Artica
Soluciones Tecnologicas
http://www.artica.es

Babel Enterprise

v1.1

http://babel.sourceforge.net

Manuel Aróstegui Ramírez
marostegui@artica.es

Babel Enterprise

What is Babel?

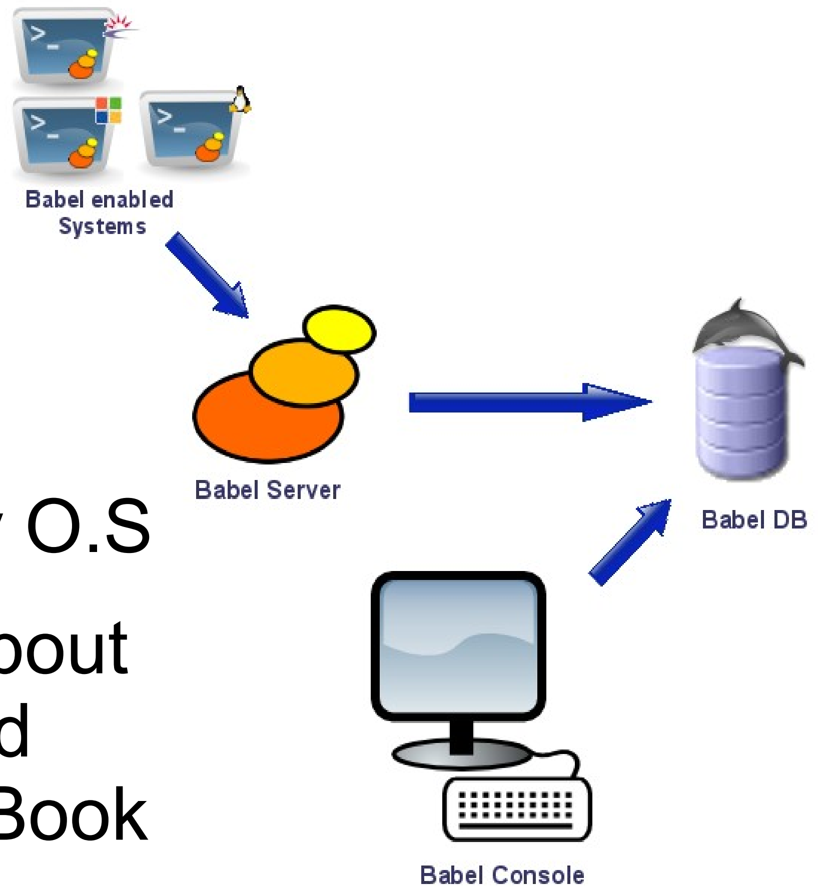
Babel Enterprise v1.1

- Babel Enterprise is a system auditing tool
- Babel performs a security level check of the machine or hardening
- The check consists of a number of auditing tests that obtain a snap of the security status of each machine
- The result is a security index of the system that is given after each execution

Babel Enterprise

Babel Enterprise architecture

- Secure connections:
  - SSH, SSL, HTTPS).
- Light Management (WEB)
- Client-Server Architecture
- Native agents for almost any O.S
- All project is documented: About 90 pages of well-documented funcionality available in DocBook and PDF.



Babel audit modules

- Centralized patch management, software inventory and file integrity.
- Listening ports, service minimization, and password strenght audits.
- Remote services, accounts, and root enviroment audit policies.
- Application hardening (Apache, Tomcat and much others).
- Much others... and very easy to define your own modules.

Babel components

- Babel Server.
- Babel Agents.
- Babel Database
- Babel Web Console

Babel Enterprise

Babel server

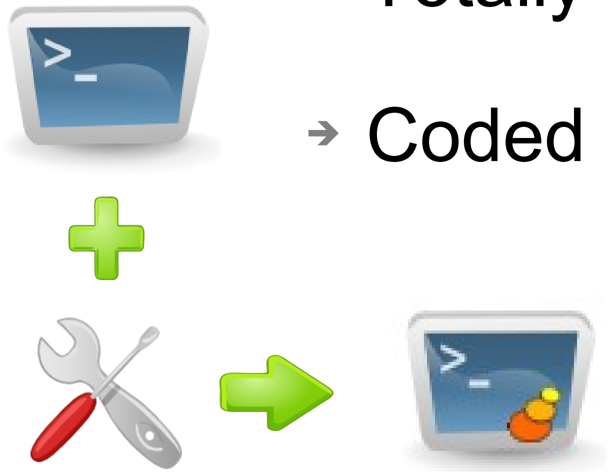
- It process data packets sent by agents and transform them into normalized datastores in database.
- Server checks if anything changed from last policy.
- Server scores the security index of the policy.
- It is written in C

Babel
Enterprise
v1.1

Babel server technology

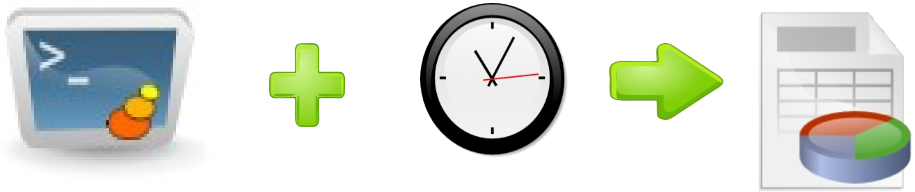
- It uses glibc, gobject.
- It uses inotify.
- Babel Server, by using inotify has become an asyncronous system.
- Every piece of code is documented using oxygen.
- It has plugin architecture to define your own co-relationships.
- It runs as a daemon.

Babel agents

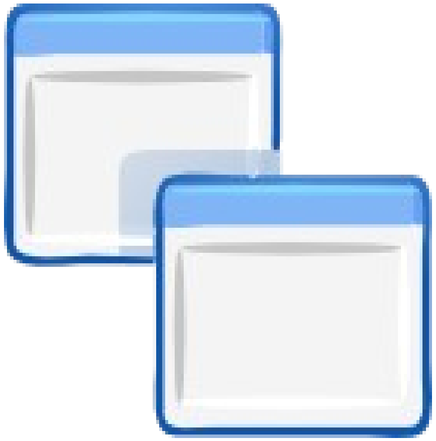


- Totally customizable
- Coded in Bash for Linux (systems)
  - Coded in ksh for Solaris & AIX Systems
  - Wizards for installation.
- Coded in C++ for Windows systems (MinGW)
- Free Source. Available to modify and improve any one of it (including install Wizards).

How Babel agents works



- Run as a daemon.
- Run their modules
- A XML file is generated and sent to the server using a secure connection.
- Run in a specific range, such hours,days or weeks



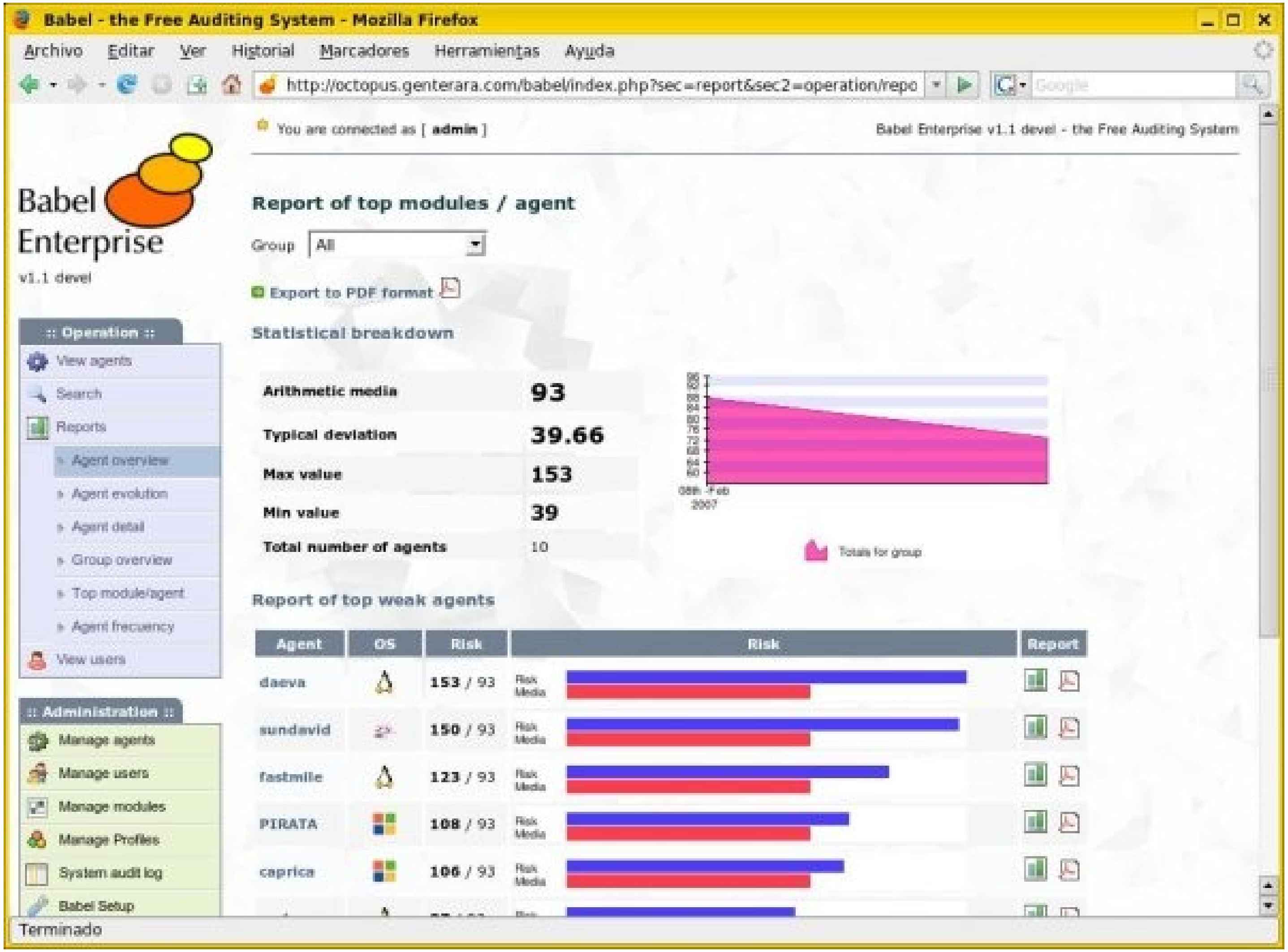
Babel agent module example (Unix)

```
.
.
cat /etc/passwd | cut -f 6 -d ":"  > $TEMP/remote_home.tmp
# Search in home directories: .rhosts, .netrc and ssh authorized_keys files
for a in `cat $TEMP/remote_home.tmp`
do
        if [ "$a" != "/" ]
        then
                # .netrc Search in home directories
                find $a -name ".netrc" -print > $TEMP/remote_netrc.tmp
                    2>/dev/null
                if [ ! -z "`cat $TEMP/remote_netrc.tmp`" ]
                then
                        for b in `cat $TEMP/remote_netrc.tmp`
                        do
                                echo "<moduledata><item><![CDATA[$b]]></item>
                                  <data>.netrc Dete
                                     cted</data></moduledata>" >> $DATA
                        done
                fi
.
.
```

Babel WEB Console

- Written in PHP5.
- Graphics generated using GD directly and Image Graph (PEAR) library.
- PDF reports using a custom made LATEX report engine.
- Babel Server can be totally managed from Babel Console.
- Database management included.

Babel Enterprise



You are connected as [**admin**]

Babel Enterprise v1.1 devel - the Free Auditing System

Report of top modules / agent

Group: All

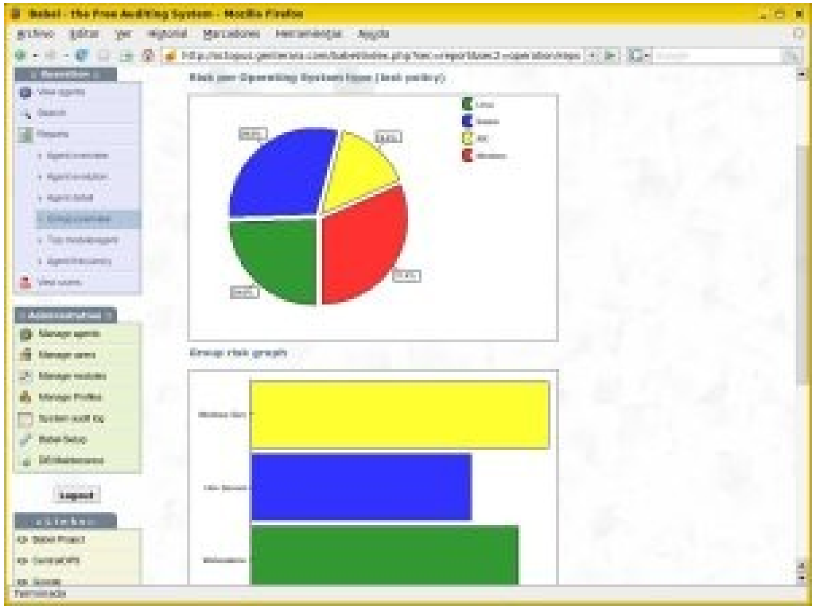
Statistical breakdown

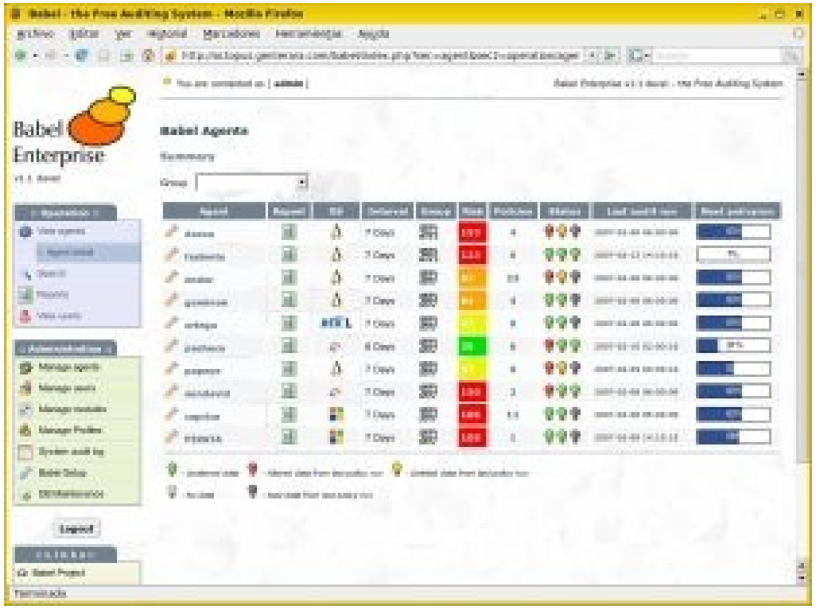
Arithmetic media	**93**
Typical deviation	**39.66**
Max value	**153**
Min value	**39**
Total number of agents	10

Report of top weak agents

Agent	OS	Risk	Risk	Report
daeva		**153** / 93	Risk Media	
sundavid		**150** / 93	Risk Media	
fastmile		**123** / 93	Risk Media	
PIRATA		**108** / 93	Risk Media	
caprica		**106** / 93	Risk Media	

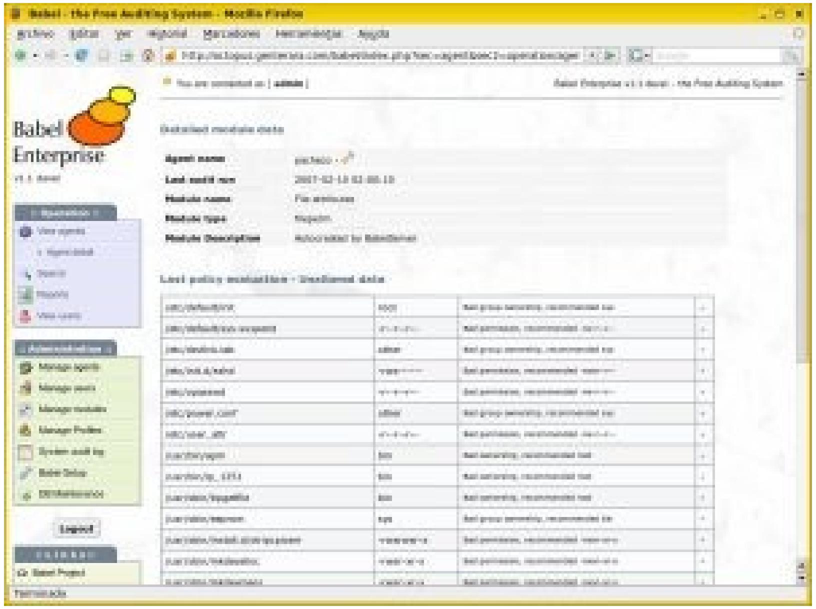
Screenshots


Babel - the Free Auditing System - Mozilla Firefox
Archivo Editar Ver Historial Marcadores Herramientas Ayuda
Risk per Operating System type (last policy)
Linux
Solaris
AIX
Windows
Group risk graph
Logout
Babel Project
Terminado


Babel - the Free Auditing System - Mozilla Firefox
Archivo Editar Ver Historial Marcadores Herramientas Ayuda
You are connected as [admin]
Babel Enterprise
Babel Agents
Summary
Group
7 Days
6 Days
Logout
Babel Project
Terminado

Babel Enterprise

Screenshots



You are connected as [admin]

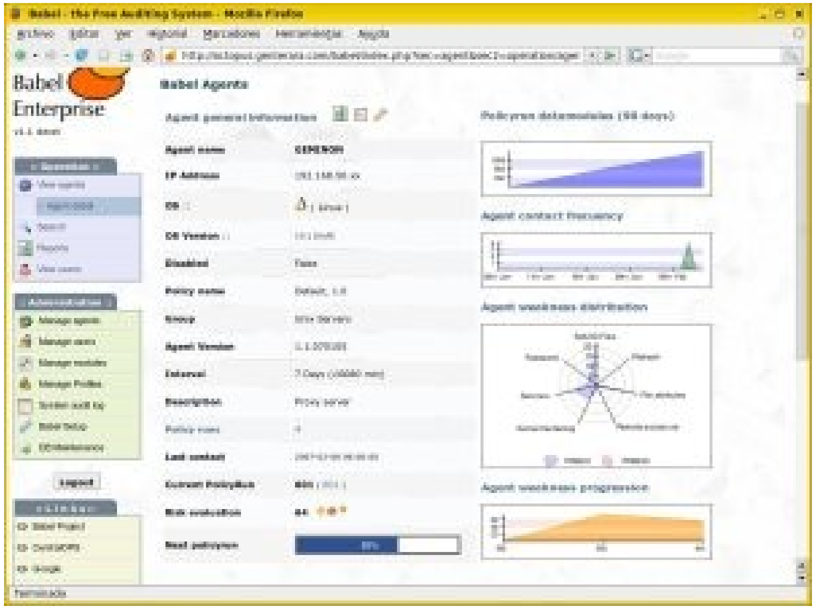
Babel Enterprise v1.1 devel - the Free Auditing System

Detailed module data

Agent name	pacheco
Last audit run	2007-02-13 02:00:13
Module name	File attributes
Module type	Plugin
Module Description	Autocreated by BabelServer

Last policy evaluation - Unallowed data

/etc/default/[illegible]	root	Bad group ownership, recommended: sys
/etc/default/[illegible]	-r--r--r--	Bad permission, recommended: -r--r--r--
/etc/[illegible]	other	Bad group ownership, recommended: sys
/etc/[illegible]	-rwx------	Bad permission, recommended: -rwxr--r--
/etc/[illegible]	-r--r--r--	Bad permission, recommended: -rw-r--r--
/etc/[illegible]	other	Bad group ownership, recommended: sys
/etc/[illegible]	-r--r--r--	Bad permission, recommended: -rw-r--r--
/usr/bin/[illegible]	bin	Bad ownership, recommended: root
/usr/bin/[illegible]	bin	Bad ownership, recommended: root
/usr/sbin/[illegible]	bin	Bad ownership, recommended: root
/usr/sbin/[illegible]	sys	Bad group ownership, recommended: bin
/usr/sbin/[illegible]	-rwsr-xr-x	Bad permission, recommended: -rwxr-xr-x
/usr/sbin/[illegible]	-rwxr-xr-x	Bad permission, recommended: -rwxr-xr-x
/usr/sbin/[illegible]	-rwxr-xr-x	Bad permission, recommended: -rwxr-xr-x



Babel Agents

Agent general information

Agent name	GIMENOR
IP Address	192.168.50.[illegible]
OS	(Linux)
OS Version	[illegible]
Disabled	False
Policy name	Default, 1.0
Group	Unix Servers
Agent Version	1.1.[illegible]
Interval	7 Days (10080 min)
Description	Proxy server
Policy rules	[illegible]
Last contact	[illegible]
Current PolicyRun	[illegible]
Risk evaluation	84
Next policyrun	[illegible]

Policyrun data modules (60 days)

Agent contact frequency

Agent weakness distribution

Agent weakness progression

About ArticaST

- Free Software I+D. Working also with Universities
- Pioneer Free Sofware projects developed.
- System and Security Experts.

Babel OpenSource project

- Currently 5 developers
- All code licensed under GPL2
- Everybody is welcome to the project.
- Feeling like to contributed? Tell us.

http://babel.sourceforge.net