

# 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.ulsal.mx](mailto:elinos@ci.ulsal.mx)

<http://seguridad.internet2.ulsal.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 sensor 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 extraída 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 t3mp0r4l
# 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

### Cacti Installation Guide

Thanks for taking the time to download and install cacti, the complete graphing solution for your network. Before you can start making cool graphs, there are a few pieces of data that cacti needs to know.

Make sure you have read and followed the required steps needed to install cacti before continuing. Install information can be found for [Unix](#) and [Win32](#)-based operating systems.

Also, if this is an upgrade, be sure to reading the [Upgrade](#) information file.

Cacti is licensed under the GNU General Public License, you must agree to its provisions before continuing:

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.

Next >>

## Instalación

### Cacti Installation Guide

Please select the type of installation

New Install

The following information has been determined from Cacti's configuration file. If it is not correct, please edit 'include/config.php' before continuing.

Database User: cacti

Database Hostname: localhost

Database: cacti

Server Operating System Type: unix

Next >>

# Instalación

## Cacti Installation Guide

Make sure all of these values are correct before continuing.

**[FOUND] RRDTool Binary Path:** The path to the rrdtool binary.

/usr/bin/rrdtool

[OK: FILE FOUND]

**[FOUND] PHP Binary Path:** The path to your PHP binary file (may require a php recompile to get this file).

/usr/bin/php

[OK: FILE FOUND]

**[FOUND] snmpwalk Binary Path:** The path to your snmpwalk binary.

/usr/bin/snmpwalk

[OK: FILE FOUND]

**[FOUND] snmpget Binary Path:** The path to your snmpget binary.

/usr/bin/snmpget

[OK: FILE FOUND]

**[FOUND] snmpbulkwalk Binary Path:** The path to your snmpbulkwalk binary.

/usr/bin/snmpbulkwalk

[OK: FILE FOUND]

**[FOUND] snmpgetnext Binary Path:** The path to your snmpgetnext binary.

/usr/bin/snmpgetnext

[OK: FILE FOUND]

**[FOUND] Cacti Log File Path:** The path to your Cacti log file.

/var/www/cacti/log/cacti.log

[OK: FILE FOUND]

**SNMP Utility Version:** The type of SNMP you have installed. Required if you are using SNMP v2c or don't have embedded SNMP support in PHP.

NET-SNMP 5.x

**RRDTool Utility Version:** The version of RRDTool that you have installed.

RRDTool 1.2.x

**NOTE:** Once you click "Finish", all of your settings will be saved and your database will be upgraded if this is an upgrade. You can change any of the settings on this screen at a later time by going to "Cacti Settings" from within Cacti.

Finish

## Instalación

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

## Nagios

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

**Nagios**<sup>®</sup>

## 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
```

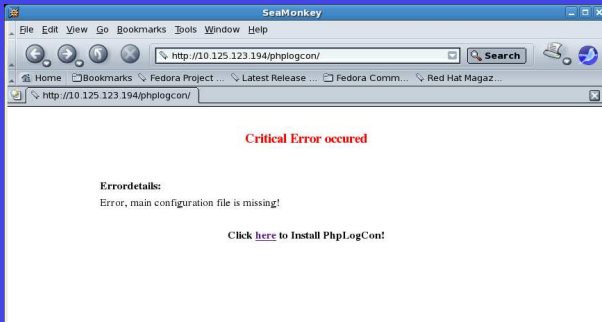
**Instalación: Agregar al archivo */etc/rsyslog.conf***

```
$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



The screenshot shows a web browser window titled "phpLogCon :: Installer Step %1 - SeaMonkey". The address bar contains the URL "http://10.125.123.194/phplogcon/install.ph". The main content area displays the "phpLogCon V2" logo and the heading "Installing phpLogCon Version 2.1.6 - Step 1". Below this, the section "Step 1 - Prerequisites" contains the following text:

Before you start installing phpLogCon, the Installer setup has to check a few things first. You may have to correct some file permissions first.

Click on  to start the Test!

At the bottom of the installer window, there is a progress bar labeled "Install Progress:" which is partially filled with green. To the right of the progress bar is a "Next" button. The footer of the installer window contains the following information:

Created 2008 - By Adiscon GmbH      phpLogCon Version 2.1.6      Partners:      rsyslog | WinSyslog



# Instalación

The screenshot shows a web browser window titled "phpLogCon :: Installer Step %1 - SeaMonkey". The address bar contains the URL "http://10.125.123.194/phplogcon/install.ph". The browser's address bar also shows "phpLogCon :: Installer Step %1".

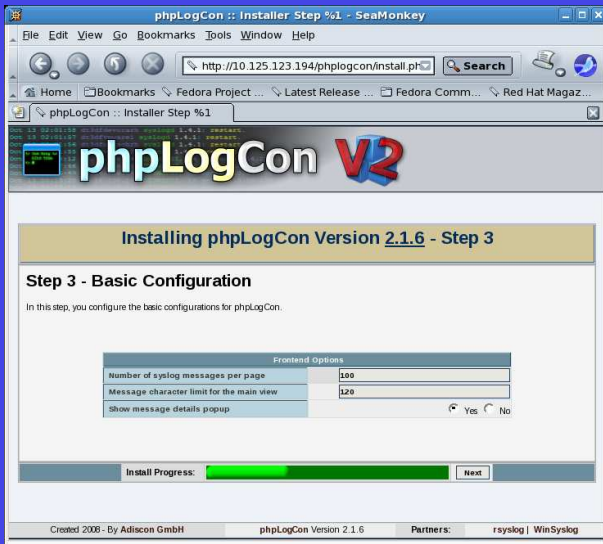
The main content area features the "phpLogCon V2" logo. Below the logo, a yellow banner reads "Installing phpLogCon Version 2.1.6 - Step 2".

The section is titled "Step 2 - Verify File Permissions". Below the title, it states: "The following file permissions have been checked. Verify the results below! You may use the `configure.sh` script from the `contrib` folder to set the permissions for you."

A progress bar shows the status of the file permissions check for "file './config.php'". The bar is green and labeled "Writable".

At the bottom of the installer, there is a footer with the following information: "Created 2008 - By Adiscon GmbH", "phpLogCon Version 2.1.6", "Partners: rsyslog | WinSyslog", and an "Install Progress:" indicator with a green bar and a "Next" button.

# Instalación



The screenshot shows a web browser window titled "phpLogCon :: Installer Step %1 - SeaMonkey". The address bar contains "http://10.125.123.194/phplogcon/install.ph". The page content includes the "phpLogCon V2" logo, a title "Installing phpLogCon Version 2.1.6 - Step 3", and a section "Step 3 - Basic Configuration". Below this, a text block states: "In this step, you configure the basic configurations for phpLogCon." A table titled "Frontend Options" contains three rows: "Number of syslog messages per page" with a value of 100, "Message character limit for the main view" with a value of 120, and "Show message details popup" with radio buttons for "Yes" (selected) and "No". At the bottom of the configuration area is a progress bar labeled "Install Progress:" and a "Next" button. The footer contains: "Created 2008 - By Adiscon GmbH", "phpLogCon Version 2.1.6", "Partners: rsyslog | WinSyslog", and logos for "Grupo Aridad" and "Integrat" in the bottom right corner.

phpLogCon V2

## Installing phpLogCon Version 2.1.6 - Step 3

### Step 3 - Basic Configuration

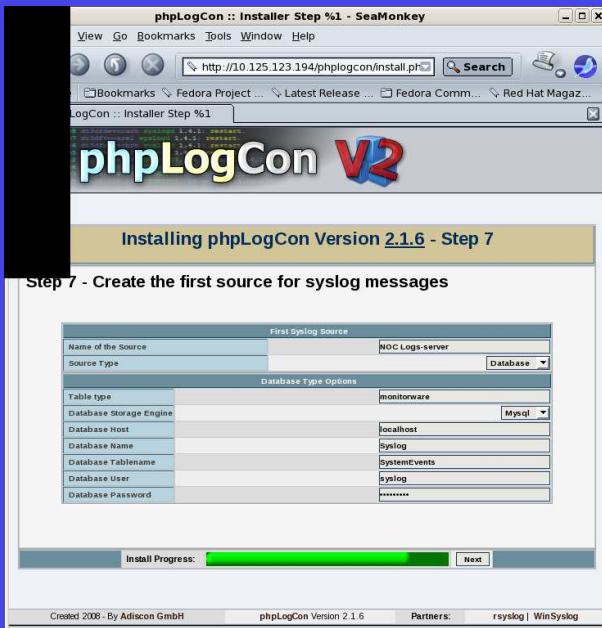
In this step, you configure the basic configurations for phpLogCon.

Frontend Options	
Number of syslog messages per page	100
Message character limit for the main view	120
Show message details popup	<input checked="" type="radio"/> Yes <input type="radio"/> No

Install Progress:

Created 2008 - By Adiscon GmbH      phpLogCon Version 2.1.6      Partners: rsyslog | WinSyslog

Grupo Aridad  
Integrat



The screenshot shows a web browser window titled "phpLogCon :: Installer Step %1 - SeaMonkey". The address bar contains "http://10.125.123.194/phplogcon/install.ph". The page content includes the "phpLogCon V2" logo and a yellow banner that reads "Installing phpLogCon Version 2.1.6 - Step 7". Below the banner, the heading "Step 7 - Create the first source for syslog messages" is displayed. The main form is titled "First Syslog Source" and contains the following fields:

First Syslog Source	
Name of the Source	NOC Logs-server
Source Type	Database
Database Type Options	
Table type	monitorware
Database Storage Engine	Mysql
Database Host	localhost
Database Name	Syslog
Database Tablename	SystemEvents
Database User	syslog
Database Password	*****

At the bottom of the form, there is an "Install Progress:" indicator with a green progress bar and a "Next" button.

Created 2006 - By Adiscon GmbH      phpLogCon Version 2.1.6      Partners:      rsyslog | WinSyslog

# Instalación



The screenshot shows a web browser window titled "phpLogCon :: Installer Step %1 - SeaMonkey". The address bar contains the URL "http://10.125.123.194/phplogcon/install.ph". The browser's address bar also shows "phpLogCon :: Installer Step %1". The main content area features the "phpLogCon V2" logo at the top. Below the logo, a yellow banner reads "Installing phpLogCon Version 2.1.6 - Step 8". The main text area is titled "Step 8 - Done" and contains the following text: "Congratulations! You have successfully installed phpLogCon :D!", "To finish the Installation, remove the file install.php from the main directory!", and "Click [here](#) to go to your installation." At the bottom of the main content area, there is a progress bar labeled "Install Progress:" which is filled with green, and a "Finish!" button. The footer of the page contains the text: "Created 2008 - By Adiscon GmbH", "phpLogCon Version 2.1.6", "Partners: rsyslog | WinSyslog".

## 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.ulsal.mx](mailto:elinos@ci.ulsal.mx)

<http://seguridad.internet2.ulsal.mx/>

May 25, 2011

