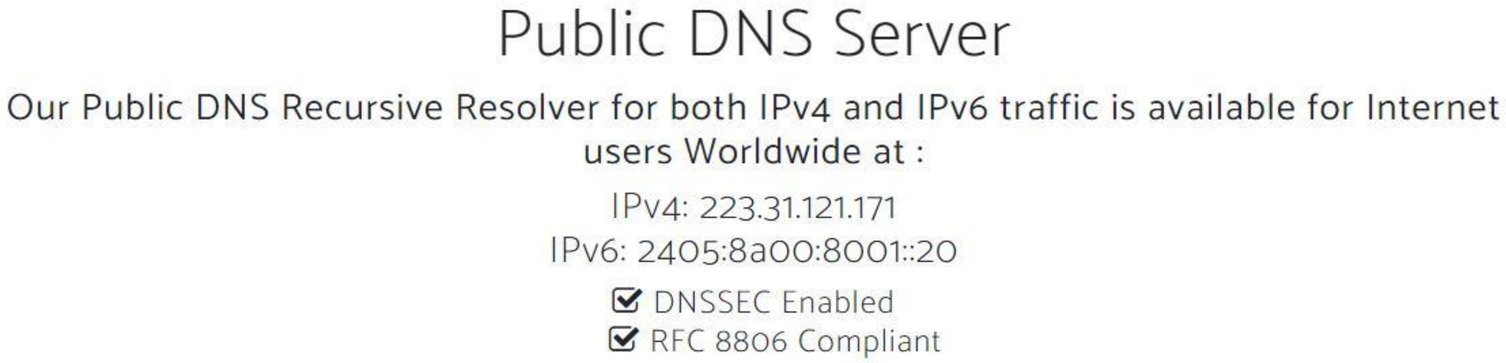
Centre of Excellence in
DNS
SECURITY

Webinar on

Fine tuning DNS performance and hardening using BIND

Thursday, 29th October 2020

03:00 PM - 05:00 PM



Public DNS Server

Our Public DNS Recursive Resolver for both IPv4 and IPv6 traffic is available for Internet users Worldwide at :

IPv4: 223.31.121.171
IPv6: 2405:8a00:8001::20

☑ DNSSEC Enabled
☑ RFC 8806 Compliant

Ministry of Electronics and
Information Technology
Government of India

nixi

सी-डैक CDAC | प्रगत संगणन विकास केंद्र
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING

Agenda

- Introduction
- Bind Components
- DNS Query Resolution
- Configuring for Performance & Security
- Enabling Logging in Bind
- DNS Query Resolution using RFC 8806
- Q & A

Introduction

- BIND is the most popular Domain Name System (DNS) server.
- It is FOSS (Free & Open Source Software)
- BIND means Berkeley Internet Name Domain.
- It was developed in the 1980s at the University of Berkeley.
- It can be used both as a Caching Server as well as an Authoritative Server.
- The demonstrations are based on Bind 9.16.6

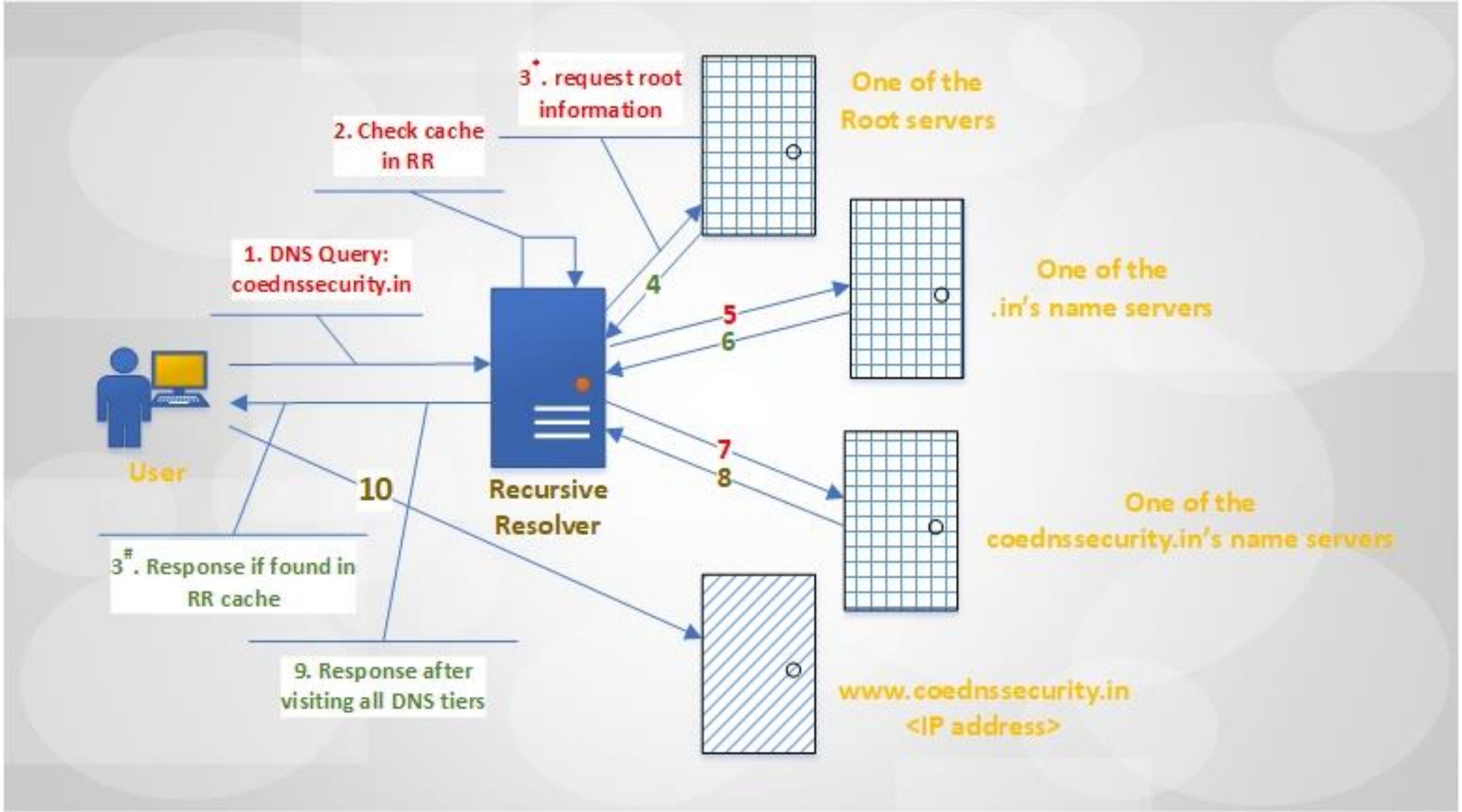
BIND Components

- *Name Server.*
  - Maintains a DNS Zone file and responds to DNS Requests
  - Acts either as a Caching only Name Server (Recursive Resolver) or Authoritative Name Server.
- *Lightweight Resolver.*
  - It contains a lightweight resolver library that can be run on DNS clients like host Operating System and routers
  - It also contains resolver daemon process which can run on a local host.
- *Name Server Tools.*
  - **dig** - allows users to resolve DNS queries
  - **host** - converts hostnames to IP addresses
  - **nslookup** - queries DNS servers for information about hosts and domains
  - **named-checkconf :** This tool checks the syntax of *named.conf* file
  - **Remote Name Daemon Control (rndc)**
    - Remote Name Daemon Control
    - It allows the System Administrators to control the operation of a name server over a TCP connection

Dig – Domain Information Groper

- Dig is an administrative tool for querying DNS Name Servers
- It is useful for performing DNS Lookups and displays the answers that are returned from the name server
- It is also useful for verifying and troubleshooting DNS Problems

DNS Query Resolution


3*. request root information
2. Check cache in RR
One of the Root servers
1. DNS Query: coednssecurity.in
4
5
6
One of the .in's name servers
User
Recursive Resolver
10
7
8
One of the coednssecurity.in's name servers
3#. Response if found in RR cache
9. Response after visiting all DNS tiers
www.coednssecurity.in <IP address>

"In the conventional approach, the RR server spends considerable time to reach out to the closest root server"

Configuring for Performance and Security

- **dump-file**: stores the resolver cache. Default file name is *named_dump.db*
- **statistics-file:** stores statistics details of resolver. Default file name is *named.stats*
- **memstatistics-file:** stores the memory usage statistics. Default file name is *named.memstats*
- **recursing-file:** the resolver stores the queries that are currently recursing. Default file is *named.recursing*

Configuring for Performance and Security

- **memstatistics**: This writes memory statistics to the file specified by *memstatistics-file.* The default option is **no.**
- **managed-keys-directory:** This specifies the directory in which to store the files that track managed DNSSEC keys.
- **pid-file:** the server stores its process ID. If not specified, the default is usr/local/var/run/named/named.pid.
- **session-keyfile:** the server stores a TSIG session key generated by named
- **dnssec-validation:** This option enables DNSSEC Validation
  - If set to auto, DNSSEC validation is enabled and a default trust anchor for the DNS root zone is used.
  - If set to yes, DNSSEC validation is enabled, but a trust anchor must be manually configured using a trustanchors statement.
  - If set to no, DNSSEC validation is disabled.
  - The default is auto, unless BIND is built with configure --disable-auto-validation, in which case the default is yes.

Configuring for Performance and Security

- **minimal-any**: If set to **yes**, the server replies with only one of the RRsets for the query name when generating a positive response to a query of type ANY over UDP. The default is **no**.
- **querylog**: Query logging provides a complete log of all incoming queries and all query errors.
- **zone-statistics**: If yes, the server collects statistical data on all zones, unless specifically turned off on a per zone basis by specifying zone-statistics terse or zone-statistics none in the zone statement.
- **minimal-responses:** This option controls the addition of records to the authority and additional sections of responses. If the option is **yes** the server responds with only the answer section, avoiding the authority and additional sections.

Configuring for Performance and Security

- **qname-minimization:** This option controls QNAME minimization behavior in the BIND resolver.
- **stale-answer-enable:** If yes, enable the returning of “stale” cached answers when the name servers for a zone are not answering and the stale-cache-enable option is also enabled. The default is not to return stale answers.
- **Stale-cache-enable:** If yes, enable the retaining of “stale” cached answers. Default yes.
- **clients-per-query:** This is the initial value (minimum) number of recursive simultaneous clients for any given query that the server accepts before dropping additional clients. Default is 10.
- **max-clients-per-query:** This is the initial value (maximum) number of recursive simultaneous clients for any given query that the server accepts before dropping additional clients. Default is 100.

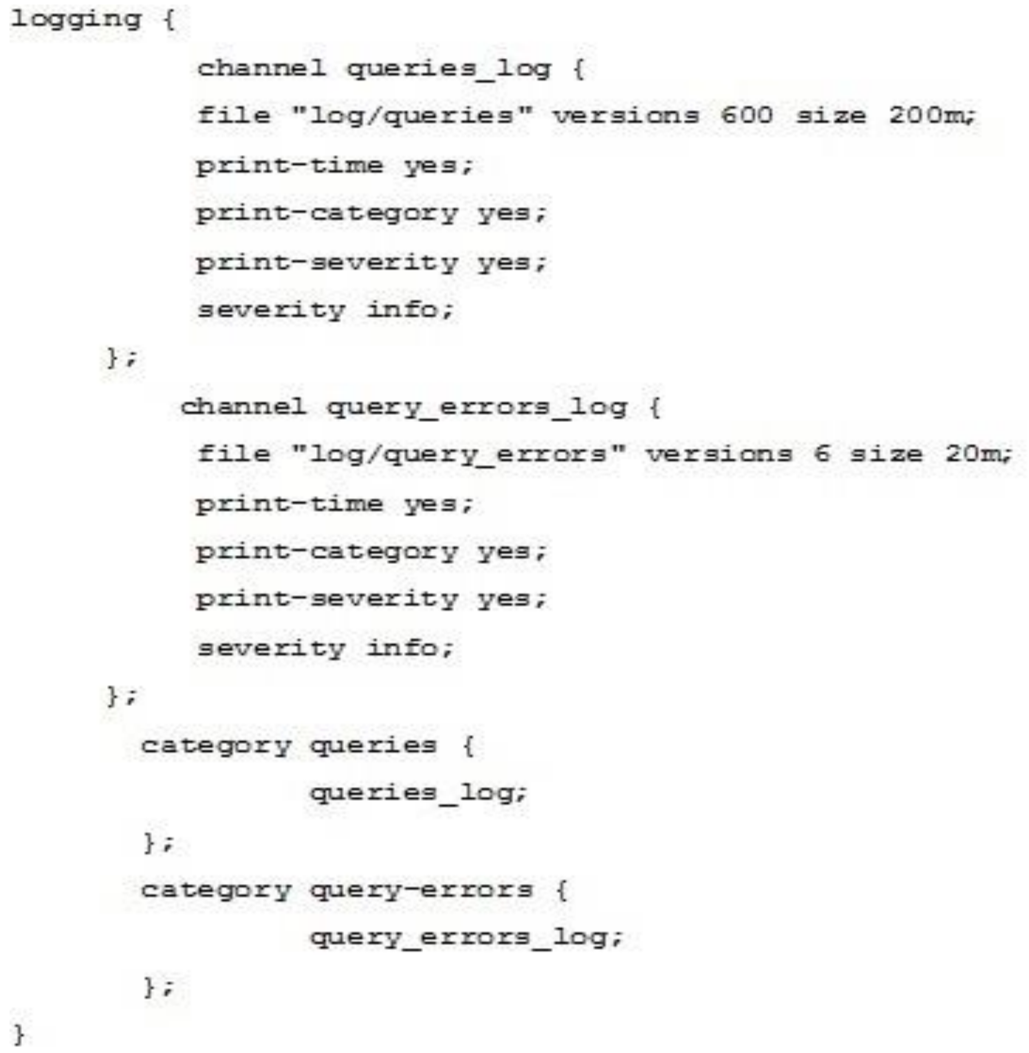
Enabling Logging in Bind

- Logging configuration is only established when the entire configuration file has been parsed
- At start-up all logging messages regarding syntax errors in the configuration file go to the default channels
- Commenting
  - // or # - for single line comments
  - /*   */ - for multi-line comments

Enabling Logging in Bind

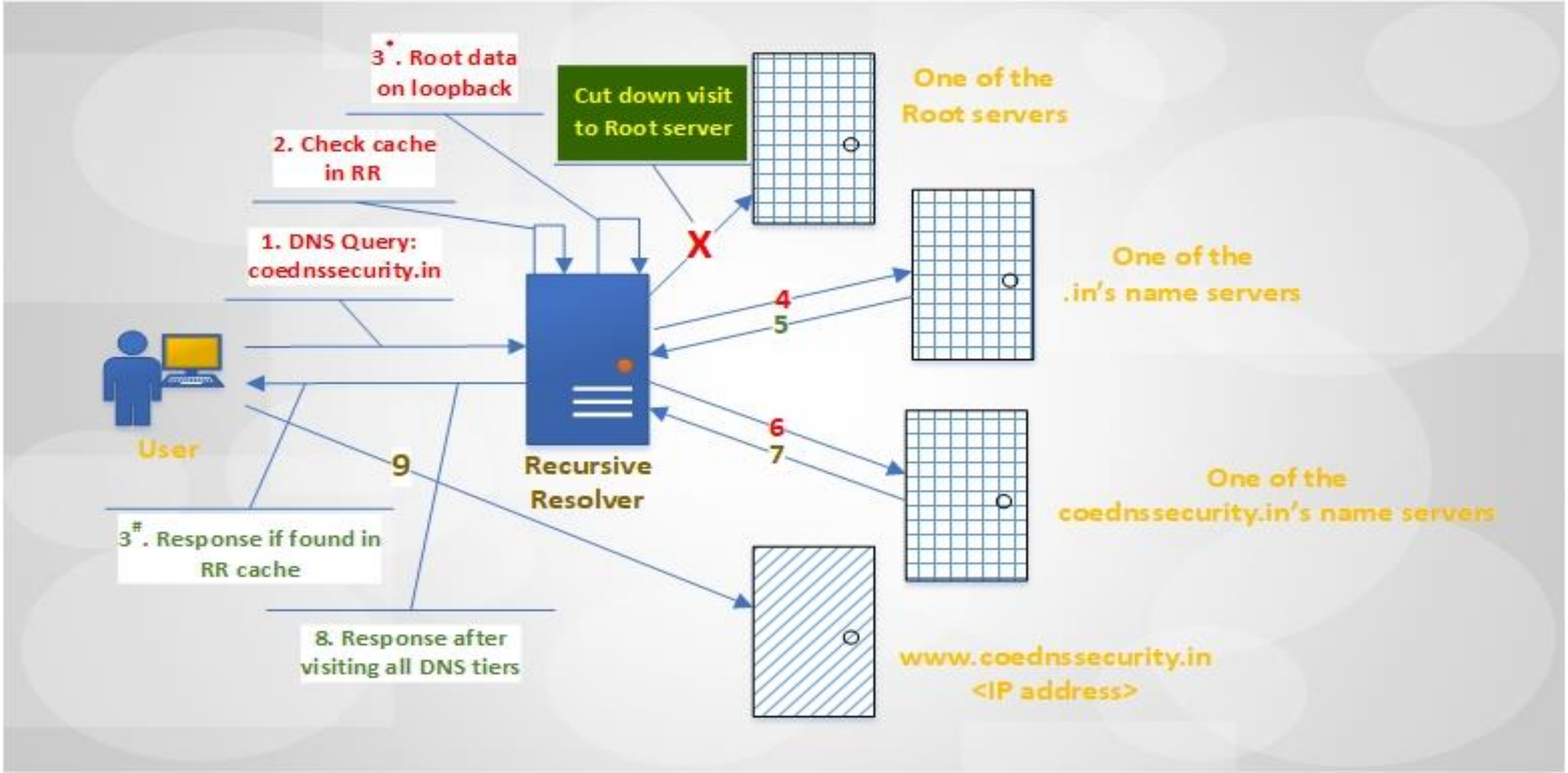
- Channels:
  - All log output goes to one or more channels
  - There is no limit to the number of channels that can be created
  - The file destination clause directs the channel to a disk file
  - The size option is used to limit log file growth.
  - The versions option specifies how many backup versions of the file
  - should be kept
  - The suffix option can be set to either increment or timestamp
- Categories:
  - queries: all query transactions
  - query-errors: all query failures
  - security: approval and denial of requests
  - xfer-in, xfer-out: zone transfers received and sending respectively
  - dnssec: all errors in dnssec validation
  - rpz: Response Policy Zone (Black-listing)

Sample Logging File



```
logging {
          channel queries_log {
          file "log/queries" versions 600 size 200m;
          print-time yes;
          print-category yes;
          print-severity yes;
          severity info;
     };
         channel query_errors_log {
          file "log/query_errors" versions 6 size 20m;
          print-time yes;
          print-category yes;
          print-severity yes;
          severity info;
     };
       category queries {
                queries_log;
       };
       category query-errors {
                query_errors_log;
       };
}
```

RFC 8806 based approach of DNS Query Resolution

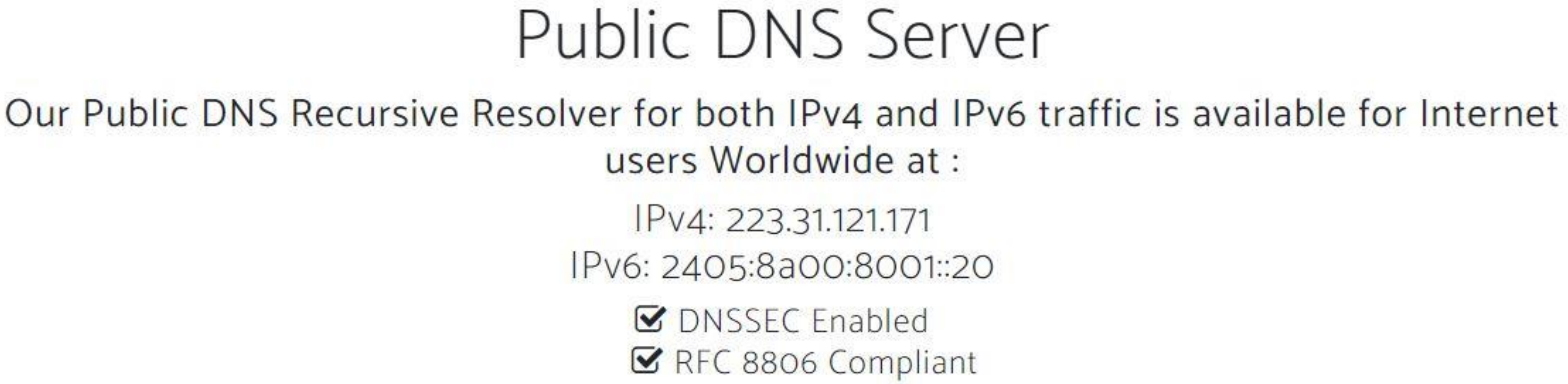

3*. Root data on loopback
Cut down visit to Root server
One of the Root servers
2. Check cache in RR
X
1. DNS Query: coednssecurity.in
4
5
One of the .in's name servers
User
9
Recursive Resolver
6
7
One of the coednssecurity.in's name servers
3#. Response if found in RR cache
8. Response after visiting all DNS tiers
www.coednssecurity.in <IP address>

"In the RFC 8806 based approach, the loopback server containing root data is hosted on the RR server itself to avoid visiting the root servers for root data"

References

- Bind 9.16.6 Software: https://coednssecurity.in/pdf/bind-9.16.6.tar.xz
- Bind 9.16.6 Manual: https://coednssecurity.in/pdf/DNS-Bind-Server-Installation-Configuration.pdf
- Bind DNS Server Security and Performance Enhancement: https://coednssecurity.in/pdf/DNS-Hardening-by-Security-Enrichment-and-Performance-Enhancement-of-Recursive-Resolver.pdf
- Reducing RTT of DNS Query Resolution using RFC 7706: https://coednssecurity.in/pdf/ReducingRTTofDNSQueryResolution-V1.pdf
- Bind Administration Manual: https://bind9.readthedocs.io/en/v9_16_7/

Q & A



Public DNS Server

Our Public DNS Recursive Resolver for both IPv4 and IPv6 traffic is available for Internet users Worldwide at :

IPv4: 223.31.121.171
IPv6: 2405:8a00:8001::20

☑ DNSSEC Enabled
☑ RFC 8806 Compliant

Please help us improve our email security solution by forwarding your spam emails to our SPAM BOX at:
spam@coednssecurity.in

Thank you