Linux Days 2003, Advanced Tutorial

Alain Knaff
alain.knaff@linux.lu

Summary

- 1. System tools
- 2. Configuration files and configuration tools
- 3. Server applications

System tools

- 1. Network configuration:
  - `ifconfig eth0 158.64.28.133 netmask 255.255.255.0`
  - `ifconfig`
  - `ifconfig -a`
  - `route add default gw 158.64.28.129`
  - `route -n`

System tools

- 2. Network analysis
  - Ping
    - Tests whether a remote host is available
  - Traceroute
    - Displays path to remote host
  - Tcpdump
    - Lists network packets
    - Can show contents of network packets
  - Iptraf
    - Network traffic statistics

System tools

- 3. Netstat
  - List currently active network connections
  - "Who is connected to my server"
  - "Which network daemons are running"
  - Servers that are passively listening
  - Established connections

System tools

- 4. Hardware and drivers
  - Lspci
    - Lists currently active PCI devices
    - "Which network card does this machine have?"
  - Lsusb
    - Lists currently connected USB devices
  - Lsmod
    - List currently loaded modules

System tools

- 5. Lsof
  - Lists processes owning given "file" resource
  - "Which process currently hogs the CD drive?"
  - "Which process owns TCP port 25?"
  - "Which files or resources does process 1234 have open?"

```
frisbee:/root # lsof -i tcp:25
COMMAND   PID USER   FD   TYPE DEVICE SIZE NODE NAME
sendmail 1263 root    4u  IPv4   4360       TCP *:smtp (LISTEN)
```

System tools

- 6. /proc filesystem
  - Information about system settings
    - `/proc/sys/...`
  - Information about processes
    - `/proc/pid/cmdline`
    - `/proc/pid/fd`
    - `/proc/pid/maps`

System tools

- 7. Strace
  - Lists all system calls that a given program performs
  - Debugging
  - Finding unknown locations of configuration files

Configuration files and tools

- Unix files (/etc)
- /etc/sysconfig files
- Yast
- webmin
- vi

Configuration files: Unix files

- /etc/resolv.conf
  - Default domain and name servers

```
search lll.org.lu lll.lu ltnb.lu
nameserver 158.64.28.133
nameserver 158.64.28.242
```

- /etc/hosts
  - Locally defined host-to-ip mappings

```
158.64.28.133 tuxtux.lll.lu tuxtux
127.0.0.1 localhost
::1  ipv6-localhost ipv6-loopback
```

Configuration files: Unix files

- /etc/passwd : User information
  - Login name
  - User Id
  - Main Group Id
  - Full Name
  - Home Directory
  - Login Shell

```
alain:x:500:100:Alain Knaff:/home/aknaff:/usr/bin/zsh
```

- System users (applications)
- Real users (people)
- Users are usually created with the command `useradd`

Configuration files: Unix files

- /etc/shadow : Users' passwords
  - Only readable by privileged processes
  - Passwords encrypted

Configuration files: Unix files

- /etc/fstab : File systems to mount
  - Device / Origin
  - Mountpoint
  - Filesystem type
  - Options
    - noauto
    - user
- Example:

```
/dev/md5        /       reiserfs        defaults 1 2
/dev/md9        /home   reiserfs        defaults 1 2
proc    /proc   proc    defaults 0 0
...
laptop:/nfs     /ld-2003        nfs     noauto,user
//winserver/share1     /share1        smbfs
username=myuser,password=mypass,workgroup=TUX-NET
//winserver/share2     /share2        smbfs
credentials=/root/credfile,workgroup=TUX-NET
```

Configuration files: Unix files

- Once this is defined, mount the partition with the following command:
  `mount /ld-2003`

Configuration files: /etc

- /etc/HOSTNAME

```
laptop.hitchhiker.org.lu
```

- To set it manually: `hostname laptop`

Configuration files: /etc/sysconfig

- /etc/sysconfig/network-scripts/ifcfg-eth0

```
BOOTPROTO='static'
MTU=''
REMOTE_IPADDR=''
STARTMODE='onboot'
UNIQUE='CLZK.VirkPazOL06'
BROADCAST='192.168.1.255'
IPADDR='192.168.1.2'
NETMASK='255.255.255.0'
NETWORK='192.168.1.0'
```

To start it

```
ifup eth0
```

Configuration tools

- SuSE: Yast
- webmin: http://www.webmin.com/
- Demo
- Vi

Server applications

- Standalone servers: apache, sendmail, sshd, ...
- Servers started by `xinetd`: ftpd, imapd, ...
  - `/etc/services`
  - `/etc/xinetd.d`

Server applications

- Started by `/etc/init.d/xyz start`
- Automatic activation using `chkconfig`
  - `chkconfig --list apache`
  - `chkconfig --add apache`
  - `chkconfig --set apache 3,5`

Server applications

- General
- DNS (name server): bind
- Apache
- Squid
- Ssh
- Ftp: vsftpd

Server apps: DNS (name service)

- Goal: translate names to IP addresses and vice-versa
- Standalone daemon
- Hierarchical system: delegation
- Master configuration in `/etc/named.conf`
- Configuration for individual domains in `/var/lib/named/*`

Server apps: DNS > named.conf

- Global configuration options
  - `query-source address 158.64.28.133 port 53;`
  - `forwarders { 158.64.1.25; 158.64.1.14; };`

- Domain configuration

```
zone "lll.lu" IN {
        type master;
        file "lll.lu.zone";
        allow-transfer { 213.166.63.242; };
        notify yes;
};
```

- Slave domain (secondary ns):

```
zone "freeducation.org.lu" IN {
        type slave;
        file "slave/freeducation.org.lu";
        masters {  213.166.63.242; };
        transfer-source 158.64.28.133;
};
```

Server apps: DNS > zone file

- Defines individual name-to-IP translations
- Usually located in `/var/lib/named`

Server apps: DNS > zone file (1)

- SOA Record

```
@       1D      IN      SOA     ns.lll.org.lu.  hostmaster.lll.org.lu. (
                 2003110601      ; serial date + 2 digits
                 28800           ; refresh, seconds
                 7200            ; retry, seconds
                 604800          ; expire, seconds
                 86400 )         ; minimum, seconds
```

- NS Record: tells who is nameserver

```
          1D IN NS      ns.lll.lu.
          1D IN NS      sendar.prophecy.lu.     ; secondary ns
```

- A Record: name to IP translation

```
tuxtux    1D IN   A       158.64.28.133
```

- MX Record: who handles the mail for this domain?

```
          1D IN MX      10 mail.lll.lu. ; primary mail host
          1D IN MX      20 lll.lgl.lu.  ; backup mail host
```

Server apps: DNS > zone file (2)

- CNAME : an alias for a full name

```
www         1D IN   CNAME tuxtux
```

- Delegatation: configure lower-level name server

```
lgl.lu.     IN      NS      ns.lgl.lu.
lgl.lu.     IN      NS      ns.restena.lu.
ns.lgl.lu.  IN      A       158.64.72.230
```

Server apps: DNS analysis

- Dig command
  - `dig -t ns @ns1.dns.lu lgl.lu`

Server apps: DNS > rev. lookup

- In master file (named.conf)

```
zone "28.64.158.in-addr.arpa" IN {
        type master;
        file "158.64.28.zone";
        allow-update { none; };
};
```

- In zone file

```
133     IN PTR   tuxtux.lll.lu.
```

Server apps: Apache

- Serves Web pages
- Standalone daemon
- Configured using `/etc/httpd/httpd.conf` and `.htaccess`
  - `ServerName`
  - `DocumentRoot`
  - `DirectoryIndex`
  - `NameVirtualHost`
  - `<VirtualHost>`
  - `Include`
  - `Options +ExecCGI +FollowSymLinks`
- Documentation at `http://httpd.apache.org/`

Server apps: VirtualHost example

```
<VirtualHost *:80>
ServerName www.udpcast.linux.lu
ErrorDocument 404 http://udpcast.linux.lu
UserDir disabled
ServerAlias *udpcast*
ServerAdmin aknaff@lll.lu
DocumentRoot /home/aknaff/public_html/udpcast
</VirtualHost>
```

Server apps: Squid

- Caches Web requests
- Standalone daemon

Server apps: Squid > configuration

- Configured via `/etc/squid/squid.conf`:
  - `acl name criterion parameters`
  - `http_access allow|deny [!]aclname`
  - `deny_info FILE aclname`
  - `auth_param basic program /usr/sbin/pam_auth`
  - Order is important

Server apps: Squid > configuration

- Example:
  - Allow all access from inside
  - For outside access, ask for password

```
auth_param basic program /usr/sbin/pam_auth
auth_param basic children 5
auth_param basic realm Squid proxy-caching web server
auth_param basic credentialsttl 1 minute
acl localNets src 10.0.0.0/255.0.0.0 127.0.0.1
acl password proyx_auth REQUIRED
http_access allow localNets
http_access allow password
http_access deny all
```

- Documentation at `http://www.squid-cache.org/`

Squid > transparent proxy

- The NAT router intercepts all connections meant for external Web servers and pipes them through a local Squid (proxy) process

```
iptables -t nat -I PREROUTING -p tcp --dport 80 -i eth0 \
-j DNAT --to-destination 10.10.0.1:3128
```

- Squid must be prepared to receive transparent requests

```
httpd_accel_uses_host_header on
httpd_accel_with_proxy on
httpd_accel_host virtual
```

Server apps: Squid > logfile

- Log files can be found in `/var/log/squid/access.log`
- Example:

```
1033291882.682    132 127.0.0.1 TCP_MISS/200 14634 GET http://www.pt.lu/ -
DIRECT/194.154.192.107 text/html


1033377731.635    130 192.168.37.143 TCP_MISS/200 14626 GET
http://www.pt.lu/ aknaff DIRECT/194.154.192.107 text/html
```

Server apps: SSH

- Encrypted remote login to other sites
- Possibility to tunnel X protocol: `ssh -X somehost`
- Possibility to tunnel aribitrary ports (protection against snooping):
  - `ssh -L 5900:localhost:5900 somehost`
  - `ssh -R 6001:localhost:6000 somehost`
- Default configuration suitable for most uses
- Optional key-based authentication

Server apps: Vsftpd

- Access to downloadable files
- Started by `xinetd`
- Not encrypted
- Possibility to have "anonymous" users
- `/etc/ftpusers`
- Advanced configuration in `/etc/vsftpd.conf`
  - enable/disable anonymous users
  - upload directories
  - ...

Server apps: Vsftpd (config)

- Enable writing
  - `write_enable=YES`
- Anonymous access
  - `anonymous_enable=YES`
- Enable uploading
  - `anon_upload_enable=YES`
  - `chown_uploads=YES`
  - `chown_username=ftpadmin`
  - `anon_umask=077`
- Chrooted environment for local users
  - `chroot_local_user=YES`
  - `chroot_list_enable=YES`
  - `chroot_list_file=/etc/vsftpd.chroot_list`
- Resource limits
  - `anon_max_rate=7200`
  - `max_clients`
  - `max_per_ip`

Server apps: Mail

- Sendmail
  - sends mail to other machines
  - receives mail from other machines
- Imap, Pop
  - allows users to browse their mailbox

Server apps: Mail > Sendmail

- Standalone daemon
- /etc/mail directory

Server apps: Mail > Sendmail (1)

- aliases
  - nice names for users (incoming)
- virtusertable
  - same as aliases, but for managing several mail domains
- genericstable
  - nice names for users (outgoing)
- mailertable
  - "manually" configure paths to certain destinations

Server apps: Mail > Sendmail (2)

- local-host-names (sendmail.cw)
  - Defines which domains are local mailboxes
- access
  - Spam control
- relay-domains
  - Defines who may use this mailer
  - Destination or origin must be local (or both)
- sendmail.mc (linux.mc)
  - Master configuration files

- After changing one of the files, you need to type

```
make
/etc/init.d/sendmail reload

newaliases
```

Server apps: Mail > Sendmail

sendmail.mc / linux.mc:

- MASQUERADE_AS: outgoing domain name
- FEATURE(‘dnsbl’, ..., ...): spamcontrol
- GENERICS_DOMAIN(‘mailhost.test.lu’)

Server apps: Mail > Sendmail

- Documentation at http://www.sendmail.org

Server apps: Mail > Imap

- Started by `xinetd`
- Needs almost no configuration
- For encrypted operation, key File in `/etc/ssl/certs/imapd.pem`
- Access by mail client such as `kmail` or `mozilla`

Server apps: Mail > Imp

- Web application: started by apache
- Part of the Horde project
- Horde is composed of several projects:
  - Imp: web mail
  - Turba: address book
  - Kronolith: calendar

Horde preparations (1)

- Install php (`rpm -i php-4*.rpm`)
- On Redhat switch on
  `short_open_tag = On`
- Install missing pear modules

```
pear install http://pear.php.net/get/Log
pear install http://pear.php.net/get/Net_Socket
pear install http://pear.php.net/get/Mail_Mime
```

- Download and untar Horde

Horde preparations (2)

- Webmail.conf file

```
# ##########################################
# Webmail configuration
Alias /horde/ "/usr/local/horde-2.2.4/"
Alias /webmail "/usr/local/horde-2.2.4/imp-3.2"


<Directory /usr/local/horde-2.2.4>
   DirectoryIndex index.php
   Options Indexes FollowSymLinks
   AllowOverride None
   order allow,deny
   allow from all
   <IfModule mod_php4.c>
      php_flag session.bug_compat_42 off
      php_flag session.bug_compat_warn off
      php_flag short_open_tag on
   </IfModule>
</Directory>
```

Horde preparations (3)

- Include it from httpd.conf:

```
Include "/etc/httpd/webmail.conf"
```

- Or (on SuSE) put it into `/etc/sysconfig/apache` and run `SuSEconfig --module apache`:

```
HTTPD_CONF_INCLUDE_FILES="webmail.conf"
```

Horde basic setup

- File: `horde/config/horde.php`
- Where to store user's preferences?

```
$conf['prefs']['driver'] = 'sql';
```

- Where is the database located?

```
$conf['prefs']['params']['phptype']='mysql';
$conf['prefs']['params']['hostspec']='localhost';
$conf['prefs']['params']['username']='horde';
$conf['prefs']['params']['password']='xxxxxx';
$conf['prefs']['params']['database']='horde';
$conf['prefs']['params']['table']='horde_prefs';
```

- How to send mail?

```
$conf['mailer']['type'] = 'smtp';
```

Horde basic setup (alternatively).

/usr/local/horde-2.2.4/config/horde.php:

```
<?php
   require "/usr/local/horde-2.2.4/password.inc";
...
   $conf['prefs']['params']['phptype']='mysql';
   $conf['prefs']['params']['hostspec']='localhost';
   $conf['prefs']['params']['username']='horde';
   $conf['prefs']['params']['password']=$horde_pass;
   $conf['prefs']['params']['database']='horde';
   $conf['prefs']['params']['table']='horde_prefs';
...
```

/usr/local/horde-2.2.4/password.inc:

```
<?
$horde_pass="xxxx";
?>
```

Horde registry (apps and auth)

- File: `horde/config/registry.php`
- Chose application which manages login:

```
$this->registry['auth']['login'] = 'imp';
$this->registry['auth']['logout'] = 'imp';
```

- Activate applications:

```
$this->applications['imp'] = array(
     'fileroot' => dirname(__FILE__) . '/../imp',
     'webroot' => $this->applications['horde']['webroot'].'/imp',
     'icon' => $this->applications['horde']['webroot'].'/imp/graphics/imp.gif',
     'name' => _("Mail"),
     'allow_guests' => false,
     'show' => true
);

$this->applications['turba'] = array(
     'fileroot' => dirname(__FILE__) . '/../turba',
     'webroot' => $this->applications['horde']['webroot'].'/turba',
     'icon' => $this->applications['horde']['webroot'].'/turba/graphics/turba.gif',
     'name' => _("Addressbook"),
     'allow_guests' => false,
     'show' => true
);
```

Imp header menu

- File: `horde/imp/config/menu.php`
- Add icon for Turba, the address manager

```
$_menu[] = array(
    'url' =>        '/horde/turba',
    'text' =>       'Address Book',
    'icon' =>       'turba.gif',
    'icon_path' =>  '/horde/turba/graphics',
    'target' =>     '_blank',
    'onclick' =>    ''
);
```

URL of this presentation

- This presentation will be placed at the following address

`http://www.lll.lu/Presentations/ld2003adv/ld2003.pdf`