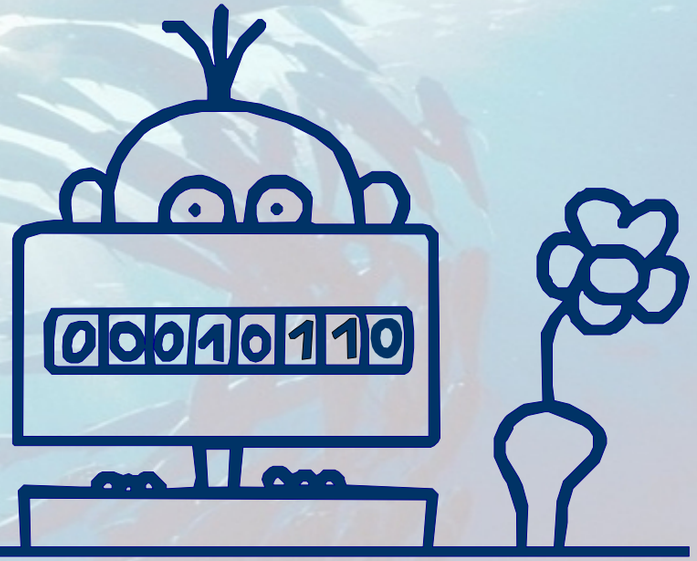
Netzwerkkonzeption des UVE

Wie sich die VM-Infrastruktur in ihre Umgebung integriert



OSL aktuell

Schöneiche / Berlin • 29. Mai 2024

eduard.broese@osl.eu

UVE als Appliance

Eine Plattform für virtualisierte Services

Flexible Topologien durch virtuelle Netze

- Einzelne VMs
- Komplexere Vernetzung von “VM-Inseln“

Isolation der Netze

- Mehrere Mandanten in einem UVE
- Kommunikation nach außen durch externe Interfaces
- Sicheres Routing zwischen den Netzen oder zum/vom Internet

Storageengine

- Spiegelung
- Backups
- Hoher Durchsatz

Aufbau der physischen Netzinfrastruktur

UVE integriert sich als ein System

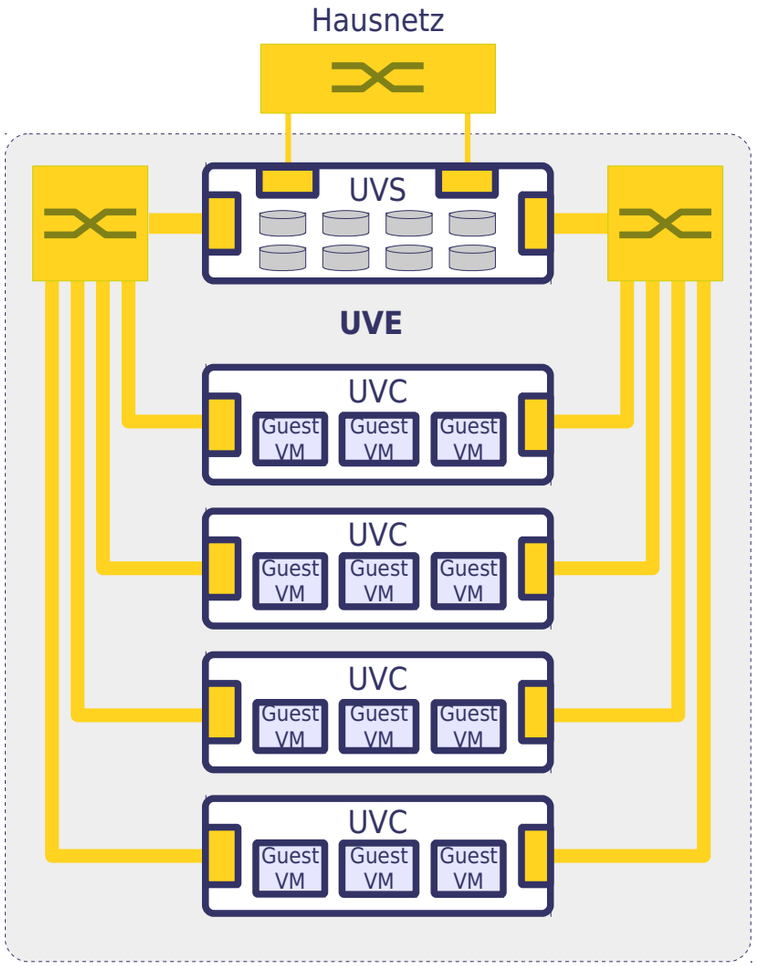
- HCI-Gedanke: *Ein* System
- Übergabepunkt ins Hausnetz sind externe UVS-Interfaces
- VM-Netze sind untereinander sowie vom Hausnetz L2-isoliert und werden erst per Routing erreichbar

Einfache Verkabelung des Clusters

- Redundante physische Netze
- Parallele Nutzung für I/O, Infrastruktur und VMs
- Keine besondere Konfiguration der Switches
- UVE verteilt virtuelle Netze dynamisch

Wartung im laufenden Betrieb

- Hinzufügen der weiteren Knoten
- Erweiterung oder Reparatur der Hardware
- Aktualisierung der Software



Aufgeteilte Netzwerkinfrastruktur im UVE

Virtuelle Netze für die VMs und für die interne Nutzung der UVE-Engine

Infrastukturdienste für die Virtualisierung

- Speicher für gemeinsam genutzte Dateien (z.B. Installations-ISOs)
- VM Migration zwischen den Knoten
- Konsolenzugang
- nicht zugänglich für die VMs

VM-IP Netze

- Kommunikation zwischen den VMs
- Kommunikation zu oder aus dem externen Netz bzw. Internet
- Verfügbar in den VMs über virtuelle Netzwerkadapter

Netzwerkinfrastruktur im UVE

Trennung der Netze durch VLANs

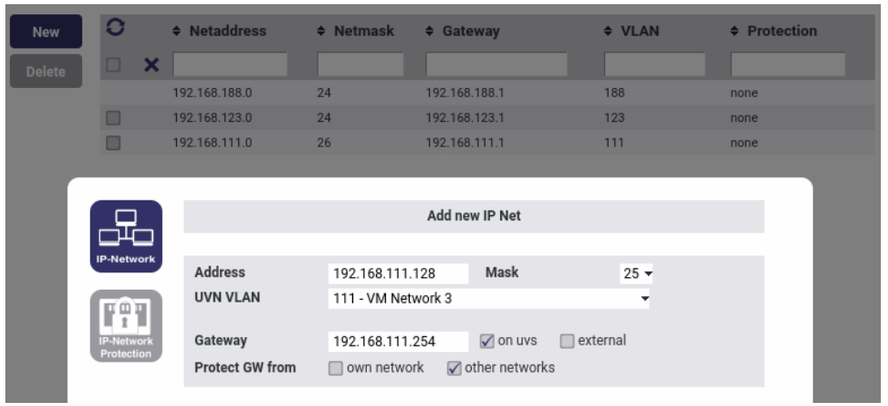
- VLANs sind für den VM-Gast unsichtbar („Access Ports“)
- Trennung der Mandantennetze oder VM-Konstellationen
- Trennung der UVE-Netze von VM-Netzen

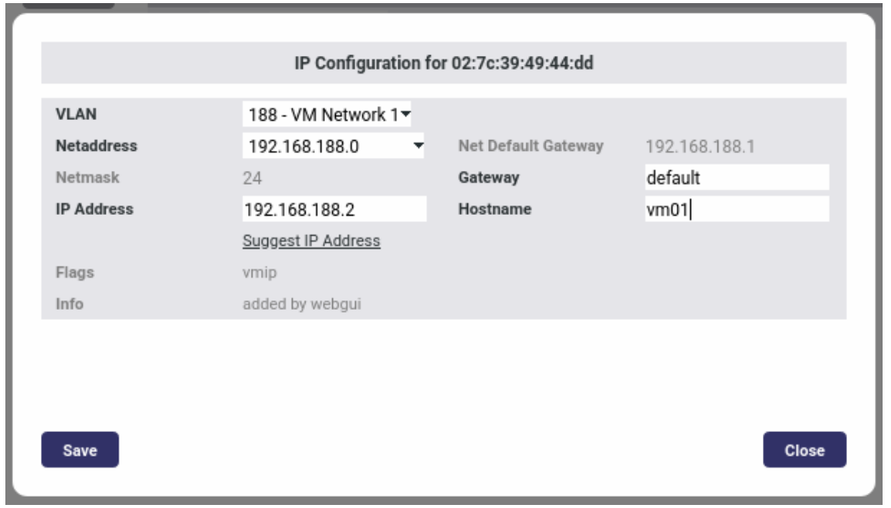
Flexibilität der Konfiguration

- Mehrere VLANs pro VM
- Mehrere IP-Netze innerhalb eines VLAN möglich

Dienste auf dem UVS

- DHCP-Dienst für automatische IP-Zuweisung
- Gateway für den Zugang zu externen Netzen
  → auf dem UVS, extern oder optional ausgeschaltet
- NFS, NTP, weitere Server nach Bedarf





VN-Framework

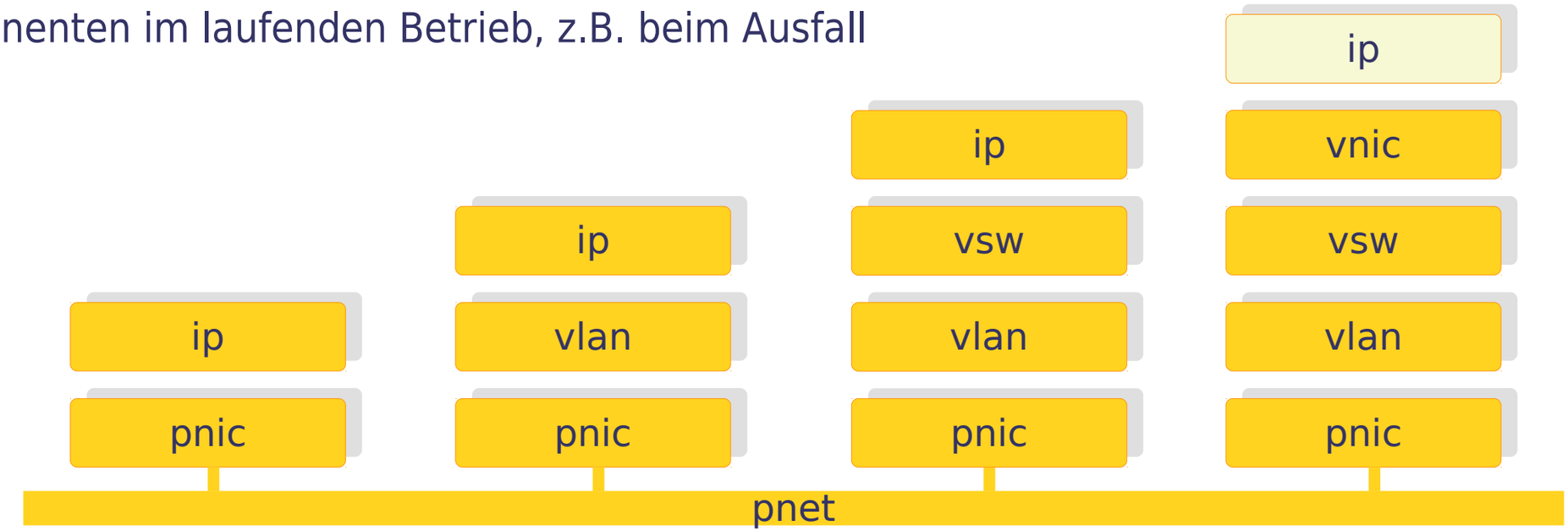
Virtual Network Objects

Generisches Interface für die Konfiguration der (virtuellen) Netzwerke

- Im Einsatz bei UVE und Storage Cluster ab v4.8
- Netzkonfiguration für Knoten, VMs, Anwendungen, usw.
- Einheitliche Administration auf verschiedenen Plattformen

Flexible Netzwerkstacks

- Unterstützung PNICs, VLANs, Bridges, VNICs, IP in beliebigen Kombinationen
- Austausch der Komponenten im laufenden Betrieb, z.B. beim Ausfall

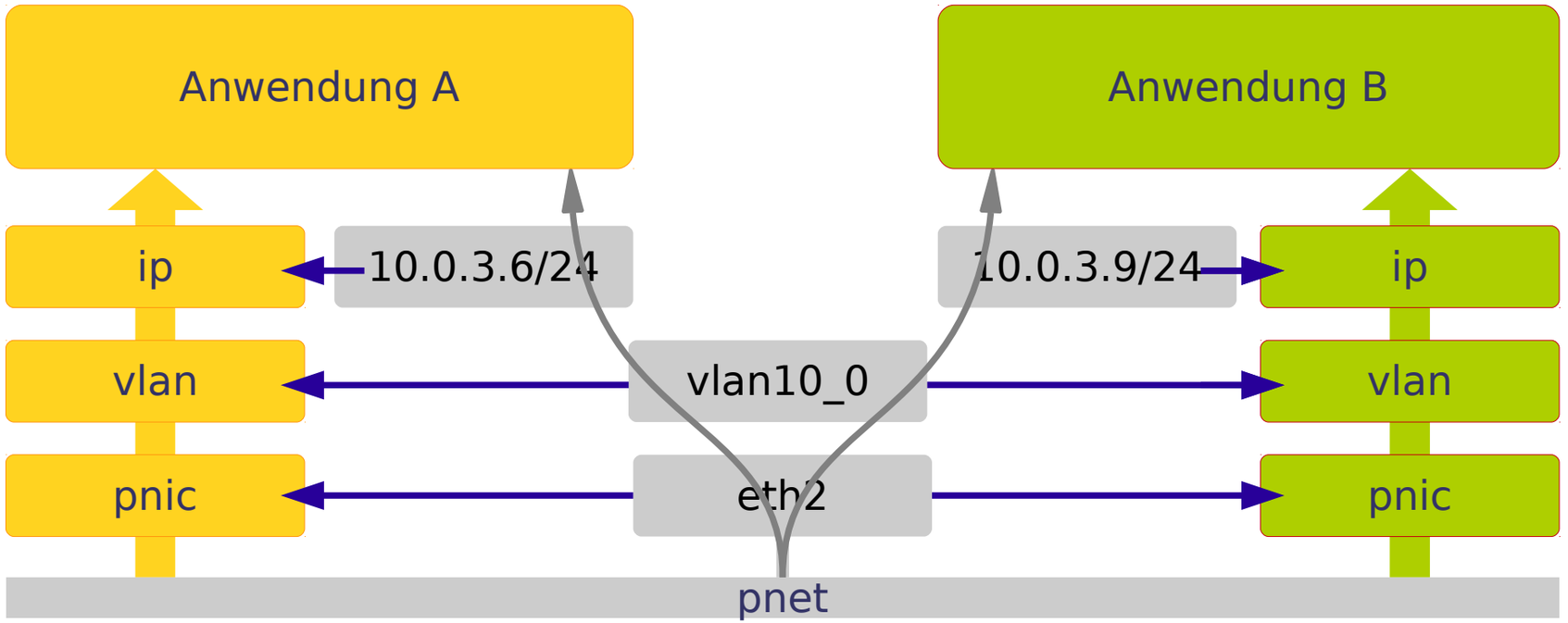


VN-Framework

Virtual Network Objects (VNO)

Eigene Konfiguration pro Anwendung/VM/Dienst

- VNOs sind auf SNO (System Network Objects) N:1 abgebildet
- Automatisches Abräumen nach Reference-Count-Prinzip
- Übersichtliche Darstellung



Ausfallsicherheit

Mehrere Redundanzen im UVE gegen Ausfall von Komponenten

Ausfall eines UVN-Netzes

- Interfaces der Knoten, Kabel oder Switch
- VLANs werden zu dem funktionierenden physischen Netz verschoben
- kurzer Netzausfall für die betroffenen VMs

Ausfall des Serverknotens (UVS)

- der sekundäre Knoten übernimmt die Aufgaben
- Übernahme des Plattenspeichers, Netze und Dienste
- kurze Pause in I/O und Netzkommunikation

Ausfall des Computeknotens (UVC)

- Ausfall der zur Zeit laufenden VMs
- essenzielle VMs können automatisch auf einem anderen Knoten gestartet werden

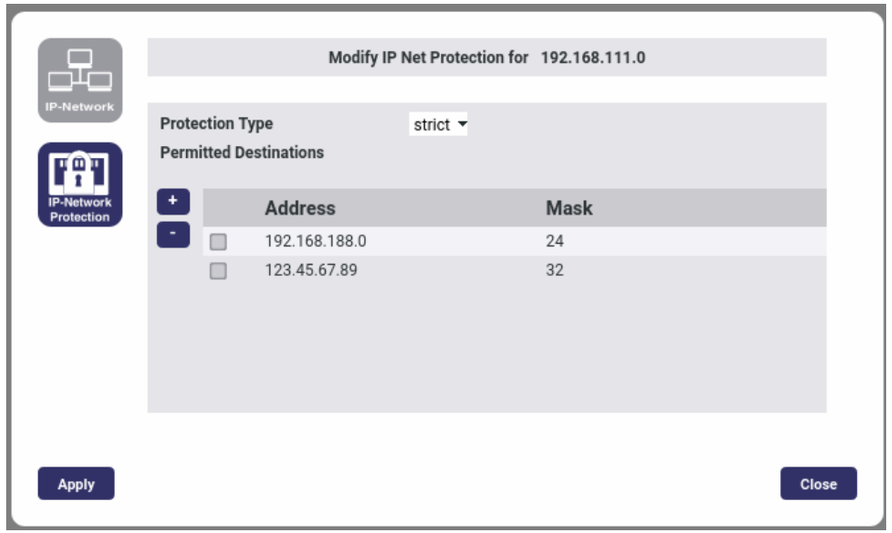
In allen Fällen ist keine Umkonfiguration der Gastsysteme erforderlich

Sicheres Routing

Schutz des UVS und der Netze vor unerlaubten Zugriffen

VM-Netze sind in der Regel auch auf dem UVS eingebunden

- UVS dient als Gateway zum Internet oder anderen Netzen
- Unerlaubte Zugriffe müssen / sollen unterbunden werden
  - aus den VMs auf den UVS
  - aus dem Internet auf die VMs
  - zwischen den nicht verwandten VM-Netzen



UVE 4.8 definiert veschiedene Schutztypen pro IP-Netz

- „none” : alle Zugriffe erlaubt
- “basic” : Zugriff von/auf andere VM-Netze und auf den UVS blockiert
- “strict” : Zugriffe auf andere Netze oder Internet nur anhand einer Whitelist erlaubt

virtualization and clustering – made simple