

# How to Install Proxmox Virtual Environment on Debian 11

Learn how to install Proxmox Virtual Environment on Debian 11 with our step-by-step guide. Create a powerful virtualization platform for your servers.

---

# Contents

01	Introduction	3
02	Prerequisites	3
03	Install Proxmox Virtual Environment	3
04	Serving Management Interface using Nginx	7
05	Securing Management Interface using an SSL Certificate	9
06	Conclusion	10

# Introduction

---

Proxmox Virtual Environment is an open-source virtualization management program. It provides a single platform to manage services and functions like KVM Hypervisor, Linux Containers (LXC), storage & networking. In addition, it comes with an easy-to-use web-based management interface that provides full control at ease.

This article explains the installation of Proxmox Virtual Environment, using Nginx as a reverse proxy to serve the management interface & securing the management interface with an SSL certificate on a Debian 11 machine.

## Prerequisites

---

To complete this guide, you will need to:

- Deploy a fresh [Debian 11](#) Server
- Point a subdomain to your server

Please note that you can not use KVM Virtualization on Vultr's Cloud Compute instances as they are already virtualized. You can still use PVE for creating & managing LXC Containers. If you want to use KVM virtualization, you may proceed with Vultr Bare Metal or any other dedicated server.

## Install Proxmox Virtual Environment

---

### Change Hostname

You are required to point a subdomain to your server using A record. The same subdomain will be used throughout the article. For example, pve.domain.tld

Add hostname in `/etc/hostname`

```
# nano /etc/hostname
```

Overwrite the existing content with your subdomain and save the file using Ctrl + X then Enter

Add hostname in `/etc/hosts`

```
# nano /etc/hosts
```

Paste the following line below `127.0.0.1 localhost` and save the file using Ctrl + X then Enter

```
your_public_ip your_subdomain your_subdomain_name
```

**Example:** if your public IP is 169.254.169.254 and subdomain is pve1.example.com then your line should look like `169.254.169.254 pve1.example.com pve1`

Reboot the server to ensure everything works

```
# reboot
```

## Verifying Hostname

After your server is up and running, run the following command and check if the output matches with your subdomain & IP address.

Check hostname.

```
# hostname
```

Expected output.

```
your_subdomain
```

Check hostname IP.

```
# hostname --ip-address
```

Expected output.

```
your_public_ip
```

## Network Configuration (Optional)

Skip this section if your network wasn't set up using cloud-init. You can verify that by checking if `/etc/network/interfaces.d/50-cloud-init` file exists on your machine.

Change default network configuration.

- Identify your main interface (refer to `ifconfig` command).
- Add your main interface configuration in `/etc/network/interfaces`.

Disable cloud-init networking.

```
# nano /etc/cloud/cloud.cfg.d/99-custom-networking.cfg
```

Paste the following line and save the file using `Ctrl + X` then `Enter`.

```
network: {config: disabled}
```

Remove cloud-init network config file.

```
rm -f /etc/network/interfaces.d/50-cloud-init
```

Reboot the server to ensure everything works.

```
# reboot
```

## Add Required Repository

Add repository in `/etc/apt/sources.list`.

```
# nano /etc/apt/sources.list
```

Paste the following line and save the file using `Ctrl + X` then `Enter`.

```
deb http://download.proxmox.com/debian/pve bullseye pve-no-subscription
```

Add GPG key to the APT sources keyring.

```
# wget https://enterprise.proxmox.com/debian/proxmox-release-bullseye.gpg -O /etc/apt/trusted.gpg.d/proxmox-release-bullseye.gpg
```

Refresh package information.

```
# apt update
```

## Installing Proxmox Virtual Environment

Install the `ifupdown2` package.

```
# apt install -y ifupdown2
```

**Warning:** Installing the `ifupdown2` package might cause network interruption. It is recommended to connect through the web console so that you don't lose access in case of a network interruption.

Install the Proxmox VE.

```
# apt install -y proxmox-ve open-iscsi
```

Reboot the server to boot using Proxmox's kernel.

```
# reboot
```

## Verifying PVE Installation

After your server is up and running, you can verify if the installation was done successfully by opening the following link in your web browser.

```
https://your_subdomain:8006/
```

You can log into the management interface using the same credentials you use for SSH.

## Serving Management Interface using Nginx

Some environments do not allow connections to non-standard ports, and it is not recommended to change PVE's port configuration. Using Nginx is the best solution for port standardization and handling high traffic.

### Install Nginx

```
# apt install -y nginx
```

### Adding vhost for Management Interface

Add vhost file to `sites-available` directory.

```
# nano /etc/nginx/sites-available/pve
```

Paste the following content (replace `your_subdomain` with your actual subdomain) and save the file using `Ctrl + X` then `Enter`.

```
server {  
  
    listen 80;  
    server_name your_subdomain;  
  
    proxy_redirect off;  
    location / {  
        proxy_http_version 1.1;  
        proxy_set_header Upgrade $http_upgrade;  
        proxy_set_header Connection "upgrade";  
        proxy_pass https://localhost:8006;  
        proxy_buffering off;  
        client_max_body_size 0;  
        proxy_connect_timeout 3600s;  
        proxy_read_timeout 3600s;  
        proxy_send_timeout 3600s;  
        send_timeout 3600s;  
    }  
  
}
```

Add a soft link of the vhost file in `sites-enabled` directory.

```
# ln -s /etc/nginx/sites-available/pve /etc/nginx/sites-enabled/pve
```

Test the configuration.

```
# nginx -t
```

Expected output.

```
nginx: the configuration file /etc/nginx/nginx.conf syntax is ok  
nginx: configuration file /etc/nginx/nginx.conf test is successful
```

Reload Nginx.

```
# systemctl reload nginx
```

## Verify the Accessibility

You can verify if the reverse proxy is working properly or not by opening the following link in your web browser.

```
http://your_subdomain/
```

## Restrict Direct Access

Once you've verified that your reverse proxy works, you can change the listener IP of the management interface to restrict direct access.

Add listener IP in `/etc/default/pveproxy`.

```
# nano /etc/default/pveproxy
```

Paste the following line and save the file using `Ctrl + X` then `Enter`.

```
LISTEN_IP="127.0.0.1"
```

Restart the `pveproxy` service.

```
systemctl restart pveproxy
```

# Securing Management Interface using an SSL Certificate

We will use Let's Encrypt to obtain an SSL Certificate for free. Please make sure you have pointed your subdomain to the server's IP address. The steps given below will only work if you are serving the management interface using Nginx.

## Install Certbot

```
apt install -y certbot python3-certbot-nginx
```

## Install Certificate on Nginx

You will be asked to enter your email address when you run the following command, please enter your email address and leave the rest set as default.

```
certbot --nginx -d your_subdomain
```

## Verify Accessibility

You can verify if the SSL Certificate is configured properly or not by opening the following link in your web browser.

```
https://your_subdomain/
```

## Test Auto Renewal

Let's Encrypt certificates are only valid for 90 days, but since we are using certbot, it will handle auto-renewals for us. You can verify if the auto-renewal works by running the following command.

```
certbot renew --dry-run
```

If the above command doesn't throw an error, it means your SSL certificate will be renewed automatically without any issues.

## Conclusion

In this article, you installed Proxmox Virtual Environment, used Nginx as a reverse proxy for PVE's management interface & installed an SSL Certificate

using `certbot`. If you're new to Proxmox Virtual Environment and don't know how it works, their [official documentation](#) is a good place to start.



VULTR

