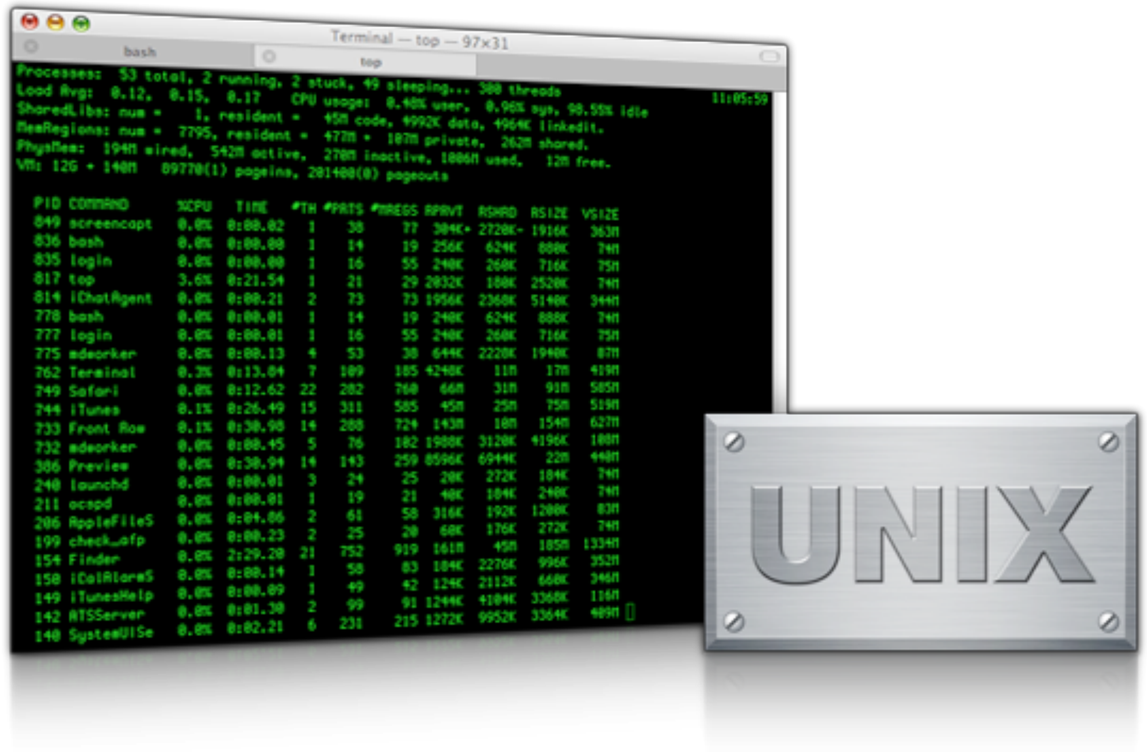
SSH, övervakning och loggning, X

Linuxadministration I 1DV417

SSH

OpenSSH


Terminal — top — 97×31
bash
top
Processes: 53 total, 2 running, 2 stuck, 49 sleeping... 380 threads 11:05:59
Load Avg: 0.12, 0.15, 0.17 CPU usage: 0.48% user, 0.96% sys, 98.55% idle
SharedLibs: num = 1, resident = 45M code, 4992K data, 4964K linkedit.
MemRegions: num = 7795, resident = 477M + 107M private, 262M shared.
PhysMem: 194M wired, 542M active, 278M inactive, 1006M used, 12M free.
VM: 12G + 140M 89770(1) pageins, 201400(0) pageouts
PID COMMAND %CPU TIME #TH #PRTS #MREGS RPRVT RSHRD RSIZE VSIZE
849 screencapt 0.0% 0:00.02 1 38 77 304K+ 2728K- 1916K 363M
836 bash 0.0% 0:00.00 1 14 19 256K 624K 888K 74M
835 login 0.0% 0:00.00 1 16 55 240K 260K 716K 75M
817 top 3.6% 0:21.54 1 21 29 2032K 108K 2520K 74M
814 iChatAgent 0.0% 0:00.21 2 73 73 1956K 2360K 5140K 344M
778 bash 0.0% 0:00.01 1 14 19 240K 624K 888K 74M
777 login 0.0% 0:00.01 1 16 55 240K 260K 716K 75M
775 mdworker 0.0% 0:00.13 4 53 38 644K 2220K 1940K 87M
762 Terminal 0.3% 0:13.04 7 189 185 4248K 11M 17M 419M
749 Safari 0.0% 0:12.62 22 282 760 66M 31M 91M 585M
244 iTunes 0.1% 0:26.49 15 311 585 45M 25M 75M 519M
733 Front Row 0.1% 0:30.90 14 288 724 143M 18M 154M 627M
732 mdworker 0.0% 0:00.45 5 76 182 1988K 3120K 4196K 108M
386 Preview 0.0% 0:30.94 14 143 259 8596K 6944K 22M 440M
240 launchd 0.0% 0:00.01 3 24 25 20K 272K 184K 74M
211 ocspd 0.0% 0:00.01 1 19 21 40K 184K 240K 74M
206 AppleFileS 0.0% 0:04.06 2 61 58 316K 192K 1200K 83M
199 check_afp 0.0% 0:00.23 2 25 20 68K 176K 272K 74M
154 Finder 0.0% 2:29.20 21 752 919 161M 45M 185M 1334M
150 iCalAlarmS 0.0% 0:00.14 1 58 83 184K 2276K 996K 352M
149 iTunesHelp 0.0% 0:00.09 1 49 42 124K 2112K 668K 346M
142 ATSServer 0.0% 0:01.30 2 99 91 1244K 9184K 3360K 116M
140 SystemUISe 0.0% 0:02.21 6 231 215 1272K 9952K 3364K 489M
UNIX

SSH - Transportlagret

1. Anslut

2. Nyckelutbyte

3. Säker tunnel

SSH - Verifikationslagret

1. Anslut

2. Nyckelutbyte

3. Säker tunnel

4. Tillgängliga verifieringsmetoder

5. Verifiering

SSH - Anslutningslagret

1. Anslut

2. Nyckelutbyte

3. Säker tunnel

4. Tillgängliga verifieringsmetoder

5. Verifiering

6. Multipla kanaler öppnas för kommunikation

Konfigurera SSH

/etc/ssh/sshd_config

port
HostKey
KeyRegenerationInterval
ListenAddress
PermitRootLogin
AllowGroups
AllowUsers
Banner

```
port 22
HostKey /etc/ssh/ssh_host_key
KeyRegenerationInterval 3600
ListenAddress 10.0.0.1
PermitRootLogin yes
AllowGroups students teachers
AllowUsers kalle nisse@challenger
Banner /etc/ssh/warning
```

SSH-verifiering

hosts.equiv/shosts.equiv
Publik nyckel för klientdatorn
Publik nyckel för användaren
Användarnamn och lösenord

sshd_config

host.equiv / shosts.equiv

/etc/hosts.equiv
/etc/shosts.equiv
.rhosts
.shosts

challenger

sshd_config

```
RhostAuthentication no
IgnoreRhosts yes
```

Publik nyckel för klientdatorn

/etc/ssh_known_hosts

```
ssh-keyscan -t rsa klient.kalmar.se
```

sshd_config

```
HostbasedAuthentication yes
```

Publik nyckel för användaren

Logga in på klienten

```
ssh-keygen –q –t rsa –f ~/.ssh/id_rsa
```

```
scp ~/.ssh/id_rsa.pub 10.0.0.1:~/.ssh/id_rsa.client
```

Logga in på SSH-servern
Gå i katalogen ~/.ssh och verifiera att filen id_rsa.client återfinns där

```
cat id_rsa_client >> authorized_keys
```

Rekommenderade rättigheter på filen authorized_keys är 600, då endast du själv ska kunna läsa och skriva i filen

sshd_config

```
PubkeyAuthentication yes
```

Lösenordsautentisiering

sshd_config

```
PasswordAuthentication yes
```

SSH-klient

PuTTY (Windows)
ssh (Linux/Unix)

```
ssh 10.0.0.1
```

/etc/ssh/ssh_config

Kommandon som använder SSH

scp - Secure Copy

```
scp marcus@challenger:~/list.txt marcus@voyager:~/
scp ~/list.txt marcus@voyager:~/
```

sftp - Secure FTP

SSH-tunnel

```
ssh -f user@personal-server.com -L 2000:personal-server.com:25 -N
```

Skapar en SSH-tunnel från localhost:2000 via personal-server.com's SSH daemon till port 25 på samma maskin

```
ssh -f -L 3000:talk.google.com:5222 home-server.com -N
```

Skapar en SSH-tunnel från localhost:3000 via home-server.com's SSH daemon till port 5222 på talk.google.com

Övervakning

Processer och processortid	vmstat
Minnet	uptime
Hårddisksaktivitet	free
Hårddisksutrymme	swapon
	iostat
	df

vmstat

ps, top, vmstat

```
marcus@server1:/var/log$ vmstat
procs -----------memory---------- ---swap-- -----io---- -system-- ----cpu----
 r  b   swpd   free   buff  cache   si   so    bi    bo   in   cs us sy id wa
 2  0  99872  23216  27204 3230924    0    0   151   212    2    0  2 53 41  3
```

uptime

```
# uptime
 11:10am  up  1:35,  1  user,  load average:  0.95,  0.38,  0.31
```

Tim O'Reilly and Crew

What's high? ... Ideally, you'd like a load average under, say, 3, ... Ultimately, 'high' means high enough so that you don't need uptime to tell you that the system is overloaded.

free

```
marcus@callisto:~$ free -t
             total       used       free     shared    buffers     cached
Mem:       2051720     856080    1195640          0     187640     379256
-/+ buffers/cache:     289184    1762536
Swap:            0          0          0
Total:     2051720     856080    1195640
marcus@callisto:~$
```

swapon

```
swapon –s
Filename        Type            Size        used    priority
/dev/sda3       partition       265064      0       -1
```

iostat

```
root@callisto:~# iostat
Linux 3.2.0-24-generic (callisto.nickebo.net)   02/22/2013      _x86_64_        (1 CPU)

avg-cpu:  %user   %nice %system %iowait  %steal   %idle
          0.03    0.00    0.02    0.20    0.00   99.74

Device:            tps    kB_read/s    kB_wrtn/s    kB_read    kB_wrtn
vda               0.24         0.12         1.49     393175    4851116

root@callisto:~#
```

df

```
# df -hlt ext3
Filesystem      Size  Used Avail Use% Mounted on
/dev/sda2       2.9G  1.4G  1.3G  50% /
/dev/sda1       144M  9.3M  127M   7% /boot
/dev/sda6       618M   17M  570M   3% /home
/dev/sda3       190M  4.1M  176M   3% /tmp
/dev/sdb        3.9G  1.8G  1.9G  47% /opt/kickstart
```

syslog

Konfiguration av syslogd / rsyslogd

/etc/syslogd.conf

/etc/rsyslogd.conf
/etc/rsyslog.d/*

```
mail.info;news.info   /var/log/mailnewslog
ftpd.crit             @voyager
```

Säkerhetsnivåer för syslogd

Tjänster	Beskrivning
*	Alla tjänster
auth	Säkerhets- och verifieringskommandion
authpriv	Känslig/privat verifieringsinformation
cron	Crondemonen
daemon	Systemdemoner
ftp	FTP-demonen ftpd
kern	Kernel
lpr	Utskriftsdemonen LPD/LPRng
mail	Sendmail och andra maildemoner
mark	Tidsstämplar
news	Usenet-demonen
syslog	syslogs interna information
user	Användarprogram

Säkerhetsnivå	Beskrivning
none	Inga meddelanden
emerg	Panikmeddelanden
alert	Viktiga meddelanden
crit	Kritiska meddeladen
err	Andra typer av fel
warning	Varningsmeddeladen
notice	Meddelanden som behöver undersökas av administratör
info	Informationsmeddelanden
debug	Används endast för felsökning

Olika typer av åtgärder

```
*.info;mail.none;authpriv.none;cron.none    /var/log/messages
```

```
*.info;mail.none;authpriv.none;cron.none    @challenger
```

```
*.info;mail.none;authpriv.none;cron.none    |/var/log/sysfifo
```

Olika typer av åtgärder forts.

```
*.info;mail.none;authpriv.none;cron.none    kalle,olle,nisse
```

```
*.info;mail.none;authpriv.none;cron.none    *
```

```
*.info;mail.none;authpriv.none;cron.none    /dev/tty12
```

rsyslogd

- Nyare version av syslogd med fler funktioner
  - /etc/rsyslogd.conf
  - /etc/rsyslog.d/*.conf

X

X Server

X-server

Skärmenhet för att rita ut grafiska komponenter på
En eller flera inmatningsenheter (tangentbord, mus)

X11Forwarding

X11Forwarding forts.

Programserver

Arbetsstation med X-server

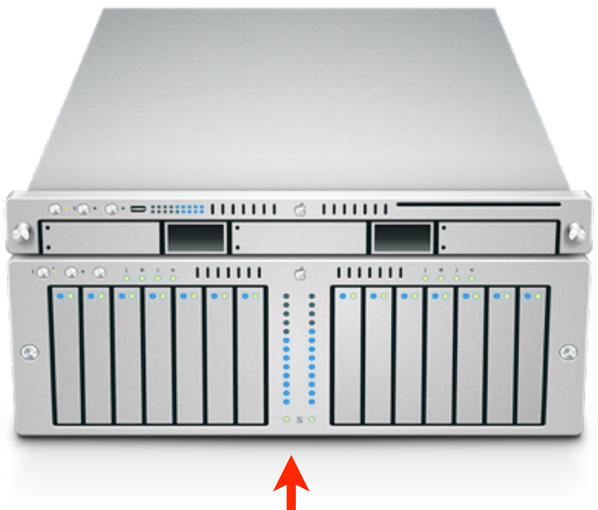
Programserverkonfiguration

```
> echo $DISPLAY
:0.0
```

```
> export DISPLAY=10.0.0.10:0.0
```

Körning av grafiska applikationer

10.0.0.2



Program

10.0.0.10:0.0

Vidarebefodra X genom SSH

/etc/ssh/sshd_config

```
X11Forwarding yes
```

/etc/ssh/ssh_config

```
ForwardX11 yes
```