Proxmox Lab: Game of Active Directory - Environment Setup


benheater.com/proxmox-lab-goad-environment-setup

0xBEN August 26, 2024

In this module, we'll be taking steps to set up the initial environment and prepare to deploy Game of Active Directory (GOAD) v3 in our existing Proxmox environment.

Aug 26, 2024 6 min read

About this Project

ℹ️

This module is part of a larger project on setting up ***Game of Active Directory (GOAD) v3*** on Proxmox alongside our existing lab infrastructure. Click here to be taken back to the project landing page.

⚠️

This project also assumes that you've already built out the original Proxmox lab environment, as you'll need to lay some foundational network topologies before configuring GOAD here

Objectives for this Step

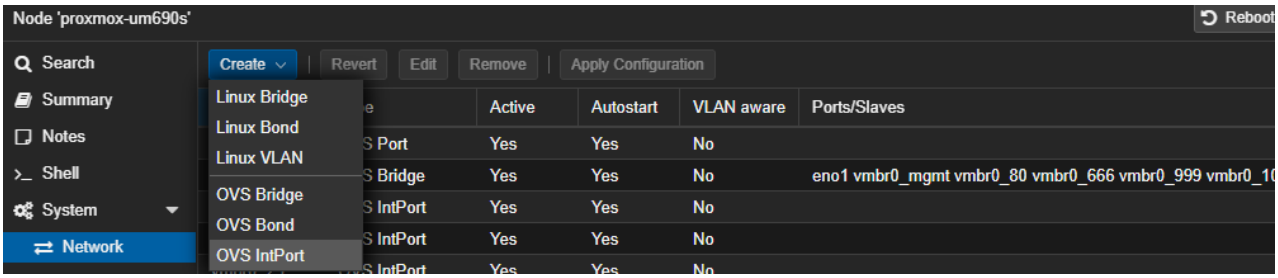
- Add the VLAN to our existing Proxmox and pfSense Setup
- Add DHCP scopes and add or update firewall rules
- Create a Linux Container and install tools that will be used to automate provisioning and configuration of resources

Updating the Network

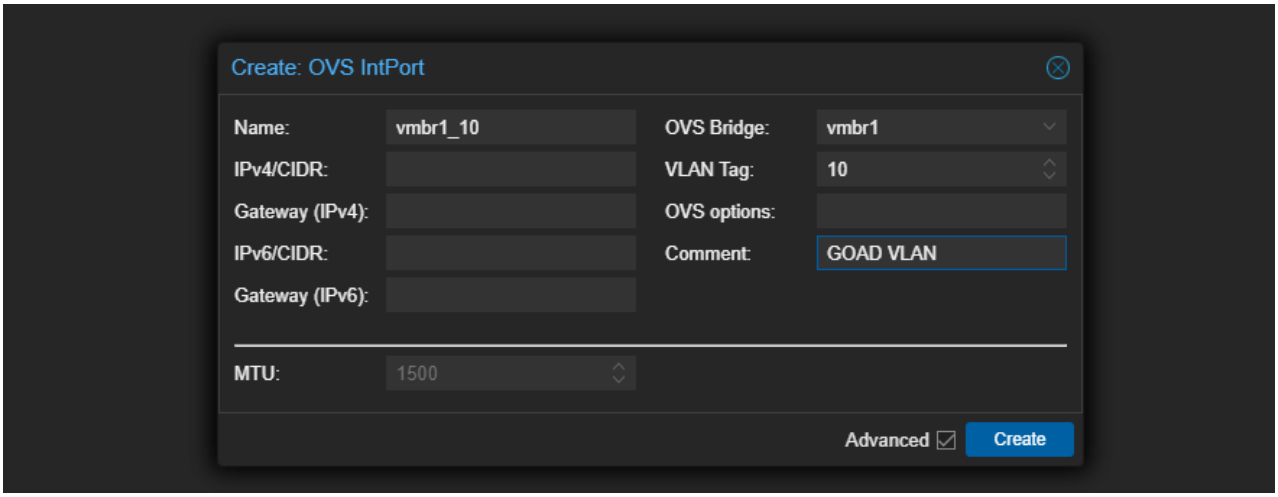
Add the GOAD VLAN

ℹ️

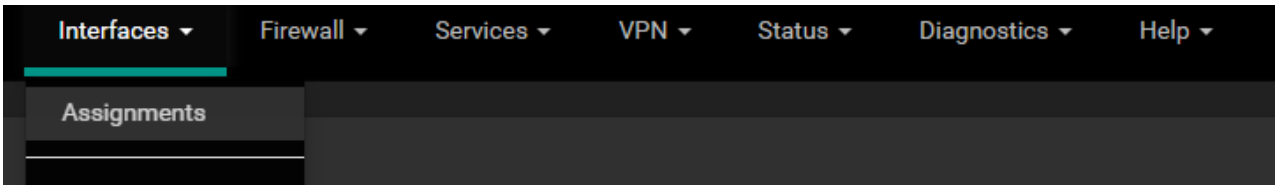
I'm going to keep things brief here, because I've already demonstrated multiple times in the main lab guide how to add / remove VLANs to / from the lab configuration.



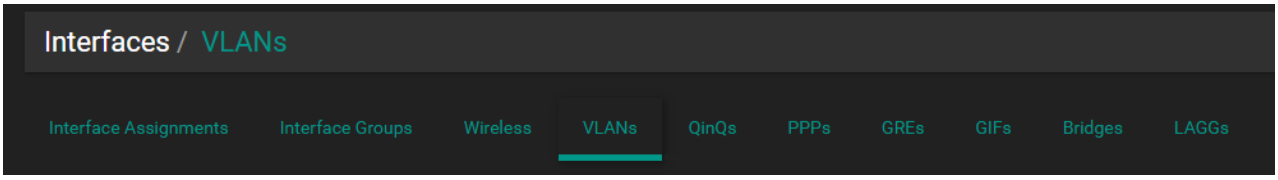
Create OVS IntPort



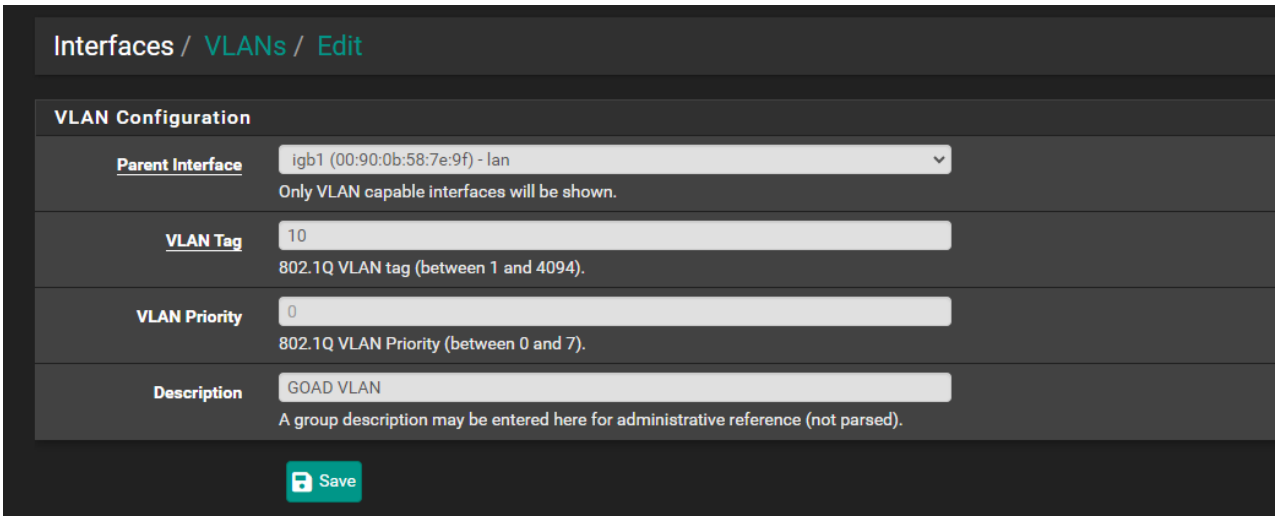
Click **Create**



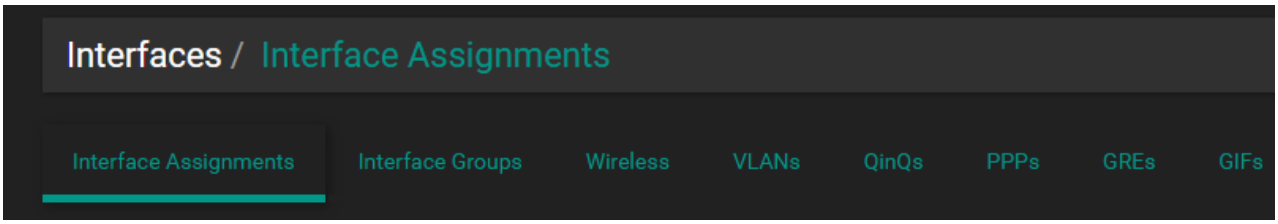
Log into pfSense and go to `Interfaces > Assignments`



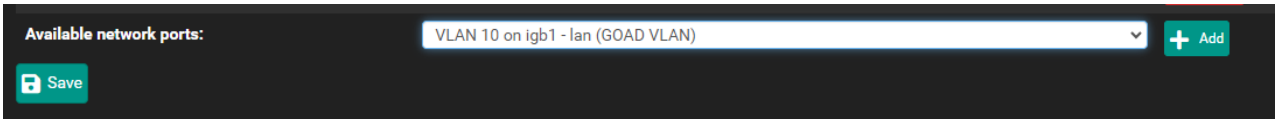
Click on VLANs > Click `+ Add`



Fill out and click **Save**



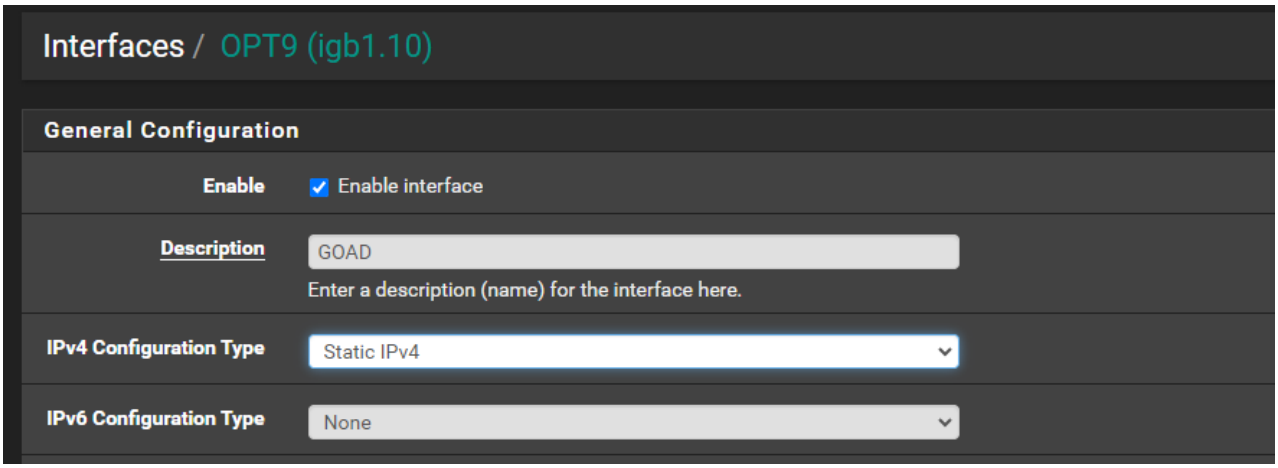
Click **Interface Assignments**

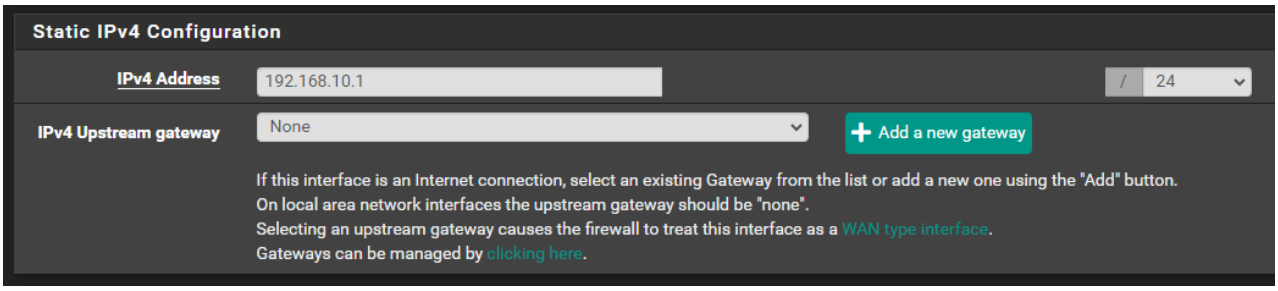


Choose the VLAN, click **Add**,and click **Save**

Configure the pfSense Interface

Click on your new interface -- `OPT9` in my case

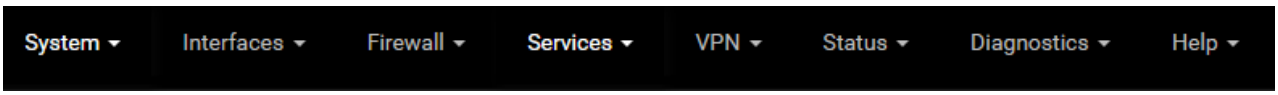




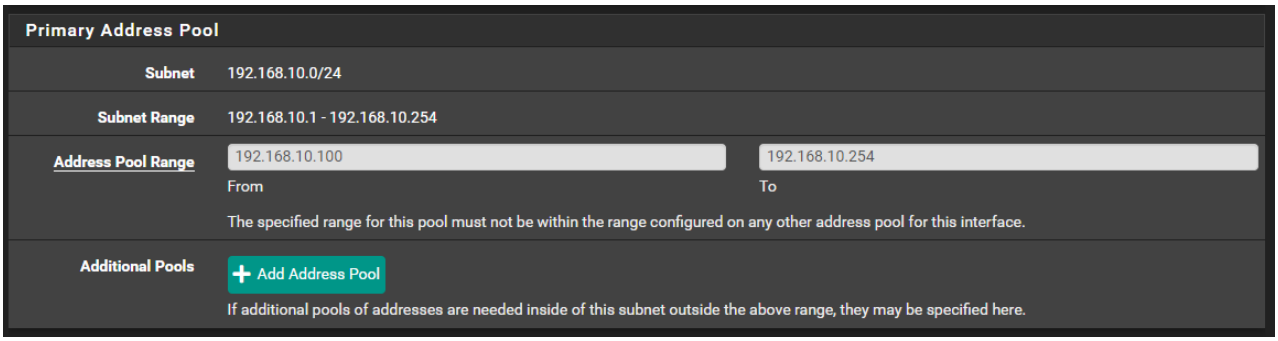
Click **Save**

Configure the DHCP Server

Typically, I'd have the DHCP server running on the Domain Controller, alongside DNS, but due to the size of the GOAD project and all of the various pieces, I'm going to stick with the creator's original design



Go to `Services > DHCP Server > GOAD`

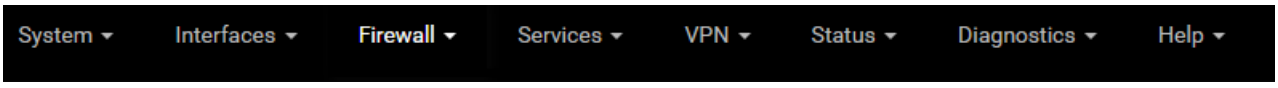


Click **Save**

Configure the Firewall Rules

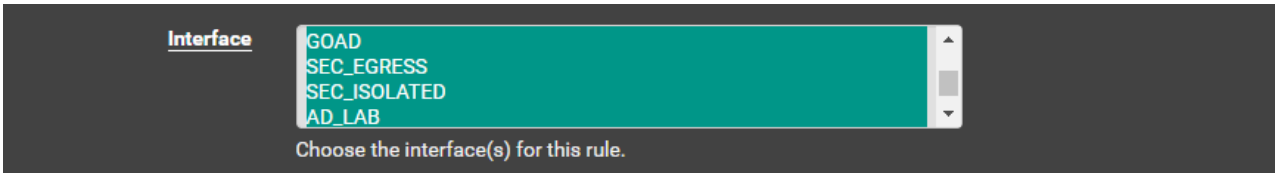
Floating Rule Updates

Note, that in the original lab guide, we've created various aliases and firewall rules that will be referenced here, so refer back to the original pfSense setup for more information



Go `Firewall > Rules > Floating`

Edit on the original floating rule here we created to block firewall management access

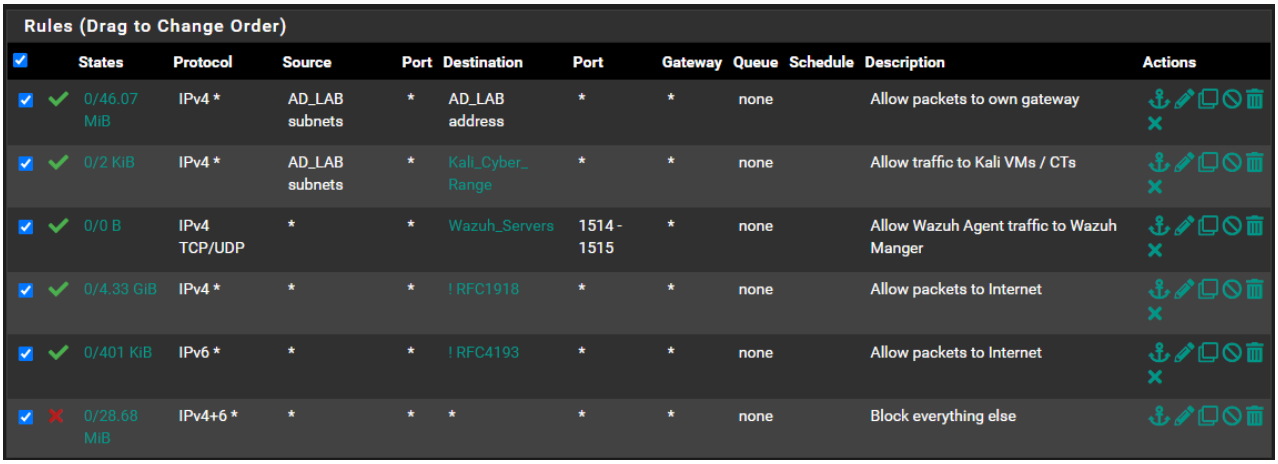


Add GOAD to the list of interfaces and click **Save**

GOAD Rules

💡

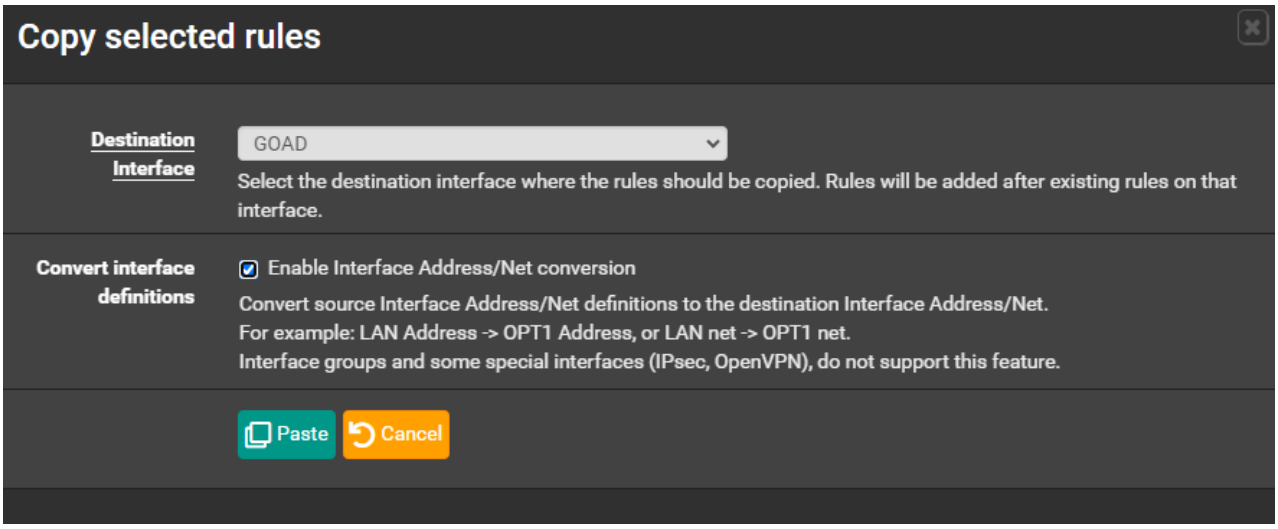
We're going to take a little bit of a shortcut here and borrow the rules that already exist for the **AD_LAB** interface



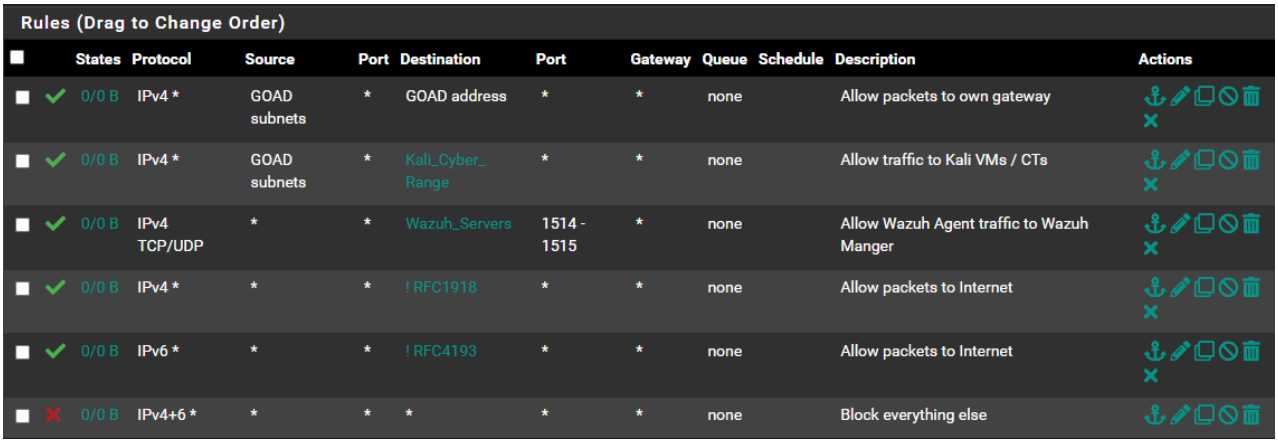
Select all the rules and click **"Copy"**

❗

Disregard the `Wazuh_Servers` rule in the screenshot, as that is out of the scope of the original lab guide and this lab guide



Fill out accordingly and click **"Paste"**



You should now see your GOAD rules are filled out accordingly. Click **"Apply Changes"** at the top.

Stage the Provisioning Host

This is the Linux Container that we'll log into and run Packer, Terraform, and Ansible to build and configure resources for the environment.

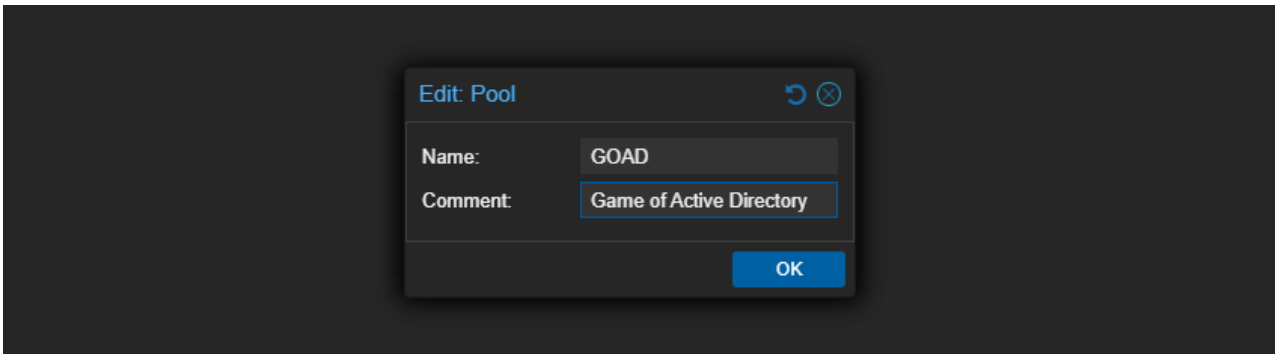
⚠️

Since the environment we've created in this Proxmox lab differs quite a bit from the one the original author, Mayfly created, we'll be making some changes to the Infrastructure-as-Code (IaC). Please be mindful of these changes while reading.

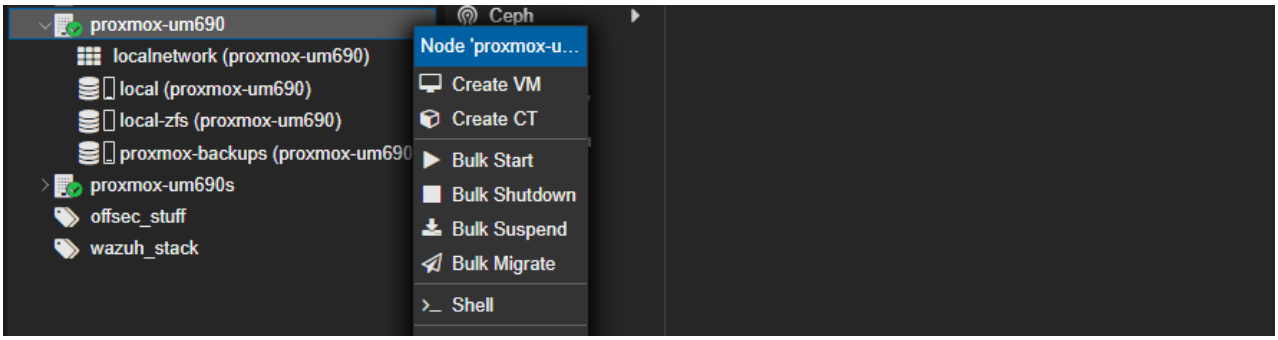
Create the Container

Click on "Datacenter"

Click on "Pools



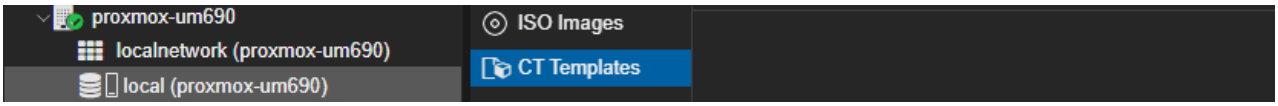
Click "Create" and fill out the form to your preference, then click OK



Right-click on your PVE node and choose `>_ Shell`

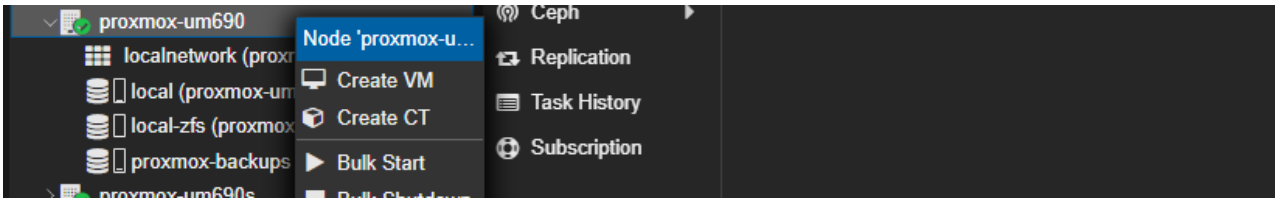
```
pveam update
```

Bash
Update the Linux Container template database

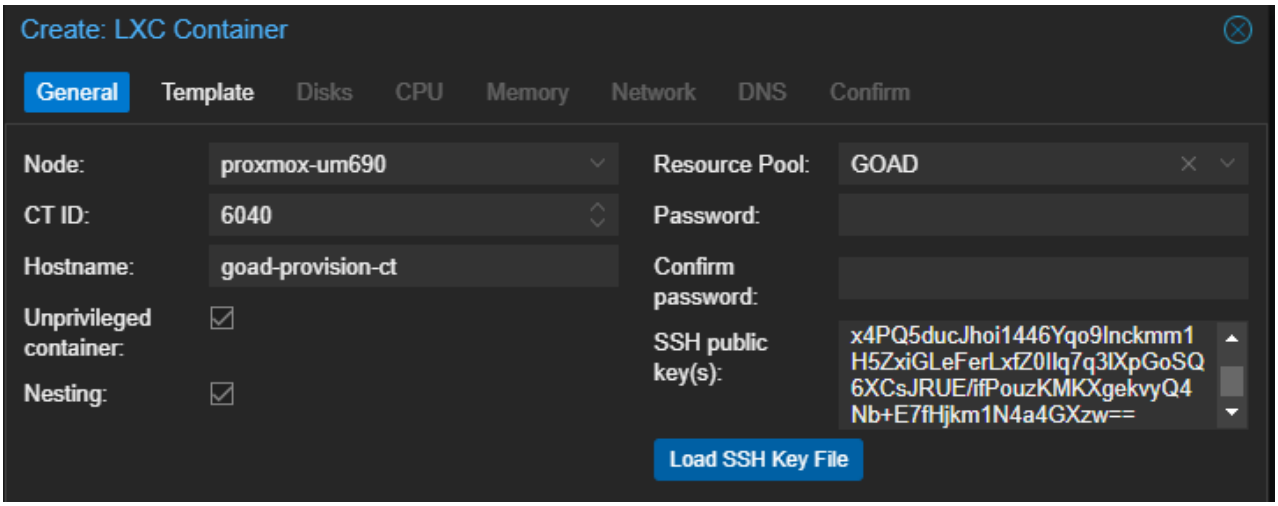


Click on your PVE node, click on "CT Templates", click on the "Templates" button

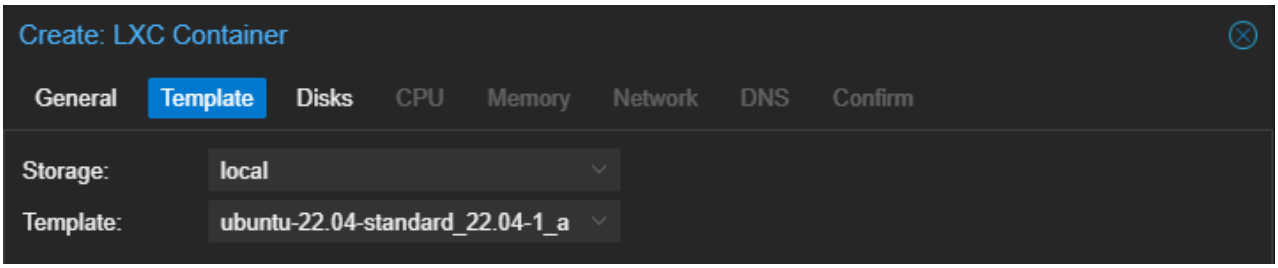
I'm going to use `22.04` version of Ubuntu, click "Download"



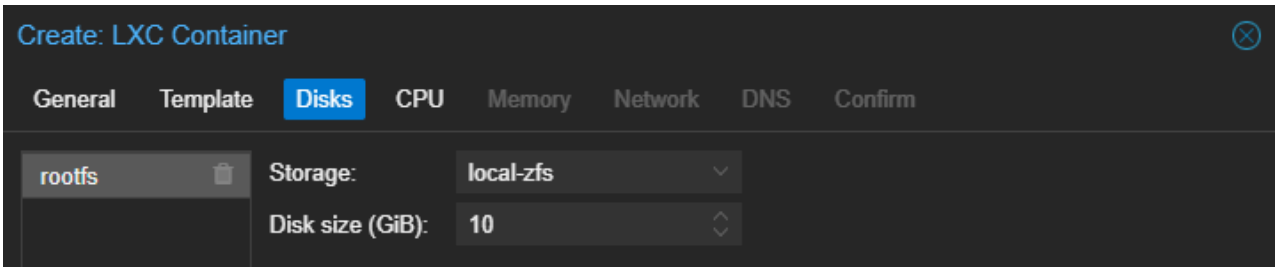
Right-click on your PVE node and choose "Create CT"



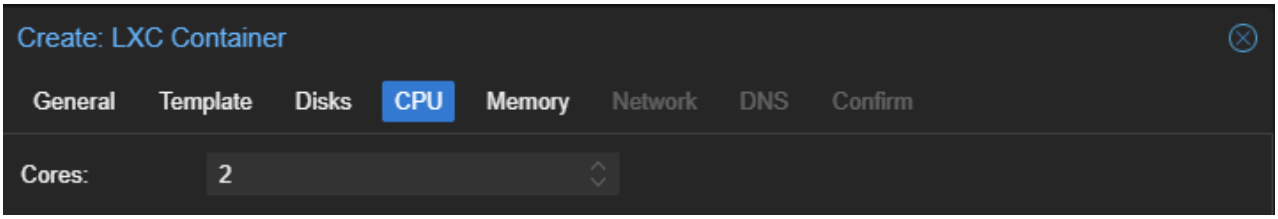
I'm going to authenticate using SSH keys, so my password field is empty

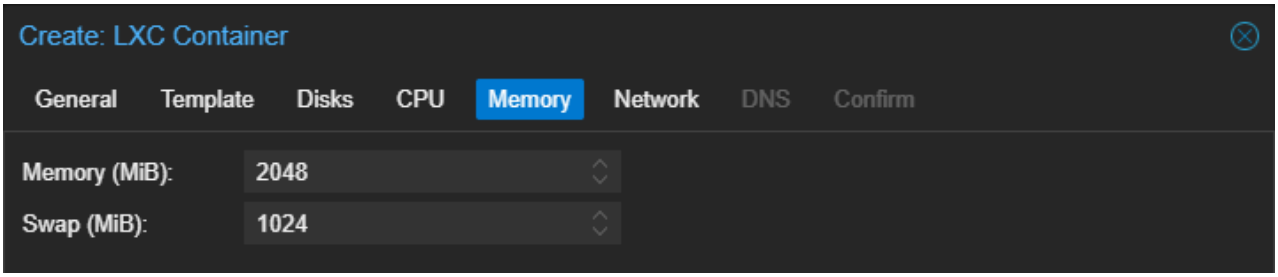


Choose your CT template

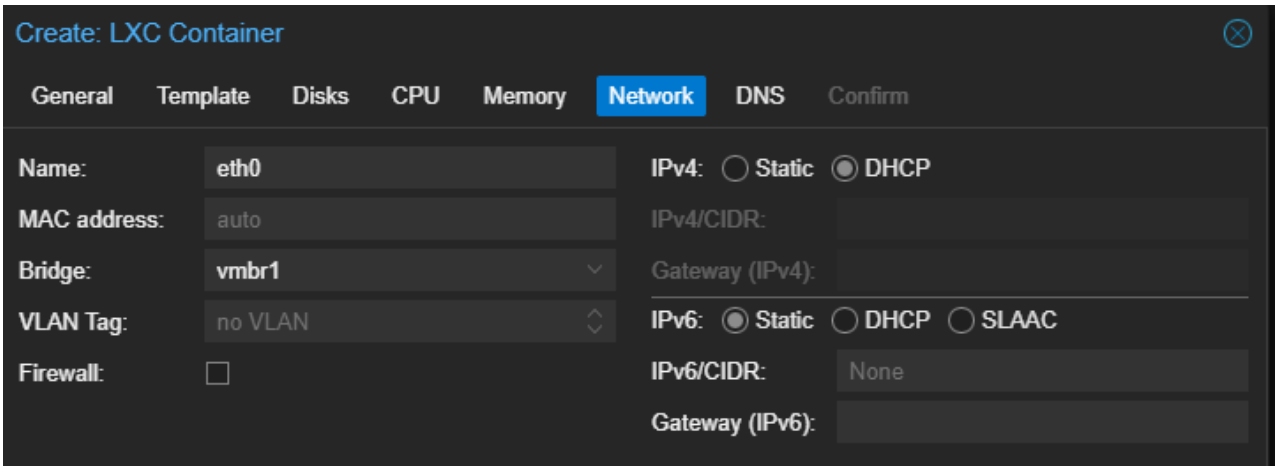


I'll start off with a 10 GiB disk, as it's trivial to add more storage later





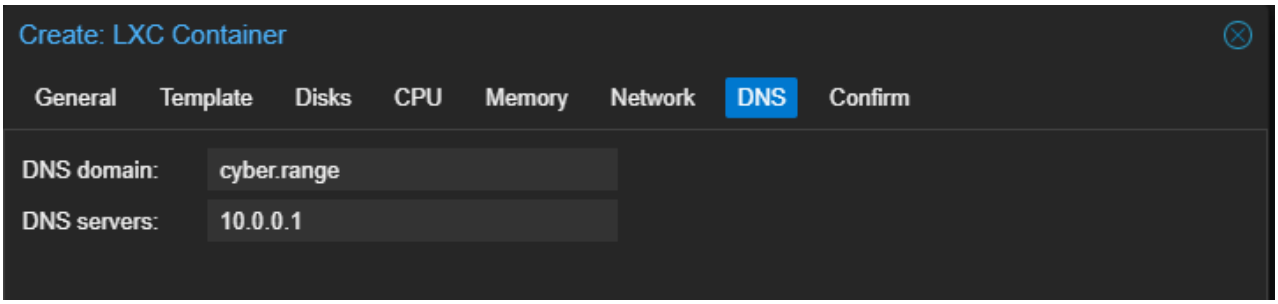
2048 MiB RAM should be sufficient



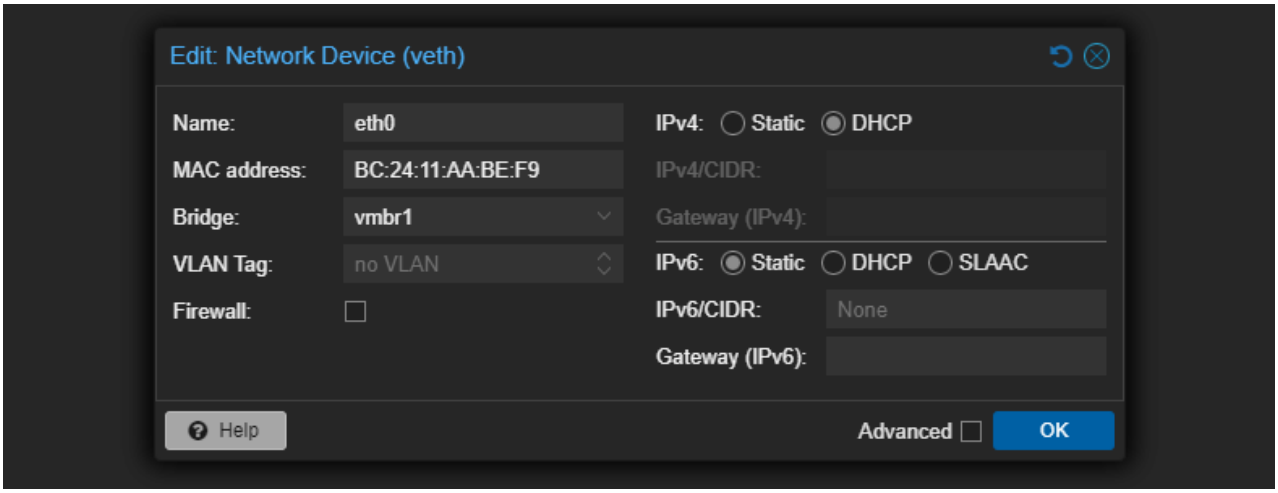
Putting the LXC on `vmbr1` will put the LXC on the pfSense internal LAN (`10.0.0.0/24`)

⚠️

If you haven't already done so, you'll want to add a static route on your home router, so that you can SSH into your provisioning LXC from your home network side



This will provide DNS settings to the container, so that it uses the pfSense local domain and default gateway as the DNS resolver



ℹ️

I'm going to take the MAC address from the container's settings, now that it's created, log into my pfSense VM on `vmbr1`, and allocate a DHCP reservation to this container, so that it is always at the same IP address. This is better for crafting firewall rules later.

✔️

When ready, you may start the container

Environment Setup

Log into the Provisioning Container

Log into your provisioning container via SSH key or password to open a terminal.

ℹ️

The `ssh` client application is available on all current versions of Windows and of course, has been available on Linux for ages

⚠️

If you're tying to SSH into the container, remember that the container is on `vmbr1` behind pfSense on the default LAN -- `10.0.0.0/24` with Kali. If you haven't added a static route into the LAN, please do so in order to reach it via SSH.

```
ssh -i id_rsa root@10.0.0.3
```

Bash

Authenticating via SSH key. I gave my LXC a DHCP reservation of `10.0.0.3` in my pfSense VM.

Install Dependencies

```
apt install python3-venv
```

Bash

```
cd /root
```

Bash

```
git clone https://github.com/Orange-Cyberdefense/GOAD
```

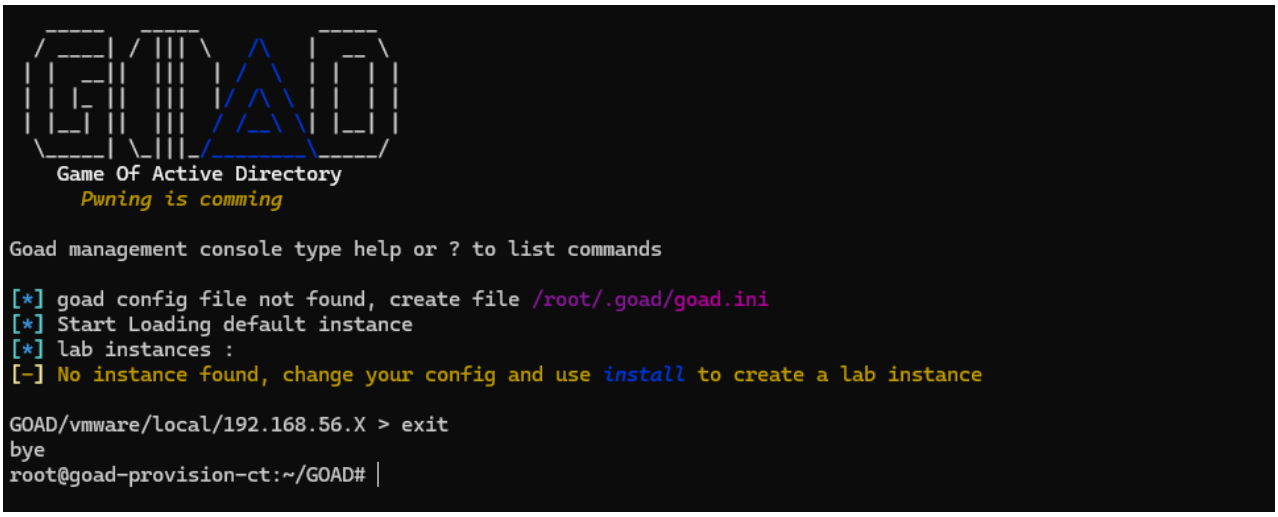
Bash

```
cd GOAD
```

Bash

```
./goad.sh
```

Bash



`exit` the interactive menu once the installation is complete

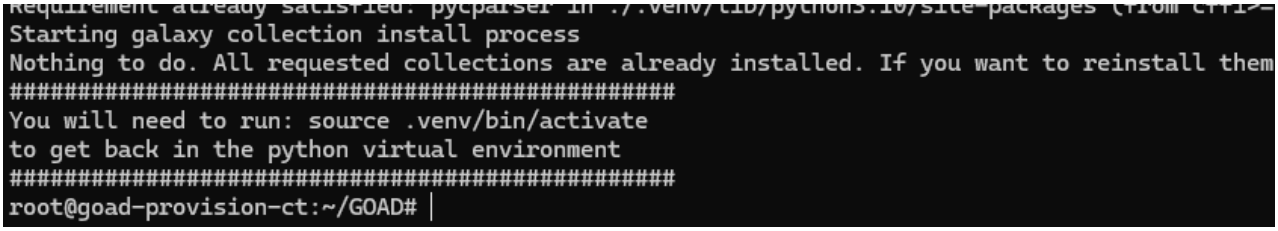
Prepare for Proxmox Installation

```
cd /root/GOAD
```

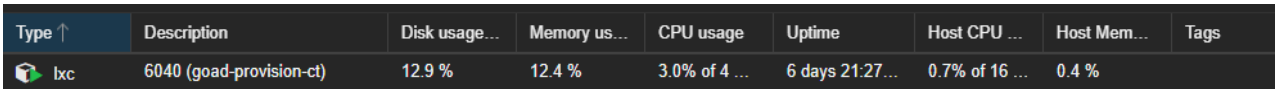
Bash

```
bash -f ./scripts/setup_proxmox.sh
```

Bash



Current State of the Lab



VLAN is added, firewall rules created, and the provisioning host is ready to do its job

Next Step

Proxmox Lab: Game of Active Directory - Creating VM Templates

In this module, we'll be taking steps to create some Windows Server 2016 and Windows Server 2019 templates using Packer for use in the Proxmox Game of Active Directory lab