BelWü

Landeshochschulnetz Baden-Württemberg

Ansible bei BelWü

Matthias Schlecht / Tübix 04.07.2026

BelWü

- Landeshochschulnetzwerk
- Internet sei 1987
- Unix seit ~1990, Linux seit ~2010
- Netzknoten in allen Hochschulen und Unis in BW.
- ~20 Mitarbeiter



Facts Server

- Momentan knapp 80 Bleche von Dell
- Davon ~50 mit 64C/128C 1/2TB RAM
- Davon ~25 mit Debian 13.
- Momentan ca 130 VMs mit Debian 13
- Während der Hochzeit (2020 - 2024) liefen auf dem Cent-OS Setup ca 400 Vms auf 88 Blechen.

Facts Speicher und SAN

- Server haben nur 2 SSDs im RAID1
- Alle Daten liegen auf einem HA-SAN-System
- Momentan ca ~100 TiB Nutzkapazität

Virtualisierungs-Stack

```
libvirt_packages:
    - qemu-system
    - libvirt-daemon-system
    - libvirt-clients
    - virtinst
    - virt-manager
    - qemu-utils
```

→ Alles default, keine Config-Anpassungen

(Netzwerk)-Stack, BGP, SAN

- SAN: zwei NICs in einer LAG, darüber eine Bridge.
- Netz:
  - Zwei seperate „Linknetze“ in /31 und /127
  - Ein loopback-Interface mit einer v4 und v6 Adresse
  - Mittels BGP werden 4 Sessions zu zwei DC-Routern aufgebaut
  - libvirt-Hook für beim Start und Stop einer VM der das richtige vnet-Interface zum loopback routet und IP-Spoofing erlaubt.
  - NAT für die Installation der VMs mit debian-Preseeds.
  - systemd-networkd :-)

Dienste bei BelWü bis ~2019

- Wir haben da $viele Solaris Büchsen
- Die hat eventuell mehrere Zonen
- Da läuft ein (Perl-)Skript und tut Dinge
- Da laufen tausende Webserver drauf

  ⟶ Oh hubsi kaputt…

  ⟶ Quasi keine zentrales Konfigmanagement

  ⟶ Keine Versionierung



Zeile des jetzigen Linux Setups

- Hosts sollten schnell ausgerollt werden
- Änderungen in Konfigs sollen nachverfolgbar sein
- „Pfusch“ soll automagisch korrigiert werden
- Händisches Frickeln muss beendet werden.
- Grundkonfiguration ist überall gleich, Änderungen daran sollen einfach sein.
- Dienste sollen dokumentiert sein.

Ansible?

- Ansible kann mittels Playbooks Tasks auf Hosts ausführen
- Push oder Pull-Konzept unterstützt. ⟶ BelWü pullt.
- Konfigurationsänderungen an Hosts werden nicht händisch gemacht.
- Es können schnell viele Hosts eines Typs ausgerollt werden
- Es gibt für quasi alle Tasks Module.

Voraussetzungen

- Wir installieren im preseed:
  - git
  - ansible
- Alle Playbooks liegen in unserem github
- Die Erstinstallation eines Hosts erfolgt mittels ansible-playbook
- Es gibt einen deploy-ssh-key der mit dem git spricht

Begriffe

- Host: Ein Blech oder eine VM
- Group: Eine Gruppe an Hosts
- Playbook: Definition an Roles die auf Hosts/Groups laufen
- Inventory: Datei mit allen Hosts und Gruppen
- Role: eine Sammlung an Tasks, Dateien, Templates
- Template: Ein jinja2-Template aus dem Konfig gebaut wird
- Tag: ein Schlagwort um nur bestimmte Tasks zu aktivieren

Demo ansible-playbook

Was macht BelWü mit Ansible

- Netzwerk-Konfiguration
- Firewall
- Pakete installieren
- Pakete konfigurieren
- Komplette Dienste (z.B. DNS-Resolver) ausrollen

Ansible-Pull

- Jeden Morgen um 5:00 +0-3600 s Delay läuft ein ansible-pull
- Damit sind alle Hosts immer auf dem aktuellen Stand
- Wenn das Ansible-Pull umfällt gibt es einen Alarm

https://sysmon02.belwue.de/grafana/d/edulhk409zuv4d/ansible-pull

Demo ansible-pull

Variablen

- Ansible hat 22* verschiedene Wege Variablen zu definieren
- Variablen werden überschrieben und nicht gemerged
- Vereinfacht:

  Defaults → Group → Host → Playbook → Role

* https://docs.ansible.com/projects/ansible/latest/playbook_guide/playbooks_variables.html#understanding-variable-precedence

Templates

- Jinja2 – Templates sind sehr mächtig
- Iterationen über Host-Vars und in den Tasks gegebene Variablen.
- Verzweigungen aller Art sind zur Laufzeit möglich
- Perfekt um Konfigs zu erstellen.

Demo Variablen und Templates

Takeaways

- Disziplin beim bauen der Playbooks
- Es führen viele Wege nach Rom…
- Es gibt viele Kleinigkeiten in yaml und jinja2 die tun
- Updates von Betriebssystemen werden erstaunlich stressfrei
- Schnelles Ausrollen von VMs im Havariefall machbar
- Aber: Ansible ersetzt keine Backups!

Grenzen

- Installation von Software die nicht aus Paketen kommt
- Konfigurationsskripte
- Übermäßige Verschachtelung oder gar mergen von Variablen
- Daten einspielen

show & tell


Questions?
schlecht@belwue.de