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
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 attack? ... 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

```
kcall <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
- `ls/of [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**

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

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, OK shrd, 88516K buff
Swap: 2096472K av, 52560K used, 2043912K free, 1380948K cached
```
# 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, 185684k used, 979880k free, 50644k cached
```

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

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

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

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