ACME Service Discovery

draft-tweedale-acme-discovery

Fraser Tweedale
ftweedal@redhat.com

November 19, 2020

Why service discovery?

- There are now multiple public (and private) ACME services
- Different servers will support different identifier types and validation methods
- Clients need to know: *what server(s) can I use?*
- Explicit client configuration can be challenging
- Goal: automatic selection of "best" server in the environment, without explicit configuration

Service discovery protocols

- Central registry vs distributed/P2P (e.g. DNS-SD/mDNS)
- In enterprise environments, DNS SRV records [RFC2782] are used for LDAP, Kerberos and mail servers [RFC6186]
- DNS-SD [RFC6763] = SRV + supplementary data (TXT) + listing (PTR)

Assumptions

- ACME client has network configuration (e.g. via DHCP)...
  - including a domain name (or something similar)
- Organisation can manage its DNS records
- Successful retrieval of directory object $\rightarrow$ server is available

ACME Service Discovery (1)

- Based on DNS-SD
- Client determines "parent domain(s)"
  - DNS search domain(s), Kerberos realm(s), etc
  - or explicit configuration

ACME Service Discovery (2)

- Client constructs name `_acme-server._tcp.$PARENT`
- *Service Instance Names* listed in the PTR records:

```
$ORIGIN corp.example.

_acme-server._tcp PTR CorpCA._acme-server._tcp
_acme-server._tcp PTR C4A._acme-server._tcp
```

ACME Service Discovery (3)

- Each *Service Instance Name* owns SRV and TXT records that describe the service:

```
$ORIGIN corp.example.

CorpCA._acme-server._tcp SRV 10 0 443 ca
CorpCA._acme-server._tcp TXT "path=/acme" "i=email,dns"

C4A._acme-server._tcp    SRV 20 0 443 certs4all.example.
C4A._acme-server._tcp    TXT "path=/acme/v2" "i=dns"
```

ACME Service Discovery (4)

- Client chooses "best" server, e.g.:

```
CorpCA._acme-server._tcp SRV 10 0 443 ca
CorpCA._acme-server._tcp TXT "path=/acme" "i=email,dns"
```

- Construct URL <https://ca.corp.example/acme>; GET directory
- Any problem, try the next server / parent domain

Working code

- Certbot plugin: https://github.com/frasertweedale/certbot/tree/feature/discovery
- Blog post: https://frasertweedale.github.io/blog-redhat/posts/2020-11-13-acme-service-discovery.html

Needs discussion

- Scope of SRV priority and weight
- Exclude names in `.local`?
- DNS security: mention DoT and DoH?
- Parent domain selection; better / more secure examples

Next steps

- Give feedback
  - Issues / PRs to https://github.com/frasertweedale/i-d
- WG adoption?

Other work

- Express server capabilities in directory "meta" fields
  - draft-tweedale-acme-server-capabilities-00
- Is anyone interested in SRVName support?