Provisioning to Proxmox Terraform & Packer

HUG – COLUMBUS
MAY 8, 2024

PROXMOX

Introduction

Chris Deever

- 3 years Unix/C working on process control
- 9 years in Telecom – mostly Java
- 15 years in Infrastructure various roles
  - Network Device Inventory
  - Network Services - IPAM, DNS, Firewall
  - Cloud Services - IaaS, On-Premise Cloud
- Home Lab Enthusiast

chris@deevnet.com

https://github.com/cdeever

aws certified

Solutions Architect

ASSOCIATE

Agenda

- Overview of Proxmox VE (PVE)
- Deevnet Labs Home & Mobile – What? Why?
- Proxmox Deeper Dive and Feature Tour
- Packer, Terraform & IaC Deployment Options
- Pitfalls / Troubleshooting
- Walkthrough / Demo
- Q & A

Proxmox Overview

- Hypervisor for Virtual Servers and Containers
- Hosted on Debian-based Linux
- Extensive Web-based Admin UI
- Free to Use / Support Subscriptions Available
- Comprehensive Documentation and Community Support

https://pve.proxmox.com/pve-docs/index.html

https://pve.proxmox.com/wiki/Get_support#_community_support_forum

Deevnet Home Lab Deployment

1994-2023 – Deevnet Home lab (DVNT)

Why Build It?

- Playground for related work
- Evolution
  - 90s - Multi-boot PC
  - 90s - White Box Servers
  - 00s-10s - 1U, 2U, 4U rack servers
  - 20s - SBCs
- Media Server, VM Playground
- Future: “Production” IoT Backend

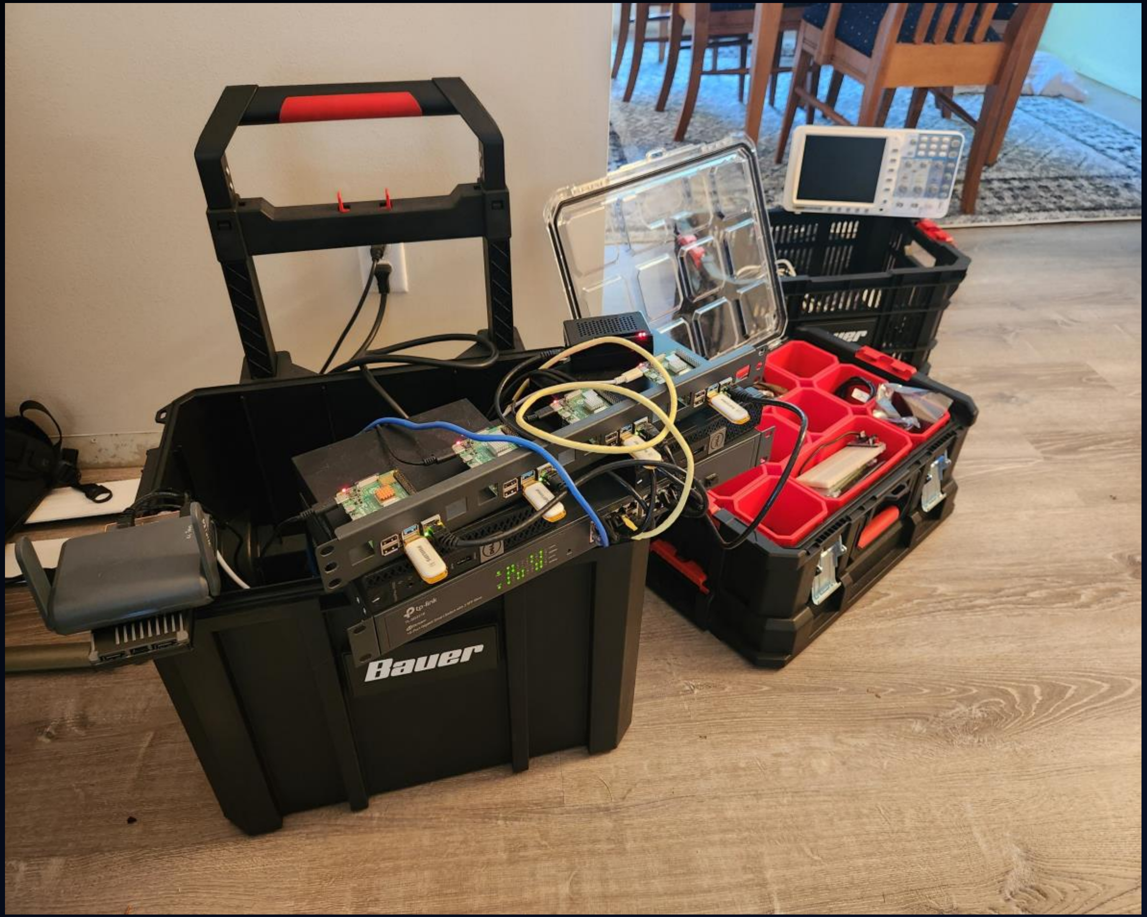
I’m moving away from ATX and rack servers!

Deevnet Home Lab Incident

- ESXi Host ATX Power Supply
- Literally Crash & Burn Event!
- Repaired, but fear lingers on
- Moving toward SBCs

Deevnet Mobile Lab Deployment

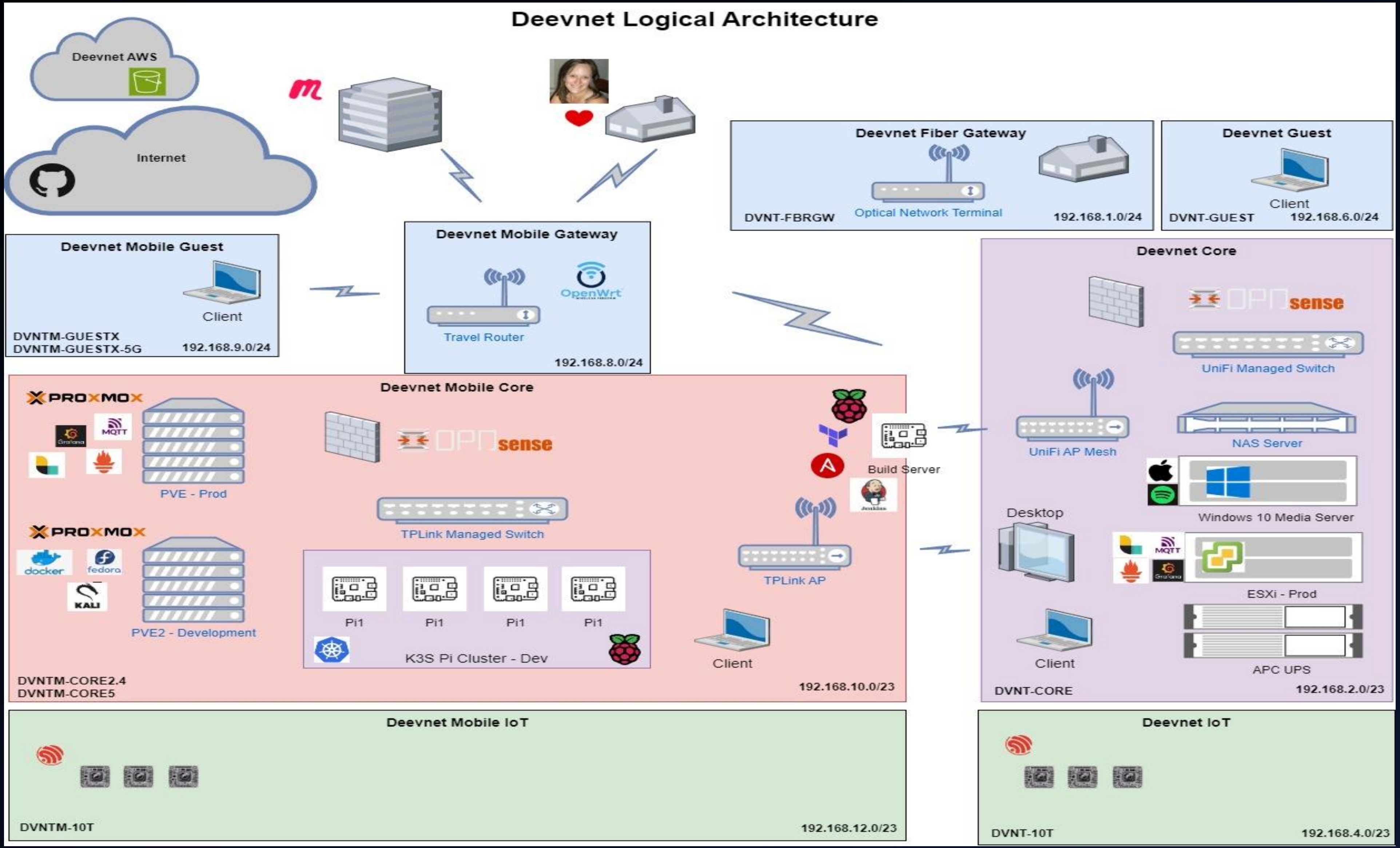
Deevnet Mobile (DVNTM) + IoT Lab



Why?

- CARPE Meetup (Columbus Arduino/Raspberry Pi Enthusiast)
- Same LAN everywhere there's a different Internet connection
- IoT Dev at Girlfriend's house
- No fear of unexpected Cloud charges or security risks of exposing via Internet
- Cause I wanted to!

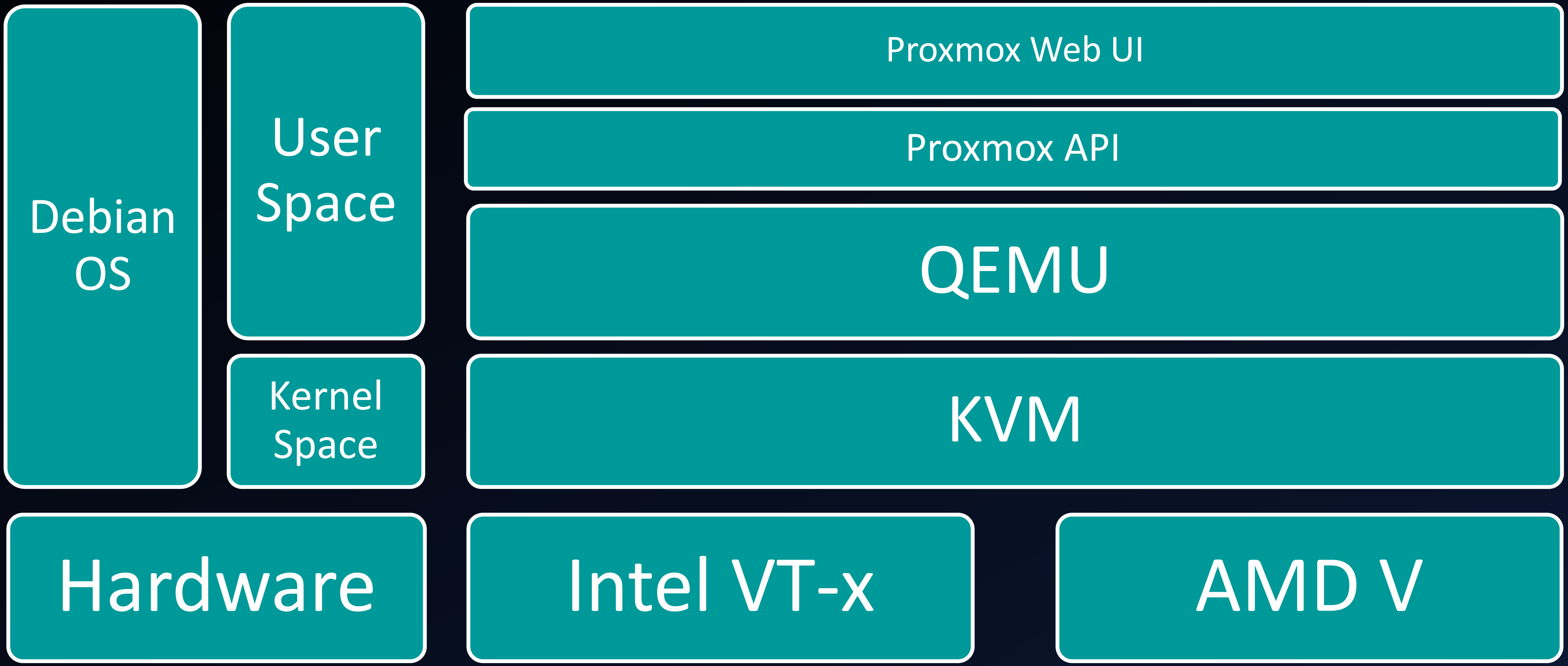
Deevnet Logical View



Proxmox – Inside Look

- Type 1 Hypervisor (Bare Metal)
  - Near native performance on par with ESXi, Hyper-V and Xen
  - KVM integrates directly with Linux Kernel
  - Contrast to VirtualBox as Type 2 Hypervisor (Hosted on OS)
- QEMU emulates various hardware functions
  - E.g.: BIOS/EFI, graphic cards, disk controllers, network interfaces, etc.
  - QEMU leverages KVM for hardware acceleration to optimize performance
- Proxmox API: Enables script-driven virtual resource management

Proxmox VE API Layers for Virtualization



Business Class Features

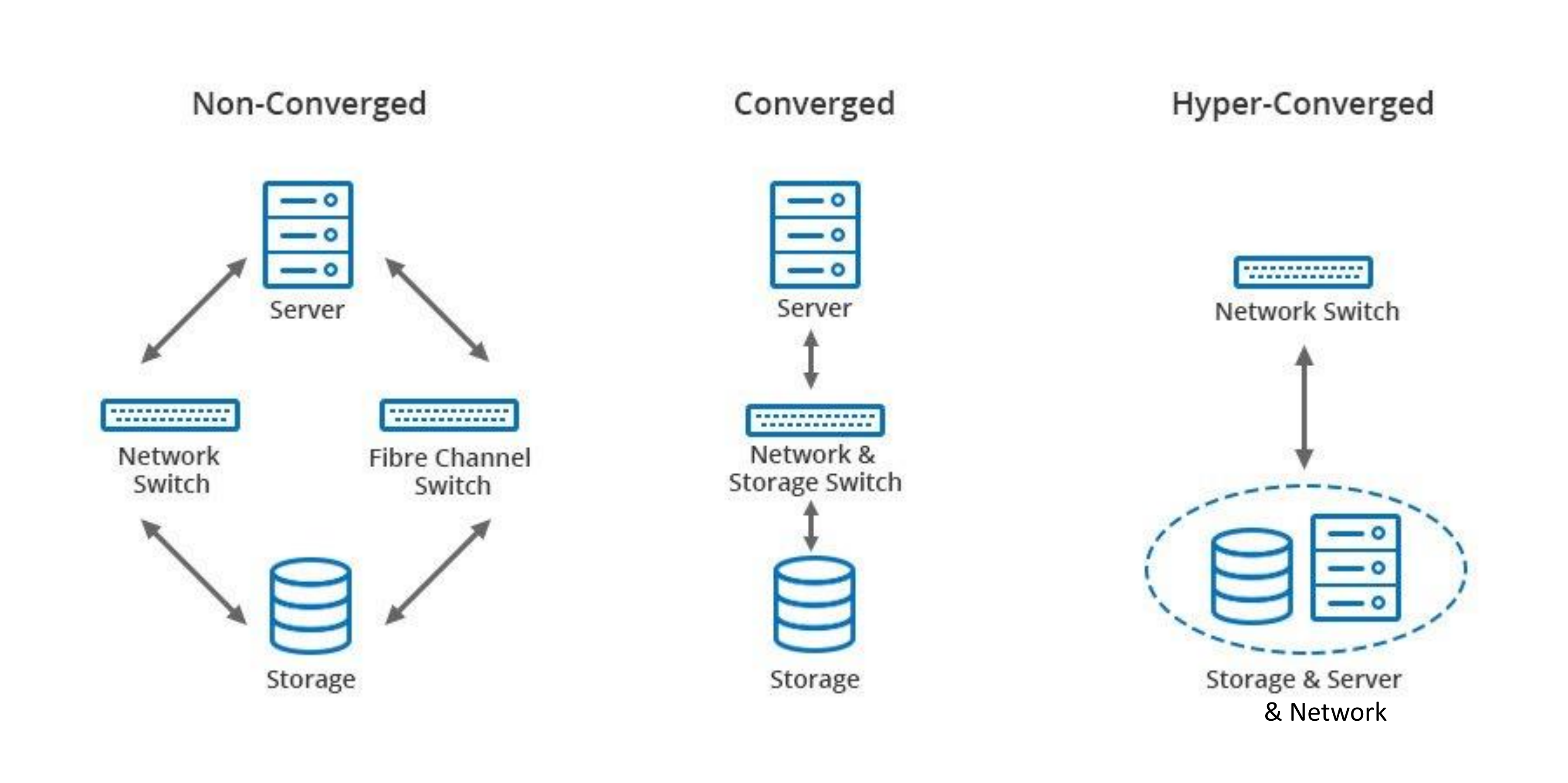
- Software Defined Networking
  - Linux Bridge - Network bridging, Traffic filtering, VLAN tagging (4096 segments)
  - Open vSwitch (OvS) - Advanced VLANs, VXLAN support (16 million segments!), QoS
  - Network Segmentation and Isolation - Secure environments, Customizable policies, Enhanced privacy

- High Availability
  - Clustering up to 32 nodes
  - Automatic VM Failover
  - Live Migration (VMs only, not LXC containers!)

- Clustered Storage Options
  - GlusterFS (SMB or NFS)
  - ZFS over iSCSI (Replication, Snapshotting, Deduplication)
  - Ceph integration (Block, File and Object)

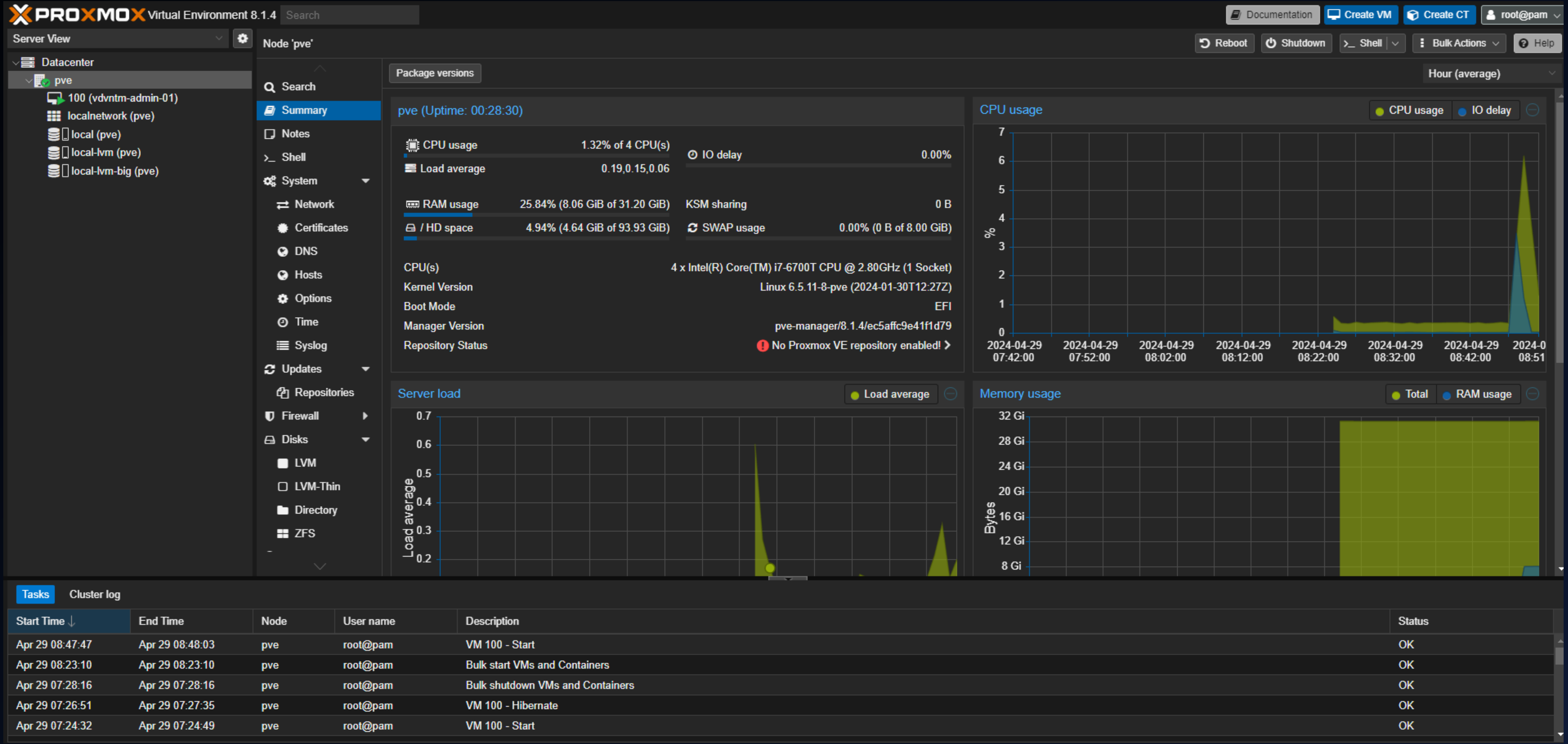
Hyper-Converged Infrastructure (HCI)

Software-Defined Compute, Network and Storage on commodity hardware



Source: https://commons.wikimedia.org/wiki/User:Fishezz

Proxmox VE Dashboard



pve (Uptime: 00:28:30)

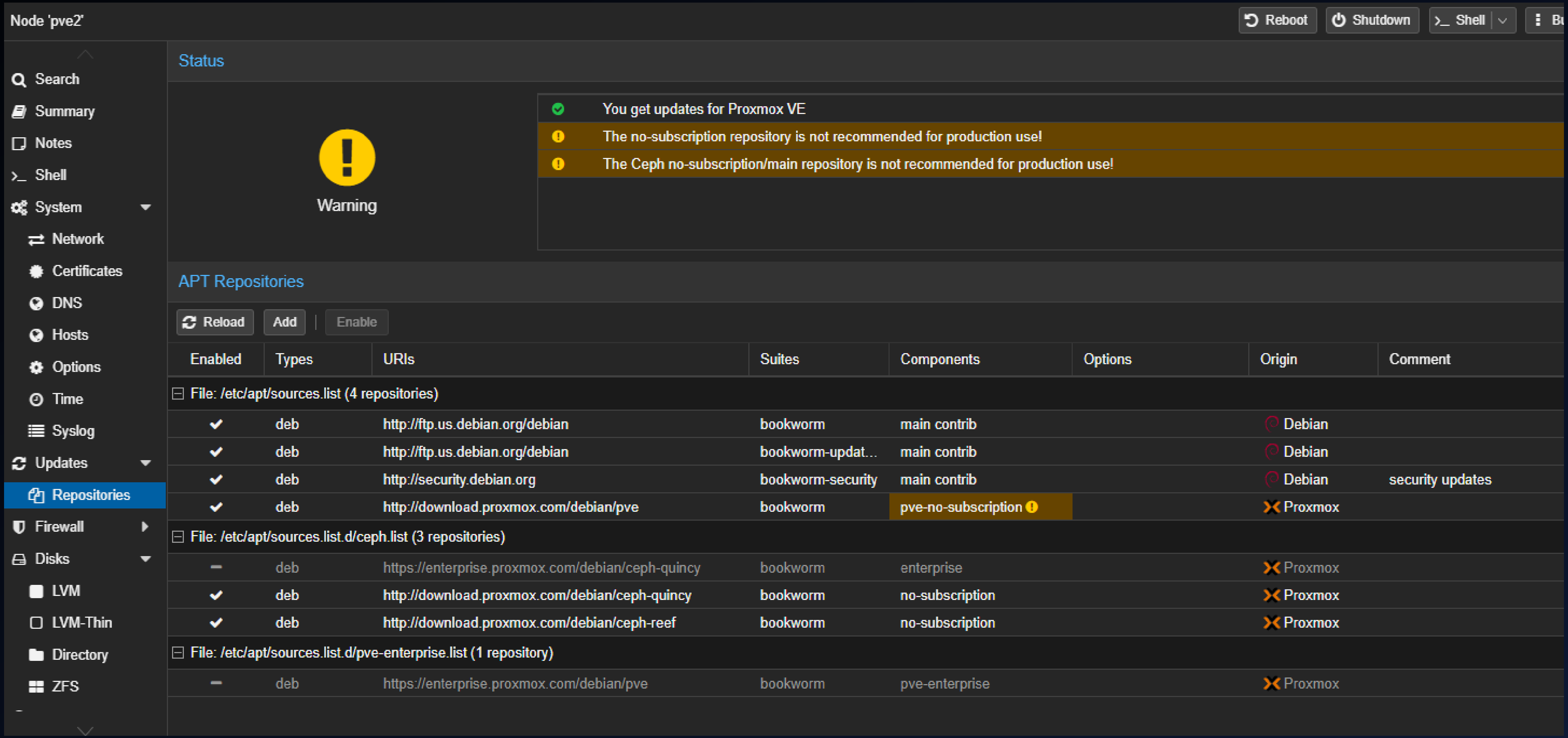
CPU usage 1.32% of 4 CPU(s)
Load average 0.19,0.15,0.06
IO delay 0.00%
RAM usage 25.84% (8.06 GiB of 31.20 GiB)
KSM sharing 0 B
/ HD space 4.94% (4.64 GiB of 93.93 GiB)
SWAP usage 0.00% (0 B of 8.00 GiB)

CPU(s) 4 x Intel(R) Core(TM) i7-6700T CPU @ 2.80GHz (1 Socket)
Kernel Version Linux 6.5.11-8-pve (2024-01-30T12:27Z)
Boot Mode EFI
Manager Version pve-manager/8.1.4/ec5affc9e41f1d79
Repository Status No Proxmox VE repository enabled!

Start Time ↓	End Time	Node	User name	Description	Status
Apr 29 08:47:47	Apr 29 08:48:03	pve	root@pam	VM 100 - Start	OK
Apr 29 08:23:10	Apr 29 08:23:10	pve	root@pam	Bulk start VMs and Containers	OK
Apr 29 07:28:16	Apr 29 07:28:16	pve	root@pam	Bulk shutdown VMs and Containers	OK
Apr 29 07:26:51	Apr 29 07:27:35	pve	root@pam	VM 100 - Hibernate	OK
Apr 29 07:24:32	Apr 29 07:24:49	pve	root@pam	VM 100 - Start	OK

Repositories Update

Action Item: Remove Enterprise Repos and Add No-Subscription Repos



- ✓ You get updates for Proxmox VE
- ! The no-subscription repository is not recommended for production use!
- ! The Ceph no-subscription/main repository is not recommended for production use!

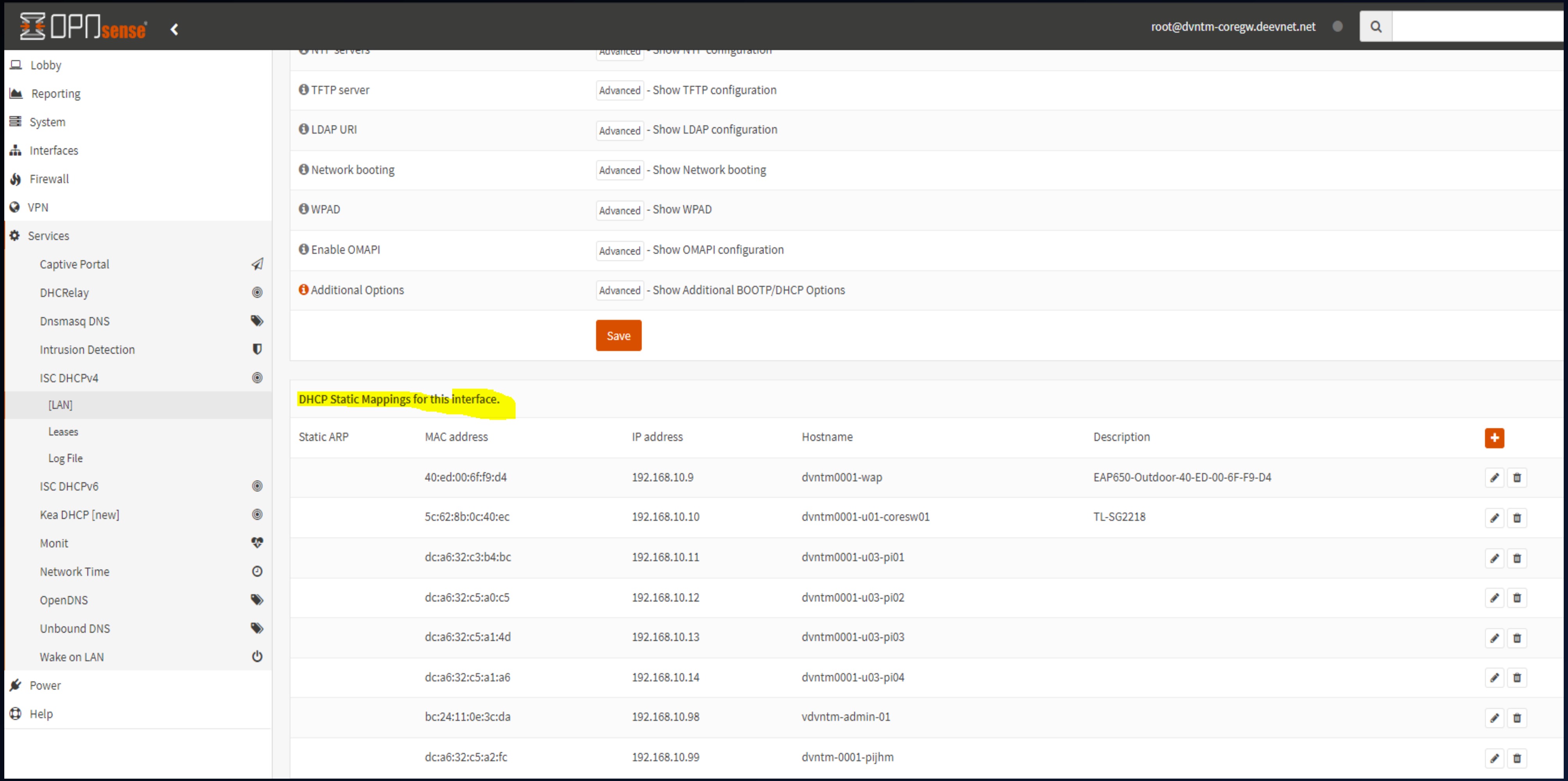
Enabled	Types	URIs	Suites	Components	Options	Origin	Comment
File: /etc/apt/sources.list (4 repositories)							
✓	deb	http://ftp.us.debian.org/debian	bookworm	main contrib		Debian	
✓	deb	http://ftp.us.debian.org/debian	bookworm-updat...	main contrib		Debian	
✓	deb	http://security.debian.org	bookworm-security	main contrib		Debian	security updates
✓	deb	http://download.proxmox.com/debian/pve	bookworm	pve-no-subscription !		Proxmox	
File: /etc/apt/sources.list.d/ceph.list (3 repositories)							
–	deb	https://enterprise.proxmox.com/debian/ceph-quincy	bookworm	enterprise		Proxmox	
✓	deb	http://download.proxmox.com/debian/ceph-quincy	bookworm	no-subscription		Proxmox	
✓	deb	http://download.proxmox.com/debian/ceph-reef	bookworm	no-subscription		Proxmox	
File: /etc/apt/sources.list.d/pve-enterprise.list (1 repository)							
–	deb	https://enterprise.proxmox.com/debian/pve	bookworm	pve-enterprise		Proxmox	

Proxmox Dual Screen with SPICE driver

OPNSense – Just Enough

- ISC DHCPv4
  - Enabled on LAN interface - 192.168.10.0/23
  - DHCP Range 192.168.10.110 – 192.168.10.254
  - Static Mappings for WAP, TP Link Switch, 4 Pis cluster, 1 build Pi, 1 admin VM (builder)
- DNS Resolution
  - Running UnboundDNS
  - DHCP Provided DNS comes from WAN IP
  - Register ISC DHCP Static Mappings - Enabled

OPNSense – DHCP Static Mappings



NTP servers	Advanced - Show NTP configuration
TFTP server	Advanced - Show TFTP configuration
LDAP URI	Advanced - Show LDAP configuration
Network booting	Advanced - Show Network booting
WPAD	Advanced - Show WPAD
Enable OMAPI	Advanced - Show OMAPI configuration
Additional Options	Advanced - Show Additional BOOTP/DHCP Options

DHCP Static Mappings for this interface.

Static ARP	MAC address	IP address	Hostname	Description
	40:ed:00:6f:f9:d4	192.168.10.9	dvntm0001-wap	EAP650-Outdoor-40-ED-00-6F-F9-D4
	5c:62:8b:0c:40:ec	192.168.10.10	dvntm0001-u01-coresw01	TL-SG2218
	dc:a6:32:c3:b4:bc	192.168.10.11	dvntm0001-u03-pi01	
	dc:a6:32:c5:a0:c5	192.168.10.12	dvntm0001-u03-pi02	
	dc:a6:32:c5:a1:4d	192.168.10.13	dvntm0001-u03-pi03	
	dc:a6:32:c5:a1:a6	192.168.10.14	dvntm0001-u03-pi04	
	bc:24:11:0e:3c:da	192.168.10.98	vdvntm-admin-01	
	dc:a6:32:c5:a2:fc	192.168.10.99	dvntm-0001-pijhm	

End Goals and Requirements

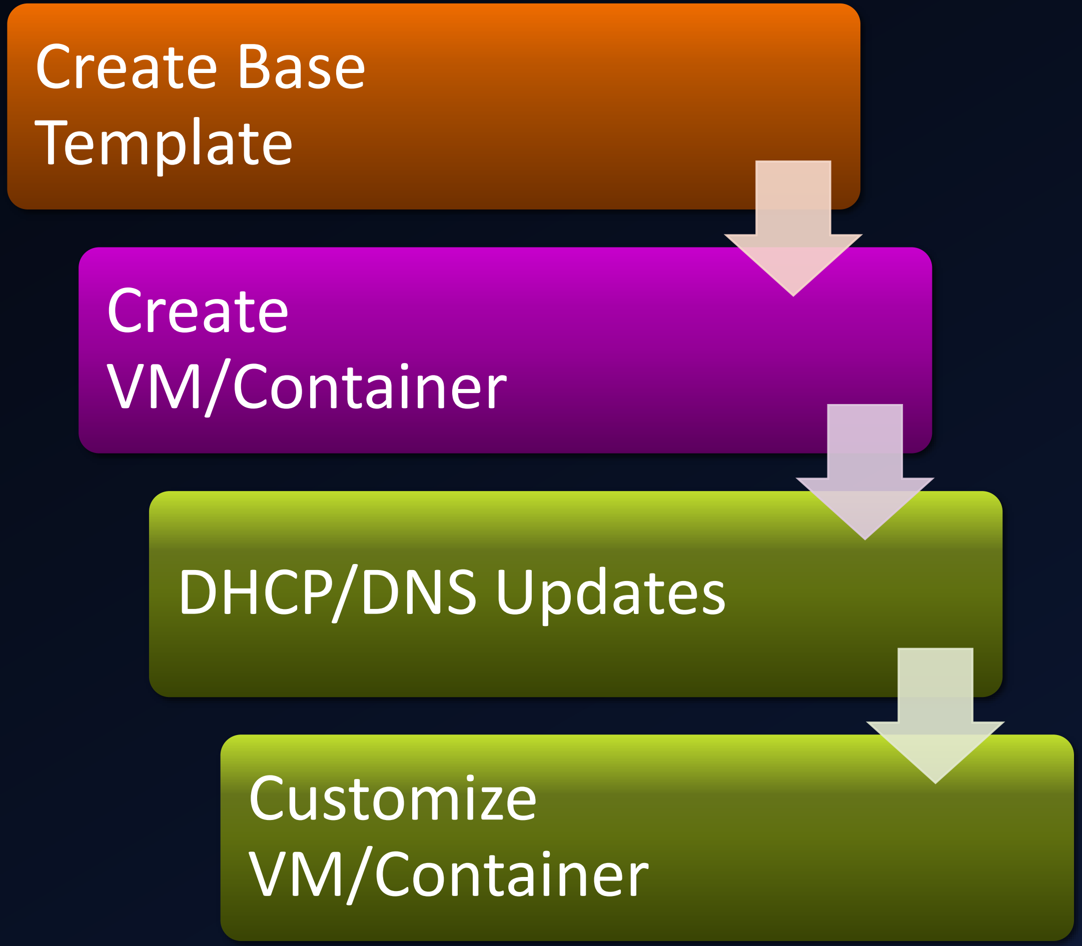
Mission: Deploy an Open Source IoT Backend to Proxmox

IoT backend will consist of ELK Stack, Prometheus, Grafana, MQTT, Home Assistant or another front end.

- **IaC Deployment End-to-End**
- **Leverage Packer and Terraform**
- **VMs should have consistent IP and DNS resolution**
- **IoT data (business data) should be separate from infra**
- **Important IoT data will back up to cloud**

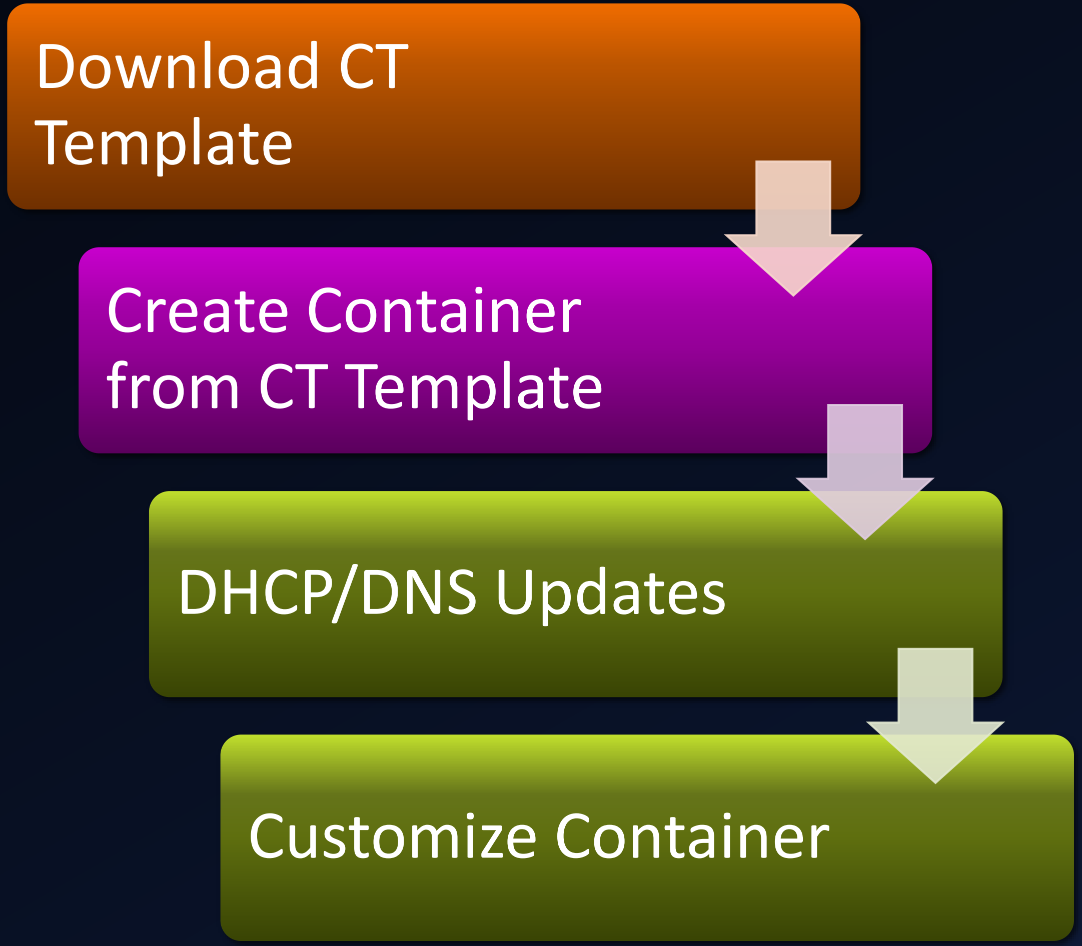
IaC VM Deployment Steps

- Packer/Kickstart/Ansible: Start with Fedora ISO to create “golden” Proxmox VM template
- Terraform: Create VM from template
- Terraform: Create DNS/DHCP Entries
- Ansible: Further customize VM Third bullet point here



IaC’ish Proxmox LXC Container Deployment Steps

- Proxmox: Download CT Template
- Terraform: Create CT from template
- Terraform: Create DNS/DHCP Entries
- Ansible: Further customize VM Third bullet point here



Download CT Template

Create Container from CT Template

DHCP/DNS Updates

Customize Container

IaC Deployment Options

Overwhelming number of Options for IaC and Deployment Automation!

What about Packer Cloning VM template?

What about Docker?, what about Kube?

What about Cloud-Init?

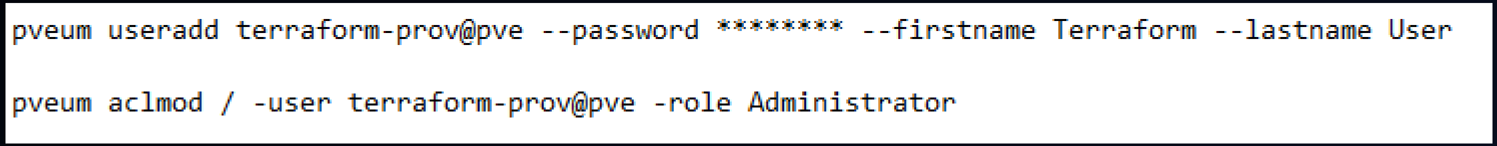
What about, what about? WHAT ABOUT?

Hey Man!

More than one way to skin a cat!

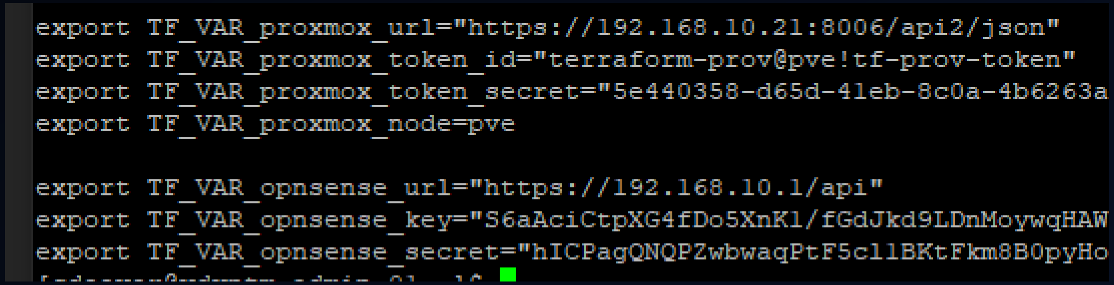
Setup for Terraform & Packer

1. **Create Proxmox provisioning accounts**



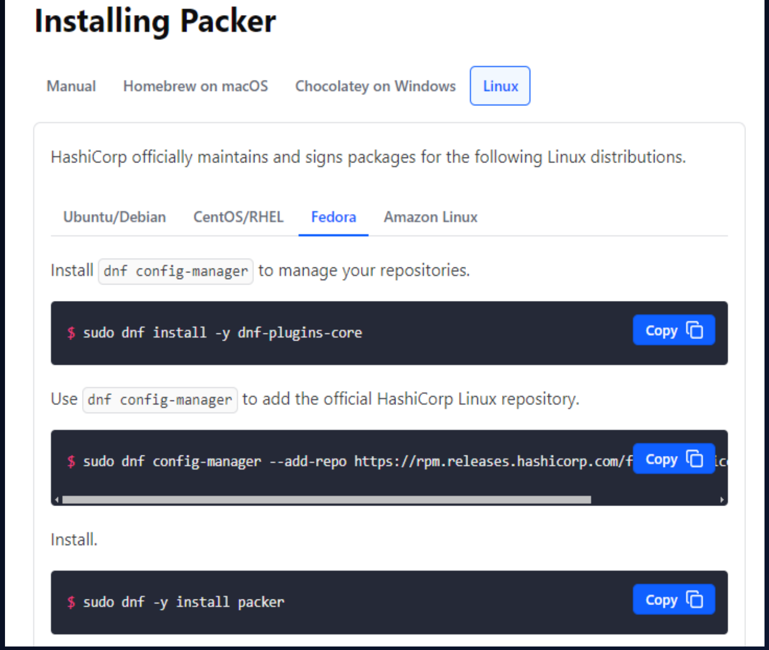
```
pveum useradd terraform-prov@pve --password ******** --firstname Terraform --lastname User

pveum aclmod / -user terraform-prov@pve -role Administrator
```

2. **Set up environment scripts**



```
export TF_VAR_proxmox_url="https://192.168.10.21:8006/api2/json"
export TF_VAR_proxmox_token_id="terraform-prov@pve!tf-prov-token"
export TF_VAR_proxmox_token_secret="5e440358-d65d-41eb-8c0a-4b6263a
export TF_VAR_proxmox_node=pve

export TF_VAR_opnsense_url="https://192.168.10.1/api"
export TF_VAR_opnsense_key="S6aAciCtpXG4fDo5XnKl/fGdJkd9LDnMoywqHAW
export TF_VAR_opnsense_secret="hICPagQNQPZwbwaqPtF5cllBKtFkm8B0pyHo
```

3. **Install Terraform & Packer**



Installing Packer

HashiCorp officially maintains and signs packages for the following Linux distributions.

Install `dnf config-manager` to manage your repositories.

```
$ sudo dnf install -y dnf-plugins-core
```

Use `dnf config-manager` to add the official HashiCorp Linux repository.

```
$ sudo dnf config-manager --add-repo https://rpm.releases.hashicorp.com/f
```

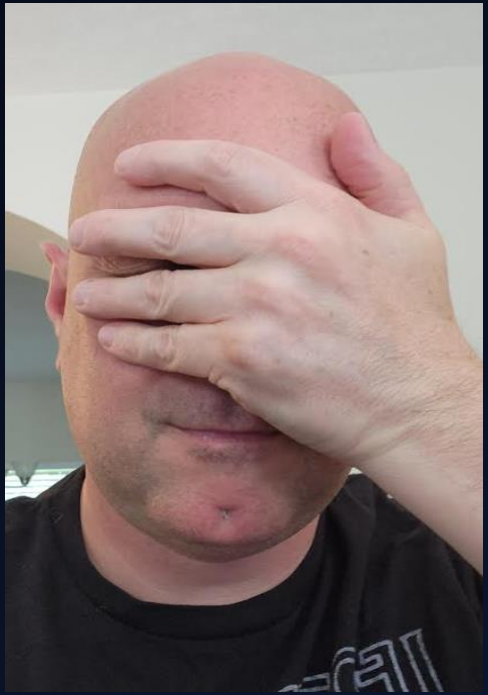
Install.

```
$ sudo dnf -y install packer
```

Dumb Things I Did!

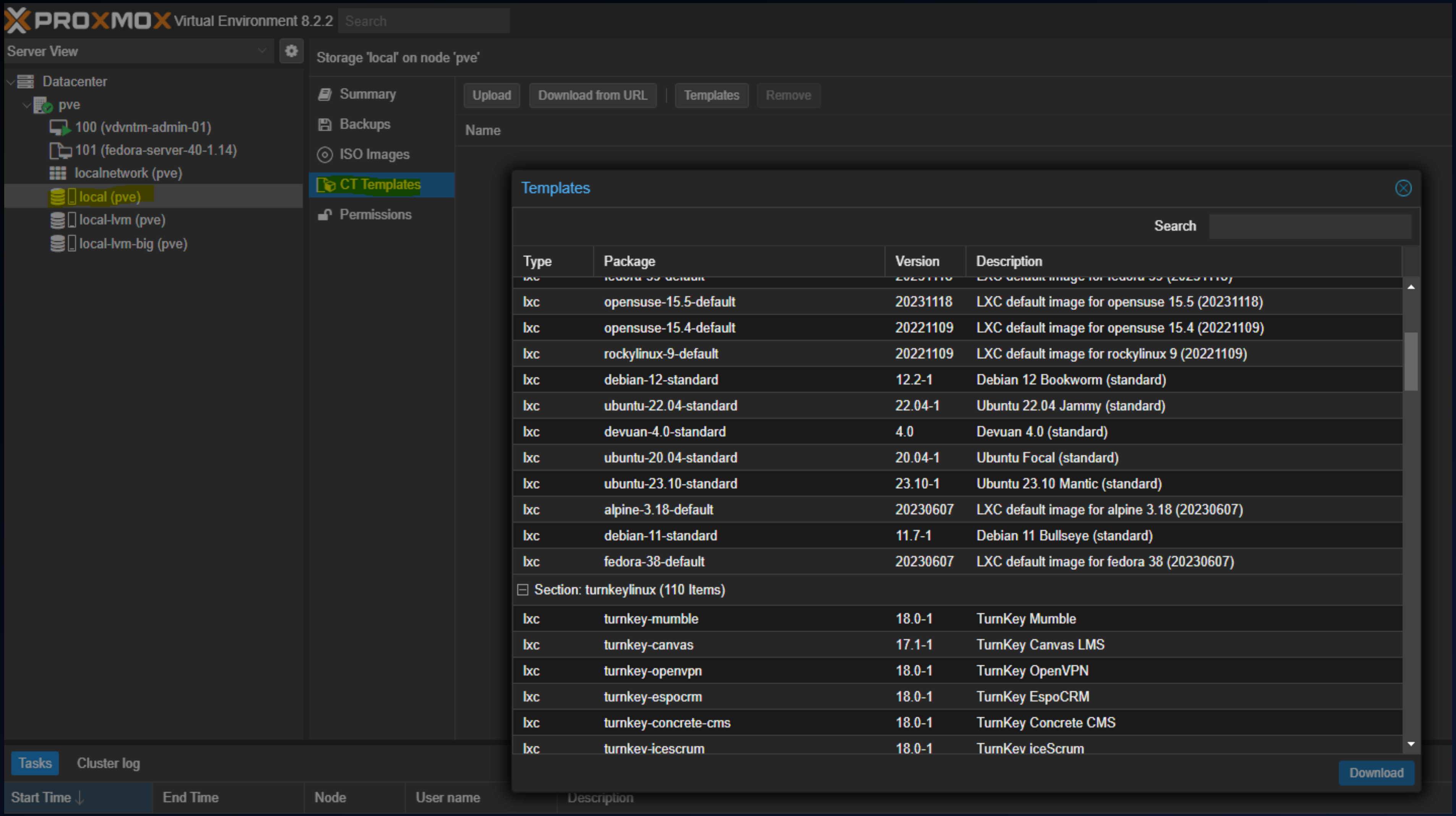
Learn from my silly mistakes

- Attempted to Build Packer QEMU Image for x86 on Raspberry Pi
- Used ARM ISO for Fedora instead of x86
- Skipped over checksum check in Packer
- Not enough RAM/CPU for Packer image build
- Layer in correct security at the end, not the beginning
- Reliance on ChatGPT over documentation



Demo 1: Build an LXC Container

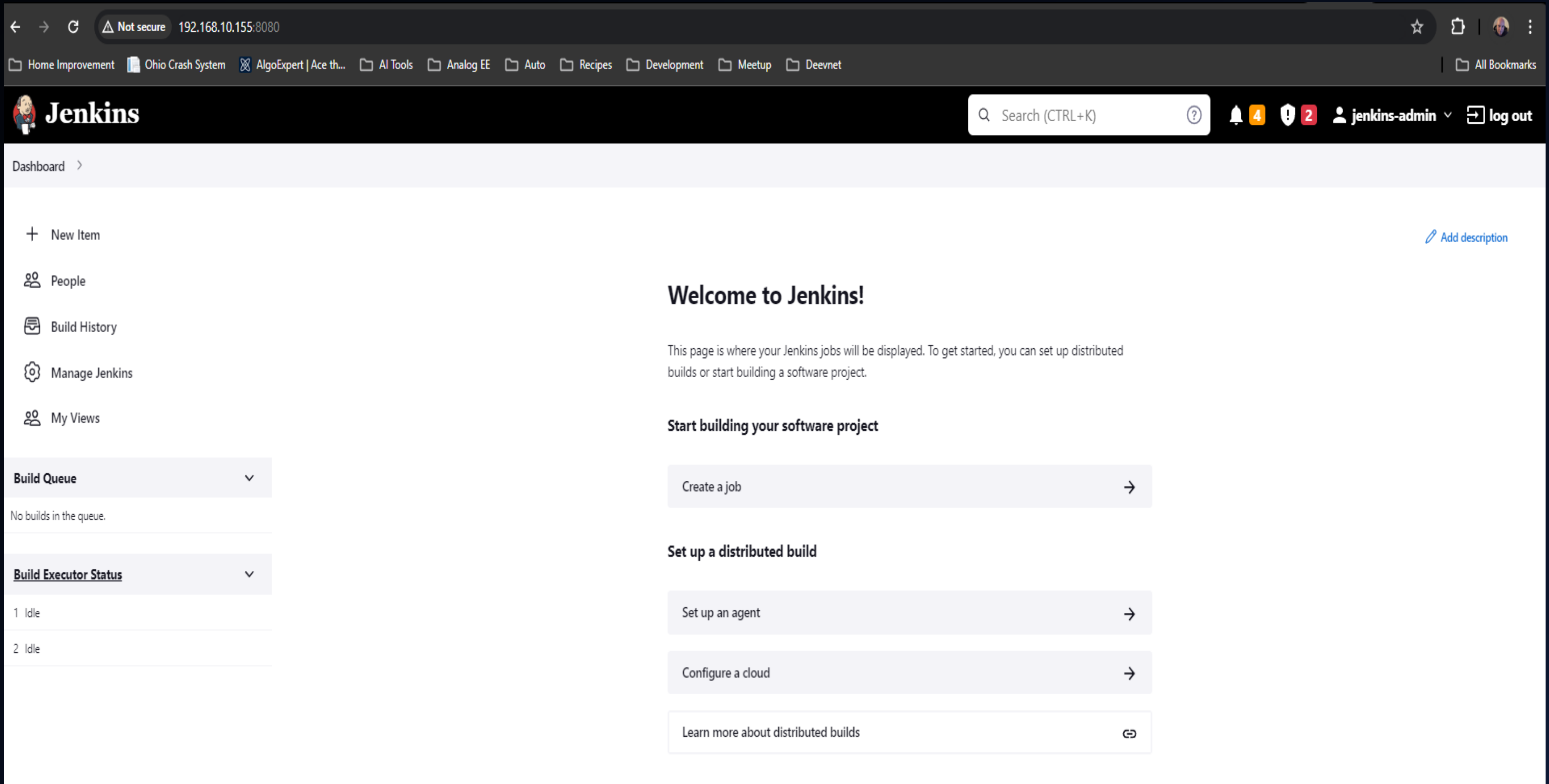
Pick a ready to go image template



Type	Package	Version	Description
lxc	fedora-39-default	20231118	LXC default image for fedora 39 (20231118)
lxc	opensuse-15.5-default	20231118	LXC default image for opensuse 15.5 (20231118)
lxc	opensuse-15.4-default	20221109	LXC default image for opensuse 15.4 (20221109)
lxc	rockylinux-9-default	20221109	LXC default image for rockylinux 9 (20221109)
lxc	debian-12-standard	12.2-1	Debian 12 Bookworm (standard)
lxc	ubuntu-22.04-standard	22.04-1	Ubuntu 22.04 Jammy (standard)
lxc	devuan-4.0-standard	4.0	Devuan 4.0 (standard)
lxc	ubuntu-20.04-standard	20.04-1	Ubuntu Focal (standard)
lxc	ubuntu-23.10-standard	23.10-1	Ubuntu 23.10 Mantic (standard)
lxc	alpine-3.18-default	20230607	LXC default image for alpine 3.18 (20230607)
lxc	debian-11-standard	11.7-1	Debian 11 Bullseye (standard)
lxc	fedora-38-default	20230607	LXC default image for fedora 38 (20230607)
⊟ Section: turnkeylinux (110 Items)			
lxc	turnkey-mumble	18.0-1	TurnKey Mumble
lxc	turnkey-canvas	17.1-1	TurnKey Canvas LMS
lxc	turnkey-openvpn	18.0-1	TurnKey OpenVPN
lxc	turnkey-espocrm	18.0-1	TurnKey EspoCRM
lxc	turnkey-concrete-cms	18.0-1	TurnKey Concrete CMS
lxc	turnkey-icescrum	18.0-1	TurnKey iceScrum

Demo 1: Build an LXC Container

Jenkins LXC container up in just a few minutes



Build Queue

No builds in the queue.

Build Executor Status

1 Idle

2 Idle

Welcome to Jenkins!

This page is where your Jenkins jobs will be displayed. To get started, you can set up distributed builds or start building a software project.

Start building your software project

Create a job →

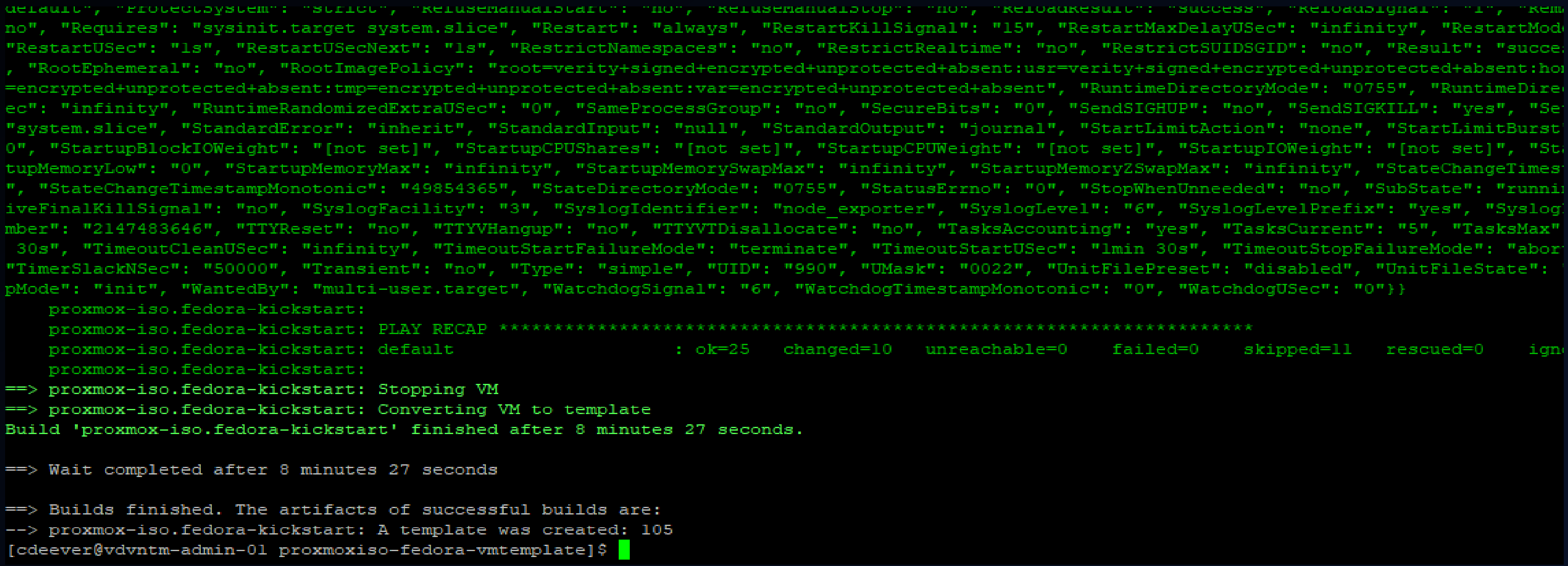
Set up a distributed build

Set up an agent →

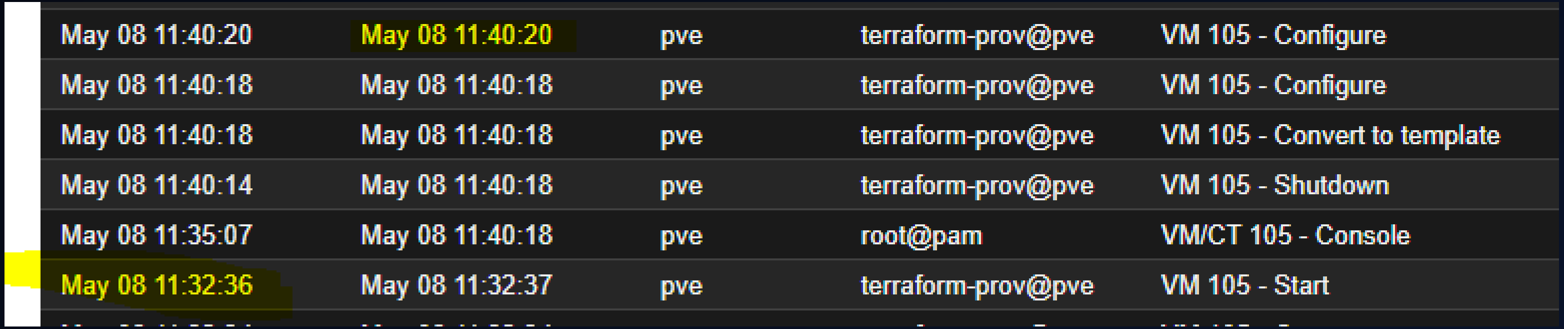
Configure a cloud →

Learn more about distributed builds

Demo 2: Packer ISO Creating VM Template



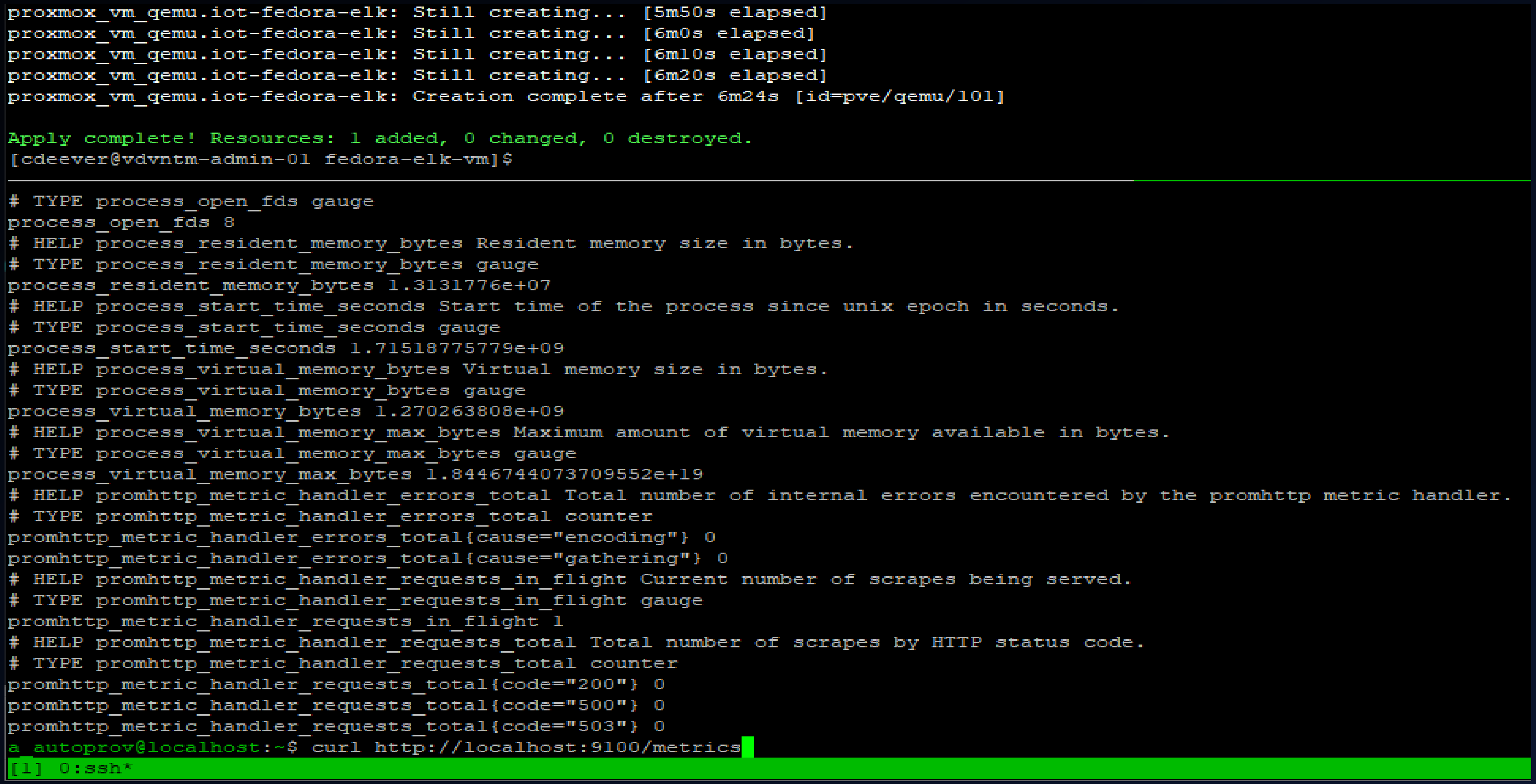
```
default", "ProtectSystem": "strict", "RefuseManualStart": "no", "RefuseManualStop": "no", "ReloadResult": "success", "ReloadSignal": "1", "Rem
no", "Requires": "sysinit.target system.slice", "Restart": "always", "RestartKillSignal": "15", "RestartMaxDelayUSec": "infinity", "RestartMod
"RestartUSec": "1s", "RestartUSecNext": "1s", "RestrictNamespaces": "no", "RestrictRealtime": "no", "RestrictSUIDSGID": "no", "Result": "succe
, "RootEphemeral": "no", "RootImagePolicy": "root=verity+signed+encrypted+unprotected+absent:usr=verity+signed+encrypted+unprotected+absent:ho
=encrypted+unprotected+absent:tmp=encrypted+unprotected+absent:var=encrypted+unprotected+absent", "RuntimeDirectoryMode": "0755", "RuntimeDire
ec": "infinity", "RuntimeRandomizedExtraUSec": "0", "SameProcessGroup": "no", "SecureBits": "0", "SendSIGHUP": "no", "SendSIGKILL": "yes", "Se
"system.slice", "StandardError": "inherit", "StandardInput": "null", "StandardOutput": "journal", "StartLimitAction": "none", "StartLimitBurst
0", "StartupBlockIOWeight": "[not set]", "StartupCPUShares": "[not set]", "StartupCPUWeight": "[not set]", "StartupIOWeight": "[not set]", "St
tupMemoryLow": "0", "StartupMemoryMax": "infinity", "StartupMemorySwapMax": "infinity", "StartupMemoryZSwapMax": "infinity", "StateChangeTimes
", "StateChangeTimestampMonotonic": "49854365", "StateDirectoryMode": "0755", "StatusErrno": "0", "StopWhenUnneeded": "no", "SubState": "runni
iveFinalKillSignal": "no", "SyslogFacility": "3", "SyslogIdentifier": "node_exporter", "SyslogLevel": "6", "SyslogLevelPrefix": "yes", "Syslog
mber": "2147483646", "TTYReset": "no", "TTYVHangup": "no", "TTYVTDisallocate": "no", "TasksAccounting": "yes", "TasksCurrent": "5", "TasksMax"
 30s", "TimeoutCleanUSec": "infinity", "TimeoutStartFailureMode": "terminate", "TimeoutStartUSec": "1min 30s", "TimeoutStopFailureMode": "abor
"TimerSlackNSec": "50000", "Transient": "no", "Type": "simple", "UID": "990", "UMask": "0022", "UnitFilePreset": "disabled", "UnitFileState": 
pMode": "init", "WantedBy": "multi-user.target", "WatchdogSignal": "6", "WatchdogTimestampMonotonic": "0", "WatchdogUSec": "0"}}
    proxmox-iso.fedora-kickstart:
    proxmox-iso.fedora-kickstart: PLAY RECAP *********************************************************************
    proxmox-iso.fedora-kickstart: default                    : ok=25   changed=10   unreachable=0    failed=0    skipped=11   rescued=0    ign
    proxmox-iso.fedora-kickstart:
==> proxmox-iso.fedora-kickstart: Stopping VM
==> proxmox-iso.fedora-kickstart: Converting VM to template
Build 'proxmox-iso.fedora-kickstart' finished after 8 minutes 27 seconds.

==> Wait completed after 8 minutes 27 seconds

==> Builds finished. The artifacts of successful builds are:
--> proxmox-iso.fedora-kickstart: A template was created: 105
[cdeever@vdvntm-admin-01 proxmoxiso-fedora-vmtemplate]$
```



May 08 11:40:20	May 08 11:40:20	pve	terraform-prov@pve	VM 105 - Configure
May 08 11:40:18	May 08 11:40:18	pve	terraform-prov@pve	VM 105 - Configure
May 08 11:40:18	May 08 11:40:18	pve	terraform-prov@pve	VM 105 - Convert to template
May 08 11:40:14	May 08 11:40:18	pve	terraform-prov@pve	VM 105 - Shutdown
May 08 11:35:07	May 08 11:40:18	pve	root@pam	VM/CT 105 - Console
May 08 11:32:36	May 08 11:32:37	pve	terraform-prov@pve	VM 105 - Start

Demo 3: Terraform Creating VM from Packer Template

Logged in. Confirmed Prometheus Node Exporter Running



```
proxmox_vm_qemu.iot-fedora-elk: Still creating... [5m50s elapsed]
proxmox_vm_qemu.iot-fedora-elk: Still creating... [6m0s elapsed]
proxmox_vm_qemu.iot-fedora-elk: Still creating... [6m10s elapsed]
proxmox_vm_qemu.iot-fedora-elk: Still creating... [6m20s elapsed]
proxmox_vm_qemu.iot-fedora-elk: Creation complete after 6m24s [id=pve/qemu/101]

Apply complete! Resources: 1 added, 0 changed, 0 destroyed.
[cdeever@vdvntm-admin-01 fedora-elk-vm]$
```

```
# TYPE process_open_fds gauge
process_open_fds 8
# HELP process_resident_memory_bytes Resident memory size in bytes.
# TYPE process_resident_memory_bytes gauge
process_resident_memory_bytes 1.3131776e+07
# HELP process_start_time_seconds Start time of the process since unix epoch in seconds.
# TYPE process_start_time_seconds gauge
process_start_time_seconds 1.71518775779e+09
# HELP process_virtual_memory_bytes Virtual memory size in bytes.
# TYPE process_virtual_memory_bytes gauge
process_virtual_memory_bytes 1.270263808e+09
# HELP process_virtual_memory_max_bytes Maximum amount of virtual memory available in bytes.
# TYPE process_virtual_memory_max_bytes gauge
process_virtual_memory_max_bytes 1.8446744073709552e+19
# HELP promhttp_metric_handler_errors_total Total number of internal errors encountered by the promhttp metric handler.
# TYPE promhttp_metric_handler_errors_total counter
promhttp_metric_handler_errors_total{cause="encoding"} 0
promhttp_metric_handler_errors_total{cause="gathering"} 0
# HELP promhttp_metric_handler_requests_in_flight Current number of scrapes being served.
# TYPE promhttp_metric_handler_requests_in_flight gauge
promhttp_metric_handler_requests_in_flight 1
# HELP promhttp_metric_handler_requests_total Total number of scrapes by HTTP status code.
# TYPE promhttp_metric_handler_requests_total counter
promhttp_metric_handler_requests_total{code="200"} 0
promhttp_metric_handler_requests_total{code="500"} 0
promhttp_metric_handler_requests_total{code="503"} 0
a autoprov@localhost:~$ curl http://localhost:9100/metrics
[1] 0:ssh*
```

THANK YOU!!!

HashiCorp

PROXMOX