Table of Contents

Micro Cloud (Hybrid) Architecture DRAFT

Disposable HW and SW architecture requied! Vendor-lock-in may be kept at minimum levels. SDDC (Software-Defined Data Center): A data storage facility where networking, storage, CPU and security are virtualized and delivered as a service. Stable, cheap, good enough.

Tier	Description
I	A Tier 1 data center is a basic server room implementing the general guidelines for computer system installations. This first level runs within a 99.671 percent availability through one non-redundant distribution path with non-redundant capacity components.
II	A Tier 2 data center Includes all requirements of Tier 1, plus a guarantee of 99.741 percent availability with redundant site infrastructure capacity components.
III	In addition to fulfilling requirements of Tiers 1 and 2, Tier 3 data centers provide dual-powered IT equipment to receive data from multiple independent distribution paths with an increased availability of 99.982 percent guaranteed.
IV	Tier 4 data centers include the components of the first three Tiers with the addition of independently dual-powered cooling equipment. The site infrastructure is fault-tolerant with distribution capability and the capacity to store electrical power. An availability of 99.995 percent is guaranteed.

Basic Topology Important parts

Command and conquer	Openstack Horizon, Proxmox Datacenter Manager, Nutanix Prism etc.
Compute Nodes	KVM
Storage Nodes	File, Block, Objects

Network remarks

Disable Spanning Tree Protocol for servers

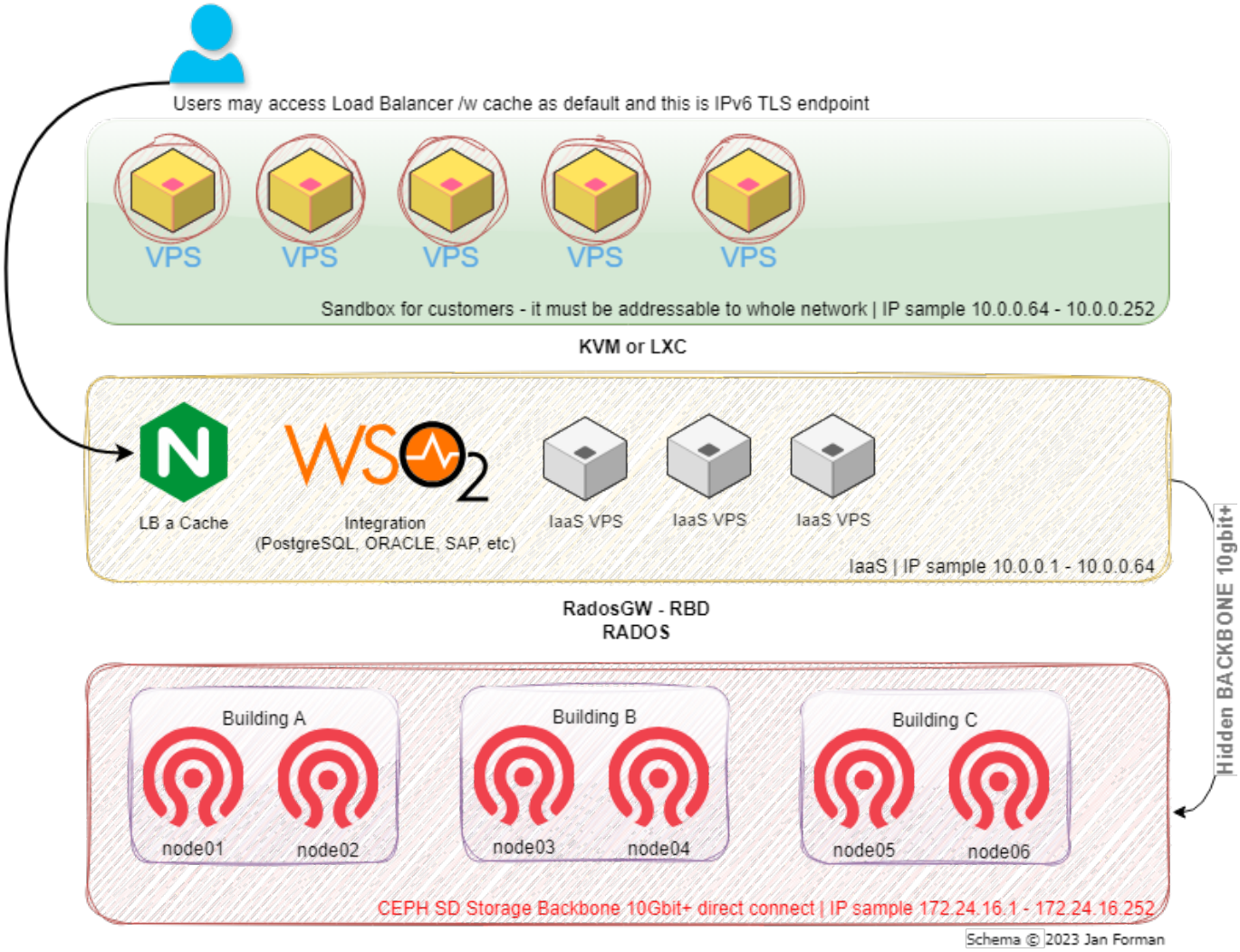
AWS Basic knowledge (Introduction by Chetan)

This is My Architecture playlist from AWS

This is my architecture

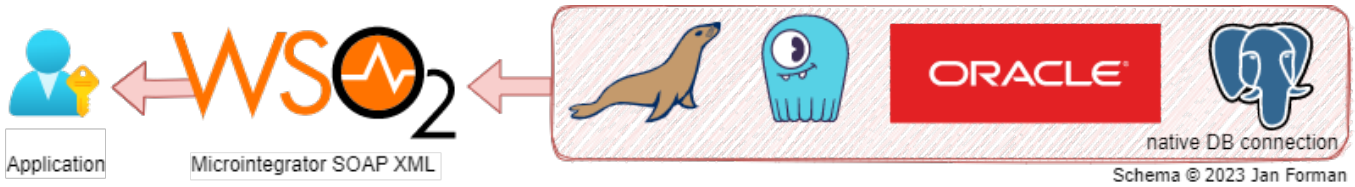
Schematics

Basic Topology



Firewalls are templates linked to VPS instance

Integration Schema

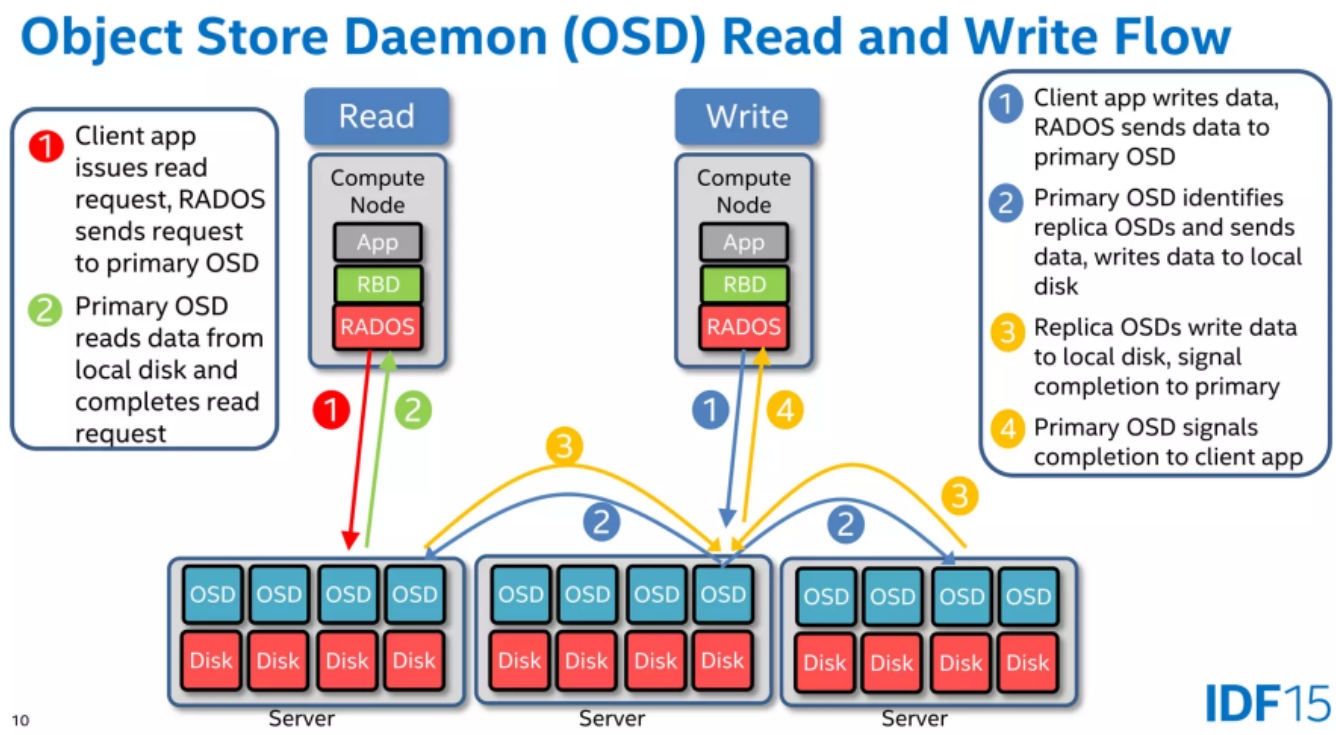


Service Flow

CEPH SD Storage Schema

Ceph Storage at CERN (IT Department)

Exabyte storage scaleout with Geocluster and autoscaling



© 2015 Jian Zhang Intel CEPH software optimizations for cloud workloads

Replication HA schema

- root
- ↘ datacenter
- ↘↘ row
- ↘↘↘ rack
- ↘↘↘↘ host
- ↘↘↘↘↘ osd

AZ recommendation

EBS	**1x AZ**
EFS	**~3x AZ (Full region)**
S3	**~3x AZ (Full region)**

HA granularity

By service	No HA	Single AZ	MultiAZ
VPS	Yes	No	No
CephFS	No	Yes	may
Blockstorage - CEPH	No	Yes	may
Blockstorage - Minio	Yes	may	No
Blockstorage - Garage	Yes	may	No
GalleraCluster	No	Yes	may
ScyllaDB	No	Yes	may
MariadDB	Yes	Yes	may
Postgresql	Yes	Yes	may
Citus	No	Yes	may

Software Stack

Cloud Core Infrastructure (IaaS)

Type	Cloud Service Description	CPU support
Compute Nodes and Management	**AWS EC2 replacement with cloudinit support**	**ARM support**
Openstack	Full, but as LEGO style	YES
Proxmox	Light, but EASY to implement	YES
	– LXC may deploy container templates – both have native CEPH support	
SD Storage (Object, Block, File) Scaleout	**AWS S3 compatible and EBS replacement**	
AWS EBS - CEPH SD Block Storage	Hyperconverged or PetaSAN	YES
AWS EFS - CEPH SD File Storage	Hyperconverged or PetaSAN	YES
SD Load Balancer, Cache	**AWS ELB / Citrix Netscaler replacement**	
NGINX	or AlibabaCloud clone	YES
Integration + Enterprise Service Bus	**IBM WebSphere replacement**	
WSO2 Integrator		YES
Mass webhosting		
ISP Config		YES
MQTT Platform	**AWS IoT core replacement**	
Mosquitto		YES
Cloud Data Synchronization / Backup		
Rclone		YES
Restic		YES
Infrastructure Monitoring System	**AWS CloudWatch replacement**	
NetXMS		agent only
Grafana		YES
Kubernetes Orchestrator	**AWS EKS replacement**	
Mikro K8s		
Microsoft Windows	**Windows Infrastructure**	**$$$ not recommended**
1x Datacenter - dedicated HW	Xx Server Standard on KVM	no/LIMITED
XXX users	CAL (client access licence) per user	
		Cloudinit for Windows

Deployment

Ansible
Terraform
Juju

Security as a Service (SECaaS)

Type	Cloud Service Description	CPU support
WAF (Application Firewall)		
OWASP® ModSecurity	+nginx connector	YES
SD Firewall	**AWS VPC, Security groups replacement**	
Integrated firewall with templates	inside hypervisor	YES
pfSense	+platform integrated (VPS sandboxing)	LIMITED

Software as a Service (SaaS)

Type	Info	Service Description	Location
Services and Management	**API catalog**	WSO2 API Manager	KVM or LXC
DB	PostgreSQL	CitusData (Sharding Cluster)	KVM or LXC
DB	PostgreSQL	Postgresql	KVM or LXC
DB	PostgreSQL	Neon	KVM or LXC
DB	MariaDB	MariaDB with GalleraCluster	KVM or LXC
DB	AWS DynamoDB replacement	ScyllaDB Alternator	KVM or LXC
Storage	AWS S3	Ceph version	CEPH Cluster
Storage	AWS S3	Garage	Garage
Storage	AWS S3	Minio version	Minio Cluster

Platform as a Service (PaaS)

Type	Name	Service Description	Location
Web Publishing	Info	Wordpress	ISPConfig
Web Storage	Network Drive	NextCloud * can use AWS S3	ISPConfig, LXC or KVM
Videoconferencing	Talk	Talk * WebRTC	Inside Nextcloud + coTurn Server
Bug Tracking	Bug Tracking	Mantis Bug Tracker	ISPConfig
Forum	Discussion Forum	VanillaForums	ISPConfig
Knowledge Base	Wikipedia	DokuWiki	ISPConfig

* WebRTC is decentralized protocol it may needs some help from CDN

Cloud-Init

KVM - Virtual drive with configuration
LXC - scripts for distribution executed directly in container

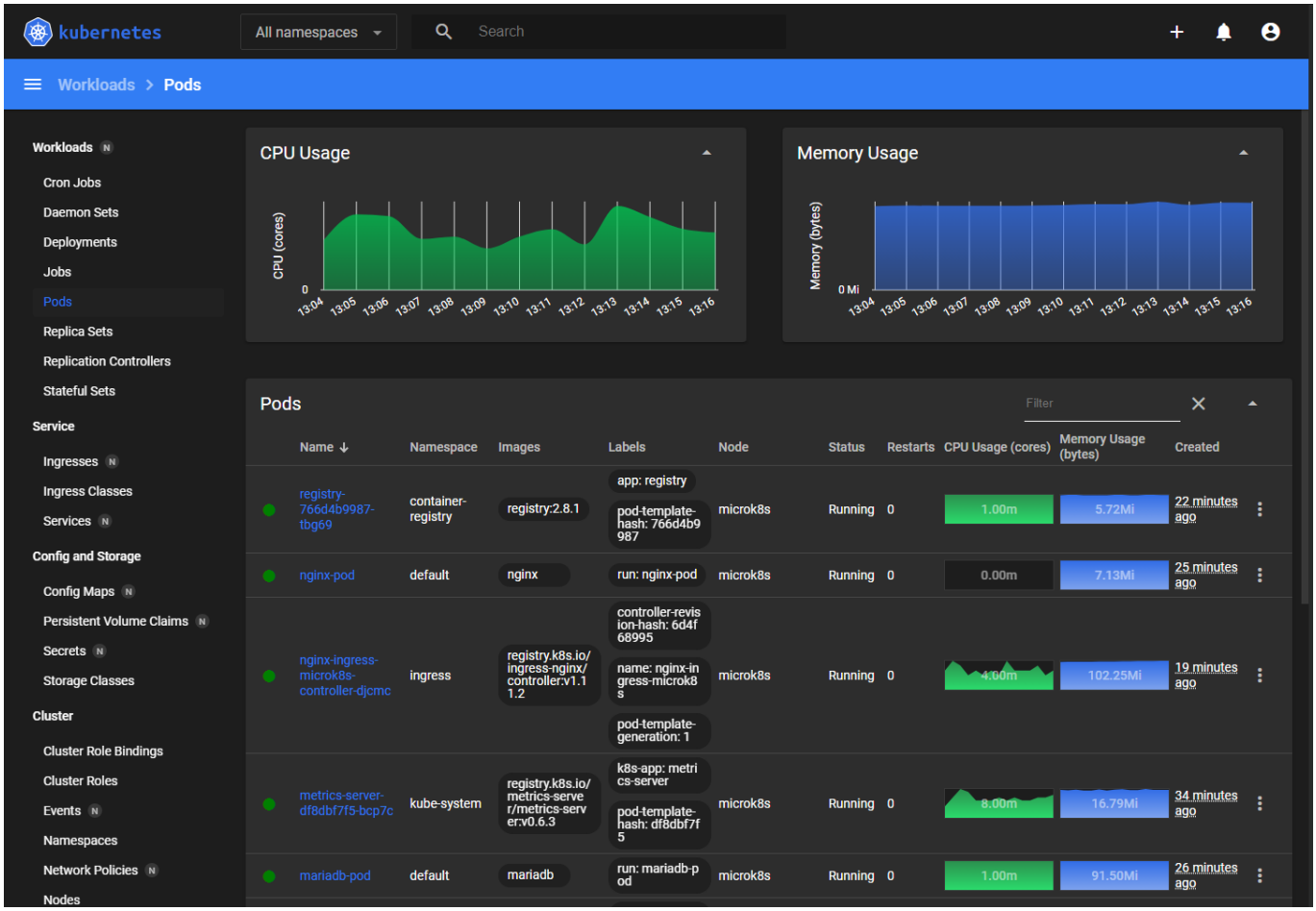
API + CLI

PROXMOX API documentation

Multiuser setups

You may use pools inside Proxmox to separate users and namespaces inside Kubernetes

Kubernetes (MicroK8s)



Hardware Draft

Compute nodes
AMD Epyc
EBS - SD Storage
Ampere / ARM 4x core+

Security

Biometric Readers + card

Power Backup

Inside everyrack plus diesel generators outside building

Man-Trap

Cage or room with Biometric Readers + card

Zero-Trust-Security

Every microservice must not trust to anyone else

Main-Distribution-Frame (MDF)

Incoming and outgoing communication and power lines within a building
A panel or set of panels where all communication cables from different parts of the building are both terminated and connected.
Cage or room with Biometric Readers + card

Intermediate Distribution Frame (IDF)

A wall-mounted or free-standing rack used to manage and interconnect a telecommunications cable between end-user devices and the main distribution frame (MDF).

Meet-Me-Room (MMR)

Network interchange place
Cage or room with Biometric Readers + card

Carrier Hotel

Internet exchange points for an area.

East-West Traffic

From server to server within a network's data center

North-South Traffic

Data flowing from or to a system physically residing outside the data center

CDN

Content Delivery Network with NGINX or TENGINE

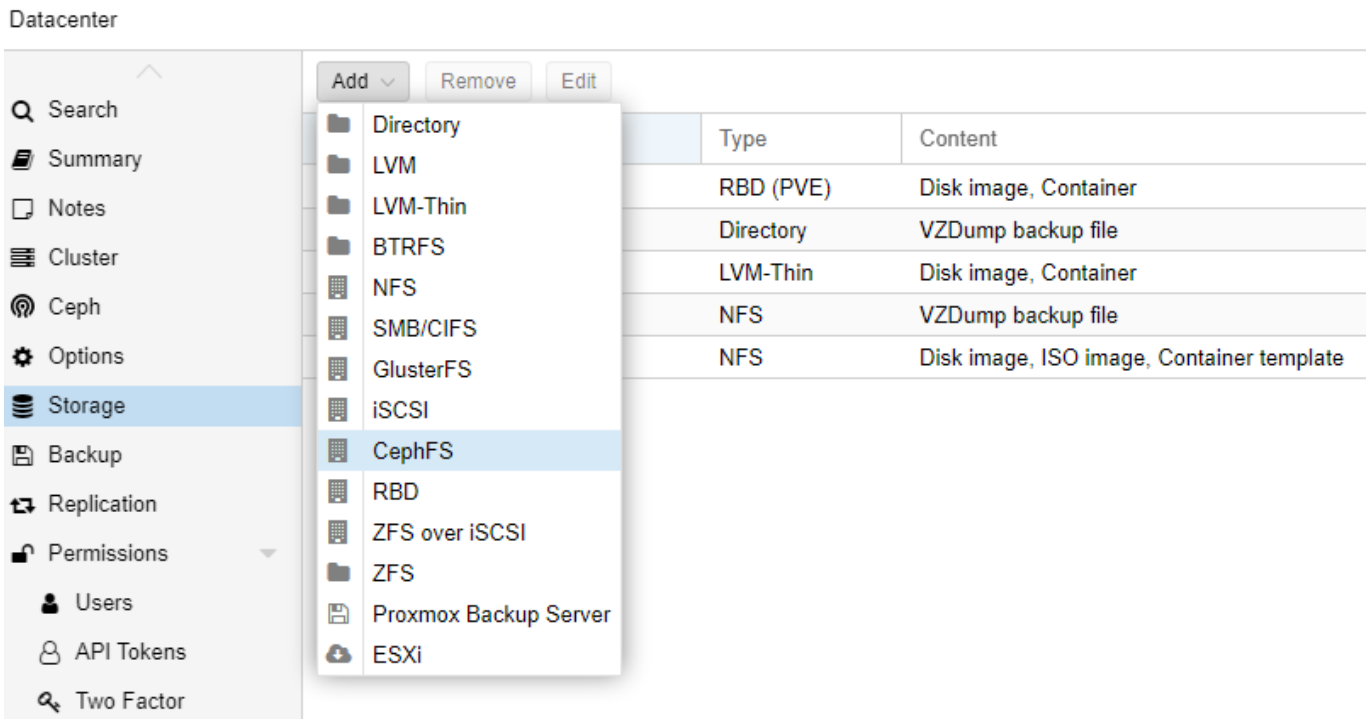
Hardware suppliers & Datacenter vendors

Reuse what's possible and make sense
Custom boards from 1000+ pcs

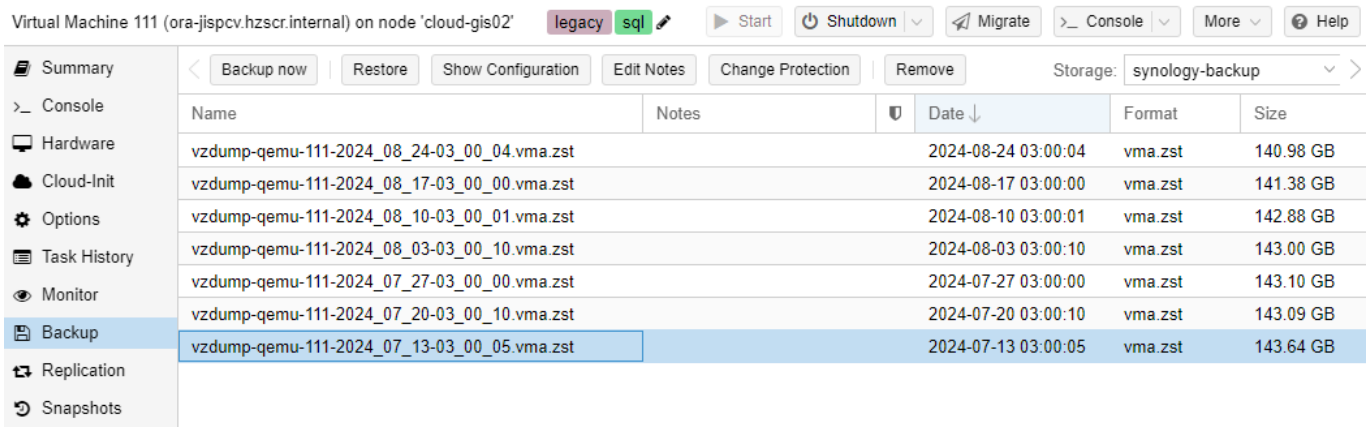
Hardware	Datacenter builders
ASRock Rack	Equinix
Gigabyte Enterprise	Digital Realty
Ingrasys	Cologix
Wiwynn	Aligned
Quanta Cloud Technology	DataBank
Tyan	NTT Data
Inventec	Digital Edge
ZT systems	EdgeConneX
Supermicro	
Aivres	

Remarks

Add Storage type

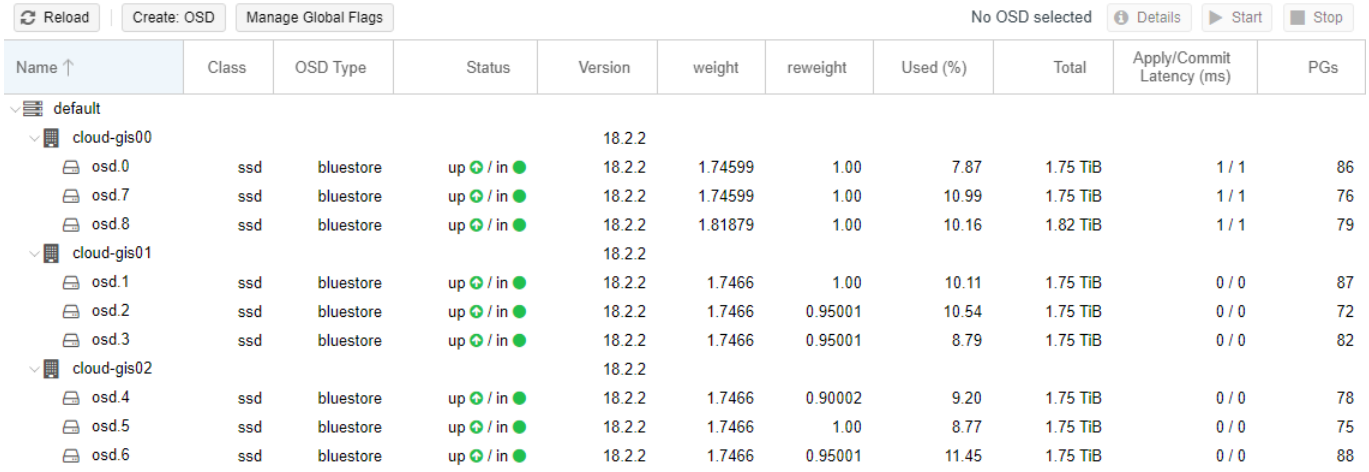


Backup

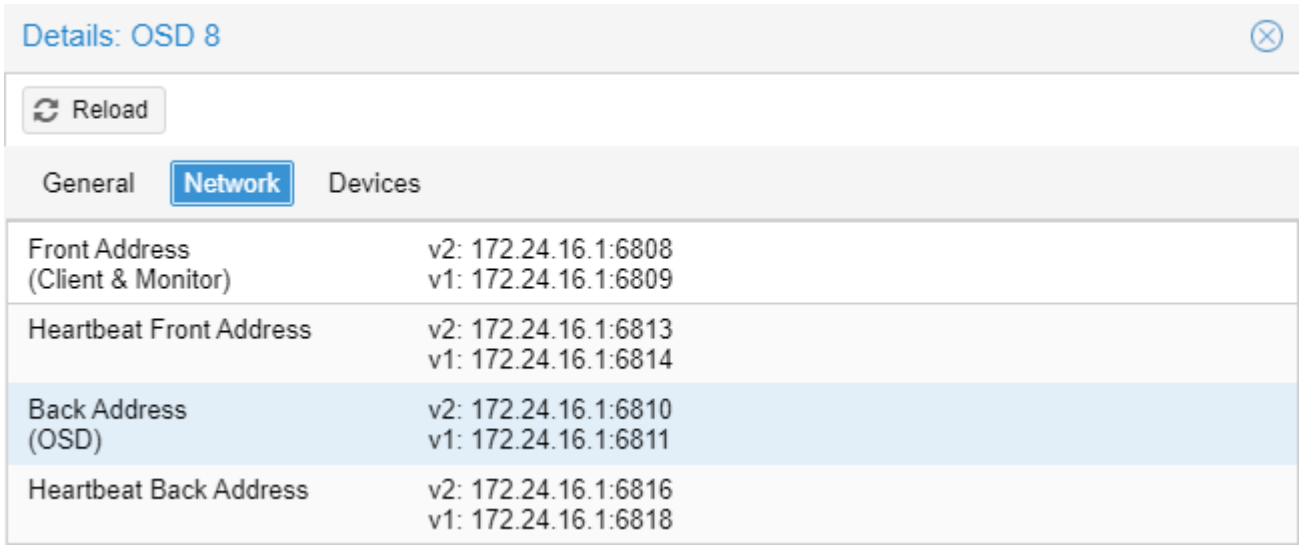


Storage CEPH

Replication schema



CEPH One SSD backbone network connnectivity

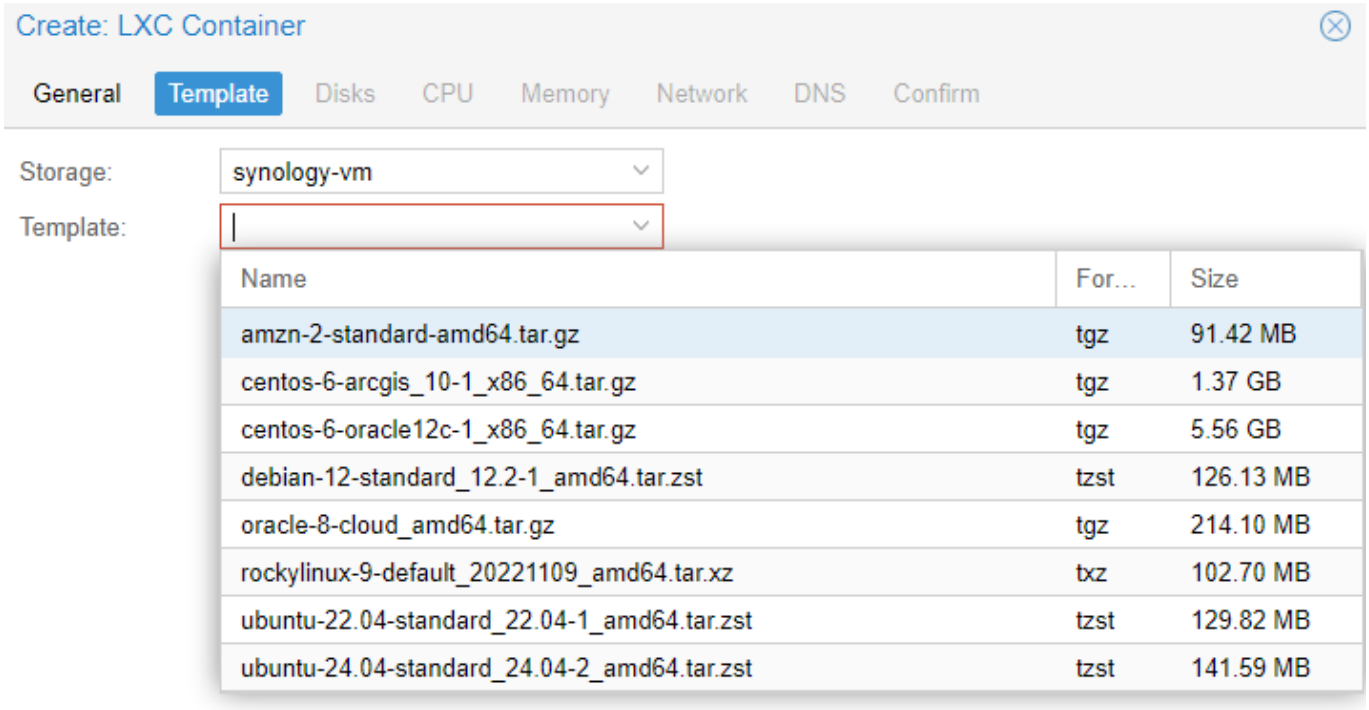


CEPH Pools (replication config)

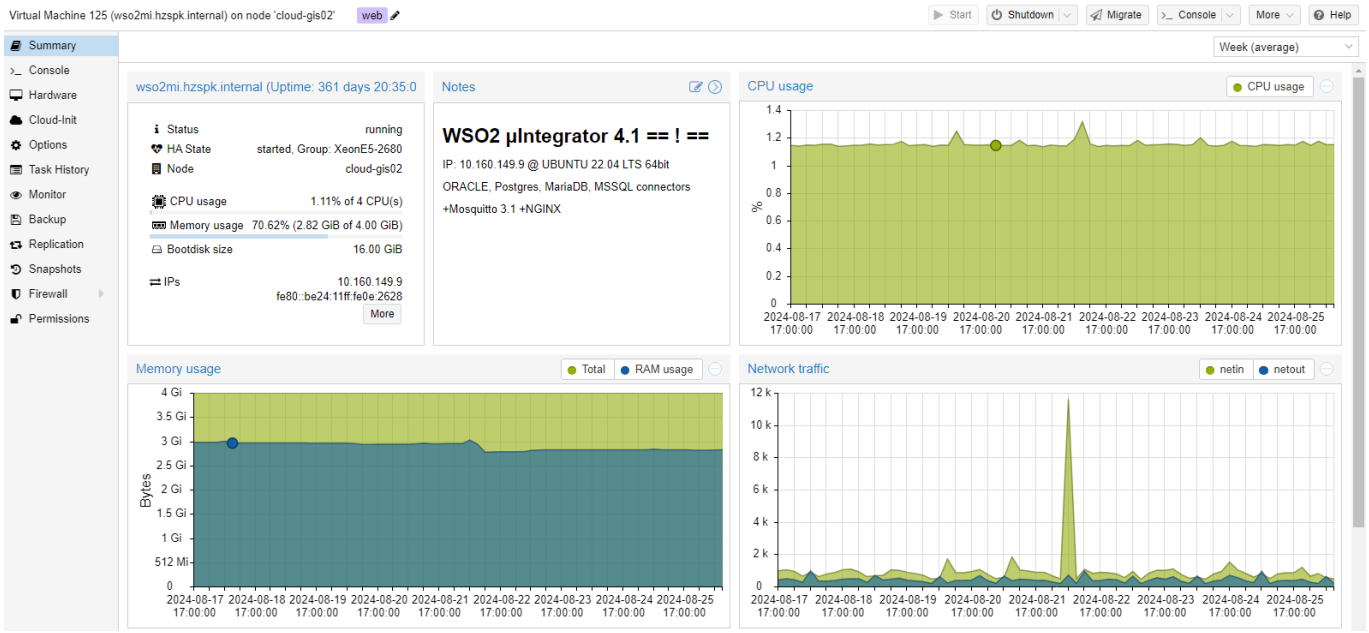
Create | Edit | Destroy

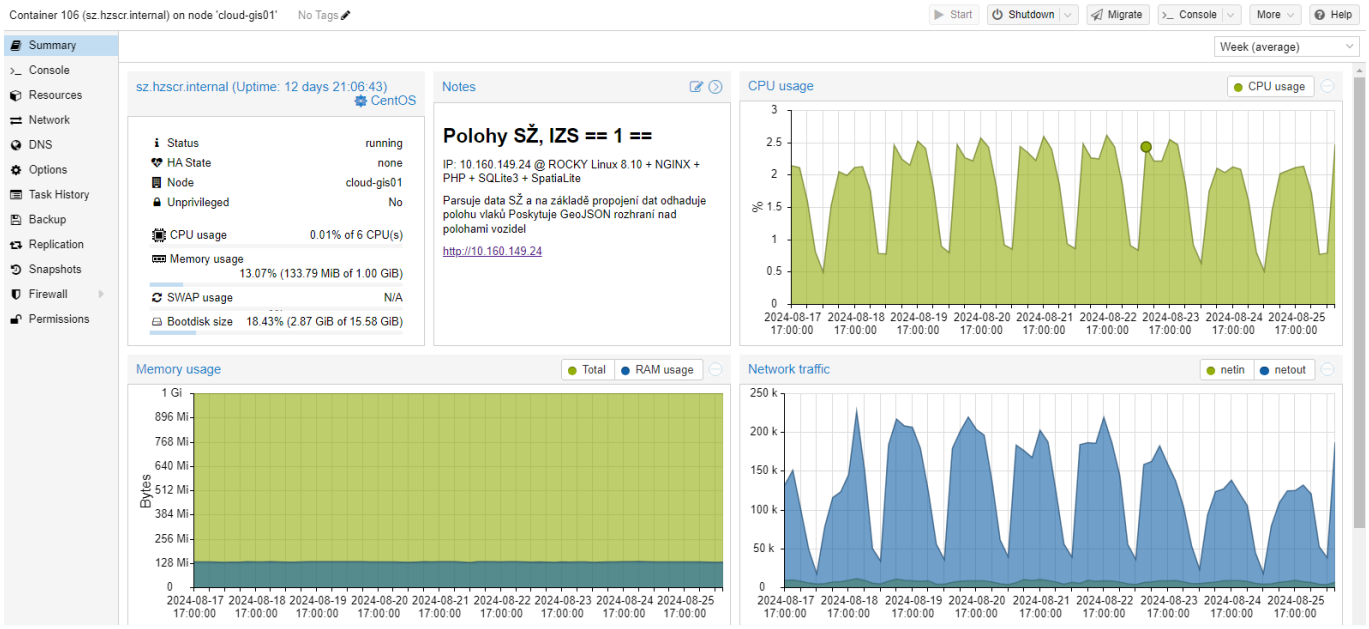
Pool #	Name	Size/min	# of Placement Groups	Optimal # of PGs	Autoscale Mode	CRUSH Rule (ID)	Used (%)
3	ceph-pool	3/2	64	32	off	replicated_rule (0)	1.61 TiB (12.81%)
12	.mgr	3/2	1	1	on	replicated_rule (0)	209.26 MiB (0.00%)
13	.rgw.root	3/2	32	32	warn	replicated_rule (0)	48.00 KiB (0.00%)
14	default.rgw.log	3/2	32	32	warn	replicated_rule (0)	408.00 KiB (0.00%)
15	default.rgw.control	3/2	32	32	warn	replicated_rule (0)	0 B (0.00%)
16	default.rgw.meta	3/2	8	8	warn	replicated_rule (0)	119.21 KiB (0.00%)
17	default.rgw.buckets.index	3/2	8	8	warn	replicated_rule (0)	157.69 KiB (0.00%)
18	default.rgw.buckets.data	3/2	32	32	warn	replicated_rule (0)	93.65 GiB (0.83%)
19	default.rgw.buckets.non-ec	3/2	32	32	warn	replicated_rule (0)	15.59 KiB (0.00%)
							1.70 TiB

Create VM



Running VM





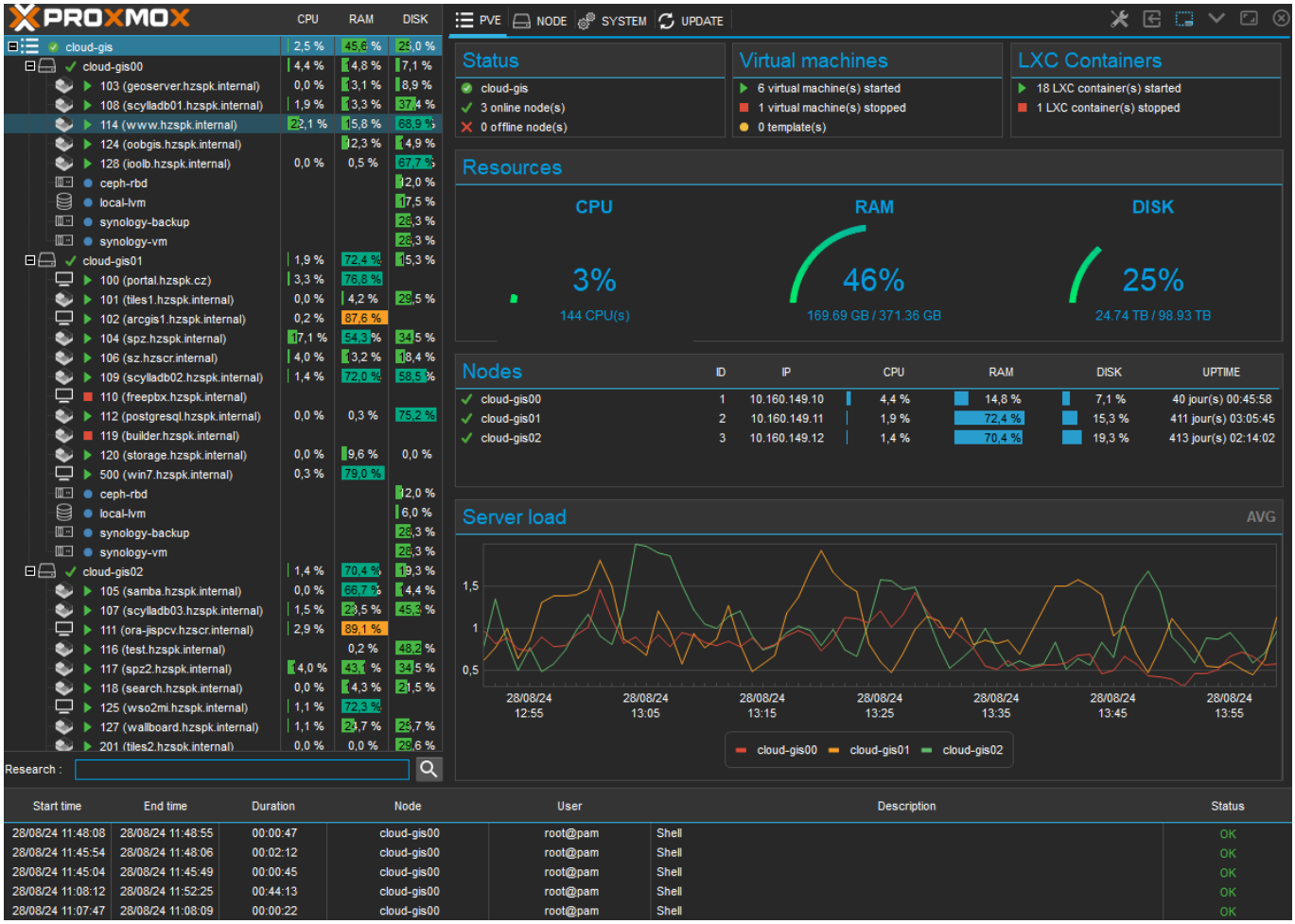
Firewall Template (SECaaS)

Group: Create Remove Edit

Rules: Add Copy Remove Edit

Group	Comment		On	Type	Action	Macro	Protocol	Source	S.Port	Destination	D.Port
ags	ArcGIS Enterprise	0	☑	out	ACCEPT	Ping					
lb	Load Balancer	1	☑	out	DROP						
scylladb	Big Data	2	☑	in	ACCEPT	Ping					
web	Accept HTTP traffic	3	☑	in	ACCEPT		tcp			+cloud	8080
wso2	Micro Integrator	4	☑	in	ACCEPT	HTTP		+cloud		+cloud	
		5	☑	in	ACCEPT	HTTPS		+cloud		+cloud	
		6	☑	in	DROP						

MultiCluster Proxmox Dashboard



MultiCluster Kubernetes Dashboard

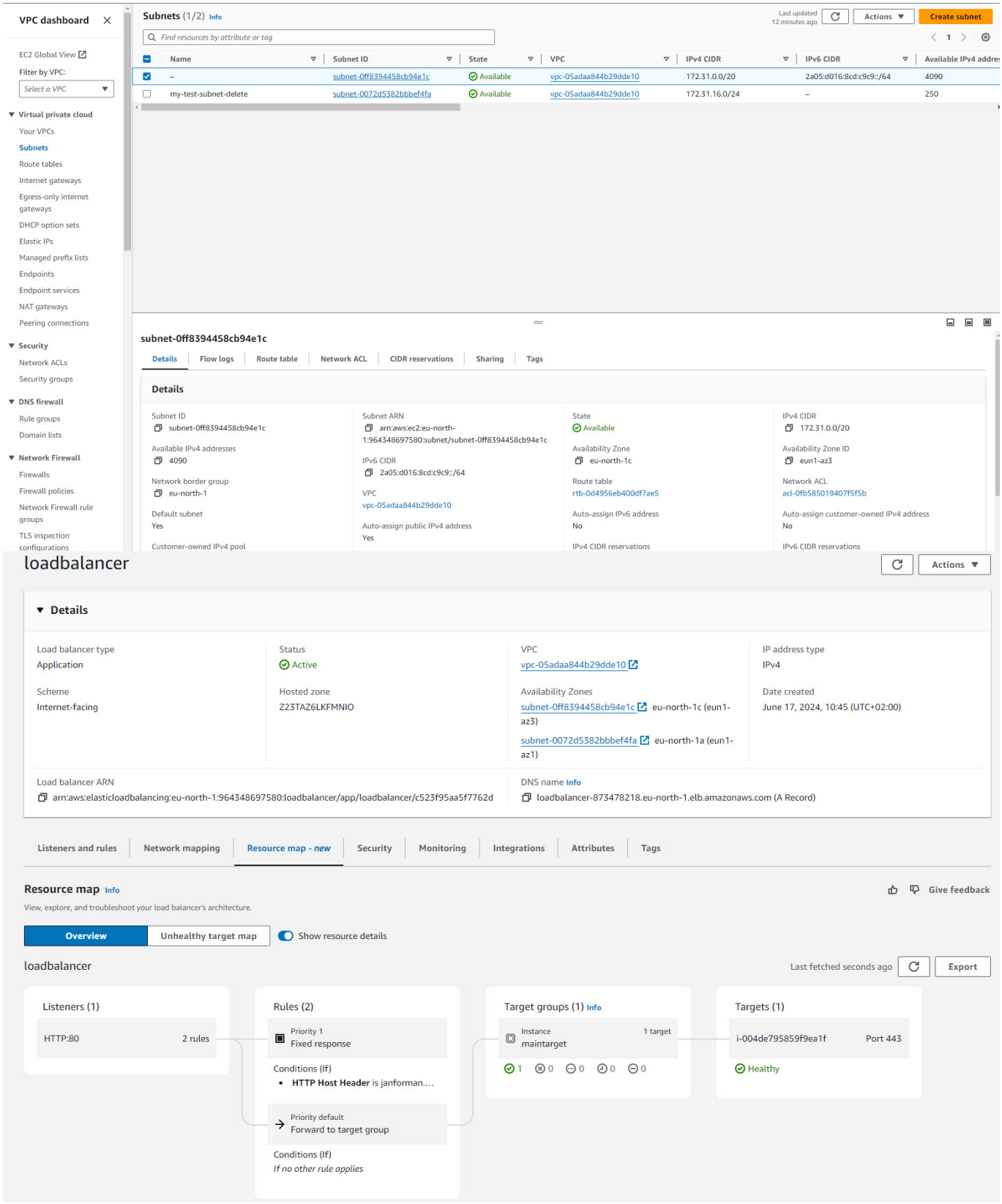
Kubernetes KubeWall

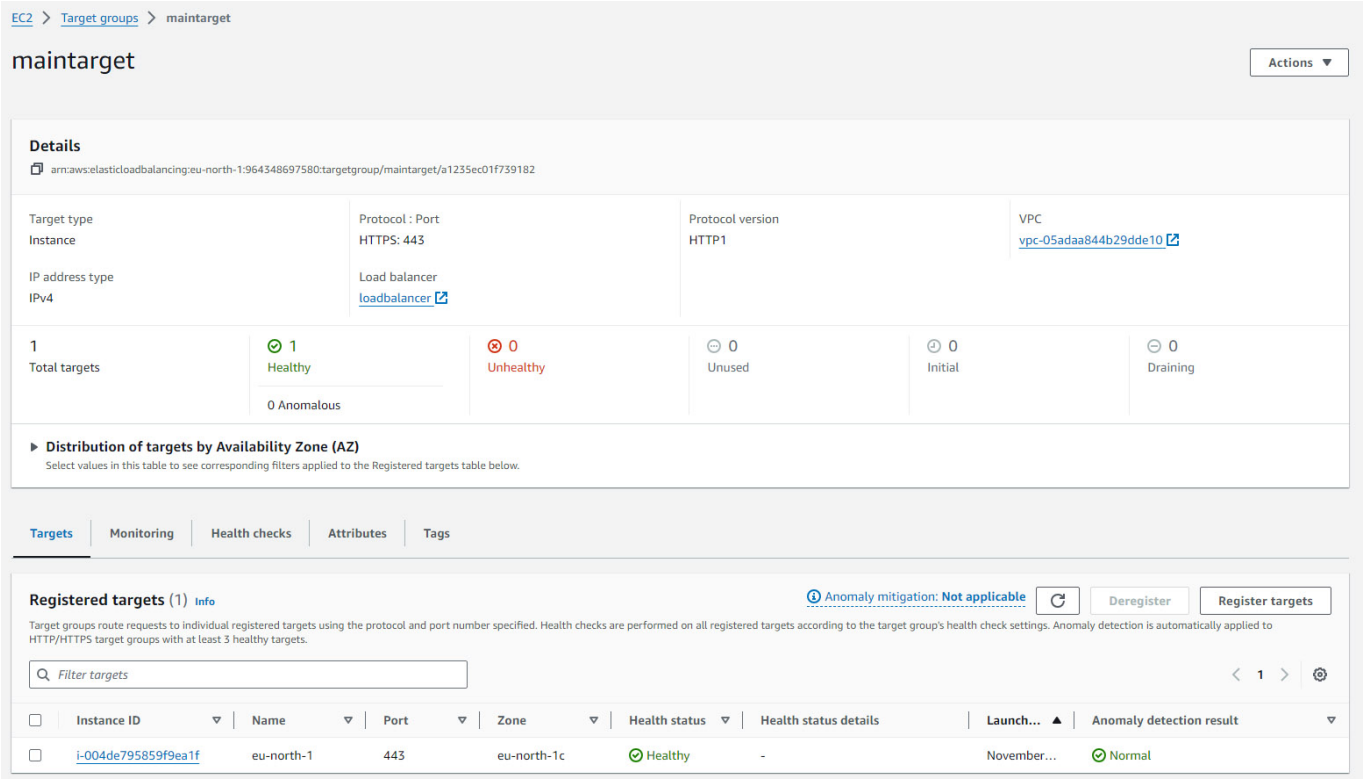
Proxmox on RaspberryPI 5 / with Win11 ARM inside

Proxmox direct import from VMWare ESXi

https://www.youtube.com/watch?v=8Z9Zvt2RxlA

AWS Load Balancer


VPC dashboard
EC2 Global View
Filter by VPC:
Select a VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
DHCP option sets
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
NAT gateways
Peering connections
Security
Network ACLs
Security groups
DNS firewall
Rule groups
Domain lists
Network Firewall
Firewalls
Firewall policies
Network Firewall rule groups
TLS inspection configurations
Subnets (1/2) Info
Last updated 12 minutes ago
Actions
Create subnet
Find resources by attribute or tag
Name
Subnet ID
State
VPC
IPv4 CIDR
IPv6 CIDR
Available IPv4 addres
– subnet-0ff8394458cb94e1c Available vpc-05adaa844b29dde10 172.31.0.0/20 2a05:d016:8cd:c9c9::/64 4090
my-test-subnet-delete subnet-0072d5382bbbef4fa Available vpc-05adaa844b29dde10 172.31.16.0/24 – 250
subnet-0ff8394458cb94e1c
Details
Flow logs
Route table
Network ACL
CIDR reservations
Sharing
Tags
Details
Subnet ID
subnet-0ff8394458cb94e1c
Subnet ARN
arn:aws:ec2:eu-north-1:964348697580:subnet/subnet-0ff8394458cb94e1c
State
Available
IPv4 CIDR
172.31.0.0/20
Available IPv4 addresses
4090
IPv6 CIDR
2a05:d016:8cd:c9c9::/64
Availability Zone
eu-north-1c
Availability Zone ID
eun1-az3
Network border group
eu-north-1
VPC
vpc-05adaa844b29dde10
Route table
rtb-0d4956eb400df7ae5
Network ACL
acl-0fb585019407f5f5b
Default subnet
Yes
Auto-assign public IPv4 address
Yes
Auto-assign IPv6 address
No
Auto-assign customer-owned IPv4 address
No
Customer-owned IPv4 pool
IPv4 CIDR reservations
IPv6 CIDR reservations
loadbalancer
Actions
Details
Load balancer type
Application
Status
Active
VPC
vpc-05adaa844b29dde10
IP address type
IPv4
Scheme
Internet-facing
Hosted zone
Z23TAZ6LKFMNIO
Availability Zones
subnet-0ff8394458cb94e1c eu-north-1c (eun1-az3)
subnet-0072d5382bbbef4fa eu-north-1a (eun1-az1)
Date created
June 17, 2024, 10:45 (UTC+02:00)
Load balancer ARN
arn:aws:elasticloadbalancing:eu-north-1:964348697580:loadbalancer/app/loadbalancer/c523f95aa5f7762d
DNS name Info
loadbalancer-873478218.eu-north-1.elb.amazonaws.com (A Record)
Listeners and rules
Network mapping
Resource map - new
Security
Monitoring
Integrations
Attributes
Tags
Resource map Info
Give feedback
View, explore, and troubleshoot your load balancer's architecture.
Overview
Unhealthy target map
Show resource details
loadbalancer
Last fetched seconds ago
Export
Listeners (1)
HTTP:80
2 rules
Rules (2)
Priority 1
Fixed response
Conditions (If)
HTTP Host Header is janforman....
Priority default
Forward to target group
Conditions (If)
If no other rule applies
Target groups (1) Info
Instance
maintarget
1 target
1 0 0 0 0
Targets (1)
i-004de795859f9ea1f
Port 443
Healthy



AWS S3 (replicated across AZs within location), S3 Express One Zone (faster, cheaper only one zone)

Software stack overview

Sorted by my recommendation

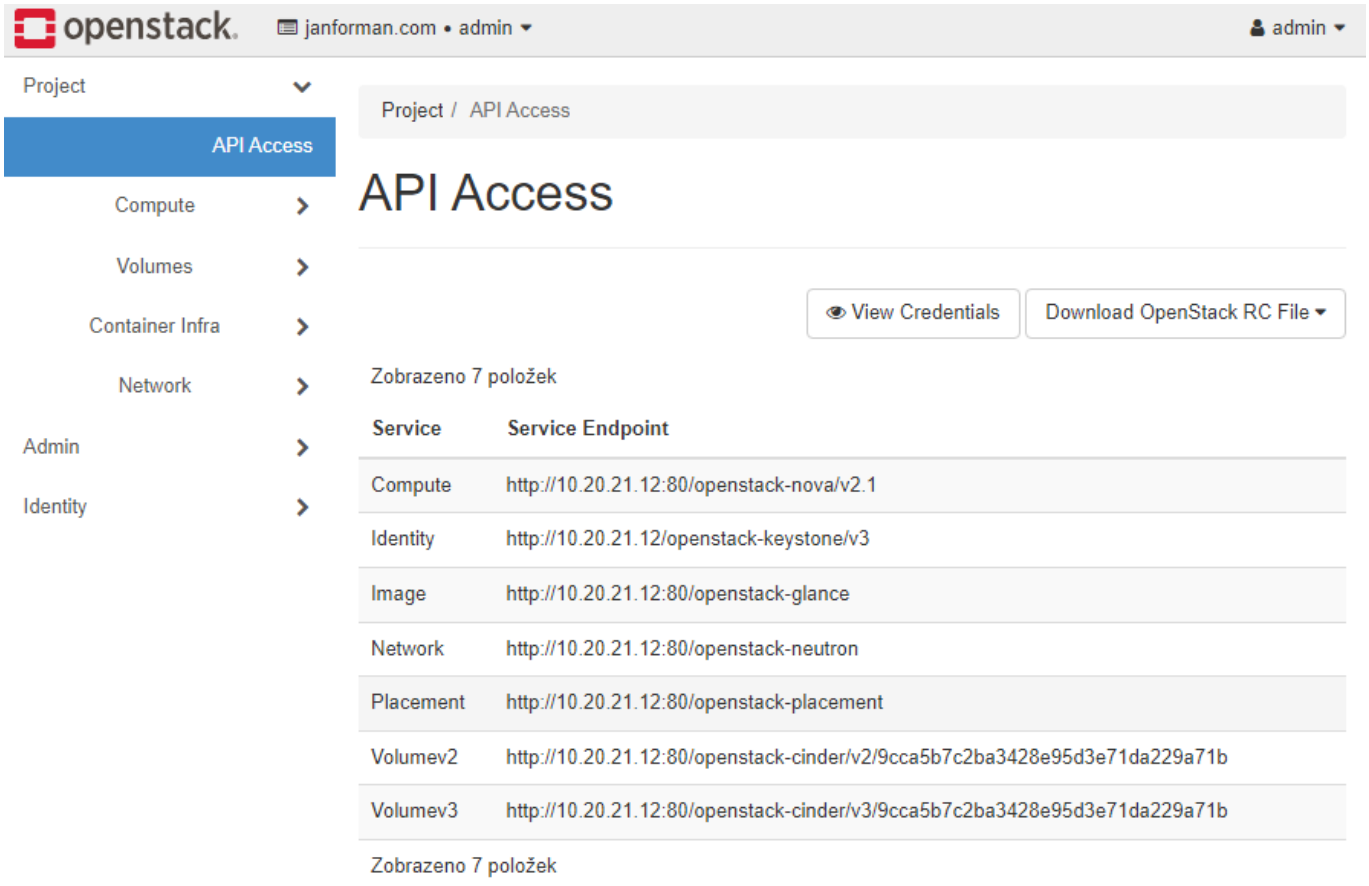
Openstack	**Pros**	**Cons**
	OpenSource,cost-effective	Hard to setup
	Modular design	Modular design
	Ultimate solution for very large clouds	Higher maintenance costs
NASA Hybrid Cloud Amazon AWS and OpenStack, SEZNAM.cz		
AT&T runs its mobile core network on an OpenStack cloud, serving millions of subscribers.		
China Mobile, one of the world's largest telecom providers, is building the biggest NFV network based on OpenStack with over 50,000 servers.		
OpenStack is more alive than ever with 40 million cores in production and over 300 public cloud data centers worldwide.		
Proxmox	**Pros**	**Cons**
	OpenSource,cost-effective	Scalability issues for very large environments
	Easy to setup	approx. 32 servers in group more needs MultiCluster manager
	Multiple HV KVM, LXC	Limited enterprise support
	LXC is very lightweight	Upgrade on OS level
	Integrated SD storage, SD firewall (like AWS sg)	
	CEPH and ZFS implemented, IPAM support	
	Can consume CEPH from a dedicated cluster	
	Open vSwitch alternative to vSphere Distributed Switch	
	SDN Network alternative to NSX-T Data Center	
OpenNebula	**Pros**	**Cons**
	Multiple HV KVM, LXC, vCenter	
	Kubernetes included	
Nutanix AHV	**Pros**	**Cons**
	Kubernetes Support	Vendor-lock-in (Closed opensource products)
	Integrated storage and networking solutions	Messy Architecture
	Rocky Linux, Cassandra	No external storage support
Microsoft Hyper-V	**Pros**	**Cons**

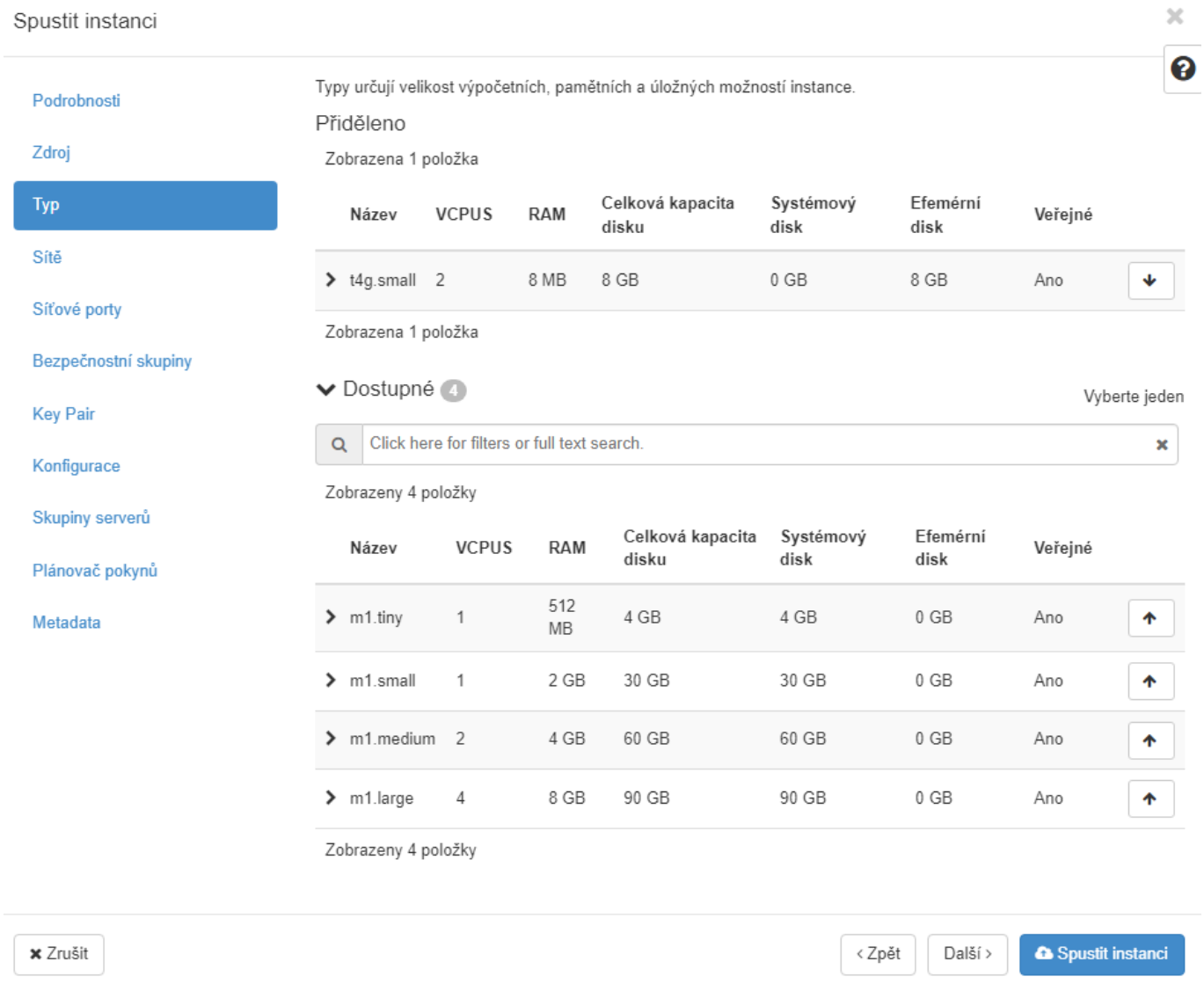
Openstack	**Pros**	**Cons**
	Easy to setup	Cost, limited functionality
		Additional licensing costs!
		Vendor-lock-in
VMWare	**Pros**	**Cons**
	Easy to setup	Higher cost
		Additional licensing costs!
		Vendor-lock-in

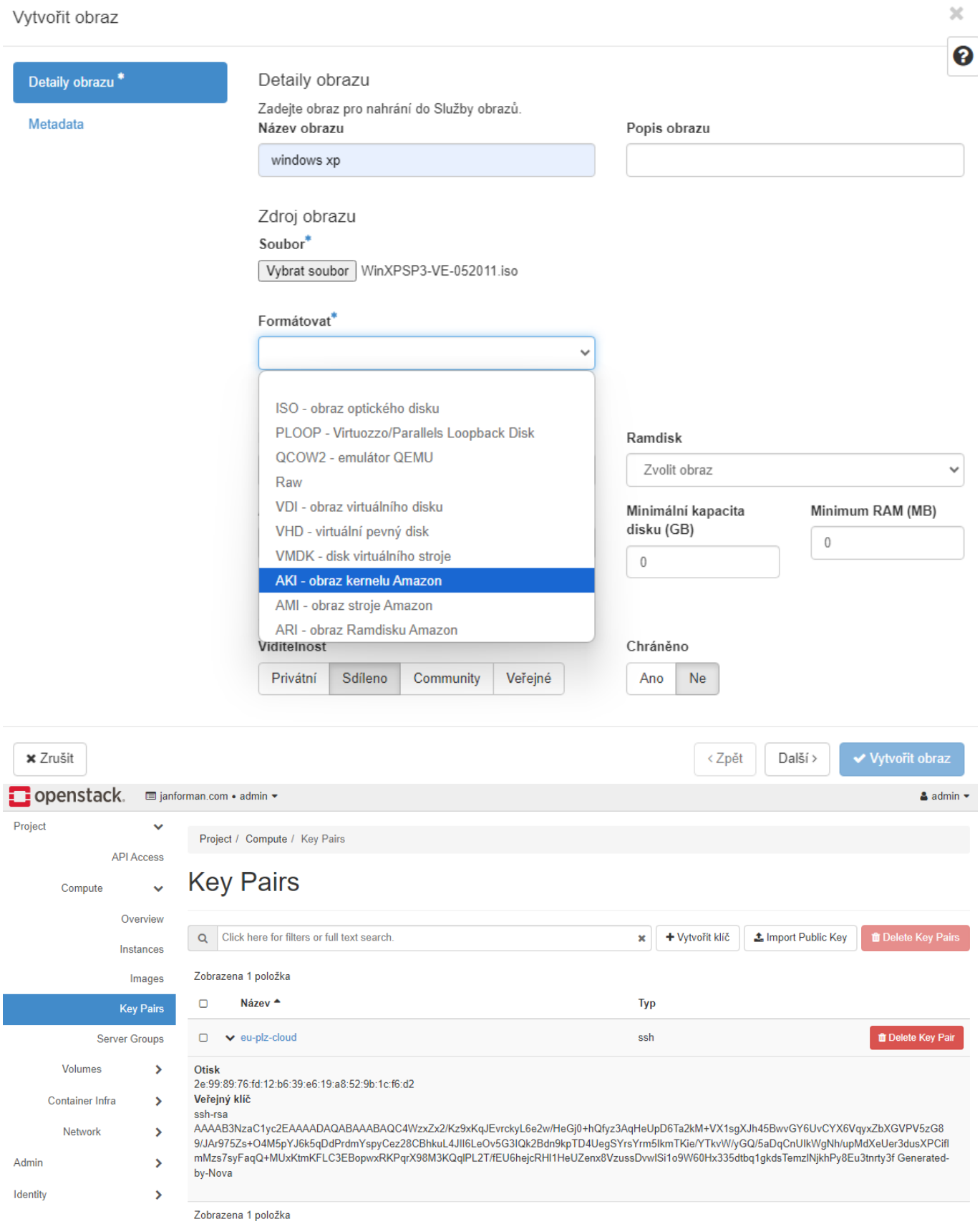
CEPH	**Pros**	**Cons**
	No single point of failure	Complex
	Data durability via replication or erasure coding	minimum 8nodes+ recommended
	No interruption of service from rolling upgrades, online expansion, etc.	QoS on pool
	A single cluster can serve object, block, and file	
	Compatibility with Openstack, S3, K8s, Proxmox	
Notable known references		
Approx 3500 clusters worldwide with more than 1.5EB capacity		
CERN storage services and its support of experiments, 37000 users 5100 projects in data centers.		
SAMSUNG	CHINA MOBILE	DigitalOcean
My experience from 7.3.2018 in production 18TB MLC AllFlash		

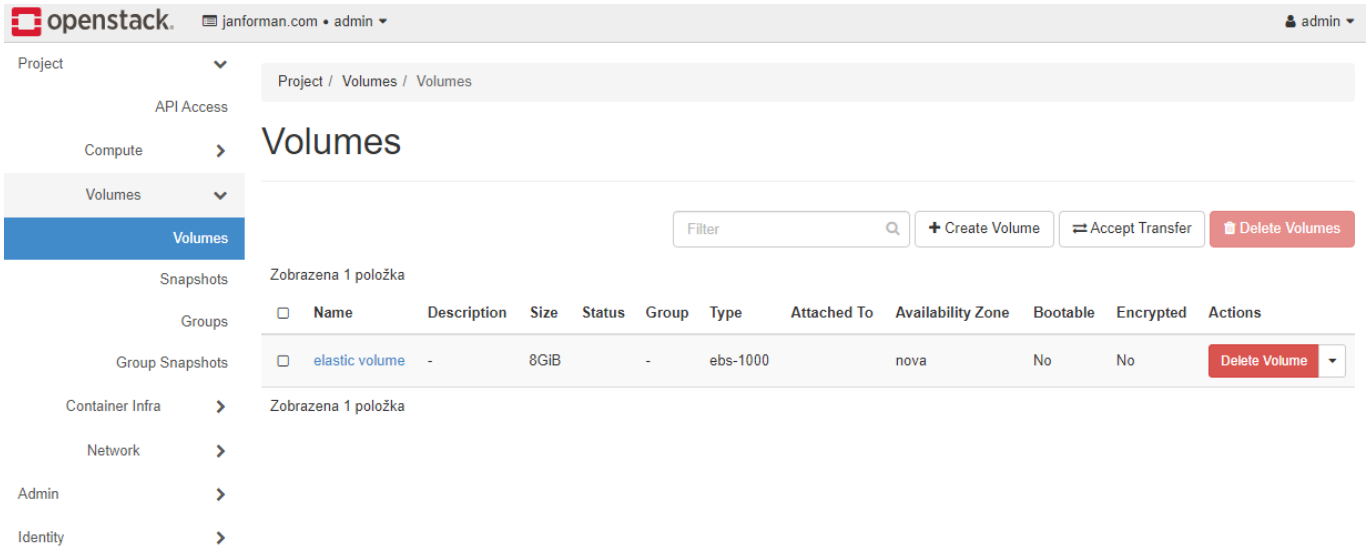
Competitors Dell Isilon Dell Powerflex
You may connect storage nodes with one network card and compute nodes with two (in LACP mode)

Openstack

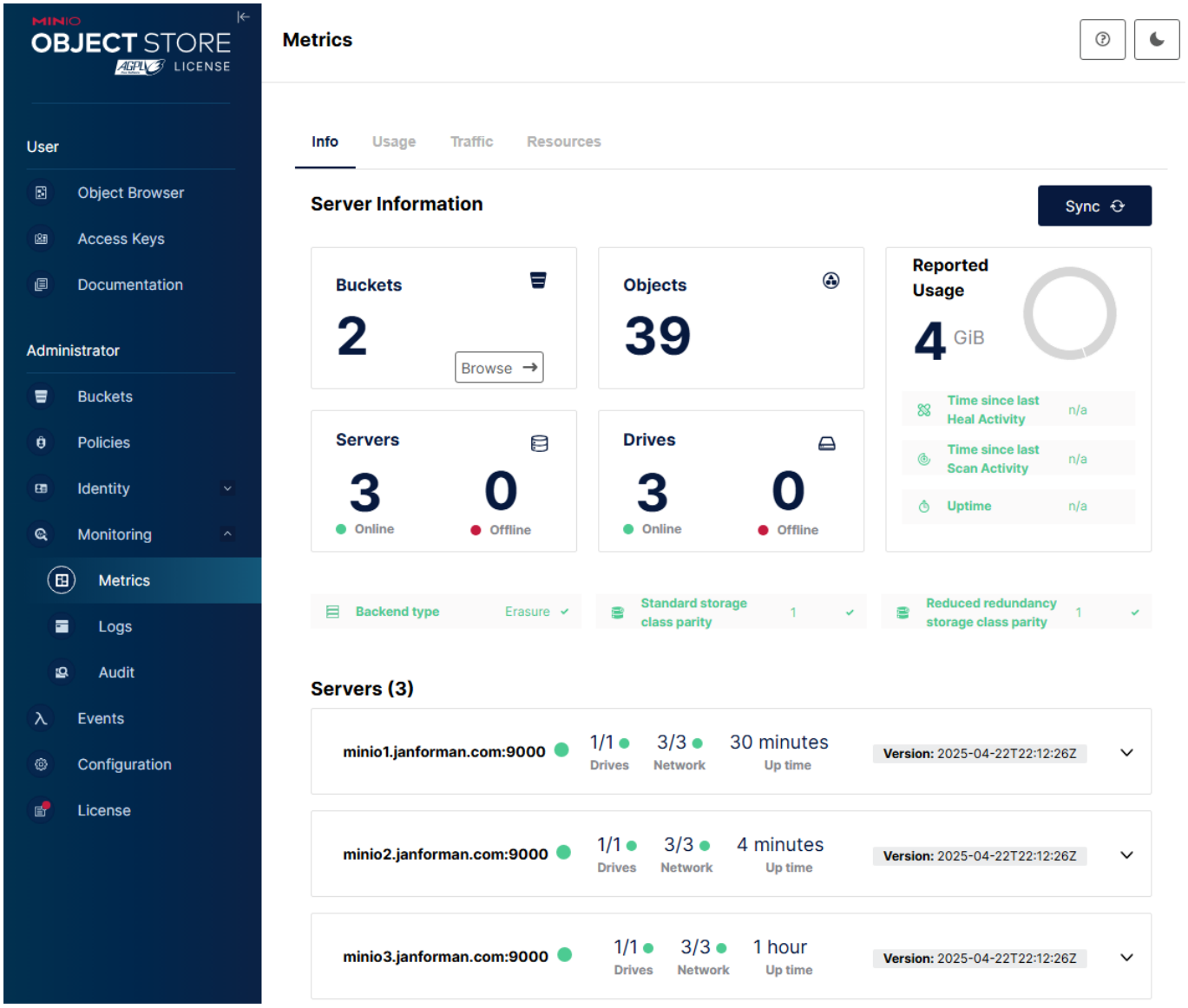



Spustit instanci
Podrobnosti
Zdroj
Typ
Sítě
Síťové porty
Bezpečnostní skupiny
Key Pair
Konfigurace
Skupiny serverů
Plánovač pokynů
Metadata
Typy určují velikost výpočetních, pamětních a úložných možností instance.
Přiděleno
Zobrazena 1 položka
Název VCPUS RAM Celková kapacita disku Systémový disk Efemérní disk Veřejné
t4g.small 2 8 MB 8 GB 0 GB 8 GB Ano
Zobrazena 1 položka
Dostupné 4
Vyberte jeden
Click here for filters or full text search.
Zobrazeny 4 položky
Název VCPUS RAM Celková kapacita disku Systémový disk Efemérní disk Veřejné
m1.tiny 1 512 MB 4 GB 4 GB 0 GB Ano
m1.small 1 2 GB 30 GB 30 GB 0 GB Ano
m1.medium 2 4 GB 60 GB 60 GB 0 GB Ano
m1.large 4 8 GB 90 GB 90 GB 0 GB Ano
Zobrazeny 4 položky
Zrušit
‹ Zpět
Další ›
Spustit instanci


Vytvořit obraz
Detaily obrazu *
Metadata
Detaily obrazu
Zadejte obraz pro nahrání do Služby obrazů.
Název obrazu
windows xp
Popis obrazu
Zdroj obrazu
Soubor*
Vybrat soubor
WinXPSP3-VE-052011.iso
Formátovat*
ISO - obraz optického disku
PLOOP - Virtuozzo/Parallels Loopback Disk
QCOW2 - emulátor QEMU
Raw
VDI - obraz virtuálního disku
VHD - virtuální pevný disk
VMDK - disk virtuálního stroje
AKI - obraz kernelu Amazon
AMI - obraz stroje Amazon
ARI - obraz Ramdisku Amazon
Ramdisk
Zvolit obraz
Minimální kapacita disku (GB)
0
Minimum RAM (MB)
0
Viditelnost
Privátní
Sdíleno
Community
Veřejné
Chráněno
Ano
Ne
Zrušit
Zpět
Další
Vytvořit obraz
openstack.
janforman.com • admin
admin
Project
API Access
Compute
Overview
Instances
Images
Key Pairs
Server Groups
Volumes
Container Infra
Network
Admin
Identity
Project / Compute / Key Pairs
Key Pairs
Click here for filters or full text search.
Vytvořit klíč
Import Public Key
Delete Key Pairs
Zobrazena 1 položka
Název
Typ
eu-plz-cloud
ssh
Delete Key Pair
Otisk
2e:99:89:76:fd:12:b6:39:e6:19:a8:52:9b:1c:f6:d2
Veřejný klíč
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQC4WzxZx2/Kz9xKqJEvrckyL6e2w/HeGj0+hQfyz3AqHeUpD6Ta2kM+VX1sgXJh45BwvGY6UvCYX6VqyxZbXGVPV5zG89/JAr975Zs+O4M5pYJ6k5qDdPrdmYspyCez28CBhkuL4JII6LeOv5G3IQk2Bdn9kpTD4UegSYrsYrm5IkmTKie/YTkvW/yGQ/5aDqCnUIkWgNh/upMdXeUer3dusXPCifl
mMzs7syFaqQ+MUxKtmKFLC3EBopwxRKPqrX98M3KQqlPL2T/fEU6hejcRHI1HeUZenx8VzussDvwISi1o9W60Hx335dtbq1gkdsTemzlNjkhPy8Eu3tnrty3f Generated-by-Nova
Zobrazena 1 položka



MINIO S3 service for small networks



CEPH 3node 10gbit performance (KVM-VirtIO)

3 servers with 3xSSD (9 OSD)

Block Size	4k	(IOPS)	64k	(IOPS)
Read	49.45 MB/s	(12.3k)	220.80 MB/s	(3.4k)
Write	49.54 MB/s	(12.3k)	221.96 MB/s	(3.4k)
Total	98.99 MB/s	(24.7k)	442.76 MB/s	(6.9k)
Block Size	512k	(IOPS)	1m	(IOPS)
Read	597.15 MB/s	(1.1k)	663.25 MB/s	(647)
Write	628.88 MB/s	(1.2k)	707.43 MB/s	(690)
Total	1.22 GB/s	(2.3k)	1.37 GB/s	(1.3k)

CEPH Performance Proxmox

https://www.proxmox.com/images/download/pve/docs/Proxmox-VE-Ceph-Benchmark-202312-rev0.pdf

https://cilium.io

From:
https://wiki.janforman.com/ - **wiki.janforman.com**

Permanent link:
https://wiki.janforman.com/microcloud

Last update: **2026/01/21 10:12**