Bellator User Manual

1. INTRODUCCIÓN.

Bellator is an IT systems audit tool based on predefined security templates.

Therefore the *Bellator* intention is to check if the parameters included in the templates are applied and review its deployment status.

Bellator can be used to audit an IT system after apply the secure configuration or in a scheduled manner to know the secure configuration fulfillment and to find out if any no declared modification has occurred.

There are two types of templates:

- Security Local Policy, of which extension is .INF.
- Security Administrative Templates (within the Local Computer Directive, both the Computer Configuration and the User Configuration), of which extension is .POL.

The Security Local Policy template can be obtained in two ways:

- Through Microsoft, thanks to its secure configuration guides, the templates (.INF) to check can be downloaded.
- Exporting from a previously secure configured system, (secedit /export /cfg [*filename.inf*]), in this way it could be checked scheduled any modification in the initial configuration.

The Security Administrative Templates can be obtained from the secure configured system Group Policy folder.

In addition the information related to the previously exposed templates, the *Bellator* audit tool shows other interesting data as users, groups, operating system details, service packs, partitions, disk space and RAM memory.

2. USERS MANUAL

a. Requirements

To work properly *Bellator* require the Microsoft tool "SubInACL.exe" to obtain security information about files, registry keys, and services in SDDL (Security Descriptor Definition Language).

It is also essential to have the library msvcr70.dll in the audited system, which is a module which contains functions of the C standard library.

Both files are are integrated in the *Bellator* executable, if not, they should be included in the same folder.

Bellator requires as input the templates (INF and POL) which previously have been described. It is essential to rename the files as:

- **Template.inf**. As the Security Local Policy.
- **RegistryM.pol** and **RegistryU.pol**. As computer administrative configuration template and user administrative configuration template respectively.

Bellator has been tested in standalone computers which do not belong to any domain (Windows Server/Professional eng and spa, and Windows XP Professional eng and spa).

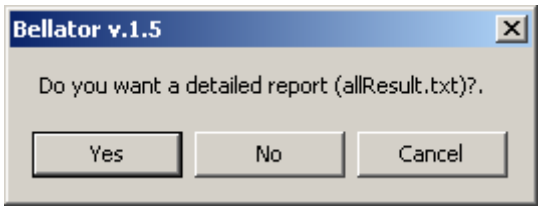
The most of the functions work properly over computers which belong to any domain, specifically those local related parameters. All the policies different to registry parameters could not work properly due to it has not been tested in domain computers.

Nowadays it is going tested correctly in Windows 2003.

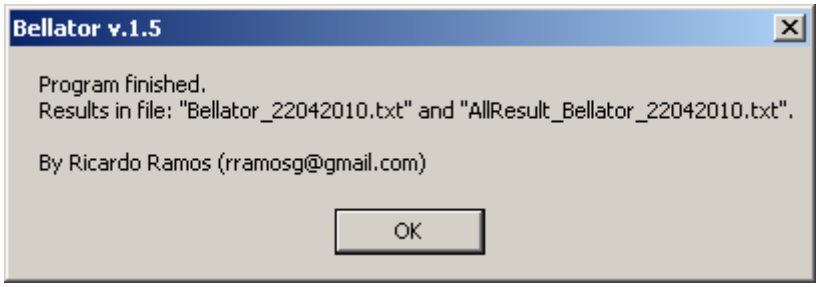
b. Execution

After the configuration the *Bellator*.exe shall be executed.

Bellator will ask if the user wants a detailed report with the data obtained, in addition to the results report generated anyway.



When finish *Bellator* notify user the correct execution, as well as reports name.



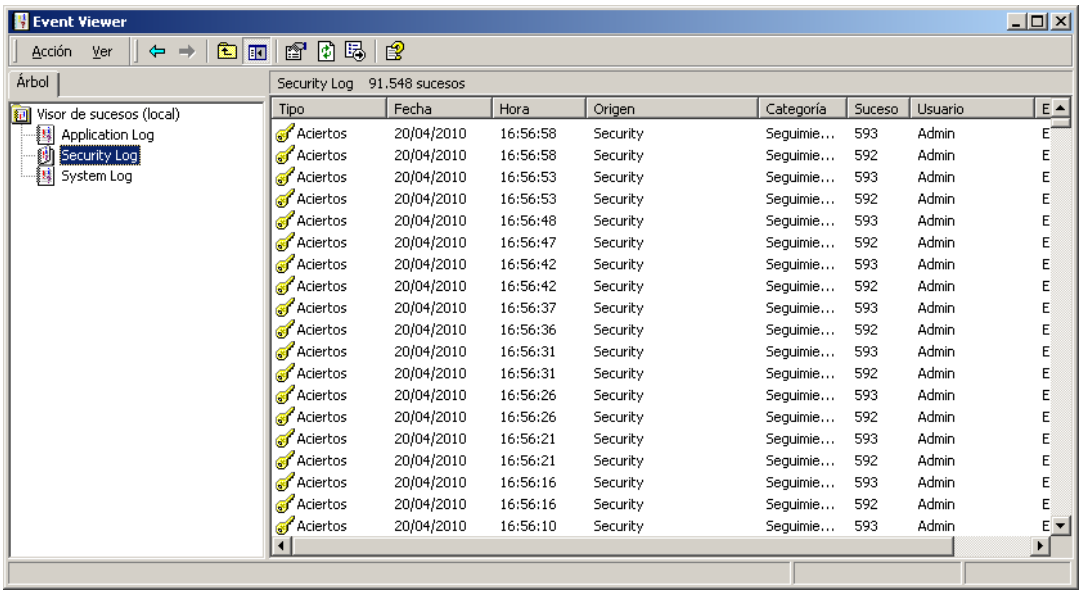
c. Security Local Directive templates structure

Security template must have a specific format, grouping each audit module according to specific labels (i.e. [Application Log]):

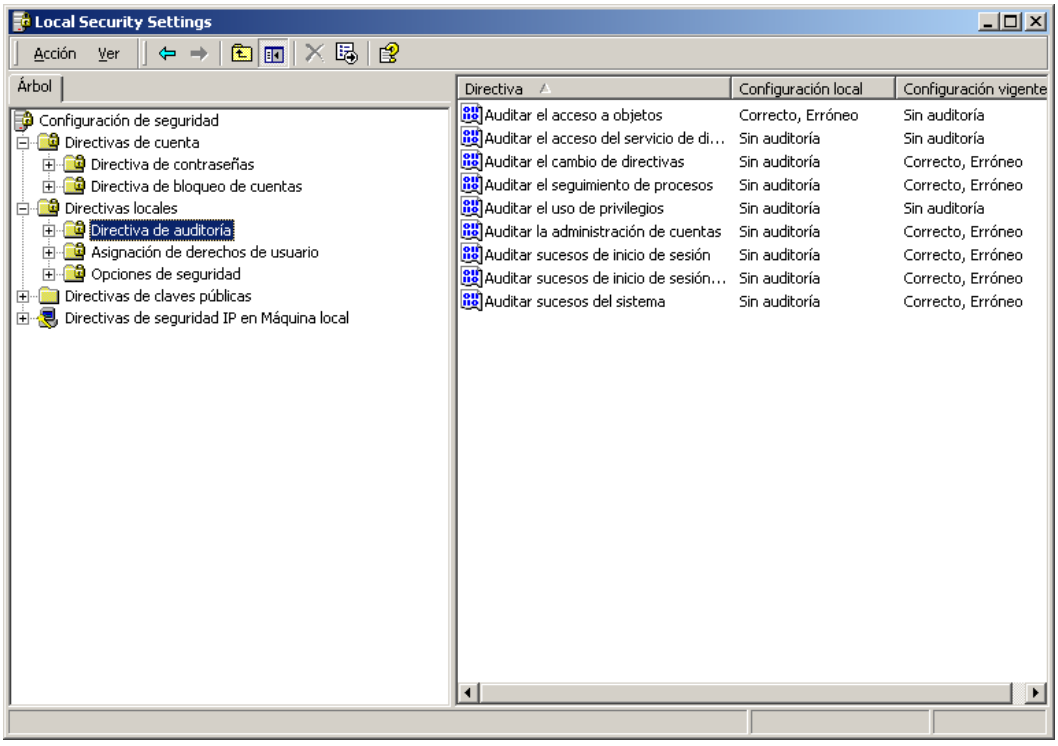
```
[Event Audit]
AuditSystemEvents = 3
AuditLogonEvents = 3
AuditObjectAccess = 3
AuditPrivilegeUse = 2
AuditPolicyChange = 1
[Service General Setting]
Alerter,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCLCSWLOCRRC;;;AU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
CiSvc,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCLCSWLOCRRC;;;AU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
```

They are listed below:

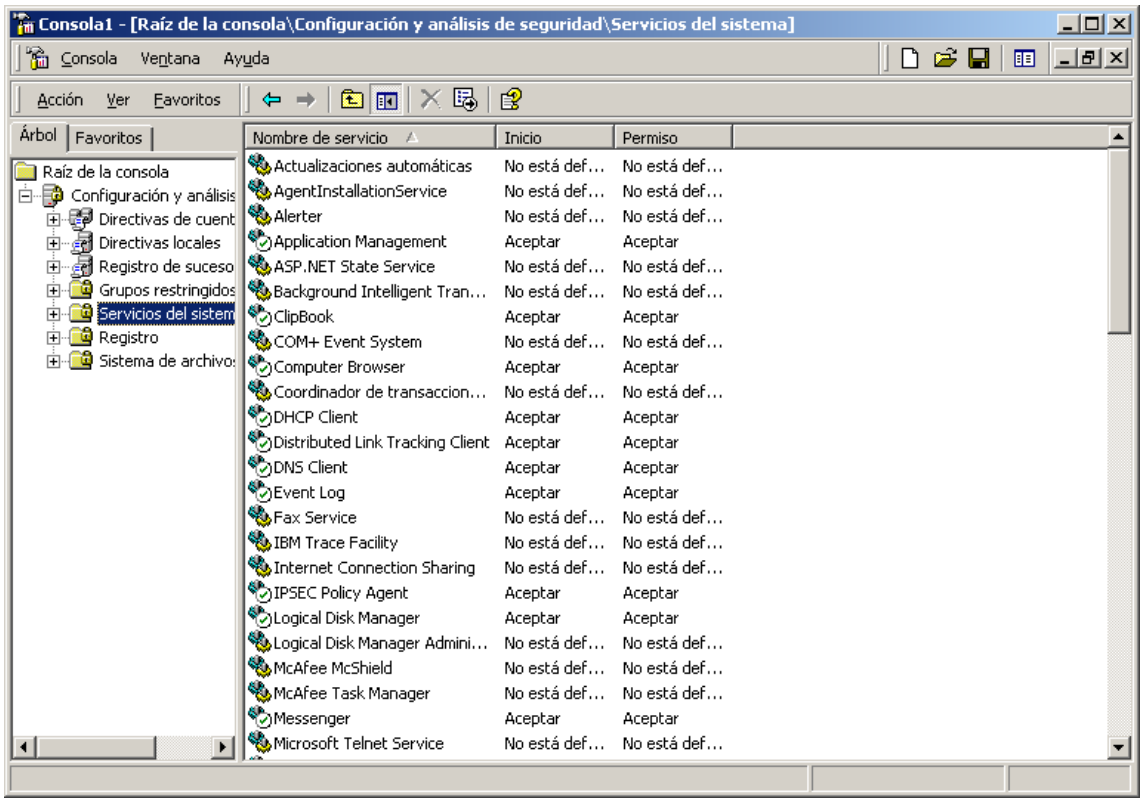
- [System Log], [Security Log], [Application Log]: System, Security and application Events.



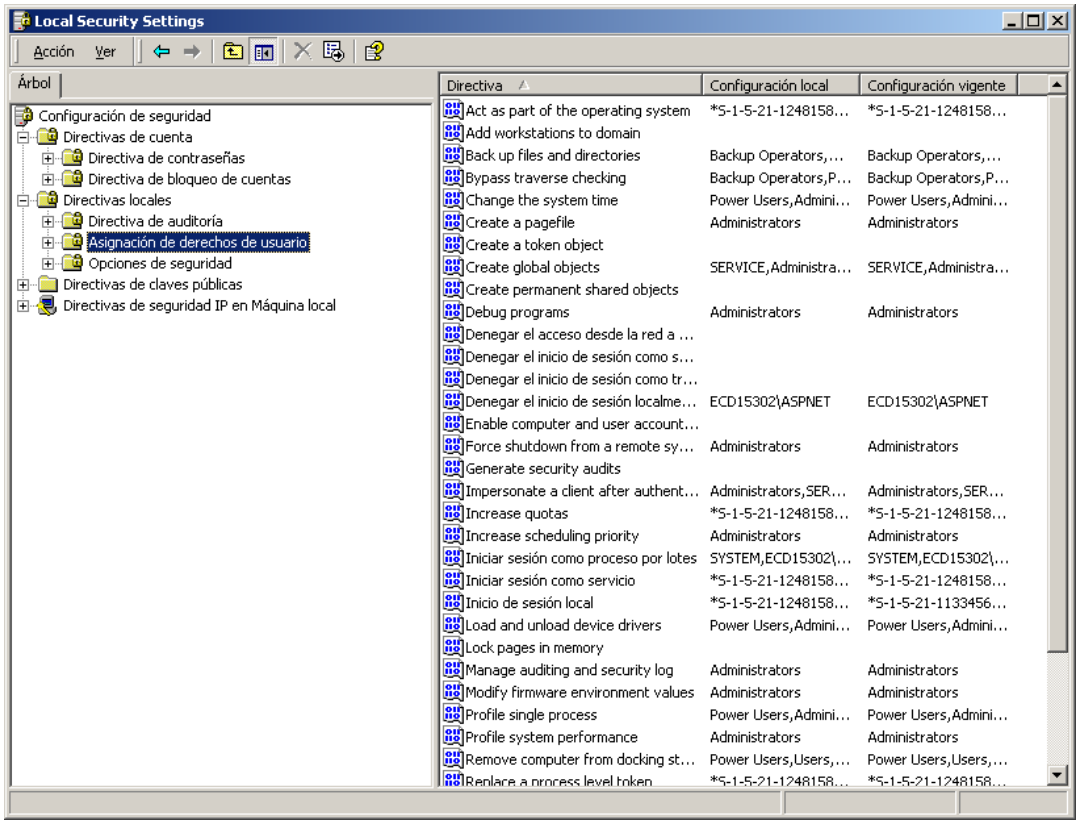
- [Event Audit]: Audit directive.



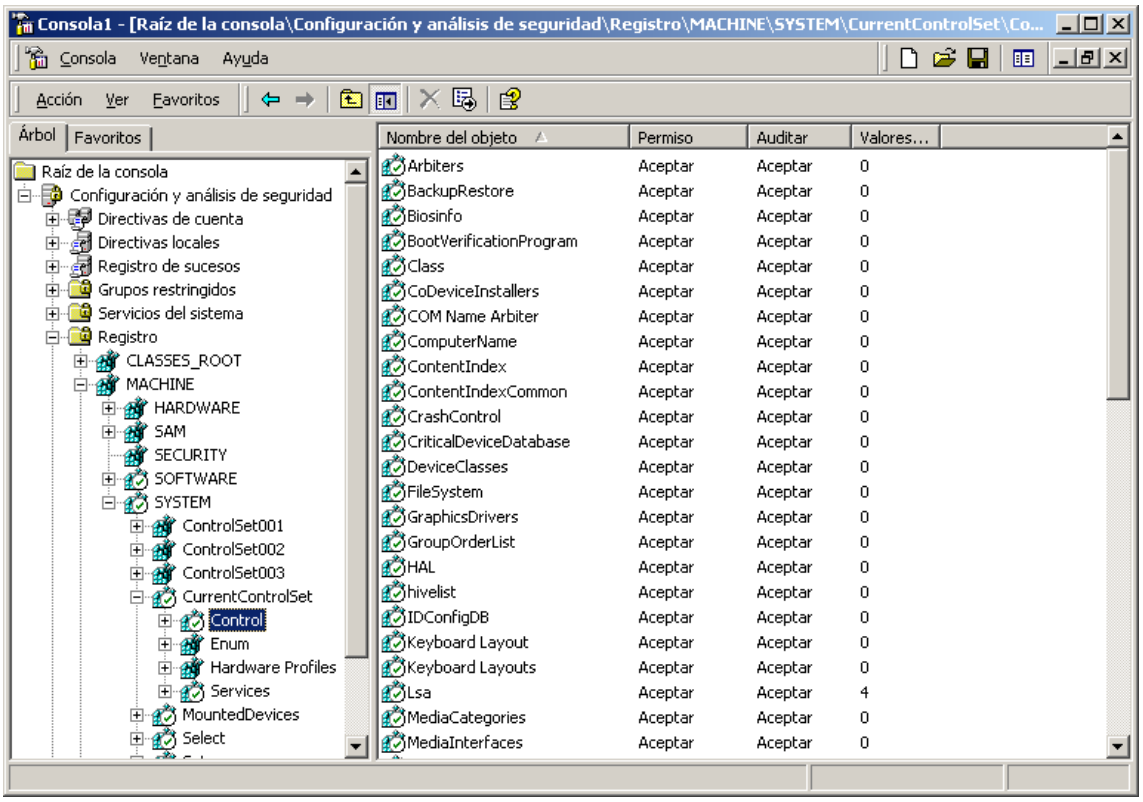
- [Service General Setting]: Security information about the system services.



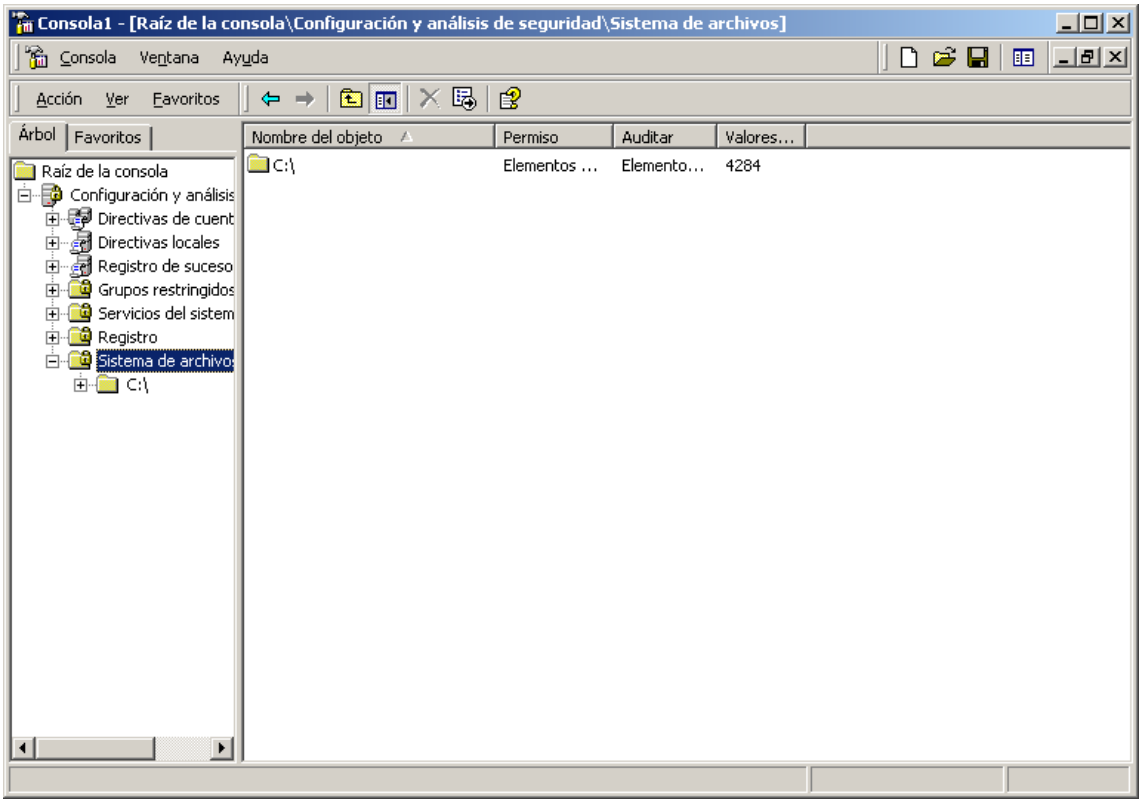
- [Privilege Rights]: User Privilege Rights.



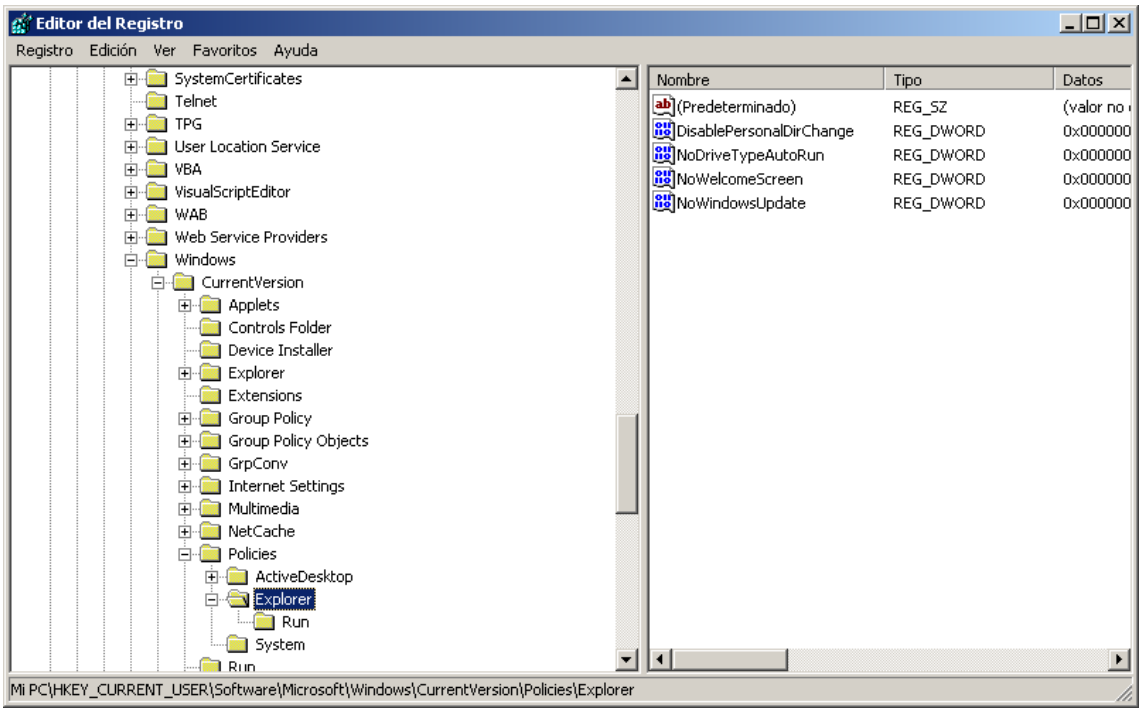
- [Registry Keys]: Rights over system registry keys.



- [File Security]: System file security rights.



- [Registry Values]: System Registry Keys values. It is related to security options from the configuration guide.



For the moment *Bellator* do not cover the [System Access] Account Directives.

d. Security Administrative Templates Structure

The RegistryM.pol and RegistryU.pol must fulfill the ABNF format. It must not be modified with a text editor due to it is in a hexadecimal format and could contains special characters.

3. COLLABORATIONS

Bellator is a project started time ago and it is the result of the effort realized by its author, but it counts with collaborations in the different parts of the projects, people who the author wants to thank for their altruist support.

They are:

Manuel Rodríguez. In charge of coordinate the *Bellator* test over different systems and environments.

Serg. For his contributions and his *commercial actions*.

Yago Molina. For his invaluable help, helping to start in the Windows programming world.

Any other partner/friend/colleague by its ideas and something more.

4. CONTACT

For any suggestion, error, criticism (constructive) or simply for any question related to *Bellator*, you can use the e-mail address *Bellator*.audit@gmail.com.

Thanks a lot.
Ricardo.