



Garden Linux **Debian-based foundation for the Cloud Operating System**

Andre Russ, Dirk Marwinski, Dominik George, Michael Banck

SAP Business Technology Plattform
October 2, 2021

PUBLIC



credativ
An Instaclustr Company

THE BEST RUN



Agenda

Why yet another distribution?

Why this "Gardening" subject?

Where do we come from?

Debian and the Enterprise Lie

Features in Focus

Why open? Why here?

What is Garden Linux

- Garden Linux is a ContainerOS
- It is the Debian based interpretation of CoreOS
- It is absolutely minimal (based on minbase of Debian)
- Minbase + systemd + kernel = Garden Linux
- Kernel on steroids
- Filling the gap:
 - without installer (smaller then netinst)
 - Easy to customize
 - executable



Gardenlinux.io

github.com/gardenlinux

Motivation

- CoreOS as container Operation System was EOL
 - Other solutions like FedoraCore, SuSE JeOS, Kinfolk Flatcar...
 - Problem: \$\$\$, support, feature request, Gardener support, Competition ...
- Maximum flexibility - Owning the stack
- Mandatory
 - large user base = acceptance
 - enterprise capabilities = security, licenses, processes
- Support concept
 - External Partner (internal only is not enough)

Container – the OS of the future

- Evolving Cloud markets
- OS wars are over, Cloud wars is next
 - openness in the cloud
 - ownership of the platform
- CoreOS was an interesting approach
- Big Players are already in position
- New Players are around:
 - Hyperscalers
 - SuSE / RedHat started as Challenger



What is Gardener

100%
KUBERNETES

OPEN
SOURCE

CNCF
officially
certified!

KUBERNETES
IN KUBERNETES!
"★"

hybrid
cloud

HOMOGENEOUS
INFRASTRUCTURE

ARCHITECTURE
IN THREE COMPONENTS



RUNS
THE GARDENER
a kubernetes
controller
responsible
for managing
custom
resources



WHAT IS GARDENER?

@ANTHEAJUNG

AN EXTENDED
API SERVER &

A BUNDLE OF
KUBERNETES CONTROLLERS

THAT DEFINES AND MANAGES
NEW API OBJECTS USED FOR
MANAGEMENT OF KUBERNETES
CLUSTER

A SERVICE TO MANAGE
LARGE-SCALE KUBERNETES
CLUSTER

INTERACT
WITH

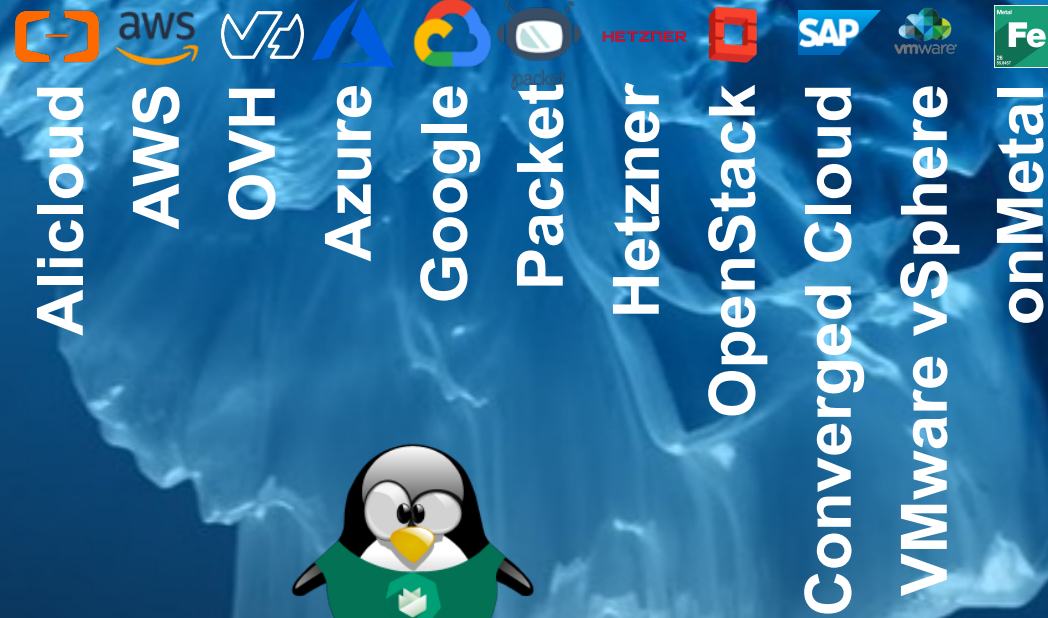


COMMAND LINE
CLIENT
\$ gardenctl
WRITTEN
IN go



THE KUBERNETES
BOTANIST

Own the stack



Garden Linux

Where do we come from

- We are from SAP
 - We have an excellent expertise in Lenox

Where do we come from

- We are from SAP
 - We have an excellent expertise in Lenox
 - We are not known for Open Source
 - We are known for being the cash cow

Cash cow ?

Vendor 1

Our Operating System costs for either
2 Sockets (we have ~300.000 sockets) or
4 Virtual Machines (we have ~500k) or
8 Container (we have a lot more)

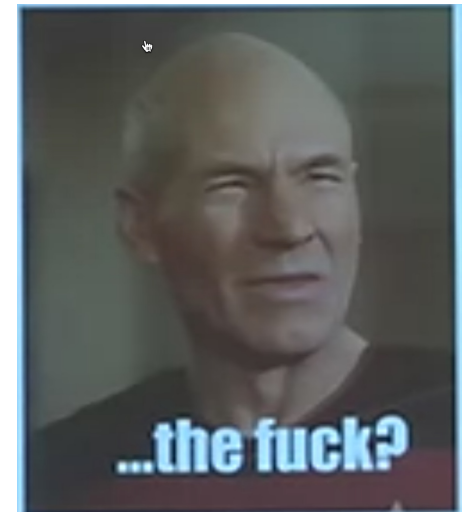
<400€ per year

Vendor 2

We don't support our operating system for your
Kubernetes offering. You can buy our
Container OS product. We give you a discount.
It is < 900€ per year per node

Vendor 3

Description	Standard	Premium
Single node annual subscription	€449	€679
Base price (5000 nodes)	€2,245,000	€3,395,000
Volume discount (50%)	-€1,122,500	-€1,697,500
Total after discount (5,000 nodes)	€1,122,500	€1,697,500



Where do we come from

- We are from SAP
- We are competition
- We are a large Enterprise
- We need Extensibility
- We need real open source
 - SuSE / Red Hat is open (partly)
 - But really open?

*Man muss es nicht nur koennen,
man muss es auch wollen.*

- small footprint (based on minbase of Debian)
- regular updates via a Pipeline
- thorough automated testing
(unit tests local, integration tests on cloud Providers, tests on Gardener)
- supporting major platforms out-of-the-box
major cloud providers AWS, Azure, Google, Alicloud
major virtualizer VMware, OpenStack, KVM
bare metal
- running scans against common issues like
license violations
scans for outdated software versions

Easy to use

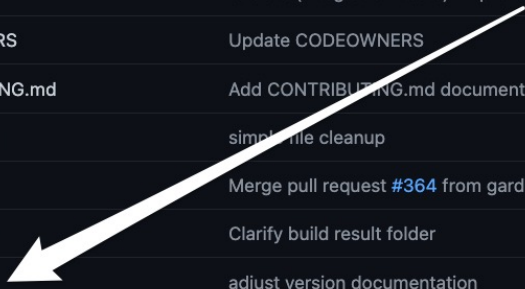


- Total heterogenous Enterprise
- Total heterogenous Knowledge
- Problems to distribute
 - Github was easy
 - Binary export? German Enterprise !
 - Export classification -> German Customs
 - Legal
 - Brand
 - Business
- We are a container OS: git, docker, make, gnupg, bash

repeatable and auditable builds



- Enterprise needs this feature
- Feature is usually pricy but free
- Changing VERSION brings you back in time
snapshot.debian.org
- Of course git brings also the tooling back!



.flake8	add default linter-cfg for python3 (using flake8)	5 months ago
.gitignore	refactor(integration-tests): improve container for integration tests	14 days ago
CODEOWNERS	Update CODEOWNERS	2 years ago
CONTRIBUTING.md	Add CONTRIBUTING.md document	yesterday
LICENSE.md	simplify file cleanup	15 months ago
Makefile	Merge pull request #364 from gardenlinux/clean-containers	15 days ago
README.md	Clarify build result folder	18 days ago
VERSION	adjust version documentation	16 months ago
VERSION.md	Fix 2 typos in VERSION.md & remove RELEASE.md	11 months ago
build.sh	Merge pull request #359 from gardenlinux/bookworm	15 days ago
flavours.md	better key handling	12 months ago
flavours.yaml	hack: patch-back flags/elements -> modifiers	8 months ago
security-response-process.md	initial commit for Security Response Process	8 months ago

purely systemd based



- Kubernetes is heavily using systemd, so is Gardener
- Network -> no ifup, ifdown, no network/interfaces
- Fstab (supported but not used)
- Repart (Growpart required too many resources)
- Initramfs is dracut, because of systemd (faster, clearly structured, less extra tools, easier to audit)

Booting is no grub

- Focus on systemd is what it is
- Grub is not easy to audit / pentest (boothole!)
- So we boot via systemd bootctl
- Sadly not signed by Debian
- Sadly only supports UEFI
syslinux on legacy
- Results in simple boot structure
ESP + root

Immutability



- Signed boot (but who? – we!)
- Feature activatable
- Without
- Poor mans (readonly /usr)
- Hard (root squashfs)
- Keeps snakeoil away

License issues!

- Debian is not good – it is excellent
- But SAP is paranoid
- BerkeleyDB is a licensing disaster
- Yes Debian stays below 6! Top
- No SAP cannot distinguish
- BerkeleyDB is a no go – So not in
- Iproute2, apt, python, pam
- Old bugs are in Debian atm!

Rolling upgrades



- We subscribe to debian/testing
no huge (problematic) version jumps
needed
- Is the last machine selected Debian stage
- Naming is not enterprise compatible
- We always aim for the latest LTS kernel

Where do we come from

- We are from SAP
- We are competition for established Vendors
- We are a large Enterprise with not so special needs
- We need Extensibility, flexible
- We need real open source
- Certification
- Security

To Enterprise or not to Enterprise?

What is an Enterprise Linux?

- License verification
 - Security hardening
 - Security tracker
 - Immutability
 - Support
-
- That is what we provide to intern and share with extern
 - Support we buy at a high quality provider: credativ.de

Why open? Why here?

Debian and the clean licensing

Security process

Patch maturity and acceptance -> Process

Debian is more Enterprise then obvious

But nobody speaks for it

No vendor interests

Missing the small edition

Kernel on steroids

The Enterprise and the Community

Community OSes are great! Companies should not be the sole owner of a distribution.

Companies tend to have distinct use cases, limitations, and requirements (compliance!)

Open Source / Free Software companies provide glue

- Thanks to SAP for encouraging us to contribute back to Debian!

On the relevance of Debian packages in the cloud

Supply Chain Security – trust as few vendors/sources as possible

License compliance

Reproducible builds

Thanks to

Debian

Snapshot Debian

Debuerreotype

All the external and internal acceptance (more then 10K intallation we know of, without call home)

Credativ

Thank you.

Contact information:

andre.russ@sap.com

dirk.marwinski@sap.com

dominik.george@credativ.de

michael.banck@credativ.de

gardenlinux.io

