Podman containers with systemd and Ansible

openSUSE Conference 2023

May 26, 2023

Johannes Kastl
Linux Trainer & Consultant
B1 Systems GmbH
kastl@b1-systems.de

Agenda

- Introduction
- Podman
- Podman and systemd
- Ansible
- Quadlet
- Live-Demo

About me

- Johannes Kastl
- he/him
- Linux Trainer and Consultant at B1 Systems
- OBS: `ojkastl_buildservice`
- Mastodon: `@johanneskastl@digitalcourage.social`
- GitHub/GitLab/Codeberg/...: `johanneskastl`

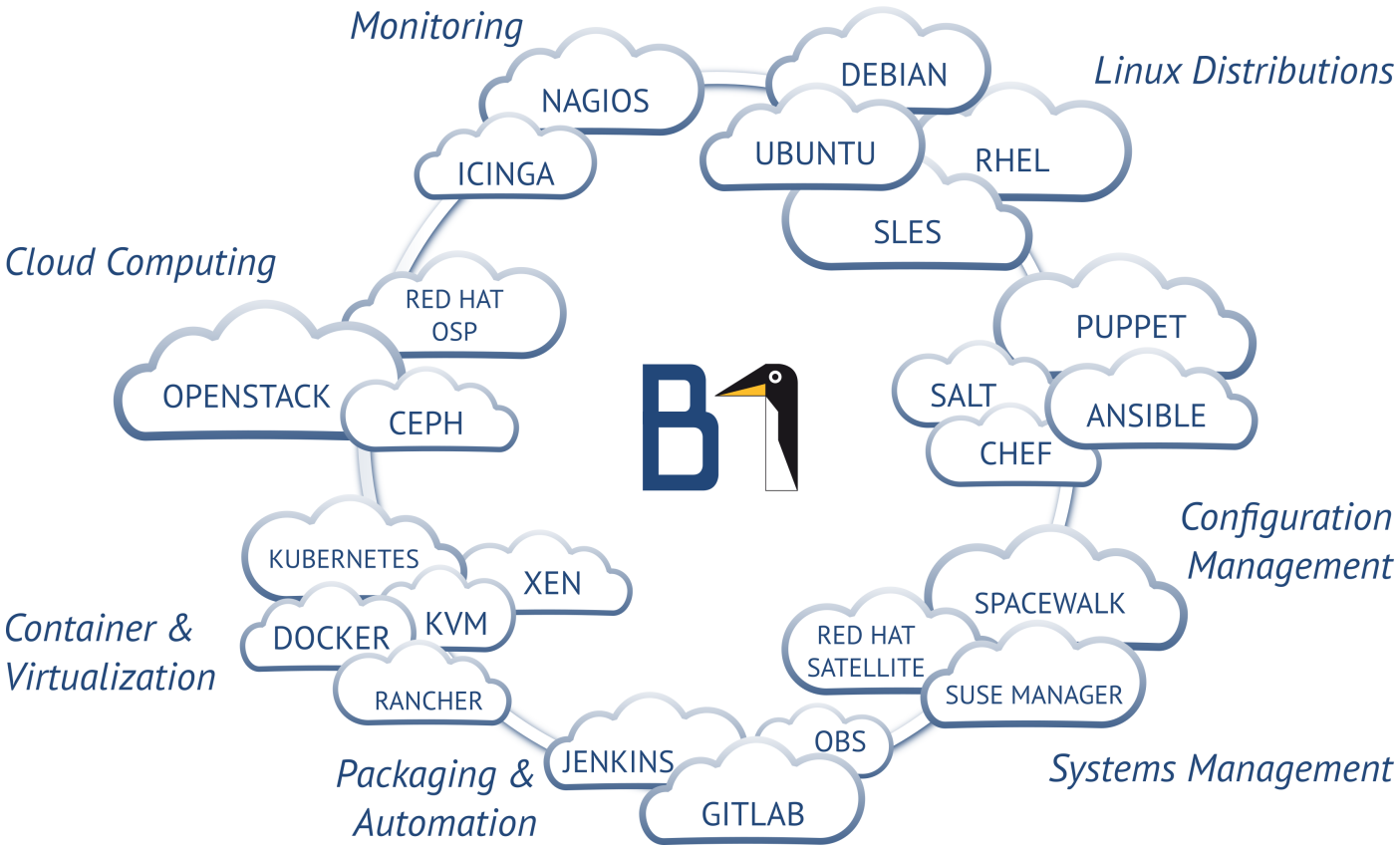
What I do

- trainer, consultant, systems administrator, architect, spielkind
- configuration management (Ansible, Puppet, Chef, SaltStack)
- Infrastructure as Code (Terraform, . . .)
- Kubernetes and Containers (Podman, Docker, LXC, . . .)
- CI/CD (Jenkins, GitLab CI, GitHub Actions)
- agile and lean (Scrum, Kanban)
- maintainer for Ansible and some cloud-native tools

Introducing B1 Systems

- founded in 2004
- operating both nationally & internationally
- more than 140 employees
- vendor-independent (hardware & software)
- focus:
  - consulting
  - support
  - training
  - managed service & operations
  - solutions & development
- branch offices in Rockolding, Berlin, Cologne, Dresden & Jena

Areas of Expertise



Podman

- container engine
- runs OCI containers based on OCI container images ("docker images")
- rootless and rootful containers
- replacement for Docker
- does not need a service

podman

Podman and systemd

- systemd is a system and service manager
  used by many Linux distributions
- systemd manages service startup
- systemd uses unit files (e.g. `*.service`)
- Podman can generate systemd unit files
  - allows running containers as systemd units
  - allows managing containers like systemd units
  - both system or user scope

Ansible

- configuration management system (like Puppet, Chef, SaltStack)
- no central server (unlike Puppet, Chef, SaltStack)
- no agent required
  - SSH access needed to the target
  - Python3 needed on the target
- small core with lots of collections and roles
  - PostgreSQL, Podman, Grafana, NetBox, ...
  - AWS, Azure, GCP, OpenStack, ...
  - Arista, Cisco, Juniper, F5, ...

Quadlet

- Quadlet is part of Podman 4.4 and higher
- stores configuration files in `/etc/containers/systemd/`
  - `*.container`
  - `*.kube`
  - `*.network`
  - `*.volume`
- Podman generates systemd unit files “on the fly”
- redhat.com/sysadmin/multi-container-application-podman-quadlet
- github.com/ygalblum/quadlet-demo

Live-Demo

github.com/johanneskastl/
osc23_Podman_Containers_with_Ansible_Nginx

github.com/johanneskastl/ansible-role-podman_nginx

Live-Demo

```
Vagrant.configure("2") do |config|
  config.vm.define "podman-nginx" do |node|
    node.vm.box = "opensuse/Leap-15.4.x86_64"
    node.vm.provider "libvirt" do |lv|
      lv.random_hostname = false
      lv.memory = 2048
      lv.cpus = 2
    end
    node.vm.hostname = "podman-nginx"
    node.vm.provision "ansible" do |ansible|
      ansible.playbook = "ansible/playbook-all_nodes.yml"
    end
  end
end
```

Live-Demo

```
- name: 'Run a simple rootful nginx container'
  hosts: 'all'
  gather_facts: true
  become: true

  roles:
    - role: 'johanneskastl.podman_nginx'
      podman_nginx_rootful_container: true
```

Live-Demo

```
- name: 'Run a simple (unprivileged) nginx container'
  hosts: 'all'
  gather_facts: true
  become: false

  roles:
    - role: 'johanneskastl.podman_nginx'
      podman_nginx_data_directory: '/[...]/nginx_Podman'
      podman_nginx_default_user: 'vagrant'
      podman_nginx_default_group: 'vagrant'
      podman_nginx_rootful_container: false
```

Thank you for your attention!
Questions?

For more information, refer to info@b1-systems.de
or +49 (0)8457 - 931096

Thank You!