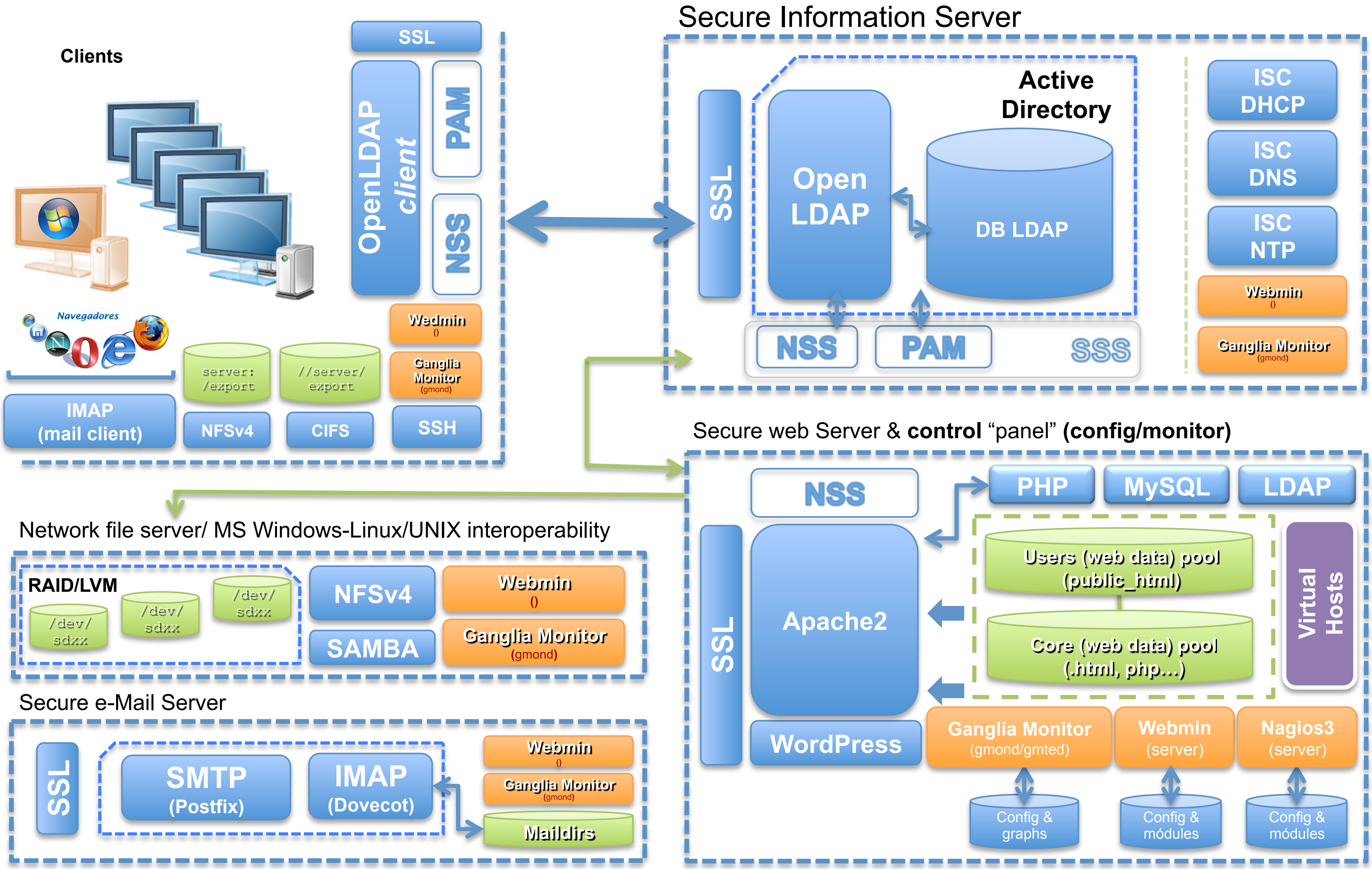
Computer System Design and Administration

Topic 14. Linux tools

José Ángel Herrero Velasco

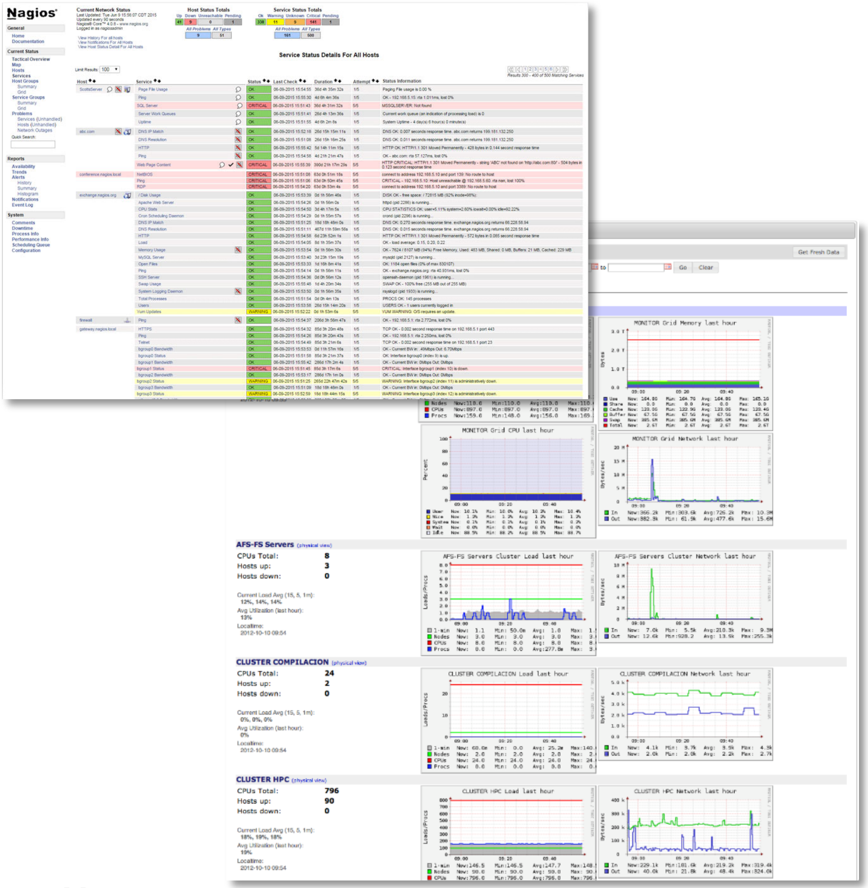
Department of Computer and
Electrical Engineering

Puzzle


Secure Information Server
Clients
SSL
OpenLDAP client
PAM
NSS
Wedmin ()
Ganglia Monitor (gmond)
SSH
Navegadores
IMAP (mail client)
server: /export
//server/ export
NFSv4
CIFS
SSL
Open LDAP
Active Directory
DB LDAP
NSS
PAM
SSS
ISC DHCP
ISC DNS
ISC NTP
Webmin ()
Ganglia Monitor (gmond)
Secure web Server & control "panel" (config/monitor)
NSS
PHP
MySQL
LDAP
SSL
Apache2
Users (web data) pool (public_html)
Core (web data) pool (.html, php…)
Virtual Hosts
WordPress
Ganglia Monitor (gmond/gmted)
Webmin (server)
Nagios3 (server)
Config & graphs
Config & módules
Config & módules
Network file server/ MS Windows-Linux/UNIX interoperability
RAID/LVM
/dev/ sdxx
/dev/ sdxx
/dev/ sdxx
NFSv4
SAMBA
Webmin ()
Ganglia Monitor (gmond)
Secure e-Mail Server
SSL
SMTP (Postfix)
IMAP (Dovecot)
Webmin ()
Ganglia Monitor (gmond)
Maildirs

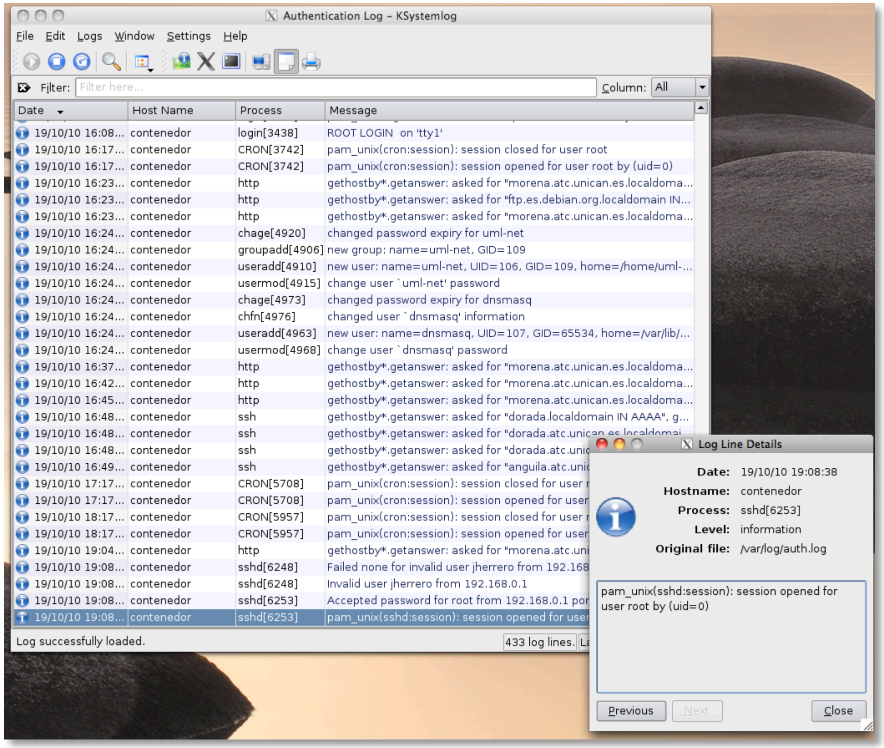
Target: Control panel (configuration)

- Deployment of a **<u>unified</u> control system** to configure and monitor a whole *computing environment*, based on:
  - Global configuration:
    - Webmin.
  - Global monitoring:
    - Ganglia-monitor.
    - Nagios 3.
  - Others:
    - **Log File Viewers:**
      - **Webalizer Logfile Analysis (Webmin module).**
      - **Ksystemlog.**
      - **Logwatch.**
    - **Linux tools:**
      - **System:**
        - `sysstat, lsof`
      - **Accounting:**
        - `acct (lastcomm, sa)`
      - **Networking:**
        - `iptraf, netstat, nmap`


Nagios
Service Status Details For All Hosts
AFS-FS Servers
CLUSTER COMPILACION
CLUSTER HPC
MONITOR Grid Memory last hour
MONITOR Grid CPU last hour
MONITOR Grid Network last hour

Linux tools: Ksystemlog

- Graphical tool for the on-line **“display”** of **system logs:**
  - Orderly and friendly.
- It’s part of **KDE4 environment.**
- Main features:
  - Display of any Linux log file.
  - Colors.
  - Filters.
  - Order.
- …



Authentication Log – KSystemlog

Date	Host Name	Process	Message
19/10/10 16:08...	contenedor	login[3438]	ROOT LOGIN on 'tty1'
19/10/10 16:17...	contenedor	CRON[3742]	pam_unix(cron:session): session closed for user root
19/10/10 16:17...	contenedor	CRON[3742]	pam_unix(cron:session): session opened for user root by (uid=0)
19/10/10 16:23...	contenedor	http	gethostby*.getanswer: asked for "morena.atc.unican.es.localdoma...
19/10/10 16:23...	contenedor	http	gethostby*.getanswer: asked for "ftp.es.debian.org.localdomain IN...
19/10/10 16:23...	contenedor	http	gethostby*.getanswer: asked for "morena.atc.unican.es.localdoma...
19/10/10 16:24...	contenedor	chage[4920]	changed password expiry for uml-net
19/10/10 16:24...	contenedor	groupadd[4906]	new group: name=uml-net, GID=109
19/10/10 16:24...	contenedor	useradd[4910]	new user: name=uml-net, UID=106, GID=109, home=/home/uml-...
19/10/10 16:24...	contenedor	usermod[4915]	change user `uml-net' password
19/10/10 16:24...	contenedor	chage[4973]	changed password expiry for dnsmasq
19/10/10 16:24...	contenedor	chfn[4976]	changed user `dnsmasq' information
19/10/10 16:24...	contenedor	useradd[4963]	new user: name=dnsmasq, UID=107, GID=65534, home=/var/lib/...
19/10/10 16:24...	contenedor	usermod[4968]	change user `dnsmasq' password
19/10/10 16:37...	contenedor	http	gethostby*.getanswer: asked for "morena.atc.unican.es.localdoma...
19/10/10 16:42...	contenedor	http	gethostby*.getanswer: asked for "morena.atc.unican.es.localdoma...
19/10/10 16:45...	contenedor	http	gethostby*.getanswer: asked for "morena.atc.unican.es.localdoma...
19/10/10 16:48...	contenedor	ssh	gethostby*.getanswer: asked for "dorada.localdomain IN AAAA", g...
19/10/10 16:48...	contenedor	ssh	gethostby*.getanswer: asked for "dorada.atc.unican.es.localdomai
19/10/10 16:48...	contenedor	ssh	gethostby*.getanswer: asked for "dorada.atc.unic
19/10/10 16:49...	contenedor	ssh	gethostby*.getanswer: asked for "anguila.atc.unic
19/10/10 17:17...	contenedor	CRON[5708]	pam_unix(cron:session): session closed for user r
19/10/10 17:17...	contenedor	CRON[5708]	pam_unix(cron:session): session opened for user
19/10/10 18:17...	contenedor	CRON[5957]	pam_unix(cron:session): session closed for user r
19/10/10 18:17...	contenedor	CRON[5957]	pam_unix(cron:session): session opened for user
19/10/10 19:04...	contenedor	http	gethostby*.getanswer: asked for "morena.atc.uni
19/10/10 19:08...	contenedor	sshd[6248]	Failed none for invalid user jherrero from 192.168
19/10/10 19:08...	contenedor	sshd[6248]	Invalid user jherrero from 192.168.0.1
19/10/10 19:08...	contenedor	sshd[6253]	Accepted password for root from 192.168.0.1 por
19/10/10 19:08...	contenedor	sshd[6253]	pam_unix(sshd:session): session opened for user

Log successfully loaded. 433 log lines. La

Log Line Details

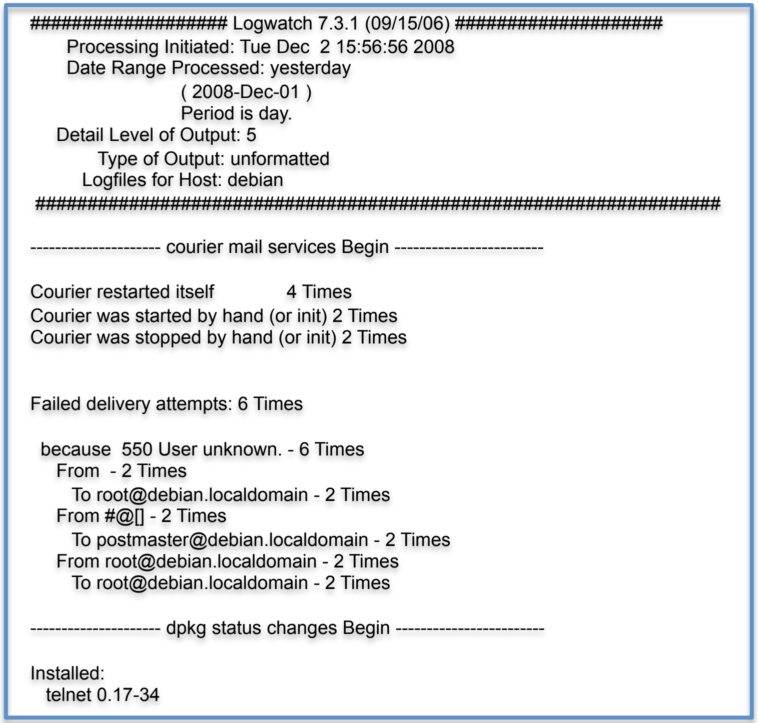
Date: 19/10/10 19:08:38
Hostname: contenedor
Process: sshd[6253]
Level: information
Original file: /var/log/auth.log

pam_unix(sshd:session): session opened for user root by (uid=0)

Linux tools: Logwatch

- It is a *powerful* and *versatile* **log parser** and **analyzer:**
  - Gives a **unified report** of all activity on a computer.
  - Enables you to take a look at the system activity using the system logs:
    - **Summary.**
  - Command line or *email.*
  - Very useful.
- Results:
  - Synthesized.
  - Summarized.
  - Organized.
- Uses **cron** to perform the checkups systematically.

```
$ logwatch --detail Med --print →
```



```
################### Logwatch 7.3.1 (09/15/06) ####################
       Processing Initiated: Tue Dec  2 15:56:56 2008
       Date Range Processed: yesterday
                             ( 2008-Dec-01 )
                             Period is day.
     Detail Level of Output: 5
             Type of Output: unformatted
          Logfiles for Host: debian
 ##################################################################

-------------------- courier mail services Begin ------------------------

Courier restarted itself              4 Times
Courier was started by hand (or init) 2 Times
Courier was stopped by hand (or init) 2 Times


Failed delivery attempts: 6 Times

  because  550 User unknown. - 6 Times
     From  - 2 Times
        To root@debian.localdomain - 2 Times
     From #@[] - 2 Times
        To postmaster@debian.localdomain - 2 Times
     From root@debian.localdomain - 2 Times
        To root@debian.localdomain - 2 Times

-------------------- dpkg status changes Begin ------------------------

Installed:
   telnet 0.17-34
```

Linux tools: System tools

- **Global monitoring** from command line.
- You must install several packages (.deb).

```
$ apt-get install sysstat lsof…
```

- `sysstat`:
  - `iostat`:
    - Reports (CPU) statistics and input/output statistics for devices and partitions.
  - `nfsiostat`:
    - Emulates `iostat` for NFS mount points using `/proc/self/mountstats`.
  - `pidstat`:
    - Reports statistics for individual tasks currently being managed by the Linux kernel.
  - `sadf`:
    - Displays data collected by `sar` (system activity information) in multiple formats (CSV, XML, etc.).
  - `mpstat`:
    - Reports processors related statistics.
  - `cifsiostat`:
    - Reports statistics about read and write operations on CIFS filesystems.
- `lsof`:
  - `lsof`:
    - Lists on its standard output file information about files opened by processes running.
    - Identifies the processes running under a file system.

Linux tools: Accounting

- The GNU Accounting Utilities provide **login and process accounting** utilities for GNU/Linux and other systems:
  - Useful information about **system usage.**
  - Connections, programs executed, and utilization of system resources.

- First of all, it must be enabled (activated):
  - On every *system boot:*

```
$ accton /var/log/account/pacct
```

- Tools:
  - `lastcomm:`
    - Prints out information about previously executed commands:
      - **By default, it prints info about all of the commands in *acct.***
    - It can be considered a "security tool”:
      - “$ `man lastcomm`”
  - `sa:`
    - Summarizes *more detailed* accounting information:
      - CPU, IO, MEM.
    - “`$ man sa`”

Linux tools: Networking

- **`netstat`**:
  - Prints:
    - Network connections, (**`-a`**).
    - Routing tables, (**`-r`**).
    - Interface statistics.
    - Masquerade connections.
    - Multicast memberships.
- **`iptraf`**:
  - Interactive Colorful **IP LAN Monitor**
- **`nmap (nmapfe)`**:
  - Network **exploration tool** and security.
  - Port scanner:
    - local/remote.
- **`tcpdump/wireshark/sniffit`**:
  - Allows monitoring of data being sent/received on each connection.
- **`netperf`**:
  - Measures the **performance** of network links.