MyDesktopManager

Administration Manual

Version 1.0

OPEN SOURCE COMPETENCY CENTRE (OSCC) MAMPU

Level 3, APT E302-E304
Enterprise Building, Persiaran APEC
63000 Cyberjaya
Selangor
Tel: (6)03-8319 1200
Fax: (6)03-8319 3206
E-mail: helpdesk@oscc.org.my
http://opensource.mampu.gov.my

Table of Contents

1 Introduction

Desktop Management System (DMS) is a comprehensive approach for asset management within an organisation. The principle purpose of this product is to simplify the tasks of system/network administrators, e.g. deploying software in a network and keeping track of an organisation's IT inventory information (software and hardware) as well as network and system health monitoring

DMS will also help to monitor and alert which desktop is online. This saves time for the administrator by reducing administrative errors when performing inventory management. Inevitably, it also reduces manpower overheads.

The administrative interface is accessible by using a web-browser. Being web-based, no installation of additional software is required on the user's PC. The desktops that are being managed and monitored will have agents installed for communication with the system.

2 Web Access

MyDesktopManager can be accessed by pointing the web browser to the dedicated URL :

http://<IP Address>/dms (e.g. http://10.20.20.172/dms)

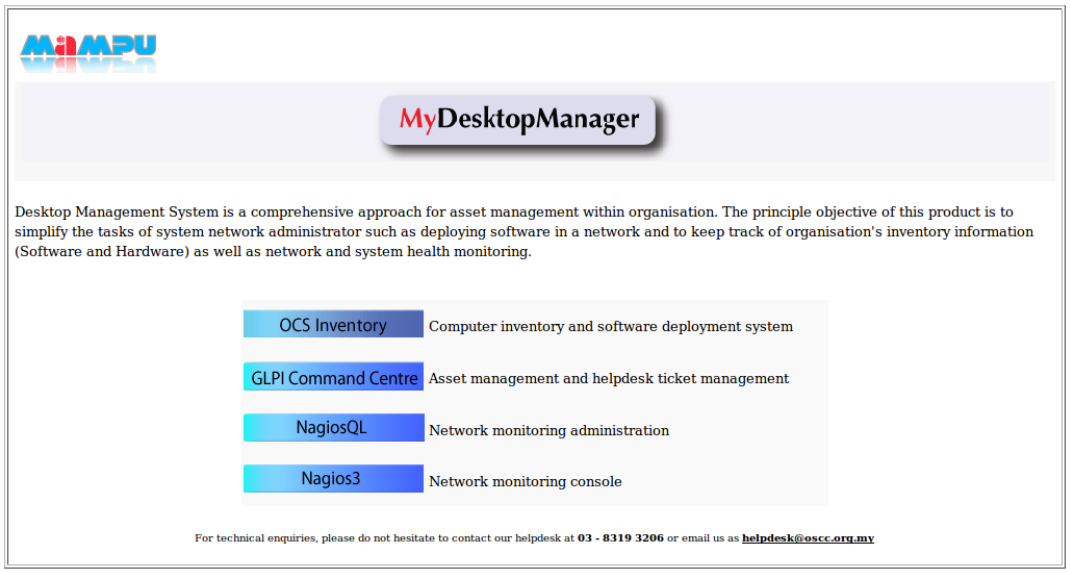


Figure 1

Figure 1 shows the front page of DMS comprising links to the four core modules of MyDesktopManager, i.e. OCS Inventory, GLPI, NagiosQL and Nagios3. Click the link and the core modules will be opened in a new tab in the web browser.

3 OCS Inventory

Open Computer and Software Inventory Next Generation (OCS inventory NG) is free software that enables an inventory of IT assets. OCS-NG collects information about hardware and software of networked machines running the OCS client program ("OCS Inventory Agent").

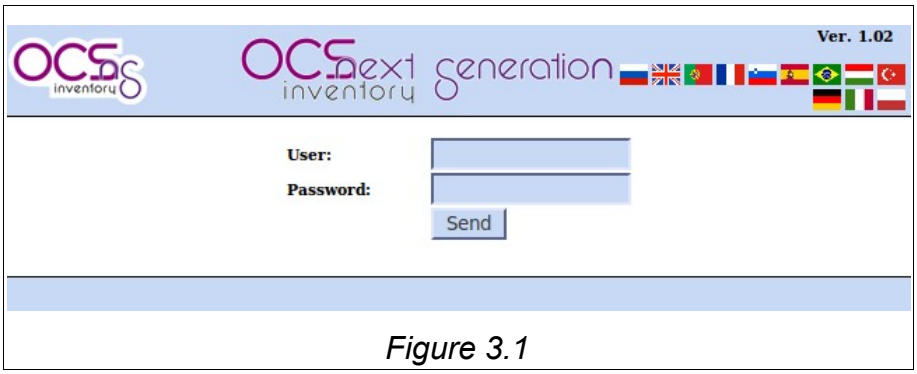


Figure 3.1

Figure 3.1 shows the login page for OCS Inventory. The username is admin and` the password is admin123. The password should be changed with the first login for security reasons.

3.1 OCS Main Page

Figure 3.2 is OCS Inventory main screen. It contains Main Toolbar and Summary of its inventory. Main Toolbar is separated into 2 section, i.e. blue background is view menu and yellow background is configuration menu.

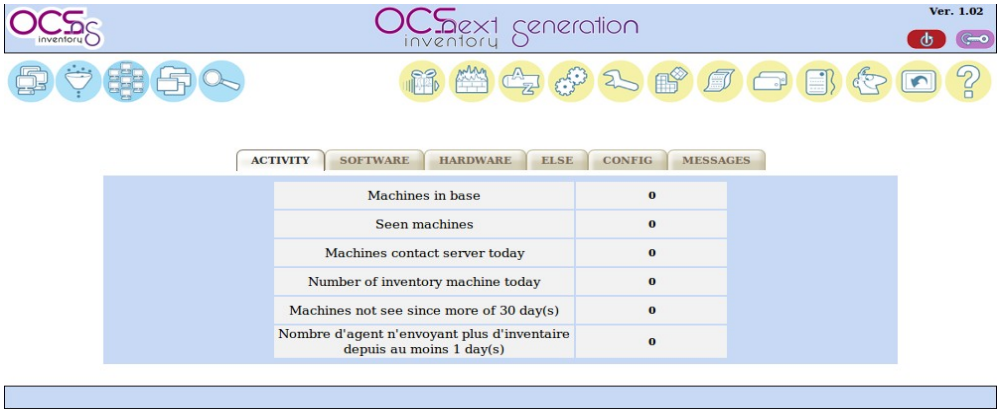


Figure 3.2

3.2 View Computer

 Click this icon on the top menu to view all computers.

This query will allow you to display all inventoried computers as seen in Figure 3.3. Computers marked with a red bullet at the beginning of line are those which have specific customized options.

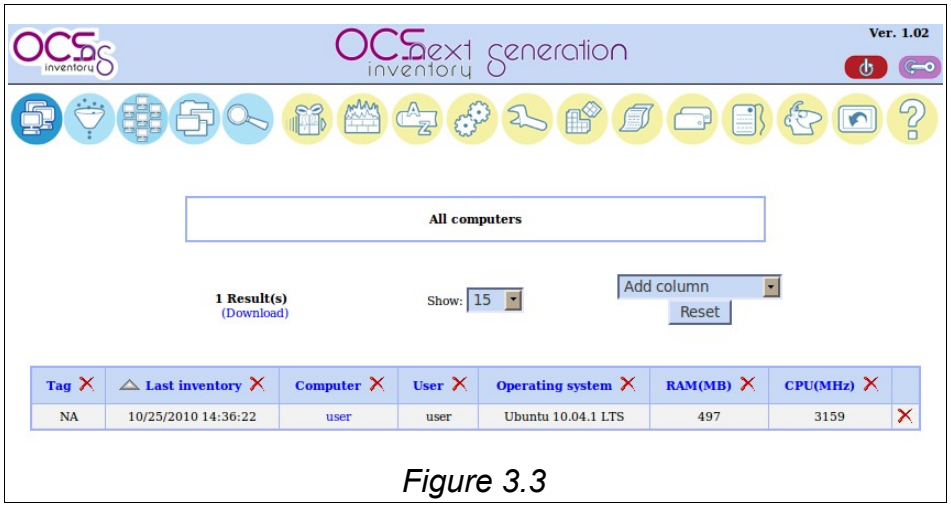


Figure 3.3

Click a computer name to display its properties in a new web browser window.

- Top banner (Figure 3.4) – Displays general information for the current device

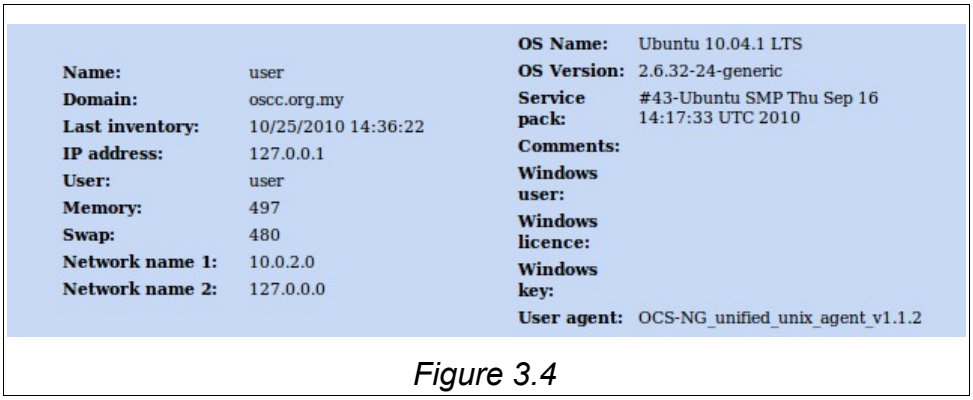


Figure 3.4

- Links section (Figure 3.5) – Click the appropriate link to display the corresponding information.

Figure 3.5

- Bottom section (Figure 3.6) - Use “show everything” to display all sections. To print, use “print this page” icon.

Figure 3.6

- Special section Administrative data (Figure 3.7) – Use this section to display the device's administrative data. This page fits with settings in “admininfo” tab. Use the “update” button to change values.

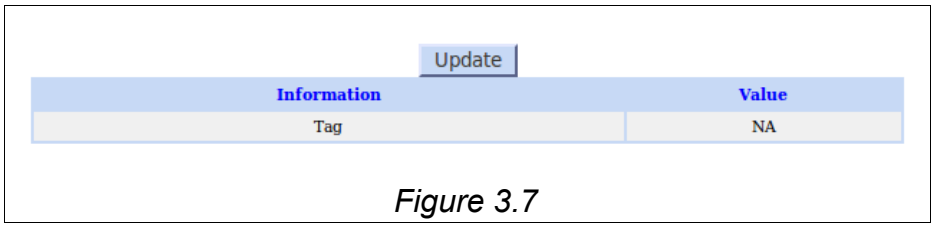


Figure 3.7

- Special section Customization (Figure 3.8) – Use this section to customize configuration options for individual computers. Packages can be selected here to deploy on a particular computer.

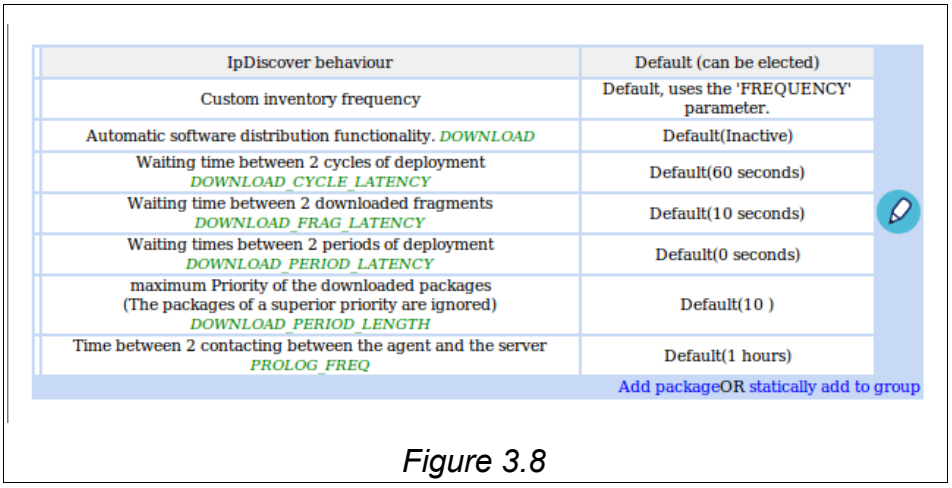


Figure 3.8

3.3 Managing OCS Inventory Admin users

Click the toolbar “Users” menu as in Figure 3.9 to display all configured OCS Inventory NG Administration server users.

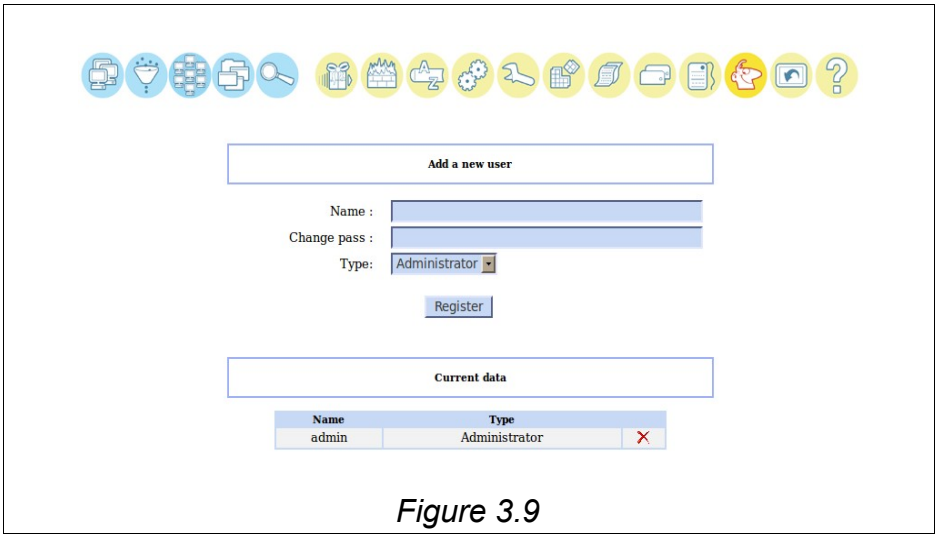


Figure 3.9

New users can be added by entering their name, password (user will be able to change it when logged in), and selecting their type. You can choose between:

- Administrator: user has the ability to configure all parameters of the product.
- User: user can only query the database and view results of inventory. It just has the top left Combo-box of menu toolbar to run general queries.
- To delete a user, just click on red cross at the end of the corresponding line.

3.4 Software Deployment

Refer to Figure 3.10 to learn how to upload packages which will be downloaded through HTTP/HTTPS and executed by the agent on client computers. There are 11 levels of priority, ranging from level 0 to 10. Level 0 is the highest priority and level 10 the lowest.

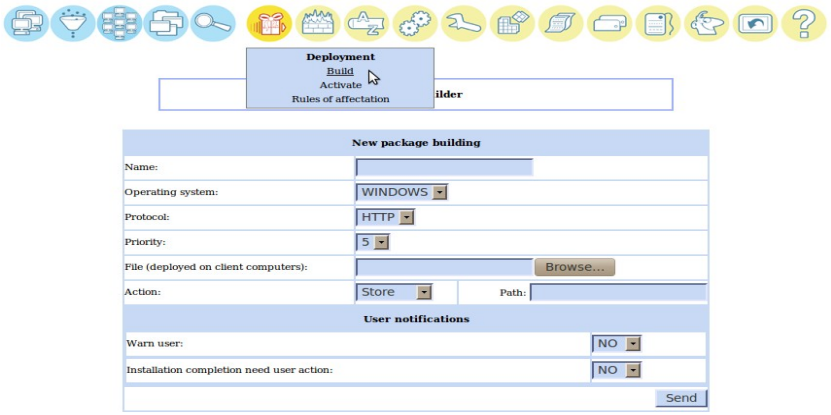


Figure 3.10

Action is associated with file to deploy and command to launch

- **Launch** - to deploy with or without parameters an executable file included in ZIP or TAR.GZ file.ZIP
- **Execute** - to deploy with binary installer
- **Store** - To store in a client machine

4 GLPI

GLPI, an acronym for Gestionnaire libre de parc informatique (Free Management of Computer Equipment), is free, trouble ticket software that can used to build and maintain an inventory database for computer equipment (computers, software, printers, etc.). It has enhanced functions like job-tracking system with mail notification and methods to build a database with basic information about network topology.

Figure 4.1

Figure 4.1 shows the login page for OCS Inventory. The username is glpi and the password is glpi. The password should be changed with first time login for security reasons.

4.1 Setup OCS Inventory Link

A link must be established between OCS Inventory and GLPI in order for GLPI to share OCS Inventory's data. Referring to Figure 4.2, go to Setup > OCSNG Mode,click on the plus (+) sign which is in the red circle.

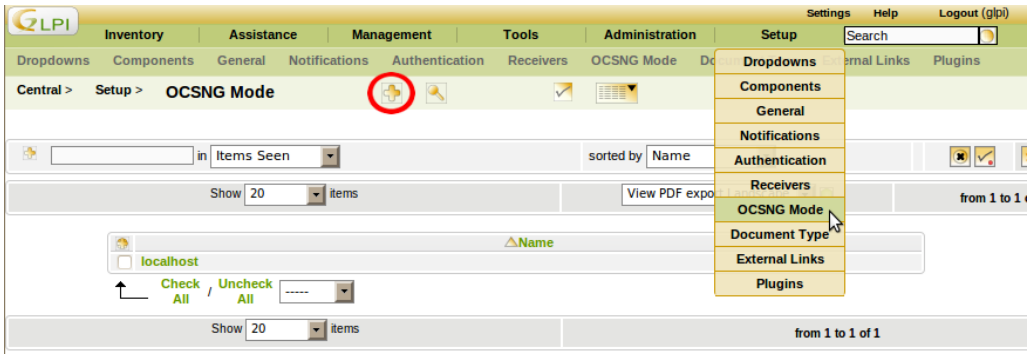


Figure 4.2

Refer to Figure 4.3, key in the following information. Figure 4.4 shows a successful connection to OCS Inventory.

- **Name** – Reference name of OCS Inventory
- **OCSweb host** – OCS Inventory IP address
- **Name of OCS database** – OCS Inventory database name
- **OCSweb database user** – OCS Inventory database username
- **OCSweb user password** – OCS Inventory database password

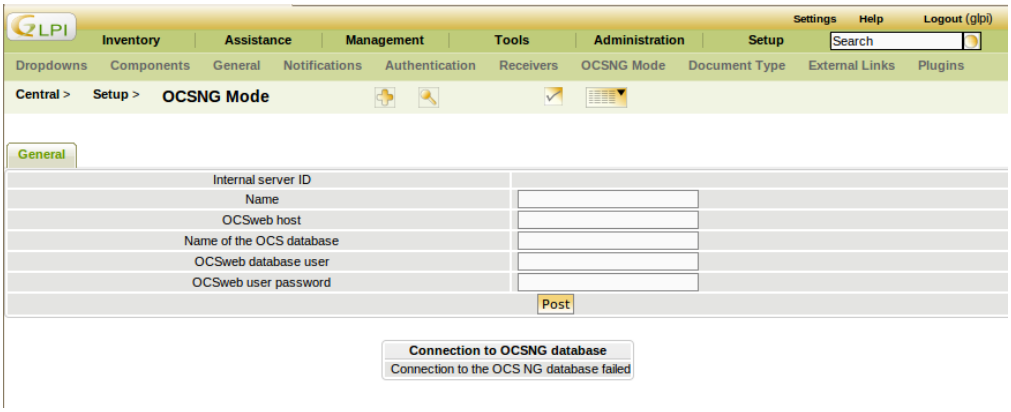


Figure 4.3

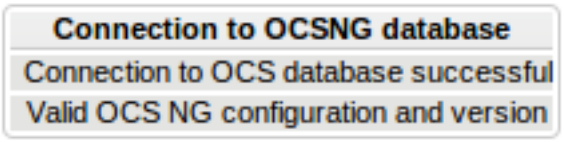


Figure 4.4

4.2 Sync OCS Inventory

When GLPI has a valid connection to OCS Inventory, the databases must be synchronised. Figure 4.5, go to Tools → OCSNG → Import new computers

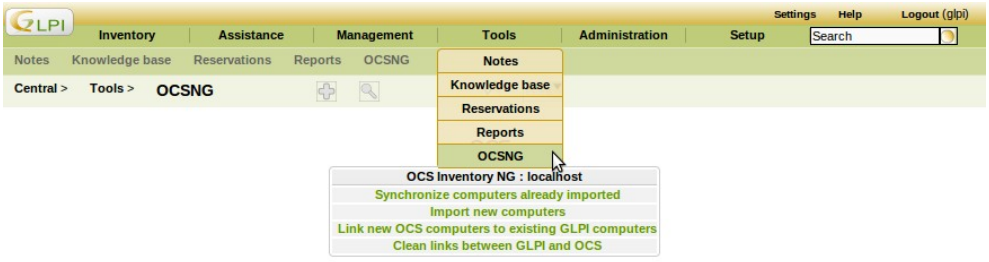


Figure 4.5

After synchronisation is complete, go to Inventory Computers. Figure 4.6 shows the same information with OCS Inventory. Click the Computer Name to view/edit more information, Figure 4.7.

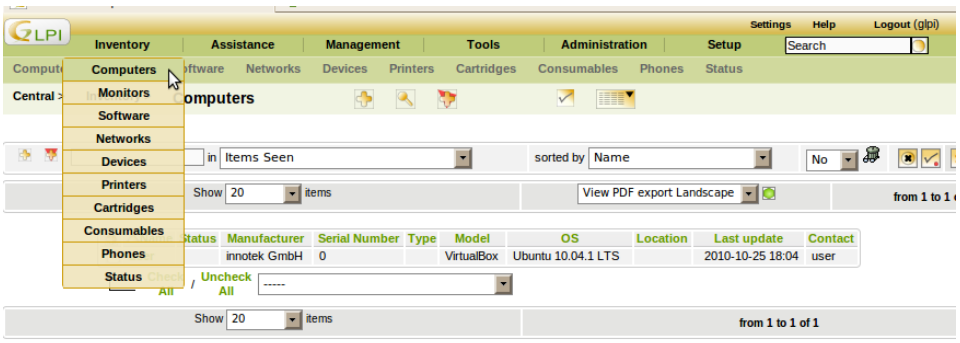


Figure 4.6

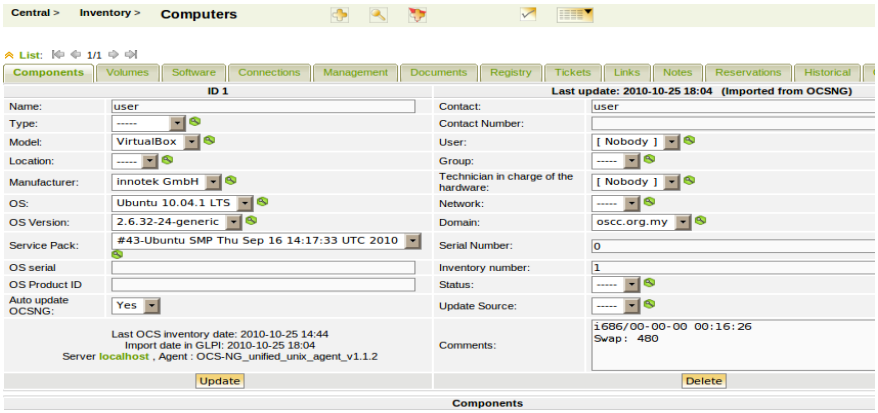


Figure 4.7

4.3 Helpdesk

GLPI comes with a helpdesk, which can be accessed at Assistance Helpdesk , Figure 4.8. Submitted tickets are then routed to respective technician or support personal based on configured rules.

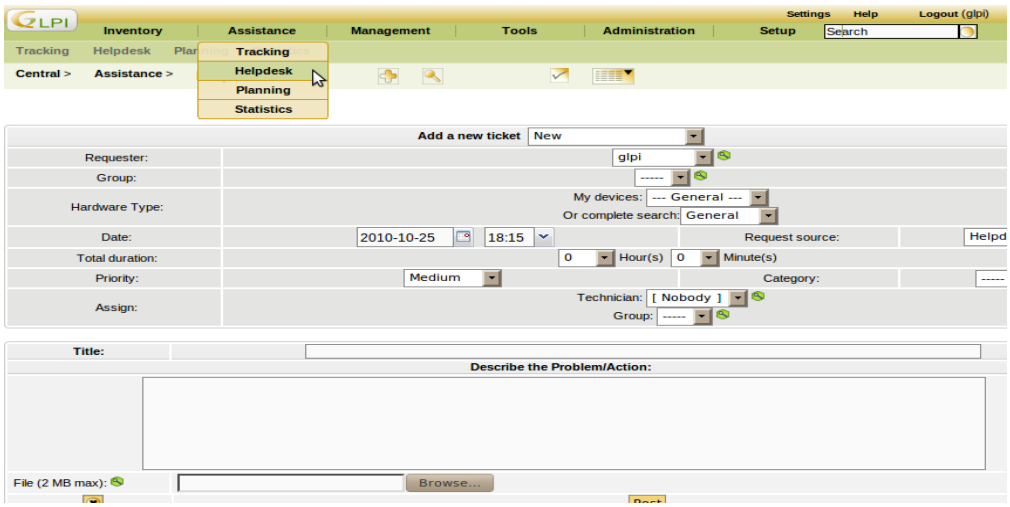


Figure 4.8

4.4 Ticket Tracking

At Tracking, which is under **Assistance** menu, a ticket and its status can be searched, Figure 4.9.

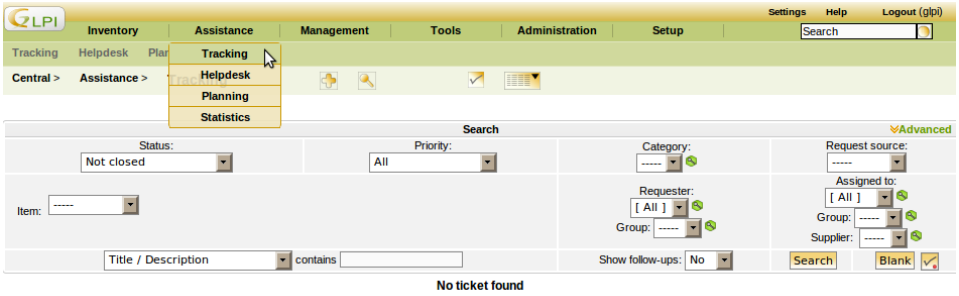


Figure 4.9

4.5 Reports

GLPI provides a set of reports, Figure 4.10. It will show hardware statistics and other information. Figure 4.11 shows a sample report generated by GLPI.

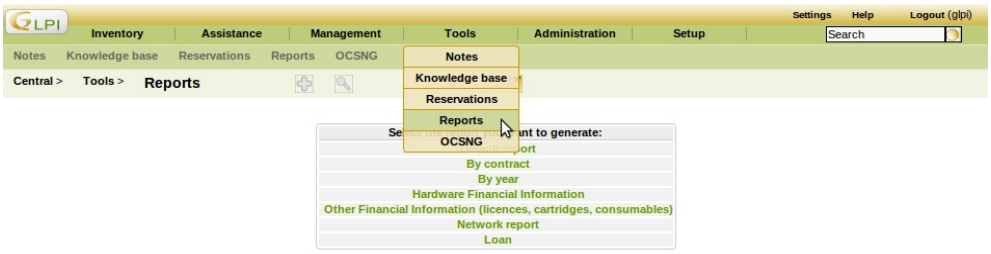


Figure 4.10

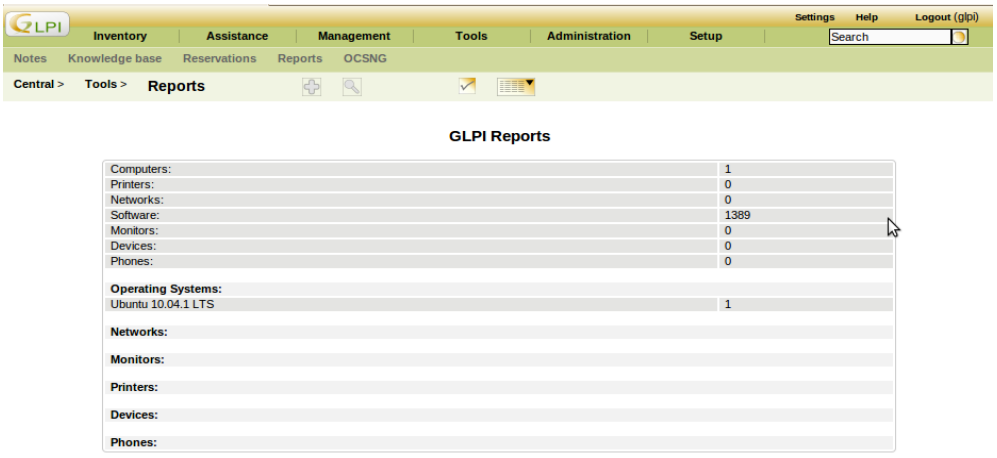

GLPI
Settings
Help
Logout (glpi)
Inventory
Assistance
Management
Tools
Administration
Setup
Search
Notes
Knowledge base
Reservations
Reports
OCSNG
Central >
Tools >
Reports
GLPI Reports
Computers: 1
Printers: 0
Networks: 0
Software: 1389
Monitors: 0
Devices: 0
Phones: 0
Operating Systems:
Ubuntu 10.04.1 LTS 1
Networks:
Monitors:
Printers:
Devices:
Phones:

Figure 4.11

5 NagiosQL

NagiosQL is a web-based administration tool for Nagios3. It helps to easily build a complex configuration with all options, then manage and use it. The data is stored using MySQL database.

Figure 5.1

Figure 5.1 shows the login page for NagiosQL. The username is admin and the password is admin123. The password must be changed with the first log-in for security reasons.

5.1 NagiosQL Main Page

NagiosQL main page is shown in Figure 5.2 The most commonly used menus for Nagios3 in MyDesktopManager are Supervision and Alarming.

Figure 5.2

5.2 Supervision

Supervision page in NagiosQL administration tool is used to define and manage hosts and services as well as their groups.

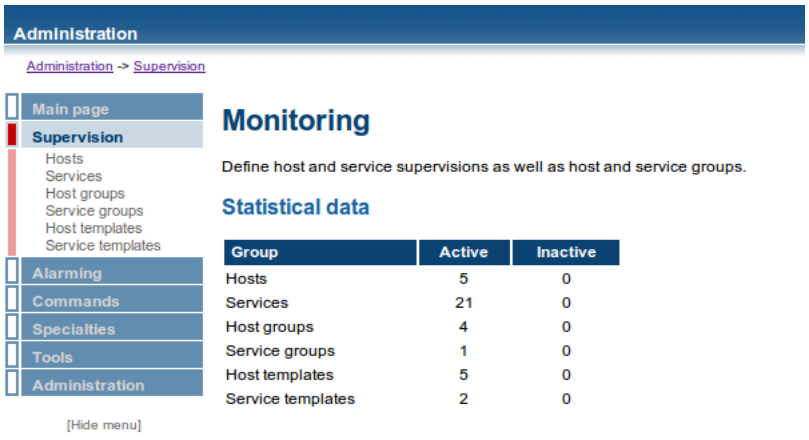


Figure 5.3

Figure 5.3 shows the supervision page with the summary of statistical data of the hosts, services, groups and templates.

5.2.1 Hosts

Host is a computer that is connected to a network, usually the Internet or other TCP/IP (transmission control protocol/Internet protocol) network, such as a LAN (local area network). Each host on a TCP/IP network has a unique IP address, which is detected and monitored using Nagios. Figure 5.4 shows the list of current hosts being monitored by Nagios.

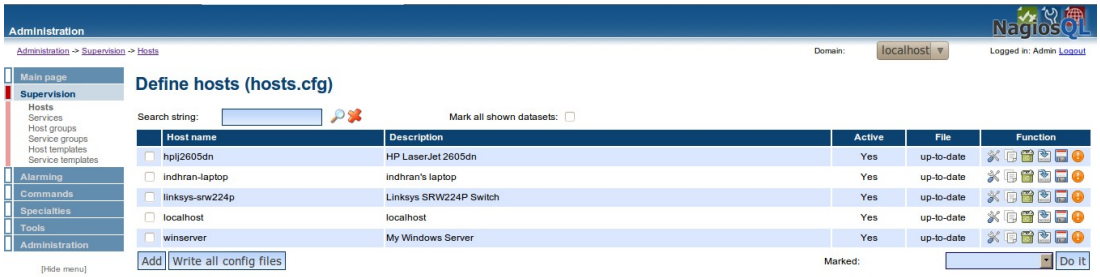


Figure 5.4

5.2.1.1 Adding hosts

Click the Add button as shown in Figure 5.5 to manually add a new host.

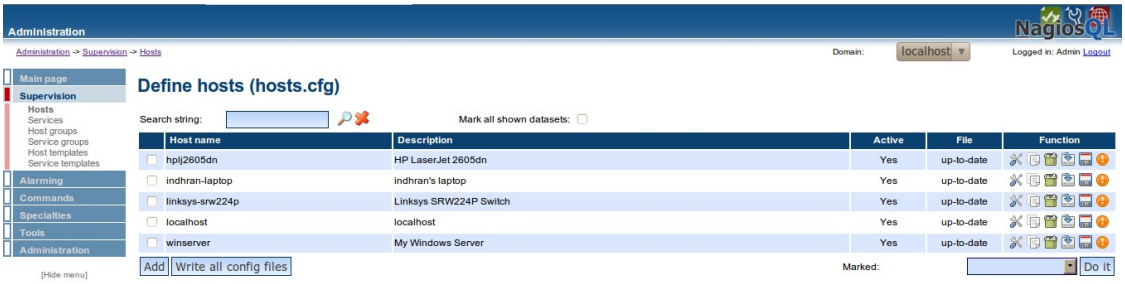


Figure 5.5

This will display a tabbed set of forms as in Figure 5.6 where all of settings for new host are manually specified. After adding the new host, click '**Write all config files**' to re-load the configuration. All form fields labeled with an asterisk or highlighted in red are required fields.

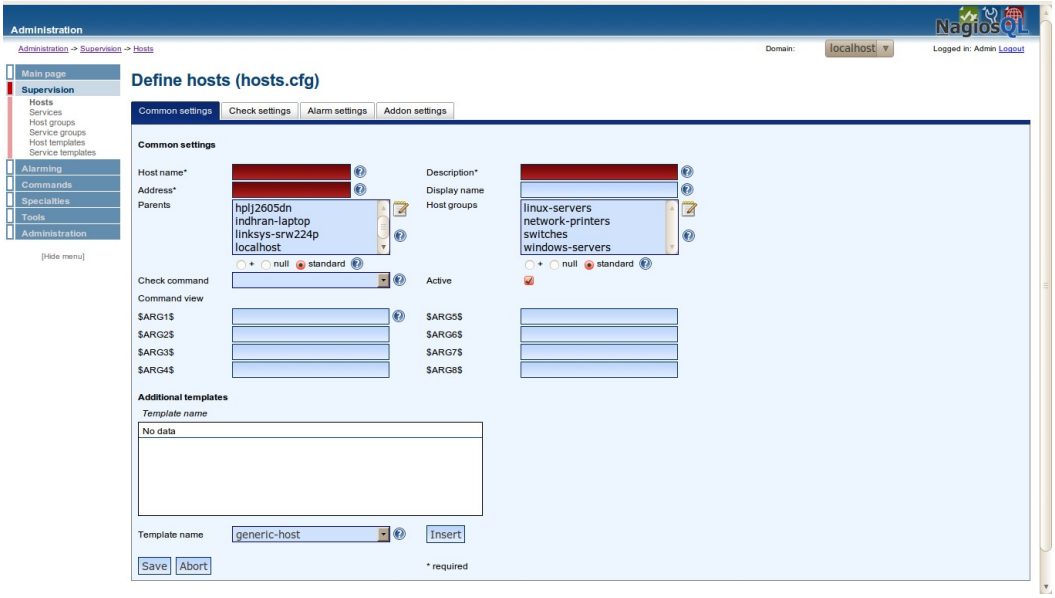


Figure 5.6

The **Common Settings** tab allows definition of the primary host parameters, templates, and host groups. **Hostname** is the name of the computer and the **address** should be mapped to the machine's IP address. **Description** can be anything to resemble the machine in a network. The question mark shows details of each form field.

Every command in the **Check command** dropdown list is associated with a set of Nagios Core commands and arguments. Host parameters can be defined from an existing template, which is accessible from the dropdown menu labeled

Template Name .

Hosts can also be assigned to an existing **Host group** by selecting the modify icon located to the right of the Host groups field. This will display a selection box to choose which existing groups to assign to the host.

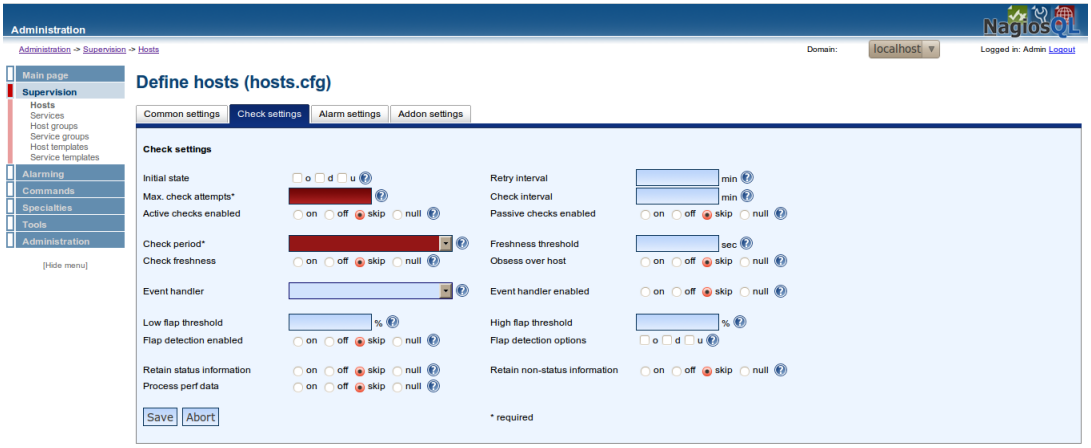


Figure 5.7

Figure 5.7 shows check settings tab which allows settings to be specified for frequency of checks and also the host state. The **Max. check attempts** is used to define the number of times that Nagios will retry the host check command if it returns any state other than an OK. The **Check period** is used to specify the short name of the time period during which active checks of this host can be made. For the details of the other optional fields, please view the help boxes.

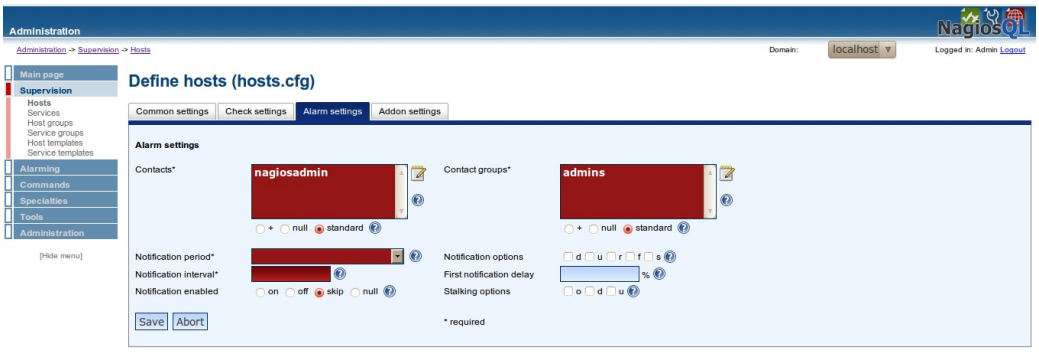


Figure 5.8

Figure 5.8 shows the Alert Settings tab which allows specification of notification settings using existing contacts and contact groups.

5.2.2 Services

5.2.2.1 Adding Services

Figure 5.9 shows the list of current services being monitored by Nagios. Click the Add button as shown in Figure 5.9 to manually add a new service.

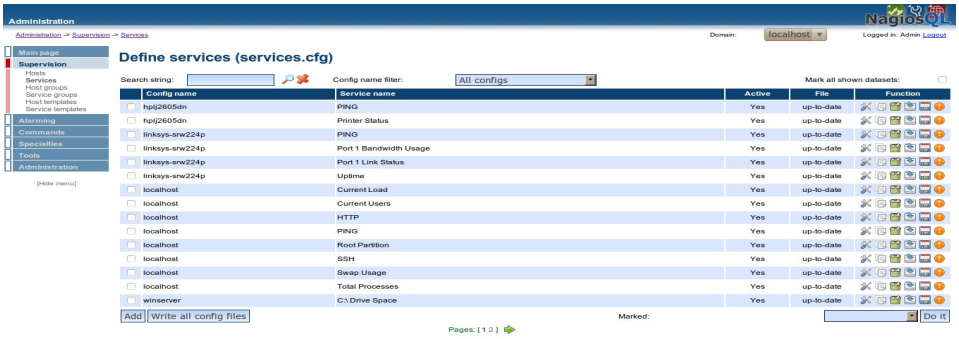


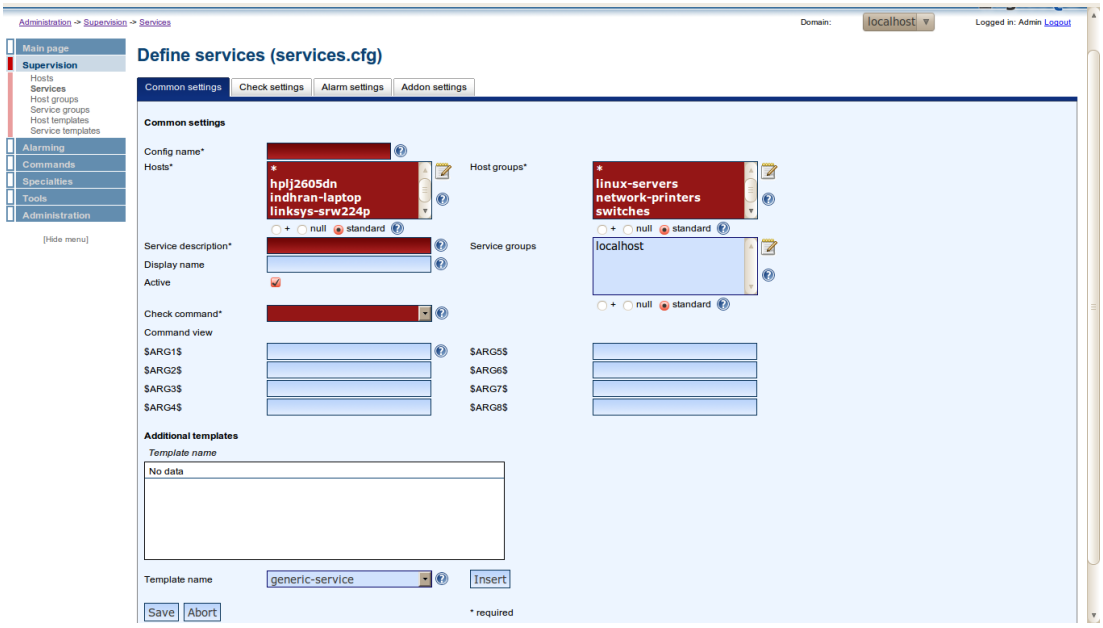
Figure 5.10

This displays a tabbed set of forms as in Figure 5.10 where all settings for new service are manually specified. After adding the new service, click the '**Write all config files**' to re-load the configuration.

The **Common Settings** tab allows definition of a service to be monitored. The question mark shows details of each form field. The **config name** is a common config name for a group of service definitions while, **hosts** and the **hostgroup** are the host and the hostgroup(s) that the service "runs" on or is associated with. Service can also be assigned to an existing **service group** by selecting the modify icon located to the right of the Host groups field. This

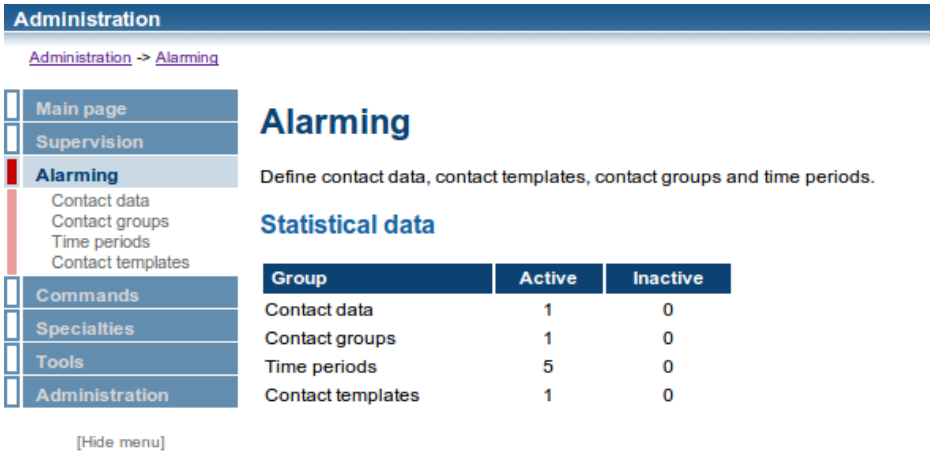
displays a selection box where existing groups to assign the service to are selected.

The other 3 tabs are similar with section 5.2.1.1



5.3 Alarming

Alarming page in NagiosQL administration tool is used to define and manage contacts and contact group that will receive notification or alerting through email. Figure 5.11 shows the alarming page with the summary of statistical data of the contact data, contact groups, time periods and templates. Contact data is the contact information of the system administrator while contact group is a group to which the contact person is associated. Time period is used to define a range of time to be used in adding contact data time period during which the contact person can be notified about host problems or recoveries.



5.3.1.1 Adding Contact Data

Figure 5.12 shows the list of current contacts that are being notified by Nagios. Click the Add button to manually add new contact data. This will display a tabbed set of forms as in Figure 5.13 where all of the settings for your new contact can be manually specified. After adding the new contact, click the '**Write all config files**' to re-load the configuration. All form fields labeled with an asterisk or highlighted in red are required fields.

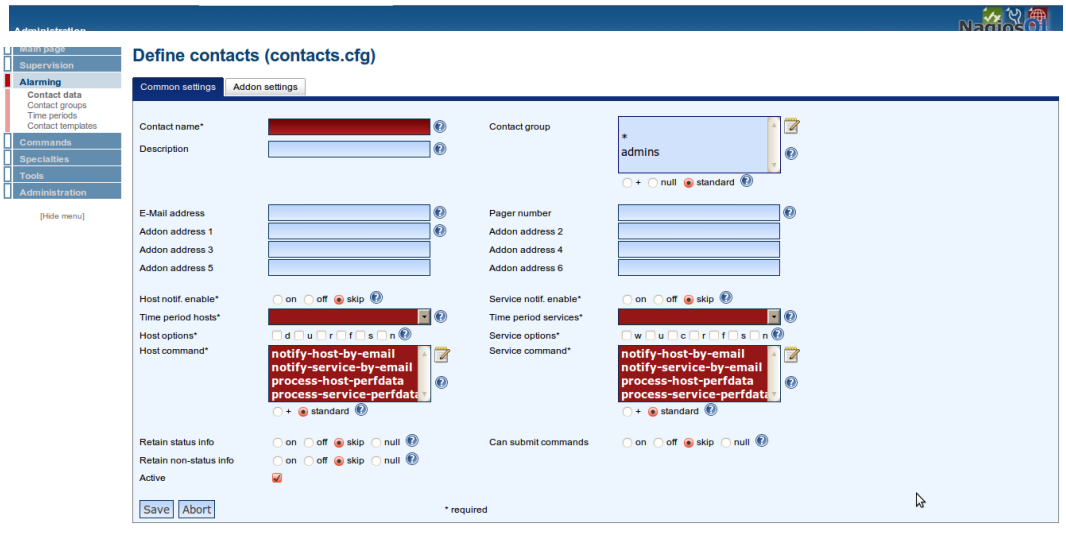


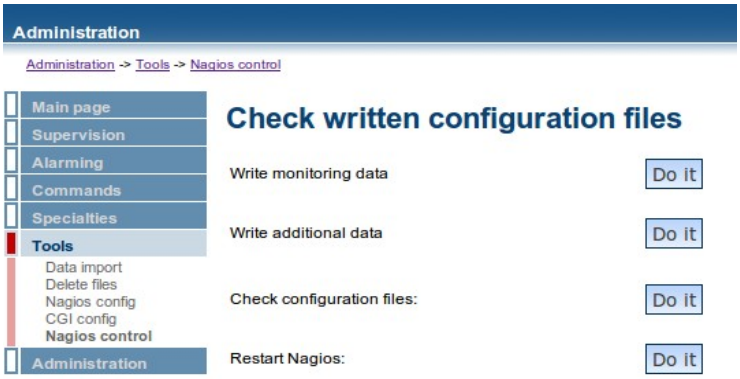
Figure 5.13

Figure 5.13 shows the form to add a new contact. As explained in previous sections, please use the help functions to find out details and required directives. The contact name can be any to define the contact person. Time period host is used to specify the time period during which the contact can be notified about host problems or recoveries. Host command is used to define a list of commands to notify the contact of a host problem while the service command is used to notify the contact of a service problem.

5.4 NagisoQL Administration

NagiosQL user administration can be done using the Administration link on the menu as shown in Figure 5.14.

5.5 NagiosQL Tools



NagiosQL tools can be used to backup and manage configuration files. Figure 5.15 shows the Nagios control tool to check the written configuration files. Each time changes are made to any of the forms or configuration files, users need to submit all four 'Do it' buttons in order to re-load and apply the changes.

6 Nagios3

Nagios3 is an open source network monitoring solution. It is capable of checking remote hosts in any platform, i.e. Linux, Unix, Windows, FreeBSD and Mac. Nagios3 is included in MyDesktopManager to ease the system administrator's task in monitoring their assets and as well as networks.

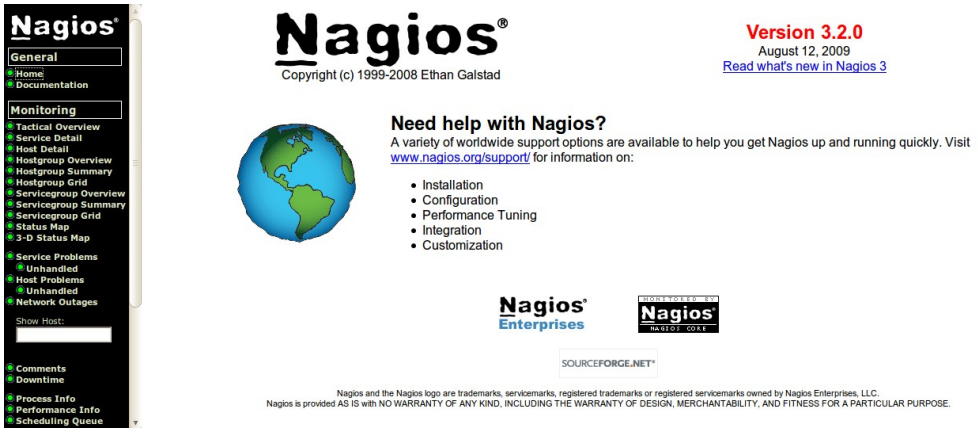


Figure 6.1 shows the main splash screen upon login. The username is **admin** and password is **admin123**. Nagios3 is capable to access network services with various network protocol. It is also able to identify host/service unavailability and trigger aleerts to the system administrator.

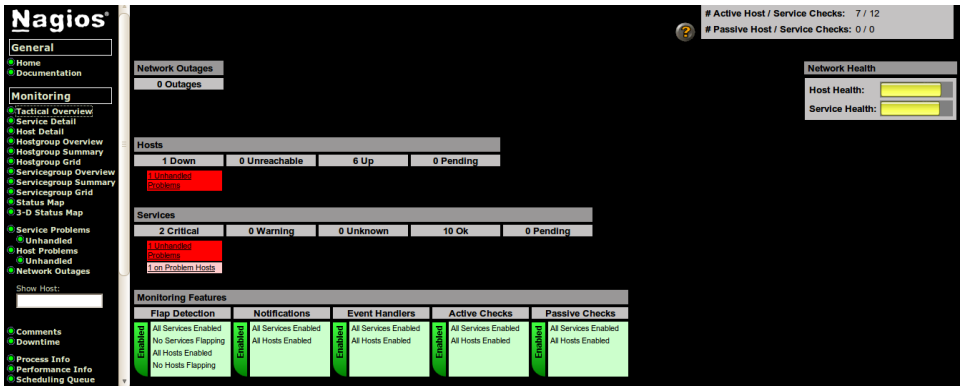


Figure 6.2 shows the tactical overview which serves as a "birds-eye view" of all network monitoring activity. It allows quick view of network outages, host status, and service status. It distinguishes between problems that have been "handled" in some way and those which have not been handled, and thus need attention.

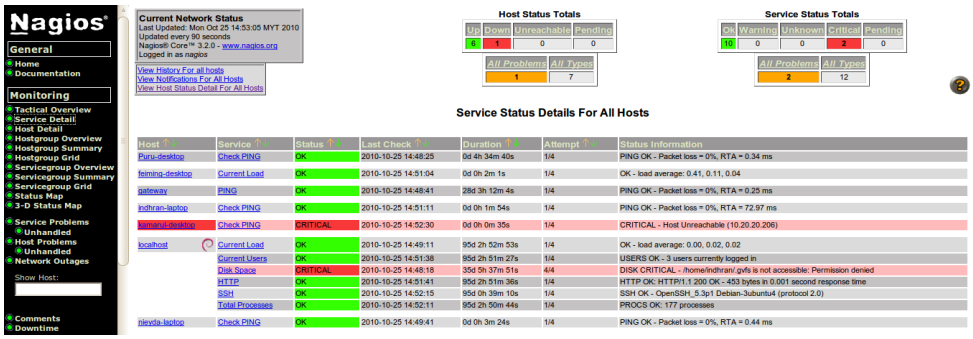
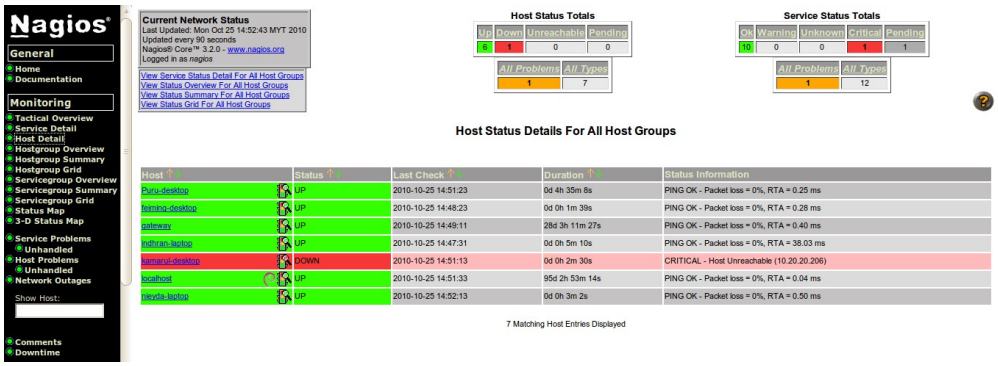


Figure 6.3

Figure 6.3 shows the service details that have been defined in NagiosQL. It shows service status details for all associated hosts. 'The status with green shows that the service is up and running while red is down or critical and needs attention from the system administrator.



The host details in Figure 6.4 shows the overall status of the host defined. It displays total entries and those which are accessible are shown in green and those wich are unreachable are shown in red. It also shows the ping status information in the last column.

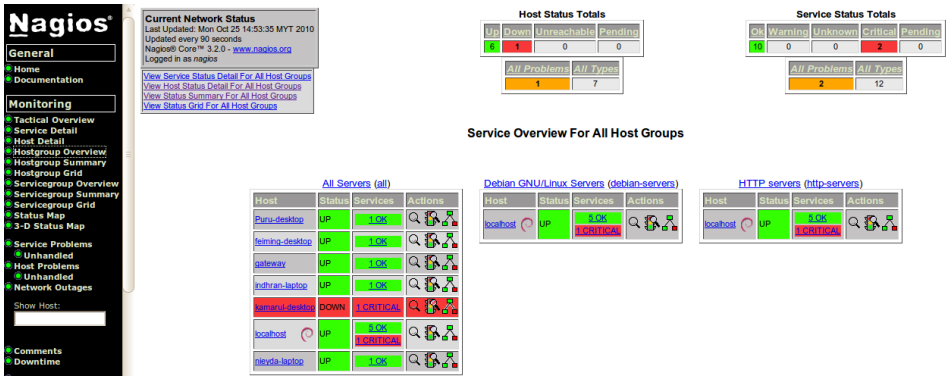


Figure 6.5

The host group and service group overview will display the hosts and services by group. As per example in Figure 6.5, the hosts are shown in groups of 'All Servers', 'Linux Servers' and 'HTTP Servers'. Status is also shown in green and red to differentiate between OK and Critical. The actions are meant to view

extended information, to view service details and to locate host on the map from the current page.

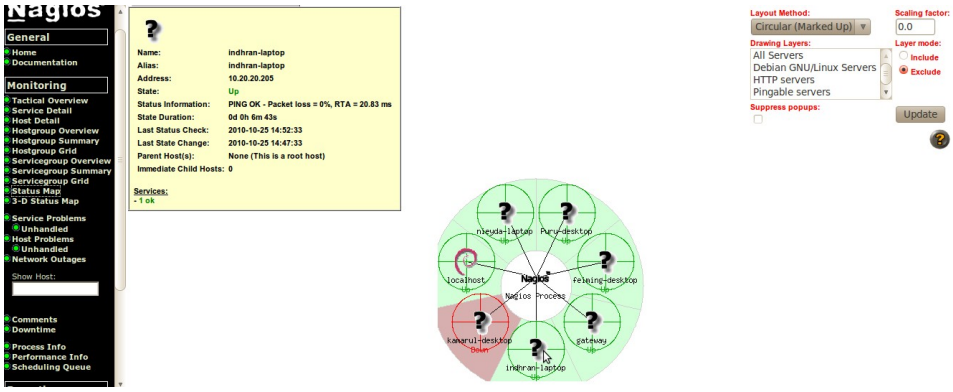


Figure 6.6

Figure 6.6 shows the status map of the defined hosts. This helps the system administrator to visualize the status of hosts and services being monitored by Nagios3. Use mouse-over of a host to receive a pop-up in the same page to show the host in detail.

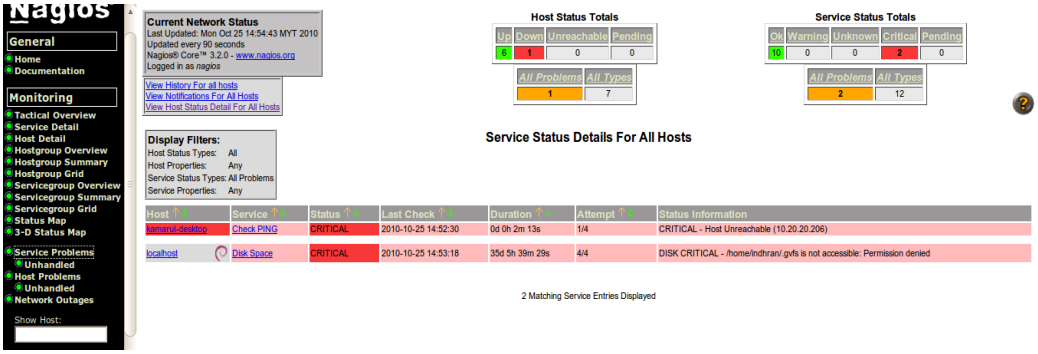


Figure 6.7

Service problems on Figure 6.7 produce a list of "problem" hosts on network that are causing network outages. This is useful to quickly identify problem sources. Hosts are sorted based on the severity of the outage they are causing.

The notifications under reporting is used to display host and service notifications that have been sent to various contacts. The output is basically a subset of the information that is displayed by the log file.