DNS/DNSSEC Workshop

A few Linux/UNIX basics

UNIVERSITY OF OREGON

NSRC
Network Startup Resource Center

Our chosen platform

Ubuntu Linux

- LTS = Long Term Support
- no GUI, we administer using ssh
- Ubuntu is Debian underneath

- There are other platforms you could use:
  - CentOS / RedHat, FreeBSD, …
- This isn’t a UNIX admin course, but some knowledge is necessary:
  - Worksheets are mostly step-by-step
  - Please help each other or ask us for help

Some things we'll need to do…

Be *`root`* when necessary: `sudo <cmd>`

Install packages:

```
apt-get install <package_name>
```

Edit files:

```
sudo editor /etc/motd
```

Installed editors include nano, jed, joe and vi*

Some things we'll need to do…

Check for the process "apache"

```
ps auxwww | grep apache
```

Start/Stop/Status of services

```
service <NAME> [start|stop|status]
```

vi editor

- The default editor for all UNIX systems
  - Can be difficult to use
  - If you know it and prefer to use vi please do
- We provide a PDF reference in the materials on the workshop wiki

THE MUG OF VI
move to line n
left, right, up, down one character
left or right n words
backward, forward one screen
up, down one screen
go to end of line, end of file
go to beginning of line (zero)
move to next, previous sentence
move to next, previous paragraph
move forward, back one word
go to end of current or next word
COOL STUFF
change case
transpose characters
combine current line with next
create a mark called p
return to p
del, copy text from mark to cursor
indent n lines

Other editors

- jed
  - F10 brings up the editor menu
  - Cursors work as you expect
- joe
  - Ctrl-k-h brings up the editor menu
  - Ctrl-c aborts
  - Cursors work as you expect

Other editors

- nano
  - – Ctrl-x y “n” quit without saving
  - – Ctrl-x y “y” to quit and save
  - – Ctrl-g for help
  - – Ctrl-w for searching
  - – Cursors work as you expect

Other tools

Terminate foreground program: CTRL+C

```
$ ping yahoo.com
PING yahoo.com (67.195.160.76): 56 data bytes
64 bytes from 67.195.160.76: icmp_seq=0 ttl=45 time=221.053 ms
64 bytes from 67.195.160.76: icmp_seq=1 ttl=45 time=224.145 ms
^C     🡐 here press CTRL + C
```

Browse the filesystem:

```
cd /etc
ls
ls -l
```

Rename and delete files

```
mv file file.bak
rm file.bak
```

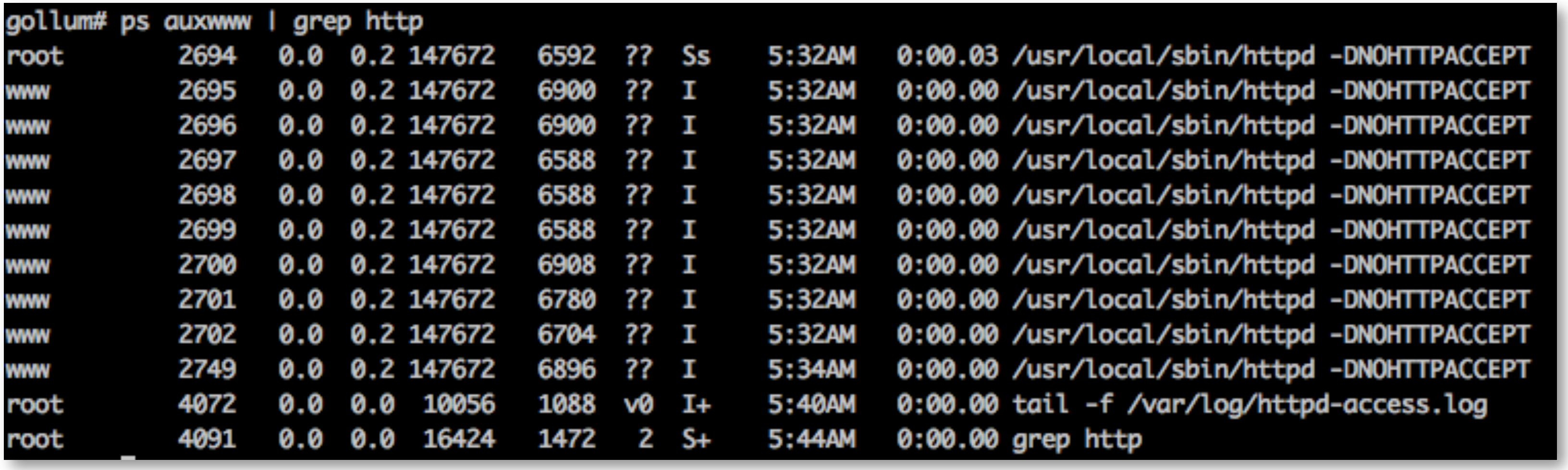
Starting and stopping services

- Standard method

```
sudo service SERVICE_NAME
[stop|start|restart]
```

Check for a process by name

- `ps auxwww | grep http`



```
gollum# ps auxwww | grep http
root        2694  0.0  0.2 147672   6592  ??  Ss     5:32AM   0:00.03 /usr/local/sbin/httpd -DNOHTTPACCEPT
www         2695  0.0  0.2 147672   6900  ??  I      5:32AM   0:00.00 /usr/local/sbin/httpd -DNOHTTPACCEPT
www         2696  0.0  0.2 147672   6900  ??  I      5:32AM   0:00.00 /usr/local/sbin/httpd -DNOHTTPACCEPT
www         2697  0.0  0.2 147672   6588  ??  I      5:32AM   0:00.00 /usr/local/sbin/httpd -DNOHTTPACCEPT
www         2698  0.0  0.2 147672   6588  ??  I      5:32AM   0:00.00 /usr/local/sbin/httpd -DNOHTTPACCEPT
www         2699  0.0  0.2 147672   6588  ??  I      5:32AM   0:00.00 /usr/local/sbin/httpd -DNOHTTPACCEPT
www         2700  0.0  0.2 147672   6908  ??  I      5:32AM   0:00.00 /usr/local/sbin/httpd -DNOHTTPACCEPT
www         2701  0.0  0.2 147672   6780  ??  I      5:32AM   0:00.00 /usr/local/sbin/httpd -DNOHTTPACCEPT
www         2702  0.0  0.2 147672   6704  ??  I      5:32AM   0:00.00 /usr/local/sbin/httpd -DNOHTTPACCEPT
www         2749  0.0  0.2 147672   6896  ??  I      5:34AM   0:00.00 /usr/local/sbin/httpd -DNOHTTPACCEPT
root        4072  0.0  0.0  10056   1088  v0  I+     5:40AM   0:00.00 tail -f /var/log/httpd-access.log
root        4091  0.0  0.0  16424   1472   2  S+     5:44AM   0:00.00 grep http
```

Viewing files

- Sometimes files are viewed through a pager program (“more”, “less”, “cat”).
- Example: `man sudo`
  - Space bar for next page
  - “b” to go backwards
  - “/” and a pattern (/text) to search
  - “n” to find *next* match, “N” to find *previous*
  - “q” to quit

Troubleshooting: Logfiles

- Log files are critical to solve problems. They reside (largely) in /var/log/<service_name>
- Some popular log files include:

```
/var/log/syslog
```

`/var/log/messages` (not always available)

- To view the last entry in a log file:

```
tail /var/log/syslog
```

- To view new entries as they happen:

```
tail –f /var/log/messages
```

Connecting via SSH to machines

- Login to your virtual machine using ssh
- On Windows use putty.exe - download from:

  http://the.earth.li/~sgtatham/putty/latest/x86/putty.exe

  or

  http://www.ws.nsrc.org/downloads/putty.exe
- Connect as user "**sysadm**" to:

  ns1.grpX => 10.1XX.2.1
  ns2.grpX => 10.1XX.2.2
  soa.grpX => 10.1XX.1.1
  Resolv.grpX => 10.1XX.1.2
- where "X" is your group number (01 -> 16)
- The password is given in class.

Logging in

- Linux/MacOS
  - First, open a terminal, then:

```
ssh sysadm@ns1.grpX.dns.nsrc.org
```

- Windows
  - Putty (or other SSH program) connect to:

    ns1.grpX.dns.nsrc.org

    1. As user ”sysadm”
    2. Accept the key
    3. Repeat for resolv.grpX, ns2.grpX and soa.grpX

- “X” is the number of your group

Using ssh

Configuring and using ssh incorrectly will guarantee a security compromise…

The wrong way:

- – Using simple passwords for users
- – Allowing root to login with a password
- – In reality – allowing *any* login with a password

The right way:

- – Disable all password access
- – Disable root access with password
- – Some disable root access completely

After you are logged in…

- Experiment with an editor
  - … vi, joe, nano
- Navigate the filesystem (cd, ls, pwd)
- Log out and log in again to see your changes. Repeat this for each virtual machine…

Questions?

?