System Monitoring

René Serral-Gracià[1]

[1] Universitat Politècnica de Catalunya (UPC)

April 1, 2024

Lectures

1. System administration introduction
2. Operating System installation
3. User management
4. Application management
5. **System monitoring**
6. Filesystem Maintenance
7. Network services
8. Security and Protection
9. Introduction to Public Cloud

Outline

1. Introduction
   - Goals
2. System Monitoring
3. Process management
4. User monitoring
5. Network monitoring

Goals

Knowledge

- Monitoring commands
- Meaning of the different signals

Abilities

- Obtain information about the system's behavior
  - CPU activity
  - Memory activity
  - Disk activity
- Process status monitoring
  - Priority change
  - Stop and Continue processes

Outline

1. Introduction

2. System Monitoring
   - CPU
   - Memory
   - Disk
   - Network
   - Users
   - Other monitoring tasks

3. Process management

4. User monitoring

5. Network monitoring

System Monitoring

Why monitoring?

- Proactively control the resource status
- Control service status
- Security

Actions

- Automatic
- Manual

System Monitoring

What do we monitor?

- CPU
- Memory
- I/O
- Network
- Users
- Services
- Logs

System Monitoring

Other factors

- When a resource is monitored?
- Who do we contact in case there is a problem?
- Which is the criteria to notify a warning?
- And for a critical issue?

CPU Activity

Monitoring

- Inactive processors
- Monopolized processors
    - By a single process
    - By a single user

Tools

`uptime`, `top`, `ps`

Memory activity

Monitoring

- Lack of memory
- Memory monopolization
  - By a single process
  - By a single user
- Swap

Tools

`free`, `vmstat`, `top`

I/O Activity

Monitoring

- Filesystem
- Anomalous I/O activity
- Virtual memory
  - Excessive Pagination
  - Free Space

Tools

`vmstat`, `df`, `iostat`

Network Activity

Monitoring

- Bandwidth
- Local and remote services
- Incoming/outgoing connections
- Traffic profile

Tools

`ip -s -d`, `netstat`, `tcpdump`, `nmap`, logs del sistema

User activity

Monitoring

- Active sessions
  - Locally
  - Remotely
- Connected users
- What are they doing?

Tools

`w`, `last`, `finger`, `fuser`, `lsof`

Other monitoring tasks

Service and server activity

- Web server load
- E-mail queues
  - Input
  - Output
- Printer queues

Registry files (logs)

- System errors
- Anomalous activity (security)

Outline

1. Introduction
2. System Monitoring
3. Process management
   - Priority change
   - Signals
4. User monitoring
5. Network monitoring

Tasks and process management

Process identification

- Who is the owner of the process?
- Which is its purpose?
  - Is it important?
  - Is it an atack? ... or an error?

Actions on the process

- Priority changes
- Stop and reactivation of a process
- Killing a process

Priority change

- When executing the process
  - `nice +10 command...`
- Once it is already running
  - `renice +10 <pid>`
- Only root can increase the priority

Negative values indicate higher priorities

Some advise

High priority Shell

- Higher priority than swap
  - Allows a more efficient detection/solving of a memory issue
- The child processes inherit the priority of the parent

Relative priorities

- Priority is a relative term
- Not useful if all the processes have high priority

Sending signals to processes

`kill <signal> <pid>`

- `-KILL`: immediately stops the process
- `-TERM`: ask a process to gracefully finish (kill, by default)
- `-INT`: interrupt a process (kill, by default)
- `-STOP`: stop a process
  - Do not allow it to be enqueued in the ready queue
- `-CONT`: reactivate the selected process

`killall <signal> <command name>`

- Sends the signal to **ALL** the processes matching the name

Outline

1 Introduction

2 System Monitoring

3 Process management

4 User monitoring

- Examples

5 Network monitoring

User monitoring

User activity

- `w [user]`
  - List of connected users and the command being executed
  - Given a username, it lists his/her connections
- `last [user]`
  - Lists the last established connections. . . either finished or not
- `finger [user]`
  - Lists all the sessions or the ones belonging to an user

File monitoring

File activity monitoring

- `fuser <filename>`
  - Identifies the processes being used by a file
- `lsof [filename | directory name]`
  - Lists open files

Disk activity

Used space

- `du [filename | directory name]`
  - Indicates used space per directory (including subdirs)

Free space

- `df [filename | directory name]`
  - Free space on each partition

I/O activity

- `vmstat`
- `iostat`

Example top

```
top - 10:01:50 up 4 days,  8:40,  5 users,  load average: 1.77, 1.51, 1.56
Tasks: 281 total,   1 running, 279 sleeping,   0 stopped,   1 zombie
%Cpu0  : 13.2 us,  3.3 sy,  0.0 ni, 82.9 id,  0.3 wa,  0.0 hi,  0.3 si,  0.0 st
%Cpu1  : 10.2 us,  1.5 sy,  0.0 ni, 87.3 id,  0.3 wa,  0.0 hi,  0.6 si,  0.0 st
%Cpu2  : 12.7 us,  1.5 sy,  0.0 ni, 84.6 id,  0.6 wa,  0.0 hi,  0.6 si,  0.0 st
%Cpu3  : 16.3 us,  1.7 sy,  0.0 ni, 81.6 id,  0.0 wa,  0.0 hi,  0.3 si,  0.0 st
KiB Mem : 16314076 total,  5436464 free,  3590272 used,  7287340 buff/cache
KiB Swap: 16360444 total, 16318936 free,    41508 used. 10859404 avail Mem

PID   USER      PR  NI    VIRT    RES    SHR S  %CPU %MEM     TIME+ COMMAND
17901 rserral    1   0 1429512 265436 126648 S  16.5  1.6   4:51.75 slack
17115 rserral    5   0 2640856 349772 137352 S   9.6  2.1   5:00.66 gnome-shell
17340 rserral    1   0 1667320 157220  91880 S   4.6  1.0   0:33.14 slack
444   root     -51   0       0      0      0 S   2.0  0.0  17:17.13 irq/17-i2c_desi
17133 rserral    1   0  562520 236400 201880 S   1.7  1.4   0:51.53 Xwayland
17343 rserral    1   0  471912  48636  30472 S   1.7  0.3   0:00.92 python2
18210 rserral    1   0 3021200 577976 253764 S   1.3  3.5   4:42.75 firefox
286   root     -51   0       0      0      0 S   1.0  0.0   8:01.12 irq/17-idma64.1
20211 rserral    6   0   46988   3904   3044 R   1.0  0.0   0:00.33 top
19472 root       1   0       0      0      0 S   0.7  0.0   0:11.71 kworker/u8:2
6     root       1   0       0      0      0 S   0.3  0.0  13:19.49 ksoftirqd/0
7     root       1   0       0      0      0 S   0.3  0.0   2:02.42 rcu_preempt
17    root       1   0       0      0      0 S   0.3  0.0  13:23.78 ksoftirqd/1
23    root       1   0       0      0      0 S   0.3  0.0  14:30.76 ksoftirqd/2
29    root       1   0       0      0      0 S   0.3  0.0  16:11.32 ksoftirqd/3
445   root     -51   0       0      0      0 S   0.3  0.0   3:06.32 irq/51-DLL075B:
621   message+   1   0   48732   6700   3072 S   0.3  0.0   4:09.41 dbus-daemon
```

Exercise

We have a database server with 1 CPU (and hyperthreading)

- Which is the problem present on the server if any?
- Which actions would you take?

```
top - 09:38:09 up 1 day, 18:29,  6 users,  load average: 4.08, 4.93, 4.39
Tasks: 425 total,  12 running, 413 sleeping,   0 stopped,   0 zombie
%Cpu(s): 91.0 us,  6.8 sy,  0.9 ni,  1.3 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem : 16355660 total,   125088 free,  6559812 used,  9670760 buff/cache
KiB Swap: 33691644 total, 33689476 free,     2168 used.  8286212 avail Mem

PID   USER      PR  NI    VIRT     RES    SHR S  %CPU %MEM     TIME+ COMMAND
4102  pcomp     20   0 2920500 1.029g  98884 S  46.1  6.6 103:32.24 firefox-esr
12802 pcomp     20   0  102332  68188  14164 R  30.6  0.4   0:00.93 chrome-bg-proc
12818 pcomp     20   0   80856  51980  17732 R  22.4  0.3   0:00.68 chrome-bg-proc
12835 pcomp     20   0   88840  49892  10524 R  17.1  0.3   0:00.52 chrome-bg-proc
3947  pcomp     20   0 2207552 505540  69276 S  14.5  3.1  49:25.10 gnome-shell
12861 pcomp     20   0   75972  37808  10480 R  12.2  0.2   0:00.37 chrome-bg-proc
12834 pcomp     20   0   65460  25816   8488 R  11.2  0.2   0:00.34 chrome-bg-proc
12873 pcomp     20   0   69680  32032  10508 R   9.2  0.2   0:00.28 chrome-bg-proc
12858 pcomp     20   0   59056  18824   8452 R   7.6  0.1   0:00.23 chrome-bg-proc
12833 pcomp     20   0   14312  11436   1356 R   6.9  0.1   0:00.21 mysqld
```

Exercise

We have a server with 32 logical CPU

- Which is the problem present on the server?
- How would you solve it?

```
top - 16:31:15 up  3:04, 20 users,  load average: 29.76, 17.88, 10.19
Tasks: 1016 total,   2 running, 1013 sleeping,   1 stopped,   0 zombie
Cpu(s):  2.5%us,  1.2%sy,  0.0%ni, 86.8%id,  9.4%wa,  0.0%hi,  0.1%si,  0.0%st
Mem:  65969572k total, 33193236k used, 32776336k free,     8656k buffers
Swap: 16777208k total,  7635416k used,  9141792k free,    31292k cached
PID  USER      PR  NI  VIRT  RES  SHR S %CPU  %MEM    TIME+  COMMAND
3164 tst8      20   0 23.1g  21g  584 R 100.0 34.1   7:44.76 emacs
4576 tst8      20   0  104m 1080  476 S  53.3  0.0   2:17.90 genarray.sh
1010 root      20   0     0    0    0 D   2.0  0.0   2:07.06 kmirrord
3342 g_users   20   0 15868 1528  476 R   1.0  0.0   1:43.80 top
168  root      20   0     0    0    0 S   0.3  0.0   0:02.09 events/21
2568 tst6      20   0  101m  376  240 S   0.3  0.0   1:27.30 sshd
```

Outline

1 Introduction

2 System Monitoring

3 Process management

4 User monitoring

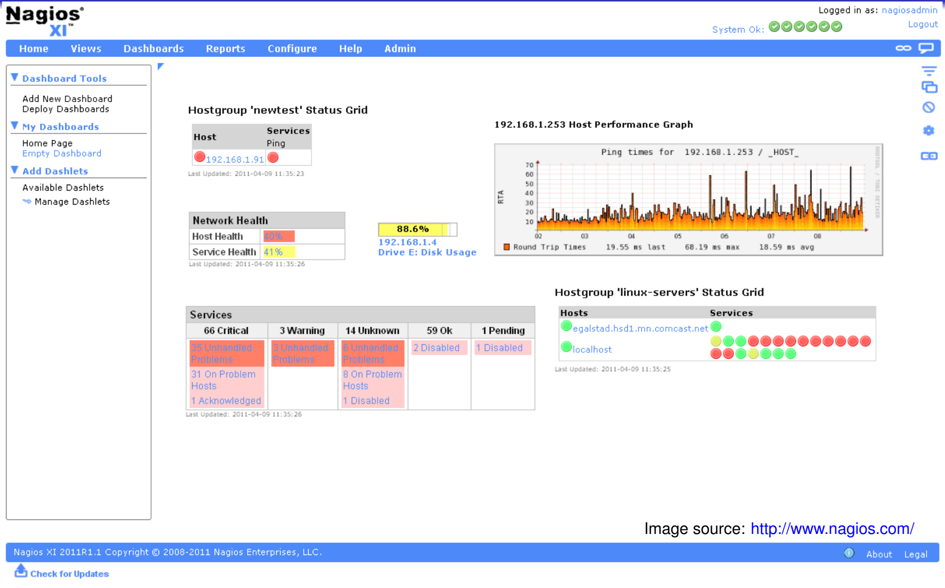
5 Network monitoring

Network monitoring

Integrated systems

- Centralized information for various servers
  - Resources
  - Services
  - Uptime
  - Connectivity
  - Logs
- Ease the issue detection
- NagiOS, Splunk

Example: Nagios XI



Nagios XI

Logged in as: nagiosadmin

Logout

System Ok: ✓✓✓✓✓✓

▼ Dashboard Tools

Add New Dashboard
Deploy Dashboards

▼ My Dashboards

Home Page
Empty Dashboard

▼ Add Dashlets

Available Dashlets
Manage Dashlets

Hostgroup 'newtest' Status Grid

Host	Services Ping
● 192.168.1.91	●

Last Updated: 2011-04-09 11:35:23

Network Health	
Host Health	40%
Service Health	41%

Last Updated: 2011-04-09 11:35:26

88.6%
192.168.1.4
Drive E: Disk Usage

192.168.1.253 Host Performance Graph

■ Round Trip Times 19.55 ms last 68.19 ms max 18.59 ms avg

Services				
66 Critical	3 Warning	14 Unknown	59 Ok	1 Pending
35 Unhandled Problems 31 On Problem Hosts 1 Acknowledged	3 Unhandled Problems	6 Unhandled Problems 8 On Problem Hosts 1 Disabled	2 Disabled	1 Disabled

Last Updated: 2011-04-09 11:35:26

Hostgroup 'linux-servers' Status Grid

Hosts	Services
● egalstad.hsd1.mn.comcast.net	●
● localhost	●●●●●●●●●●●●● ●●●●●●●

Last Updated: 2011-04-09 11:35:25

Image source: http://www.nagios.com/

Nagios XI 2011R1.1 Copyright © 2008-2011 Nagios Enterprises, LLC.

About Legal

Check for Updates

Personal homework

- Backup tools
  - dump
  - tar
  - gzip, bzip2, zip, rar, partimage, Norton Ghost