

UNIFY Open Scape Fault Management

Basic Administration

Basic Administration

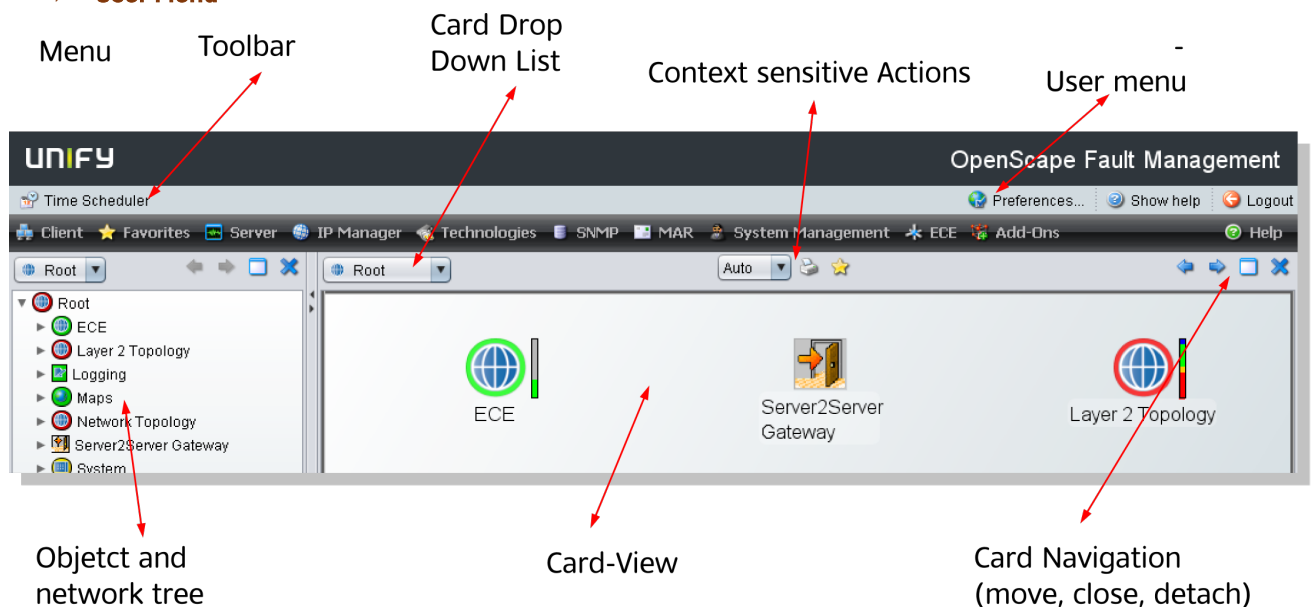
Administration with the CLIENT

The two "magic" of the CLIENT

- ▶ "Everything is an object"
- ▶ "The context menu is a friend."

Elements of the user interface

- ▶ Menu bar
- ▶ Object tree (LINKS): Context menu with the right mouse button
- ▶ Card View (RIGHT): Table, Texts, Graphical Submap
- ▶ Card Navigation
- ▶ Card View actions (context sensitive)
- ▶ Toolbar
- ▶ User Menu



"Everything is an object"

The CLIENT user interface is based on working with objects. The client provides all functions as objects. This means that the administrator works most of the time with these objects. An object exists for all monitored systems, networks, connections, configurations, folders/containers and hosts, which provides information and actions according to the type.

Objects represent hosts and networks and are used to display status, actions and information. Deleting these objects has no effect on the target systems.

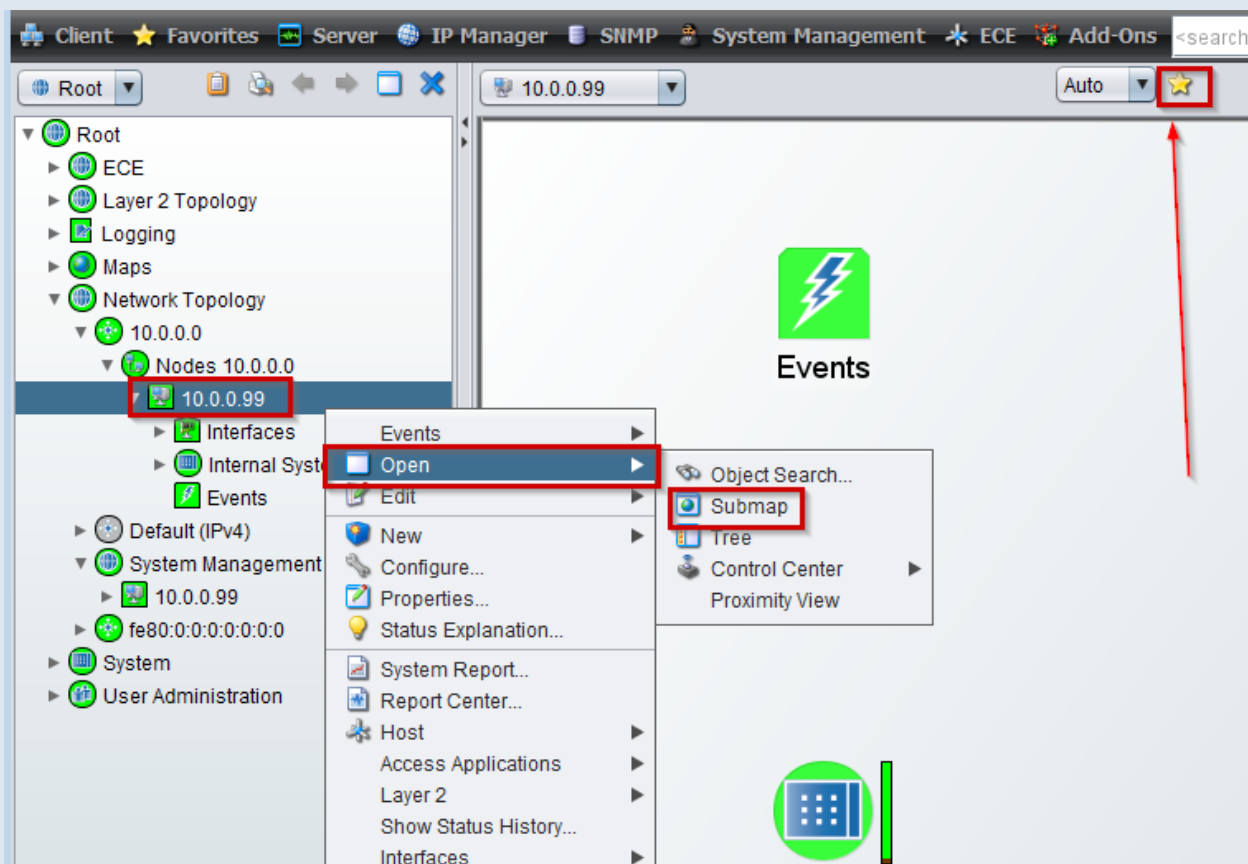
Navigate in the object tree:

- ▶ **Container**, can contain other containers or objects
- ▶ **Object**, can contain sub objects, also called child objects.

First steps in CLIENT

TASK 1 > Open submap of OSFM server object + save as favorites

- Object tree: expand "Root" → expand "Network Topology" -> expand any network object
- expand "Nodes x.x.x.x"
- Open context menu with right mouse button on OSFM server Host object
- Choose "Open" -> "Submap" in context menu
- Use the star symbol above the submap card ro create a favorite.



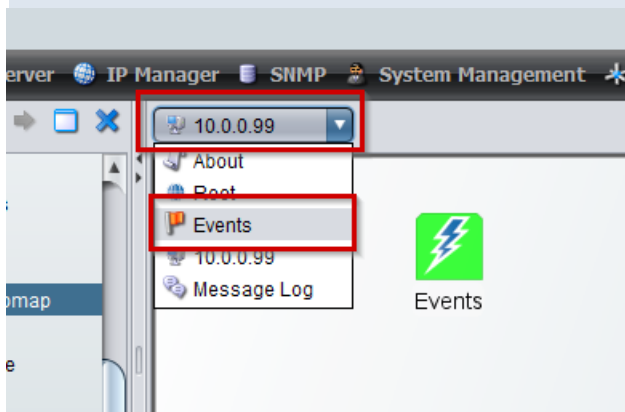
TASK 2 > Creating an Entry in the Toolbar

- Object tree: Open "Root" → "User Administration"
- Open "root" -> "Favourites"
- Open "Toolbar"
- Drap 'n Drop a favorite from "Favorites" to "Toolbar"

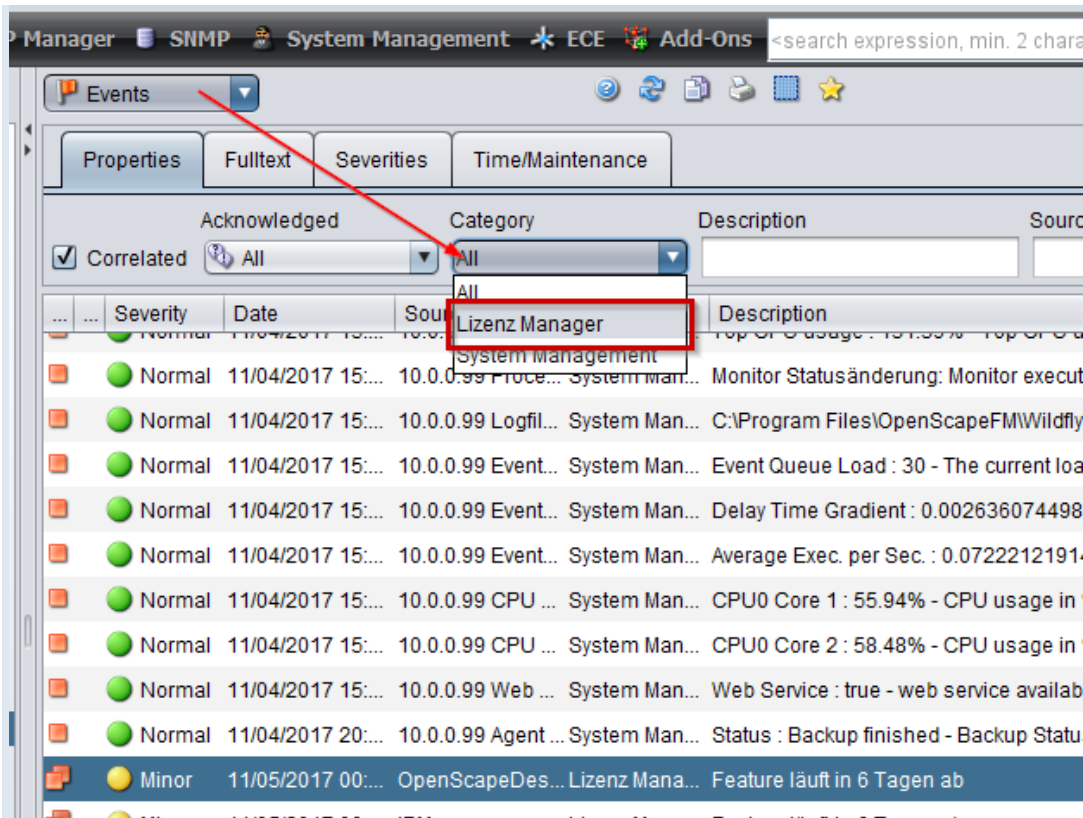


TASK 3 > View events with license information

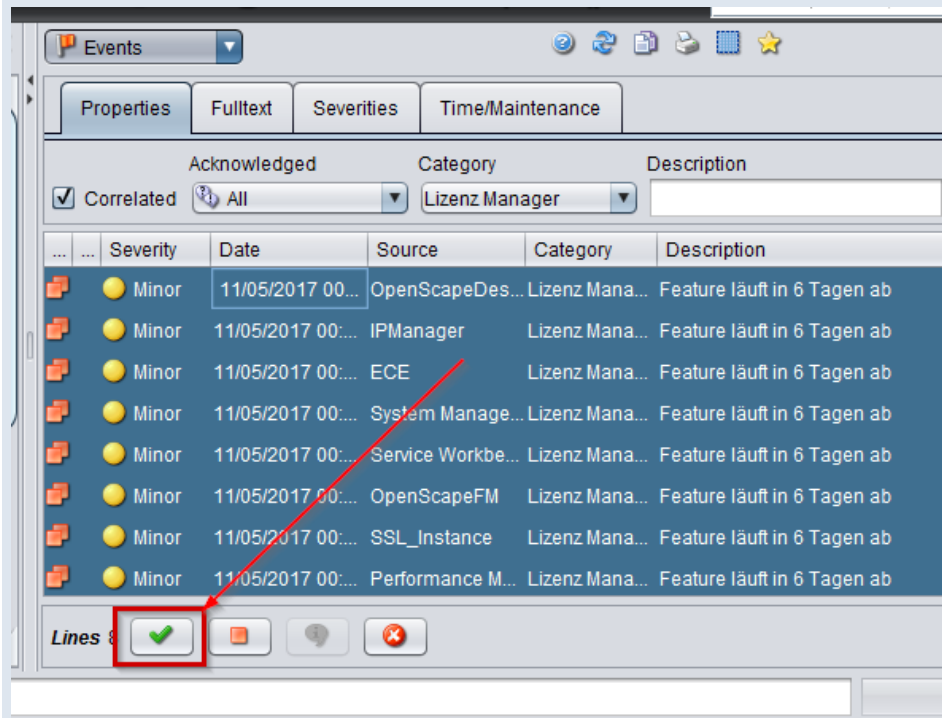
→ On Card Dropdown List pick "Events"



→ Select "License Manager" Category

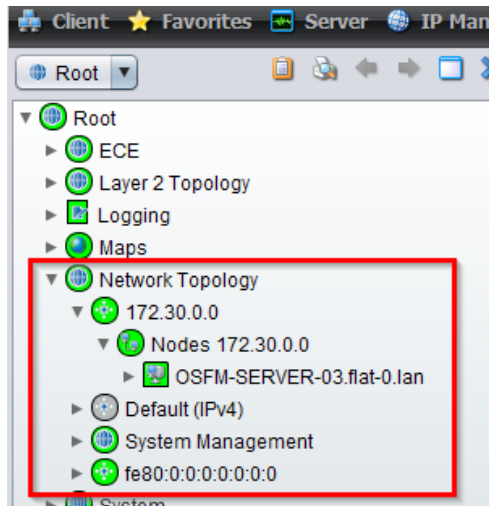


→ Select and confirm all events using the key combination CTRL-A.



CLIENT: Manage hosts and networks

A basic object is the "host" object. For OSFM every device accessible in the network like e.g. Servers, printers, switches, routers, telephone system components, etc. a "host", which can be assigned to an IP network. Accordingly, the CLIENT represents these hosts, organized in networks:



A first step in administration is to add or discover hosts and networks.

- ▶ **Hosts can be added individually, as a list, or through automatic/manual discovery of IP subnets.**
- ▶ **Networks can be created as empty networks or detected automatically/manually**

Discovery of the networks

In general, there are two ways to scan IP networks. As a third possibility it should be mentioned that a network can be announced and the IP nodes for this network can be entered manually. A network scan can started

- ▶ **Manually over an IP range**
- ▶ **Automatically by polling the ARP cache via SNMP**

During scanning the network, OSFM

- ▶ **check for new IP addresses**
- ▶ **checks whether an IP node object has been created.**
- ▶ **Controls where IP nodes are added in the topology**

It is based on the Discovery Model, which is hierarchically structured. A discovery filter checks a specific discovery condition, e.g: the existence of a specific attribute "there is an SNMP agent". The Root Discovery Filter is the "IP Node Discovery". It performs a check to see if an IP address is responding.

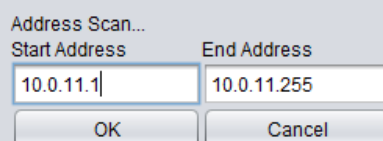
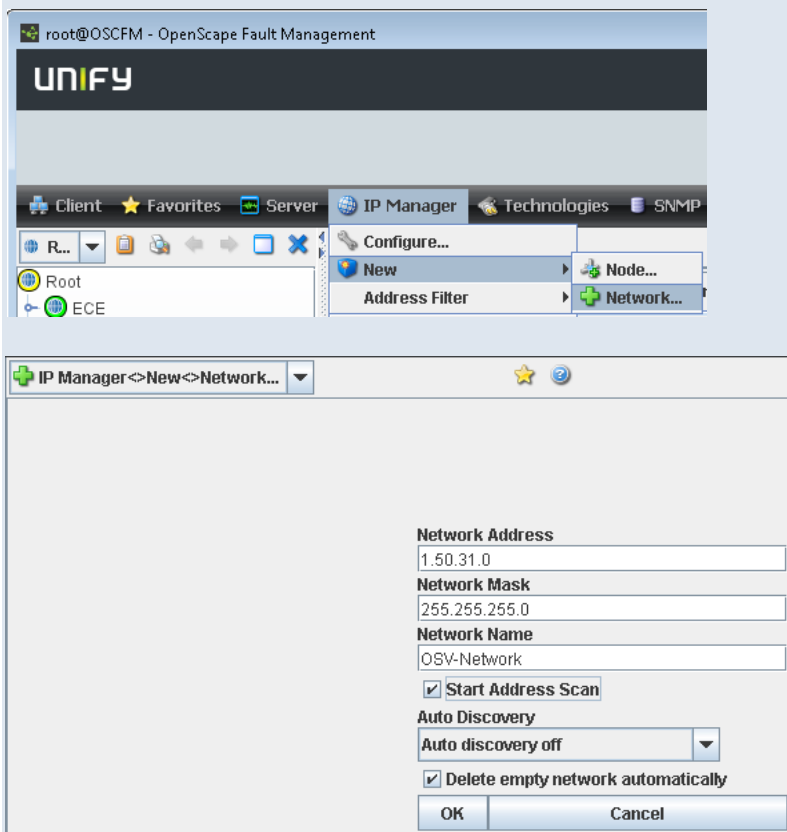
Manual Scan over an IP range

The manual scanning of a network is a user controlled function that runs in the foreground. All IP addresses of the range are checked and the results of the discovery are displayed to the user.

Scanning a network can be performed immediately after the network is announced. A network that is to be managed by OSFM must first be made known to OSFM.

TASK 4 > Add Network and Perform Manual Discovery

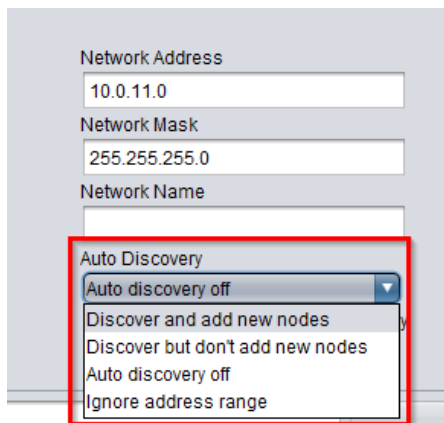
- Menu -> IP Manager -> New -> Network...
- Enter the network address, the network mask and the network name (optional)
- Enable the "Start address scan" option
- Finish adding with OK
- Confirm the address scan with OK.



The scan process is displayed in a separate Info Browser in the foreground. Depending on the activated plugins, the information for the detected IP nodes is read via SNMP accordingly. If an IP node exists, the OSFM also gets a response and an IP node object can be created.

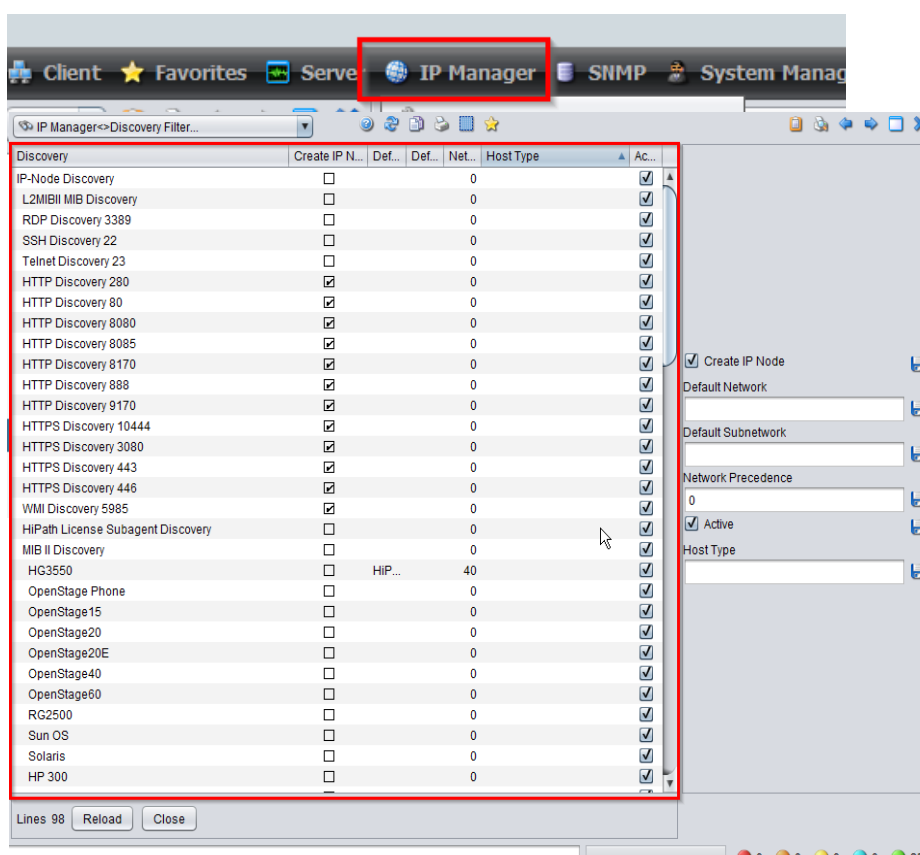
Automatic scanning of a network

This mechanism is a background function that accesses the MIB II -> ipNet2MediaTable during configuration polling. An SNMP agent must be present on the IP node to be able to read the cache. The IP addresses that are read out are checked and displayed in the network accordingly. This function is not deterministic and the ARP cache is usually very dynamic. The automatic discovery of a network is activated via the option Detect and create network elements.



Configuration of the Discovery

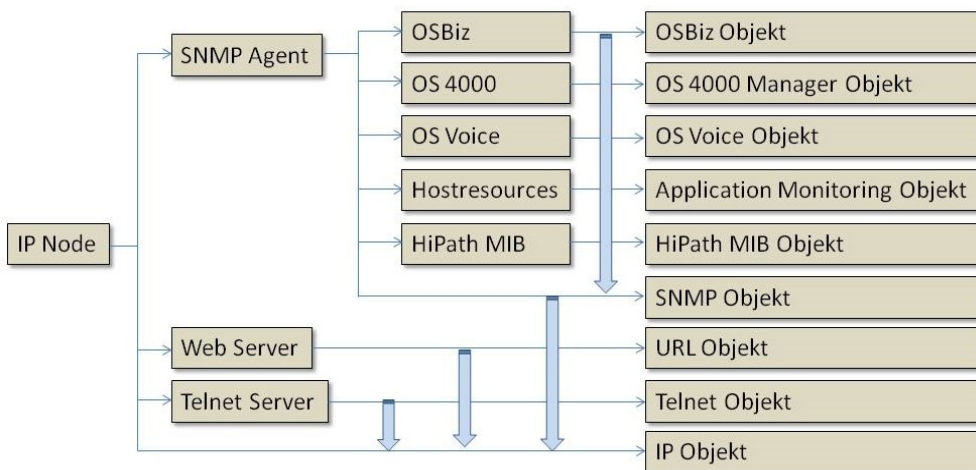
Discovery of networks and technologies is performed using discovery filters. These can be activated and configured by the administrator:



Select the Discovery Filter to perform the configuration. The individual parameters must be saved separately using the Save icon. If the network discovery detects that an IP node is a HiPath / OpenScape 4000 Manager, this IP node is additionally created in the HiPath 4000 Manager network.

- ▶ **Create IP Node**
If enabled, an IP node will be created if the filter matches.
- ▶ **Default Network**
The IP node is displayed in the specified topology network.
- ▶ **Default Subnetwork**
The IP node is displayed in the specified subnet of the topology.
- ▶ **Network Precedence**
Which discovery rules are paramount when placing the IP node in the network topology.

Schema representation of the use of discovery filters



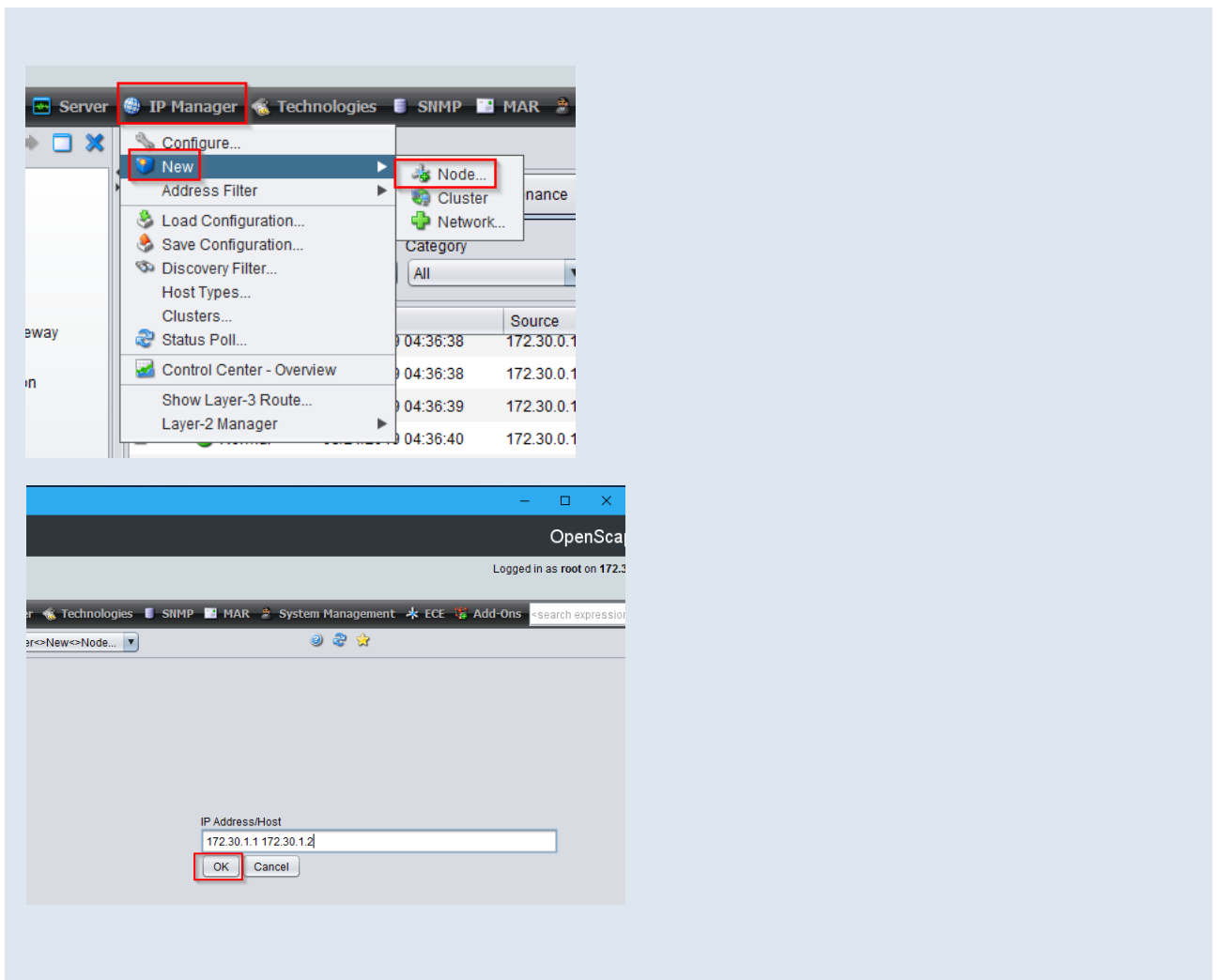
Adding hosts

Host objects are central objects in OSFM for displaying information and performing configurations. A host object is always used for each monitored OpenScape technology. If no automatic scan of the new IP network has been performed, a host can be manually added to OSFM.

After the automatic or manual addition of a host, monitoring for availability (status polling) and technology detection (discovery poll) is started immediately!

TASK 5 > Add a new host to OSFM

- Menu -> IP Manager -> New -> Node
- Enter one or more IP addresses or hostnames (separated by spaces).
- Finish adding with OK



Hosts and networks: Configuring IP Parameters

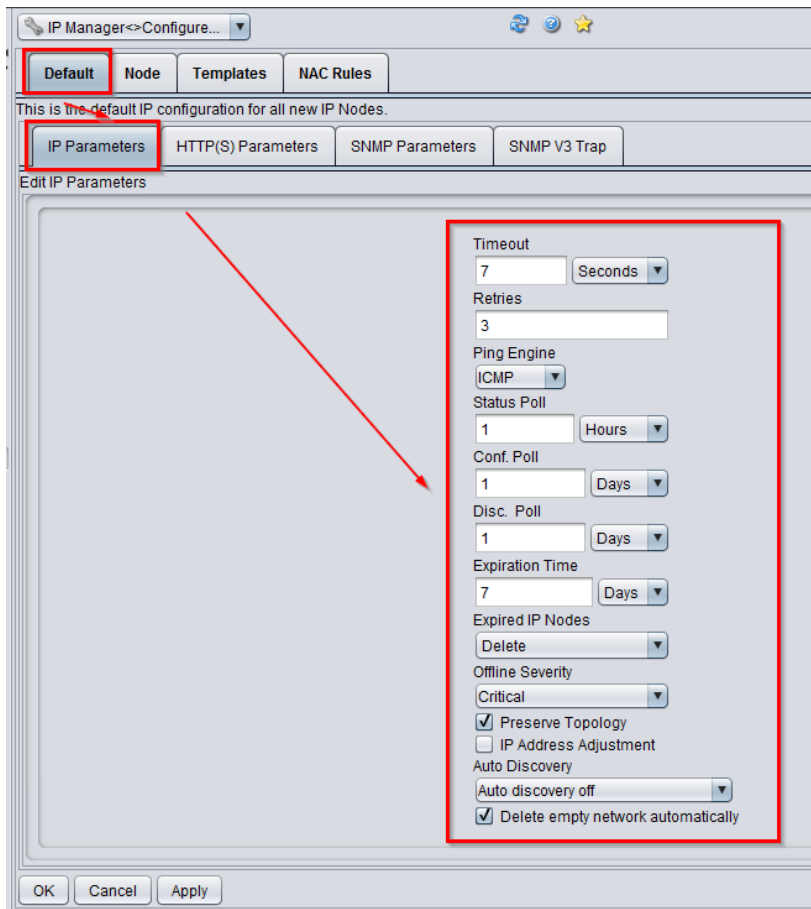
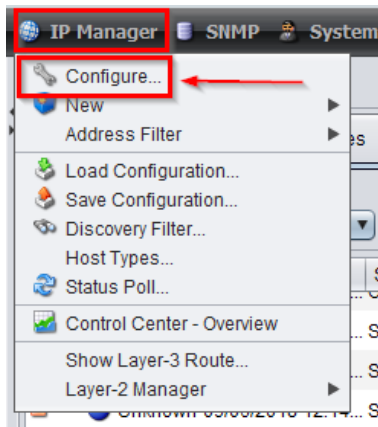
For each new host in OSFM, an availability check and a discovery by technology takes place automatically. This procedure can be configured. For hosts that will be added in the future, default values can be set.

The configuration is carried out via the menu "IP Manager -> Configuration...". It is divided into three sections,

- ▶ **Configuration of IP parameters,**
- ▶ **Configuration of the SNMP parameter and**
- ▶ **Configuration of HTTP Parameters.**

Changes to these parameters are now only effective for newly discovered IP nodes!

If IP nodes have already been detected, the existing configuration of the host must be changed.



► Timeout

the time taken to respond to the verification. The check is only successful if a response is received from the IP node within this time.

► Retries

How often should the check be repeated if it was unsuccessful

► Ping Engine

Here you define how the availability check of the IP nodes is to be performed (TCP/IP, SNMP, ICMP). If AUTO has been set, ICMP is preferred.

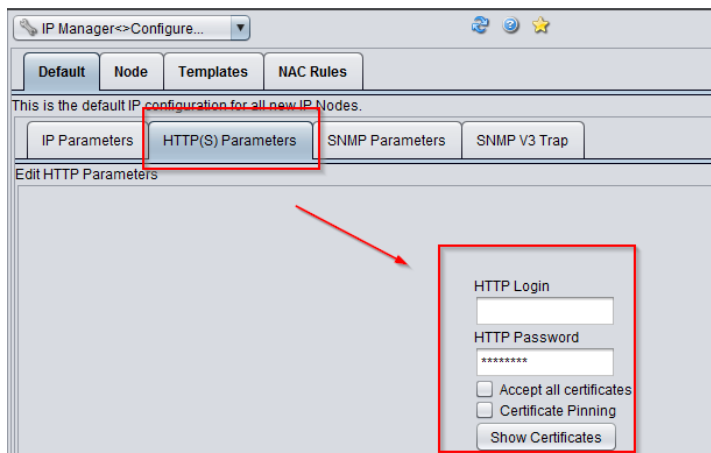
- ▶ **Status-Poll**
a status poll checks whether an IP node is reachable or not. If it is accessible, the subordinate objects are also prompted to update their status.
- ▶ **Configuration-Poll**
a configuration poll requests the child objects to update their configuration data.
- ▶ **Discovery-Poll**
performs a check for new child components of the IP node.
- ▶ **Expiration Time**
If an IP node can no longer be reached during this period, it can be deleted or set to unmanaged. This can also be ignored.
- ▶ **Expired IP Nodes**
If the expiration time has reached, these IP nodes are deleted from the OpenScope FM.
- ▶ **Offline Severity**
If an IP node goes into the Offline state, the status can be adjusted accordingly. The status Critical is set by default.
- ▶ **Preserve Topology**
if an IP node is assigned a new IP address, you can specify that the topology is to be retained or that the topology for this IP node is to be recreated according to the Discovery Filter rules.
- ▶ **IP-Address Adjustment**
for the IP node with multiple interfaces/IP addresses, the IP address to be queried is changed if the previously queried IP address can no longer be reached.
- ▶ **Auto Discovery**
it can generally be set that the ARP cache is read to scan the network.
- ▶ **Delete empty Network automatically**
A network is automatically removed from OpenScope FM if the last object was removed from the network.

TASK 6 > Change the default value for the status poll (availability check).

- MENU → IP Manager → Configure ...
- Change value for Status Poll to "1 minute"

Hosts and Networks: configuring HTTPS Parameters

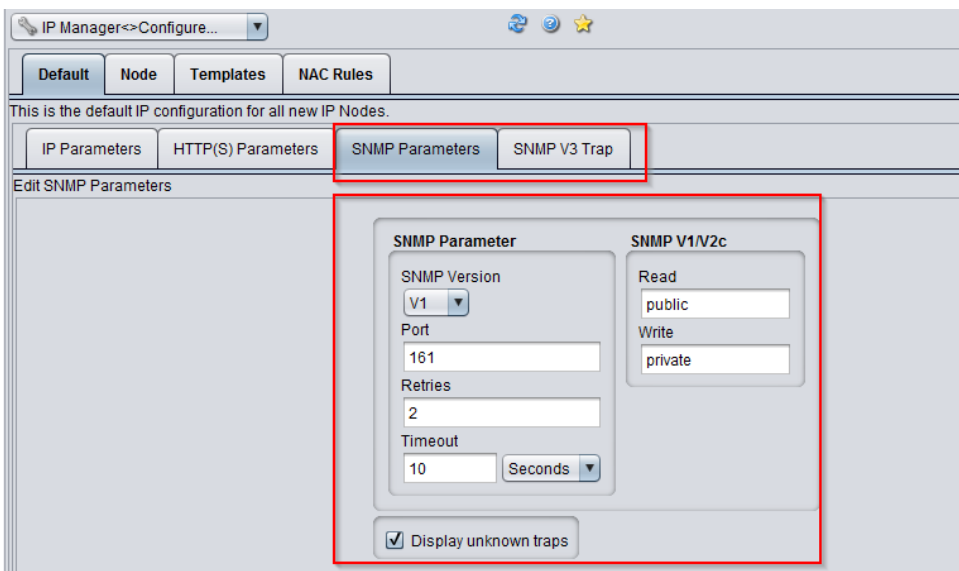
In the HTTP(S) tab, the login and password for recognized HTTP(s) web servers of a host can be defined.



1

Hosts and Networks: configuring SNMP Parameters

In the tab SNMP parameters the communities for the SNMP V1/V2c protocol are announced. These are necessary to read information about SNMP from the MIB of the SNMP agent, or make changes (GET and SET commands). The values entered here are valid for all newly discovered IP nodes. For the SNMP V3 protocol the security name, the authentication protocol (MD5, SHA) with authentication password and the encryption protocol (DES, AES128, AES192, AES256) with security password must be entered.



The OpenScape FM also receives SNMP traps from various devices. For the reception of SNMP V3 traps, it is necessary to specify whether and which encoding parameters are to be used. On the SNMP V3 Trap tab you can define the security level, the authentication protocol, the encryption protocol and the corresponding passwords under which OSFM receives the incoming traps.

Manage Configurations

▶ Menu -> IP Manager

Save Configuration ...

The current network configuration can be saved to an XML file and loaded at a later time. This can be done via the main menu entries IP Manager->Save Configuration...

Load Configuration ...

Load previous saved configuration (file)

▶ Menu -> IP Manager -> Configure -> Tab "Node"

IP-Node List

List of all hosts for bulk modification in multi-selection

▶ Menu -> IP Manager -> Configure -> Tab "Templates"

Templates for configuring multiple hosts

Creating and deleting templates for configuring IP/SNMP/HTTP

Advanced features in IP networks

▶ Menu -> IP Manager -> Configure -> Reiter "NAC"

NAC Rules, Network Access Control: Control network access by MAC/IP address

▶ Menu -> IP Manager -> Host Types ...

Managing Host Categories

▶ Menu -> IP Manager -> Cluster ...

Display of existing clusters

▶ Menu -> IP Manager

Update Status opens a dialog where you can enter the IP address of an IP node for which you want to update the status.

▶ Show Layer-3 Route

The Layer-3 connection from the start node to the destination node is displayed in a new window.

▶ Layer-2 Manager

Physical connections, switch ports, etc.

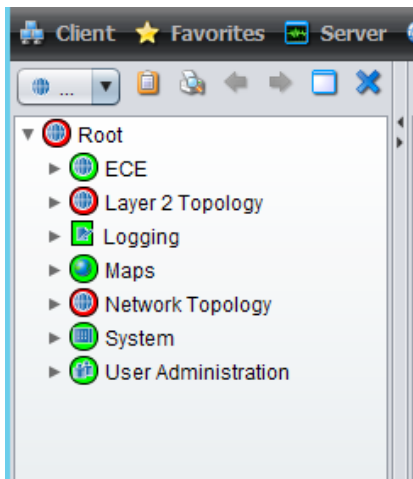
Working with the object tree: Containers and objects

Objects in OSFM Server ...

- ▶ always have object properties (symbol, name ...)
- ▶ always have a status value, the severity
- ▶ a detailed description of their status, the status explanation
- ▶ can be copied (and pasted), the copy is a "symbol"
- ▶ their processing can be stopped (unmanaged/not managed)
- ▶ offer an optional configuration
- ▶ can forward/propagate their status upwards in the object tree
- ▶ always have object rights
- ▶ can be commented

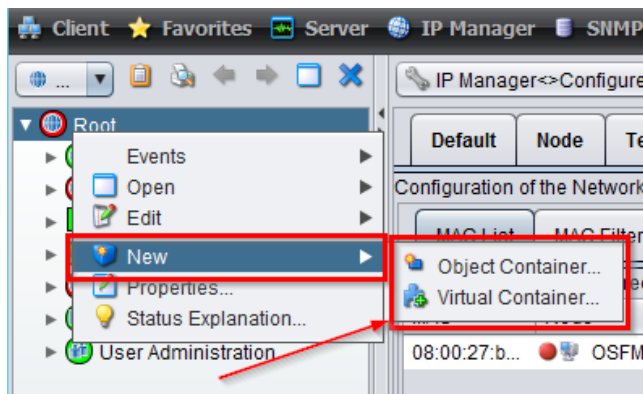
- **can be connected (new connection object)**
- **often offer extended/specific information and configuration in the context menu**
- **can be hidden**

Objects in the OSFM object tree are organized in containers, similar to folders. OSFM creates some (non-erasable, but hidden) system containers with the installation:



- **ECE**
Workflow engine for orchestration
- **Layer 2 Topology**
Display of physical connections (SNMP access required to switches/routers)
- **Logging**
Access logging
- **Maps**
Access and configuration of views of the CLIENT (NO geographical representation!)
- **Network Topology**
Representation of the logical IP network (subnets)
- **System**
internal objects for configuration
- **User Administration**
Manage users, groups, and permissions

In powerful tool in OSFM are custom containers:



► **Objektcontainer**

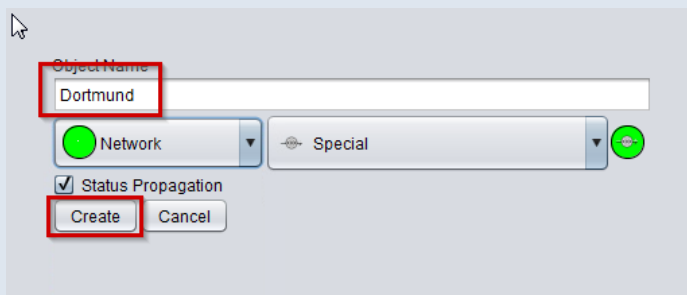
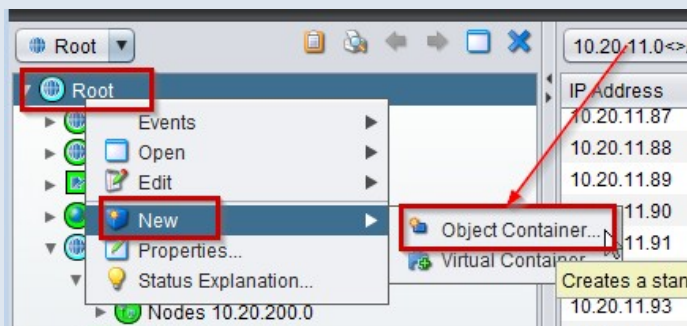
Display of objects of all types e.g: Hosts, Interfaces, Containers ...

► **Virtuelle Container**

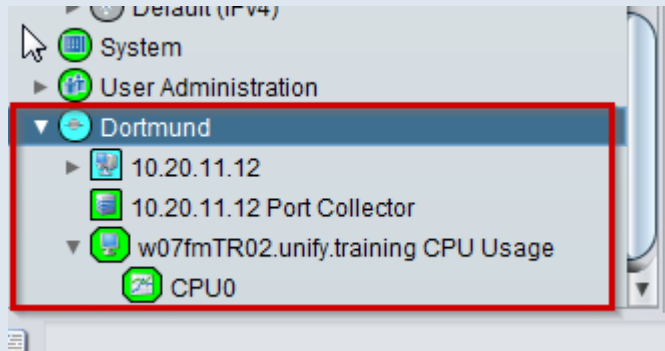
Display of objects based on a search/query. Always shows the current status.

TASK 7 > Create object container

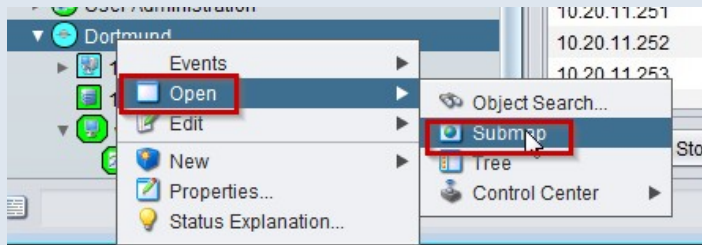
- Context menu (right mouse button) on the top node in the "Root" object tree open
- Select "New" -> "Object Container"
- Enter a name and confirm with OK.



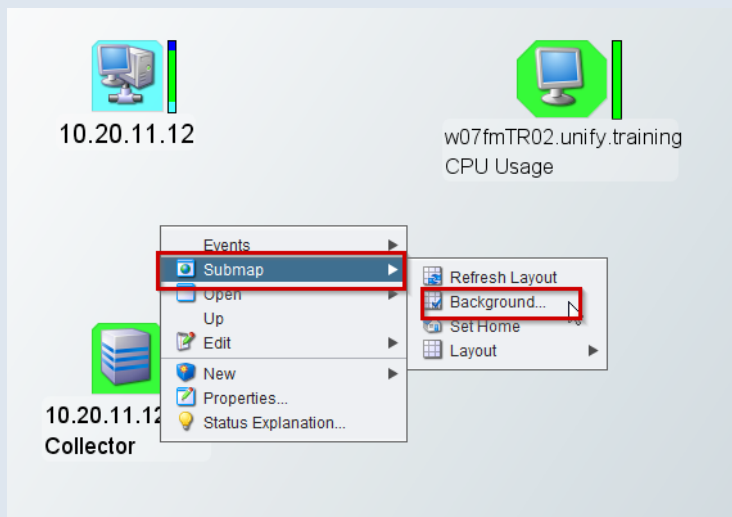
- Drag any objects of different types (hosts, containers, technologies) in this container or via context menu "Copy/Paste".



→ Open the graphical submap view of this container

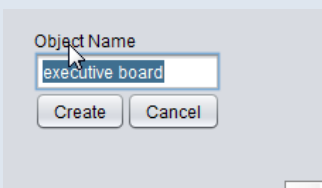
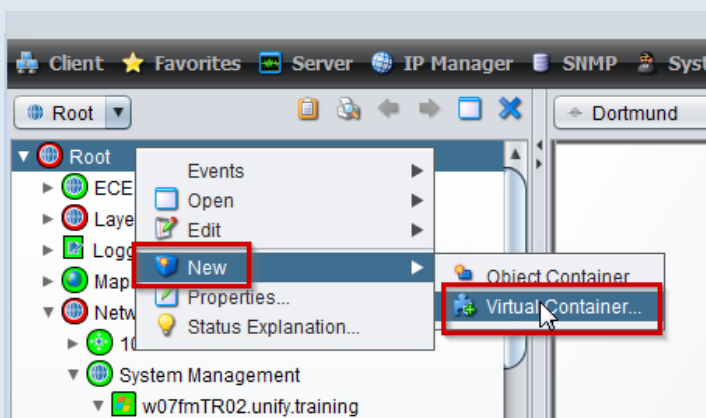


→ Changing the background image of the graphical submap view

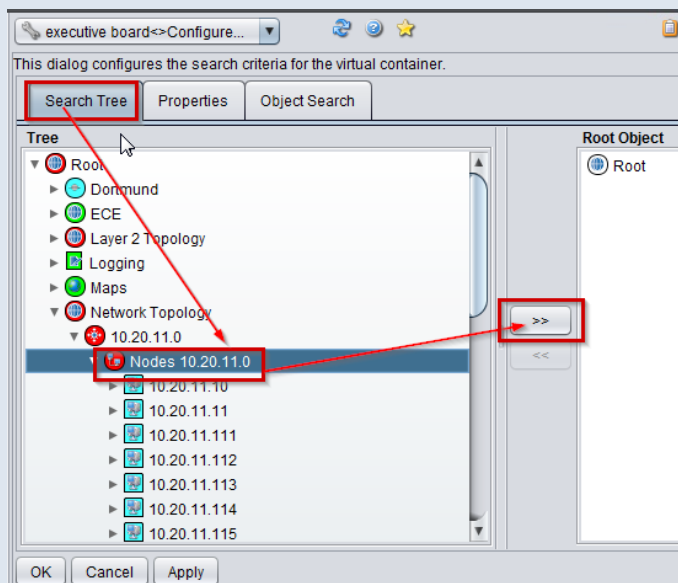


TASK 8 > Creating a Virtual Container

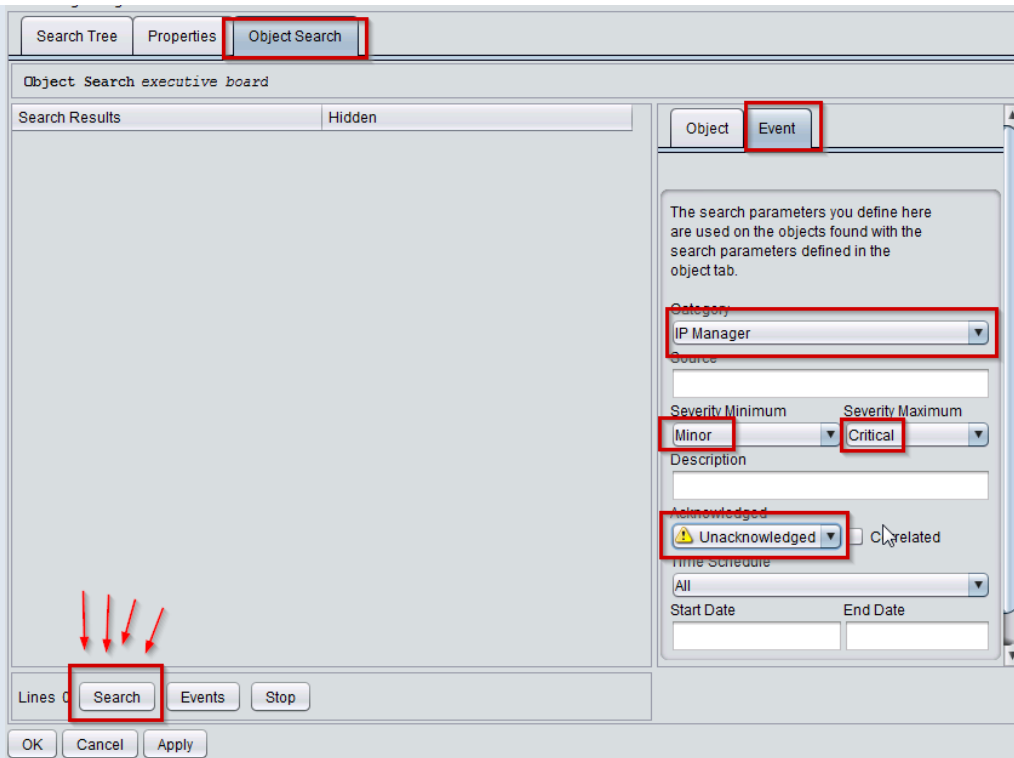
- Context menu (right mouse button) on the top node in the "Root" object tree open
- Select "New" -> "Object Container"...
- Enter a name and confirm with OK.



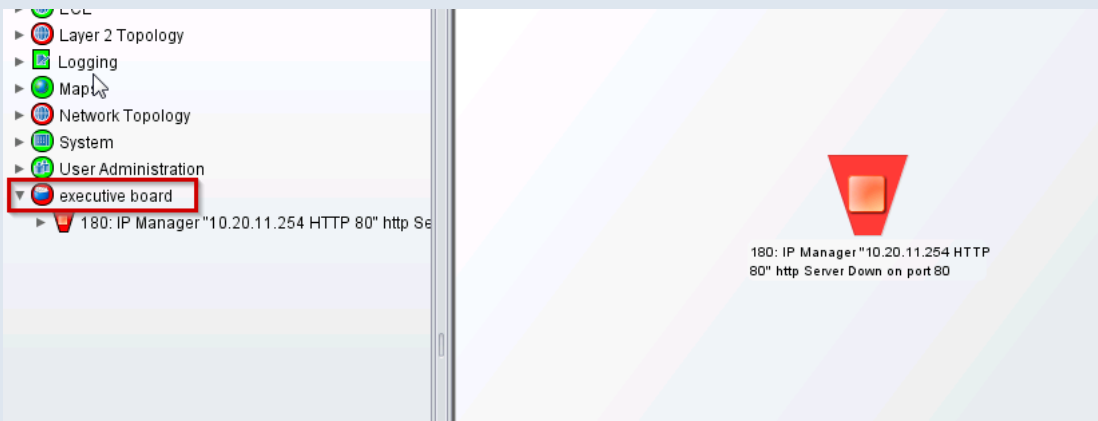
→ In the "Search Tree" tab select the container of the network nodes



→ Select tab "Object Search" -> sub-tab "Event"



- Set the following parameters
 - Category=IP Manager
 - Acknowledged=Unacknowledged
 - Severity Minimum = Minor
 - Severity Maximum=Critical
- Test query with "Search"
- Create container with OK
- Open submap of virtual container



Working with Events

Events are a central component of OSFM. All information is processed by OSFM and made available as an event. Each event was evaluated by OSFM in its significance (severity), is assigned to an object and contains information about ...

- ▶ **Acknowledge/UnAcknowledge**
- ▶ **Severity (Critical, Major, Minor, Warning, Normal, Unknown, Unmanaged, Restricted, Testing, Disabled)**
- ▶ **Date of creation**
- ▶ **Category**
- ▶ **Description**
- ▶ **Related Events**
- ▶ **Events of the same type**
- ▶ **Event-ID**

The administrator and operator can and should work with events, confirm them, delete them or comment on them.

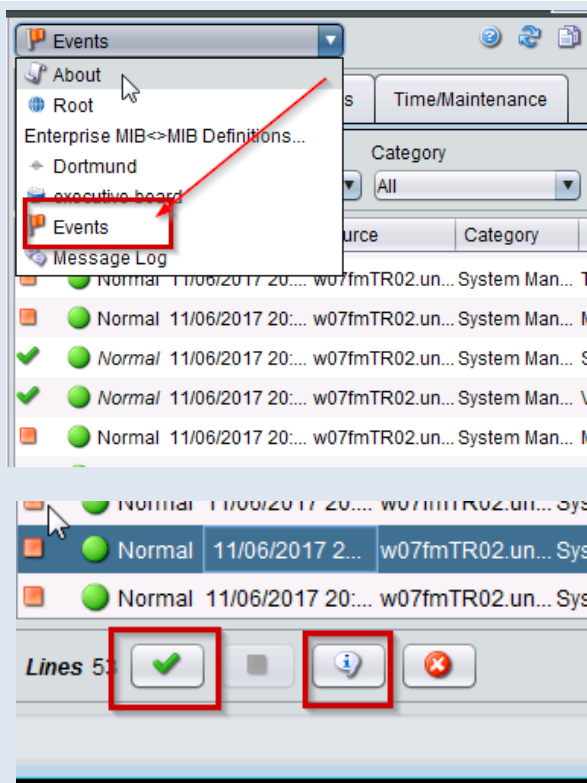
Examples of information for which events are generated:

- ▶ **SNMP Trap, Value, Threshold**
- ▶ **Change in object availability**
- ▶ **OpenScape 4000/Voice Alarm and Error**
- ▶ **Monitoring Parameter/Threshold**
- ▶ **internal Triggers, z.B. Licensing Issues**

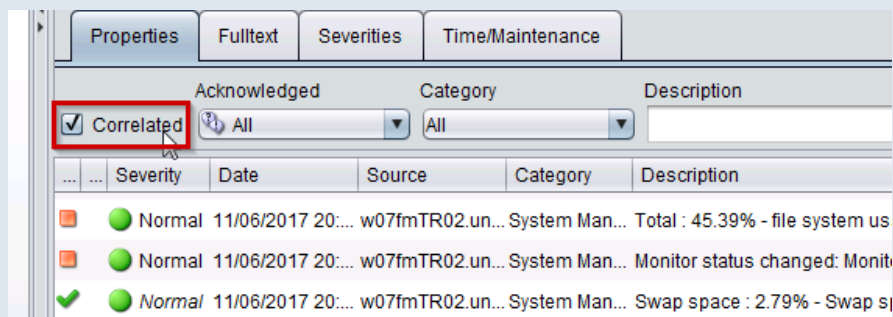
For a good overview in the list of events, events of the same type are summarized, correlated, displayed. This view can be deactivated, i.e. it can be displayed not correlated.

TASK 9 > Use list of events

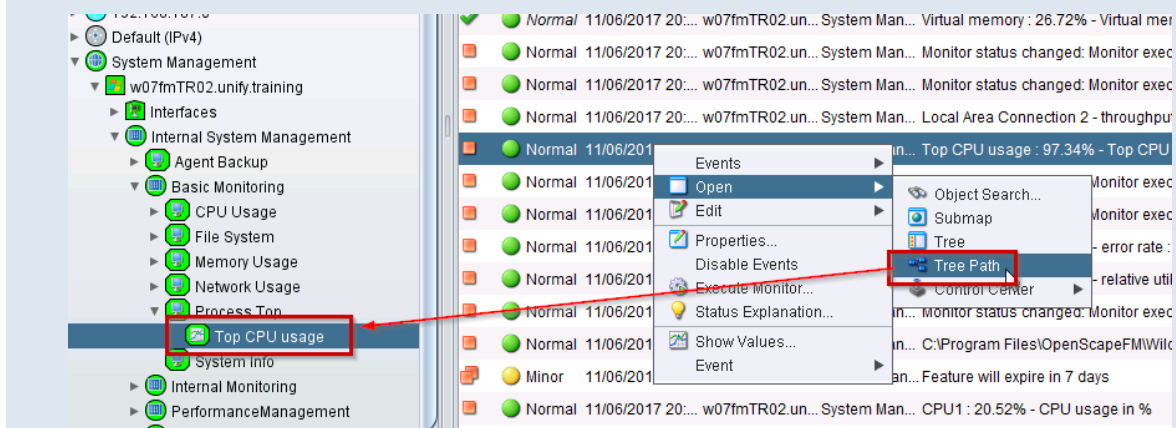
- **Open the list of events from the CardView drop-down box**
- **Confirm and comment on events using buttons at the end of the list**



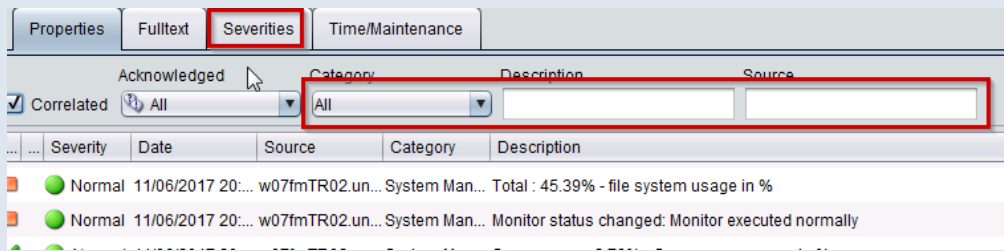
→ **Disable correlated view**



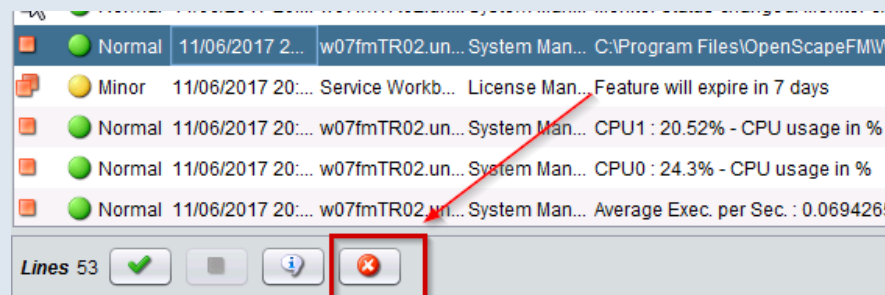
→ **Display affected object in object tree (context menu)**



→ **Filter list of events (severity, category, description...)**



→ **Delete event (status of object changes)**



Backup of object and monitoring database

OSFM stores all objects and their configuration in an internal object database and data from monitoring in an internal Java SQL database.

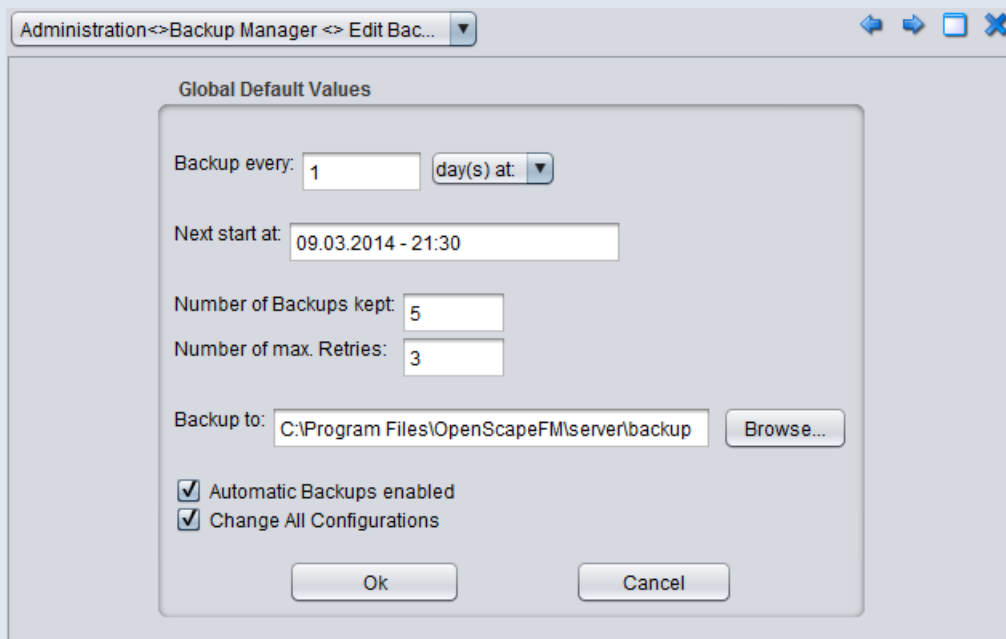
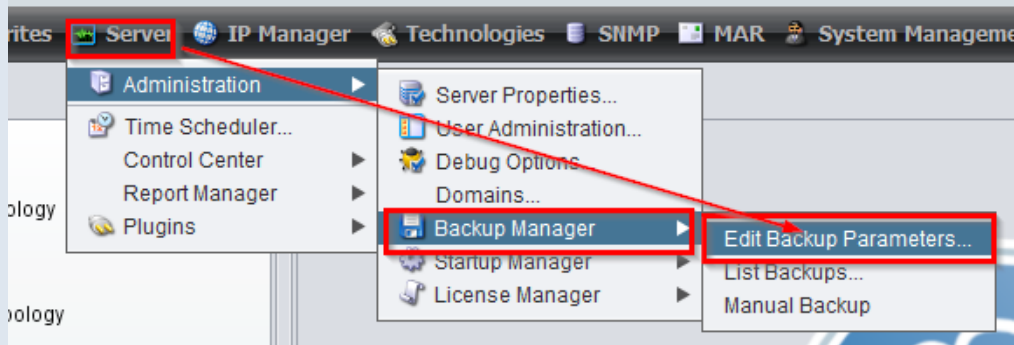
OSFM Server automatically and regularly backs up these databases after installation. The backup can be started manually or its configuration can be changed.

Possible use cases for using a backup:

- ▶ **accidental deletion of an object**
- ▶ **Restore a configuration of an object**
- ▶ **Restoring the installation in case of server migration**

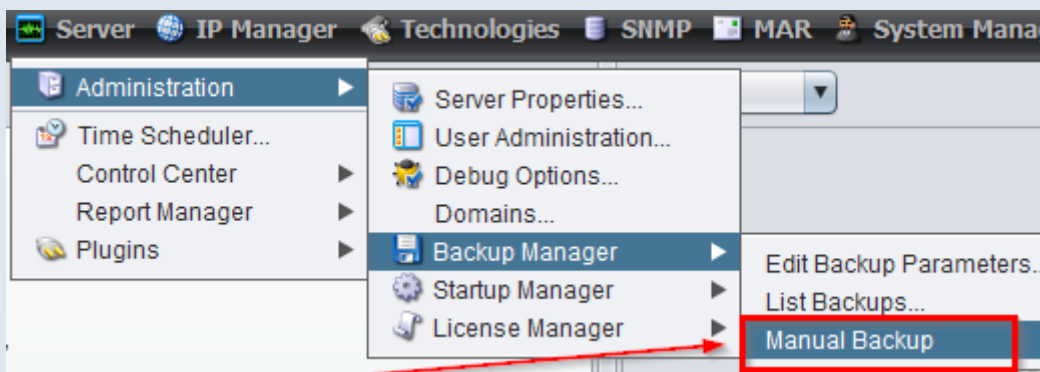
TASK 10 > Configuring Automatic Backup

→ **Menu -> "Server" -> "Administration" -> "Backup Manager" -> "Edit Backup Parameters"**



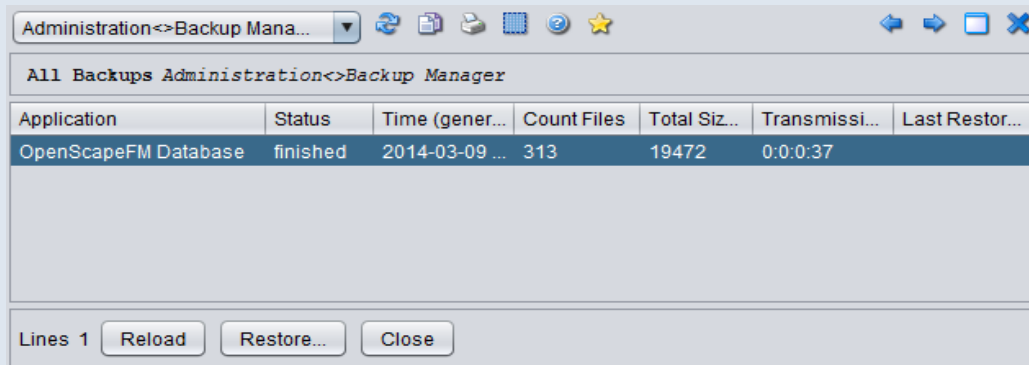
TASK 11 > Start one-time manual backup

→ Menu -> "Server" -> "Administration" -> "Backup Manager" → "Manual Backup"



TASK 12 > Restore backup

→ Menu -> "Server" -> "Administration" -> "Backup Manager" -> "List Backups..."



The screenshot shows a window titled "Administration<>Backup Mana...". Inside, there is a table titled "All Backups Administration<>Backup Manager". The table has the following columns: Application, Status, Time (gener..., Count Files, Total Siz..., Transmissi..., and Last Restor... The first row of data shows "OpenScapeFM Database" with a status of "finished", a time of "2014-03-09 ...", 313 files, a size of 19472, and a duration of 0:0:37. Below the table, there are buttons for "Reload", "Restore...", and "Close".

Application	Status	Time (gener...	Count Files	Total Siz...	Transmissi...	Last Restor...
OpenScapeFM Database	finished	2014-03-09 ...	313	19472	0:0:37	

Lines 1 Reload Restore... Close

→ Select Backup and then RESTORE