System Monitoring

René Serral-Gracià Xavier Martorell-Bofill[1]

[1] Universitat Politècnica de Catalunya (UPC)

May 26, 2014

Lectures

1. System administration introduction
2. Operating System installation
3. User management
4. Application management
5. **System monitoring**
6. Filesystem Maintenance
7. Local services
8. Network services
9. Security and Protection
10. Virtualization

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

`ifconfig`, `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

```
  4:50pm  up 11 days,  8:23,  7 users,  load average: 0.01, 0.06, 0.02
128 processes: 126 sleeping, 1 running, 1 zombie, 0 stopped
CPU0 states:  0.1% user,  0.0% system,  0.0% nice, 99.4% idle
CPU1 states:  1.0% user,  0.0% system,  1.0% nice, 98.4% idle
CPU2 states:  0.1% user,  1.4% system,  0.0% nice, 97.4% idle
CPU3 states:  0.0% user,  0.0% system,  0.0% nice, 100.0% idle
Mem:  2064296K av, 2028024K used,   36272K free,       0K shrd,   88516K buff
Swap: 2096472K av,   52560K used, 2043912K free                 1380948K cached

  PID USER     PRI  NI  SIZE  RSS SHARE STAT %CPU %MEM   TIME COMMAND
   10 root      16   2     0    0     0 SWN   1.9  0.0  46:40 kscand/HighMem
20527 pareta    13   2  129M 120M 18824 S N   0.5  5.9  19:43 mozilla-bin
12283 admac-e   15   5 24308  23M  3676 S N   0.5  1.1   0:10 mysqld
14988 pareta     9   0  129M 120M 18824 S     0.1  5.9   0:00 mozilla-bin
29291 aduran    11   0  1000 1000   760 R     0.1  0.0   0:00 top
    1 root       8   0   480  440   416 S     0.0  0.0   0:11 init
    2 root       9   0     0    0     0 SW    0.0  0.0   0:03 keventd
    3 root      19  19     0    0     0 SWN   0.0  0.0   0:00 ksoftirqd_CPU0
    4 root      18  19     0    0     0 SWN   0.0  0.0   0:00 ksoftirqd_CPU1
    5 root      19  19     0    0     0 SWN   0.0  0.0   0:00 ksoftirqd_CPU2
    6 root      18  19     0    0     0 SWN   0.0  0.0   0:00 ksoftirqd_CPU3
    7 root       9   0     0    0     0 SW    0.0  0.0   1:40 kswapd
    8 root       9   0     0    0     0 SW    0.0  0.0   0:11 kscand/DMA
    9 root      12   2     0    0     0 SWN   0.0  0.0  25:44 kscand/Normal
   11 root       9   0     0    0     0 SW    0.0  0.0   0:04 bdflush
   12 root       9   0     0    0     0 SW    0.0  0.0   0:17 kupdated
   13 root      -1 -20     0    0     0 SW<   0.0  0.0   0:00 mdrecoveryd
   17 root       9   0     0    0     0 SW    0.0  0.0   1:30 kjournald
   96 root       9   0     0    0     0 SW    0.0  0.0   0:00 khubd
```

vmstat out

```
 # vmstat -n 30
procs -----------memory---------- ---swap-- -----io---- -system-- ----cpu----
 r  b   swpd   free   buff  cache   si   so    bi    bo   in   cs us sy id wa
 0 10 249496  54376   6172 113464    3    2    35    52   36   57  9  1 83  6
 1 10 249496   8132   6188   3584   13    0    38    12  353  611  5  0 88  7
 1 10 124949   4960   6204   3720    0   54    26     6  349  611  5  5 86  4
 1  9 109496   2832   6220   3840   10   10    26     6  352  623  1 10 85  4
 1  8  49496   1708   3236   2848   13  117    13     6  349  595  1 25 65 10
 1  9   9496    596   1252   1976  150  200    26    14  349  607  3 20 72  4
```

Exercise

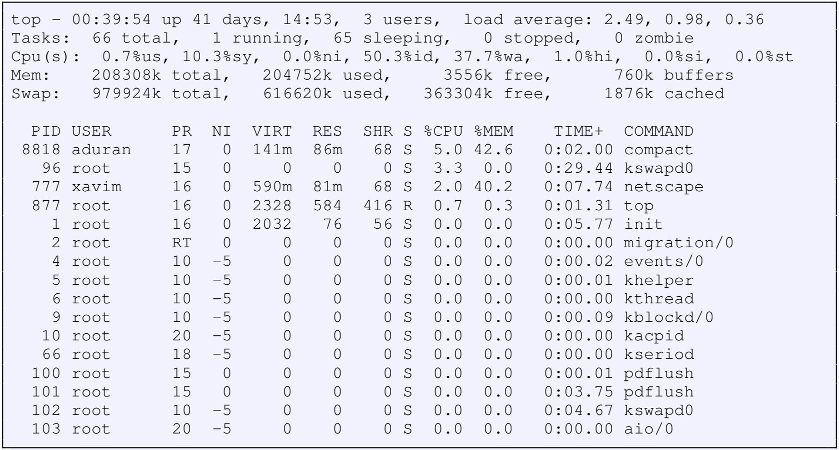
Which is the problem present on the server if any?
Which actions would you take?

```
 top - 17:10:26 up 11 days,  8:33,  2 users,  load average: 2.65, 1.22, 0.48
Tasks:  70 total,   4 running,  66 sleeping,   0 stopped,   0 zombie
Cpu0  : 48.2%us,  0.4%sy,  0.0%ni, 51.4%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Mem:    191952k total,   185684k used,     6268k free,    49984k buffers
Swap:   979924k total,       44k used,   979880k free,    50644k cached

  PID USER       PR  NI  VIRT  RES  SHR S %CPU %MEM   TIME+  COMMAND
22835 aduran     25   0  1520  272  216 R 33.2  0.1   4:15.23 updateSW
22838 aduran     25   0  1516  268  216 R 33.2  0.1   0:38.99 merge
22839 aduran     25   0  1520  268  216 R 33.2  0.1   0:29.82 merge
22805 aduran     18   0  2336 1156  896 R  0.7  0.6   0:03.77 top
    1 root       15   0  2036  692  592 S  0.0  0.4   0:02.89 init
    2 root       RT   0     0    0    0 S  0.0  0.0   0:00.00 migration/0
    3 root       34  19     0    0    0 S  0.0  0.0   0:00.06 ksoftirqd/0
    4 root       10  -5     0    0    0 S  0.0  0.0   0:00.02 events/0
    5 root       10  -5     0    0    0 S  0.0  0.0   0:00.01 khelper
    6 root       10  -5     0    0    0 S  0.0  0.0   0:00.00 kthread
    9 root       10  -5     0    0    0 S  0.0  0.0   0:00.09 kblockd/0
   10 root       20  -5     0    0    0 S  0.0  0.0   0:00.00 kacpid
   66 root       18  -5     0    0    0 S  0.0  0.0   0:00.00 kseriod
  101 root       15   0     0    0    0 S  0.0  0.0   0:03.75 pdflush
  102 root       10  -5     0    0    0 S  0.0  0.0   0:04.67 kswapd0
  103 root       20  -5     0    0    0 S  0.0  0.0   0:00.00 aio/0
```

Exercise

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



```
top - 00:39:54 up 41 days, 14:53,  3 users,  load average: 2.49, 0.98, 0.36
Tasks:  66 total,   1 running,  65 sleeping,   0 stopped,   0 zombie
Cpu(s):  0.7%us, 10.3%sy,  0.0%ni, 50.3%id, 37.7%wa,  1.0%hi,  0.0%si,  0.0%st
Mem:    208308k total,   204752k used,     3556k free,      760k buffers
Swap:   979924k total,   616620k used,   363304k free,     1876k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
 8818 aduran    17   0  141m  86m   68 S  5.0 42.6   0:02.00 compact
   96 root      15   0     0    0    0 S  3.3  0.0   0:29.44 kswapd0
  777 xavim     16   0  590m  81m   68 S  2.0 40.2   0:07.74 netscape
  877 root      16   0  2328  584  416 R  0.7  0.3   0:01.31 top
    1 root      16   0  2032   76   56 S  0.0  0.0   0:05.77 init
    2 root      RT   0     0    0    0 S  0.0  0.0   0:00.00 migration/0
    4 root      10  -5     0    0    0 S  0.0  0.0   0:00.02 events/0
    5 root      10  -5     0    0    0 S  0.0  0.0   0:00.01 khelper
    6 root      10  -5     0    0    0 S  0.0  0.0   0:00.00 kthread
    9 root      10  -5     0    0    0 S  0.0  0.0   0:00.09 kblockd/0
   10 root      20  -5     0    0    0 S  0.0  0.0   0:00.00 kacpid
   66 root      18  -5     0    0    0 S  0.0  0.0   0:00.00 kseriod
  100 root      15   0     0    0    0 S  0.0  0.0   0:00.01 pdflush
  101 root      15   0     0    0    0 S  0.0  0.0   0:03.75 pdflush
  102 root      10  -5     0    0    0 S  0.0  0.0   0:04.67 kswapd0
  103 root      20  -5     0    0    0 S  0.0  0.0   0:00.00 aio/0
```

Outline

1 Introduction

2 System Monitoring

3 Process management

4 User monitoring

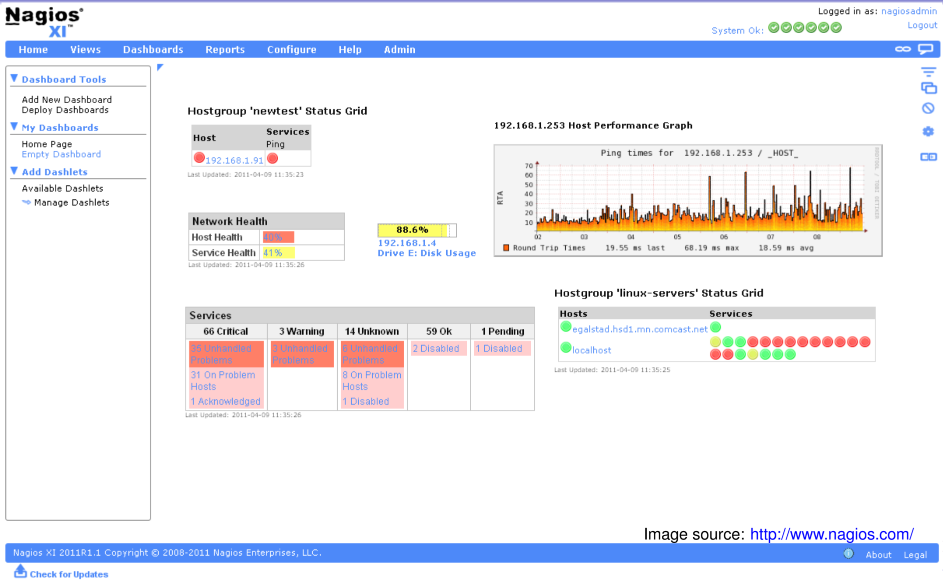
5 Network monitoring

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

System Ok: ✓✓✓✓✓✓

Logout

Home Views Dashboards Reports Configure Help Admin

▼ 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

Ping times for 192.168.1.253 / _HOST_
RTA
70
60
50
40
30
20
10
02
03
04
05
06
07
08
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