Υποδομές Cloud

Διάλεξη 4η

Θωμάς Καμαλάκης

Χαροκόπειο Πανεπιστήμιο Αθηνών

Χειμερινό Εξάμηνο, 2024

Περιεχόμενα

1. Proxmox Setup
2. Διαχείριση από το UI
3. ZFS
4. Ceph
5. HCI
6. Proxmox Features

Proxmox SSO

- Το επόμενο βήμα είναι να επιτρέψουμε σε χρήστες του Πανεπιστήμιου να χάνουν χρήση του Proxmox.
- Αυτό μπορεί να γίνει είτε χρησιμοποιώντας έναν LDAP server είτε έναν OpenID provider.
- Στο ίδρυμα χρησιμοποιούμε και τα δύο.
- Επιλέγουμε να διασυνδεθούμε μέσω του ιδρυματικού openldap server.

LDAP server

- Ένας LDAP server (Lightweight Directory Access Protocol server) είναι ένας διακομιστής που χρησιμοποιεί το πρωτόκολλο LDAP για την αποθήκευση, ανάκτηση και διαχείριση δεδομένων καταλόγου.
- Είναι ένα ελαφρύ πρωτόκολλο πρόσβασης σε καταλόγους, που χρησιμοποιείται κυρίως για την αποθήκευση και οργάνωση πληροφοριών σχετικά με χρήστες, ομάδες, υπολογιστές και άλλους πόρους δικτύου.

LDAP server

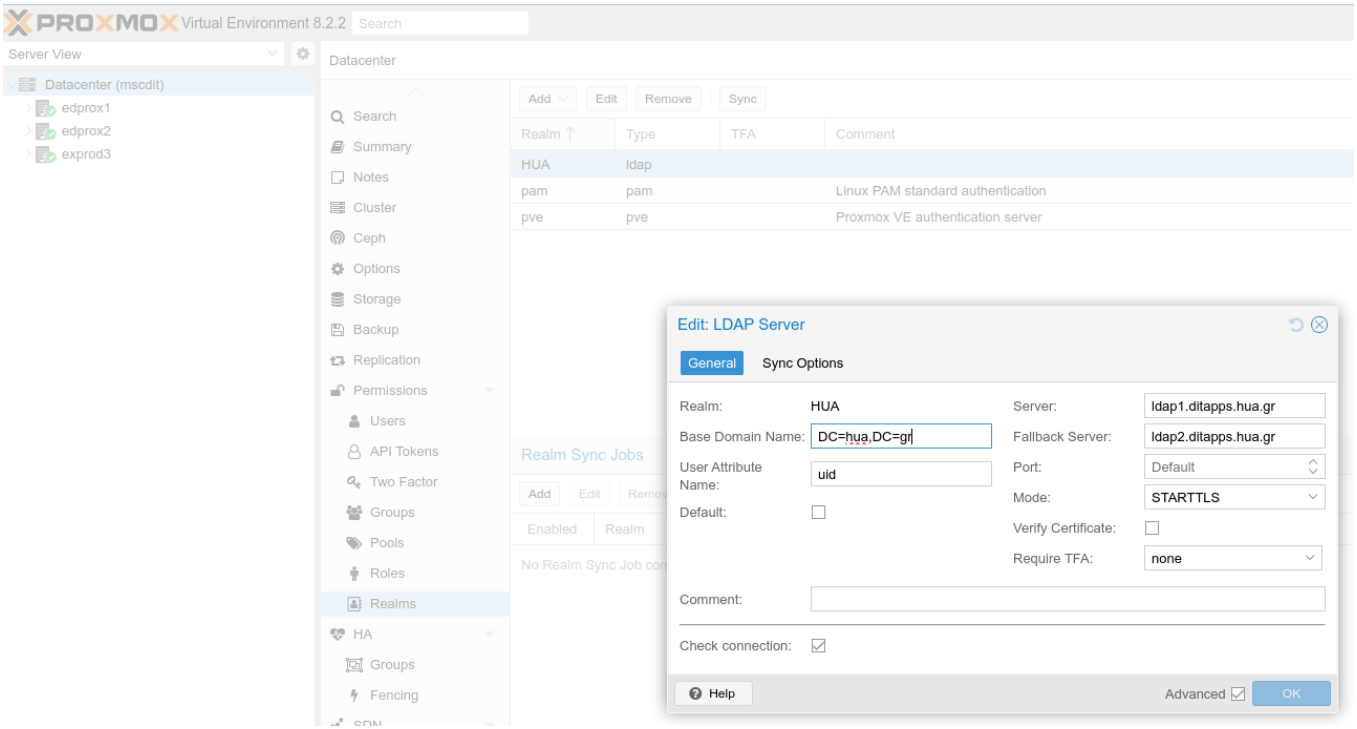
- Αποθήκευση πληροφοριών: Τα δεδομένα καταλόγου, όπως ονόματα χρηστών, κωδικοί πρόσβασης, διευθύνσεις email κ.λπ., αποθηκεύονται σε μια δομή δέντρου.
- Αναζήτηση και αυθεντικοποίηση: Οι χρήστες ή εφαρμογές μπορούν να κάνουν αναζητήσεις στον κατάλογο ή να αυθεντικοποιηθούν (δηλ. να συνδεθούν) μέσω LDAP.
- Κεντρική διαχείριση χρηστών: Ένας LDAP server επιτρέπει την κεντρική διαχείριση των λογαριασμών χρηστών σε ένα δίκτυο, διευκολύνοντας την διαχείριση πρόσβασης.

LDAP server

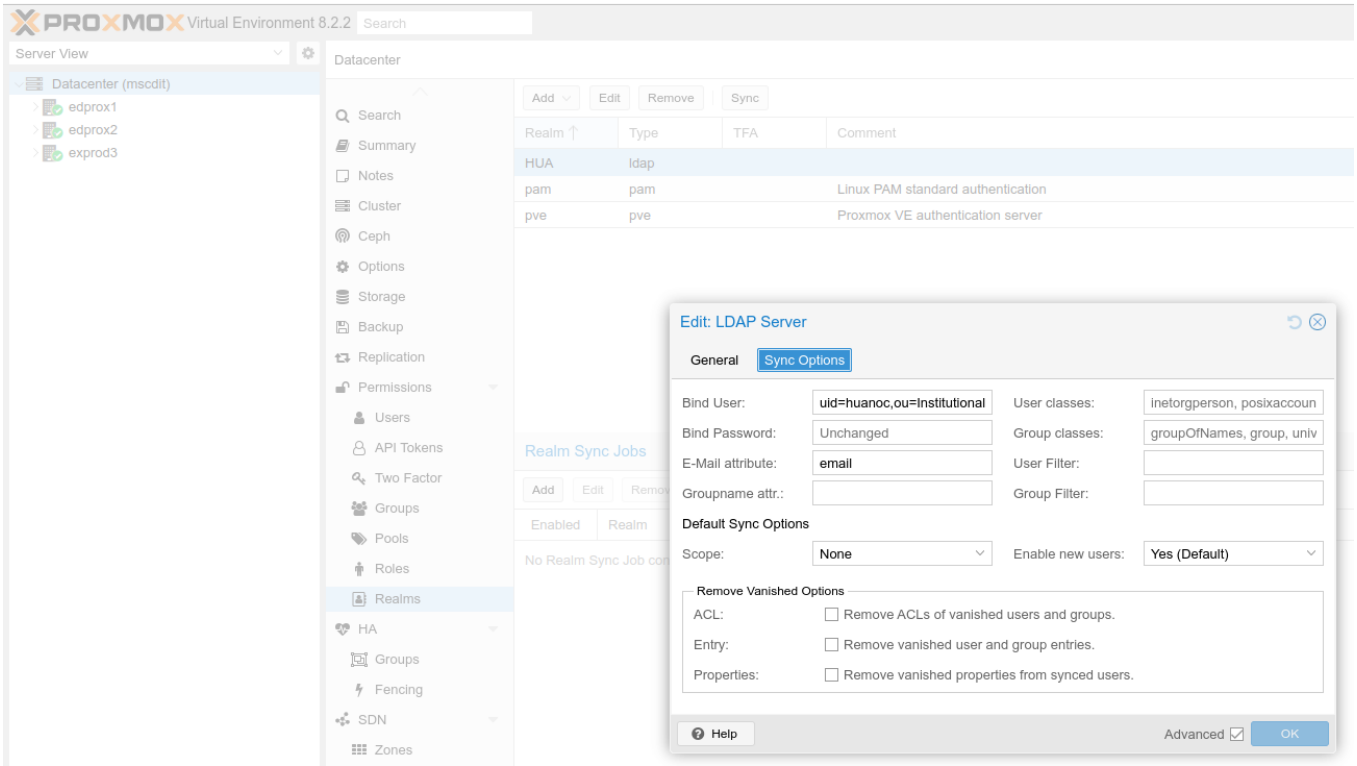
- OpenLDAP: Ανοιχτού κώδικα LDAP server που χρησιμοποιείται ευρέως σε περιβάλλοντα Linux και Unix. Προσφέρει μεγάλη ευελιξία και δυνατότητα επέκτασης.
- Microsoft Active Directory: Χρησιμοποιείται στα περισσότερα Windows domains. Επεκτείνεται και με περισσότερες λειτουργίες
- Apache Directory Server (ApacheDS): Opensource από το Apache Software Foundation. Ενσωματώνει επίσης και άλλα πρωτόκολλα, όπως Kerberos.
- Samba DC (open source AD!)

3

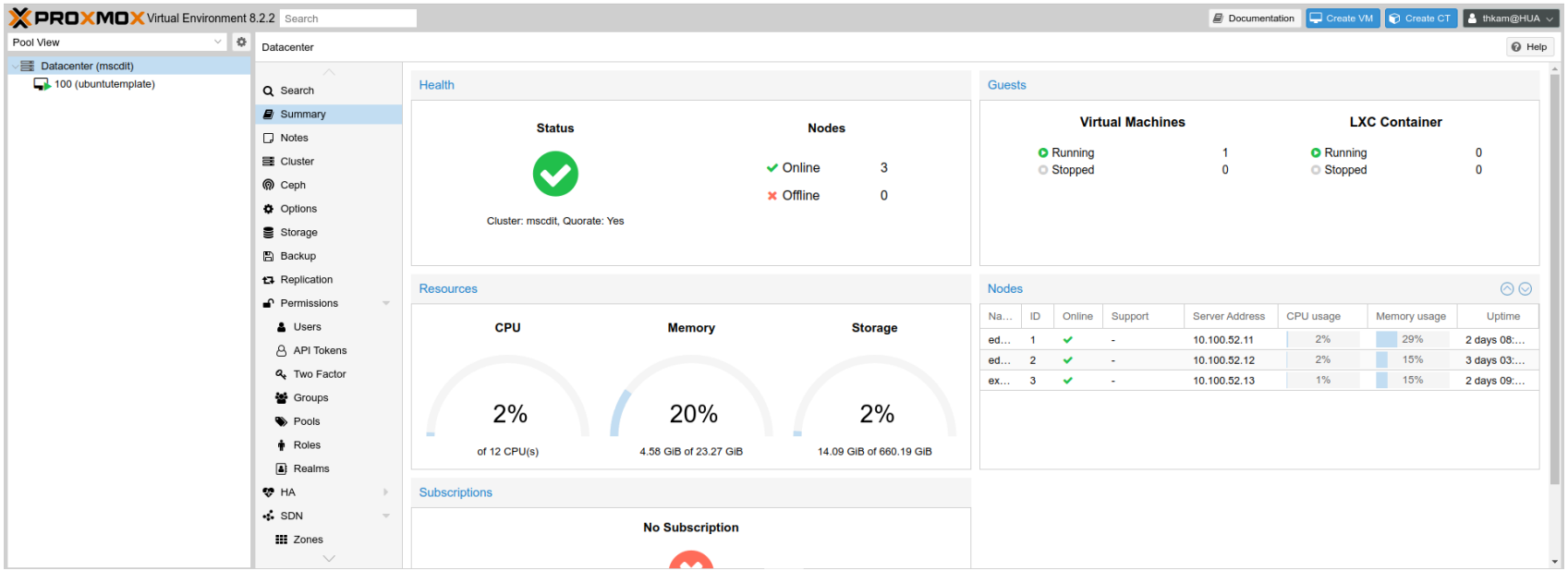
Proxmox SSO


PROXMOX Virtual Environment 8.2.2
Search
Server View
Datacenter (mscdit)
edprox1
edprox2
exprod3
Datacenter
Search
Summary
Notes
Cluster
Ceph
Options
Storage
Backup
Replication
Permissions
Users
API Tokens
Two Factor
Groups
Pools
Roles
Realms
HA
Groups
Fencing
Add
Edit
Remove
Sync
Realm
Type
TFA
Comment
HUA
ldap
pam
pam
Linux PAM standard authentication
pve
pve
Proxmox VE authentication server
Realm Sync Jobs
Enabled
Realm
Edit: LDAP Server
General
Sync Options
Realm:
HUA
Base Domain Name:
DC=hua,DC=gr
User Attribute Name:
uid
Default:
Server:
ldap1.ditapps.hua.gr
Fallback Server:
ldap2.ditapps.hua.gr
Port:
Default
Mode:
STARTTLS
Verify Certificate:
Require TFA:
none
Comment:
Check connection:
Help
Advanced
OK

Proxmox SSO


PROXMOX Virtual Environment 8.2.2
Search
Server View
Datacenter (mscdit)
edprox1
edprox2
exprod3
Datacenter
Search
Summary
Notes
Cluster
Ceph
Options
Storage
Backup
Replication
Permissions
Users
API Tokens
Two Factor
Groups
Pools
Roles
Realms
HA
Groups
Fencing
SDN
Zones
Add
Edit
Remove
Sync
Realm
Type
TFA
Comment
HUA
ldap
pam
pam
Linux PAM standard authentication
pve
pve
Proxmox VE authentication server
Realm Sync Jobs
Add
Edit
Enabled
Realm
Edit: LDAP Server
General
Sync Options
Bind User:
uid=huanoc,ou=Institutional
Bind Password:
Unchanged
E-Mail attribute:
email
Groupname attr.:
User classes:
inetorgperson, posixaccoun
Group classes:
groupOfNames, group, univ
User Filter:
Group Filter:
Default Sync Options
Scope:
None
Enable new users:
Yes (Default)
Remove Vanished Options
ACL:
Remove ACLs of vanished users and groups.
Entry:
Remove vanished user and group entries.
Properties:
Remove vanished properties from synced users.
Help
Advanced
OK

Το Proxmox UI



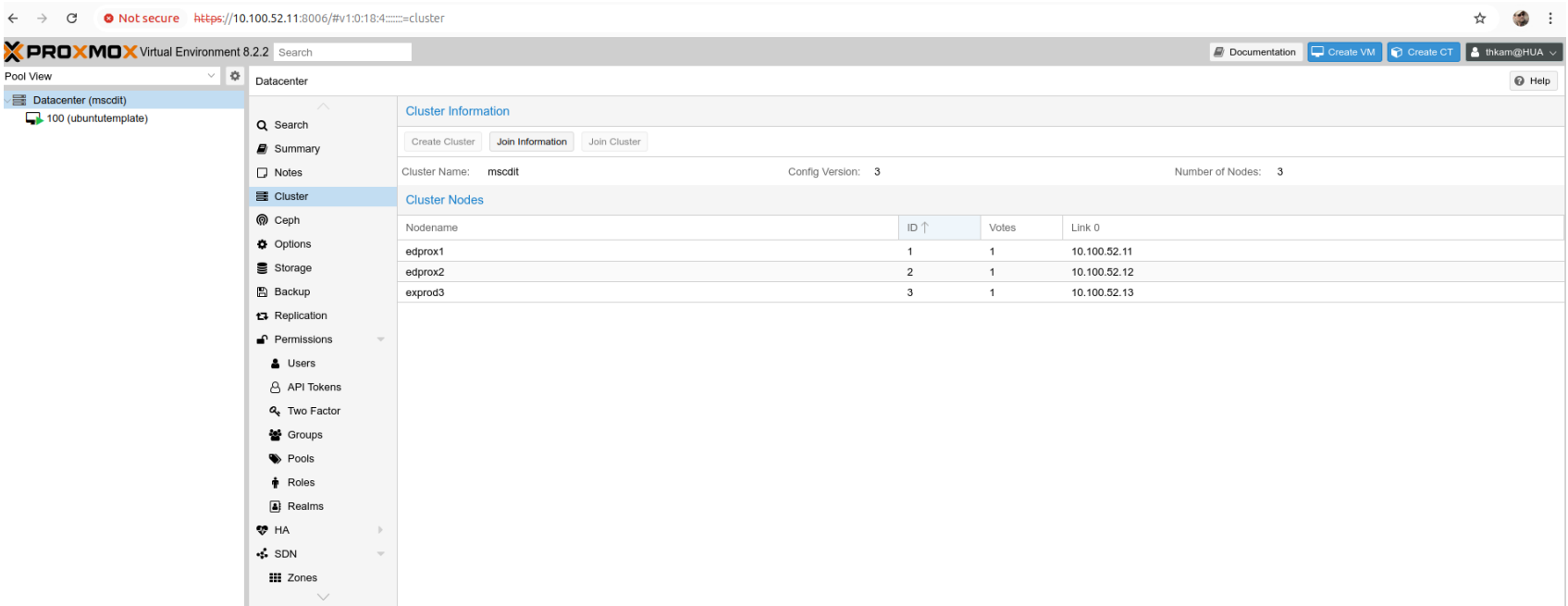
Summary

- Το Summary μας δίνει ένα απλό Dashboard που περιγράφει την κατάσταση του cluster μας.
- Δηλαδή πόσα nodes είναι ζωντανά, την συνολική κατανάλωση μνήμης και δίσκου κτλ.

Notes

- Αν το επιθυμούμε μπορούμε να προσθέσουμε σημειώσεις.
- Κάτι σαν του READ.ME του git δηλαδή

Cluster


Not secure https://10.100.52.11:8006/#v1:0:18:4:::::=cluster
PROXMOX Virtual Environment 8.2.2
Search
Documentation
Create VM
Create CT
thkam@HUA
Pool View
Datacenter (mscdit)
100 (ubuntutemplate)
Datacenter
Help
Search
Summary
Notes
Cluster
Ceph
Options
Storage
Backup
Replication
Permissions
Users
API Tokens
Two Factor
Groups
Pools
Roles
Realms
HA
SDN
Zones
Cluster Information
Create Cluster
Join Information
Join Cluster
Cluster Name: mscdit
Config Version: 3
Number of Nodes: 3
Cluster Nodes
Nodename
ID
Votes
Link 0
edprox1 1 1 10.100.52.11
edprox2 2 1 10.100.52.12
exprod3 3 1 10.100.52.13

Cluster

- Εδώ βλέπουμε πληροφορίες που αφορούν το cluster.
- Επίσης προσθέτουμε και αφαιρούμε κόμβους στο cluster.

Options

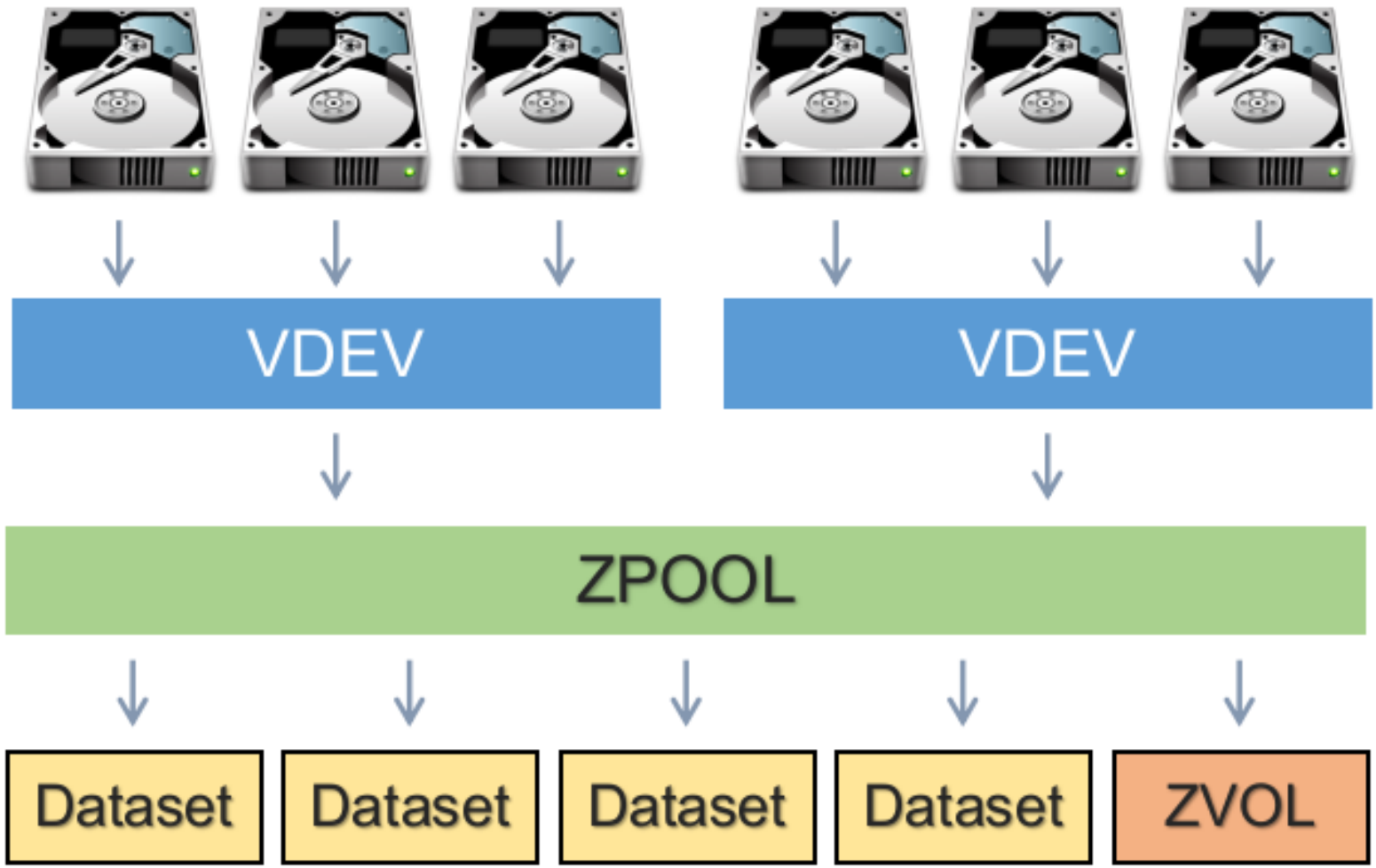
- Στην καρτέλα Options μπορούμε να ορίσουμε μερικές επιπλέον ρυθμίσεις του cluster.
- Default MAC addresses
- Default console
- Bandwidth limits
- ...

Storage

- Στην καρτέλα Storage βλέπουμε τα storage devices που είναι διαθέσιμα στο cluster μας.
- local (/var/lib/vz): Ένας default προορισμός για τα VM για ISOs, templates και backups.
- local-lvm: default προορισμός για VM disks.
- Συνήθως χρησιμοποιούμε κάποιο shared storage αντί για αυτά.

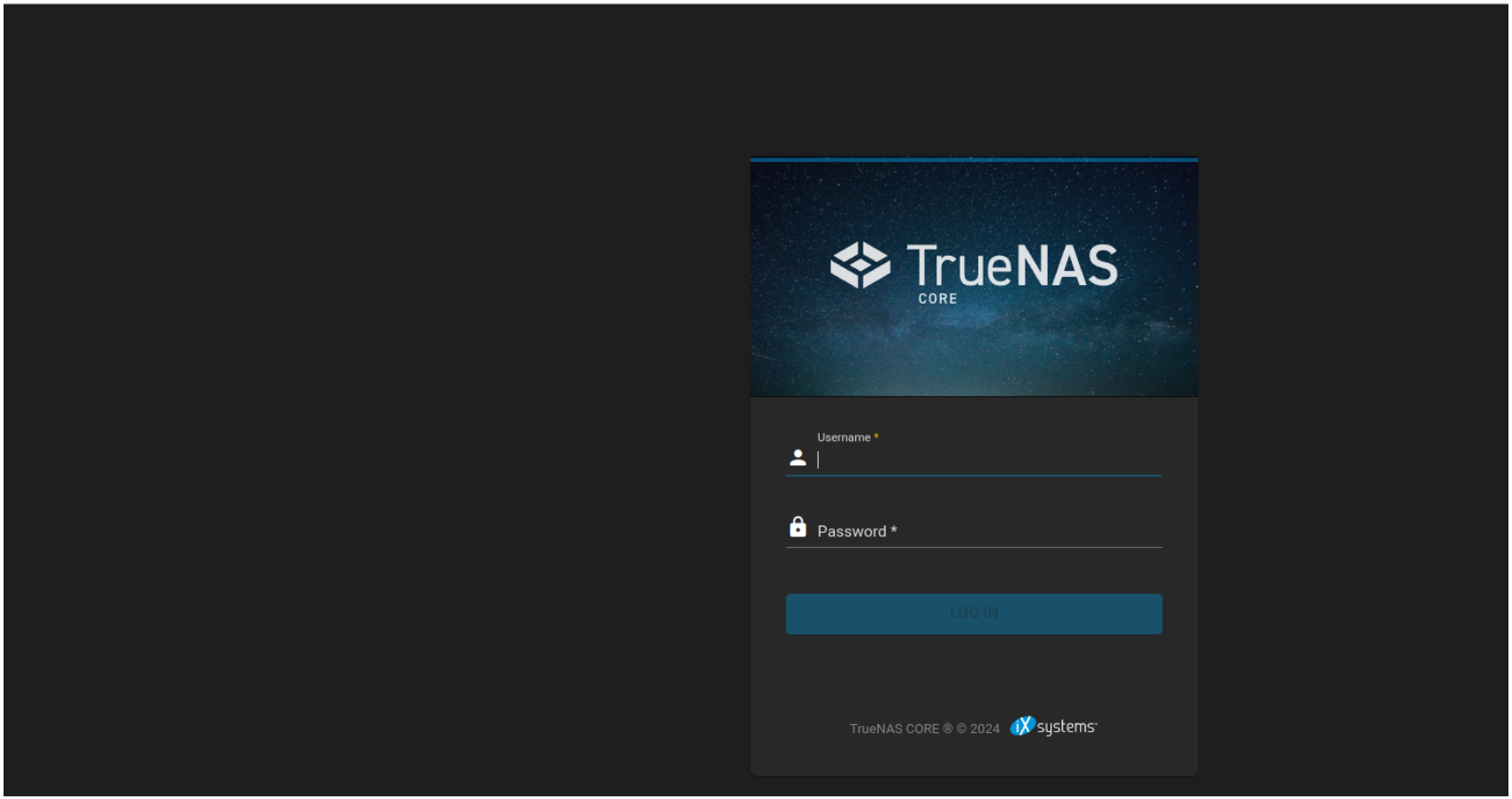
ZFS

- ZFS (Zettabyte File System): Σύστημα αρχείων και διαχείρισης αποθηκευτικού χώρου που χρησιμοποιείται ευρέως για την ανθεκτικότητα του και τις δυνατότητές του.
- Copy-on-Write (COW): όταν γίνεται τροποποίηση δεδομένων, το ZFS δεν αντικαθιστά τα αρχικά δεδομένα απευθείας.
- Έτσι το σύστημα παραμένει συνεπές ακόμη και σε περίπτωση διακοπής ή σφάλματος κατά τη διάρκεια της εγγραφής.
- Επιτρέπει τη δημιουργία snapshots, τα οποία είναι σημεία στο χρόνο που «παγώνουν» την κατάσταση του συστήματος αρχείων.
- Τα snapshots καταλαμβάνουν ελάχιστο χώρο και μπορούν να ληφθούν χωρίς να διακόψουν τη λειτουργία του συστήματος.


VDEV
VDEV
ZPOOL
Dataset
Dataset
Dataset
Dataset
ZVOL

ZFS

- Το ZFS χρησιμοποιεί pools, όπου οι συσκευές αποθήκευσης μπορούν να προστεθούν και να αφαιρεθούν δυναμικά.
- Το ZFS ενσωματώνει μια παραλλαγή του RAID που ονομάζεται RAID-Z όπου η απώλεια περισσότερων από έναν δίσκων μπορεί να οδηγήσει σε απώλεια δεδομένων.
- Υποστηρίζει δυναμικές αλλαγές στο μέγεθος του αποθηκευτικού χώρου χωρίς διακοπή λειτουργίας.


TrueNAS
CORE
Username *
Password *
LOG IN
TrueNAS CORE ® © 2024
iXsystems

TrueNAS

- Μια λύση ανοιχτού κώδικα (open-source) για Network Attached Storage (NAS).
- Χρησιμοποιεί το σύστημα αρχείων ZFS
- Web-based πίνακα ελέγχου (GUI)
- Μπορεί να διαθέσει σε διάφορες συσκευές και χρήστες μέσω πρωτοκόλλων όπως SMB, NFS, iSCSI, FTP, και AFP.
- Βασίζεται στο FreeBSD (!)

FreeBSD

- Το FreeBSD είναι ένα λειτουργικό σύστημα ανοιχτού κώδικα που βασίζεται στο Unix και έχει τις ρίζες του στο Berkeley Software Distribution (BSD),
- Πρόκειται για μια έκδοση του Unix που αναπτύχθηκε στο Πανεπιστήμιο της Καλιφόρνιας στο Μπέρκλεϊ.
- Ενσωματώνει το σύστημα αρχείων ZFS
- Είναι βάση για το TrueNAS και το Junos OS της Juniper Networks, που χρησιμοποιείται σε δρομολογητές και switch.
- Το λειτουργικό σύστημα του PlayStation 4 (που ονομάζεται Orbis OS) είναι μια τροποποιημένη έκδοση του FreeBSD.

FreeBSD

- Το pfSense είναι μια δημοφιλής λύση ανοιχτού κώδικα για firewall και δρομολόγηση (routing), που βασίζεται στο FreeBSD.
- Στο παρελθόν, το backend του WhatsApp (όταν ανήκε στην Facebook) χρησιμοποιούσε το FreeBSD.
- Το Citrix NetScaler, μια λύση για εξισορρόπηση φορτίου (load balancing) και βελτιστοποίηση εφαρμογών δικτύου, βασίζεται σε μεγάλο βαθμό στο FreeBSD.

Proxmox και TrueNAS

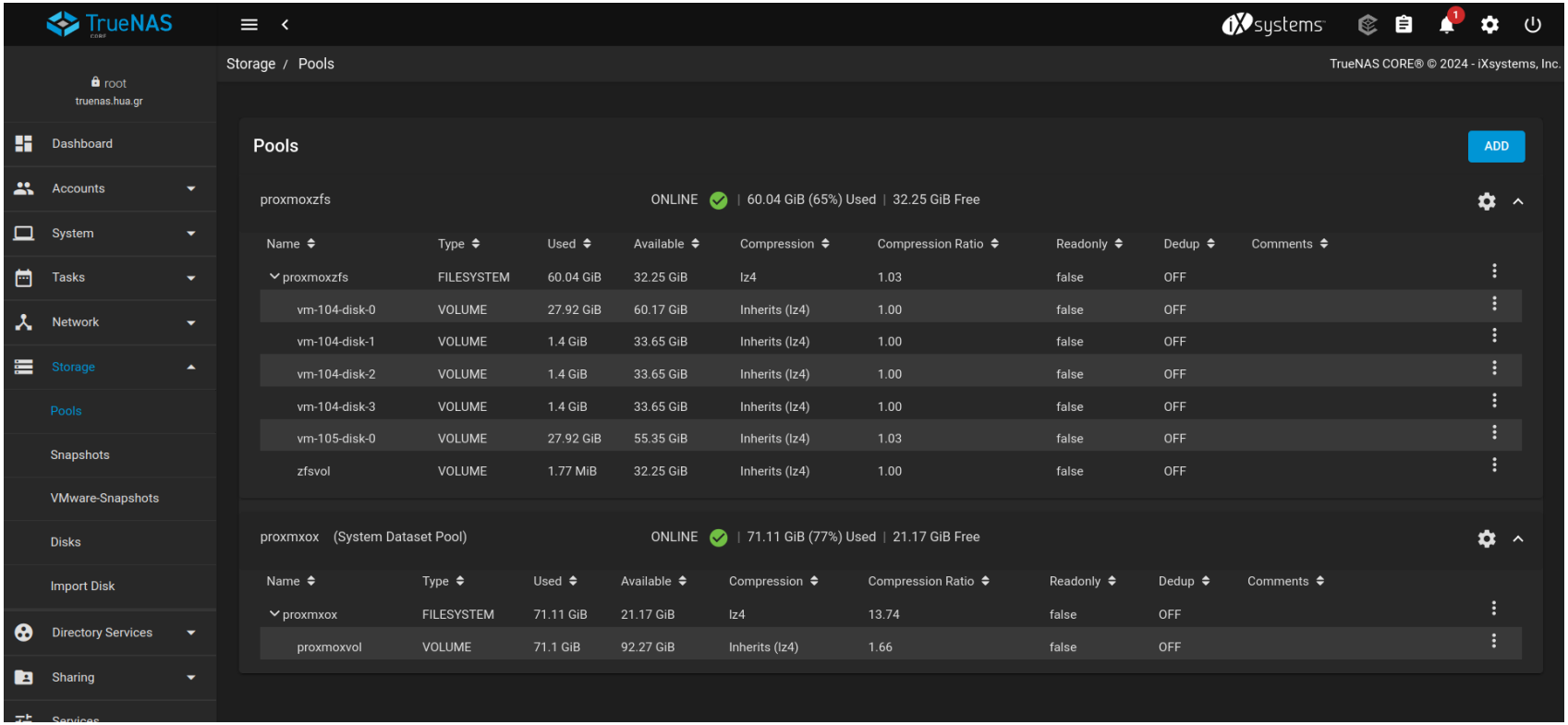
- Υπάρχουν διάφοροι τρόποι να χρησιμοποιήσουμε το TrueNAS ως shared storage στο Proxmox.
- Θα μπορούσαμε να εξάγουμε με NFS κάποιο ZFS pool.
- Μία άλλη τακτική (και ίσως πιο σωστή) είναι το ZFS over iSCSI.
- Οπότε φτιάχνουμε ένα pool και το εξάγουμε μέσω iSCSI.
- Χρειαζόμαστε ένα Proxmox plugin το `freenas-proxmox`.

Proxmox και TrueNAS

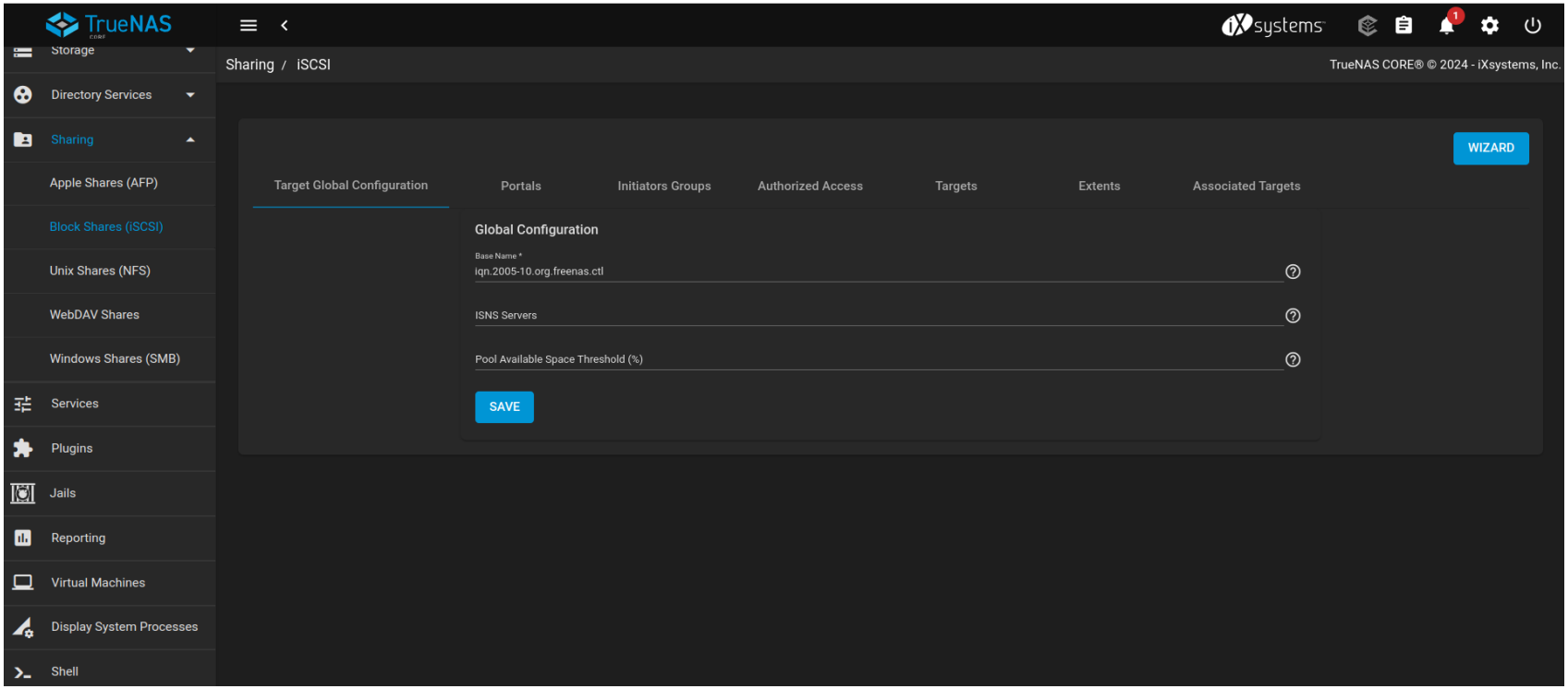
Table 1. Available storage types

Description	Plugin type	Level	Shared	Snapshots	Stable
ZFS (local)	`zfspool`	both[1]	no	yes	yes
Directory	`dir`	file	no	no[2]	yes
BTRFS	`btrfs`	file	no	yes	technology preview
NFS	`nfs`	file	yes	no[2]	yes
CIFS	`cifs`	file	yes	no[2]	yes
Proxmox Backup	`pbs`	both	yes	n/a	yes
GlusterFS	`glusterfs`	file	yes	no[2]	yes
CephFS	`cephfs`	file	yes	yes	yes
LVM	`lvm`	block	no[3]	no	yes
LVM-thin	`lvmthin`	block	no	yes	yes
iSCSI/kernel	`iscsi`	block	yes	no	yes
iSCSI/libiscsi	`iscsidirect`	block	yes	no	yes
Ceph/RBD	`rbd`	block	yes	yes	yes
ZFS over iSCSI	`zfs`	block	yes	yes	yes

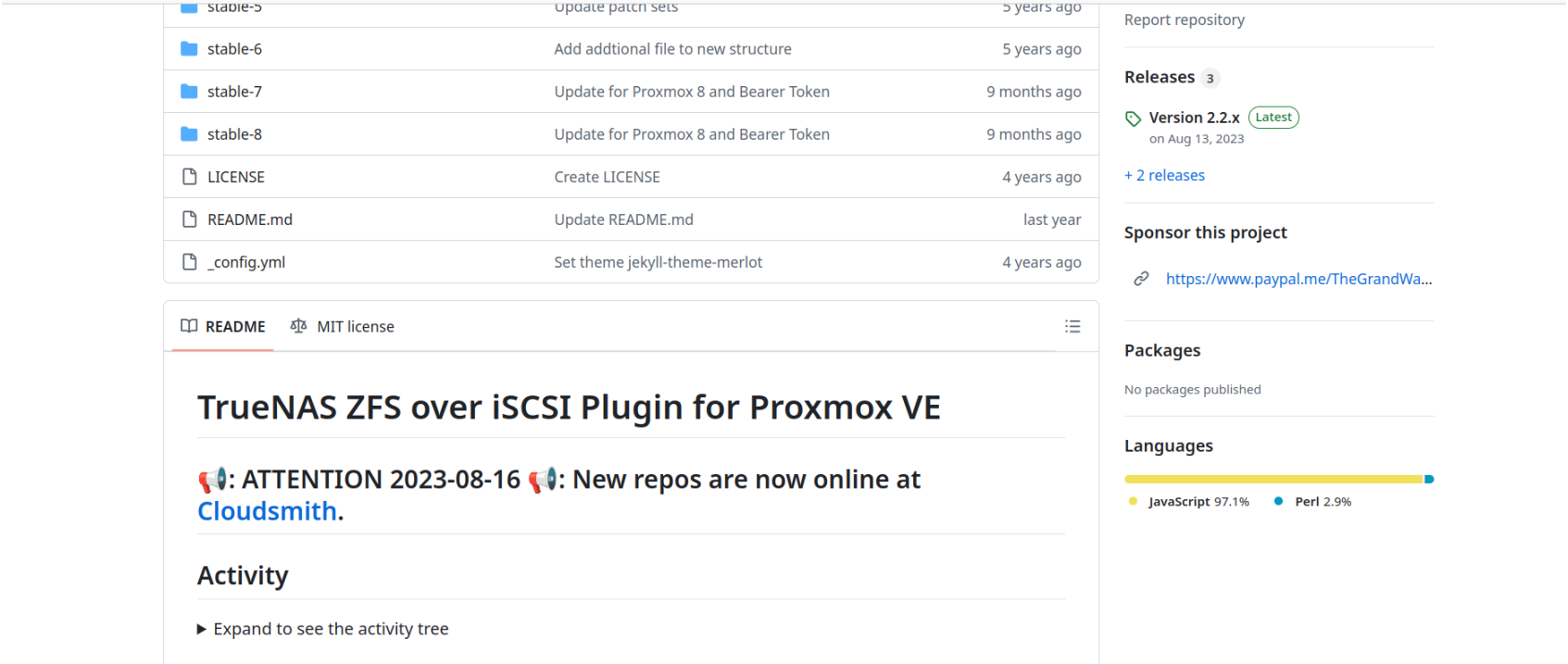
Proxmox και TrueNAS



Proxmox και TrueNAS



Proxmox και TrueNAS



stable-5	Update patch sets	5 years ago
stable-6	Add addtional file to new structure	5 years ago
stable-7	Update for Proxmox 8 and Bearer Token	9 months ago
stable-8	Update for Proxmox 8 and Bearer Token	9 months ago
LICENSE	Create LICENSE	4 years ago
README.md	Update README.md	last year
_config.yml	Set theme jekyll-theme-merlot	4 years ago

README MIT license

TrueNAS ZFS over iSCSI Plugin for Proxmox VE

📢: ATTENTION 2023-08-16 📢: New repos are now online at Cloudsmith.

Activity

▶ Expand to see the activity tree

Report repository

Releases 3

Version 2.2.x Latest
on Aug 13, 2023

+ 2 releases

Sponsor this project

https://www.paypal.me/TheGrandWa...

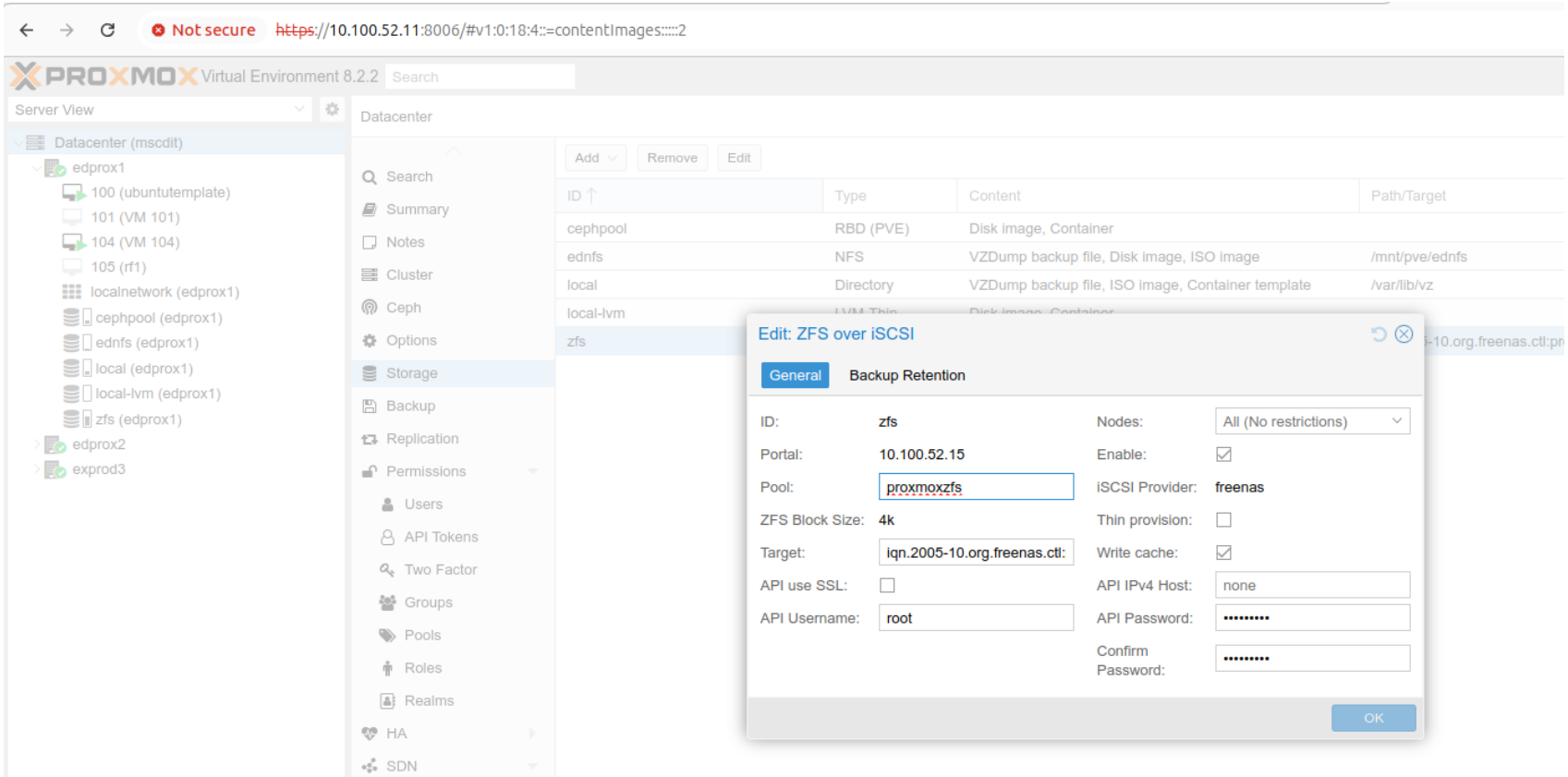
Packages

No packages published

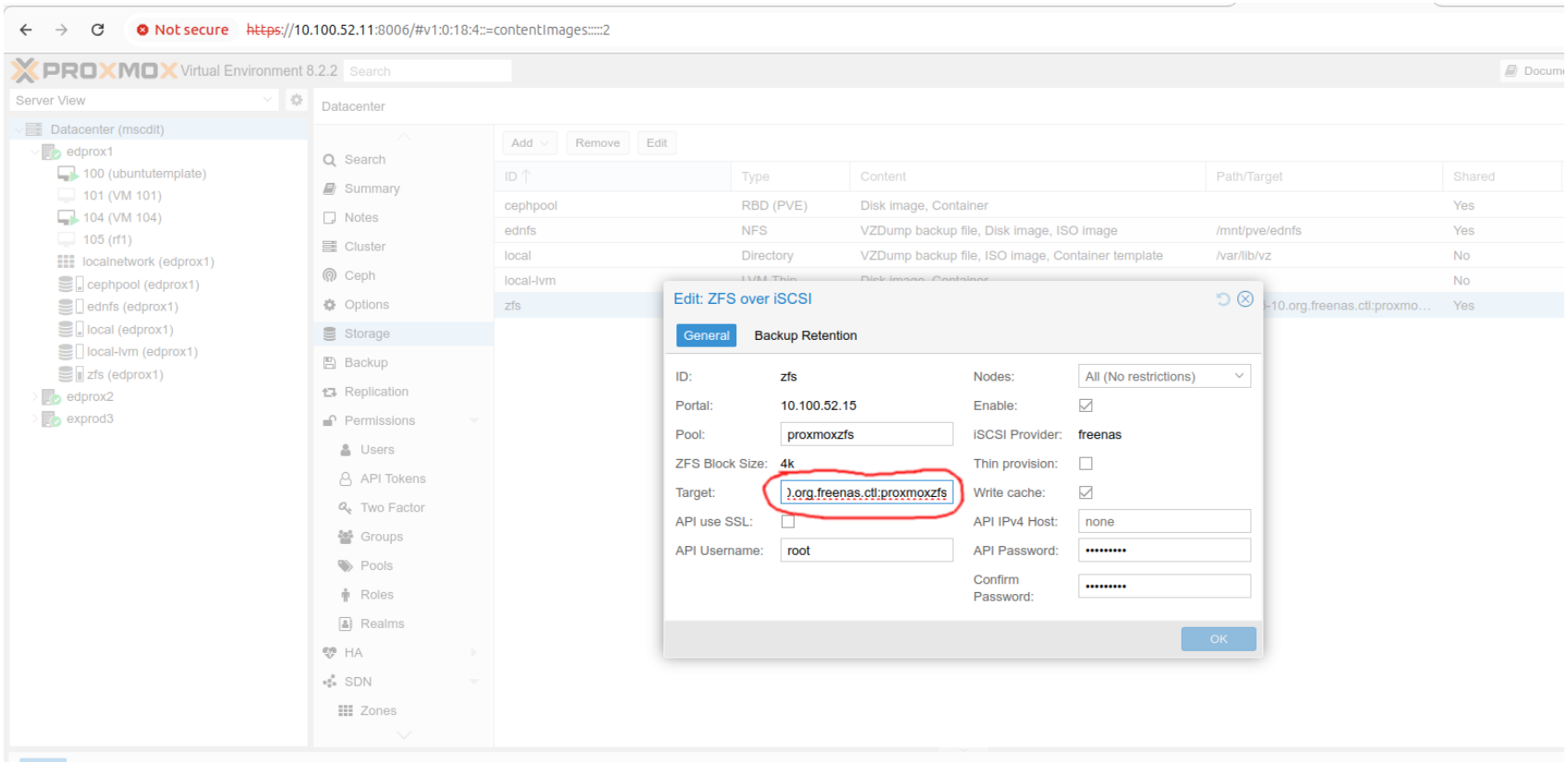
Languages

JavaScript 97.1% Perl 2.9%

Proxmox και TrueNAS



Proxmox και TrueNAS



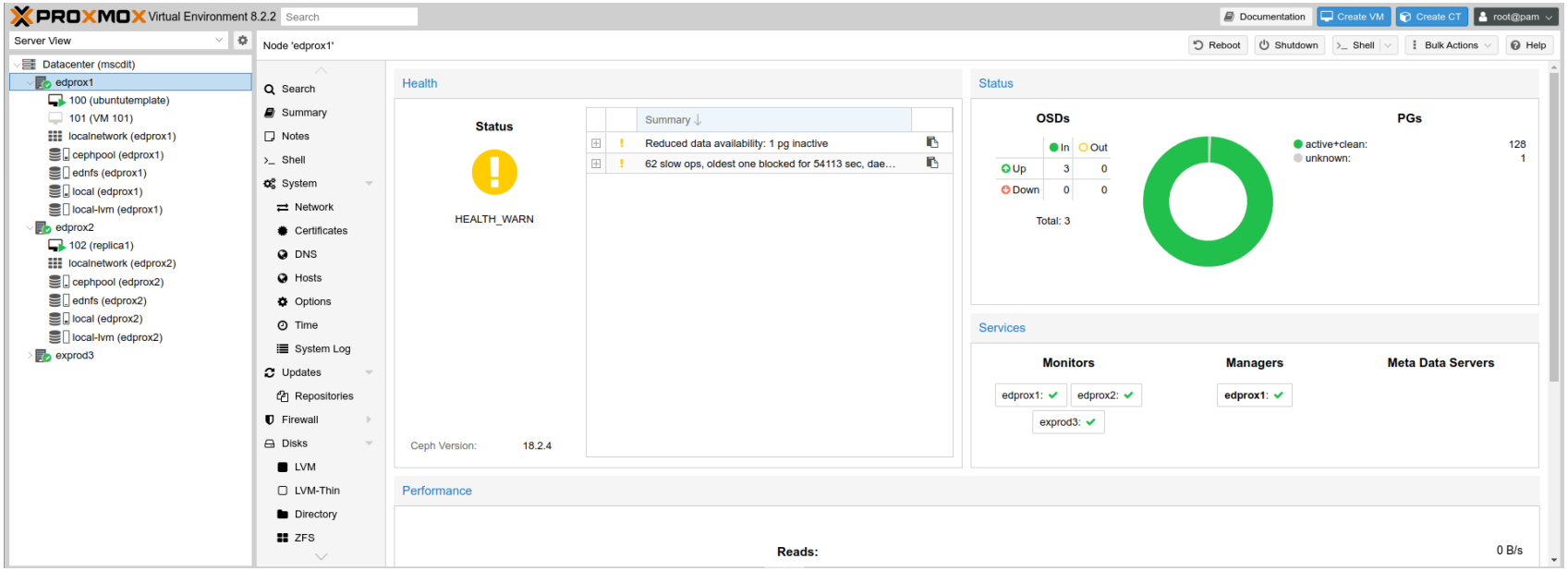
Ceph

- Στην χαρτέλα Ceph βλέπουμε την υγεία του Ceph storage (αν το χρησιμοποιούμε).
- Object Storage Daemon (OSD): Υπεύθυνοι για την αποθήκευση δεδομένων, τη διαχείριση της αντιγραφής, της επαναφοράς και της επανακατανομής των δεδομένων.
- Monitor (MON): παρακολουθούν την κατάσταση του cluster, κρατούν μια κεντρική εικόνα της τοπολογίας του συστήματος και της κατάστασης των κόμβων, των OSDs και των δεδομένων.
- Εξασφαλίζουν τη συνοχή και τον συντονισμό του cluster.

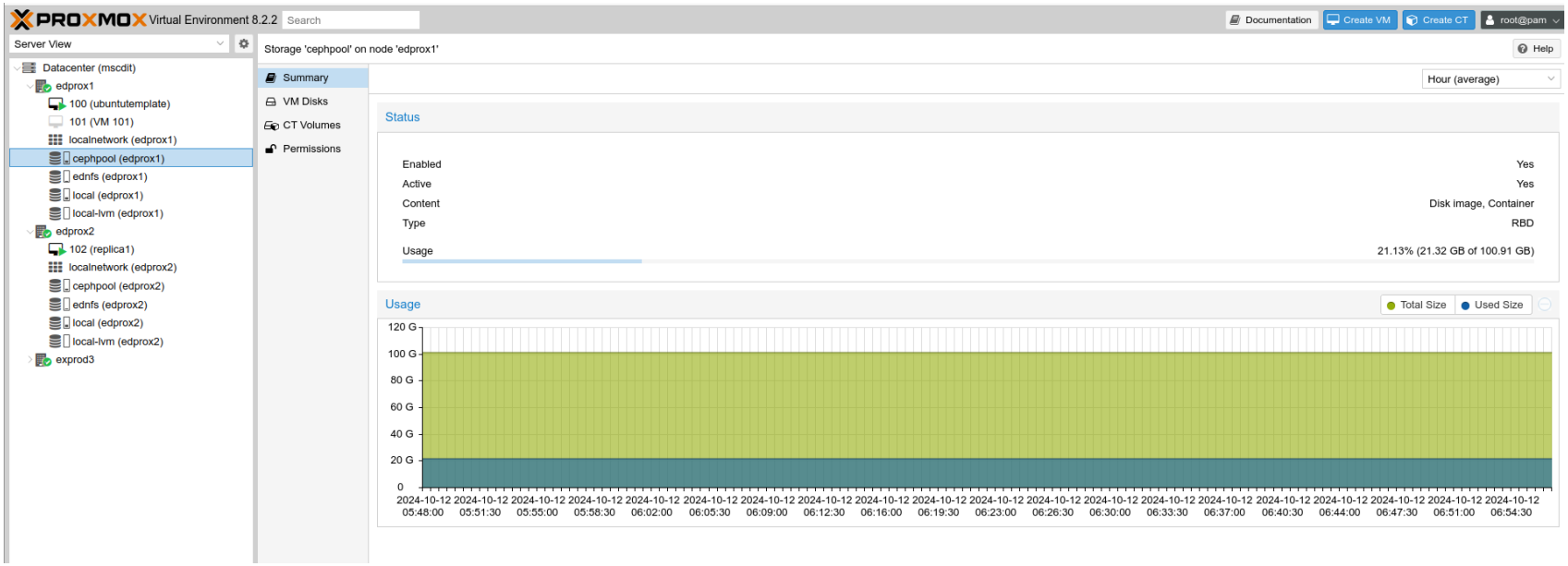
Ceph

- Manager (MGR): συλλέγουν στατιστικά δεδομένα και μετρούν την απόδοση και τη χρήση του συστήματος.
- Metadata Server (MDS): χρησιμοποιούνται στο CephFS (Ceph File System) και είναι υπεύθυνοι για την αποθήκευση των μεταδεδομένων των αρχείων, επιτρέποντας στο σύστημα αρχείων να υποστηρίζει λειτουργίες όπως την αναζήτηση και την πλοήγηση στους φακέλους.
- Pools: Τα δεδομένα στο Ceph αποθηκεύονται σε pools, τα οποία είναι λογικές οντότητες που οργανώνουν τα δεδομένα.

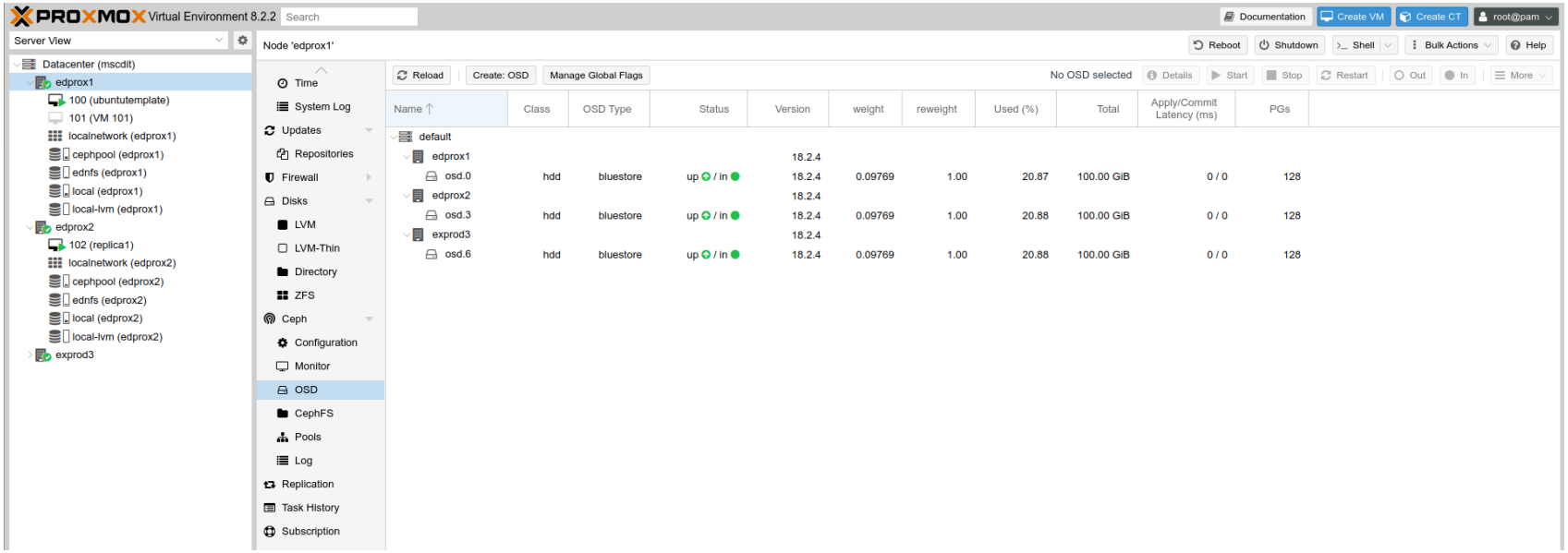
Ceph


PROXMOX Virtual Environment 8.2.2
Search
Documentation
Create VM
Create CT
root@pam
Server View
Node 'edprox1'
Reboot
Shutdown
Shell
Bulk Actions
Help
Datacenter (mscdit)
edprox1
100 (ubuntutemplate)
101 (VM 101)
localnetwork (edprox1)
cephpool (edprox1)
ednfs (edprox1)
local (edprox1)
local-lvm (edprox1)
edprox2
102 (replica1)
localnetwork (edprox2)
cephpool (edprox2)
ednfs (edprox2)
local (edprox2)
local-lvm (edprox2)
exprod3
Search
Summary
Notes
Shell
System
Network
Certificates
DNS
Hosts
Options
Time
System Log
Updates
Repositories
Firewall
Disks
LVM
LVM-Thin
Directory
ZFS
Health
Status
HEALTH_WARN
Summary
Reduced data availability: 1 pg inactive
62 slow ops, oldest one blocked for 54113 sec, dae…
Ceph Version: 18.2.4
Status
OSDs
In
Out
Up
3
0
Down
0
0
Total: 3
PGs
active+clean:
128
unknown:
1
Services
Monitors
edprox1:
edprox2:
exprod3:
Managers
edprox1:
Meta Data Servers
Performance
Reads:
0 B/s

Ceph


PROXMOX Virtual Environment 8.2.2
Search
Documentation
Create VM
Create CT
root@pam
Server View
Storage 'cephpool' on node 'edprox1'
Help
Datacenter (mscdit)
edprox1
100 (ubuntutemplate)
101 (VM 101)
localnetwork (edprox1)
cephpool (edprox1)
ednfs (edprox1)
local (edprox1)
local-lvm (edprox1)
edprox2
102 (replica1)
localnetwork (edprox2)
cephpool (edprox2)
ednfs (edprox2)
local (edprox2)
local-lvm (edprox2)
exprod3
Summary
VM Disks
CT Volumes
Permissions
Hour (average)
Status
Enabled Yes
Active Yes
Content Disk image, Container
Type RBD
Usage 21.13% (21.32 GB of 100.91 GB)
Usage
Total Size
Used Size
120 G
100 G
80 G
60 G
40 G
20 G
0
2024-10-12 05:48:00
2024-10-12 05:51:30
2024-10-12 05:55:00
2024-10-12 05:58:30
2024-10-12 06:02:00
2024-10-12 06:05:30
2024-10-12 06:09:00
2024-10-12 06:12:30
2024-10-12 06:16:00
2024-10-12 06:19:30
2024-10-12 06:23:00
2024-10-12 06:26:30
2024-10-12 06:30:00
2024-10-12 06:33:30
2024-10-12 06:37:00
2024-10-12 06:40:30
2024-10-12 06:44:00
2024-10-12 06:47:30
2024-10-12 06:51:00
2024-10-12 06:54:30

Ceph


PROXMOX Virtual Environment 8.2.2
Search
Documentation
Create VM
Create CT
root@pam
Server View
Node 'edprox1'
Reboot
Shutdown
Shell
Bulk Actions
Help
Datacenter (mscdit)
edprox1
100 (ubuntutemplate)
101 (VM 101)
localnetwork (edprox1)
cephpool (edprox1)
ednfs (edprox1)
local (edprox1)
local-lvm (edprox1)
edprox2
102 (replica1)
localnetwork (edprox2)
cephpool (edprox2)
ednfs (edprox2)
local (edprox2)
local-lvm (edprox2)
exprod3
Time
System Log
Updates
Repositories
Firewall
Disks
LVM
LVM-Thin
Directory
ZFS
Ceph
Configuration
Monitor
OSD
CephFS
Pools
Log
Replication
Task History
Subscription
Reload
Create: OSD
Manage Global Flags
No OSD selected
Details
Start
Stop
Restart
Out
In
More
Name
Class
OSD Type
Status
Version
weight
reweight
Used (%)
Total
Apply/Commit Latency (ms)
PGs
default
edprox1 18.2.4
osd.0 hdd bluestore up / in 18.2.4 0.09769 1.00 20.87 100.00 GiB 0 / 0 128
edprox2 18.2.4
osd.3 hdd bluestore up / in 18.2.4 0.09769 1.00 20.88 100.00 GiB 0 / 0 128
exprod3 18.2.4
osd.6 hdd bluestore up / in 18.2.4 0.09769 1.00 20.88 100.00 GiB 0 / 0 128

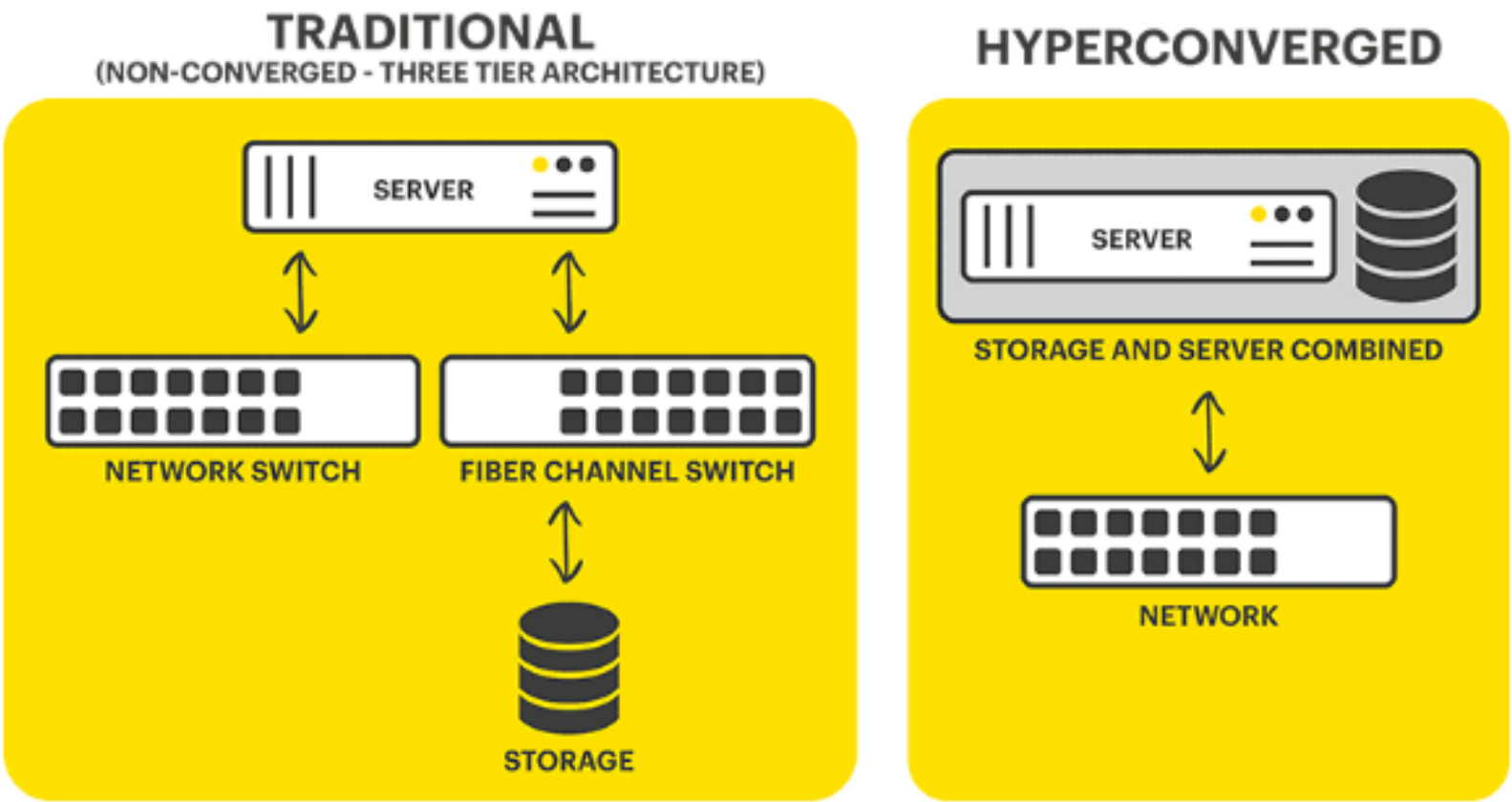
Ceph

- RADOS Gateway (RGW): Δίνει τη δυνατότητα πρόσβασης σε Object Storage μέσω API τύπου Amazon S3 ή Swift.
- Ceph Block Device (RBD): Παρέχει πρόσβαση σε block storage για VM ή άλλες εφαρμογές.
- CephFS: Παρέχει ένα POSIX συμβατό σύστημα αρχείων, προσφέροντας πρόσβαση σε δεδομένα μέσω της παραδοσιακής ιεραρχίας αρχείων.

BTW: Hyperconverged Computing Infrastructure

- Χρήση λογισμικού για τη συνένωση πόρων σε ένα ενιαίο σύστημα
- καταργείται η ανάγκη για εξειδικευμένο υλικό και χωριστές πλατφόρμες για κάθε κατηγορία πόρων.
- Software-defined storage - SDS: ένα επίπεδο λογισμικού που ενοποιεί πολλούς δίσκους σε πολλούς κόμβους, δημιουργώντας κατανεμημένη αποθήκευση.
- Virtualized Compute: πόροι υπολογιστικής ισχύος (CPU, RAM) εικονικοποιούνται, επιτρέποντας τη δυναμική διαχείριση
- Virtualized Networking: Το λογισμικό διαχειρίζεται τη δικτύωση των κόμβων

HCI


TRADITIONAL
(NON-CONVERGED - THREE TIER ARCHITECTURE)
SERVER
NETWORK SWITCH
FIBER CHANNEL SWITCH
STORAGE
HYPERCONVERGED
SERVER
STORAGE AND SERVER COMBINED
NETWORK

HCI

README Apache-2.0 license Security

Harvester

build passing go report A+ release v1.3.2 slack join

Harvester is a modern, open, interoperable, hyperconverged infrastructure (HCI) solution built on Kubernetes. It is an open-source alternative designed for operators seeking a cloud-native HCI solution. Harvester runs on bare metal servers and provides integrated virtualization and distributed storage capabilities. In addition to traditional virtual machines (VMs), Harvester supports containerized environments automatically through integration with Rancher. It offers a solution that unifies legacy virtualized infrastructure while enabling the adoption of containers from core to edge locations.

Backup

- Το Proxmox δίνει την δυνατότητα να παίρνουμε live backup των VMs (δηλαδή όταν τρέχουν).
- Κάνει συμπίεση των δίσκων χρησιμοποιώντας snapshots.
- Μπορούμε να προγραμματίσουμε την λήψη backups σε external storage (π.χ. NFS, κτλ)
- Υπάρχει και η λύση το Proxmox Backup Server αλλά δεν είναι διαθέσιμη στην community έκδοση.

Replication

- Το Proxmox υποστήριζει την δυνατότητα οι δίσκοι των VM να γίνονται replicate σε storage διαφορετικών nodes.
- Αυτό έχει νόημα ιδιαίτερα όταν δεν υπάρχει shared storage.
- Υποστηρίζεται μόνο για το ZFS *local* file system.
- Ο συγχρονισμός γίνεται σε περιοδικά χρονικά διαστήματα.

Διαχείριση ιδεατών μηχανών

- Μπορούμε να χρησιμοποιήσουμε το UI του Proxmox για να κάνουμε βασικές αλλά και πιο σύνθετες λειτουργίες.
- Να δημιουργήσουμε VM και να τα παραμετροποιήσουμε.
- Συνήθως πρώτα δημιουργούμε templates τα οποία κάνουμε clone ώστε να μην εγκαθιστούμε ξανά και ξανά το λειτουργικό.

Τι πρέπει να έχει ένα template?

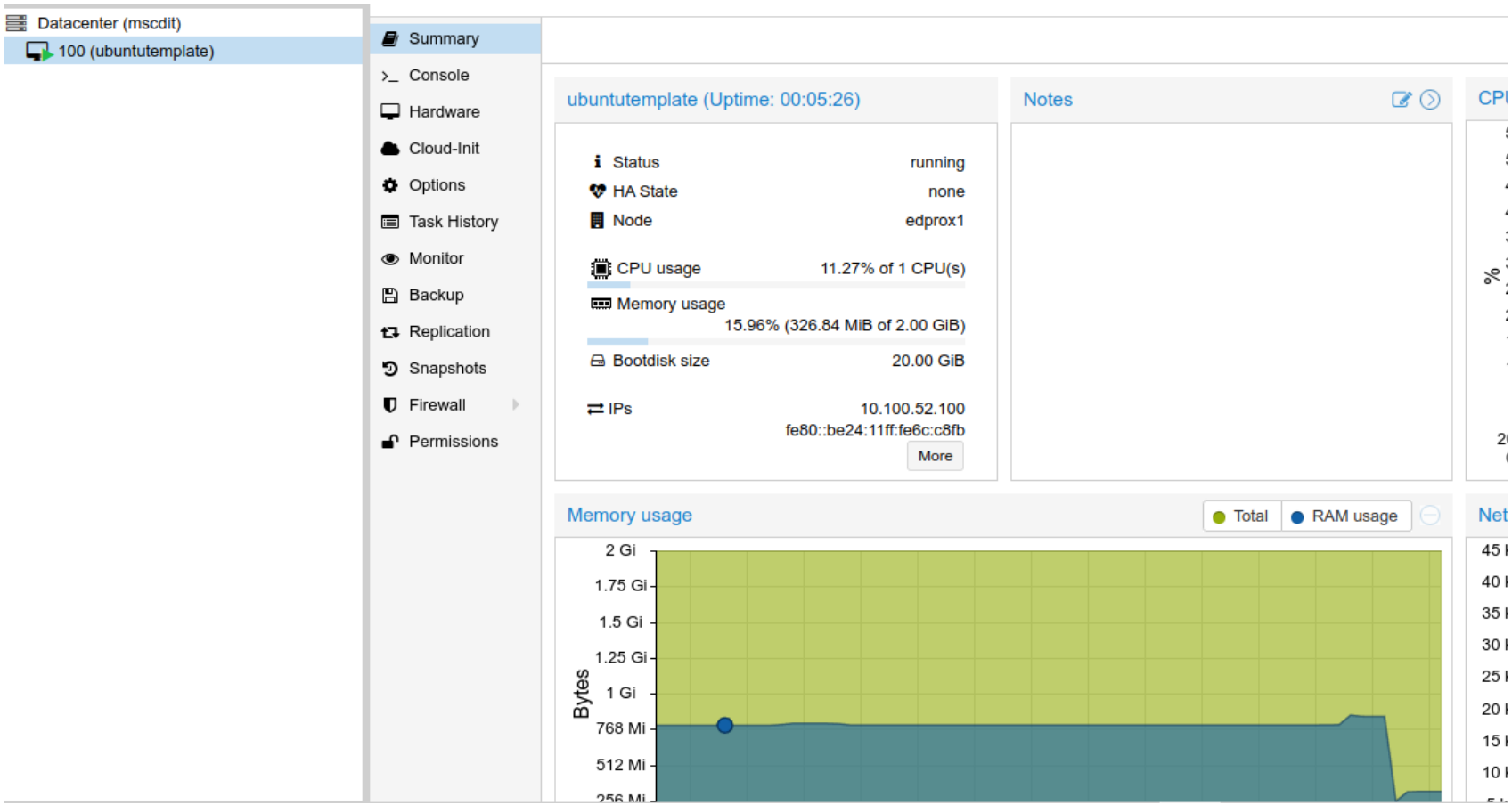
- Καλό είναι να εγκαταστήσουμε το qemu-guest-agent ώστε να έχουμε καλύτερο overview του VM (IP addresses etc).
- Κλειδιά διαχειριστή για το SSH.
- Παραμετροποίηση του firewall.
- Agents για το monitoring (π.χ. Zabbix agent κτλ)
- Γενικά ότι άλλο χρειαζόμαστε να εγκαταστήσουμε ξανά και ξανά...

QEMU guest agent

```
root@ubuntutemplate:/home/user# service qemu-guest-agent start
root@ubuntutemplate:/home/user# service qemu-guest-agent status
● qemu-guest-agent.service - QEMU Guest Agent
     Loaded: loaded (/usr/lib/systemd/system/qemu-guest-agent.service; static)
     Active: active (running) since Fri 2024-10-11 03:42:03 UTC; 34s ago
   Main PID: 696 (qemu-ga)
      Tasks: 2 (limit: 2276)
     Memory: 1.4M (peak: 1.6M)
        CPU: 77ms
     CGroup: /system.slice/qemu-guest-agent.service
             └─696 /usr/sbin/qemu-ga

Oct 11 03:42:03 ubuntutemplate systemd[1]: Started qemu-guest-agent.service - QEMU Guest Agent.
```

QEMU guest agent



Κλειδιά SSH

- Καλό είναι να επιτρέψουμε το ssh για τον root μόνο με κλειδιά
- Επίσης να μην επιτρέπουμε το login με password.
- Για τον σκοπό αυτό αλλάζουμε το /etc/ssh/sshd_config και προσθέτουμε το public κλειδί στο /root/.ssh/authorize_keys

Κλειδιά SSH

GNU nano 7.2 /etc/ssh/sshd_config

```
# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

#Include /etc/ssh/sshd_config.d/*.conf

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin prohibit-password
#StrictModes yes
```

Κλειδιά SSH

```
  GNU nano 7.2                                                    /etc/ssh/s
#AuthorizedKeysFile     .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication no
#PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
KbdInteractiveAuthentication no

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no
```

Παραμετροποίηση του firewall

- Υπάρχουν πολλές επιλογές για το firewall και πολλές φορές και η ίδια η διανομή μας δίνει εργαλεία
- Μία λύση είναι το `ufw`
- Στο template μας απαγορεύουμε τα πάντα εκτός από το ssh (πόρτα 22)

Παραμετροποίηση του firewall

```
root@ubuntutemplate:~# ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
root@ubuntutemplate:~# ufw allow ssh
Skipping adding existing rule
Skipping adding existing rule (v6)
root@ubuntutemplate:~# ufw status
Status: inactive
root@ubuntutemplate:~# ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
root@ubuntutemplate:~# ufw status
Status: active

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
22/tcp (v6)                ALLOW       Anywhere (v6)

root@ubuntutemplate:~# ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW IN    Anywhere
22/tcp (v6)                ALLOW IN    Anywhere (v6)
```

Cloning

- Εφόσον ορίσαμε ως template το VM στη συνέχεια μπορούμε να χάνουμε cloning

