Infrastructure: A Bottom-Up Approach

what do I use and why

Nick Cao

September 24, 2022

why

I must admit that I was a bit gleeful when the effort I've put into not having to trust and rely on a hosted password manager finally paid off!

(You don't want to be on Cloudflare's naughty list)

approaches

cloud native

- container
- container orchestrator
- declarative

old school

- package manager
- init system
- imperative *or not?*

approaches

container/package manager

	container [1]	package manager
granularity	layer	package
metadata	tag and label	dependencies and more

composability

Contrary to common belief, container layers are not composable. You cannot compose `docker.io/golang` and `docker.io/rust` to get `docker.io/golang+rust`.

[1] as a software distribution format

approaches

container orchestrator/init system

	kubernetes	docker-compose	systemd
scope	cluster	node	node
state storage	etcd	transient	transient
dependency mgmt.	coarse	coarse	fine
complexity	high	low	medium

scalability

Distributed systems **SHOULD NOT** require a distributed orchestrator. Even with the presence of an orchestrator, system specific synchronization mechanisms are still **REQUIRED** to be implemented.

approaches

declarative/imperative

> *All declarative systems, are at their core, imperative ones.*

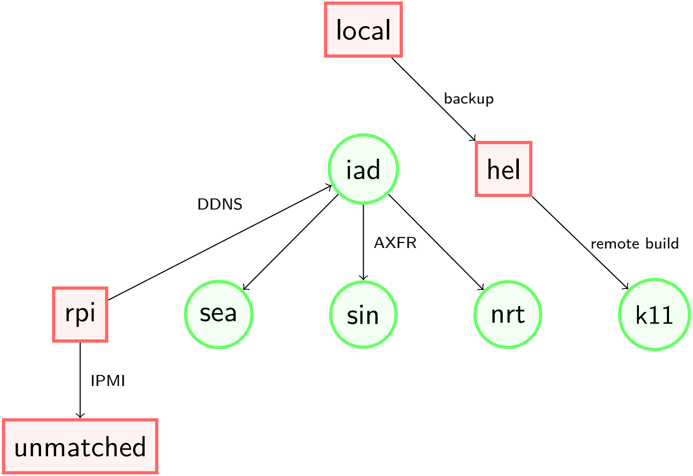
declarative

All approaches to system administration are inherently imperative. Just some disguise themselves as declarative by the process of reconciliation.

possible choices

- Ansible
- Salt
- NixOS

overview


local
backup
hel
iad
DDNS
AXFR
remote build
rpi
sea
sin
nrt
k11
IPMI
unmatched

server

Hetzner https://www.hetzner.com Vultr https://www.vultr.com

Hetzner

- bang for the buck
- solid IP reputation

Vultr

- more regions than AWS
- bring your own IP at no cost

Common

- official terraform provider

backup

Restic `https://restic.net`

> *Anything that can be regenerated does not qualify to be backed up.*

- reliable (despite being a 0.x release)
- secure (there is no way to create a plaintext backup)
- incremental
- verifiable

authoritative DNS

Knot DNS `https://www.knot-dns.cz`

Public resolvers do have heuristics for choosing an optimal nameserver.

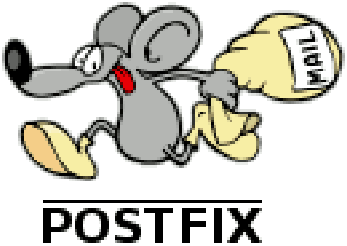
- the world's fastest authoritative DNS server, featuring multi-threaded and mostly lock-free operation, with optional XDP support
- automatic DNSSEC key management (including key rollovers) and signing
- support for modern DNS standards, including SVCB, DNS-over-QUIC and zone catalog

Mail Transfer Agent

Postfix `https://www.postfix.org`

All programmers are optimists – Frederick P. Brooks, Jr.

- known for being extremely flexible[2]
- a sane set of defaults that just works
- only 8 CVE compared to exim's 45 CVE[3]
- the second most popular MTA with over 25% market share

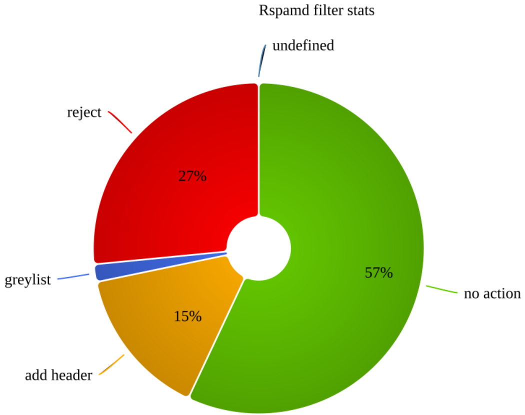


[2] in other words, with thousands of knobs

[3] six of them are scored over 9

Spam Filtering

Rspamd `https://rspamd.com`



Mail Delivery Agent

Dovecot https://www.dovecot.org

- one of the only [4] MDAs that correctly implements IMAP
- one of the fastest MDAs while still supporting the standard mbox and Maildir formats
- a wide range of authentication mechanisms including static password, PAM and OAuth2

OAuth2

sadly, thunderbird does not support generic OAuth2
bugzilla.mozilla.org/show_bug.cgi?id=1602166

[4] one out of three, actually

API Gateway

https://traefik.io/traefik

You do not want to configure all your services with their own ports and certificates, do you?

nginx

- relies on external programs for ACME
- having trouble supporting HTTP/2 or HTTP/3 properly
- a configuration format for humans, but not for machines

traefik

- structured dynamic configurations from multiple sources
- powerful routing and middlewares

Monitoring

Prometheus `https://prometheus.io`

All time spent on building a dashboard is time wasted.

prometheus

- the de facto standard for monitoring
- a text-based wire format for ease of implementation
- built-in support for alerting via multiple channels [5]

[5] via alertmanager, an official prometheus project