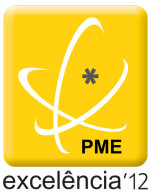
Manual UnitBox G2 v1.2.2

Eurotux Informática, S.A.

April 11, 2013

Rua Irmãs Missionárias do Espírito Santo, 27
4715-340 Braga
Portugal

Tel: +351 253 680 300
Fax:+351 253 680 319



Change Log

2013-02-11 – Carlos Rodrigues <cmar@eurotux.com>
Update some images, add Section *Changelog* and change name UnitBox

2012-10-03 – Carlos Rodrigues <cmar@eurotux.com>
Section *Servers*, *Snapshots* added

2012-10-01 – Carlos Rodrigues <cmar@eurotux.com>
Section *Virtual cluster*, *Edit cluster* update *Node High availability*

2012-07-23 – Carlos Rodrigues <cmar@eurotux.com>
Section *Virtual cluster*, sub-section *Nodes* updated and rebrand some images for NUXIS

2012-07-20 – Carlos Rodrigues <cmar@eurotux.com>
Sub-section *Storage* updated

2012-07-13 – Carlos Rodrigues <cmar@eurotux.com>
Sub-section *Edit virtual machine* updated

2012-05-17 – Manuel Dias <mfd@eurotux.com>
Name change from ETVM to NUXIS. Sub-section *Edit virtual machine* updated

2012-04-20 – Carlos Rodrigues <cmar@eurotux.com>
Version change

2011-12-19 – Manuel Dias <mfd@eurotux.com>
English version of the manual

2011-11-30 – Manuel Dias <mfd@eurotux.com>
Sub-section *Drivers virtio* of Section *Virtual machine*

2011-11-21 – Manuel Dias <mfd@eurotux.com>
Sub-section *Virtual cluster management* of Section *System administration*

2011-10-13 – Manuel Dias <mfd@eurotux.com>
Sub-section *User, groups and permission administration* of Section *System administration*

2011-07-13 – Carlos Rodrigues <cmar@eurotux.com>
Sub-section *ETFW* of Section *ETVA Management Agents*

2011-07-01 – Carlos Rodrigues <cmar@eurotux.com>
Sub-section *Primavera* of Section *ETVA Management Agents*

2010-08-06 – Ricardo Gomes <rjg@eurotux.com>
Initial version.

Contents

List of Figures

1. UnitBox

Description

NUXIS is a centralized tool that allows the management of available resources on a network. It consists of a Linux distribution pre-installed and configured, which allows you to manage servers' resources.

The NUXIS is divided into two functional blocks:

- *Central Management* (CM)
- *Virtualization Agent* (VA)

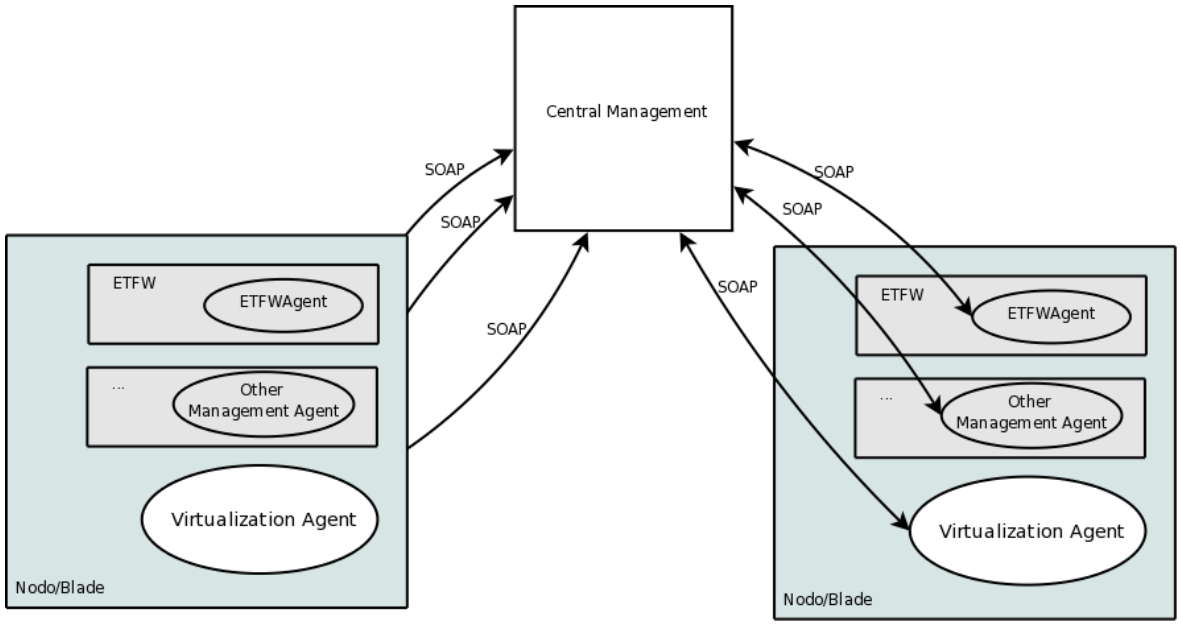


Figure 1.1.: NUXIS architecture

The CM (Central Management) is the block responsible for managing the entire infrastructure. The *Virtualization Agents* are responsible for processing the requests between the virtualization server (*node*) and CM.

Within a virtualization server there may be virtual machines with *Management Agents*. These type agent enables the managing of existing services/applications on the virtual machine (see Figure 1.1).

In the NUXIS, there are several virtualization servers (nodes) that communicate with the CM. The initial network configuration is performed, using VLANs through the *One time setup wizard* as shown in Figure 3.67.

In this particular version, the model of NUXIS consists of a single virtualization server where the CM and VA are pre-installed. The node's network configuration in this model consists of four network interfaces: Internet, LAN, DMZ and Management.

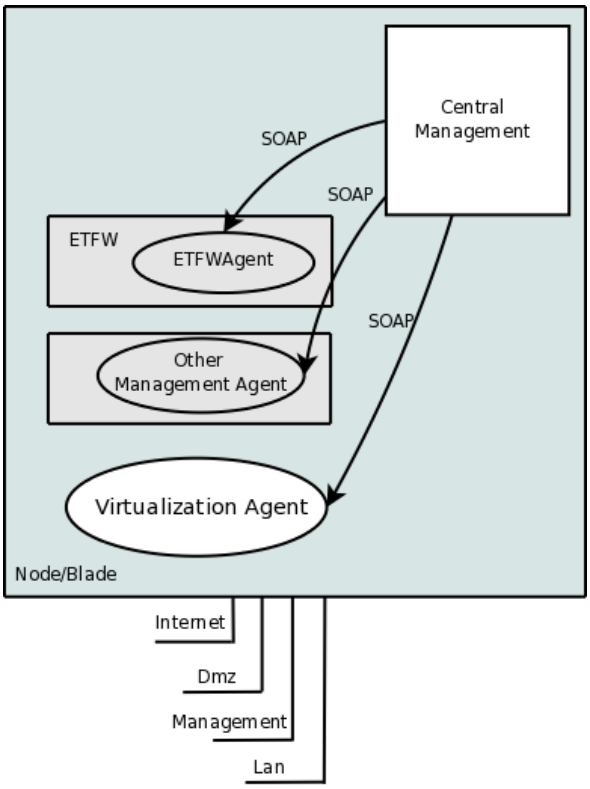


Figure 1.2.: UnitBox NUXIS model

This user's manual describes the configuration management tool (CM - *Central Management*).

2. Installation

2.1. Standard version

To make the installation we should plug the appliance into: electricity, a keyboard, a monitor, and an external USB CD drive. Then the appliance should boot from de cd drive, and we can see the installation menu as shown on Figure 2.1:

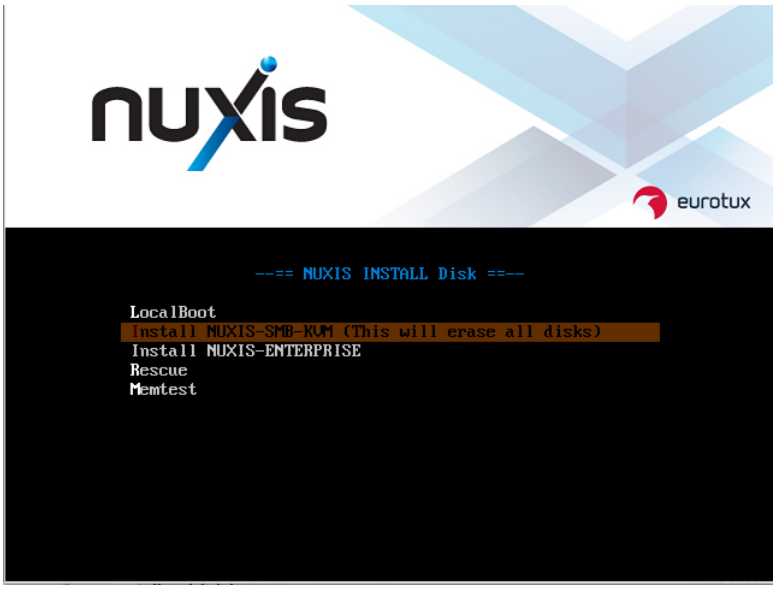


Figure 2.1.: NUXIS installation menu

Then, by selecting the option *"Install ETVA-SMB KVM-(This will erase all disks)"*, will start the installation as:

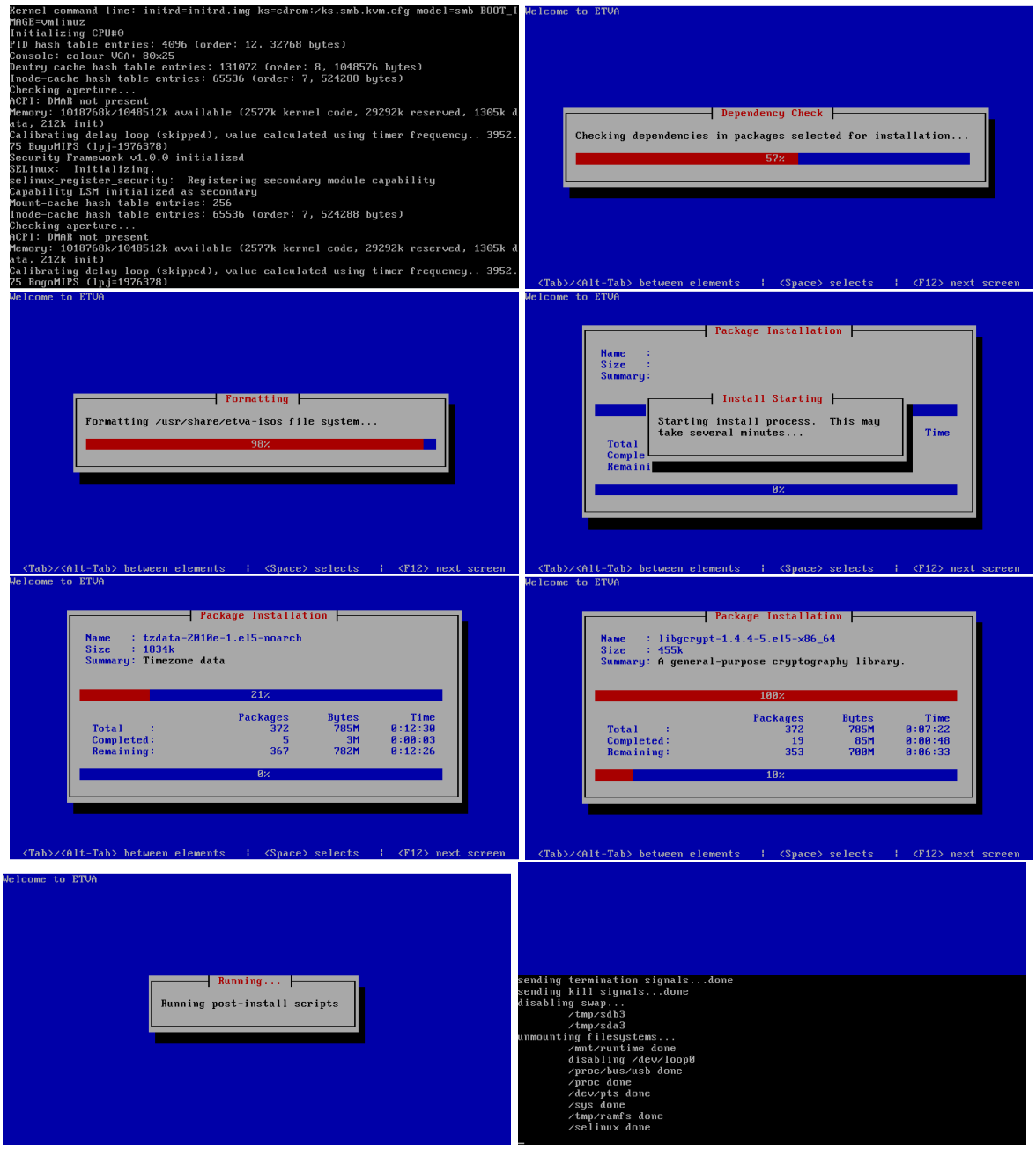


Figure 2.2.: NUXIS installation process

After the installation, the appliance boot must be done from the hard drive and then we should see a window like the following (2.3):

Figure 2.3.: NUXIS boot menu

At the end of the installation, connect a network cable in your PC and in the appliance management port as stated in Figure 2.4.

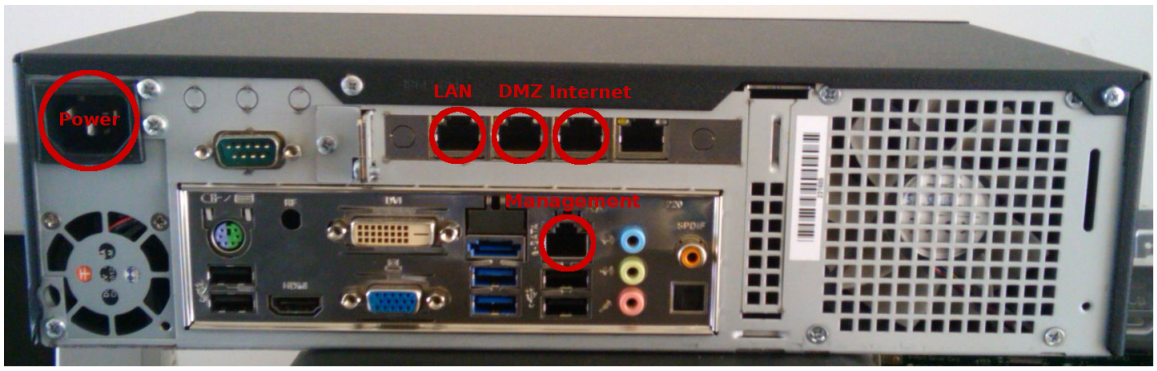


Figure 2.4.: UnitBox version - Management ports

Then set up the network card of your PC with the following settings:

IP address: 10.10.4.1
Network mask: 255.255.255.0

Finally, open a web browser and access the following address:

http://10.10.4.254/

3. Central Management

The main frame of Central Management consists in four areas:

Top panel - This panel provides the necessary menus for main system configuration, such as user administration, ISOs management and the interface that shows the system events.

Left panel (*Nodes*) - This panel lists the real machines/virtualization servers - ***nodes*** - and any existing virtual machines - ***servers***. The first level of the tree show the system datacenters. After that level we can find the available physical servers, and on the bottom nodes the virtual machines. All functionalities that can be donne on each node of the tree, are described on Section 3.4(Node) and in Section 3.5(Server). When some node is clicked, its information is loaded and appears on the main panel.

Main panel (at right) - In this area is displayed the information about the selected node.

Information panel (at bottom) - This areas shows the volatile information about any operations made on the interface. Here we can found the success of the operations.

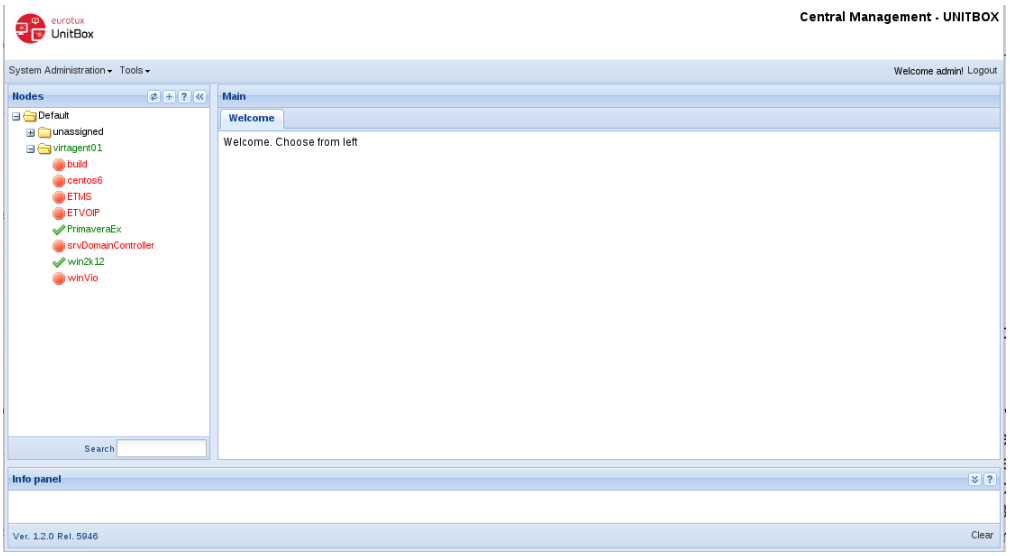


Figure 3.1.: Layout principal

3.1. First access

After the installation, the CM can be accessed on the web browser by entering the address http://<IP ADDRESS>[1]

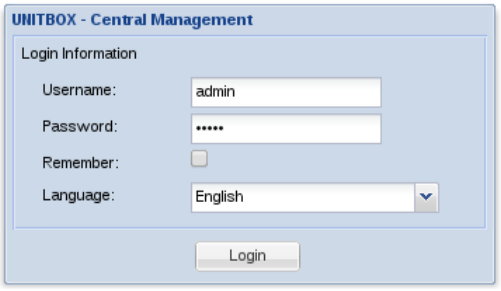


Figure 3.2.: Authentication window

The Figure 3.2 shows the first displayed frame, that asks the user his username and password. In this window we can also select the pretended language[2].

Note

The default credentials are:

Username: admin

Password: admin

For safety reasons the default password should by changed. This can be donne after the first access, on the *first time wizard*.

During the first access, the user is prompted with some questions, that allows him to setup the system (see Section 3.7).

After the installation and configuration of the CM, and having an already installed agent, it should appear automatically on the left panel.

On the left panel, see Figure 3.1, will appear the virtualization *node* registered on CM. We can right click the *node* and select the option *Authorize*. In this case the cm sends a message to the virtualization agent, requesting information about the *node*. After the end of the authorization process, the *node* can be managed as stated on Section 3.4.

[1] The ip address is specified during the installation process , described in Chapter 2 .
[2] Currently two languages are available: Portuguese an English

3.2. Default cluster

In this panel we can see an overview of the CM. The virtualization servers can be seen as well as any existing networks (see Figure 3.3).

3.2.1. Nodes

In *Nodes* we can see some information about the virtualization servers such as the supported hypervisor, the state of the virtualization server, among other info.

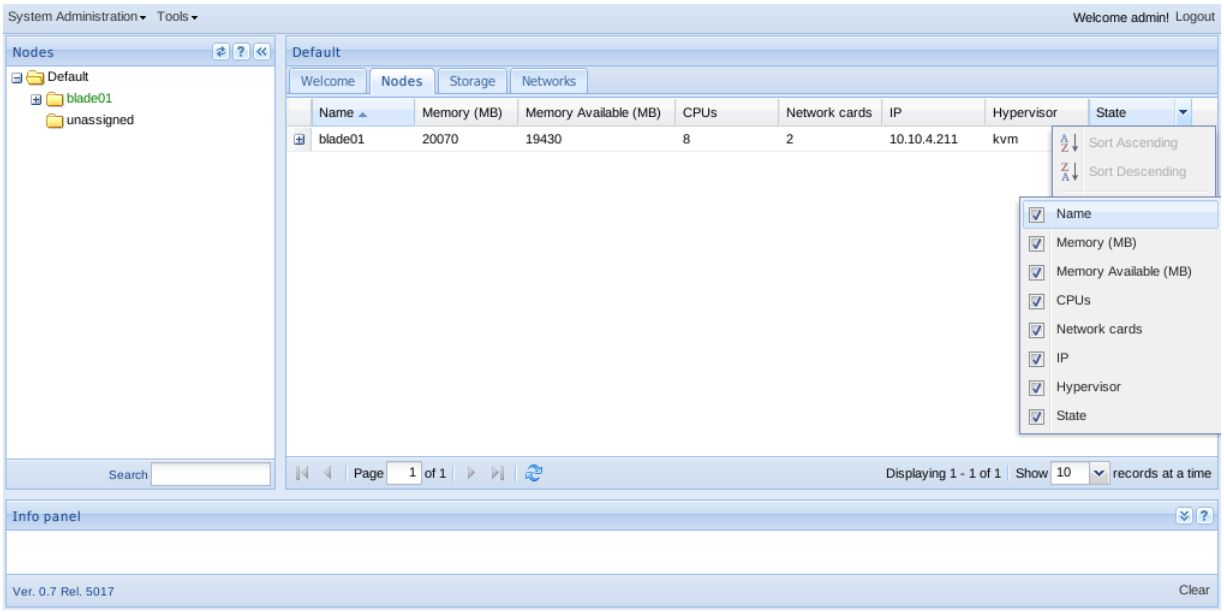


Figure 3.3.: Central Management nodes view

3.2.2. Networks

This panel allow us to do the following operations:

- System's network administration
- MAC address pool management
- Manage the virtual machines' network interfaces

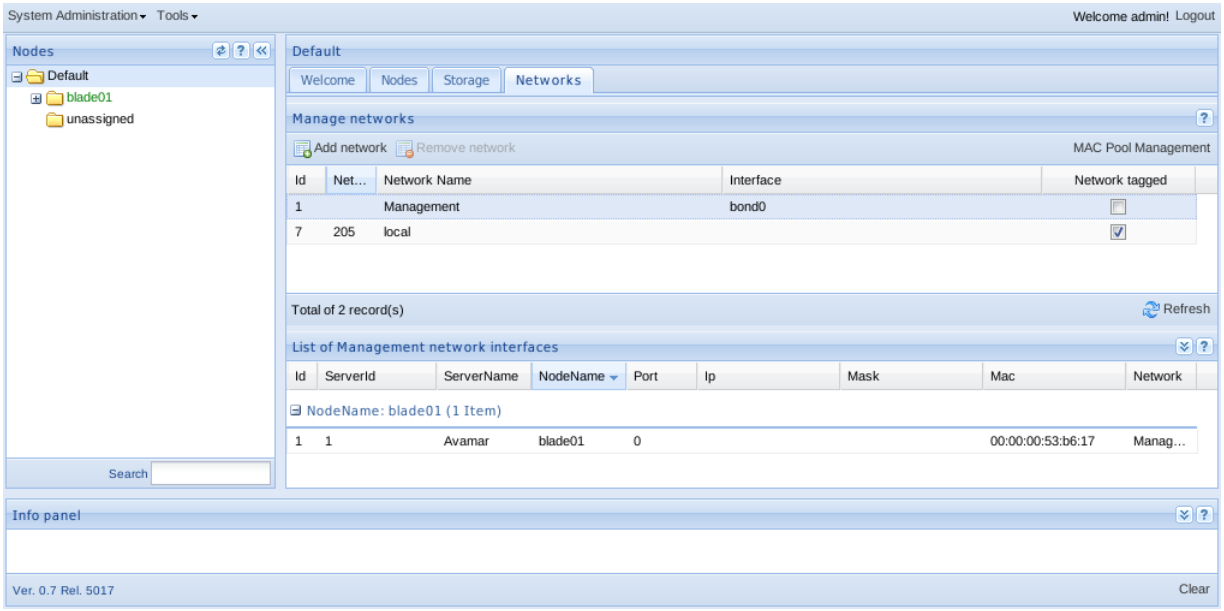


Figure 3.4.: System networks view and virtual machines' interfaces

Also, it's possible to filter the network interfaces by a given network, as stated on Figure 3.4. The Figure 3.4 lists the network interfaces for the network *Internet*.

3.2.2.1. Network administration

To add a network, click on the *Add network* button.

The network info is constituted by its name and ID[3]

To remove a network, choose the desired network and press the button *Remove network*.

> **Note**
>
> The add/remove operations are only available on version UnitBox .

[3] If the network/vlan is *tagged*, the field *network ID* refers to its *VLAN ID* (see Figure 3.5)

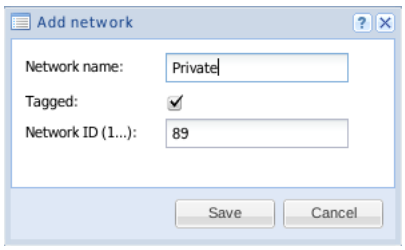


Figure 3.5.: Add network window

After successfully add or remove a network, all Central Management nodes are notified.

3.2.2.2. MAC address pool management

On *MAC Pool Management* (see Figure 3.4), its possible to create new addresses. Also, we can see the associated network for each MAC address, and the available addresses.

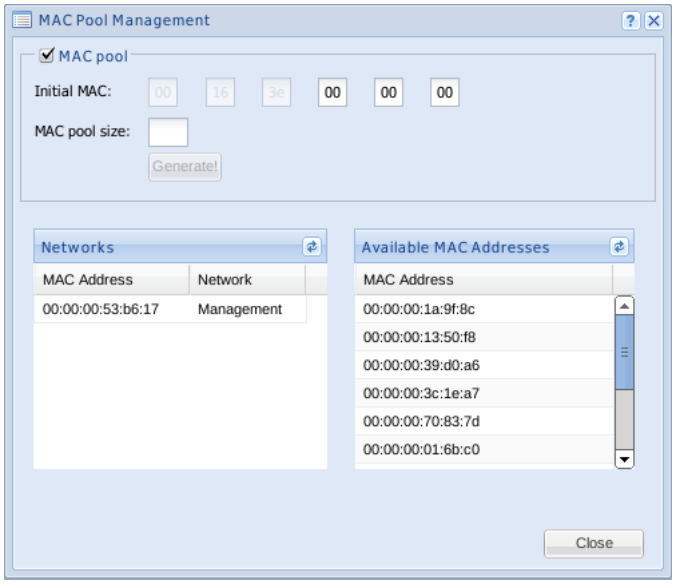


Figure 3.6.: MAC pool creation window

3.2.2.3. Virtual machines' network interfaces management

If we select a network interface and access to the context menu, it's possible to remove the network interface associated to this record - *Remove network interface* or change the network interfaces for the associated virtual machine - *Manage network interfaces*.

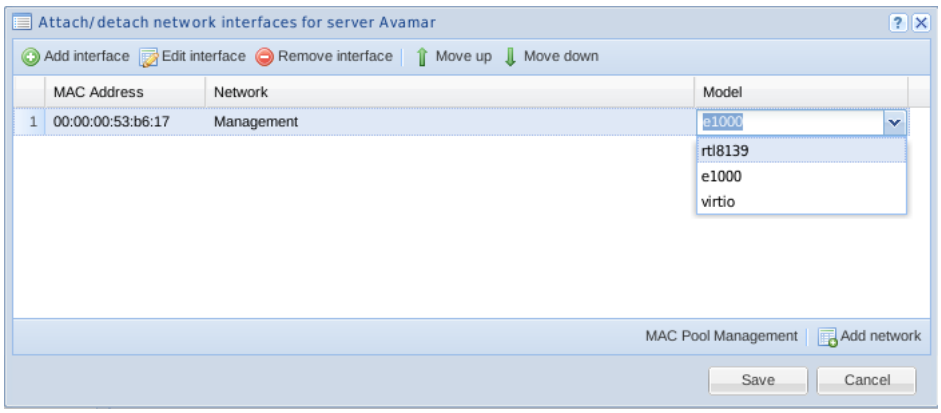


Figure 3.7.: Virtual machine interfaces (management window)

On the management window it's possible to select the network card's driver[4].

3.3. Virtual cluster

On left side panel it's possible to select a *cluster*(virtual cluster) and do the following operations:

- *Nodes* - View information about nodes (see Section 3.2.1)
- Storage - Storage management on *Cluster* context (see Section 3.4.3)
- Networks - Network management (see Section 3.2.2)

In addition. it's possible to access the context menu (right click) to perform the following operations:

- Edit cluster
- Remove cluster

In *Edit cluster* it's possible to change the name of *cluster* and allow use to activate nodes high availability.

[4]This option is available on HVM or KVM machines. The available drivers are: e1000, rtl8139 e virtio

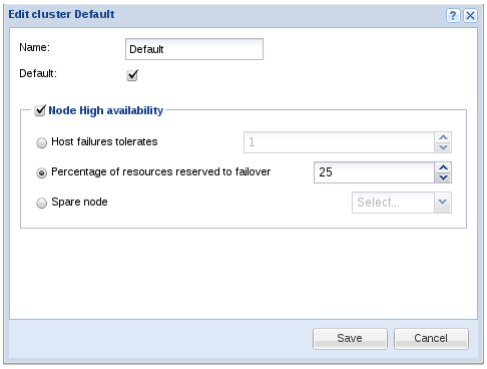


Figure 3.8.: Edit cluster

When we enable *Node High availability*[5], we may choose one of this options:

- *Host failures tolerates* - number of hosts in failure that we can garantee high availability with restrictions of resources allocation;
- *Percentage of resources reserved to failover* - percentage of resources reserved to garantee the high availability of critical services;
- *Spare node* - it's define one *spare node* that will be used to garantee the high availability of one of the others nodes. This *spare node* should have necessary resources to ensure the availability of critical virtual servers of fail node.

The *Node High availability* provides, in failure case, the migration of the virtual servers by priority order (see figure 3.27), to keep the services of this virtual servers operational.

The operation *Remove cluster* removes information related to *cluster* (nodes, networks and storage) from the *Central Management* database.

3.4. Virtualization server

On panel *Nodes* it's possible to select a *node*(virtualization server), and do the following operations:

- See the *node* information (see Section 3.4.1)
- Manage its virtual machines (see Section 3.4.2)
- Manage *node* storage (see Section 3.4.3)

In addition to these options, it's possible to access the context menu (right click). This menu allow us to perform the following operations:

[5]The option *Node High availability* will be enable only if *fencing* configuration is defined for all node (see 3.4)

- Load node
- Edit node
- Remove node
- Connectivity options [6]
- Change keymap
- Check node state

In *Load node*, it's send one request to *Central Management* for node state update.

For operation *Edit node* it's available edition of server virtualization proprieties like name and *fencing* device configuration.

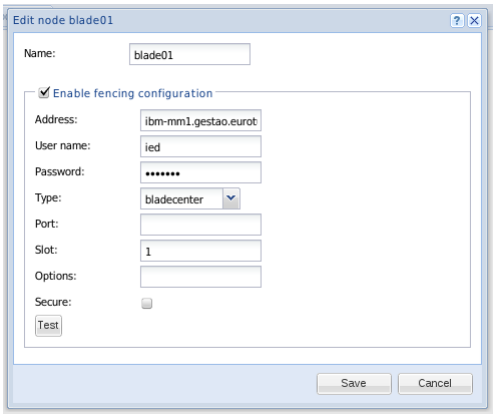


Figure 3.9.: Edit node

In *Enable* fencing *configuration* we can activate *fencing* device for node management and configure the parameters accord on following types: *bladecenter*, *virsh*, *ilo*, *ipmilan* e *rsa*.

The operation *Remove node* removes one node from the *Central Management* and delete the information related to it on database.

In *Connectivity options*, it's possible to configure the interface *Management* that is connected with the virtualization agent.

[6] Only available on version *NUXIS*

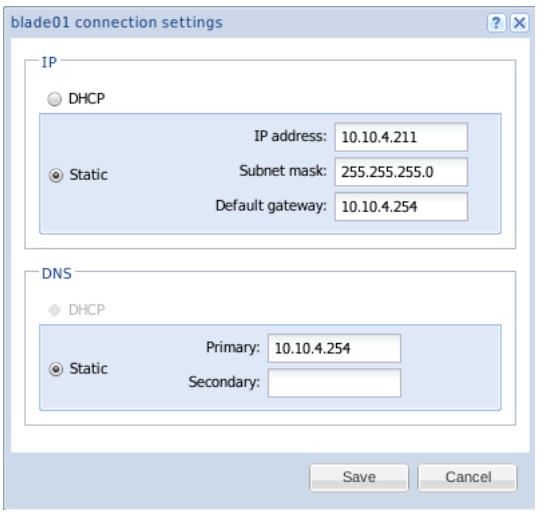


Figure 3.10.: Agent connectivity configuration

In *Change keymap*, depending on the selected item, the virtualization server or virtual machine, it's possible to define the standard VNC keymap, or the specific virtual machine keymap.

In *Node status*, it's possible to access to subset of options:

- Check status - it send an request to the virtualization server to check the agent connectivity
- Maintenance / Recover - Put the node in maintenance/recover mode
- Shutdown - it shuts node down (see Section 3.4.5).

In operation *Maintenance* we able to put node in maintenance mode in order to run maintenance tasks.

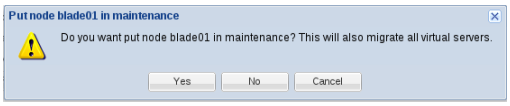


Figure 3.11.: Node maintenance

When node is moved to maintenance mode, the virtual servers will be migrated by priority order (see figure 3.27).

The operation *Recover* runs some tasks like node agent status check, connectivity and storage info consistency, before recover node from maintenance mode.

3.4.1. Node information

In *Node information* we can see the information about the virtualization server. We can see the "real" machine supported hypervisors and, among other information, the virtualization agent's state.

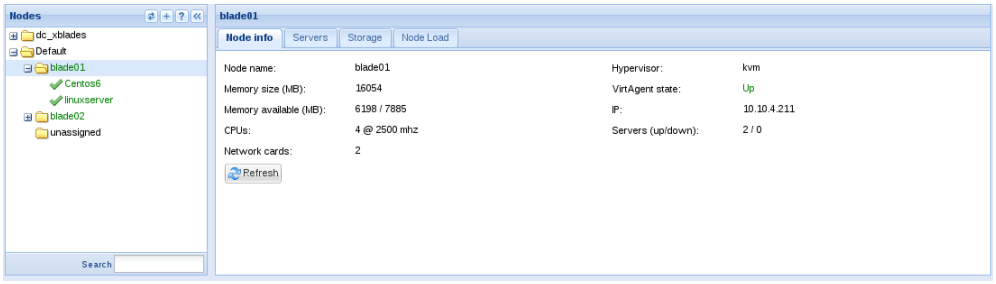


Figure 3.12.: Node's information

3.4.2. Servers

In *Servers* we can see the information of every virtual machines existing on the selected virtualization server. In addition, allows to perform the following operations:

- Add a virtual machine
- Edit a virtual machine
- Remove virtual machine
- Access virtual machine in a VNC console
- Start/Stop virtual machine
- Migrate virtual machine
- Snapshots

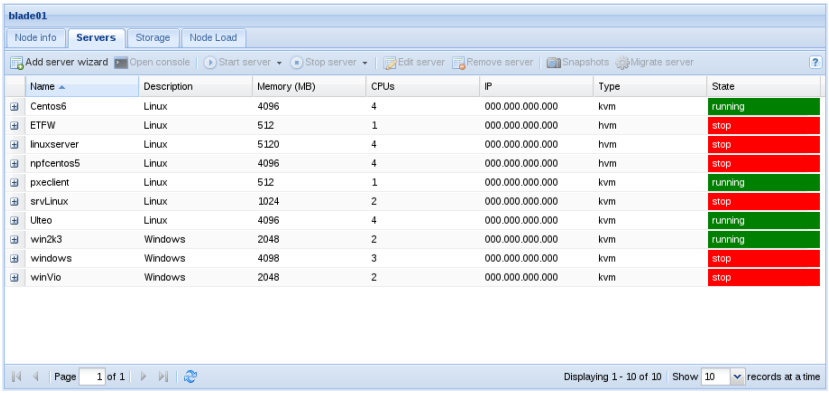


Figure 3.13.: Node's virtual machines

3.4.2.1. Add virtual machine

To add a new virtual machine, press the button *Add server wizard*.

Note

The panel options will be enable, if the virtualization agent is running on the *node* (physical machine) and if it is able to stablish a connection with the CM.

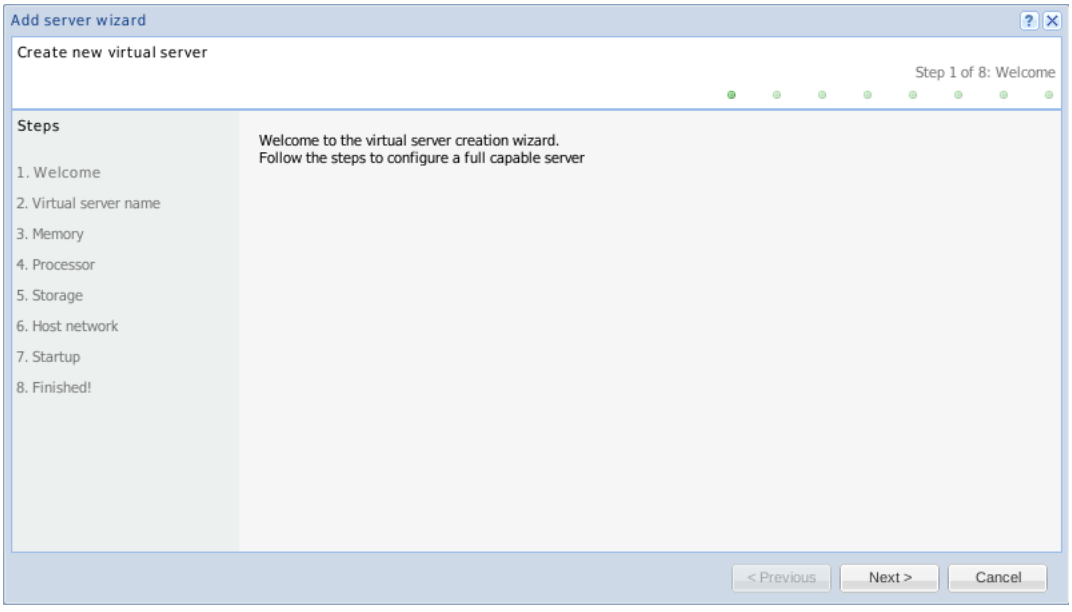


Figure 3.14.: Add server wizard - Welcome

The server wizard has the following steps:

Virtual machine name: In this step we can define the virtual machine name and the type of the operating system. The operating system option varies depending on the type of virtualization node.

- with XEN e hardware virtualization support:
  - Linux PV
  - Linux HVM
  - Windows
- with XEN without hardware virtualization support:
  - Linux PV
- with KVM
  - Linux
  - Windows

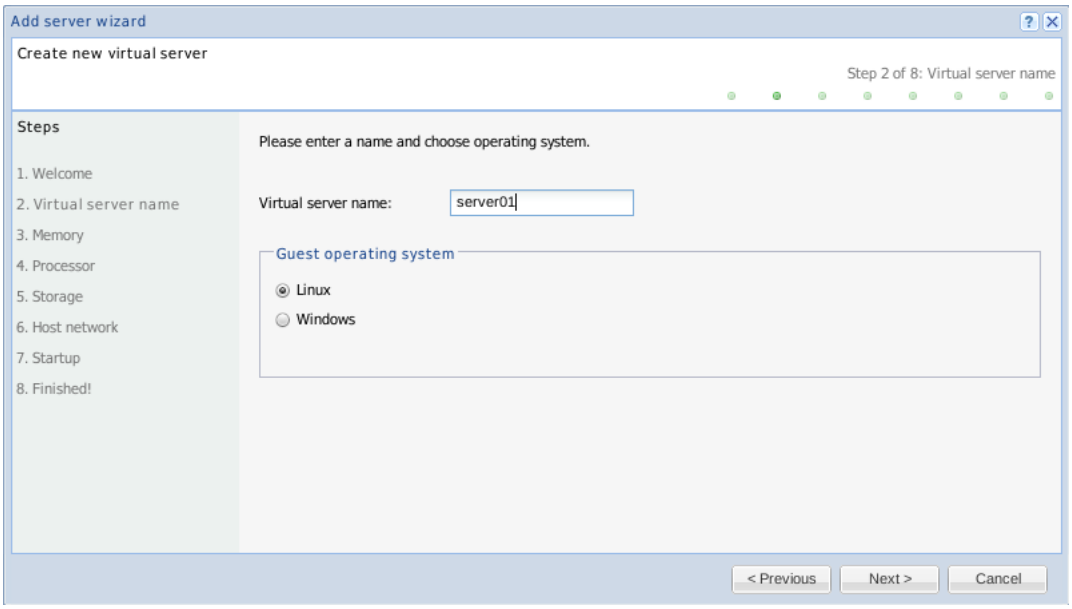


Figure 3.15.: Add server wizard - Virtual machine name

Memory: Total assigned memory.

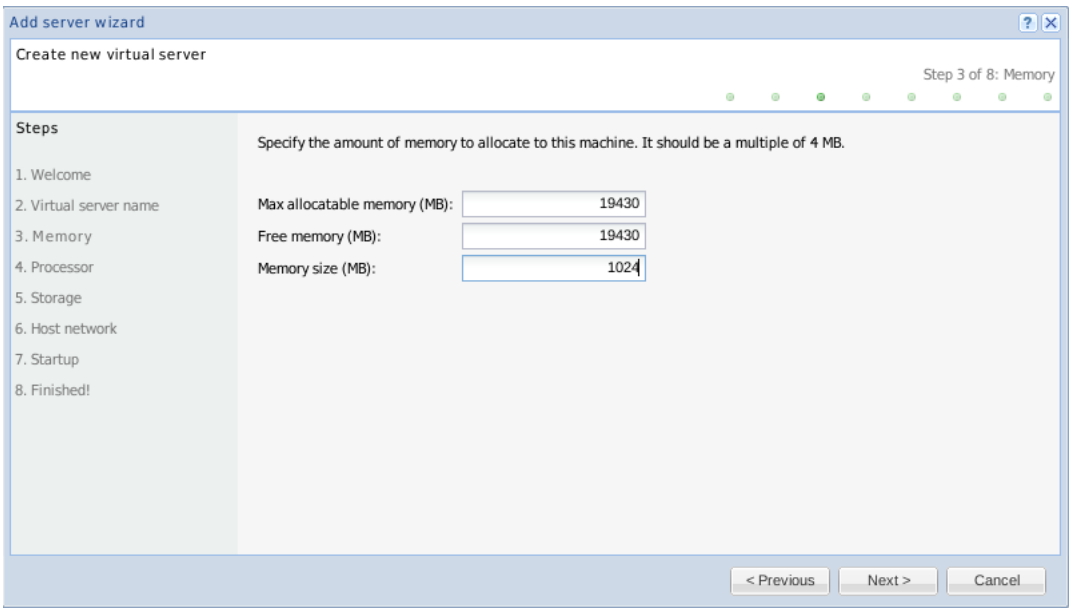


Figure 3.16.: Add server wizard - Memory

Processor: In this stage is necessary choose the number of processor that the virtual machine will have access.

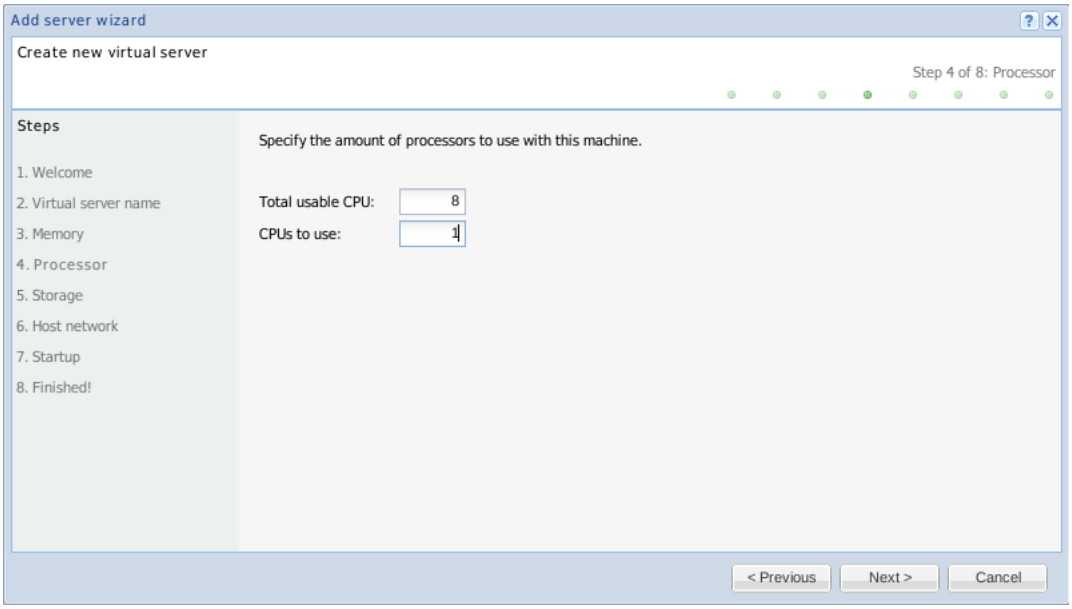


Figure 3.17.: Add server wizard - Processors

Storage: Defines the boot disk for the virtual machine. One of three options can be chosen:

- use an existing logical volume/file - *Existing logical volume*

- create a new logical volume - *New logical volume*
- at last, a file can be created on the option *New file*

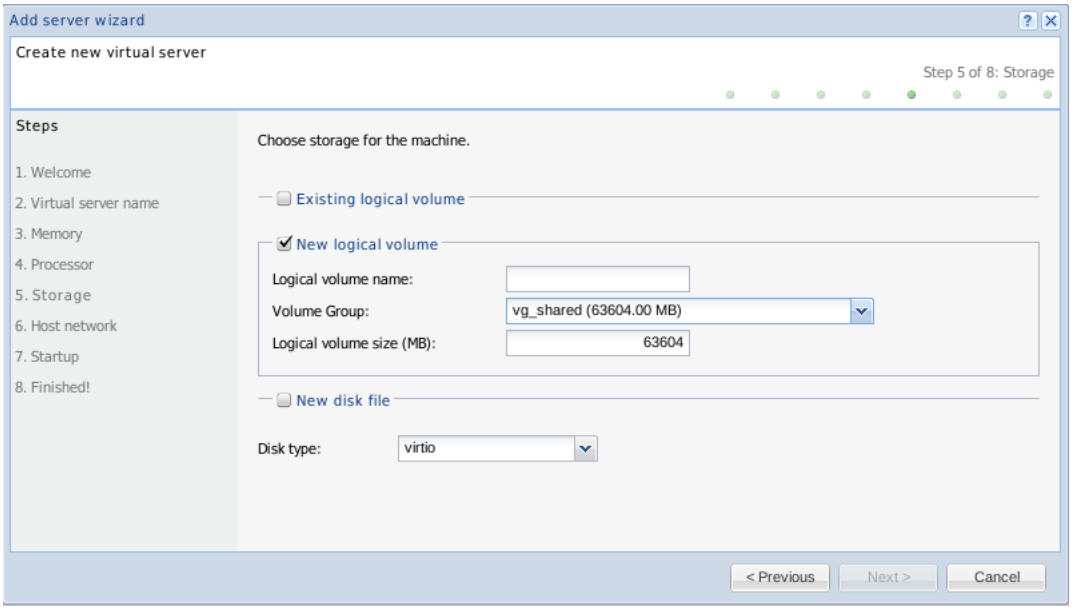


Figure 3.18.: Add server wizard - Storage

Note

If the *node* does not support *physical volumes* the option *Existing logical volume* will be disabled.

Host network: Network interfaces for the server. If there are no available MAC addresses, it's possible to create new ones by pressing the *MAC pool management*. Is also possible to create networks in this step using the button *Add network*.

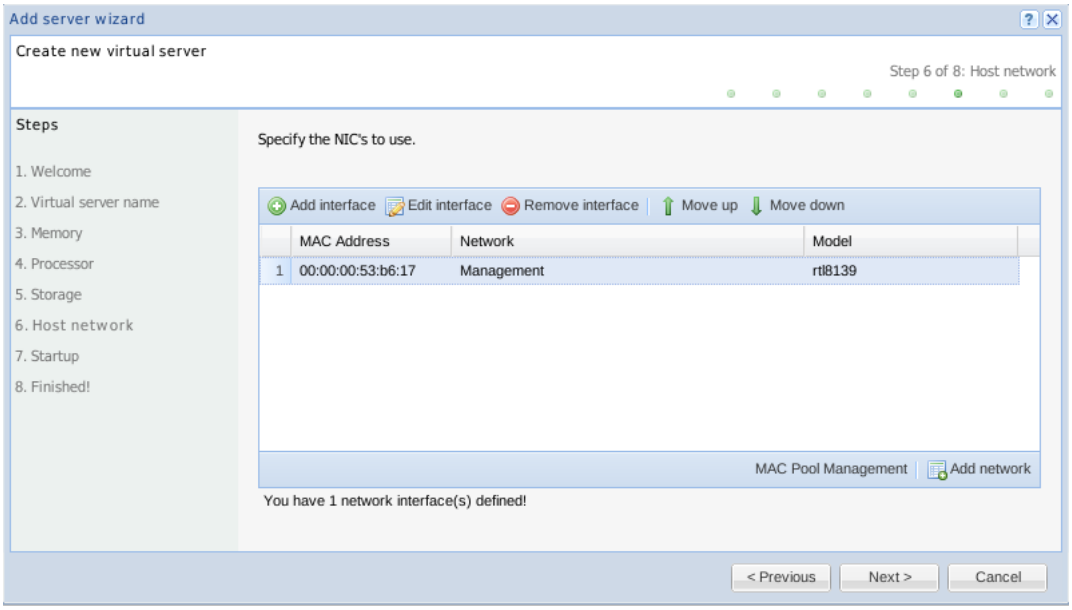


Figure 3.19.: Add server wizard - Host network

Startup: Specifies startup parameters of the virtual machine. The options at this stage vary with the type system, defined in step *Virtual machine name*:

- *Linux PV*
  - Network installation. Url of the kernel.
- Others
  - Network Boot (PXE)
  - CD-ROM (ISO)

The figure 3.20 refers to a virtual machine options for *Linux* in *KVM*.

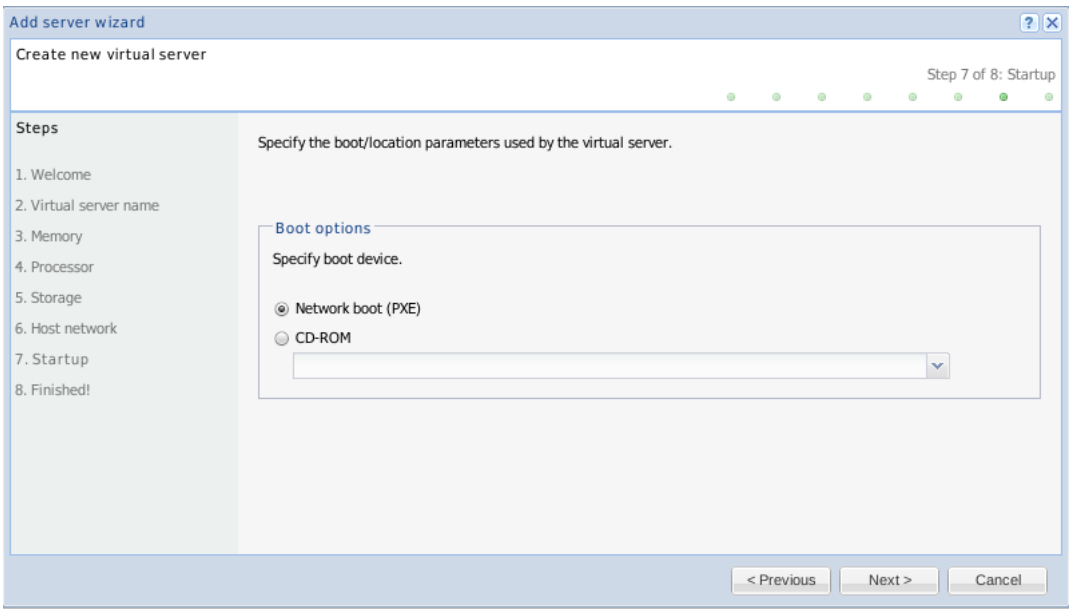


Figure 3.20.: Add server wizard - Startup

Finished! Final step of the wizard. After confirmation of the creation of the server, the data collected in previous steps are processed and sent to the virtualization server. Later in the panel *servers* the virtual machine can be initiated through the option *Start server*.

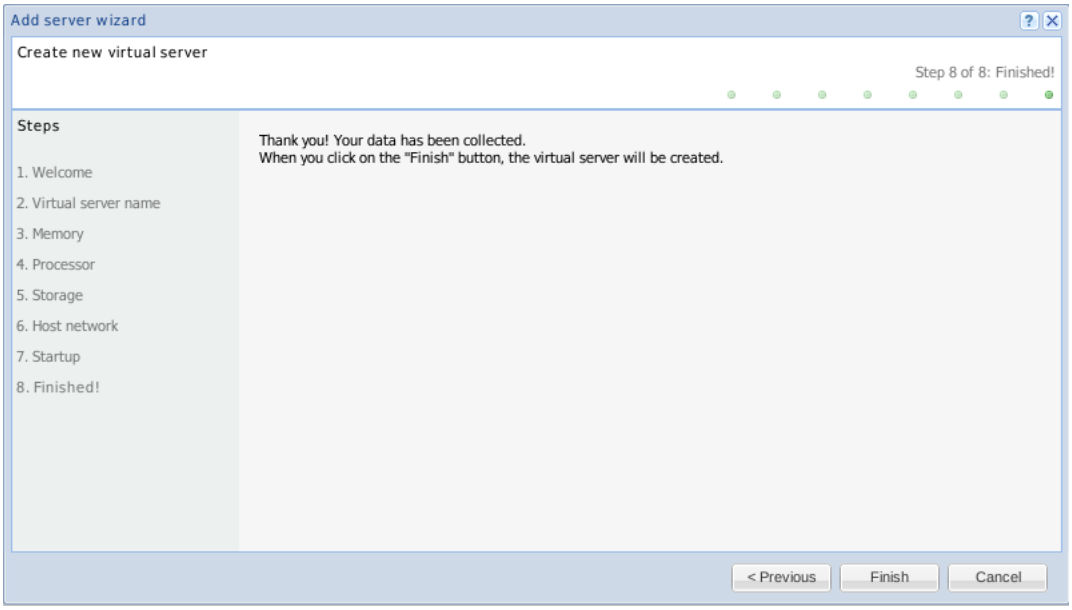


Figure 3.21.: Add server wizard - Finished!

3.4.2.2. Edit virtual machine

To edit a server, you choose the machine you want and click on *Edit server*.

> **Note**
>
> If the virtual machine is running, depending on the virtual machine type and the virtualization system, some options will be disabled, it is require stop the machine in order to make the changes.

The following options are available on virtual machine configuration:

General: This allows change the name, memory, number of CPUs and number of sockets, cores and threads, operating system and boot parameters. The boot parameters vary depending on the virtual machine type and the virtualization system. (see Section 3.4.2.1).

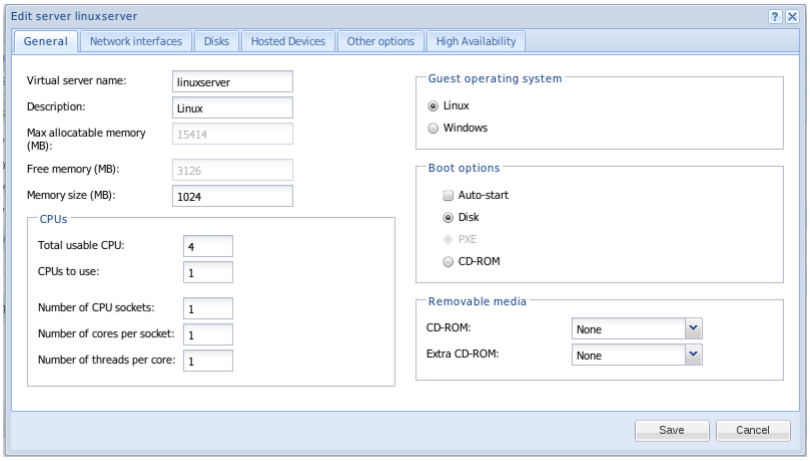


Figure 3.22.: Edit server - General

Network interfaces: Add/remove interfaces. Here we can change the type of driver to use[7].

[7] You can only specify the driver to use if the virtual machine is HVM and KVM

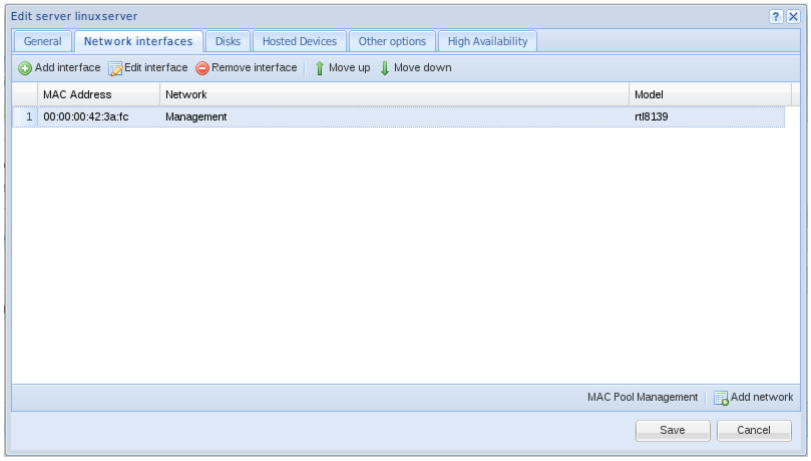


Figure 3.23.: Edit server - Network interfaces

Disks: Add/remove machine disks. To add/remove a disk, select the desired disc and drag-n-drop between the tables.

Note

The boot disk is the disk of the machine that is in first position of the table.

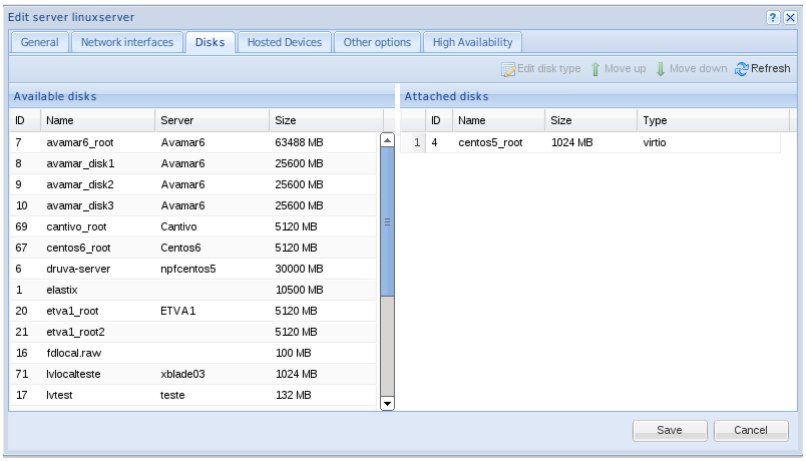


Figure 3.24.: Edit server - Disks

Devices: Attach/detach USB/PCI devices into the virtual server. A device can only be associated with one virtual server.

Note

If the virtual server have any associated devices, it cannot be migrated/move into another node of the cluster.

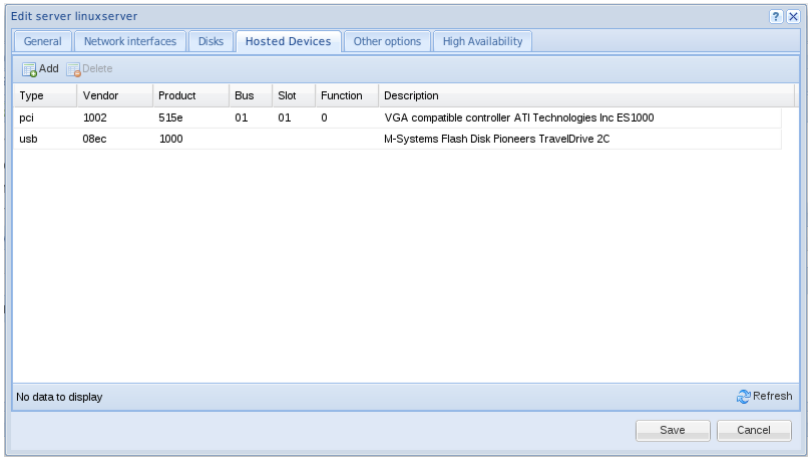


Figure 3.25.: Edit server - Devices

Other options: Lets you set VNC options like keymap and configure ACPI, APIC and PAE flags.

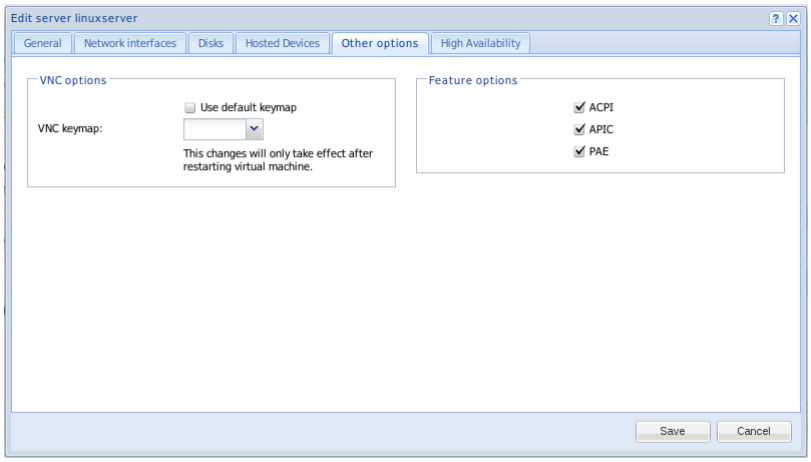


Figure 3.26.: Edit server - Other options

High availability: Provides a way to configure server priority to start and to migrate and define if high availability is active on this server.

Nota

For *VM High availability* we set heartbeat timeout that server should be restart if not responding. This option will be available only if the guest tools are installed on virtual machine.

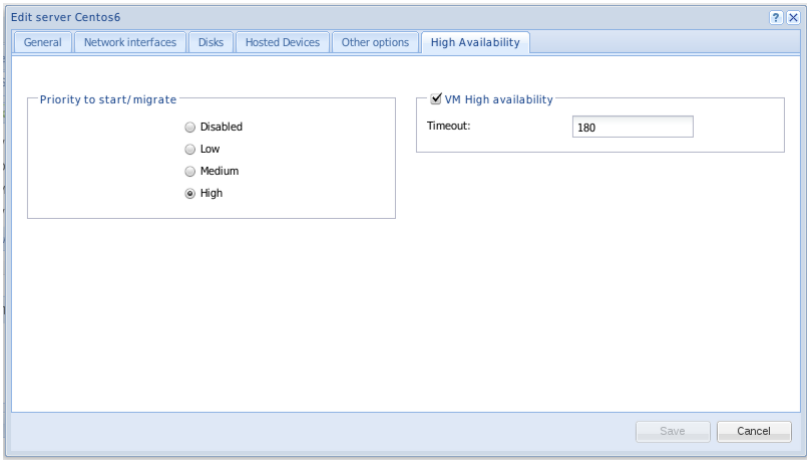


Figure 3.27.: Edit server - High availability

3.4.2.3. Remove virtual machine

To remove a server, choose the machine to remove and click on the button *Remove server*.

The *Keep disks* option keeps the hard disks connected to the machine, otherwise it will also be removed.

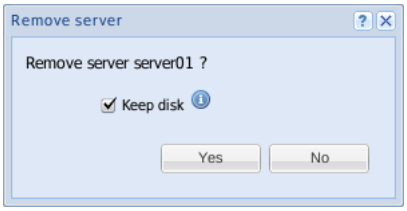


Figure 3.28.: Remove server window

3.4.2.4. Connect to a virtual machine over VNC

Selecting a server and then clicking on button *Open console* is possible to establish a VNC connection with the machine, since the machine is running.

Note 1

If the keyboard is mangled you can change the *VNC keymap* through the option *Set keymap* available in parent node context menu. Also, the *keymap* can be defined in each server, through the option *Edit server*.

Note 2

When open VNC console with HTTPS we may get the following error:

```
Network Error: sun.security.validator.ValidatorException: PKIX path building fa
```

In this case, it maybe required to add server certificate to Java *keystore*[8]. For do that, we can run this command:

```
keytool -import -keystore $JAVA_HOME/lib/security/jssecacerts -file server-cert

# Note: for keystore without password we can use "changeit"
```

After that, we need restart the browser.

3.4.2.5. Start/stop virtual machine

It's possible to choose between one of the following boot parameters to start the virtual machine:

VM Filesystem: Boot from the disk associated with the server.

PXE: Boot from PXE[9].

Location URL: Boot from url defined in *Location*[10].

CD-ROM: Boot from a CD-ROM image[9].

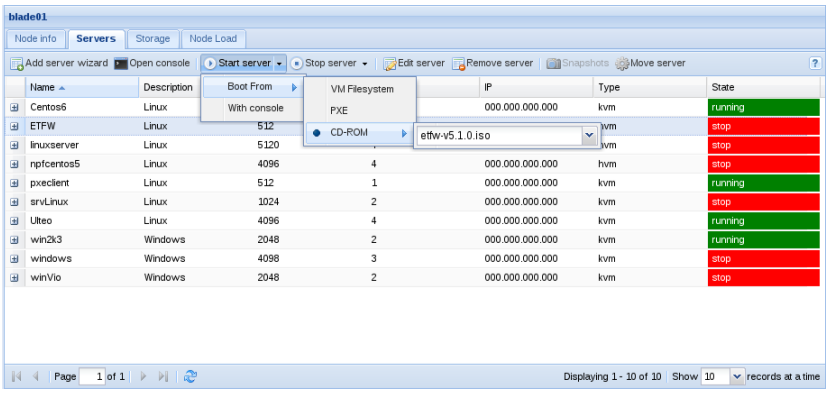


Figure 3.29.: Virtual machine boot parameters

It's possible to choose the option *Start server With console* to allow start the server and open console.

[8]For more information acess to the following links: http://docs.oracle.com/javase/7/docs/technotes/tools/solaris/keytool.html and http://docs.oracle.com/javase/7/docs/technotes/guides/deployment/deployment-guide/jcp.html

[9]Only available if the type of virtual machine is not *Linux PV*

[10]Only available if the type of virtual machine is *Linux PV*

3.4.2.6. Migrate virtual machine

Selecting a server and then clicking on *Migrate server* you can migrate a machine from a *node* to another, since they share the same storage.

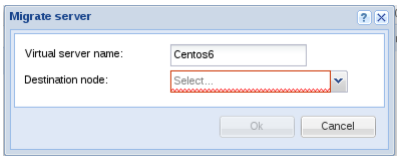


Figure 3.30.: Virtual machine migration

Note

This option is only available on *NUXIS*.

3.4.2.7. Snapshots

In *Snapshots* we can create one *snapshot* of virtual machine state, that consists on disks snapshots and, if virtual machines is running, the state of virtual machine on that moment. It's also possible revert, remove or download of backup of one virtual machine snapshot.

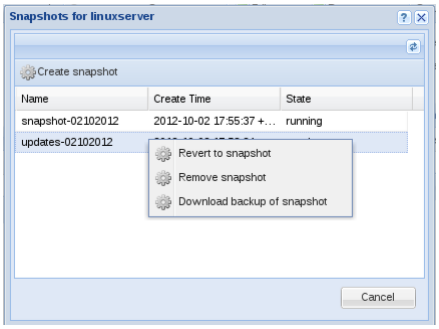


Figure 3.31.: Snapshots

3.4.3. Storage

The information about the existing volumes on the *node* can be found on the tab *Storage*. This panel is divided into three sections:

Devices - Information about the *physical volumes*[11] and its state. Allows to do the *physical volumes* administration of the *node*.

[11] A *physical volume* it's a physical device, such as a disk

Volume Groups - List of *volumes groups*[12] existing in the node and its associated *physical volumes*. Allow *volume groups* management.

Logical Volumes - Displays information about the *logical volumes*[13] *node*. *Logical volumes* administration area.

Note

There is a special *volume group*, __DISK__, used in the handling of files. When creating a *logical volume*, this tag is used to indicate that the disk to be used is not a *logical volume* but a file.

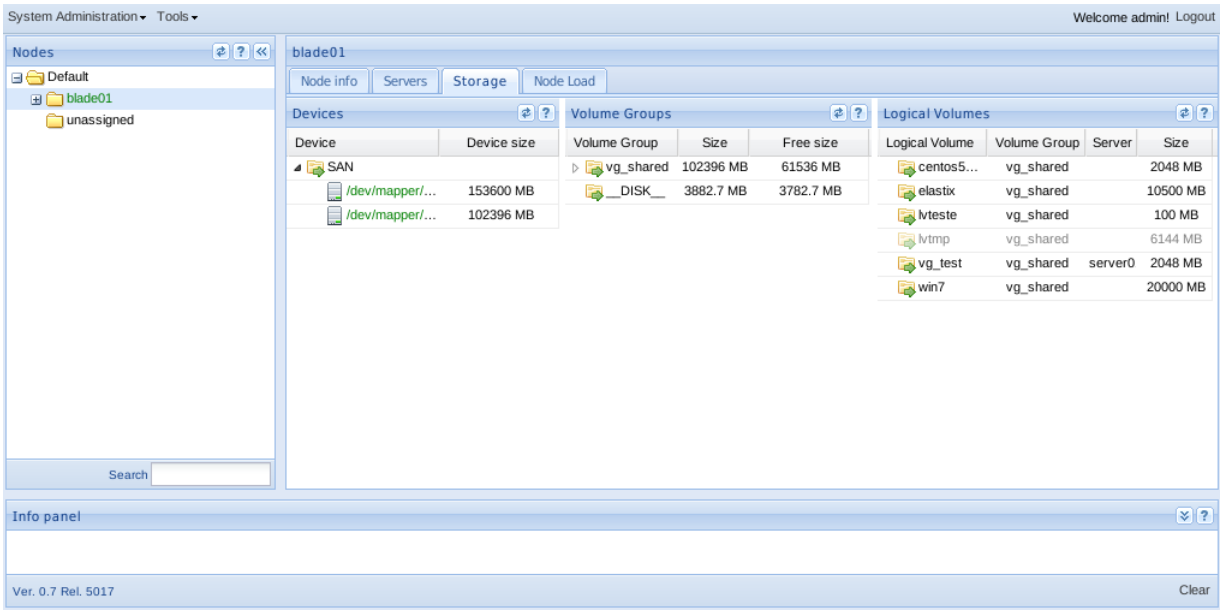


Figure 3.32.: Information about node's storage

3.4.3.1. Physical Volumes administration

The *physical volumes* administration consists of the following operations:

- Initialize *physical volume*
- Uninitialize *physical volume*
- Register/Unregister *physical volume*

[12] A *volume group* is the aggregation of several *physical volumes* in a single virtual volume
[13] A *logical volume* it's a slice of a *volume group*. It's used as a system's partition

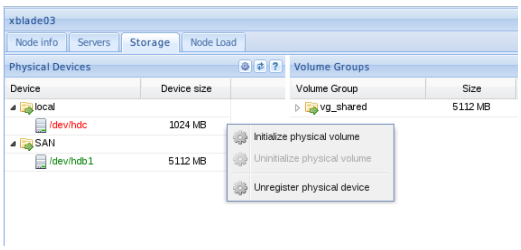


Figure 3.33.: Context menu of a physical volume

To initialize a *physical volume*, access to the sub-context menu of the device and select *Initialize physical volume*. To remove a *physical volume* the operation is similar, simply select the option *Uninitialize physical volume* in the context menu.

Note

The *physical volume* can only be removed if it does not belong to any *volume group*.

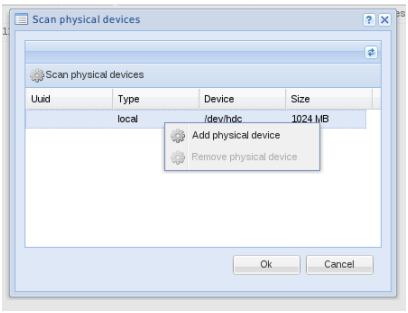


Figure 3.34.: Scan *physical devices*

On "Scan *physical devices*" it is possible to run a task on virtualization agent to lookup new disks and to register them on *Central Management*. It is also possible to unregister the physical device on *Central Management* to get it out of system management.

3.4.3.2. Volume groups administration

In the administration of *volume groups* is allowed to:

- Add *volume groups*
- Extend a *volume group*
- Re-size a *volume group*
- Remove a *volume group*

- Register/Unregister *volume group*

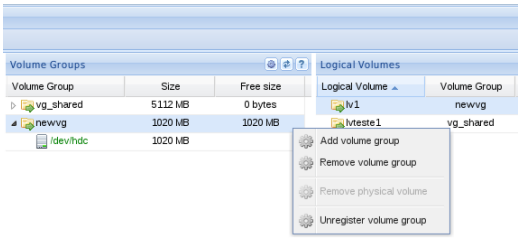


Figure 3.35.: Context menu of a volume group

To create a *volume group*, access to the context menu on any *volume group* and select *Add volume group*. The *volume group* name should be introduced and selected one or more *physical volumes* available.

A *physical volume* is available when volume is not allocated to any *volume group* and it's initialized.

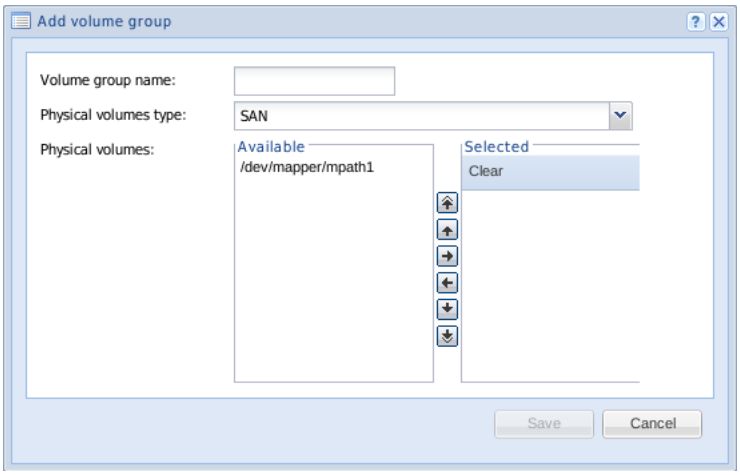


Figure 3.36.: Create volume group window

To extend a *volume group* drag and drop a *physical volume* into a *volume group*.

In the removal/reduction of a *volume group*, select the *volume group*/*physical volume* to remove and choose the corresponding option in the context menu.

Note

It's only allowed to remove a *volume group* if there is no associated *logical volumes*.

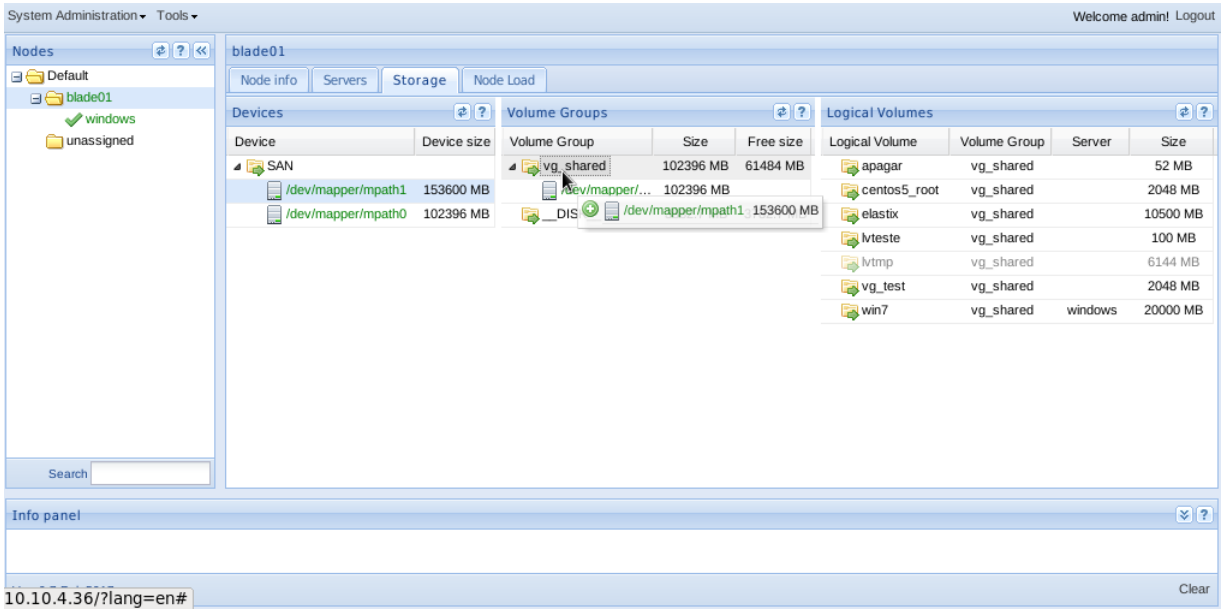


Figure 3.37.: Volume group extension

On Figure 3.37 we extend a *volume group* with a new *physival volume*.

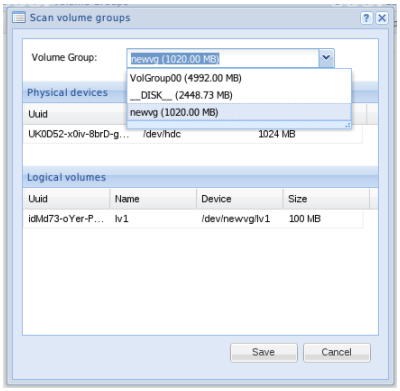


Figure 3.38.: Scan *volume groups*

On ”Scan *volume groups*”, it is possible to get *volume groups* from virtualization agent and register them on *Central Management*. Is is also possible to unregister the *volume group* on *Central Management* to get it out of system management.

3.4.3.3. Logical volumes administration

The operations available on the *logical volumes* are:

- Create a *logical volume*
- Resize a *logical volume*
- Remove a *logical volume*
- Register/Unregister *logical volume*
- Clone *logical volume*
- Convert *logical volume*

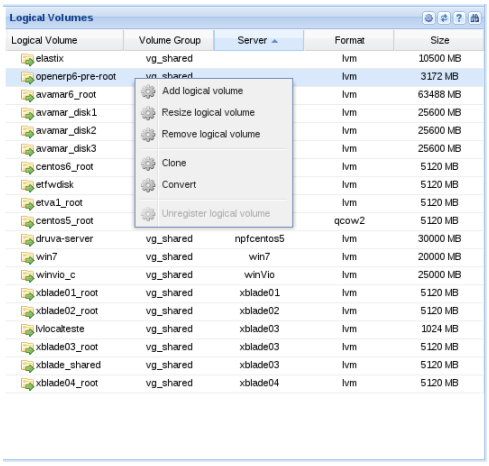


Figure 3.39.: Logical volume context menu

To create a new *logical volume*, we access the context menu (over any *logical volume*, and select the option *Add logical volume*.

The pretended name should be introduced in the creation window form, such as the *volume group* size. Note that the size should not exceed the *volume group* available size. It's also possible define the format of disk (raw, cow2,qcow,cow and vmdk - raw by default) and percentage of *snapshot* usage.

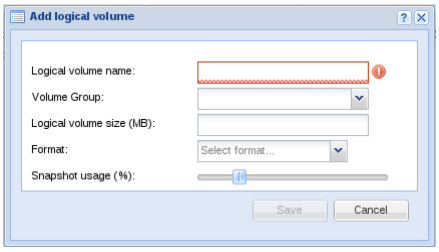


Figure 3.40.: Create a new logical volume window

To resize a *logical volume*, select and access into the context menu. The we can find the option *Resize logical volume*, that allow us to increase/reduce the *logical volume* size.

Note

By reducing the size of a *logical volume* could make existing data unusable. It is your responsibility to check that it is affordable/secure resizing the *logical volume* without affecting the data.

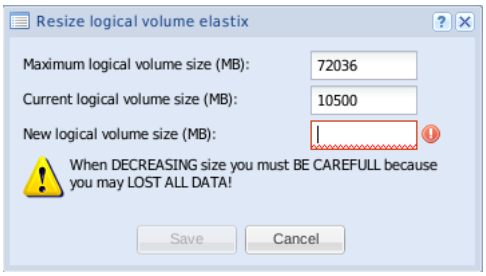


Figure 3.41.: Resize of a volume group

To remove a *logical volume*, access the context menu and select the option *Remove logical volume*. The *logical volume* will be removed if it's not assigned to any virtual machine. To verify if is in use you may pass the mouse over the *logical volume* and observe the information contained in the *tooltip*.

We have the operation to clone one *logical volume*, if *volume group* have free space to do the copy. And we can convert the disks format to one of the formats (raw, qcow2, qcow, cow and vmdk).

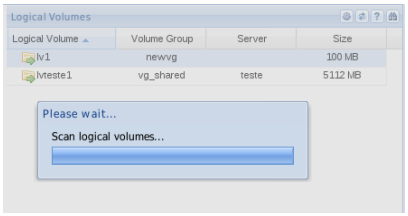


Figure 3.42.: Scan *logical volumes*

On "Scan *logical volumes*" it synchronizes *logical volumes* that are on virtualization agent and they are not registered on *Central Management*. It is may be possible that exist *logical volumes* that are registered on *Central Management* but really don't exist for some reason. In this cases, it is possible remove the register from the system and get the *logical volumes* synchronized with "Scan *logical volumes*".

3.4.4. Node Load

In the *Node Load* panel, we can find information about the node's load. In Figure 3.43, we can see the load information of the node in a hour range.

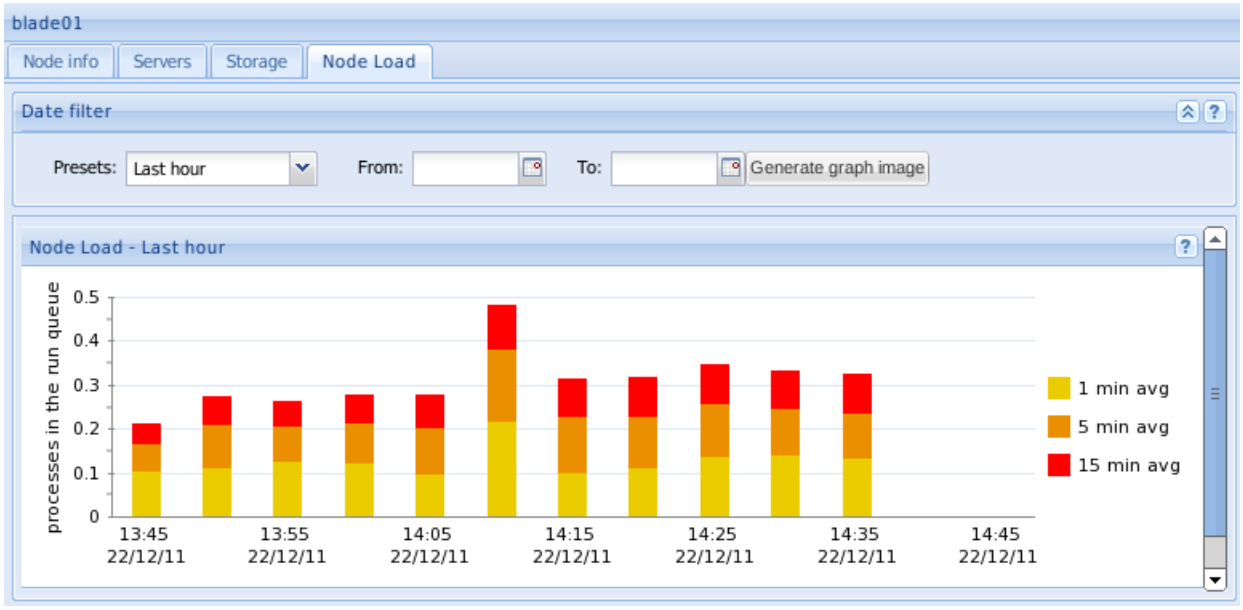


Figure 3.43.: Node load

In this panel we can also view the data by intervals:

- Last hour
- Last 2 hours
- Last 24 hours
- Last week

To view other time intervals use the option *Generate graph image*. The image is generated as shown in figure 3.44.

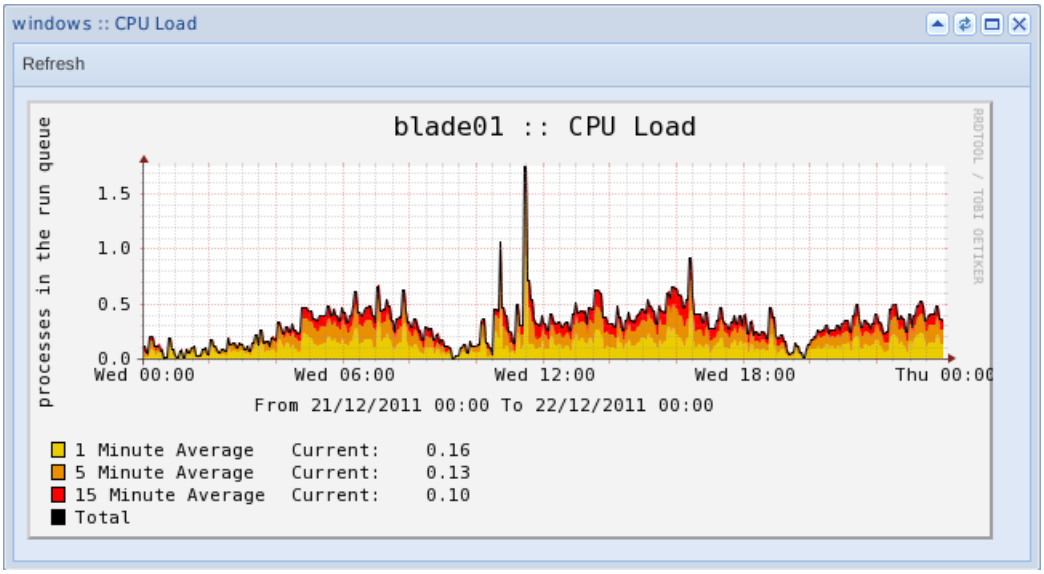


Figure 3.44.: Node usage statistics - CPU load

3.4.5. Shutdown node

Through the Central Management interface we can power off a physical node. To do so do the following steps:

- On the left panel, select the desired node. Then access to it's context menu;
- Press the option *Shutdown*.

Note

During the procedure, all node's virtual servers will also turned off.

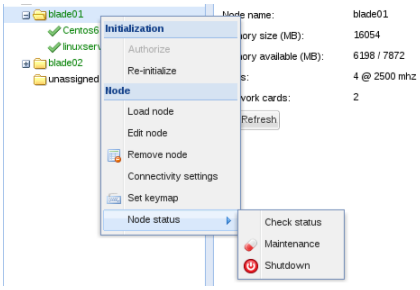


Figure 3.45.: Shutting down a node

3.5. Virtual machine

In the nodes pane we can select the virtual machine on which we intend to perform operations such as:

- Manage the virtual machine
- View usage statistics
- Manage *Management Agent* services

3.5.1. Server information

In *Information Server* we can see the state of the virtual machine and, among other information, the state of the *Management Agent*. In addition to displaying information, this panel lets you perform the following operations:

- Add a virtual machine (see Section 3.4.2.1)
- Edit a virtual machine (see Section 3.4.2.2)
- Remove virtual machine (see Section 3.4.2.3)
- Open a virtual machine in a VNC console (see Section 3.4.2.4)
- Start/stop virtual machine (see Section 3.4.2.5)
- Migrate a virtual machine (see Section 3.4.2.6)
- Snapshots (see Section 3.4.2.7)

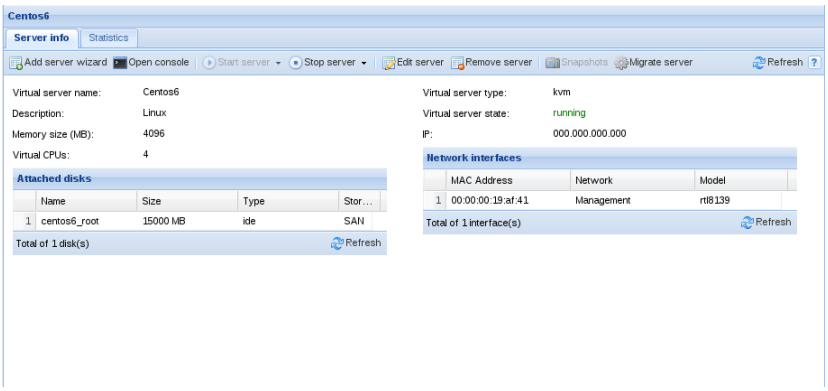


Figure 3.46.: Information about the virtual machine

3.5.2. Statistics

In *statistics* tab it's possible to see, graphically, information about:

- Cpu Usage (Figure 3.47)
- Networks (Figure 3.48)
- Memory Usage (Figure 3.49)
- Disk (Figure 3.50)

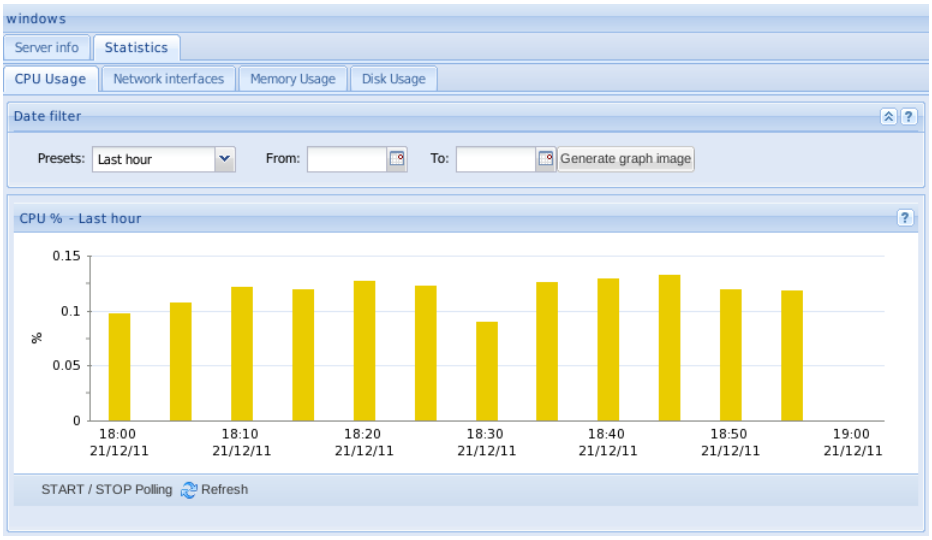


Figure 3.47.: Virtual machine cpu load

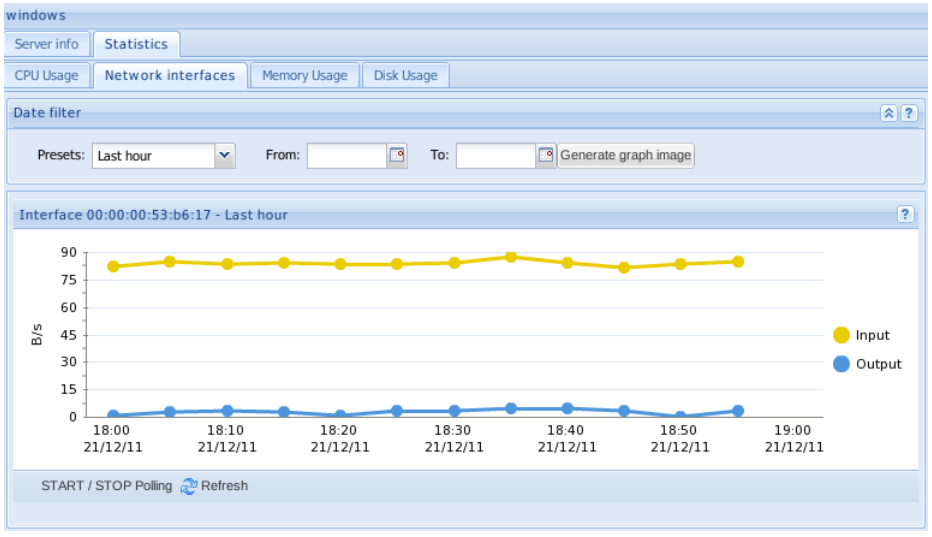


Figure 3.48.: Virtual machine network interfaces

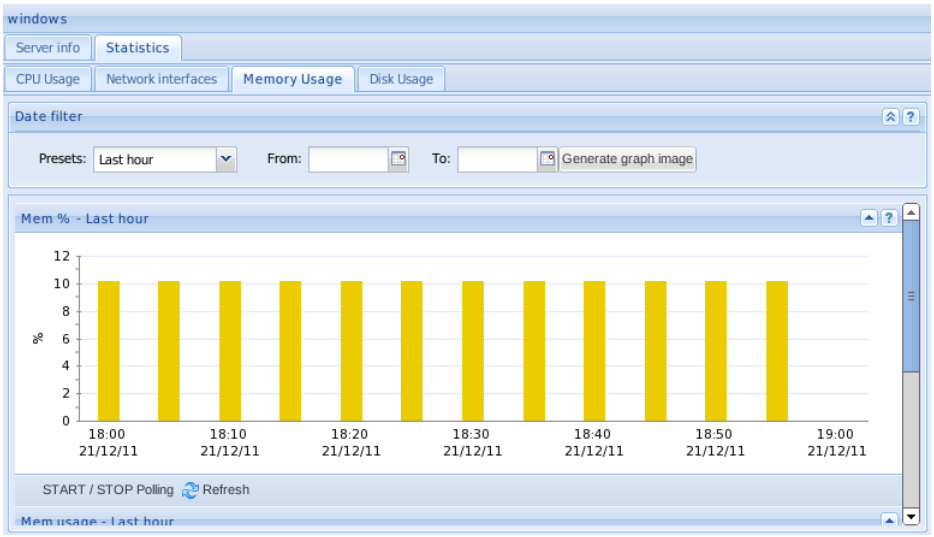


Figure 3.49.: Virtual machine memory usage

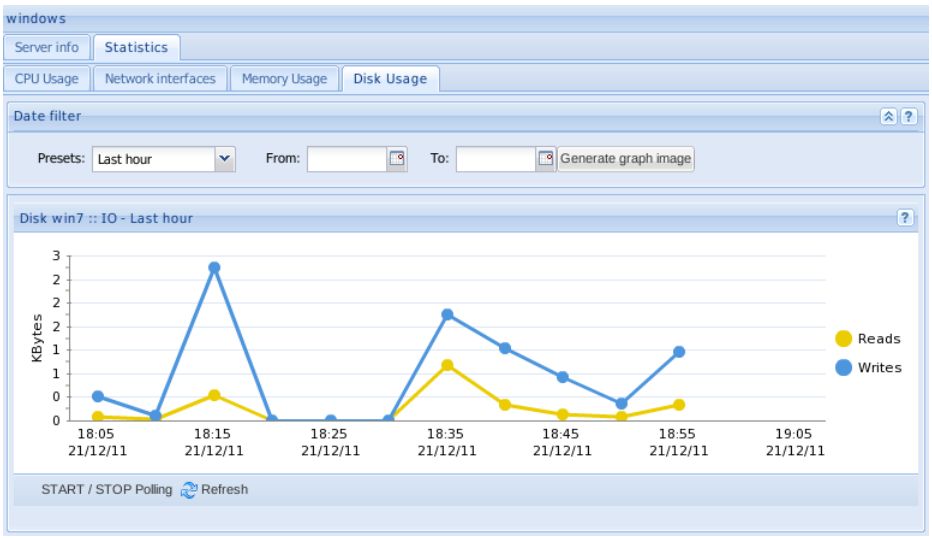


Figure 3.50.: Virtual machine disk input/output

In each of these panels we can view the data by pre-set intervals. For more information see Section 3.4.4.

3.5.3. Services

In *Services* tab panel, we can configure the available services on the corresponding management agent.

3.5.4. Virtio drivers

The virtio drivers facilitate communication between the operating system that runs the virtual machine, and the various hardware components. These components are the network devices and storage units - disks. As the use of the virtio drivers increases the overall system, its installation is recommended.

If the virtual machine's operating system is a complete Linux distribution whose kernel is a version less than 2.6.25, the virtio is supported without the need to follow any procedure to install the drivers. To take advantage of, simply select the driver tab virtio *Network Interfaces* and *Disks* on *server edit* window.

The requirements for the use of the virtio drivers can be found at:

http://wiki.libvirt.org/page/Virtio

Installation on windows virtual machines

Download the iso with the drivers, available at:

http://alt.fedoraproject.org/pub/alt/virtio-win/latest/images/bin/.

Upload iso with the drivers - more information in Section 3.6.3. *Tools*, *ISO Manager*, *upload applet*, select the file and upload. The file should appear in the list of ISOs.

Then select the server where you want to install the drivers, and choose the *Edit server*. Choose the ISO image with the drivers as shown in Figure 3.51. Go to the tab *Disk* and assign a new volume, choosing the virtio driver - Figure 3.52.

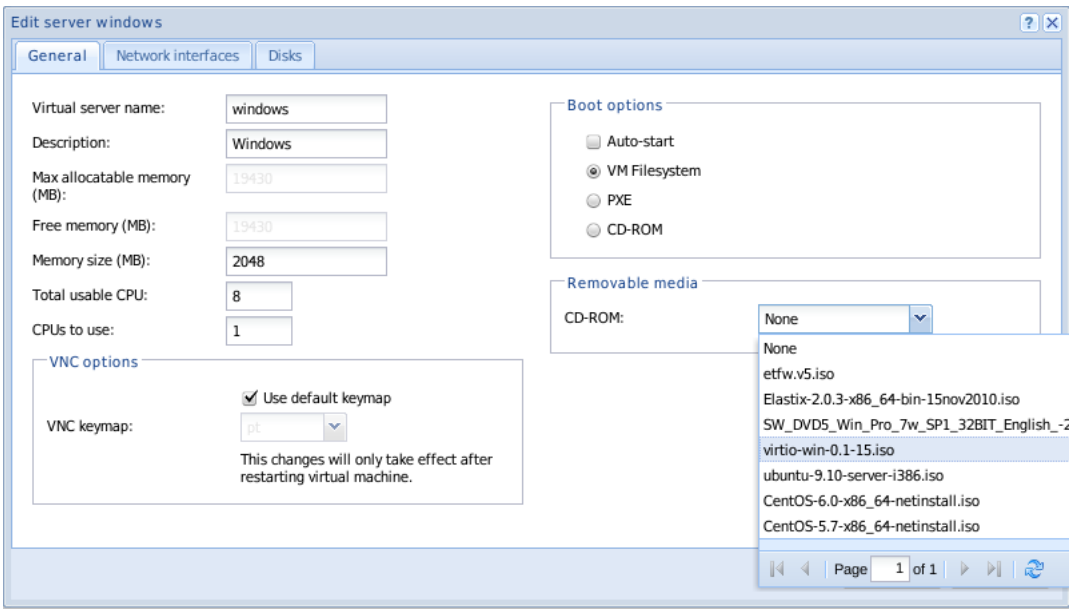


Figure 3.51.: Driver's - iso selection

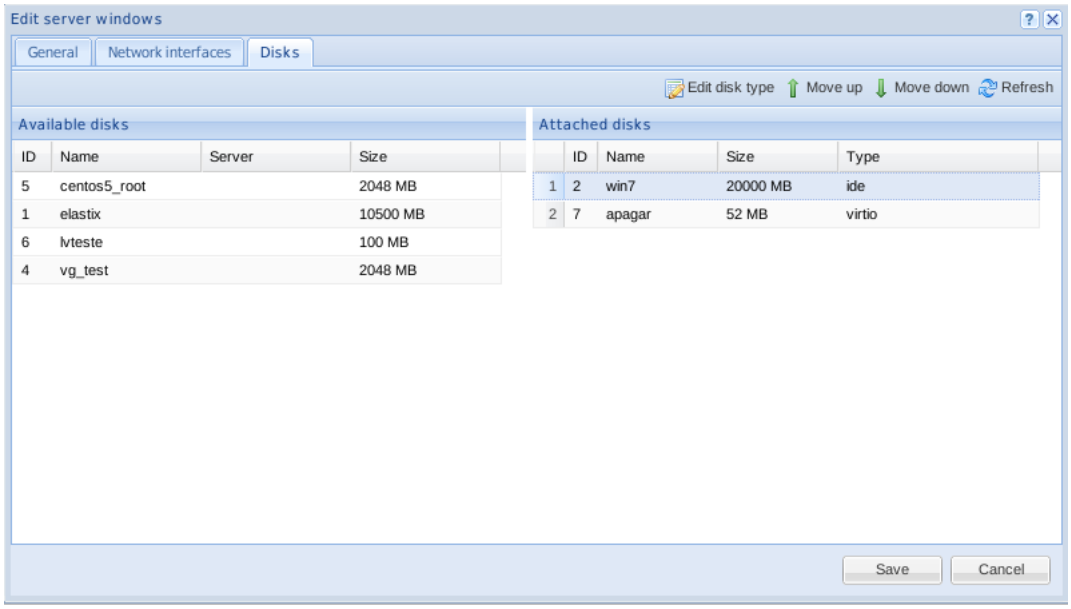


Figure 3.52.: Set logical volume (drivers virtio)

Set the startup disk server as shown in Figure 3.53.

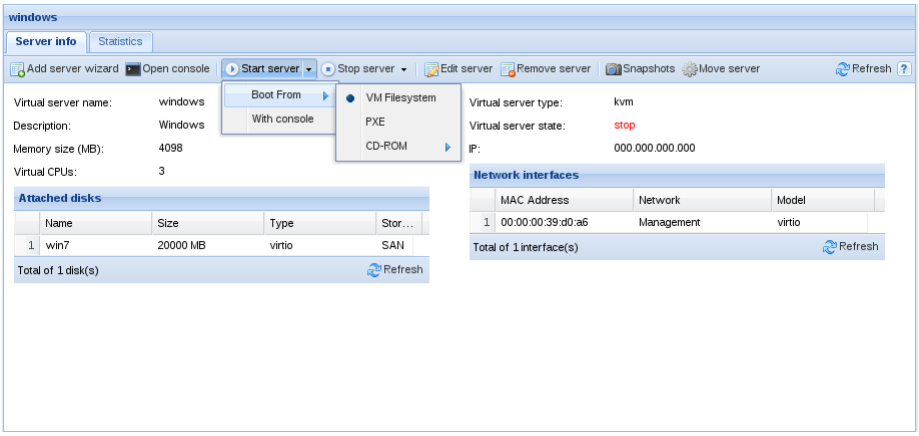


Figure 3.53.: Set the startup disk

With Windows running, go to device manager. Note that the added logical volume appears as shown in Figure 3.54.

Then select the *Update Driver Software*, *Browse my computer for driver software*, indicate where is the drivers (in the virtual CD drive), completing the installation procedure.

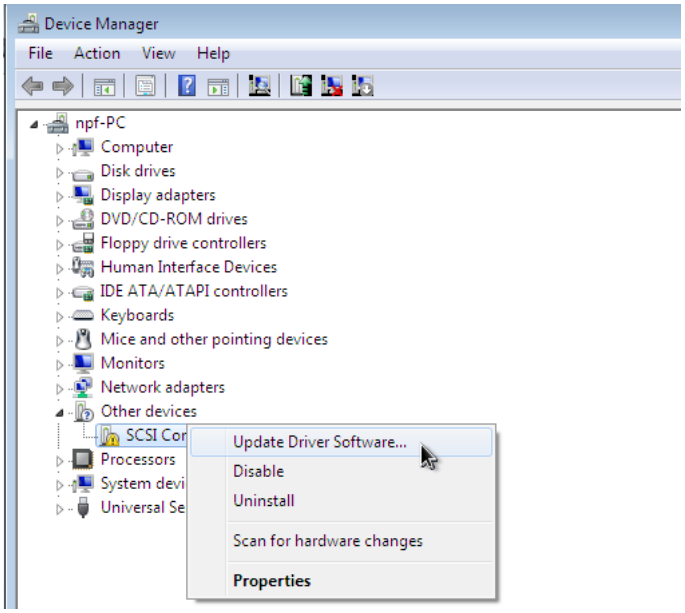


Figure 3.54.: Windows - driver update

Stop the virtual machine and edit the settings by changing the main driver of the logical volume where you installed the operating system - Figure 3.55.

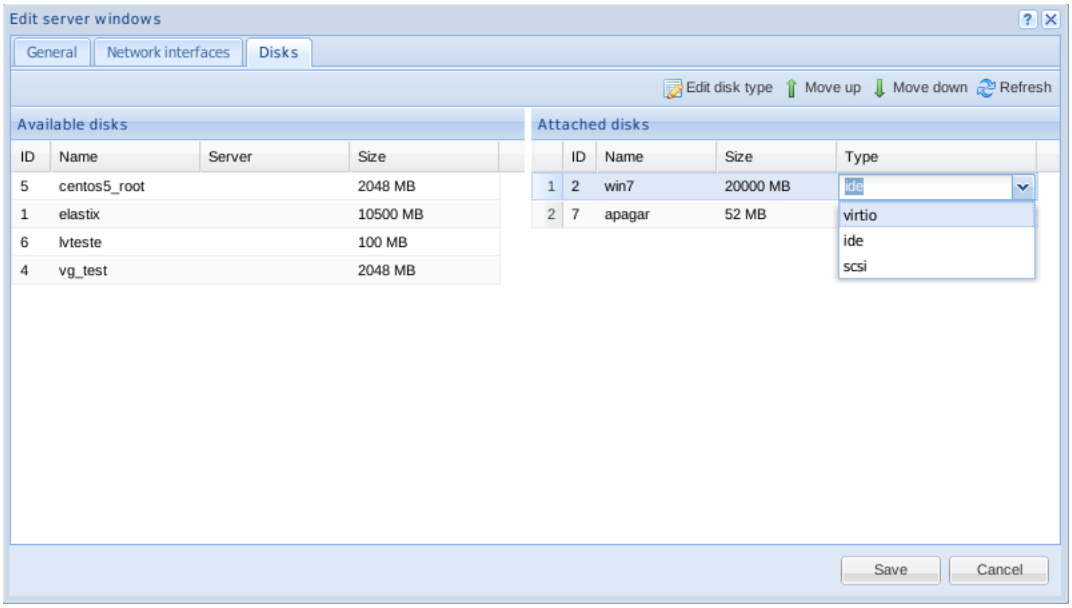


Figure 3.55.: Change the disk driver to virtio

3.6. Tools

In menu *Tools* we can access the folloing options:

- Import OVF
- Export OVF
- ISO Manager
- Node agent monitor
- System events' log

3.6.1. Import OVF

This tool allows you to import virtual machines in OVF format (*Open Virtualization Format*).

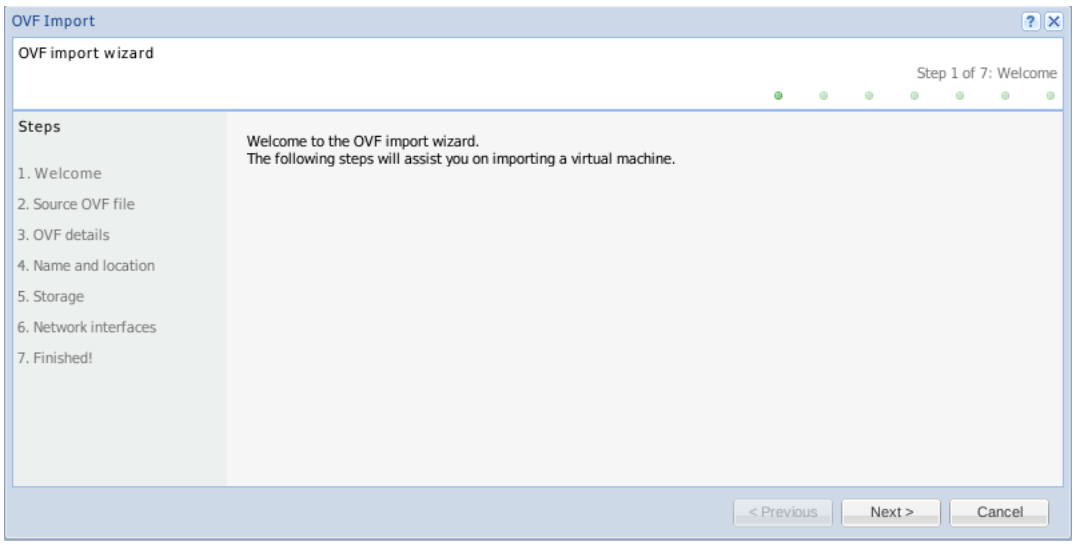


Figure 3.56.: OVF import wizard - Welcome

The OVF import wizard is constituted by the following stages:

Source OVF file: In this stage we define the OVF file URL (see Figure 3.57).

Note

The CM must have HTTP access to the specified URL.

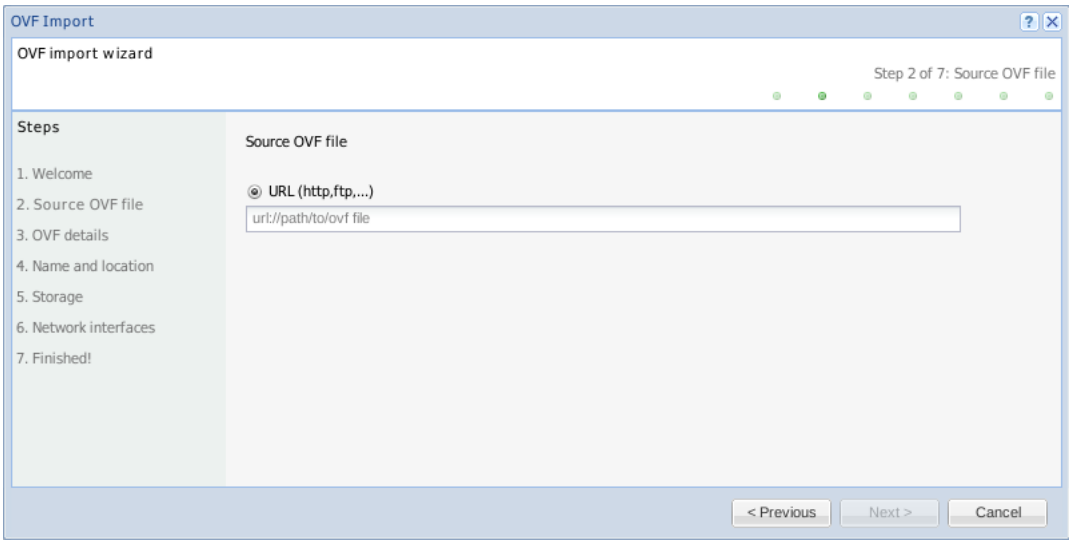


Figure 3.57.: OVF import wizard - Source OVF file

OVF details: OVF file details. Provides information about the product, version, total size of the files referenced by the OVF, if available.

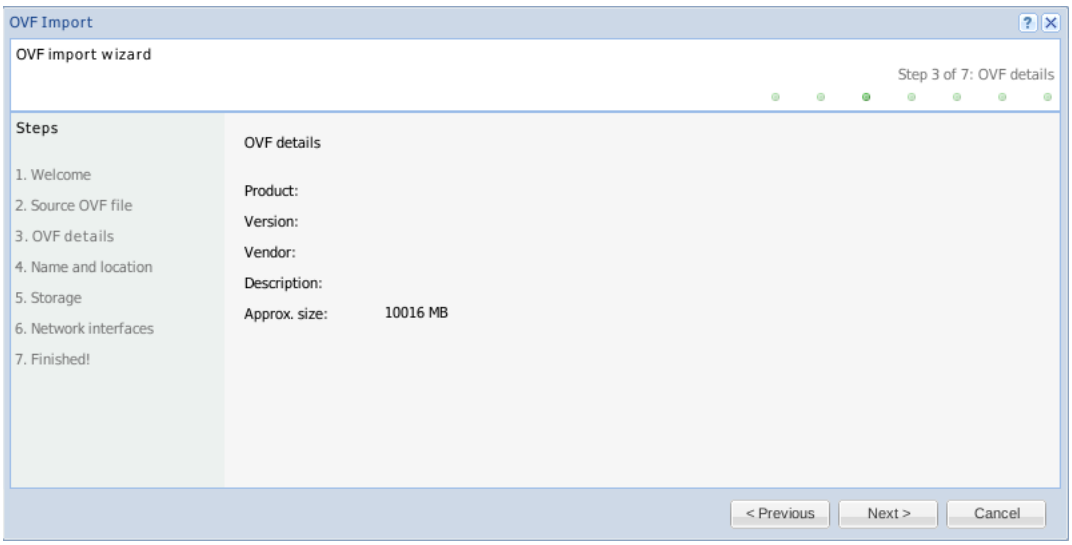


Figure 3.58.: OVF import wizard - OVF details

License: If specified in the OVF file, this step will come with the EULA. Otherwise, this step is omitted.

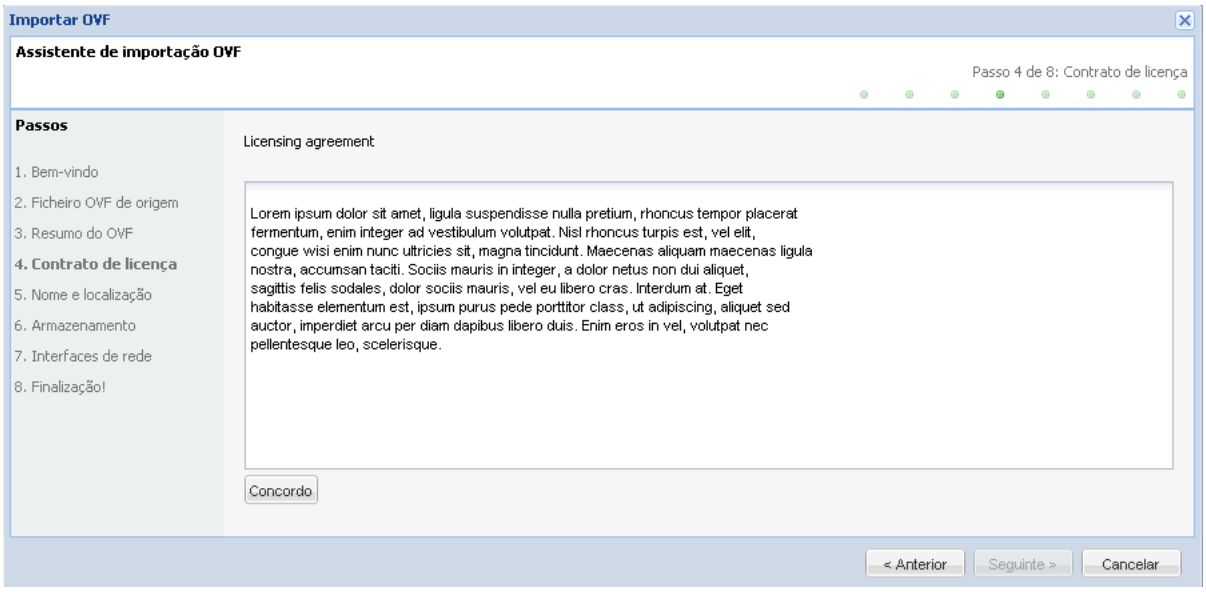


Figure 3.59.: OVF import wizard - License

Name and location: This step defines the virtual machine name, the destination node and the type of operating system. The operating system options vary depending on the specification of the node:

- with XEN and hardware hardware support:

  - Linux PV
  - Linux HVM
  - Windows
- with XEN and without the hardware support:
  - Linux PV
- with KVM
  - Linux
  - Windows

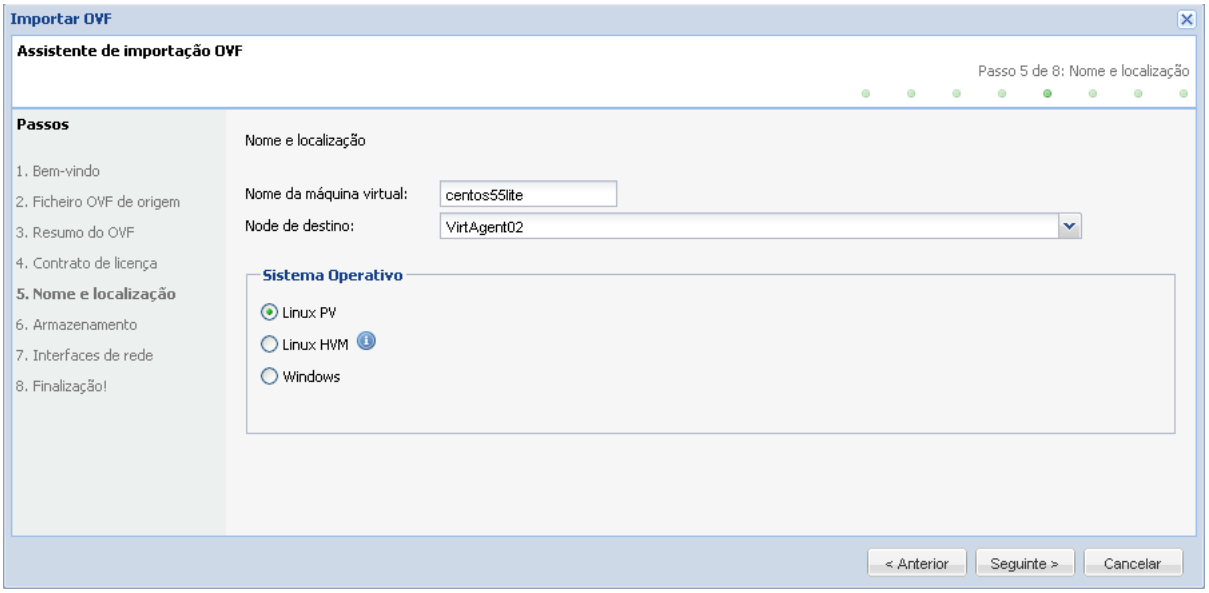


Figure 3.60.: OVF import wizard - Name and location

Before proceeding to the next step, the wizard checks if the disks' drivers and network interfaces mentioned in the OVF are supported by the chosen virtualization server.

The supported drivers by XEN machines, with or without hardware virtualization, are: IDE, SCSI and xen and in machines with KVM drivers are: ide, virtio and scsi.

The supported network card drivers for HVM and KVM machines are: e1000, virtio and rtl8139. On a XEN machine without hardware virtualization support, no drivers can be used.

If the selected virtualization server does not to support the drivers mentioned, the OVF import can not be performed.

Storage: This step is carried out mapping of disks in the node. You can specify the name of the *logical volume* and define the its *volume group*. It is required that all disks are mapped to proceed to the next step.

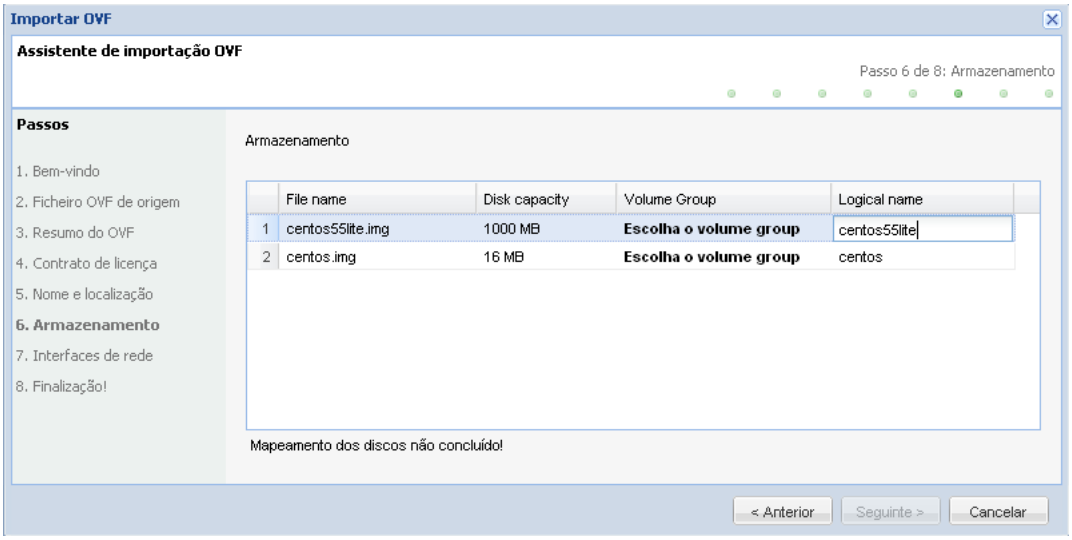


Figure 3.61.: OVF import wizard - Storage

Network interfaces: In this stage we map the network interfaces. You can specify new network interfaces. It is necessary that all the network interfaces are mapped to proceed to the next step.

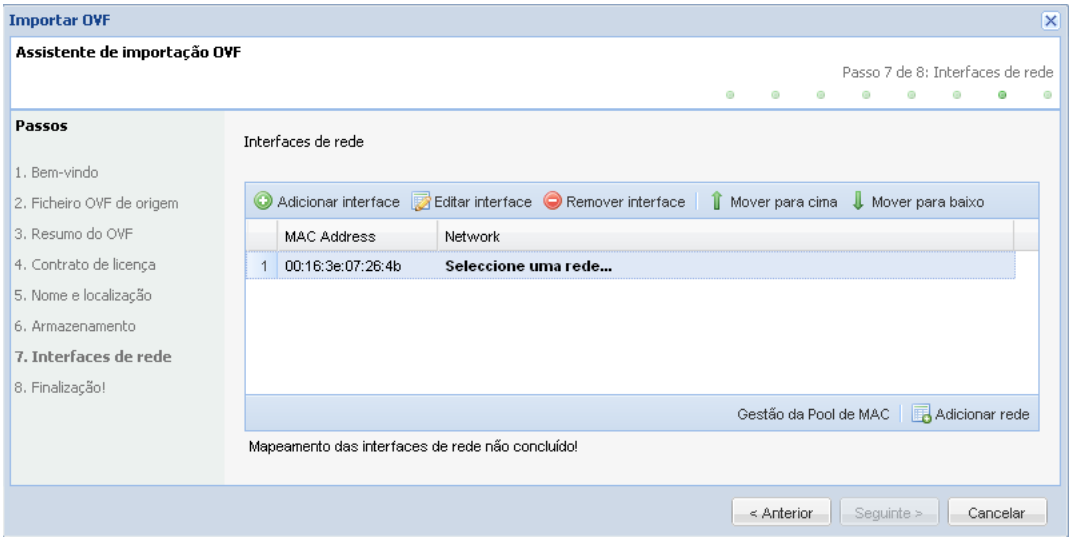


Figure 3.62.: OVF import wizard - Network interfaces

Finished!: Final step of the wizard. After confirmation of the import of virtual machine, the collected data in previous steps are processed and sent to the virtualization server. Later in the panel *server* the virtual machine can be initiated through the option *Start server*.

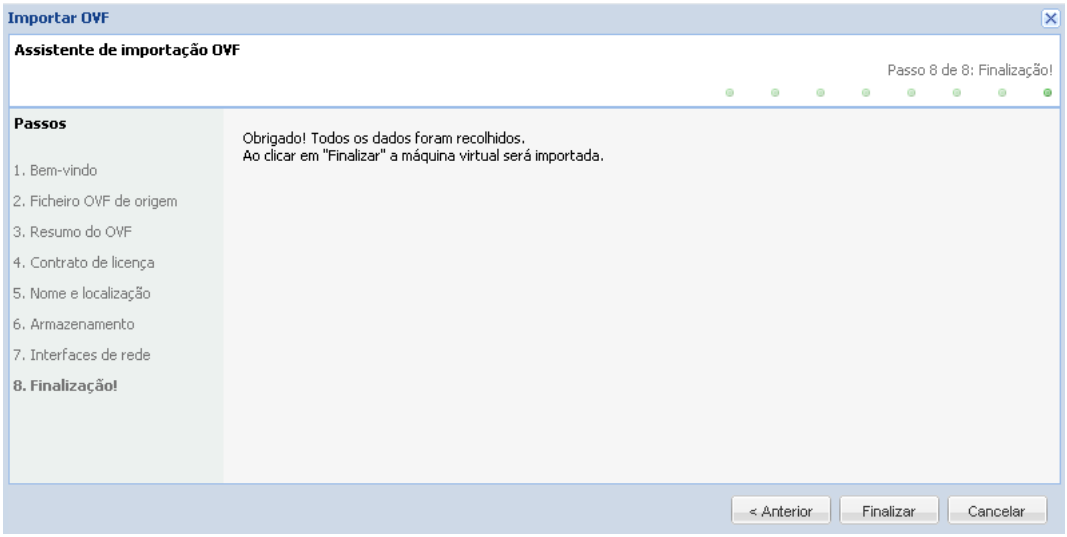


Figure 3.63.: OVF import wizard - Finished!

3.6.2. Export OVF

This tool allows you to export virtual machines in OVF format (*Open Virtualization Format*). The generated file will be in the OVA format (*Open Virtualization Archive*).

Note

The virtual machine to export needs to be stopped to perform the export.

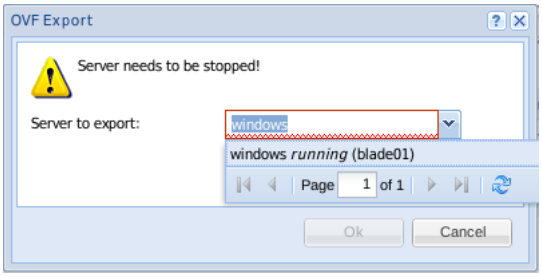


Figure 3.64.: OVF export window

3.6.3. ISO manager

this tool allows you to manage the images that will be available for use in virtual machines. The files will be used later for mounting virtual machine's *CD-ROM* unit.

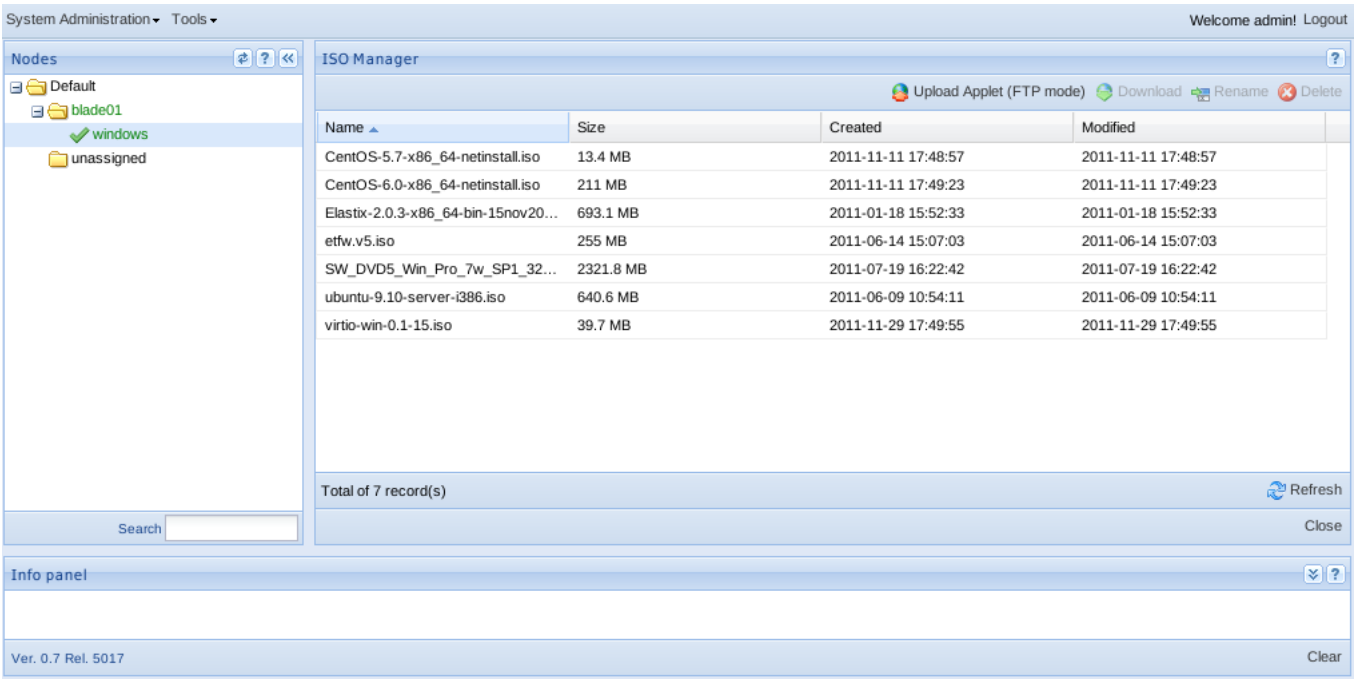


Figure 3.65.: Iso management panel

The supported operations are:

- Upload of multiple files
- Download of files
- Rename files
- Delete files

Note

Changes to existing images that are set at boot from CD-ROM of any virtual machine, will not be reflected automatically. The user must check if the mounted image on the CD-ROM unit is still valid.

3.6.4. Nodes' agent monitor

This tool is for real-time communication testing of the multiple nodes of the CM. Verification is done periodically. To stop checking close the pop up that appears when activating the tool.

3.6.5. System events log

In *System events log* menu it's possible to see the changes made by user interaction.

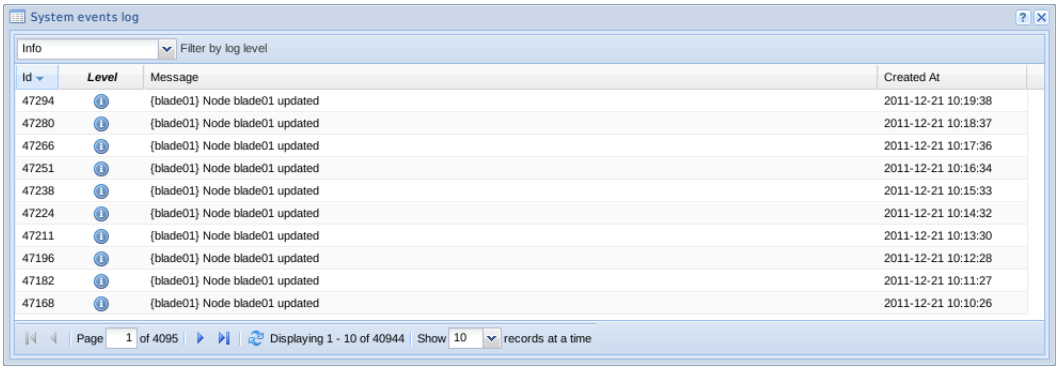


Figure 3.66.: System events log window

The event log messages can be filtered by three message types:

- **Debug** - Displays all messages. Aggregate levels *Info* and *Error*
- **Info** - Messages with information on events that have been successful
- **Error** - Messages with information on events that haven't been successful

3.7. System administration

In the *System administration* menu it's possible we can access to:

- One-time setup wizard
- Change preferences
- Users' and permissions' administration

3.7.1. One time set wizard

The initialization setup wizard gathers the set of operations to be carried out on first access to the CM. Lets you make a quick system configuration.

The setup wizard, as shown in Figure 3.67, consists in the following steps:

- Default password change
- MAC pool generation
- System preferences

- Network setup

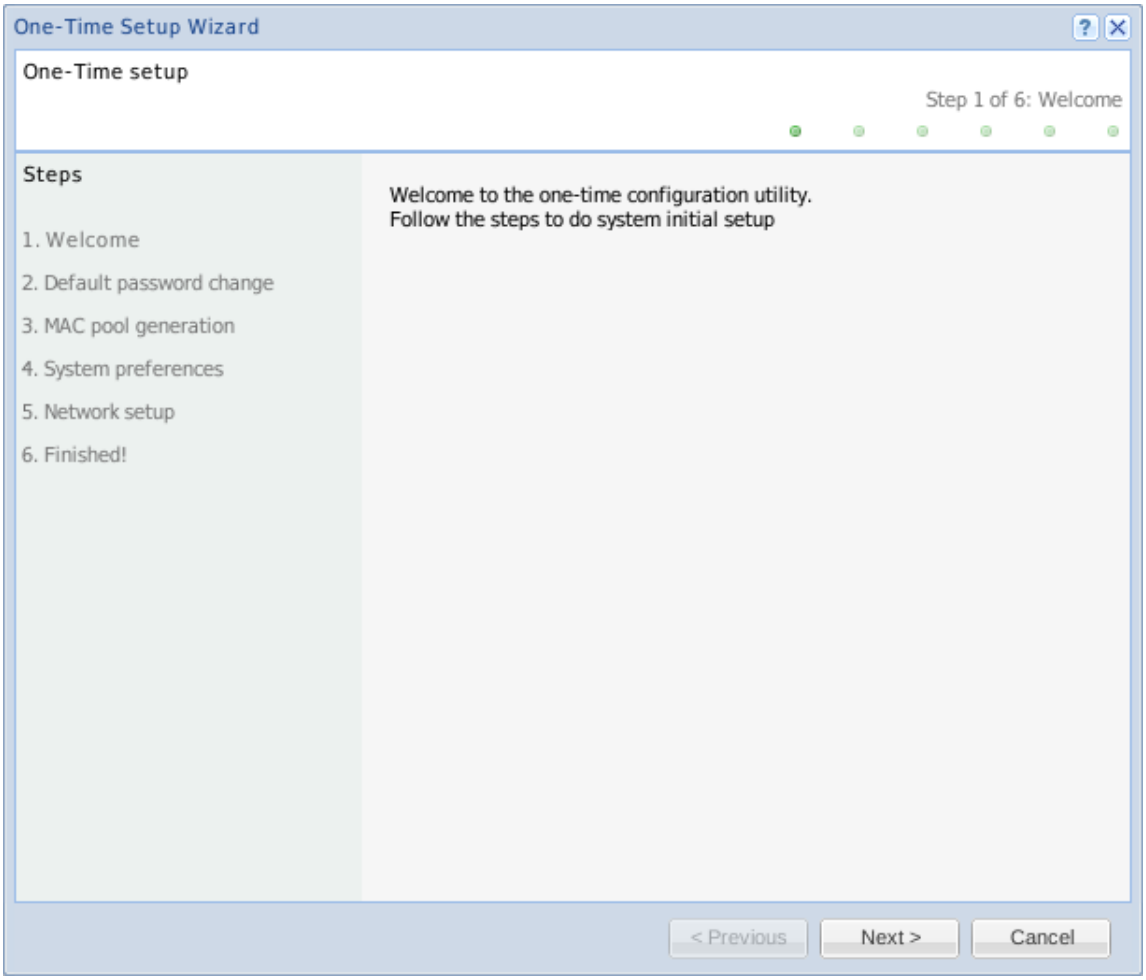


Figure 3.67.: One time setup wizard

Note

On version *NUXIS*, the network configuration step is omitted.

3.7.2. System Preferences

By accessing the system references you can set some parameters. In the general panel you can specify the default VNC keymap to access virtual machines as well as define the duration of the event logs of the system.

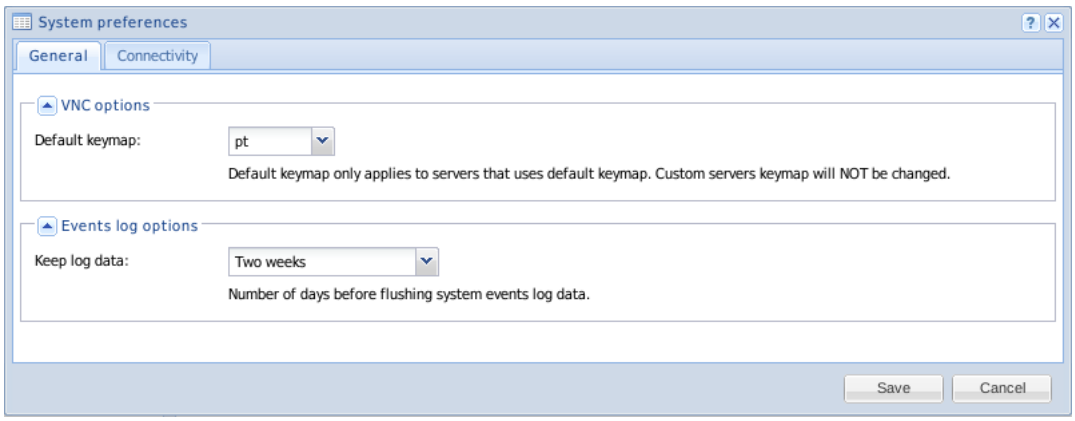


Figure 3.68.: System preferences window - General panel

In the connectivity tab you're allowed to change the CM IP address and for the LAN network (only available in *NUXIS* version). In the *UnitBox* version you are only allowed to change the CM IP.

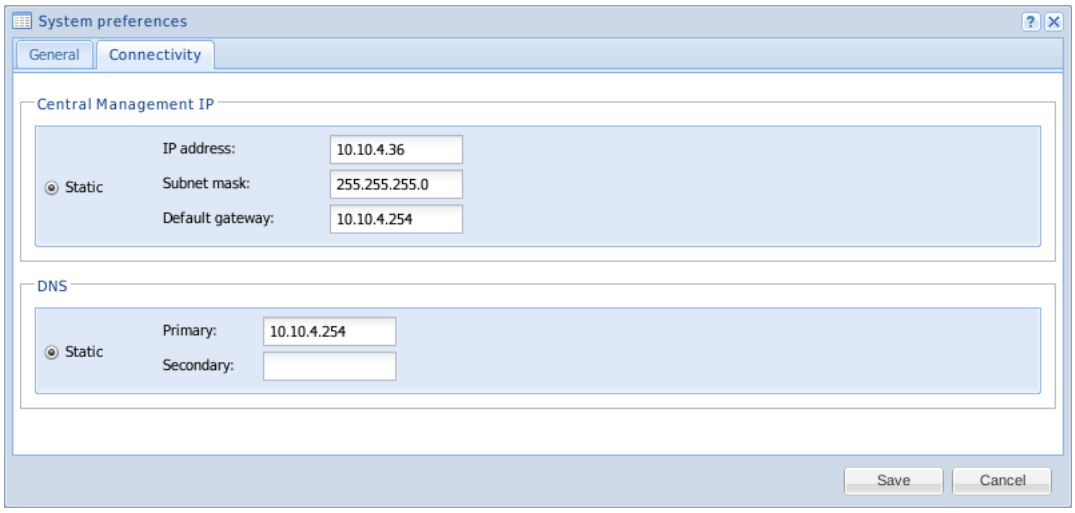


Figure 3.69.: System preferences window - Connectivity tab

3.7.3. Users, groups and permission administration

The administration menu is available to the super users the system, and can be found on the top bar (then tools), in *Users' and permissions' administration*.

When we select this option, a window with three following tabs is open:

- *User management*;

- *Group management*;
- *Permission management*.

The image 3.70 illustrates the window that appears. In this window you can set the necessary permissions. Users can be created to access the management interface, and assigned access permissions on virtual machine level, or on cluster cluster level.

To facilitate the assignment of permissions you can set groups. For example, one group can have several associated permissions, and can be assigned to multiple users. This makes adding/removing a set of permissions to users easier.

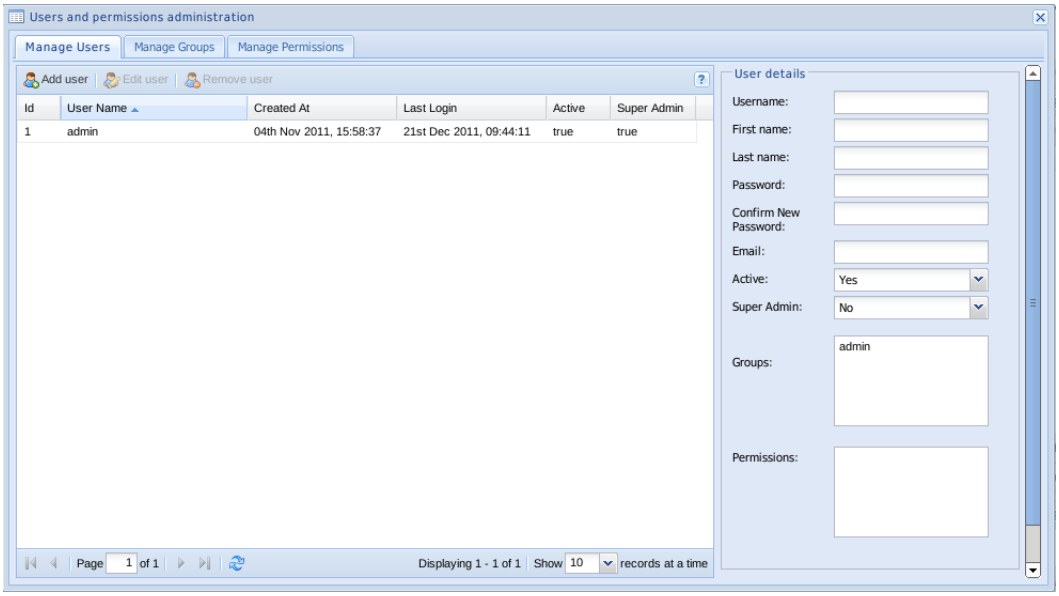


Figure 3.70.: Users' and permissions' administration

In addition, you have another way to assign permissions and/or groups, right clicking the mouse on the desired node/server, as stated on Figures 3.71, 3.72 and 3.73.

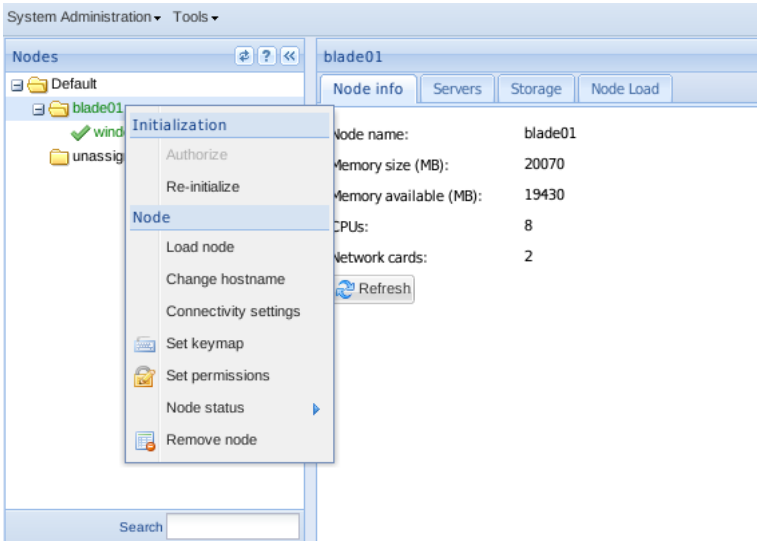


Figure 3.71.: Permission option in node's context

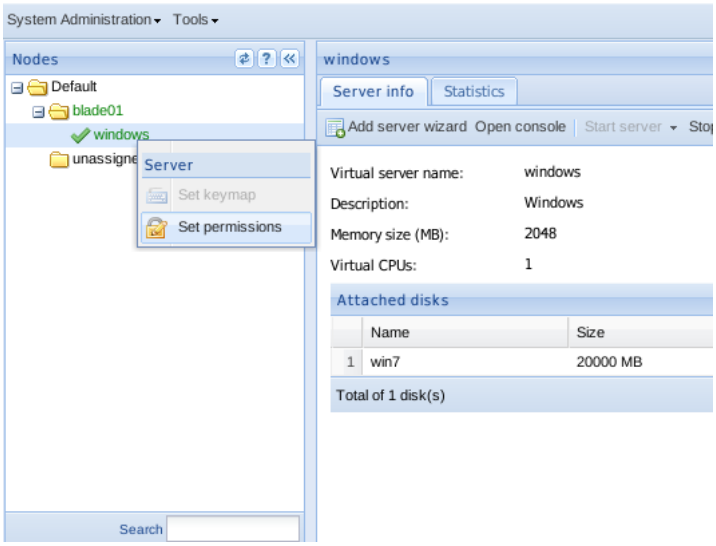


Figure 3.72.: Permission option in server's context

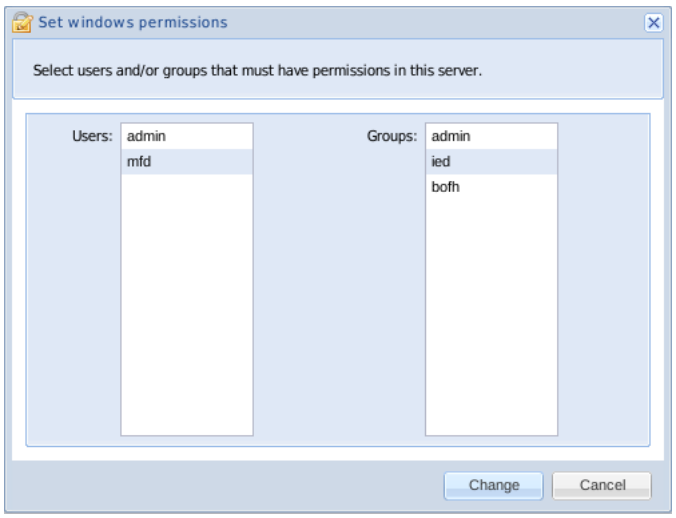


Figure 3.73.: Changing servers' access permissions

Note

In *Manage groups* it's not possible to remove the group with ID=1 (system reserved).

3.7.4. Shutdown appliance

There are two methods to turn off the *UnitBox appliance*. The first method is through the management interface, executing the steps below:

- Access the Central Management interface
- Select the desired node and access it's context menu
- Press the option *Shutdown*. This option will also turn off any virtual machines of the node.

The other way of shutting down is using the appliance's display buttons (see Figure 3.74).

- Select MENU;
- Search the option SHUTDOWN;
- Press the ENTER button.

Figure 3.74.: UnitBox display and buttons

4. Management Agents

With the UnitBox it's possible to manage over the central management interface some of the Eurotux service, such as:

- ETFW - Firewall solution
- ETMS - Mail Server solution
- ETVOIP - VOIP solution

The management of services is possible through the installation and configuration of management agents in the virtual machines that support the services.

4.1. ETFW

In a virtual machine with the image of *ETFW* you can configure the service via Central Management, on tab *ETFW*.

In the main panel you can access the *Network setup wizard* or access the *Webmin* interface to make changes in any configuration.

The site also has the *Save configuration* option that makes the changes effective. Without this option, any changes made lost after *reboot*.

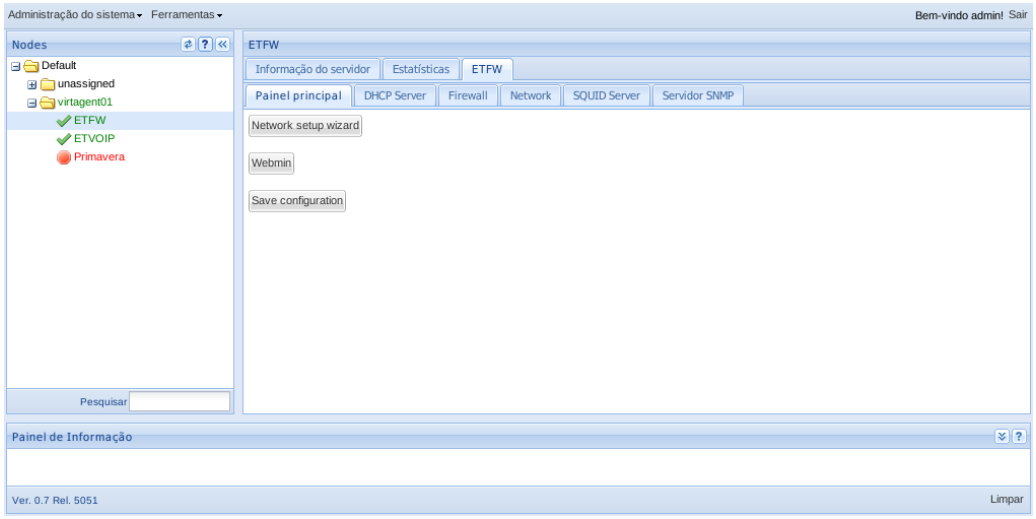


Figure 4.1.: Main panel

4.1.1. Network setup Wizard

To configure the module *ETFW* quickly and efficiently it's provided a step by step setup wizard.

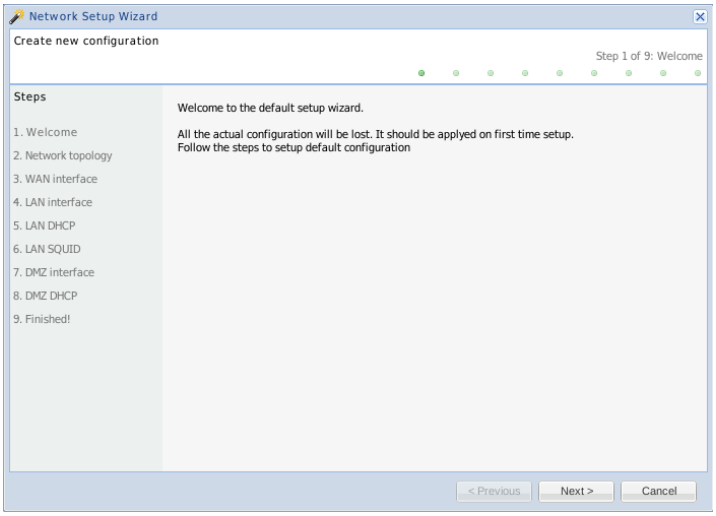


Figure 4.2.: Welcome

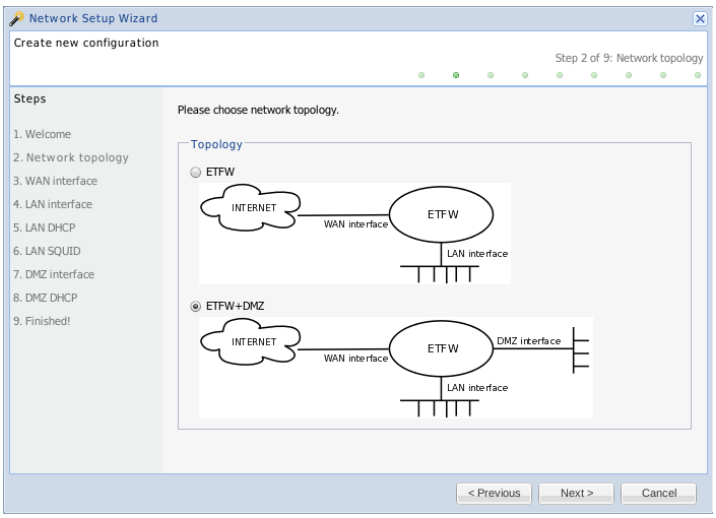


Figure 4.3.: Topology setup

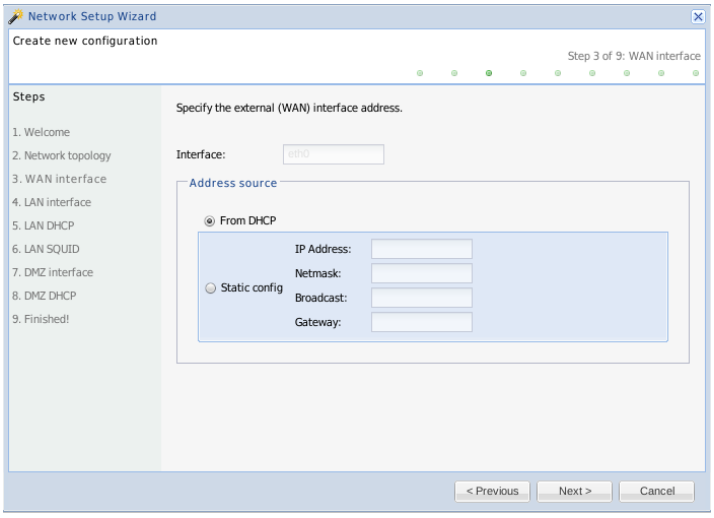


Figure 4.4.: Configuring the WAN interface

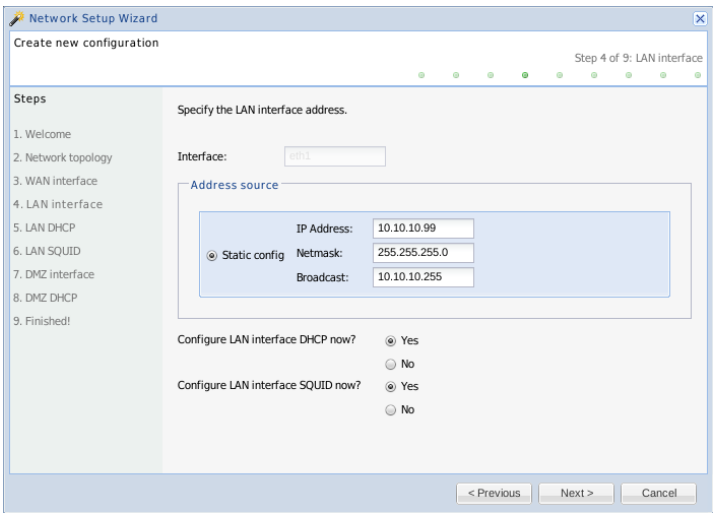


Figure 4.5.: Configuring the LAN interface

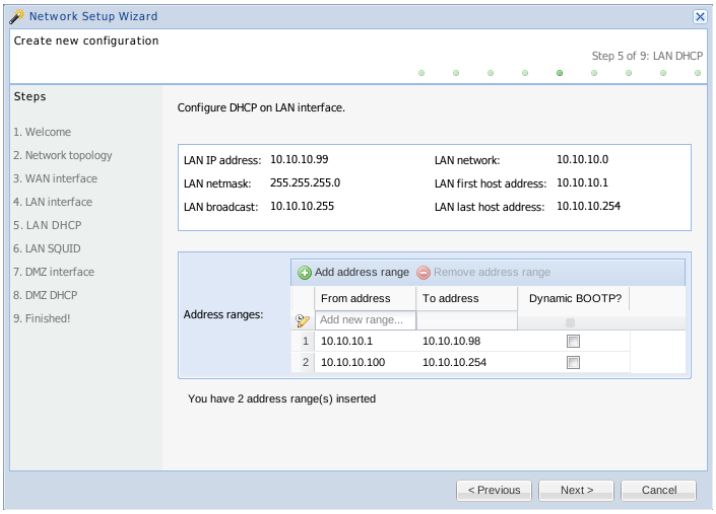


Figure 4.6.: Configuring of the DHCP service for LAN network

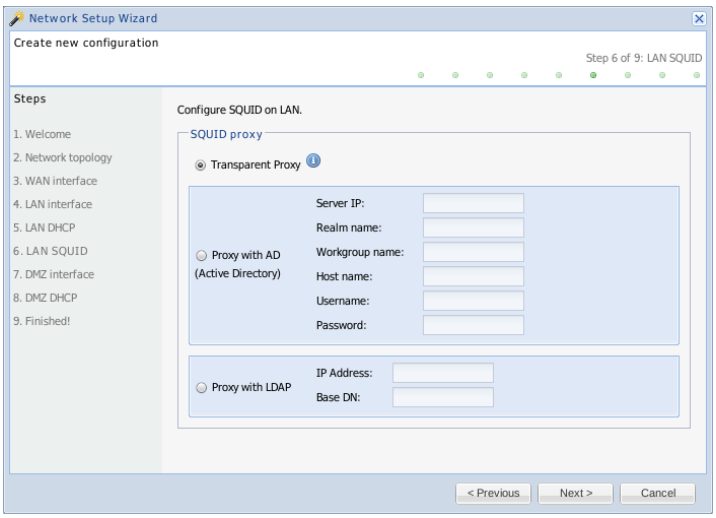


Figure 4.7.: Configuring SQUID proxy

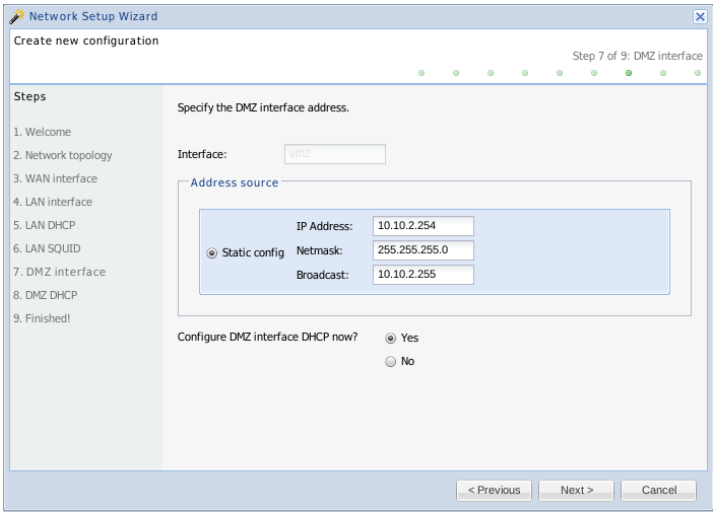


Figure 4.8.: Configuring DMZ interface

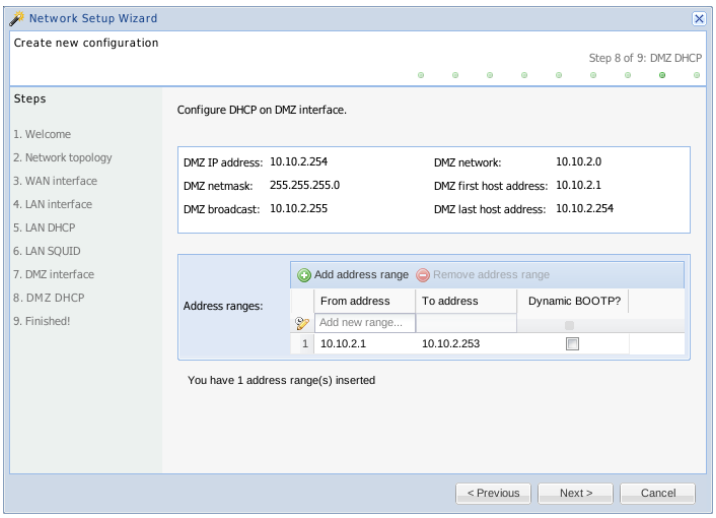


Figure 4.9.: Configuring DHCP service for DMZ network

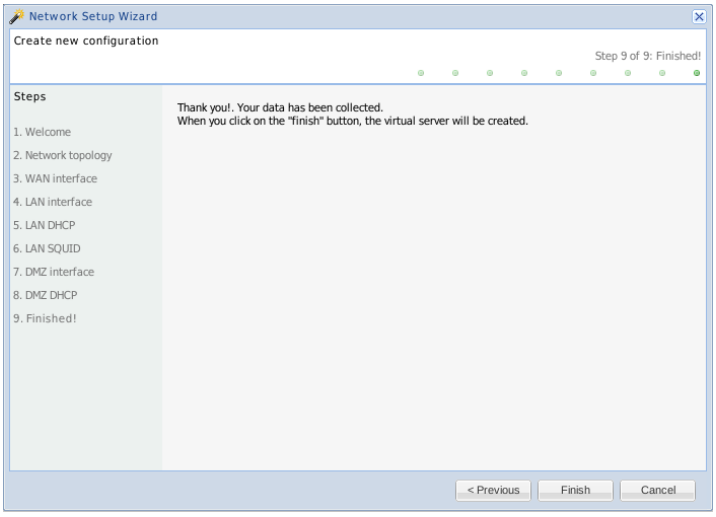


Figure 4.10.: Completion of the configuration

4.1.2. Network setup - *Network*

In addition to the wizard configuration process you can change the network configuration manually. To do this, go to the *network* tab where we have access to the configuration of network interfaces (*Network interfaces*), routing rules (*Routing and gateways*), address configuration (*Host Addresses*) and client *DNS* (*Hostname and DNS client*).

4.1.2.1. Network interfaces

In *Network interfaces* we can see the network interfaces that are configured and which are going to be active at the machine start.

When selecting an interface we can edit the parameters of the interface, such as the IP address, netmask, broadcast, and aliases in virtual interfaces. To add a new interface, select the add button and fill in the required fields for the interface configuration.

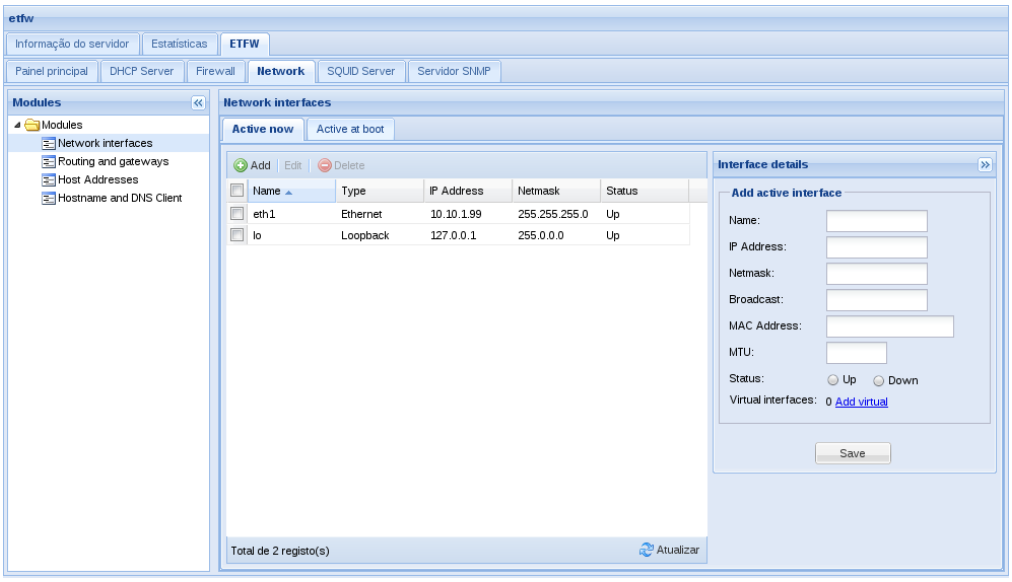


Figure 4.11.: Active interfaces

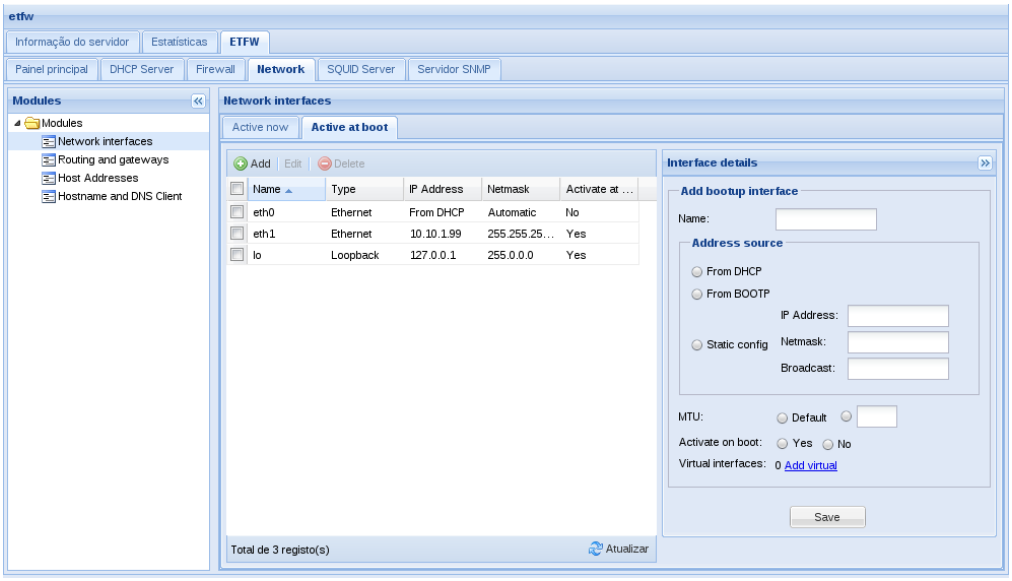


Figure 4.12.: After boot active interfaces

If you wish to define an alias for a network interface, you must select the desired interface, edit and choose *Add virtual* in *Virtual interfaces*. Next, fill out the required parameters and save.

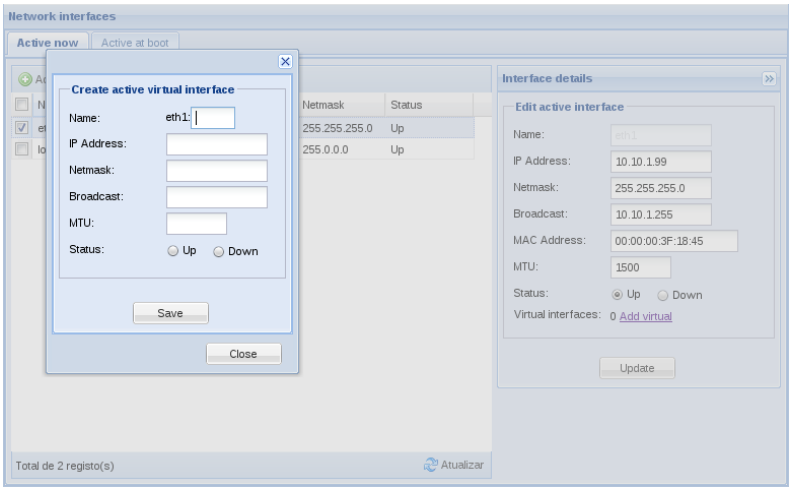


Figure 4.13.: Alias interface

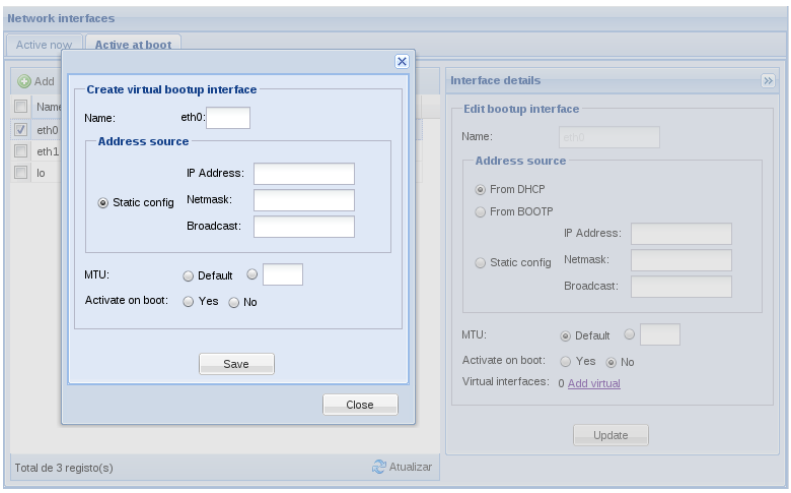


Figure 4.14.: Alias interface active at boot

4.1.2.2. Routing and gateways

In *Routing and gateways* we can query the active routing rules and remove or add new rules. We can also define routing rules that are set at startup.

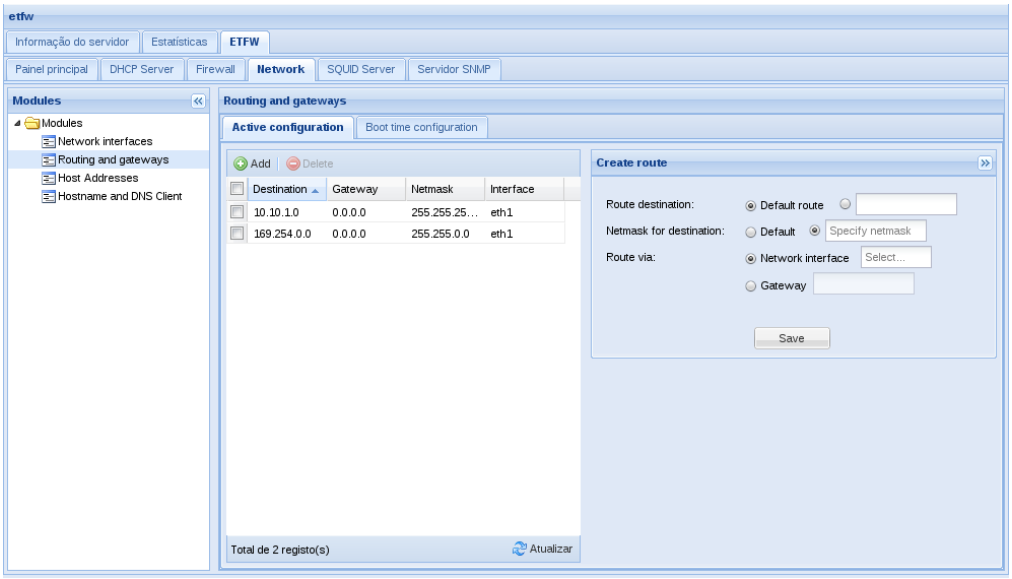


Figure 4.15.: Active forwarding rules

To create a routing rule, we choose the *add* option and define the parameters of the route:

- *Route destination* - Destination of the forwarding route. It can be *default*, destination

IP address or network address;

- *Netmask for destination* - Netmask for the route of destination;
- *Route via* - *Gateway* or network interface of output route.

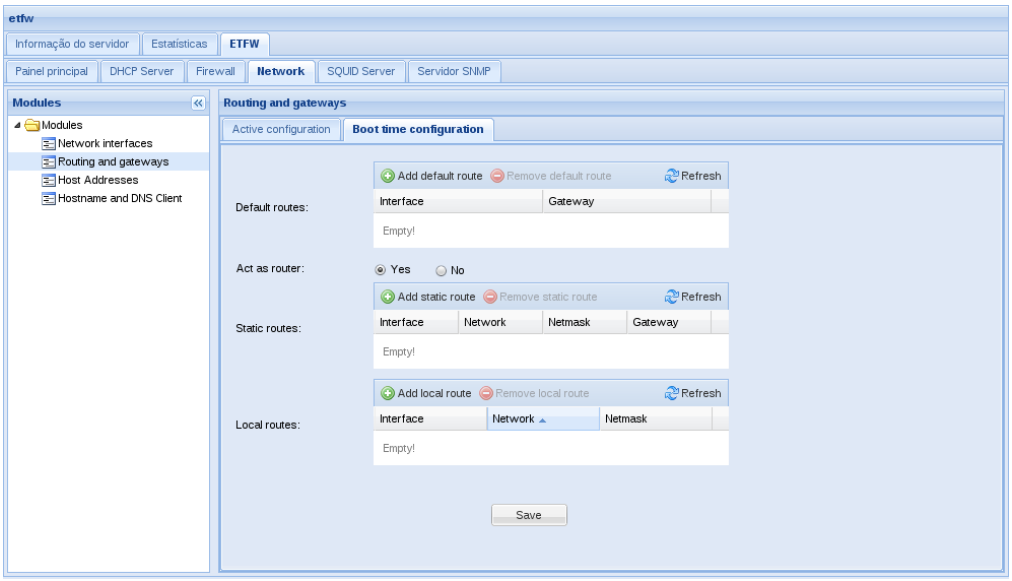


Figure 4.16.: Defined routing rules at startup

In the routing rules defined at startup we can configure the following rule types:

- *Default routes* - to define the default gateway;
- *Static routes* - static routes to other networks/machines;
- *Local routes* - static routes where IP addresses are defined, netmask and the interface of each route.

4.1.2.3. Host Addresses

In *Host Addresses* you can define static names and locals, associated with IP addresses, in order to reduce response time in name resolution.

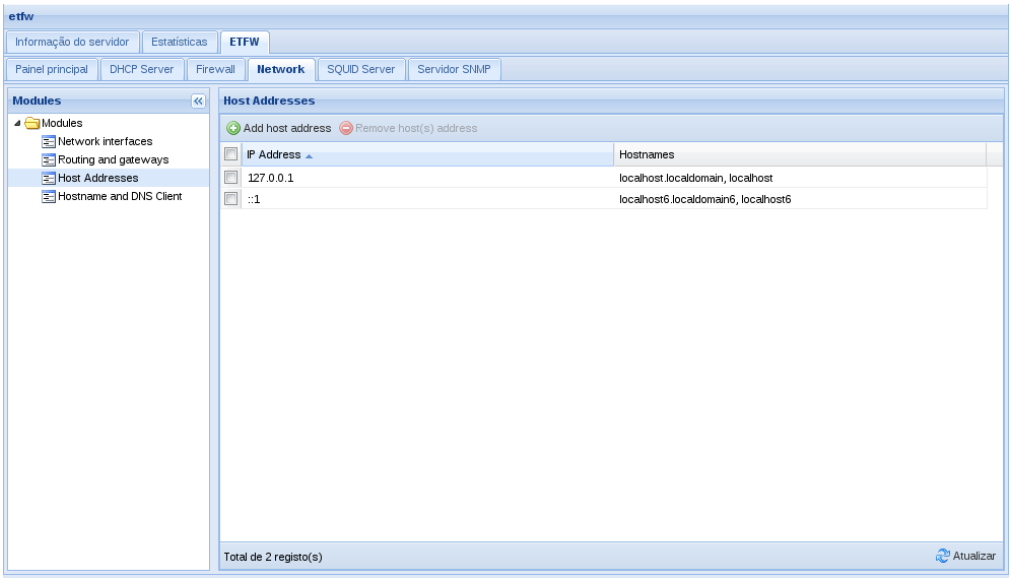


Figure 4.17.: Address setup

4.1.2.4. Hostname and DNS Client

From this option you can set the name that the machine will have locally and the configuration parameters of the DNS client service (DNS server addresses, order of name resolution on addresses and search domains names).

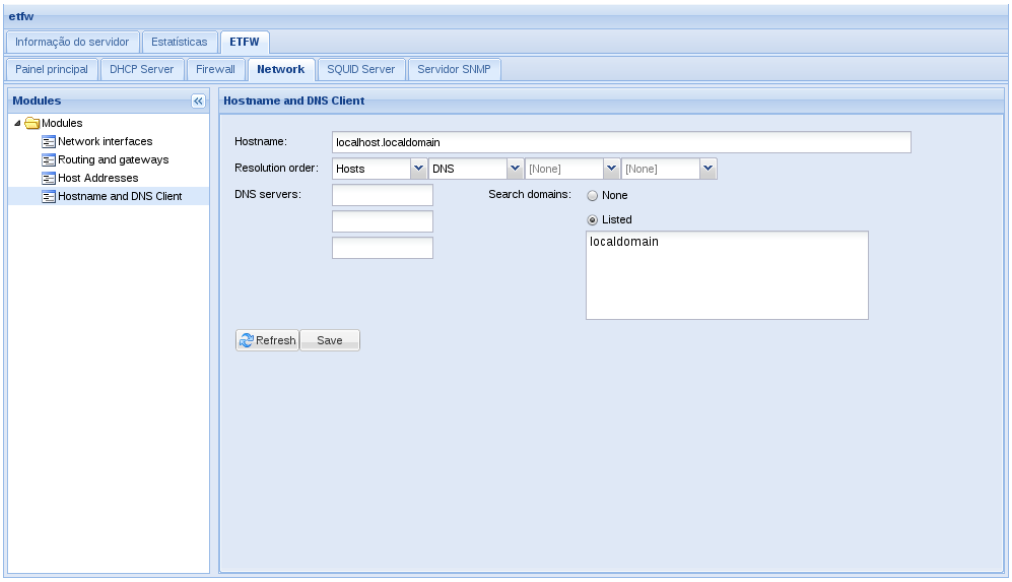


Figure 4.18.: DNS client

4.1.3. Firewall rules

By accessing the tab *Firewall* we have the ability to set the rules of Firewall. This firewall is based on *iptables*, formed by three basic objects:

- Rules
- Chains
- Tables

The rules are lower-level objects that perform packet filtering or manipulation. A rule consists of the following parts:

- The table were the rule will be added;
- The chain chain to which the rule will be added;
- The filtering or manipulation instructions.

The rules are organized in chains and act as a checklist of rules ordered.

The chains are organized in tables that group a large number of possible rules to filter and/or manipulate packets.

The operation of the firewall proceeds as follows: if the packet header meet the requirements of the rule, this will follow the destiny imposed by the rule, otherwise it will be evaluated further by the next rule.

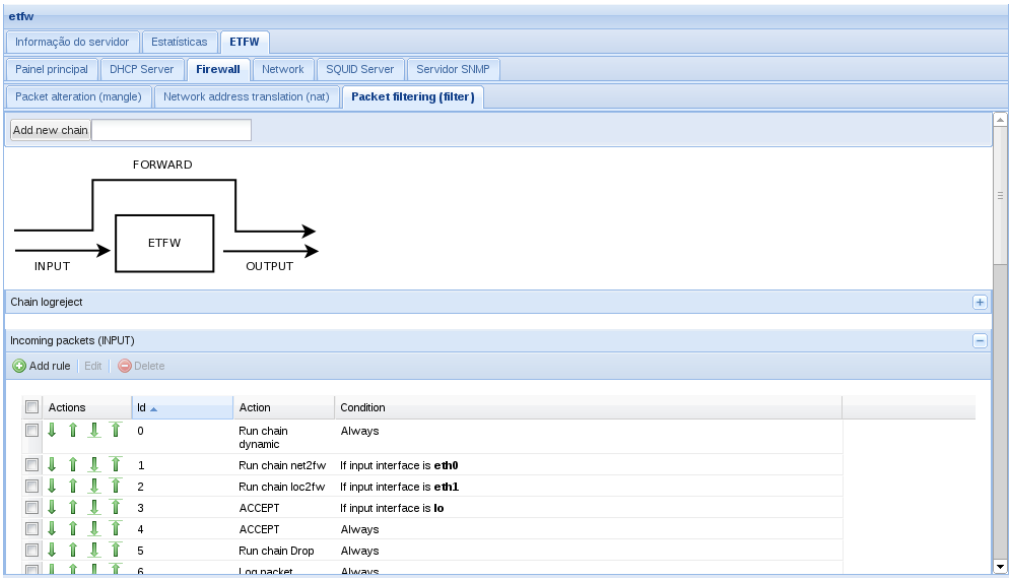


Figure 4.19.: Firewall: Filter table

By accessing the firewall tab the interface shows three tables: *Packet alteration - mangle*, *Network address translation - nat* and *Packet filtering - filter*.

4.1.3.1. Table *Filter - Packet Filtering*

The table *filter* is used to filter packets that pass through the firewall and presents three firewall pre-defined chains:

- **INPUT** - filter packets whose destination is the own firewall;
- **OUTPUT** - filters packets whose origin is firewall;
- **FORWARD** - filter packets that pass through the firewall which are not the source nor the destination of the firewall.

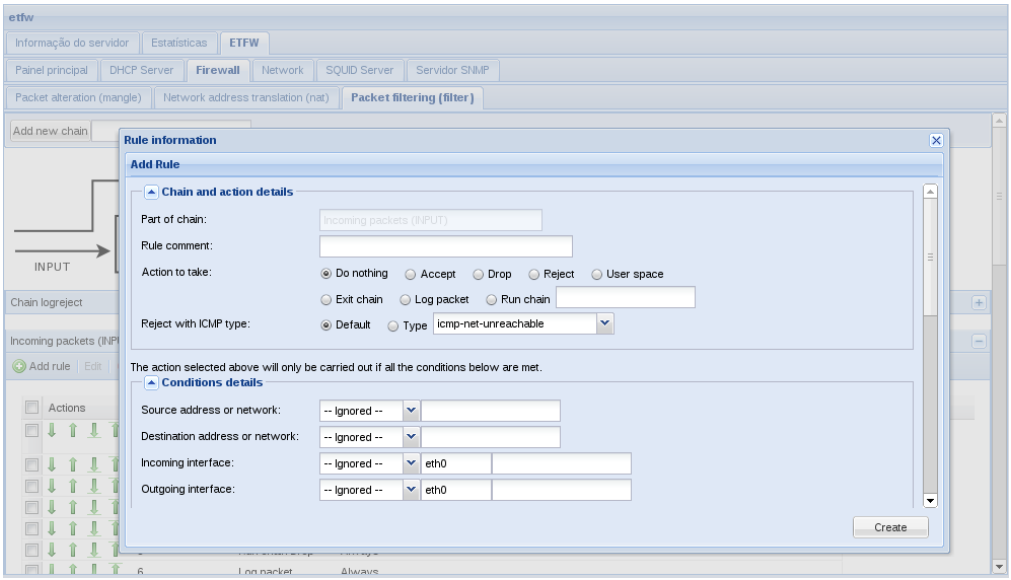


Figure 4.20.: Creating a rule on table *filter* - Chain and action

When creating a rule in a filter table's chain some parameters are required for action to take:

- **Rule comment** - allows you to write a short comment to identify the rule to be created;
- **Action to take** - action to be taken, who decides what should be done with the package, if it matches the rule. The most important actions are:

  Drop - removes the packet without doing anything else;

  Accept - the firewall lets the packet pass through and the data is sent to the recipient;

  Reject - works the same way as the drop but is sent an *ICMP* error back to the sender of the package;

  Userspace - if this option is active, a multicast is donne by kernel into a socket where can be a listening process.

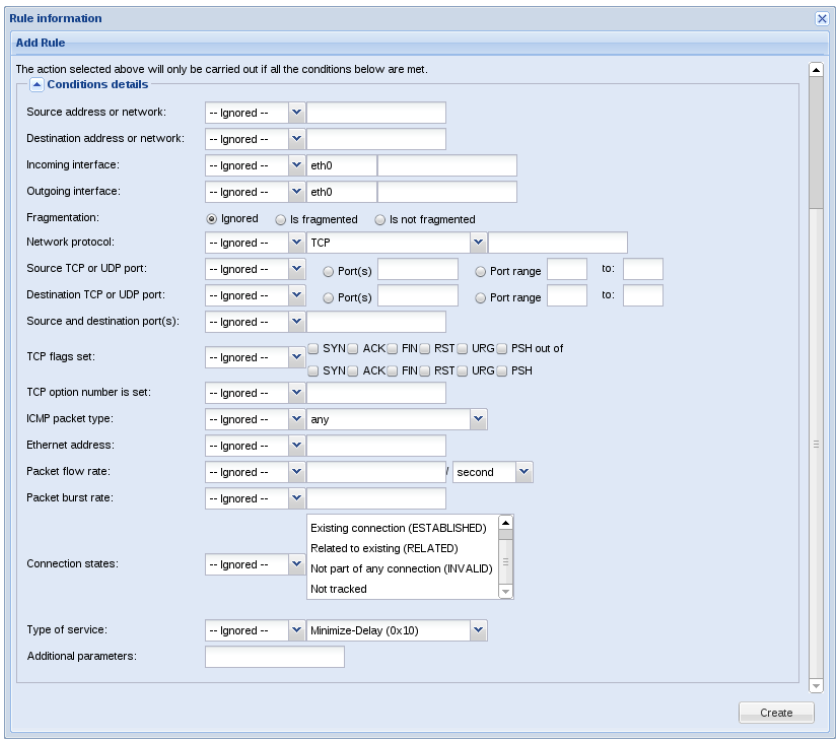


Figure 4.21.: Creating a rule on table *filter* - Condition details

Other options that can be completed in the condition are the following:

- **Source address or network** - Network address that establish the origin of the package. It is usually a combination of IP address with the subnet mask separated by a slash (eg 192.168.1.0/255.255.255.0 or 192.168.1.0/24);
- **Destination address or network** - Network address to which the packet is intended. It has the same combination as before;
- **Incoming interface** - Specifies the input interface of the package;
- **Outgoing interface** - Specifies the output interface of the package;
- **Fragmentation** - Sometimes a packet undergoes fragmentation because of its size, being its part joined together later in the destination. This option sets whether the rule is matched by fragmented packets or not;
- **Network protocol** - Network protocol;
- **Source TCP or UDP port** - Sets the match rule with the incoming port (tcp or udp), and may be defined a range of ports (example: 1000:1050) or a list doors separated by commas;
- **Destination TCP or UDP port** - Sets the output port match and may be offered a range of ports (example: 1000:1050) or a list of ports separated by commas;

- **Source and destination port(s)** - Sets the door match, both incoming and outgoing, may be offered a range of ports or a list of ports separated by commas;
- **ICMP packet type** - ICMP packet type;
- **Ethernet address** - Defines a physical address of a network that will serve to match the rule;
- **Packet flow rate** - Sets the volume of packages that will make the rule match;
- **Packet burst rate** - Sets the threshold at which the packets begin to make match with the rule;
- **Connection states** - Specifies the number of links that make the rule match;
- **Type of service** - Defines the type of service for which we want the rule to do match;
- **Additional parameters** - Specifies additional parameters that will be passed directly to the line of the rule to be applied.

4.1.3.2. NAT table - Network address translation

The NAT table is used for network address translation, or translate a package with a particular field of origin or destination. Only the first packet will be affected by this chain, after which the remaining packages will apply the same actions as the first. This table presents three pre-defined chains:

- **PREROUTING** - applies the changes to the packages when the target needs to be changed;
- **POSTROUTING** - applies the changes to the packages when the source needs to be changed;
- **OUTPUT** - applies the changes to packets originated by the firewall.

The current targets in this table are:

- **DNAT** - used in cases where you have a public IP address in the firewall and if you want to redirect the access to another host (a DMZ for example), thus allowing forward traffic.
- **SNAT** - used when you want to change the origin of package, usually to hide the addresses of local network or *DMZ*.
- **MASQUERADE** - used the same way that the SNAT and for the same reason, but the outgoing IP address is not specified, by using the source address of the interface package. This rule is used primarily for dynamic IP addresses, because if the link goes down, the source address that was being used is discarded yielding place to a new source address of the interface when the connection is restored.

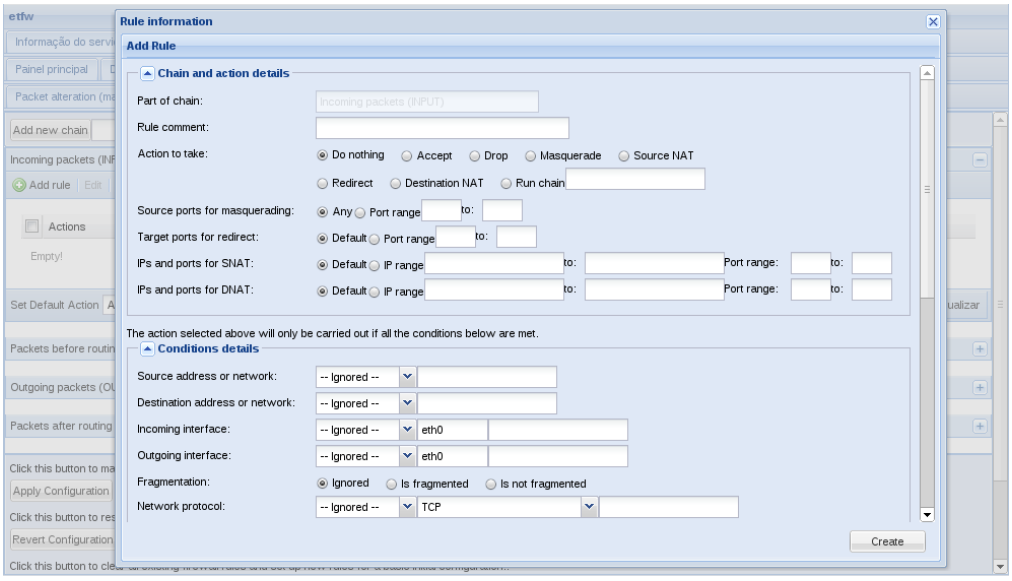


Figure 4.22.: Creating a rule on NAT table

The options used in the NAT table are identical to the Filter table. The differences are listed bellow:

- **Action to take** - action to be taken, has the same functionality described in the Filter table, but has two different options:

  Masquerade - Rewrites the outgoing IP address, when it comes to dynamic IP addresses;

  Source NAT / **Destination NAT** - Depending on the chain (PREROUTING, POSTROUTING or OUTPUT), available options may vary. They will be *Source NAT* and *estination NAT*, respectively. Also, they will re-write the IP's input and output respectively.

4.1.3.3. Mangle table - Packet alteration

This table is not addressed in this version of the manual.

4.1.4. DHCP Server

In this tab we can configure the DHCP server, including IP range to allocate the hosts, router address, DNS server address, view active leases, and to start/stop the server.

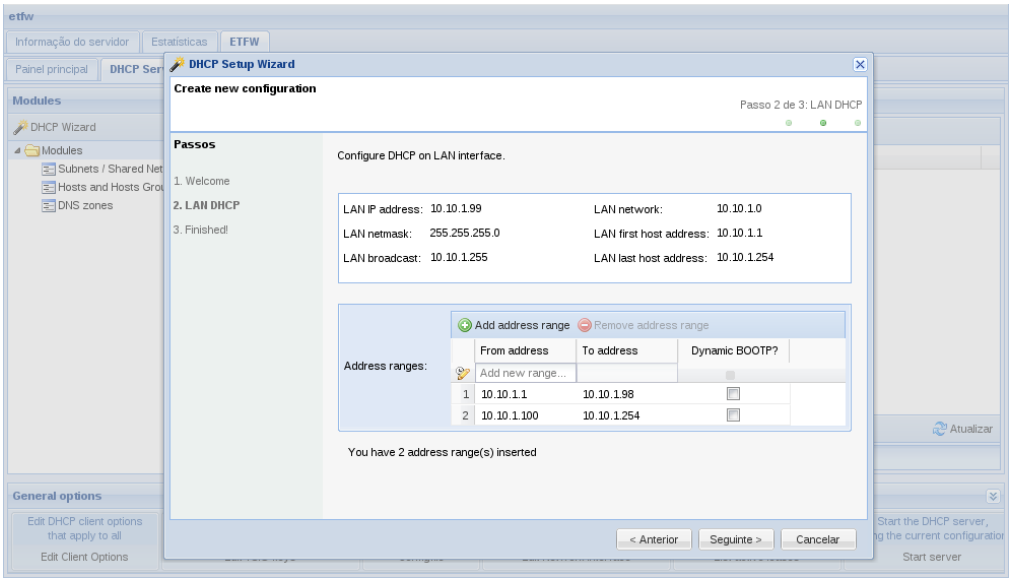


Figure 4.23.: IP range setup

From the DHCP Wizard we can, in a first stage, set the IP ranges allocated to hosts.

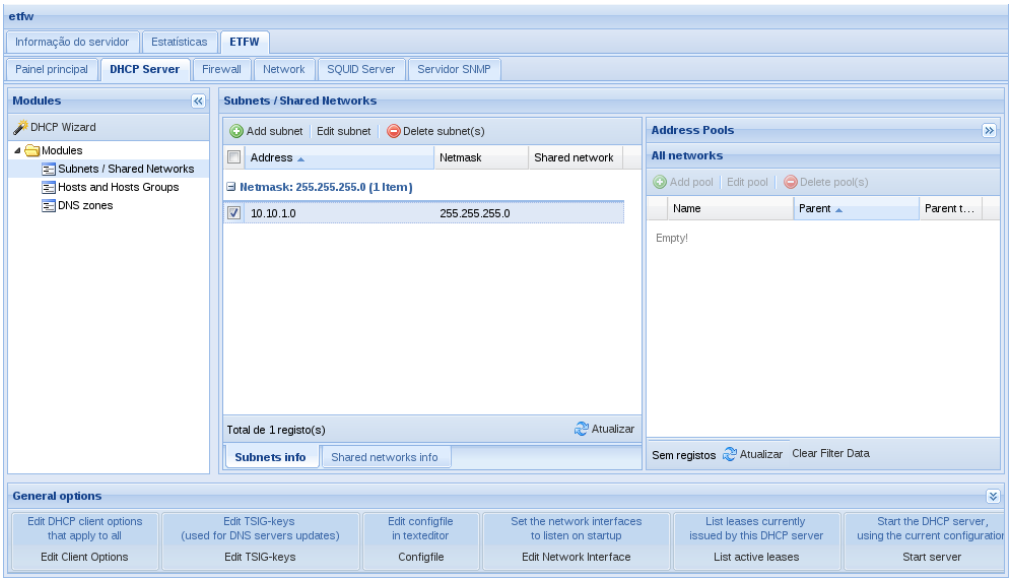


Figure 4.24.: Subnets setup

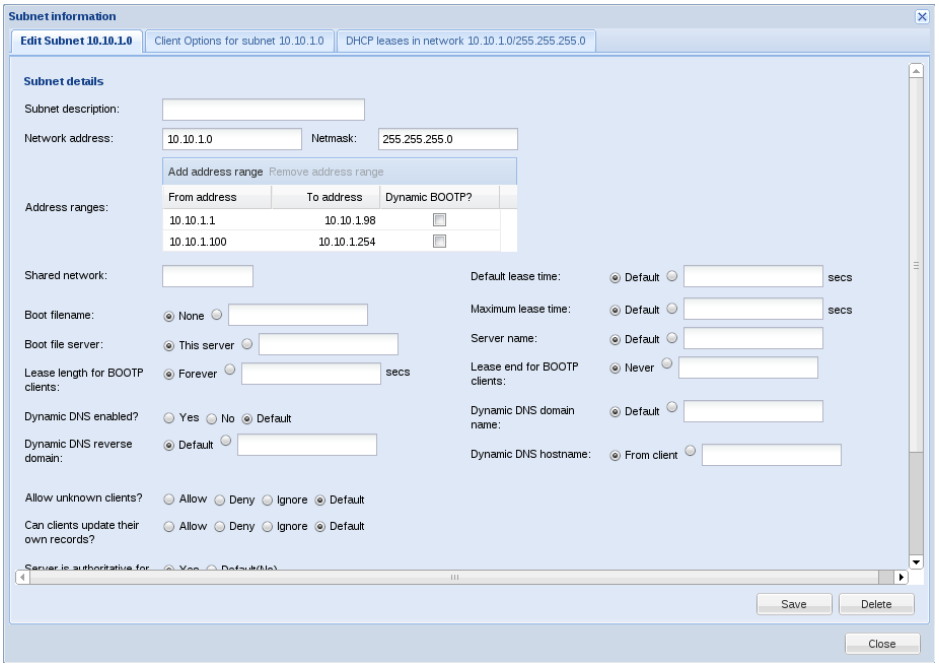


Figure 4.25.: Subnet edit

Later, you can edit the subnets and set the appropriate parameters to our setting for the network address, netmask, address range, among others.

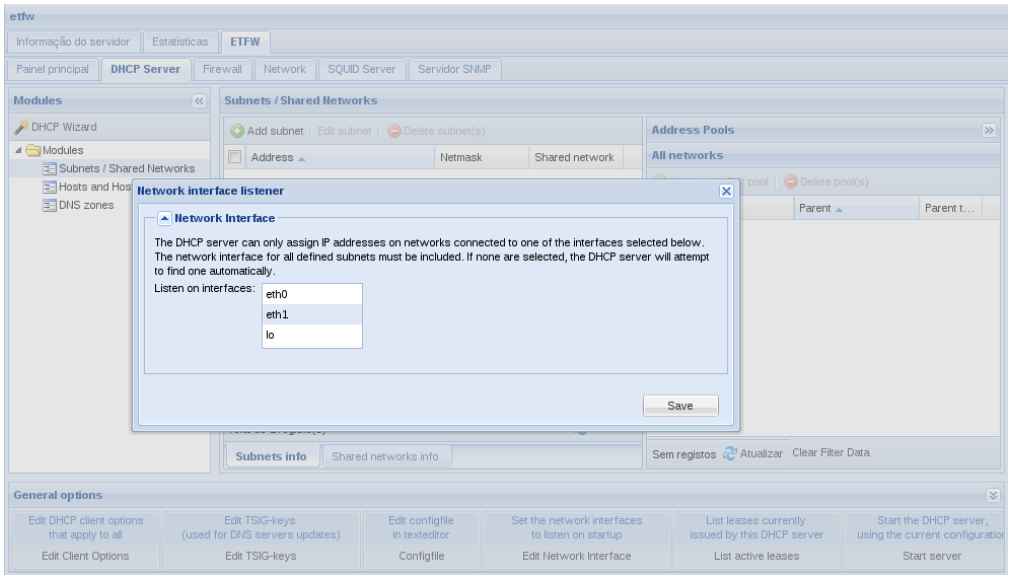


Figure 4.26.: Choose an interface

To configure the server properly you must set the interface on which service will operate. Go

to *Edit Network Interface* and choose the desired network interface.

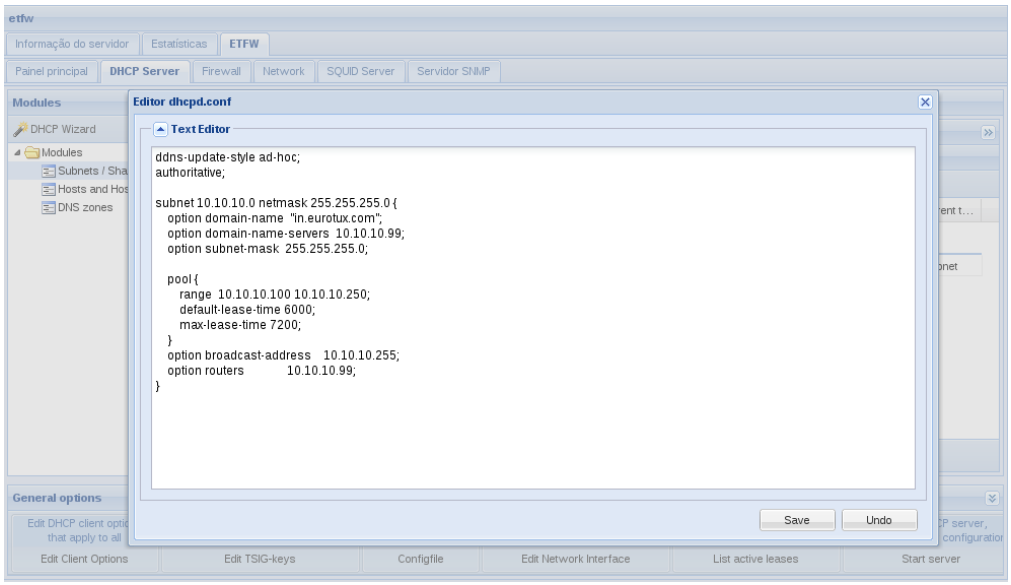


Figure 4.27.: Configuration file edition

Additionally, you can always view and edit the configuration file directly and put the desired options.

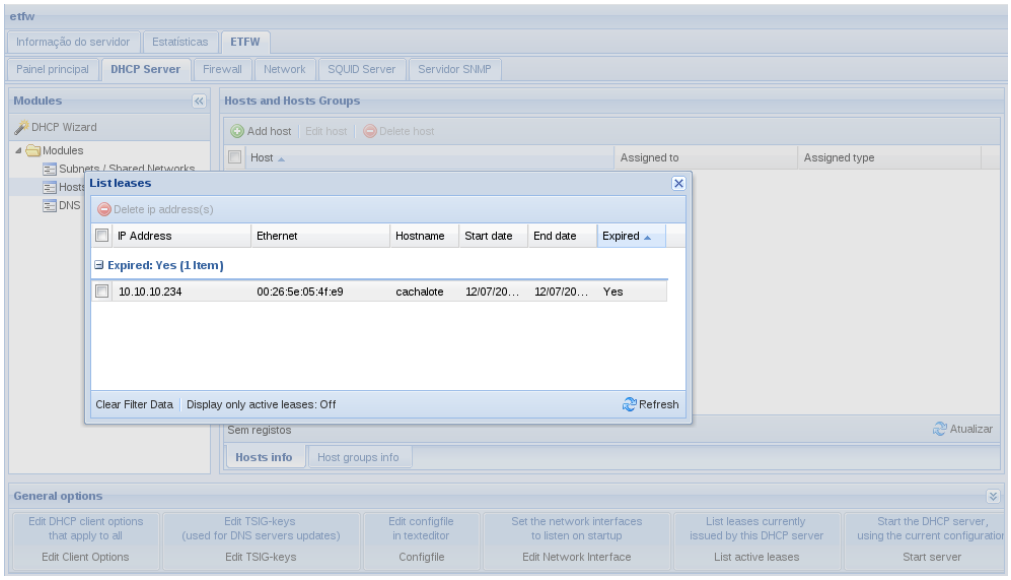


Figure 4.28.: List of active leases

In any time you can find a list of assigned IPs by selecting the option *List active leases*. This

option is also available for each subnet.

4.1.5. SQUID server

In the *SQUID Server* tab you can configure the SQUID Proxy service.

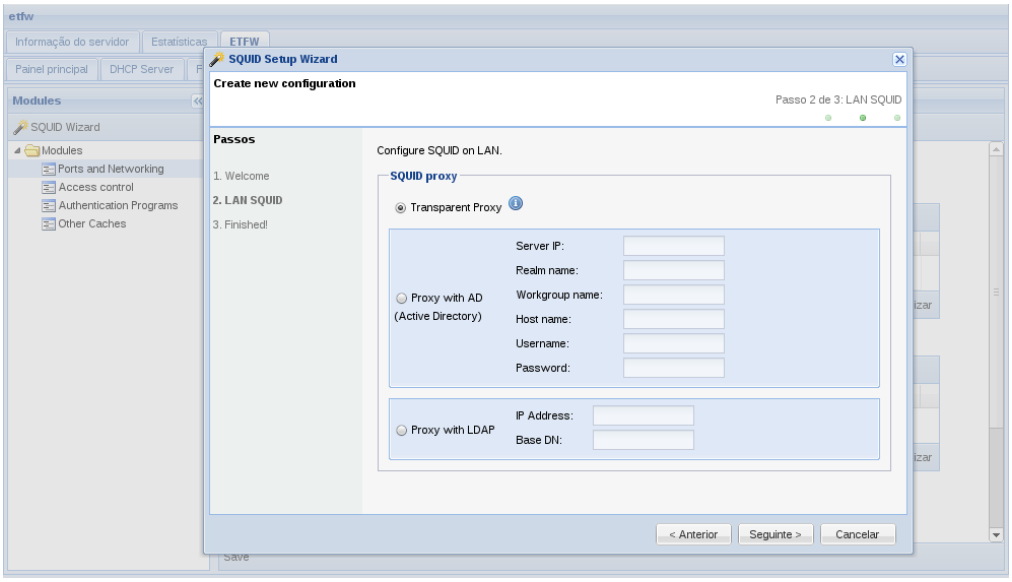


Figure 4.29.: SQUID server setup

The proxy service forward requests to the Internet and keeps a content's cache in a way to speed up the display when they are requested again.

In the *SQUID Wizard* we can configure the proxy service easily. It has three pre-defined configuration options:

- *Transparent Proxy* - Transparent Proxy;
- *Proxy with AD* - Proxy with authentication in Active Directory;
- *Proxy with LDAP* - Proxy with LDAP authentication.

In the first case, the transparent proxy, allows you to have a cache system cache completely invisible to the customers. This system does not support authentication.

In the other two cases, the proxy makes use of authentication systems, such as Active Directory or LDAP.

Additionally, you can customize the service in accordance with the needs, in particular define: Ports and Networking, Access Control, Authentication Programs, among other types of cache.

4.1.5.1. Ports and Networking

In *Ports and Networking* you can define the port (SSL or not), and IP address or hostname of the proxy service that will fill orders, in addition to other possible configurations, including:

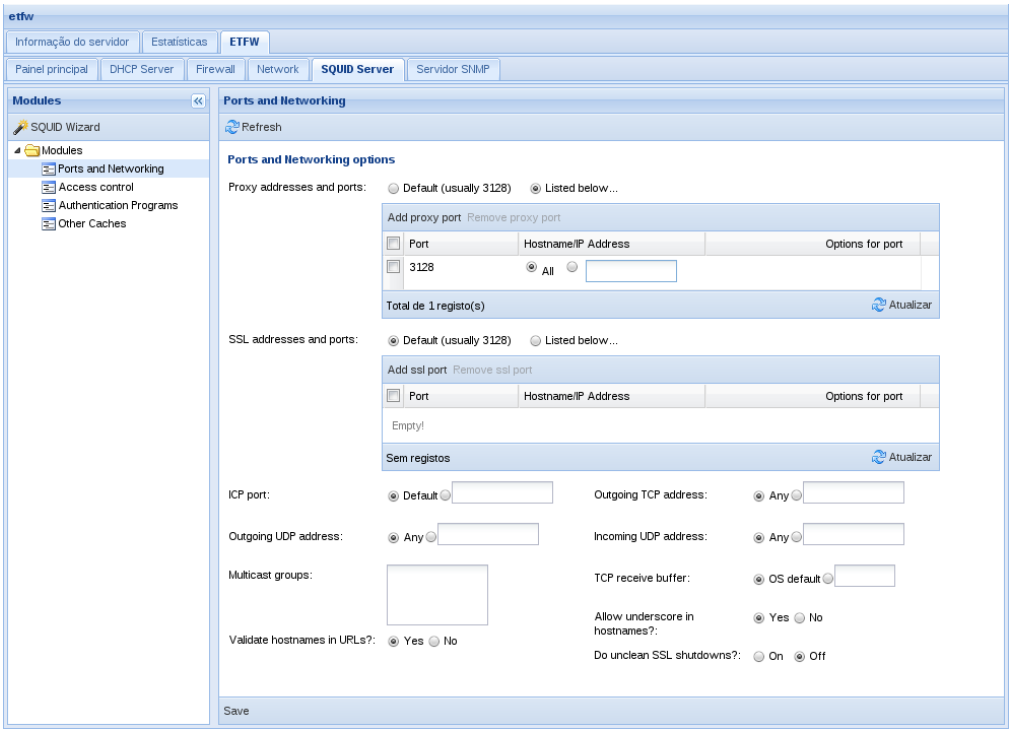


Figure 4.30.: Port and network configuration

Request port *ICP*; Validation name addresses of URLs; Specification group *multicast*; Output address of TCP traffic; Output address UDP traffic;

- *ICP port* - ICP request port;
- *Validate hostnames in URLs?* - Validation of urls' address;
- *Multicast groups* - Multicast groups;
- *Outgoing TCP address* - Output address for TCP traffic;
- *Outgoing UDP address* - Output address for UDP traffic;
- *Incoming UDP address* - Input address for UDP traffic;
- *TCP receive buffer* - Buffer *TCP*;

4.1.5.2. Access Control

The access control policies are based on a combination of *ACL*(*Access Control Lists*).

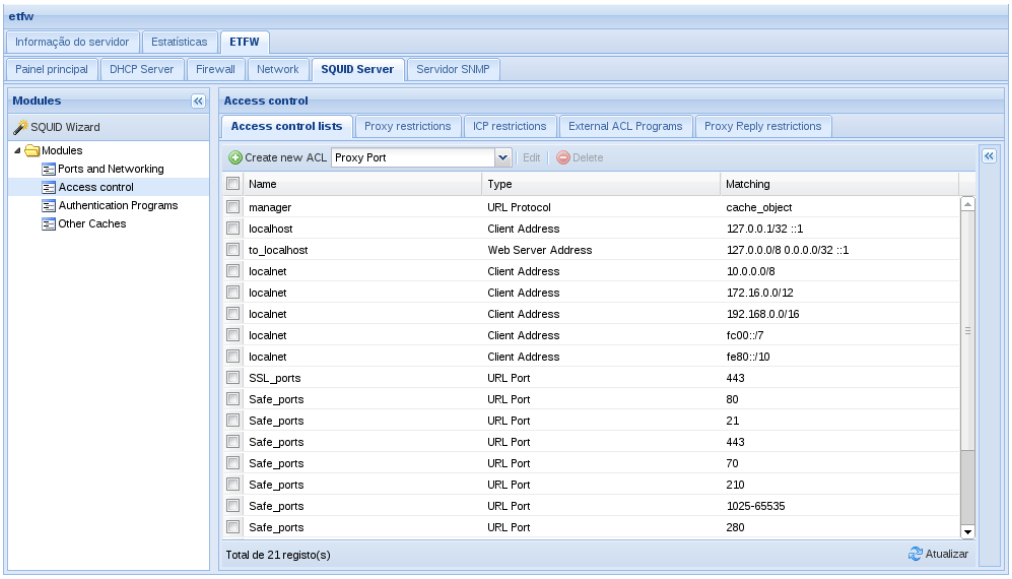


Figure 4.31.: Setup of access control policies

In the configuration of access control policies we can define filtering models that can be used later in the sections of restrictions of access (*Proxy Restrictions*, *ICP Restrictions*, *Proxy Reply Restrictions*) .

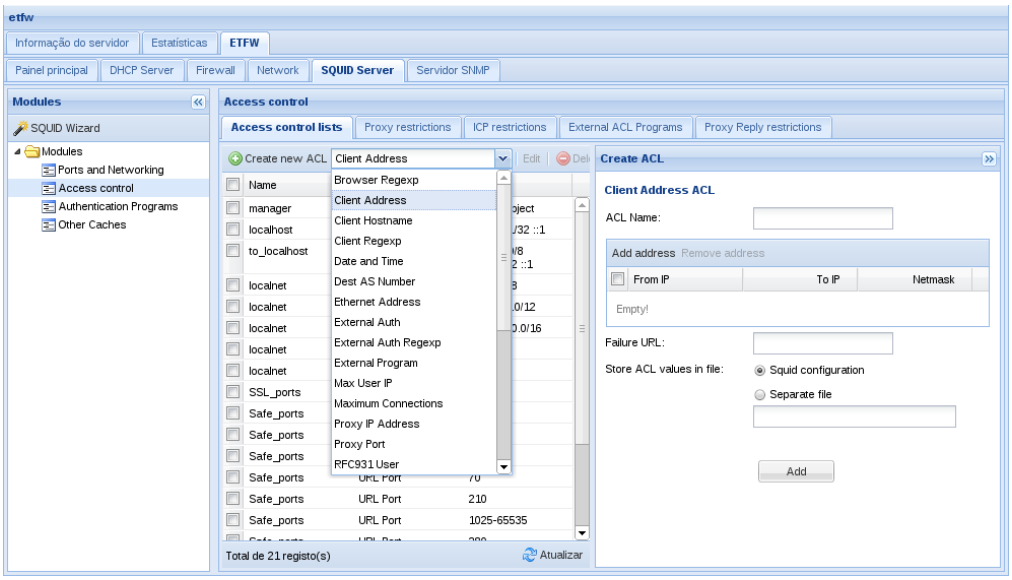


Figure 4.32.: Creating a new ACL

To create a new ACL, we select the type and fill with the desired parameters.

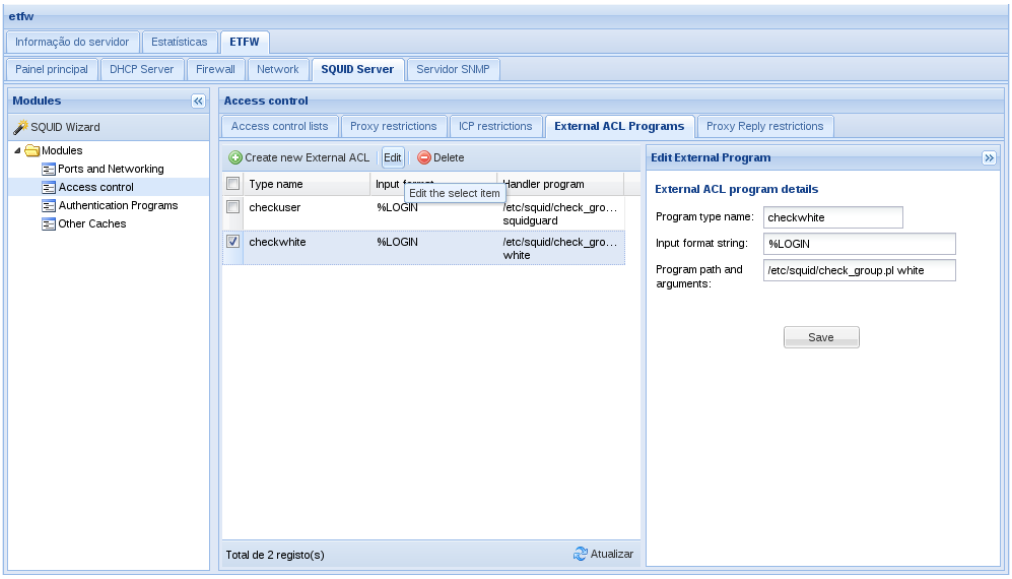


Figure 4.33.: Creating a new external acl

It is also possible to define external ACLs that allow to expand the functionalities of the proxy, using for this purpose external programs that manage the access. These ACLs allow, for example, the authentication in a server such as a Active Directory or a LDAP, or even the verification of source addresses in a SQL database.

The creation of an external *ACL* external requires the creation of an internal ACL with reference to the first one.

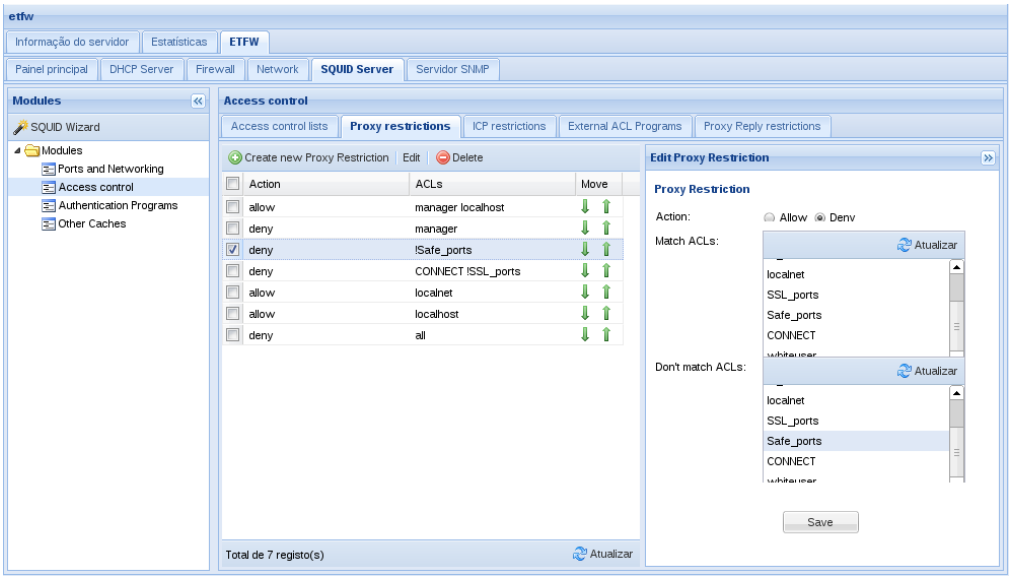


Figure 4.34.: Restriction definition - *Proxy restrictions*

After the ACL definition, you must associate the restrictions with the ACLs to be applied in every situation, or what action to do: accept or deny. The rules are applied in top-bottom order, and when a match is found the action takes place. Importantly, if there is a deny all rule, all requests that pass the rules are accepted.

4.1.5.3. Authentication Programs

In *Authentication Programs* are defined programs that ask the browser/user what's his authentication credentials.

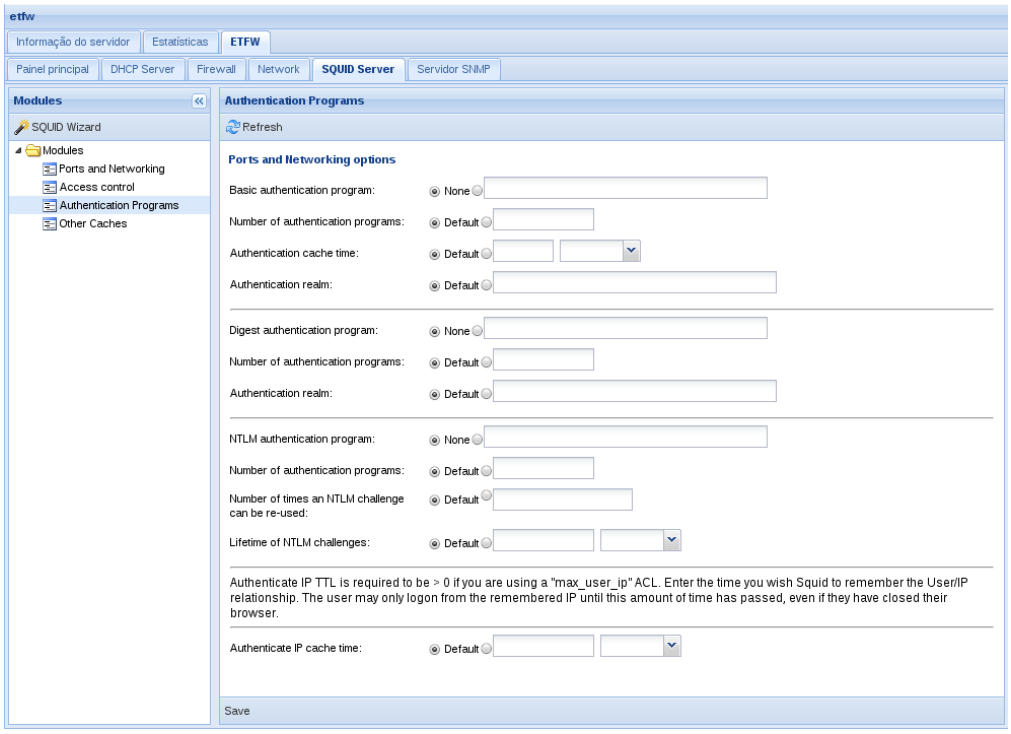


Figure 4.35.: Authentication Programs

There are two types of authentication:

- *Basic* - when the browser does not support transparent authentication, it will show a popup asking the user credentials
- *NTLMSSP* - transparent authentication for the user

We can even set the following parameters:

- *authentication program* - Specifies the user program for authentication. The program reads a line containing user and the password separated by space, and responds *OK* on success or *ERR* on failure;

- *Number of authentication programs* - Maximum number of process that the authentication could have;
- *Authentication realm* - Text that will appear in the dialog box in case of basic authentication;
- *Authentication cache time* - Specifies how long a valid authentication is maintained avoiding requests;
- *Number of times an NTLM challenge can be re-used* - A maximum number of times that can be used in NTLMSSP authentication type;
- *Lifetime of NTLM challenges* - Lifetime of the *NTLMSSP* authentication type;
- *Authenticate IP cache time* - Specifies for how long the cache is kept about the user-IP association.

4.1.5.4. Other Caches

In *Other caches* we can specify other proxies to be used in a chain the get information.

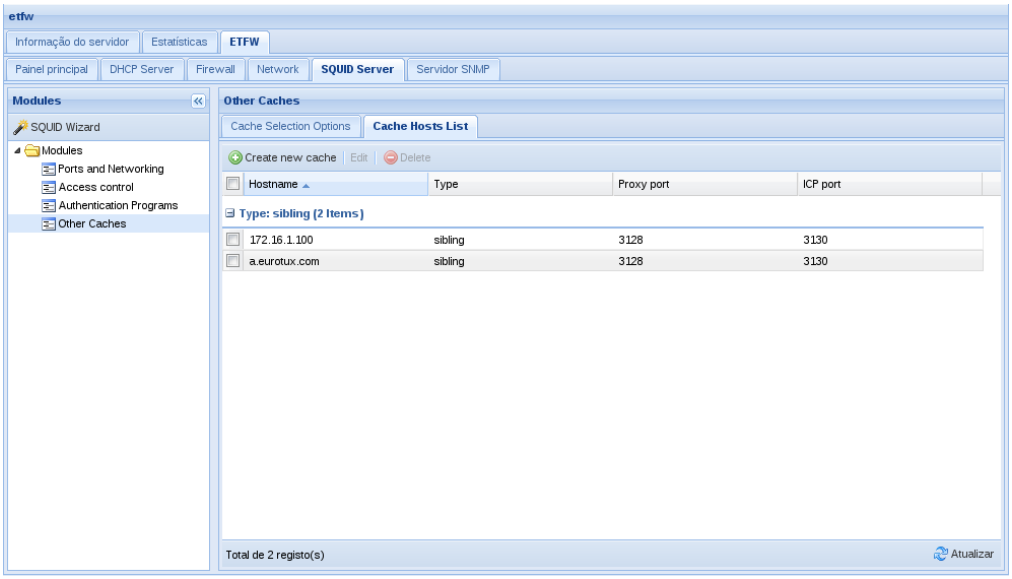


Figure 4.36.: Proxies - Other Caches

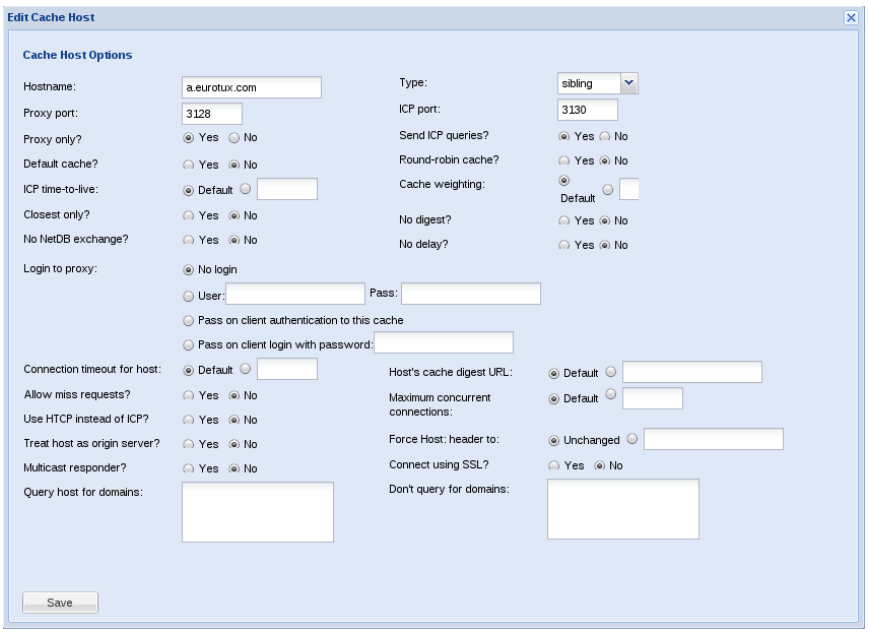


Figure 4.37.: Edit host cache

To specify a different proxy it's necessary to specify the following fields:

- *Hostname* - IP address or hostname (*FQDN*) of the cache to being used;
- *Type* - Type hierarchy to be used between the proxies:

  parent;

  sibling;

  multicast;
- *Proxy port* - The port that proxy uses for listening requests;
- *ICP port* - Used port to ask neighbors about the cache objects that they have;
- *Proxy only?* - Indicates that the requested content to this proxy is not to save locally;
- *Send ICP queries* - Used for proxies that does not have ICP, i.e., that indicates if they have a object or not;
- *Default cache* - It is used when the proxy is the last in the hierarchy line;
- *Round-robin cache* - To use the round-robin algorithm of search for proxies;
- *ICP time-to-live* - Specifies the Time-To-Live(ttl) used in multicast protocol;
- *Cache weighting* - Specifies the importance of the cache on the process o choosing proxy (1 for lower priority).

4.1.5.5. Usage exemples

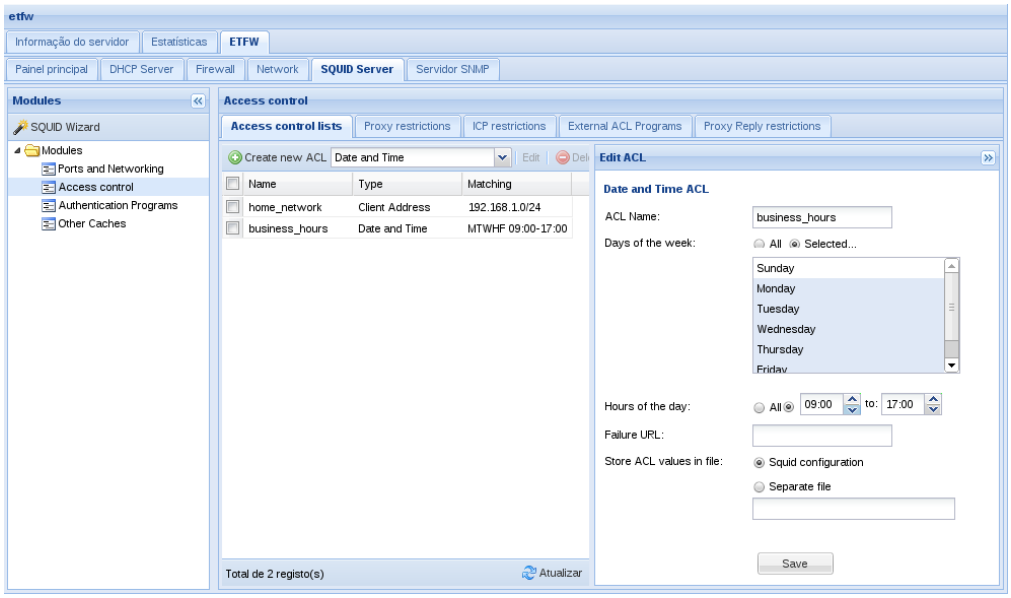


Figure 4.38.: Restrict internal network access only during work hours - Creating ACLs.

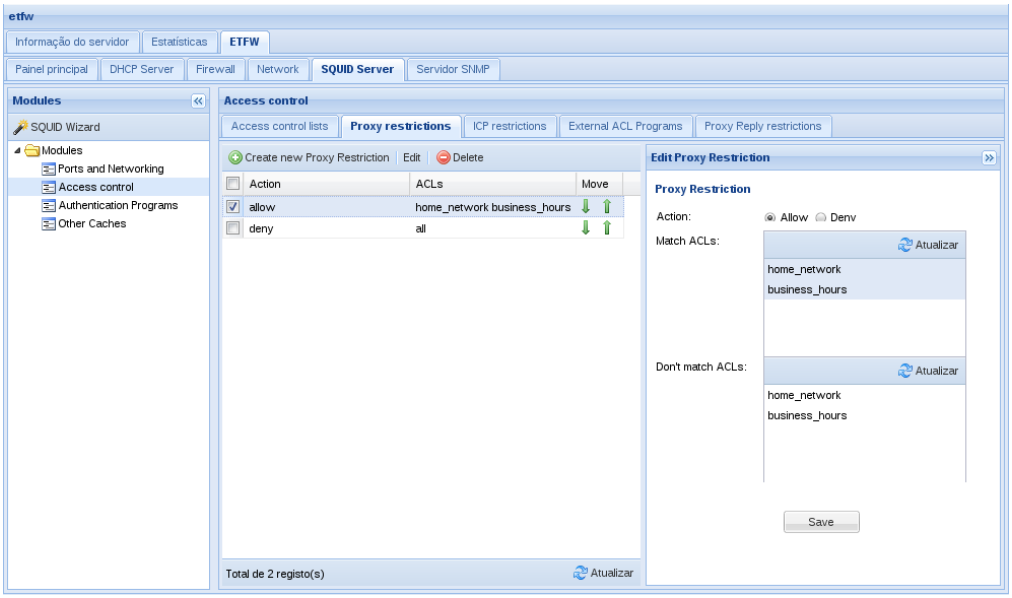


Figure 4.39.: Restrict internal network access only during work hours - Creating restriction using previously defined ACLs

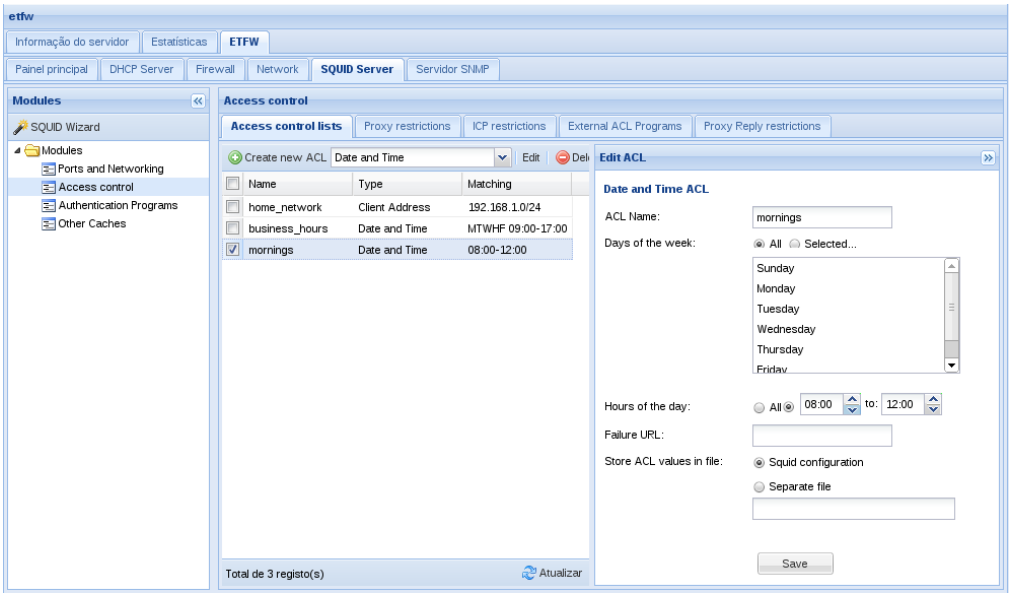


Figure 4.40.: Restrict access only in the morning - Creating ACLs

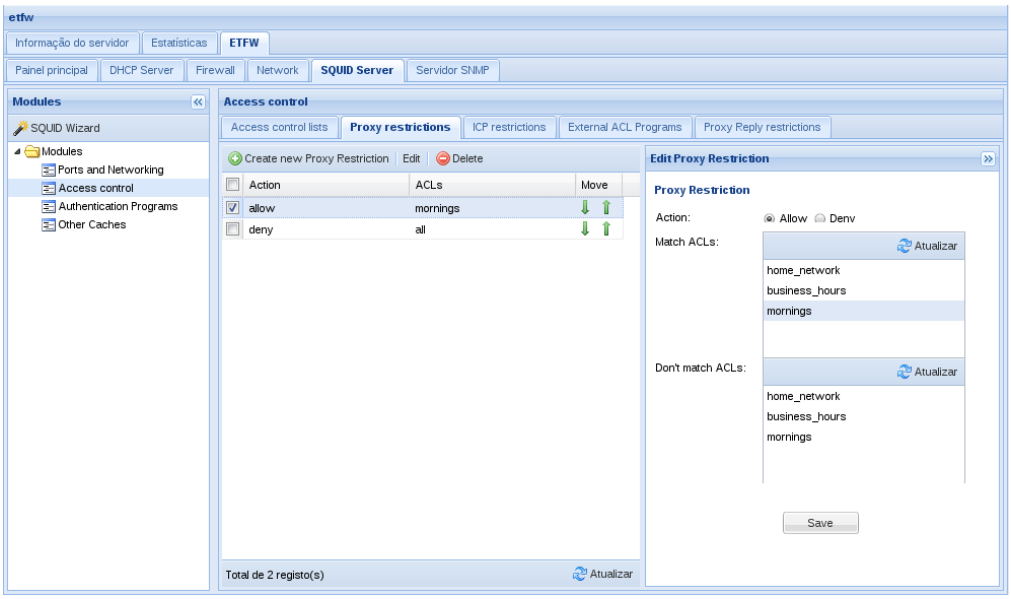


Figure 4.41.: Restrict access only in the morning - Creating restriction using previously defined ACLs

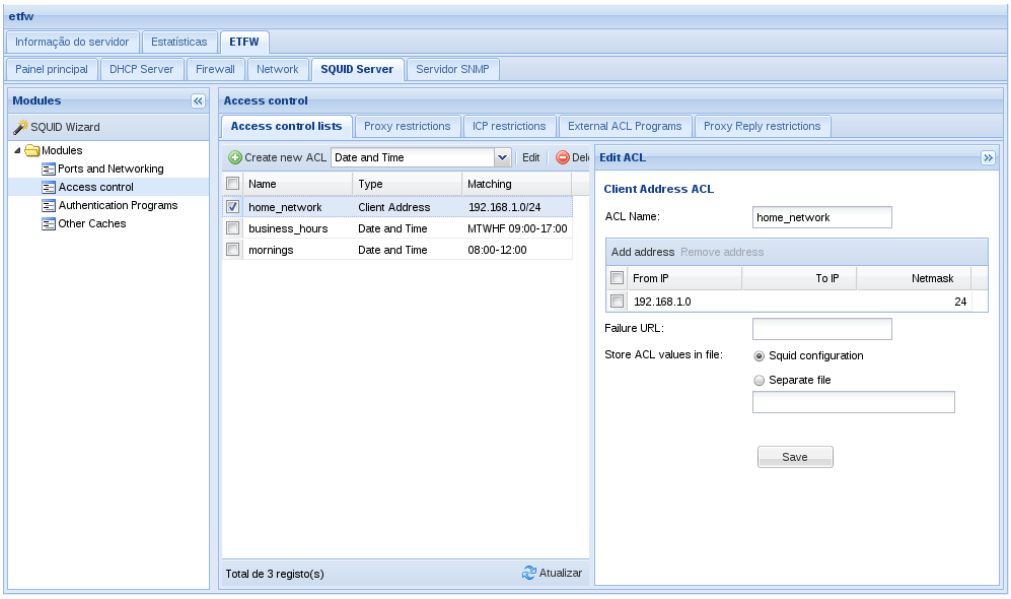


Figure 4.42.: Restrict access by IP address - Creating ACLs

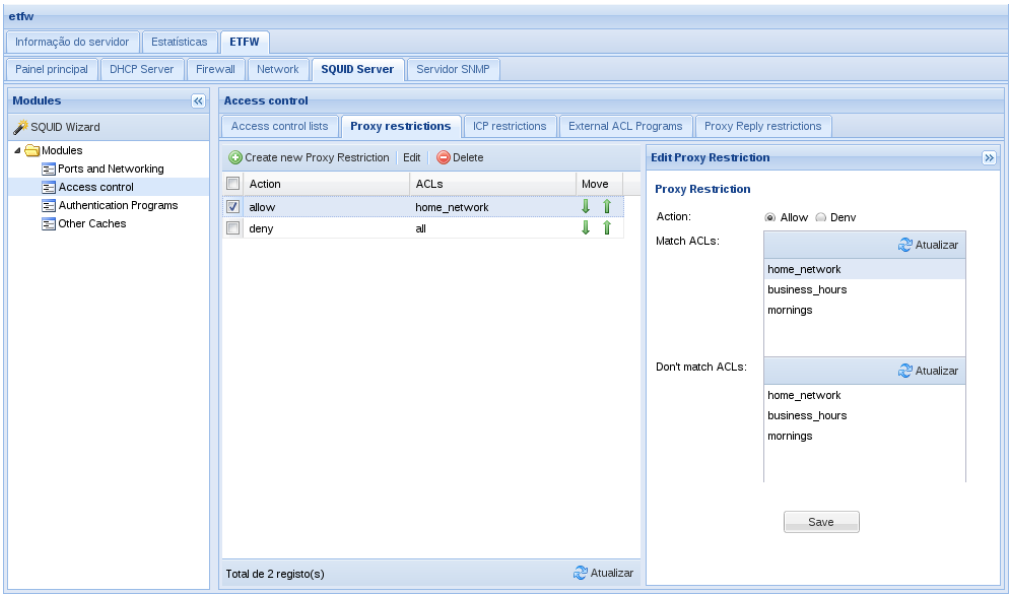


Figure 4.43.: Restrict access by IP address - Creating restriction using previously defined ACLs

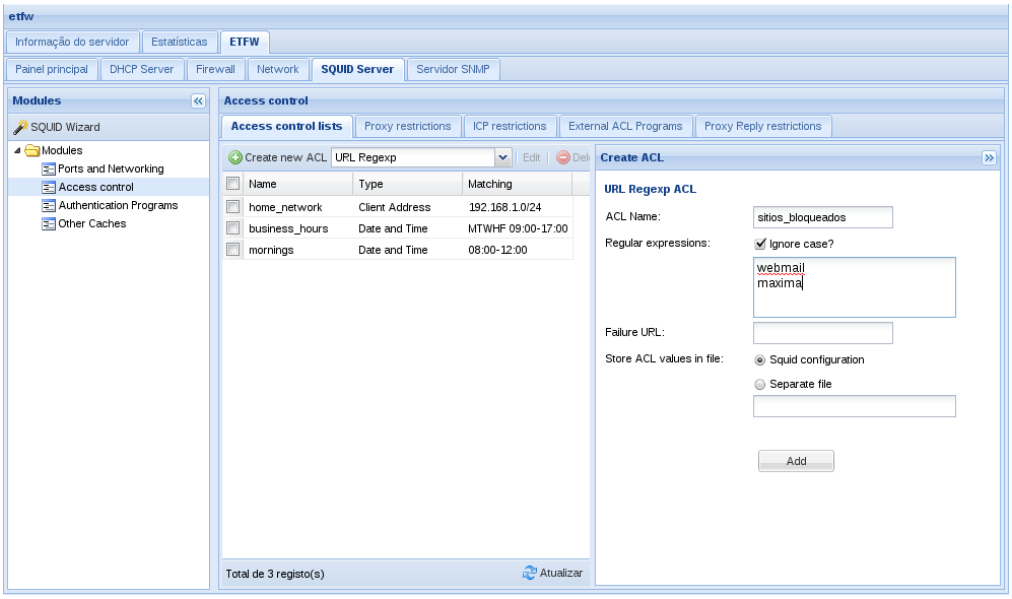


Figure 4.44.: Denying access based on a regular expression on the URL - Creating ACLs

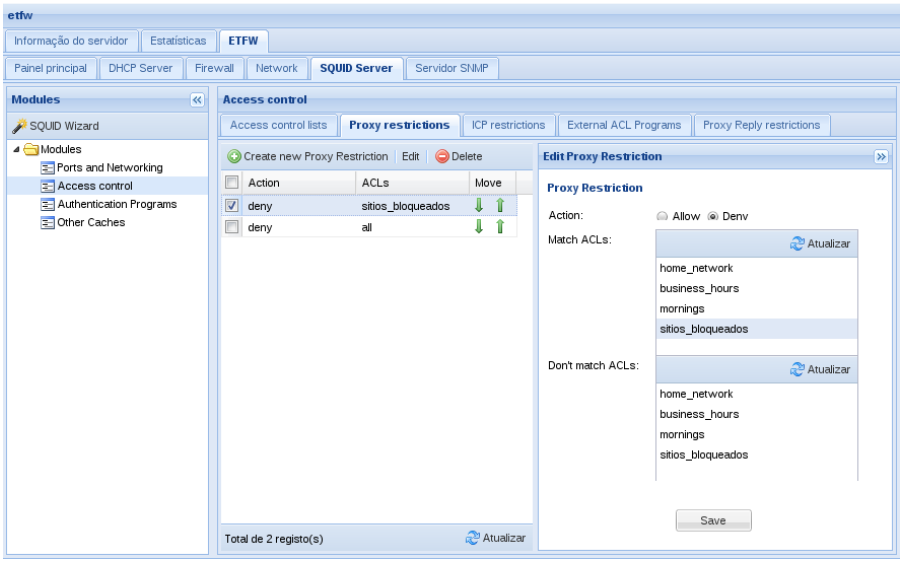


Figure 4.45.: Denying access based on a regular expression on the URL - Creating restriction using previously defined ACLs

4.1.6. SNMP server

In the SNMP server configuration interface you can define the following configuration:

- System information: location and contact;

- Trap server's IP address;
- Trap community;
- Monitoring stations.

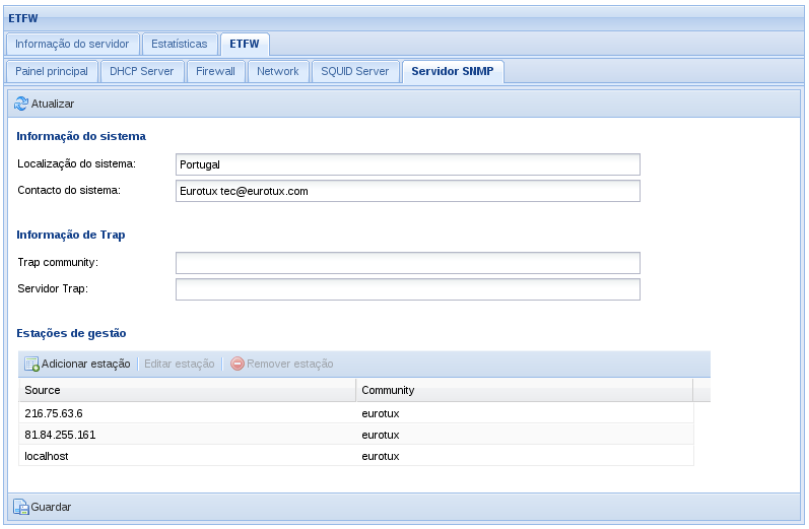


Figure 4.46.: SNMP server setup

4.2. ETMS

Through the Central Management interface its possible to configure all the settings needed to run the mail server [1].

The management is divided into three tabs relating to different configuration contexts. The first tab shows the status of the service and lets you start, stop or restart the service. It is also possible to make backups of your configuration (in the agent itself) and restoration of it - useful for testing new configurations. In the second separator can be made the domain configuration. Finally, the third tab allows the configuration of email accounts. The sub-sections 4.2.2 and 4.2.2.4 indicate the possible configurations.

The Figure 4.47 illustrates the existing tabs. To find them select the virtual machine that contains the installation of ETMS, followed by the option *ETMS* that is on the tabs of the right side panel.

[1] The system was implemented in order to maintain compatibility with the *Webmin* interface

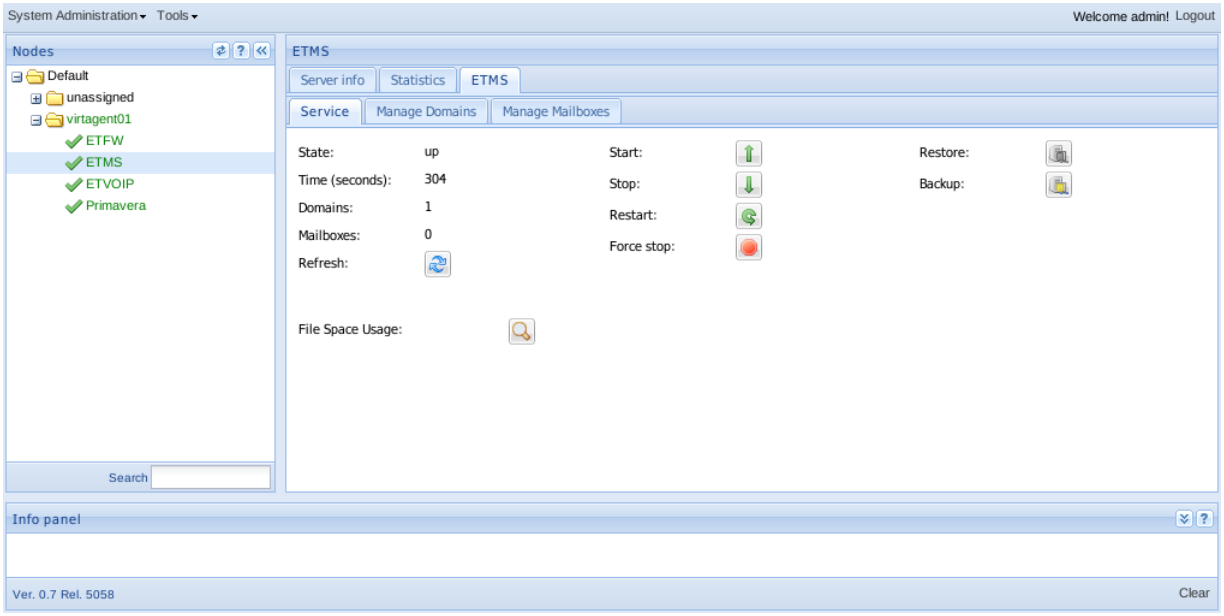


Figure 4.47.: ETMS - Main information panel

4.2.1. Tab 1 - Service

The separator *service* is divided into three columns (Figure 4.47). On the left we can see some information about the running process of the service including: information about its state (*Up* - working, *Down* - stopped), the number of domains and email accounts, and the total space occupied by emails on the server. Note that the total space occupied is not visible immediately after the opening of the tab, because it is a potentially lengthy operation. Thus, to request this information you must select the icon on the right. Information on the service status is updated the first time the tab is open and can be refreshed when requested explicitly, through the button *Update*.

In the center column are options for *Start*, *Stop* and *Restart* the process that supports the service. If you are have problems stopping the service, try using the *force stop* button instead the normal one.

In the right column are defined operations for backup and restore settings. These options should only be used to test new settings, because its storage is done locally (on the machine where the mail server).

4.2.2. Tab 2 - Manage domains

The contents of the separator *Manage Domains* is divided into two main areas/grills, where you can select lines (Figure 4.48). The grid on the left lists any existing domains. The right grid, lists the existing alias for the selected domain.

In both areas it is possible to perform operations over the selected items by using the buttons available on the toolbar under the grill in question. Note that selecting a domain, the list of alias gets refreshed.

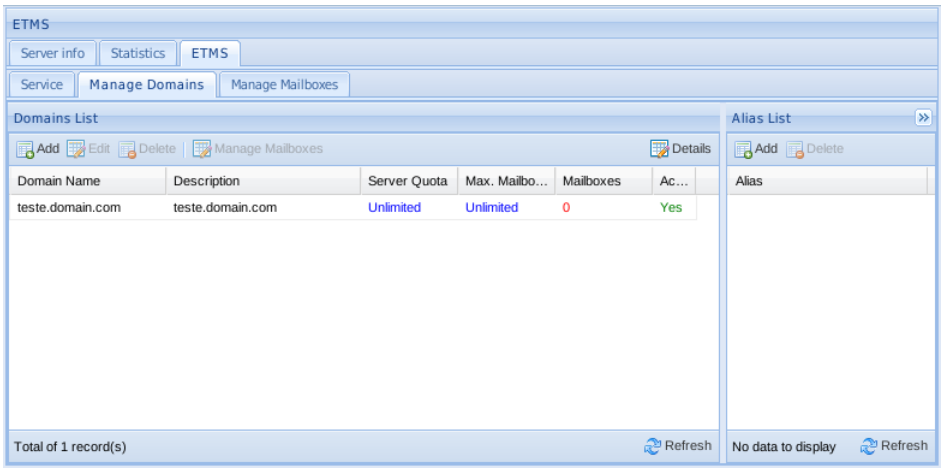


Figure 4.48.: ETMS - Manage domains panel

4.2.2.1. Add a new domain

To create a domain use the *Add domain* button, which opens a window with some fields to fill, as shown in Figure 4.49. After filling the fields press the button *Save* to make the changes. Please note that the first three fields are mandatory; the grid with existing domains is refreshed after adding a new domain.

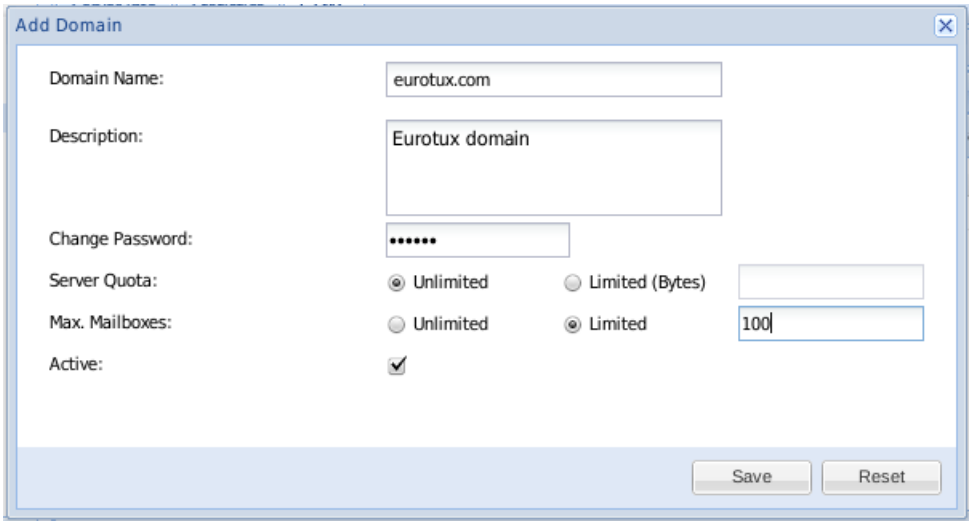


Figure 4.49.: Add domain

For a better understanding, we describe briefly the existing fields, indicating for each example:

- **Domain name** - Desired domain name (E.g.: eurotux.com)
- **Description** - Short description about the domain (E.g.: IT department)
- **Password** - *Password* to use for webmin login, bigger than 6 characters. (E.g.: PassWord)
- **Server quota** - Maximum value in Byte for storing email (E.g.: 1000000000 Bytes)
- **Number of mailboxes** - Maximum number of mailboxes that can be created in this domain. The reduction of the number of mailboxes (available in option *Edit domain*) will not remove any existing mailboxes. (E.g.: 10)
- **Active** Activate or not the domain. This option inhibits the delivery of new messages.

4.2.2.2. Edit domain

To edit a domain, select the corresponding line and choose the **Edit domain** button. It will open a window (see Figure 4.49) with the attributes of the domain pre-filled with the settings previously made (in previous Section 4.2.2.1).

After saving, the grid that lists your existing domains is updated with the new settings.

4.2.2.3. Remove a domain

The removal of a domain also requires the removal of its alias and associated email accounts (including any existing emails). For removal of a domain, select the line that identifies the domain to remove, and choose the option **Remove**. Then answer yes to the confirmation question, as shown in Figure 4.50. The success of the operation is shown in *Information Panel*.

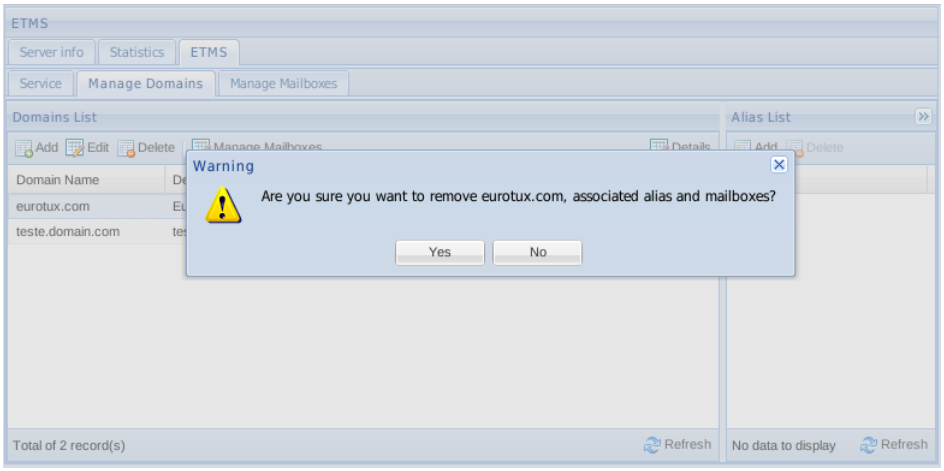


Figure 4.50.: Remove domain

4.2.2.4. Manage domain's mailboxes

The *Manage Mailboxes* button allows to edit mailboxes. When selected, this option changes the selected tab into *Manage Mailboxes* one. Then a search by domain name is performed (see Figure 4.51). Note that the *Manage Mailboxes* is only visible if a domain is selected.

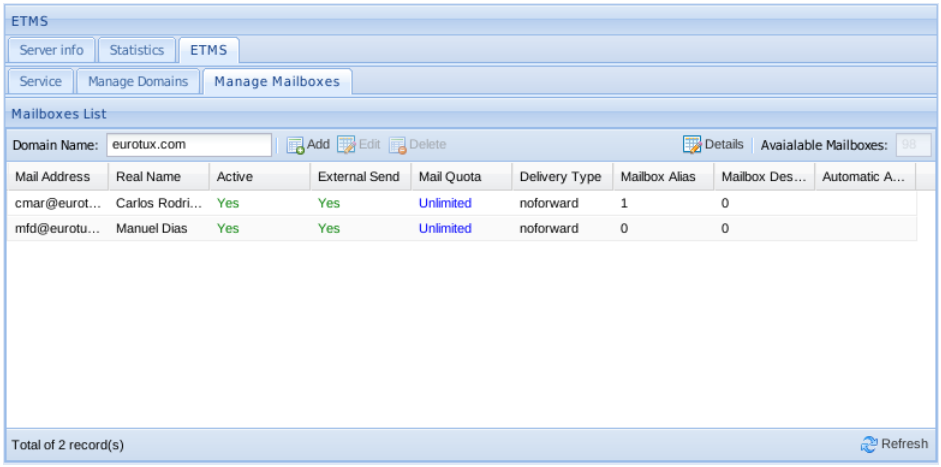


Figure 4.51.: Manage domain mailboxes

4.2.2.5. Details option

The option *Details*, belongs to the toolbar that is under the domains List (at right). Selecting this option is added a column to the grid that lists some information about the occupied space by each domain (see Figure 4.52). Note that, because it could be a computational intensive operation this column is only showed on demand. So, whenever you want to update/view the disk space in use, you should use this option.

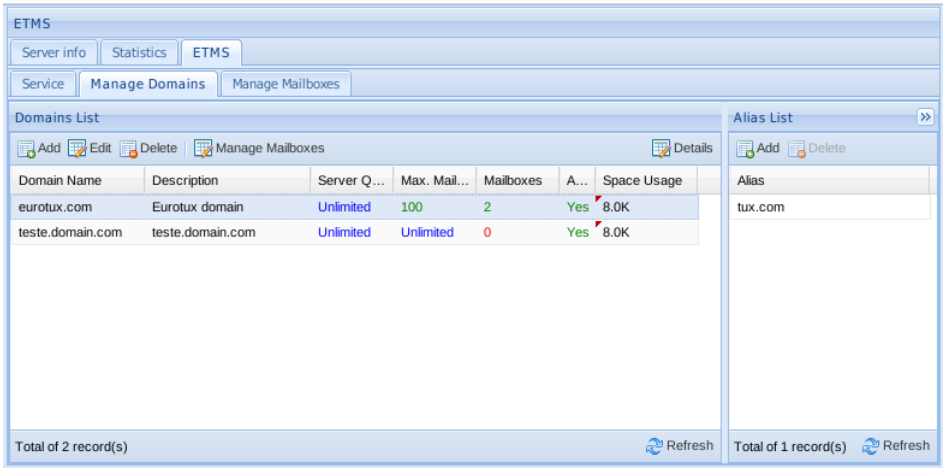


Figure 4.52.: Domains' needed space

4.2.2.6. Adding alias

To add an *alias*, select the desired domain. In the right area where you can see the alias list, press the *Add* button. Note that an entry is added to the top of the list where you can set the new alias name (see Figure 4.53). After editing the row, the new *alias* is sent to the service agent. If the operation was successfully accomplished, a notification is displayed (Figure 4.54], and added an entry to the information panel.

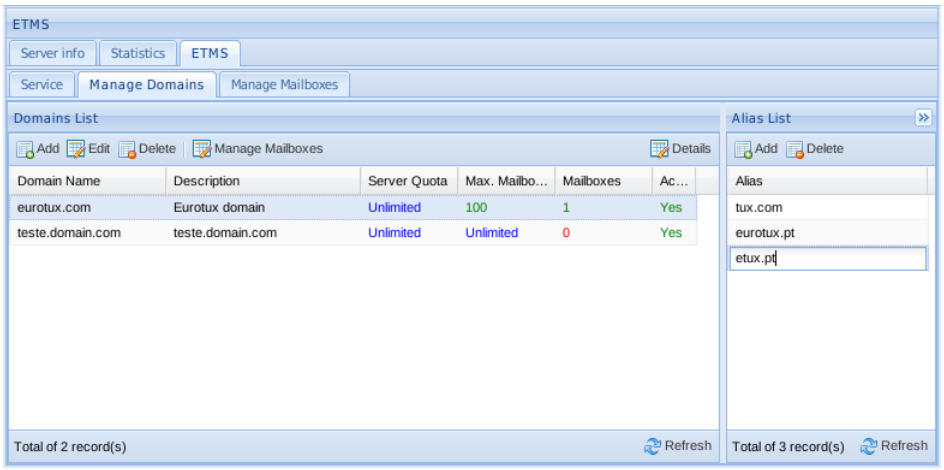


Figure 4.53.: Adding a domain alias

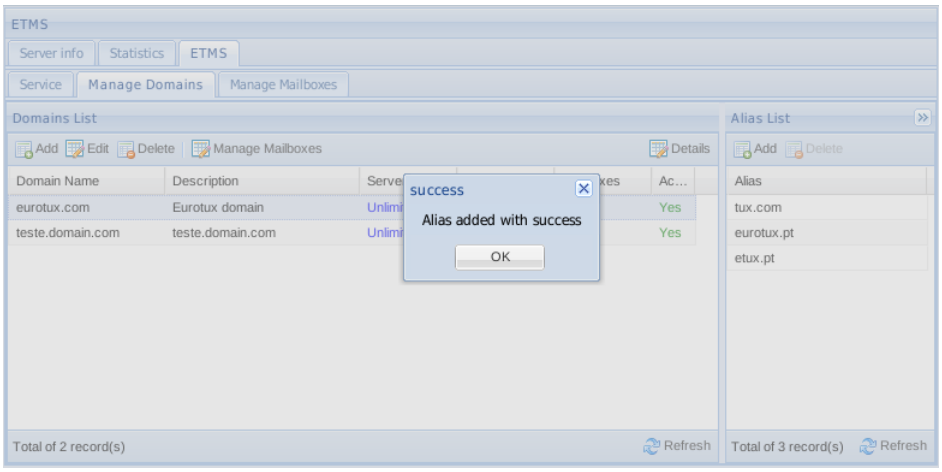


Figure 4.54.: Alias created successfully

4.2.2.7. Removing domain's alias

To remove an alias: select the domain that contains the alias (Figure 4.53); In the alias list, select the alias that you want to remove; Press the *Remove* button; Answer yes to the confirmation message.

Note that, when necessary, the alias list can be updated through the lower toolbar by pressing the refresh button.

4.2.3. Tab 3 - Manage mailboxes

The Manage Mailboxes' tab is an area/grid where each row corresponds to a mailbox (see Figure 4.55). The grid lines are selectable and can perform operations on each selection. To see the mailboxes it's necessary to perform a search of mailboxes, that can be done by following the steps given in Section 4.2.3.1.

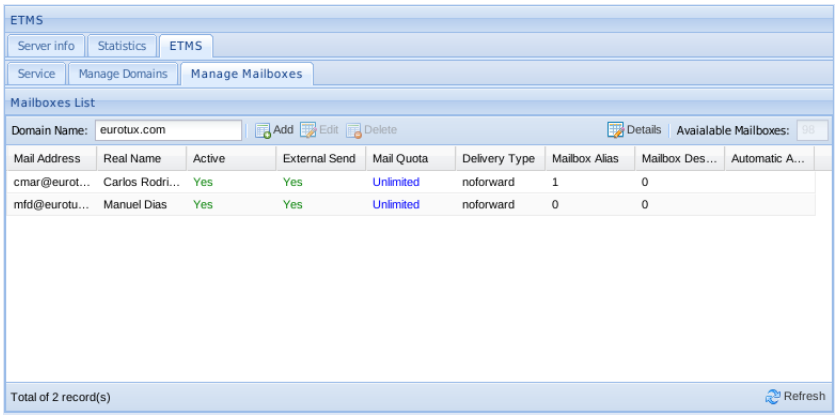


Figure 4.55.: ETMS - Mailbox management panel

4.2.3.1. Searching for mailboxes

You can search mailboxes for a particular domain, simply enter the domain's name in the box that is over the grill (on the toolbar), and press *ENTER*. Note that during the process of communication with the machine that hosts the service, the icon on the bottom right gets animated (close to the *Update* button). If the domain is not found, an error message is displayed. The success of a search, enables the options for managing mailboxes (see Figure 4.55).

4.2.3.2. Adding a mailbox

To create a mailbox we need to perform a a search by a domain (see Section 4.2.3.1), then use the **Add** button (It will open a window with fields to fill, as shown in Figure 4.56). Press the *Save* to make the change effective. Please note that: the first three fields are mandatory; the grid with existing domains gets refreshed after the addition of the new domain.

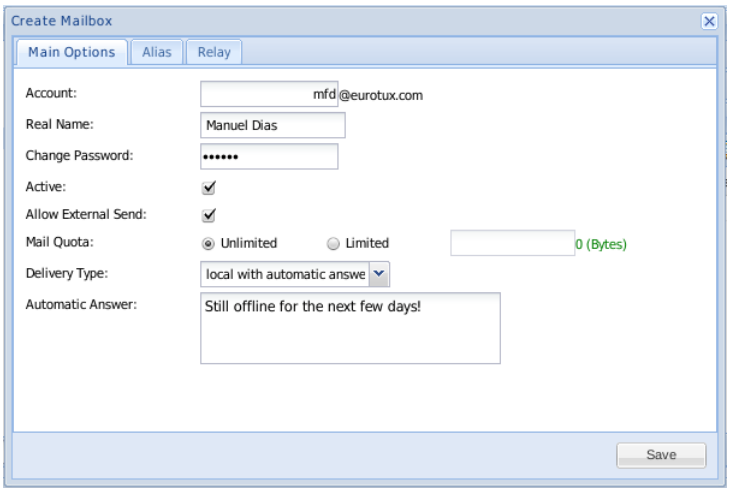


Figure 4.56.: Adding a mailbox

The window for creating a new mailbox is comprised of three tabs: *Main options*, *Alias* (see Subsection 4.2.3.5), *Forwarding* (see Subsection 4.2.3.6).

For a better understanding, we describe briefly the existing fields indicating, where appropriate, examples of use:

- **Account** - Desired account name(Ex: mfd@eurotux.com)
- **Real name** - User name [2] (E.g.: Jorge Leal)
- **Change password** - *Password* to access into the mailbox. Must be at least six chars long. (E.g.: PassWord)
- **Active** - Change the email account's state.
- **Allow external send** - Allows the account to send emails off the server that is, domains that are not defined on the server.
- **Email quota** - Maximum value to be used for mail storage. Note that at the right, the green indicates the maximum value defined for the domain, and the mail quota cannot exceed this value (e.g. 10000 bytes).
- **Delivery type** - There are four modes of delivery: local, forwarded, local and forwarded, forwarded with automatic answer.

[2] I.e. for contacting purposes

- **Automatic answer** - Automatic answer message.

Here is a list with the various delivery types: *Local* - Only made mail delivery in the local account, considering also the any existing alias. *Forwarded* - Only delivers email in the mailboxes defined on tab *Forwarding*. *Local and forwarded* - The incoming emails are delivered to the local mailbox and sent to mailboxes defined in tab *Forwarding*. *Local and forwarded with automatic answer* - Emails are delivered in the local mailbox, and a message is sent back to the origin of the email, with text set in *Automatic answer* field.

4.2.3.3. Edit a mailbox

The window for editing a mailbox is similar to create mailbox window, described on Section 4.2.3.2. The main difference is that you must select the desired mailbox to change, and choose the option *Edit*. The mailbox form is automatically populated with the account settings and the field*Change Password* is disabled by default. To change the password follow the steps described on Section 4.2.3.4.

4.2.3.4. Change password

To change the *password* of a given account is necessary: select in the grid the desired account, then press edit. In the field *Change Password* select the box that follows it and set the new password. Finally press the save button to complete the configuration (see Figure 4.57).

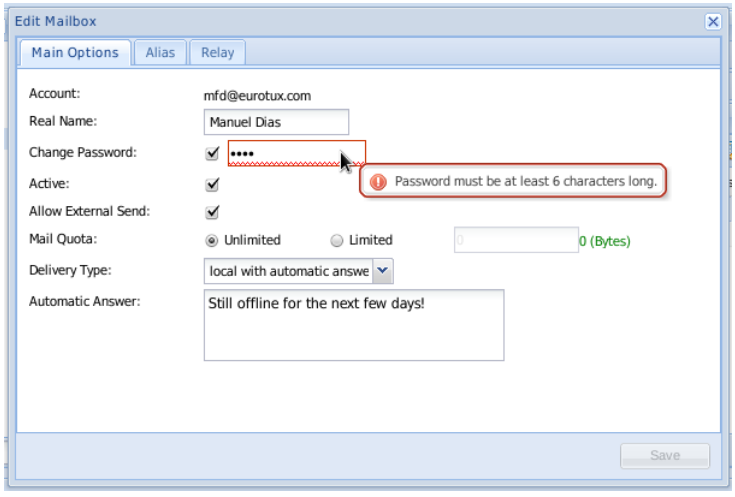


Figure 4.57.: Change mailbox password

4.2.3.5. Define mailbox alias

New mailbox alias can be defined to existing mailboxes. Simply add entries in the grid *Alias* in the process of creating/editing a mailbox (described in Section 4.2.3.2). Note that it **must** be given the full email address (e.g. mfd.alias@eurotux.com), and that the changes take effect after selecting the save option (see figure 4.58).

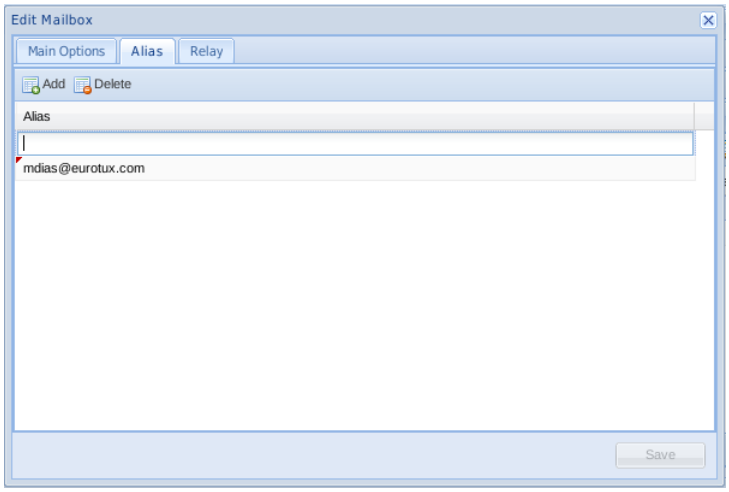


Figure 4.58.: Add mailbox's alias

To remove alias select the alias you want to remove and choose the option *Remove*. Finally press the save button to make the change effective (see Figure 4.59 and 4.60).

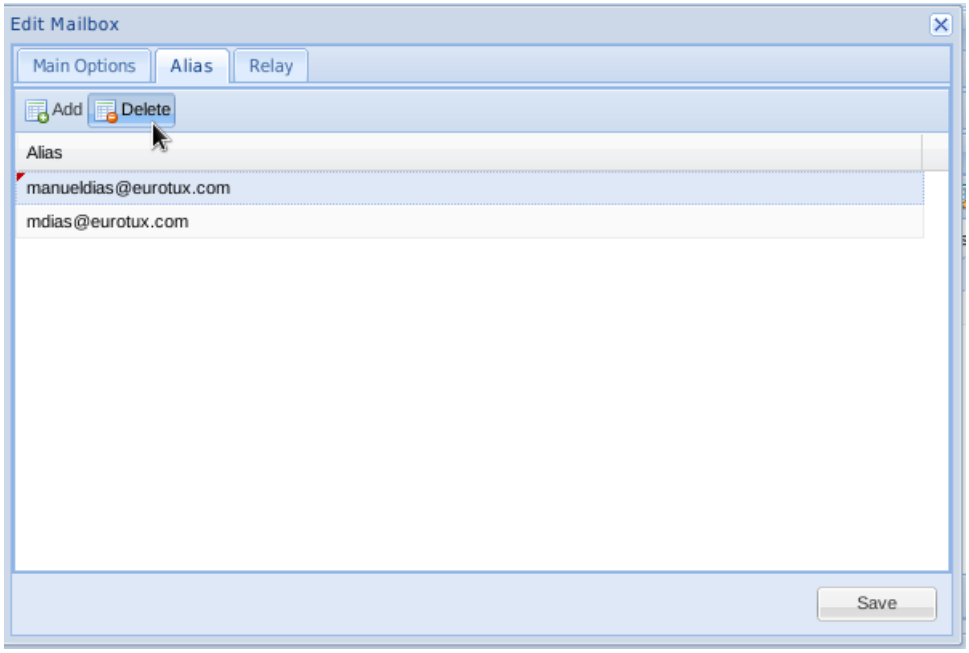


Figure 4.59.: Remove a mailbox alias - step 1

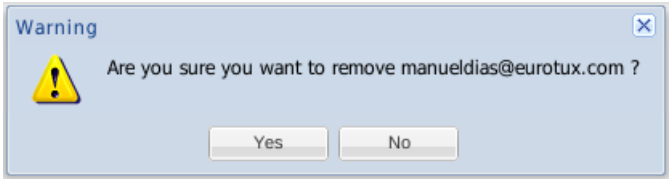


Figure 4.60.: Remove a mailbox alias - step 2

4.2.3.6. Define forwarding email addresses

You can define mailboxes into which emails are sent, simply add entries in the grid *Forwarding* in the process of creating/editing, described in 4.2.3.2 of a mailbox. Note that you **must** give the full email address (e.g. mfd@eurotux.pt). Changes will take effect after press the save button (see Figure 4.58).

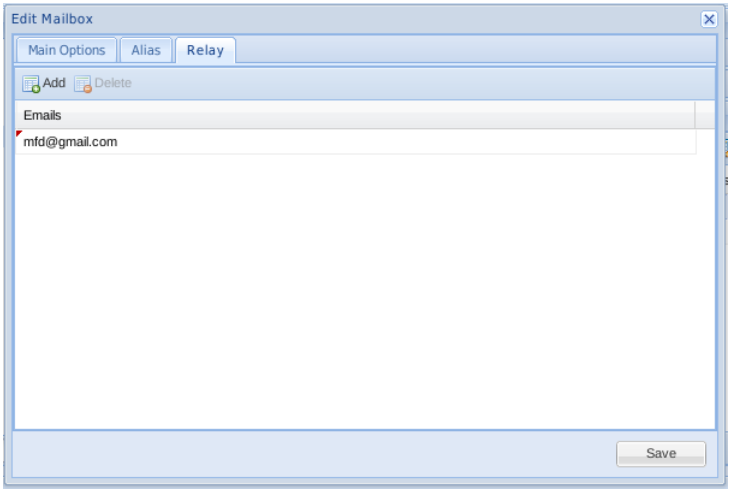


Figure 4.61.: Defining forwarding email addresses

The procedure to remove mailboxes is analogous to the removal of domain's alias, simply select the email in question and choose the option *Remove*. Press the save button to changes take effect (analogous to the procedure described in 4.2.3.5).

4.2.3.7. Available mailboxes

In the case where the domain has a limited number of mailboxes, the number of available mailboxes appears on the right corner of the tab (see Figure 4.62). Every time a mailbox is created, this number is decremented, disabling the option that allows the creation of new mailboxes when the number of mailboxes is equals or exceeds the the domain limit.

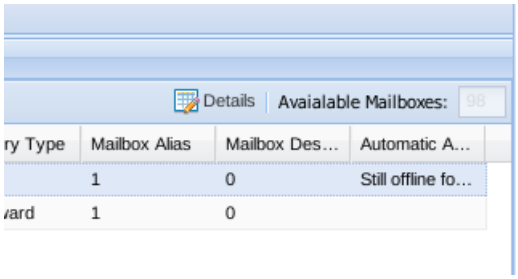


Figure 4.62.: Available mailboxes

4.2.3.8. Details option

The details option, belongs to the toolbar that it's under the mailbox's list (at right). When selected, this option append to the grid two columns to the grid that lists mailboxes with

information on the space occupied by the messages received (see Figure 4.63). Note that, because it can be a computational intensive operation and potentially time-consuming, the columns only appears on request. So, whenever you want to update/view the disk space occupied, it should be used if this option. If new mailboxes are added, the value does not appear, this happens because of the directories that store the emails have not yet been created.

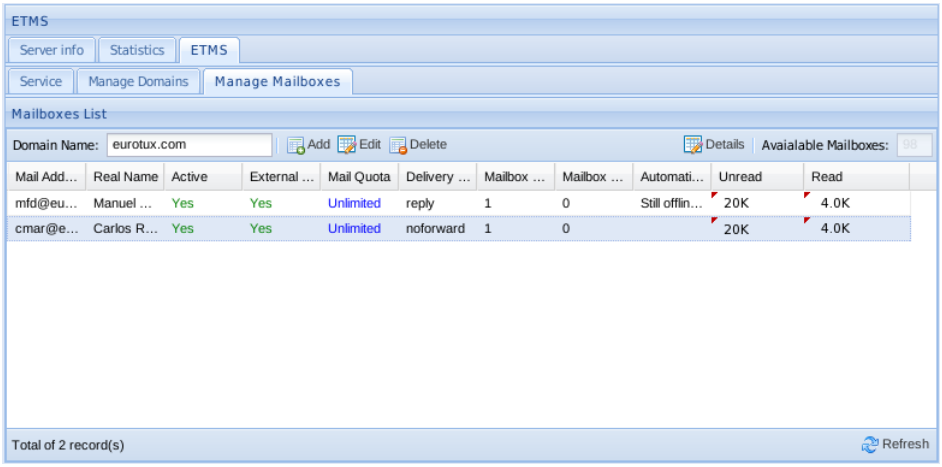


Figure 4.63.: Occupied disk space by mailboxes emails

4.2.3.9. Remove a mailbox

Removing a mailbox, in addition to removing all settings, deletes all the emails in the selected account (and you can not retrieve them through the process of restoration of settings). To remove an account, search for the desired mailbox 4.2.3.1, choose the corresponding line, press the *Remove* button (Figure 4.64).

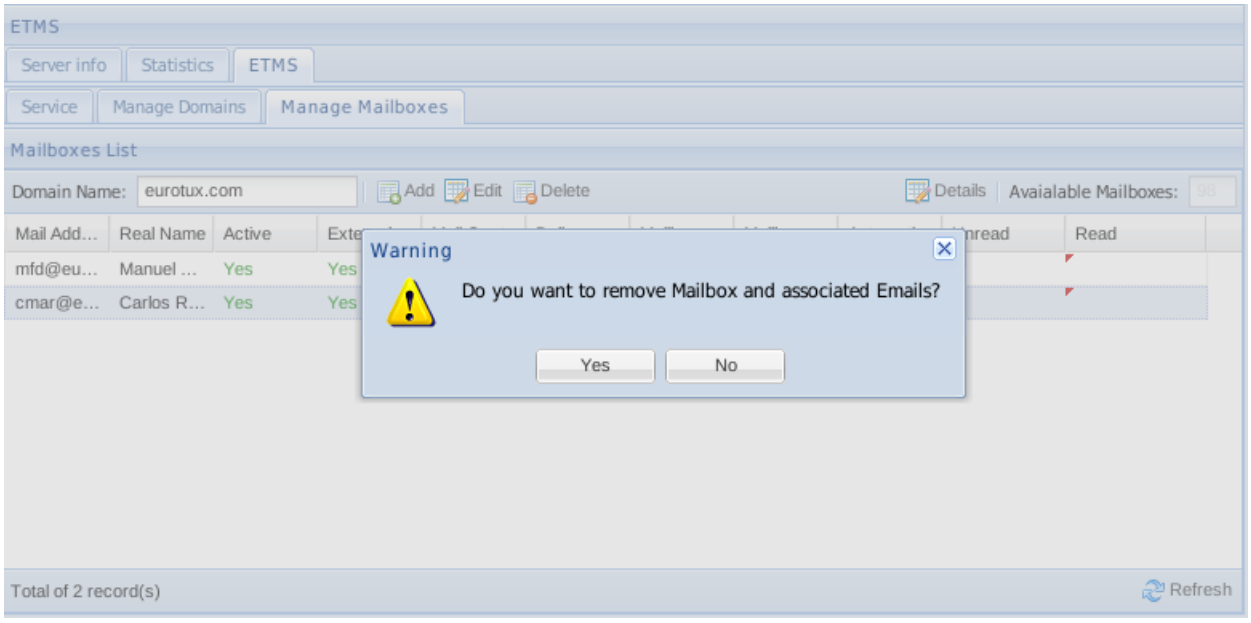


Figure 4.64.: Remove mailbox - confirmation question

4.3. ETVOIP

In the ETVOIP tab of a virtual machine that, has the solution installed, we are enabled to manage a VOIP solution ETVOIP. Currently ETVOIP is the interaction with the PBX component and may interact with other future developments. The available modules for this agent are:

- Extensions
- Trunks
- Outbound routes
- Inbound routes

Note

At the end of all operations/changes you should use the *Apply changes* button available in any of the modules, in order to reflect these changes in the current configuration of the VOIP system.

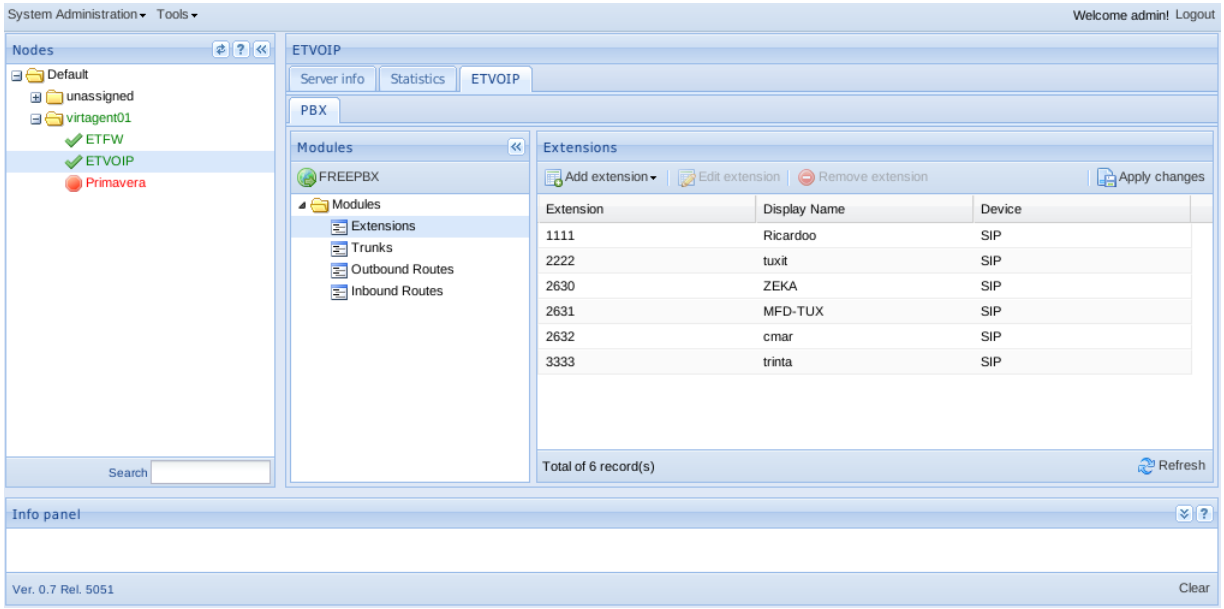


Figure 4.65.: Main ETVOIP panel management

In addition to these modules there is also the option to open a window FREEPBX alone, having access to advanced settings (Menu FREEPBX).

4.3.1. Extensions

In extensions pane it's possible to add, edit an remove extensions.

> **Note**
>
> You can only create/edit SIP extensions [3] and/or IAX[4].

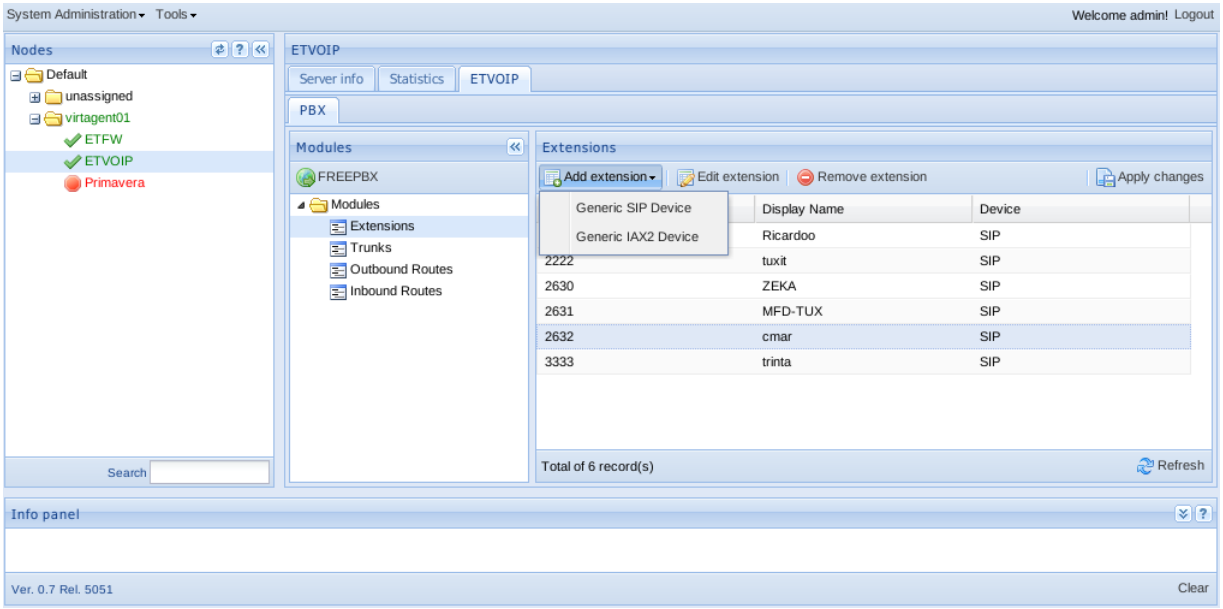


Figure 4.66.: Extension management panel

4.3.1.1. Add extension

When creating an extension is possible to choose between the basic/advanced settings view.

[3] SIP is a standard protocol designed for VoIP devices
[4] IAX it's the protocol "Inter Asterisk" used to interconnect asterisk servers.

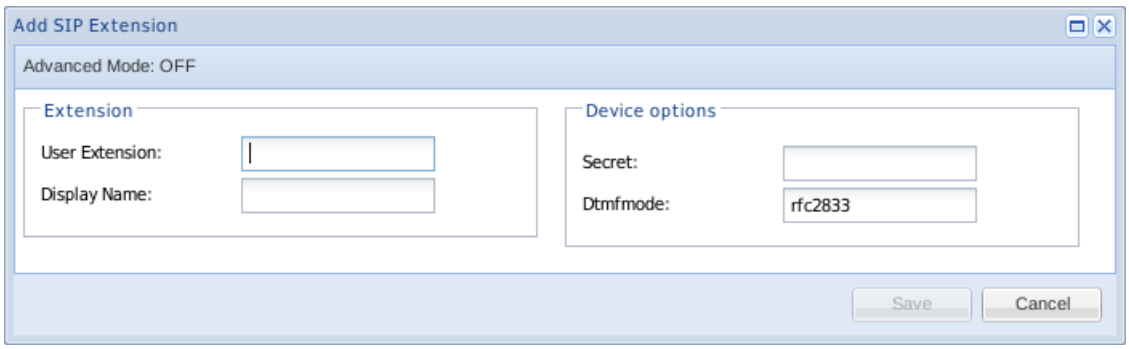


Figure 4.67.: Add extension window (SIP)

Advanced mode: OFF - This mode is available only the basic fields to create an extension.

Extension - Extension parameters.

- User extension - User extension number. Must be unique.
- Display name - User name shown on his calls. Introduce a name, not a number.

Device options - Options for the type of device chosen.

- Secret - Password that devices must use to authenticate on the asterisk server.
- Dtmfmode - Multi Dual-Tone frequency.
  - inband - The sending device generates DTMF tones.
  - outband - The ring tones are removed from the audio data and sent from a different channel.
  - rfc2833 - Specify a format for sending RTP packets, in order to reduce the transmitted data. Used by default.

Advanced mode: ON - In this mode beyond the parameters mentioned above you can configure the following:

Extension - Configuration parameters for extension configuration.

- Alternative CID number - CID number to be used for internal calls, if different from the extension number. Used to masquerade as a different user. A common example is when a support team need to have your internal caller ID to show the overall number of support. Has no effect on incoming calls.
- Alternative SIP - If you want to support direct sip calls to internal users or through anonymous sip calls, can provide a friendly name that can be used instead of the user's extension.

Extension options - Advanced extension options.

- Outbound CID - Replaces the caller ID if passes a trunk. Overrides the outbound CID of the trunk.
- Ring time - Number of seconds ringing before sending the caller to voicemail. If you do not have voicemail set this parameter is ignored.

- Call waiting - Sets the initial state of call waiting for this extension
- Call screening - Requires the caller to say his name, which is then heard by the user, allowing him to accept or reject the call. Memory Screening (*Screen Caller:Memory*) checks only once the source of the caller ID. Screening without memory (*Screen Caller: No Memory*) always requires that the external user say his name. Either way will announce whenever the user from the last entry saved with this caller ID.
- Pinless dialing - Enabled allows you to make outgoing calls from this extension without dialing PIN.
- Emergency CID - This caller ID is used whenever you select an exit route marked out as an emergency. The Emergency CID overrides all other settings the caller ID.

Assigned DID/CID - Definition of the incoming route for this extension.

- DID description - Incoming route description.
- Add inbound DID - Sets the incoming number associated with this extension (Direct Inward Dialing).
- Add inbound CID - Allows you to specify a best route DID + CID. DID should be specified in the above parameter.

Voicemail & Directory - Voicemail parameters.

- Status - Enable/disable this voicemail extension.
- Voicemail Password - Password to access the voicemail system. The password can only contain numbers. A user can change the password after accessing the voicemail system (*98) in his voip phone.
- Email Address - Email address of destination where voicemail notifications are sent.
- Pager Email Address - Email address (pager/mobile) phone for sending voicemail notifications.
- Email Attachment - Allows you to attach voicemails to email.
- Play CID - Read the phone number of origin before playing the incoming message.
- Play Envelope - Read the date/time of the message.
- Delete Voicemail - If enabled the message will be deleted from voicemail (after AIDS mailed). Allows a user to get his voicemail via email, without having to retrieve voicemail via the web interface or phone. CAUTION: It needs to have voicemail attached to the email, otherwise the messages will be lost.
- IMAP Username - IMAP username, if in use.
- IMAP Password - IMAP password.
- VM Options - Extra voicemail options separated by | (such as review = yes | maxmessage = 60).
- VM Context - Context used by the voicemail system. Use 'default' if you do not know the implications.

Dictation services - Parameters for diction service. If enabled, allows the user to dial *34 from his phone and record the conversation. The speech will be record in the defined format and sent to the specified e-mail.

- Dictation Device
- Dictation Format
- Email Address

Language - Parameters of the extension language.

- Language Code - If installed, it will ask if the user want to use the selected language.

Recording options - Extension recording parameters.

- Record Incoming - Record all incoming calls from this extension.
- Record Outgoing - Record all outgoing calls from this extension.

4.3.1.2. Edit an extension

To edit an extension is necessary to select the desired extension and click on button *Edit extension*. Then you will see a window (see Figure 4.67) filled with the extension's settings. The parameters are identical to those provided in section 4.3.1.1.

4.3.1.3. Remove an extension

Select the extension to be removed and then click on *Remove extension* button. A window will appear confirming the removal (Figure 4.68). After removing the extension and if you do not want to perform any other operation, you must apply the changes made in button *Apply changes*.

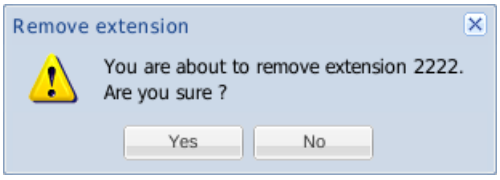


Figure 4.68.: Remove an extension

4.3.2. Trunks

In the section *Trunks* you do add/edit and remove operations.

Note

It's only possible to create/edit SIP/IAX trunks.

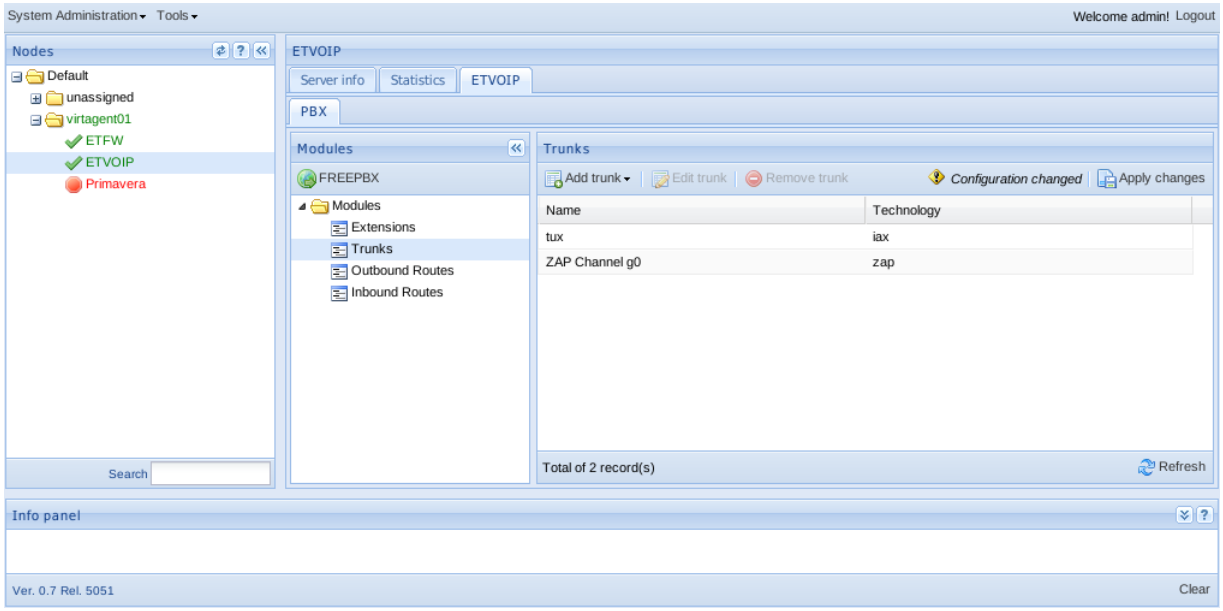


Figure 4.69.: Trunk management panel

4.3.2.1. Add Trunk

When creating a trunk you can choose between the basic or advanced view by pressing the top left button.

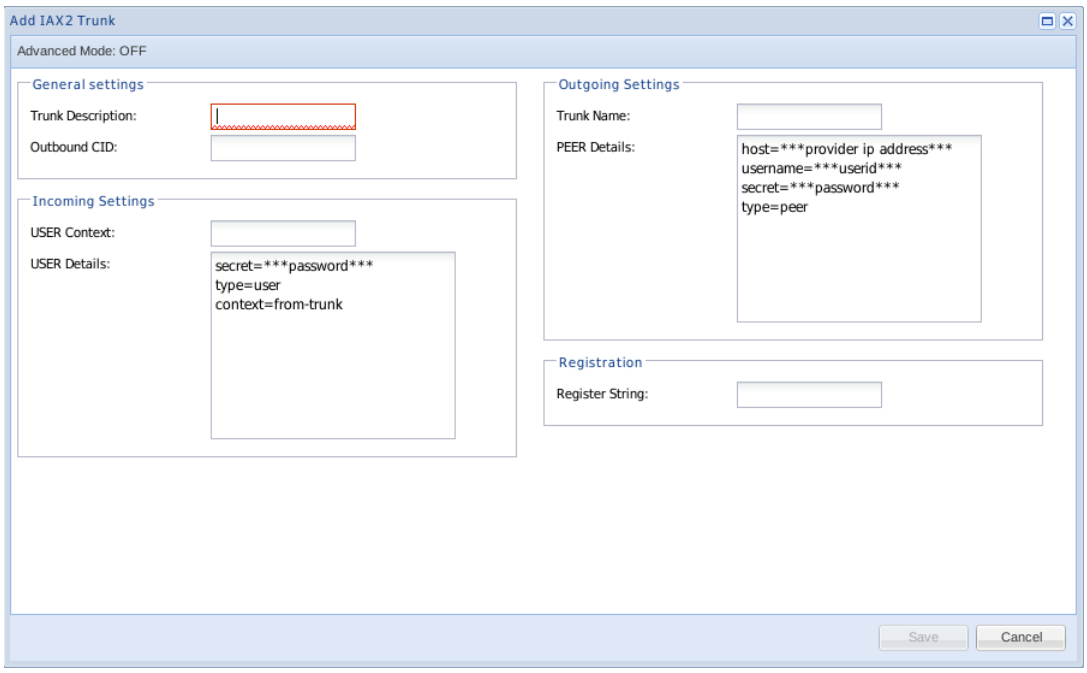


Figure 4.70.: IAX2 trunk creation window

Advanced mode: OFF - This mode only show the basic fields needed in order to create a trunk.

General settings - Trunk parameters.

- Trunk description - Name that better describes the trunk.
- Outbound CID - Call identifier used in calls made through this trunk.

Incoming setting - Input configurations.

- USER Context - This is usually the account name or number that the provider is waiting. This USER Context is used to define the details of the user outlined below.
- USER Details - User connection parameters to the VOIP system.

Outgoing setting - Output configurations.

- Trunk name - Unique name of the trunk.
- PEER details - Connection parameters between the PEER and the VOIP system.

Registration - VOIP registration parameters.

- Register string - Many VoIP providers require the system to REGISTER. Enter the online registration here (example: username:password@switch.voipprovider.com). Many providers require a DID number (ex: username:password@switch.voipprovider.com/ to work the match DID

Advanced mode: ON - This mode shows the available advanced parameters.

General settings - Advanced trunk parameters.

- CID Options - Determines what CIDs are allowed on this trunk. IMPORTANT: CIDs emergency defined in an extension will always be used if the trunk is part of an emergency route regardless of the settings.
  - Allow Any CID - All CIDs including those from external forwarded calls will be transmitted.
  - Block Foreign CIDs - Blocks forwarded CIDs. The defined CIDs will be transmitted.
  - Remove CNAM - This option will remove CNAM from each CID sent by this trunk.
  - Force Trunk CID - Always use the CID set to trunk unless it is part of an emergency route to an emergency CID set to an extension.
- Maximum Channels - Controls the maximum number of output channels (simultaneous calls) that can be made in this trunk. Incoming calls are not considered. Leave blank to not specify a limit.
- Disable Trunk - Disable the use of this trunk in all routes where it is used.
- Monitor Trunk Failures - If enabled, enter the name of an AGI script to be used for logging, email, or perform any action in case of failure, if the failures are not caused by NOANSWER or CANCEL.

Outgoing dial rules - Advanced dial options.

- Dial Rules - A dialing rule controls how calls will be marked in this trunk. It can be used to add or remove prefixes. If the numbers didn't match the standards setted here, they will be dialled with no change. A pattern without + or | (to add or remove a prefix) will not make changes but will create a match. Only the first match found will be performed:
  - X - Pattern matching with digits from 0 to 9.
  - Z - Pattern matching with digits from 1 to 9.
  - N - Pattern matching with digits from 2 to 9.

  1237-9 - Pattern matching with number or letters between brackets (e.g. 1,2,3,7,8,9).
  - . - Wildcard, pattern matching with one or more chars (not allowed before | or +).
  - | - Removes a dial prefix (e.g., 613|NXXXXXX matches when someone dial "6135551234", but only "5551234" passes into the trunk).
  - + - Adds a dial prefix into the number (for example, 1613+NXXXXXX matches when someone dial "5551234", but only "16135551234" is passed into the trunk).

  We can use, simultaneously, + and |, for example: 01+0|1ZXXXXXXXXX does match with "016065551234" and marks it as "0116065551234". Note that the order does not matter, ie, 0|01+1ZXXXXXXXXX does exactly the same thing.
- Outbound Dial Prefix - The outbound prefix is used to put a prefix on all outgoing calls from this trunk. For example, if the trunk has behind another

PBX, we can use 9 to access an outgoing line. Most users should leave the option blank.

4.3.2.2. Edit Trunk

To edit a trunk we need to select the trunk to remove and click on option *Edit trunk*. Then we see a window (see Figure 4.70) filled with the definitions of the trunk. The parameters are identical to those provided in section 4.3.2.1.

4.3.2.3. Remove trunk

To remove a selected trunk click on *Remove trunk* option. A window will appear confirming removal of the trunk (Figure 4.71). After removal of the trunk and if they do not want to perform any other operation, you must apply the changes made - *Apply changes* option.

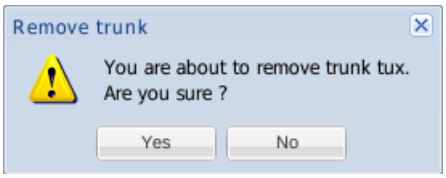


Figure 4.71.: Remove trunk

4.3.3. Outbound routes

The *Outbound routes* configures the behavior of outgoing calls. The dialed number is analyzed, and a pattern matching is made in order to find the outbound route. After that the call is forwarded to the respective trunk.

You can add, edit and remove exit routes.

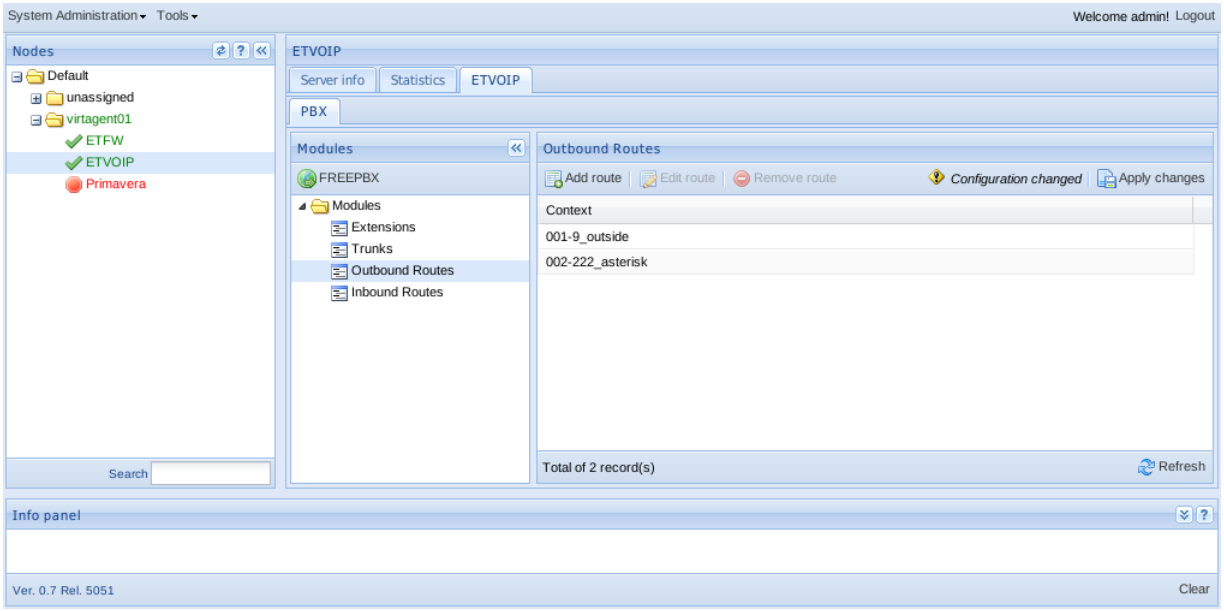


Figure 4.72.: Outbound management panel

4.3.3.1. Add route

When you select the option *Add route* a window will appear (see Figure 4.73) where you can choose between the basic/advanced settings view setting mode. The following parameters are available:

Advanced mode: OFF - In this mode you can define the route basic settings.

General settings - Route parameters.

- Route Name - Route name (e.g., 'local').
- Dial Patterns - Pattern that the dialing number must match to select this route:
  - X - Pattern matching with digits from 0 to 9.
  - Z - Pattern matching with digits from 1 to 9.
  - N - Pattern matching with digits from 2 to 9.

1237-9 - Pattern matching with number or letters between brackets (e.g. 1,2,3,7,8,9).

  - . - Wildcard, pattern matching with one or more chars (not allowed before | or +).
  - | - Removes a dial prefix (e.g., 613|NXXXXXX matches when someone dial "6135551234", but only "5551234" passes into the trunk).
  - / - Adds to the pattern. Does the match with a CID or pattern (e.g., NXXXXXX/104 matches only with the "104" extension).

Trunks - Sequence output trunks. The sequence of trunks control the order of trunks that will be used when the number matches the defined patterns.

Advanced mode: ON - This mode shows some additional configurations that can be made:

General settings - Trunk parameters.

- Route CID - If selected will re-write all specific CIDs except:
  - Emergency CIDs (extension/device) if this route was marked as an emergency route.
  - Trunk CID if the trunk is marked to force the CID.
  - CIDs from forwarded calls (CF, Follow Me, Ring Groups, etc).
  - CIDs from extensions/users if enabled.
- Route Password - The route can request the user to insert a password before allowing the call. Useful in cases of international call barring. A numerical password, or the path to a file with the password to be used. Leave this field blank unless required for a password.
- Emergency Dialing - Selecting this option will force the use of an emergency CID (if configured). This option allows that a given set of routes must been used to dial the emergency number (eg: 112).
- Internal Company Route - By selecting this option the route will be treated as an intra-company connection, preserving the internal CID information and not using the output CID either the extension or trunk.
- Music On Hold? - Defines the type of music when the call is on hold.

Figure 4.73.: Add outbound route window

4.3.3.2. Edit route

To edit an outbound route is necessary to select the desired route and click on *Edit route*. Then you will see a window (see Figure 4.73) filled with the definitions of the route. The parameters are identical to those provided in section 4.3.3.1.

4.3.3.3. Remove route

To remove a selected outbound route click on the *Remove route* button. A window will appear confirming the removal of the route (Figure 4.74). After the removal and if you do not want to

perform any other operation, you must apply the changes made pressing the *Apply changes* button.

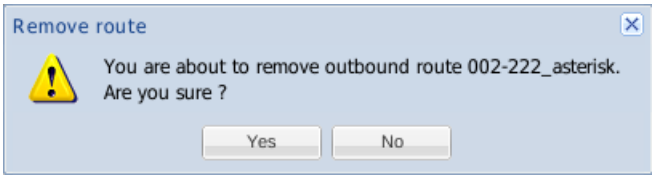


Figure 4.74.: Remove outbound route

4.3.4. Incoming routes

In *Inbound Routes* we can configure the behavior of incoming calls of all trunks. When receiving an incoming call, the VOIP server needs to know where to redirect it. Can be redirected to a Ring Group, an extension or IVR, among other options.

Therefore, it is possible to perform operations to add, edit and remove routes of entry. In the management panel you can view the description and the numbers DID/CID associated with each route.

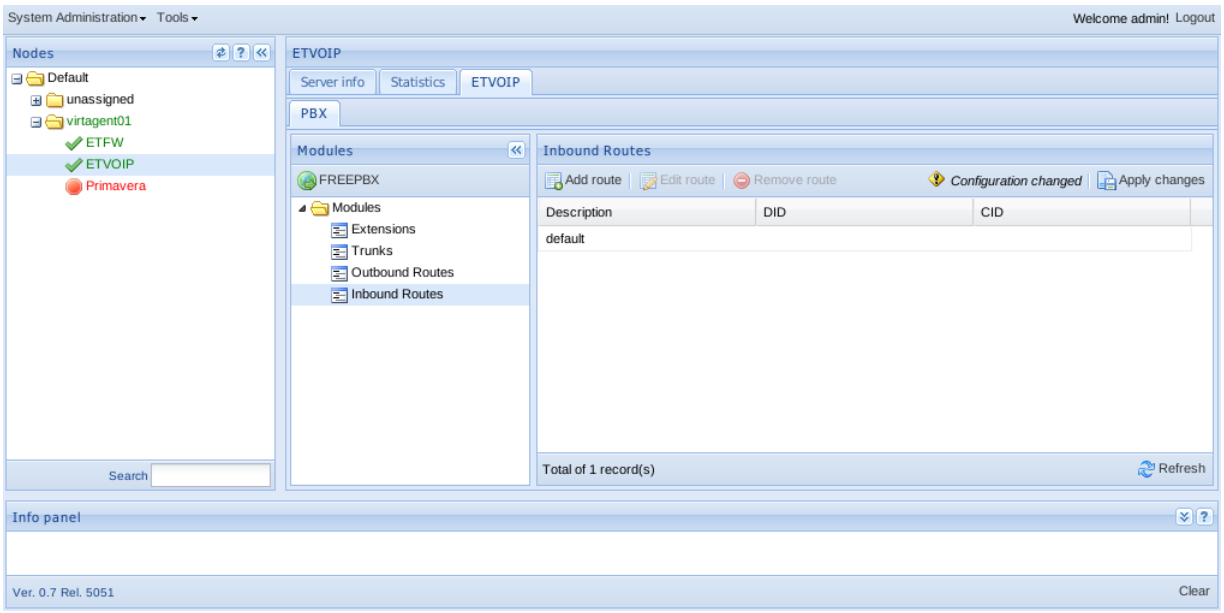


Figure 4.75.: Inbound routes management panel

4.3.4.1. Add route

When you select *Add route*, a window will appear (see Figure 4.76) where you can set the following parameters:

General Settings - General route parameters.

- **Description** - Description of the route.
- **DID Number** - Expected DID number, if the DID trunk accept incoming calls. Leave it blank to match all DID.
- **Caller ID Number** - Sets the CID to match the incoming calls. Leave it blank to match all the ICD.

Set Destination - Destination of calls that match the DID/CID number.

- **Ring Groups** - Extension group.
- **Terminate Call** - The call is automatically ended.
- **Phonebook Directory** - The contact list is shown.
- **IVR**[5] - virtual receptionist.
- **Extensions** - Pre-defined extension.

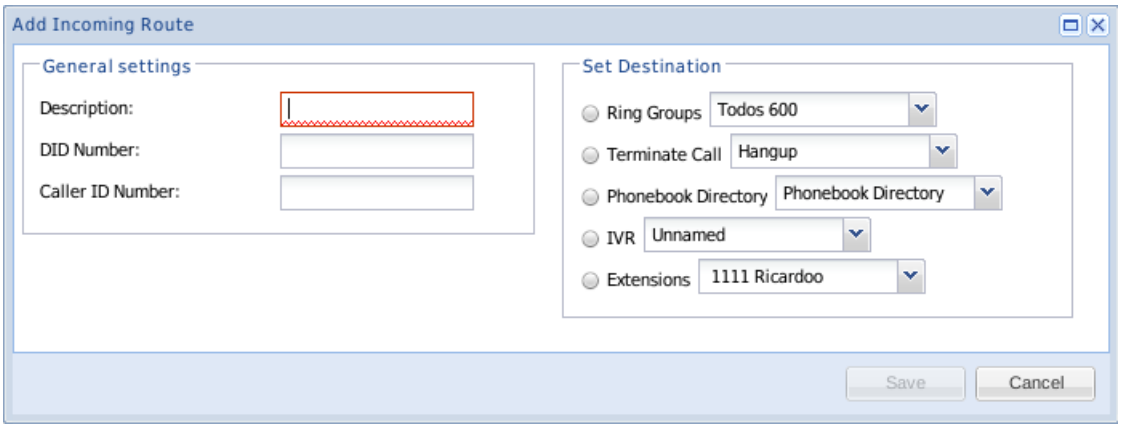


Figure 4.76.: Inbound route creation window

4.3.4.2. Edit route

To edit a route you must select the desired route and click on *Edit route* option. Then, you will see a confirmation window (see Figure 4.76) filled with the definitions of the route. The parameters are identical to those provided in section 4.3.4.1.

[5]Acronym for *Interactive Voice Response*

4.3.4.3. Remover rota

To remove a selected route entry click on *Remove route* option. A window will appear confirming the removal (Figure 4.77). After removal and if you do not want to perform any other operation, you must apply the changes made - *Apply changes* option.

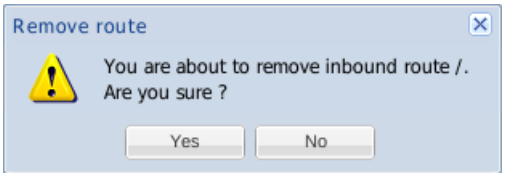


Figure 4.77.: Remove inbound route

4.4. Primavera

The UnitBox allows the configuration via Central Management of the Primavera solution.

4.4.1. Installation

In order to use the Primavera service via Central Management, you must ensure that the virtual machine's agent is installed and running.

The installation process has the following steps:

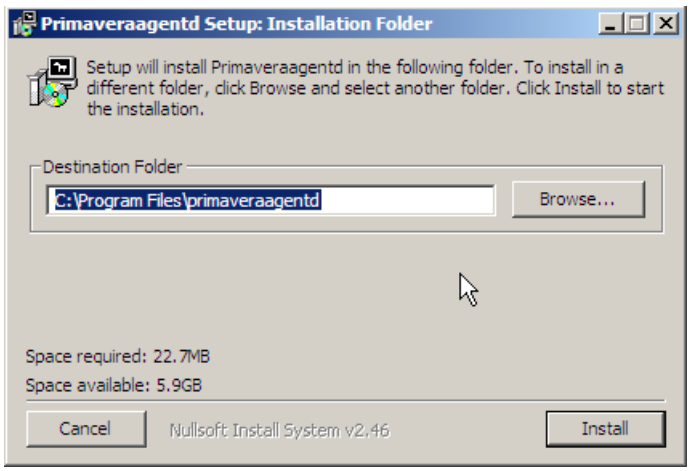


Figure 4.78.: Step 1 - Choosing installation directory

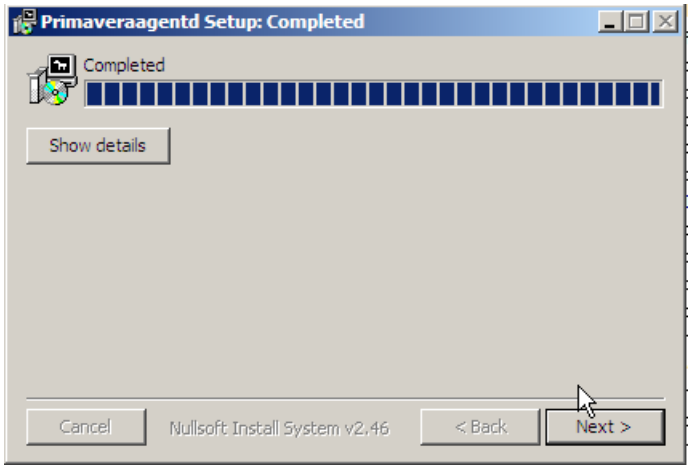


Figure 4.79.: Step 2 - Installation progress

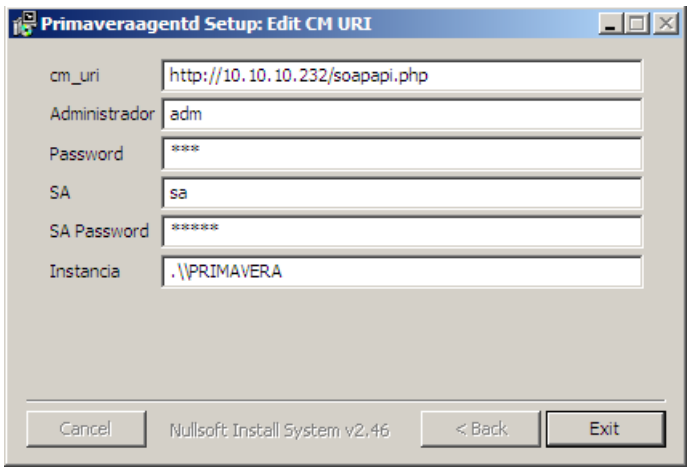


Figure 4.80.: Step 3 - Agent setup

In step 3, you need to set some parameters that will allow access to the Primavera's engine thus enabling its management.

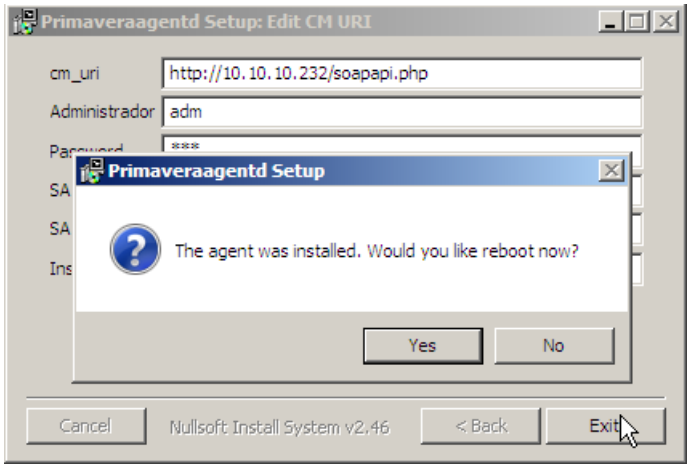


Figure 4.81.: Step 4 - Reboot confirmation

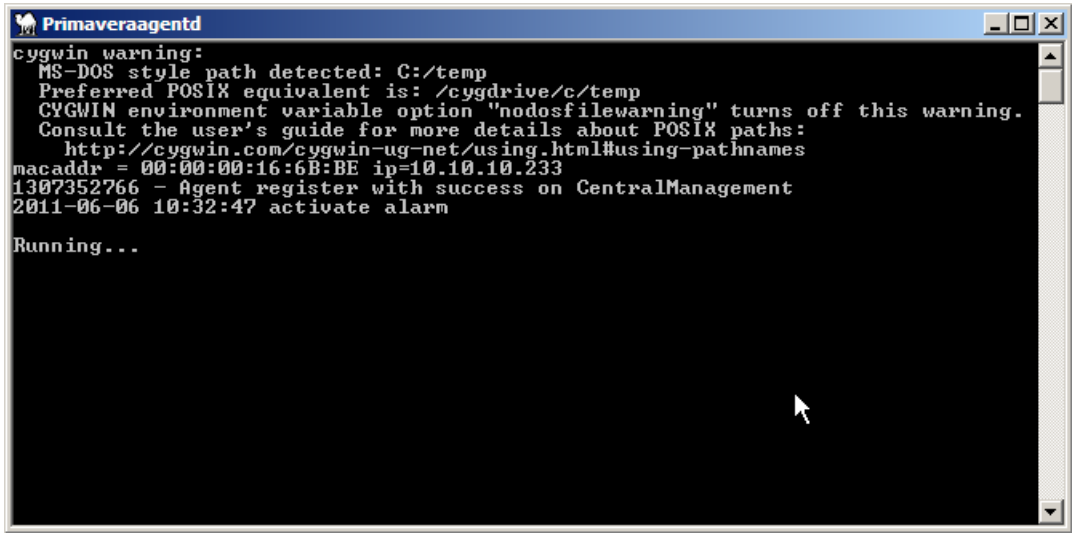


Figure 4.82.: Step 5 - Agent startup

After installation is necessary to reboot the virtual machine to initialize the agent. From this moment you can manage the Primavera service from the Central Management interface.

4.4.2. Interface

The Primavera's management interface allows you to access some essential features for the service's maintenance, including backup management, start and stop operations, manage users and change the IP address of the virtual machine.

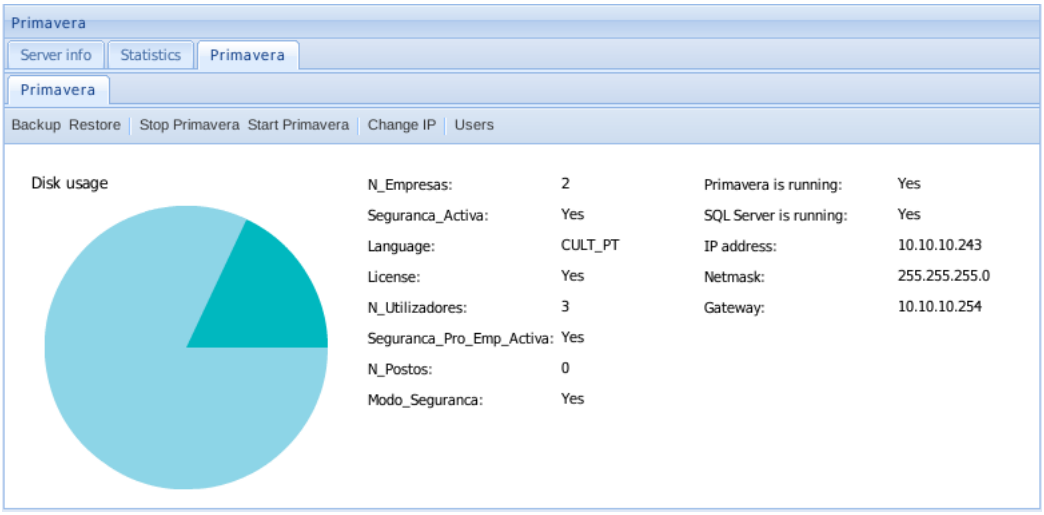


Figure 4.83.: Service information

When you access the Primavera tab, it's possible to see some information about the service's state such as: disk space usage, number of companies, Primavera's license, number of jobs, state of the Primavera's services and SQL server, and at last the network info.

From the menu bar you can access some other features such as: Backup and restore, start and stop Primavera's service, change network configuration and user management.

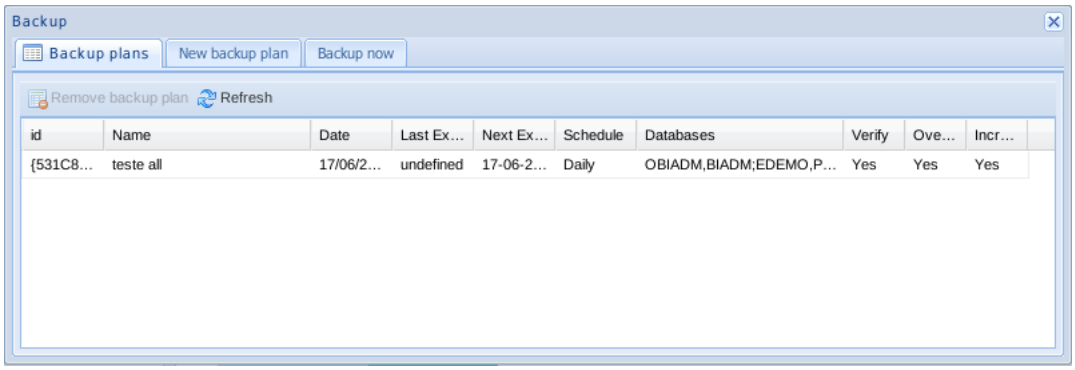


Figure 4.84.: Listing backup plans

In backup menu we can access the backup feature that allows you to manage backup plans. To create a new plan, go to the tab *New backup plan* and define the following parameters: *name* - identification of the plan, *frequency* - frequency the backup plan (daily, weekly, monthly), *database* - database that will be carried out *up*, options *check*, *Overwrite* and *Incremental* , set up the plan to check after making *up*, on-call in case of the file already exists and *Incremental backup*.

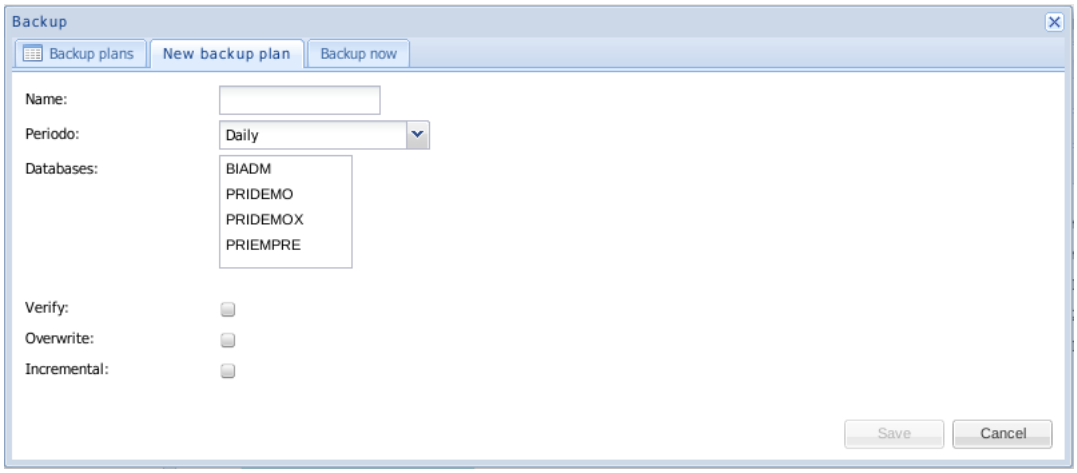


Figure 4.85.: Defining a backup plan

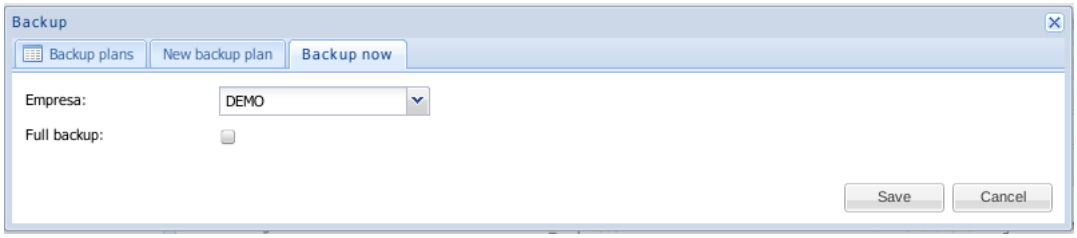


Figure 4.86.: Performing a backup

There is also the option to make an immediate backup, on tab *Backup now*. Here we choose the company to make backup or we can perform an entire Primavera's platform backup, choosing the option *Full backup*.

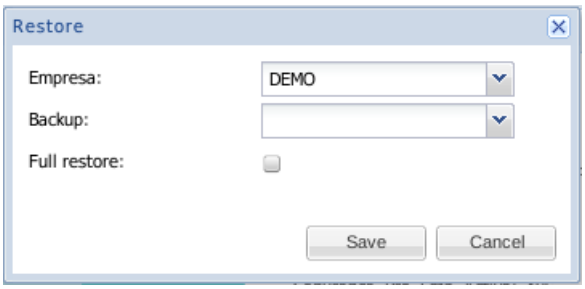


Figure 4.87.: Restoring process

In the *Restore* tab we can perform a backup restore. We can restore a partial backup (for a company), or perform a full Primavera's system restore by selecting the option *Full restore*.

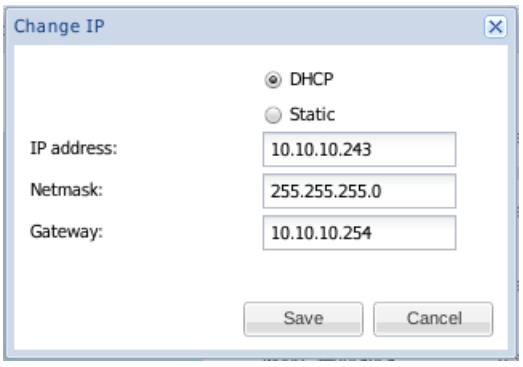


Figure 4.88.: Changing the IP address

To make change in network configuration we can access the tab *Change IP*, where we can modify the IP address settings, netmask and the gateway of Primavera's virtual machine. We can also define the configuration over DHCP.

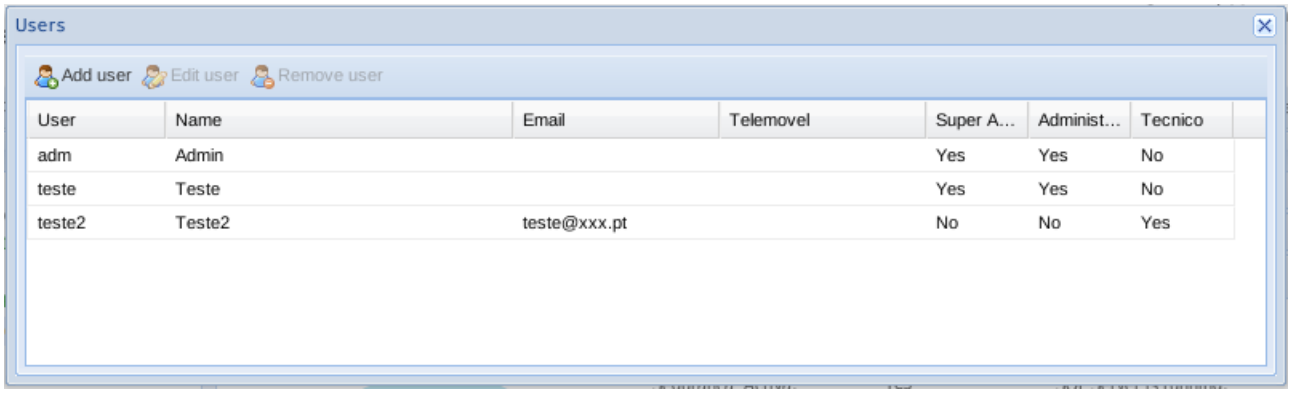


Figure 4.89.: List of Primavera's users

We can manage Primavera's users on tab *Users*. Here you can list any existing users, configure a new user with several parameters (User Name, Email, and Password options Super Administrator, Administrator and / or technical). It's even possible to edit and user's data or remove users.

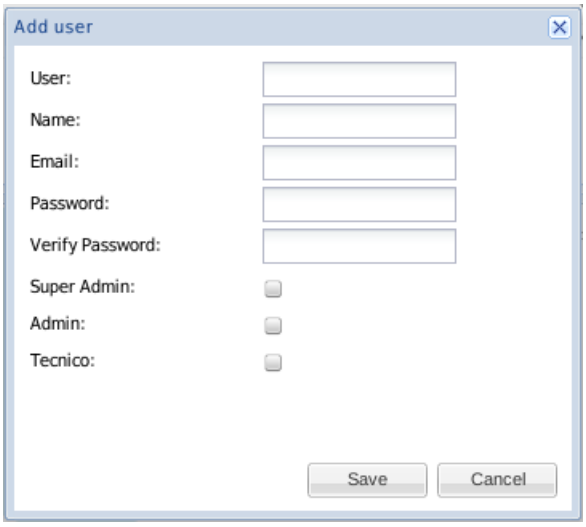


Figure 4.90.: Adding a Primavera user

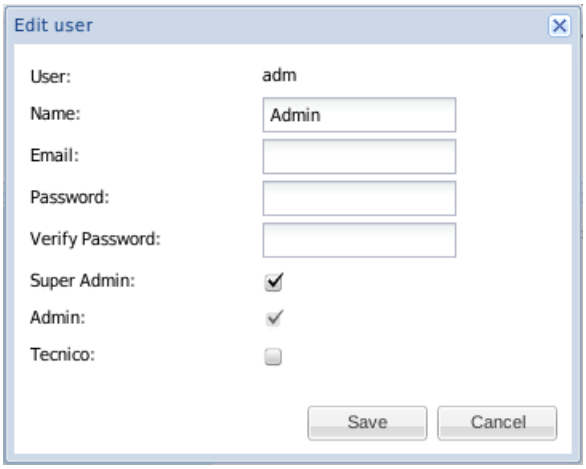


Figure 4.91.: Editing a Primavera user

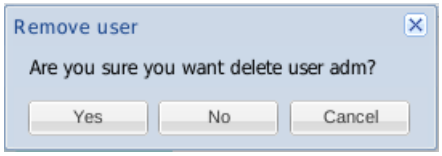


Figure 4.92.: Removing a Primavera user

5. Appendix

5.1. Changelog

5.1.1. Release 1.0

- feature - Multiple datacenter support (see #209)
- bug fix - OVF network import
- bug fix - several fixes on browser interface (ExtJS)
- bug fix - devices consistency check
- bug fix - "resize" and "remove" logical volume messages
- bug fix - consistency check when cloning a logical volume
- bug fix - user permissions in server context
- feature - better debug messages (on nodes)
- bug fix - Servers' state check: unassigned VMs filtered
- feature - crons reviewed for failure notification
- bug fix - refresh button of the tree that lists all Nodes/Servers
- bug fix - VMs icons after a state change
- bug fix - logrotate configuration
- feature - NRPE Plugin for Nagios integration (see #272)
- improvement - Symfony ORM updated to version 1.6
- bug fix - refresh of the "not mounted" logical volumes
- bug fix - total number of fork in the VA
- improvement - interface translations
- feature - diagnostic mechanism (see #189)
- feature - validator for the location field available during the installation of paravirtualized VMs (see #193)
- bug fix - virtagent memory leak (see #179)
- feature - servers with autostart

5.1.2. Release 1.0.1

- bug fix - PAE and APIC defined by default (see #400)
- bug fix - update mounted logical volume (see #392)
- bug fix - LVM compatibility commands (see #311)
- bug fix - read-only devices (see #311)
- bug fix - mounted flag and swap devices (see #311)
- bug fix - ccis/c* devices (see #311)
- bug fix - parser for pvinfo devices (/dev/mapper/...) (see #311)
- bug fix - consistency check on devices (see #320)
- bug fix - default gateway setting when a new network is added (see #372)
- bug fix - SOAP commands to unauthorized nodes (see #333)
- bug fix - Boot from logical volume option (new server wizard) (see #373)
- bug fix - choose from available mac-addresses on server network interfaces configuration (see #371)
- bug fix - network boot scripts (see #332)
- bug fix - mouse bus for paravirtualized servers (see #341)
- bug fix - VLAN Name-Type configuration VLAN_NAME_TYPE_PLUS_VID_NO_PAD (see #328)
- bug fix - cluster node election reviewed. (errors in logical volumes creation on cluster context) (see #323)
- bug fix - concurrent logical volume creation (see #301)
- bug fix - IE9 compatibility errors (JS) (see #307)
- bug fix - field validation on server wizard (KVM) (see #309)
- bug fix - netmask calculation for network interfaces (see #315)
- bug fix - user permissions in cluster level (see #397)
- bug fix - Virtagent IP address (see #409)
- bug fix - logical volume clone in two steps (1 - lv create; 2 - lv clone) (see #391 and #393)
- bug fix - disallowance of 'dev' named networks (see #379)
- bug fix - server info panel changed to include the disk type and network interface model (see #405)
- bug fix - improved error messages (see #382)
- bug fix - bus=xen when device=cdrom and hypervisor for xen (see #381)
- bug fix - Anaconda's selinux doesn't work. SeLinux? disabled in postscript. (see #410)

5.1.3. Release 1.1

- bug fix - problem with VMs without state identified as notrunning when really are running (see #386)
- bug fix - problem in changing the agent's hostname (see #434)
- bug fix - problem generating CA certificate's cn (see #432)
- bug fix - fix spec to correct certificates (see #436 and #472)
- bug fix - increase dom0_mem to 1500MB (see #411)
- bug fix - fix xend-config to allow migration of vms (see #437)
- bug fix - problem adding physical volumes to volume group (see #440)
- bug fix - xen driver support to nics in Xen+HVM (see #446)
- bug fix - automatic start of vms that are marked as 'running' (see #460)
- bug fix - conflict in disk type of shared harddisks between vms (see #462)
- bug fix - error removing harddisk from vm (see #463)
- bug fix - error opening Mac Pool in vm creation wizard (see #465)
- bug fix - nos paths do physical disks (see #471)
- bug fix - physical disk initialization (see #473)
- bug fix - context menus in storage (pvs,vgs,lvs) (see #474)
- bug fix - move vm while node is down (see #412)
- enhancement - update kvm to 0.15.0 (see #316)
- enhancement - update xen to 4.1.2 (see #420)
- enhancement - update virtio-win to 0.1-22 (see #424)
- enhancement - add feature for specify CPU sockets, cores and threads (see #425)
- enhancement - Add windows xen drivers (see #427)
- enhancement - upgrade libvirt to 0.9.4
- enhancement - Allow the creation of vms without harddisk (see #292)
- enhancement - pass-through of USB and PCI devices (see #300)
- enhancement - Allow the creation of vms without nics (see #308 and #345)
- enhancement - Windows and Linux guest agent (see #353)
- enhancement - VM Priority Restart (see #355)
- enhancement - Rebrand Nuxis (see #422)
- enhancement - VM High-available (see #431)
- enhancement - Node High availability (see #430)

- enhancement - harddisk search (see #258)
- enhancement - Node shutdown (see #205)
- enhancement - Allow vm edit while it is running (see #461)
- enhancement - Change the type of vm (see #399)
- enhancement - Define APIC, ACPI and PAE of the VM (see #374)
- enhancement - Menu start/stop vm in treeview (see #347)
- enhancement - Order logical volumes (see #343)
- enhancement - Improve storage management (see #325, #329, #331 and #335)
- enhancement - Search new physical disks (see #247)
- enhancement - Allow resizing vm disks while running (see #228)
- enhancement - Support the installation of RedHat? 6, Ubuntu e Debian in XEN-PV (see #288 and #321)

5.1.4. Release 1.2.0

- bug fix - Flags pae, acpi, apic (see #520)
- bug fix - edit live server change os to windows (see #510)
- bug fix - boot by cdrom on VMs with HVM (see #518)
- bug fix - Problem installing Centos 6 guest VM on Xen+HVM (see #446)
- bug fix - USB pass-through problems (see #413)
- bug fix - Migrate in mode live (see #531)
- enhancement - Update virtio drivers to 0.1-30 (see #503)
- enhancement - rename default datacenter (see #368)
- enhancement - start server with console (see #287)
- enhancement - create/convert disks with format (raw, qcow2, qcow, cow, vmdk) (see #479)
- enhancement - datacenter permissions on datacenter level (see #398)
- enhancement - ovf import: allow mac-address configuration (see #370)
- enhancement - Snapshots and backups using snapshots (see #127)
- enhancement - Node High-available without Spare Node (see #514)
- enhancement - VM Admission Gate (see #513)

5.1.5. Release 1.2.1

- bug fix - edit server (see #557)
- bug fix - boot from disk on XEN PV (see #560)
- bug fix - user permissions (see #546 see #547)
- bug fix - edit datacenter (see #558)
- bug fix - save connectivity preferences (see #564, see #581 and #584)
- bug fix - edit server live mode (see #570 and #569)
- bug fix - edit server and change cdrom on XEN+HVM (see #574)
- bug fix - issues with USB passthrough (see #568)
- bug fix - issues server HA (see #563)
- bug fix - ETVA::NetworkTools::fix_hostname_resolution (see #516)
- bug fix - start VM (see #554)
- bug fix - disks interface of edit server (see #501)
- bug fix - remove datacenter (see #572)
- bug fix - remove server and disk (see #571)
- bug fix - problem with create datacenter (see #565)
- bug fix - problems when don't have snapshots support (see #550)
- bug fix - issues with update and install scripts (see #542 and #527)
- bug fix - requires qemu-img > 0.14 (see #548)
- bug fix - edit server to change VM type (see #543)
- bug fix - missing icons on server menu (see #578)
- bug fix - on call for scan of Fiber-channel disks (see #593)
- bug fix - problem with LV names (see #595)
- bug fix - VNC console with HTTPS/SSL connection (see #597)
- bug fix - xend configuration to accept live migrate connections (see #599)
- bug fix - remove/resize lv when agent restarts (see #604)
- bug fix - agent lock after restarts (see #607)
- bug fix - on detect LV format function caused by names conflict (see #608)
- bug fix - mount etva_iso call after CM URL changed (see #611)
- bug fix - problems with VNC console authentication (see #612)
- bug fix - agent doesn't restart properly (see #614)

5.1.6. Release 1.2.2

- bug fix - Fetch install logs script with diagnostics (see #639)
- bug fix - Add new checks to lcdagent (see #645)
- bug fix - scan new physical volumes (see #629)
- bug fix - virtagent-libs requires perl(Sys::Virt) (see #648)
- bug fix - datacenter permissions (see #644)
- bug fix - call diagnostic (see #640 and #641)
- bug fix - VNC errors after some time (see #634)
- bug fix - VNC Authentication Required errors for different Timezone (see #626)
- bug fix - rename VM for KVM (see #625)
- bug fix - send stats after VM migrate (see #576)
- bug fix - VM maintenance that migrate all servers (see #628)
- bug fix - Agent doesn't restart properly (see #614)
- bug fix - lvclone makes agent to restart (see #655)
- bug fix - problems with system-config-network-cmd (see #656 and #657)
- bug fix - conflict with USB vendorid on USB pass-through (see #664)
- bug fix - kvm 1.2.0 updated with patches for smart cards by USB pass-through support (see #660)
- bug fix - VM drag/drop for move/migrate operations (see #631)
- bug fix - logs _ERR_LIST_SNAPSHOTS_ (see #666)
- bug fix - manuals and documentation (see #667)
- bug fix - VM with qcow2 disks on XEN (see #669)
- bug fix - error on hvmloader for KVM when try to start VM (see #674)
- bug fix - parsing output of new versions of multipath and scsi_id commands (see #658)
- bug fix - segfault after live migrate on XEN (see #606)
- bug fix - problems with VM live migrate for version 0.10.2 of libvirt on KVM (see #675)
- bug fix - log service-run (see #636)
- bug fix - NTP synchronization (see #601)