Self-Hosting 101

Author: JJ Quinlivan

Date: December 5, 2019

Self-Hosting 101 Agenda

- Self-Hosting Introduction
- Local Network Access
  - NFS
  - Samba
  - Syncthing
- Internet Access
  - Domain name & DDNS
  - OpenVPN & Wireguard
  - Let’s Encrypt
  - Reverse Proxy
  - Firewall/Router
  - NextCloud
  - Jellyfin

Why self-host?

- Advantages
  - Privacy
  - You will own your own data
  - Learning Experience
  - Reuse old equipment – give it a second life
  - Saving Money
- Disadvantages
  - Not backed up by corporation – no guaranteed uptimes
  - Risk of failure is higher
  - You need knowledge to manage by yourself

Misconceptions

- I can’t afford it
  - Many services will run on something as small as a Raspberry Pi.
- I cannot secure it
  - Let’s Encrypt is free
  - Reverse Proxy is easy to setup
  - OpenVPN and Wireguard for VPN access
- I can only run one app from home
  - Can run multiple services from containers, snaps, VMs, etc.

My Self-Hosting Setup

- Old Intel Dual Core Xeon Server
  - Two ZFS Mirrors: Two 250GB SSDs (root) and Two 8TB HDDs (data)
  - Ubuntu 19.10 with latest ZFS on root partition
    - Samba, NFS, Syncthing
    - NextCloud Snap
    - Cockpit and Netdata for administration
  - CentOS 8 VM with Podman for Containers
    - Jellyfin for media files
    - Gitea git server
    - Transmission, Sonarr (TV), Radarr, (Movies), Lidarr (Music)
    - Unifi Controller

My Self-Hosting Setup

- Mini-PC with Celeron dual core processor for backup
  - ZFS: One 250GB SSD (root) and Two 4TB HDDs (data)
  - Ubuntu 19.10 with latest ZFS on root partition
- Pfsense Firewall
  - ACME for Let’s Encrypt
  - OpenVPN Server
  - HAproxy Reverse Proxy
- Domain Name quinlivan.org registered at namecheap.com

Local Access

- Certain services run better on host server
  - Admin services that require access to host server
    - Cockpit, Netdata, etc
  - Direct user access of files runs better on host server
    - Container: UserIDS must match host server – disables security
    - VMs: Files must be in VM or accessed through NFS

Local File Access

- Webdav
  - Very fast, low resources - Good for read only access to multimedia files
  - Can access Nextcloud files through webdav
- NFS
  - Very fast, low resources - Great for read only access to multimedia files or admin access to full drive
  - No user security without complex setup
  - Can limit access by host, including read only access to specific hosts
- Samba
  - Slower than NFS & webdav and requires more resources on host server, but still viable option
  - Great for giving each user their own home directory only they have access to
  - Can also setup “Inboxes” or download directories for multimedia files so most of multimedia library is stays read-only
- Syncthing
  - Continuous directory synchronization
  - Peer-to-peer – not client-server
  - No backups – files deleted on one device get deleted on 2nd device if two way sync setup

NFS

- Setup
  - Install nfs: Ubuntu – nfs-kernel-server, Arch – nfs-utils
  - Setup shared/exported directory(s): /mnt/sharedfolder
  - Configure /etc/exports file for host access:
    - /mnt/sharedfolder 192.168.1.50(rw,sync,no_subtree_check)
    - /mnt/sharedfolder 192.168.1.0/24(rw,sync,no_subtree_check)
  - ZFS can configure NFS access per dataset
  - Start nfs services: systemctl enable –now nfs

Samba

- Setup
  - Install samba
  - Setup users:
    - useradd -d /home/username -g maingroupname -s /bin/null
    - passwd username
    - smbpasswd -a username
  - Configure /etc/samba/smb.conf – add additional directories and permissions:

    -
      ```
      [<share name>]
      path = /path/to/share
      valid users = username
      read only = no
      ```
  - Start samba service: systemctl enable –now samba

Syncthing

- Setup
  - Install Syncthing on at least two devices
  - In Linux start Syncthing service: systemctl enable –now syncthing
  - Configure both devices in parallel – configure on one device and accept changes on 2nd device
    - Add new device – easier on mobile with QR code
    - Add folders
  - Setup automatic backup of synced directories on host server
    - I use ZFS snapshots and replication

Syncthing Setup Demo

Internet Access

- Limit external access to home services
  - Put all home services in containers or VMs
    - VMs more secure but require more resources
    - Best policy – run all containers in one VM on host server
  - Limit access through VPN and/or Reverse Proxy
    - Run VPN and/or reverse proxy on firewall/router or in containers on host server
    - Keep firewall/router, VPN and reverse proxy up to date since first point of attack
    - VPN good for 1 or 2 users, or full access to network for admin in case of issue with host server
    - Reverse proxy easier for users to access

Internet Access - Domain

- Domain Name & Dynamic DNS (DDNS)
  - Most ISPs give customers IP addresses through DHCP that can change at any time
  - Register a domain name with a name service like namecheap.com
    - Name service should provide DDNS and access to create DNS records
    - If no DDNS can point subdomain to Cloudflare or other free DDNS service
  - Cost: $10 - $20 per year for .com address more for unique addresses (i.e. .local, info, .network, etc.)
- Run DDNS client on router or home server to update domain name with current IP address

Internet Access - VPN

- OpenVPN
  - Many routers have built-in OpenVPN server setup on the router.
  - If not can install 3rd party router software (i.e. tomato, DD-WRT, etc.)
  - Run router like pfsense or opnsense
  - Can install OpenVPN docker container on host server and open port on router
- Wireguard
  - New and still considered beta, but many use it for production with no issues
  - Much faster than OpenVPN
  - No options available on routers, but not too difficult to setup on Linux.
  - Creates an additional network device on Linux, but must setup forwarding rules if you want to access more than that IP address
    - Additional tools available in most package repositories to make this easy

Let’s Encrypt

- Let’s Encrypt – free SSL certificates
  - Must own your own domain
    - Can confirm domain ownership through custom DNS entry on name service or file stored on web server
  - Can create generic subdomain SSL certificate for reverse proxy
    - i.e. *.quinlivan.org – includes all subdomains
  - Auto renew every 90 days
  - Let’s Encrypt software usually automatic setup with most web services
    - Nginx docker container, NextCloud Snap, pfsense, opnsense, etc.

Reverse Proxy

- Sits behind firewall and intercepts client requests and directs them to appropriate backend server
- Can also run reverse proxy on VPS like digitalocean.com.
- Benefits
  - Load balancing: distributing requests to multiple backend servers
  - Web acceleration: compress and cache data
  - Security: Single, locked down access to multiple services
- Options
  - Nginx docker container – easy to setup and very secure
  - HAproxy on pfsense or opnsense router/firewall – can handle more than just web services
  - Traefik – great for kubernetes, council or other orchestrated container options – can also handle more that just web services

Reverse Proxy

Docker/Nginx Install Demo

Firewall/Router Setup

Forward Ports for VPN server and reverse proxy to home server

- TCP 443 for reverse proxy
- UDP 1194 for OpenVPN (can change port)
- UDP 51872 for Wireguard Peer A (UDP 51902 for Peer B)
- TCP 22000 for Syncthing sync port, UDP 21027 for Syncthing discovery port
- TCP 22 for SSH (if you don’t setup VPN server then setup SSH so you can access server remotely for issues)

- Recommend pfsense or opnsense for firewall/router
  - Comes with OpenVPN, DDNS, VLANs, HAProxy, etc.
  - Opnsense can run TOR and Wireguard

Remote File Access Options

- NextCloud
  - Open source, very popular
  - Can access or sync files remotely
  - Lots of other features (i.e. shared calendar, contacts, tasks, etc.)
  - Lots of addons to add features (i.e. music, 2FA, etc.)
- Seafile
  - Open source
  - Only does file sharing but does it VERY WELL
  - Best option if you only want to access or sync files
- Syncthing
  - Open source, very popular
  - Sync files only no access
  - Works anywhere with own encryption, very secure

NextCloud

- Easiest Setup through NextCloud Snap
  - Complete setup of everything you need to run NextCloud
  - Run behind reverse proxy since not in container
- Other options
  - Official NextCloud docker container
    - Has issues if you add a lot of addons/features
  - Unofficial NextCloud docker containers
    - NextCloudPi is best
  - Run Mysql container to provide NextCloud database

NextCloud Snap Install Demo

Multimedia Sharing Options

- Kodi
  - Open source client only software, Great interface
  - Local access only – technically can access files through webdav using NextCloud but very slow
  - Can run mysql server so multiple Kodi installations can share database
- Plex
  - Most popular multimedia sharing option
  - Per month fee or purchase mobile client for each device
  - No privacy – tracking, must opt-out
- Emby
  - Similar to Plex, but not as mature
  - Again per month fee or purchase mobile client for each device
- Jellyfin
  - Open source version of Emby
  - Not as mature – clients include web, android and kodi addon, but works well

Docker/Jellyfin Install Demo

My Current/Future Projects

- Orchestration for Containers
  - HashiCorp Council, Vault and Nomad
  - Replace HAProxy with Traefik
- Additional Services
  - Bitwarden server
  - Ansible AWX
  - Zabbix for monitoring
  - Smoke Ping for monitoring network performance
- Change OpenVPN to Wireguard