Failover for type=FWD entries in the RouterOS DNS proxy

The Mikrotik DNS resolver supports static entries with type=FWD (forward). Combining this with the regex (and now the match-subdomain option since v7.6) allows you to forward queries for specific domains to a server. Unfortunately, *the type=FWD resolver does not support any sort of failover*.

No native failover for type=FWD

The first example below shows two FWD entries for the myad.loc domain. Each entry is configured to forward-to a different DNS server, as you would expect in a normal Active-Directory environment.

```
# RouterOS 7.6 and newer example
# the second FWD entry will never actually be used
/ip dns static
add name=myad.loc ttl=1m type=FWD forward-to=10.0.0.11 match-subdomain=yes
add name=myad.loc ttl=1m type=FWD forward-to=10.0.0.12 match-subdomain=yes



# older RouterOS example
# the second and fourth FWD entries will never actually be used
/ip dns static
add regexp="myad\\.loc" ttl=1m type=FWD forward-to=10.0.0.11
add regexp="myad\\.loc" ttl=1m type=FWD forward-to=10.0.0.12
add regexp=".*\\.myad\\.loc" ttl=1m type=FWD forward-to=10.0.0.11
add regexp=".*\\.myad\\.loc" ttl=1m type=FWD forward-to=10.0.0.12
```

Because there is no failover mechanism for type=FWD entries, the second entry will never actually get used, even if the forward-to target of the first entry is offline.

There is a workaround - sort of

Since the forward-to target can be a hostname, a workaround that has been discussed on the forums is to create multiple type=A records for a fake hostname, one for each DNS server you wish to forward to, and then set the forward-to target of the type=FWD record to this overloaded fake hostname.

Here's a configuration using our myad.loc example domain:

```
# RouterOS 7.6 and newer example
/ip dns static
add name=myad.loc.rslv ttl=1m address=10.0.0.11
add name=myad.loc.rslv ttl=1m address=10.0.0.12
add name=myad.loc ttl=1m type=FWD forward-to=myad.loc.rslv match-subdomain=yes



# older RouterOS example
/ip dns static
add name=myad.loc.rslv ttl=1m address=10.0.0.11
add name=myad.loc.rslv ttl=1m address=10.0.0.12
add regexp="myad\\.loc" ttl=1m type=FWD forward-to=myad.loc.rslv
add regexp=".*\\.myad\\.loc" ttl=1m type=FWD forward-to=myad.loc.rslv
```

There is no real failover using this method, but rather "dumb round robin". If one of your servers is offline, queries will still be sent to it. Verified using Wireshark, the RouterOS DNS proxy will make five FWD attempts to one DNS server, and then pass a failure back to the client.....

... more details to come ...

:end

Revision #3
Created 2023-03-01 19:30:08 UTC by bluecrow76
Updated 2023-06-02 05:20:54 UTC by bluecrow76