BARIBAL STUDIOS

Netzwerkmanagement mit OPNsense, SDN und Proxmox

#2 Q&A

Agenda

1. Vorstellung
2. Rückschau
3. Q&A – Proxmox
4. Q&A - OPNsense
5. Fazit

Leistungen

BARIBAL STUDIOS

IT

Effizient und sicher arbeiten durch „state of the art"-Systeme nach deinem Bedarf.

- Open Source Lösungen (z. B.: Proxmox, Ceph, Kubernetes)
- IT-Architektur
- Aufbau und Implementierung
- Wartung und Pflege

Marketing

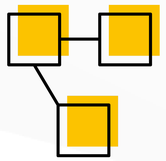
Aufmerksamkeit generieren über prägnante Kampagnen mit cross-medialem Charakter.

- Markenstrategie
- Kampagnen
- Content Creation
- SEO

Design

Wow-Faktor erleben mit hochwertigen Werbemitteln und Gestaltung nach Maß.

- Branding (Logo und Corporate Design)
- Werbemittel (Flyer, Anzeigen, Messestand etc.)
- Editorial Design (Broschüren, Magazine, etc.)
- UX/UI Design



Management

Komfortable Projekte genießen durch Koordination aus einer Hand.

- Projekt-Management
- Partner-Management
- Prozessanalyse
- Dokumentation

Referenzen

BARIBAL STUDIOS

Kunden

FAM

Alzheimer-Gesellschaft Brandenburg e.V.
Selbsthilfe Demenz

BÜROEXPRESS

Art Gourmet

Zimmerei | Dachdeckerei
Haberland Pechstein

Dachbau · Zimmerei · Service

BUNDESVEREINIGUNG
WIR HELFEN DENEN,
DIE HELFEN.

BÜRO PROFI

Kordes Gruppe

Partner

THOMAS KRENN®

h3ko Unternehmensgruppe

alfahosting
Powered by dogado

TOSHIBA

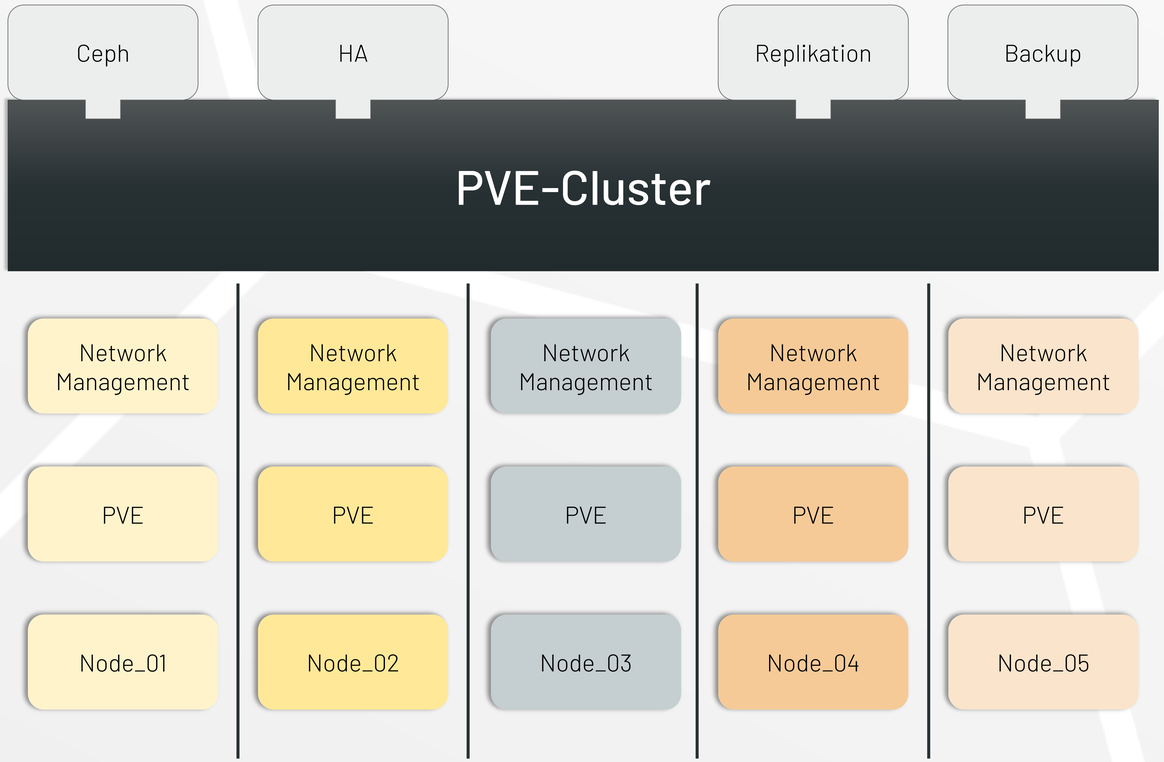
BARIBAL STUDIOS

Rückschau

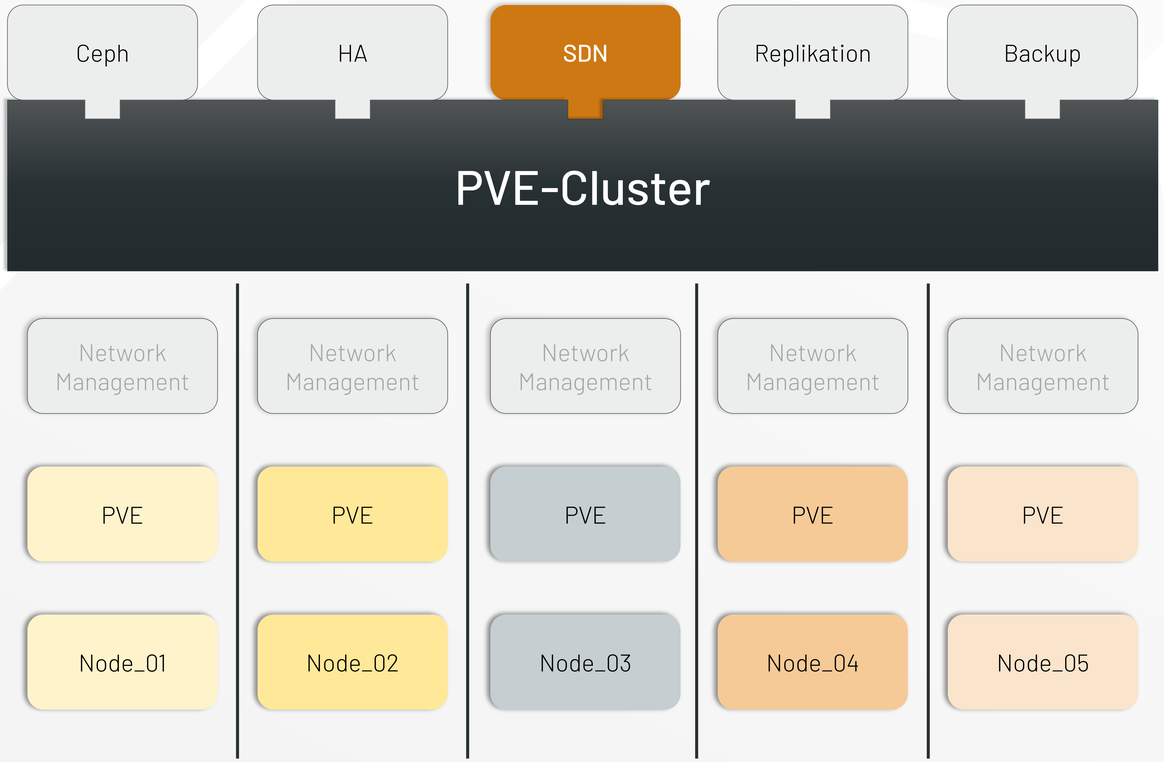
Proxmox VE & SDN

BARIBAL STUDIOS

PVE 7.x

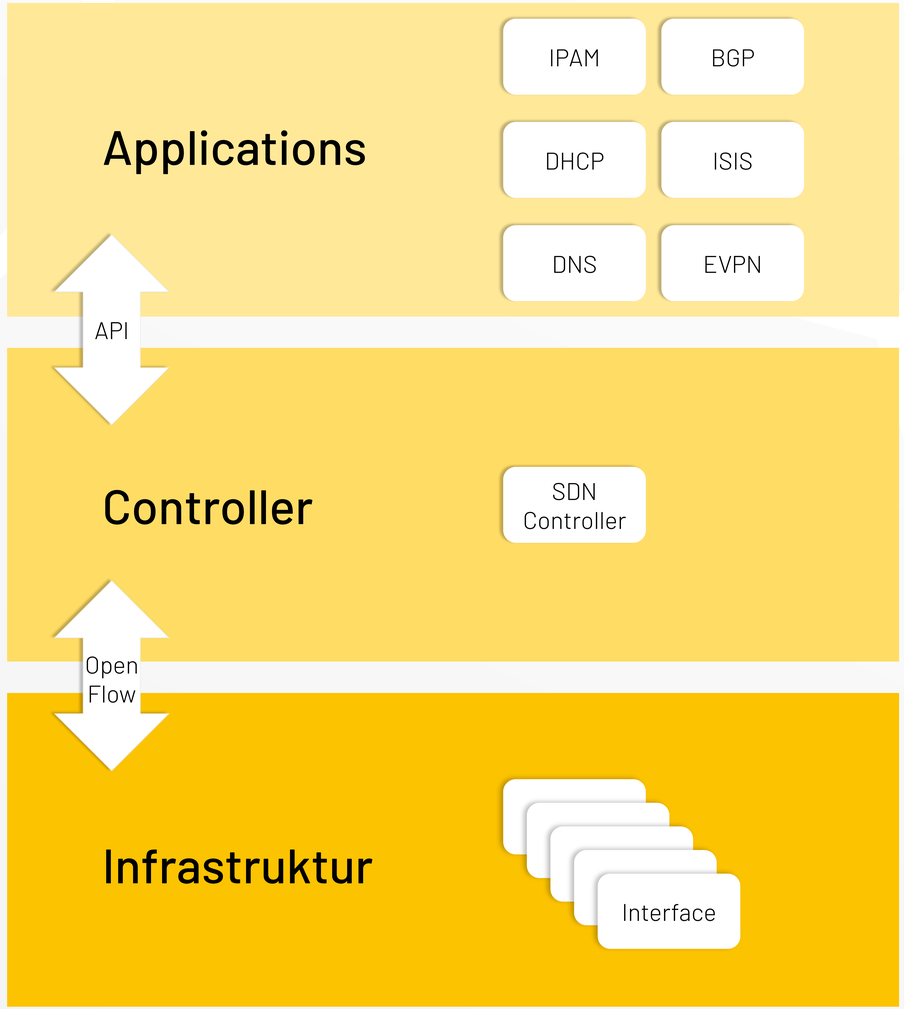


PVE 8.1+



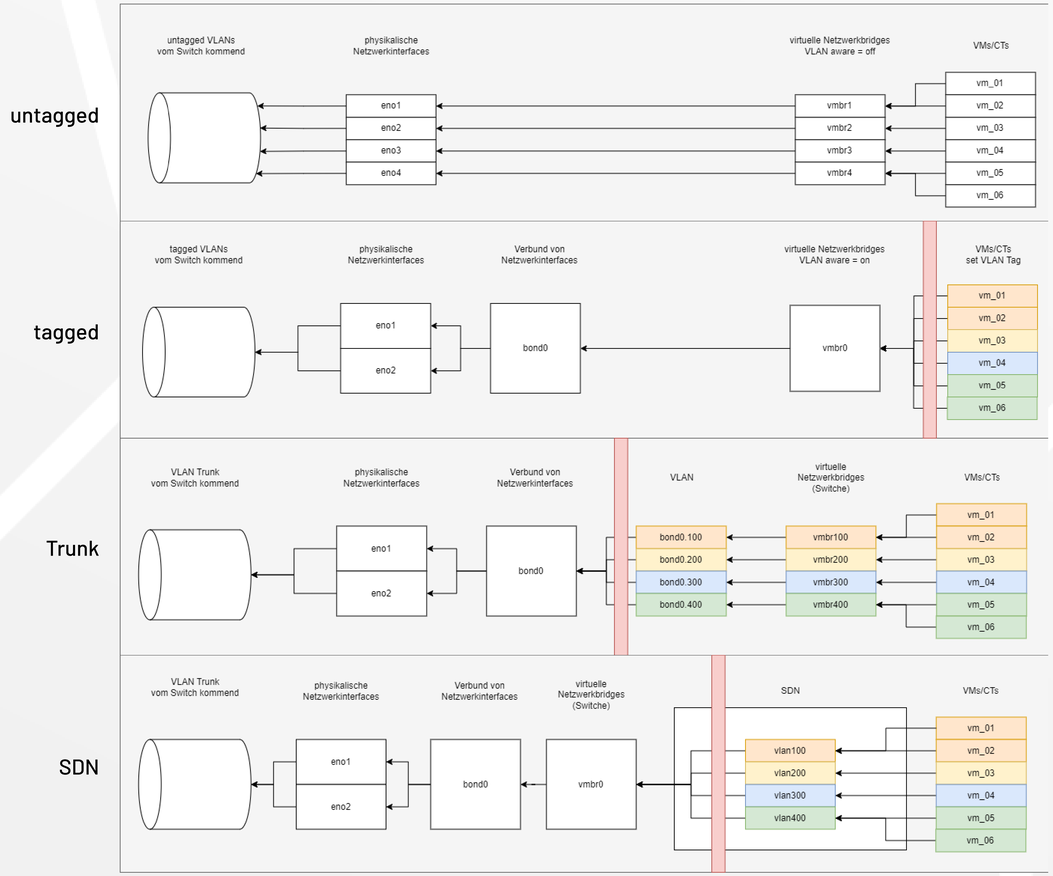
SDN

- SDN = **S**oftware **D**efined **N**etwork
- Ansatz für Netzwerkvirtualisierung und Containerisierung
- Schnittstellen für Monitoring und Administration



VLAN-Management

Präambel	SFD	Ziel MAC Adresse	Quell MAC Adresse	**VLAN Tag (optional)**	Typ	Daten	FCS
Ethernet Frame							



Strategie 1: VLAN-Tagging am physikalischen Switch außerhalb von PVE

Vorteile
- keine VLAN-Administration in PVE nötig

Nachteile
- Netzwerkkonfigurationen müssen auf allen Nodes händisch synchronisiert werden
- physikalische Anbindungen pro Netzwerk nötig / limitierte Anbindungen pro PVE-Node kostspielig
- alle Netzwerke für alle PVE-User nutzbar

Strategie 2: VLAN-Tagging an der VM-Konfiguration

Vorteile
- einfach zu konfigurieren
- Netzwerkkonfigurationen müssen nicht auf allen Nodes händisch synchronisiert werden

Nachteile
- erschwerte Übersicht aller VLANs in der PVE
- alle VLANs für alle PVE-User nutzbar

Strategie 3: VLAN-Tagging über „Linux VLAN“

Vorteile
- bessere Übersicht aller verfügbaren VLANs in der PVE
- per Kommentare kann den PVE-Usern eine Netzbeschreibung mitgegeben werden

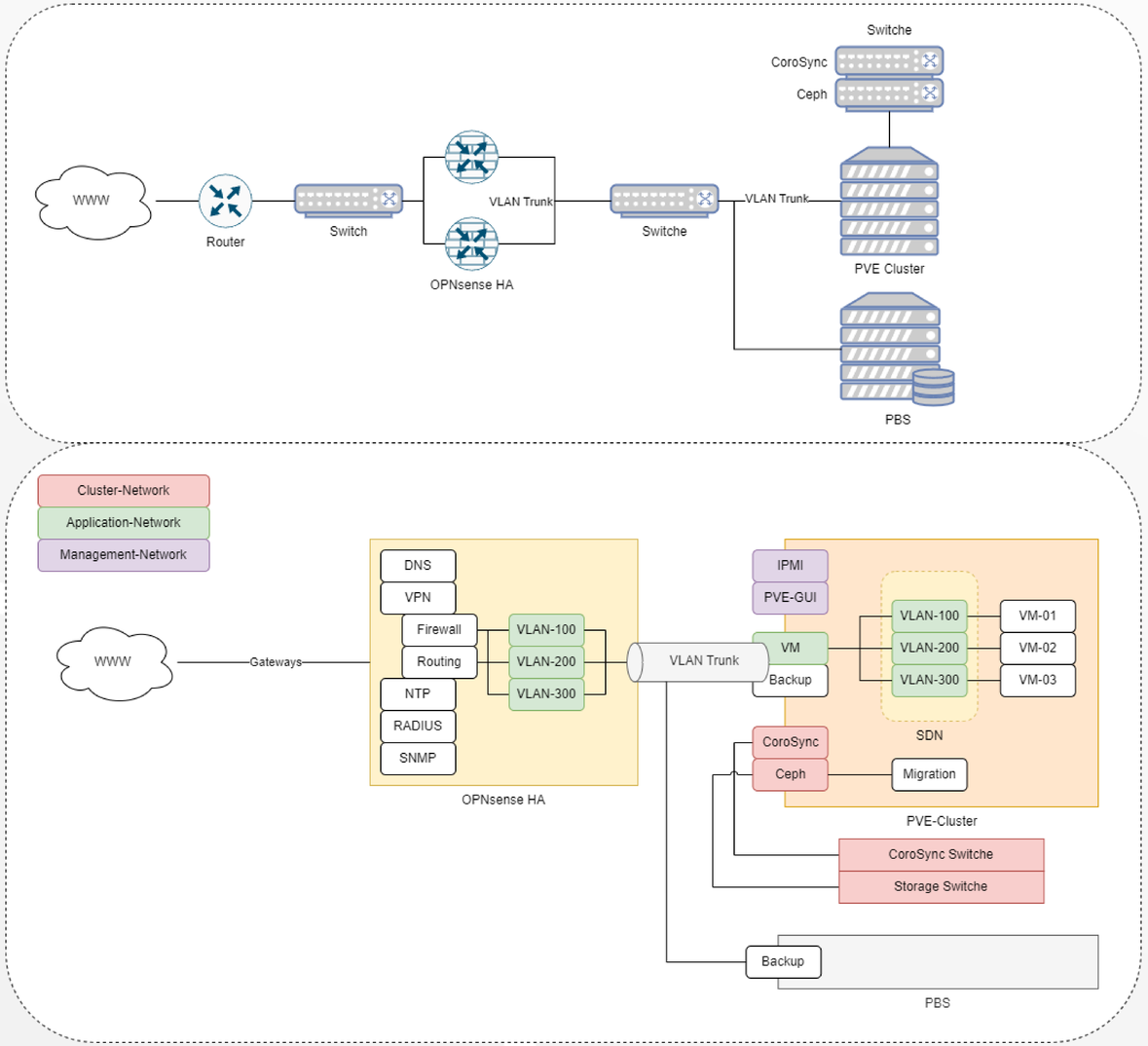
Nachteile
- Netzwerkkonfigurationen müssen auf allen Nodes händisch synchronisiert werden
- alle VLANs für alle PVE-User nutzbar

Strategie 4: VLAN-Tagging über SDN

Vorteile
- bessere Übersicht und Administration aller verfügbaren VLANs in der PVE
- Zugriffsregelung der Netzwerke für die PVE-User
- IPAM (eingeschränkt / OneWay)
- Netzwerkkonfigurationen werden automatisch zwischen den PVE-Nodes synchronisiert

Nachteile
- noch stark begrenzte Funktionalitäten des SDNs – siehe Doku

Architektur



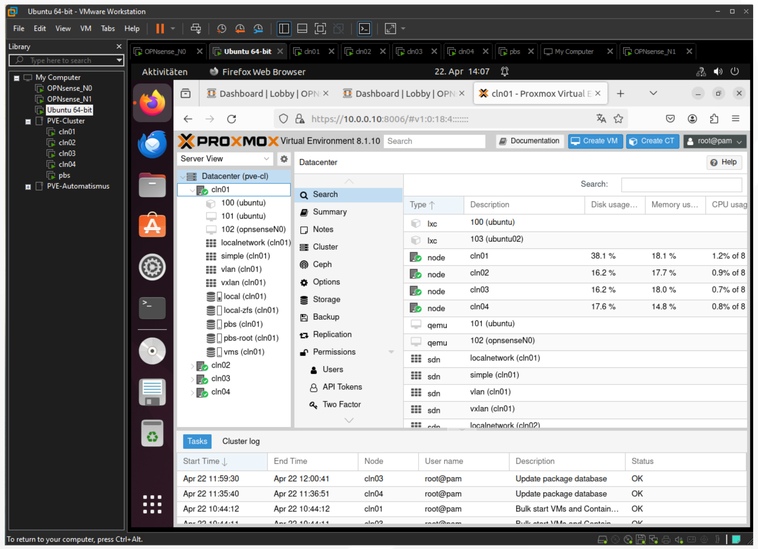
BARIBAL
STUDIOS

Q&A - Proxmox

BARIBAL STUDIOS

„Was wäre eine gute Testumgebung, um die Strategien zu erforschen und zu testen?“

Testumgebungen



All-in-One 1HE Bundle (TK)

- Edge 4L als OPNsense und ein Maxtang VHWL30 i5-10210U für PVE
- Günstige Standalone Komplettlösung
- Kein Ceph

Simulation in VE

- ggf. Lizenzen benötigt
- Host muss ausreichend Performance mitbringen (16/32-Kerne/Threats, 64GB-RAM, 2TB-NVME, nested virtualization“
- Netzwerkkonfigrationen sind herausfordernd
- Hohe Belastung des Host Storages (IOPS)

Physikalische Lösung

- Altgeräte können eingesetzt werden
- HBA Controller wird benötigt
- Testmöglichkeiten orientieren sich an der Hardwarekonfiguration (Mesh vs Switch)
- Platz wird benötigt

BARIBAL STUDIOS

„Wie gelingt der Umstieg von VLAN-Strategie #2 zu SDN in Proxmox 8.x am besten?“

Migration Netzwerkstrategien

BARIBAL STUDIOS

Downtime

- VMs/CTs herunterfahren
- Netzwerkkonfigurationen umstellen
- VMs/CTs Netzwerkkarten umstellen
- VMs/CTs hochfahren

Parallelwelt

- Vorhandene Netzwerkstruktur mit SDN nachbauen (neue IDs verwenden)
- VMs/CTs Netzwerkkarten umstellen

Mischbetrieb

- Vorhandene Netzwerkstruktur mit SDN nachbauen (Netz für Netz)
- Für jedes Netz alle zugehörigen VMs/CTs die Netzwerkkarten gleichzeitig umstellen

BARIBAL STUDIOS

„Wie kann eine Migration von VMware aussehen?“

VMware Migration

BARIBAL STUDIOS

Automatisiert

– ESXi Importer per Storage Plugin

Manuell

– SSH-Verbindung zwischen VMware und PVE-Cluster

– ovftool

Proxmox Wiki

https://pve.proxmox.com/wiki/Migrate_to_Proxmox_VE

BARIBAL STUDIOS

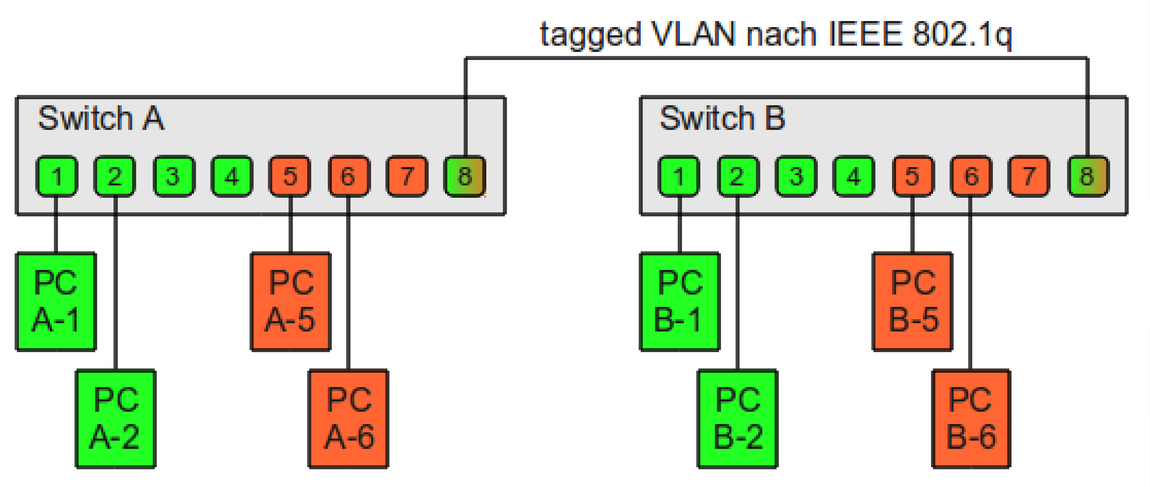
„Sind die der Proxmox nachgelagerten Switche an den jeweiligen Ports für die VM auch tagged?“

Switchport – tagged || Trunk

BARIBAL STUDIOS

Tagged

VLAN-Informationen müssen auf der ganzen Datenstrecke bei jeder Komponente (Router oder Switche) eingetragen werden (VLAN-Database)



https://www.thomas-krenn.com/de/wiki/VLAN_Grundlagen

Trunk

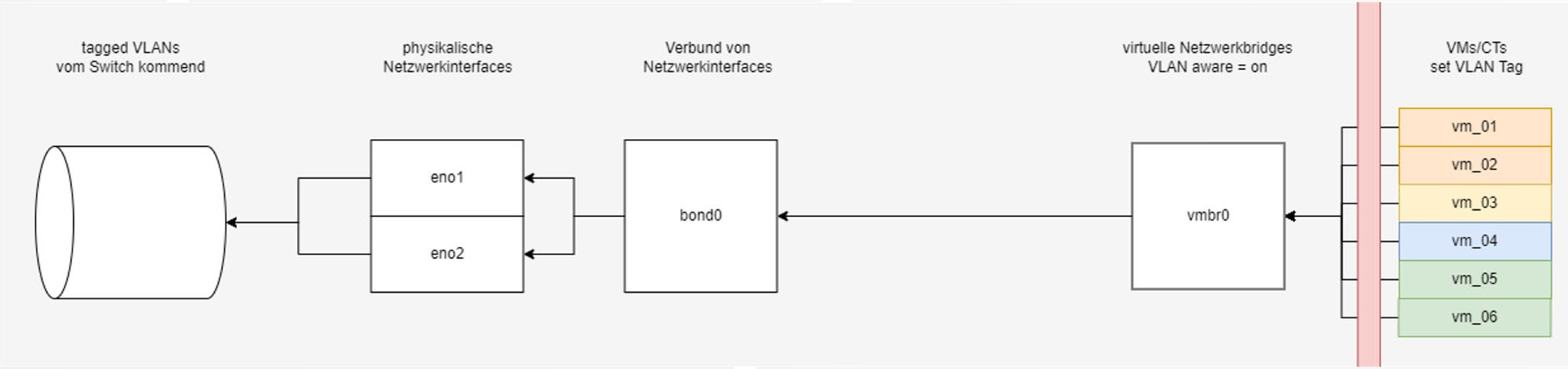
VLAN-Informationen werden über den Trunk an alle Komponenten weitergereicht

Switchport – tagged || Trunk

Präambel	SFD	Ziel MAC Adresse	Quell MAC Adresse	**VLAN Tag (optional)**	Typ	Daten	FCS
Ethernet Frame							

Strategie 2:

VLAN-Tagging an der VM-Konfiguration

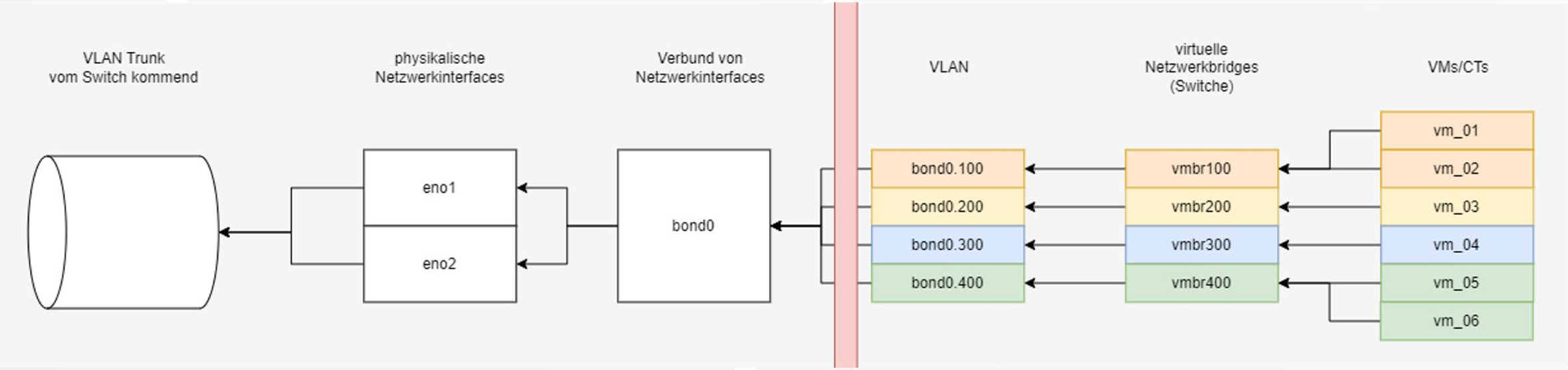


Switchport – tagged || Trunk

Präambel	SFD	Ziel MAC Adresse	Quell MAC Adresse	**VLAN Tag (optional)**	Typ	Daten	FCS
Ethernet Frame							

Strategie 3:

VLAN-Tagging über „Linux VLAN“



BARIBAL STUDIOS

„Wie sieht die Unterstützung von Proxmox durch Hard- und Software Hersteller aus?“

Proxmox Support

Eigenes KnowHow wird bei OpenSource Lösungen gefordert (Schulungen)

Externe Dienstleister/Partner können unterstützen (Proxmox-Partner)

Support direkt von Proxmox (Proxmox-Subscriptions)

„Wie schnell ist die Netzwerkbandbreite zwischen den VMs, die zusammen an einer vmbr hängen?“

Linux Bridge - Bandbreite

```
administrator@ubuntu:~$ iperf3 -c 192.168.101.2
Connecting to host 192.168.101.2, port 5201
[  5] local 192.168.101.1 port 43386 connected to 192.168.101.2 port 5201
[ ID] Interval           Transfer     Bitrate         Retr  Cwnd
[  5]   0.00-1.00   sec  3.81 GBytes  32.7 Gbits/sec    0   2.43 MBytes
[  5]   1.00-2.00   sec  3.53 GBytes  30.3 Gbits/sec    0   2.97 MBytes
[  5]   2.00-3.00   sec  3.36 GBytes  28.9 Gbits/sec    0   2.97 MBytes
[  5]   3.00-4.00   sec  3.49 GBytes  29.9 Gbits/sec    0   2.97 MBytes
[  5]   4.00-5.00   sec  3.64 GBytes  31.2 Gbits/sec    0   2.97 MBytes
[  5]   5.00-6.00   sec  3.55 GBytes  30.5 Gbits/sec    0   2.97 MBytes
[  5]   6.00-7.00   sec  3.64 GBytes  31.3 Gbits/sec    0   2.97 MBytes
[  5]   7.00-8.00   sec  3.85 GBytes  33.0 Gbits/sec    0   3.12 MBytes
[  5]   8.00-9.00   sec  3.87 GBytes  33.2 Gbits/sec    0   3.12 MBytes
[  5]   9.00-10.00  sec  3.81 GBytes  32.8 Gbits/sec    0   3.12 MBytes
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate         Retr
[  5]   0.00-10.00  sec  36.5 GBytes  31.4 Gbits/sec    0             sender
[  5]   0.00-10.00  sec  36.5 GBytes  31.4 Gbits/sec                  receiver

iperf Done.
administrator@ubuntu:~$
```

Hängt vom CPU und RAM-Speed ab!

https://forum.proxmox.com/threads/proxmox-support-maximum-network-speed-10gbps.131443/

BARIBAL
STUDIOS

Q&A - OPNsense

Netzwerk, VLANs, VPNs

BARIBAL STUDIOS

Wann verwendet man welchen Netzwerktyp für OPNsense VMs?

Linux Bridge bei Proxmox. Bonding wird nicht empfohlen.

Empfehlungen nützlicher PlugIns, Verwaltung DHCP, einfache Einrichtung VPN?

AdGuard PlugIn, Kea DHCP-Server, einfache VPN Verwaltung nur mit Bastelarbeit (LDAP + VPN-Exporter-PlugIn)

Verwaltung und Management

BARIBAL STUDIOS

Zentralles Manegement von Konfigurationen Keys Aliasen etc, Monitoring VPN und Stabilität IPsec?

OPNcentral PlugIn von Deciso, Central Management Plugin von max IT

Pitfalls bei OPNsense auf Proxmox?

Netzwerkkarten durchreichen, VLANs direkt zuweisen

Verwaltung und Management

BARIBAL STUDIOS

Größte Risiken/Hürden bei virtualisierter OPNsense Firewall?

Favorisiert separat außerhalb von Proxmox VE. Störungsanfälliger bei Virtualisierung.

Was sind die größten Herausforderungen bei der Implementierung von OPNsense?

Ausarbeitung Migrationsverfahren, Anlass zur Revision, Zeitmanagement

Verwaltung und Management

BARIBAL STUDIOS

Wie sieht ein klassisches HA-Setup für die wichtigsten Dienste aus?

Sehr umfangreiche Frage. Dazu gibt es ein extra E-Book:
https://www.thomas-krenn.com/de/tkmag/expertentipps/e-book-ha-cluster-mit-opnsense/

Monitoring mit Zabbix von OPNsense/Proxmox?

OPNsense – https://www.zabbix.com/de/integrations/opnsense
Proxmox – https://www.zabbix.com/de/integrations/proxmox

BARIBAL
STUDIOS

Fazit

Fazit

BARIBAL STUDIOS

Skalierung

IT-Sicherheit

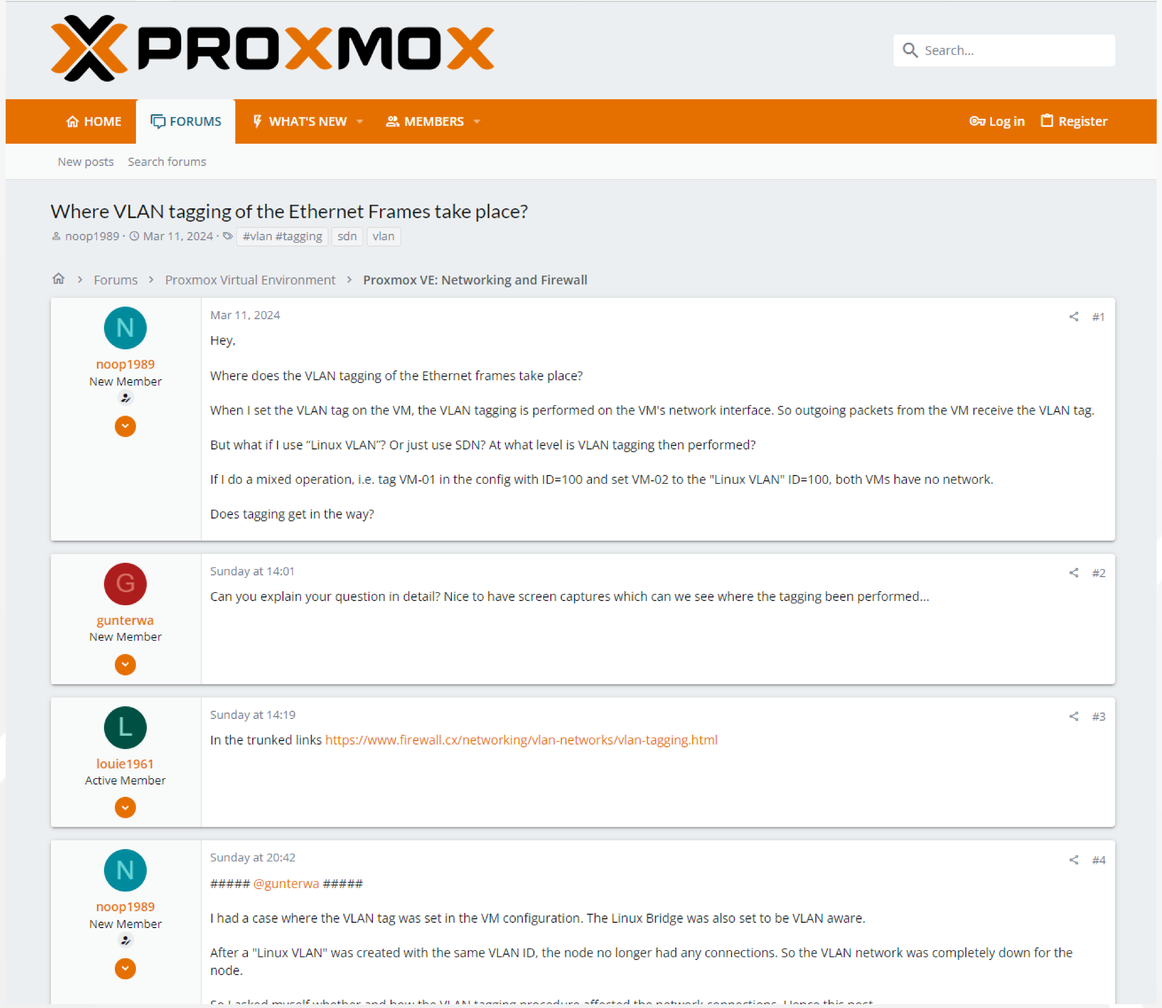
Monitoring-Möglichkeiten

Administrations-aufwand

Dokumentations-aufwand

Störungsquellen

Proxmox-Forum



Diskutiere mit unter:

https://forum.proxmox.com/threads/where-vlan-tagging-of-the-ethernet-frames-take-place.143141/

weitere Webinare

OPNsense Migration

https://www.thomas-krenn.com/de/tkmag/expertentipps/praxisbericht-migration-auf-einen-opnsense-ha-cluster

Proxmox VE – Q&A

https://www.thomas-krenn.com/de/tkmag/webinare/qa-proxmox-ve-ihre-fragen-zur-open-source-virtualisierungsplattform/

Kontakt

BARIBAL STUDIOS

Baribal Studios

kontakt@baribal-studios.de

www.baribal-studios.de

Daniel Richter

Chief Technical Officer (CTO)

daniel.richter@baribal-studios.de

+49 162 2026945

Ansprechpartner für IT-Projekte

Thomas Niedermeier

Senior Solution Engineer OPNsense

Thomas-Krenn.AG

tniedermeier@thomas-krenn.com

+49 8551 9150 264