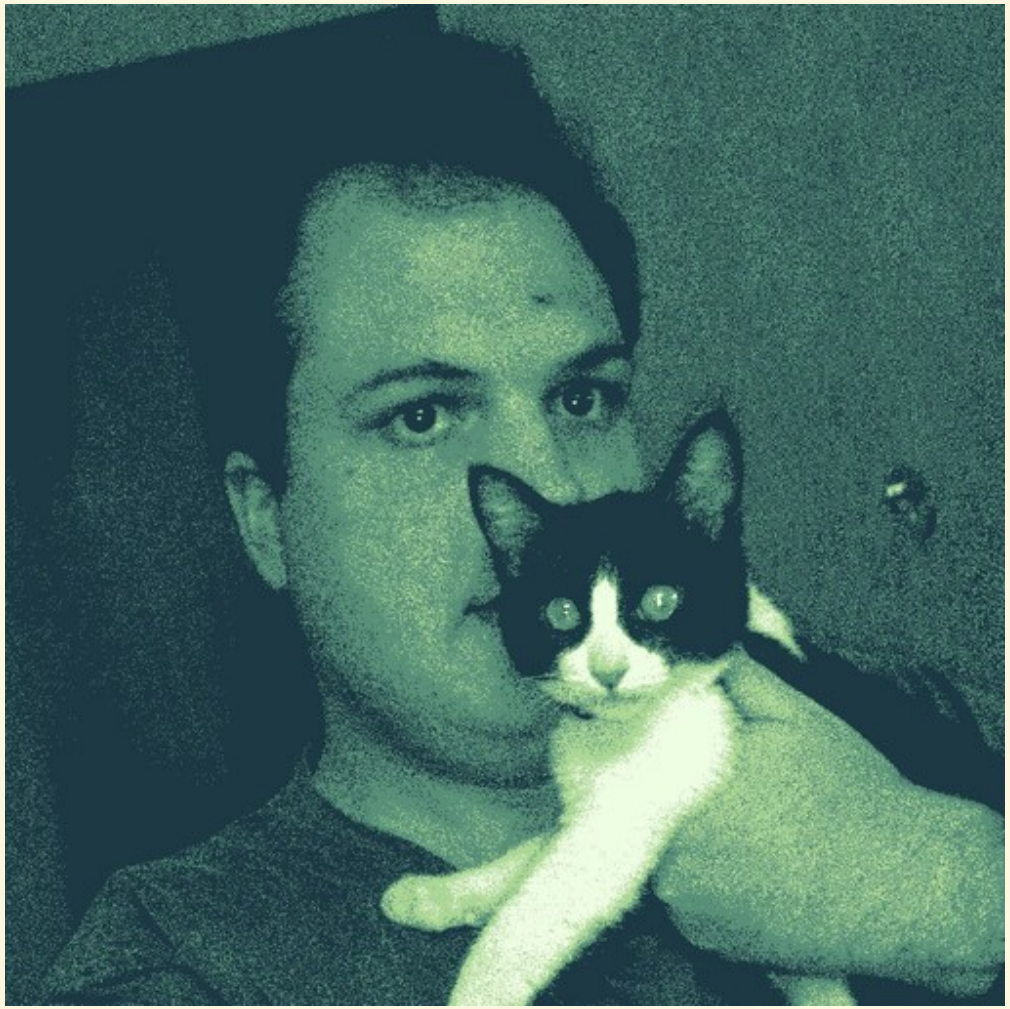
Como operar uma infra on premisses

Caio Volpato (caioau)

cryptorave.org

5 de maio de 2023



$ whoami

Matemático aplicado de formação

Atuo como Devops

Projetos: Casa Hacker
e medium.com/computando-arte

Hobbies: Sci-fi e Academia 💪

site: caioau.net

Texto original

Essa palestra foi originada de um texto do mesmo autor (Primeiros passos com self-hosting), publicado pelo grupo Computando arte.

Somos um grupo de divulgação cientifica no medium.

Escrevemos sobre Ciência da Computação, Matemática Aplicada, Estatística e Ciência de Dados em geral e em português.

- Link: medium.com/computando-arte
- Fundado em Nov/2020 🎂
- A informação quer ser livre: Licenciado sob CC BY-SA 4.0

Qual a proposta?

Por que?

Quais aplicações hospedar?

- Nextcloud: Hub completo de produtividade (como teams): tem arquivos, email, agenda/contatos, videoconferências etc ...
- syncthing: Sincronização contínua de arquivos.
- bitwarden: Gerenciador de senhas completo na nuvem.
- Plex ou Jellyfin: Um "netflix" pra chamar de seu.
- homeassistant: Automações residenciais sem precisar usar alexa/google assistente.
- Pi-Hole: Bloqueie propagandas na sua rede local.

awesome-selfhosted: Lista completa de apps self-hosted.

Onde vai ficar? Em casa? na nuvem ? ambos?

Ficar tudo em casa é mais simples e rápido.

Mas acessar os serviços fora de casa não é fácil e muito confiável.

Que tal os dois? Coloque o que precisa de velocidade (como backups) em casa e o serviços que requerem acesso remoto como nextcloud na nuvem.

E o hardware?

Para criar seu homelab precisamos de um hardware, pode ser:

- Um notebook antigo
- Uma raspberry-pi
- mini-pc
- NAS
- Talvez alguns discos, dependendo da sua necessidade.
- NoBreak é uma boa também

Falhas de storage

Toda forma de armazenamento está sujeita a falhar.

Principalmente os SD card da raspberry-pi, esses não tem uma vida útil longa. Com uso contínuo vai sobreviver por 1~2 anos.

Sempre faça backups!

Falhas de storage: Algumas estatísticas

Os discos tem uma tecnologia chamada S.M.A.R.T. (Self-Monitoring, Analysis, and Reporting Technology)
Que reporta parâmetros da saúde do disco.

Porém um estudo de 2007 do google mostrou que o SMART sozinho não é um bom indicador que o disco vai falhar.

Falhas de storage: Algumas estatísticas

A backblaze é uma empresa de soluções de storage publica a cada bimestre estatísticas de falhas dos discos, mostrando quais parâmetros SMART mais importam.

O scrutiny é uma tool que mostra os parâmetros SMART com os dados do backblaze.

Uma boa prática indicada antes de utilizar é fazer o teste de burnin que procura os badblocks e evita problemas com o drive: New Hard Drive rituals

Storage: RAID

RAID (Redundant Array of Independent Disks)

Combina discos físicos independentes em um único disco lógico, criando redundância e/ou expandindo espaço (dependendo o nível do RAID escolhido).

Dessa forma quando um disco falhar basta trocá-lo, sem perder dados ou ficar fora do ar.

RAID não é backup! Caso seja infectado com um ransomware o RAID não vai te proteger.

Storage: ZFS

O ZFS é um filesystem copy-on-write, com features interessantes:

- RAID e integridade dos dados
- Compressão e Deduplicação
- Criptografia
- Snapshots
- Quotas

Backups: Borgbackup

O Santo graal dos backups

- compressão e deduplicação
- backups completos (versionados)
- integridade dos dados (check) e monitorados (healthchecks.io)
- criptografado
- A prova de ransomware (modo append-only)

Blogpost: Como parei de me preocupar e passei a adorar minha solução de backups

Storage: Criptografia e acesso remoto

Quando criptografamos o disco precisamos inserir a senha sempre que reiniciamos.

Mas muitas vezes não temos um monitor e teclado e precisamos fazer de forma remota.

O pacote `dropbear-initramfs` (tutorial) resolve isso.

Ele cria um servidor SSH (antes do boot do kernel) permitindo desbloquear o disco remotamente.

Como acessar os serviços fora de casa?

Com muitas operadoras você não consegue acessar sua casa diretamente, pois você está no CGNAT (Carrier Grade NAT).

As alternativas são:

- Pedir pra sair do CGNAT.
- Usar um "proxy como ponte".
- Criar um onion service.

Saindo do CGNAT

Depois de sair do CGNAT, para acessar suas coisas, você precisa de:

- "pinar" um IP fixo para seu server no DHCP do seu roteador.
- Ter um DNS dinâmico: duckdns é gratuito e o Google Domains.
- Criar os port forward no roteador.
- (opcional) Configurar port knocking para ter segurança adicional.
- (opcional) Configurar o wireguard como VPN.

Usando um proxy

Se optar por usar um proxy como ponte você tem as seguintes alternativas:

- Usar o proxy reverso da cloudflare
- Usar serviços como ngrok.com ou pagekite
- Caso tenha uma VPS (virtual private server) sua você pode:
  - Fazer um tunnel SSH
  - Criar uma VPN com wireguard

Criando um Tor onion service

É a opção mais rápida e simples :)

Basta instalar o Tor: `sudo apt install tor`

E editar o arquivo de configuração `/etc/tor/torrc`

```
# /etc/tor/torrc
HiddenServiceDir /var/lib/tor/sshd/
HiddenServicePort 22 127.0.0.1:22
```

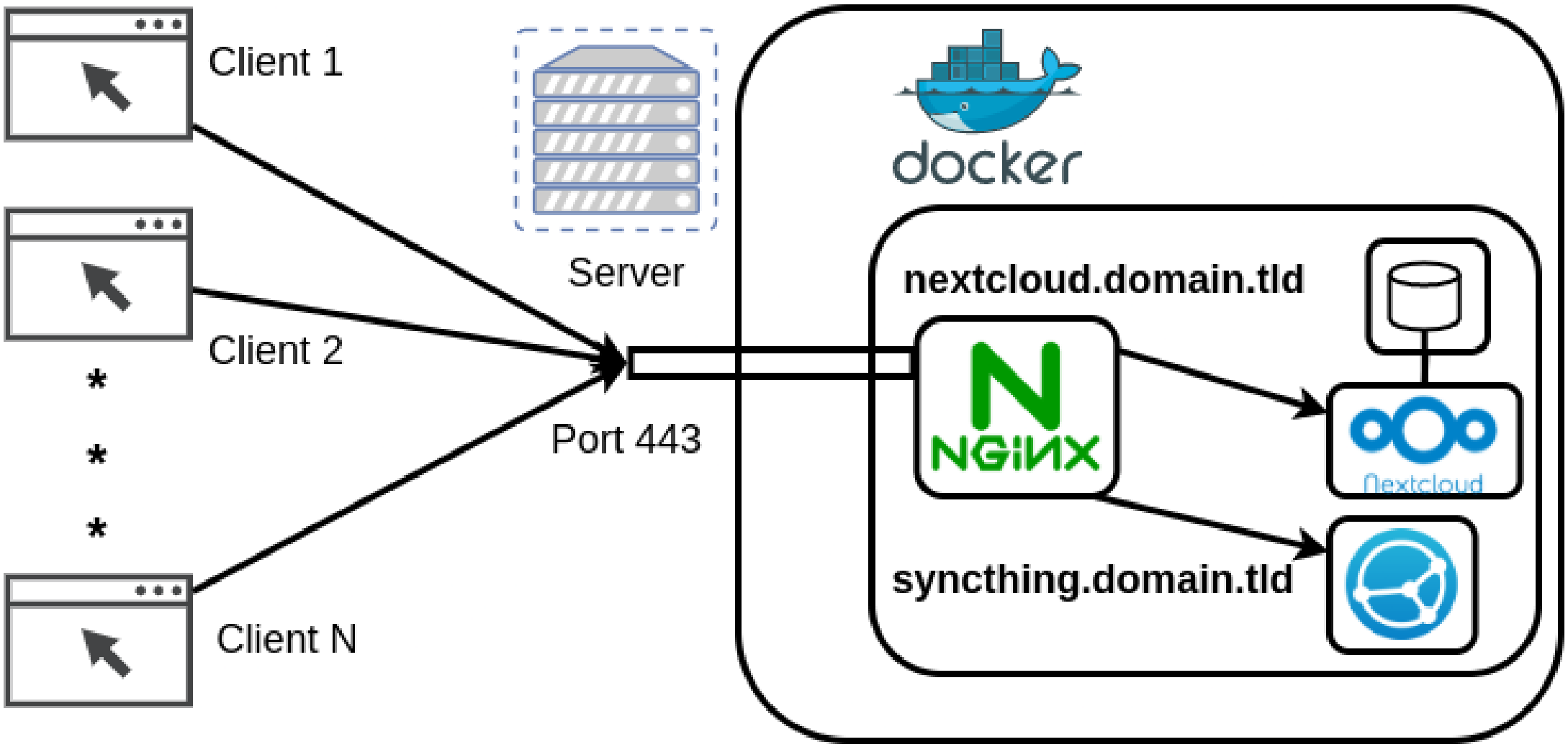
Veja a documentação: community.torproject.org/onion-services/

Proxy reverso

Outro elemento importante é configurar um proxy reverso como nginx ou traefik

O proxy reverso é a porta de entrada unica do mundo externo para suas aplicações.

Proxy reverso: diagrama



Proxy reverso: o nginx

O nginx é o proxy reverso mais tradicional.

A imagem docker que recomendo é a linuxserver/swag

Além de vir incluso o certbot para gerar os certificados https

Vem com fail2ban (que bloqueia bruteforce e outras regras)

E tem uma documentação excelente com diversos exemplos prontos.

Proxy reverso: O traefik

O traefik é um proxy mais recente e tem ganhado destaque.

O diferencial dele é pode ser integrado com Docker e kubernetes.
A configuração das "rotas" vive nos próprios contêineres ✨

```
# docker-compose.yml
  whoami:
    image: "containous/whoami"
    restart: unless-stopped
    labels:
      - "traefik.enable=true"
      - "traefik.http.routers.whoami2.rule=PathPrefix(`/whoami/`)"
      - "traefik.http.routers.whoami.rule=Host(`whoami.domain.tld`)"
      - "traefik.http.routers.whoami.entrypoints=web"
```

Security

É recomendado seguir algumas boas práticas:

- Use senhas fortes e únicas (use um gerenciador de senhas).
- Sempre aplique atualizações de segurança:
  - no host tem o UnattendedUpgrades
  - o diun permite te notificar quando tem novas imagens docker.
  - e o watchtower pra atualizar automaticamente.
- Use imagens docker confiáveis
- Cartilha da OWASP: Docker Security Cheat Sheet

Monitoramento

Já que cedo ou tarde alguma coisa vai falhar, tem como "ficar de olho" para evitar os problemas antes que as coisas piorem?

As soluções de monitoramento fazem isso: monitoram a CPU, memória, temperaturas e disco e te alertam em caso de algum ponto de atenção.

As soluções mais conhecidas é o zabbix e o prometheus.

Infra as code (IaC)

Quando precisar configurar um novo server, não precisa fazer tudo manualmente.

Ferramentas como ansible, chef e puppet automatizam o processo de configuração dos ambientes.

Além de ser mais rápido, torna a configuração (e manutenção) do seu ambiente reprodutível, padronizada e centralizada em um repo git.

Como começar os estudos?

Fonte:[Mateus Müller]

Referencias para aprender

- sadservers.com Desafios praticos de Linux
- GuiaFoca Linux: Apostilas completas sobre Linux e security (pt-br)
- LinuxTips, github.com/badtuxx Vídeos, lives e cursos (pt-br)
- selfhosted.show: Podcast sobre selfhosting
- Techno Tim e NetworkChuck canais sobre redes, Linux e DevOps
- Comunidades:
  - DevOps Campinas: Slack de profissionais de DevOps campineiros
  - /r/DataHoarder

Obrigado! Perguntas?