

The infrastructure owners will access to tutorials for: joining federation, deploying GEs, connecting GEs with their advances capabilities (e.g. sensor networks).

The infrastructure owners will access to the help desk granting Level 1 and Level 2 support for federation services and the installation process.

The infrastructure owners will deploy GEs to be made available in their datacenter.

A.2.4 XIFI Design Principles

In this section the authors highlight the most relevant design principles that have been followed in the definition of XIFI architecture and that should drive as well definition of single components of XIFI described in other technical deliverables. XIFI architecture defines a community cloud platform and as such it should adhere to canonical cloud computing design principles [2] and heterogeneous cloud deployment best practises [3]:

On-demand self service [2]. “A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider”

Broad network access [2]. “Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations)”.

Resource pooling [2]. “The provider’s computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but
may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth”.

Rapid elasticity [2]. “Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time”.

Measured service [2]. “Cloud systems automatically control and optimize resource usage by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service”.

User centric [3]. Well-designed services and user interfaces are key to deliver best user experience that will facilitate adoption of cloud services.

Simplicity [3]. The adoption of complex solutions may impact delivery time and the service quality. Dealing with heterogeneous environments may require complex solutions to automate some of the processes. Some processes may be kept to a manual mode in an initial phase for time-to-market, rather than designing with full functionality and for all IT services.

Reuse [3]. Cloud computing is nowadays a well-established field where a plethora of solutions are available off the shelves to be deployed to support the creation of cloud based infrastructures. Such solutions should be reused as much as possible to allow for a fast kick-start of cloud provisioning activities, unless there are strong reasons to develop a new solution. Within XIFI, we will aim at adoption of FI-PPP technologies to achieve our architecture and to reuse, where needed, complementary Open Source software and Open Standards. XIFI when extending software to align them with its requirements will contribute back to the communities that originated adopted software.

Service dependability [4]. Dependability is a fundamental characteristic of cloud computing platforms. Service availability is one of the key attributes for a service to be defined dependable. Service availability requires dealing with issues such as no single point of failure and scalability/elasticity mentioned above. While some of these features are not dependant on the provisioning platform, but rather on the services developed on top of the platform, in the design of Cloud provisioning platform service availability should be careful planned also taking into consideration derived costs [3]. XIFI architecture aims at delivery dependable services, with focus on availability, reliability, safety and transparency [21] attributes [4]. Services available in the single XIFI nodes, should be available regardless the availability of other nodes. Highly availability and reliability should be provided as well for management tools provided by XIFI platform. Integrity, maintainability and confidentiality should be guaranteed by the reuse of dependable cloud tools.

Flexibility. The requirements that XIFI will face may change over the time, as such XIFI architecture should be designed for adapting to new requirements. In this sense modularity and service orientation are fundamental principles to be considered to design XIFI architecture.

Compatibility. XIFI aims at bringing on board as nodes existing Future Internet infrastructures, as such it is important that the design of XIFI architecture keeps into consideration the continuity of their operational and business activities and that allows for integration of XIFI architecture on top of existing tools adopted by infrastructures (where this does not conflict with FI-PPP technology centric principle).

A.3 Network Setup

The most complex part of creating a XIFI site is the network deployment and configuration. The following guide is based on the experience of existing nodes.
A3.1 Network Configuration

In order to set up correctly the network, a good approach is to follow the OpenStack guidelines. OpenStack distinguishes four logical networks:

- Management network
- Data network
- External network
- API network

![OpenStack Networking Architecture](image)

Basically the first two are intended as “internal networks”. The former is used for management purpose and provides connection between OpenStack components. The latter is used for VM data communication. These networks should have IP addresses reachable only within data centre. As stated in OpenStack Operations Guide[4], the recommended option is to use a management network with separate switch and separate NICs: “this segregation prevents system administration and monitoring system access from being disrupted by traffic generated by the guests themselves”. The external network and the API network are intended as “public networks” because they allow inbound connections: the IP addresses should be reachable by anyone on the Internet. In particularly the external network is used to provide both VMs inbound and outbound connection from VMs, whereas the API network exposes all OpenStack APIs to tenants. These networks can be merged into a single network. If it is not possible to have physically separated networks, i.e. different switches and NICs for different networks, is possible to use VLANs to segregate network data. In this case the switch must be configured accordingly (the configuration steps are different for different networks). For instance, assuming nodes with at least 3 NICs, we can use the interfaces as follow:

- eth0: Management Network
- eth1: External/API Network
- eth2: Data Network
Each interface must be configured with the correct(s) VLAN(s) ID: in this way is possible to create logical separated networks.

### A3.2 Géant

This section describes the MD-VPN Multi-domain GÉANT Service found in [5]. The GN3plus Multi-Domain Virtual Private Network (MD-VPN) service will deliver seamless private interconnection of two or more networks across multiple network domains such as GÉANT and the NREN backbones. The MD-VPN service is able to deliver L2-VPN (point-to-point) and L3-VPN (multi-point) across multiple network domains. This allows the users of the IPv4/IPv6 and/or layer 2 networks to work as if their networks are coupled together. The use of a VPN improves end-user performance, security, and facilitates the use of private IP addresses, RFC 1918[6], across the distributed user environment.

A typical scenario would be one where an organisation seeks to connect a number of sites from different physical locations as if they were in the same physical location, to enable the organization to access remote resources with the same level of security. This security improvement enables high network performance by avoiding deep firewall inspection, such as the case with standard IP.

Figure A illustrates how the NRENs are connected together to provide the MD-VPN service. The service is offered collaboratively by GÉANT and a set of adjacent NREN domains that adhere to the service. These joint networks form the multi-domain area where the service is provided (this is known as the "GÉANT service area."). The MD-VPN service guarantees that the data of VPN1 users cannot be delivered to sites outside VPN1, and that sites or machines outside VPN1 are unable to connect to machines that are in VPN1. This is achieved by isolating the MD-VPN customer data flows from any other traffic, standard IP traffic and traffic of other MDVPN customers.

![Figure 11 - The Multi Domain VPN](image)

The multiple networks forming the MD-VPN service peer VPN information at the borders between NREN networks. These peering points are referred to as Service Stitching Points (SSPs) in Figure A. The Service Demarcation Points (SDPs) are the end points where the service is terminated for the end users of the MD-VPN service. These points are located at the interfaces of Provider Edge (PE) devices found at the NREN end of the site access link, which forms the edge of the federated MD-VPN service.
The MD-VPN service is based on the VPN transport service, provided by the GÉANT network, which allows transporting all the multi-domain VPNs set-up within MP-VPN service from one domain (NREN) to another domain. In fact GÉANT provides a Carrier of Carriers (CoC) VPN to connect the NREN resources together, with each NREN-GÉANT BGP-labelled unicast peering session being established as an ABR-PE session between the respective routers. Simply, the NREN network will function as a CoC VPN end user. This approach introduces a hierarchy and maintains great network flexibility and a peer model in NREN cooperation. The main goal of using BGP labelled-unicast protocol for the MD-VPN service is the distribution of routes and MPLS labels for all PE routers in all domains used to provide services for end users. BGP also introduces high scalability and robust solutions such as Route Reflectors, denoted by RR in Figure A.

For NRENs that do not support MPLS switching on the SSPs, the VPNs from those NRENs must be stitched to the service in back-to-back mode (Option A RFC 4364). This means that on the SSP, each VPN that a NREN would like to transport has to have its own sub-interface identified with a service delimiter (e.g. VLAN ID). The traffic and signalling for a particular VPN is exchanged over this sub-interface, and typically in the case of L3-VPN, a standard BGP protocol with VPN extension will be enabled for each VPN instance.

A VPN proxy system is defined in the GÉANT network that will provide access to the Carrier of Carriers VPN. This allows GÉANT to provide MD-VPN services for end users directly connected to the GÉANT network or to connect NRENs that do not support MPLS and BGP labelled unicast.

### A.4  Hardware Deployment

Based on [7], we’ve gathered the models of hardware deployment for use in different scenarios.

#### A4.1  Deployment Architecture Reference Model

This section discusses the reference model for the physical and software deployment of a XIFI node based on OpenStack Grizzly, FI-WARE add-ons and XIFI tools. It is important to understand that there is no one model fits all, since the deployment architecture depends on, and is heavily related to resources available in an infrastructure. Dealing with existing infrastructures that connect to the federation has the impact that the deployment architecture must be adapted according to the existing hardware and to the planned upgrade of the infrastructure.

The following text is largely inspired by best practices in the deployment and operations of OpenStack based-clouds [8][9].

#### A4.1.1  Concepts

##### A4.1.1.1  Physical Equipment

In the deployment of a cloud-based data centre we deal with interconnected physical equipment that composes the physical architecture of the data centre. The most important equipment types for the definition of the deployment architecture are:

- **Rack**: Modern servers and network equipment are designed to be installed in a framework called a rack. A rack contains multiple mounting slots called bays, each designed to hold a hardware unit. Hardware may occupy more than one unit. Recent evolution for high-density servers, introduces blade servers that are hosted in a blade (which allows packing several hardware component in a blade enclosure). Blade enclosures are mounted within racks.

- **Server**: A server is a node in the data centre (usually hosted in a rack) that offers computation and storage capacities. A server node in a cloud-based data centre may have different role according to his hardware configuration, and hence being able to host different services (that correspond to a given role). Generally speaking, server equipped with large number of CPUs...
and RAM are more efficient for computational tasks, while server equipped with large amount of hard drives are more efficient for storage tasks. This discussion will become clearer in the next paragraphs that discuss node roles in an OpenStack based-cloud.

- **Switch**: Hardware equipment that allows the physical interconnection of different server nodes. Like a server, a switch may have different roles according to the network services it provides (e.g. management network or data network).

### A4.1.1.2 Node Roles

In a cloud environment, servers usually have different roles. In the following discussion we take into consideration roles usually adopted in OpenStack deployments. These roles are:

- **Controller (node)**. A controller node provides the central management for multi-node OpenStack deployments.
- **Compute (node)**. A compute node provides the computational capacity (i.e. virtual machines) to OpenStack deployments.
- **Block storage (node)**. A block storage node provides non ephemeral storage for virtual machines.
- **Object storage (node)**. An object storage node provides access to large storage solutions via Web APIs.
- **Object proxy (node)**. A proxy that distribute the objects to different storage nodes according to replica settings and region availability settings.
- **Network management (node)**. A network management node provides (dynamic) configuration on the VLANs that interconnect the VMs.

Furthermore XIFI will consider the following roles:

- **Load balancer (node)**. A node that in high-availability configurations, provides load balancing of requests among the available redundant services.
- **Monitor (node)**. A monitor node provides monitoring of resources included in a XIFI node.
- **Deployment (node)**. A deployment node provides the ability to control the deployment of a XIFI node, including a monitor node and all other nodes needed to run OpenStack and FI-WARE extensions.

It is important to underline that a node may serve different roles according to the OpenStack services it runs. Given the difference of type of service, different roles may perform better on different type of hardware. Accordingly, certain roles should not be covered by the same machine in a well-designed cloud deployment. In the next paragraphs we discuss quickly the different services. The distribution of services on actual nodes defines the role of a node and the architecture of the OpenStack deployment, according to the type of configuration of the services.

### A4.1.1.3 OpenStack Services

The XIFI installation of OpenStack considers the following services distributed on the nodes [10]:

- **Nova** [11]: Provides the management of computational resources. It includes three basic services: the scheduler, to define where the VM will be allocated, an API to remotely control the scheduler, the compute service that actually provides the VM on the single nodes and other support services.

- **Neutron** [12]: Provides network management for OpenStack. It includes the following services: server to manage the network as service functionality for Nova, agent to apply the configuration of the single nodes, DHCP-agent to automatically assign IPs to VMs, and other services. It requires specific plugins to configure the different network apparatus (e.g. OpenVSwitch [13]).
Glance[^14]: provides image management for OpenStack. It includes the following services: a registry that provides a catalogue of available VM templates and an API to control the services. Different back end are available for glance[^15].

Keystone[^16]: provides identity and service registry functionalities.

Cinder[^17]: provides block storage (i.e. volumes) functionalities for OpenStack. It includes three basic services: the scheduler to define where the volume will be stored, an API to remotely control the scheduler, and the volume service that actually provides the storage;

Swift[^18]: provides object storage functionalities. It includes the following services: the proxy to accept API requests and to route them to storage services, the object storage that take care of the actual storage.

Horizon[^19]: provides a graphical user interface to support management and self-provisioning of cloud resources for the services mentioned above.

### A4.1.1.4 Network Services

As mentioned above, Neutron requires an actual plugin to be able to configure switches and creating VLANs in an OpenStack cluster.

**DOVE**: The reference plugin for XIFI is a customized version of IBM’s Distributed Overlay Virtual Ethernet (DOVE), provided by FI-WARE. DOVE is an SDN management solution for data centres that allows traffic shaping inside the data centre. It is based on OpenVSwitch.

**OpenVSwitch**: as an alternative; we foresee the adoption of the standard version of OpenVSwitch.

Other network services are required to support the inter-node XIFI connectivity. These are currently under development. More details will be provided in the next version of this guide.

### A4.1.1.5 Other Services

XIFI deployment will require other services:

**HAProxy**: to provide load balancing across OpenStack and FI-WARE APIs in the high-availability configuration.

**XIFI Monitoring Management Middleware**: a middleware that is currently under development in XIFI to integrate physical and virtual infrastructure monitoring data collected from the nodes. The XIFI Monitoring Management Middleware provides adapter mechanisms for monitoring tools adopted by infrastructures (e.g. OpenNMS[^20], Perfsonar[^21]).

### A4.1.2 Physical Deployment Models

The physical architecture of a node influences the software architecture and QoS characteristics such as availability of services. Servers are usually hosted in racks and if all servers, for example, playing the role of a controller are in the same rack and power to the rack is interrupted, the cluster may not be available externally even though other services may be still running in other racks. Similar issues apply in case of switches. Therefore when possible, it is better to plan the physical architecture without a single point of failure.

### A4.1.2.1 Basic Physical Deployment

In a basic physical deployment, resources are not redundant and are not made resilient. In the simplest case, we will have a rack (or more racks) with a single power source that will power all servers part of the node including the switches that connect the servers. In the simplest configuration this requires:

- 1 controller node
• 3+ compute nodes
• 1 manager node
• 1 switch 24 port (OpenFlow enabled)
• Optionally, we can include as well:
• 3+ object storage nodes

Such flat configuration is not recommended for production nodes, unless high-availability deployment cannot be achieved. Production nodes should refer to the high-availability deployment. Corresponding service architecture deployment is discussed separately.
Figure 12 - Basic Physical Deployment
<table>
<thead>
<tr>
<th>Node Type</th>
<th>Recommended Hardware</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controller</td>
<td>Processor: quad core</td>
<td>More disk space is required if you do not plan to deploy an object storage or other storage backend to act as back end for the VM registry (2TB). RAID configuration is suggested to increase controller reliability. See [22] and [23].</td>
</tr>
<tr>
<td></td>
<td>Memory: 8 GB RAM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Disk space: 1TB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Network: one 1 GB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Network Interface Card (NIC)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Processor: 16 or 32 cores</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Memory: 64 GB RAM or 128 GB RAM</td>
<td>If you adopt a 16 core server, you should have 6+ servers.</td>
</tr>
<tr>
<td></td>
<td>Disk space: 2 TB</td>
<td>RAID configuration can be used but it is not recommended. The disk space, unless you have also a SAN in your data centre, will be as well used for block storage services (volumes) in shared modality. See [22] and [24].</td>
</tr>
<tr>
<td></td>
<td>Network: 2x1 GB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Network Interface Card (NIC)</td>
<td></td>
</tr>
<tr>
<td>Object Storage</td>
<td>Processor: quad core</td>
<td>RAID configuration is highly discouraged. See [25].</td>
</tr>
<tr>
<td></td>
<td>Memory: 8 GB RAM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Disk space: optimized for cost per GB (at least 4TB per node)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Network: one 1 GB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Network Interface Card (NIC)</td>
<td></td>
</tr>
</tbody>
</table>

Table 14 - Hardware Recommendation for basic physical deployment

A4.1.2.2 High Availability Physical Deployment

In a high availability physical deployment, resources are redundant and they are located to be resilient. The objective of high availability deployment is to minimize:

- System downtime — the unavailability of a user-facing service beyond a specified maximum amount of time, and
- Data loss — the accidental deletion or destruction of data.

To avoid system downtime and data loss it is important to avoid the presence of single point of failure. Either in the hardware or in the software. In this section we highlight the deployment from the hardware perspective.

We assume to have two (or more) racks where the nodes are replicated with separate line power supply. This will ensure that if a power line will go down and hence turn off a rack, the second power line will be still accessible. As better alternative it is possible to consider single racks with support for 2 independent power lines. In this case all equipment in the rack should be equipped with 2 power supply units attached to the 2 power lines of the rack. This reference configuration requires:

- 2+ controller node
- 6+ number of compute nodes
- 3+ object storage nodes
- switch 24 port 1GB and 10GB up-link (OpenFlow enabled)
- 1 manager node (also a laptop may do the work)

This reference configuration is the recommended one for XIFI nodes. Tweaks may be applied according to specificity of XIFI nodes.
Figure 13 - High availability physical deployment
Services are discussed separately in the service architecture section.

<table>
<thead>
<tr>
<th>Node Type</th>
<th>Recommended Hardware</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controller</td>
<td>Processor: 4 or 8 core Memory: 12 GB RAM Disk space: 1TB Network: 2 x 1 GB Network Interface Card (NIC)</td>
<td>More disk space is required if you do not plan to deploy an object storage or other storage backend to act as back end for the VM registry (2TB). RAID configuration is suggested to increase controller reliability. See [22] and [23].</td>
</tr>
<tr>
<td>Compute</td>
<td>Processor: 16 or 32 cores Memory: 64 GB RAM or 128 GB RAM Disk space: 2 TB Network: 2x1 GB Network Interface Card (NIC)</td>
<td>If you adopt a 16 core server, you should have 12+ servers. RAID configuration can be used but it is not recommended. The disk space, unless you have also a SAN in your data centre, will be as well used for block storage services (volumes) in shared modality. See [22] and [24].</td>
</tr>
<tr>
<td>Object Storage</td>
<td>Processor: quad core Memory: 8 GB RAM Disk space: optimized for cost per GB (at least 4TB per node) Network: 2 x 1 GB Network Interface Card (NIC)</td>
<td>RAID configuration is highly discouraged. See [23].</td>
</tr>
</tbody>
</table>

*Table 15 - Hardware recommendations for High Availability physical deployments*

**A4.1.3 Services Architecture Deployment Models**

In the previous section we discussed the physical deployment and listed the nodes type needed for that. But we didn't enter in any details regarding the services to be deployed on the nodes. Depending on the selected architecture, the different nodes will support different roles[9].

**A4.1.3.1 Basic Architecture**

In the basic deployment services are not configured in high-availability. In this section we details which services are supposed to run on the different nodes discussed in the section #Basic Physical Deployment. It is important to underline that we foresee the computational node to cover as well the block-storage node role through the set-up of a shared file system (e.g. NFS). Also, we foresee the installation of XIFI specific services on the controller node, if the node offers enough capacity to run them.

The controller node will host all the services related to the management of the XIFI node. The services include:

- The nova-scheduler service, that allocates VMs on the compute nodes.
- The cinder-scheduler service, that allocates block storage on the compute nodes.
• The glance-registry service that manages the images and VM templates. The backend for the registry maybe the controller node, or the Object Storage if included in the deployment architecture.

• The neutron-server service that manages the VM networks.

• The swift-proxy service (optional) that manages request to the object storage nodes.

• The nova-api service, that exposes the APIs to interact with the nova-scheduler.

• The cinder-api service, that exposes the APIs to interact with the cinder-scheduler.

• The glance-api service, that exposes the APIs to interact with the glance-registry. If the object storage nodes are deployed, we recommend their usage as back-end for glance [15].

• The keystone service that manages OpenStack services in a node.

• The horizon service, that provides a dashboard for the management of OpenStack in a node.

• The IdM GE service, that provides identity management for users.

• The SLM GE service, that provides scalability and elasticity management. it is connected the SOM GE service, hosted in the Main XIFI node.

• The XIFI-MMM service, that collects monitoring data for physical appliances.

• The DCRM GEs is not listed as it is essentially a plugin to nova-scheduler and neutron.

• The compute node will host all the services related to the provisioning of VMs and block storage. The services include:

  • The nova-compute service that manages VMs on the local node.

  • The cinder-volume service that manages block storage on the local node.

  • The neutron-agent service that manages VM networks on the local node.

• The object storage node (optional) will host all the services related to the provisioning of object storage. The services include:

  • The swift-account-server service, that handles listing of containers.

  • The swift-container-server service, that handles listing of stored objects.

  • The swift-object-server service, that provides actual object storage capability.
In the high availability services are redundant and they are located to be resilient. In this section we details which services are supposed to run on the different nodes discussed in the section #High Availability Physical Deployment. In this section we discuss the deployment from the software perspective. The deployment, except the injection of services to support high-availability of the controllers (the other are in high-availability modality by default so to say), is very similar to the basic one. In fact in OpenStack, computational, block storage and object storage nodes, are handled by the different scheduler to provide high-availability. The issue is to guarantee high-availability as well to the controller.

Generally speaking, high-availability can be provided in two modalities:

- active/passive: in this configuration, a main controller operates the resources and in case of a problem, it switches the request to a backup controller.
- active/active: in this configuration, a number of controller operates the resources at the same time, in case of a problem to a controller instance, requests are not issued anymore to that node.

In this paragraph we refer to the active/active configuration.

The controller node will host, additionally to the services mentioned in the previous section, the services needed to ensure the high-availability of the controller node:

- ha-proxy service, that provides load balancing across OpenStack and FI-WARE APIs in the high-availability configuration.
- pacemaker service [26], that provides high-availability for neutron and other services.
- galera service [27], that provides high availability for databases used by the different services.
- RabbitMQ service, present as well in the basic deployment, should be configured for high-

![Figure 14 - Service per node in the basic architecture deployment model](image-url)
availability policy support.

More information is available in [28]

A4.1.3.3 Block Storage Configuration

Different modalities to run block storage services are possible in OpenStack refer to [9] [29] for a complete discussion. In this section we refer to the default configuration selected for XIFI, that relies on shared file system across the compute nodes. In this configuration, each compute node has a large storage capacity that is share through a distributed file system that allows the disks of the different compute node to be seen as a single drive. This configuration allows for high scalability and easy live-migration and does not require for dedicated nodes to the block storage. Of course, the solution may have drawbacks such as high network i/o in case the block is accessed from a remote virtual machine instead than locally. The default shared file system solution foreseen in XIFI is NFS.

A5 Software Deployment

A5.1 IT Box

The ITBox supports the automated installation of the main components of a XIFI node. The download version and some configuration parameters will be provided by the portal, following the registration of the new node. Monitoring and network adapters will be included (or linked) in the ITBox distribution from the adapters repository, while the same applies to GEs and related software needed to complete the XIFI node installation.

A5.1.1 Installation Manual

ITBox is distributed as an ISO image which contains an installer for ITBox Master Server. The ISO can be installed in the same way, using a virtualization software package, such as VirtualBox, or a
bare-metal server. The first solution is suggested for testing scopes, whereas the second solution is suggested for production environment.

Suggested minimum hardware requirements for installation in testing environment:

- Dual-core CPU
- 2+ GB RAM
- 1 gigabit network port
- HDD 80 GB with dynamic disk expansion

Suggested minimum hardware requirements for installation in production environment:

- Quad-core CPU
- 4+ GB RAM
- 1 gigabit network port
- HDD 128+ GB

Once the Master server is installed, all other servers can be powered on, and the user can login into the ITBox UI using the default address http://10.20.0.2:8000/, or he can start using the command line interface [7]. The cluster’s servers will be booted in bootstrap mode (CentOS based Linux in memory) via PXE. Thus, these servers will be seen by the system as “discovered”, and user will see notifications in the user interface. At this point the user can create an environment, add servers into it and start with the configuration.

A5.1.1.1 How to update ITBox to the latest version

If you would update your ITBox node to the latest version, you can install the new version and migrate the production nailgun database instance.

The main steps are:

- `pg_dump --c -h 127.0.0.1 -U nailgun nailgun > outfile.sql` with password nailgun (on the old ITBox installation)
- `psql -d nailgun -U nailgun < outfile.sql` with password nailgun (on the new ITBox installation)

Note: it is possible that the system may show the following error message: “FATAL: Ident authentication failed for user “. To fix this error open /var/lib/pgsql/data/pg_hba.conf file and in local section change as follows:

```
local all all md5
```

Finally, restart the database (/etc/init.d/postgresql restart)

You can find the PostgreSQL’s official documentation at the url [http://www.postgresql.org/docs/8.4/static/backup-dump.html][8]

A5.1.2 User Manual

When the user has completed the master node installation, he can access ITBox UI, visiting the default url [http://10.20.0.2:8000/](http://10.20.0.2:8000/) (Fig. 3).
The user sets bare-metal servers to boot from network via PXE and power them on. They will start automatically with a bootstrap operating system, based on Centos. The ITBox will notify discovered nodes on ITBox UI (see Fig. 3 in the upper right corner). At this moment, the user could create a new environment.

The first step that involves the user is the “New OpenStack Environment” creation (Fig. 4), where the user inserts such basic information about the environment as name, operating system, deployment...
mode (multi-node or multi-node with High Availability), hypervisor, DCRM GE with Pivot or Pulsar scheduler and network manager (Nova-Network, Neutron with GRE, Neutron with VLAN).

The DCRM GE installation (Fig. 5) is a XIFI specific feature. If the user selects a DCRM GE scheduler, the ITBox will install all necessary packages and configure Pivot or Pulsar scheduler. If the user skips this step, then the ITBox will install the FilterScheduler as default.

---

**Figure 18 - DCRM install options**

Now the environment is ready for deployment.

---

**Figure 19 - Final creation step**
In environment creation process the user should define the architecture of his cloud infrastructure. The user assigns the role to every server, configures the network and defines the space allocated to hard disks and settings other OpenStack options (Fig.21).
Giving roles to servers

In “Nodes” tab, the user can view the state of his environment, where the nodes are ordered by Roles. Thus, the user can view the node’s details and configure them appropriately.

By clicking on “Add Nodes” button, the ITBox shows users the list of available roles and the list of unallocated nodes. After selecting a role, other incompatible roles are automatically disabled. For example, a controller node cannot be together with a compute node simultaneously, and so on.

Finally the user applies changes (Fig. 22).
When the changes are applied, it is possible to tune the node, by clicking on the right button indicated by the gear icon. The ITBox shows a dialog where the user can configure network interfaces, defines
the space allocated to hard disks and views server information (e.g. Service tag, Mac addresses, hardware specifications, etc.) (Fig.22, 23, 24).

![Network interface configurations](image1)

**Figure 23 - Network interface configurations**

![Hard disk configuration](image2)

**Figure 24 - Hard disk configuration**
Network settings

In the Network section, the user can manage configuration parameters. Based on the OpenStack network architecture, ITBox considers three networks: Public, Management and Storage. Management and Storage sections indicate the network subnet in CIDR notation and VLAN tags, whereas the Public section allows to set the IPs pool and its VLAN tag (Fig. 26).
Figure 26 - Infrastructure network settings

The ITBox gives user the opportunity to manage the Neutron plugin and to define the L2 connection tunnel ID range and the L3 floating IP range. Furthermore, the user can verify the network configuration by clicking the “Verify Network” button, which checks for connectivity between nodes using the configured VLANs. It also checks if some external DHCP interferes with the current deployment (Fig. 27).
General Settings

The "Settings" tab contains options useful to manage the current environment. For example, the user can change the OpenStack admin account or can change the hypervisor type or the scheduler driver. To make variations permanently it is necessary re-deploy the changes. (Fig. 26, 27).
Figure 28 - Infrastructure settings (monitoring, admin account, common)
Logs
The log section is designed to monitor the state of installation and support the troubleshooting. The user can select the node to monitoring, the log level and the generator source.

Health Check
It is very useful, running a post deployment test, to see if the installation process is correctly finished. The Health check process runs a set of tests, and when it is done, the user will see green Thumbs Up sign if it was correct and a red Thumbs Down sign if something went wrong (Fig. 30).
Start deploy  When the user has finished setting the environment, he can start the deployment process, clicking on "Deploy changes" button (Fig. 31).
A5.2 DCA

The Deployment and Configuration Adapter (DCA) is the XIFI component that caters for the enhanced deployment functionality, as needed by the project users forming in parallel a Deployment Registry. Briefly the DCA provides:

Deployment of multiple GEs and XiFi components upon XiFi infrastructure The DCA supports the deployment and configuration of multiple GEs in a batch mode (as images, through recipes or in a combination), allowing the user to select details (including the sequential or parallel deployment and the notification capabilities). Such multi-GE deployment can take place in a single node or upon federated XiFi nodes. The DCA can also be used to deploy XiFi components upon the infrastructure.

Check of Available Resources prior to the Deployment The DCA performs check on the resources that are available to the user, prior to the deployment of one or multiple GEs and according to the documented hardware requirements of the GEs. This functionality can protect the user from receiving errors (by the platform) after invoking the deployment procedure. The resource availability check is performed considering the user’s quota upon the XiFi infrastructure, the resources that have been already reserved by the user and the hardware needs of the GEs under deployment (currently quantified in CPU cores, memory and storage). The checks can be performed per node and / or federated nodes.

Persistency of information related to the deployed GE instances The DCA holds all pertinent information from the whole lifecycle of GE deployment. This includes the requests on behalf of the users (through the portal) and the system responses as related to the GE instances (going well beyond the typical awareness of the VM instances). This information is adapted and then exposed upon request to the components of WP4, through a set of meaningful queries.
A5.2.1 Installation Manual

This section provides a step-by-step guide for the installation and configuration of the required software components in order to setup the DCA component in a particular node in XIFI federation.

In particular, guided manuals are foreseen for:

- installation and configuration of Apache Tomcat,
- installation and configuration of MySQL Server,
- installation of the DCA binaries.

Further, configuration instructions are given for all the aforementioned software components.

Prerequisites

For the node that will accommodate the DCA (XiFi federation platform):

- CentOS (6.2 and above) is already installed
- Oracle Java Runtime Environment (1.7.0 and above) is already installed
- Apache Tomcat (7.0.35 and above)

The cloud-hosting Generic Enablers (GEs) that support the deployment and configuration of the GEs. Namely the PaaS Manager and the SDC.

A persistency server (DCA currently tested with MySQL DB Server)

For the Infrastructure Node:

The DCRM GE or OpenStack Grizzly

Installation steps:

First of all, verify that the right version of Oracle Java has been installed:

```
[root@dca ~]# java -version
java version "1.7.0_45" Java(TM) SE Runtime Environment (build 1.7.0_45-b18) Java HotSpot(TM) 64-Bit Server VM (build 24.45-b08, mixed mode)
```

Then, install Apache Tomcat as follows:

```
[root@dca ~]# cd /opt
[root@dca opt]# wget http://archive.apache.org/dist/tomcat/tomcat-7/v7.0.41/bin/apache-tomcat-7.0.41.tar.gz
[root@dca opt]# tar xzf apache-tomcat-7.0.41.tar.gz
[root@dca opt]# ./apache-tomcat-7.0.41/bin/startup.sh
```

Tomcat should be up and running. Optionally, you may want to redirect the traffic of port 8080 to port 80 using the following iptables rule:

```
[root@dca opt]# iptables -t nat -A PREROUTING -p tcp --dport 8080 -j REDIRECT --to-port 80
[root@dca opt]# iptables -I INPUT -p tcp --dport 8080 -j ACCEPT
[root@dca opt]# service iptables save
[root@dca opt]# service iptables restart
```

Upon successfully installing Apache Tomcat, MySQL server and the respective Java JDBC connector should be also installed by issuing the following commands:

```
[root@dca opt]# yum install mysql-server mysql-connector-java
[root@dca opt]# chkconfig --levels 235 mysql on
[root@dca opt]# service mysqld start
```

Next, place the database creation script (dca.sql) in the root directory (/root) and issue the following commands:

```
[root@dca opt]# cd ~ [root@dca ~]# mysql -uroot -p < dca.sql
```
Next, the DCA binaries (dca.war) should be uploaded to the webapps directory of the Apache Tomcat installation (in the context of the present installation guide, this should be /opt/apache-tomcat-7.0.41/webapps). Apache Tomcat should then automatically deploy the war file and extract its contents under the webapps directory. In order to enable transactions, one should initialize a keystone instance into the DCA platform. Supposing that the DCRM instance of the datacenter operator advertises its identity service at the URL http://hostname.example.com/keystone/v2.0 and is located in a region identified as A REGION, then, the following command should be issued:

```
curl http://<dca-server-ip>/dca/addEndpoint -X POST -H "Content-Type: application/json" \   -d '{region:"A Region", url:"http://hostname.example.com/keystone/v2.0"}'
```

The answer of the DCA server is the following:

```
{url:"http://hostname.example.com/keystone/v2.0", region:"A Region"}
```

### A5.2.2 User Manual

The user manual describes the requests and responses of the methods currently offered by the DCA (version 1.0). The interaction has been performed using two trial accounts in the FI-WARE infrastructure (one in lab.fi-ware.eu and one in testbed.fi-ware.eu, regions RegionOne and RegionTwo, respectively), as well as a local (deployed in SYNELIXIS) OpenStack environment (RegionThree). This means that many of the (proprietary) fields are currently blank (appearing as having null values).

#### List flavors

We request the flavors available in RegionThree. Request

```
curl http://localhost:8080/dca/flavors?region=RegionThree
```

Response

The available flavours are retrieved (tiny, small, medium).

```
{
    "flavors": [
        {
            "id": "1",
            "name": "m1.tiny",
            "vcpus": "1",
            "ram": 512,
            "disk": "0",
            "swap": "",
            "links": [
                {"rel": "self",
                 "href": "http://cloud.lab.fi-ware.eu:8774/v2/0000000000000000000000000000001807/flavors/1",
                 "type": null},
                {"rel": "bookmark",
                 "href": "http://cloud.lab.fi-ware.eu:8774/v2/0000000000000000000000000000001807/flavors/1",
                 "type": null}
            ],
            "public": null,
            "OS-FLV-EXT-DATA:ephemeral": 0,
            "rxtx_factor": 1.0,
            "OS-FLV-DISABLED:disabled": null,
            "rxtx_quota": null,
            "rxtx_cap": null,
            "os-flavor-access:is_public": null
        },
        {
            "id": "2",
            "name": "m1.small",
            "vcpus": "1",
            "ram": 2048,
            "disk": "10",
            "swap": "",
            "links": [
                {"rel": "self",
                 "href": "http://cloud.lab.fi-ware.eu:8774/v2/0000000000000000000000000000001807/flavors/2",
                 "type": null},
                {"rel": "bookmark",
                 "href": "http://cloud.lab.fi-ware.eu:8774/v2/0000000000000000000000000000001807/flavors/2",
                 "type": null}
            ],
            "public": null,
            "OS-FLV-EXT-DATA:ephemeral": 20,
            "rxtx_factor": 1.0,
            "OS-FLV-DISABLED:disabled": null,
            "rxtx_quota": null,
            "rxtx_cap": null,
            "os-flavor-access:is_public": null
        },
        {
            "id": "3",
            "name": "m1.medium",
            "vcpus": "2",
            "ram": 4096,
            "disk": "10",
            "swap": "",
            "links": [
                {"rel": "self",
                 "href": "http://cloud.lab.fi-ware.eu:8774/v2/0000000000000000000000000000001807/flavors/3",
                 "type": null},
                {"rel": "bookmark",
                 "href": "http://cloud.lab.fi-ware.eu:8774/v2/0000000000000000000000000000001807/flavors/3",
                 "type": null}
            ],
            "public": null,
            "OS-FLV-EXT-DATA:ephemeral": 60,
            "rxtx_factor": 1.0,
            "OS-FLV-DISABLED:disabled": null,
            "rxtx_quota": null,
            "rxtx_cap": null,
            "os-flavor-access:is_public": null
        }
    ]
}
```
List the Keypairs

We request the user keypairs on RegionThree.

Request

curl http://localhost:8080/dca/keypairs?region=RegionThree

Response

The response is retrieved.

```
{  "keypairs": [       {          "name": "panos",          "fingerprint": "22:ec:58:0a:c5:f5:c6:d4:7b:91:64:26:5f:17:e9:8b",          "user_id": null,          "public_key": "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAgQDBgi/eZqP7IKqygkvTn2pkr1Pn3LKg57SU8jyRQnxMq37 fG6R2UtF7SzaJa01nQTQvFhfuRwXs/9eYQ2CDZ2BcF0qQFrq6p2CyhgYzMNev4xXtiz35fUFXGq SjsvUb-yrR66bsH1b30aXlKhhg4FQH41GQHDeVQEBgCyagYQPuP== nova@gcsic001.ifca.esn",          "private_key": null } ] }
```

List the Security Groups Request

The security groups available to the user on RegionThree are requested.

```
curl http://localhost:8080/dca/securitygroups?region=RegionThree
```

Response

The security groups are retrieved.

```
{    "security_groups": [       {          "id": 2372,          "name": "context_broker",          "description": "context broker security group",          "rules": [             {                "id": 4211,                "name": null,                "group": {                   "name": null,                   "tenant_id": null                },                "parent_group_id": 2372,                "from_port": 1026,                "to_port": 1026,                "ip_protocol": "tcp",                "ip_range": {                   "cidr": "0.0.0.0/0"                }            },             {                "id": 4212,                "name": null,                "group": {                   "name": null,                   "tenant_id": null                },                "parent_group_id": 2372,                "from_port": 0,                "to_port": 8,                "ip_protocol": "icmp",                "ip_range": {                   "cidr": "0.0.0.0/0"                }            },             {                "id": 4213,                "name": null,                "group": {                   "name": null,                   "tenant_id": null                },                "parent_group_id": 2372,                "from_port": 0,                "to_port": 0,                "ip_protocol": "icmp",                "ip_range": {                   "cidr": "0.0.0.0/0"                }            },             {                "id": 4214,                "name": null,                "group": {                   "name": null,                   "tenant_id": null                },                "parent_group_id": 2372,                "from_port": 0,                "to_port": 0,                "ip_protocol": "icmp",                "ip_range": {                   "cidr": "0.0.0.0/0"                }            } ],          "links": null,          "tenant_id": "000000000000000000000000000000001807"        },       {          "id": 2078,          "name": "default",          "description": "default",          "rules": [             {                "id": 3425,                "name": null,                "group": {                   "name": null,                   "tenant_id": null                },                "parent_group_id": 2078,                "from_port": 22,                "to_port": 22,                "ip_protocol": "tcp",                "ip_range": {                   "cidr": "0.0.0.0/0"                }            },             {                "id": 2079,                "name": null,                "group": {                   "name": null,                   "tenant_id": null                },                "parent_group_id": 2078,                "from_port": 22,                "to_port": 22,                "ip_protocol": "tcp",                "ip_range": {                   "cidr": "0.0.0.0/0"                }            } ],          "links": null,          "tenant_id": "000000000000000000000000000000001807"        },       {          "id": 2078,          "name": "default",          "description": "default",          "rules": [             {                "id": 3425,                "name": null,                "group": {                   "name": null,                   "tenant_id": null                },                "parent_group_id": 2078,                "from_port": 22,                "to_port": 22,                "ip_protocol": "tcp",                "ip_range": {                   "cidr": "0.0.0.0/0"                }            },             {                "id": 2079,                "name": null,                "group": {                   "name": null,                   "tenant_id": null                },                "parent_group_id": 2078,                "from_port": 22,                "to_port": 22,                "ip_protocol": "tcp",                "ip_range": {                   "cidr": "0.0.0.0/0"                }            } ],          "links": null,          "tenant_id": "000000000000000000000000000000001807"        }    ] }
```
"description" : "For FIWARE monitoring",
"rules": [
  {
    "id": 4137,
    "name": null,
    "group": {
      "tenant_id": null
    },
    "parent_group_id": 2079,
    "from_port": 1026,
    "to_port": 1026,
    "ip_protocol": "tcp",
    "ip_range": {
      "cidr": "0.0.0.0/0"
    }
  },
  {
    "id": 4141,
    "name": null,
    "group": {
      "tenant_id": null
    },
    "parent_group_id": 2079,
    "from_port": 80,
    "to_port": 80,
    "ip_protocol": "tcp",
    "ip_range": {
      "cidr": "0.0.0.0/0"
    }
  }
],
"links": null,
"tenant_id": "00000000000000000000000000001807"
]
]

List Images

Request
The already available images on RegionThree are requested.

curl http://localhost:8080/dca/images?region=RegionThree

Response
The response is retrieved. The images are presented along with the related details.

```json
{
  "images": [
    {
      "status": "active",
      "name": "CentOS 6.4",
      "deleted": false,
      "container_format": "bare",
      "created_at": "2013-11-04T19:13:46",
      "disk_format": "iso",
      "updated_at": "2013-11-04T19:14:01",
      "id": "79e9245c-3a02-8da-8dd2-ad9d93331e",
      "protected": false,
      "min_disk": 0,
      "min_ram": 0,
      "checksum": "4a5fa01c81cc300f4729736e28ebe600",
      "owner": "e9312e85dde04636a63c1b340f89242a",
      "is_public": true,
      "deleted_at": null,
      "properties": {
      }
    },
    {
      "status": "active",
      "name": "Cirros 0.3.1",
      "deleted": false,
      "container_format": "bare",
      "created_at": "2013-10-23T14:28:21",
      "disk_format": "qcow2",
      "updated_at": "2013-10-23T14:28:22",
      "id": "c4ce643f-0ac-de0-8051-1e4070c154d",
      "protected": false,
      "min_disk": 0,
      "min_ram": 0,
      "checksum": "d792013792949d0d83ba682f8835bce",
      "owner": "e9312e85dde04636a63c1b340f89242a",
      "is_public": false,
      "deleted_at": null,
      "properties": {
      }
    },
    {
      "status": "active",
      "name": "orion",
      "deleted": false,
      "container_format": "bare",
      "created_at": "2013-11-20T18:06:47",
      "disk_format": "qcow2",
      "updated_at": "2013-11-20T18:12:22",
      "id": "791c1279-4d3e-4f89-a33b-a3a93a29e75c",
      "protected": false,
      "min_disk": 0,
      "min_ram": 0,
      "checksum": "d60b7cfc2f87a9b6905c627805bf0",
      "owner": "e9312e85dde04636a63c1b340f89242a",
      "is_public": false,
      "deleted_at": null,
      "properties": {
        "instance_uuid": "a9259820-dd5e-4f84-9581-09acaddff99b",
        "image_location": "snapshot",
        "image_state": "available",
        "instance_type_memory_mb": "2048",
        "instance_type_swap": "0",
        "instance_type_vcpu_weight": "None",
        "image_type": "snapshot",
        "instance_type_id": "5",
        "ramdisk_id": null,
        "instance_type_name": "m1.small",
        "instance_type_ephemeral_gb": "0",
        "instance_type_rtxx_factor": "1",
        "kernel_id": null,
        "instance_type_flavorid": "2",
        "instance_type_vcpus": "1",
        "user_id": "752627b3561f46b08bc27726ce2630ce",
      }
    }
  ]
```
List Networks Request

The networks available to the user on RegionThree are requested.

curl http://localhost:8080/dca/networks?region=RegionThree

Response

```json
{    "networks": [        {            "status": "ACTIVE",            "subnets": [                "3b873329-6469-4d44-9814-93be7b6d7eb2"            ],            "name": "net-0",            "id": "a714bca6-7f2d-4181-91fb-44e6b603a7e4",            "shared": "false",            "provider: physical_network": null,            "admin_state_up": true,            "tenant_id": "e9312e85dde04636a63c1b340f89242a",            "provider: network_type": "gre",            "router: external": "false",            "provider: segmentation_id": "1"        }    ]}
```

List Servers Request

The already deployed (in total) GEs are requested.

curl http://localhost:8080/dca/servers/ge

Response

```json
[    {        "id": "6fda6be8-0e70-4d08-9731-c85866a27f50",        "name": "test-xifi-proton",        "imageRef": "90d4865d-5e7b-4d95-af2c-69753e1740d6",        "flavorRef": "2",        "keyName": "xifi",        "securityGroups": "default,cep",        "created": 1390051880000,        "status": null,        "tenantId": "0000000000000000000000000101",        "userId": "artemis-voulkidis",        "region": "RegionOne"    },    {        "id": "a335265d-777e-42fa-8f5a-3551f0b91",        "name": "test-xifi-proton-r1",        "imageRef": "90d4865d-5e7b-4d95-af2c-69753e1740d6",        "flavorRef": "2",        "keyName": "xifi",        "securityGroups": "default",        "created": 1390135180000,        "status": null,        "tenantId": "0000000000000000000000000101",        "userId": "artemis-voulkidis",        "region": "RegionOne"    },    {        "id": "29c1ee5e-fac8-451d-85d9-9637ae2386",        "name": "test-xifi-orion",        "imageRef": "02fdb0bc-6b47-4af4-ab13-95508333cd84",        "flavorRef": "2",        "keyName": "xifi",        "securityGroups": "default",        "created": 1390135180000,        "status": null,        "tenantId": "0000000000000000000000000101",        "userId": "artemis-voulkidis",        "region": "RegionOne"    },    {        "id": "1ae2d8d8-e8ed-4e4e-88bd-4209b808eeda",        "name": "test-xifi-proton-r2",        "imageRef": "02fdb0bc-6b47-4af4-ab13-95508333cd84",        "flavorRef": "2",        "keyName": "xifi",        "securityGroups": "default",        "created": 1390135180000,        "status": null,        "tenantId": "0000000000000000000000000101",        "userId": "artemis-voulkidis",        "region": "RegionOne"    }]
```
More complex queries are also supported by issuing relevant API calls containing http parameters. For example, the CEP instances deployed in RegionOne could be discovered as follows:

Request

curl http://localhost:8080/dca/servers/ge?desc=cep&region=RegionTwo

Response

[  {    "id":"1ae2d8d8-e8ed-4e4e-88bd-4209b808eeda",    "name":"test-xifi-proton-r2",    "imageRef":"7b001833-5ea4-84fa-803e3c59377d",    "flavorRef":"2",    "keyName":"xifi",    "securityGroups":null,    "created":139052553000,    "status":null,    "tenantId":"00000000000000000000000000000158",    "userId":"artemis-voulkidis",    "region":"RegionTwo"  },  ]

The DCA component also support active VM (GE) listing, where the data is requested directly by the DCRM instances of the federation. For example, an infrastructure owner may be interested on checking the GEs that are deployed on its own infrastructure, located at RegionOne:

Request

curl http://localhost:8080/dca/servers/live?region=RegionOne

The response of the DCA module could be as follows (the full listing has been suppressed for reasons of brevity):

Response

Combinatorial requests are also supported. For example, assume that it is of interest to know on which XIFI nodes are instances of CEP and Marketplace GEs simultaneously deployed:

Request

\[
\text{curl http://localhost:8080/dca/servers/ge/multiple?desc1=cep&desc2=marketplace}
\]

Assuming that in the present state of the XIFI federation, only RegionOne has these two GEs deployed, the answer would have been:

Response

\[
[    "RegionOne"
]
\]

Single Server Deployment Request

In this request we ask for the deployment of a single CEP instance on RegionOne. Necessary information is provided through the POST method. The response is condensed for reasons of brevity.

Request

\[
\text{curl http://localhost:8080/dca/servers -X POST -H "Content-Type: application/json" -d '{ "name":"test-3", "imageRef":"90d4865d-5e7b-4d95-af2c-69753e1740d6", "flavorRef":"2", "keyName":"xifi", "securityGroups":[ { "name":"default" } ], "region":"RegionOne" },' }
\]

Response

The response is retrieved and it shows that the server is created.

\[
\{
  "id": "ffae6295-9aba-48a8-908d-4eebc71bd79c",
  "name": "null",
  "addresses": "null",
  "diskConfig": "MANUAL",
  "adminPass": "hRmXkm97DRqY"
\}
\]

Multiple Servers Deployment Request

In this request we ask for the deployment of a CEP instance, destined for RegionOne, and an Orion CPB instance, destined for RegionTwo.

Request

\[
\text{curl http://localhost:8080/dca/multiple -X POST -H "Content-Type: application/json" -d '{ "list": [ { "name": "test-xifi-proton-r1", "imageRef": "90d4865d-5e7b-4d95-af2c-69753e1740d6", "flavorRef": "2", "keyName": "xifi", "securityGroups": [ { "name": "default" } ], "region": "RegionOne" } ], "list": [ { "name": "test-xifi-proton-r2", "imageRef": "90d4865d-5e7b-4d95-af2c-69753e1740d6", "flavorRef": "2", "keyName": "xifi", "securityGroups": [ { "name": "default" } ], "region": "RegionTwo" } ]}' }
\]

Response

The response is retrieved and it shows that the servers are created.

\[
\{
  "list": [ { "id": "ffae6295-9aba-48a8-908d-4eebc71bd79c", "name": "null",
  "addresses": "null",
  "diskConfig": "MANUAL",
  "adminPass": "hRmXkm97DRqY"
},
  { "id": "test-xifi-proton-r2", "name": "null",
  "addresses": "null",
  "diskConfig": "MANUAL",
  "adminPass": "hRmXkm97DRqY"
]}
\]
Response
The response is retrieved and proves the creation of the two requested servers (VMs).

```
```

Delete Server Request
We request the deletion of a specific server.

```
curl -X DELETE http://localhost:8080/dca/servers/d5c22170-38d6-4344-9d62-c9770e550cee
```

Response
The response is retrieved and show the deletion of the server.

```
{       "deleted":"d5c22170-38d6-4344-9d62-c9770e550cee"    }
```

Note that the region of the server is inferred through the DCA persistency layer, described later.

DCA Persistency Layer
One of the primary goals of DCA is to log the requests made by the users of the federation to the federation, in order to provide meaningful statistics to the infrastructure owners and the federation operators, through a set of predefined queries. Further, DCA could as well operate as a means of federation cache, providing quick information on the characteristics of the VM instances deployed in the federation, including Ids and regions of the host XIFI-nodes, the type of the instances etc. The architecture of the DCA persistency layer, currently implemented upon a MySQL server, is depicted in the following figure.
As may be deduced from the above figure, DCA logs the requests made by the federation users and relates them to the federation responses, in an attempt to provide information related to the federation status. This information may be forwarded to the XIFI recommendation tool and the infrastructure owners for further elaboration.

```
mysql> describe dca.request;
+----+----------+------+-----+----------------+---------+
| Field | Type     | Null | Key | Default        | Extra   |
| id    | bigint(20) unsigned | NO   | PRI | NULL           | auto_increment |
| ip-source | varchar(45) | NO   |     | NULL           |         |
```

Figure 32: The architecture of the DCA persistency layer
Apart from storing the requests made by the users and the related responses, the DCA persistency layer allows for storing information related to the federation nodes DCRM identity services (most likely based on Keystone) in a table called `keystone`.

```sql
mysql> describe dca.keystone;
```

Also, DCA has built-in information related to the GE images already available through FI-WARE lab and tested. This information is related to the image reference UUID that can be used to identify the type of the deployed VM (if it constitutes a GE) when the installation is made directly through image deployment. Further, to ensure proper a priori monitoring of the user quotas and assure minimal/recommended operation of the GE images offered by the FI-WARE environment, DCA has populated another table, called `hwrequirements` that describes the minimum and recommended resources a GE requires for proper operation. This information is coupled to the GE database representation as deduced both by Fig. 3 and the following MySQL output:

```sql
mysql> describe dca.hwrequirements;
```

---

© 2013 - 2015 XIFI Consortium Parties

Page 82 of 85
When a request for a VM deployment in a specific region is issued to the DCA component, the request is logged and the request is forwarded to the controller of the node belonging to the specified region. If the image ID corresponds to a GE image ID, then the respective reference is passed to the database server representation and the VM is onwards considered to be a GEi. DCA also logs the id of the identity service that was contacted to acquire the necessary information to get the VM (GE) deployed, the name of the deployed VM (GE), the flavor that was chosen by the user, the security groups that were identified, as well as other user- and date/time-related information. A representation of the structure of the database representation of a deployed VM (GE) is depicted below.

```sql
mysql> describe dca.server;
+------------------ +------------------ +------------------ +------------------ +------------------ +------------------+
| id               | varchar(45)      | NO   | PRI | NULL    | keystokeId       |
| keystoneId       | varchar(45)      | YES  |     | NULL    | imageRef         |
| name             | varchar(45)      | YES  |     | NULL    | flavorRef        |
| flavorRef        | varchar(45)      | YES  |     | NULL    | keyName          |
| keyName          | varchar(45)      | YES  |     | NULL    | GERef            |
| securityGroups   | varchar(255)     | YES  |     | NULL    | created          |
| created          | int(10)          | YES  |     | NULL    | status           |
| status           | timestamp        | YES  |     | NULL    | tenant_id        |
| tenant_id        | varchar(45)      | YES  |     | NULL    | user_id          |
| user_id          | varchar(45)      | YES  |     | NULL    | +------------------+
```
REFERENCES

[1] In Cloud environments based on the high-availability principle, traditional backup services offered by data centres are not more required.

[2] Transparency, as the capability of inspect a service so as that QoS can be observed and validated is strictly related to the “Measured Service” principle.


