

ANSIBLE ALL THE THINGS

WAS MIR DABEI GEHOLFEN HAT ALLES
MIT ANSIBLE ZU AUTOMATISIEREN

Created by [Heiko Borchers](#) with [reveal.js](#)

ÜBER MICH

- SysAdmin
- Cloud Infrastructure für (E)-Autos
- Automatisiert am liebsten alles weg
- Terraform & Ansible im täglichen Einsatz

MOTIVATION

Ansible ist für mich das Tool der Wahl und auf Twitter hab ich dieses Jahr viel gelesen "ich würde es ja gern lernen, aber wie steige ich ein?"

WARUM ANSIBLE?

- Agentless
- Braucht keine zentrale Infrastruktur (Es gibt aber auf Wunsch die Option)
- Relativ leicht zu lernen
- Open Source (GPL-3.0)
- Eigentlich idempotent

WARUM VIELLEICHT DOCH NICHT ANSIBLE?

- Performance
- YAML

BASICS

ORDNERSTRUKTUR

```
.
├── ansible.cfg
├── credentials
│   └── Server1.sha512
├── group_vars
│   └── Server1.yml
├── hosts.yml
├── playbook.yml
├── roles
│   ├── awx_requirements
│   │   ├── handlers
│   │   │   └── main.yml
│   │   ├── tasks
│   │   │   └── main.yml
│   │   └── templates
```

DIE ANSIBLE.CFG

[defaults]

```
inventory=./hosts.yml
remote_user=root
log_path=ansible.log
gathering = smart
fact_caching = jsonfile
fact_caching_connection = .fact_cache/
fact_caching_timeout = 86400
vault_password_file=~/.pw/ansiblevault
remote_tmp      = .ansible/tmp
local_tmp       = .ansible/tmp
```


DAS INVENTORY:

```
---
MyServers:
  hosts:
    rootserver:
      ansible_host: example.host
      ansible_user: example_user
      vars:
        snmp_location: "Big Data Center"
    raspi:
      ansible_host: 192.168.1.1
      ansible_user: root
      vars:
        snmp_location: "Somewhere in the House"
WorkServers:
[...]
```

EIN EINFACHES PLAYBOOK:

```
- hosts: all
gather_facts: True
remote_user: root
become: yes
vars:
  users:
    - "{{all_users.my_username}}"
roles:
  - role: packages
  - role: date_time
  - role: hosts
  - role: user
```

ROLLEN:

```
└─ user
    ├── README.md
    ├── defaults
    │   └─ main.yml
    ├── files
    │   ├── my_username
    │   ├── password_gen.py
    │   └─ sudoers.j2
    ├── handlers
    │   └─ main.yml
    ├── tasks
    │   └─ main.yml
    └─ vars
        └─ all_users.yml
```

DEFAULTS

```
non_unique: no  
sudoers: False  
user_update_password: no
```

FILES

Dateien die ihr nicht als Templates habt, sondern so wie sie sind auf dem Zielcomputer haben wollt

- name: Copy sudoers file for safety
command: cp -f /etc/sudoers /etc/sudoers.tmp
- name: **Create** sudoers **file backup**
command: cp -f /etc/sudoers /etc/sudoers.bak
- **name:** make sure we can sudo **as admin group**
lineinfile: dest=/etc/sudoers.tmp state=**present** regexp='^%a
- **name:** also make sure ssh-**agent** works via sudo
lineinfile: dest=/etc/sudoers.tmp state=**present** regexp='^De
- **name:** **Final** sudoers **file check**
shell: visudo -q -c -f /etc/sudoers.tmp && cp -f /etc/sudoe

HANDLERS

```
---
```

```
- name: restart ssh daemon  
  service: name=sshd state=restarted
```

TASKS (1/2)

```
---
- name: installing base software
  package:
    name: "{{os_packages[ansible_os_family][item]}}"
    state: present
  with_items:
    - vim
    - monitoring_Plugins
```


TASKS (2/2)

```
---  
- name: secure ssh daemon  
  lineinfile: dest=/etc/ssh/sshd_config regexp=^PermitRootLogi  
  when: permitrootlogin is not defined  
  notify: restart ssh daemon  
  tags:  
    - new_system
```

VARS (1/2)

```
os_packages:
  Debian:
    monitoring_Plugins: monitoring-plugins-basic
  RedHat:
    monitoring-plugins: nagios-plugins
  ArchLinux:
    monitoring-plugins: monitoring-plugins
```

VARS (2/2)

```
vault_masterpassword: !vault |
  $ANSIBLE_VAULT;1.1;AES256
13372342133723421337234213372342133723421337234213372342133
13372342133723421337234213372342133723421337234213372342133
13372342133723421337234213372342133723421337234213372342133
13372342133723421337234213372342133723421337234213372342133
1337
```

DANKE FÜR EURE AUFMERKSAMKEIT

Den Code für die Slides findet ihr auf [Github](#)
und auf [Meinem Server](#)