SNORT−ACID install on Solaris9

Revision 1.1

Guillaume.rix@sun.com

I − Contents

This manual concern the installation and configuration of snort and acid on Solaris9.

Of course, all installation of necessary components as mysql, SSL, PHP, adodb, etc .... will be explained too.

What you will learn :

- Install and configure Snort on Solaris9
- Install and configure Acid on Solaris9
- Compile and configurate Apache with PHP and mod_ssl

What you won't learn :

- Reinforce your OS
- Create rules for Snort
- Use of all options of Snort

II − Before the installation

1 − System

Here is the environment where I installed snort and acid :

```
/usr/bin/bash

bash−2.05# prtdiag

Configuration du système : Sun Microsystems sun4u Sun Ultra 5/10 UPA/PCI (UltraSPARC−IIi 440MHz)
Fréquence d'horloge système : 110 MHz
Taille de mémoire : 512 mégaoctets

========================= CPUs =========================

Run Ecache CPU CPU
Brd CPU Module MHz MB Impl. Mask
−−− −−− −−−−−−− −−−−− −−−−−− −−−−−− −−−−
0 0 0 440 2,0 12 9.1
```

2 − Security

Before **ALL** things, secure your box !!!!!!!
An IDS on an insecure machine isn't.
Just to be patient, reinforce and protect your OS.
Here is a good begin :

http://www.sun.com/bigadmin/docs/indexSec.html

This document concern the install of Snort and not the OS security where Snort will be installed, it's why I would not say any more on the subject, that being very well explained in thousands of other documents on the net.

Of course, I strongly recommend to you to verify the integrity of **ALL** files that you will download.
You can make this with the command "gmd5sum" (from the package "textutils").
Two major possibilities for download it :

From the Solaris Companion CD :

http://wwws.sun.com/software/solaris/freeware/s9pkgs_download.html

or from the GNU site itself :

http://www.gnu.org/software/textutils/

Just have a look on each site where you will dowload your archives and you should find an MD5 fingerprint of these archives.

For SUN, the MD5 fingerprint are here :

http://sunsolve.sun.com/pub−cgi/fileFingerprints.pl

3 − Environment

Uinstall the version of Apache supplied with Solaris9.We will install a new version with ssl and PHP ===>

```
bash−2.05# pkgrm SUNWapchS ( Source for the Apache httpd server )
bash−2.05# pkgrm SUNWapchr ( Apache Web Server Documentation )
bash−2.05# pkgrm SUNWapchu ( Apache Web Server User )
bash−2.05# pkgrm SUNWapchd ( Apache Web Server Root )
bash−2.05# rm −Rf /usr/apache
bash−2.05# rm −Rf /etc/apache
bash−2.05# rm −Rf /var/apache
```

Install these following packages for futures installations ===>

ftp://ftp.sunfreeware.com/pub/freeware/sparc/9/gcc−3.2.3−sol9−sparc−local.gz
ftp://ftp.sunfreeware.com/pub/freeware/sparc/9/flex−2.5.4a−sol9−sparc−local.gz
ftp://ftp.sunfreeware.com/pub/freeware/sparc/9/bison−1.75−sol9−sparc−local.gz

```
bash−2.05# gunzip −d gcc−3.2.3−sol9−sparc−local.gz
bash−2.05# gunzip −d flex−2.5.4a−sol9−sparc−local.gz
bash−2.05# gunzip −d bison−1.75−sol9−sparc−local.gz
bash−2.05# pkgadd −d gcc−3.2.3−sol9−sparc−local
bash−2.05# pkgadd −d flex−2.5.4a−sol9−sparc−local
bash−2.05# pkgadd −d bison−1.75−sol9−sparc−local
```

III − MySQL

1 − Installation

You can use the generation 3.x or 4.x of MySQL.

For a version 3.x, you can download here :

ftp://ftp.sunfreeware.com/pub/freeware/sparc/9/mysql−3.23.53−sol9−sparc−local.gz

```
bash−2.05# gunzip −d mysql−3.23.53−sol9−sparc−local.gz
bash−2.05# pkgadd −d mysql−3.23.53−sol9−sparc−local
```

For a version 4.x, it's here :

http://www.ibiblio.org/pub/packages/solaris/csw/stable/sparc/5.9/mysql4−4.0.10−SunOS5.8−sparc−CSW.pkg.gz

```
bash−2.05# gunzip −d mysql4−4.0.10−SunOS5.8−sparc−CSW.pkg.gz
bash−2.05# pkgadd −d mysql4−4.0.10−SunOS5.8−sparc−CSW.pkg
```

WARNING : You must use "gtar" instead of "tar" for decomress the MySQL archive.
Solaris tar has a problem with long filenames and reports checksum errors.
You can download the GNU version of tar here :

ftp://ftp.sunfreeware.com/pub/freeware/sparc/9/tar−1.13.19−sol9−sparc−local.gz

If you want more recent, use a source distribution and compile it :

http://www.mysql.com/downloads/

I didn't wrote again the compile instruction, I follow the following guide and had a successfull compilation :

http://www.mysql.com/doc/en/Solaris.html
http://www.mysql.com/doc/en/Installing_source.html

For the rest of this document, we will consider that mysql is the version 4.0.12 and is installed in "/usr/local/mysql".

2 − Configuration

```
bash−2.05# mysql −u root −p
```

Password for root local access :

```
mysql> set password for 'root'@'localhost' = password('your_root_password');
```

Delete unnecessary database :

```
mysql> drop database test
```

Delete the anonymous access :

```
mysql> connect mysql
mysql> delete from user where user="";
mysql> delete from db where user="";
mysql> exit
```

3 − Test

```
bash−2.05# ln −s /usr/local/mysql/bin/mysql /usr/bin/mysql
bash−2.05# mysql −u snort −p
mysql> show databases;
+−−−−−−−−−−−−−−−−−−+
| Database |
+−−−−−−−−−−−−−−−−−−+
| mysql
+−−−−−−−−−−−−−−−−−−+
1 row in set (0.02 sec)

mysql> connect mysql
mysql> exit
```

IV − Snort

1 − Installation

Snort need of the "libpcap" library for sniff the network :

ftp://ftp.sunfreeware.com/pub/freeware/sparc/9/libpcap−0.7.2−sol9−sparc−local.gz
http://www.snort.org/dl/snort−2.0.0.tar.gz

```
bash−2.05# gunzip −d libpcap−0.7.2−sol9−sparc−local.gz
bash−2.05# pkgadd −d libpcap−0.7.2−sol9−sparc−local
bash−2.05# gunzip −c snort−2.0.0.tar.gz | tar xvf −
bash−2.05# cd snort−2.0.0
bash−2.05# sh ./configure −−with−mysql=/usr/local/mysql −−host=sparc−sun−solaris2.9
```

If you wish to use the plugin "flexresp", you must install the "libnet" library :

http://www.packetfactory.net/libnet/

```
bash−2.05# sh ./configure −−enable−flexresp −−with−mysql=/usr/local/mysql −−host=sparc−sun−solaris2.9 −−with−libnet−libraries=/usr/local/libnet
−−with−libnet−includes=/usr/local/libnet

bash−2.05# make
bash−2.05# make install
```

2 − Configuration

Create a database for snort :

```
bash−2.05# ln −s /usr/local/mysql/bin/mysql /usr/local/bin/mysql
bash−2.05# mysql −u root −p
mysql> create database snort;
mysql> source /download/snort−2.0.0/contrib/create_mysql
```

Configure the good rights for this new database :

```
mysql> connect snort
mysql> grant CREATE,INSERT,SELECT,DELETE,UPDATE on snort.* to snort;
mysql> grant CREATE,INSERT,SELECT,DELETE,UPDATE on snort.* to snort@localhost;
```

Create the user "snort" in the database "mysql" :

```
mysql> connect mysql
mysql> set password for 'snort'@'localhost' = password('your_snort_password');
mysql> set password for 'snort'@'%' = password('your_snort_password');
mysql> flush privileges;
```

Install the tables from "contrib/snortdb−extra.gz" :

```
mysql> connect snort
mysql> source snort−db
mysql> exit
```

Here is an exemple on how use these extra tables :

http://archives.neohapsis.com/archives/snort/2003−04/0381.html

3 − Test

```
bash−2.05# mysql −u root −p
mysql> connect snort
mysql> show tables;
+−−−−−−−−−−−−−−−−−−+
| Tables_in_snort |
+−−−−−−−−−−−−−−−−−−+
| acid_ag |
| acid_ag_alert |
| acid_event |
| acid_ip_cache |
| data |
| detail |
| encoding |
| event |
| icmphdr |
| iphdr |
| opt |
| reference |
| reference_system |
| schema |
| sensor |
| sig_class |
| sig_reference |
| signature |
| tcphdr |
| udphdr |
+−−−−−−−−−−−−−−−−−−+
20 rows in set (0.00 sec)
mysql> exit
```

V − Apache & mod_ssl

1 − Installation

WARNING : Notice the names of the mod_ssl archive (mod_ssl−2.8.14−1.3.27.tar.gz) and Apache archive (apache_1.3.27.tar.gz).
In fact, each version of mod_ssl works with a specific version of apache.
Here, in the name of the mod_ssl archive, "2.8.14" represent the version of mod_ssl and
"1.3.27" represent the supported version of Apache. BE CAREFUL ABOUT THIS.

We need openssl, apache and mod_ssl :

http://www.openssl.org/source/openssl−0.9.7b.tar.gz
http://www.modssl.org/source/mod_ssl−2.8.14−1.3.27.tar.gz
http://apache.ttlhost.com/httpd/apache_1.3.27.tar.gz

```
bash−2.05# gunzip −c openssl−0.9.7b.tar.gz | tar xvf −
bash−2.05# gunzip −c mod_ssl−2.8.14−1.3.27.tar.gz | tar xvf −
bash−2.05# gunzip −c apache_1.3.27.tar.gz | tar xvf −
bash−2.05# cd openssl−0.9.7b
bash−2.05# sh config −fPIC
bash−2.05# make
bash−2.05# make test (optional)
bash−2.05# make install (optional)
bash−2.05# cd ../mod_ssl−2.8.14−1.3.27
bash−2.05# ./configure −−with−apache=../apache_1.3.27 −−with−ssl=../openssl−0.9.7b −−prefix=/usr/local/apache −−enable−shared=ssl
bash−2.05# cd ../apache_1.3.27
bash−2.05# make
bash−2.05# make certificate TYPE=custom
bash−2.05# make install
```

2 − Configuration

Here, the more important file is "hhtpd.conf" in "/usr/local/apache/conf".

Read this file absolutly and configure it as your need.

I will use the path "/web" for the DocumentRoot in Apache for the rest of installation.

3 − Test

```
bash−2.05# ln −s /usr/local/apache/bin/apachectl /usr/local/bin/apache
bash−2.05# apache start
```

http://your_acid_computer/

```
bash−2.05# apache stop
bash−2.05# apache startssl
```

https://your_acid_computer/

VI − PHP & Apache/mod_ssl

1 − Installation

http://www.php.net/get/php−4.3.1.tar.gz/from/a/mirror

```
bash−2.05# gunzip −c php−4.3.1.tar.gz | tar xvf −
```

The option "−−with−gd=[DIR]" is obsolete as the version 4.3.0 and early includes a version of gd as "standard equipment."

http://www.boutell.com/gd/

"If you wish to use gd with PHP, it is probably best to get php 4.3.0 and use the included gd library."

```
bash−2.05# cd ../php−4.3.1
bash−2.05# CFLAGS='−DEAPI' ./configure −−with−apxs=/usr/local/apache/bin/apxs −−with−mysql=/usr/local/mysql −−with−zlib=/usr/local
−−with−gd
bash−2.05# make

gcc −Imain/ −I/space/IDS/apache/php−4.3.2RC3/main/ −DPHP_ATOM_INC −I/space/IDS/apache/php−4.3.2RC3/include
−I/space/IDS/apache/php−4.3.2RC3/main −I/space/IDS/apache/php−4.3.2RC3 −I/space/IDS/apache/php−4.3.2RC3/Zend
−I/usr/local/mysql/include −I/space/IDS/apache/php−4.3.2RC3/ext/xml/expat −D_POSIX_PTHREAD_SEMANTICS
−I/space/IDS/apache/php−4.3.2RC3/TSRM −c main/internal_functions.c −o main/internal_functions.o && echo > main/internal_functions.lo
main/internal_functions.c:41: `phpext_xml_ptr' undeclared here (not in a function)
main/internal_functions.c:41: initializer element is not constant
main/internal_functions.c:41: (near initialization for `php_builtin_extensions[0]')
main/internal_functions.c:42: `phpext_tokenizer_ptr' undeclared here (not in a function)
main/internal_functions.c:42: initializer element is not constant
main/internal_functions.c:42: (near initialization for `php_builtin_extensions[1]')
main/internal_functions.c:43: `phpext_standard_ptr' undeclared here (not in a function)
main/internal_functions.c:43: initializer element is not constant
main/internal_functions.c:43: (near initialization for `php_builtin_extensions[2]')
main/internal_functions.c:44: `phpext_session_ptr' undeclared here (not in a function)
main/internal_functions.c:44: initializer element is not constant
main/internal_functions.c:44: (near initialization for `php_builtin_extensions[3]')
main/internal_functions.c:45: `phpext_posix_ptr' undeclared here (not in a function)
main/internal_functions.c:45: initializer element is not constant
main/internal_functions.c:45: (near initialization for `php_builtin_extensions[4]')
main/internal_functions.c:46: `phpext_pcre_ptr' undeclared here (not in a function)
main/internal_functions.c:46: initializer element is not constant
main/internal_functions.c:46: (near initialization for `php_builtin_extensions[5]')
main/internal_functions.c:47: `phpext_overload_ptr' undeclared here (not in a function)
main/internal_functions.c:47: initializer element is not constant
main/internal_functions.c:47: (near initialization for `php_builtin_extensions[6]')
main/internal_functions.c:48: `phpext_mysql_ptr' undeclared here (not in a function)
main/internal_functions.c:48: initializer element is not constant
main/internal_functions.c:48: (near initialization for `php_builtin_extensions[7]')
main/internal_functions.c:49: `phpext_ctype_ptr' undeclared here (not in a function)
main/internal_functions.c:49: initializer element is not constant
main/internal_functions.c:49: (near initialization for `php_builtin_extensions[8]')
*** Error code 1
make: Fatal error: Command failed for target `main/internal_functions.lo'
```

OK, I see how the file "main/internal_functions.c" had been cretad by "./configure" :

```
bash−2.05# grep internal_functions config.status
echo "creating main/internal_functions.c"
sh ./build/genif.sh ./main/internal_functions.c.in . "" gawk $extensions > main/internal_functions.c

bash−2.05# pkgrm SMCgawk

bash−2.05# cp main/internal_functions.c /tmp/internal_functions.c;bad

bash−2.05# rm −Rf php−4.3.1.tar
bash−2.05# gunzip −c php−4.3.1.tar
bash−2.05# cd ../php−4.3.1
bash−2.05# CFLAGS='−DEAPI' ./configure −−with−apxs=/usr/local/apache/bin/apxs −−with−mysql=/usr/local/mysql −−with−zlib=/usr/local
−−with−gd

bash−2.05# grep internal_functions config.status
echo "creating main/internal_functions.c"
```

```
sh ./build/genif.sh ./main/internal_functions.c.in . "" nawk $extensions > main/internal_functions.c
```

Here, nawk is used instead of gawk now.

```
bash−2.05# make
bash−2.05# make install
```

All is OK now and all work correctly.

If I make a diff on the new "main/internal_functions.c" and the old one "/tmp/internal_functions.c", I can see a big difference.

The reason is a BUG in the version of Sed on Solaris
(the sed in PATH in most of the solaris systems is the broken one which can't handle lines over 1024 chars)
For more information, you can read this archive e−mail ===>

http://mail.gnu.org/archive/html/libtool/2001−07/msg00101.html

2 − Configuration

Verify that all these lines have been added in your "httpd.conf" in "/usr/local/apache/conf" :

```
LoadModule php4_module libexec/libphp4.so
AddModule mod_php4.c
AddType application/x−httpd−php .php
```

You can add "index.php" in the DirectoryIndex property too.

Restart apache :

```
bash−2.05# apache stop
bash−2.05# apache startssl
```

3 − Test

Create a file "test.php" contening the following code :

```
<?
$date = date("d−m−Y");
$heure = date("H:i");
Print("Nous sommes le $date et il est $heure");
?>
```

and place it in your DocumentRoot, here it's "/web".

Open your browser and see the result :

https://your_acid_computer/test.php

If you see the date, it's OK.

VII − Acid

1 − Installation

```
bash−2.05# gunzip −c jpgraph−1.12.1.tar.gz | tar xvf −
bash−2.05# gunzip −c adodb340.tgz | tar xvf −
bash−2.05# gunzip −c acid−0.9.6b23.tar.gz | tar xvf −
bash−2.05# cp −R jpgraph−1.12.1 /web/jpgraph
bash−2.05# cp −R adodb /web/
bash−2.05# cp −R acid /web/
bash−2.05# vi /web/acid/acid_conf.php
```

2 − Configuration

```
$DBlib_path = "../adodb";
$DBtype = "mysql";
```

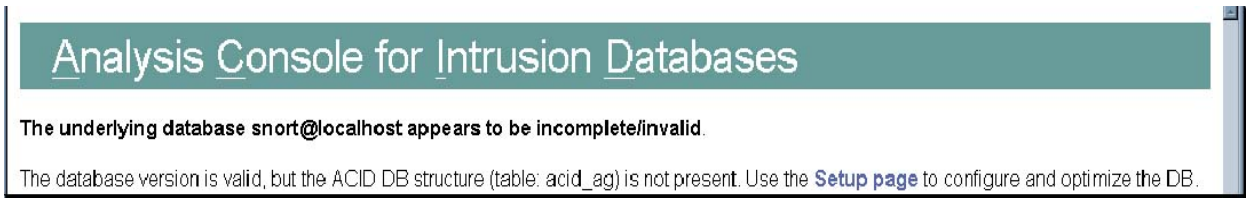
```
$alert_dbname = "snort";
$alert_host = "localhost";
$alert_port = "";
$alert_user = "snort";
$alert_password = "your_snort_password";
$ChartLib_path = "../jpgraph/src";
```

For all information on all parameters in the file "acid_vonf.php",
you can have a look at this URL ===>

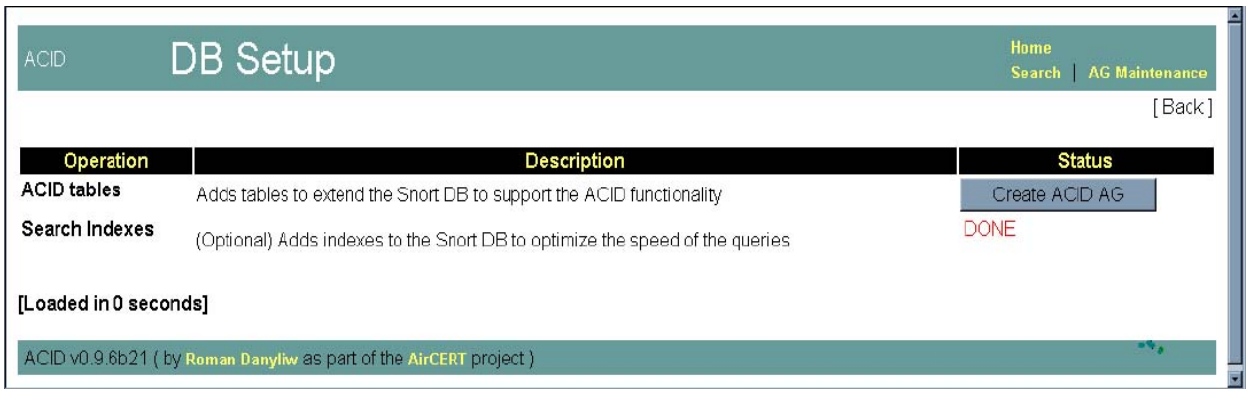
http://acidlab.sourceforge.net/acid_params.html

After, we can go to :

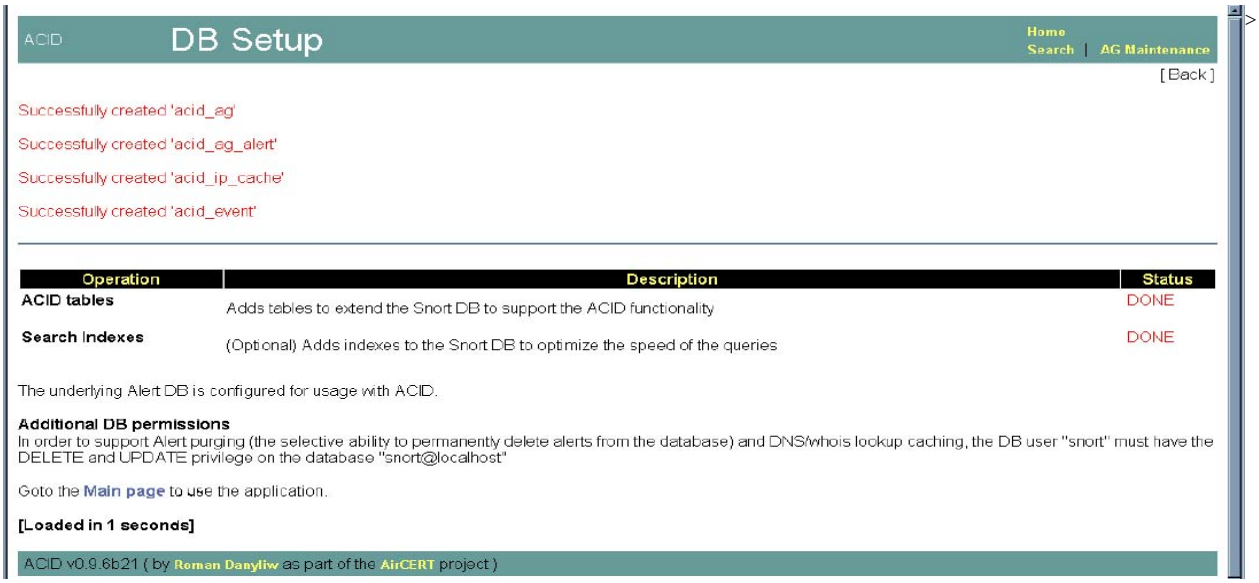
https://your_acid_computer/acid/acid_main.php



Click on "Setup Page".



On this third page, click on the button "Create ACID AG" will create the necessary tables for ACID



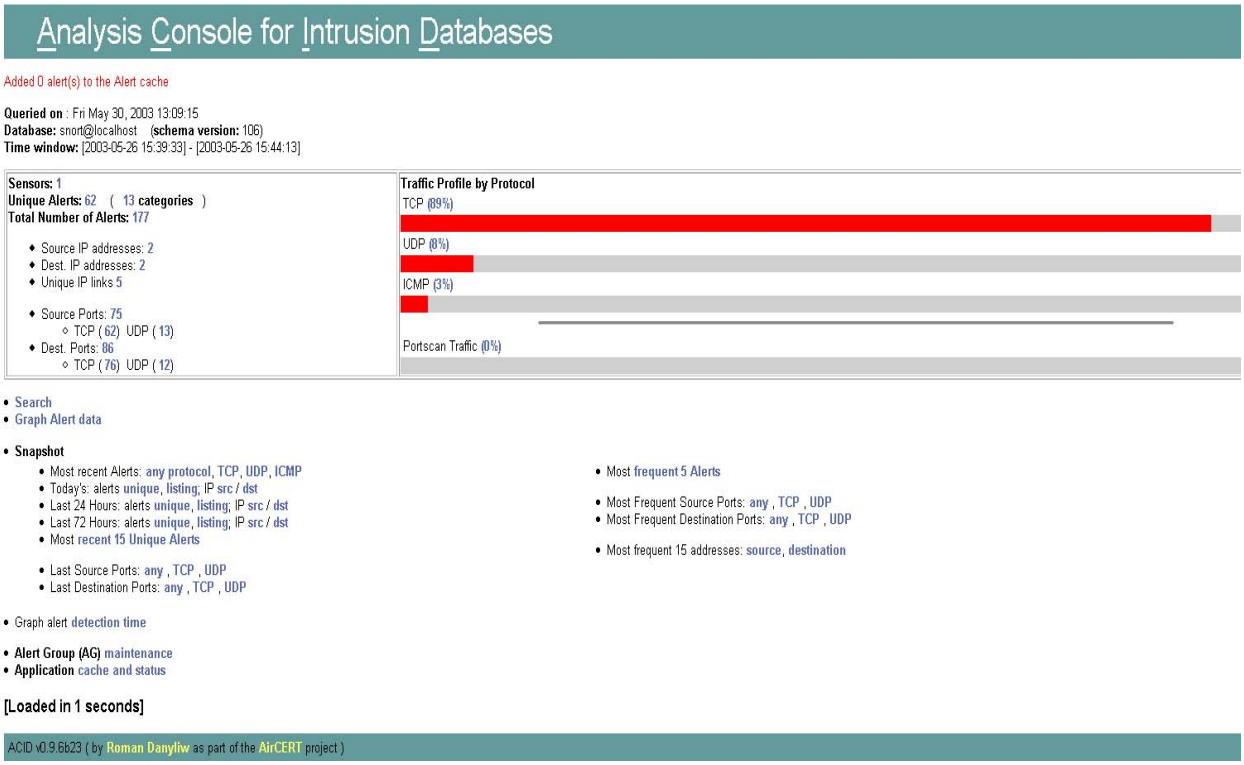
You can verify this by the following way :

```
bash−2.05# mysql−u snort −p
mysql> connect snort
mysql> show tables;
+−−−−−−−−−−−−−−−−−−+
| Tables_in_snort |
+−−−−−−−−−−−−−−−−−−+
| acid_ag |
| acid_ag_alert |
| acid_event |
| acid_ip_cache |
| data |
| detail |
| encoding |
| event |
| icmphdr |
| iphdr |
| opt |
| reference |
| reference_system |
| schema |
| sensor |
| sig_class |
| sig_reference |
| signature |
| tcphdr |
| udphdr |
+−−−−−−−−−−−−−−−−−−+
20 rows in set (0.00 sec)
mysql> exit
```

3 − Test

```
bash−2.05# mkdir −p /var/snort/log
bash−2.05# snort −devyq −c /usr/local/snort/etc/snort.conf −l /var/snort/log −D
```

https://your_acid_computer/acid/acid_main.php



VIII − After the installation

You can update you ".bashrc", ".cshrc" or ".profile" file.
Here is an extract of my ".bashrc" file :

```
bash−2.05# more /.bashrc"

PATH=/usr/bin:/usr/sbin:/usr/local/bin:/usr/dt/bin:/usr/openwin/bin:/usr/ccs/bin:/usr/local/ssl/bin
export PATH

MANPATH=/usr/dt/man:/usr/man:/usr/openwin/share/man:/usr/local/man
export MANPATH

LD_LIBRARY_PATH=/usr/lib:/usr/local/lib:/usr/local/sll/lib
export LD_LIBRARY_PATH

alias ids='snort −devyq −c /usr/local/snort/etc/snort.conf −l /var/snort/log −D'
```

Subscribe quickly to the mailling list of snort :

http://www.snort.org/lists.html

Explore all programs in relation with Snort. Do not rewrite when it's already existing :

http://www.snort.org/dl/

Test your Snort installation with several product :

http://www.nessus.org/

http://ftester.sourceforge.net/

http://tcpreplay.sourceforge.net/

Need specific help :

http://marc.theaimsgroup.com/?l=snort−users