MEROS CLOUD

Markus [redacted] markus@meros.one

Yannic [redacted] yannic@meros.one

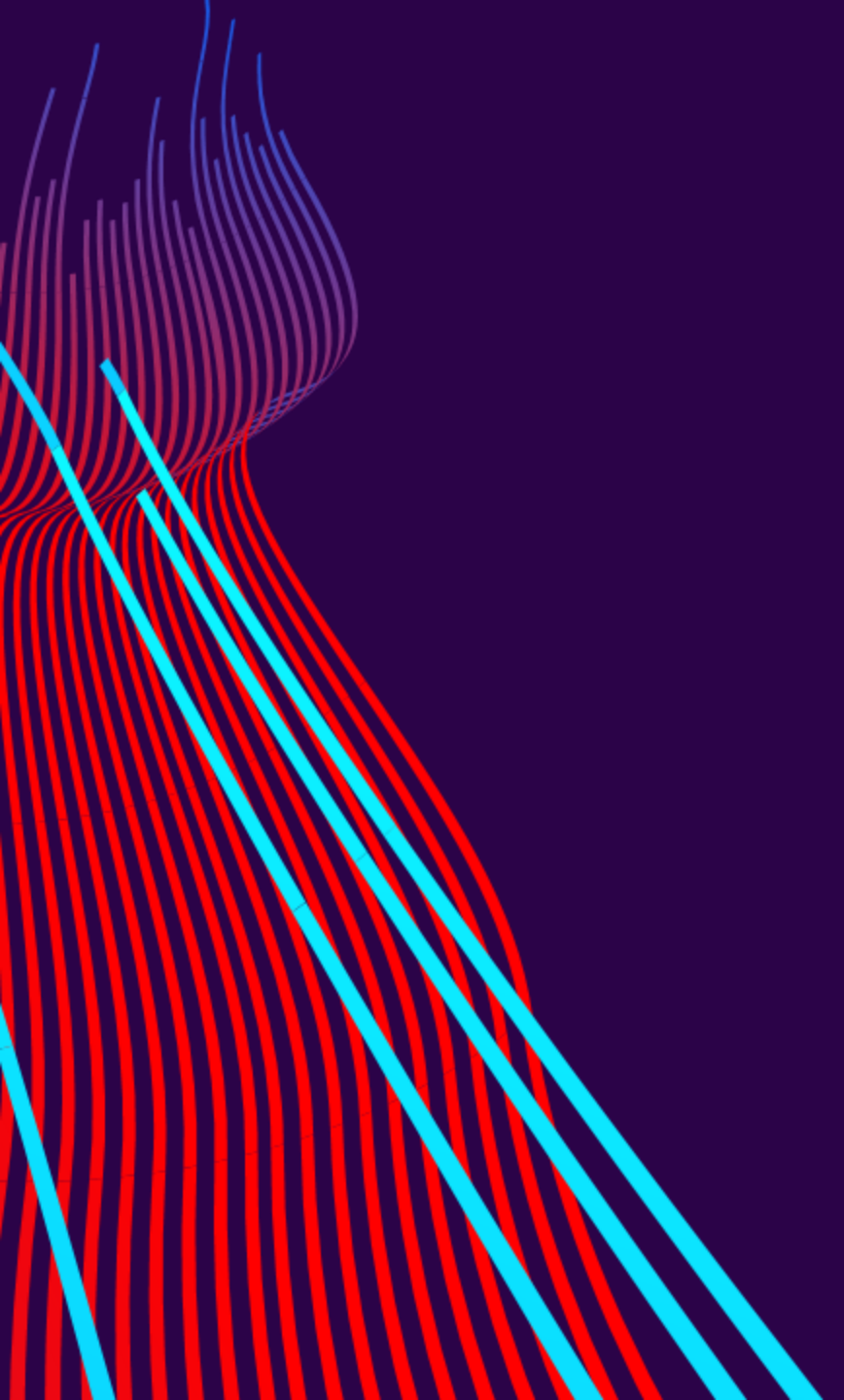
ÜBER UNS

- Markus:
  - Ausbildung zum FISI
  - Alter: 23
  - Schwerpunkte: Infrastruktur und Entwicklung

  BackInBash

- Yannic:
  - Ausbildung zum FISI
  - Alter: 25
  - Schwerpunkte: Infrastruktur und Netzwerk

  Rub-i



AGENDA

Einführung

- Motivation
- Vorbereitung
- Planung

Basis Infrastruktur

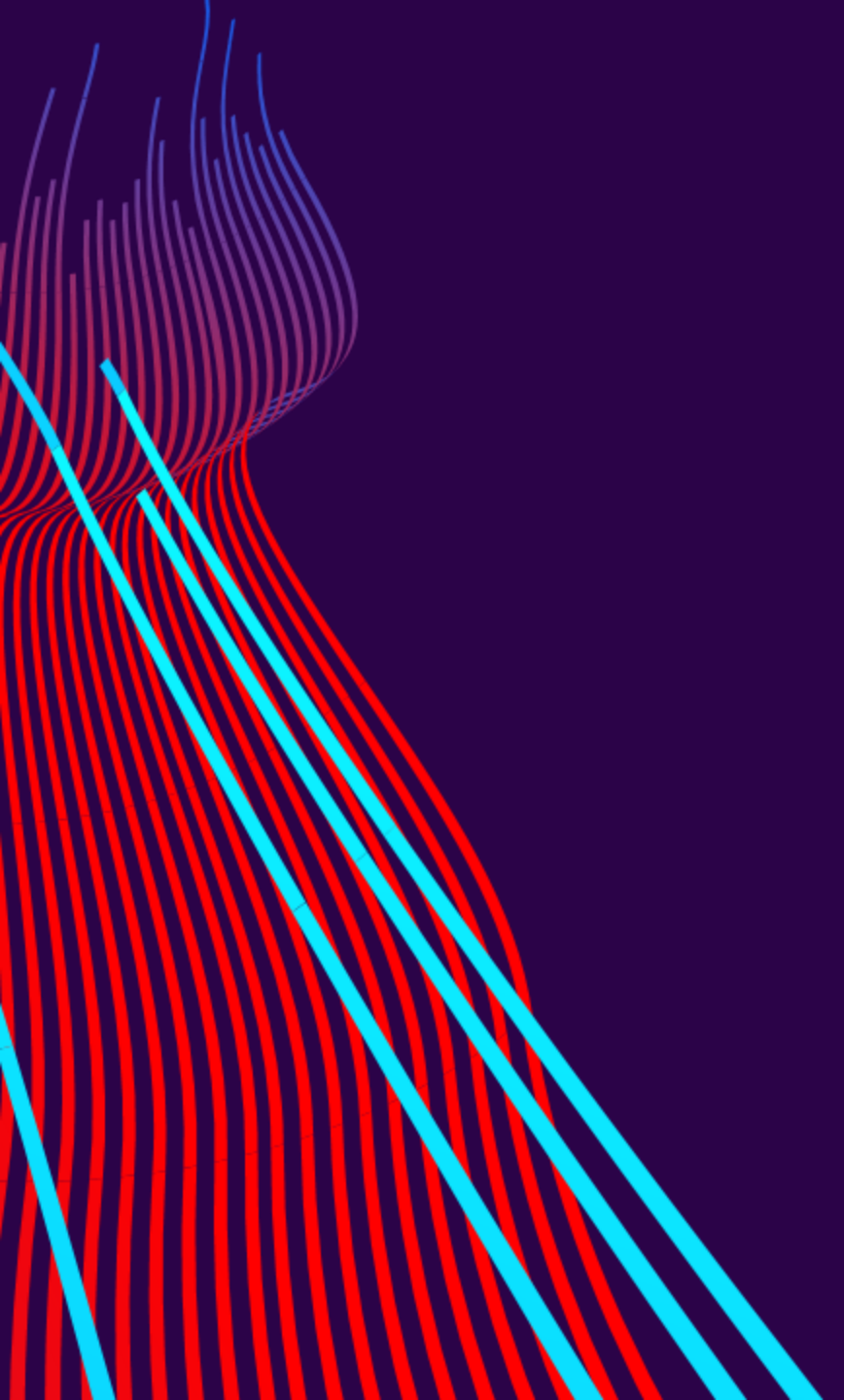
- Rechenzentrum
- Netzwerk
- Hardware
- Firewall
- Monitoring

Cloud Infrastruktur

- Public Key Infrastruktur
- OpenStack
- Open vSwitch (SDN)
- OS Images

Aktuelle Lage

- Ist-Zustand
- Learnings
- Fazit



MOTIVATION

CLOUD

- Individuelles Angebot
- CLOUD Made in Germany
- Alternative zu großen Anbietern

IaaS

- Geringe Latenz
- Hohe Verfügbarkeit
- Kostenersparniss

Technologieren

- Neue Technologien
- Machbarkeit

MSP

- Managed Services
- Neues Produktprotfolio

VORBEREITUNG

Welches Rechenzentrum?

Welche Hardware?

Welche Software?

Kostenberechnung

PLANUNG

Beschaffung Hardware

- Kauf von Hardware
- Spenden
- Zuschüsse

Installation

- Einbau
- Konfiguration Vorort

IPAM

- Vergabe von IP Adressen
- Zukauf von Adressen

Konfiguration

- Erstellung von Plänen
- Planung von Konzepten

ÜBERSICHT

Rechenzentrum

nepustil.net

Netzwerk

MikroTik

Hardware

Hewlett Packard Enterprise

Firewall

SOPHOS

Monitoring

ICINGA

RECHENZENTRUM

- Rechenzentrum RZz10a Stuttgart Zettachring
- Aktuell 1Gbit Anbindung bis zu 100Gbit möglich
- Anbindung an den Stuttgarter Internet Exchange
- USV Anbindung möglich
- Wichtige Carrier und ISP‘s Vorort
- Redundante Anbindungen möglich

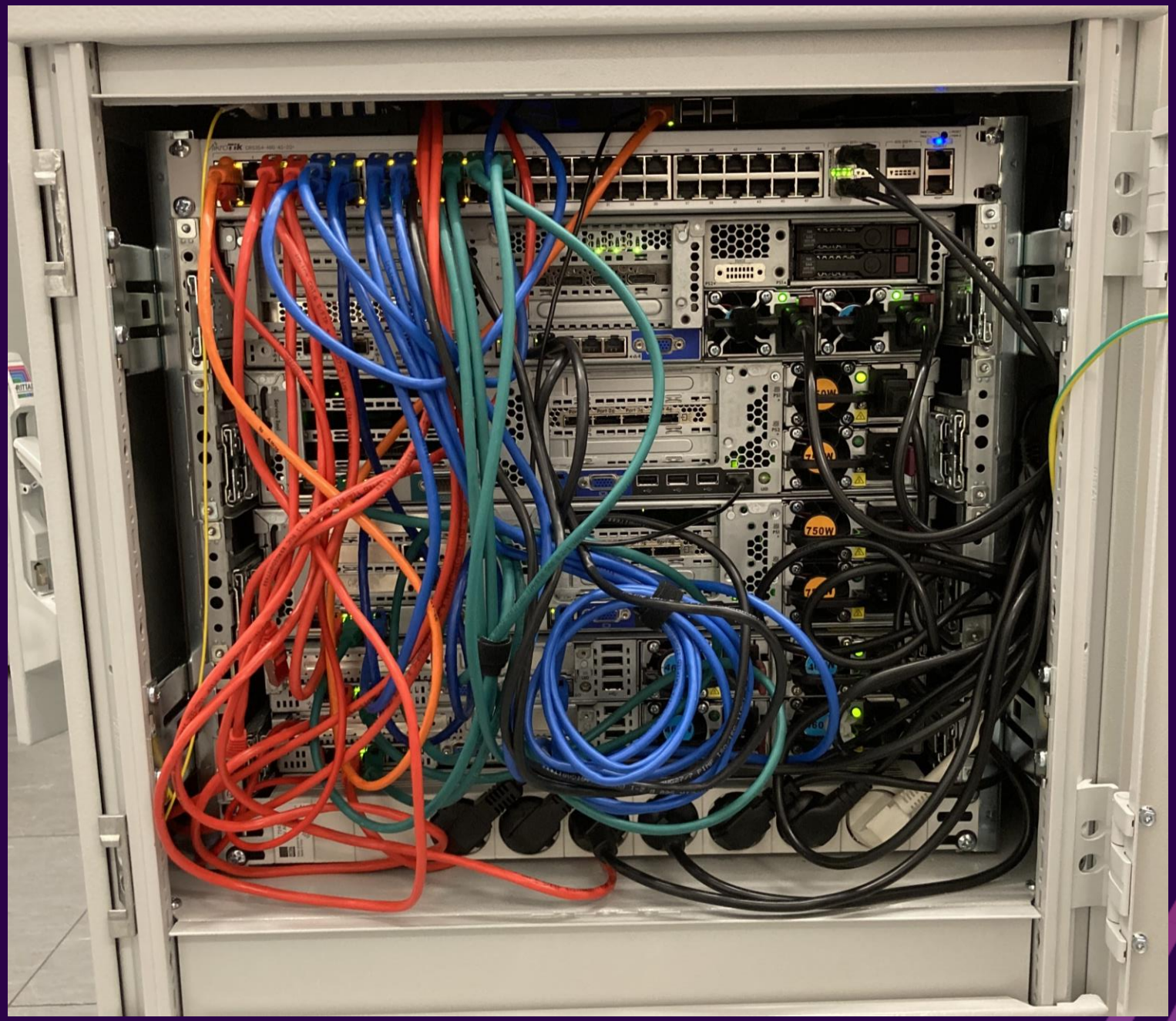
NETZWERK

- Farbige Kabel
- Mikrotik 48 Port Switch
- 10G zwischen Switch und Firewall
- Routing on a Stick

HARDWARE

- 2x Firewall als HA Cluster
- 1x Core Switch
- 2x HP ProLiant DL380 Gen8 Server
- 2x HP ProLiant DL360p Gen8 Server
- 1x Raspberry PI 3 für ein OOB Netz
- Netzwerkkabel und Rackmount Schienen

Ansicht:
Von Hinten




TECHNISCH
BEDENKLICH
1 2 3 4 5 6 7 8 9 10 11 12 22 23 24 25 26 27


NOTLÖSUNG
SEIT
1 2 3 4 5 6 7 8 9 10 11 12 22 23 24 25 26 27

MEROS CLOUD

Ansicht:
Von Vorn

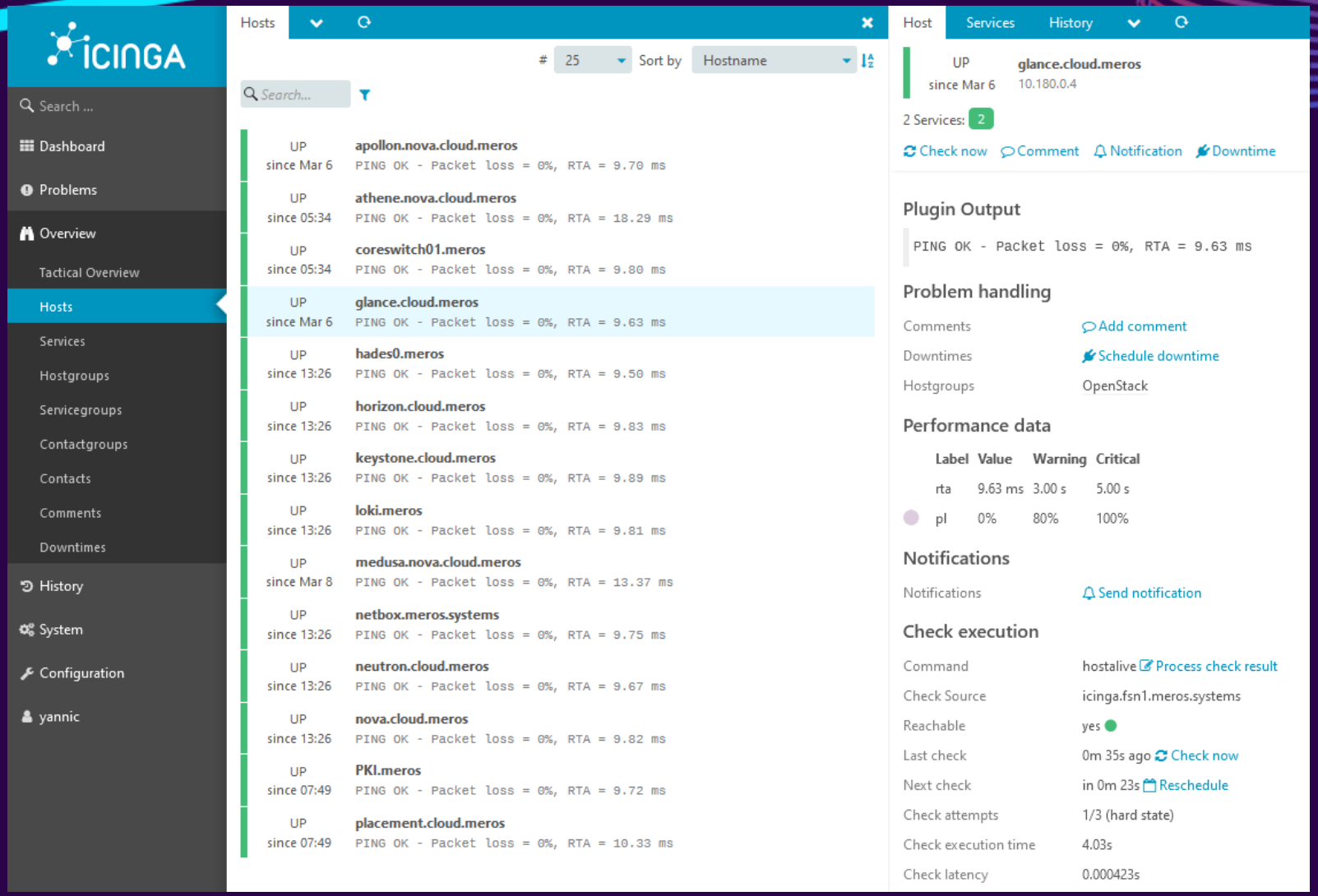
FIREWALL

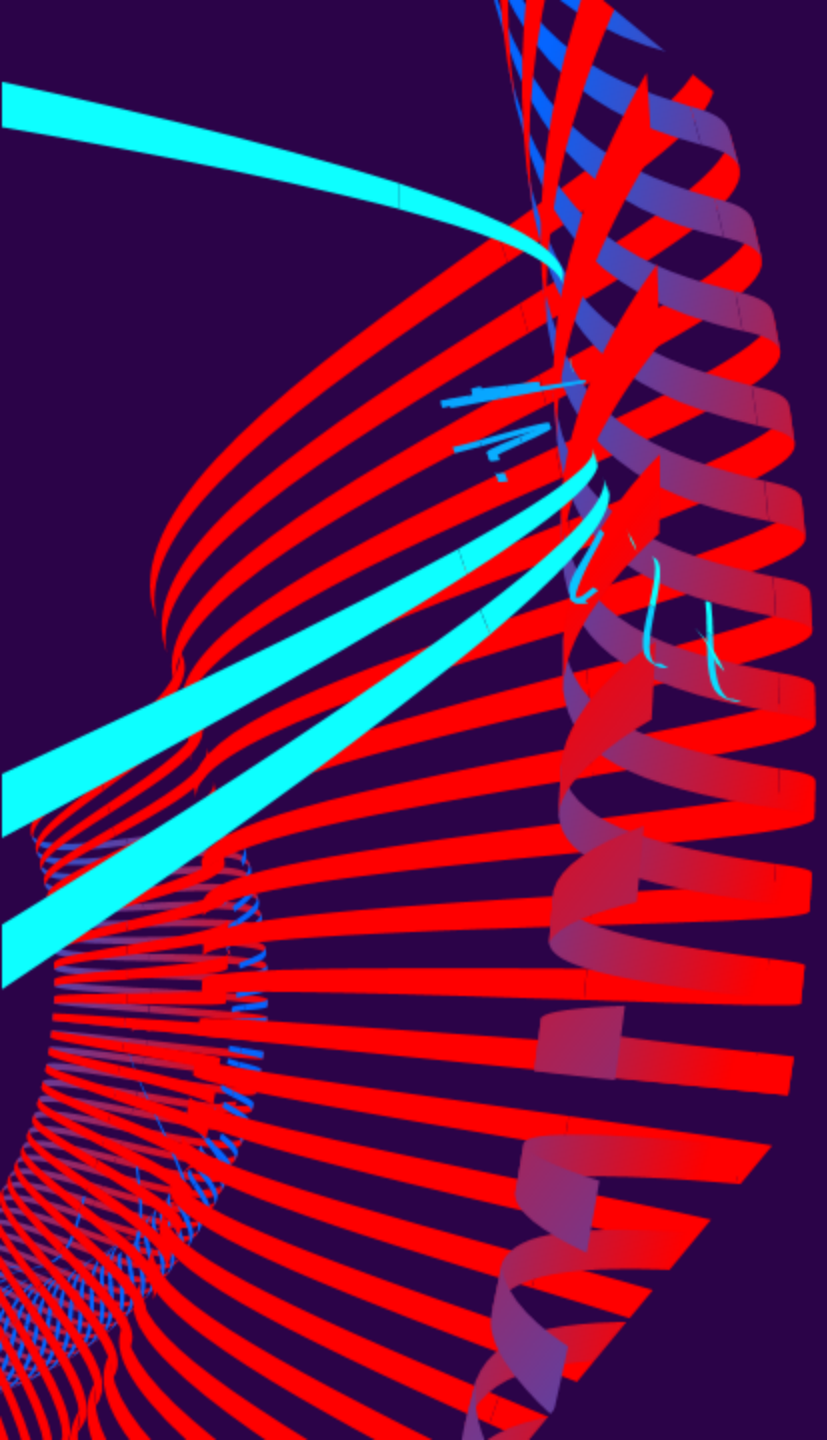
- SOPHOS UTM Version 9
- HA Cluster (Hochverfügbarkeit)
- 10GB Verkabelung
- Routing der Netze
- NAT, NTP, DNS Server
- Advanced Threat Protection und Portscan detection
- Web Application Firewall


Manchmal fehlt einem nur ein
kleines Teil, um glücklich zu sein.
Tabellenbuch
Metall

MONITORING

- Icinga2
- OpenSource
- Überwachung der gesamten Infrastruktur
- Informationen über Website oder App
- System befindet sich offsite in einen anderen RZ


ICINGA
Search ...
Dashboard
Problems
Overview
Tactical Overview
Hosts
Services
Hostgroups
Servicegroups
Contactgroups
Contacts
Comments
Downtimes
History
System
Configuration
yannic
Hosts
25
Sort by Hostname
Search...
UP since Mar 6 apollon.nova.cloud.meros PING OK - Packet loss = 0%, RTA = 9.70 ms
UP since 05:34 athene.nova.cloud.meros PING OK - Packet loss = 0%, RTA = 18.29 ms
UP since 05:34 coreswitch01.meros PING OK - Packet loss = 0%, RTA = 9.80 ms
UP since Mar 6 glance.cloud.meros PING OK - Packet loss = 0%, RTA = 9.63 ms
UP since 13:26 hades0.meros PING OK - Packet loss = 0%, RTA = 9.50 ms
UP since 13:26 horizon.cloud.meros PING OK - Packet loss = 0%, RTA = 9.83 ms
UP since 13:26 keystone.cloud.meros PING OK - Packet loss = 0%, RTA = 9.89 ms
UP since 13:26 loki.meros PING OK - Packet loss = 0%, RTA = 9.81 ms
UP since Mar 8 medusa.nova.cloud.meros PING OK - Packet loss = 0%, RTA = 13.37 ms
UP since 13:26 netbox.meros.systems PING OK - Packet loss = 0%, RTA = 9.75 ms
UP since 13:26 neutron.cloud.meros PING OK - Packet loss = 0%, RTA = 9.67 ms
UP since 13:26 nova.cloud.meros PING OK - Packet loss = 0%, RTA = 9.82 ms
UP since 07:49 PKI.meros PING OK - Packet loss = 0%, RTA = 9.72 ms
UP since 07:49 placement.cloud.meros PING OK - Packet loss = 0%, RTA = 10.33 ms
Host
Services
History
UP since Mar 6
glance.cloud.meros
10.180.0.4
2 Services: 2
Check now
Comment
Notification
Downtime
Plugin Output
PING OK - Packet loss = 0%, RTA = 9.63 ms
Problem handling
Comments
Add comment
Downtimes
Schedule downtime
Hostgroups
OpenStack
Performance data
Label Value Warning Critical
rta 9.63 ms 3.00 s 5.00 s
pl 0% 80% 100%
Notifications
Notifications
Send notification
Check execution
Command
hostalive
Process check result
Check Source
icinga.fsn1.meros.systems
Reachable
yes
Last check
0m 35s ago
Check now
Next check
in 0m 23s
Reschedule
Check attempts
1/3 (hard state)
Check execution time
4.03s
Check latency
0.000423s

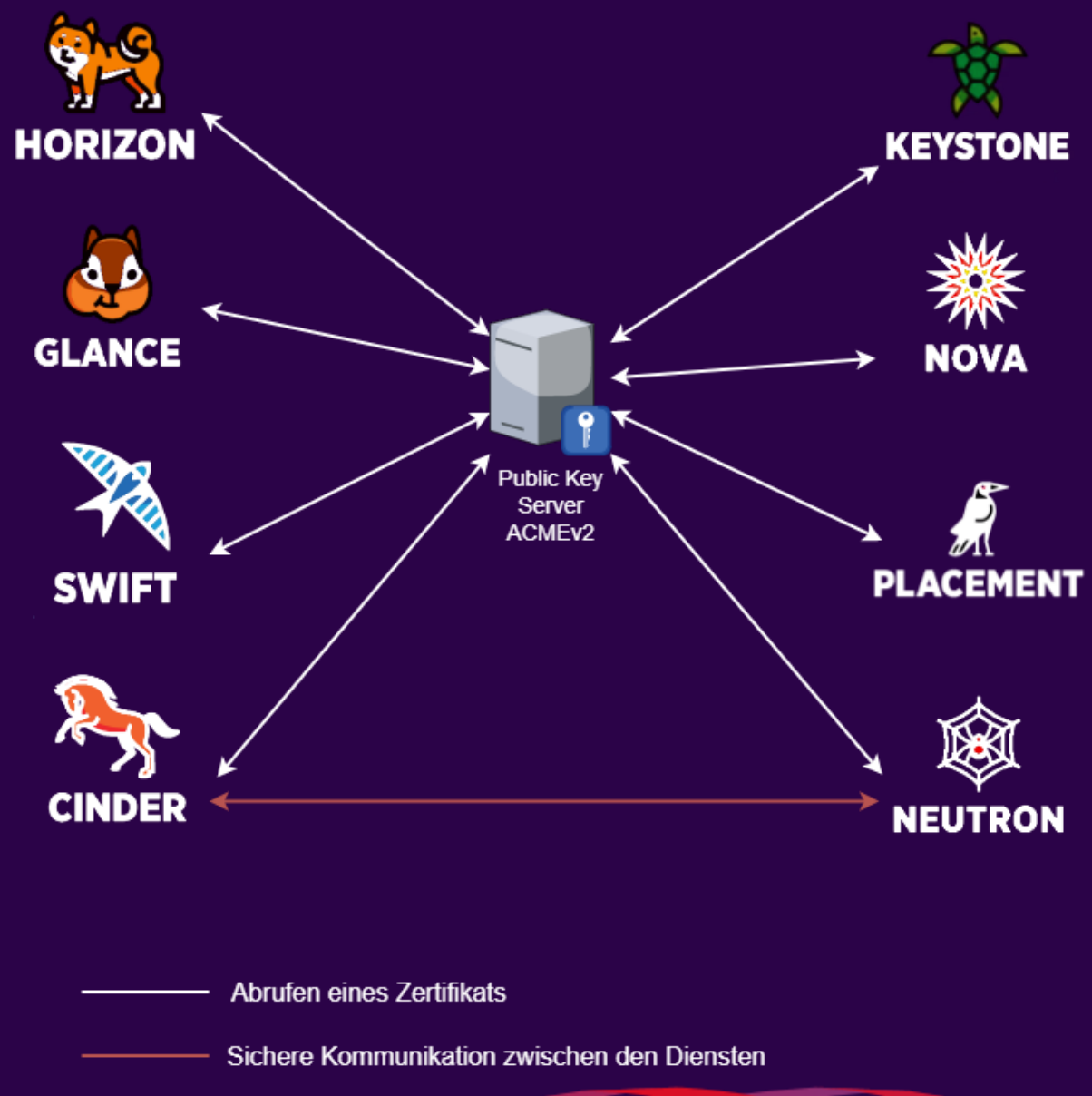


CLOUD INFRASTRUKTUR

PUBLIC KEY INFRASTRUKTUR

Smallstep CA

- Certbot Implementierung
- ACMEv2 Support
- Kurze Ablaufdauer

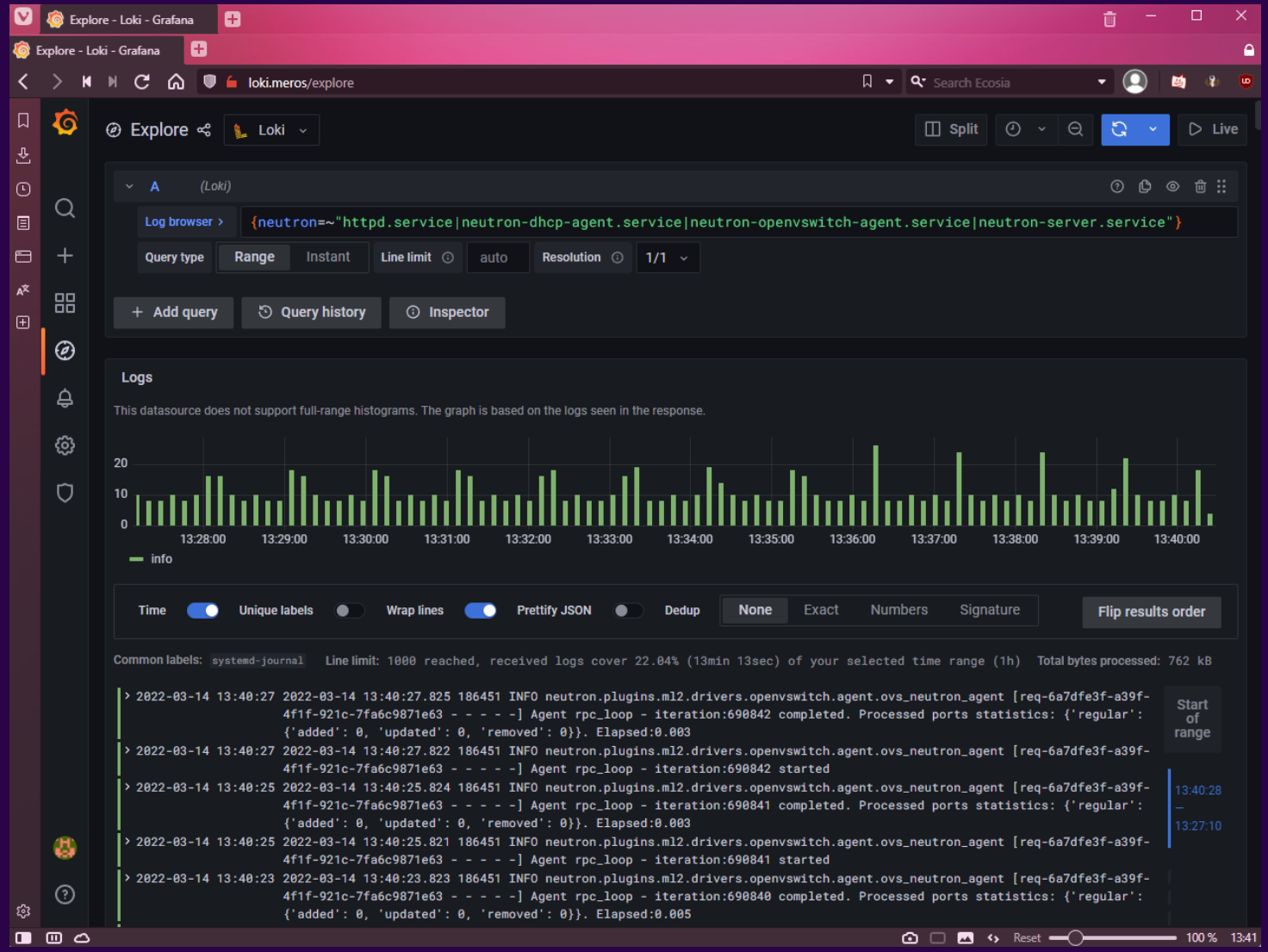


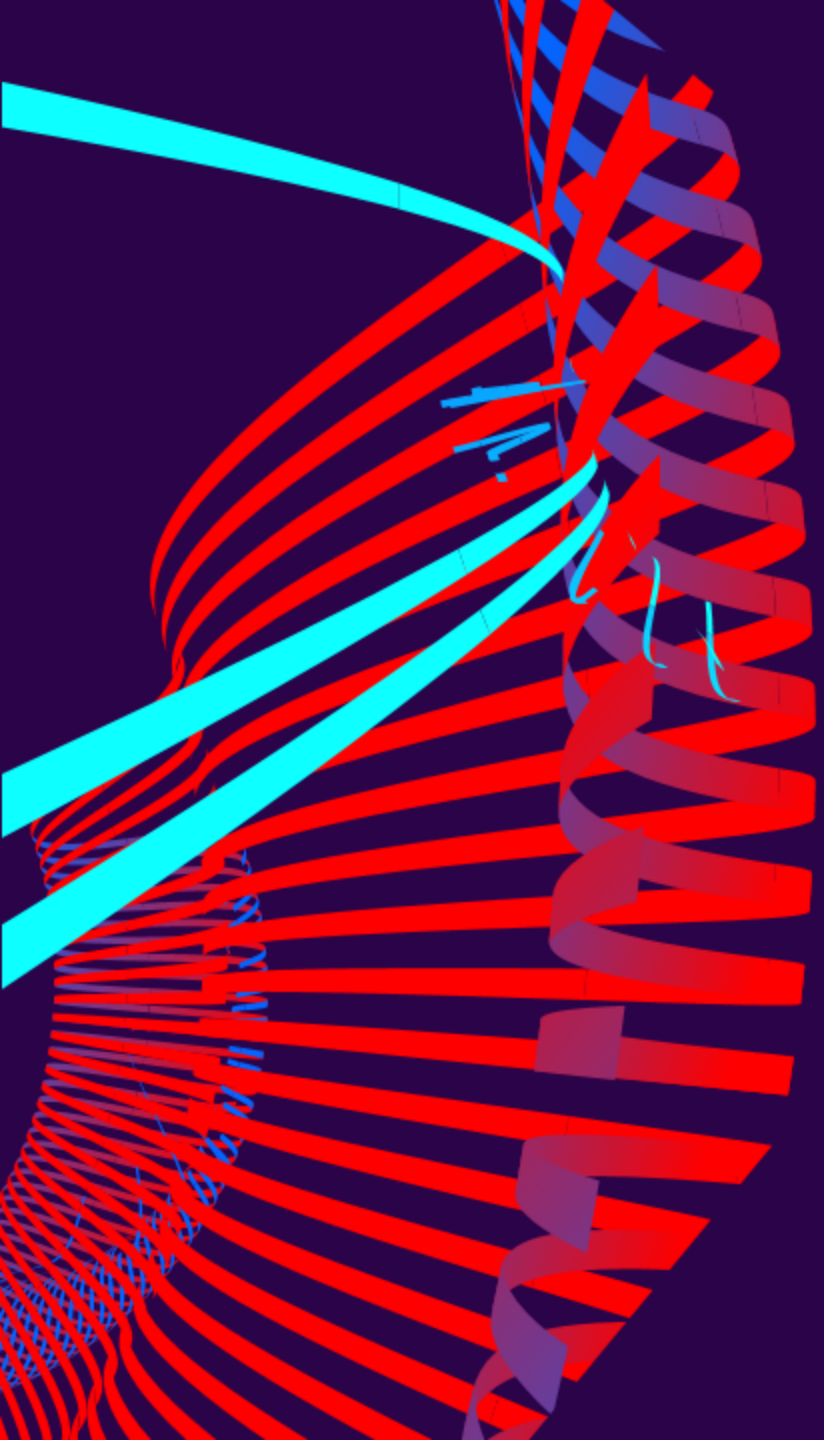
LOGSERVER

Grafana - Loki

- Promtail Client
- Syslog
- Systemd Journal

github.com/United-NetworX/loki-pkgs



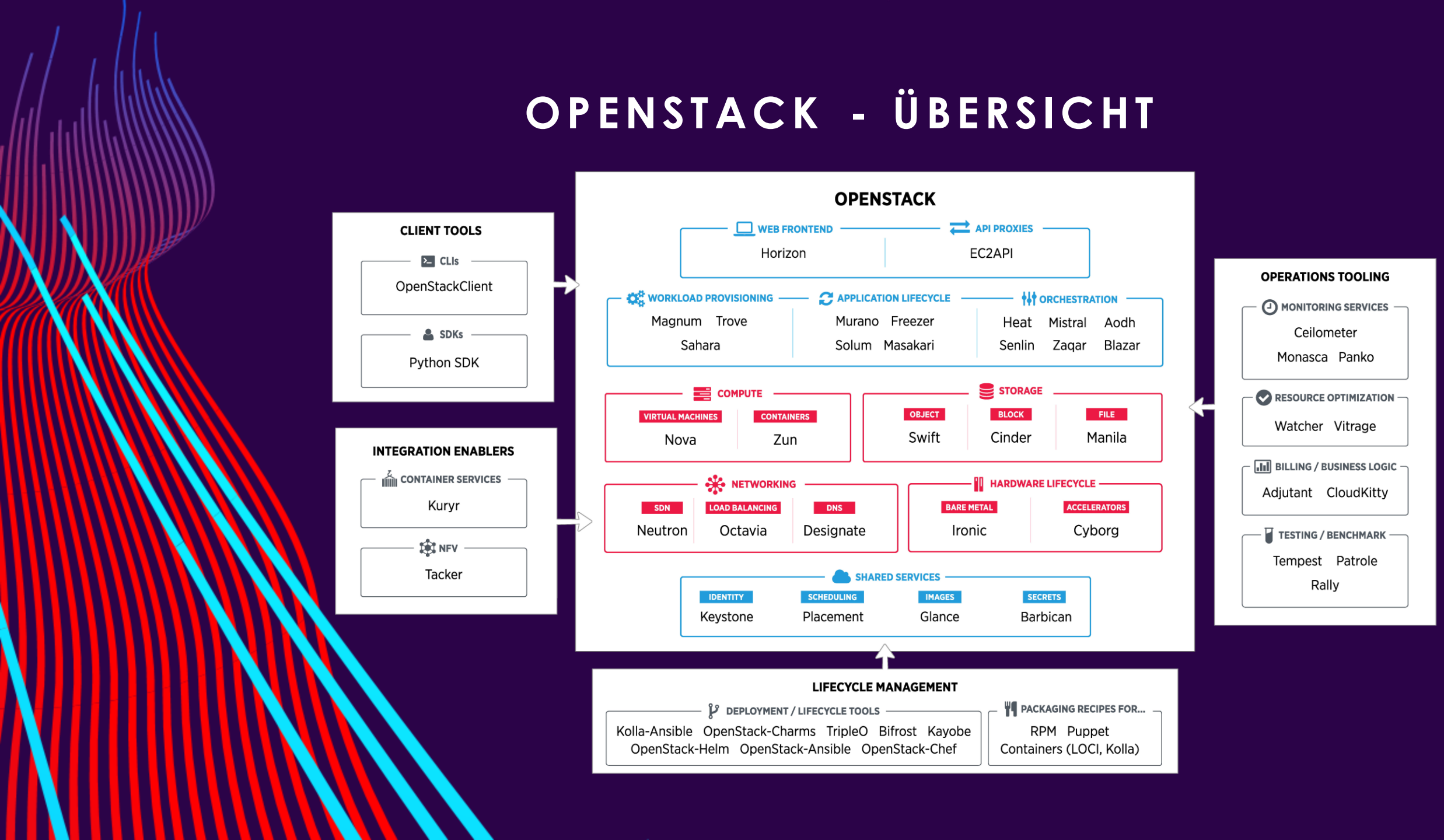


OPENSTACK

MEROS

CLOUD-PLATTFORM

OPENSTACK - ÜBERSICHT



KEYSTONE

Authentication

Authentifizierung aller OpenStack Services

Authorization

Zentrale Autorisierung aller OpenStack Services

Users

Internes Benutzermanagement

Groups

Internes Gruppenmanagement

GLANCE

Snapshots

- Snapshot Repository
- Nach Tenant getrennt

OS Images

- VM Template Images
  - Debian 10/11
  - Ubuntu 18 - 22.04
  - Almalinux 8
  - FreeBSD 13

External Storage

- Storage Providers
  - Swift
  - Cinder
  - S3
  - LVM

NOVA

Compute

- noVNC Web Proxy
- Hypervisor Management
- VM Inventory

Metadata

- Cloud Init Metadata
- Custom Value Store
- Hostname
- IP Konfiguration

Scheduler

- Ausgelagert in Placement
- Zuweisung von VMs
- Hostgruppen

Flavors

- VM Hardware:
  - CPU
  - RAM
  - Festplatte
  - Netzwerk

NEUTRON

DHCP-Agent

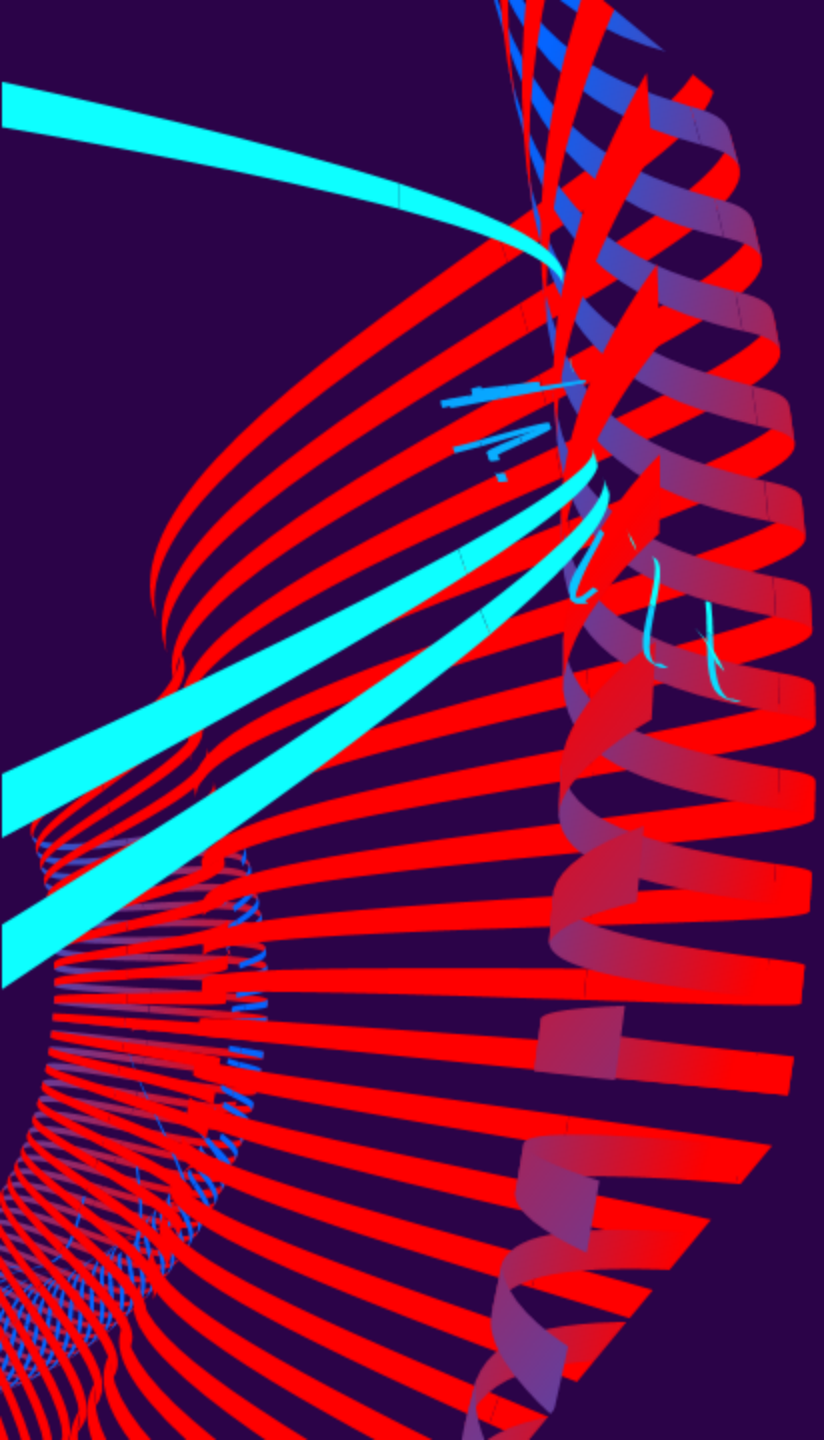
- Vergabe von öffentlichen und privaten Adressen

L3-Router

- Inter VLAN Routing für private Netzwerke
- Managed NAT/Border Router

SDN

- Open vSwitch
- Abstraktion auf L3 via VxLAN

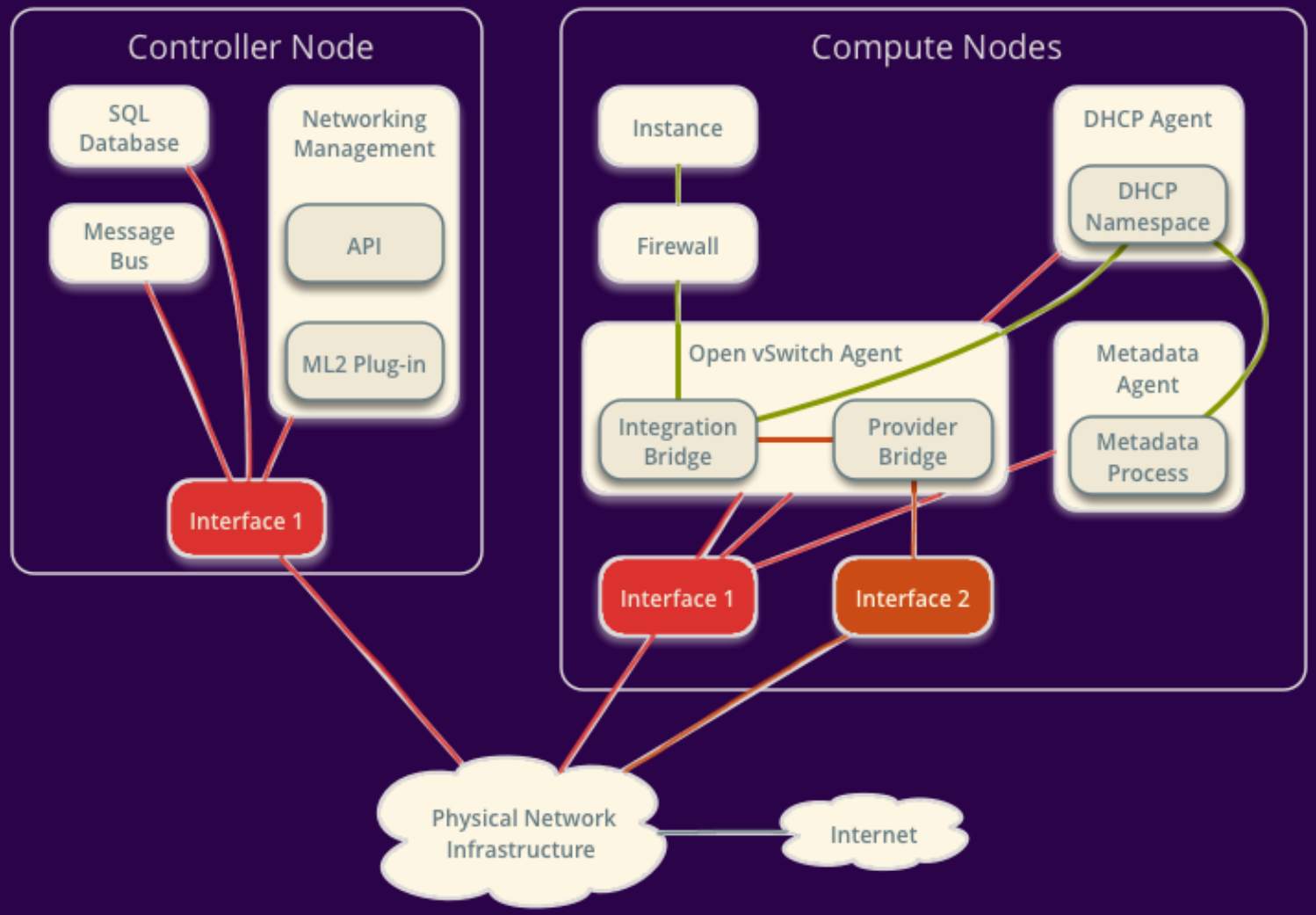


OvS

Open vSwitch

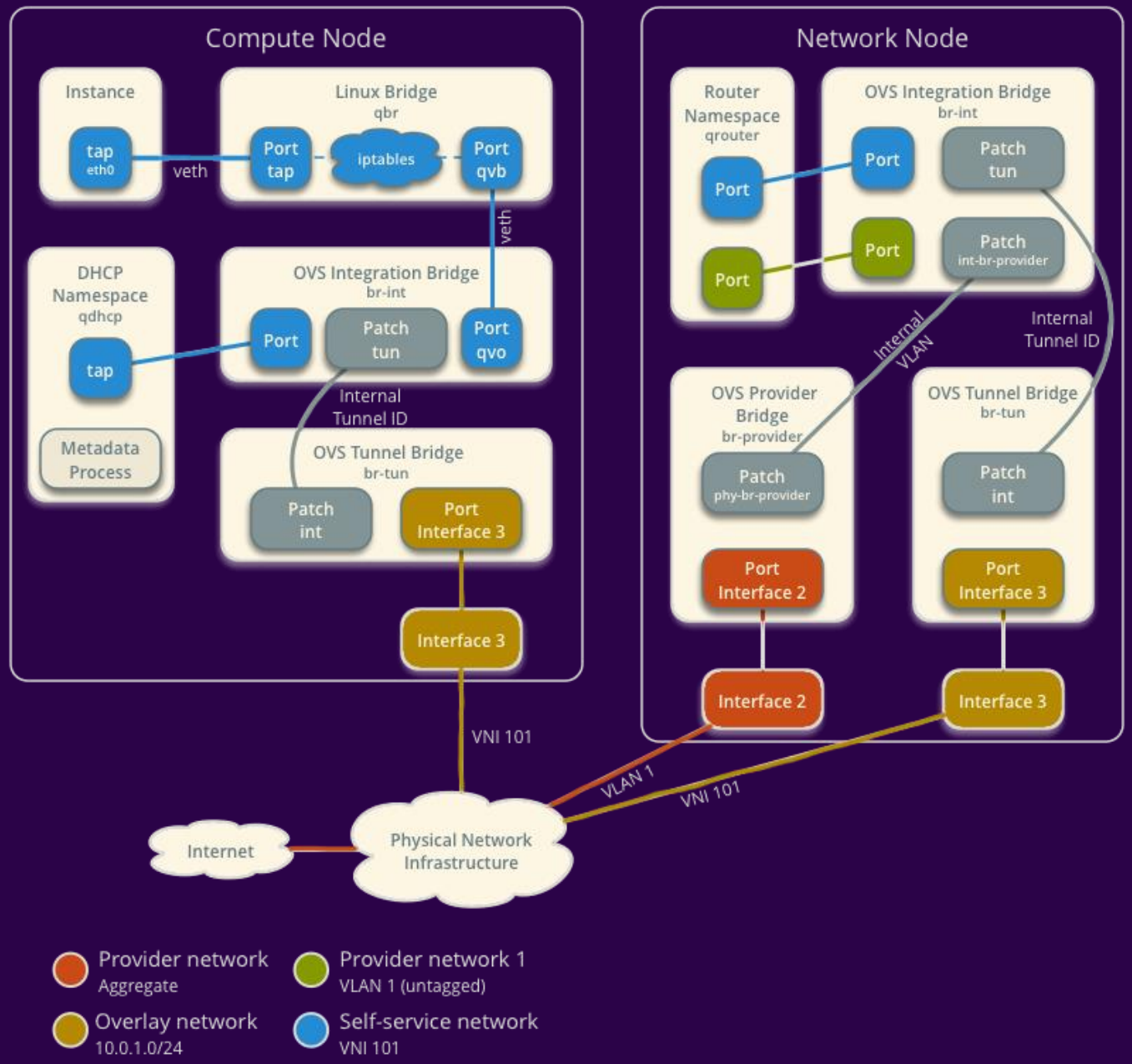
Open vSwitch - Provider Networks

Overview



Open vSwitch - Self-service Networks

Components and Connectivity



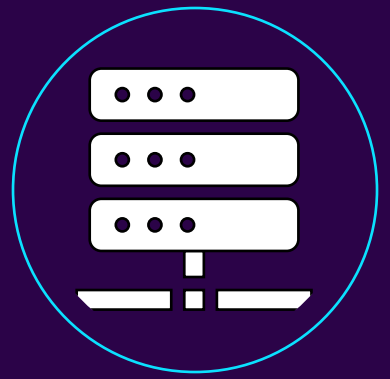
OS-IMAGES

- Packer
- DevSec Hardening
- GitHub Actions
- Linux / FreeBSD

github.com/United-NetworX/OpenStack-Images

MEROS
CLOUD-PLATTFORM

MSP



IAAS, PAAS, SAAS

KUBERNETES

PRIVATE CLOUD

FRAGEN?

Yannic [redacted]

Markus [redacted]

info@meros.one

www.meros.one

QUELLEN

- [1] Images - docs.openstack.org
- [2] Icons – openstack.org
- [3] Icons – openvswitch.org
- [4] Doku Technikerarbeit Meros Cloud
- [5] Icons – mikrotik.com
- [6] Icons – hpe.com
- [7] Icons – sophos.com
- [8] Icons – icinga.com
- [9] Icons – packer.io