

server-01

Table of contents

Table of contents
Main goals
Getting started: Creating the snapshots for lab6
Assignment 1: The Setting Updating and initial configuration for monitor (server-04)
Assignment 2: The Core I Installation and configuration of remote <i>configuration</i> tools: WEBMIN6
Assignment 3: The Core II Installation and configuration of remote monitoring tools: GANGLIA 8
[OPTIONAL] Assignment 4: More interesting tools I: Installation and configuration of remote
monitoring tools: NAGIOS 3
[OPTIONAL] Assignment 5: More interesting tools II: Installation and use of basic administration
tools: LINUX tools

Main goals

 \circ $\,$ To learn about processes for adapting basic servers to certain needs. In this case:

- Installation and configuration of some of the most relevant tools for remote **configuration and monitoring** in Linux (Open Source).
- Adapting the web service under specific organizational and security premises:
 - o Webmin
 - o Ganglia Monitor
 - o Nagios 3
 - Linux tools (auxiliary)

Getting started: Creating the snapshots for lab6

- 1. Create a new snapshot on the following **VMs**:
 - a. Clone_P1 \rightarrow snapshot_P6.
 - b. Clone_P3 \rightarrow snapshot_P6.
 - c. Clone_P4 \rightarrow snapshot_P6.
 - d. $Clone_{P5} \rightarrow snapshot_{P6}$.
 - e. Remember to keep the VM off.

Assignment 1: The Setting

Updating and initial configuration for **monitor** (server-04)

We will re-use *clone_P4* (server-04) to deploy a monitoring and configuration center that allows us to keep control of our entire service in our virtual infrastructure. Make sure that snapshot_P6 on *clone_P4* is available.

- 1. You will have to adapt your clone_P4 to turn it into a **monitoring and configuration center** for all our deployed services. So, carry out the tasks required as follows:
 - a. First, update the system from debian repositories.
 - b. Then, make an "alias" for server-04 in the DNS service deployed in Lab1 (server-01). Also, be sure that /etc/hosts is properly updated on both servers.
 - 1. Alias: monitor \rightarrow server-04
- Configure the VirtualBox environment to access the web services on server-01, server-03, server-04 and server-05 from your host (PC or Laptop), using its web browser:
 - a. Add the following new rules in the custom NAT network "network_1":
 - i. IP host (127.0.0.1), port 8014 → IP server-04 (192.168.0.14), port 80.
 - ii. IP host (127.0.0.1), port 10011 → IP server-01 (192.168.0.11), port 10000.
 - IP host (127.0.0.1), port 10013 → IP server-03 (192.168.0.13), port 10000.
 - iv. IP host (127.0.0.1), port 10015 → IP server-05 (192.168.0.15), port 10000.
 - v. IP host (127.0.0.1), port 10014 → IP server-04 (192.168.0.14), port 10000.

Assignment 2: The Core I

Installation and configuration of remote configuration tools: WEBMIN

Once that's done, we will begin with the configuration service <u>Webmin</u> that allows us to configure every feature of both operating systems and services running on our servers. Webmin uses a centralized web interface, restricted access and form-based, to enable administrators to configure everything.

- 1. *Installation* of the **Webmin** app¹. Keep the default configuration during the installation process.
 - a. Install it on all our virtual servers:
 - 1. server-01
 - 2. server-03
 - 3. server-04
 - 4. server-05
 - b. Add (link) the webmin apps on server-01, server-03 and server-05 to monitor (server-04) as webmin clients.
 - 1. Clue: Webmin Server Index
- 2. Initial configuration:
 - a. Restrict IP access to webmin to only computers in the 192.168.0.0 subnet.
 - b. Modify the *default* language to the Spanish language (Spanish ES.UTF-8).
- 3. Advanced configuration:
 - Administrator profiles: Enable a new administrator profile (*operator*). This will have a sub-set of root (*administrator*) rights. The administrator will have all available rights. However, the operator will have only have the rights required to manage the service. For server-04, those are WEB, MySQL and SSH services. Design these profiles (roles) yourself.
 - b. Enable the necessary webmin modules to manage configuration of the following services:
 - 1. server-01:
 - 1. LDAP Server/Client/Users and Groups
 - 2. BIND DNS
 - 3. NTP
 - 4. DHCP
 - **2**. server-03:
 - 1. NFS
 - 2. Samba File Sharing
 - 3. Linux RAID

¹ Use the official debian software repositories

- 3. server-04/monitor:
 - 1. Web (Apache)
 - 2. Webalizer logfile analysis
- **4**. server-05:
 - 1. Postfix Mail Server
 - 2. Dovecot IMAP/POP3 Server
- c. Perform the following monitor setup tasks using Webmin:
 - 1. Modify the default "runlevel" for server-05 to "single user"
 - 2. Create a new LDAP group and user:
 - 1. Username: user_monitor
 - 2. UID: 2010
 - 3. GID: 2000 (grp1)
 - 4. Default shell: /bin/bash
 - 5. User must change password at first login.
 - 6. Account expires on January 1st, 2020
 - 7. Force user to change password every 3 months
 - 8. Add GECON data: Phone number, e-mail address ...
- d. From server-04, using Webmin, configure the follow services:
 - 1. NFS service on server-02:
 - 1. Disable /scratch as directory exported by NFS.
 - 2. WEB service on server-04:
 - 1. Disable the **secure_csda** *virtualhost* in apache2.
 - 3. MAIL services on server-05:
 - 1. Send every mail log of postfix/imap services to /var/log/correocorporativo.log on server-04

Assignment 3: The Core II

Installation and configuration of remote monitoring tools: GANGLIA

- 1. *Installation* of the **Ganglia Monitor** app². Install and configure as a global monitoring tool. Remember that you will have to install the following items on monitor:
 - a. Gmetad (server)
 - b. Gmond (client)
 - c. Web-frontend (server)
- 2. Initial configuration:

We will begin by configuring the virtual host monitor as a ganglia **server/client**. In other words, it will act as a monitoring server and monitored client. To do this, follow the instructions below:

- a. Server side:
 - 1. Define a new "cluster" called "CSDA". Server-04 (monitor) will be the first host to monitor.
 - 2. Use the **8655** TCP port to link clients to server.
- b. Client side:
 - 1. Link clients to "CSDA" cluster.
 - 2. Use "multicast" communications.
 - 1. Multicast address: 239.2.11.71
 - 3. Remember to use the 8655 TCP port between clients and server.
- 3. Adding new hosts to monitor:
 - a. Install Ganglia Monitor (client) on server-01, server-03 and server-05.
 - b. Configure the Ganglia client side on server-01, server-03 and server-05, according to the following data:
 - 1. Link clients to "CSDA" cluster.
 - 2. Use "multicast" communications.
 - 1. Multicast address: 239.2.11.71
 - 3. Remember to use the **8655** TCP port between clients and server.
- 4. *Improving security*. Add a new security mechanism to HTTP apache2 on server-04:
 - a. Configure apache2 so that it restricts access to Ganglia. Access from clients (browsers) will be protected by an administrator password.
 - 1. To do this, use **htaccess** Apache mechanism.
 - b. Also, restrict IP access to Ganglia to 192.168.0.0.

² Use the official debian software repositories

[OPTIONAL] Assignment 4: More interesting tools I:

Installation and configuration of remote monitoring tools: NAGIOS 3

- 1. *Installation* of the **Nagios 3** app³. Install and configure as a global monitoring and *warning* tool. Remember that you will have to install the following items on monitor:
 - a. Nagios3
- 2. Configuration:
 - a. Define the Nagios network with these clients:
 - server-01
 server-03
 server-04 (monitor)
 - 4. server-05
 - b. Add 4 new profiles of host. Each one will mean a different *computing* feature and include as members all the hosts previously defined:
 - 1. Groups (profiles):
 - 1. ALL
 - a. Members: everyone
 - 2. HTTP servers
 - a. Members: server-04 (monitor)
 - 3. SSH servers
 - a. Members: everyone
 - 4. Affordable Hosts
 - a. Members: everyone
 - c. Associated service configuration for each host:
 - 1. server-01
 - 1. ping
 - 2. SSH
 - 2. server-03
 - 1. ping
 - 2. SSH
 - 3. server-04/monitor
 - 1. ping
 - 2. SSH
 - 3. http
 - 4. defaults:
 - a. Local disks checking (free space)
 - b. System load (activity) checking

³ Use the official debian software repositories

```
c. System processes (number of) checking
d. System users (number of) checking
4. client

ping
SSH
```

The final objective is for the Nagios monitoring service to look as follows:

Last Updated: I Updated every : Nagios® Core* Logged in as ma View History F View Notificati View Host Stat	Mon Apr 28 17:52:3 90 seconds '3.4.1 - www.nagios agiosadmin for all hosts tons For All Hosts us Detail For All Ho	org	2	Down Unreacl 3 0 All Problems 3	aable Pending 0 All Types 5	B O O 6 O All Problems All Types 6 14
Host **	Service **	Status **	Last Check **	Duration **	Attempt **	Status Information
cliente	Check Ping	CRITICAL				CRITICAL - Host Unreachable (192.168.0.20)
	SSH	CRITICAL	2014-04-28 17: 50: 03	0d 0h 42m 4s	4/4	No existe ninguna ruta hasta el `host'
monitor O	Current Load	OK	2014-04-28 17:51:12	0d 0h 36m 48s	1/4	OK - load average: 0.01, 0.05, 0.05
montor (o						USERS OK - 2 users currently logged in
						DISK OK
	нттр	ок				HTTP OK HTTP/1.1 200 OK - 316 bytes in 0,002 second response time
	SSH	ок	2014-04-28 17:47:55	Od Oh 33m Os	1/4	SSH OK - OpenSSH 6.0p1 Debian-4+deb7u1 (protocol 2.0)
	Total Processes	OK	2014-04-28 17:51:35	0d 0h 36m 26s	1/4	PROCS OK: 85 processes
server-01	Check Ping	OK	2014-04-28 17:52:12	Od Oh 10m 18s	1/4	PING OK - Packet loss = 0%, RTA = 0.43 ms
	SSH	OK	2014-04-28 17:50:49	0d 0h 38m 48s	1/4	SSH OK - OpenSSH_6.0p1 Debian-4 (protocol 2.0)
server-02	Check Ping	CRITICAL	2014-04-28 17:48:59	0d 0h 8m 31s	1/4	CRITICAL - Host Unreachable (192, 168, 0, 12)
	SSH	CRITICAL	2014-04-28 17: 50: 46	0d 0h 6m 44s	1/4	No existe ninguna ruta hasta el `host'
server-03	Check Ping	CRITICAL	2014-04-28 17:47:33	0d 0h 9m 57s	1/4	CRITICAL - Host Unreachable (192, 168,0, 13)
	SSH	CRITICAL				No existe ninguna ruta hasta el `host'
Results 1 - 14 oj	f 14 Matching Servi	ces				
	Last Updated. Updated every Nagios® Core" Logged in av View History View HothFat View HothFat Limit Results Hot ** cliente monitor server-01 server-02 server-03	Updated every 90 seconds Nagios Core* 3.4.1. www.nagios Logged in as nagiosadmin View History Torall hots View Notifications For All Hots View Hots Status Detail For All Hot View Hots Status Detail For All Hot Host ◆ Service ◆ cliente Check Ping SSH inchitor Conserve Core Disk Space HTTP SSH Total Processes server-01 Check Ping SSH server-03 Check Ping SSH	Latt Updated Mon Apr 78 17 52 30 CEST 2014 Updated every 900 econds Nagios® Core" 3 41 - www.nagios.org Logged in a nggiosadmin View History For all hosts View Host Status Detail For All Hosts View Host Status Detail For All Hosts Limit Remits 100 • Host • Service • Status • Cliente Check Ping CRITICAL SSH OK Dick Space 0K HTTP OK SSH OK server-01 Check Ping CRITICAL SSH OK server-02 Check Ping CRITICAL SSH OK	Last Updated Mon Apr 38 17 52 30 CEST 2014 Updated were 90 osconds Nagios® Core" 3.41 . www nagios org Logged in a nagiosadmin View History Far all hots View Hote Status Detail For All Hots View Hote Status Detail For All Hots View Hote Status Detail For All Hots Cervice Hots ** Service * Status * Last Check ** cliente Check Ping CRITICAL 2014-04-28 17.52.12 Disk Space OK 2014-04-28 17.52.12 Disk Space OK 2014-04-28 17.52.12 Disk Space OK 2014-04-28 17.52.12 Disk Space OK 2014-04-28 17.52.12 SH OK 2014-04-28 17.54.12 OK 2014-04-28 17.52.12 SH OK 2014-04-28 17.54.12 OK 2014-04-28 17.52.12 SH OK 2014-04-28 17.54.20 SH OK 2014-04-28 17.64.50 SH OK 2014-04-28 17.54.20 SH OK 2014-04-28 17.64.50 SH OK 2014-04-28 17.64.50 S	Last Updated Mon Apr 38 17 52 30 CEST 2014 Updated were 90 osconds Nagios® Core" 3.41 www nagios org Logged in a nagiosadmin View History Far all hots View Hote Status Detail For All Hots View Hote Status Detail For All Hots View Hote Status Detail For All Hots Carrote Logged in a constraint of the status of the status of the status Detail For All Hots SSH CARTEGAL 2014-04.28 17.51.21 04 0h 35m 51s Disk Space OK 2014-04.28 17.51.21 04 0h 35m 54s Processes Server-02 Check Ping Carrotal OK 2014-04.28 17.51.21 04 0h 35m 54s SSH OK 2014-04.28 17.54.50 04 0h 55m 45s SSH OK 2014-04.28 17.48.50 04 0h 55	Last Updated Mon Apr 28 17 52 30 CEST 2014 Updated were 90 esconds Nagios® Core" 3.41 - www.nagios.org Logged in a nagiosadimus View History Fer all hosts View Host Status Detail For All Hosts SH CRITICAL 20140428 17:50 00 do hosts Sis 1/4 SH CRITICAL 20140428 17:52 10 do hosts Sis 1/4 SH CRITICAL 20140428 17:54 50 do host Sis 1/4 SH CRITICAL 20140428 17:54 50 do host Sis 1/4 SH CRITICAL 20140428 17:54 50 do host Sis 1/4 SH CRITICAL 20140428 17:49 20

- 3. *Improving security*. As with Ganglia, add a new security mechanism to HTTP apache2 on server-04:
 - a. Configure apache2 so that it restricts access to Nagios. Access from clients (browsers) will be protected by an administrator password.
 - To do this, use **htaccess** Apache mechanism.
 - b. Also, restrict IP access to Nagios to 192.168.0.0.

[OPTIONAL] Assignment 5: More interesting tools II:

Installation and use of basic administration tools: LINUX tools ...

- 1. Enable process accounting on monitor: acct
 - a. Check and evaluate its proper operation. What do you think this tool might be useful for?
- 2. Configure **rsyslog** on server-01, server-03 and server-05 in order to dump the main log information about *auth* and *syslog* on our monitor server server-04.
- Install and configure the following tools about log analysis, early detection of potential attacks and system failures, bug detections ... Briefly describe their operation modes and how they can be useful. → (Maybe, you can use some Webmin modules)
 - a. Webalizer Logfile Analysis ("unused")
 - b. Ksystemlog
 - c. Logwatch
- 4. Install and <u>check the proper operation</u> of these tool packages:
 - a. iostat
 - b. pidstat
 - c. mpstat
 - d. sar
 - e. nfsstat
 - f. lsof

For each command, you have to show its main functionality as a monitoring tool and its operation mode.

- 5. Install and <u>check the proper operation</u> of these *tool packages*:
 - a. iptraf (no configuration, only install)
 - b. nmap (no configuration, only install)
 - c. tcpdump

Once again, for each command, you have to show its main functionality as a monitoring tool and its operation mode.

Document all the installation and configuration processes carried out for the use of these tools, as well as therelevantchecksoftheiroperation.

References and resources

- 1. man
- 2. Google
- 3. Slides:
 → https://gitlab.com/herreroja/G679
- 4. And more:

Webmin

[1] http://www.webmin.com/

Ganglia

[2] http://ganglia.sourceforge.net/

Nagios

[3] http://www.nagios.org/