

Let's Encrypt Guides

- [Setup an ACME DNS with Knot](#)

Setup an ACME DNS with Knot

Installation

[documentation](#)

```
export KNOT_ZONED="/etc/knot/zone.d/"
```

```
sudo apt-get -y install knot
sudo mkdir -p "$KNOT_ZONED"
sudo chmod 0750 "$KNOT_ZONED"
sudo chown root:knot "$KNOT_ZONED"
```

```
cat << EOF | sudo tee /var/lib/knot/acmeauth.havlas.me.zone > /dev/null
acmeauth.havlas.me. 300 SOA hugin.havlas.me. hugin.havlas.me. 1 10000 2400
604800 300
acmeauth.havlas.me. 300 NS hugin.havlas.me.
acmeauth.havlas.me. 300 A 185.8.166.47
acmeauth.havlas.me. 300 AAAA 2a03:3b40:101:da::1
EOF
```

```
include: /etc/knot/zone.d/*.conf
```

```
zone:
- domain: acmeauth.havlas.me
```

Setup on Authoritative DNS

```
hugin.havlas.me. 900 IN A 185.8.166.47
hugin.havlas.me. 900 IN AAAA 2a03:3b40:101:da::1
acmeauth.havlas.me. 300 IN NS hugin.havlas.me.
```

Setup Certificate Authentication

```
uuid -v4 | tr -d '-'
```

```
_acme-challenge.staging.havlas.me. 60 IN CNAME  
944d7c102df14a678063452e7ac356fa.acmeauth.havlas.me.
```

```
keymgr tsig generate -t staging.havlas.me hmac-sha512 | sudo tee  
/etc/knot/zone.d/staging.havlas.me.conf  
sudo chmod 0640 /etc/knot/zone.d/staging.havlas.me.conf  
sudo chown root:knot /etc/knot/zone.d/staging.havlas.me.conf
```

```
acl:  
- id: acmeauthacl.staging.havlas.me  
  action: update  
  update-type: [TXT]  
  update-owner: name  
  update-owner-match: equal  
  update-owner-name: [944d7c102df14a678063452e7ac356fa]  
  key: staging.havlas.me  
  
zone:  
- domain: 944d7c102df14a678063452e7ac356fa.acmeauth.havlas.me  
  acl: [ acmeauthacl.staging.havlas.me ]
```

```
sudo tee /var/lib/knot/944d7c102df14a678063452e7ac356fa.acmeauth.havlas.me.zone  
> /dev/null <<EOF  
944d7c102df14a678063452e7ac356fa.acmeauth.havlas.me. 300 SOA  
hugin.havlas.me. hugin.havlas.me. 1 10000 2400 604800 300  
944d7c102df14a678063452e7ac356fa.acmeauth.havlas.me. 300 NS  
hugin.havlas.me.  
EOF  
chown knot:root  
/var/lib/knot/944d7c102df14a678063452e7ac356fa.acmeauth.havlas.me.zone
```

Request a Certificate

```
key "staging.havlas.me" {  
  algorithm hmac-sha512;  
  secret "[REDACTED]";  
};
```

```
#!/bin/bash
```

```
ACMEAUTH_SUBJECT="944d7c102df14a678063452e7ac356fa.acmeauth.havlas.me"
```

```
echo "  
server hugin.havlas.me  
update delete $ACMEAUTH_SUBJECT TXT  
update add $ACMEAUTH_SUBJECT 60 TXT $CERTBOT_VALIDATION  
send  
" | nsupdate -k "/etc/letsencrypt/manual/staging.havlas.me.key"
```

```
#!/bin/bash
```

```
ACMEAUTH_SUBJECT="944d7c102df14a678063452e7ac356fa.acmeauth.havlas.me"
```

```
echo "  
server hugin.havlas.me  
update delete $ACMEAUTH_SUBJECT TXT  
send  
" | nsupdate -k "/etc/letsencrypt/manual/staging.havlas.me.key"
```

```
certbot certonly \  
  --manual -n -m tomas@havlas.me --agree-tos \  
  --expand --preferred-challenges=dns \  
  --manual-auth-hook=/etc/letsencrypt/manual/staging.havlas.me.sh \  
  --manual-cleanup-hook=/etc/letsencrypt/manual/staging.havlas.me-cleanup.sh \  
  -d "*.staging.havlas.me" -d "staging.havlas.me"
```