Robert Sander <r.sander@heinlein-support.de>

Singularity

Eine einfache Containerengine

- **Heinlein Support**
  - IT-Consulting und 24/7 Linux-Support mit ~40 Mitarbeitern
  - Eigener Betrieb eines ISPs seit 1992
  - Täglich tiefe Einblicke in die Herzen der IT aller Unternehmensgrößen

- 24/7-Notfall-Hotline: 030 / 40 50 5 – 110
  - 28 Spezialisten mit LPIC-2 und LPIC-3
  - Für alles rund um Linux & Server & DMZ
  - Akutes: Downtimes, Performanceprobleme, Hackereinbrüche, Datenverlust
  - Strategisches: Revision, Planung, Beratung, Konfigurationshilfe

Singularity?

- Build-Umgebung
- Runtime

- für Container

- Container-Image ist ausführbare Datei
- integriert sich gut in Cluster Resource Manager

- "transportable chroot-Umgebung"
- vermeidet Software-Installationen auf Compute-Cluster

Container?

- Linux-Kernel bietet mehrere Namespaces
  - Dateisystem
  - Prozesse (PIDs & IPC)
  - Netzwerk
  - User
- Linux-Kernel bietet Control Groups
  - Nutzungseinschränkung für eine Gruppe von Prozessen
- Jeder Prozess sieht nur den Inhalt des eigenen Namespace
  - /proc/<pid>/ns

Container!

- eth0 != eth0 in Network Namespaces
- / != / in Mount Namespaces
- PID 1 != PID 1 in Process Namespaces

- aktuell gibt es 8 Namespaces (IPC, Time, UID, UTS, CGroup)

- Control Groups steuern Resourcenverwendung (CPU, RAM, IOPS)

- Isolierung von Anwendungs-Prozessen auf dem selben Kernel
  - oft mit eigenem Filesystem (Image) für einfache Portierung

Linux-Container

- Docker
- Podman
- LXC / LXD
- OpenVZ
- Singularity
- systemd-nspawn

Singularity – Entstehung

- 2015 veröffentlicht am Lawrence Berkeley National Laboratory (LBNL)
- BSD Lizenz
- 2017 "Best HPC Programming Tool or Technology"
- schnelle Verbreitung an Forschungsinstituten und Universitäten

- Der Name kommt aus der Astrophysik
- Er meint nicht den Zeitpunkt, zu dem künstliche Intelligenz die Herrschaft übernimmt

Besonderheiten

- Software-Installation & Ausführung von Programmen reproduzierbar
  - Prüfsumme oder Signatur auf Containerdatei
- Einfach transportierbar

- Anderes Sicherheitskonzept als Docker
  - kein "trusted user" im "trusted container"
  - kein root oder Daemon notwendig zum Starten eines Containers
  - Benutzer-Account "auβen" ist Benutzer-Account "innen"
  - einfacher Datenaustausch über Host-Dateisystem ($PWD, /home & /tmp sowie weitere bind-mounts)

- Container laufen wie jede andere Applikation
  - Container-Image ist das Executable

Funktionen

- Baut Container-Images als Single Image Files
- Führt Container aus
  - Setup der Namespaces
- Kann Host-Hardware direkt verwenden (GPUs)
- Kann Host-Netzwerk direkt verwenden (InfiniBand)
- MPI-Unterstützung
  - verteiltes Rechnen im Cluster

Integrationen

- Viele HPC-Systeme
- HTCondor
- Univa Grid Engine
- SLURM
- TORQUE

- Docker Hub als Quelle von Container-Base-Images
- Eigene Singularity-Container-Library

Sicherheit

- Container-Filesystem mit `nosuid` gemountet
- Container-Prozesse läuft mit `PR_NO_NEW_PRIVS`, d.h. kein sudo o.ä. im Container
- Verschlüsselung und Signierung der Container-Images (.sif) möglich
- SIF-Container werden ohne Auspacken gestartet, sind unveränderbar

- Nutzt zum Starten des Containers einen kleinen suid-Helfer
  - nicht notwendig auf modernen Linux-Systemen mit unprivileged user namespace support.

- https://sylabs.io/guides/3.7/admin-guide/security.html

Image-Bau

- Aus einem Docker-Image
  - `sudo singularity build lolcow.sif docker://godlovedc/lolcow`
- Über eine Sandbox
  - ```
    sudo singularity build --sandbox lolcow/ docker://godlovedc/lolcow
    sudo singularity shell --writable lolcow/
    sudo singularity build lolcow.sif lolcow/
    ```
- Mit Hilfe von Definitionsdateien
  - ```
    $EDITOR container.def
    sudo singularity build contaner.sif container.def
    ```

Container-Definitionsdatei .def

```
Bootstrap: docker
From: debian:10

%environment
    export LC_ALL=C
    export PATH=/usr/games:$PATH

%post
    apt-get -y update
    apt-get -y install fortune cowsay lolcat

%runscript
    fortune | cowsay | lolcat
```

Container ausführen

- `./container.sif`
- `singularity run ./container.sif`
- `singularity shell ./container.sif`
- `singularity exec ./container.sif`

- `/path/to/r40.sif /home/r.sander/example.r`

Container-Instanzen für Dienste

- ```
  Bootstrap: docker
  From: nginx
  Includecmd: no

  %startscript
     nginx
  ```
- `sudo singularity build nginx.sif nginx.def`
- `sudo singularity instance start --writable-tmpfs nginx.sif web`
- `curl http://localhost`
  ```

Demo

- Natürlich und gerne stehe ich Ihnen jederzeit mit Rat und Tat zur Verfügung und freue mich auf neue Kontakte.
  - Robert Sander
  - Mail: r.sander@heinlein-support.de
  - Telefon: 030/40 50 51 – 43
- Wenn's brennt:
  - Heinlein Support 24/7 Notfall-Hotline: 030/40 505 - 110

Soweit, so gut.

Gleich sind Sie am Zug:
Fragen und Diskussionen!

Wir suchen:
Admins, Consultants, Trainer!

Wir bieten:
Spannende Projekte, Kundenlob, eigenständige Arbeit, ein tolles Team, Work-Life-Balance

...und natürlich: Linux, Linux, Linux...

http://www.heinlein-support.de/jobs

Heinlein Support hilft bei allen Fragen rund um Linux-Server

HEINLEIN AKADEMIE

Von Profis für Profis: Wir vermitteln die oberen 10% Wissen: geballtes Wissen und umfangreiche Praxiserfahrung.

HEINLEIN HOSTING

Individuelles Business-Hosting mit perfekter Maintenance durch unsere Profis. Sicherheit und Verfügbarkeit stehen an erster Stelle.

HEINLEIN CONSULTING

Das Backup für Ihre Linux-Administration: LPIC-2-Profis lösen im CompetenceCall Notfälle, auch in SLAs mit 24/7-Verfügbarkeit.