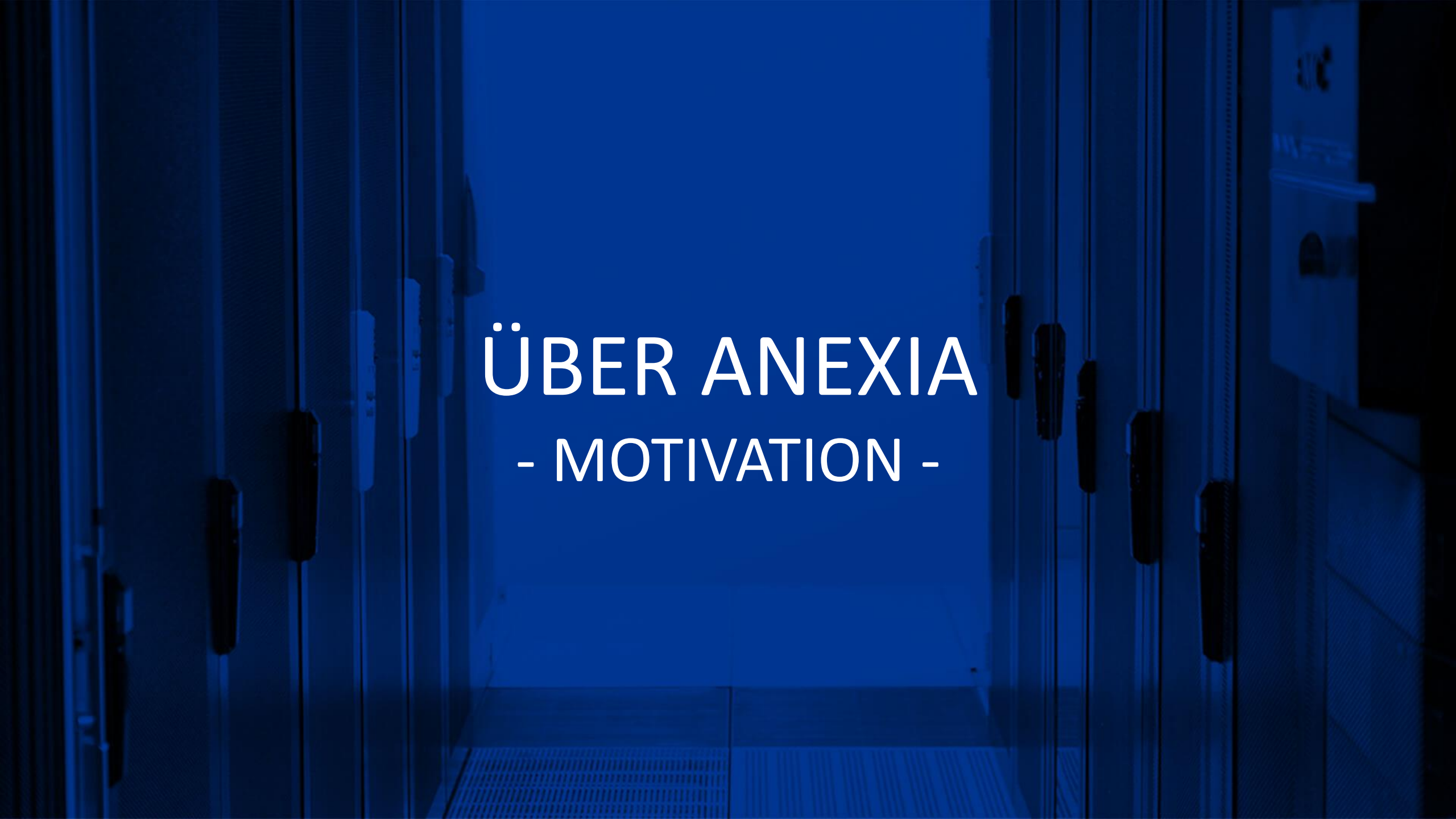
Mehrere 100 Systeme mit Ansible verwalten

Stefan Jakobs

anexia

WORUM ES GEHT

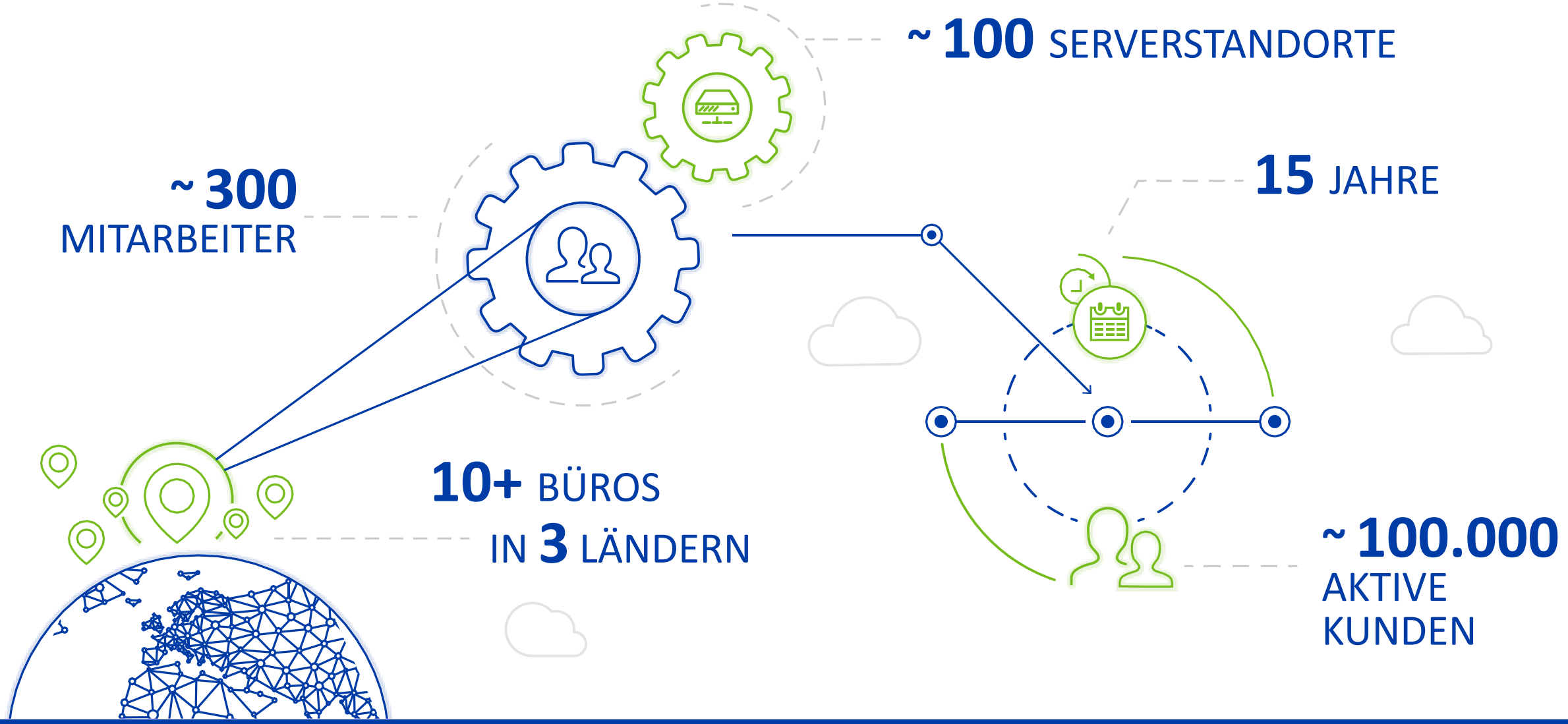
- Über Anexia - Motivation
- Infrastruktur
- Bootstraping
- Inventories & Roles
- Entwicklung und Test
- Ausblick



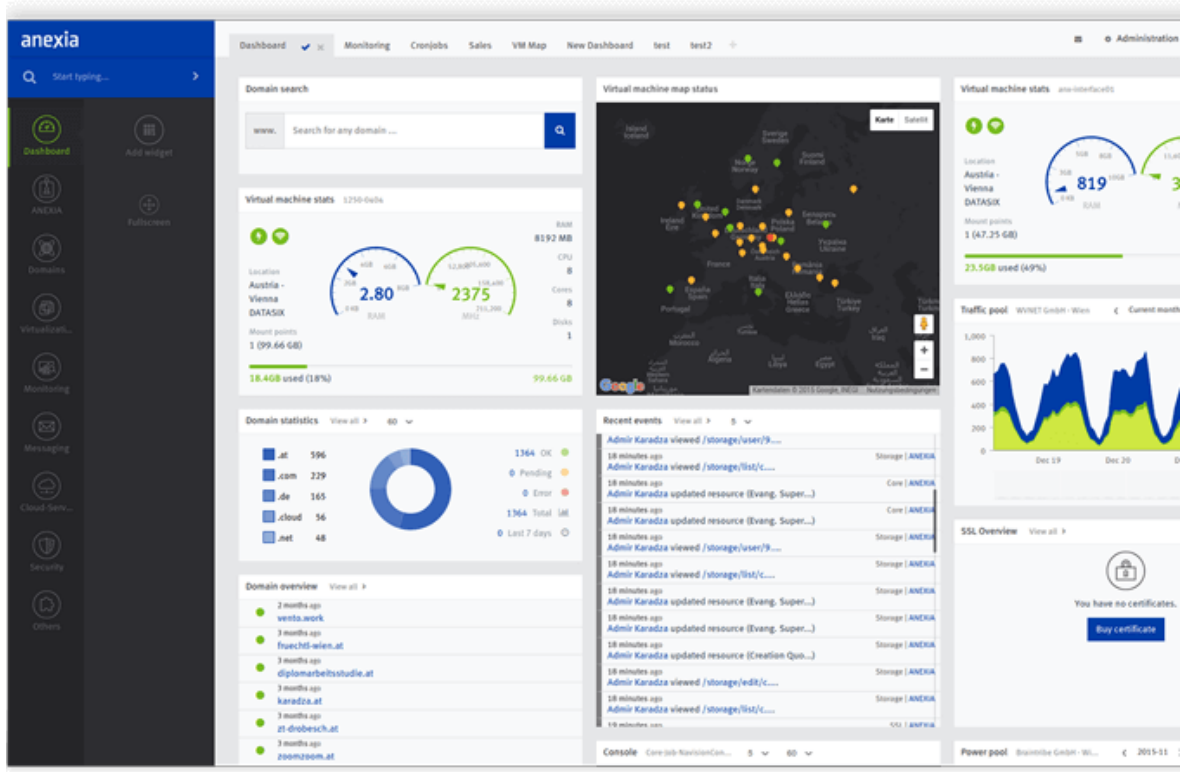
ÜBER ANEXIA

- MOTIVATION -

EIN PAAR FACTS



ANEXIA ENGINE



- Kundenportal
- Verwaltung (Compute/Network/Storage/…)
- CMDB

WARUM EIN WEITERES TOOL?

- Engine
  - Sehr hohe Abstraktion
  - Aufwendige Implementierung
- Entwickler-Ressourcen sind begrenzt
- „Automatisierung für Jedermann“
- Standardisierung ermöglichen
- Day 2 Operations

WARUM ANSIBLE?

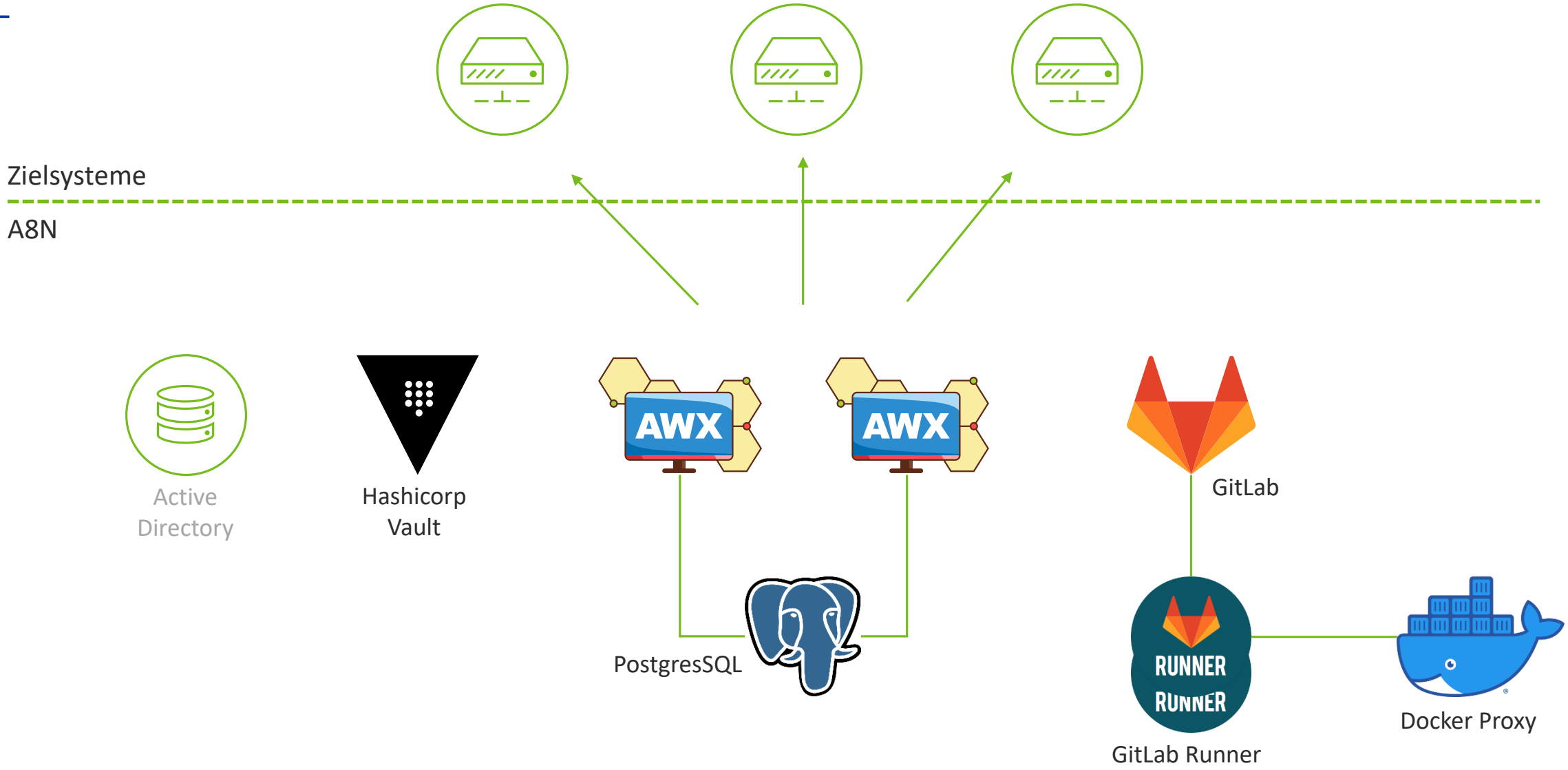
- Einfacher Einstieg
- Einfach zu lesen (YAML)
- OpenSource
- Weit verbreitet
- Unterstützt viele Systeme
  (Linux, Windows, VMware, Netconf)
- Agent-less

WARUM ALS PLATTFORM?

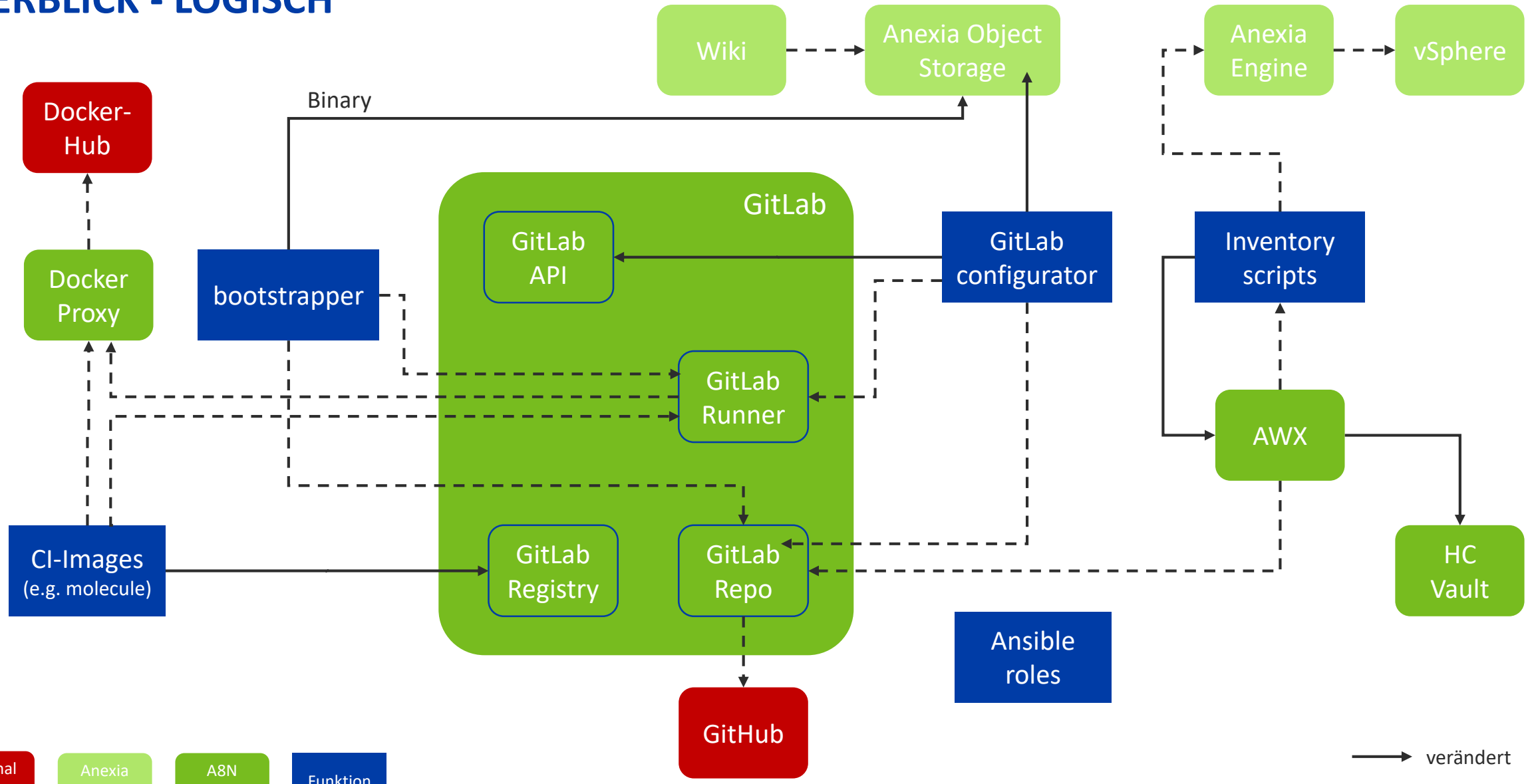
- Für andere Teams
- Leichter Einstieg
- Wiederverwendbarkeit

INFRASTRUKTUR

ÜBERBLICK


Zielsysteme
A8N
Active Directory
Hashicorp Vault
AWX
AWX
PostgresSQL
GitLab
RUNNER
GitLab Runner
Docker Proxy

ÜBERBLICK - LOGISCH



BOOTSTRAPPER

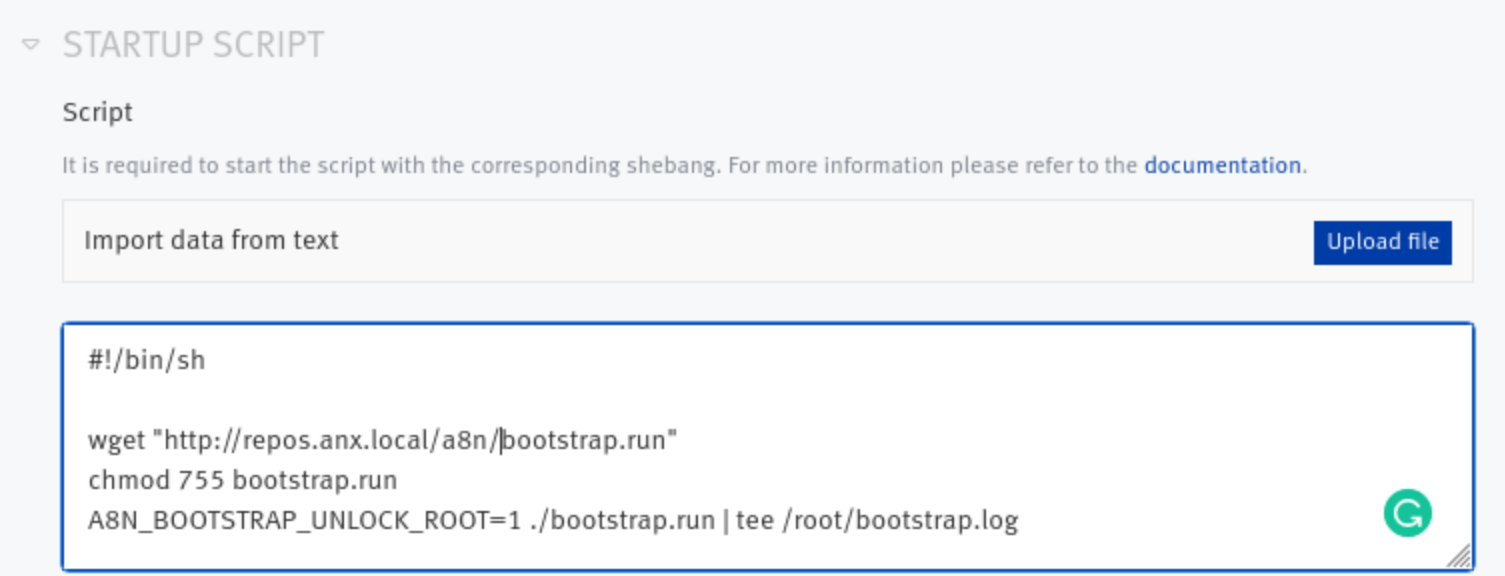
PROBLEMBESCHREIBUNG

- Wie kann der initiale Zugriff erfolgen?
  - Public Key muss auf dem Zielsystem hinterlegt sein
  - Ansible/AWX muss Private Key kennen
- Wie kann der SSHd geschützt werden?
  - Eigener SSH daemon
  - Eigener Port

BOOTSTRAPPER

- Ansible-portable in einem Self-executable Shellscript
- Installiert:
  - zusätzlichen ssh daemon auf zusätzlichem Port
  - ssh authorized keys
- Dieselbe Logik (Rolle) verwaltet später diesen Dienst

```
/usr/local/a8n/a8n.roles.sshd/a8nsshd/
├── bin
│   └── a8nsshd -> /usr/sbin/sshd
└── etc
    ├── authorized_keys
    ├── sshd_config
    ├── ssh_host_ecdsa_key
    ├── ssh_host_ecdsa_key.pub
    ├── ssh_host_ed25519_key
    ├── ssh_host_ed25519_key.pub
    ├── ssh_host_rsa_key
    └── ssh_host_rsa_key.pub
```



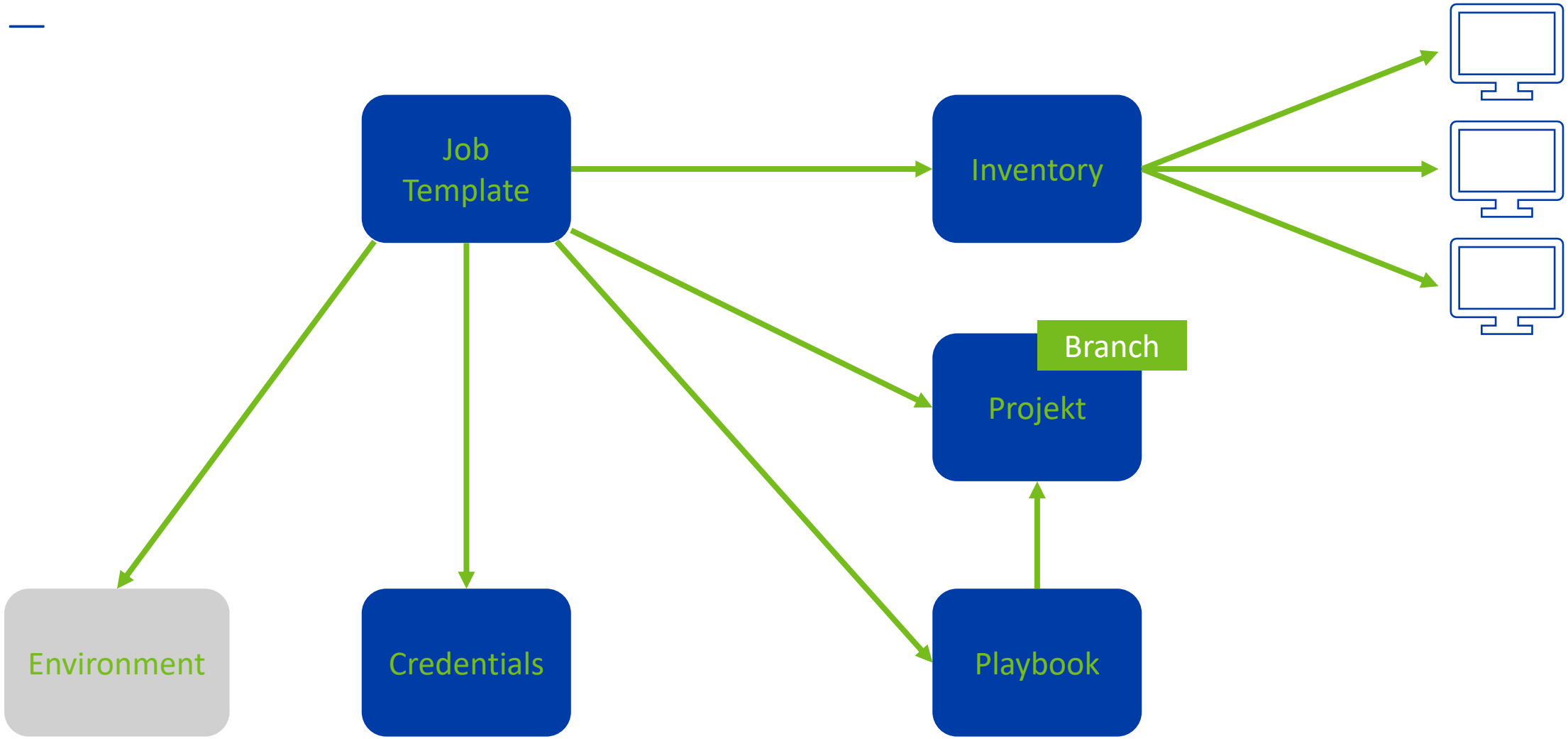
CI-PIPELINE

- Änderungen werden automatisch getestet
- Tests erfolgen für verschiede Distributionen: Debian, Ubuntu, CentOS
- Deployment neuer Version via AWX.

```
image: $CI_REGISTRY/a8n/tools/molecular:2-9
stages:
 - test
 - deploy

molecular:
 stage: test
 script:
   - molecular test
 tags:
   - dind

deploy:
 image: $CI_REGISTRY/a8n/ci-images/tower-cli:master
 stage: deploy
 variables:
   A8N_TEMPLATE_ID: 12
 script:
   - a8n-launch-job
 only:
   - master
```

INVENTORIES & ROLES

JOB TEMPLATES



INVENTORIES

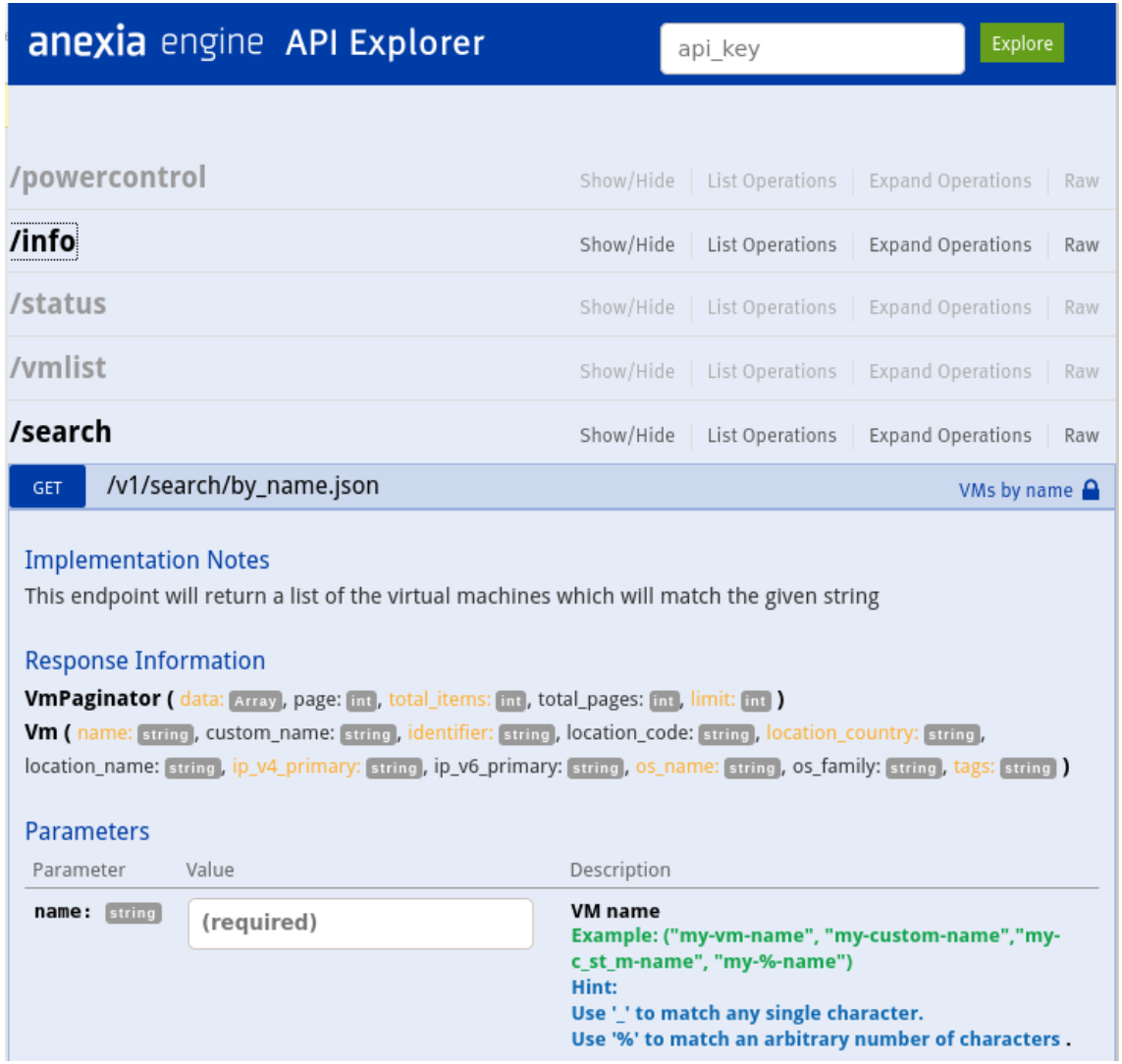
- AWX Unterstützt verschiedene Inventories:
  - Statisch, z.B. aus dem Projekt
  - Dynamisch, z.B. durch Script Aufruf

INVENTORIES

- Problem:
  - (Host-)Variablen und Facts sind ans Inventory gebunden
- Folge:
  - Ein Host ist einem Inventory zugeordnet
  - Hosts sollten nur einmal existieren

INVENTORIES

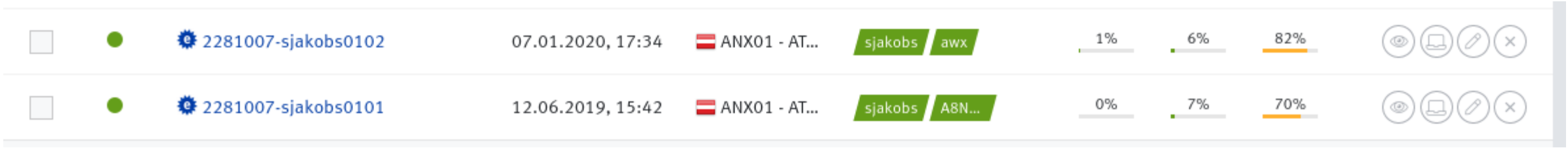
- Anexia Engine bietet eine API für VMs
- Ermöglicht dynamische Inventories (ähnlich vSphere Inventory Plugin)



INVENTORIES

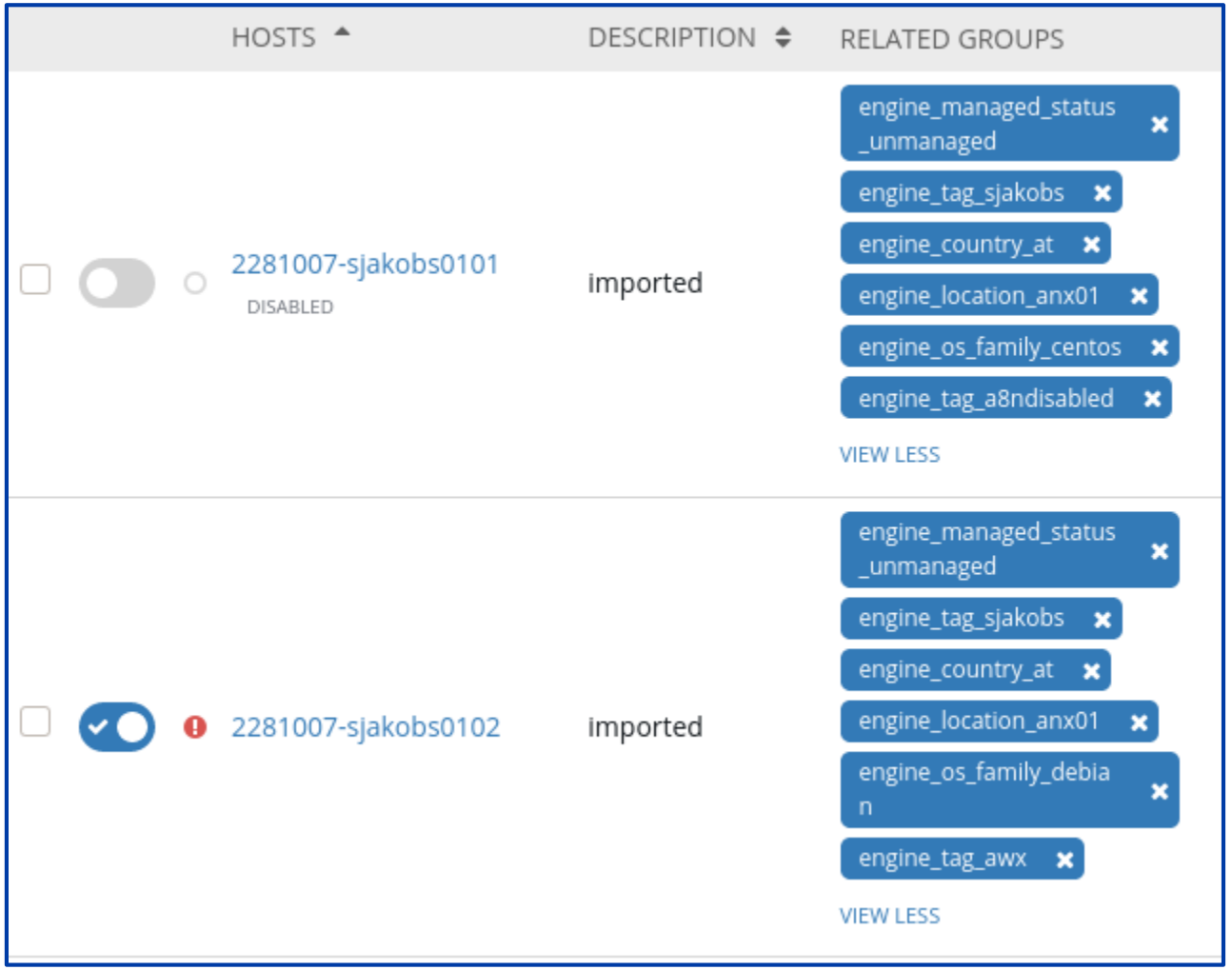
- Engine API erlaubt die Verknüpfung mit zusätzlichen Attributen:
  - OS family
  - Location
  - Customer
  - Tags
  - …

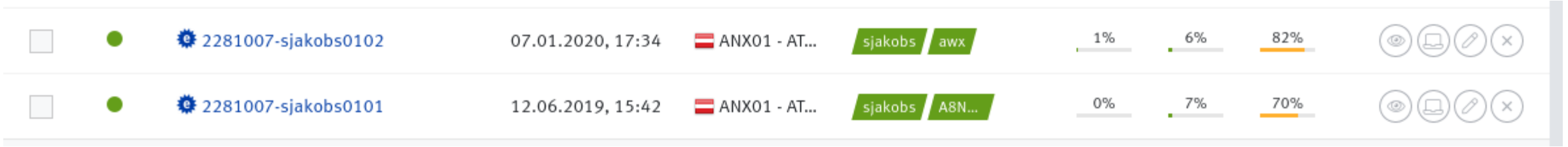
```yaml
ansible_connection: ssh
ansible_host: 10.0.60.160
ansible_port: 8022
enabled: true
engine_customer_name: ANEXIA INTERN
engine_customer_number: '2281007'
engine_id: af53768ad96a4ff
engine_location_code: ANX01
engine_location_country: AT
engine_location_name: 'ANX01 - AT, Klagenfurt, STW'
engine_managed_status: unmanaged
engine_name: 2281007-sjakobs0102
engine_os_family: Debian
engine_os_name: Debian GNU/Linux 10 (64-bit)
engine_tags:
  - sjakobs
  - awx
tags:
  - 2281007-sjakobs0102
  - sjakobs
  - awx
```



INVENTORIES

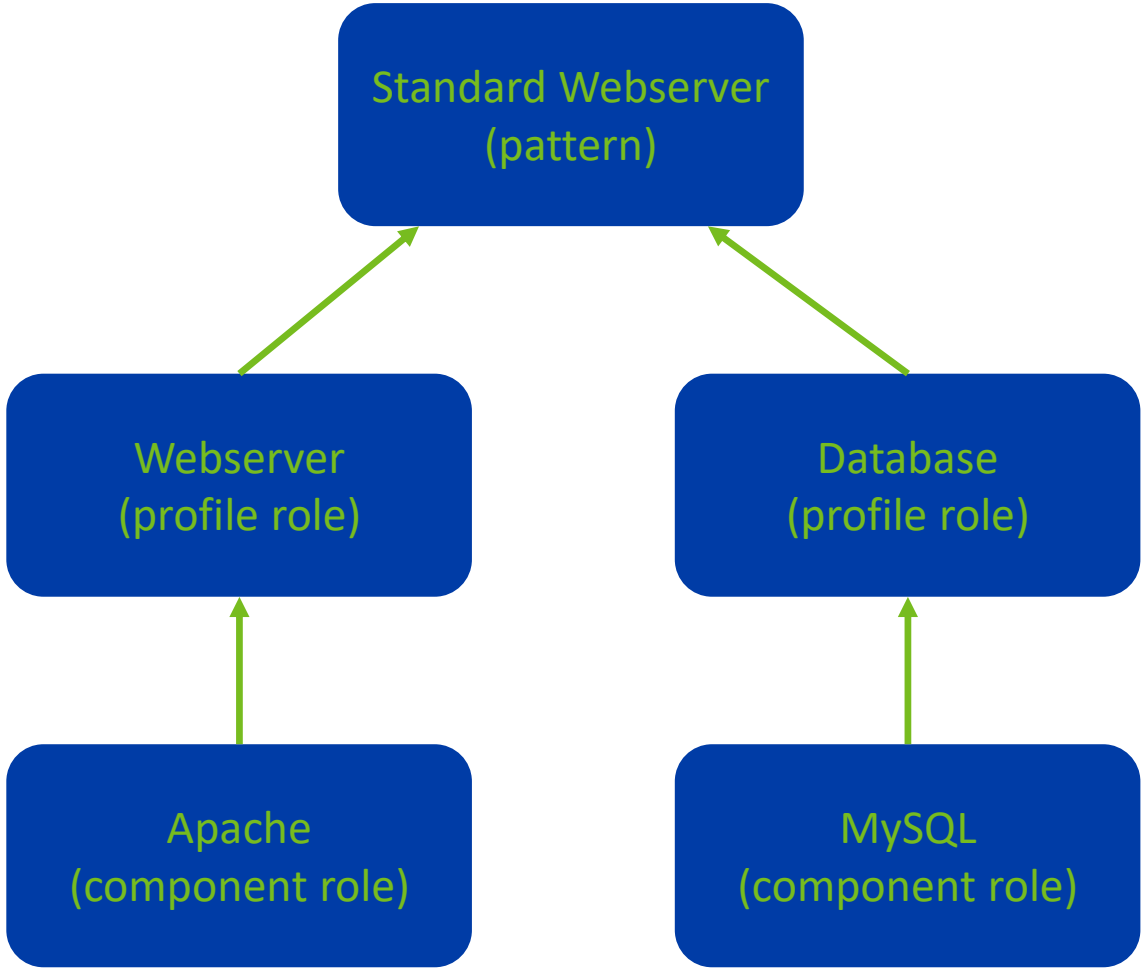
- Engine API erlaubt die Verknüpfung mit zusätzlichen Attributen:
  - OS family
  - Location
  - Customer
  - Tags
  - …





ROLES

- Ziel: Wiederverwendung
- Gestaffelte Hierarchie
  - Components
  - Profiles
  - Patterns



ENTWICKLUNG & TEST

ENTWICKLUNG

Zur Erinnerung: Wir möchten anderen Teams die Benutzung unserer Plattform möglichst einfach machen.

- **Einfache** Entwicklung einer Rolle
- **ABER** die Rolle muss
  - bestimmte Variablen enthalten
  - ein standardisiertes README mitliefern
  - bestimmte Distros unterstützen
  - Tests unterstützen

=> **Molecular / molecule init**

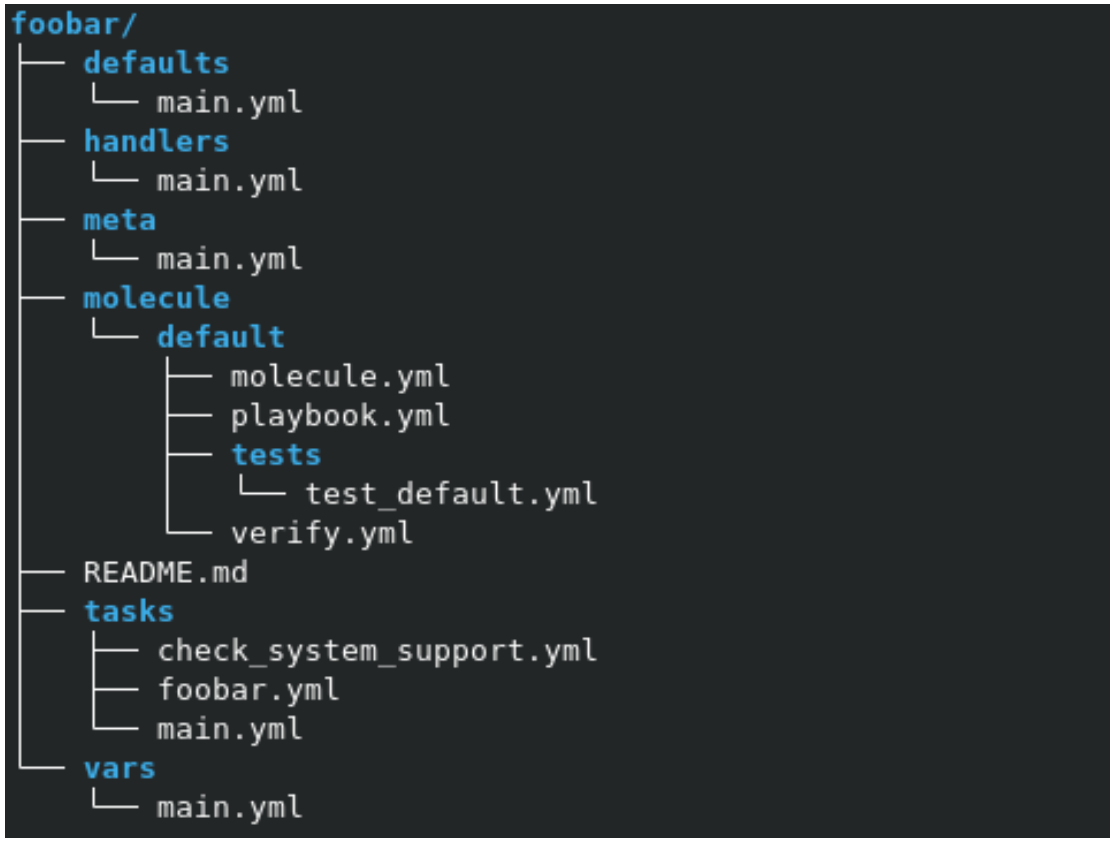
```
molecular init -r foobar -d vagrant
> Python version: 3.9.1
> Ansible version: 2.9.16
>   default strategy: linear
> molecule version: 2.22
> molecular version: 2.9.3
> VirtualBox version: 6.1.18_RPMFusionr142142
> executing 1 step: init
> [01/01] starting step "init"
>> template url: python3.9/site-packages/molecular/data/cookiecutter
>> Initializing new role foobar...
>> Initialized role in /tmp/foobar successfully.
>> [01/01] finished step "init"
```

ENTWICKLUNG

Zur Erinnerung: Wir möchten anderen Teams die Benutzung unserer Plattform möglichst einfach machen.

- **Einfache** Entwicklung einer Rolle
- **ABER** die Rolle muss
  - bestimmte Variablen enthalten
  - ein standardisiertes README mitliefern
  - bestimmte Distros unterstützen
  - Tests unterstützen

=> **Molecular / molecule init**



tree foobar

ENTWICKLUNG

Zur Erinnerung: Wir möchten anderen Teams die Benutzung unserer Plattform möglichst einfach machen.

- **Einfache** Entwicklung einer Rolle
- **ABER** die Rolle muss
  - bestimmte Variablen enthalten
  - ein standardisiertes README mitliefern
  - bestimmte Distros unterstützen
  - Tests unterstützen

=> **Molecular / molecule init**

```
# so.components.foobar

A brief description of the role goes here.

## Installation

roles/requirements.yml

    - name: so.components.foobar
      version: master

## Example Playbook

    - hosts: servers
      roles:
        - role: so.components.foobar
          foobar__enable: true

## Role Variables

| Parameter | Choices/Defaults | Comments |
| --------- | ---------------- | -------- |
| foobar__enable | true/**false** | Set to true to enable this role |
```

README.md (gekürzt)

ENTWICKLUNG

Zur Erinnerung: Wir möchten anderen Teams die Benutzung unserer Plattform möglichst einfach machen.

- **Einfache** Entwicklung einer Rolle
- **ABER** die Rolle muss
  - bestimmte Variablen enthalten
  - ein standardisiertes README mitliefern
  - bestimmte Distros unterstützen
  - Tests unterstützen

=> **Molecular / molecule init**

```
---
dependency:
  name: galaxy
driver:
  name: vagrant
  provider:
    name: virtualbox
lint:
  name: yamllint
platforms:
  - box: centos/7
    cpus: 1
    memory: 256
    name: linux-centos-7
  - box: centos/8
    cpus: 1
    memory: 256
    name: linux-centos-8
  - box: debian/stretch64
    cpus: 1
    memory: 256
    name: linux-debian-9
```

molecule.yml

CI-TESTS

- GitLab Runner mit Docker-in-Docker
- Molecular/molecule:

```
molecular:
 stage: test
 image: $CI_REGISTRY/a8n/tools/molecular:2-9
 script:
  - molecular test
 tags:
  - dind
```

- Driver:
  - Docker
  - Vagrant (VirtualBox, Libvirt)

- Verifier:
  - goss

```
port:
 tcp:22:
  listening: true
  ip:
   - 0.0.0.0
 tcp6:22:
  listening: true
  ip:
   - '::'
user:
 sshd:
  exists: true

...
```

ÜBERBLICK BEHALTEN

- Welche Rollen gibt es?
- Wo sind diese Rollen zu finden?
- Welche Abhängigkeiten gibt es?
  - Zu Rollen
  - Zu Playbooks

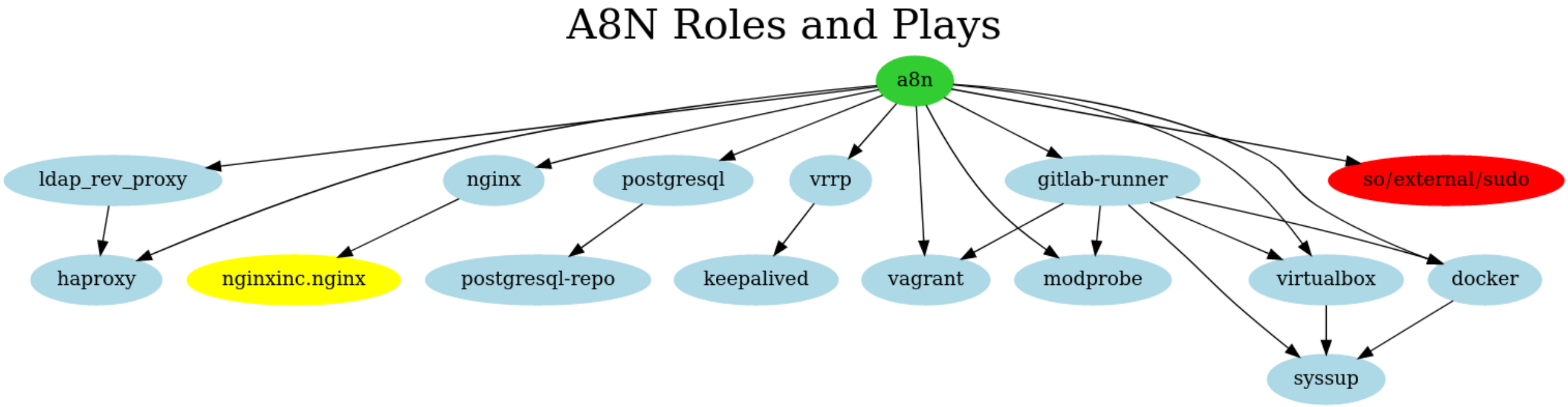
⇒ GitLab API hilft hier!

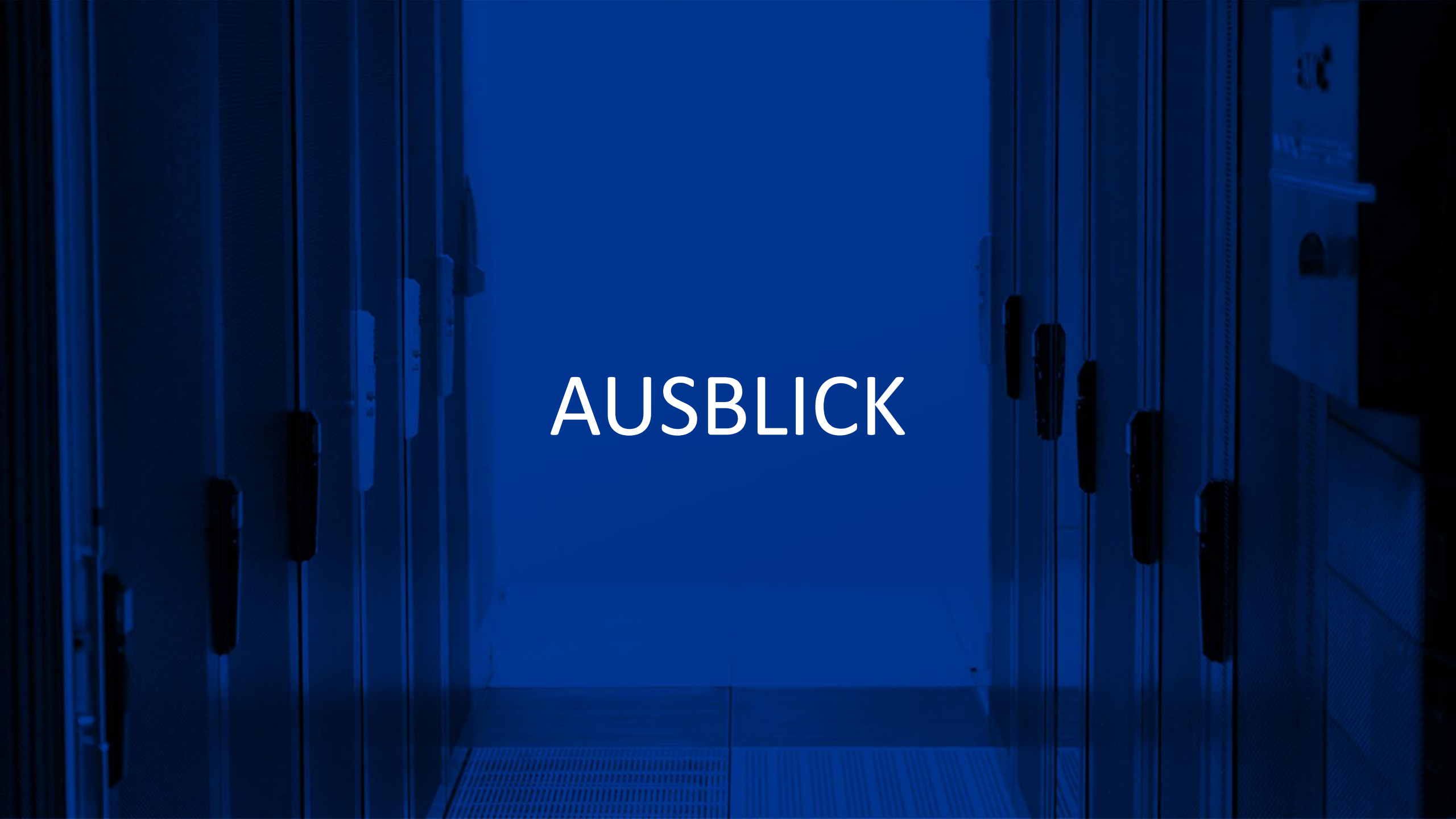
```
gl = gitlab.Gitlab(GITLAB_URL, private_token)
projects = gl.projects.list(all=True)
real_project = gl.projects.get(p.id)

for p in projects:
 content = get_yaml_content(real_project, 'meta', 'main.yml')
 if content:
  # This is a role
  # ....
 else:
  content = get_yaml_content(real_project, 'roles', 'requirements.yml')
   if (content):
    # This is a playbook with dependencies
    # ....
```

ÜBERBLICK BEHALTEN

Name	Group	Desc	Platform	Vers	Tags	Used by role	Used by play
haproxy	so/components	…	CentOS, Debian	0.1	haproxy	ldap_rev_proxy	lb-haproxy
nginx	so/components	…	RedHat, Debian		nginx		a8n
vrrp	so/profiles	…	RedHat, Debian	0.1	vrrp		a8n
keepalived	so/components	…	RedHat, Debian	0.2, 0.1	vrrp		a8n
vagrant	a8n/roles	…	CentOS, Debian, Ubuntu		vagrant	gitlab-runner	a8n
gitlab-runner	a8n/roles	…	Debian				a8n
….							

ÜBERBLICK BEHALTEN




AUSBLICK

AUSBLICK

Ansible entwickelt sich weiter:

- Collections – Ersatz für Patterns ?
- Ansible-builder / Execution Environments
  - Selbes Image für Tests und Deployments !?
  - Integration in *molecular*

AUSBLICK

AWX entwickelt sich weiter:

- Execution Environments
- Kubernetes

AUSBLICK

Engine Integration:

- Jobs direkt aus der Engine triggern
- Mehr SaaS Angebote

DANKE

JOINOUR REVOLUTION

JOINOURREVOLUTION.NET

IT SERVICES & SOFTWARE DEVELOPMENT

anexia.com | sjakobs@anexia-it.com