Debian/Linux Administration

Stefan Hornburg (Racke)

Contents

systemd is covered in a separate document.

Logging

Watch log file entries for sympa and postfix services (analogous to `tail -f`):

```
journalctl -u sympa.service -u postfix.service -f
```

Test remote syslog server:

```
~# logger --server=audit.intern -P 40615 "Test Splunk connnection"
```

Recommended Debian packages

cron-apt

etckeeper

On Ubuntu, the preconfigured VCS is `bzr`. In order to use Git, please edit the VCS lines in `/etc/etckeeper/etckeeper.conf`:

```
# The VCS to use.
#VCS="hg"
VCS="git"
#VCS="bzr"
#VCS="darcs"
```

After that, run `etckeeper init` to setup the Git repository.

fail2ban

See Fail2ban below. An alternative to Fail2ban is SSHGuard.

ferm

Check configuration file for errors:

```
ferm --noexec /etc/ferm/ferm.conf
```

Show the *iptables* commands before they are executed:

```
ferm --lines /etc/ferm/ferm.conf
```

needrestart

screen

Security

Fail2ban

Fail2ban activates only the *sshd* jail by default:

```
$ fail2ban-client status
Status
|- Number of jail:     1
`- Jail list:     sshd
```

Unban an ip

```
$ fail2ban-client set nextcloud unbanip 93.184.216.34
93.184.216.34
```

SSH

Password authentication

Turn off password authentication in `/etc/ssh/sshd_config`:

```
PasswordAuthentication No
```

Conditions

Allow weak algorithm for old server only:

```
Match Address 10.11.12.13
  PubkeyAcceptedAlgorithms +ssh-rsa
```

Negation:

```
Match Address *,!10.11.12.13
  PasswordAuthentication no
```

Remove host keys

By domain:

```
$ ssh-keygen -R foo.linuxia.de
```

By IP and port:

```
$ ssh-keygen -R '[10.11.12.137]:77127'
```

Networking

TCP and Unix Sockets

Show listening TCP sockets (long and short form):

```
ss --listen --tcp
ss -l -t
```

See also: lsof

Outgoing SSH connections from server with the IP `146.0.35.17` through network interface `eth0`:

```
tcpdump -i eth0 port 22 and 'tcp[tcpflags] == tcp-syn' and src 146.0.35.17
```

UDP

Display UDP packages going to another server *foomachine*:

```
tcpdump -i eth0 ip host foomachine
```

Network Manager

The commandline tool `nmcli` may show you the list of wireless networks with the following command:

```
$ nmcli dev wifi list
```

Be aware that shows you an **empty list** (without error message) when *wpa_ supplicant* service is not running.

To show a list of connections:

```
$ nmcli con show
```

Resources

Monitoring and Tuning the Linux Networking Stack: Sending Data

Libvirt

Domains

Show all domains:

```
~# virsh list
 Id   Name                    State
--------------------------------------
 4    buster-test-box    running
```

Networks

Show network list:

```
~# virsh net-list
 Name              State    Autostart   Persistent
-------------------------------------------------------
 default           active   no          yes
 vagrant-libvirt   active   no          yes
```

Show network info:

```
~# virsh net-info default
Name:           default
UUID:           0532c102-48d1-4c0e-a8f3-1024a83b3f4a
Active:         yes
Persistent:     yes
Autostart:      no
Bridge:         virbr0
```

Show info on DHCP leases:

```
~virsh net-dhcp-leases default
```

Apt

Installation from package file

You need to pass the path to be´the package file. It doesn't work with the filename only.

```
apt install ./containerd_1.4.4~ds1-1_amd64.deb
```

This also allows you to install multiple package files:

```
apt install /usr/local/pkgs/*.deb
```

Repositories

To use Debian repositories on Ubuntu install package *debian-archive-keyring* first. After that you need to add the required key to the trusted keys (`https://wiki.debian.org/SecureApt`), e.g.:

```
apt-key add /usr/share/keyrings/debian-archive-stretch-stable.gpg
```

Show all versions of a package

```
$ apt-cache madison gitlab-runner
gitlab-runner |     15.0.0 | https://packages.gitlab.com/runner/gitlab-runner/ubuntu focal/main amd6
gitlab-runner |    14.10.1 | https://packages.gitlab.com/runner/gitlab-runner/ubuntu focal/main amd6
gitlab-runner |    14.10.0 | https://packages.gitlab.com/runner/gitlab-runner/ubuntu focal/main amd6
gitlab-runner |     14.9.2 | https://packages.gitlab.com/runner/gitlab-runner/ubuntu focal/main amd6
...
```

Upgrade distribution to a new release

Make sure that you know the root password, in case you want to login through a remote console to troubleshoot the upgrade.

Problems

Sometimes maintainer scripts are failing without useful error messages.
It can be useful in these cases to trace the processing of *debconf* values:

```
export DEBCONF_DEBUG=developer
```

Hold and unhold packages

Packages in *hold* state are skipped by upgrades.
Set package `nginx` into *hold* state:

```
apt-mark hold nginx
```

Re-enable upgrades for `nginx`:

```
apt-mark unhold nginx
```

Preferences

In order to set lower priority for packages from unstable (sid) add a file to the `/etc/apt/preferences.d` directory:

```
~ cat /etc/apt/preferences.d/00sid
# Lower priority for unstable
Package: *
Pin: release o=Debian,a=unstable,n=sid
Pin-Priority: 300
```

Proxies

```
Acquire::http::Proxy "http://proxy.example.com:6123";
Acquire::https::Proxy "http://proxy.example.com:6123";
Acquire::http::Proxy::repo.example.com DIRECT;
```

Upgrades

Download packages only:

```
apt-get dist-upgrade --download-only
```

Unattended upgrades

Install the following packages:

```
apt-get install unattended-upgrades apt-listchanges
```

Activate unattended upgrades by creating or editing /etc/apt/apt.conf.d/20auto-upgrades:

```
APT::Periodic::Update-Package-Lists "1";
APT::Periodic::Unattended-Upgrade "1";
```

On Debian 9 and above the package includes two systemd timers:

apt-daily.timer APT updates

apt-daily-upgrade.timer APT upgrades

You find the log file at `/var/log/unattended-upgrades/unattended-upgrades.log`.
The default configuration file is `/etc/apt/apt.conf.d/50unattended-upgrades`.
See also:
Debian Wiki page on Unattended upgrades

Diversions

Diversions are used by Debian packages to prevent conflicts between files with the same name in different packages. Using *alternatives* or *Conflicts* relation is the preferred method though.

List diversions:

```
dpkg-divert --list '*'
```

The diversions are saved in `/var/lib/dpkg/diversions`.

Users

Change login shell

`$ usermod -s /bin/bash sympa`

Locales

Show enabled locales:

```
$ locale -a
C
C.UTF-8
POSIX
en_US.utf8
```

LVM

Debian Wiki

Architectures

Display current architecture:

```
~# dpkg --print-architecture
amd64
```

Display supported architectures (needs `arch-test` package to be installed):

```
~# arch-test
amd64
i386
```

See also: `https://wiki.debian.org/Multiarch/HOWTO`
CrossGrading: https://wiki.debian.org/CrossGrading
Never tried that though.

Grub

Default kernel

In order to set the default kernel to boot you need to change the GRUB_DEFAULT variable in /etc/default/grub as follows:

{{ GRUB_DEFAULT=saved }}

After that, you can set it with the `grub-set-default` command:

```
$ grub-set-default 'Debian GNU/Linux, with Linux 3.2.0-4-amd64'
$ update-grub
```

Reboot into specific kernel

```
$ grub-reboot gnulinux-3.16.0-5-amd64-advanced-3871a2a4-6faf-4fec-b5f9-99fb3c75a731
$ reboot
```

RAID

You find Debian packages for proprietary and opensource tools at `https://hwraid.le-vert.net/wiki/DebianPackages`

MegaCLI

- Make sure that use the correct disk.

- The parameter `-a` refers to the adapter number (starting with 0) or to all adapters `-aALL`

Disable disk in RAID array

```
root@devserver:/var/cache# megacli -pdoffline -physdrv[32:1] -a0

Adapter: 0: EnclId-32 SlotId-1 state changed to OffLine.

Exit Code: 0x00
root@devserver:/var/cache# megacli -pdmarkmissing -physdrv[32:1] -aALL

EnclId-32 SlotId-1 is marked Missing.

Exit Code: 0x00
root@devserver:/var/cache# megacli -pdprprmv -physdrv[32:1] -aALL


Prepare for removal Success

Exit Code: 0x00
```

Clear disk in RAID array

Please be careful with these commands!
Starting the process:

```
root@fileserver:~# megacli -pdclear -start  -physdrv[32:1] -aALL

Started clear progress on device(Encl-32 Slot-1)

Exit Code: 0x00

root@fileserver:~# megacli -pdclear -showprog  -physdrv[32:1] -aALL

Clear Progress on Device at Enclosure 32, Slot 1 Completed 2% in 0 Minutes.

Exit Code: 0x00
```

```
root@fileserver:~# megacli -pdclear -showprog  -physdrv[32:1] -aALL

Device(Encl-32 Slot-1) is not in clear process

Exit Code: 0x00
```

Resources

Reference docs https://things.maths.cam.ac.uk/computing/docs/public/megacli_raid_lsi.html

Replacing disk with MegaCLI http://www.advancedclustering.com/act_kb/replacing-a-disk-with-megacli

Troubleshooting

Check whether system files have been changed:

```
debsums -c
```

Speed test

```
apt-get install speedtest-cli
speedtest-cli
```

Building from source

Problems and solutions

Problem:

```
configure.ac:31: warning: macro 'AM_PO_SUBDIRS' not found in library
configure.ac:31: error: possibly undefined macro: AM_PO_SUBDIRS
      If this token and others are legitimate, please use m4_pattern_allow.
      See the Autoconf documentation.
autoreconf: /usr/bin/autoconf failed with exit status: 1
```

Solution:
You need to install the *gettext* package first.

Linuxia Wiki

Stefan Hornburg (Racke)
Debian/Linux Administration

wiki.linuxia.de