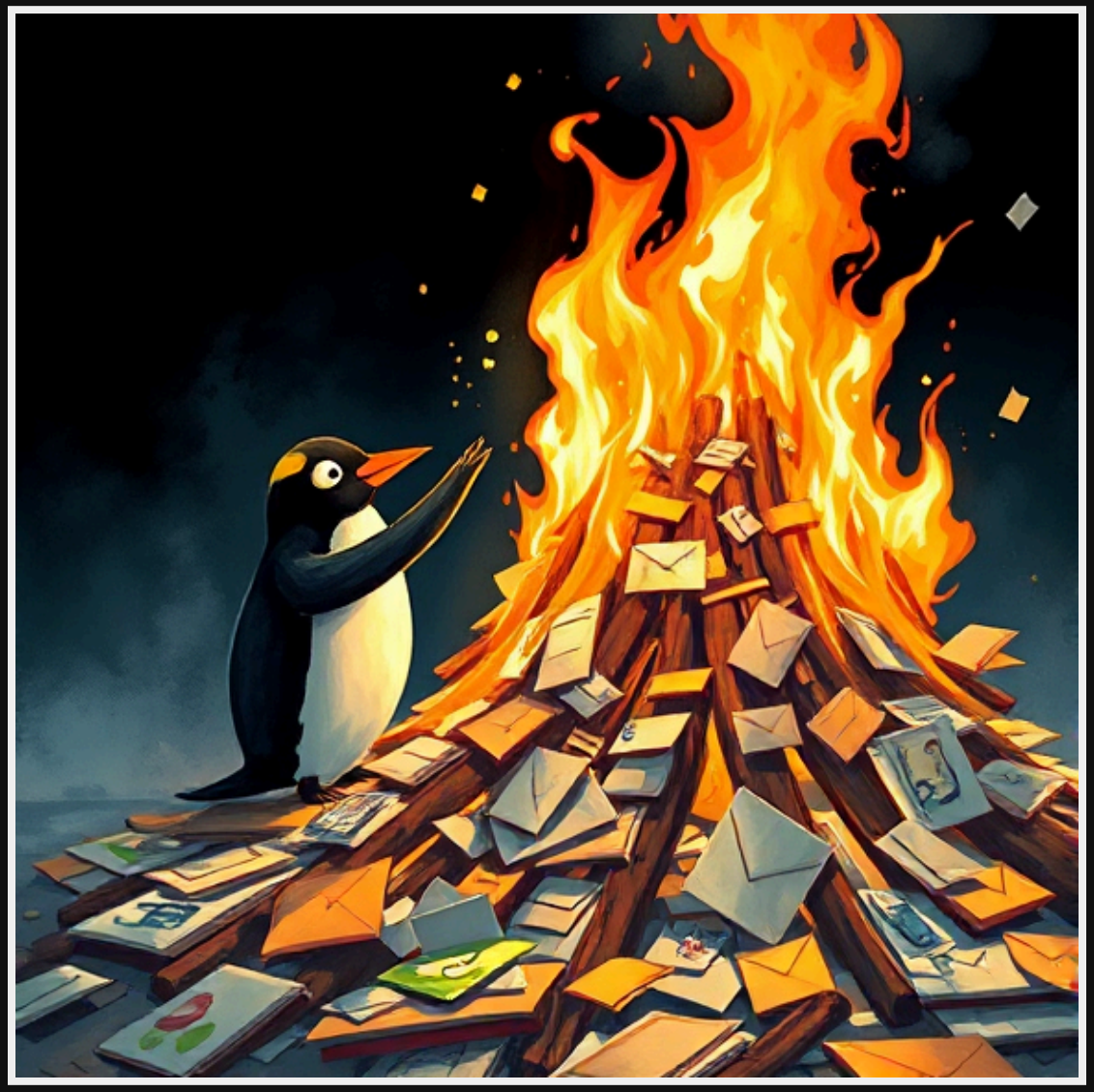
# Self-hosted Email

How I spent a handful of weekends swearing at my computer.

# Don’t do it.



# Questions?

danny@nerdcruft.net

# Seriously

```
(host mx-20.au-east.atmailcloud.com[3.106.43.229]
    refused to talk to me: 550-conn-502: IP [203.57.50.179]
    is listed on Cloudmark CSI - please refer to 550
    https://csi.cloudmark.com/reset-request/?ip=203.57.50.179)
        duncan_roe@optusnet.com.au
```

# Seriously

```
The 'From' header Danny Robson <danny@nerdcruft.net>
    does not match the DKIM domain nerdcruft.net.
    Be careful with this message as the sender may
    be spoofing the 'From' header identity.
```

# Seriously

Feel free to poke at the server if you need (in a friendly way), but: fail2ban is set to be pretty aggresssive...

# Goals

- IMAP and SMTP for maybe half a dozen people
- One VPS
- The bare minimum of hardware, software, and complexity

# Requirements

- Static IP
- 2GB RAM
- Domain name
- Significant free time

# Components

| | |
|---|---|
| postfix | send and receive email |
| dovecot | local auth, sieves, IMAP |
| rspam | filtering, DKIM |
| bind9 | DNS (optional) |

# Supporting players

| | |
|---|---|
| certbot+nginx | certficate creation and renewal, HTTP |
| ansible | automated depolyment |
| SSH, bash, etc | sysadmin tasks |

# References

- https://git.nerdcruft.net/nerdcruft/ansible-katamari
- https://workaround.org/ispmail-bookworm/
- danny@nerdcruft.net

# Trial runs

- Fits on a Pi
- Your home IP is **probably** stable enough
- Setup on a subdomain
  - eg `two.nerdcruft.net`

# DNS

```
D("nerdcruft.net", reg_namecheap,
    A('@', vps_addr)
    MX('@', 'nerdcruft.net.'),
    TXT('@', 'v=spf1 mx a ptr a:nerdcruft.net -all'),
)
```

# DNS:
# mail.example.com

Don’t. A and PTR must roundtrip.

# Certificates

```
apt install nginx certbot
```

# certs: NGINX

/etc/nginx/sites-enabled/default

```
server {
    listen 80 default_server;

    # This MUST be accessible without TLS
    location ~ ^/.well-known/acme-challenge/ {
        root /var/www/certbot;
    }

    location / {
        return 302 https://$host$request_uri;
    }
}
```

# certs: certbox

```
/usr/bin/certbot
    certonly
    --no-interactive --agree-tos --email danny@nerdcruft.net
    --webroot --webroot-path /var/www/certbot
    -d "$DOMAIN"
```

# certs: letsencrypt

```
root@nerdcruft:~# ls /etc/letsencrypt/live/nerdcruft.net/
cert.pem
chain.pem
fullchain.pem
privkey.pem
README
```

# Dovecot

Locally authenticates, stores user email, provides IMAP.

```
apt install
    dovecot-imapd
    dovecot-lmtpd
    dovecot-sieve
    dovecot-managesieved
```

# Dovecot: lmtp

Receive emails from Postfix

10-master.conf

```
service lmtp {
  unix_listener /var/spool/postfix/private/dovecot-lmtp {
    group = postfix
    user = postfix
    mode = 0600
  }
}
```

# Dovecot: auth

Expose auth to Postfix

10-master.conf

```
service auth {
  unix_listener /var/spool/postfix/private/auth {
    user = postfix
    group = postfix
    mode = 0660
  }
}
```

# Dovecot: certs

## 10-ssl.conf

```
ssl = required
ssl_cert = </etc/letsencrypt/live/nerdcruft.net/fullchain.pem
ssl_key = </etc/letsencrypt/live/nerdcruft.net/privkey.pem
```

# rspamd

```
apt install rspamd redis
```

# rspamd: vs spamassassin

- Less configuration(?)
- Includes DKIM signing
- Less open

# rspamd: headers

## milter_headers.conf

```
extended_spam_headers = true;
skip_local = false;
skip_authenticated = false;
```

# rspamd: headers

```
X-Rspamd-Server: nerdcruft.net
X-Rspamd-Queue-Id: D00A225BB2A
X-Rspamd-Action: no action
X-Spamd-Result: default: False [-1.21 / 150.00];
        BAYES_HAM(-3.00)[100.00%];
        TO_EXCESS_QP(1.20)[];
        SUBJ_EXCESS_QP(1.20)[];
        DMARC_POLICY_ALLOW(-0.50)[igea.net,none];
        FORGED_SENDER(0.30)[GCAP@igea.net,bounce-mc.us12_51253277
        R_DKIM_ALLOW(-0.20)[igea.net:s=k3];
        R_SPF_ALLOW(-0.20)[+ip4:198.2.182.38];
        MANY_INVISIBLE_PARTS(0.10)[2];
        MIME_GOOD(-0.10)[multipart/alternative,text/plain];
        RWL_MAILSPIKE_GOOD(-0.10)[198.2.182.38:from];
        ZERO_FONT(0.10)[1];
```

# DKIM

Lets cryptographically sign emails.

I’m sure that will solve things.

# DKIM

Cryptographic keys

SMTP signs outgoing email.

`DNS: ${selector}._domainkey.${domain}`

# DKIM: dig

```
dig TXT 2025._domainkey.nerdcruft.net
```

```
; <<>> DiG 9.18.31 <<>> TXT 2025._domainkey.nerdcruft.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7700
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;2025._domainkey.nerdcruft.net. IN      TXT

;; ANSWER SECTION:
2025._domainkey.nerdcruft.net. 600 IN   TXT     "v=DKIM1; k=rsa;

;; Query time: 45 msec
;; SERVER: 192.168.1.1#53(192.168.1.1) (UDP)
```

# DKIM: generating

```
# Private+Public
openssl genrsa -out "$key_path" 2048
# Public
openssl rsa -in "$key_path" -pubout -outform der 2>/dev/null | op
```

```
create_dkim.sh
```

# DKIM: overkill

```
apt install bind9
```

# DKIM: NS

```
D("nerdcruft.net", reg_namecheap,
    A('ns', vps_addr),
    NS('_domainkey', 'ns.nerdcruft.net.'),
)
```

# DKIM: zones

/etc/bind/zones/_domainkey/nerdcruft.net.2025.txt

```
2025 IN TXT ( "v=DKIM1; k=rsa; "
    p="MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAudD9BGEL0vFKak
    "lO8+G4oxSe2+khVq7eVVYIZWGvnU60lf2YOcNbo3N9M7FsL3xwBGIRLDEir1
);
```

# DKIM: rspamd files

/etc/rspamd/dkim_selectors.map

```
nerdcruft.net 2025
```

Private key:

`/var/lib/rspamd/dkim/nerdcruft.net.2025.ke`

# DKIM: rspamd

## dkim_signing.conf

```
path = "/var/lib/rspamd/dkim/$domain.$selector.key";
selector_map = "/etc/rspamd/dkim_selectors.map";
sign_local = true;
sign_authenticated = true;
use_esld = false;
allow_username_mismatch = true;
```

# DKIM: headers

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=nerdcruft
    to:to:cc:mime-version:mime-version:content-type:content-type
        content-transfer-encoding:content-transfer-encoding; bh=
```

# Postfix

Delivers and receives emails between servers

```
apt install postfix
```

# Postfix: domains

main.cf

```
myhostname = nerdcruft.net
mydestination = $myhostname, localhost.localdomain, localhost
```

# Postfix: TLS

## main.cf

```
smtpd_tls_cert_file=/etc/letsencrypt/live/nerdcruft.net/fullchain
smtpd_tls_key_file=/etc/letsencrypt/live/nerdcruft.net/privkey.pe
smtpd_tls_security_level=may
```

# Postfix: auth

main.cf

```
smtpd_sasl_type=dovecot
smtpd_sasl_path=private/auth
smtpd_sasl_auth_enable=yes
# no-unencrypted auth
smtpd_tls_auth_only=yes
```

# Postfix: rspamd

## main.cf

```
smtpd_milters=inet:localhost:11332
non_smtpd_milters=inet:localhost:11332
milter_mail_macros=i {mail_addr} {client_addr} {client_name} {aut
```

# Postfix: dovecot

main.cf

```
mailbox_transport = lmtp:unix:private/dovecot-lmtp
```

# Testing: swaks

```
swaks
    --to person@exxample.com
    --from other@example.com
    --server example.com
    --port 587
    --tls
    --auth-user other@example.com
    --auth-password 'redacted
```

# Testing: misc

- `journalctl -f`
- `postqueue -p`
- Send to GMail, sources include DKIM
- https://dkimvalidator.com/

# Questions

- https://git.nerdcruft.net/nerdcruft/ansible-katamari
- https://workaround.org/ispmail-bookworm/
- mailto:danny@nerdcruft.net