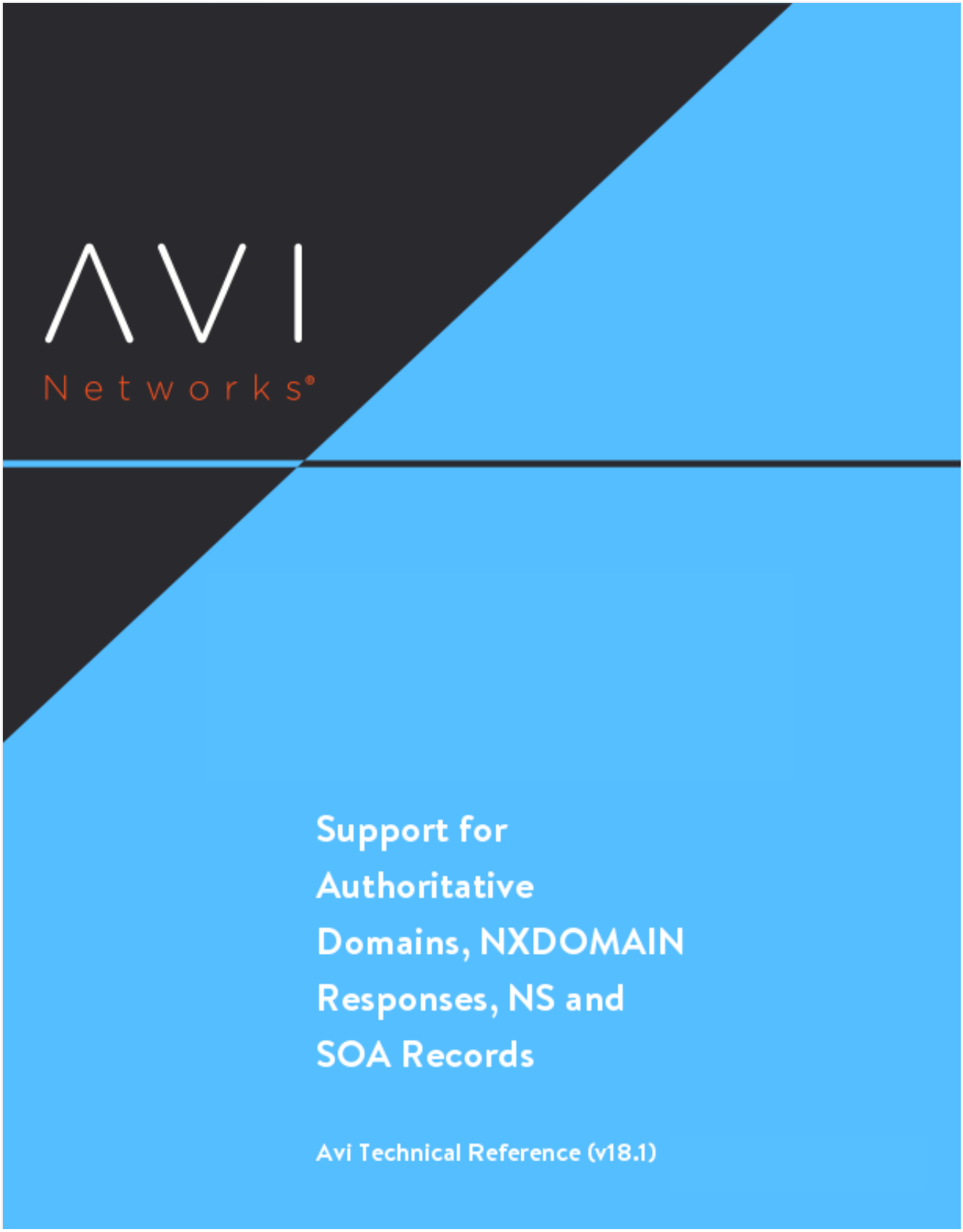

Support for Authoritative Domains, NXDOMAIN Responses, NS and SOA Records

Avi Technical Reference (v18.1)

Support for Authoritative Domains, NXDOMAIN Responses, NS and SOA Records

view online

If back-end DNS servers are configured for an Avi DNS virtual service, the VS will not pass them client queries containing FQDNs that are subdomains of the domains for which the DNS VS is authoritative.

An Avi Vantage DNS virtual service includes a Start of Authority (SOA) record with its NXDOMAIN (and other) replies.

> *NOTE: Responses to SOA queries are not supported.*

Related Reading

- Name Server Records in Avi DNS

Features

An `NXDOMAIN` ("the domain does Not eXist") response is accompanied by an `SOA` record if the incoming query's domain is a subdomain of one of the configured authoritative domains in the DNS application profile.

Negative caching, i.e., the caching of the fact of non-existence of a record, is determined by name servers authoritative for a zone which must include the Start of Authority (SOA) record when reporting no data of the requested type exists. The value of the minimum field of the SOA record and the TTL of the SOA itself is used to establish the TTL for the negative answer.

If the query's FQDN matches an entry in the DNS table but the query type is not supported, by default the Avi SE generates a `NOERROR` response, optionally with an `SOA` record if the domain matches a configured authoritative domain.

Configuration Using the Avi UI

Refer to figure 1.

Queries for FQDNs that are subdomains of the authoritative domain names and do not have any DNS record in Avi are dropped or the NXDOMAIN response is sent. The Avi System-DNS profile comes preconfigured to respond to unhandled DNS requests. However, when creating a DNS profile afresh, the default value of the (Options for) Invalid DNS Query processing field is set to *drop* unhandled requests. Change it to *respond* to ensure `NXDOMAIN` responses get sent when appropriate.

When an `NXDOMAIN` reply is appropriate for an FQDN that ends with one of the authoritative domains, the value appearing in the Negative TTL field will be incorporated into the attached SOA record. Note the 30-second default; the allowed range is 1 to 86400 seconds.

An Avi DNS VS need not have a back-end DNS server pool. If it does have a back-end pool, the Avi DNS' Service Engines will only load balance to it if the FQDN is *not* a subdomain of one of those configured in the Authoritative Domain Names field. All are configured with Ends-With semantics.

Values in the Valid subdomains field are for validity checking and thus optional. If not configured, all subdomains of `acme.com` will be processed and looked up in the DNS table.

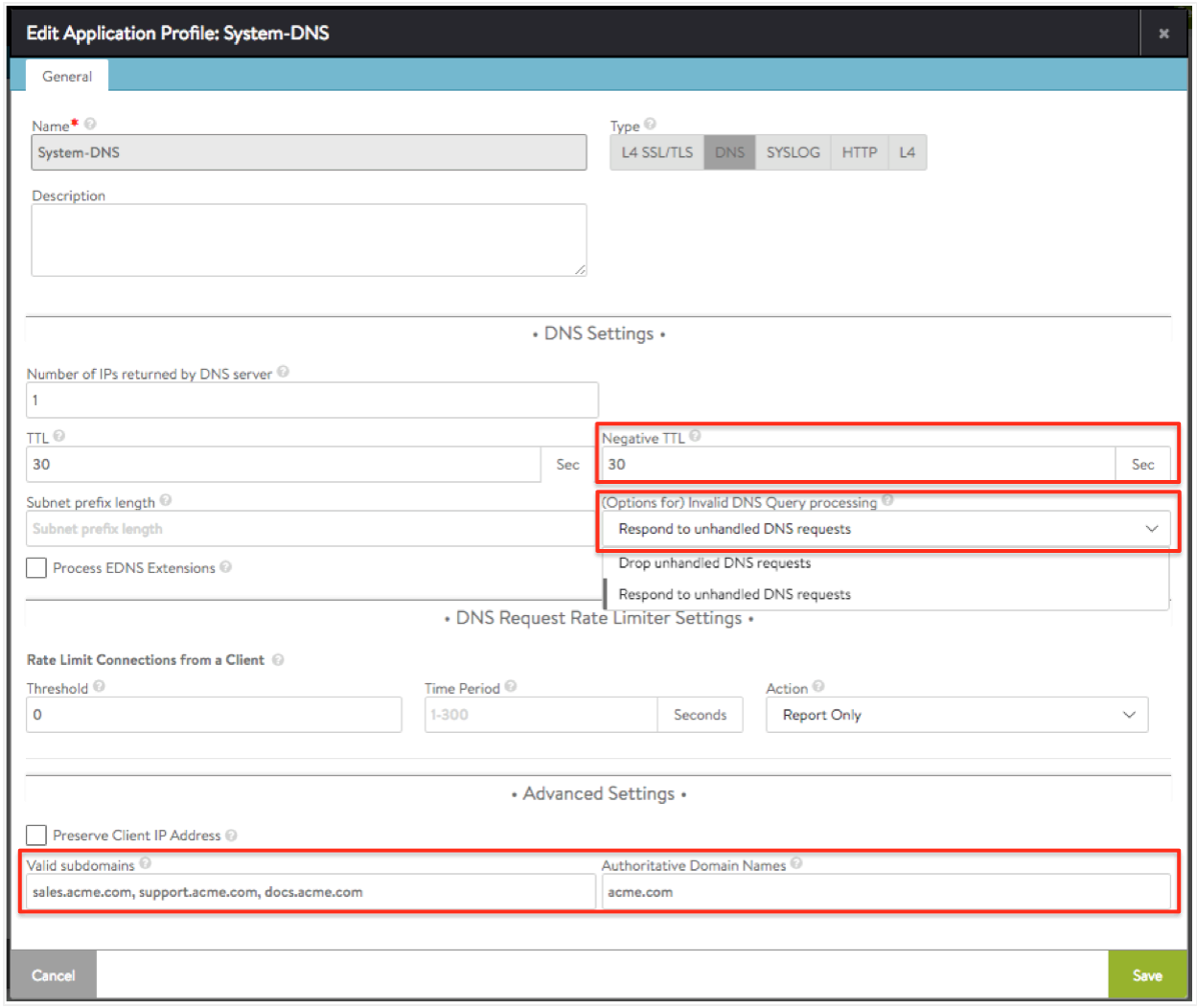

Figure 1. Setting DNS options with the Avi Vantage application profile editor

Configuration Using the Avi CLI

In the below example, we see the before and after configurations of the System-DNS application profile. Various `applicationprofile:dns_service_profile` subcommands are used to:

- Define the authoritative domain names. In this example, they are `acme.com` and `coyote.com`.
- Enable NXDOMAIN responses. To do this, the value of `error_response` is changed from `DNS_ERROR_RESPONSE_NONE` (the default) to `DNS_ERROR_RESPONSE_ERROR`. The `negative_caching_ttl` is left unchanged from its 30-second default.
- Specify subdomains of `acme.com` for which the DNS can provide an IP address. The subdomains are `sales.acme.com`, `docs.acme.com`, and `support.acme.com`. These subdomains are for validity checking and thus optional. If not configured, all subdomains of `acme.com` and `coyote.com` will be processed and looked up in the DNS table.

{% cli %} [admin:10-10-25-20]: > configure applicationprofile System-DNS Updating an existing object. Currently, the object is: +------------------------+---+ | Field | Value | +------------------------ +---+ | uuid | applicationprofile-fdb6a5d6-bbf8-4f15-b851-f436b599992c | | name | System-DNS | | type | APPLICATION_PROFILE_TYPE_DNS | | dns_service_profile | | | num_dns_ip | 1 | | ttl | 30 sec | |

error_response | DNS_ERROR_RESPONSE_NONE | | edns | False | | dns_over_tcp_enabled | True | | aaaa_empty_response | True | | negative_caching_ttl | 30 sec | | ecs_stripping_enabled | True | | preserve_client_ip | False | | tenant_ref | admin | +------------------------+--+ [admin:10-10-25-20]: applicationprofile> dns_service_profile [admin:10-10-25-20]: applicationprofile:dns_service_profile> authoritative_domain_names acme.com [admin:10-10-25-20]: applicationprofile:dns_service_profile> authoritative_domain_names coyote.com [admin:10-10-25-20]: applicationprofile:dns_service_profile> error_response dns_error_response_error Overwriting the previously entered value for error_response [admin:10-10-25-20]: applicationprofile:dns_service_profile> domain_names sales.acme.com [admin:10-10-25-20]: applicationprofile:dns_service_profile> domain_names docs.acme.com [admin:10-10-25-20]: applicationprofile: dns_service_profile> domain_names support.acme.com [admin:10-10-25-20]: applicationprofile:dns_service_profile> save [admin:10-10-25-20]: applicationprofile> save +--------------------------------- +--+ | Field | Value | +--------------------------------- +--+ | uuid | applicationprofile-fdb6a5d6-bbf8-4f15-b851-f436b599992c | | name | System-DNS | | type | APPLICATION_PROFILE_TYPE_DNS | | dns_service_profile | | | num_dns_ip | 1 | | ttl | 30 sec | | error_response | DNS_ERROR_RESPONSE_ERROR | | domain_names[1] | sales.acme.com | | domain_names[2] | docs.acme. com | | domain_names[3] | support.acme.com | | edns | False | | dns_over_tcp_enabled | True | | aaaa_empty_response | True | | authoritative_domain_names[1] | acme.com | | authoritative_domain_names[2] | coyote.com | | negative_caching_ttl | 30 sec | | ecs_stripping_enabled | True | | preserve_client_ip | False | | tenant_ref | admin | +--------------------------------- +--+ [admin:10-10-25-20]: >{% endcli %}