链滴

家庭基建不完全指南

作者：evling

原文链接：https://ld246.com/article/1602549314758

来源网站：链滴

建设需求

出于兴趣爱好，更出于是对自己劳动成果的数字化保留，易雾君经历过惨痛的数据丢失，很 2 地将 Excel 的主密码放到了 Excel 里边，由于主密码是随机的，也是临时产生，还未记住，当然磁盘加密的密也存储在了 Excel 里，自己给自己锁住了，导致 2017 年和 2018 年积攒的数据全给弄没了，故期望设一套完善的家庭网络系统来提升生活便利性，同时能保障生活中积攒的点滴长久保存。

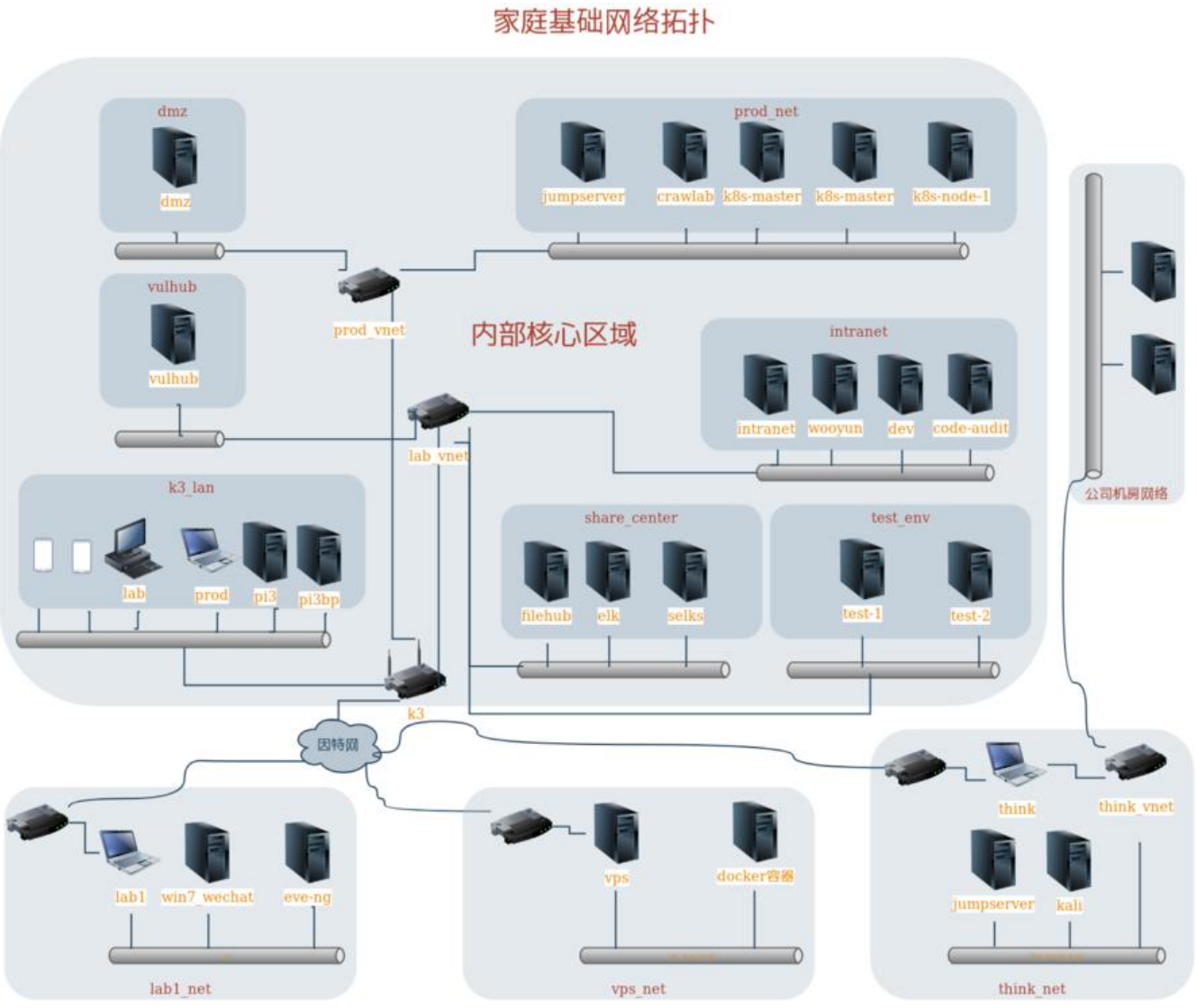
建设发展历史

● **2018年：** 初来乍到深圳，手上有台台式机，和两个树莓派3B和3B+，没有牵宽带，本身可折腾空极小。而且树莓派最大的硬伤是网口带宽太小。

● **2019年：** 建设力度集中的一年，开始拥有自己的家庭宽带并申请了公网IP，有闲置的一台笔记本脑和朋友送我的一台 K2T 路由器，结识 Proxmox 虚拟化技术，很符合当下组网需求，整体框架进行重构。

● **2020年：** K2T 升级为 K3 整体框架再次进行重构，本次考虑的因素，开机时长决定了哪些应用适在哪些设备上，于是将 24 小时开机的树莓派 3B+ 用于部署基础应用，避免了机器关机期间无法提供务。机器主要职能更明确化，爬虫性质的应用集中部署在一台定时开关机的生产机器上，试验环境及必需的应用部署在不定时开机的机器上。

网络拓扑示意图



原文链接：家庭基建不完全指南

设备基本信息

目前加入网络的设备详情如下：

斐讯K3

- 名称：vnet
- CPU：BCM4709C Cortex A9 双核 1.4GHz
- 内存：512M
- 存储：128M + 外挂 3T 机械
- 操作系统：OpenWRT 19.07.3
- 主要角色：核心路由、OpenVPN服务、DNS服务
- 开机策略：24小时开机，定时重启
- 加入方式：本地网络

生产机器

- 名称：prod
- CPU：i7 3540M 3.00GHz
- 内存：16G 双通道 1600 GHz
- 存储：128G 固态 + 1T 机械
- 操作系统：Debian 10
- 角色：生产力机器
- 开机策略：8:00开机、第二天凌晨0:30关机
- 加入方式：本地网络

台式机

- 名称：lab
- CPU：i5 6500 3.20GHz
- 内存：32G 双通道 2133GHz
- 存储：256 固态 + 3T 企业硬盘
- 操作系统：Debian 10
- 角色：实验机器、日常使用
- 开机策略：按需通过 etherwake 唤醒，主要考虑到节能问题
- 加入方式：本地网络

Pi3

- 名称：pi3

- CPU：BCM2837 1.20GHz
- 内存：1GB LPDDR2 SDRAM
- 存储：1T 机械
- 操作系统：Debian 10
- 角色：核心内部文件存储服务
- 开机策略：24 小时开机，定时 6:00 重启
- 加入方式：本地网络

Pi3bp

- 主机名：pi3bp
- CPU：BCM2837B0 1.40GHz
- 内存：1GB LPDDR2 SDRAM
- 存储：300G 机械
- 操作系统：Debian 10
- 角色：对外发布服务
- 开机策略：24 小时开机，定时 6:00 重启
- 加入方式：本地网络

老弟的闲置笔记本

- 主机名：lab1
- CPU：i3 8130U 2.20GHz
- 内存：8G
- 存储：机械512G
- 角色：实验机器、应用挂机等
- 开机策略：24 小时开机，想起的时候，手动重启下
- 加入方式：OpenVPN

老弟的主力机器

- 名称：samson
- CPU：i7 8750H 2.20GHz
- 内存：16G
- 存储：1T 机械
- 角色：共用账户，远程视频剪辑、PS，老弟工作日常
- 开机策略：由老弟定
- 加入方式：OpenVPN

工作用机

- 名称：think
- CPU：i5 7200U
- 内存：16G
- 存储：256G 固态 + 512G 机械
- 操作系统：Debian 10
- 角色：工作主力机器
- 开机策略：24 小时开机，偶尔带走会不在线，对在线没有硬性要求
- 加入方式：OpenVPN

现有解决方案

基础组网

通过 OpenVPN 连接异地主机，为便于审计，整个内网主要采取路由转发方式，只在外网出口、和工机接入处做源地址转换，OpenVPN 客户端所在子网则通过 OpenVPN 自带的 iroute 技术进行逆向由数据包。Dnsmasq 用作内部核心 DNS 解析服务器。网络主要分家庭网和工作网，家庭网与工作没有直接打通，而是需要先登录工作机上的跳板机方可进一步操作工作网资产，出于规避将家庭网中风险引渡到工作网络的风险。

虚拟化技术

最开始采用纯 Docker ，发现内网有虚拟化 win 系统的需求，实属刚需，后来调研到 Proxmox 能很地进行虚拟机管理，是个比较适合于中小企业及家庭的虚拟化管理平台。初次感受到它的魔力后，全PC统统采用 Debian 系统，搭载 Proxmox ，简直好用到不要不要，目前一直很稳定。重在没出什么娥子，且备份快照非常实用。

存储应用服务

NFS: K3 等本身不可以安装 filebeat 日志采集程序，可通过 NFS 挂载到其他能运行 filebeat 的机器实现对 K3 日志的采集；挂载 PVE 主机以便远程备份。

Samba：常规文件共享、家庭影音共享给TV

Kodbox：通过远程上传文件（尤其是大文件）、文件预览、电子书阅读等的体验很不错，用过都说。还支持 onlyoffice 等应用，远程协作也挺不错。目前还支持 Webdav ，可用性大大延展。极力推大家试试。

Nextcloud：该应用其实和 Kodbox 一样，都是网盘性质，技术成熟度比较高，当然安全性也更高，应用内子应用特别多，场景化适应能力强，阅读文章的你不妨部署两个应用，根据后期需求实现主力移，再做最后的决定，毕竟部署很简单，docker-compose 一键可以搞定的事。易雾君将它用于外文件的分享，24小时运行于 PI3B+ 机器上。

密码管理

密码这个东西真的很重要，极度敏感，易雾君个人的建议是：使用专业开源的密码管理工具，最好是线的，避免使用浏览器插件及浏览器自带的密码管理工具。易雾君在权衡安全性及便利性后，最终选择 Keeweb 结合 Nextcloud webdav 实现多机器共享的方式集中管理密码。

安全备份

备份的网盘有许多，国内产品，易雾君当然首选百度网盘，自动化上传则利用的 bypy 客户端，bypy

运行于 K3 路由器全天值守。由于普通用户上传文件大小有 4G 限制，需要 split 对文件分割，而且，度网盘这种公共类网盘，考虑到信息泄漏问题，易雾君采取了 GPG 对待传文件做了加密后再分割处，最后再上传，这些操作均在 K3 路由完成，如果你对 K3 核心路由的转发包性能要求高的话，建议将 GPG 加密过程转移到其他机器。

日志管理

日志管理方案采取 ELK 方案，redis服务运行于 24 小时开机的树梅派 3B ，redis 服务集中汇集各路志，集中提供给 logstash ，当部署有 ELK 一开机就可有日志数据消费，这样的方式可以确保即日志遗漏，那么装有 ELK 的机器能够随意歇气，节省电能，延长寿命。目前重点采集的日志包括如下几大：Nginx、OpenVPN、Proxmox、Modsecurity。

对外发布

对外开放的 OpenVPN 网关服务，供异地主机接入内网，如果机器在海外，可能不好使，最好都是在内网络环境。

部署 Web 站点主要有：主站（Solo）、论坛（Symphony）、即时聊天（RocketChat）、网盘（Nxtcloud）。

入侵检测

家庭网络对外开放，直接威胁到咱们的彻身利益，有必要部署一个简易的入侵检测系统，这里选取 SEKS 作为核心检测系统，K3 核心路由通过 Iptables TEE 模块将流量镜像到 SELKS 虚机。

树梅派持久化

相信 PI 粉的你总会遇到文件系统崩溃的问题，用着用着意外断电啥等莫名的因素导致莫名的开不了，易雾君也曾为之烦恼过，现采取的方案是将硬盘通过 USB 连接树梅派，分出两个区，一个系统盘区和数据盘分区，操作系统采用 64 位 openfans-community-offical/Debian-Pi-Aarch64 ，它自已经安装有 Docker ，需要额外装个 docker-compose ，将 docker 的存储卷配置到数据分区（如载的 /data 目录），最后将系统分区采用 Overlayfs 固化只读，最后咱们的主力操作均在 docker 下任何改动都不影响系统分区，你说安逸不。

堡垒机

Jumpserver 毋庸置疑成为堡垒机首选，易雾君主要将它用作集中运维管理，它对你每步操作均有记，回头忘记了操作命令，或者系统发生故障需要复盘，可以参考 Jumpserver 的历史会话，这些历史话还能轻松用做视频教程，传播分享。

笔记方案

对于笔记记录，优秀的有网易笔记、印象笔记，但本着对个人数据的保密性原则，易雾君依旧采取开措施u，选用 Joplin 配合 Nextcloud 的 webdav 功能实现远程同步，Joplin 支持加密数据、支持 we 网页截取（重要网页资产本地保存值得拥有，日后细品），同时还是款优秀的待做事项清单管理工具方便规划你的任务计划。

爬虫

crawlab 是易雾君最近发现的一款优秀爬虫框架集合，集成主流爬虫框架，可考虑将它用作统一的爬管理平台，其强大的引擎需要后续深入挖掘，暂时先讲这么多。

公众号讯息采集

公众号信息关注这方面，易雾君很早就意识到它的重要性，我们日常有喜欢的公众号，关注着，但是脑的记忆有限度，分析能力停留在几个小时，最多也就是几天的样子，文章更新太多后，最后只对最资讯有印象，若是本地能存储下来，不仅对最新的资讯有分析空间还对历史资讯也有参考余地，更重的是，可借助微信平台的关联能力，拓宽资讯的关注面。经过半年的沉淀，终于捣鼓出了一款爬虫系

。

靶场实验室

非常值得推荐的漏洞研究实验基地 Vulhub 。Vulhub 是一个基于 docker和 docker-compose 的漏环境集合，进入对应目录并执行一条语句即可启动一个全新的漏洞环境，让漏洞复现变得更加简单，安全从业者更加专注于漏洞原理本身。虽然易雾君是个低级网络玩家，但对安全还是有那么丝丝兴趣。