

Pandora v1.2



Pandora v1.2

First Edition(v1.2) Edition

Published September 11th, 2006

Copyright © 2006 Artica Soluciones Tecnologicas S.L, Sancho Lerena, Esteban Sanchez y otros.

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.1 or any later version published by the Free Software Foundation. A copy of the license is included in the section entitled “GNU Free Documentation License”.

Revision History

Revision 1.1 10 October 2006

Submitted.

Revision 1.0 11 Sept 2006

Submitted.

Revision 0.1 11 Sept 2006

First draft for review.

Table of Contents

1. Introduction to Pandora.....	1
1.1. Pandora. The Free monitoring system	1
1.2. Introducing Pandora.	1
1.3. What kind of systems/ services can be monitored?	3
1.3.1. Global architecture	4
1.4. Information gathering with Pandora agents	4
1.4.1. XML Data files	5
1.4.2. Pandora servers.....	7
1.4.3. Pandora console.....	7
1.4.4. Pandora database	8
1.5. Pandora 1.2 new features	8
1.6. About Pandora.....	9
2. Users.....	10
2.1. Profile manager	10
2.2. Adding a user	11
2.3. Deleting a user	14
2.4. Statistics	15
2.5. Messages to users	16
2.5.1. Messages to groups.....	16
3. Agents.....	17
3.1. Group Manager	17
3.2. Adding an agent	18
3.2.1. Assigning modules	19
3.2.2. Alerts	21
3.2.3. Agent module and agent's alert management.....	24
3.2.4. Agents group detail.....	25
3.3. Agent monitoring	26
3.3.1. Agent view.....	26
3.3.2. Accessing the data of an agent	27
3.3.3. Group details	32
3.3.4. Monitors view	33
3.3.5. Alert details	33
3.3.6. Data Export.....	34
3.3.7. Statistics.....	35
3.4. SNMP Console.....	36
3.4.1. SNMP Alerts	36
4. Incident management	37
4.1. Adding an incident	39
4.2. Incident follow up	40
4.2.1. Adding comments to an incident.....	42
4.2.2. Attaching files to an incident.....	43
4.3. Searching for an incident	44
4.4. Statistics	44

5. Events.....	47
5.1. Statistics	48
6. System audit	50
6.1. Statistics	51
7. Pandora Servers.....	52
8. Database Maintenance	53
8.1. DB Information	53
8.2. Manual purge of the Datadase.....	55
8.3. Agent's data purge.....	55
8.3.1. Debuging selected data from a module	55
8.3.2. Purging all the agent's data.....	56
8.4. Purging system data	57
8.4.1. Audit data purge	57
8.4.2. Event data purge	58
9. Pandora Configuration.....	60
9.1. Links.....	61
A. GNU Free Documentation License.....	62
A.1. 0. PREAMBLE	62
A.2. 1. APPLICABILITY AND DEFINITIONS	62
A.3. 2. VERBATIM COPYING.....	63
A.4. 3. COPYING IN QUANTITY	63
A.5. 4. MODIFICATIONS.....	64
A.6. 5. COMBINING DOCUMENTS.....	65
A.7. 6. COLLECTIONS OF DOCUMENTS	66
A.8. 7. AGGREGATION WITH INDEPENDENT WORKS.....	66
A.9. 8. TRANSLATION	66
A.10. 9. TERMINATION.....	67
A.11. 10. FUTURE REVISIONS OF THIS LICENSE.....	67
A.12. Addendum	67
B. GNU General Public License	69
B.1. Preamble.....	69
B.2. TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION.....	70
B.2.1. Section 0	70
B.2.2. Section 1	70
B.2.3. Section 2	70
B.2.4. Section 3	71
B.2.5. Section 4	72
B.2.6. Section 5	72
B.2.7. Section 6	72
B.2.8. Section 7	72
B.2.9. Section 8	73
B.2.10. Section 9	73
B.2.11. Section 10	73
B.2.12. NO WARRANTY Section 11	74
B.2.13. Section 12	74
B.3. How to Apply These Terms to Your New Programs	74

Chapter 1. Introduction to Pandora

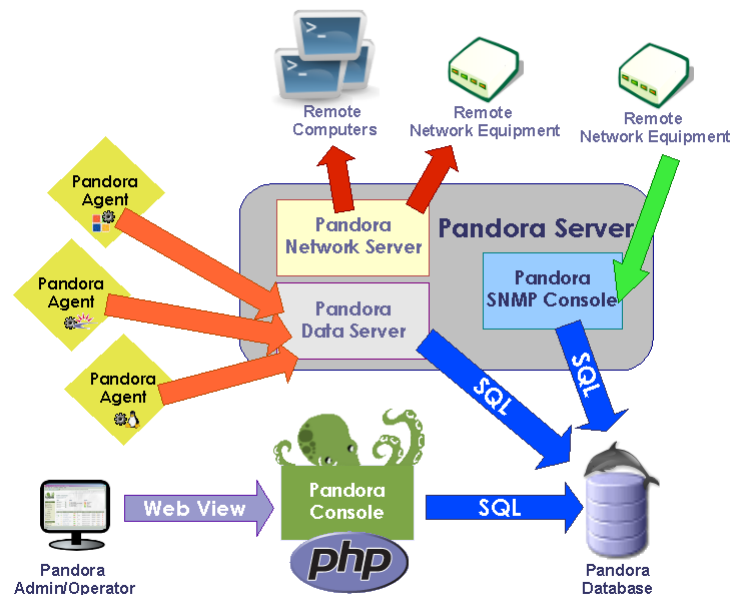
1.1. Pandora. The Free monitoring system

Pandora is a monitoring application to watch systems and applications. Pandora allows to know the status of any element of your business systems. Pandora watch for your hardware, your software, your multilayer system and of course your Operating System. Pandora could detect a network interface down and the movement of any value of the NASDAQ new technology market. If you want, Pandora could sent a SMS message when your systems fails... or when Google value low below 330\$.

Pandora adapt, like an octopus, to your systems and requirements, because has been designed to be open, modular, multiplatform and easy to customize.

1.2. Introducing Pandora.

Pandora is a monitoring tool that allows a system administrator to visually analyse the status and efficiency of Operating Systems, Servers, Applications and Hardware Systems - such as firewalls, proxies, databases, Web servers, tunnelling servers, routers, switches, processes, services, remote access servers, etc. - all integrated into an open and distributed architecture. Pandora can be implemented over any operating system, with specific agents for each platform. Pandora can also monitor any TCP/IP hardware system, such as load balancers, routers, switches, printers, etc.



Pandora architecture is formed of four main components:

- *Web Console*: Pandora's user interface. The user controls and operates the system with it. Several Web consoles can be implemented in a single system. The Web console is written in PHP, and rests on a database and a Web server. It is compatible with any platform - GNU/Linux, Solaris, Win2000, AIX, etc. However, the official supported platform is GNU/Linux.

The console permits the user to control the status of the agents, view statistical information, generate graphs and data tables, keep a system incident control, as well as to generate reports and change the alerts, agents, and user profile settings.

- *Server*: The core server is the receptor of the data packages and generates the alerts - it is the brain of the system. Several servers can work alongside for larger systems. It has been developed in Perl and works over any platform, although, the official platform is GNU/Linux.

The core server accesses Pandora database, which is shared with the Web server, and stores the processed data packages. Server executes as daemon, and processes the packages stored in its file system. Data is generated by the system agents. Despite the server's low system resources consumption and simple installation and operation, the core server is the most critical element of the system. The core server receives and processes the produced data, and fires the alerts and the events.

With the new Pandora 1.2 Network Server technology, Pandora Network Servers could monitorize remote systems using network resources like ICMP, TCP, UDP or SNMP Queries. Network Servers are acting itself like "Network Agents".

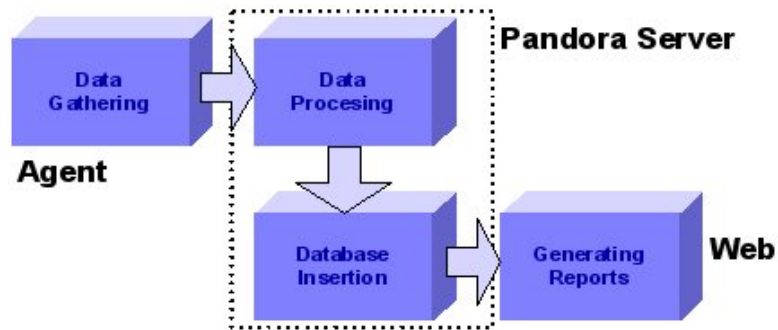
- *Central Database*: At the moment the system only supports MySQL. The central database keeps all the information Pandora needs to work - agent data, settings, user information, incidents, system settings, etc. The system can use a MySQL cluster to store the information, or a high disponibility solution for larger sytems.

This database can work with any of the platform officially supported by MySQL. Pandora can be implemented with MySQL versions 3.0 and 4.0, although the latest is recommended.

- *Pandora Agents*: They collect all the system's data. They are executed in each local system, although they can also collect remote information by intalling monitoring sytems for the agent in several different machines - called satellite agents.

They have been developed to work under a specific platform, making use of the specific tools of the used language: ShellScripting for Unix - which includes GNU/Linux, Solaris, AIX, HP-UX and BSD, as well as the Nokia's IPSO. Pandora agents can be developed in virtually any language, given its simple API and being open source. Windows agent are developed in a free development enviroment for C++ and uses the same interface and modularity than Unix agents.

The old agent for Windows platforms was developed on VBS Scripting language, and is deprecated with the new Pandora 1.2 windows agent.



1.3. What kind of systems/ services can be monitored?

At present, with Pandora any process or system that through a command returns a value can be monitored, as well as any value in any Operating System log file or similar. Some examples of already existing implementations can be the following ones:

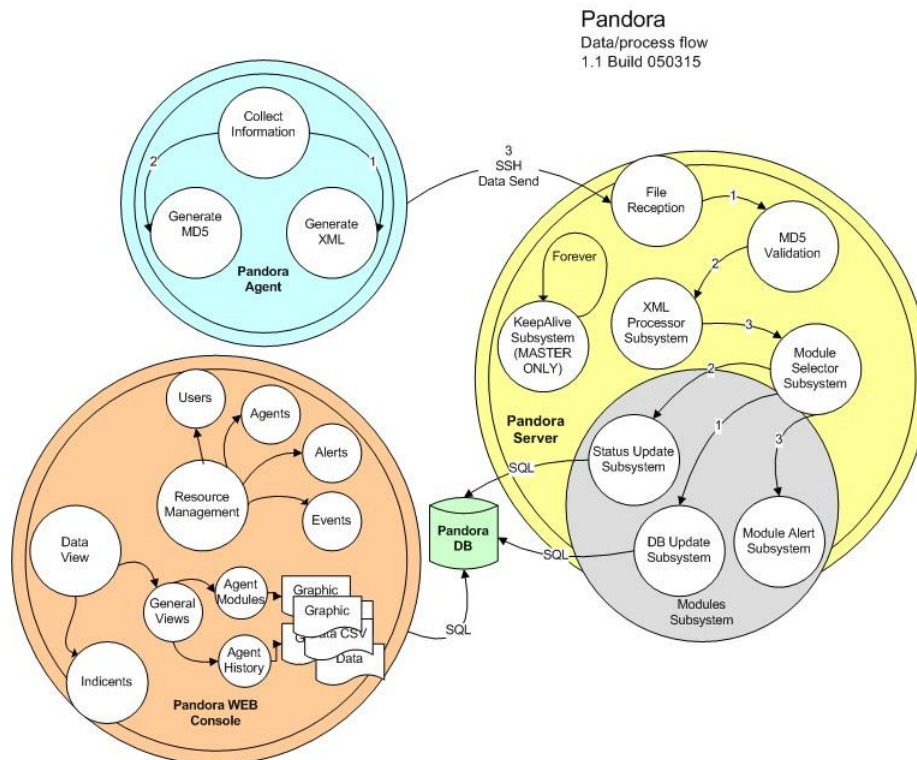
```

Number of connections (sessions) of Checkpoint FW-1
Number of NAT sessions of Checkpoint FW-1
Number of connections of Linux NetFilter / IPTables firewall
Number of FW-1 logged packets
Number of FW-1 dropped packets
Number of FW-1 accepted packets
State of High Availability in FW1 NG
Last policy installed in a Firewall-1 module
Synchronization state of the modules in FW1 NG
CPU of the system: idle, user and system
Number of processes of the system
Temperature of the CPU of a system
Value of a MS Windows registry entry
Queued jobs in a generic dispatcher
Memory of the system: free, swap, kernel Fw-1, cache
Percentage of free space on disc (for different partitions)
Messages processed by a mail gateway
Existence of a string in a text file
IP traffic (filtering based on the connections of the firewall)
Hits of pages in HTTP Servers (Apache, iPlanet, IIS, Netscape)
Percentage of erroneous packets in a Gateway
Connections established in a Remote Access Server (RAS)
Size of a file
Open sessions by a VPN server
  
```

MySQL Performance: Threads, queries, sessions...
 Snort system state
 Reported events by IDS (Snort) up to six levels of priority
 Network load
 Number of local Connections (TCP, UDP, Unix sockets)
 Detected viruses by a Web Antivirus Gateway
 ICMP latency time towards a host
 Rate of average transference in a file transfer tool
 Number of DNS requests attended by a server (including types)
 Number of FTP sessions attended by a FTP server
 (Generic) State of any active process / service in the system
 (Generic) State of any countable parameter of the system

1.3.1. Global architecture

Pandora 1.2 has changed many things from 1.1 version, but this graph representing Pandora architecture is very useful to understand in a single graph, all components.



1.4. Information gathering with Pandora agents

Pandora agents are based on native languages in every platform: scripts that can be written in any language. It's possible to reproduce any agent in any programming language and can be extended without difficulty the existing ones in order to cover aspects not taken into account up to the moment.

These scripts are formed by modules that each one gathers a "chunk" of information. Thus, every agent gathers several "chunks" of information; this one is organized in a data set and stored in a single file, called data file.

The process of transferring the data file from the agent to the server is made regularly at a defined time interval in the agent configuration file, `pandora_agent.conf`. It's possible to modify that parameter to not fill the database with non-relevant information, not to load the network or to not affect the system performance. The default interval is 300 (seconds), which is equivalent to five minutes. Minor values of 100 (seconds) are not recommended since host performance can be affected, besides loading excessively Database and the Operating System of Pandora Server. Pandora is not a real time system; it's an applications and systems general monitoring system in environments that are not critical at real time.

Packets transfers are made via SSH, with DSA authentication (although also RSA can be used). The process is completely safe since neither any password nor unencrypted confidential information is sent. Confidentiality, integrity and authentication of the connections between the agent and the server are ensured. In the Agents and Server Installation and Configuration guides, the process of generation of keys to do the automatic SCP transfer is detailed.

Also the transfer via FTP or any other file transfer system could be made, although SSH has been chosen for security and compatibility with most of the systems in the market.

Pandora Agents are thought to be executed from the agent from which they gather information, although the agents can gather information of accessible machines from the host where they are installed. In this case those agents are called "Satellite Agents". These Satellite Agents can use Telnet, SNMP or any other commands to get the information.

We can also have a host with several agents: Some that gather information from the accessible machines (acting as "satellite agents") and the Standard Agent that monitors the host where it's running.

1.4.1. XML Data files

The data file has the following syntax:

```
hostname.serialnumber.data
```

This is an XML file, and its name is the combination of the hostname where the agent runs, a different serial number for every data package and the extension .data that indicates that it's a data file.

We also have a control file for every data file:

```
hostname.serialnumber.checksum
```

This file has .checksum extension and contains a MD5 hash of the data file. This allows checking that the information has not been changed before being processed.

The XML data file generated by every agent is the core of Pandora. This file has the information gathered by the Agent. Its easy structure allows that any user could create it's own developments to be processed in Pandora, or use the included ones. An example of the information included into the data file is the following one:

```
<agent data os_name="SunOS" os_version="5.8" timestamp="300"
agent_name="pdges01" version="1.0">
  <module>
    <name>SSH Daemon</name>
    <type>generic_proc</type>
    <data>1</data>
  </module>
  <module>
    <name>FTP Daemon</name>
    <type>generic_proc</type>
    <data>0</data>
  </module>
  <module>
    <name>DiskFree</name>
    <type>generic_data</type>
    <data>5200000</data>
  </module>
  <module>
    <name>UsersConnected</name>
    <type>generic_data_inc</type>
    <data>119</data>
    <min>1</min>
    <max>250</max>
    <description>Users currently connected</description>
  </module>
  <module>
    <name>LastLogin</name>
    <type>generic_data_string</type>
    <data>slerena</data>
  </module>
</agent_data>
```

1.4.2. Pandora servers

With Pandora 1.2 version, you have three different types of servers:

- *Pandora Data Server*. This is a PERL application that processes the information sent by the agents. The agents send the XML data file via SSH and the server periodically verifies if it has new data files waiting to be processed. You can setup different data servers in different systems or in the same host (that will be different virtual servers).
- *Pandora Network Server*. This is a PERL application that execute network tasks like sending pings, TCP requests, SNMP requests and UDP request. When you assign an agent to a server, you are assigning to a network server, not a data server, so, this is very important that machines running network servers have "network visibility" to hosts assigned in network modules.

For example, if you create a module to make a ping check to 192.168.1.1 and assign this agent/module to a server in a 192.168.2.0/24 network without access to 192.168.1.0/24 module always report DOWN.

- *Pandora SNMP Server*. This is a PERL application that parse output from standard snmptrapd (we provide one binary for snmptrapd, but its possible you need to replace it with a binary that runs better in your system). This daemon receives SNMP traps, and Pandora SNMP Server stores in database and fire alerts assigned in Pandora SNMP Console.

Data are extracted from the data file, identifying origin, type and category. One classified, the data are inserted into the Database by the same Perl script.

Pandora Server can work in High Availability and/or Load Balancing. In a very big architecture, several Pandora Servers can be arranged simultaneously to be able to manage big volumes of information distributed by geographical or functional zones.

Pandora Server is always running (as a daemon) and permanently verifies if some element causes to fire an alarm. If so, it executes the action defined in the alarm, as to send a SMS, an email, to activate the execution of a SCRIPT or to send an HTTP form.

We could have several simultaneous servers, one of them is the Main Server or "Master Server " and the rest servers are "Slave Servers". The Master Server is the only one that verifies the alarms if any agent goes down. The server who receives the data file from the agent always fires the rest of alarms, defined in the agents' modules. This is also important if this server changes (due to configurations of high availability, load balancing or clustering).

1.4.3. Pandora console

The Web Console it's a web application that allows to see graphical reports, state of every agent, and to access to the information sent by the agent, to see every monitored parameter and to see its evolution throughout the time, to form the different nodes, groups and users of the system. It is the part that interacts with the final user, and that allows you to administer the system.

The Web Console is written in PHP and no plug-in, Flash, Java or ActiveX is needed to access the console, only a browser that supports HTML and CSS (IE5+ o Mozilla 4+). Pandora Web Console can run in several servers, the only thing you need is to access Pandora Database, where Pandora stores all the information.

1.4.4. Pandora database

Pandora uses a SQL Database to store all the information. Pandora maintains an asynchronous database with all the received data, making a temporary cohesion of everything what it receives and normalizing all the information from the different sources. Every Agent data module generates an entry of information for every data bundle, which implies that a real production system can have of the order of ten million of data, or information atoms.

This information is managed automatically from Pandora, carrying out a periodic and automatic maintenance of the database. This allows that Pandora should need neither any type of administration of database nor process attended by an operator or manager. This is made by a periodic purge of the past information over a date (by default 90 days), as well as a data compaction of the data that have more than, by default, 30 days.

1.4.4.1. Compacting data

Data stored by Pandora are useful to see evolutions regard through the time, to make statistics, to generate reports and to do capacity planning, as well as other tasks of statistical nature. For it, it isn't necessary to have all the data, but it's enough to have a representative sample, of smaller resolution, enough to carry out the task that is needed.

With that philosophy the compaction system has been constructed. If we have a sample of 9.000 elements, distributed during 90 days, for example, Pandora is going to take the data of last month, which would be 3.000 elements and it's going them to compress them in 300. In the graphs they will practically be seen equal, which it will serve us for the reports, statistics and other tasks. This is made by means of interpolation in temporary strips, in a totally automatic and periodic way, without the user or the administrator must himself or herself worry about it.

1.5. Pandora 1.2 new features

Alert system. Now its possible to define a "minimun" and "maximum" limit to fire an alert, just to delete "noisy" data that fires false positives.

Network Subsystem. Now its possible to monitor and analyze data using remote network tools, without using agents, from the new Pandora Network Server component. All management are made from Pandora Console, and now you will be able to make ICMP checks (Ping), size network latency, get all types of SNMP values (including scanning MIB), and makes TCP/UDP connections to check ports, and test text applications, sending texts and waiting for a specific response.

Module groups. Modules now could be grouped using a new "module groups".

Network data refresh on demand. Could be for each module or using a "global group refresh", forcing Pandora Network Servers to refresh all network modules inside a group.

Online contextual help, for Pandora WEB Console.

New Pandora server infrastructure.

New SNMP trap console to receive SNMP traps and assigning alerts.

Internal messaging system, to notify events to Pandora users.

Agent detail view autorefresh

New main agent group view

Improved database management system, that allows to manage much more data.

1.6. About Pandora

Pandora is a project initiated and mainly developed by Sancho Lerena, at present other people is working on it: Raul Mateos, David Villanueva, Esteban Sanchez, Jose Navarro and Jonathan Barajas. We want to give thanks for many other people who help us with translation, graphic design, bugs reporting and interesting ideas.

Pandora is Free Software, and is published under GPL Licence. In order to know the last features, go to the official web site of the project in <http://pandora.sourceforge.net>.

Chapter 2. Users

The definition of a user is based on the user's daily activity. One or more profiles can be assigned to a single user

A profile is a list of actions a user can or cannot perform on a given group, e.g. "view incidents", "database management", etc

Each user is given a number of groups of agents he/she has permission to access, as well as the administrative profile he/she will have in each group. Each user can belong to one or more groups, with an assigned profile for each of them.

Agent belongs to a group and only one, sharing the group with agents of similar characteristics. Groups also contain incidents.

Summarizing: User profiles in Pandora define which users can access Pandora as well as what each user can do. Groups define elements in common among various users. Each user could be in one or more groups at any one time. Each group has user profiles which are defined and attached to it. A profile is a list of things a user can do, such as view incidents, manage database or other.

2.1. Profile manager

Pandora's profile manager is used to assign specific profiles to each user. A hierarchy of users is so created, structured by the user's profile within the company. With this system different security levels can be implemented: read-only users, agent group coordinators or system administrators.

A profile is created from the Profile Manager tool in the Administration menu. There are five predefined profiles:

- Operator (Read)
- Operator (Write)
- Chief Operator
- Group coordinator
- Pandora Administrator

To create a new profile click on "Manage Profiles" > "Create Profile" in the Administration Menu

Profile management

Profiles defined in Pandora

Profiles	IR ★	IW ★	IM ★	AR ★	AW ★	LW ★	UM ★	DM ★	LM ★
Operator (Read)	✓			✓					
Operator (Write)	✓	✓		✓					
Chief Operator	✓	✓	✓	✓					
Group coordinator	✓	✓	✓	✓	✓	✓	✓		
Pandora Administrator	✓	✓	✓	✓	✓	✓	✓	✓	✓
Database Administrator								✓	
Alert manager									✓
User manager							✓		
Pandora Manager							✓		
Agent Editor				✓	✓				
Module Alert editor				✓	✓	✓			

Any of the following roles can be assigned to a new profile:

- View incidents (IR)
- Edit incidents (IW)
- Manage incidents (IM)
- View agents (AR). To view agents as well as the events generated by them
- Edit agents (AW). To modify then agent's modules
- Edit alerts (LW). To modify the alerts assigned to an agent
- Manage users (UM). To modify users and their roles
- Manage DB (DM). To modify the configuration and data of the database (Global)
- Manage alerts (LM). To define new alerts (Global)
- Manage Pandora (PM). To modify general system settings

2.2. Adding a user

A user is added clicking on "Manage Users">"Create user" in the Administration Menu

To create a new user it is necessary to, at least, fill in the user ID, the password (twice) and Pandora's global profile.

A global profile for a user maybe Administrator or Standard User.

A user with an "Administrator" profile will have the highest security privileges in Pandora.

User management

Create user

User ID	<input type="text"/>
Real name	<input type="text"/>
Password	<input type="password"/>
Password - confirmation	<input type="password"/>
E-Mail	<input type="text"/>
Telephone	<input type="text"/>
Global Profile	Administrator <input type="radio"/> ★ Standard user <input checked="" type="radio"/> ★
Comments	<div></div>

Create

Profiles defined in Pandora

Profiles	IR ★	IW ★	IM ★	AR ★	AW ★	LW ★	UM ★	DM ★	LM ★
Operator (Read)	✓			✓					
Operator (Write)	✓	✓		✓					
Chief Operator	✓	✓	✓	✓					
Group coordinator	✓	✓	✓	✓	✓	✓	✓		
Pandora Administrator	✓	✓	✓	✓	✓	✓	✓	✓	✓
Database Administrator								✓	

Profiles must be assigned for each of the groups a new "standard" profile user can access, once the user is created and his configuration updated.

User management

Update user

User ID	<input type="text" value="test"/>
Real name	<input type="text"/>
Password	<input type="password" value="*****"/>
Password - confirmation	<input type="password" value="*****"/>
E-Mail	<input type="text" value="none@none.com"/>
Telephone	<input type="text" value="3243243"/>
Global Profile	Administrator <input type="radio"/> Standard user <input checked="" type="radio"/>
Comments	<div><div></div></div>
Group(s) available	<input type="text" value="None"/>
Profiles	<input type="text" value="Agent Editor"/>

Profiles/Groups assigned to this user

Comms / Agent Editor



All / Operator (Write)




Profiles defined in Pandora

Profiles	IR	IW	IM	AR	AW	LW	UM
Operator (Read)	✓			✓			
Operator (Write)	✓	✓		✓			

A user profile is deleted by clicking on the delete icon on the right hand side of the profile.

2.3. Deleting a user

A user is deleted by clicking on the delete icon  on the right hand side of the user. The list of users is accessed through the "Manage Users" option in the Administration menu.

User management

Users defined in Pandora

UserID	Last contact	Profile	Name	Delete
sophus	2005-04-28 12:41:37	 ★	Sophus Lie	
test1	2005-04-17 19:40:23	 ★	Test user	
demo	2005-04-28 12:40:57	 ★	Demo User	
sergio	2005-02-27 17:51:11	 ★	Sergio Iglesias	
slerena	2005-04-28 13:01:53	 ★	Sancho Lerena	
david	2005-04-21 16:40:22	 ★	David Villanueva	
test	2005-04-20 16:07:46	 ★		
alex	2005-04-24 12:24:01	 ★	Alex Arnal	

Create user

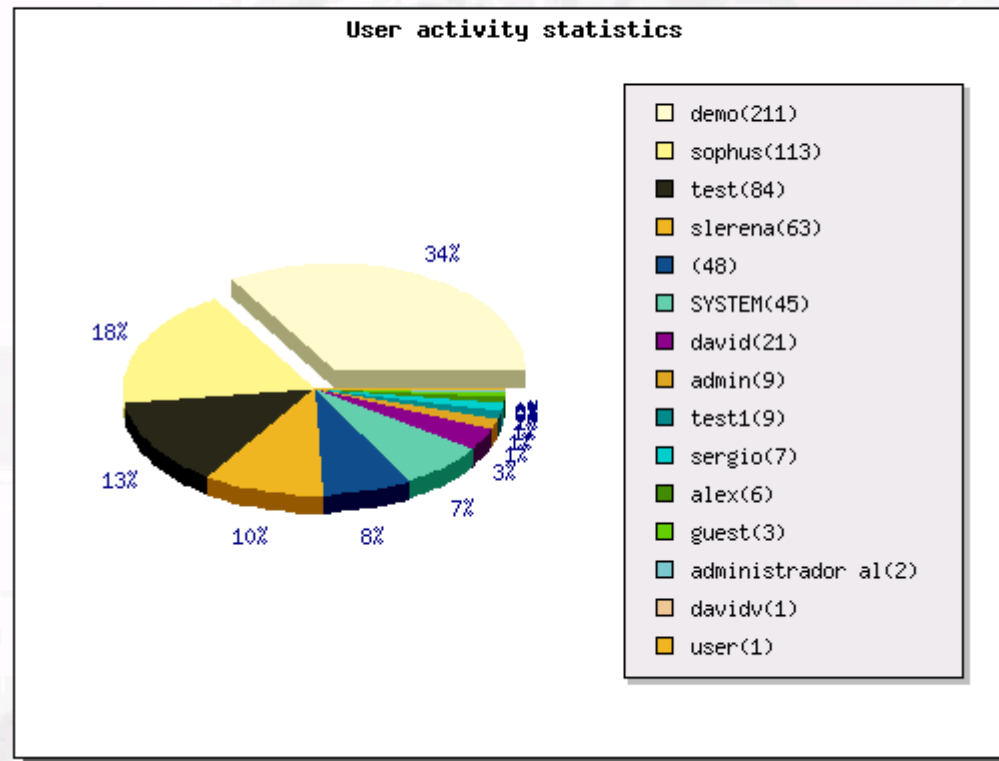
2.4. Statistics

The user activity statistics show a graph with the activity of the user, being the number of events the audit has generated for each user. The number of events of a user usually reflects the user's activity.

Click on "View Users" > "Statistics" in the Operation menu to show this graph:

Users defined in Pandora

User activity statistics



2.5. Messages to users

To create a new message to other user, go to "Messages" section in the Operation menu. You can also read the received messages, but the sent messages are not stored.

2.5.1. Messages to groups

From "Messages" > "Messages to groups" section in the Operation menu you can send messages to groups of users. The sent messages will not be stores.

Chapter 3. Agents

The agents collect information. They could be a "real" agent, based on a software agent, or a network agent, a non-physical agent, without need of installing any software, that execute network tasks in Pandora Network servers, and showing information on console inside an Agent.

For agents who need to install software onto remote systems, public key of the machine to be monitored needs to be copied onto Pandora Data server to be able to collect data, as it's specified in detail in Pandora Install documentation.

Data collected from the agents are stored in small pieces of information called "modules". Each module store only a kind of data. Value of each module is the value of one monitored variable. The agent must be activated in Pandora's server and a group assigned to the agent. The data starts then been consolidated in the database and can be accessed.

A network agent NEEDs to be assigned to a Network Server to execute network tasks. If you cannot see any Network Servers it's because you has not executed any Network Servers. Please configure and run a Network Server before trying to assign a network module to an Agent.

With Pandora Console, user is capable to:

- View the agent status
- Access to the collected information
- Access the monitored values and its evolution in time
- View graphic reports
- Configure Alerts
- Configure modules. Define max and minumun valid values for each module, set a comprehensive description or even change module name (remember that module name must be the same in console and in software agent configuration).
- Export tabular data in CSV format.


3.1. Group Manager

Pandora groups are common to agents, incidents and profiles. Groups are added in "Manage Profiles" > "Manage Groups", Administration menu.



There are several default groups defined in Pandora. You also can create your own (please use given icons or edit and add your own icons). You can also modify default ones.

A group is added by clicking "Create group" and assigning a name to it.

A group is deleted by clicking the delete icon  in the right hand side of each group.

3.2. Adding an agent

You can define new agents. Once defined in Pandora console, its ready to receive data from a Software agent (old agents, based on software installed in a remote machine), or from Network Agents (assined to a Network Server who run network tasks to monitorize remote systems). You also mix both types of module in the same agent.

Please remember that a network agent NEEDs to be assigned to a Network Server to execute network tasks. If you cannot see any Network Servers it's because you has not executed any Network Servers. Please configure and run a Network Server before trying to assign a network module to an Agent.

An agent is added in "Manage Agents" > "Create agent" in the Administration menu.

Agent Configuration

Create agent

Agent name

IP Address

Group

Interval

OS

Description

Module definition Learn mode ☐ Normal mode ☒

Disabled Disabled ☐ Active ☒

Create

To add a new agent the following parameters must be configured:

- **Agent Name:** Name of the agent. This and the "agent name" parameter in Pandora's agent.conf file *must have the same value*. By default agent takes hostname of the machine where it's running.
- **IP Address:** IP address of an agent. An agent can share its IP address with other agents. Its only for informational purposes. In network agents its useful, because use this IP address for all new network module definition by default.
- **Group:** Pandora's group the agent belongs. In this version of Pandora, an agent only can belong to a group.
- **Interval:** Execution interval of an agent. It is the time elapsed in seconds, between two executions. An agent could have a defined interval, but could have modules with different (bigger or smaller) intervals. An agent its considered "down" (not responding) when Pandora servers (any of them) has no contact with agent in Interval x 2 seconds.
- **OS:** The Operating System to be monitored. The supported Operating Systems are: AIX, BeOS, BSD, Cisco, HPUX, Linux, MacOS, Other, Solaris, Windows.
- **Description:** Brief description of an agent.
- **Module definition:** There are two modes for a module:
 - **Learning mode:** All the modules sent by the agent are accepted. If modules are not defined, they are automatically defined by the system. It is recommended to activate the agents in this mode and change it once the user is familiar with the system.
 - **Normal mode:** The modules in this mode must be configured manually. The self definition of the modules is not allowed in this mode.
- **Disabled:** This parameter shows if the agent is activated and ready to send data or deactivated. The deactivated agents don't appear in the user views.

3.2.1. Assigning modules

Pandora's agents use the operating system own commands to monitor a device. Pandora's server will store and process the output generated by those commands. The commandos are called "modules".

If the agent had been added in "normal mode", the modules to be monitored should have been assigned. Those modules must be configured in the agent configuration file.

The modules to be processed by Pandora's server are assigned in the "Manage Agents" option, Administration menu. A list with all the agents in Pandora will be shown here.

You'll get a form with all the agent's settings when the agent name is clicked. In the same screen there is a section to assign modules.

The screenshot shows a web form titled "Module association form". It includes the following fields:

- Module type:** A dropdown menu currently set to "generic_data".
- Module name:** A text input field.
- Maximum:** A numeric input field.
- Minimum:** A numeric input field.
- Comments:** A large text area for notes.
- Update:** A button at the bottom right to save the configuration.

A Pandora module could be from different types:

- *generic_data*, numeric data type.
- *generic_data_inc*, incremental numerical data type. It stores data resulting from difference between last agent data and actual data.
- *generic_data_proc*, Boolean data type: 0 means False or "bad values", and 1 means True or "good" value. Generic Proc types are also called "monitors" because could say if something is "ok" or is "wrong". Are displayed in agent view as little lamps. Red if 0, Green is 1.
- *generic_data_string*, Alphanumeric data type (text string, max. 255 characters).
- *generic_icmp* get network latency in milliseconds for remote system.
- *generic_icmp_proc*, makes a "ping" to remote system. Report 0 if system is not reachable or not responding.
- *generic_tcp_proc*, makes a "tcp" ping to remote systems and reports "1" if a listing port is responding. Optionally, you may pass parameters in "TCP SEND" (you can use the macro ^M to send carriage returns) and wait to receive string defined in "TCP RECEIVE". If Pandora Network Server received TCP RECEIVE string, it returns 1 (ok), else return 0 (wrong).
- *generic_tcp_data*, *generic_tcp_string*, *generic_tcp_inc*, gets numerical data, string data or incremental data from TCP open port. If cannot connect, no value returned.

- *generic_snmp types*: they obtain information using SNMP interface. If you enter SNMP community, and IP address, you can walk SNMP MIB from target using SNMP v1 protocol, and all MIB variables will be listed to allow you choose one. You also can enter MIB using numerical OID or human - comprehensive format.
- *generic_ucp_proc*, makes a "udp" ping to remote systems and reports "1" if a listening port is responding and 0 if are not responding.

Pandora modules have some other fields that modify their behaviour:












- *Maximum*: Upper threshold for the value in the module. Any value above this threshold will be taken as invalid and the whole module will be discarded.
- *Minimum*: Lower threshold for the value in the module. Any value below this threshold will be taken as invalid and the whole module will be discarded.
- *Comments*: Comments added to the module.

Additionally if you are defining a network module, you also have more fields related to Network options:



•

All the modules to be monitored by an agent can be reviewed by accessing the agent in the "Manage Agents" option, Administration menu.

Assigned modules

Module name	Module type	Description	Max/Min	Action
router_alive	generic_proc	Its the Router Alive ?	NA / NA	 
router_out	generic_data_inc	Router OUT Packets	50000000 / 0	 
router_discard	generic_data_inc	Autogenerated using learn mode	NA / NA	 
wlan_lat	generic_data	AUTO: ICMP Latency for 213.172	1000 / 0	 
agent_keeplive		Agent keeplive monitor	NA / NA	
router_in	generic_data_inc	Router IN packets	50000000 / 0	 

In this screen the modules can be:

- Deleted by clicking 
- Edited by clicking 

However, the type of data of the module can't be modified.

3.2.2. Alerts

An alert is Pandora's reaction to an out of range module value. The Alert can consist in sending an e-mail or SMS to the administrator, sending a SNMP trap, write the incident into the system syslog or Pandora log file, etc. And basically anything that can be triggered by a script configured in Pandora's Operating System.

3.2.2.1. Adding an Alert







The existing Alerts are accessed by clicking on the "Manage Alerts" option, Administration menu.

There are 6 default types of Alerts:

- *eMail*. Sends an e-mail from Pandora's Server
- *Internal audit*. Writes the incident in Pandora's internal audit system
- *LogFile*. Writes the incident in the log file
- *SMS Text*. Sends an SMS to a given mobile phone
- *SNMP Trap*. Sends a SNMP Trap
- *Syslog*. Sends an alert to the Syslog

Alert configuration

Alerts defined in Pandora

Alert name	Description	Delete Alert
eMail	Send email from Pandora Server. mail is a default command on all "standard" Unix systems, using: <code>_field1_</code> as destination email address, and <code>_field2_</code> as subject for message... <code>_field3_</code> as text of message.	
Internal Audit	This alert save alert in Pandora internal audit system. Fields are static and only <code>_field1_</code> is used.	
LogFile	This is a default alert to write alerts in a standard ASCII plaintext log file in <code>/var/log/pandora_alert.log</code>	
SMS Text	Send SMS via e-mail gateway. Use field1 for a short SMS text (35 chars) and field 2 for text message (full SMS)	
SNMP Trap	Send a SNMPTRAP to 192.168.0.4. Please review config and adapt to your needs, this is only a sample, not functional itself.	
Syslog	Uses field1 and field2 to generate Syslog alert in facility "daemon" with "alert" level.	

Create alert

An Alert is deleted by clicking on the delete icon  placed on the right hand side of the Alert. A new customised Alert can be created clicking in "Create Alert".

The values "_field1_", "_field2_" and "_field3_" in the customised Alerts are used to build the command line that the machine where Pandora resides will execute - if there were several servers, the one in Master mode.

Alert configuration

Create alert

Alert name

Command

Description

Create

When a new Alert is created the following field must be filled in:

- *Alert name*: The name of the Alert
- *Command*: Command the Alert will trigger
- *Description*: Description of the Alert

In 'Command' data field these variables are used to build the command line that the machine where Pandora resides will execute - if there were several servers, the one in Master mode, replacing at runtime:

- *_field1_*: Field #1, usually assigned as username, e-mail destination or single identification for this event
- *_field2_*: Field #2, usually assigned as short description of events, as subject line in e-mail
- *_field3_*: Field #3, a full text explanation for the event
- *>_agent_*: Agent name
- *_timestamp_*: A standard representation of date and time. Replaced automatically when the event has been fired
- *_data_*: The data value that triggered the alert

3.2.2.2. Assigning Alerts

The next step after an Agent has been added, its modules have been configured and the alerts have been defined, it is time to assign those Alerts to the agent.

This is done by clicking on the Agent to be configured on the "Manage Agents" option, Administration menu. The Alert Assignment form is placed at the bottom of that page.

Alert association form

Alert type:

Max value: Min value:

Description:

Field #1 (Alias, name):

Field #2 (Single Line):

Field #3 (Full Text):

Time threshold: Max. Alerts Fired:

Assigned module:

Update

To assign an Alert the next fields must be filled in:

- *Alert type*: This can be selected from the list of alerts that have been previously generated.
- *Maximum Value*: Defines the maximum value for a module. Any value above that threshold will trigger the Alert.
- *Minimum Value*: Defines the minimum value for a module. Any value below that will trigger the Alert.
- *Description*: Describes the function of the Alert, and it is useful to identify the Alert amongst the others in the Alert General View.
- *Field #1 (Alias, name)*: Define the used value for the "_field1_" variable.
- *Field #2 (Single Line)*: Define the used value for the "_field2_" variable.
- *Field #3 (Full Text)*: Define the used value for the "_field3_" variable.
- *Time threshold*: Minimum duration between the firing of two consecutive alerts, in seconds.
- *Max Alerts Fired*: Maximum number of alerts that can be sent consecutively.
- *Assigned module*: Module to be monitored by the alert.

All the alerts of an agent can be seen through "Manage Agents" in the Administration menu and selecting the agent.

3.2.3. Agent module and agent's alert management

It might happen that the user finds that modules and alerts configured for an agent would be repeated in a new agent.

In order to simplify the administrator's job Pandora offers the option of copying modules and alerts defined in an agent to be assigned to another.

The screen is accessed through "Manage Agents" > "Manage Config.", in the Administration menu:

Source Agent menu permits the selection of the agent where the needed modules and/or alerts reside. The "Get Info" button shows the modules for that agent in the Modules list box.

Copy process is performed to copy the module and/or alert configuration from the selected source agents to the selected destination agents. Several agents can be selected, pressing CTRL and the mouse right button simultaneously. The two tick boxes at the top of the form will be used to specify if the configuration to copy is from modules and/or from alerts.

Deletion process is performed to delete the configuration of the destination agents, in the multiple selection list box. Several agents can be selected at a time, and the tick boxes at the top of the form indicate whether it is the modules or the alerts configuration what is to be deleted. The application will prompt to confirm the deletion, as once deletion is performed, the data associated to them will also be deleted.

3.2.4. Agents group detail

Once you have configured your groups and agents, you can see the status of the groups of agents through "View Agents", in the Operation Menu.

If you pass the mouse over any group image, you'll see the number of agents of that group as well the number of monitors, organized by status.

By pressing the icon  at the right of any group image, you will update the info of that group.

3.3. Agent monitoring

When the agents start the data transmission to the server, and it is added in the Web console, Pandora processes and inserts the data in the Database. The data are consolidated and can be accessed from the Web console, either as row data or as graphs.

3.3.1. Agent view

All the Agents can be accessed from the Operation menu. From here the status of the agents can be quickly reviewed thanks to a simple system of bulbs and coloured circles.

Pandora Agents

Overview

All ● - Alert fired ● - Alert not fired

Agent	OS	Interval	Group	# Modules	Agent Status	Alerts	Last Contact
AIX		300	All	0 / 0	?	●	2004-01-01 00:00:00
Iris		300	Servers	18 / 7	●	●	2005-04-28 13:44:42
Router		300	Comms	5 / 1	●	●	2005-04-28 13:48:04
Serv_R1		300	Comms	3 / 3	●	●	2005-04-28 13:43:56
Serv_R2		300	Other	0 / 0	●	●	2005-04-28 13:43:41
box02		300	Workstations	8 / 2 / 2	?	●	2005-04-27 19:20:03
Daeva		300	Workstations	10 / 2	?	●	2005-04-27 22:44:45
winbox01		300	Workstations	9 / 3 / 2	●	●	2005-04-28 13:46:47
Solaris_Box		300	Applications	0 / 0	?	●	2004-01-01 00:00:00

● - All Monitors OK
 ● - At least one monitor fails
 ● - Change between Green/Red state
● - Agent without monitors
 ● - Agent without data
 ? - Agent down

The list of agents shows all the relevant the information in the following columns:

Agent: Shows the agent's name.

SO: Displays an icon that represents the Operating System.

Interval: Shows the time interval (seconds) in which the agent sends data to the server.

Group: This is the group the agent belongs to.

Modules: Under normal circumstances this field shows the values representing the number of modules

and the number of monitors, both in black. If the status of a monitor changes to "incorrect", one additional number is shown: the number of modules, the number of monitors and the number of monitors with "incorrect" status, all in black save the last one.

Status: Shows the "general" status of the agent through the following icons:



All the monitors OK. It's the ideal status.



No defined monitors. Sometimes nothing is monitored that could be right or wrong, and only numeric or text data is reported.



At least one of the monitors is failing. Usually we want to avoid this, and keep our systems in a healthy green colour.



The agent doesn't have any data. New agents with an empty data package can have this status.



Colour shifting from green to red. This icon indicates that the agent has just changed its status, from 'All OK' to 'we have a problem'.



When an agent is down or there is no news from it for 2 times the Interval value in seconds. Usually it is due to a communication issue or a crashed remote system.


Alerts: Shows if any alerts have been sent through the following icons:




No alerts have been sent.



When at least one alert has been sent within the time threshold of the alert.

Last contact: Shows the time and date of the last data package sent by the agent, using a progress bar, according to value of the interval. If you see the image , the agent has not send data during the interval. Passing the mouse over the image will show you the last contact in time and date format.





Note: The icon  is only visible if you're an administrator and it's a link to the "Manage Agents" > "Update Agent" option in the Administration menu.

3.3.2. Accessing the data of an agent

When an agent is accessed, by clicking on its name, all the information related to that agent is displayed.




































3.3.2.1. Agent general info

This shows the data introduced when the agent was created and the total number a data packages the agent has sent.

Pandora Agents	
Agent general information	
Agent name ::	Router - 
IP Address ::	192.168.0.1
OS ::	 - Cisco v2.4.29
Interval ::	300
Description ::	ADSL Router
Group ::	Comms
Agent Version ::	1.1.0rc1
Total packets ::	24795

3.3.2.2. Last data received

This is the description of all the agent modules been monitored.

Display of last data chunk. Sent by agent at (remote time): 2005-04-28 13:52:51					
Module name	Module type	Description	Data	Graph	Raw Data
wlan_lat	generic_data	AUTO: ICMP Latency for 2	87	   	  
router_alive	generic_proc	Its the Router Alive ?	1	   	  
router_in	generic_data_inc	Router IN packets	3382574	   	  
router_discard	generic_data_inc	Autogenerated using lear	0	   	  
router_out	generic_data_inc	Router OUT Packets	10025384	   	  

In this list the module information is shown in the following columns:

Module name: Name given to the module in the agent's config file.

Module type: Type of module as described in Assigning Modules section.

Description: Description given to the module in the agent's config file.

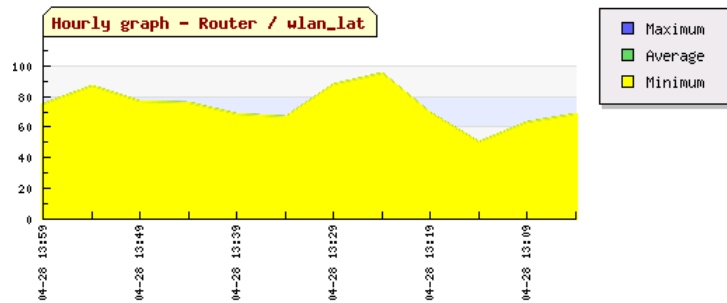
Data: Last data sent by the agent.

Graph: Monthly(M), Weekly(W), Daily(D) and Hourly(H) graphs are generated with the data sent by the agent against time.

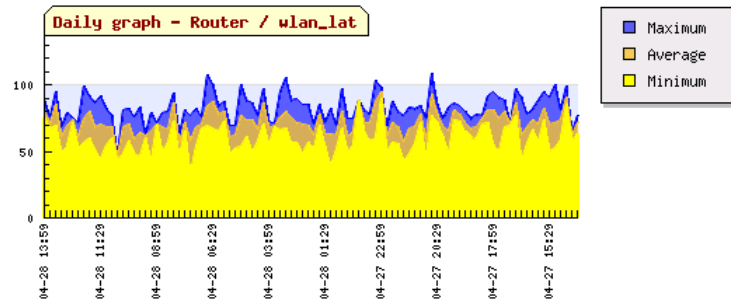
On the left hand side of the graph the newest data is represent, and on the right had side the oldest.

The generated graphs are:

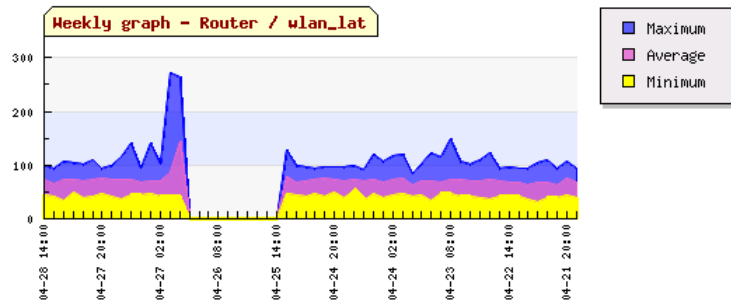
- Hourly graph (H) covers a 60 minute interval




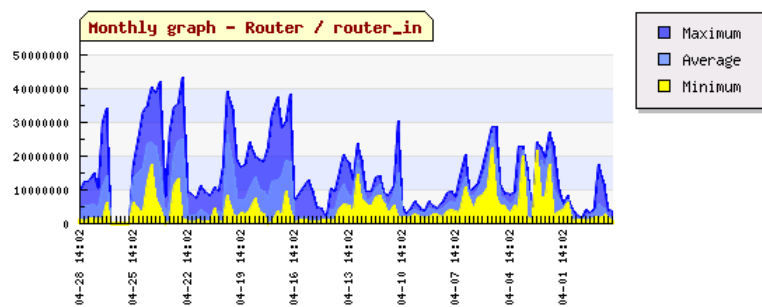
- Daily graph (D) covers a 24 hour interval




- Weekly graph (W) covers a 7 day interval



- Monthly graph () covers a 30 day interval



Raw Data: This is the raw data sent by the agent

-  Last month








-  Last week

-  Last day

3.3.2.3. Complete list of monitors

This is the description of all the monitors defined by the agent

Full list of Monitors

Agent	Type	Module name	Description	Status	Last contact
Iris	generic_proc	NFS_Daemon	NFS Daemon check		2005-04-28 13:59:57
Iris	generic_proc	DHCP_Server	Autogenerated using learn mode		2005-04-28 13:59:58
Iris	generic_proc	FTP_Daemon	FTP Daemon check		2005-04-28 13:59:57
Iris	generic_proc	sshDaemon	Autogenerated using learn mode		2005-04-28 13:59:57
Iris	generic_proc	DNS_Daemon	Autogenerated using learn mode		2005-04-28 13:59:57
Iris	generic_proc	apache	Autogenerated using learn mode		2005-04-28 13:59:57
Iris	generic_proc	MLDonkey	MLDonkey daemons		2005-04-28 13:59:57

The list shows the information about the monitors in the following columns:

Agent: Agent where the monitor is defined.

Type: Data type of the monitor. For a monitor this value is always of the generic_proc type.

Module name: Name given to the module when it was created.

Description: Description given to the module in the agent's config file.

Status: The table shows the agent status through the following icons:



The monitor is OK







The monitor is failing

Last contact: Shows the time and date of the last data packaged received from the agent

3.3.2.4. Complete list of alerts

This is the description of all the alarms defined in the agent

Full list of Alerts

ID	Type	Description	Last fired	Times Fired	Status
Iris	SMS Text	Apache down !	2001-01-01 00:00:00	0	
Iris	eMail	MLDonkey daemon down	2005-04-26 20:14:19	0	
Iris	eMail	Pandora agent shutdown	2005-04-04 21:39:35	0	
Iris	SMS Text	Disk full on /STORE partition	2005-04-24 20:06:15	0	

The monitor information is shown in the list divided in the following fields:

ID: Agent where the alert has been defined.


Type: Type of alert.

Description: Description given to the alert when it was created.

Last fired: The last time the alert was executed.

Times Fired: Number of times the alert was launched.

Status: Shows if the alert has been sent through the following icon:

 No alerts have been sent

 At least one alert has been sent

3.3.3. Group details

The groups configured in Pandora can be accessed through "View Agents">"Group detail" in the Operation menu. The group details can be reviewed quickly thanks to a system of coloured bulbs.

Pandora Agents

Agents Group detail

Group	Agents	Monitors	Status	Ok	Fail	Down
Servers	1	7		7	0	0
Other	1	0		0	0	0
Comms	2	4		4	0	0
Workstations	3	5		1	4	1
Applications	1	0		0	0	1

 - All Monitors OK
 - At least one monitor fails
 - Agent down
 - Agent without monitors


The groups are displayed ordered by the following columns:


Groups: Name of the group


Agents: Number of agents configured in the group.


Monitors: Number of monitors configured in the group.

Status: The status is described through the following icons:

 All monitors are OK.

 At least one monitor has failed.

 At least one monitor is down and there is no contact with it.

 This Agent doesn't have any monitor defined.

OK: Number of monitors that are OK.

Failed: Number of failing monitors.

Down: Number of down monitors.

3.3.4. Monitors view

The description of all the monitors defined in the server can be viewed from the "View Agents" > "Monitor detail" option in the Operation menu.

Pandora Agents

Detailed monitor view

All

Agent	Type	Module name	Description	Status	Last contact
Iris	generic_proc	NFS_Daemon	NFS Daemon check		2005-04-28 14:05:06
Iris	generic_proc	DHCP_Server	Autogenerated using learn mode		2005-04-28 14:05:07
box02	generic_proc	GAIM	AUTO:		2005-04-28 14:02:16
box02	generic_proc	MLDonkey_Sancho	AUTO:		2005-04-28 14:02:15

In this list all the monitors appear in a similar way as in the individual view, but now they are shown all together. This allows a deeper analysis of each monitor.

3.3.5. Alert details

The description of all the alerts defined in the server can be viewed from the "View Agents" > "Alert Details" option in Operation menu.

Pandora Agents

Detailed alert view

All ● - Alert fired ● - Alert not fired

ID	Type	Description	Last fired	Times Fired	Status
Iris	SMS Text	Apache down !	2001-01-01 00:00:00	0	●
Iris	eMail	MLDonkey daemon down	2005-04-26 20:14:19	0	●
Iris	eMail	Pandora agent shutdown	2005-04-04 21:39:35	0	●
Iris	SMS Text	Disk full on /STORE partition	2005-04-24 20:06:15	0	●
Router	eMail	Router down	2005-04-26 17:27:20	0	●
Router	eMail	Latencia excesiva	2005-04-26 17:48:00	0	●
Router	eMail	Agent shutdown	2005-04-04 21:39:35	0	●
Serv_R1	SMS Text	Problemas sincronizacion DNS ppp0	2005-04-27 20:52:17	0	●

In this list all the alerts appear in a similar way as in the individual view, but now they are shown all together. This allows a deeper analysis of each alert.

3.3.6. Data Export

The Data Export tool can be found in the "View Agents" > "Export data" option in the Operation Menu.

Three parameters need to be configured for exporting data: the agent where data resides, the modules to be exported and the date interval of the data to be exported:

Pandora Agents

Export data

Source agent

Iris Get Info

Modules

NFS_Daemon
DHCP_Server
WEB_Hits
eMails_proc
FTP_sessions
FTP_Daemon
sshDaemon
DNS_Daemon

Date range

From 2005-04-21 15:21:01

To 2005-04-28 15:21:21

CSV Format ☐

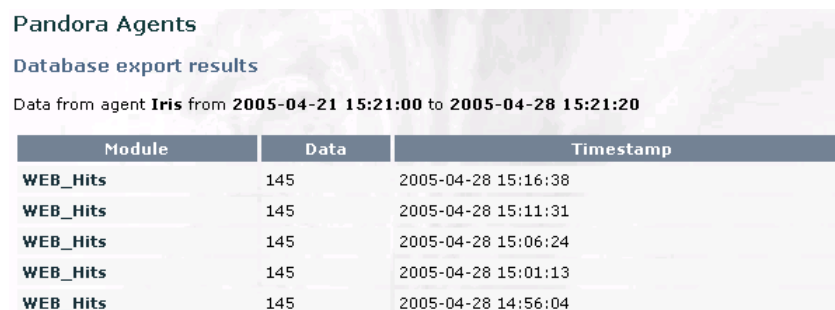
Export

The fields in the results of Exporting data are:

Module: Module name.

Data: Data contained by the module.

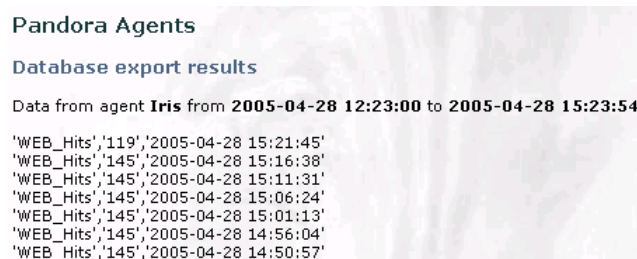
Timestamp: Date and time of the the package was sent by the agent.



Pandora Agents
Database export results
Data from agent **Iris** from **2005-04-21 15:21:00** to **2005-04-28 15:21:20**

Module	Data	Timestamp
WEB_Hits	145	2005-04-28 15:16:38
WEB_Hits	145	2005-04-28 15:11:31
WEB_Hits	145	2005-04-28 15:06:24
WEB_Hits	145	2005-04-28 15:01:13
WEB_Hits	145	2005-04-28 14:56:04

Selecting the CSV format for the output, a text file with extension `.csv` is created. The data is qualified by single quotes and the fields separated by commas:



Pandora Agents
Database export results
Data from agent **Iris** from **2005-04-28 12:23:00** to **2005-04-28 15:23:54**

```
'WEB_Hits','119','2005-04-28 15:21:45'
'WEB_Hits','145','2005-04-28 15:16:38'
'WEB_Hits','145','2005-04-28 15:11:31'
'WEB_Hits','145','2005-04-28 15:06:24'
'WEB_Hits','145','2005-04-28 15:01:13'
'WEB_Hits','145','2005-04-28 14:56:04'
'WEB_Hits','145','2005-04-28 14:50:57'
```

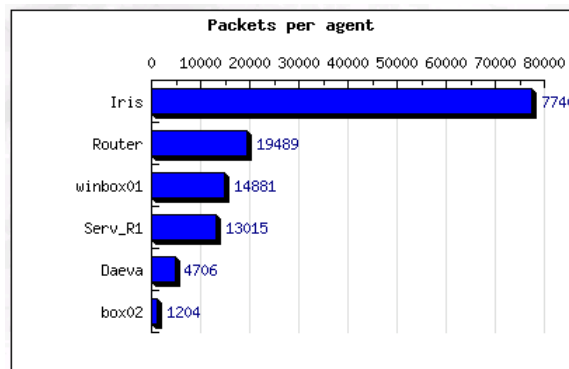
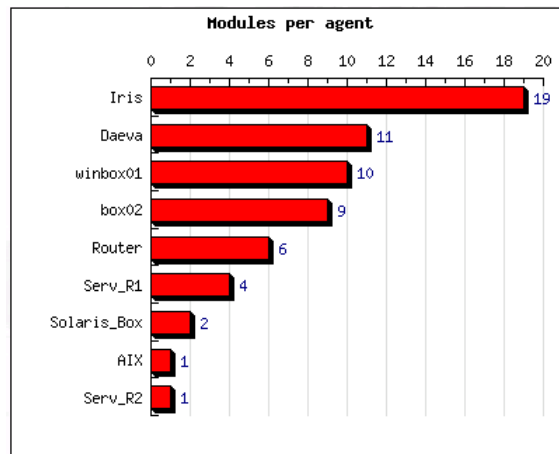
3.3.7. Statistics

Two kinds of graphical statistics are displayed from the "View Agents" > "Statistics" option, in the Operation menu:

- A graph with the number of modules configured for each agent
- A graph with number of packages sent by each Agent. A package is the number of values from the modules the agent sends after each time interval



Pandora Agents
Database Stats per Agent



3.4. SNMP Console

THIS SECTION NEEDS TO BE WRITEN

3.4.1. SNMP Alerts

THIS SECTION NEEDS TO BE WRITEN

Chapter 4. Incident management

The system monitoring process needs to follow up the incidents arising in the system besides receiving and processing the data to be monitored in each time interval

Pandora uses a tool called Incident Manager for this task, where each user can open an incident, where a description of what happened in the network is shown. This can be completed with comments and files when necessary.

This system is designed for group work. Different roles and workflow systems permit to move incidents from one group to another. The system allows different groups and different users to work on the same incident, sharing information and files.

Clicking on "Manage Incidents", in the Operation menu, a list showing all the incidents is displayed, ordered by the date-time they were last updated. Filters can be applied to display only those incidents the user is interested on.

Incidents

Filter

All incidents

All Priority

All Group

Status

- - Active incidents
- - Active incidents, with comments
- - Rejected incidents
- - Closed incidents
- - Expired incidents

Priority

- - Very Serious
- - Serious
- - Medium
- - Low
- - Informative
- - Maintenance

[1-15] [16-23]

ID	Status	Incident name	Priority	Group	Updated at	Source	
34	●	Caida Tarjeta	●●●	Comms	2005-04-20 16:33:46	Application	★
36	●	Para el Administrador	●●●	All	2005-04-19 02:22:27	Application	★
19	●	New cosmetic changes	●●●	Other	2005-04-17 19:51:08	Application	★
28	●	Mejoras de Raúl para Sancho	●●●	Comms	2005-04-10 22:30:46	Other	★
33	●	Test David	●●●	Applications	2005-04-08 09:49:39	Application	★
15	●	Test incident #8	●●●	Comms	2005-04-07 16:33:15	Application	★
17	●	Test incident #10	●●●	Comms	2005-04-07 16:33:02	Application	★
6	●	Test incident #2	●●●	Comms	2005-04-07 16:32:11	IDS	★


The filters that can be applied are:

- *Incident status filter*. The user can display:
 - All incidents
 - Active incidents
 - Closed incidents
 - Rejected incidents
 - Expired incidents
- *Property filter*. The incidents are shown by:
 - All priorities
 - Informative priority
 - Low priority
 - Medium priority
 - High priority
 - Very high priority
 - Maintenance
- *Group filter*. It can be selected to display just the incidents of a given Pandora group.


The incident list is displayed showing information in the following columns:


ID: ID of the incident.

Status: The incident status is represented by the following icons:

 Active incident

 Active incident with comments

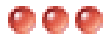
 Rejected incident

 Closed incident

 Expired incident

Incident name: Name given to the incident

Priority: The incident assigned priority is represented by the following icons:

 Very high priority

 High priority

 Medium priority

 Low priority

 Informative priority

 Maintenance priority

Group: The name of the group the incident has been assigned to. One incident can only belong to a single group.

Updated at: This is the date/time the incident was updated for the last time.

Source: The source of the incident. The source is selected from a list stored in the data base. This list can only be modified by the database base administrator.

Owner: User to whom the incident has been assigned to. It doesn't coincide with the creator of the incident, as the incident may have been moved from one user to another. The incident can be assigned to another user by its owner, or by a user with management privileges over the group the incidents belong to.

4.1. Adding an incident

The creation of incidents is performed by clicking on "Manage Incidents" > "New incident", in the Operation menu

Incidents

Create incident

Incident name	Cpu at 75% on Iris		
Opened at	2005/04/28 15:27:44	Updated at	2005/04/28 15:27:44
Owner	slerena - Sancho Lerena	Status	Open and Active
Source	Systems	Group	All
Priority	Medium	Creator	slerena (Sancho Lerena)

Detected a large lapse of time (30min +) of CPU time at 75% on Iris. It could be a

Create

The "Create Incident" form will come up, containing the necessary fields to define the incident. The process is completed by clicking on the "Create" button.

4.2. Incident follow up

All the open incidents can be followed up. The tool is reached by clicking on the "Manage Incidents" option, in the Operation menu.

The incident is selected by clicking on its name in the "Incident name" column.

The screen coming up shows us the configuration variables of the incident, its comments and attached files.

The first part of the screen contains the Incident configuration

Incidents

Review of incident # 30

Incident name	<input type="text" value="TEST #1"/>		
Opened at	<input type="text" value="2005-02-23 21:44:58"/>	Updated at	<input type="text" value="2005-04-28 15:29:42"/>
Owner	<input type="text" value="slerena - Sancho Lerena"/>	Status	<input type="text" value="Open and Active"/>
Source	<input type="text" value="Application"/>	Group	<input type="text" value="All"/>
Priority	<input type="text" value="Informative"/>	Creator	<input type="text" value="()"/>

werwerewr

Update incident

Add note

From this form the following values can be updated:

- *Incident name*
- *Incident owner*
- *Incident status*
- *Incident source*
- *Group the incident will belong to*

- *Indicent priority*

The indicent is updated by clicking on the "Update incident" button.

4.2.1. Adding comments to an incident

Comments about the incident can added clicking on "Add note". This will open up a screen with a text box in it.



Incidents

Add note to incident #30



Date 2005/04/28 15:30:26



Hello this is a note attached to an incident !, it can contain many text.

Add

The comment is written in this box. The Comment will appear in the "Notes attached to incident" section after the button "Add" is pressed.

Notes attached to incident

	Author slerena - (<i>Sancho Lerena</i>)	 Delete
	Date 2005/04/28 15:29:42	
This is a test note :)		

	Author slerena - (<i>Sancho Lerena</i>)	 Delete
	Date 2005/04/28 15:30:26	
Hello this is a note attached to an incident !, it can contain many text.		

Only users with writing privileges can add a comment, and only the owners of the incident or of the notes can delete them.

4.2.2. Attaching files to an incident

Sometimes it is necessary to link an incident with an image, a configuration file, or any kind of file.

The files are attached in the "Attach file" section. Here the file can be searched for in the local machine and attached when the "Upload" button is pressed.

Only a user with writing privileges can attach a file, and only the owner of the incident or of the file can delete it.

Attach File

Filename	<input type="text"/>	<input type="button" value="Browse..."/>	<input type="button" value="Upload"/>
Description	<input type="text"/>		

The incident follow up screen shows all the files attached to the incident in the "Attached files" section of the screen.

Attached files			
Filename	Description	Size	Delete
 firefox_banner.png	Firefox rulez!	4470	

4.3. Searching for an incident

A specific incident can be found amongst the incidents created in Pandora by either using a filter, as explained in the first section of this chapter, or by making a query using the "Manage Incidents">"Search Incident" tool, in the Operation menu.

Incidents

Please select a search criterion

User

Free text for search (*)

(*) The text search will look for all words entered as substring, in index title or description of each incident

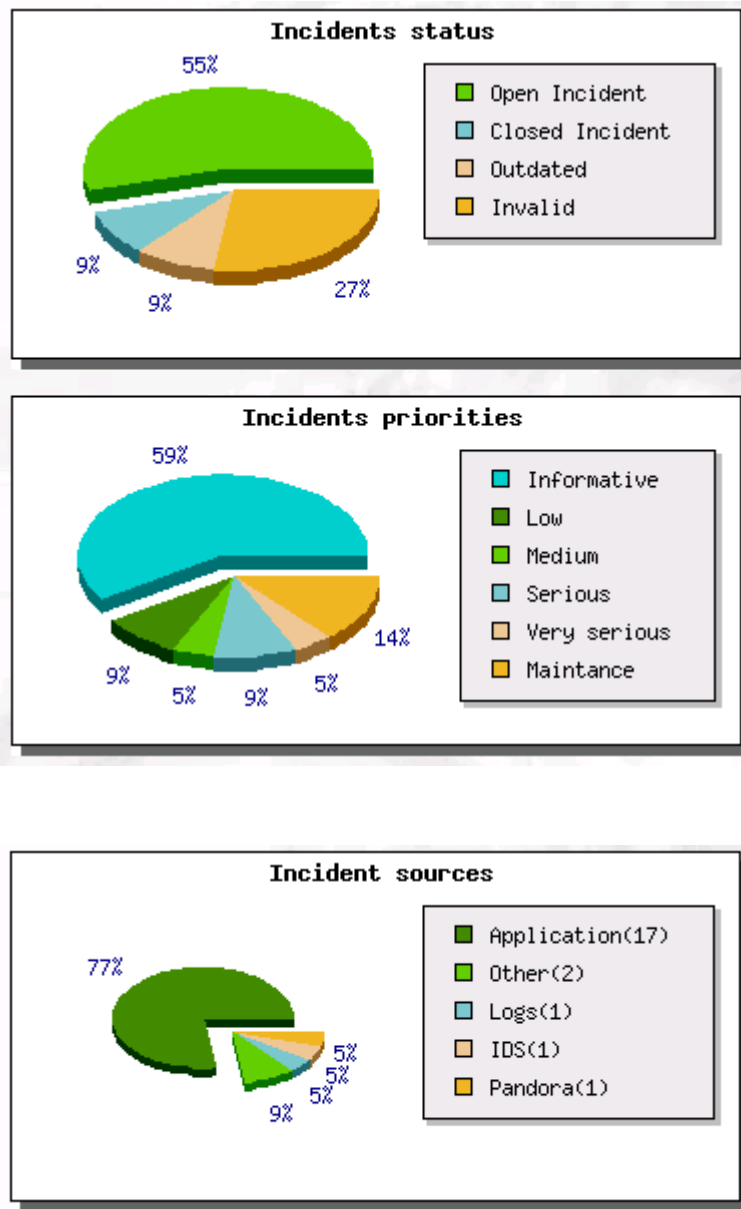
Any text string included as a sub-string in the incident can be searched for using this tool. This search engine looks for the string in the Incident title as well as in the text contained by the incident. The search engine will not search neither the Comments added to the agent nor the attached files. The search can be performed in addition to group, priority or status filters.

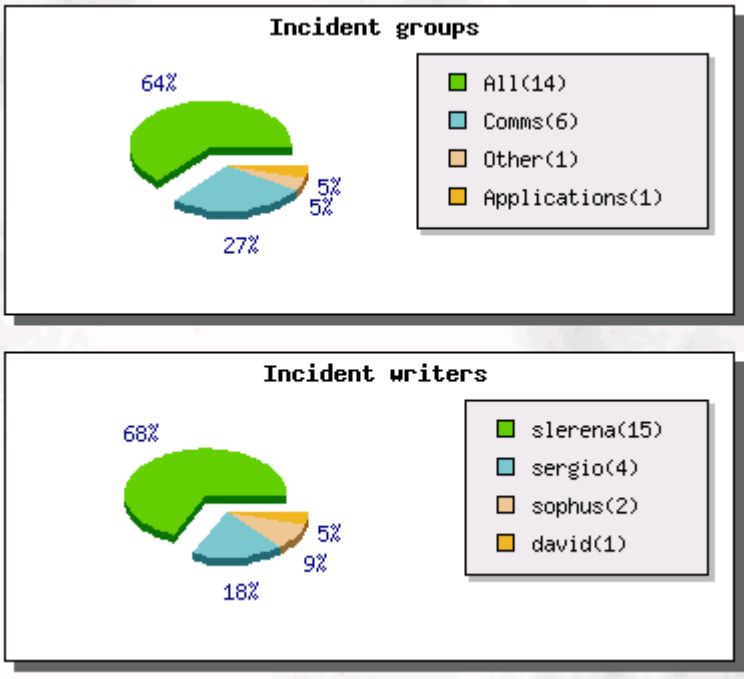
4.4. Statistics

The incident statistics are shown in the "Manage Incidents">"Statistics" option of the Operation menu. They can be of five different types:

- *Incident status*
- *Incident priority*
- *Users with the incident opened*
- *Incidents by group*

- Incident source





Chapter 5. Events

An event in Pandora is any unusual change happen in an agent.





An event is registered when an agent is down or starts up, when a monitor fails or changes its status, or when an alarm is sent.

An event is usually preceded by an issue with the system being monitored. A validation and deletion system has been created to avoid leaving unanalysed issues, so they can be easily validated or deleted if the problem can be ignored or it's been already solved.












The events appear ordered chronologically as they enter the system, and can be viewed by clicking the "View Events" option in the Operation menu. The newer events are placed at the top of the table.

Events

Main Event View

-  - Validated event
-  - Not validated event
-  - Validate event
-  - Delete event

[1-15] [16-30] [31-45] [46-60] [61-75] [76-90] [91-105] [106-120] [121-135] [136-150] >

Status	Event name	Agent name	Group name	User ID	Timestamp
	Monitor (PLC_DNS_CHECK) goes up	Serv_R1	Comms		2005-04-27 20:57:14
	Monitor (PLC_DNS_CHECK) goes down	Serv_R1	Comms	 slerena	2005-04-27 20:52:18
	Alert fired (PLC_DNS_CHECK)	Serv_R1	Comms		2005-04-27 20:52:17
	Monitor (GAIM) goes down	box02	Workstations		2005-04-27 19:00:06
	Monitor (GAIM) goes up	box02	Workstations	 slerena	2005-04-27 17:06:21
	Monitor (GAIM) goes down	box02	Workstations		2005-04-27 16:46:09
	Monitor (PLC_DNS_CHECK) goes up	Serv_R1	Comms		2005-04-26 20:56:11
	Alert fired (PLC_DNS_CHECK)	Serv_R1	Comms		2005-04-26 20:51:01
	Monitor (PLC_DNS_CHECK) goes down	Serv_R1	Comms		2005-04-26 20:51:01

The event information list shows the data in the following columns:

Status: The event status is represented by the icon below:

 The event has been validated

 The event hasn't been validated

Event name: Name assigned to the event by Pandora.


Agent name: Agent where the event happend.


Group name: Group of the agent where the event has happened.

User ID: User that validated the event.

Timestamp: Date and time when the event was raised or validated - if it has been validated.

Action: Action that can be executed over the event.

 This icon will validate the event, disappearing the icon

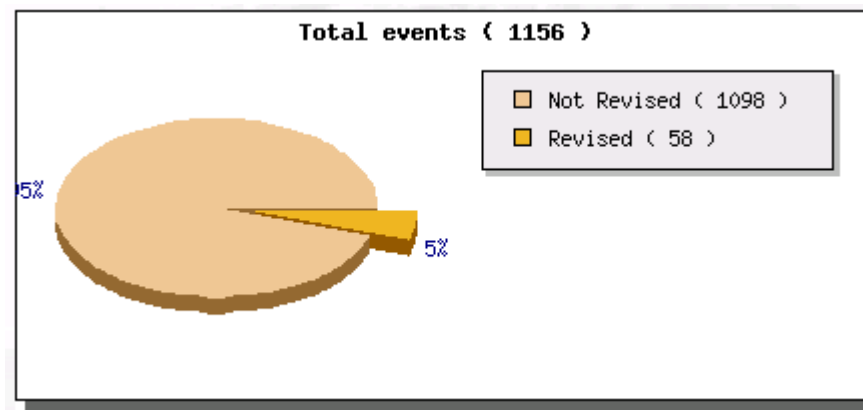
 This icon will delete the event

The events can be also validated or deleted in groups by selecting the tick boxes on the last column of the event, and pressing "Validate" or "Delete" at the bottom of the list.

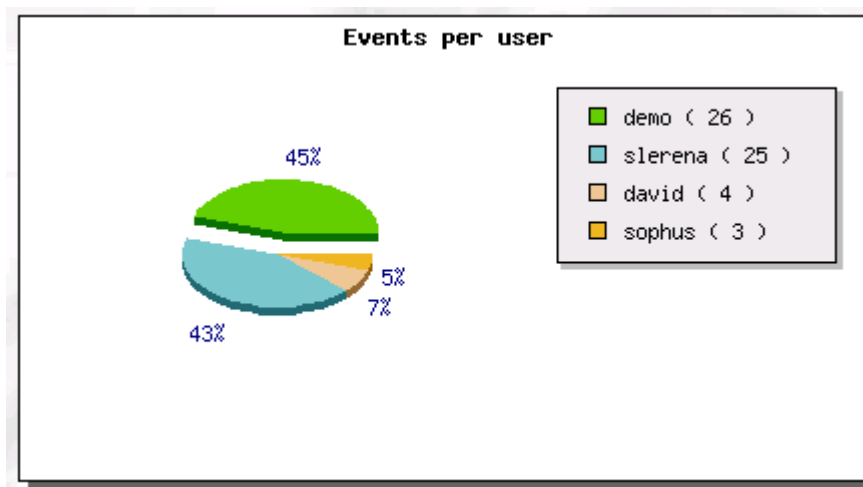
5.1. Statistics

Three different kinds of graphical statistic representation can be choosen from the "View Events">"Statistics" option in the Operation menu:

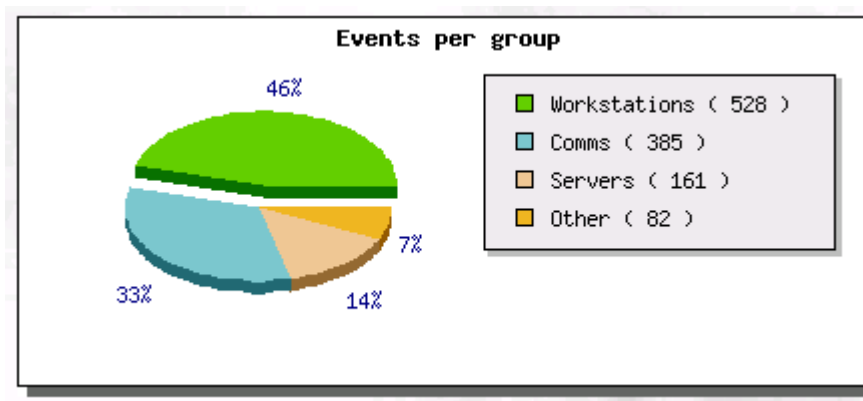
- Total number of events divided by revised and not revised



- Total events divided by the users who validated the events



- Total events divided by the group the agent raising the event belongs to



Chapter 6. System audit

The Pandora's system audit shows all the actions performed by each user, as well as the failed logins.

In the actual version of Pandora the system audit includes actions that somehow try to by pass the security system: attempts to delete an incident by an unauthorised user, attempts to change user profiles by unauthorised users, etc. Its main function is, however, to trace the user connections (login/logout).

The audit Logs can be found in the System Audit option of the Administration menu, ordered chronologicly.

Filters can be applied to the Logs displayed to show only those of interest for the user, selected by the action the Log produces.

The selectable actions are those actions stored in the Data Base at that time.

Review of Pandora audit logs

Filter

All

[1-15] [16-30] [31-45] [46-60] [61-75] [76-90] [91-105] [106-120] [121-135] [136-150] >

User	Action	Date	Source IP	Comments
demo	Logoff	2005-04-28 15:25:33	206.113.192.12	Logged out
demo	Logon	2005-04-28 15:24:11	206.113.192.12	Logged in
slerena	Logon	2005-04-28 13:01:53	194.179.83.87	Logged in
sophus	Logon	2005-04-28 12:41:37	194.158.69.201	Logged in
demo	Logon	2005-04-28 12:40:57	194.30.38.2	Logged in
sophus	Logon	2005-04-28 09:36:15	194.158.69.201	Logged in
demo	Logon	2005-04-28 09:28:09	62.23.219.97	Logged in
SYSTEM	System	2005-04-28 07:27:15	SYSTEM	Pandora Daemon starting
demo	Logon	2005-04-28 03:42:46	24.188.54.67	Logged in
demo	Logon	2005-04-28 01:51:01	61.95.45.230	Logged in
sophus	Logon	2005-04-28 00:40:36	85.94.161.74	Logged in
demo	Logon	2005-04-27 23:50:24	208.234.1.225	Logged in
admin	Logon Failed	2005-04-27 23:50:16	208.234.1.225	Invalid username: admin /
admin	Logon Failed	2005-04-27 23:50:05	208.234.1.225	Invalid username: admin /
demo	Logon	2005-04-27 23:10:32	206.195.193.254	Logged in

The following fields display the Audit Logs information:

User: User that triggered the event (SYSTEM is special user of the system).

Action: Action generated by the entry in the log.

Date: Date of the entry in the log.

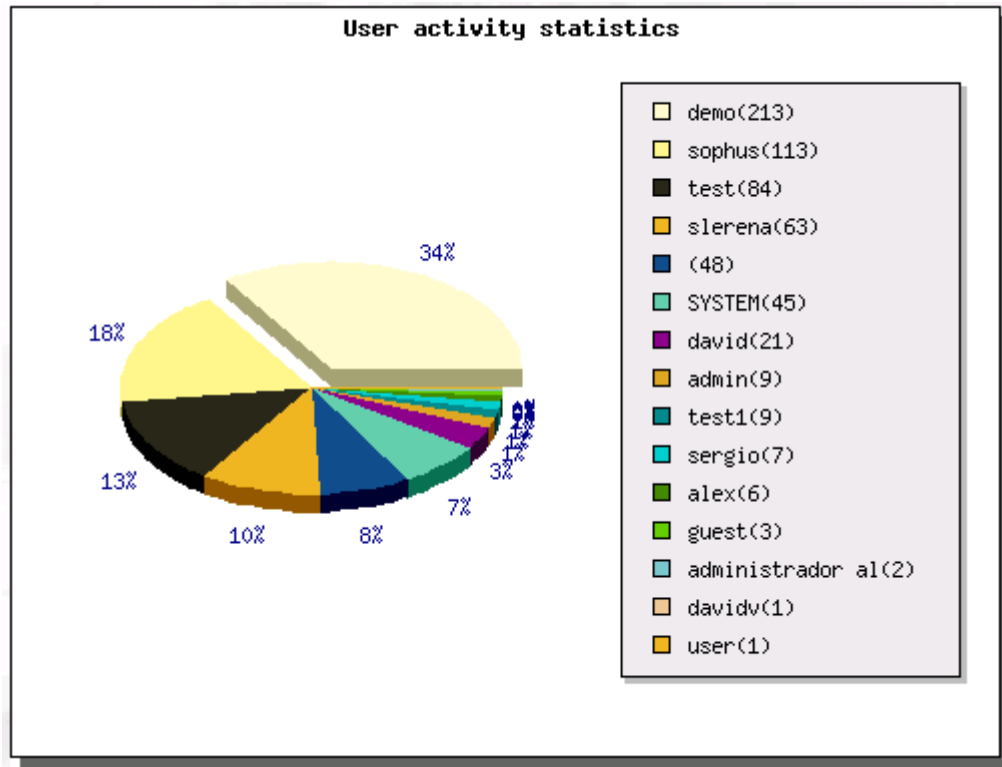
Source IP: IP of the machine or the agent that provoked the entry.

Comment: Comment describing the entry

6.1. Statistics

There isn't a special section to view system audit statistics. However, we could use a graph generated in the Users section to evaluate the actions of each user, as this graph would represent the total number of entries in the audit log for each one: the more active the user is the higher the number of entries.

The graph will also show entries of invalid users, i.e., those entries generated by failed attempts to log in.



Chapter 7. Pandora Servers

From "Manage Servers" section, in the Administration menu you can see a list of configured Pandora Servers and also can manage them.

From "Pandora Servers" in the Operation menu you can see a list of the Pandora Servers.

Chapter 8. Database Maintenance

The core of Pandora's system is its Database. All the data collected by the monitored machines is stored in this data base, from the administrator's data, to the events, incidents and audit data generated in the system at any time.

It is obvious that the efficiency and reliability of this module is vital for the correct functioning of Pandora. A regular data base maintainance is needed. To do so the data base managers can use standard MySQL commands. Maintaining Pandora database in good condition is critiral for Pandora to work properly.

As the database size will increase linearly, the data will be compacted to reduce the amount of stored data without loosing important information, specially the different graphs that are generated with the processed data.

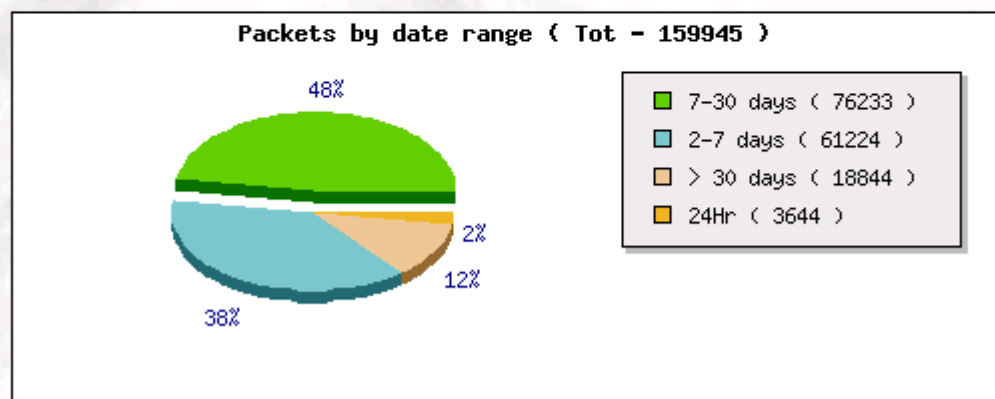
Going to "DB Maintenance" from the Administration menu we will find the Database configuration defined in the "Pandora Setup" option of the Administration menu to compact and delete data.

This is your current database maintenance setup

Max. days before compact data: 15

Max. days before purge: 60

Please check your Pandora Server setup and be sure that database maintenance daemon is running. It's very important to keep up-to-date database to get the best performance and results in Pandora



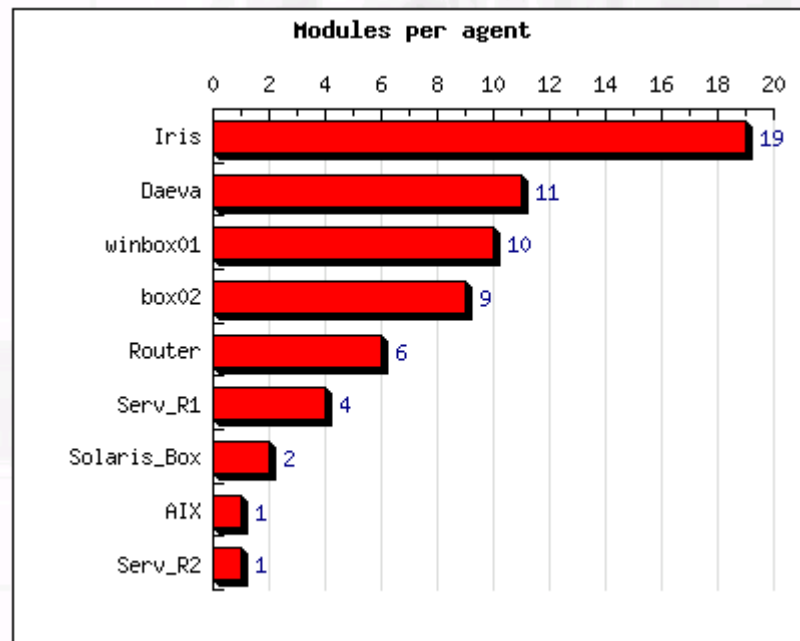
8.1. DB Information

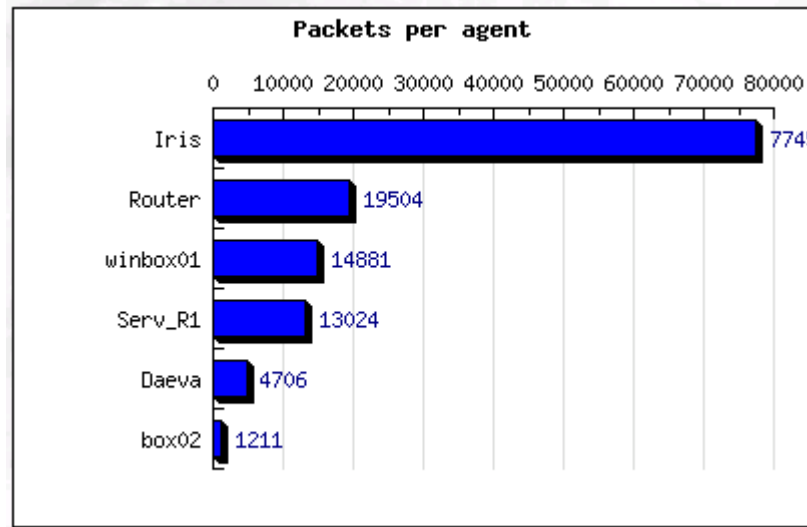
The DB statistics are generated by Agent, on the "DB Maintenance">"DB Information" in the Administration menu, and are represented in two kinds of graphs:

- Number of modules configured for each of the agents.
- Number of packages sent by each agent. A package is the group of data linked to the module the agent sends in each interval of time.

Database Maintenance

Database Information





These graphs can be also viewed from "View Agents">"Statistics" in the Operation menu.

8.2. Manual purge of the Datadase

Pandora counts with powerful tools for the Administrator to manually purge the majority of data stored in the Database. This includes data generated by both the agents and the own server.

8.3. Agent's data purge

8.3.1. Debugging selected data from a module

The option of purging selected data from a module is used to eliminate those out of range entries, whatever the reason - agent failure, out of range values, testing, DB errors, etc. Eliminating erroneous, incorrect or unnecessary data makes the graphical representation more accurate and shows the data without peaks or unreal scales.

From "DB Maintenance">"Database Debug" in the Administration menu any of the out of range data received from a agent's module can be deleted.

Database Maintenance

Database Debug

Source agent

Iris

Modules

NFS_Daemon
DHCP_Server
WEB_Hits
eMails_proc
FTP_sessions

Purge data out these limits

Maximum

Minimum

The purge settings are: agent, module, minimum and maximum data range. Any parameter out of this minimum/maximum range will be deleted.

For example, in a module registering the number of processes, if we are only interested in values between 0 and 100, any values above that number will be usually produced by errors, noise or abnormal circumstances. If we set to range between 0 and 100 all those values below and above - such as -1, 100 or 100000 - will be permanently deleted from the database.

8.3.2. Purging all the agent's data

All the out of range data received by an agent can be deleted from the "DB Maintenance">"Database Purge" option in the Administration menu.

The data is deleted by the following parameters from the "Delete data" screen:

- Purge all data
- Purge data over 90 days
- Purge data over 30 days
- Purge data over 14 days
- Purge data over 7 days
- Purge data over 3 days
- Purge data over 1 day

Get data from agent

Iris

Data from agent Iris in the Database

Packets three months old	96876
Packets one month old	83790
Packets two weeks old	70704
Packets one week old	35388
Packets three days old	5058
Packets one day old	1674
Total packets	96876

Purge data

Purge data over 14 days

8.4. Purging system data

8.4.1. Audit data purge

All the audit data generated by the system can be deleted from "DB Maintenance">"Database Audit", in the Administration menu

The data to be deleted is selected by setting the following parameters in the "Delete Data" screen

- Purge audit data over 90 days
- Purge audit data over 30 days
- Purge audit data over 14 days
- Purge audit data over 7 days
- Purge audit data over 3 days
- Purge audit data over 1 day
- Purge all audit data

Database Maintenance

Database Audit purge

Total	625 Records
First date	2005-03-29 15:51:07
Latest date	2005-04-28 15:25:33

Purge data

Purge audit data over 90 days ▼ **Do it!**

8.4.2. Event data purge

All the event data generated by the system can be deleted from "DB Maintenance">"Database Event", in the Administration menu

The data to be deleted is selected by setting the following parameters in the "Delete Data" screen

- Purge event data over 90 days
- Purge event data over 30 days
- Purge event data over 14 days
- Purge event data over 7 days
- Purge event data over 3 days
- Purge event data over 1 day
- Purge all event data

Database Maintenance

Event Database cleanup

Total	1157 Records
First date	2005-02-05 15:14:27
Latest date	2005-04-28 15:42:44

Purge data

Purge event data over 90 days ▼

Do it!

Chapter 9. Pandora Configuration

All the configurable parameters in Pandora can be set in the "Pandora Setup" section, in the Administration menu.

Pandora Setup	
Language Code for Pandora	en
Block size for pagination	15
Max. days before compact data	15
Max. days before purge	60
Graphic resolution (1-low, 5-high)	3
Compact interpolation (Hours: 1 Fine, 10 medium, 20 bad)	1
<input type="button" value="Update"/>	

These parameters are:

Language: In following versions or revisions of the actual Pandora version will support more languages. At the moment version 1.2 supports English, Spanish, Bable, Italian, French, Catalan and Portuguese of Brazil.

Page block size: Maximum size of the lists in the event, incident and audit log sections.

Max. days before compact data: This parameter controls data compacting. From the number of days in this parameter the data starts getting compacted. For large amounts of data it is recommended to set this parameter to a number between 14 and 28; for systems with less data load or very powerful systems, a number between 30 and 50 will be enough.

Max. days before purge: This parameter controls how long the data is kept before it is permanently deleted. The recommended value is 60. For systems with little resources or large work load the recommended value is between 40 and 50.

Graphic resolution (1 low, 5 high): This value represents the precision of the interpolation logarithm to generate the graphics.

Compact interpolation (Hours: 1 fine, 10 medium, 20 bad): This is the grade of compression used to

compact the Data Base, being 1 the lowest compression rate and 20 the highest. A value above 12 means a considerable data loss. It's not recommended to use value above 6 if the data needs to be represented graphically in large time intervals.

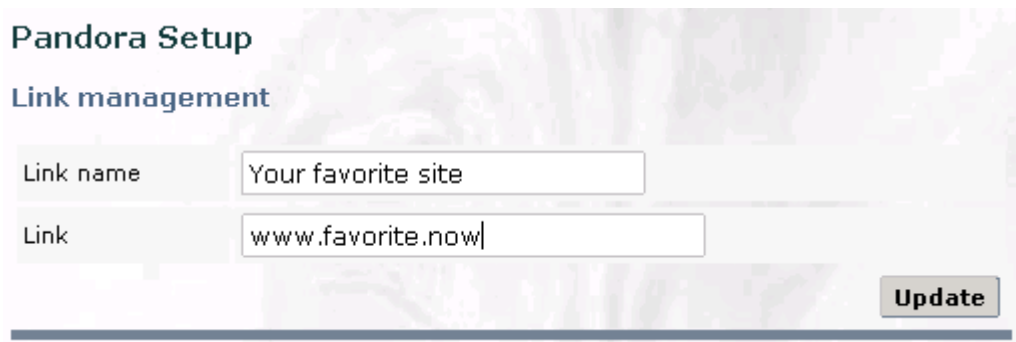
9.1. Links

Links to different Internet or private network links can be configured in Pandora. These could be search engines, applications or company Intranets.

The links configured in Pandora can be edited through the "Pandora Setup">"Links" option in the Administration menu.



A new link is created by clicking on "Create". The link can be then edited:



Appendix A. GNU Free Documentation License

A.1. 0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other written document “free” in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondly, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of “copyleft”, which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

A.2. 1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. The “Document”, below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as “you”.

A “Modified Version” of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A “Secondary Section” is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document’s overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (For example, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The “Invariant Sections” are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License.

The “Cover Texts” are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License.

A “Transparent” copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, whose contents can be viewed and edited directly and straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup has been designed to thwart or discourage subsequent modification by readers is not Transparent. A copy that is not “Transparent” is called “Opaque”.

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML designed for human modification. Opaque formats include PostScript, PDF, proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML produced by some word processors for output purposes only.

The “Title Page” means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, “Title Page” means the text near the most prominent appearance of the work’s title, preceding the beginning of the body of the text.

A.3. 2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

A.4. 3. COPYING IN QUANTITY

If you publish printed copies of the Document numbering more than 100, and the Document’s license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material

on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a publicly-accessible computer-network location containing a complete Transparent copy of the Document, free of added material, which the general network-using public has access to download anonymously at no charge using public-standard network protocols. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

A.5. 4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

- **A.** Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.
- **B.** List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has less than five).
- **C.** State on the Title Page the name of the publisher of the Modified Version, as the publisher.
- **D.** Preserve all the copyright notices of the Document.
- **E.** Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.
- **F.** Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.
- **G.** Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.
- **H.** Include an unaltered copy of this License.

- **I.** Preserve the section entitled “History”, and its title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section entitled “History” in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.
- **J.** Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the “History” section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.
- **K.** In any section entitled “Acknowledgements” or “Dedications”, preserve the section’s title, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.
- **L.** Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.
- **M.** Delete any section entitled “Endorsements”. Such a section may not be included in the Modified Version.
- **N.** Do not retitle any existing section as “Endorsements” or to conflict in title with any Invariant Section.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version’s license notice. These titles must be distinct from any other section titles.

You may add a section entitled “Endorsements”, provided it contains nothing but endorsements of your Modified Version by various parties--for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version .

A.6. 5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms

defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections entitled “History” in the various original documents, forming one section entitled “History”; likewise combine any sections entitled “Acknowledgements”, and any sections entitled “Dedications”. You must delete all sections entitled “Endorsements.”

A.7. 6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

A.8. 7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, does not as a whole count as a Modified Version of the Document, provided no compilation copyright is claimed for the compilation. Such a compilation is called an “aggregate”, and this License does not apply to the other self-contained works thus compiled with the Document, on account of their being thus compiled, if they are not themselves derivative works of the Document. If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one quarter of the entire aggregate, the Document’s Cover Texts may be placed on covers that surround only the Document within the aggregate. Otherwise they must appear on covers around the whole aggregate.

A.9. 8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License provided that you also include the original English version of this License. In case of a disagreement between the translation and the original English version of this License, the original English version will prevail.

A.10. 9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

A.11. 10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation (<http://www.gnu.org/fsf/fsf.html>) may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See <http://www.gnu.org/copyleft/> (<http://www.gnu.org/copyleft/>).

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License “or any later version” applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

A.12. Addendum

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

Copyright © YEAR YOUR NAME.

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.1 or any later version published by the Free Software Foundation; with the Invariant Sections being LIST THEIR TITLES, with the Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST. A copy of the license is included in the section entitled “GNU Free Documentation License”.

If you have no Invariant Sections, write “with no Invariant Sections” instead of saying which ones are invariant. If you have no Front-Cover Texts, write “no Front-Cover Texts” instead of “Front-Cover Texts being LIST”; likewise for Back-Cover Texts.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License (<http://www.gnu.org/copyleft/gpl.html>), to permit their use in free software.

Appendix B. GNU General Public License

B.1. Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software - to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps:

1. copyright the software, and
2. offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

B.2. TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

B.2.1. Section 0

This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The “Program”, below, refers to any such program or work, and a “work based on the Program” means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term “modification”.) Each licensee is addressed as “you”.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

B.2.2. Section 1

You may copy and distribute verbatim copies of the Program’s source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

B.2.3. Section 2

You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- a. You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

- b. You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
- c. If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: If the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

B.2.4. Section 3

You may copy and distribute the Program (or a work based on it, under Section 2 in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

- a. Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- b. Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- c. Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

B.2.5. Section 4

You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

B.2.6. Section 5

You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

B.2.7. Section 6

Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

B.2.8. Section 7

If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not

limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

B.2.9. Section 8

If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

B.2.10. Section 9

The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and “any later version”, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

B.2.11. Section 10

If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

B.2.12. NO WARRANTY Section 11

BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

B.2.13. Section 12

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

B.3. How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the “copyright” line and a pointer to where the full notice is found.

<one line to give the program’s name and a brief idea of what it does.> Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type “show w”. This is free software, and you are welcome to redistribute it under certain conditions; type “show c” for details.

The hypothetical commands “show w” and “show c” should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than “show w” and “show c”; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a “copyright disclaimer” for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program “Gnomovision” (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989 Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary

applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.