DNS Support

In this section:

Related articles:

- DNS Group - CLI
- SIP Trunk Group - Signaling - CLI
- Dns Group - Server (EMA)
- Sip Trunk Group - Signaling - TCP Fallback
- Zone - IP Peer - CLI
- Ip Peer - Path Check
- Domain Name Server (DNS) Alarms

The SBC Core supports domain name resolution through external DNS servers. Each IP address context defines one or more DNS server groups. Each DNS server group contains upto eight DNS servers. The zone and/or SIP Trunk Group indicates the DNS Server Group to use for the requests, which require a DNS resolution.

Within a DNS server group, each server has both a priority and a weight. Requests are sent to the server with highest priority (lower value) first. Servers of a lower priority are only used when all servers of a higher priority are marked unavailable based on previous timeouts. If multiple servers of the same priority exist, requests are load-balanced across servers in proportion to their weights.

The SBC supports the following functionality:

- Using DNS for either A record queries or full NAPTR+SRV+A record queries, and is configurable on a per SIP trunk group basis. Preferences for recursion and for name-server support are also configurable
- Using the following DNS queries to gather domain information:
  - DNS NS—Redirects DNS query to other DNS servers
  - DNS NAPTR—Gathers the transport information
  - DNS SRV—Gathers the port information
  - DNS A record—Gathers the address
- Maintaining a DNS Cache, where it is able to store the DNS records received from DNS servers. SBC supports removing cached records and changing Time To Live (TTL)
- ENUM queries to DNS servers for call routing
- DNS queries using both UDP and TCP transport and this is configurable
- Manual DNS queries

Locating a SIP Server Using DNS

The SBC uses the DNS procedures RFC3263 to resolve a SIP Uniform Resource Identifier (URI) into the IP address, port, and transport protocol of the next hop to contact.

When a SIP endpoint (like a UAC, for example) needs to send a request to a resource identified by a SIP or Secure SIP (SIPS) URI, it needs to resolve that URI into the IP address, port, and transport protocol. This URI can identify the desired resource to which the request is targeted (in which case, the URI is found in the Request-URI), or it can identify an intermediate hop towards that resource (in which case, the URI is found in the Route header).

For a SIP call where the transport is not known, or cannot be derived from the URI, the SIP endpoint should perform a Naming Authority Pointer (NAPTR) query for the domain name in the URI. Once the transport protocol is found from the records returned by the NAPTR query, the client can then use Location of Services (SRV) query on the protocol to target host FQDN and port number. Finally, the client can then perform an Address (A) record query to resolve the domain names returned by the SRV query to obtain the IP address of the server.

Local Cache

For network configurations where SIP Server domain resolution is not available from external DNS servers, the SBC supports a local DNS cache. DNS queries can then be made against either external DNS servers or the local cache. The following DNS record types can be configured in the local cache:

- A (Address)
- SRV (Location of Services)
- NS (Name Server)
- NAPTR (Naming Authority Pointer) records.

TCP Enhancement

The SBC supports all DNS queries over UDP from the DNS client with no option to configure the transport protocol for DNS servers. Additionally, the SBC supports DNS servers over TCP using the `transportProtocol` configuration object with two options: `udp` or `tcp`. Default value is `udp` . The flag `tcpFallback` supports TCP fallback when the configured protocol is UDP. The default value is `disabled`.

Configuration of Transport Protocol

The DNS Group Transport Protocol option allows the user to choose either UDP or TCP transport protocol for a DNS query for the associated DNS Group.

> **Note**
> The Transport Protocol option is configured per DNS server. You can configure up to eight DNS servers per DNS group, and up to 512 DNS Groups system-wide.

The figure below depicts DNS support when the transport protocol for the DNS server is configured as TCP.

Figure 1: TCP Connection

Support for TCP Fallback

DNS queries are sent over UDP to serve DNS Requests. UDP messages are preferred over TCP messages as TCP connections can consume computing resources for each connection. DNS servers get numerous connections per second and using TCP can add too much overhead. However, when the response data is received with TC flag, then DNS Client uses TCP as transport to resolve the request.

The `tcpFallback` flag can be enabled per DNS server to notify the DNS client to support TCP fallback when the DNS response on the UDP is received with TC flag. When the `tcpFallback` is enabled and the DNS client receives TC flag in response over UDP, then the DNS Client sends the same query again over TCP to the same server.

The figure below depicts TCP Fallback when the initial transport protocol is UDP and `tcpFallback` flag is enabled for that particular DNS server:

Figure 2: TCP Fallback

> **Info**
> This `tcpFallback` flag is disabled by default to support backward compatibility. The DNS over TCP works for both IPv4 and IPv6 transport protocol based on the configured address of the DNS server.

> **Note**
> The SBC supports, by default, 1300 Maximum Transmission Unit (MTU) bytes, and the MTU size used by the SBC is configurable. If the initial INVITE message size exceeds the default MTU value, the SBC sends the data over the TCP transport protocol. The TCP transport protocol is used if it is allowed by the transport profile, irrespective of its preference order.

TCP connection Pool

DNS client maintains the TCP connections in the TCP Pool, enabling DNS client to reuse those TCP connection, if DNS query is to be sent to the same server. Thus, the DNS client avoids opening TCP connection each time the DNS query comes for the same server. However, the DNS client removes the TCP connections periodically from the TCP Pool which are least recently used and their ideal timer expires.

DNS Cache Management and Override TTL

SBC supports the following functionalities:

- Flush the DNS Cache
- Override Time To Live (TTL)

Flush the DNS Cache

The SBC clears a DNS cache for:

- Specific DNS group
- FQDN (Full match or substring)
- Full cache on SBC

In case of FQDN, there are two scenarios:

1. To clear a particular record from the cache, request must match DNS group, FQDN, and the record type.
2. To clear a domain from the cache, request should match DNS group name and sub-string from the domain.

Override Time To Live (TTL)

SBC is able to override the TTL value with the new value if the matching FQDN and record type is found in the given DNS Group. If that FQDN value is not matching, it returns an error.

Manual DNS Query

The SBC supports performing a manual query where the cache receives updates of the IP address, TTL and port received in response to the query sent to the server. The response is updated if record is already present; otherwise, the SBC creates a new entry.

Two types of manual queries apply:

- Manual queries including the server : In this type, query is sent to the particular server. If the response is received, it updates the cache and if it ist not received, then it throw the error message.
- Manual queries which do not include the server: In this type, query is sent to the first server in the list. If response is not received from that server, then it tries the next server until it receives the response.

> **Note**
> A DNS group is configable with up to eight DNS servers.

If the SBC does not receive a response to the DNS query, it display an error after a configurable timeout. The manual DNS query supports re-sending the request over TCP, if the response is received with the TC (truncation flag) set and TCP Fallback is enabled.

Loss on DNS Service

The SBC supports raising an alarm when the server is blacklisted.

A server is blacklisted when:

- TCP connection with the DNS server cannot be established after a configured number of retries
- No response is received from the DNS server for TCP, despite the connection being established
- No response is received from the DNS server for UDP, after a configured number of retries

In the above scenarios, the SBC generates the following alarms:

- sonusSbxDnsServerBlacklistedNotification
- sonusSbxDnsServerRecoveredNotification

Info
For alarm details, refer to Domain Name Server (DNS) Alarms.

DNS Service Record (SRV) pathCheck

The SBC supports the following functionality:

- Service Record (SRV) lookup while performing DNS query for FQDN based targets. The SBC supports tracking of FQDN based IP peers that are configured using SRV and A/AAAA records. This provides more flexibility with the SBC tracking the FQDN peers based on SRV records and corresponding A/AAAA record combinations. Using this method, the SBC reports the availability status of the FQDN peers for each combination individually.
- SIP OPTIONS ping. The SIP OPTIONS request is periodically sent to a configured IP peer (both IPv4 and IPv6 FQDN are supported) to check the status and discover new capabilities. The OPTIONS request is sent using the Signaling Port of the zone configured for the peer. The OPTIONS ping feature is used to verify peer-to-peer connectivity, and if required, is enabled on an existing IP peer object.
- Configuring the frequency of OPTIONS requests. If the peer does not respond after a configurable number of consecutive OPTIONS timeout, it is declared as down and no new calls are sent to this peer. While the peer is down, OPTIONS based pinging continues. The peer is considered UP (recovered) after a configurable number of consecutive successful OPTIONS transactions.

  To support this feature, the default value of `hostPort` configuration under `ipPeer pathCheck` option is updated to `5060`. To enable this feature, set `hostPort` under `ipPeer pathCheck` option to `0`.

- When the `pathCheck` profile is attached to an FQDN based IP peer with `hostPort` set to `0`, the `pathCheck` task performs SRV lookup to resolve the port numbers. The resolved port numbers are used to send OPTIONS ping to the IP peer.

  Note
  For FQDN based IP peers attached with the `pathCheck` profile, A/AAAA query is already supported by the `pathCheck` task. The SBC supports SRV if `hostPort` is set to `0`.

- When the `pathCheck` profile is attached to an FQDN based IP peer configured with a `hostPort` (other than the value `0`), the `pathCheck` task does not perform SRV lookup. It uses the configured port to send OPTIONS ping to the IP peer.

The `pathCheck` task processes DNS SRV response as follows:

- When SRV query returns multiple SRV records, the `pathCheck` task sorts SRV records based on weight and priority and saves all the records. The `pathCheck` task then iterates through all the SRV records in the same order after the sorting to perform A/AAAA query on each SRV record.

The `pathCheck` task processes DNS A/AAAA response for each SRV record as follows:

- If multiple A or AAAA records are returned during A/AAAA query for a given SRV record then all those records are saved and tried. OPTIONS ping is sent to all the resolved IP addresses of a given SRV record. It then continues in the same way with the next SRV and performs A/AAAA query until all the SRV records are completed.

For example, the `pathCheck` task performed SRV query for a given FQDN target and two SRV records are returned: SRV1 and SRV2. They are in the same order after sorting based on weight and priority. SBC then sends A or AAAA query for SRV1 followed by SRV2. Assume that SRV query resulted in two A records. There are total of two SRV records with two A records each. The `pathCheck` task now sends OPTIONS ping to all the IP Address/Port combinations - A1:SRV1, A2:SRV1, A3:SRV2, and A4:SRV2.

The `pathCheck` task maintains overall status of an FQDN based Peer just like it does for the IP based Peer: It tracks and updates status of the FQDN peer using the OPTIONS ping messages sent to all learned SRV record combinations. When multiple IP Address/Port combinations are tried by the `pathCheck` task:

- if even one IP/Port combination is reachable, then the FQDN target is considered as UP.
- if all the IP/Port combinations are un-reachable, then the FQDN target is considered as DOWN.

Note

The `pathCheck` task internally sends notifications to registered tasks (such as ARS task) regarding FQDN target status change. Tasks registered with `pathCheck` receive the notification when a given FQDN target is UP or DOWN. This ensures that the task does not even attempt to send a call to the FQDN peer, which is DOWN.

If DNS query for an FQDN target fails (error, timeout, or no answer records), the `pathCheck` task retries the DNS query again after the configured retry time in the `pathCheck` profile.

If an FQDN peer to which the `pathCheck` profile is attached to is deleted, the `pathCheck` task clears all associated saved DNS records.

If an FQDN peer to which the `pathCheck` profile is attached to is modified with a new FQDN, the `pathCheck` task clears the associated DNS records for the earlier FQDN and performs a fresh DNS query using the newly updated FQDN.

Extended DNS (eDNS) Support

The SBC prefers DNS over UDP when the UDP payload limit is 512 bytes. The Extended Domain Name System (eDNS) improves the scalability of DNS. With this eDNS support, the SBC supports the maximum UDP payload size. This avoids the truncated UDP responses, which in turn try to re-enter over TCP.