Herramientas de monitoreo y administración de redes

M. Farias-Elinos

Lab. de Investigación y Desarrollo de Tecnología Avanzada (LIDETEA)
Dirección de Posgrado e Investigación, Universidad La Salle
Grupo de Seguridad de RedCUDI (Internet-2 México)
e-mail: elinos@ci.ulsa.mx
http://seguridad.internet2.ulsa.mx/

May 25, 2011

1. cacti
2. Nagios
3. Net-SNMP
4. log-servers
5. Nessus
6. RT
7. Acceso vía Internet

Cacti + cacti-plugins

- Herramienta gráfica que permite sensar los dispositivos de la red.
- Utiliza el protocolo SNMP

Operabilidad

Extracción Extraer los datos de los dispositivos, principalmente usando SNMP, pero puede utilizar scripts

Almacenamiento Guarda la información de los dispositivos en un DBMS y la información extraida en una base de datos tipo RRD

Presentación Despliegue de la información de manera gráfica vía web.

Requisitos

- httpd (Apache)
- php
- net-snmp
- php-snmp
- mysql
- php-mysql
- mysql-server (solo si el DBMS es el mismo servidor)
- rrdtool
- rrdtool-php

Instalación

```
 # yum install -y httpd php net-snmp php-snmp
mysql php-mysql mysql-server cacti cacti-docs
rrdtool rrdtool-php
# /etc/init.d/mysqld start
# mysqladmin -u root password t3mp0r41
# mysqladmin -u root -p create cacti
# cd /var/www/cacti
# mysql cacti -p < cacti-all.sql
# mysql cacti -p < cacti-plugins.sql
# mysql -u root mysql -p
mysql> grant all on cacti.* to cacti@localhost
identified by 'cactipwd';
mysql> flush privileges;
mysql> \q
```

Instalación: Editar archivo */etc/httpd/config.d/cacti.conf*

```
Alias /cacti/ /var/www/cacti/
<Directory /var/www/cacti/>
DirectoryIndex index.php
Options -Indexes
AllowOverride all
order deny,allow
deny from all
allow from all
AddType application/x-httpd-php .php
php_flag magic_quotes_gpc on
php_flag track_vars on
</Directory>
```

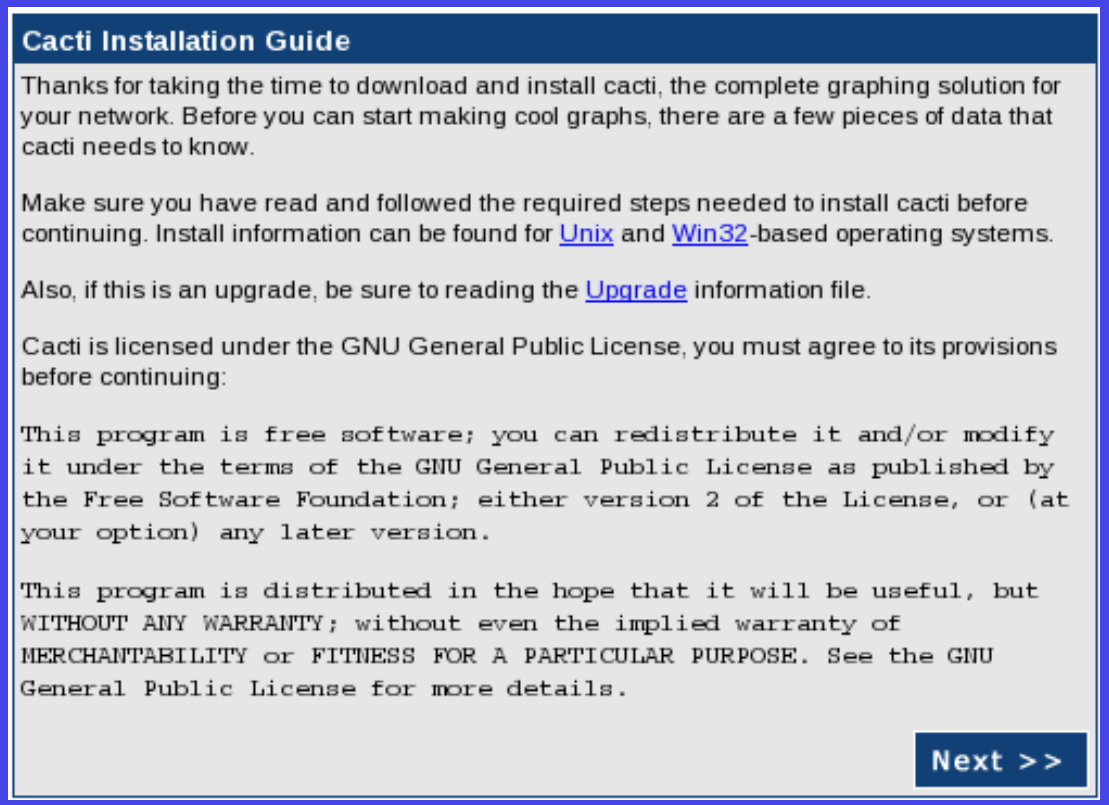
Instalación

```
 # /etc/init.d/httpd start
# chkconfig --level 235 mysqld on
# chkconfig --level 235 httpd on
```

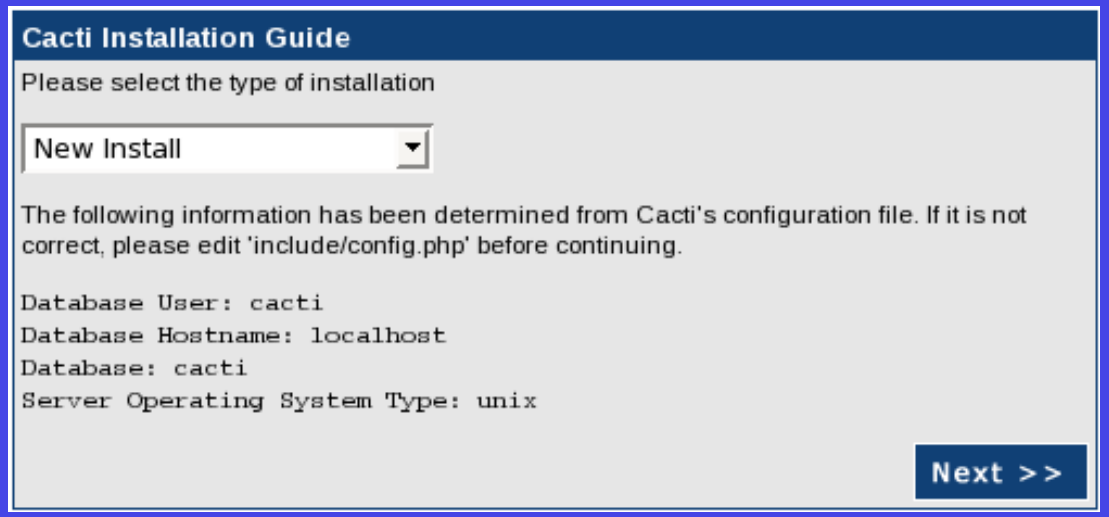
Instalación: Editar archivo *include/config.php*

```
$database_type = "mysql";
$database_default = "cacti";
$database_hostname = "localhost";
$database_username = "cacti";
$database_password = "cactipwd";
$database_port = "3306";
```

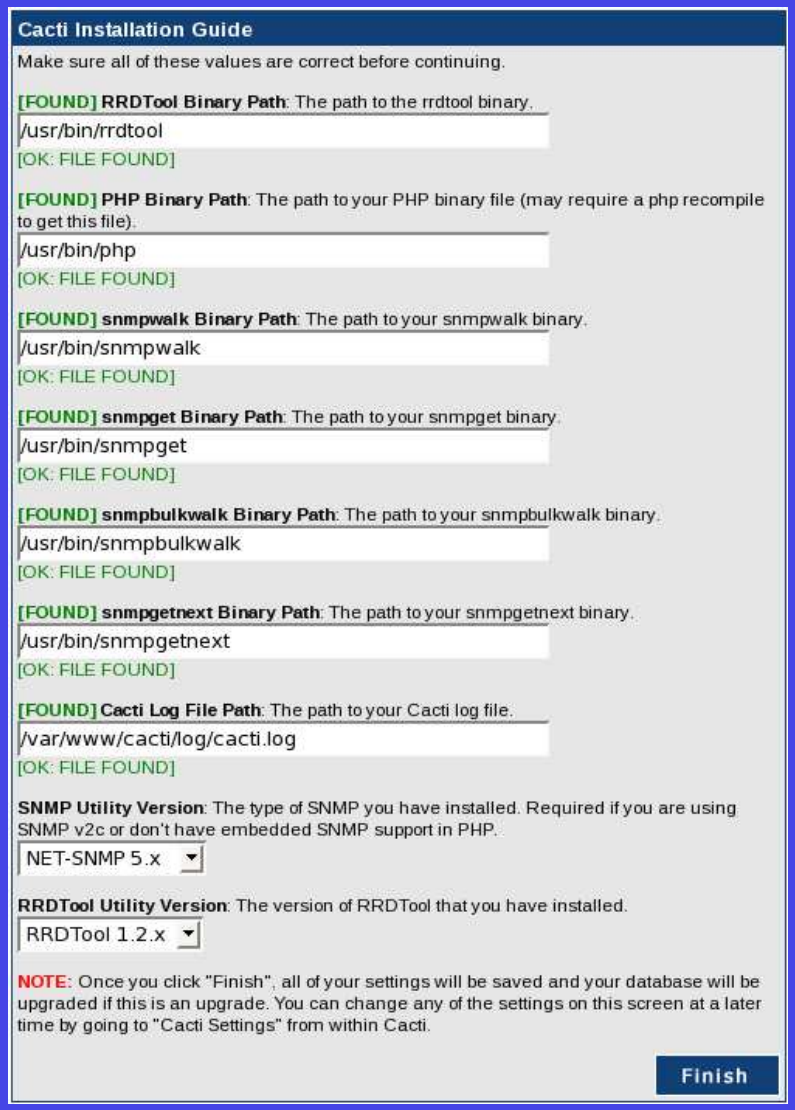
Instalación



Instalación



Instalación



Instalación

```
# mysql cacti -p < cacti-plugins.sql
```

Nagios

- Herramienta gráfica que permite sensar principalmente los servicios de una red.

Instalación

```
 # yum install -y nagios*
# /etc/init.d/nagios start
# chkconfig --level 235 nagios on
```

Archivos de configuración

```
 /etc/nagios/nagios.cfg
/etc/nagios/objects/localhost.cfg
/etc/nagios/objects/windows.cfg
/etc/nagios/objects/printer.cfg
/etc/nagios/objects/switches.cfg
/etc/nagios/objects/commands.cfg
/etc/nagios/objects/contacts.cfg
/etc/nagios/objects/timeperiods.cfg
/etc/nagios/objects/templates.cfg
```

Archivos de configuración

```
 /etc/nagios/servers
/etc/nagios/printers
/etc/nagios/switches
/etc/nagios/routers
```

Arbol de MIB’s

- 1.3.6.1.2.1 - SNMP MIB-2
- 1.3.6.1.4.1 - SNMP Private Enterprise

rsyslog + phplogcon

- Herramienta que recauda los eventos (logs) de los dispositivos y los almacena en una BD
- Consola de visualización de eventos.

Instalación

```
 # yum install -y rsyslog rsyslog-mysql
mysql-server phplogcon php httpd php-mysql
# /etc/init.d/mysqld start
# mysqladmin -u root password t3mp0r41
# useradd syslog
# cd /usr/share/doc/rsyslog-mysql-3.21.3
# mysql -p < createDB.sql
# mysql -u root mysql -p
mysql> grant all on Syslog.* to
syslog@localhost identified by 'syslogpwd';
mysql> flush privileges;
mysql> \q
# chcon -h -t httpd_sys_script_rw_t
/etc/phplogcon/config.php
```

Instalación: Agregar al archivo */etc/rsyslog.conf*

```
 $ModLoad ommysql.so
$ModLoad imudp.so
$UDPServerRun 514
*.* :ommysql:127.0.0.1,Syslog,syslog,syslogpwd
```

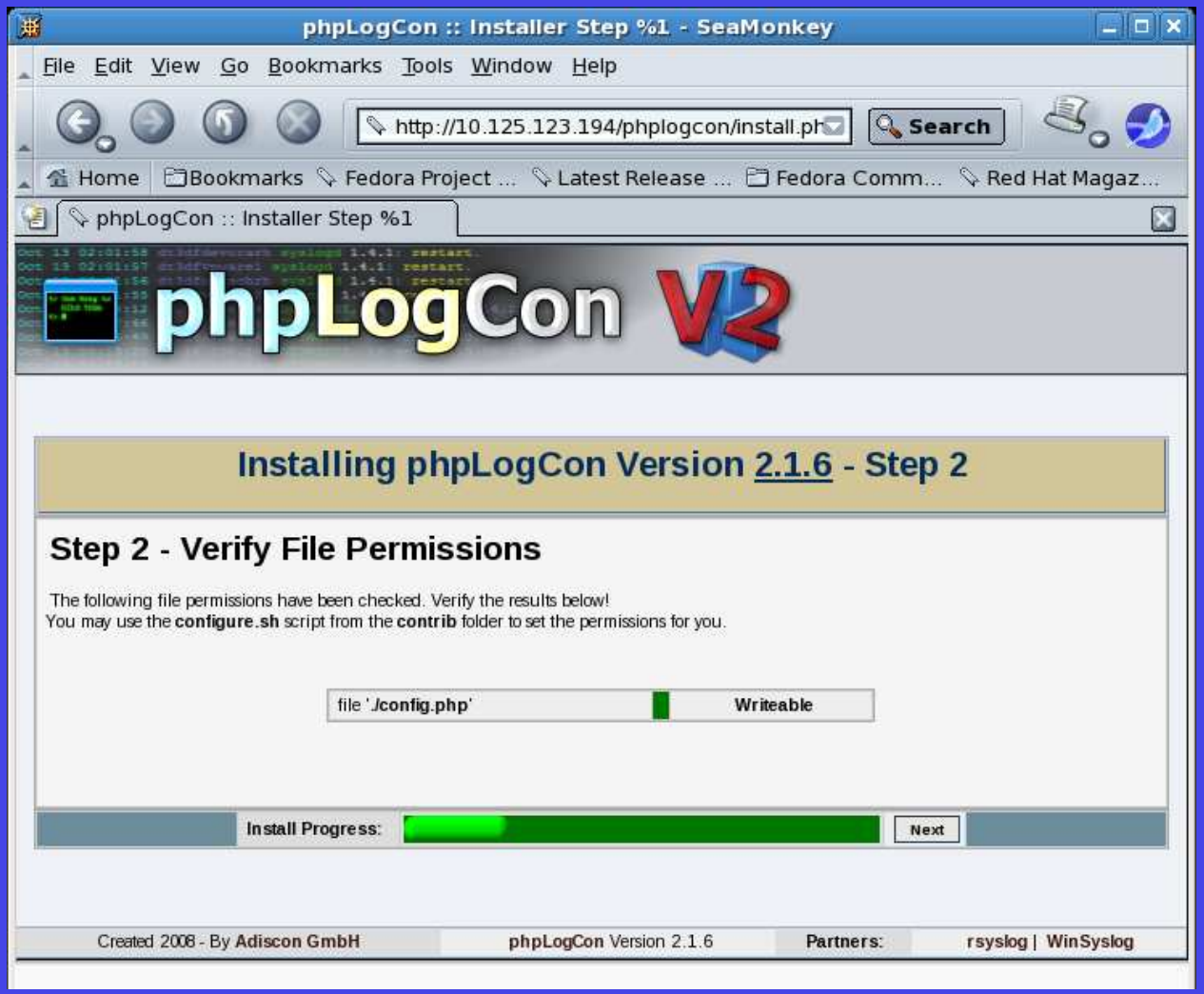
Instalación

```
 # /etc/init.d/syslog stop
# /etc/init.d/rsyslog start
# chkconfig --level 235 mysql on
# chkconfig --level 2345 syslog off
# chkconfig --level 235 rsyslog on
```

Instalación

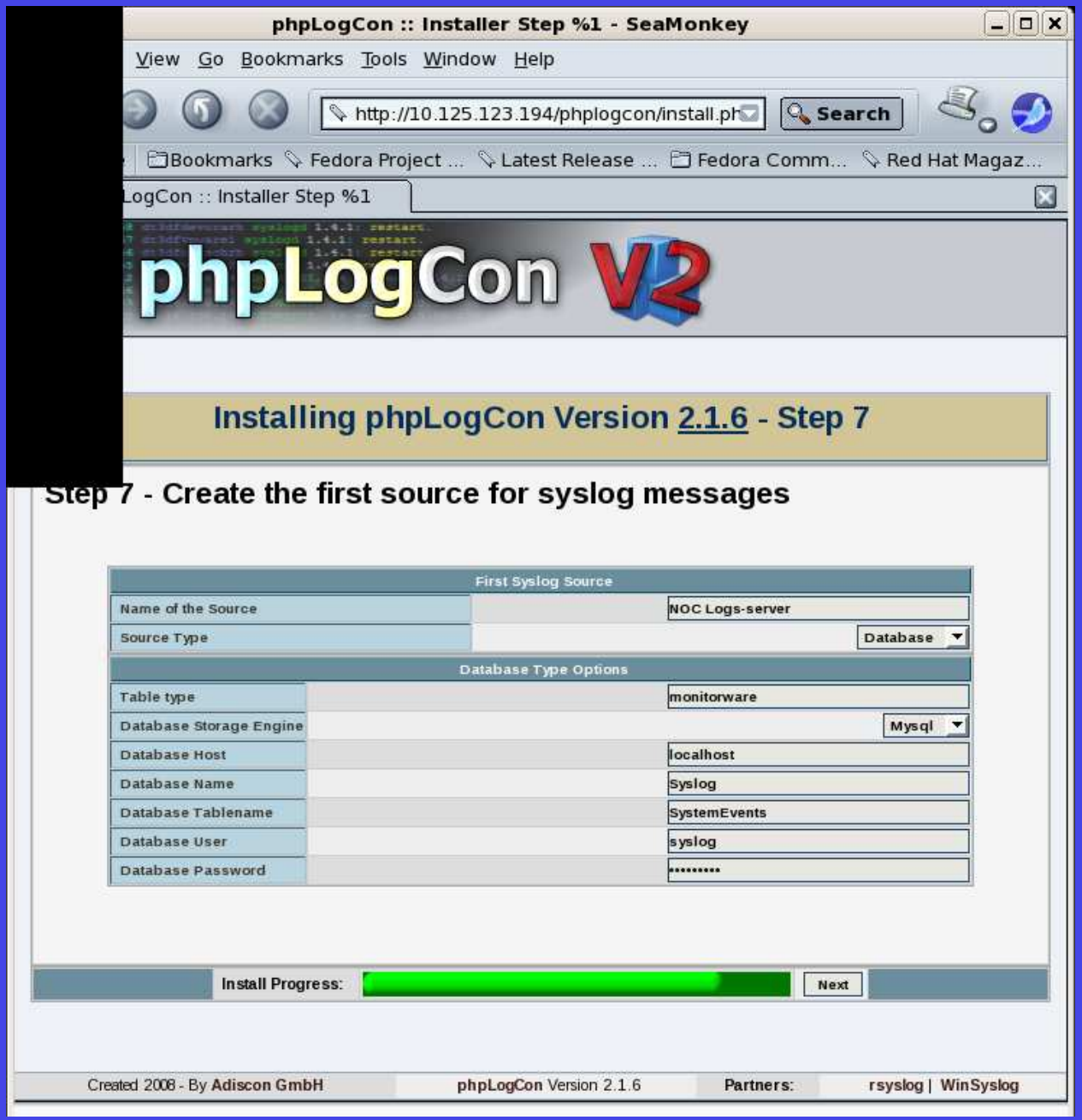
Instalación

Instalación



Instalación

Instalación



Instalación

Nessus

- Herramienta que detecta vulnerabilidades en equipos

Instalación

```
 # yum install -y nessus nessus-client
# nessus-fetch --register
8A58-1715-BCC0-1FF9-7CB4
# nessus-mkcert
# nessus-adduser
# chkconfig --level 235 nessusd on
# /etc/init.d/nessusd start
```

rt3

- Herramienta que permite administrar tickets de soporte

Instalación

```
 # yum install -y rt3 mysql-server php httpd
php-mysql
# /etc/init.d/mysqld start
# mysqladmin -u root password t3mp0r41
# useradd rt3
```

Instalación: Editar el archivo */etc/rt3/RT_Config.pm*

```
Set($DatabaseUser , 'rt3');
Set($DatabasePassword , 'rt3pwd');
Set($DatabaseName , 'rt3');
```

Instalación: Editar el archivo */etc/selinux/config*

```
SELINUX=disable
```

Instalación: Agregar al archivo */etc/group*

```
rt3:x:502:apache
```

Instalación

```
 # rt-setup-database -action init -dba root
-prompt-for-dba-password
```

Acceso a repositorio

- Losc paquetes se encuentran accesibles en el sito de *Tlapixqui*
- Seguir los siguientes paso *root*
- Posteriormente con el comando **yum** se puede instalar los paquetes que vismos.

Instalación/activación de repositorio

```
 # cd /etc/yum.repo.d
# wget -c
http://www.tlapixqui.org.mx/tlapixqui.repo
```

Herramientas de monitoreo y administración de redes

M. Farias-Elinos

Lab. de Investigación y Desarrollo de Tecnología Avanzada (LIDETEA)
Dirección de Posgrado e Investigación, Universidad La Salle
Grupo de Seguridad de RedCUDI (Internet-2 México)
e-mail: elinos@ci.ulsa.mx
http://seguridad.internet2.ulsa.mx/

May 25, 2011