ENTRADA2 Iceberg Schema Documentation

This document describes all columns in the ENTRADA2 Iceberg table schema.

Schema Columns

Column Name	Type	Required	Description
`dns_id`	Integer	Yes	Unique identifier for the DNS query/response
`time`	Timestamp	Yes	Timestamp when the DNS query was received
`dns_qname`	String	No	Query name (domain name being queried)
`dns_domainname`	String	No	Normalized domain name
`ip_ttl`	Integer	No	IP Time To Live value
`ip_version`	Integer	No	IP protocol version (4 or 6)
`prot`	Integer	No	Transport protocol (UDP=17, TCP=6)
`ip_src`	String	No	Source IP address
`prot_src_port`	Integer	No	Source port number
`ip_dst`	String	No	Destination IP address
`prot_dst_port`	Integer	No	Destination port number
`dns_aa`	Boolean	No	Authoritative Answer flag
`dns_tc`	Boolean	No	Truncated flag
`dns_rd`	Boolean	No	Recursion Desired flag
`dns_ra`	Boolean	No	Recursion Available flag
`dns_ad`	Boolean	No	Authentic Data flag
`dns_cd`	Boolean	No	Checking Disabled flag
`dns_ancount`	Integer	No	Answer record count
`dns_arcount`	Integer	No	Additional record count
`dns_nscount`	Integer	No	Authority record count
`dns_qdcount`	Integer	No	Question count
`dns_opcode`	Integer	No	DNS opcode (query type)
`dns_rcode`	Integer	No	DNS response code
`dns_qtype`	Integer	No	DNS query type (A, AAAA, MX, etc.)

Column Name	Type	Required	Description
`dns_qclass`	Integer	No	DNS query class (typically IN=1)
`ip_geo_country`	String	No	GeoIP country code for source IP
`ip_asn`	String	No	Autonomous System Number for source IP
`ip_asn_org`	String	No	Organization name for the ASN
`edns_udp`	Integer	No	EDNS UDP payload size
`edns_version`	Integer	No	EDNS version number
`edns_do`	Boolean	No	DNSSEC OK flag
`edns_options`	List[Integer]	No	List of EDNS option codes
`edns_ecs`	String	No	EDNS Client Subnet information
`edns_ecs_ip_asn`	String	No	ASN for EDNS Client Subnet IP
`edns_ecs_ip_asn_org`	String	No	Organization for EDNS Client Subnet ASN
`edns_ecs_ip_geo_country`	String	No	GeoIP country for EDNS Client Subnet
`edns_ext_error`	List[Integer]	No	EDNS Extended DNS Error codes
`dns_labels`	Integer	No	Number of labels in the query name
`dns_proc_time`	Integer	No	DNS processing time in milliseconds
`dns_pub_resolver`	String	No	Public resolver identifier
`dns_req_len`	Integer	No	DNS request message length in bytes
`dns_res_len`	Integer	No	DNS response message length in bytes
`tcp_rtt`	Integer	No	TCP Round Trip Time in milliseconds
`server`	String	Yes	DNS server identifier
`server_location`	String	Yes	Geographic location of the server
`dns_rdata`	List[Struct]	No	DNS resource record data (section, type, data)
`dns_cname`	List[String]	No	CNAME records in the response chain
`dns_tld`	String	No	Top-Level Domain from the query name
`dns_qname_full`	String	No	Full query name without normalization

DNS RDATA Structure

The `dns_rdata` column contains a list of structures with the following fields:

Field	Type	Description

Field	Type	Description
`section`	Integer	DNS section (0=Question, 1=Answer, 2=Authority, 3=Additional)
`type`	Integer	DNS record type (A, AAAA, MX, etc.)
`data`	String	The resource record data