On-premise Cloud Infrastruktur mit YAOOK Cloud&Heat Technologies GmbH

TEAM ON-PREMISE P&O

Lucas Trilken, DevOps Ingenieur
Product Owner Proxmox und Betrieb

Alexander Gräb, DevOps Ingenieur
Entwicklung und High-Security Betrieb

Stefan Dankert, Technology Advisor
Zulassungsprozesse und Betrieb

Maximilian Brandt, DevOps Ingenieur
YAOOK Entwicklung und Betrieb

Ilja Shmelkin
Leiter On-premise Projects & Operations

Green

Infrastrukturen ganzheitlich ökologisch nachhaltig gestalten.

Open

Open-Source-Software zur Stärkung der digitalen Souveränität.

Efficient

Einsatz von ökonomisch und ökologisch effizienten Technologien.

Wir sind ein ganzheitlich nachhaltiger Cloud-Service- und -Technologie-Provider aus Dresden mit dem Ziel, die digitale Souveränität in Deutschland und Europa zu stärken.

Unser Unternehmen

Erfahren Sie mehr

PRODUKT- UND SERVICE-ÜBERSICHT

Cloud Services

Services & Dienstleistungen

Infrastructure as a Service (IaaS)

Mit unserem IaaS profitieren Sie von einer nachhaltigen, open-source-basierten Cloud-Infrastruktur mit langjährig erprobtem Betriebskonzept.

Managed Kubernetes

Wir orchestrieren Ihr Kubernetes-Cluster und Sie können sich auf Ihr Kerngeschäft konzentrieren.

Cloud-Beratung

Als Cloud-Provider geben wir unser Know-how in passgenauen Beratungs- und Schulungsangeboten sowie hands-on an Sie weiter.

Digitale Infrastrukturen

On-Prem-Komplettlösung

Cloud&Heat Atlas

Wir stellen Ihnen ein nachhaltiges, digital-souveränes On-Prem-Komplettpaket für Ihre Machine-Learning Projekte zur Verfügung.

Cloud&Heat Titan

Mit dem Cloud&Heat Titan bieten wir ein hochsicheres digitales Komplettpaket für kritische Infrastrukturen (KRITIS).

Cloud&Heat Onpremix

Wir erweitern Ihre Multi- oder Hybrid-Cloud-Strategie um eine digital-souveräne On-Prem-Lösung.

Dienstleistungen

Customized Liquid Cooling Solutions

Unsere Customized Liquid Cooling Solutions machen Ihren Rechenzentrumsbetrieb energieeffizienter.

Infrastruktur-Beratung

Wir unterstützen Sie mit unseren Beratungen und Schulungen bei Planung, Aufbau und Betrieb Ihrer digitalen Infrastruktur.

ON-PREMISE INFRASTRUKTUR

Was ist ein Cloud-service?

Services & Dienstleistungen

Infrastructure as a Service (IaaS)

Mit IaaS werden dem Endkunden in der Regel Virtuelle Maschinen, Snapshots sowie Backups über einen Selfservice bereitgestellt.

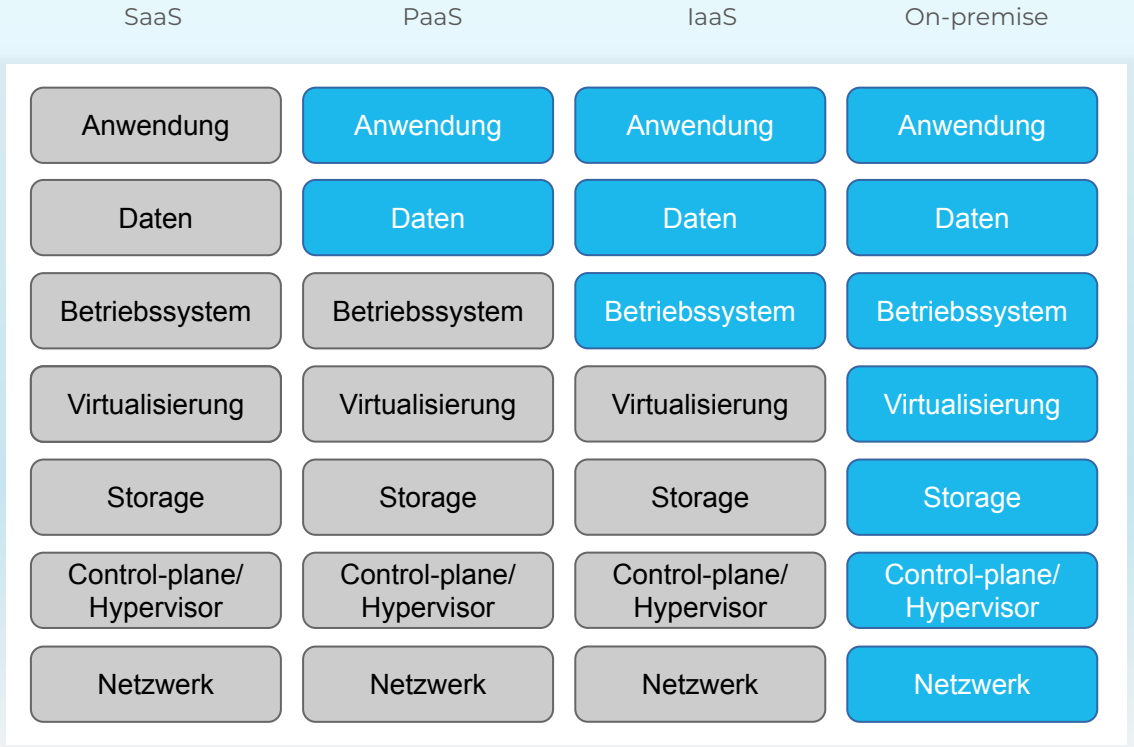
Platform as a Service (PaaS)

Mit PaaS wird dem Endkunden eine Plattform wie zum Beispiel Kubernetes, OpenShift, oder ähnlich auf Virtuellen Maschinen bereitgestellt.

Software as a Service (SaaS)

Mit SaaS wird dem Endkunden ein dediziertes Softwareprodukt wie zum Beispiel MongoDB, PostgreSQL, NGINX, Wordpress, etc. bereitgestellt.

Übersicht Cloud-service Modelle



ON-PREMISE INFRASTRUKTUR

Was ist ein Cloud-service?

Services & Dienstleistungen

Infrastructure as a Service (IaaS)

Mit IaaS werden dem Endkunden in der Regel Virtuelle Maschinen, Snapshots sowie Backups über einen Selfservice bereitgestellt.

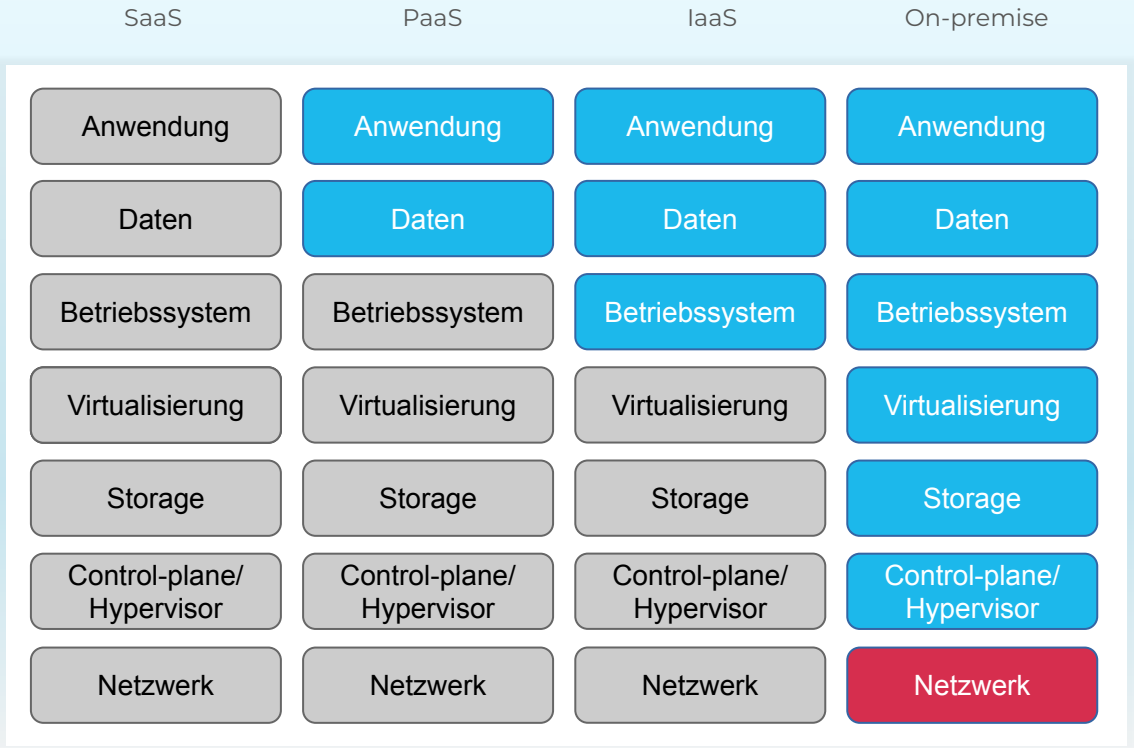
Platform as a Service (PaaS)

Mit PaaS wird dem Endkunden eine Plattform wie zum Beispiel Kubernetes, OpenShift, oder ähnlich auf Virtuellen Maschinen bereitgestellt.

Software as a Service (SaaS)

Mit SaaS wird dem Endkunden ein dediziertes Softwareprodukt wie zum Beispiel MongoDB, PostgreSQL, NGINX, Wordpress, etc. bereitgestellt.

Übersicht Cloud-service Modelle




CLOUD
&HEAT

NETZWERK IM ON-PREMISE DEPLOYMENT

Virtuelles LAN (VLAN)

IEEE 802.1Q

Verwendung und Nutzen

VLAN Trennung wird verwendet, um Netzwerkdomänen von einander zu separieren, die primär dazu dienen Hosts voneinander zu trennen bzw. um Pakete mit Firewalls filtern zu können.

Untagged VLAN

Sollte ein Netzwerkport eines Switches nur Daten eines einzigen VLANs transportieren, so wird dieses *untagged* (auch genannt *access*) an diesem Port konfiguriert. Der mit dem Port verbundene Host braucht keine spezifische VLAN Konfiguration.

Tagged VLAN

Sollte ein Netzwerkport eines Switches Daten mehrerer VLANs transportieren, so wird jedes VLAN *tagged* (auch genannt *trunk*) an diesem Port konfiguriert. Der mit dem Port verbundene Host muss für jedes VLAN ein eigenes Interface mit VLAN-ID konfigurieren.

Link Aggregation (LACP)

IEEE 802.3ad

Technische Voraussetzungen

Link Aggregation erlaubt es, mehrere gleichartige (z.B. 2x 25G) Ports auf Host und Switch-seite zu einem logischen Port (port-channel / bond) zusammenzulegen.

Bandbreite & Redundanz

Das nutzen von Link Aggregation verdoppelt die verfügbare Bandbreite (nicht zwangsläufig den realen Datendurchsatz). Wichtiger ist in der Regel aber, dass man um Redundanz zu erreichen port-channel über mehrere Switche konfigurieren kann.

Erweiterte Topologien

Um skalierbare Netzwerke für large-scale on-premise Deployments zu provisionieren benötigt man (>500 Server) benötigt man spezielle Topologien welche die Nutzung von LACP effektiv notwendig machen.

Netzwerk Firewall

VyOS - Open Source Router and Firewall

Verwendung und Nutzen

Eine Firewall filtert Pakete und Verbindungen zwischen Netzen. Dies können virtuelle Netze (SDN / VLAN) oder physische Netze sein.

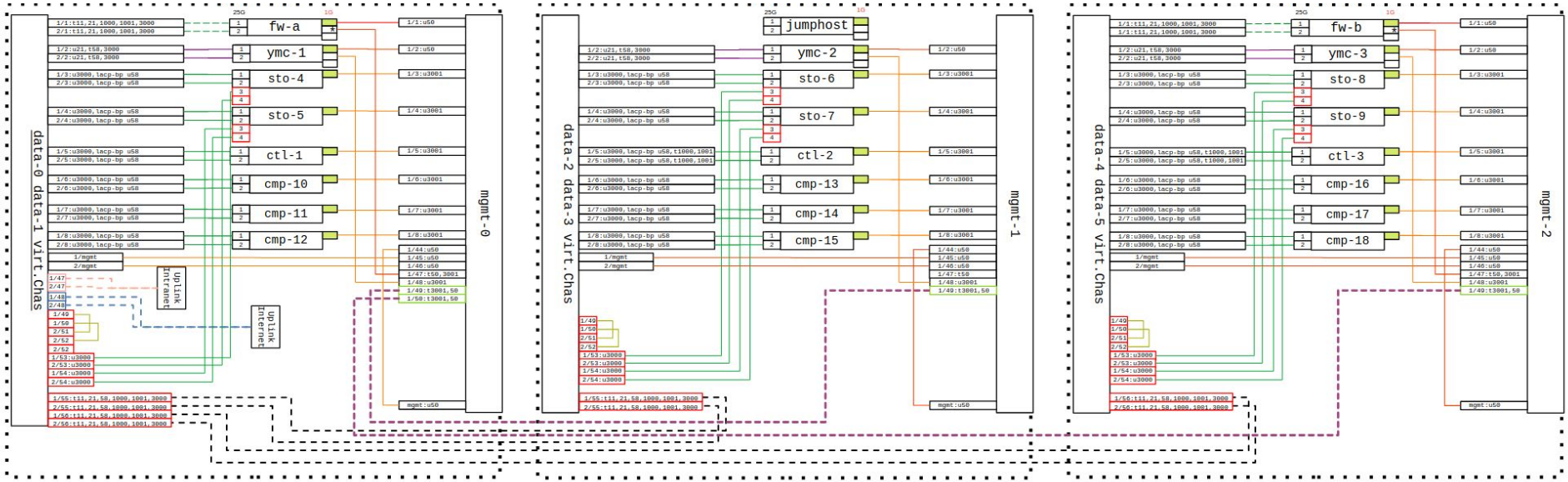
VyOS Firewall Distribution

VyOS ist eine Open Source Firewall Distribution mit einem sehr großen Funktionsumfang. Sie erlaubt den Einsatz erweiterter Netzwerk- und Firewallfunktionen sowie üblicher Dienste wie DHCP, DNS, VPN, Docker und vielem mehr.

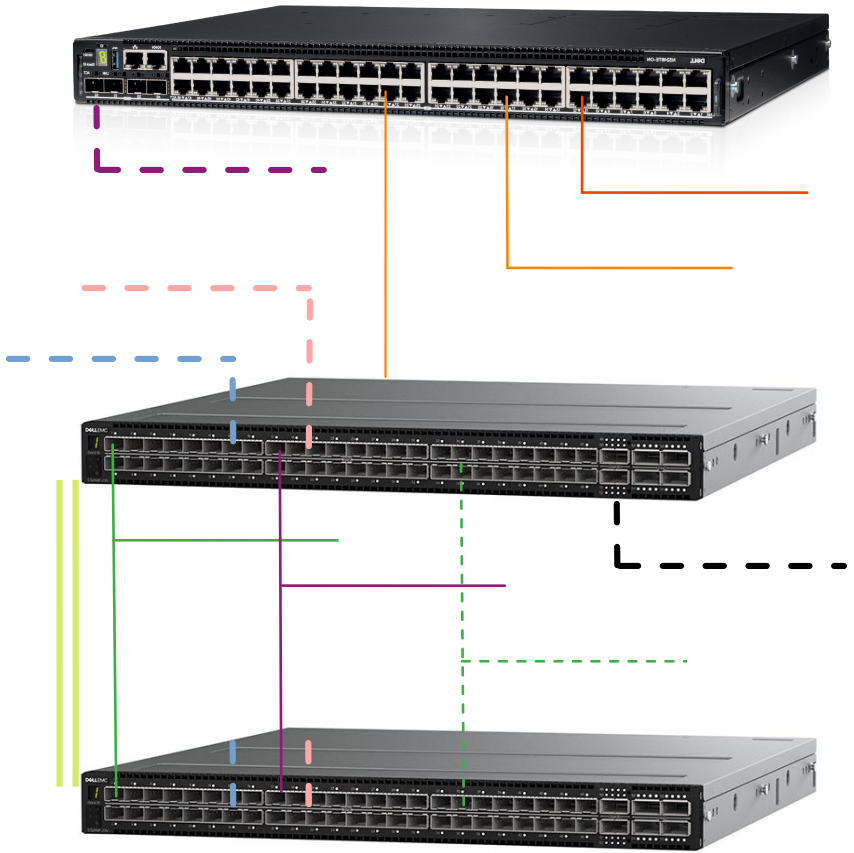
Redundanz mit VRRP

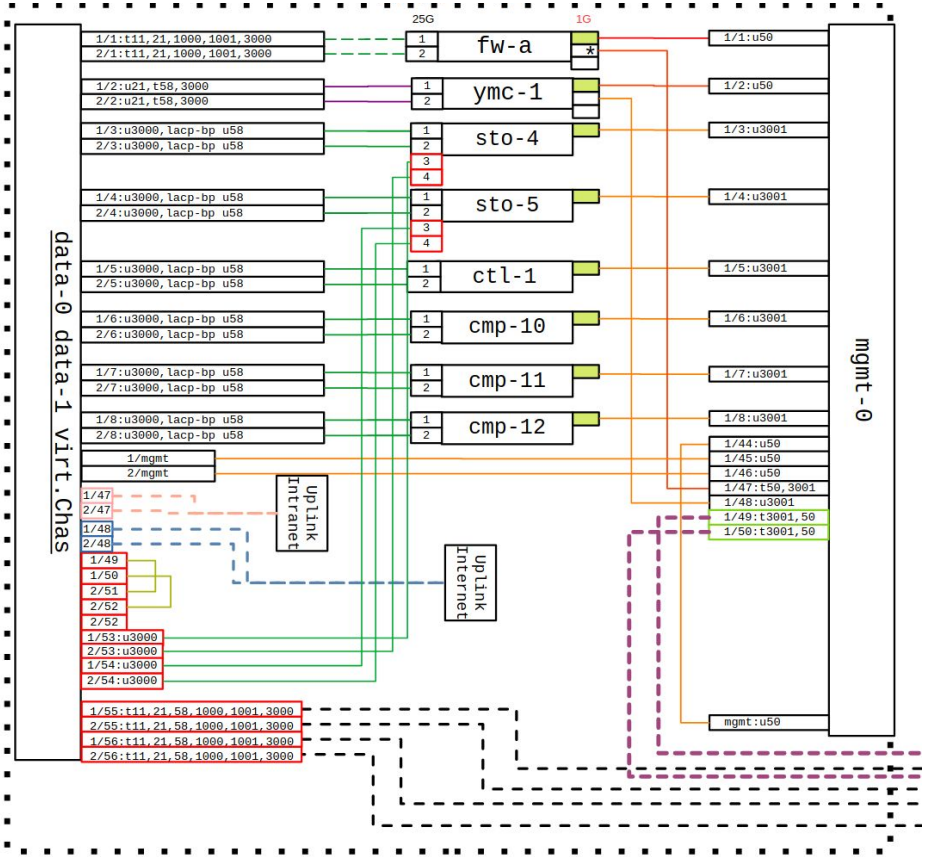
VyOS erlaubt die Konfiguration redundanter Firewall-Paare mit Virtual Router Redundancy Protocol (VRRP) im Master-Slave Prinzip. Versagt eine Firewall während der Laufzeit, so übernimmt die andere innerhalb eines ICMP Ticks.

BEISPIEL: LAYER-1 VERKABELUNGSPLAN



BEISPIEL: LAYER-1 VERKABELUNGSPLAN





VYOS: OPEN SOURCE ROUTER UND FIREWALL OS

Routing

BGP (IPv4 and IPv6), OSPF (v2 and v3), BFD(BGP, OSPF, IS-IS, Static), RIP (v1 & v2), RIPng, IS-IS, policy-based routing and Multicast Routing +MPLS LDP

Network Address Translation (NAT)

SNAT, DNAT um Pakete zwischen Netzwerken zu routen.

Automatisierungen

Native Support for API (GraphQL), Configuration-Management/IaaC Tools (Ansible/salt/Netmiko/ NAPALM/Terraform), Cloud-init(own config-modules), uvm.

Virtuelle Private Netzwerke & Tunnel

IPsec, VTI, VXLAN, L2TPv3, L2TP/IPsec and PPTP servers, tunnel interfaces (GRE, IPIP, SIT), OpenVPN in client, server, or site-to-site mode, wireguard. +GENEVE

Wichtige Netzwerkdienste

DHCP and DHCPv6 server and relay, IPv6 RA, DNS forwarding, TFTP server, web proxy, PPPoE access concentrator, NetFlow/sFlow sensor, QoS.+IPoE +VRFs support +WanLB

Containerunterstützung

...auf Basis von Podman können Container gestartet werden.

Firewall

Stateful Firewall, Zonen-basierte Firewall

Hochverfügbarkeit

VRRP for IPv4 and IPv6, ability to execute custom health checks and transition scripts; ECMP, stateful load balancing.

Einfache Upgrades

VyOS erlaubt es offizielle Images einzuhängen und von diesen ein Upgrade zur neuen Version durchzuführen. Dieser Vorgang ist besonders transparent und bei Bedarf reversibel.

ON-PREMISE INFRASTRUKTUR

Was ist ein Cloud-service?

Services & Dienstleistungen

Infrastructure as a Service (IaaS)

Mit IaaS werden dem Endkunden in der Regel Virtuelle Maschinen, Snapshots sowie Backups über einen Selfservice bereitgestellt.

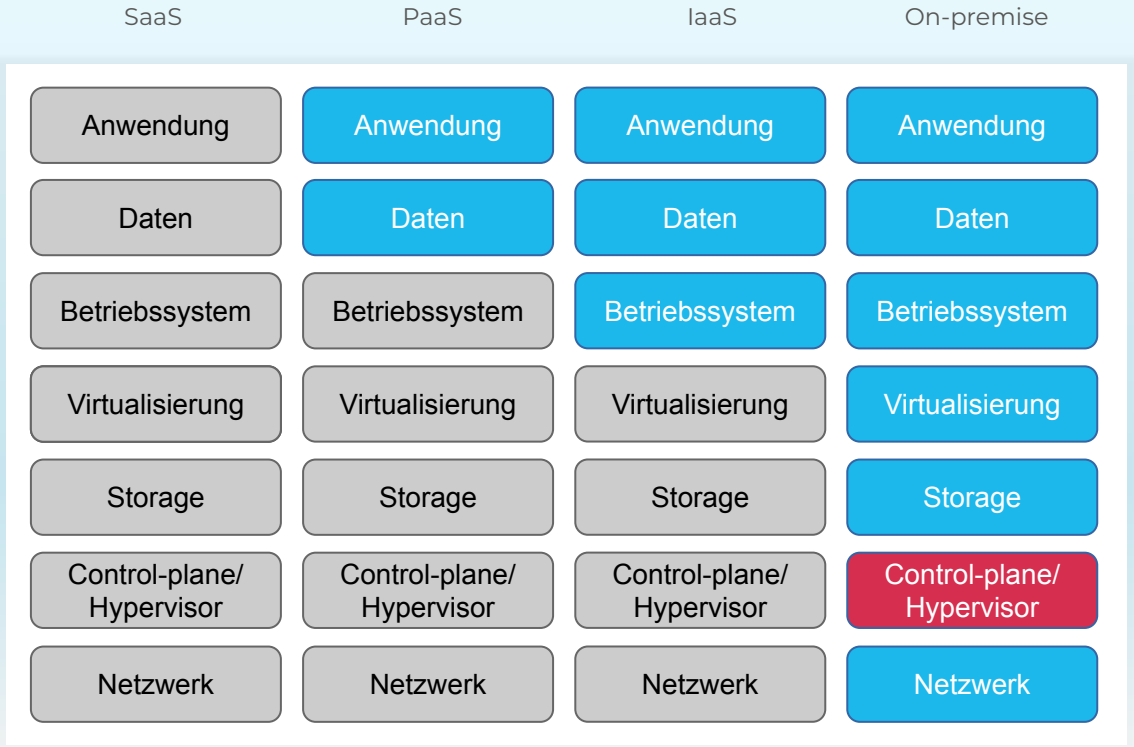
Platform as a Service (PaaS)

Mit PaaS wird dem Endkunden eine Plattform wie zum Beispiel Kubernetes, OpenShift, oder ähnlich auf Virtuellen Maschinen bereitgestellt.

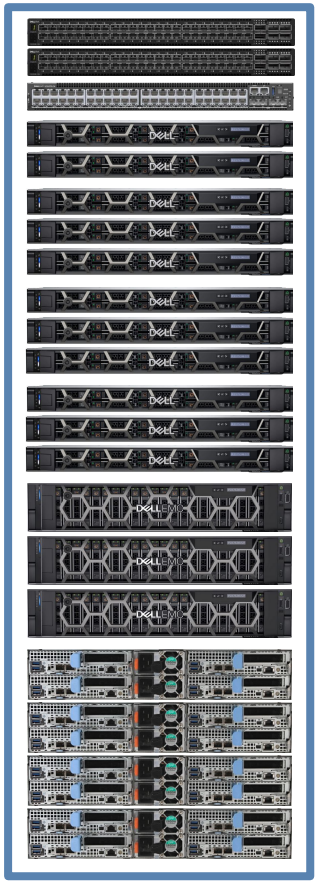
Software as a Service (SaaS)

Mit SaaS wird dem Endkunden ein dediziertes Softwareprodukt wie zum Beispiel MongoDB, PostgreSQL, NGINX, Wordpress, etc. bereitgestellt.

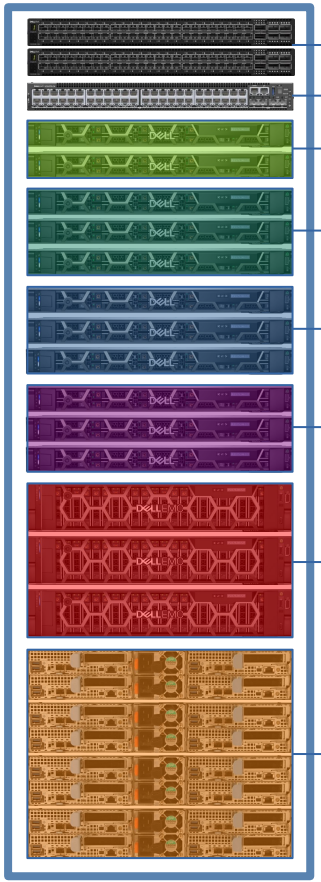
Übersicht Cloud-service Modelle



HARDWAREBEDARF YAOOK DEPLOYMENT

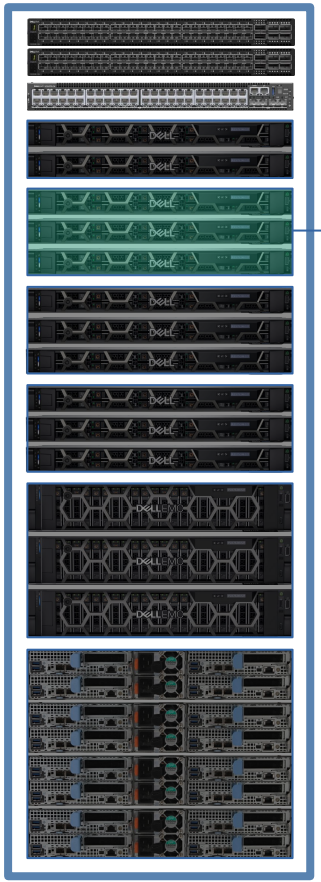


HARDWAREBEDARF YAOOK DEPLOYMENT



- Data-switches, 2Stk. pro Rack (LACP)
- Mgmt-switch, 1Stk. pro Rack
- Firewalls, 2Stk. pro Deployment (VRRP)
- YAOOK Management Cluster (YMC), 3Stk. pro Deployment (k8s-cluster)
- YAOOK-IaaS K8s-Controlplane, min. 3Stk. pro Deployment, erweiterbar (quorum!)
- YAOOK-IaaS OpenStack-Controlplane, min. 3Stk. pro Deployment, erweiterbar (multiple von 3!)
- Storage, min. 3Stk. pro Deployment (üblicherweise Ceph; andere Technologien im Projektkontext)
- Compute, so viel wie nötig (thermische / elektrische Kapazität sowie Switchports beachten!)

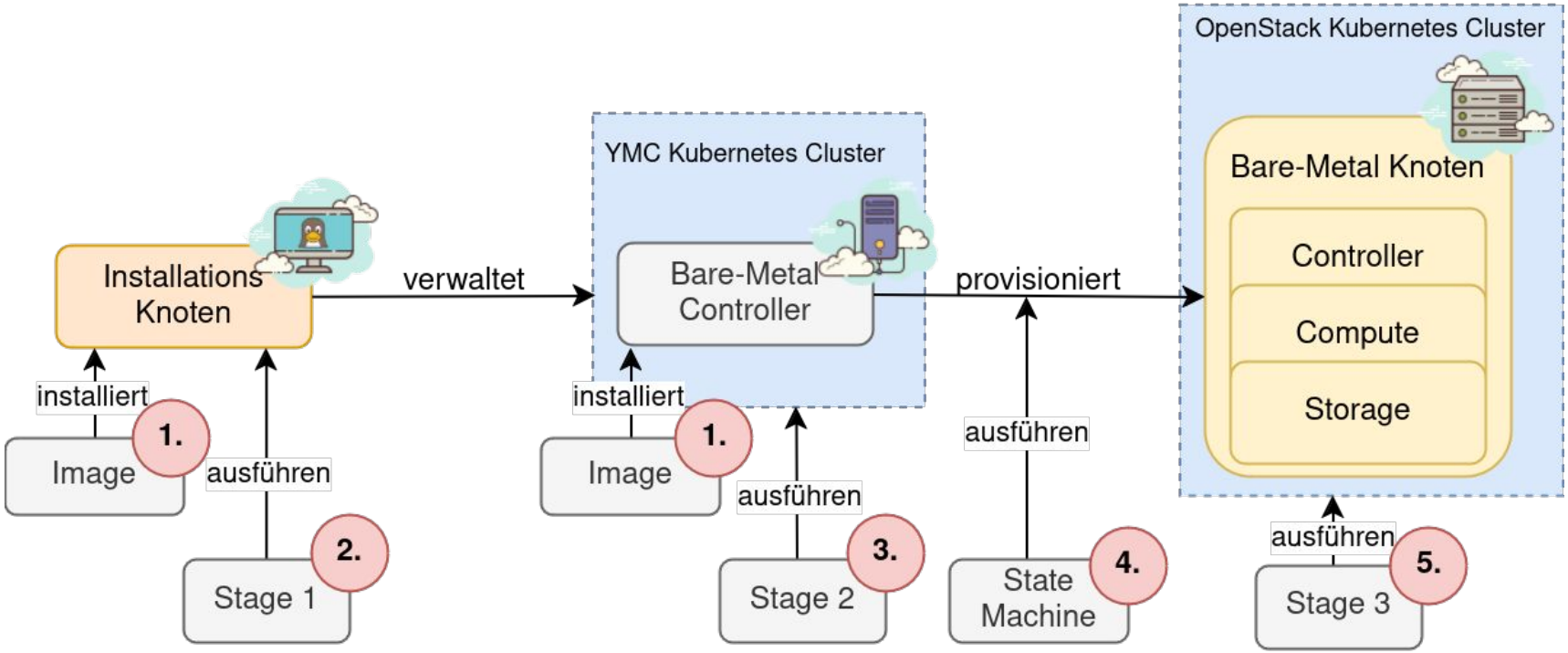
PROVISIONIERUNG MIT YMC & OPENSTACK IRONIC



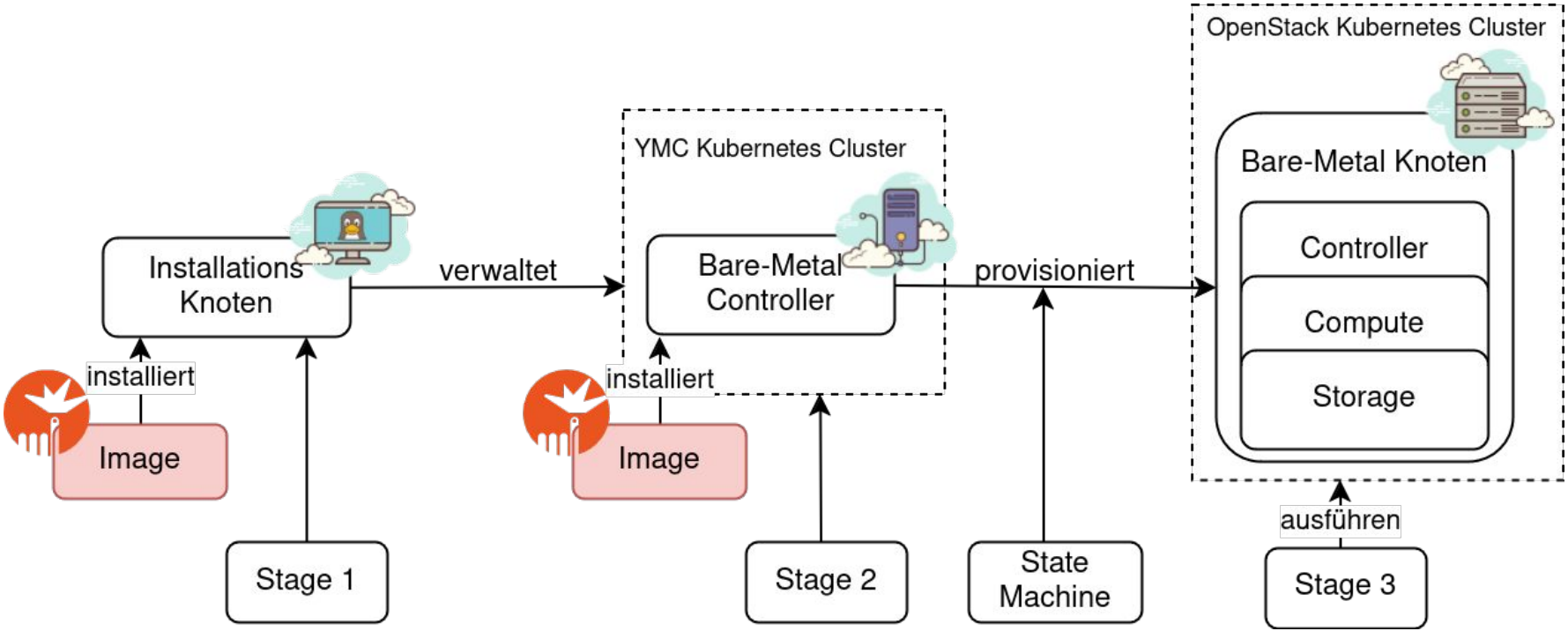
- YAOOK Management Cluster (YMC), 3Stk. pro Deployment (k8s-cluster)
  - ...ein Kubernetes Cluster auf bare-metal nodes (LCM Tarook von C&H)

- Dienste auf Kubernetes:
  - Netbox
    - Inventarisierung von Hardware
    - Management von VLANs, Nameservern, Monitoring-endpunkten, etc.
  - Keystone (notwendig für Ironic)
  - Ironic
    - Wird für die bare-metal Provisionierung von IaaS-nodes genutzt (k8s-Contr., OS-Contr., Storage, Compute)
  - Metal-controller
    - OpenSource Software für Orchestrierung von Ironic (auf Basis von Daten in der Netbox)

PROVISIONIERUNG IAAS MIT YAAOK-MGMT-CLUSTER



INSTALL-NODE UND YAOOK-MANAGEMENT-CLUSTER



CLOUD-CONFIG FÜR YAOOK-MANAGEMENT-CLUSTER

```
#cloud-config
autoinstall:
  version: 1
  locale: "de_DE.UTF-8"
  keyboard:
    layout: "de"
  user-data:
    users:
      - default
      - name: iljashmelkin
        gecos: Iljashmelkin
        sudo: ALL=(ALL) NOPASSWD:ALL
        groups: users, admin, root
        shell: /bin/bash
        lock_passwd: false
        passwd: $6$supersecrethash11!!
        ssh_authorized_keys:
          - ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAII/NWTY8d4CpGsey23vlWHa4koaPLKEvXNFJ+v94M7AP iljashmelkin
    runcmd:
      - [sudo, chown, -R, iljashmelkin:iljashmelkin, /ymc]
      - runuser -l iljashmelkin -c '/bin/bash /ymc/startup-ymc.sh'
  power_state:
    delay: "+30"
    mode: reboot
    message: done...rebooting.
    timeout: 30
    condition: True
  ssh:
    install-server: true
    allow-pw: false
  late-commands:
    - |
      cat <<EOF | sudo tee /target/tmp/crypt_setup.sh
      #!/bin/bash
      mkdir /etc/keys
      printf '#!/bin/sh\n\nprintf secretpassword' > /etc/keys/root
      chmod -R 700 /etc/keys
      sed -e 's#\$#,keyscript=/etc/keys/root#' -i /etc/crypttab
      /sbin/update-initramfs -u
      EOF
    - chmod 755 /target/tmp/crypt_setup.sh
    - curtin in-target --target /target /tmp/crypt_setup.sh
    - curtin in-target --target=/target -- mkdir /ymc
    - cp -R /cdrom/ymc/* /target/ymc
    - curtin in-target --target=/target -- sh -c 'echo "ymc" | sudo tee /etc/hostname'
    - curtin in-target --target=/target -- sh -c 'echo "127.0.0.1 localhost ymc" | sudo tee /etc/hosts'
```

```
network:
    network:
      version: 2
      bonds:
        bond0:
          interfaces:
          - eno12399np0
          - eno12409np1
          parameters:
            lacp-rate: slow
            mode: 802.3ad
            transmit-hash-policy: layer2+3
          addresses:
          - 10.254.20.4/27
          gateway4: 10.254.20.1
          nameservers:
            addresses:
            - 8.8.8.8
            search: []
      ethernets:
        eno8303:
          addresses:
          - 10.255.0.1/16
        eno8403:
          addresses:
          - 10.2.31.253/20
        eno12399np0: {}
        eno12409np1: {}
storage:
    config:
    # Create GPT partition table on disks
    - ptable: gpt
      path: /dev/sda
      wipe: superblock-recursive
      preserve: false
      name: ''
      grub_device: true
      type: disk
      id: disk-0
    - ptable: gpt
      path: /dev/sdb
      wipe: superblock-recursive
      preserve: false
      name: ''
      grub_device: false
      type: disk
      id: disk-1
```

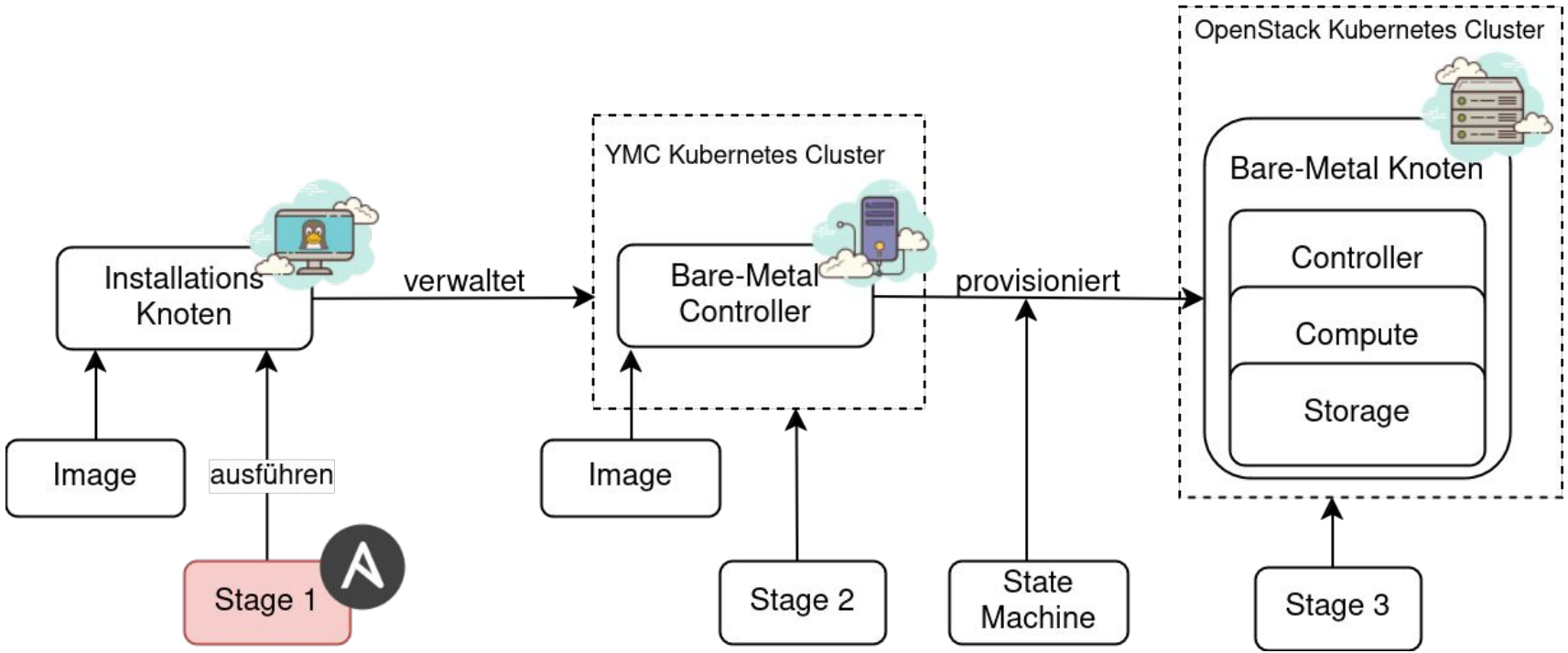
CLOUD-CONFIG FÜR YAOOK-MANAGEMENT-CLUSTER

```
# Create EFI partitions
- device: disk-0
  wipe: superblock
  size: 564133888
  flag: boot
  number: 1
  preserve: false
  grub_device: true
  type: partition
  id: partition-0
- device: disk-1
  wipe: superblock
  size: 564133888
  flag: boot
  number: 1
  preserve: false
  grub_device: true
  type: partition
  id: partition-1
# Format EFI partitions
- fstype: fat32
  volume: partition-0
  preserve: false
  type: format
  id: format-efi-0
- fstype: fat32
  volume: partition-1
  preserve: false
  type: format
  id: format-efi-1
# Mount EFI partitions
- path: /boot/efi
  device: format-efi-0
  type: mount
  id: mount-efi-0
# Partitions to form the RAID from
- device: disk-0
  size: -1
  wipe: superblock
  flag: ''
  number: 1
  preserve: false
  grub_device: false
  type: partition
  id: partition-2
- device: disk-1
  size: -1
  wipe: superblock
  flag: ''
  number: 1
  preserve: false
  grub_device: false
  type: partition
  id: partition-3
```

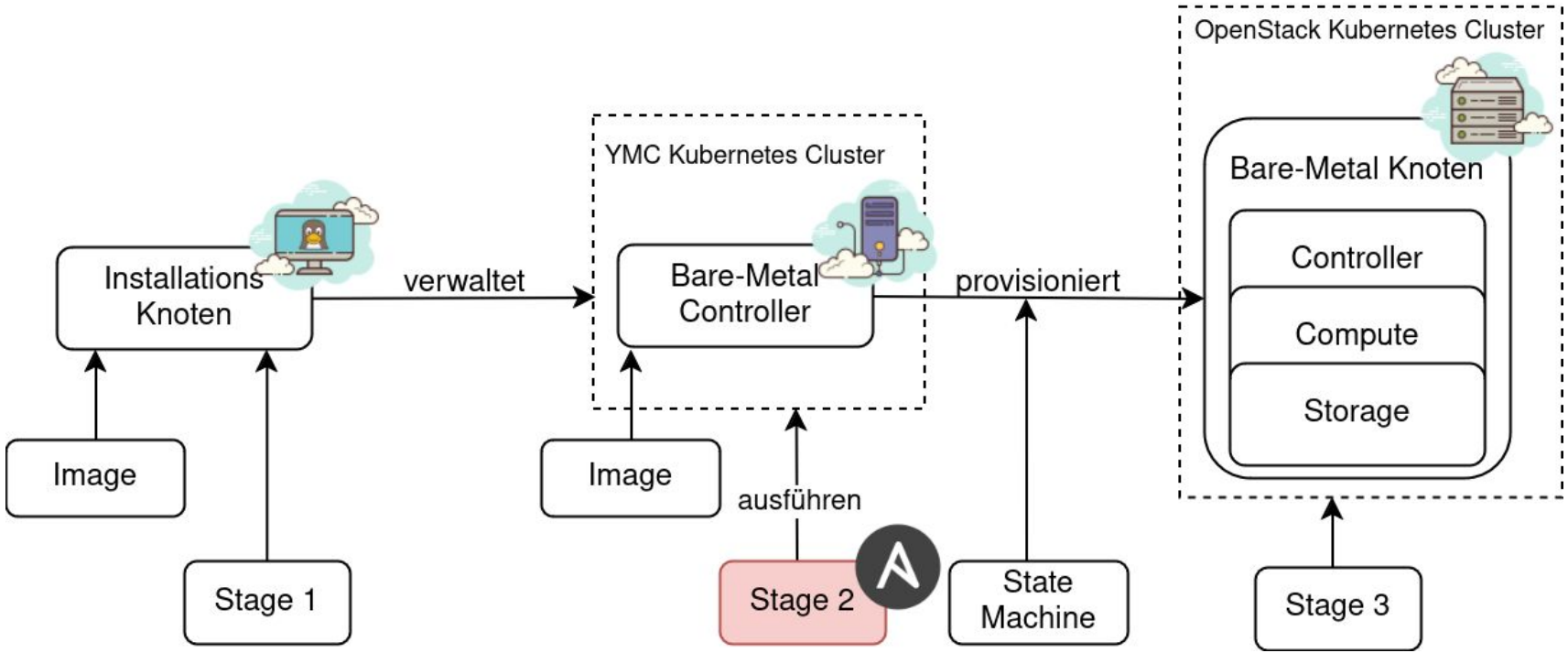
```
# RAID 1
    - name: md0
      raidlevel: raid1
      devices:
      - partition-2
      - partition-3
      spare_devices: []
      preserve: false
      wipe: superblock-recursive
      ptable: gpt
      type: raid
      id: raid-0
    # Partition for /boot
    - device: raid-0
      size: 1048576000
      wipe: superblock
      flag: ''
      number: 1
      preserve: false
      grub_device: false
      type: partition
      id: partition-5
    - fstype: ext4
      volume: partition-5
      preserve: false
      type: format
      id: format-0
    - path: /boot
      device: format-0
      type: mount
      id: mount-0
    # Partition that is encrypted and holds the LVM volume group
    - device: raid-0
      size: -1
      wipe: superblock
      flag: ''
      number: 2
      preserve: false
      grub_device: false
      type: partition
      id: partition-6
    - volume: partition-6
      key: 'secretpassword'
      preserve: false
      type: dm_crypt
      id: dm_crypt-0
    - name: ubuntu-vg
      devices:
      - dm_crypt-0
      preserve: false
      type: lvm_volgroup
      id: lvm_volgroup-0
```

```
# / (root)
- name: lv_system
  volgroup: lvm_volgroup-0
  size: 100G
  wipe: superblock
  preserve: false
  type: lvm_partition
  id: lvm_partition-0
- fstype: ext4
  volume: lvm_partition-0
  preserve: false
  type: format
  id: format-1
- path: /
  device: format-1
  type: mount
  id: mount-1
```

EINRICHTUNG INSTALL-NODE



EINRICHTUNG YAOOK-MANAGEMENT-CLUSTER



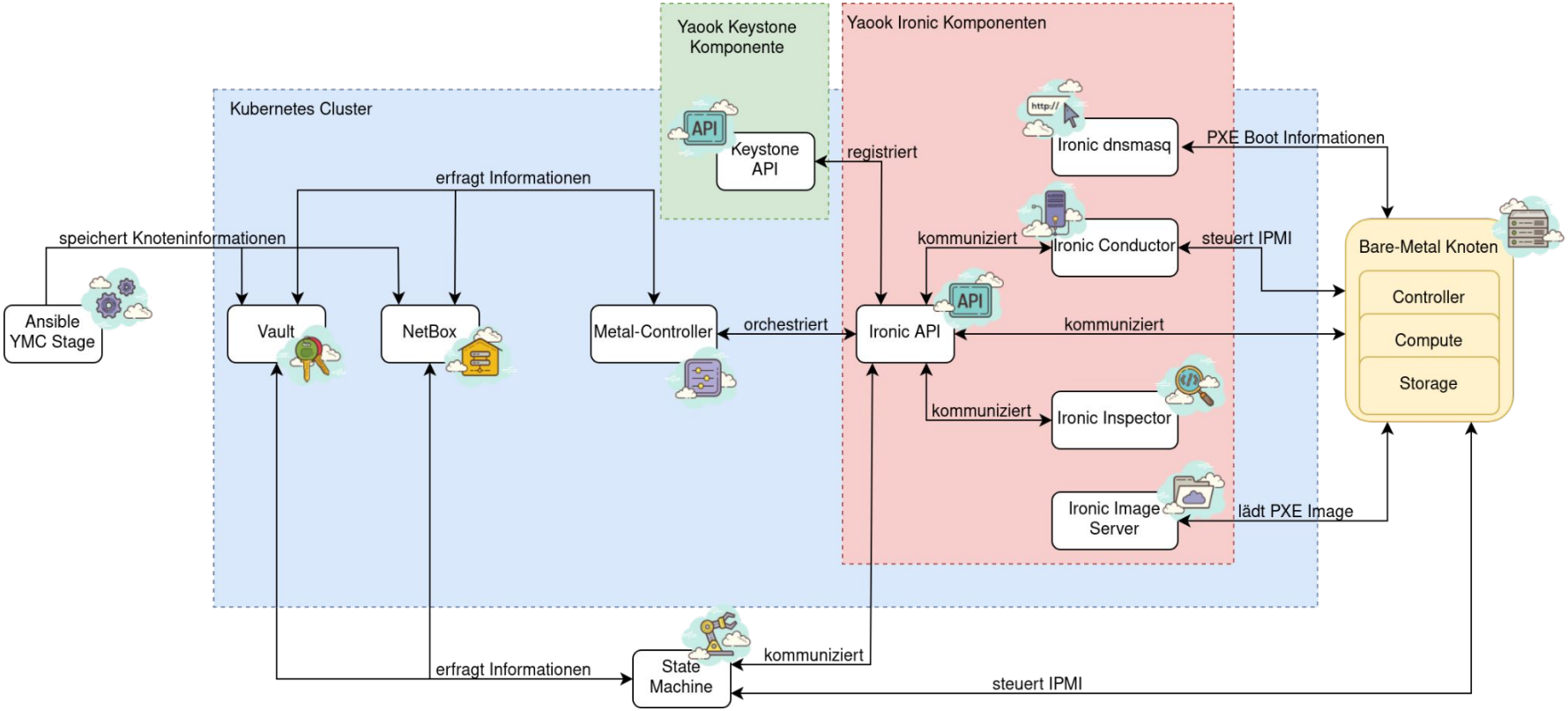
EINRICHTUNG YAOOK-MANAGEMENT-CLUSTER

- **Installation von Yaook/K8s**
- **Ausführen des Bare Metal Ansible**
  - Installation von Storage Class
  - Anwendung der CA für den Cert Manager
  - Migration des Vaults aus dem Docker ins Cluster
  - Installation und Einrichtung von Netbox
  - Installation der Yaook Operatoren mit Manifesten

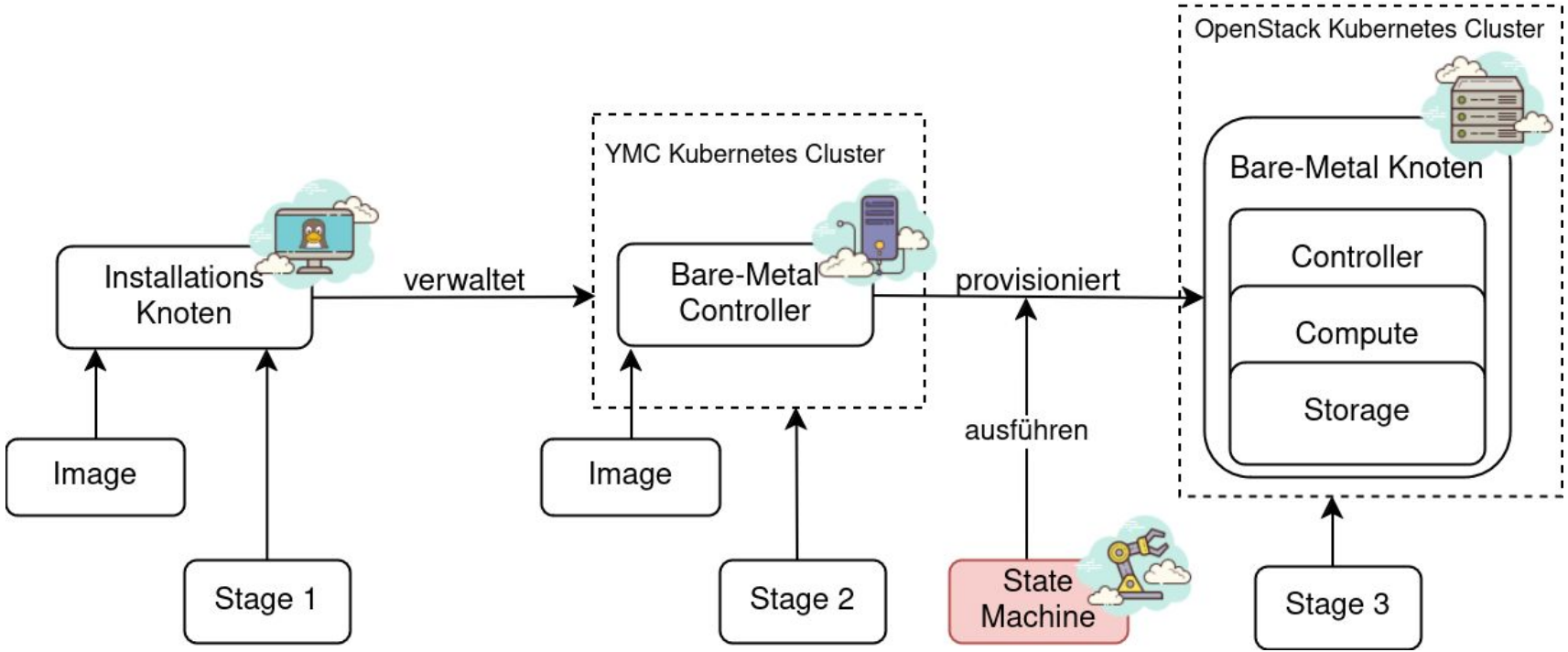
```
# YMC Variables
# ---------------------
netbox_site_name: dd0
vault_cluster_name: dd0-ymc
yaook_operator_namespace: yaook-bmc
ymc_yaook_operator_charts:
  - crds
  - infra-operator
  - keystone-operator
  - keystone-resources-operator
  - infra-ironic-operator

# OpenStack/K8s Server List
# ---------------------
netbox_manufacturers:
  - name: Lenovo
    slug: lenovo
  - name: Dell
    slug: dell
server_types:
  - manufacturer: lenovo
    model: ThinkSystem SR650
    slug: thinksystem-sr650
    part_number: 7X06
    u_height: "1"
# device_roles: controller, compute, storage
servers:
  - asset_tag: ctl-1
    device_role: controller
    model: thinksystem-sr650
    ipmi:
      ip: 10.2.17.1
      username_env: IPMI_USER
      password_env: IPMI_PASSWORD
```

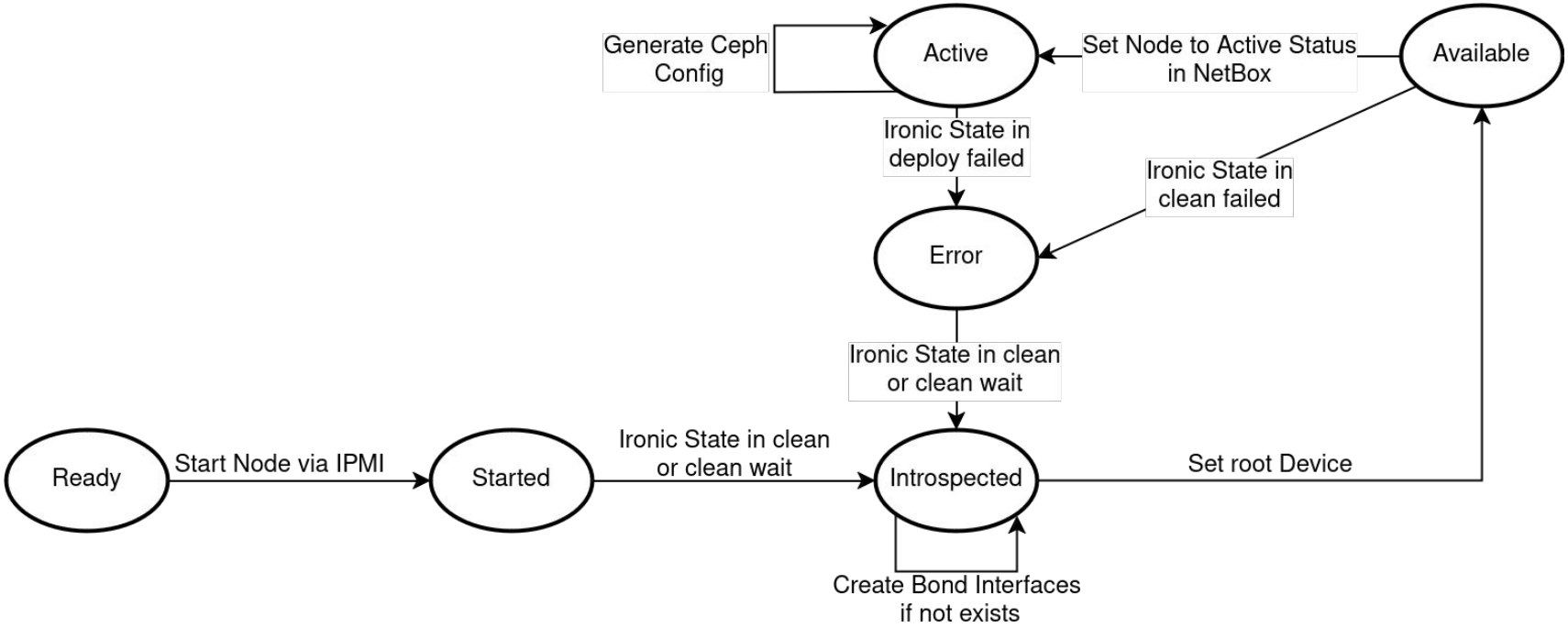
YAOOK IAAS UNDERCLOUD



EINRICHTUNG YAOOK-OPENSTACK-CLUSTER



EINRICHTUNG YAOOK-OPENSTACK-CLUSTER



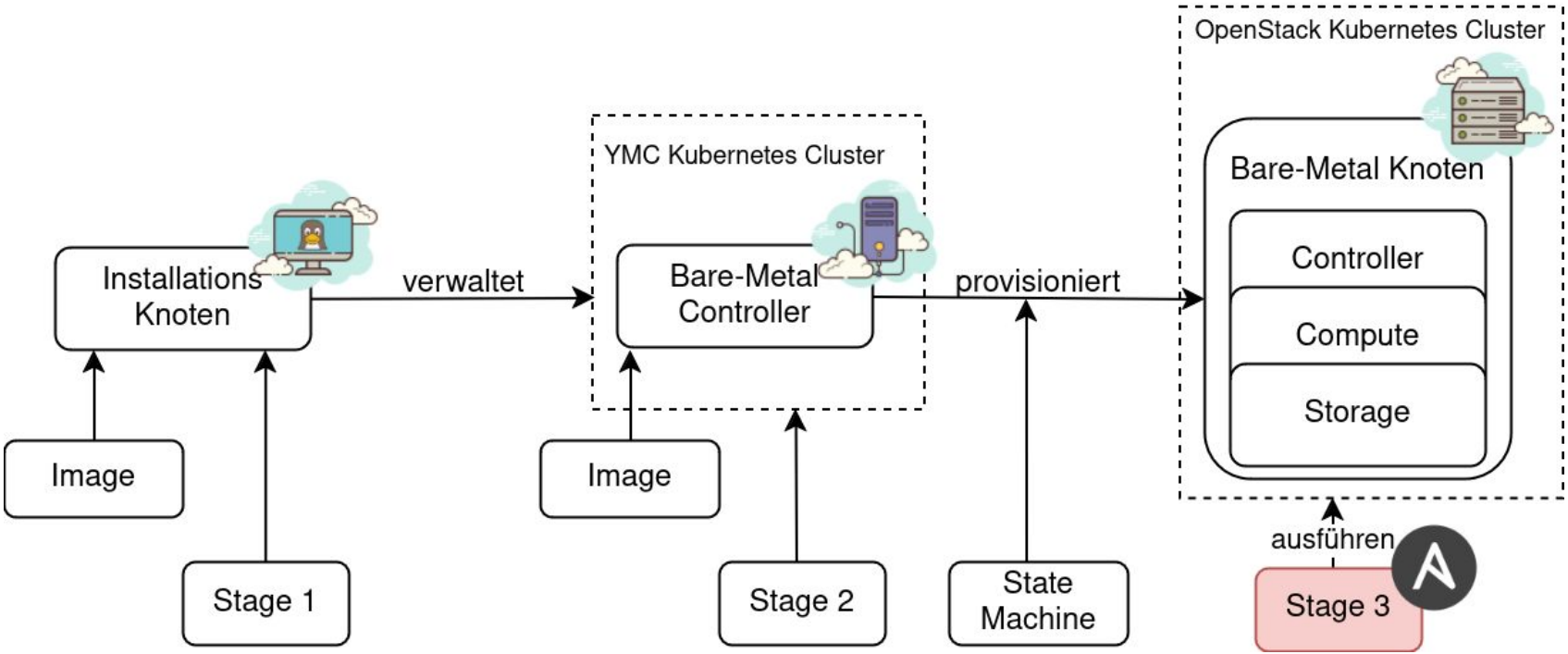
EINRICHTUNG YAOOK-MANAGEMENT-CLUSTER

```
<<K9s-Shell>> Pod: yaook-bmc/yaookctl-openstackclient-keystone-65fcdc654f-nrqkl | Container: openstackclient
root@yaookctl-openstackclient-keystone-65fcdc654f-nrqkl:/# openstack baremetal node list
+--------------------------------------+--------------+---------------+-------------+--------------------+-------------+
| UUID                                 | Name         | Instance UUID | Power State | Provisioning State | Maintenance |
+--------------------------------------+--------------+---------------+-------------+--------------------+-------------+
| 16f1394e-c8d2-4962-                  | ctl-le     l1 | None          | power on    | active             | False       |
| 1b719209-4a06-4f35-                  | ctl-lu     )3 | None          | power on    | active             | False       |
| 74eb8283-ddfc-4b3e-                  | sto-ki     32 | None          | power on    | active             | False       |
| 638bfeae-44e3-4dea-                  | ctl-su     74 | None          | power on    | active             | False       |
| 6285aa3d-3607-40d9-                  | sto-pi     56 | None          | power on    | active             | False       |
| 987ca06c-5f82-4245-                  | cmp-ka     33 | None          | power on    | active             | False       |
| 1b462aff-0fb3-46b4-                  | sto-ke     30 | None          | power on    | active             | False       |
| 4a9ba32f-f97d-491c-                  | sto-xa     73 | None          | power on    | active             | False       |
| 3db127ec-ead9-460d-                  | sto-ni     55 | None          | power on    | active             | False       |
| 81871cfe-ab15-4df8-                  | cmp-xi     )0 | None          | power on    | active             | False       |
| 4c2b55b1-0ac2-4a25-                  | cmp-le     70 | None          | power on    | active             | False       |
| 8a7f245b-4a84-4c51-                  | cmp-xo     24 | None          | power on    | active             | False       |
| 27bf1c59-8f19-4e40-                  | cmp-pu     53 | None          | power on    | active             | False       |
| 421c049b-f8f1-42ef-                  | sto-na     36 | None          | power on    | active             | False       |
| bece1440-baf3-4725-                  | cmp-re     78 | None          | power on    | active             | False       |
| d44e90b6-ab23-42e7-                  | cmp-ye     31 | None          | power on    | active             | False       |
| 4535001d-6afe-4f97-                  | cmp-tu     15 | None          | power on    | active             | False       |
| 5a8848cc-9ff3-4a3c-                  | cmp-ri     35 | None          | power on    | active             | False       |
| bfa05291-73c4-46b9-                  | None         | None          | None        | enroll             | False       |
| 86285602-c05d-47e9-                  | None         | None          | None        | enroll             | False       |
+--------------------------------------+--------------+---------------+-------------+--------------------+-------------+
root@yaookctl-openstackclient-keystone-65fcdc654f-nrqkl:/#
```

EINRICHTUNG YAOOK-MANAGEMENT-CLUSTER

```
/workplace/k8s-cluster$ kubectl get nodes -o wide
NAME          STATUS   ROLES           AGE   VERSION   INTERNAL-IP   EXTERNAL-IP   OS-IMAGE             KERNEL-VERSION   CONTAINER-RUNTIME
cmp-k  83     Ready    <none>                v1.30.6   10.           <none>        Ubuntu 22.04.5 LTS   5.15.            containerd://1.7.23
cmp-l  70     Ready    <none>                v1.30.6   10.           <none>        Ubuntu 22.04.5 LTS   5.15.            containerd://1.7.23
cmp-p  63     Ready    <none>                v1.30.6   10.           <none>        Ubuntu 22.04.5 LTS   5.15.            containerd://1.7.23
cmp-r  78     Ready    <none>                v1.30.6   10.           <none>        Ubuntu 22.04.5 LTS   5.15.            containerd://1.7.23
cmp-r  85     Ready    <none>                v1.30.6   10.           <none>        Ubuntu 22.04.5 LTS   5.15.            containerd://1.7.23
cmp-t  45     Ready    <none>                v1.30.6   10.           <none>        Ubuntu 22.04.5 LTS   5.15.            containerd://1.7.23
cmp-x  00     Ready    <none>                v1.30.6   10.           <none>        Ubuntu 22.04.5 LTS   5.15.            containerd://1.7.23
cmp-x  24     Ready    <none>                v1.30.6   10.           <none>        Ubuntu 22.04.5 LTS   5.15.            containerd://1.7.23
cmp-y  81     Ready    <none>                v1.30.6   10.           <none>        Ubuntu 22.04.5 LTS   5.15.            containerd://1.7.23
ctl-l  11     Ready    control-plane         v1.30.6   10.           <none>        Ubuntu 22.04.5 LTS   5.15.            containerd://1.7.23
ctl-l  93     Ready    control-plane         v1.30.6   10.           <none>        Ubuntu 22.04.5 LTS   5.15.            containerd://1.7.23
ctl-s  74     Ready    control-plane         v1.30.6   10.           <none>        Ubuntu 22.04.5 LTS   5.15.            containerd://1.7.23
sto-k  80     Ready    <none>                v1.30.6   10.           <none>        Ubuntu 22.04.5 LTS   5.15.            containerd://1.7.23
sto-k  82     Ready    <none>                v1.30.6   10.           <none>        Ubuntu 22.04.5 LTS   5.15.            containerd://1.7.23
sto-n  36     Ready    <none>                v1.30.6   10.           <none>        Ubuntu 22.04.5 LTS   5.15.            containerd://1.7.23
sto-n  65     Ready    <none>                v1.30.6   10.           <none>        Ubuntu 22.04.5 LTS   5.15.            containerd://1.7.23
sto-p  56     Ready    <none>                v1.30.6   10.           <none>        Ubuntu 22.04.5 LTS   5.15.            containerd://1.7.23
sto-x  73     Ready    <none>                v1.30.6   10.           <none>        Ubuntu 22.04.5 LTS   5.15.            containerd://1.7.23
```

YAOOK OPENSTACK OPERATORS



ON-PREMISE INFRASTRUKTUR

Was ist ein Cloud-service?

Services & Dienstleistungen

Infrastructure as a Service (IaaS)

Mit IaaS werden dem Endkunden in der Regel Virtuelle Maschinen, Snapshots sowie Backups über einen Selfservice bereitgestellt.

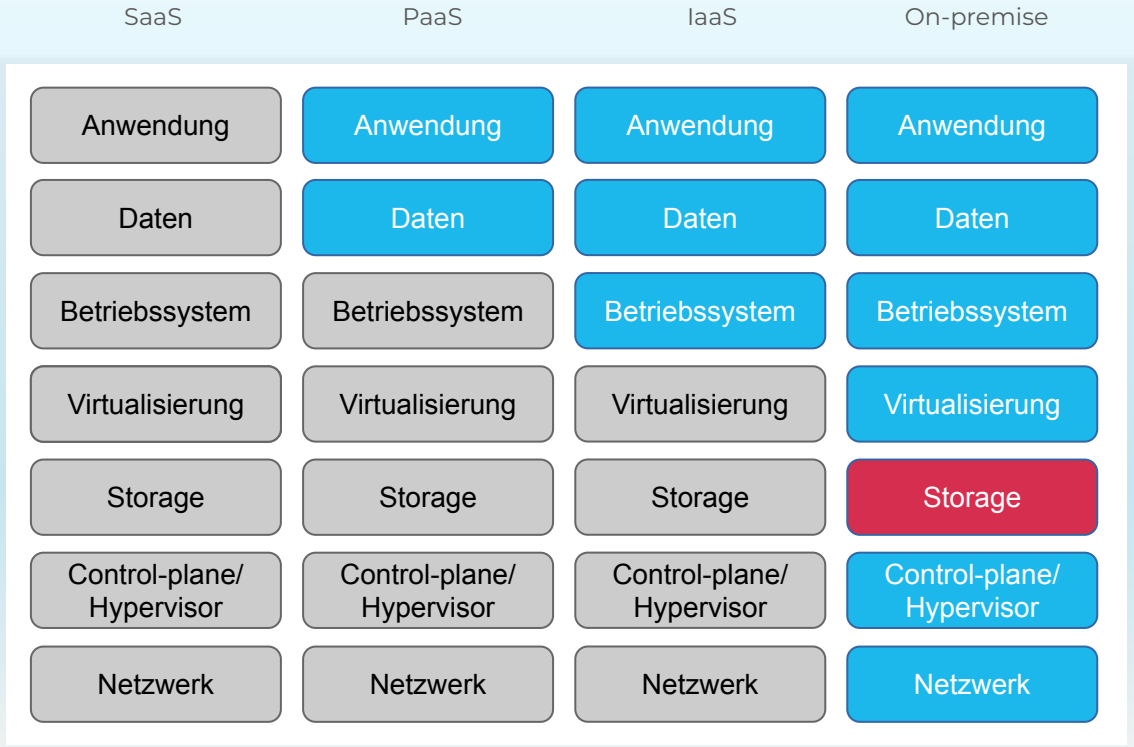
Platform as a Service (PaaS)

Mit PaaS wird dem Endkunden eine Plattform wie zum Beispiel Kubernetes, OpenShift, oder ähnlich auf Virtuellen Maschinen bereitgestellt.

Software as a Service (SaaS)

Mit SaaS wird dem Endkunden ein dediziertes Softwareprodukt wie zum Beispiel MongoDB, PostgreSQL, NGINX, Wordpress, etc. bereitgestellt.

Übersicht Cloud-service Modelle



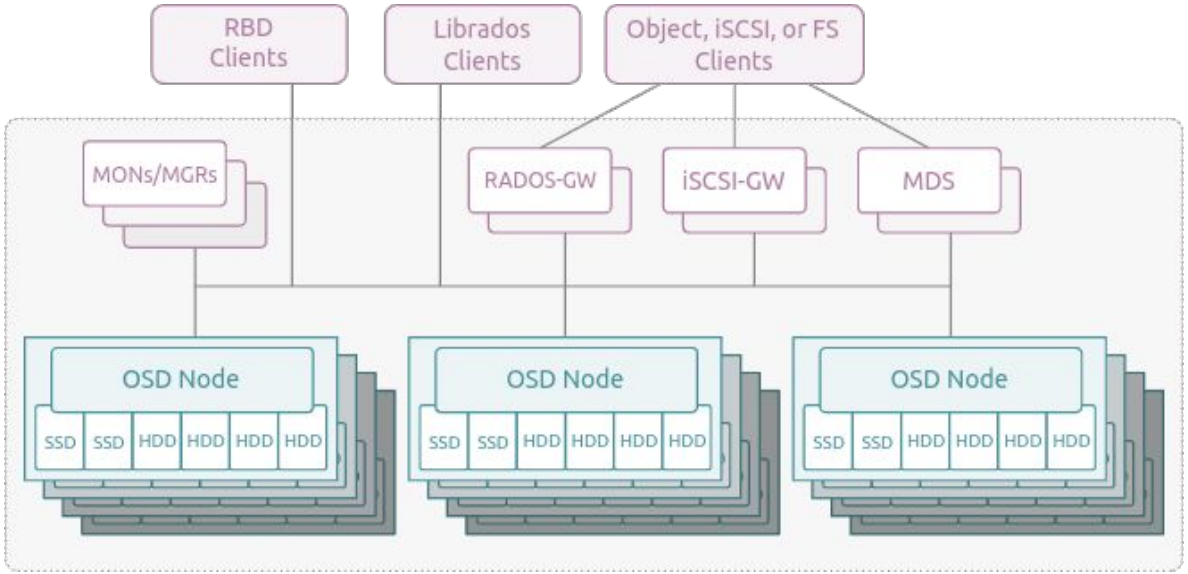

CLOUD
&HEAT

GRUNDLAGEN CEPH STORAGE

What is Ceph?

Maintenance

Ceph is an open source software-defined storage solution designed to address the block, file and object storage needs of modern enterprises. Its highly scalable architecture sees it being adopted as the new norm for high-growth block storage, object stores, and data lakes. Ceph provides reliable and scalable storage while keeping CAPEX and OPEX costs in line with underlying commodity hardware prices.



ON-PREMISE INFRASTRUKTUR

Was ist ein Cloud-service?

Services & Dienstleistungen

Infrastructure as a Service (IaaS)

Mit IaaS werden dem Endkunden in der Regel Virtuelle Maschinen, Snapshots sowie Backups über einen Selfservice bereitgestellt.

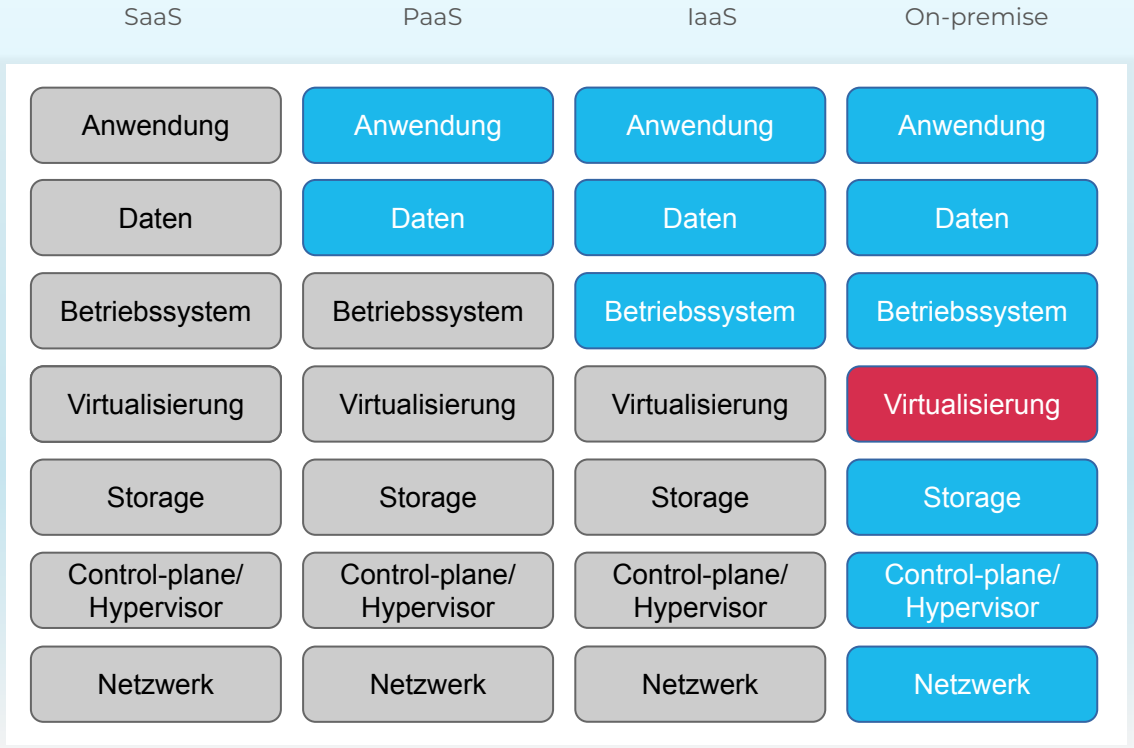
Platform as a Service (PaaS)

Mit PaaS wird dem Endkunden eine Plattform wie zum Beispiel Kubernetes, OpenShift, oder ähnlich auf Virtuellen Maschinen bereitgestellt.

Software as a Service (SaaS)

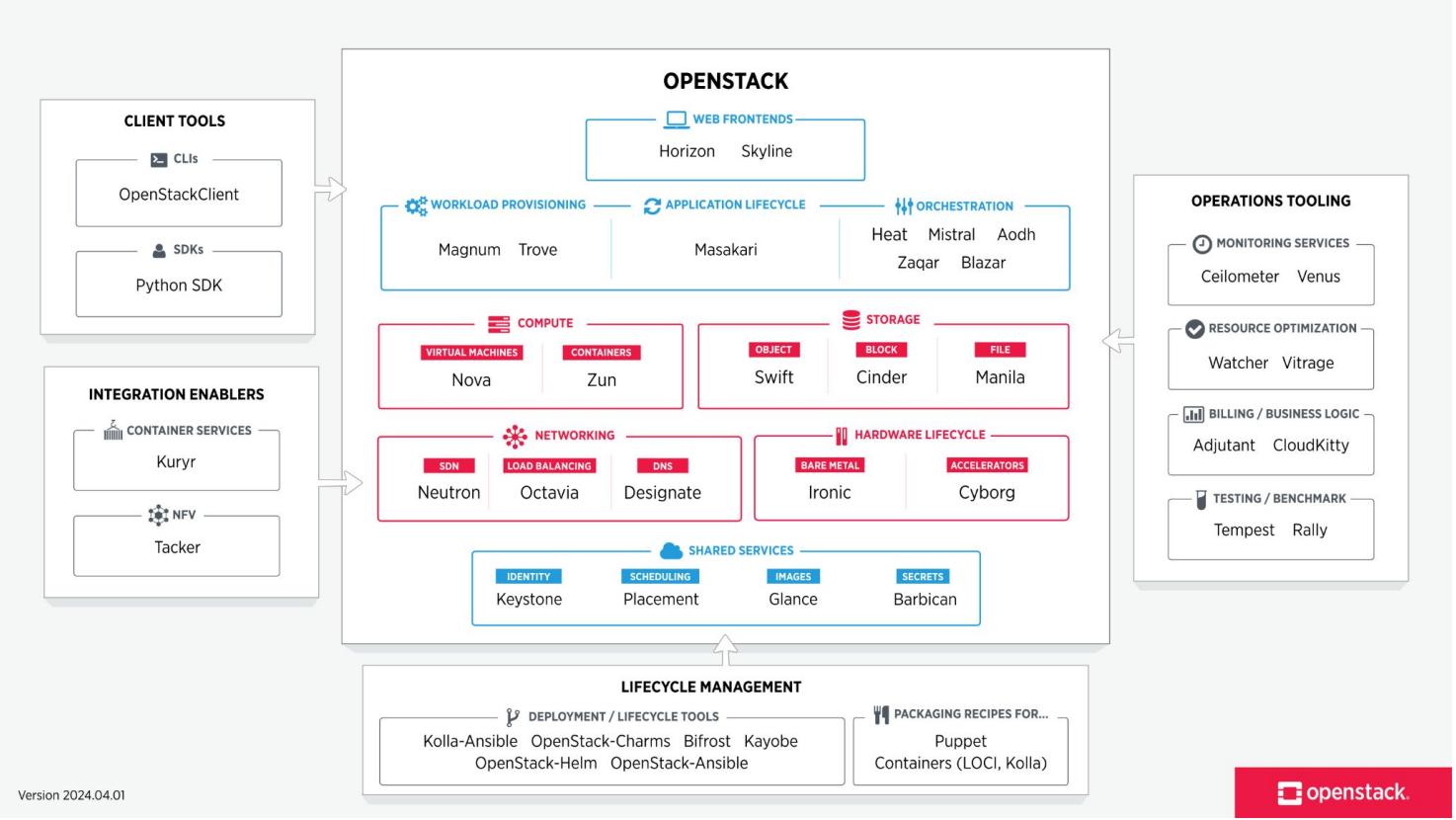
Mit SaaS wird dem Endkunden ein dediziertes Softwareprodukt wie zum Beispiel MongoDB, PostgreSQL, NGINX, Wordpress, etc. bereitgestellt.

Übersicht Cloud-service Modelle



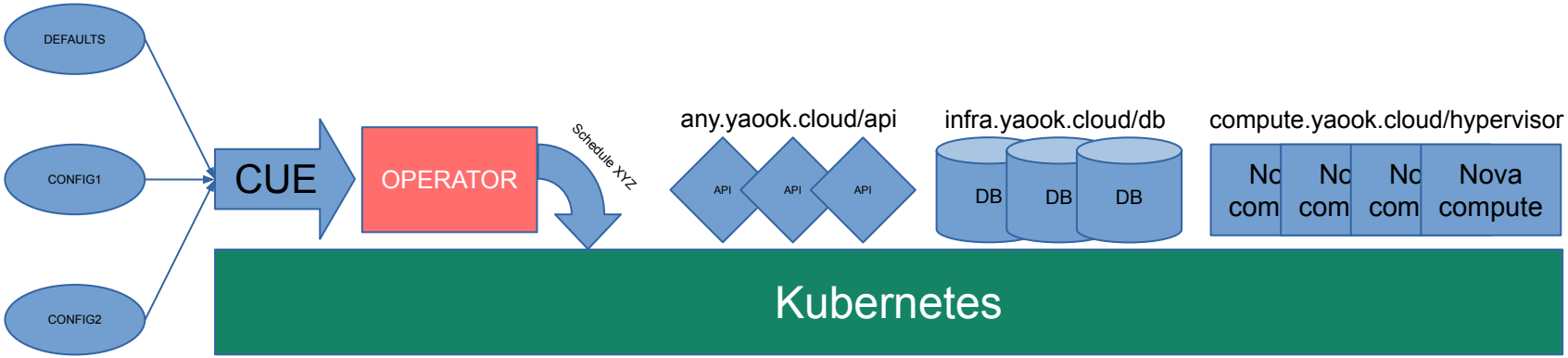

CLOUD
&HEAT
Lenovo

OPENSTACK DIENSTE



YAOOK OPENSTACK OPERATORS

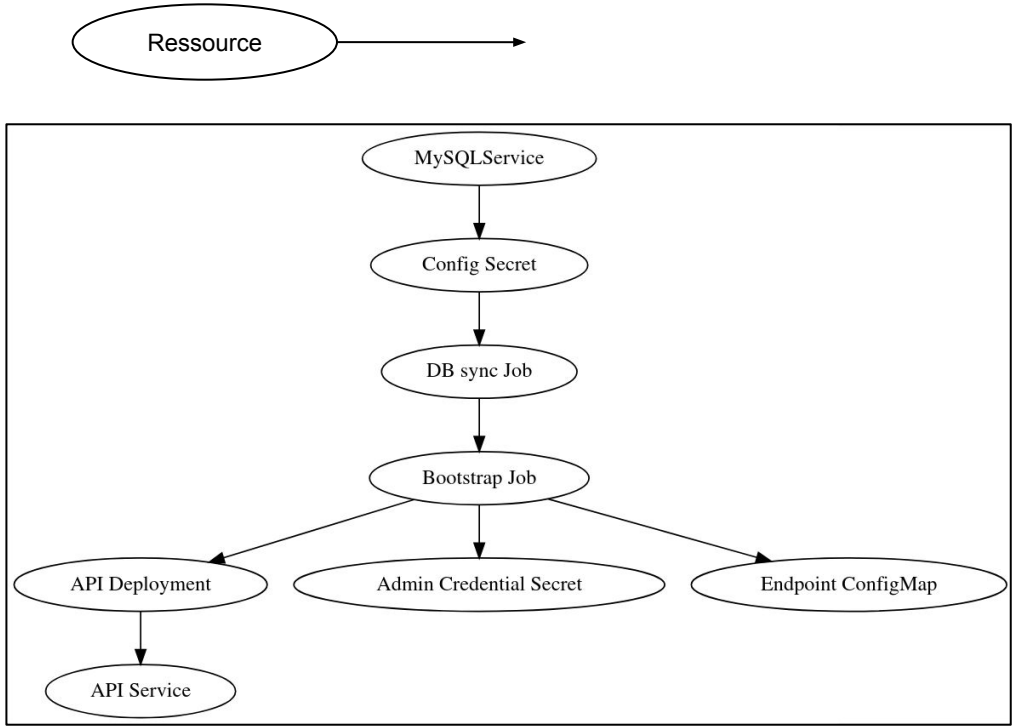
- Was ist YAOOK OpenStack?
  - Konfigurationsmanagement für OpenStack auf Kubernetes (TAROOK)
  - Übernimmt repetitive, automatisierbare Tasks und überlässt dem User wichtige **Entscheidungen und Deklarationen**
  - Nutzt das Operator-Prinzip (state-machines)
  - Macht sich Kubernetes housekeeping und scheduling zu Nutze



YAOOK OPENSTACK KEYSTONE OPERATOR

- Keystone Operator Komponentengraph (vereinfacht)
  - Verwaltet Ressourcen
  - Respektiert Abhängigkeiten

- Keystone benötigt:
  1) Datenbank mit Zugangsdaten (keystone-config) um db_sync auszuführen
- 2) Ersteinrichtung der Keystone DB
  3) Ersteinrichtung Keystone API
  4) Erstellung Keystone admin-User
  5) Erstellung einer Konfig für die Verbindung zum Keystone Dienst
  6) Kubernetes-Service (k8s) zur Bereitstellung der API



DAY 2 OPERATIONS: HINZUFÜGEN VON HOSTS

1) Wareneingang
   - Scriptgestützte Inventarisierung per Redfish API

2) Einbau und Verkabelung
   - Hier passieren die meisten Fehler! Node bootet nicht per PXE? Node hat kein Internet? Node ist nicht per IPMI erreichbar? Obskure Fehlermeldung die sich niemand erklären kann?

4) Switchkonfiguration
   - Viele Variablen im Projektkontext: VLANS, LACP/Port-channel, DHCP Relay, Multicast, Layer2 / Layer3

5) State-machine im YMC erkennt neuen Host (Geräteklassen werden anhand Inventarisierung erkannt)
   - Automatische Eintragung in Netbox, start Provisionierung wahlweise automatisch / per Bestätigung

6) Ironic bootet neuen Host per iPXE (ironic-python-agent)

7) Ironic provisioniert Betriebssystem per iPXE

8) State-machine integriert neuen Host in das Kubernetes Cluster mit korrekten Labels
   - Aktuell noch Ansible mit manuellem Start, bei großen Deployments automatisch per Pipeline.

DAY 2 OPERATIONS: CLUSTER MANAGEMENT

YAOOKCTL

- Abkürzung **mit autocomplete** für komplexe Operationen wie z.B.:
- „find me the cell1 database of my Nova deployment and get me a privileged SQL shell“
  → *yaookctl sql nova cell1_db*

  „get me a stream of the merged logs of all Keystone API pods, JSON-decoded, include last 200 lines“
  → *yaookctl logs keystone api –tail=200*
- „stop reconciling keystone databases until the maintenance is finished“
  → *yaookctl pause mysql keystone –comment „were doing XYZ“*
- „rebuild a database from replica 2 after an outage“
  → *yaookctl galera force-bootstrap keystone 2*

DAY 2 OPERATIONS: TAINTS & LABELS

- **Control Plane**
- any.yaook.cloud/api
- infra.yaook.cloud/any
- operator.yaook.cloud/any
- key-manager.yaook.cloud/barbican-any-service
- block-storage.yaook.cloud/cinder-any-service
- …

- **Layer3 Gateway Nodes**
- network.yaook.cloud/neutron-ovn-agent
- network.yaook.cloud/neutron-ovn-bpg-agent

- **Hypervisors**
- compute.yaook.cloud/hypervisor

ON-PREMISE INFRASTRUKTUR

Was ist ein Cloud-service?

Services & Dienstleistungen

Infrastructure as a Service (IaaS)

Mit IaaS werden dem Endkunden in der Regel Virtuelle Maschinen, Snapshots sowie Backups über einen Selfservice bereitgestellt.

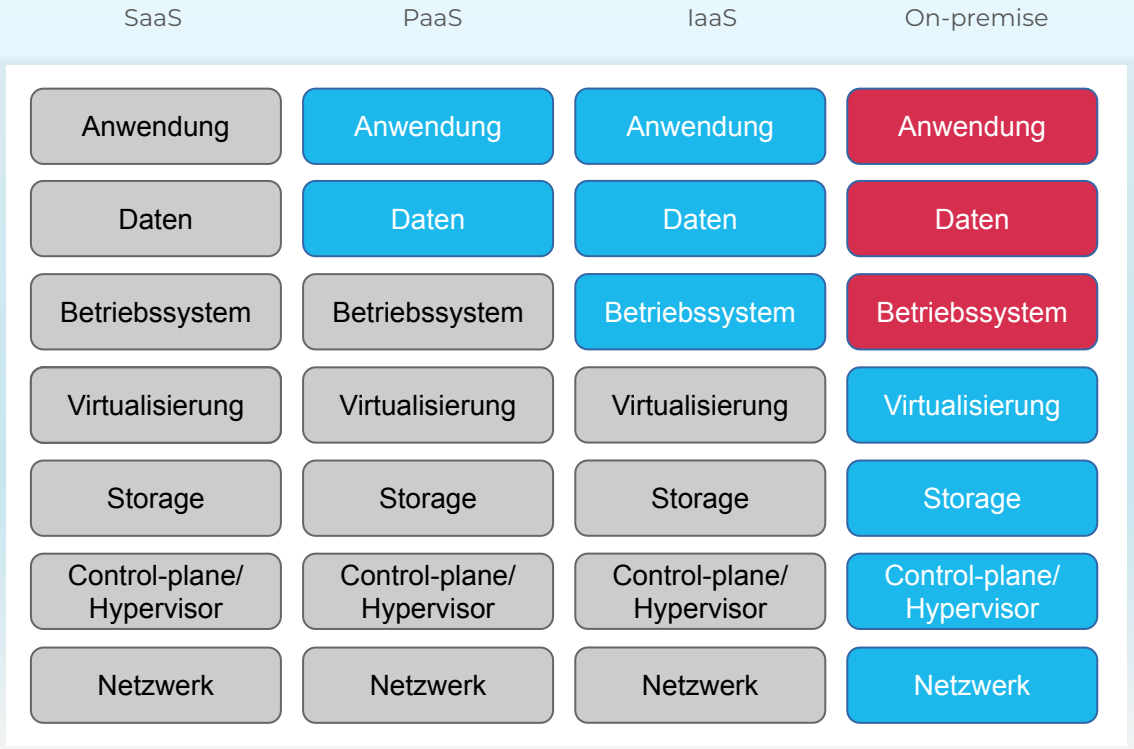
Platform as a Service (PaaS)

Mit PaaS wird dem Endkunden eine Plattform wie zum Beispiel Kubernetes, OpenShift, oder ähnlich auf Virtuellen Maschinen bereitgestellt.

Software as a Service (SaaS)

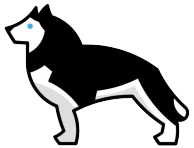
Mit SaaS wird dem Endkunden ein dediziertes Softwareprodukt wie zum Beispiel MongoDB, PostgreSQL, NGINX, Wordpress, etc. bereitgestellt.

Übersicht Cloud-service Modelle




CLOUD
&HEAT

PLATFORM AS A SERVICE MIT TAROOK



1) Was ist TAROOK?
   - Ein Ansible-basiertes life-cycle-management System für Kubernetes auf der Basis von Virtualisierung
   - Arbeitet mit Terraform auf OpenStack-Clouds
   - Transparente Handhabung von Kubernetes-Upgrades

   - Hat bereits viele Services mit integriert
     - Monitoring (kube-prometheus-stack)
     - Hashicorp Vault secret manager
     - Etcd / Vault backups
     - Keepalived (HA)
     - Provides LoadBalancers, Ingresses, StorageClasses, Certificates ...and many more

Bewirb Dich und stärke die digitale Souveränität mit Deinem Know-how. CLOUD&HEAT hat ein Jahrzehnt Erfahrung im nachhaltigen Cloud-Betrieb – auf unserer Infrastruktur in unseren Rechenzentren in Frankfurt a. M. und Dresden sowie on-premise.

info@cloudandheat.com

www.cloudandheat.com/karriere/

Kontakt

Zeitenströmung – Halle 15
Königsbrücker Straße 96
01099 Dresden, Germany

info@cloudandheat.com
+49 351 479 367 0

Unsere Webseite

Erfahren Sie mehr