NAME

dnssec-trust-anchors.d, systemd.positive, systemd.negative − DNSSEC trust anchor configuration files

SYNOPSIS

/etc/dnssec−trust−anchors.d/*.positive

/run/dnssec−trust−anchors.d/*.positive

/usr/lib/dnssec−trust−anchors.d/*.positive

/etc/dnssec−trust−anchors.d/*.negative

/run/dnssec−trust−anchors.d/*.negative

/usr/lib/dnssec−trust−anchors.d/*.negative

DESCRIPTION

The DNSSEC trust anchor configuration files define positive and negative trust anchors **systemd-resolved.service**(8) bases DNSSEC integrity proofs on.

POSITIVE TRUST ANCHORS

Positive trust anchor configuration files contain **DNSKEY** and **DS** resource record definitions to use as base for DNSSEC integrity proofs. See **RFC 4035, Section 4.4**[1] for more information about DNSSEC trust anchors.

Positive trust anchors are read from files with the suffix .positive located in /etc/dnssec−trust−anchors.d/, /run/dnssec−trust−anchors.d/ and /usr/lib/dnssec−trust−anchors.d/. These directories are searched in the specified order, and a trust anchor file of the same name in an earlier path overrides a trust anchor files in a later path. To disable a trust anchor file shipped in /usr/lib/dnssec−trust−anchors.d/ it is sufficient to provide an identically−named file in /etc/dnssec−trust−anchors.d/ or /run/dnssec−trust−anchors.d/ that is either empty or a symlink to /dev/null ("masked").

Positive trust anchor files are simple text files resembling DNS zone files, as documented in **RFC 1035, Section 5**[2]. One **DS** or **DNSKEY** resource record may be listed per line. Empty lines and lines starting with "#" or ";" are ignored, which may be used for commenting. A <consant>DS</consant> resource record is specified like in the following example:

```
. IN DS 19036 8 2 49aac11d7b6f6446702e54a1607371607a1a41855200fd2ce1cdde32f24e8fb5
```

The first word specifies the domain, use "." for the root domain. The domain may be specified with or without trailing dot, which is considered equivalent. The second word must be "IN" the third word "DS". The following words specify the key tag, signature algorithm, digest algorithm, followed by the hex−encoded key fingerprint. See **RFC 4034, Section 5**[3] for details about the precise syntax and meaning of these fields.

Alternatively, **DNSKEY** resource records may be used to define trust anchors, like in the following example:

```
. IN DNSKEY 257 3 8 AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcCjFFVQUTf6v58fLjwI
```

The first word specifies the domain again, the second word must be "IN", followed by "DNSKEY". The subsequent words encode the **DNSKEY** flags, protocol and algorithm fields, followed by the key data encoded in Base64. See **RFC 4034, Section 2**[4] for details about the precise syntax and meaning of these fields.

If multiple **DS** or **DNSKEY** records are defined for the same domain (possibly even in different trust anchor files), all keys are used and are considered equivalent as base for DNSSEC proofs.

Note that systemd−resolved will automatically use a built−in trust anchor key for the Internet root domain if no positive trust anchors are defined for the root domain. In most cases it is hence unnecessary to define an explicit key with trust anchor files. The built−in key is disabled as soon as at least one trust anchor key for the root domain is defined in trust anchor files.

It is generally recommended to encode trust anchors in **DS** resource records, rather than **DNSKEY** resource

records.

If a trust anchor specified via a **DS** record is found revoked it is automatically removed from the trust anchor database for the runtime. See **RFC 5011**[5] for details about revoked trust anchors. Note that systemd−resolved will not update its trust anchor database from DNS servers automatically. Instead, it is recommended to update the resolver software or update the new trust anchor via adding in new trust anchor files.

The current DNSSEC trust anchor for the Internet's root domain is available at the **IANA Trust Anchor and Keys**[6] page.

NEGATIVE TRUST ANCHORS

Negative trust anchors define domains where DNSSEC validation shall be turned off. Negative trust anchor files are found at the same location as positive trust anchor files, and follow the same overriding rules. They are text files with the .negative suffix. Empty lines and lines whose first character is ";" are ignored. Each line specifies one domain name which is the root of a DNS subtree where validation shall be disabled. For example:

```
# Reverse IPv4 mappings
10.in−addr.arpa
16.172.in−addr.arpa
168.192.in−addr.arpa
...
# Some custom domains
prod
stag
```

Negative trust anchors are useful to support private DNS subtrees that are not referenced from the Internet DNS hierarchy, and not signed.

RFC 7646[7] for details on negative trust anchors.

If no negative trust anchor files are configured a built−in set of well−known private DNS zone domains is used as negative trust anchors.

It is also possibly to define per−interface negative trust anchors using the *DNSSECNegativeTrustAnchors=* setting in **systemd.network**(5) files.

SEE ALSO

systemd(1), **systemd-resolved.service**(8), **resolved.conf**(5), **systemd.network**(5)

NOTES

1. RFC 4035, Section 4.4
   https://tools.ietf.org/html/rfc4035#section-4.4
2. RFC 1035, Section 5
   https://tools.ietf.org/html/rfc1035#section-5
3. RFC 4034, Section 5
   https://tools.ietf.org/html/rfc4034#section-5
4. RFC 4034, Section 2
   https://tools.ietf.org/html/rfc4034#section-2
5. RFC 5011
   https://tools.ietf.org/html/rfc5011
6. IANA Trust Anchor and Keys
   https://data.iana.org/root-anchors/root-anchors.xml
7. RFC 7646
   https://tools.ietf.org/html/rfc7646