

UNIVERSITY OF PORTO
FACULDADE DE ENGENHARIA

Systems and Network Management Tools
Lab work 5

Contents

1	Introduction	2
2	Setup	2
2.1	Web Server	2
2.2	NTP server	2
2.3	Mail server	3
2.4	DNS server	3
2.5	FTP server	4
3	Nagios	4
3.1	Features	4
4	Presenting the monitoring results of Nagios	5
4.1	Failures	6
5	Zabbix	7
5.1	Features	7
6	Presenting the monitoring results of Zabbix	7
6.1	Failures	8
7	Other monitoring tools	9
7.1	Grafana	9
7.2	Features	9
7.3	openDCIM	10
7.4	Features	10
7.5	Comparison	11
8	Conclusion	11

1 Introduction

The objective of this work is to sensitize the student to the potentialities in the use of freeware public tools for the management of equipment or services, and in particular in the monitoring component. To do this, it is suggested to use freeware network management platforms **Nagios** and **Zabbix**.

2 Setup

Tux22 has configured the following servers: Web server, an FTP/sFTP server, an NTP server, an E-mail server and a DNS cache server.

2.1 Web Server

Web server is a server that can satisfy client by replying on this requests on the World Wide Web. It receives HTTP Requests and send HTTP Responses to the browser. To demonstrate working web server on our second computer, we used a software called *curl* that provides transferring data with URLs (in Figure 1).

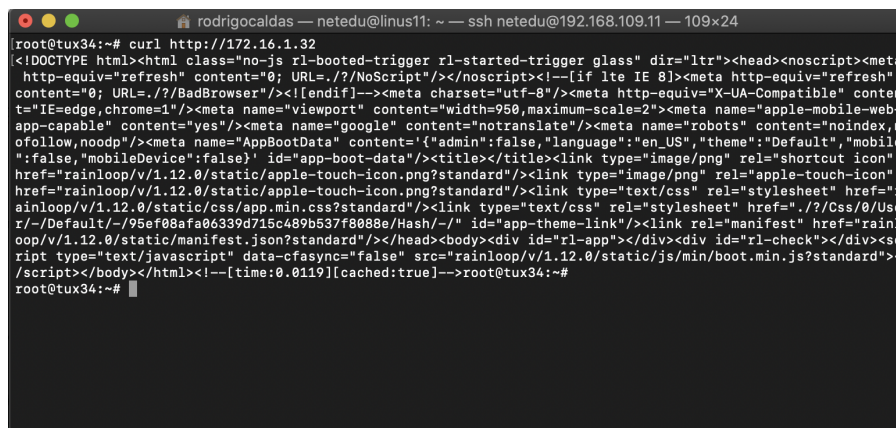
A terminal window titled 'rodrigocaldas — netedu@linus11: ~ — ssh netedu@192.168.109.11 — 109x24'. The prompt is 'root@tux34:~#'. The command 'curl http://172.16.1.32' has been executed. The output is an HTML document. The first line is '<!DOCTYPE html><html class="no-js rl-booted-trigger rl-started-trigger glass" dir="ltr"><head><noscript><meta'. The second line is 'http-equiv="refresh" content="0; URL=./?NoScript"/></noscript><!--[if lte IE 8]><meta http-equiv="refresh'. The third line is 'content="0; URL=./?BadBrowser"/><![endif]></meta charset="utf-8"/><meta http-equiv="X-UA-Compatible" conten'. The fourth line is 't="IE=edge,chrome=1"/><meta name="viewport" content="width=960,maximum-scale=2"><meta name="apple-mobile-web'. The fifth line is 'app-capable" content="yes"/><meta name="google" content="notranslate"/><meta name="robots" content="noindex,n'. The sixth line is 'ofollow,noodp"/><meta name="AppBootData" content="{"admin":false,"language":"en_US","theme":"Default","mobile'. The seventh line is '":false,"mobileDevice":false}' id="app-boot-data"/><title></title><link type="image/png" rel="shortcut icon'. The eighth line is 'href="rainloop/v/1.12.0/static/apple-touch-icon.png?standard"/><link type="image/png" rel="apple-touch-icon'. The ninth line is 'href="rainloop/v/1.12.0/static/apple-touch-icon.png?standard"/><link type="text/css" rel="stylesheet" href="r'. The tenth line is 'ainloop/v/1.12.0/static/css/app.min.css?standard"/><link type="text/css" rel="stylesheet" href="./?/Css/0/Use'. The eleventh line is 'r/-/Default/-/95ef08afa06339d715c489b537f08088e/Hash/-/" id="app-theme-link"/><link rel="manifest" href="rainl'. The twelfth line is 'oop/v/1.12.0/static/manifest.json?standard"/></head><body><div id="rl-app"></div><div id="rl-check"></div><se'. The thirteenth line is 'ript type="text/javascript" data-cfasync="false" src="rainloop/v/1.12.0/static/js/min/boot.min.js?standard"><. The fourteenth line is '/script></body></html><!--[time:0.0119][cached:true]>-->root@tux34:~#'. The prompt is 'root@tux34:~#'.

Figure 1: Web Server sends the HTTP Response to client

2.2 NTP server

Network time protocol is used to synchronize time between computers over the world according to the Coordinated Universal Time. It sends and receives timestamps using UDP diagrams on port number 123. The current protocol version is 4. The most common command is *ntpdate* to sync time from the server – in our case server *172.16.1.32* as shown in Figure 2.

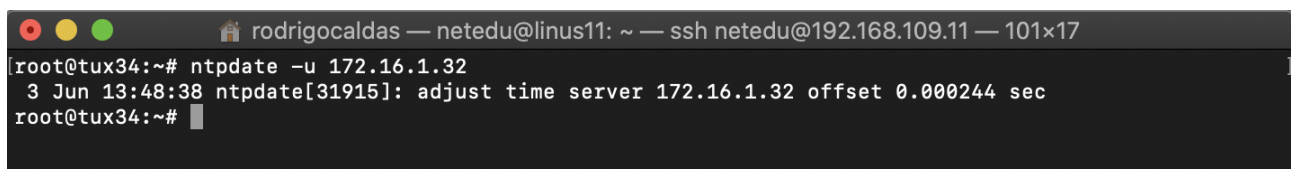
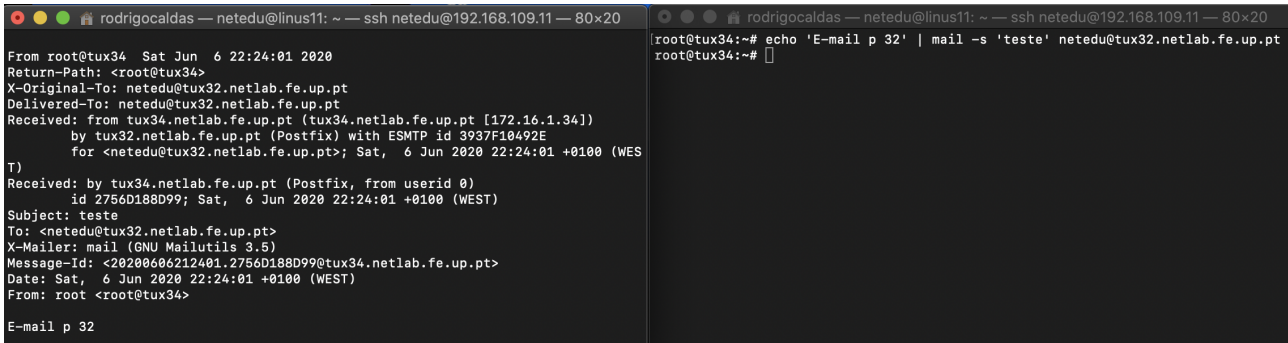
A terminal window titled 'rodrigocaldas — netedu@linus11: ~ — ssh netedu@192.168.109.11 — 101x17'. The prompt is 'root@tux34:~#'. The command 'ntpdate -u 172.16.1.32' has been executed. The output is '3 Jun 13:48:38 ntpdate[31915]: adjust time server 172.16.1.32 offset 0.000244 sec'. The prompt is 'root@tux34:~#'.

Figure 2: NTP server sends the timestamp to sync the time on client

2.3 Mail server

Mail servers care about sending an email to the right client. There are two types of mail servers – income and outcome mail servers. The most common outcome server is SMTP (Simple Mail Transfer Protocol) and the most known income servers are IMAP or POP3. We installed the mail server with Postfix using this guide <https://www.tecmint.com/install-postfix-mail-server-with-webmail-in-debian/>.

In Figure 3 there is an example of client-server communication where computer 4 sends an email to computer 2 where the mail server is running.



```
rodrigocaldas — netedu@linus11: ~ — ssh netedu@192.168.109.11 — 80x20
From root@tux34 Sat Jun 6 22:24:01 2020
Return-Path: <root@tux34>
X-Original-To: netedu@tux32.netlab.fe.up.pt
Delivered-To: netedu@tux32.netlab.fe.up.pt
Received: from tux34.netlab.fe.up.pt (tux34.netlab.fe.up.pt [172.16.1.34])
    by tux32.netlab.fe.up.pt (Postfix) with ESMTP id 3937F10492E
    for <netedu@tux32.netlab.fe.up.pt>; Sat, 6 Jun 2020 22:24:01 +0100 (WES
T)
Received: by tux34.netlab.fe.up.pt (Postfix, from userid 0)
    id 2756D188D99; Sat, 6 Jun 2020 22:24:01 +0100 (WEST)
Subject: teste
To: <netedu@tux32.netlab.fe.up.pt>
X-Mailer: mail (GNU Mailutils 3.5)
Message-Id: <20200606212401.2756D188D99@tux34.netlab.fe.up.pt>
Date: Sat, 6 Jun 2020 22:24:01 +0100 (WEST)
From: root <root@tux34>

E-mail p 32

rodrigocaldas — netedu@linus11: ~ — ssh netedu@192.168.109.11 — 80x20
root@tux34:~# echo 'E-mail p 32' | mail -s 'teste' netedu@tux32.netlab.fe.up.pt
root@tux34:~#
```

Figure 3: Client-server communication

2.4 DNS server

Domain name server is a hierarchical and decentralized naming system that is mainly responsible to find the correct IP address, but it has many other usage. In Figure 4 we used a tool *dig* to query the DNS running on computer 2.



```
rodrigocaldas — netedu@linus11: ~ — ssh netedu@192.168.109.11 — 109x24
root@tux34:~# dig @172.16.1.32 www.facebook.com

;<<>> DiG 9.11.5-P4-5.1+deb10u1-Debian <<>> @172.16.1.32 www.facebook.com
; (1 server found)
; global options: +cmd
; Got answer:
; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36147
; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 13, ADDITIONAL: 21

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 3399cf3441a83c655e576fb55ed799672877eb8985eece3f (good)
;; QUESTION SECTION:
;www.facebook.com.                IN      A

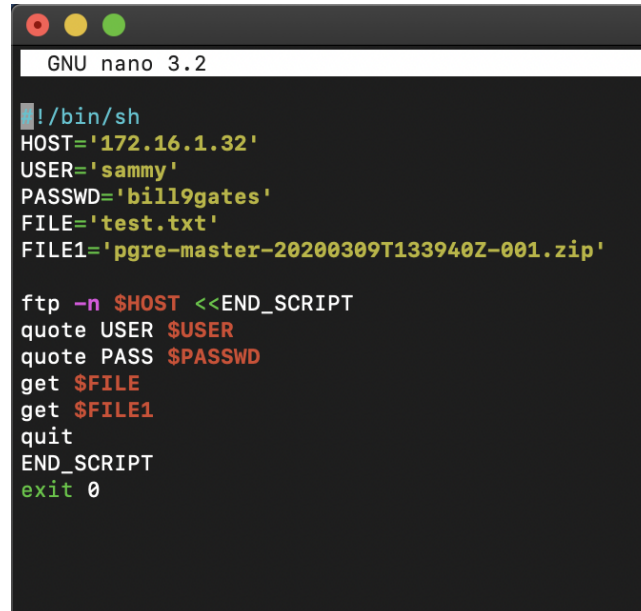
;; ANSWER SECTION:
www.facebook.com.                2136 IN    CNAME  star-mini.c10r.facebook.com.
star-mini.c10r.facebook.com.     59 IN    A      157.240.212.35

;; AUTHORITY SECTION:
.                               49354 IN    NS     k.root-servers.net.
.                               49354 IN    NS     a.root-servers.net.
.                               49354 IN    NS     f.root-servers.net.
.                               49354 IN    NS     e.root-servers.net.
```

Figure 4: DNS server

2.5 FTP server

File transfer protocol is as standard computer that is used for transferring files between client and a server. We created a script (Figure 5) that downloads a file through FTP, requested by the client to the server that is running on computer number 2.



```
GNU nano 3.2
#!/bin/sh
HOST='172.16.1.32'
USER='sammy'
PASSWD='bill9gates'
FILE='test.txt'
FILE1='pgre-master-20200309T133940Z-001.zip'

ftp -n $HOST <<END_SCRIPT
quote USER $USER
quote PASS $PASSWD
get $FILE
get $FILE1
quit
END_SCRIPT
exit 0
```

Figure 5: Script to download a file through FTP to server

3 Nagios

Is a free and open-source computer-software application that monitors systems, networks and infrastructure. Nagios offers monitoring and alerting services for servers, switches, applications and services. It alerts users when things go wrong and alerts them a second time when the problem has been resolved.

3.1 Features

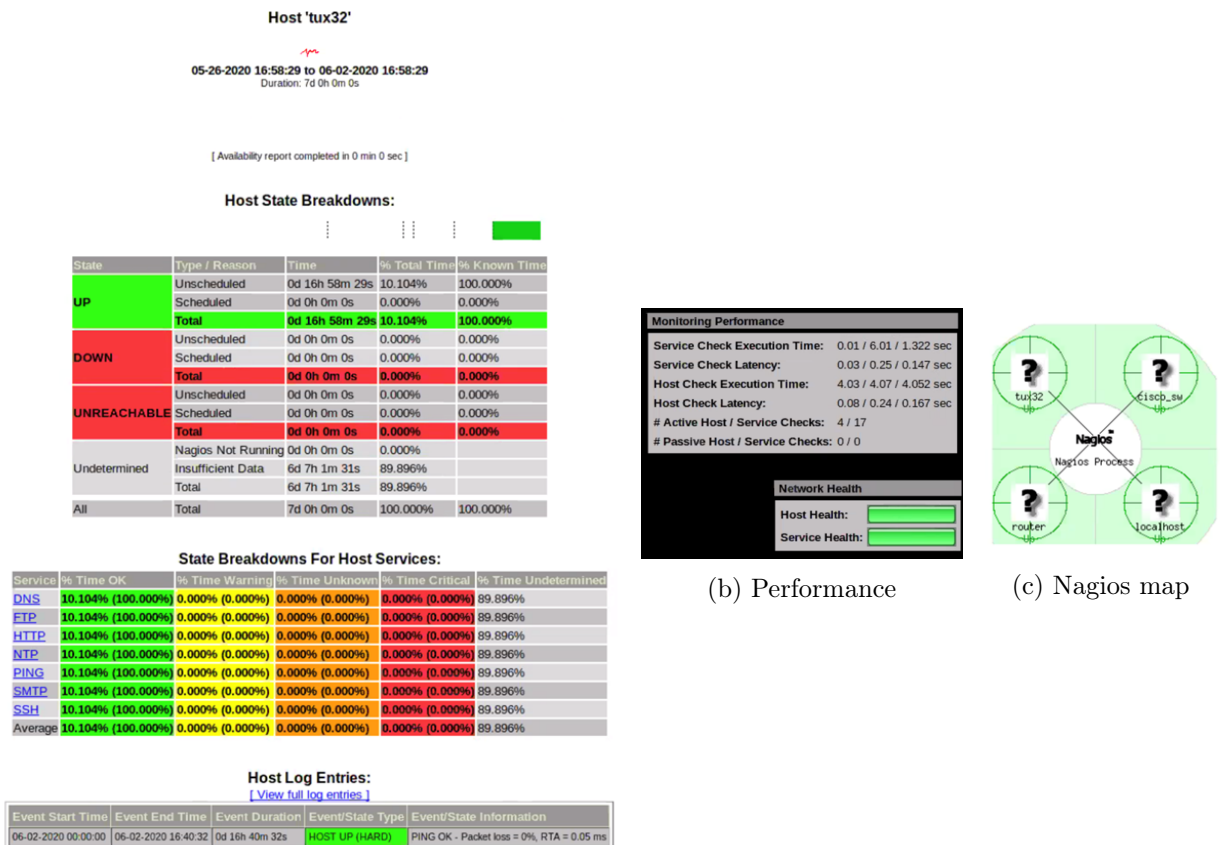
- Relatively scalable, Manageable, and Secure
- Good log and database system
- Automatically sends alerts if condition changes
- If the services are running fine, then there is no need to do check that host is an alive
- Helps you to detect network errors or server crashes
- You can troubleshoot the performance issues of the server.
- The issues, if any, can be fixed automatically as they are identified during the monitoring process
- The product's architecture is easy writing new plugins in the language of your choice
- Monitor network services like HTTP, SMTP, HTTP, SNMP, FTP, SSH, POP, etc.

4 Presenting the monitoring results of Nagios

Service Status Details For All Hosts

Host	Service	Status	Last Check	Duration	Attempt	Status Information
disc_sw	PING	OK	06-02-2020 16:54:41	1d 7h 6m 20s	1/3	PING OK - Packet loss = 0%, RTA = 1.38 ms
localhost	Current Load	OK	06-02-2020 16:50:52	3d 4h 36m 31s	1/4	OK - load average: 0.58, 0.79, 0.67
	Current Users	OK	06-02-2020 16:51:59	3d 4h 35m 53s	1/4	USERS OK - 2 users currently logged in
	HTTP	OK	06-02-2020 16:55:19	2d 6h 12m 16s	1/4	HTTP OK: HTTP/1.1 200 OK - 1873 bytes in 0.013 second response time
	PING	OK	06-02-2020 16:52:01	3d 4h 38m 37s	1/4	PING OK - Packet loss = 0%, RTA = 0.05 ms
	Root Partition	OK	06-02-2020 16:53:43	3d 4h 34m 1s	1/4	DISK OK - free space: / 62792 MB (90.95% inode=95%)
	SSH	OK	06-02-2020 16:54:35	3d 4h 38m 23s	1/4	SSH OK - OpenSSH_7.9p1 Debian-10+deb10u2 (protocol 2.0)
	Swap Usage	OK	06-02-2020 16:53:48	3d 4h 37m 46s	1/4	SWAP OK - 100% free (4050 MB out of 4077 MB)
router	Total Processes	OK	06-02-2020 16:55:42	3d 4h 37m 8s	1/4	PROCS OK - 120 processes with STATE = RSZDT
	PING	OK	06-02-2020 16:52:02	1d 19h 38m 59s	1/3	PING OK - Packet loss = 0%, RTA = 0.44 ms
tux32	DNS	OK	06-02-2020 16:51:37	1d 7h 4m 24s	1/4	DNS OK: 0.017 seconds response time. www.google.pt returns 172.217.168.163
	FTP	OK	06-02-2020 16:52:35	1d 7h 3m 26s	1/4	FTP OK - 0.002 second response time on 172.16.1.32 port 21 [vsFTPd 3.0.3]
	HTTP	OK	06-02-2020 16:53:33	1d 7h 2m 28s	1/4	HTTP OK: HTTP/1.1 200 OK - 1873 bytes in 0.014 second response time
	NTP	OK	06-02-2020 16:54:31	1d 7h 1m 30s	1/4	NTP OK: Offset -6.407499313e-06 secs
	PING	OK	06-02-2020 16:54:51	1d 7h 6m 10s	1/4	PING OK - Packet loss = 0%, RTA = 0.05 ms
	SMTP	OK	06-02-2020 16:55:49	1d 7h 5m 12s	1/4	SMTP OK - 0.001 sec. response time
	SSH	OK	06-02-2020 16:51:47	1d 7h 4m 14s	1/4	SSH OK - OpenSSH_7.9p1 Debian-10+deb10u2 (protocol 2.0)

Figure 6: Status details for all hosts



(b) Performance

(c) Nagios map

(a) Host State on TUX32

Figure 7: Results from Nagios

4.1 Failures

As a demonstration of good functioning of Nagios, two intentional server failures were intentionally caused:

- 1st failure on DNS Server

Service Status Details For All Hosts

Host	Service	Status	Last Check	Duration	Attempt	Status Information
nsco_sw	PING	OK	06-02-2020 17:19:41	1d 7h 32m 53s	1/3	PING OK - Packet loss = 0%, RTA = 2.96 ms
localhost	Current Load	OK	06-02-2020 17:22:03	3d 5h 3m 4s	1/4	OK - load average: 0.55, 0.61, 0.63
	Current Users	OK	06-02-2020 17:21:59	3d 5h 2m 26s	1/4	USERS OK - 3 users currently logged in
	HTTP	OK	06-02-2020 17:20:19	2d 6h 38m 49s	1/4	HTTP OK: HTTP/1.1 200 OK - 1873 bytes in 0.014 second response time
	PING	OK	06-02-2020 17:22:01	3d 5h 5m 10s	1/4	PING OK - Packet loss = 0%, RTA = 0.06 ms
	Root Partition	OK	06-02-2020 17:18:43	3d 5h 0m 34s	1/4	DISK OK - free space: / 62789 MB (90.95% inode=95%):
	SSH	OK	06-02-2020 17:19:35	3d 5h 4m 56s	1/4	SSH OK - OpenSSH_7.9p1 Debian-10+deb10u2 (protocol 2.0)
	Swap Usage	OK	06-02-2020 17:18:48	3d 5h 4m 19s	1/4	SWAP OK - 100% free (4053 MB out of 4077 MB)
router	Total Processes	OK	06-02-2020 17:20:42	3d 5h 3m 41s	1/4	PROCS OK: 146 processes with STATE = RSZDT
	PING	OK	06-02-2020 17:22:02	1d 20h 5m 32s	1/3	PING OK - Packet loss = 0%, RTA = 0.51 ms
sux32	DNS	CRITICAL	06-02-2020 17:21:37	0d 0h 0m 57s	1/4	CRITICAL - Plugin timed out while executing system call
	FTP	OK	06-02-2020 17:17:35	1d 7h 29m 59s	1/4	FTP OK - 0.002 second response time on 172.16.1.32 port 21 [vsFTPd 3.0.3]
	HTTP	OK	06-02-2020 17:18:33	1d 7h 29m 1s	1/4	HTTP OK: HTTP/1.1 200 OK - 1873 bytes in 0.013 second response time
	NTP	OK	06-02-2020 17:19:31	1d 7h 28m 3s	1/4	NTP OK: Offset -6.318092346e-06 secs
	PING	OK	06-02-2020 17:19:51	1d 7h 32m 43s	1/4	PING OK - Packet loss = 0%, RTA = 0.05 ms
	SMTP	OK	06-02-2020 17:20:49	1d 7h 31m 45s	1/4	SMTP OK - 0.001 sec. response time
	SSH	OK	06-02-2020 17:21:47	1d 7h 30m 47s	1/4	SSH OK - OpenSSH_7.9p1 Debian-10+deb10u2 (protocol 2.0)

Figure 8: Failure on DNS Server

- 2nd failure on NTP Server

Service Status Details For All Hosts

Host	Service	Status	Last Check	Duration	Attempt	Status Information
nsco_sw	PING	OK	06-02-2020 17:24:41	1d 7h 36m 16s	1/3	PING OK - Packet loss = 0%, RTA = 0.48 ms
localhost	Current Load	OK	06-02-2020 17:22:03	3d 5h 6m 27s	1/4	OK - load average: 0.55, 0.61, 0.63
	Current Users	OK	06-02-2020 17:21:59	3d 5h 5m 49s	1/4	USERS OK - 3 users currently logged in
	HTTP	OK	06-02-2020 17:25:19	2d 6h 42m 12s	1/4	HTTP OK: HTTP/1.1 200 OK - 1873 bytes in 0.013 second response time
	PING	OK	06-02-2020 17:22:01	3d 5h 8m 30s	1/4	PING OK - Packet loss = 0%, RTA = 0.06 ms
	Root Partition	OK	06-02-2020 17:23:43	3d 5h 3m 57s	1/4	DISK OK - free space: / 62789 MB (90.95% inode=95%):
	SSH	OK	06-02-2020 17:24:35	3d 5h 8m 19s	1/4	SSH OK - OpenSSH_7.9p1 Debian-10+deb10u2 (protocol 2.0)
	Swap Usage	OK	06-02-2020 17:23:48	3d 5h 7m 42s	1/4	SWAP OK - 100% free (4053 MB out of 4077 MB)
router	Total Processes	OK	06-02-2020 17:25:42	3d 5h 7m 4s	1/4	PROCS OK: 123 processes with STATE = RSZDT
	PING	OK	06-02-2020 17:22:02	1d 20h 8m 55s	1/3	PING OK - Packet loss = 0%, RTA = 0.51 ms
sux32	DNS	CRITICAL	06-02-2020 17:24:37	0d 0h 4m 20s	4/4	CRITICAL - Plugin timed out while executing system call
	FTP	OK	06-02-2020 17:22:35	1d 7h 33m 22s	1/4	FTP OK - 0.003 second response time on 172.16.1.32 port 21 [vsFTPd 3.0.3]
	HTTP	OK	06-02-2020 17:23:33	1d 7h 32m 24s	1/4	HTTP OK: HTTP/1.1 200 OK - 1873 bytes in 0.014 second response time
	NTP	CRITICAL	06-02-2020 17:25:31	0d 0h 1m 26s	2/4	CRITICAL - No response from NTP server
	PING	OK	06-02-2020 17:24:51	1d 7h 36m 6s	1/4	PING OK - Packet loss = 0%, RTA = 0.05 ms
	SMTP	OK	06-02-2020 17:25:49	1d 7h 35m 8s	1/4	SMTP OK - 0.001 sec. response time
	SSH	OK	06-02-2020 17:21:47	1d 7h 34m 10s	1/4	SSH OK - OpenSSH_7.9p1 Debian-10+deb10u2 (protocol 2.0)

Figure 9: Failure on NTP Server



Figure 10: Network health failures detected

5 Zabbix

Zabbix is an open-source monitoring software tool for diverse IT components, including networks, servers, virtual machines and cloud services.

5.1 Features

- High performance and high capacity.
- Auto-discovery of servers and network devices and interfaces.
- Low-level discovery, automatically starts monitoring new items, file systems or network interfaces among others.
- Distributed monitoring with centralized web administration.
- High-level (business) view of monitored resources through user-defined visual console screens and dashboards.

6 Presenting the monitoring results of Zabbix

▼ <input type="checkbox"/> Host	Name ▲	Last check	Last value	Change
▼ tux32	DNS Check (1 item)			
<input type="checkbox"/>	DNS	2020-06-02 19:51:09	1	Graph
▼ tux32	FTP service (1 item)			
<input type="checkbox"/>	FTP service is running	2020-06-02 19:51:01	Up (1)	Graph
▼ tux32	HTTP service (1 item)			
<input type="checkbox"/>	HTTP service is running	2020-06-02 19:50:57	Up (1)	Graph
▼ tux32	NTP service (1 item)			
<input type="checkbox"/>	NTP service is running	2020-06-02 19:51:02	Up (1)	Graph
▼ tux32	SMTP service (1 item)			
<input type="checkbox"/>	SMTP service is running	2020-06-02 19:50:56	Up (1)	Graph
▼ tux32	SSH service (1 item)			
<input type="checkbox"/>	SSH service is running	2020-06-02 19:51:03	Up (1)	Graph
▼ tux32	Status (3 items)			
<input type="checkbox"/>	ICMP loss	2020-06-02 19:51:02	0 %	Graph
<input type="checkbox"/>	ICMP ping	2020-06-02 19:51:02	Up (1)	Graph
<input type="checkbox"/>	ICMP response time	2020-06-02 19:51:02	0	Graph

Figure 11: Zabbix services page - all servers up

6.1 Failures

As a demonstration of good functioning of Zabbix, two intentional server failures were intentionally caused:

- 1st failure on **NTP Server**



Figure 12: Failure on NTP Server

- 2nd failure on **DNS Server**

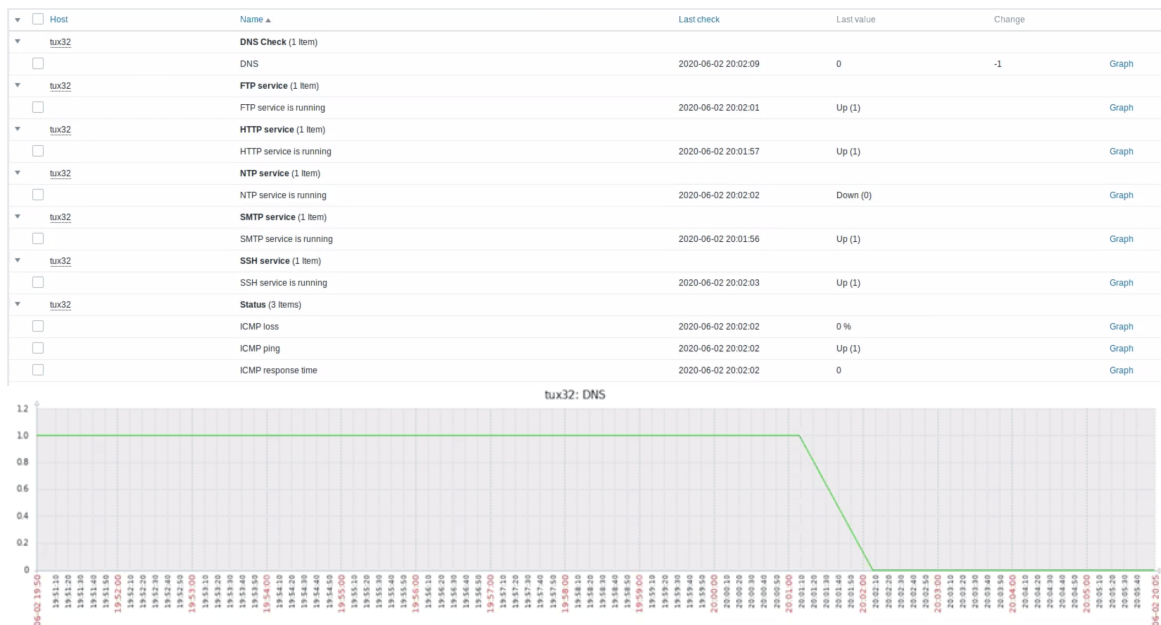


Figure 13: Failure on DNS Server

7 Other monitoring tools

7.1 Grafana

Grafana is an open source visualization tool that can be used on top of a variety of different data stores but is most commonly used together with Graphite, InfluxDB, Prometheus, Elasticsearch and Logz.io. It is designed for analyzing and visualizing metrics such as system CPU, memory, disk and I/O utilization. Grafana does not allow full-text data querying.

7.2 Features

- Visualize: Fast and flexible client side graphs with a multitude of options. Panel plugins for many different way to visualize metrics and logs.
- Dynamic Dashboards
- Explore Metrics: Explore your data through ad-hoc queries and dynamic drilldown. Split view and compare different time ranges, queries and data sources side by side.
- Searching through all your logs or streaming them live.
- Visually define alert rules for your most important metrics. Grafana will continuously evaluate and send notifications to systems like Slack, PagerDuty, VictorOps, OpsGenie.
- Mixed Data Sources: Mix different data sources in the same graph.

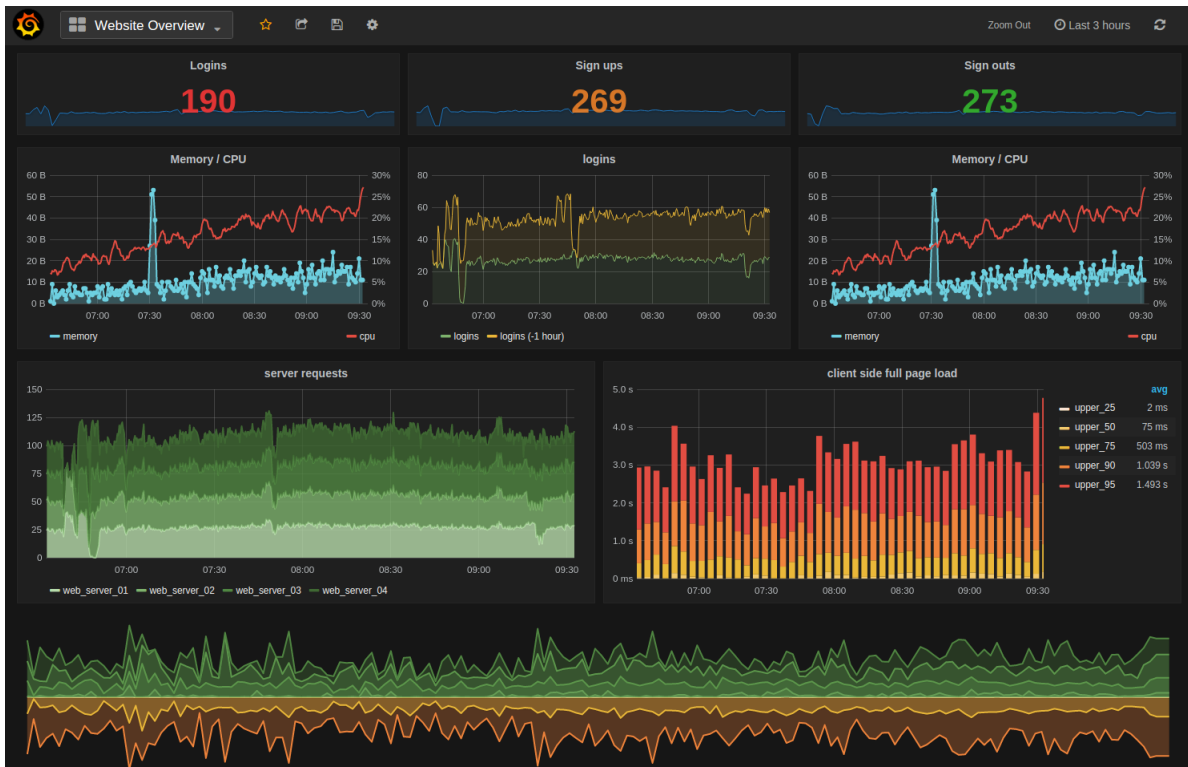


Figure 14: Grafana dashboard

7.3 openDCIM

OpenDCIM is a free, web based **Data Center Infrastructure Management** application. It covers all the majority features needed by the developers (as is often case of open source software).

7.4 Features

- Provides complete physical inventory of the data center.
- Support for Multiple Rooms (Data centers).
- Management of the three main elements - space, power, cooling.
- Integrating into existing business directory via UserID.
- Support of simulation - to see what would be affected as each source goes down (Simulated Power Outage report).
- Computation of Center of Gravity for each cabinet.
- Open Architecture - All built on a MySQL database for easy report building, or export to other applications.
- Integration with intelligent power strips and UPS devices - APC, Geist Manufacturing, Liebert, and Server Technologies. Easy to update with OIDs for other manufacturers.

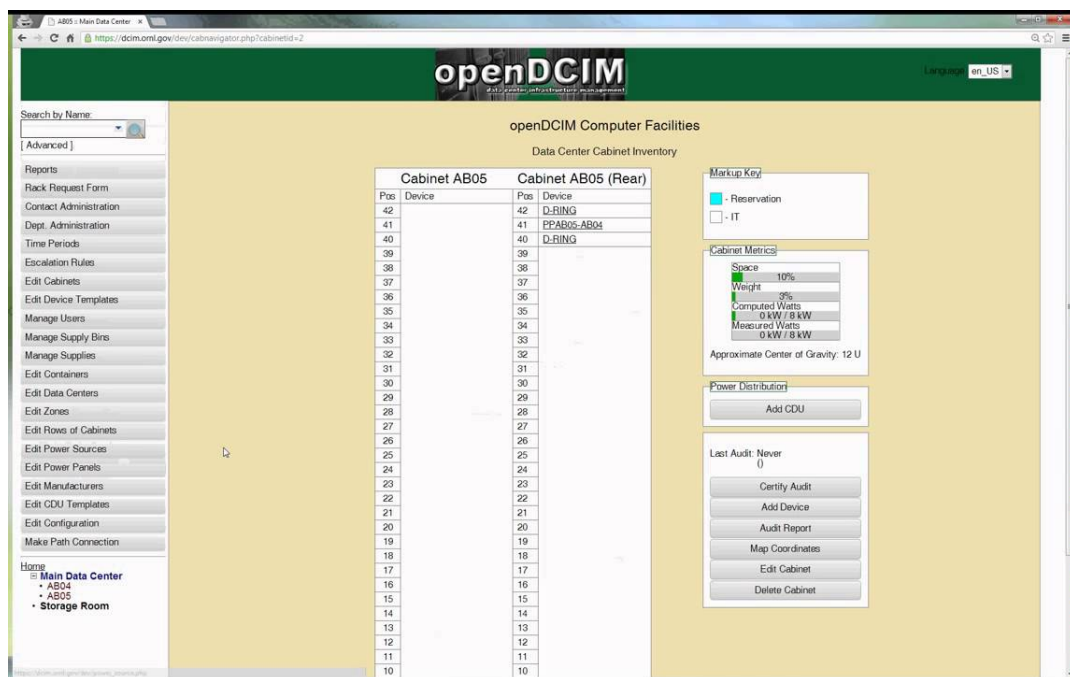


Figure 15: OpenDCIM dashboard

7.5 Comparison

Nagios and Zabbix are mainly tools for monitoring network (servers, applications, log monitoring, system metrics) that contain basic tools while Grafana is a commercial product (Grafana Enterprise version) with a lot of users containing beautiful visualization and can be integrated with various of software and tools (including Zabbix for example). It is good to use Grafana when we have multiple sources of metrics or logs and need to see them in one place and when we need to share your dashboards across the organization. Regarding openDCIM, it is made for developers, visualization is not that user-friendly as for example Grafana and all the configuration is done via Linux. However, the main different is that openDCIM is a data center infrastructure management so it manages data distributing, backup process, management of cooling and power while the other tools are specialized on network monitoring.

	Nagios	Zabbix	Grafana	openDCIM
Tool	Network monitoring software	Network monitoring software	Data visualizer software	Data Center Infrastructure Management application
Visual	Doesn't offer the same level of clarity and display quality as Zabbix	Has GUI and data visualizer, but limited customization	Great, powerful customization with the ability to correlate data from multiple sources	Aimed for developers (requires understanding the data)
Config	Enter configurations as text files	Change your configurations through a web-based interface	Configuration of .ini files (good documentation)	Config via command line
Price	Absolutely free	Absolutely free	Has free versions and paid subscriptions	Absolutely free
Advantage	Great for basic monitoring needs (servers, networks, applications)	Great for basic monitoring needs	Great if you need to perform deep analysis	Great for developers

8 Conclusion

We have successfully accomplished the objective of this laboratory work about monitoring a network in production, with the servers and services available on it. When it comes to network monitoring, there are many tools that offer an excellent monitoring experience and it is very important that we know how to choose a tool that best suits the type of analysis we want to do.

References

- [1] *Zabbix*. URL: <https://www.zabbix.com>
- [1] *Nagios*. URL: <https://www.nagios.org/>
- [2] *Zabbix*. [Online, last update 17.5.2020]. URL: <https://en.wikipedia.org/wiki/Zabbix>
- [2] *Nagios*. [Online, last update 3.4.2020]. URL: <https://pt.wikipedia.org/wiki/Nagios>