FIWARE Ops

Federico Alvarez

Universidad Politecnica Madrid

Federico.alvarez@upm.es

FIWARE Ops

FIWARE Ops Overview

- Main components and architecture
- Monitoring services
- Node installation and deployment
- Join the federation
  - How you can attach a node to FIWARE-Lab?

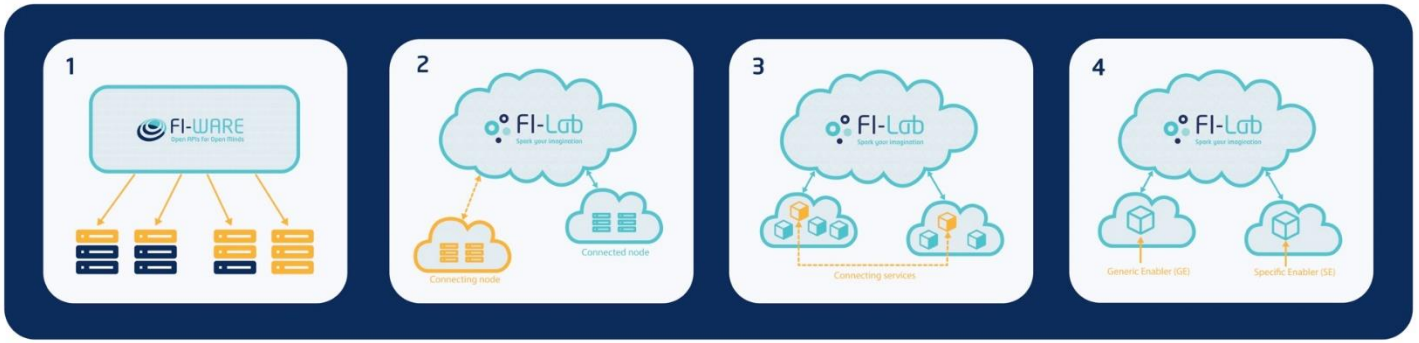
FIWARE Ops

Overview FIWARE-Ops

- **FIWARE-Ops** facilitates the **uptake**, **deployment** and **federation** of a sustainable pan-European open federation of test infrastructures integrated in FIWARE-LAB.
- This community establishes a unique marketplace crucial to:
  - Address commercial exploitation of Future Internet resources and services in Europe (and even beyond)
  - Create a common framework to overcome the current fragmentation of European infrastructures into isolated test beds that are individually unable to support large-scale trials
- Currently such federation comprises 17 cloud-based nodes along Europe

FIWARE Ops

FIWARE-Ops: easing operations of FI-WARE providers



Deployment

Deployment of basic Cloud Hosting GEs and Monitoring Adapters in a FI-WARE node

Federation Management

Federate a new FI-WARE node within a given FI-WARE instance (e.g. within FIWARE-Lab)

Connectivity Management

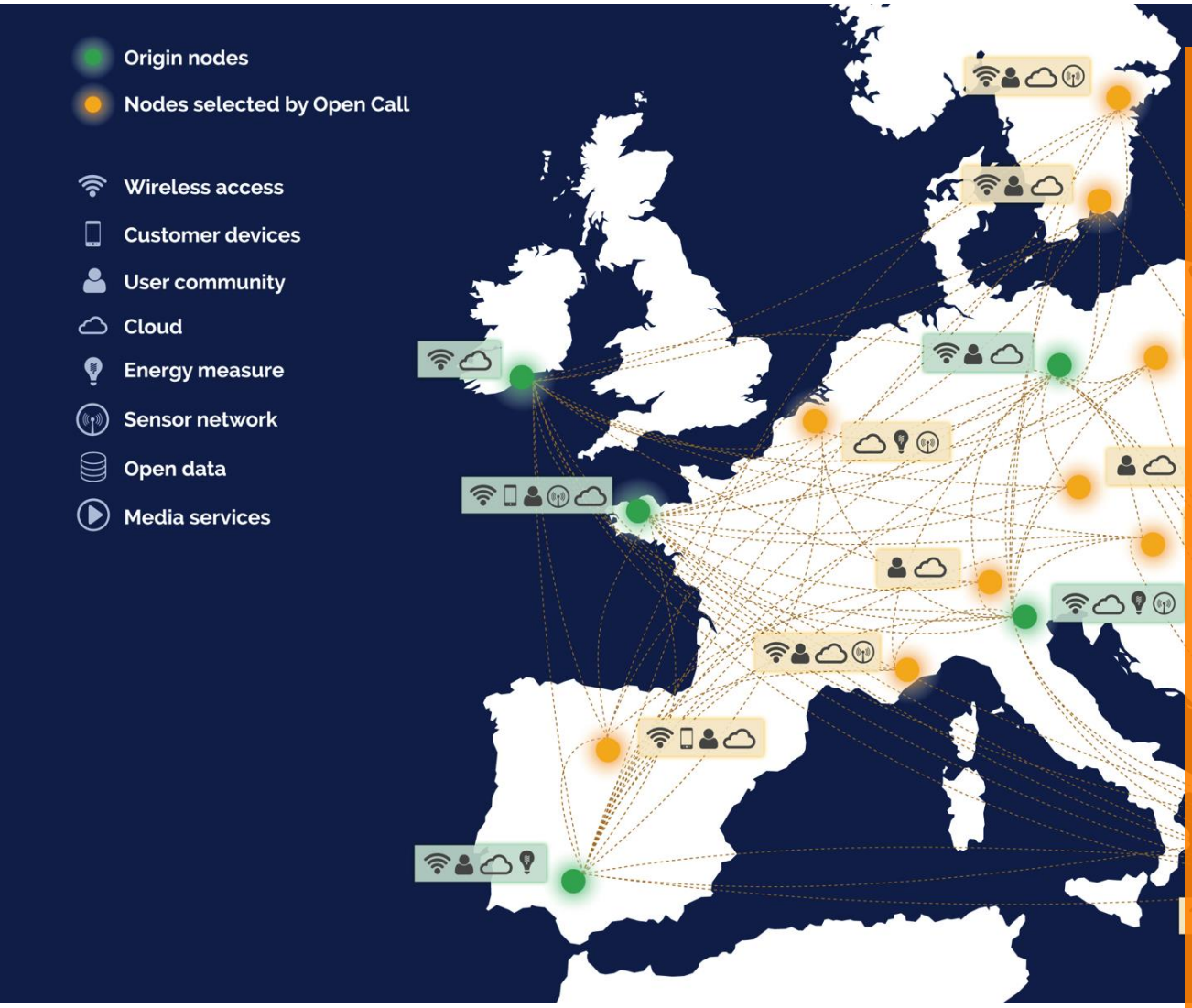
Manage connectivity of services across FI-WARE nodes of a FI-WARE instance

Service Offer Management

Registration and deployment of additional Generic Enablers, Specific Enablers and complementary Future Internet Facilities

FIWARE Ops

Extending the FIWARE-Lab offering for service providers and developers



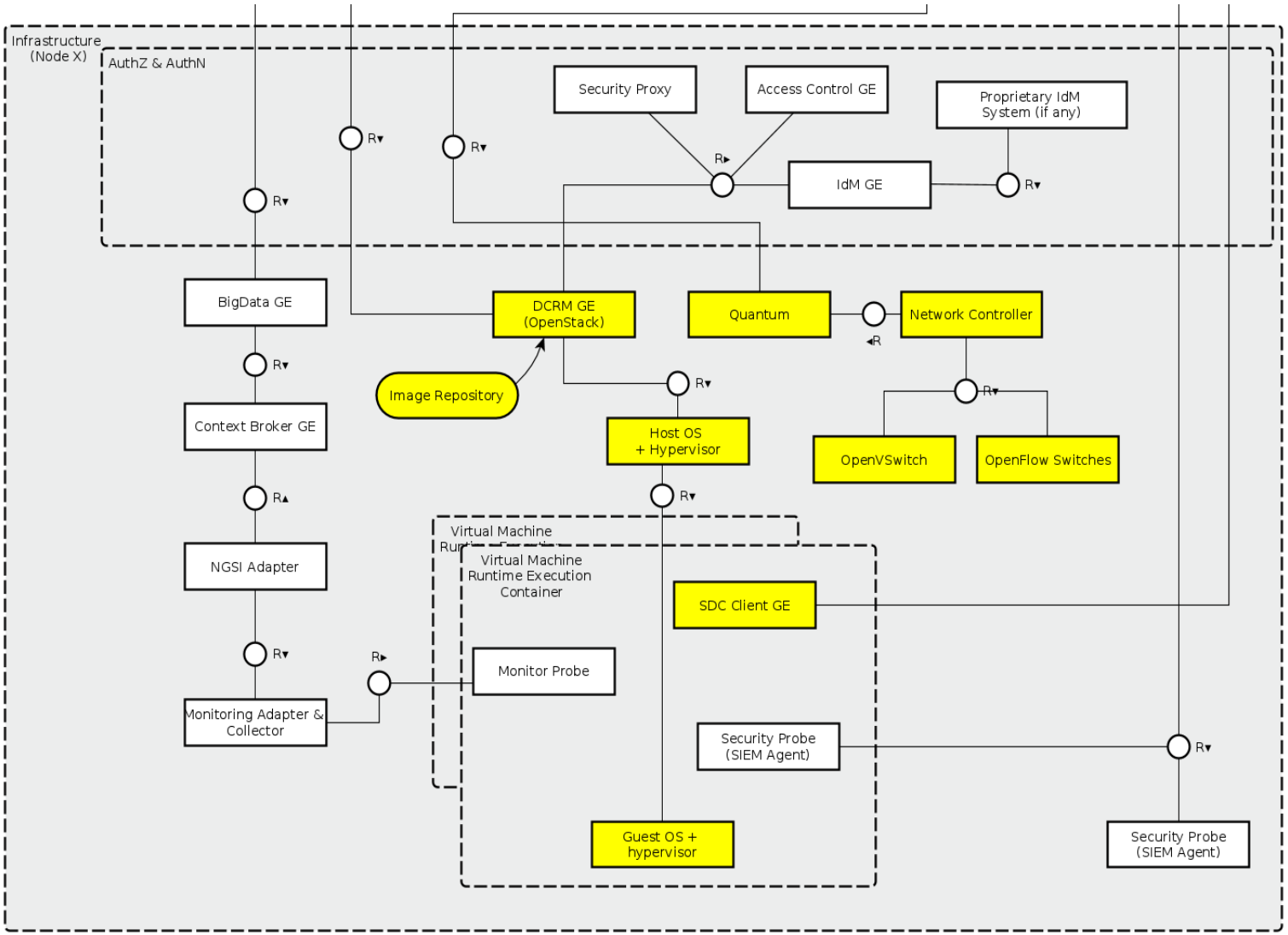
- Availability of 5 nodes (end of March 2014) with 500+ cores, 1TB+ Ram, 100TB+ HD
- Additional 12 nodes (April / September 2014) with 1000+ cores, 2TB+ Ram, 200TB+ HD
- Level 1 and Level 2 support for the nodes
- Showcases for developers, infrastructures, smart businesses

FIWARE Ops

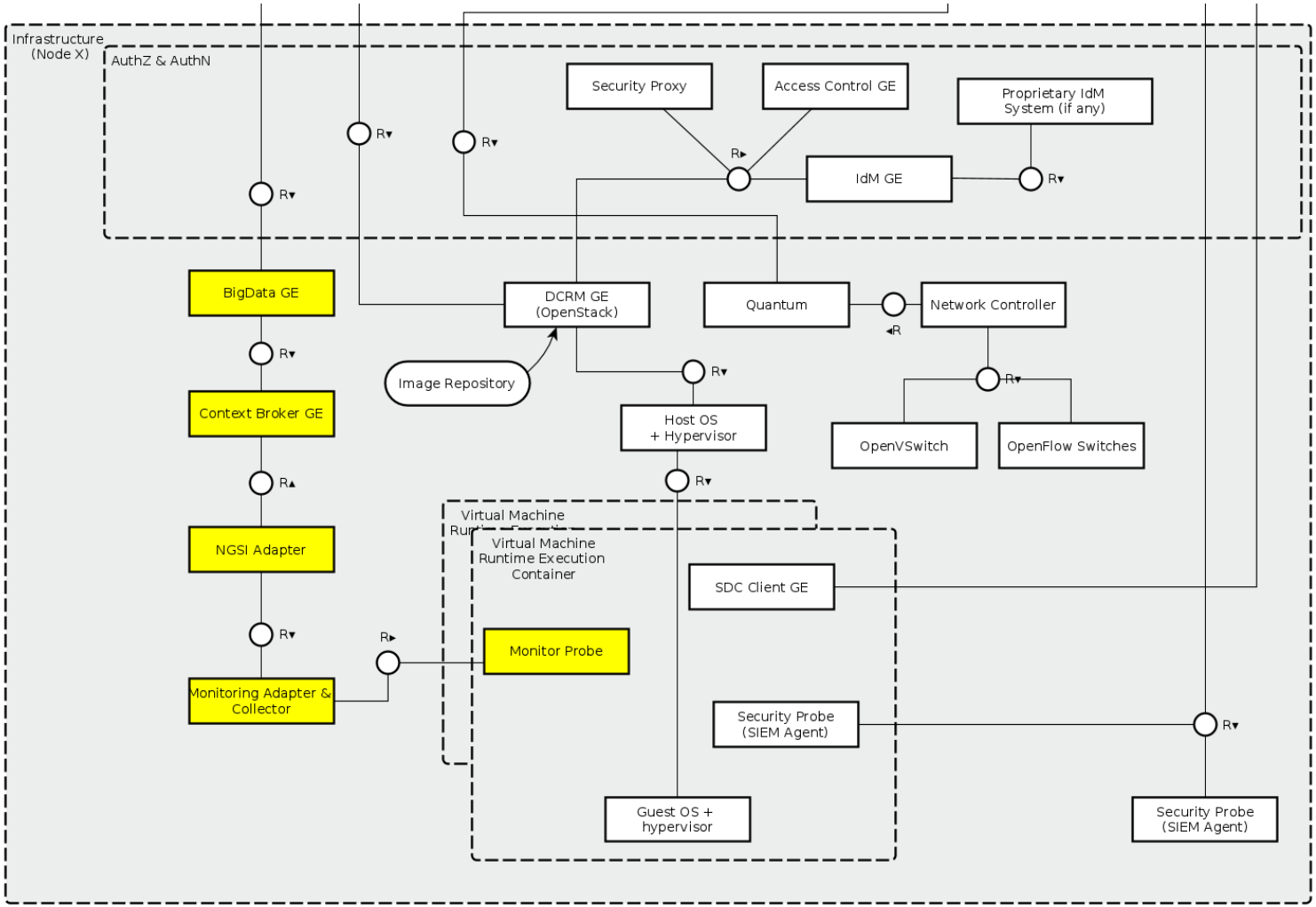
FIWARE-Ops Main Components
(just overview…not to die with the figures!)

FIWARE Ops

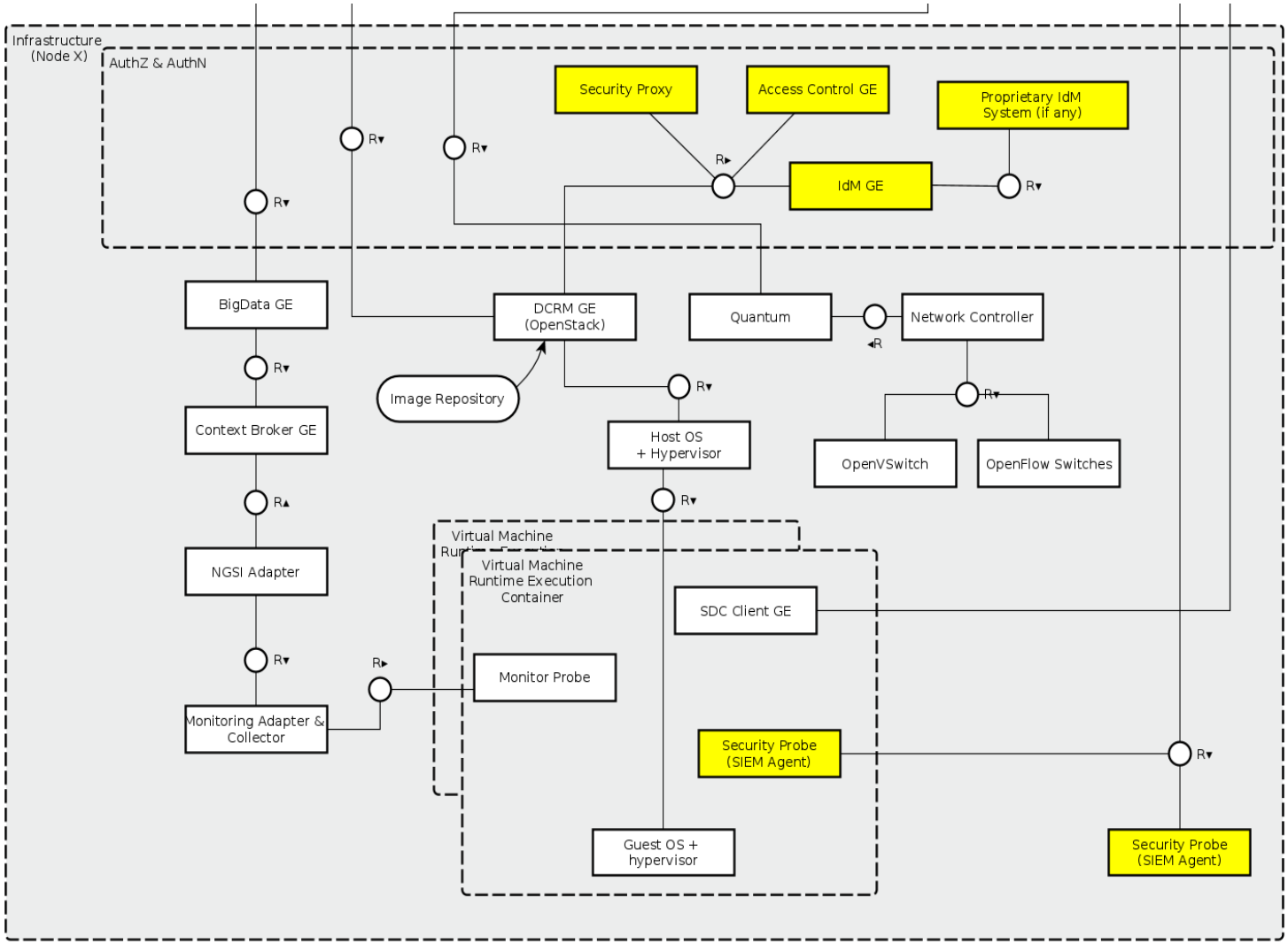
All nodes: cloud management



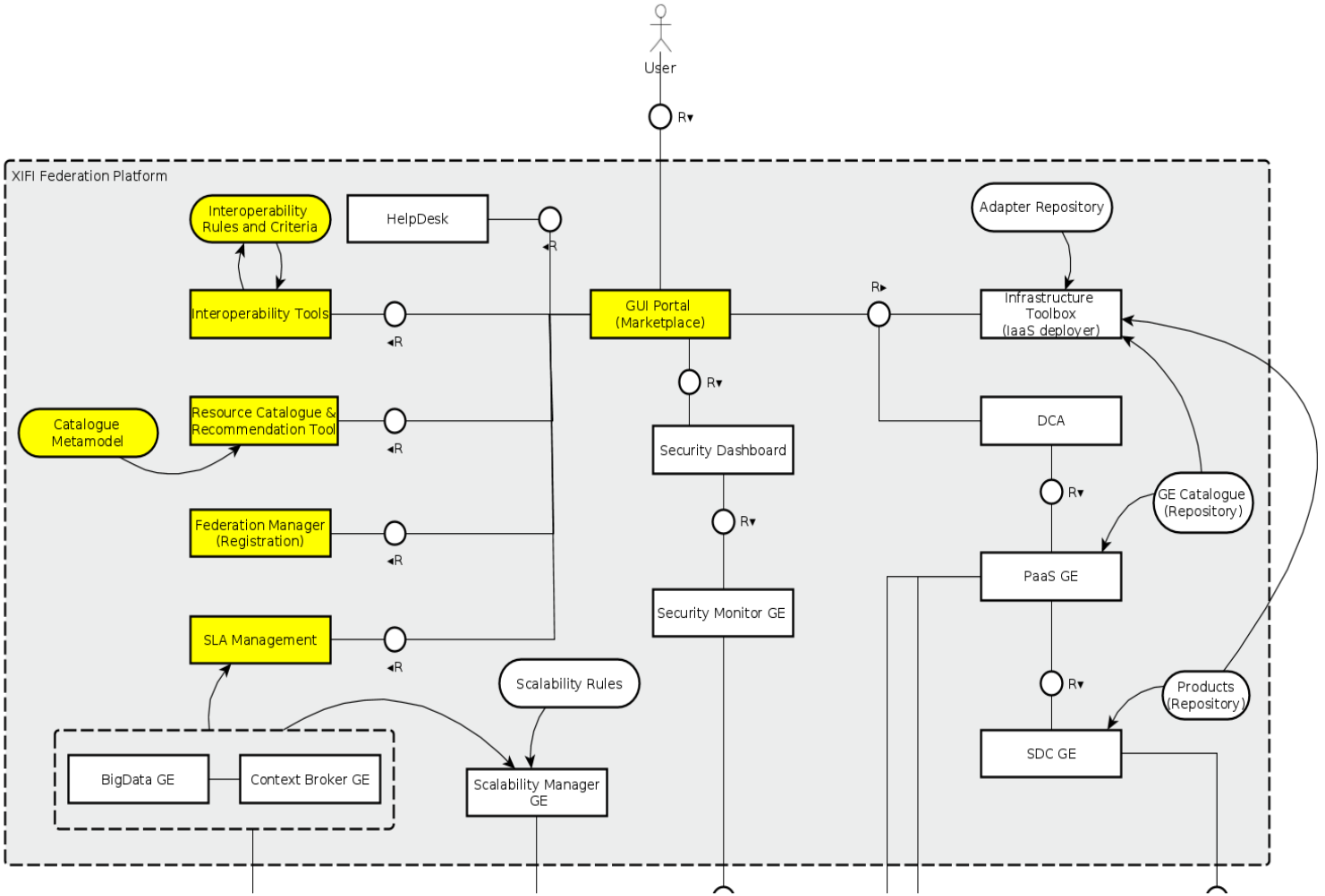
All nodes: monitoring



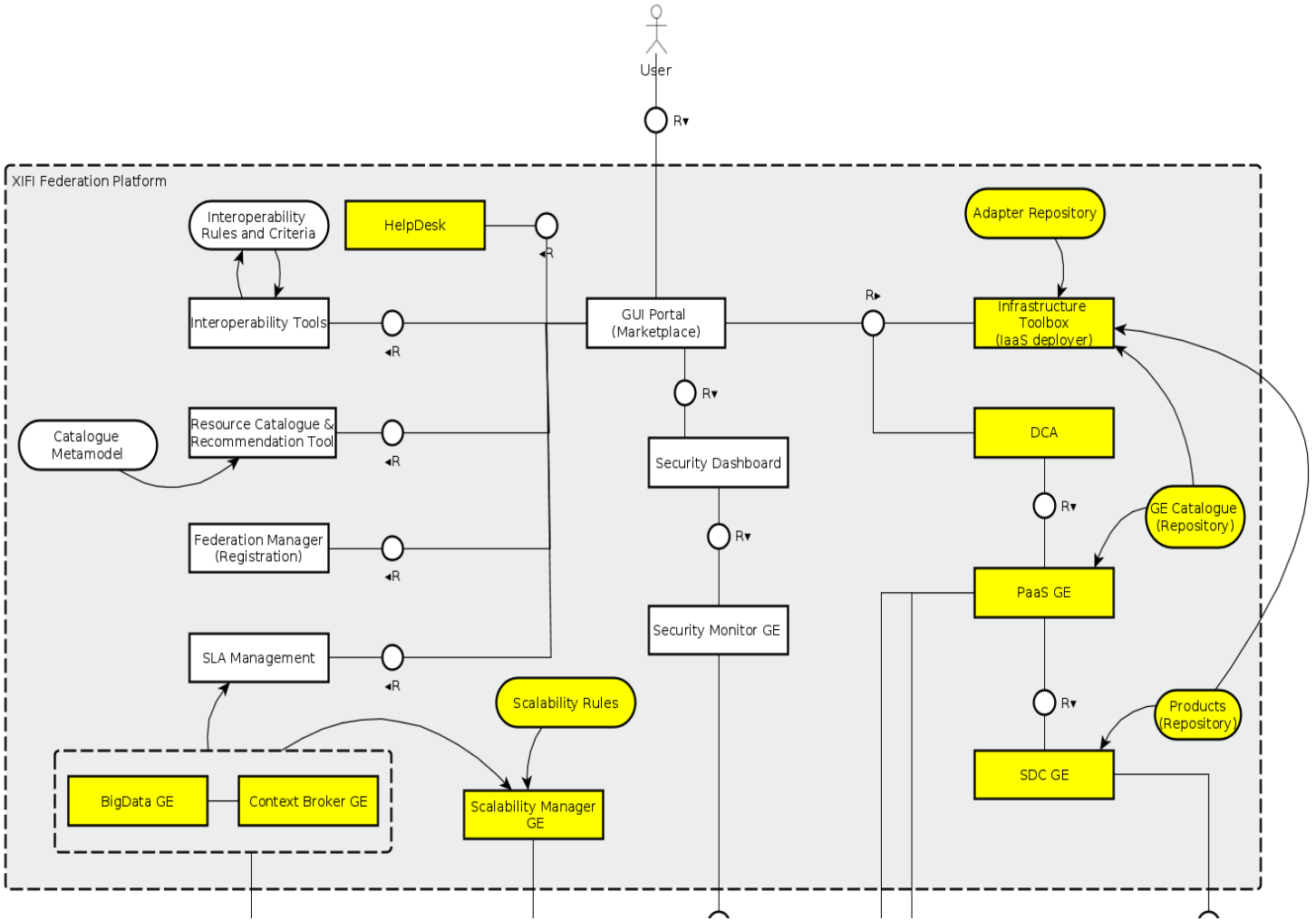
All nodes: security



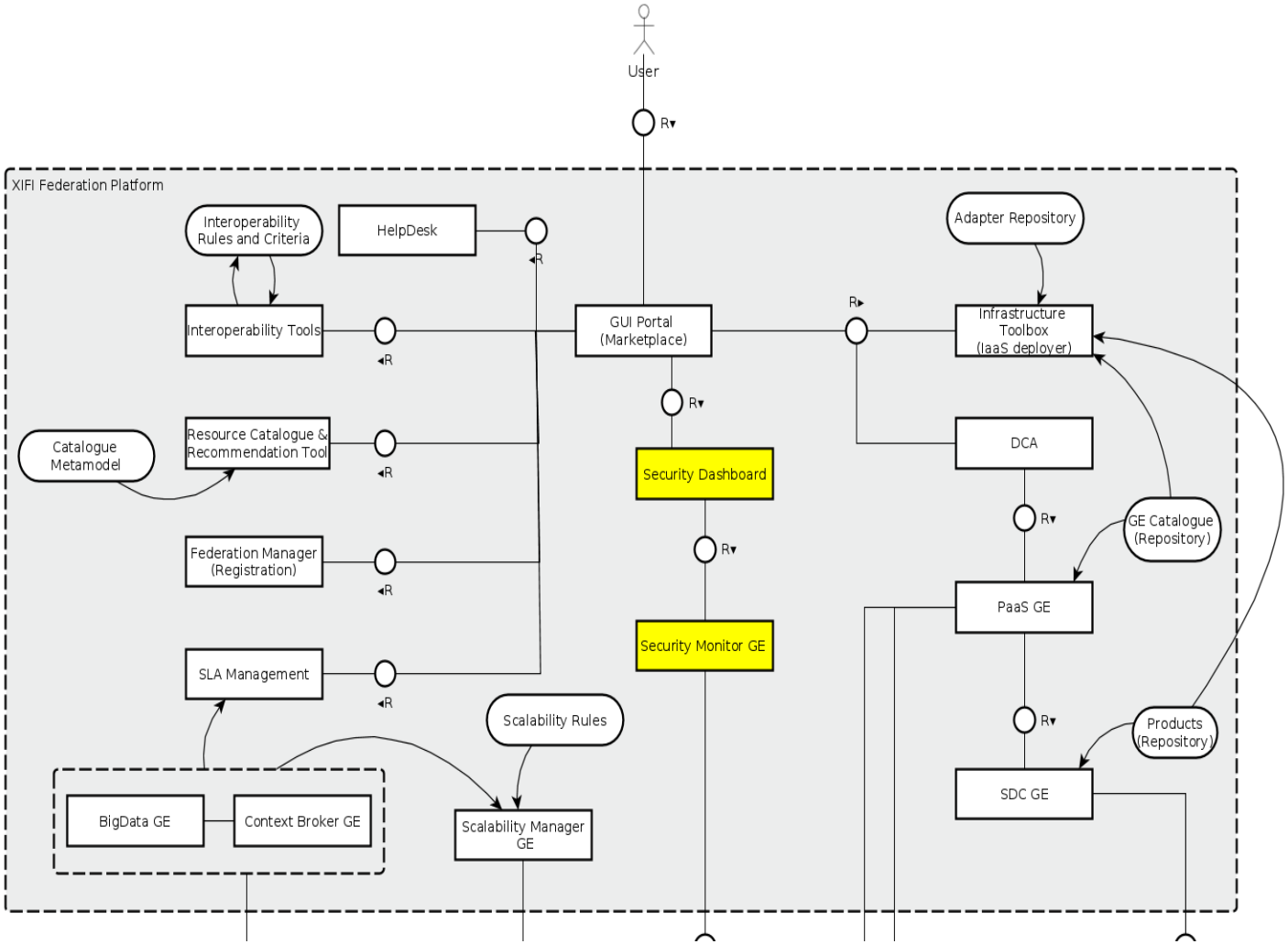
Master nodes: user tools



Master nodes: setup, deploy & ops.



Master nodes: Security Monitoring

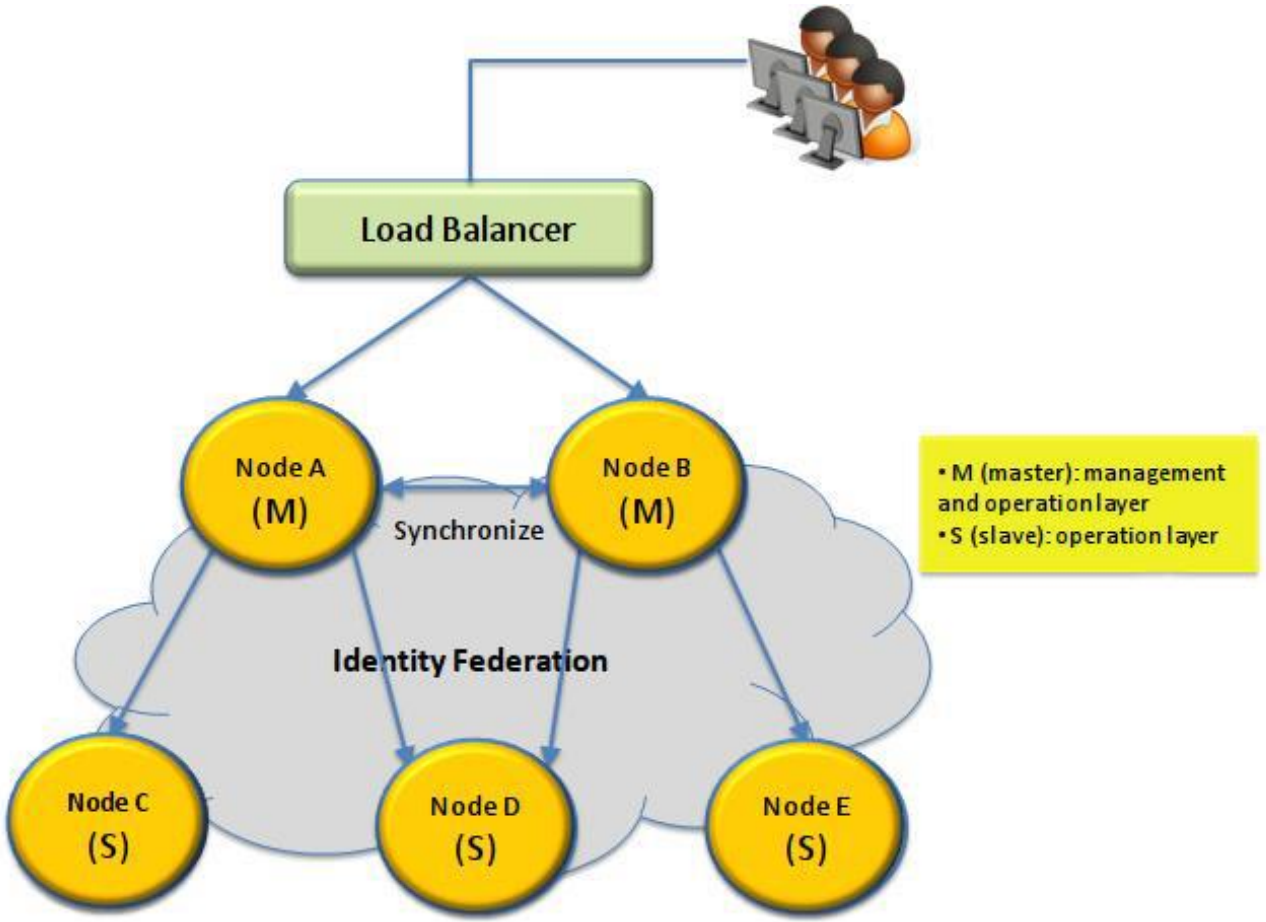


FIWARE Ops

More components are available for full operation

- Inter-domain networking and SDN support
- MD-VPNs for connectivity
- Support services
- And other relevant elements

XIFI deplyoyment architecture

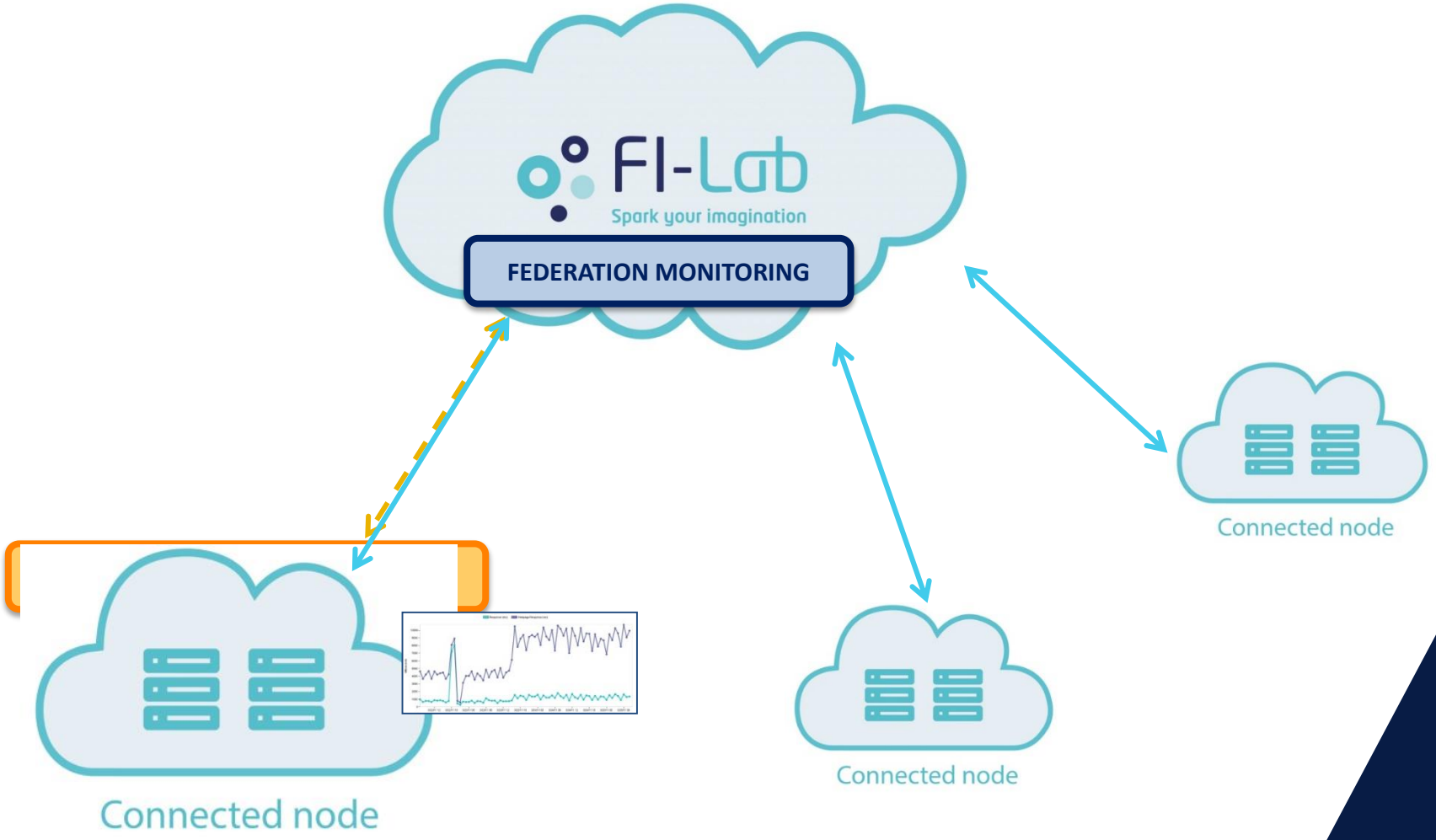


FIWARE Ops

FIWARE-Ops Federation Monitoring

FIWARE Ops

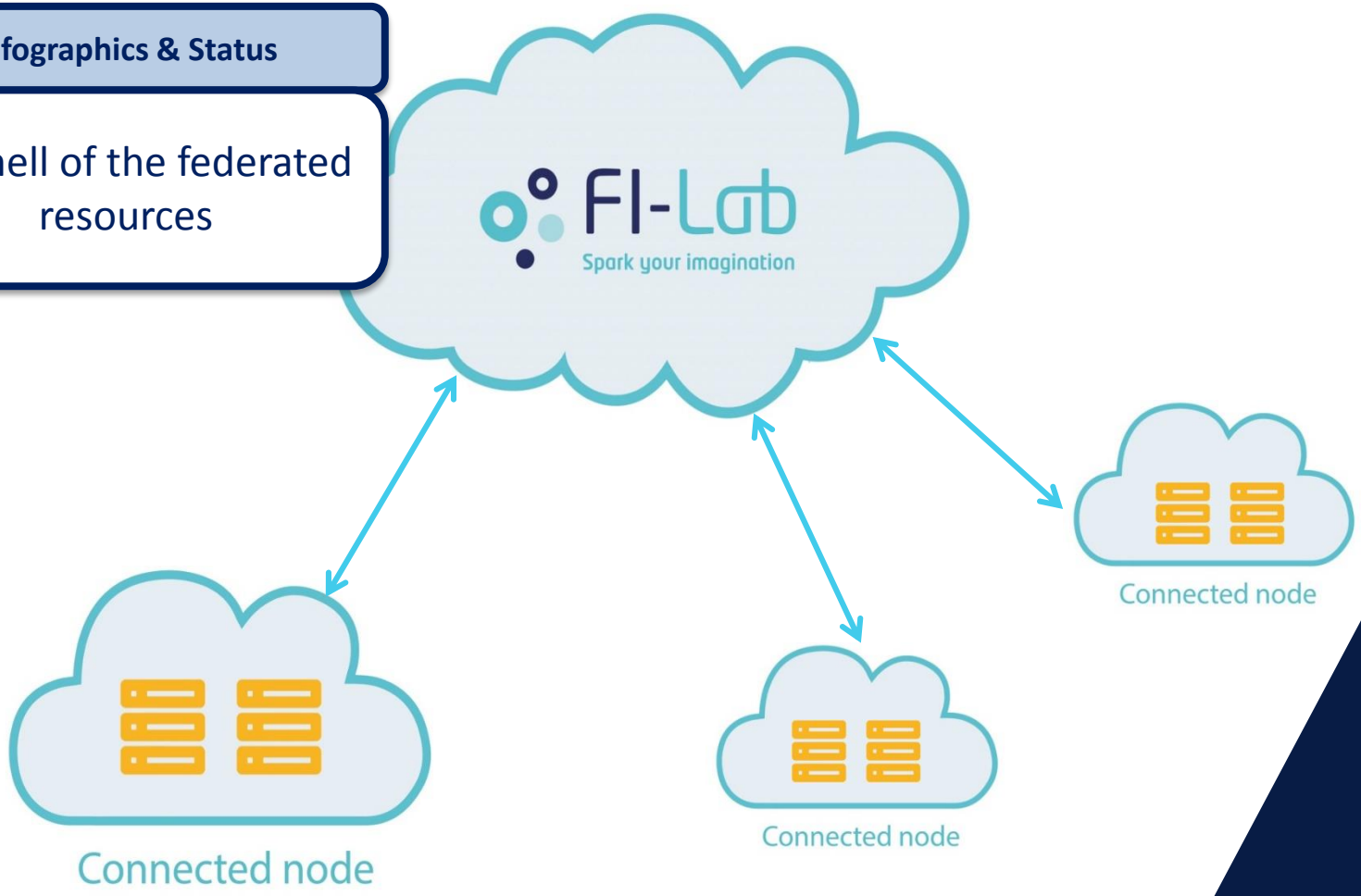
Federation Monitoring



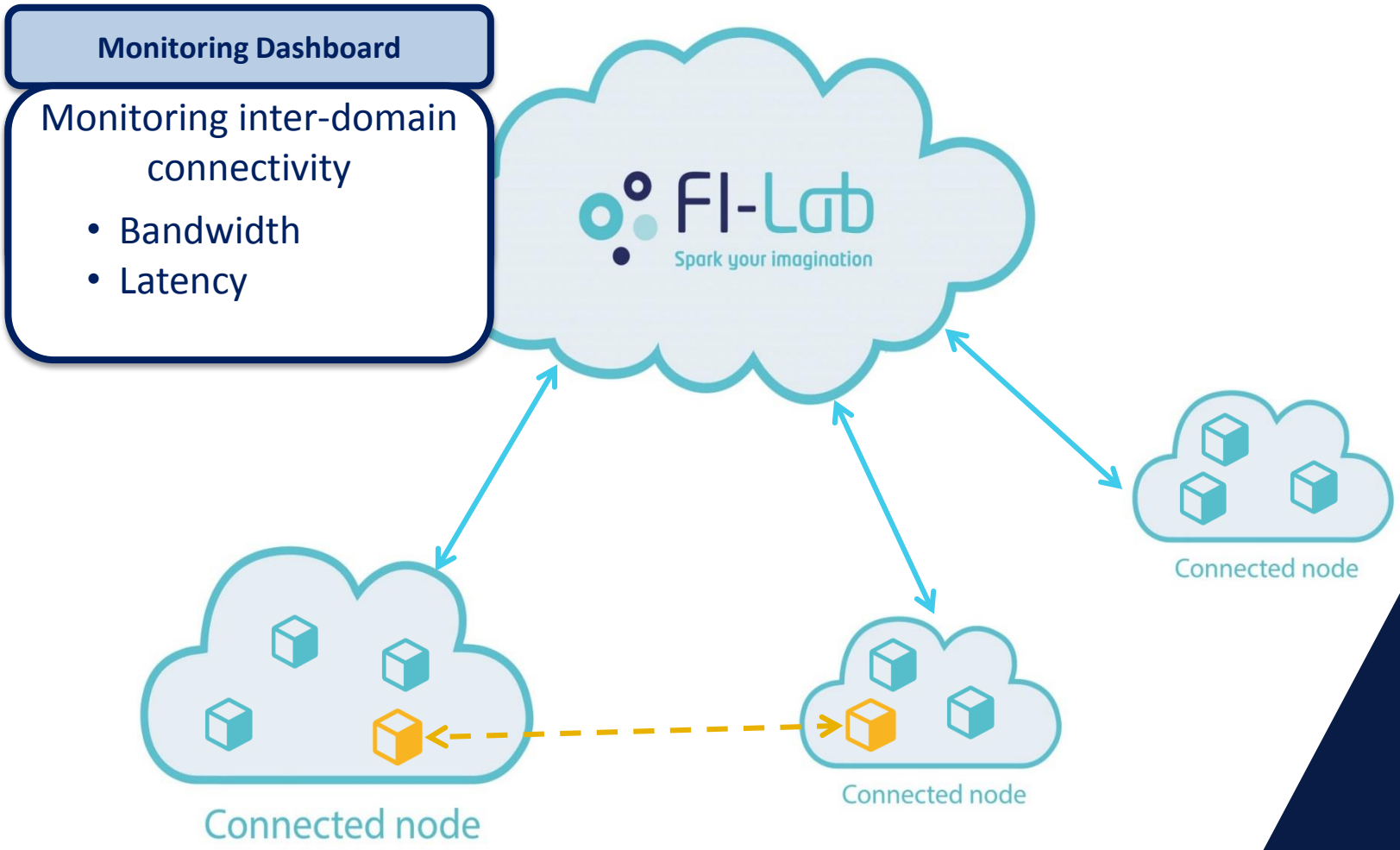
Infographics & Status

Infographics & Status

Nutshell of the federated resources



Monitoring Dashboard



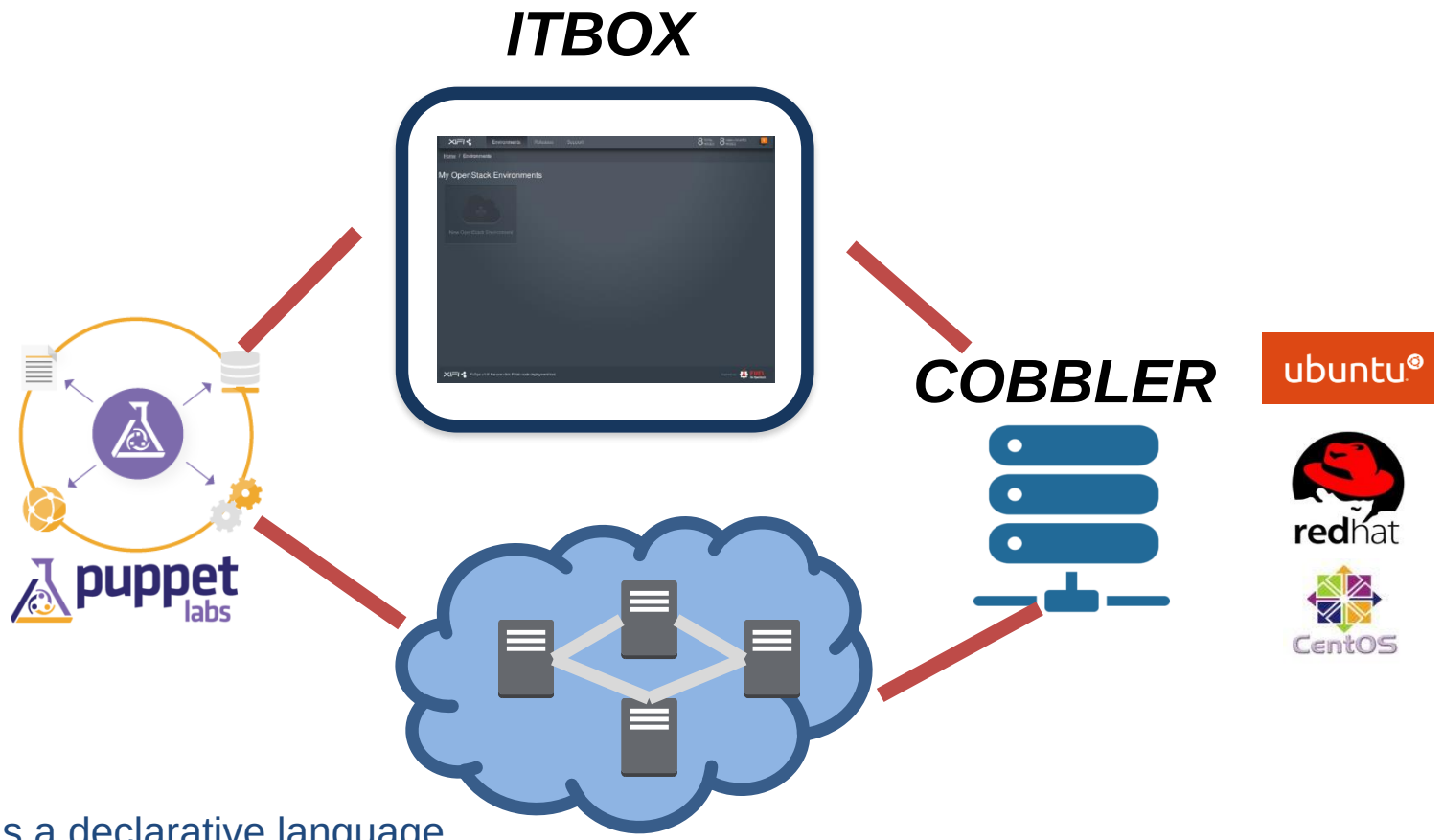
FiWARE-Ops Overview

Installation of a new node using ITBox

First step: Getting the ITBox

- You can download the ISO at: https://github.com/SmartInfrastructures/itbox-main/releases .
- Via ITBox it is possible to start configuring a node and offer FIWARE Ges
- More functions are offered, we are only presenting the main utilities
  - For more information please refer to FIWARE-Ops guides

ITBox: main components



Puppet is a declarative language through a developer manage infrastructure from provisioning and configuration to orchestration and reporting.

Cobbler is a Linux installation server that allows for rapid setup of network installation environments. It is used by ITBox in order to install operating systems.

ITBox architecture in a nutshell

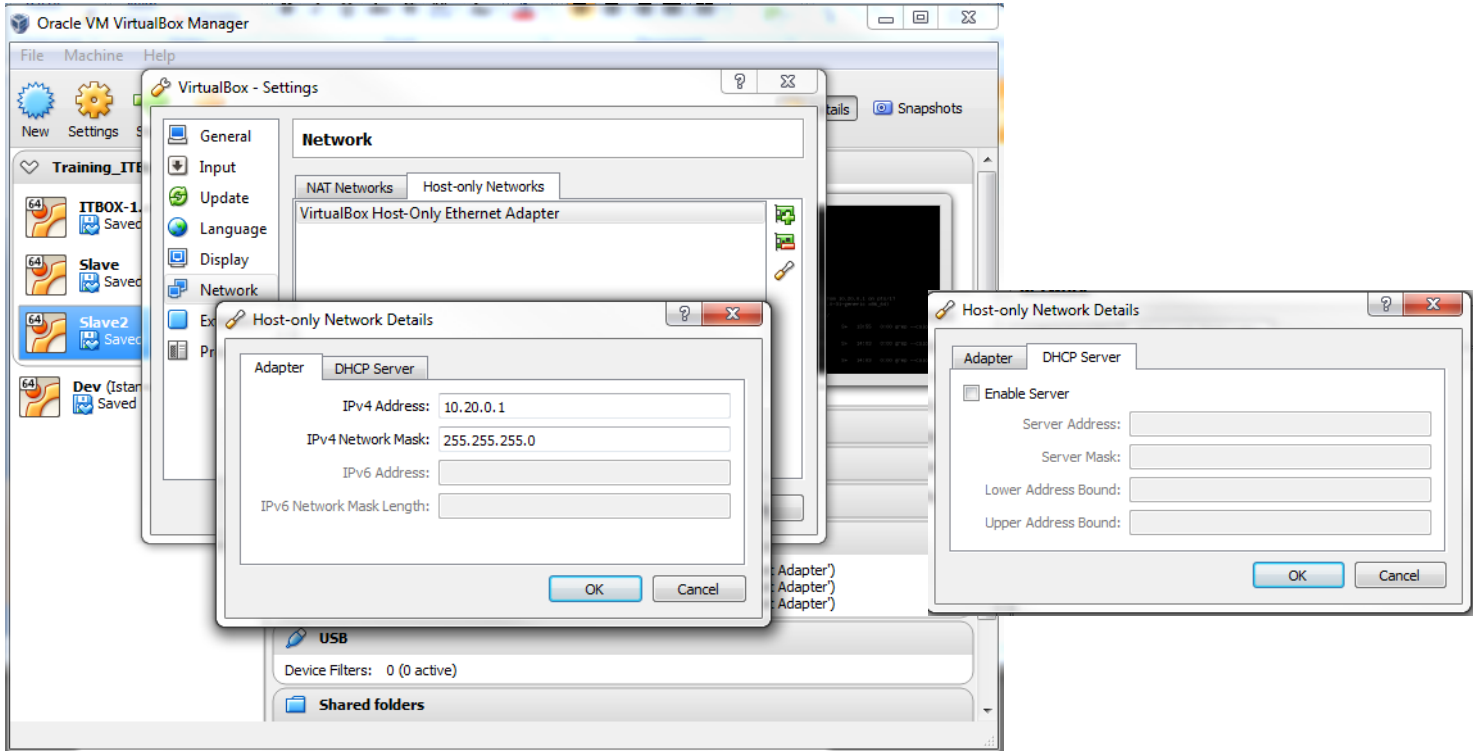
- In a nutshell, the ITBox deployment orchestration engine Astute manages OS provisioning via Cobbler, and uses an MCollective plugin to distribute a file (Facter facts) that defines node's role and other deployment variables for Puppet.
- Mcollective server is a framework to build server orchestration or parallel job execution systems.

How to set VirtualBox

- If you would like to evaluate ITBox on VirtualBox, you can create and configure all the required VMs for a test environment, including the Master node and Slave nodes for OpenStack itself.
- Host requirements
  - Windows, Linux, Mac
  - 8+ GB RAM
  - Will support 4 VMs for Multi-node OpenStack installation (1 Master node, 1 Controller node, 1 Compute + 1 Cinder, 1 monitoring node)

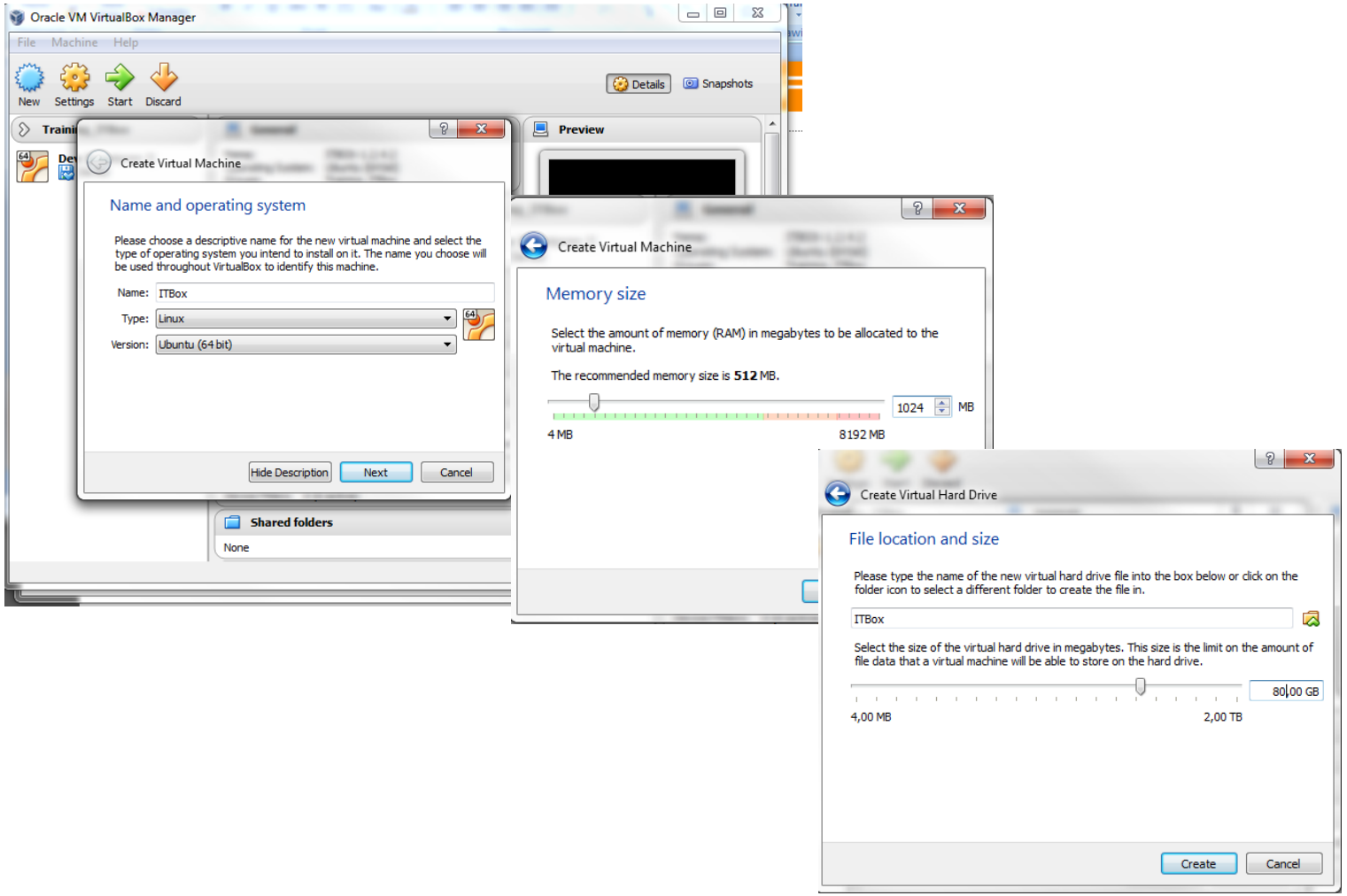
VirtualBox: network preferences

- Configure the host-only interface vboxnet0 in VirtualBox by going to *File -> Preferences -> Network and* clicking the



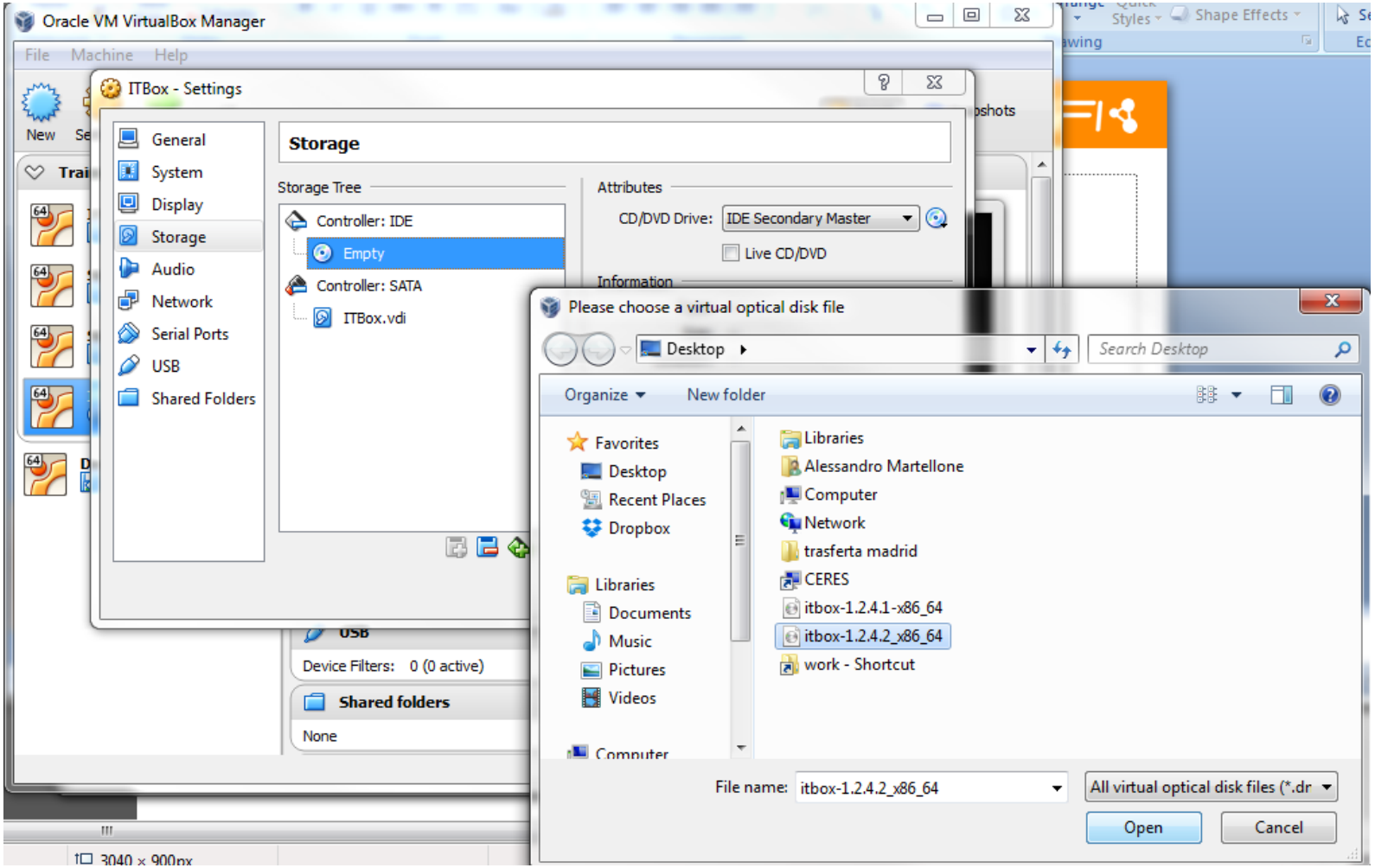
FIWARE Ops

VirtualBox: create a VM

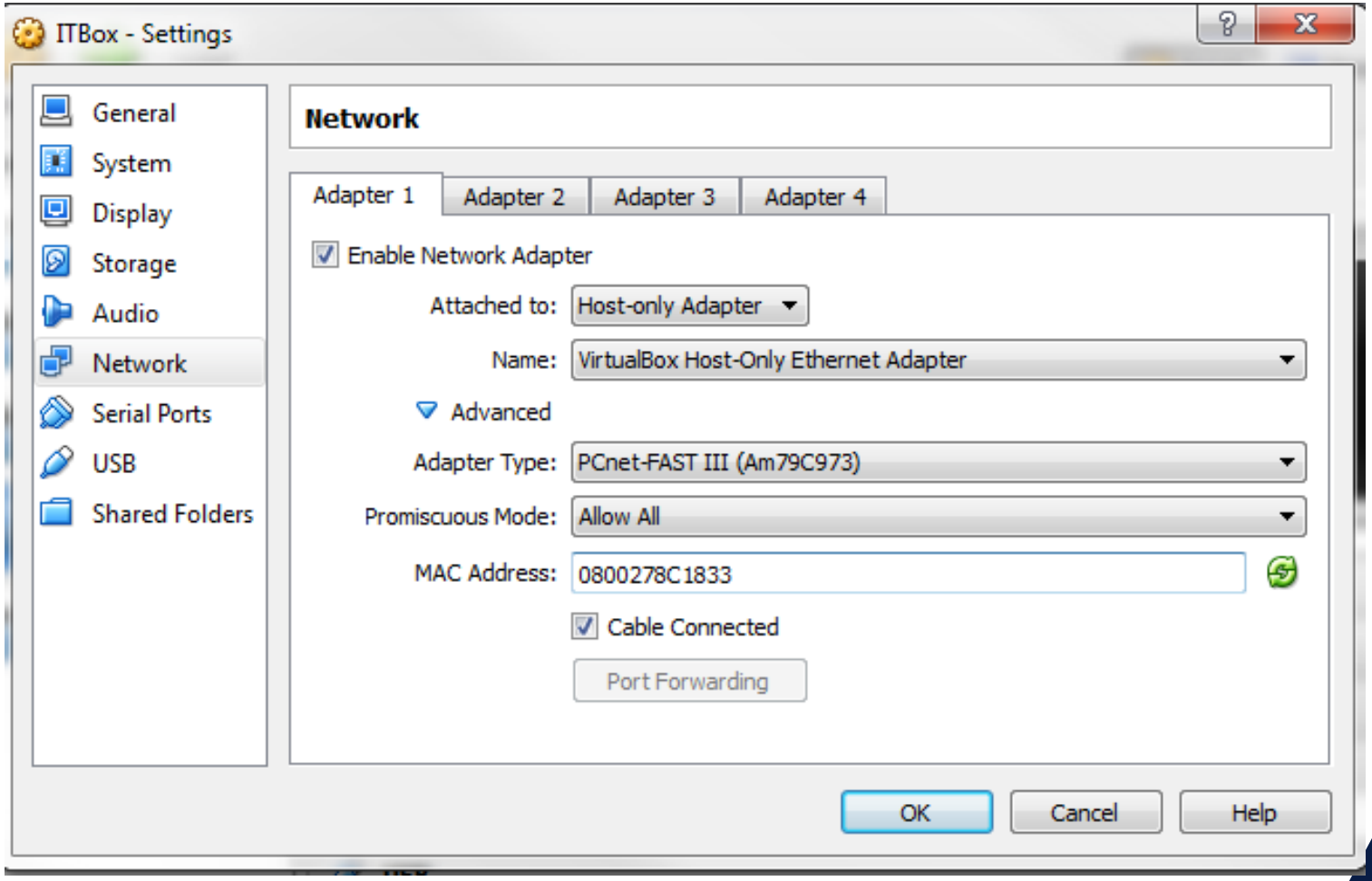


FIWARE

VirtualBox: setting up the VM



VirtualBox: Vm configuration



VirtualBox: start the VM

ITBox: edit options

- The console-based Fuel Setup allows you to customize the Fuel (PXE booting) network, which has a default network of 10.20.0.2/24, gateway 10.20.0.1.
- Within Fuel Setup you can configure the following parameters:
  - DHCP/Static configuration for each network interface
  - Select interface for Fuel network
  - Define DHCP pool (bootstrap) and static range (installed nodes)
  - Root password
  - DNS options

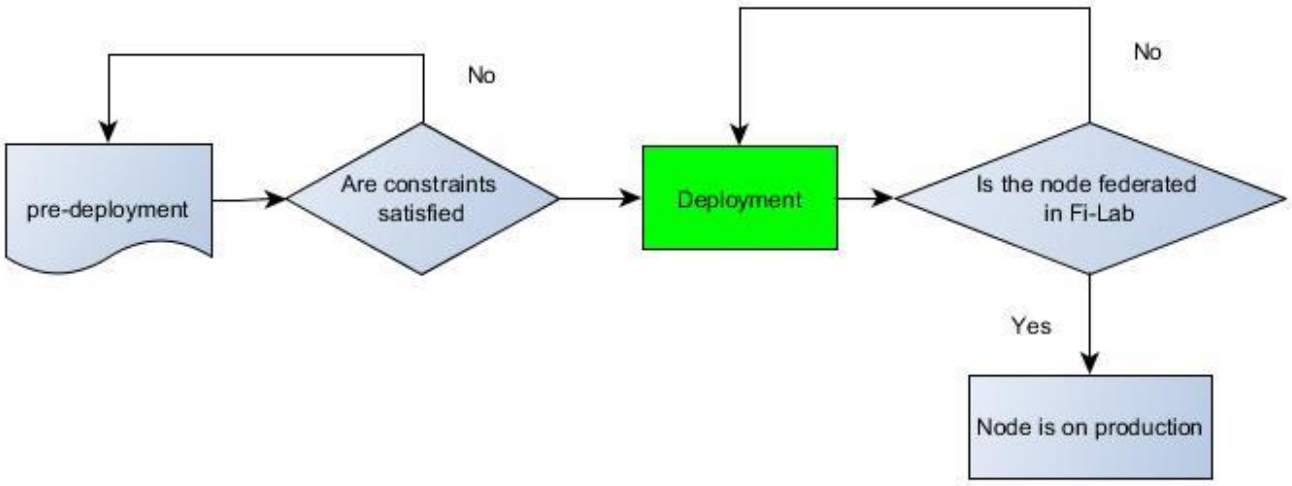
The master node is installed

- Once the Master node is installed, power on all slave nodes and log in to the ITBox UI. The default address is http://10.20.0.2:8000/
- Slave nodes will automatically boot into bootstrap mode (CentOS based Linux in memory) via PXE and you will see notifications in the user interface about discovered nodes.
- At this point, you can create an environment, add nodes into it, and start configuration.

FIWARE Ops

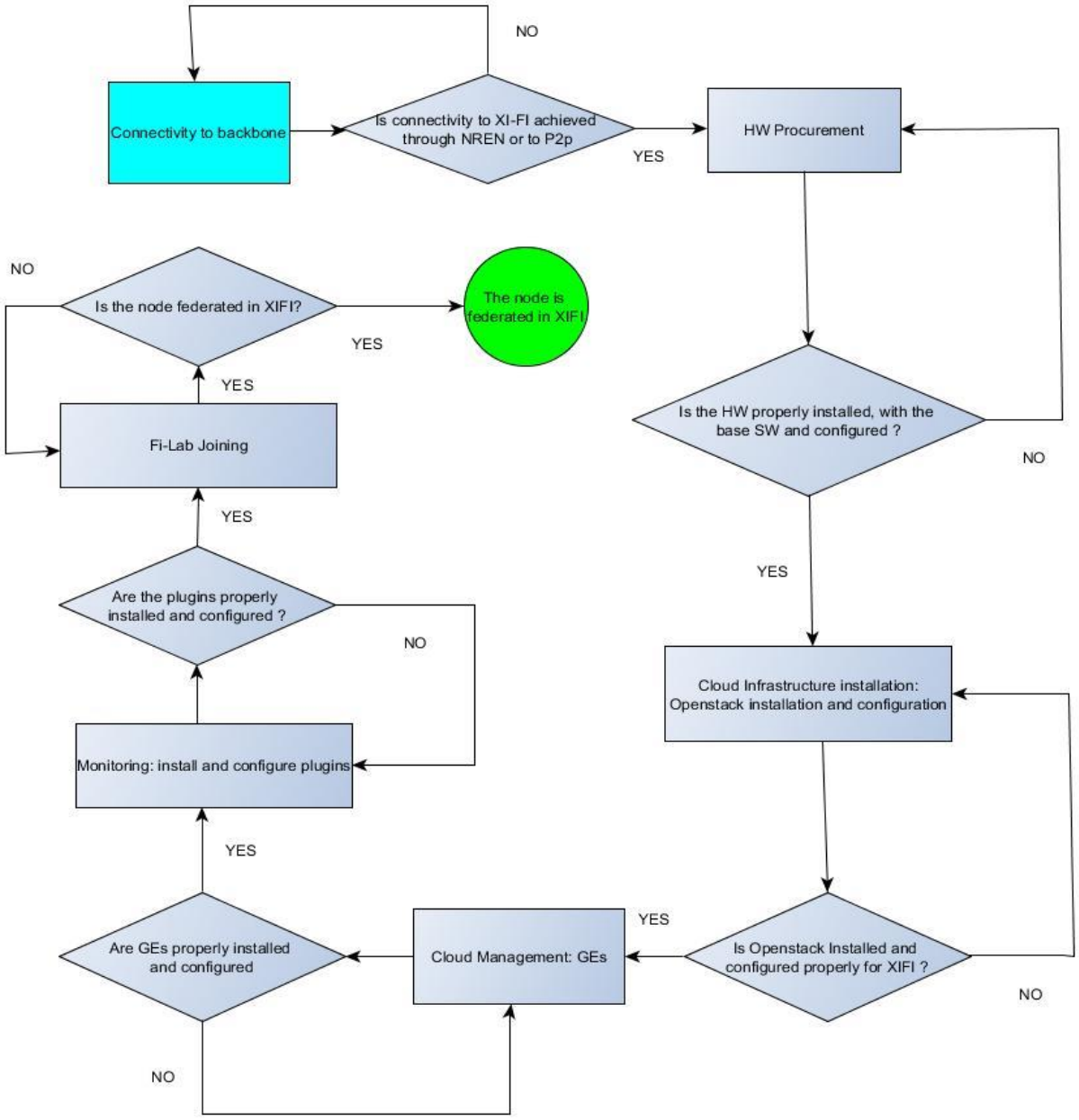
Process for joining

Federation Process



- The Federation Process manages the introduction of a new node in the FIWARE-Lab federation. An important step of this phase is the DEPLOYMENT
- In terms of lifecycle, the deployment of a new node stands before the production phase and the after the open call
- In order to successfully accomplish the deployment of a new node, some requirements have to be satisfied:
  - Connectivity to GEANT (or P2P internet VPN as backup solution)
  - Hardware procurement
- The deployment ends when the new node is in production (when a node in production is not a new node anymore!) and is managed by FIWARE-Ops support

Deployment Steps (I)



Deployment Steps (II)

Deployment has been partitioned as follows:

- **Connectivity to the Core Backbone:** MD-VPN connectivity through the local NREN (*)
- **HW procurement**: required hardware shall be procured and deployed with the base operating system
- **Cloud Infrastructure Installation:** installation and configuration of the OpenStack system (via ITBox)
- **Cloud Management (GE):** This step is inside ITBox, otherwise a manually installation of the needed GEs is required

Deployment Steps (III)

- **Monitoring:** deployment through the ITBox. A manual installation is also available
- **Join FIWARE-Lab**: This is essentially the installation and configuration of the Keystone Proxy component

NOTE: Connectivity to the backbone is mandatory for Monitoring and FIWARE-Lab joining but not for Cloud Installation and Management

Cloud Portal - Integration

- Cloud Portal allows the management of FIWARE-Lab nodes in a federated manner
- It requires to create user accounts on FIWARE-Lab
  - https://account.lab.fi-ware.org/
- Other requirements
  - MD-VPN connectivity
  - Keystone Proxy connectivity
  - DCRM GE installed
  - Joining fiware-lab-help@lists.fi-ware.org

Keystone Proxy - Integration

- The keystone proxy provides the access to the federation IdM
- Currently an unique instance of Keystone proxy is running in the Spanish node
- Requirements
  - Update the catalogue (impacts all nodes)
  - Configure the Firewall policies to allow communications with remote nodes

MD-VPN - Integration

- Provides the federation connectivity across the nodes
  - Privacy
  - Security
  - Traffic Engineering on the backbone is possible
- MD-VPN is created on top of the NREN connection
  - Typically delivered on a VLAN
  - Dedicated VRF should be used
  - BGP is used to exchange routing across the nodes

MD-VPN - Integration

- The setup must be discussed with local NRENs
- Federation IP addressing plan
  - Per node. Configuration available on FIWARE-Ops guides (and in this document: D5.2)
  - Must be implemented on the network in which all the federation related hosts are connected
- It is possible to provide backup solutions based on P2P VPN.
  - important delay of deployment of the NREN
  - if the NREN does not provide MD-VPN service
  - the infrastructure cannot get NREN connectivity

FIWARE Ops

Conclusions

- FIWARE Ops eases the deployment and configuration of nodes to offer FIWARE services and supports the process to participate in FIWARE-Lab
- This was only an overview and more information can be found in FIWARE and in the Project XIFI, including a complete online training

FIWARE Ops

Thank you for your attention!

- *More information about FIWARE-Ops: www.fi-xifi.eu/fi-ops*
- *FI Ops - by the XIFI Technical Team*

Federico Alvarez- Universidad Politecnica Madrid
federico.alvarez@upm.es