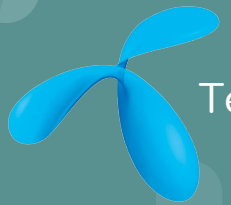
Building a secure bastion, or, 50 ways to kill your server

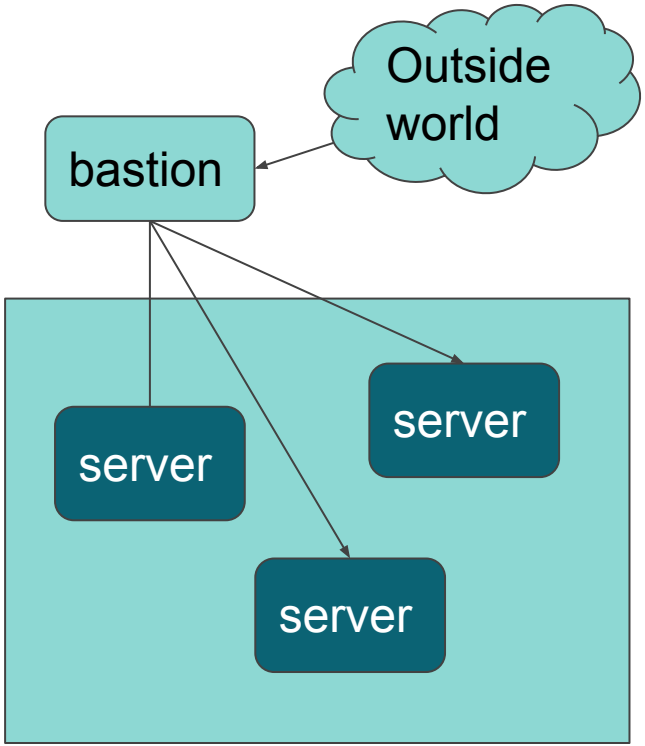
Anna Kennedy

@anna_ken_



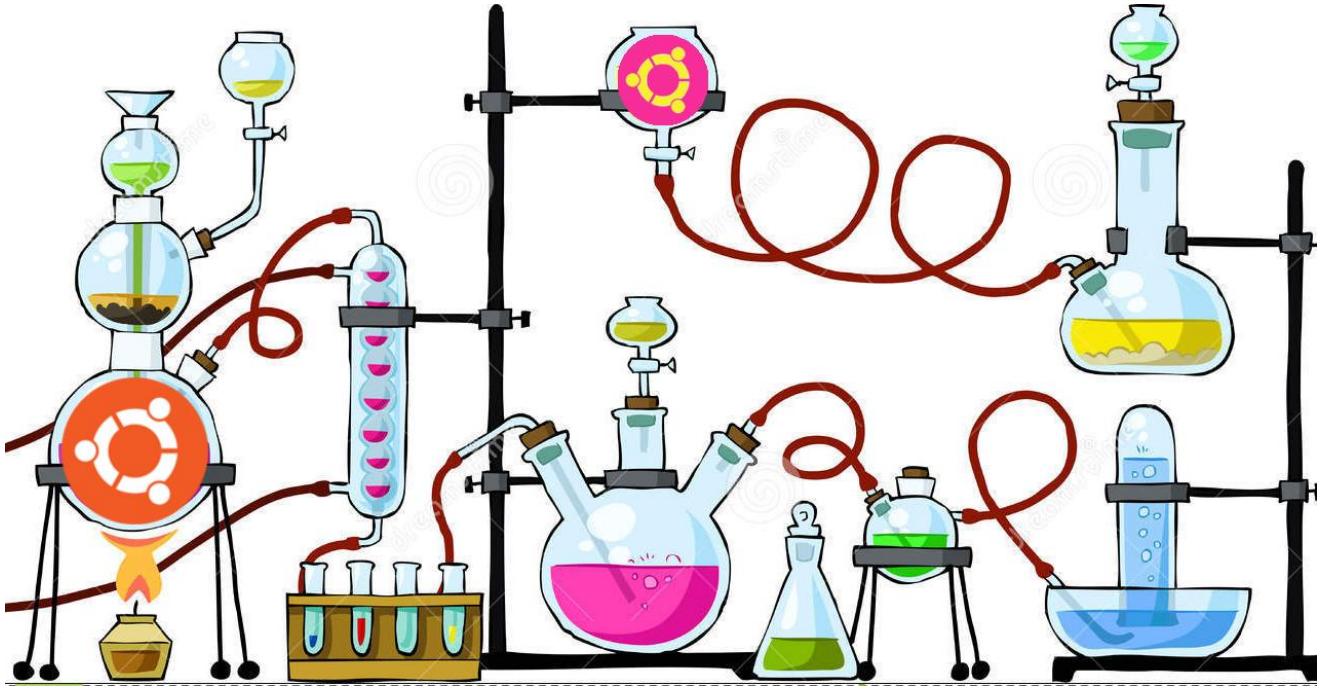
Telenor Digital

What is a bastion (jumpbox) ?



What do we mean by secure?

How do we make a custom AMI?



Technical context

HashiCorp
Packer

HashiCorp
Terraform

Ubuntu default packages

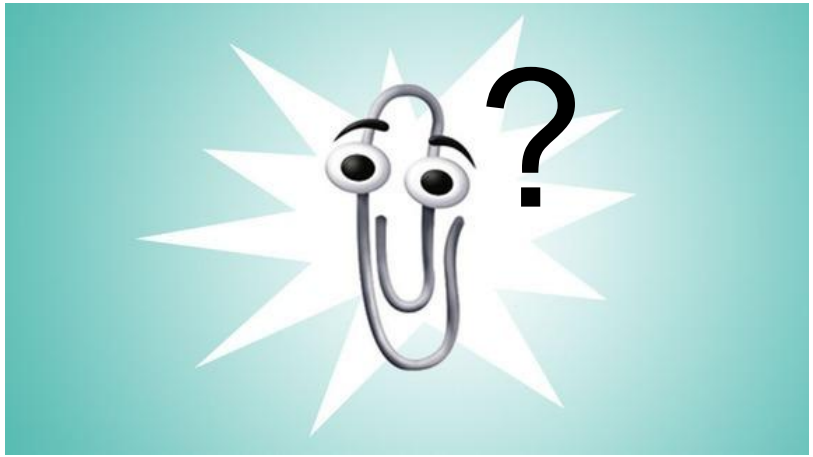
```
$ apt list --installed
Listing... Done
a11y-profile-manager-indicator/xenial,now 0.1.10-0ubuntu3 amd64 [installed]
accountsservice/xenial-updates,now 0.6.40-2ubuntu11.3 amd64 [installed]
acl/xenial,now 2.2.52-3 amd64 [installed]
acpi-support/xenial,now 0.142 amd64 [installed]
acpid/xenial,now 1:2.0.26-1ubuntu2 amd64 [installed]
activity-log-manager/xenial-updates,now 0.9.7-0ubuntu23.16.04.1 amd64 [installed]
adduser/xenial,xenial,now 3.113+nmu3ubuntu4 all [installed]
adium-theme-ubuntu/xenial-updates,xenial-updates,now 0.3.4-0ubuntu1.1 all [installed]
adwaita-icon-theme/xenial-updates,xenial-updates,now 3.18.0-2ubuntu3.1 all [installed]
aisleriot/xenial,now 1:3.18.2-1ubuntu1 amd64 [installed]
alien/xenial,xenial,now 8.95 all [installed,automatic]
alsa-base/xenial,xenial,now 1.0.25+dfsg-0ubuntu5 all [installed]
alsa-utils/xenial,now 1.1.0-0ubuntu5 amd64 [installed]
anacron/xenial,now 2.3-23 amd64 [installed]
```

~2000 packages

```
$ dpkg-query -W
a11y-profile-manager-indicator  0.1.10-0ubuntu3
accountsservice 0.6.40-2ubuntu11.3
acl     2.2.52-3
acpi-support    0.142
acpid   1:2.0.26-1ubuntu2
activity-log-manager    0.9.7-0ubuntu23.16.04.1
adduser 3.113+nmu3ubuntu4
adium-theme-ubuntu      0.3.4-0ubuntu1.1
adwaita-icon-theme      3.18.0-2ubuntu3.1
aisleriot       1:3.18.2-1ubuntu1
alien   8.95
alsa-base       1.0.25+dfsg-0ubuntu5
alsa-utils      1.1.0-0ubuntu5
anacron 2.3-23
```

Ubuntu default packages includes:

- ed
- ftp
- curl
- nano
- perl
- python
- rsync
- sed
- telnet
- wget
- vim-common



- adduser
- apt
- dpkg

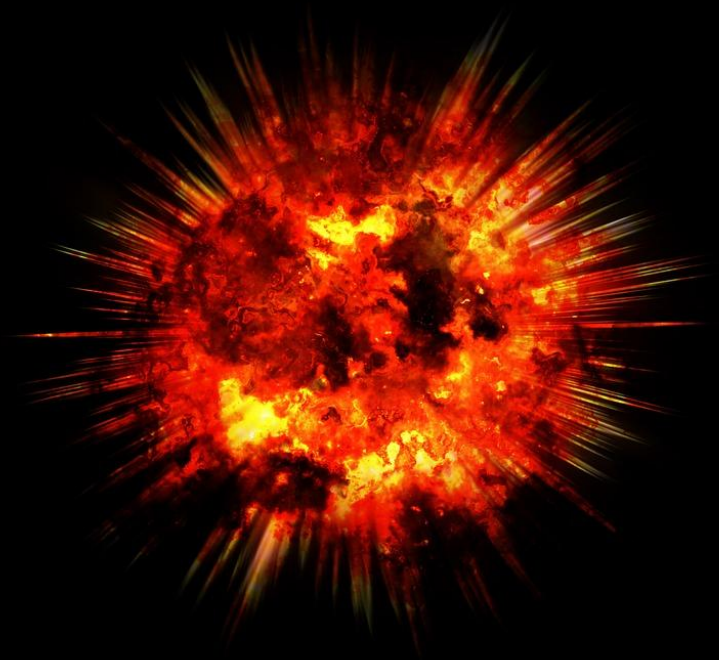
- screen
- tmux

Just remove all optional / extra packages

```
$ dpkg-query -Wf '${Package;-40}${Priority}\n'
apt                                      important
adduser                                  required
at                                       standard
a11y-profile-manager-indicator           optional
adium-theme-ubuntu                       extra
```

```
dpkg-query -Wf '${Package;-40}${Priority}\n' |
awk '$2 ~ /optional|extra/ { print $1 }' |
xargs -I % sudo apt-get -y purge %
```

Turns out optional doesn’t mean optional



‘Optional’ and ‘extra’ include:

- cloud-init
- grub
- linux-base
- openssh-server
- resolvconf
- ubuntu-server (meta-package)

Remove all packages that we don’t want

- ed
- ftp
- gawk
- nano
- rsync
- screen
- tmux
- vim
- wget
- curl
- net-tools
- perl
- python 2.7
- python 3
- tar

Remove all packages that we don't want, apart from the ones we can't

Can remove:

- ed
- ftp
- gawk
- nano
- rsync
- screen
- tmux
- vim
- wget

Can't remove:

- curl — needed for consul restarts
- net-tools — needed for sshuttle
- perl — needed for ssh
- python 2.7 — needed for Ansible
- python 3 — needed for AWS instance checks
- tar — needed for Ansible

Restricting user capabilities

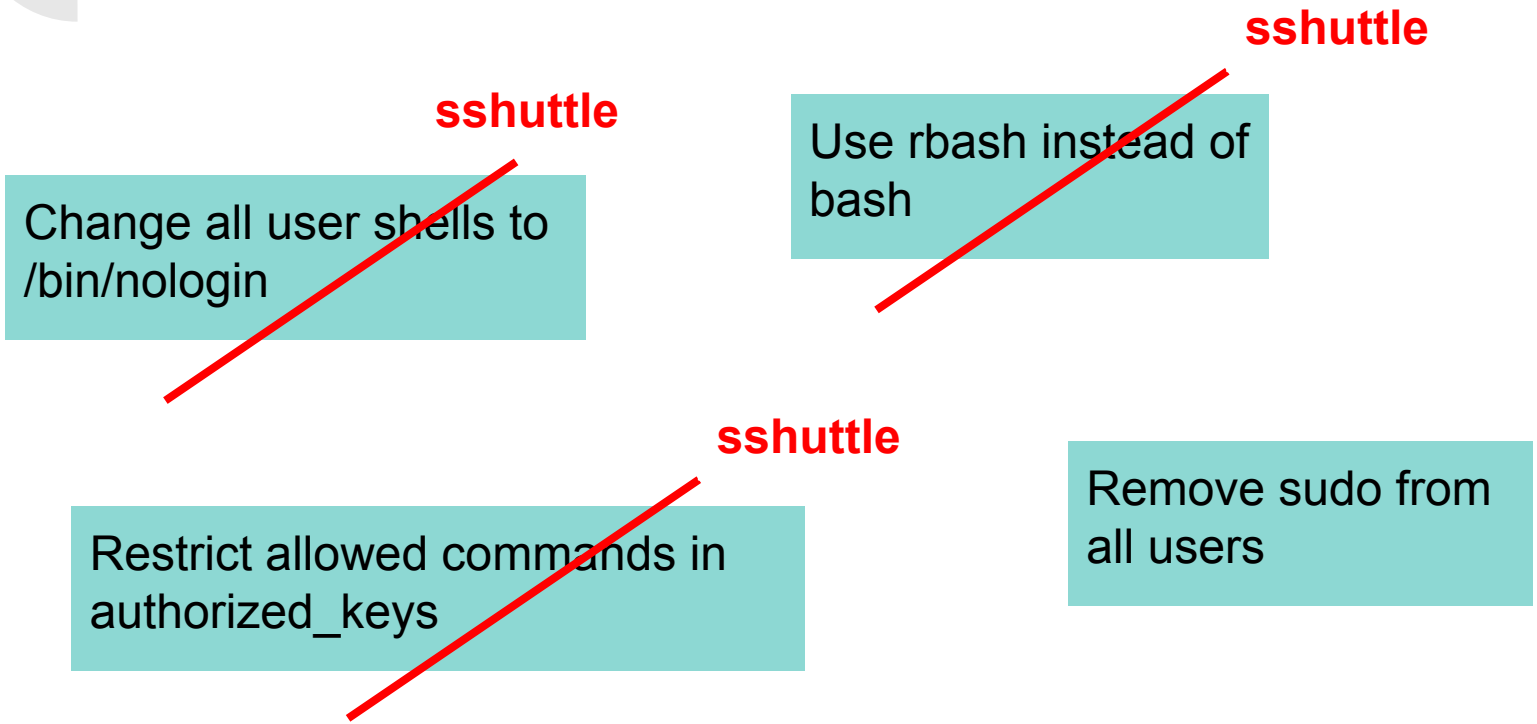
Change all user shells to /bin/nologin

Use rbash instead of bash

Restrict allowed commands in authorized_keys

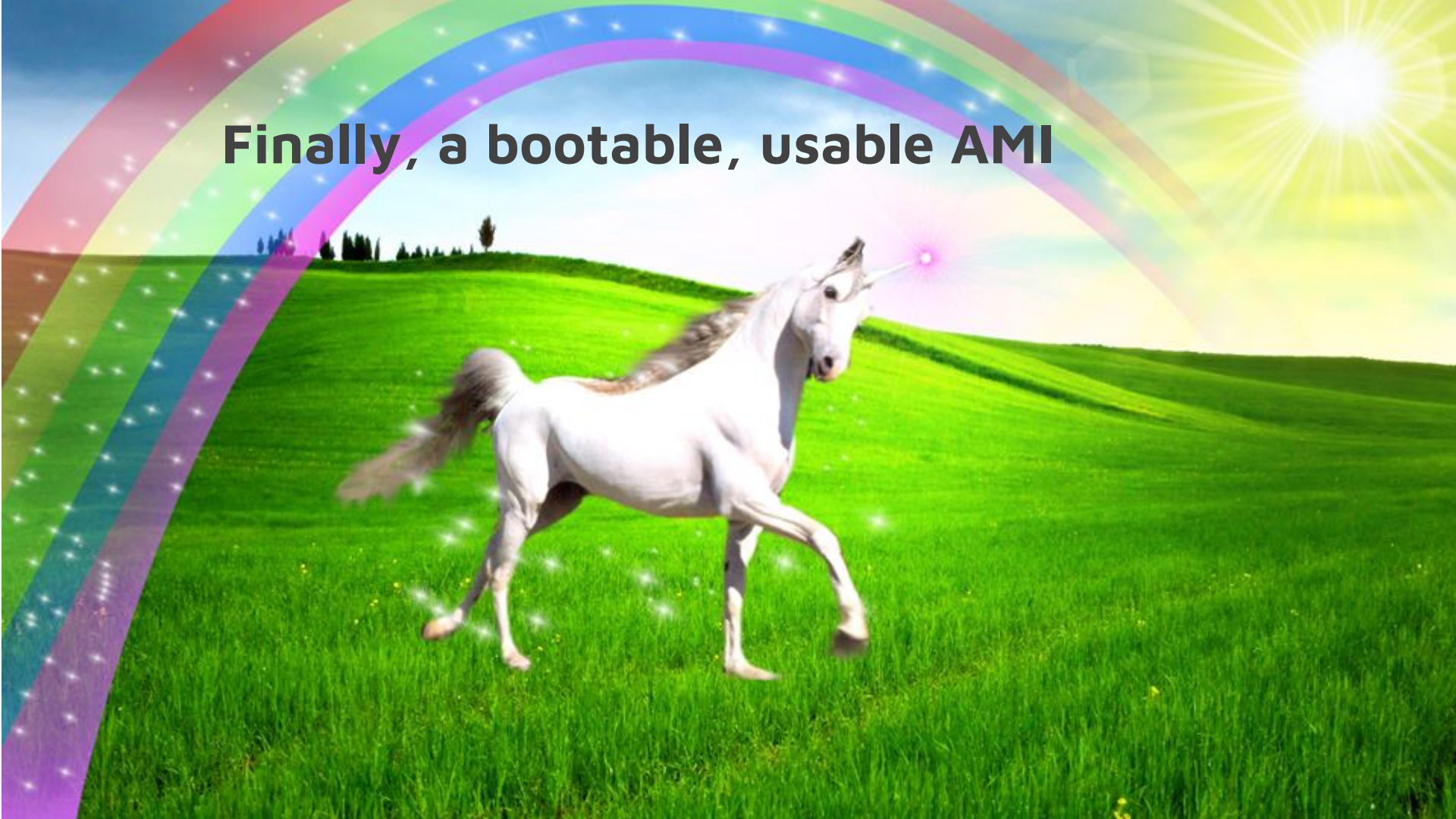
Remove sudo from all users

Restricting user capabilities



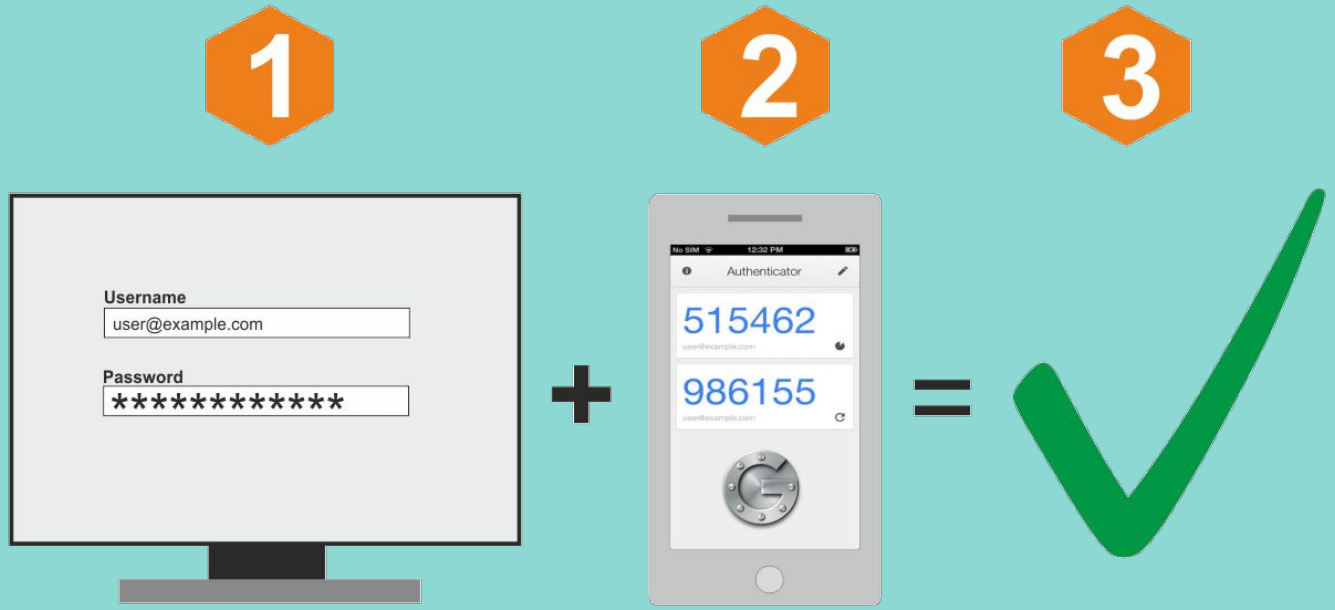
Troubleshooting without sudo

Finally, a bootable, usable AMI



Install fail2ban

Use 2FA


1
2
3
Username
user@example.com
Password
****
Authenticator
515462
986155

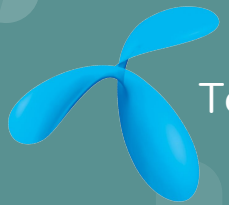
Port knocking

Safe and secure

Thanks for listening!

Anna Kennedy

@anna_ken_



Telenor Digital