Manual for

Installation and Configuration of DoH (DNS over HTTPS) and DoT (DNS over TLS)

December 2020

Centre of Excellence in DNS SECURITY

System and Software Requirements

1) OS: Ubuntu 20.04 LTS
2) Internet connection.
3) A valid IP address.
4) Hostname: doh.local
5) Software Packages Required: bind v9.16.1+, dnsdist v1.4+

Manual at Glance:

I. Prepare the system for installation. Update the OS

```
#sudo su
#apt update
#apt upgrade
#apt autoremove
```

II. Install and Verify Bind Installation

1) Install Bind 9

```
# apt install bind9
```

2) Verify installation

```
# nslookup www.cdac.in localhost
```

```
root@ubuntu:/home/anoopmis# nslookup www.cdac.in localhost
Server:         localhost
Address:        127.0.0.1#53

Non-authoritative answer:
www.cdac.in     canonical name = cdac.in.
Name:   cdac.in
Address: 196.1.113.45
Name:   cdac.in
Address: 2405:8a00:6029::45
```

III. Install and Verify dnsdist Installation

dnsdist is a highly DNS-, DoS- and abuse-aware loadbalancer. Its goal in life is to route traffic to the best server, delivering top performance to legitimate users while shunting or blocking abusive traffic. For more information visit: https://dnsdist.org/.

1) Install dnsdist

```
# apt install dnsdist
```

2) Verify dnsdist installation

```
# dnsdist --version
```

```
root@ubuntu:/home/anoopmis# dnsdist --version
dnsdist 1.4.0 (Lua 5.2.4)
Enabled features: cdb dns-over-tls(gnutls openssl) dns-over-https(DOH) dnscrypt ebpf
fstrm ipcipher libsodium lmdb protobuf re2 recvmmsg/sendmmsg snmp systemd
```

The version must be 1.4.0+.

IV. Generate TLS Certificate

If the system has a valid public domain name, then a free TLS certificate can be obtained from Let's Encrypt. The steps for obtaining the certificate are listed at: https://certbot.eff.org/

1) To generate a self-signed certificate, go to "/opt" run the following command:

```
# openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout doh.local.key -out doh.local.crt
```

```
root@ubuntu:/home/anoopmis# openssl req -x509 -nodes -days 365 -newkey rsa:2048
-keyout doh.local.key -out doh.local.crt
Generating a RSA private key
..........+++++
.....................................................................................
..........+++++
writing new private key to 'doh.local.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:IN
State or Province Name (full name) [Some-State]:Karnataka
Locality Name (eg, city) []:Bangalore
Organization Name (eg, company) [Internet Widgits Pty Ltd]:CDAC
Organizational Unit Name (eg, section) []:CSG
Common Name (e.g. server FQDN or YOUR name) []:doh.local
Email Address []:anoop@cdac.in
```

V. Configure dnsdist for DoH and DoT

1) Open dnsdist configuration file:

```
# nano /etc/dnsdist/dnsdist.conf
```

Append following line to change the listening port of dnsdist. By default, it listens on port 53 which conflicts with bind listening port. Now it will listen on all interfaces on port 5300.

```
addLocal('0.0.0.0:5300', {doTCP=true, reusePort=true, tcpFastOpenSize=0})
```

***Optionally for IPv6, add following line**

```
addLocal('[::]:5300', {doTCP=true, reusePort=true, tcpFastOpenSize=0})
```

Add Permissive ACL

```
addACL('0.0.0.0/0')
```

***Optionally for IPv6, add following line**

```
addACL('::/0')
```

Add Local Recursive Resolver to which DNS queries will be forwarded. The IP can be the local IP, or localhost IP or the Public IP.

```
newServer({address="127.0.0.1",qps=1, name="resolver1"})
```

***Optionally, multiple recursive DNS servers can be added by repeating the line above and changing the IP address and name.**
Add TLS resolver as follow. The certificate and key also need to be specified.

```
addTLSLocal('0.0.0.0','/opt/doh.local.crt, '/opt/doh.local.key)
```

***Optionally for IPv6, add following line**

```
addTLSLocal('[::]','/opt/doh.local.crt, '/opt/doh.local.key)
```

Add DoH resolver as follow. The DoH will be listening to all interfaces (0.0.0.0) on port 443 and can be queried on https://doh.local

```
addDOHLocal("0.0.0.0:443", "/opt/doh.local.crt", "/opt/doh.local.key", "/", {
doTCP=true, reusePort=true, tcpFastOpenSize=0 })
```

***Optionally add webserver to view statistics. The webserver will only accept connection from localhost.**

```
webserver("127.0.0.1:8081", "Password", "APIKey")
```

Now your file should look like this:

```
addACL('0.0.0.0/0')

addLocal('0.0.0.0:5300', {doTCP=true, reusePort=true, tcpFastOpenSize=0})

newServer({address='127.0.0.1', qps=1,name='resolver1'})

newServer({address='223.31.121.171', qps=1,name='resolver1'})

addTLSLocal('0.0.0.0', '/opt/doh.local.crt', '/opt/doh.local.key')

addDOHLocal('0.0.0.0:443', '/opt/doh.local.crt', '/opt/doh.local.key', '/', {doTCP=true, reusePort=true, tcpFastOpenSize=0})

webserver("127.0.0.1:8081", "Cdac@123", "Cdac@123")
```

2) Save the dnsdist configuration file and start & check the dnsdist service. The status should show active (running).

```
# systemctl start dnsdist

# systemctl status dnsdist
```

```
● dnsdist.service - DNS Loadbalancer
     Loaded: loaded (/lib/systemd/system/dnsdist.service; enabled; vendor preset: enabled)
     Active: active (running) since Thu 2020-08-20 17:03:53 IST; 5s ago
       Docs: man:dnsdist(1)
             https://dnsdist.org
    Process: 18457 ExecStartPre=/usr/bin/dnsdist --check-config (code=exited, status=0/SUCCESS)
   Main PID: 18474 (dnsdist)
      Tasks: 13 (limit: 8192)
     Memory: 24.1M
     CGroup: /system.slice/dnsdist.service
             └─18474 /usr/bin/dnsdist --supervised --disable-syslog -u _dnsdist -g _dnsdist

Aug 20 17:03:52 doh.local dnsdist[18457]: Configuration '/etc/dnsdist/dnsdist.conf' OK!
Aug 20 17:03:52 doh.local dnsdist[18474]: Added downstream server 127.0.0.1:53
Aug 20 17:03:52 doh.local dnsdist[18474]: Listening on 0.0.0.0:5300
Aug 20 17:03:52 doh.local dnsdist[18474]: Listening on 0.0.0.0:853 for TLS
Aug 20 17:03:52 doh.local dnsdist[18474]: Listening on 0.0.0.0:443 for DoH
```

3) To check if the DoH service is running, we can use curl. *[Install curl, if not present]*

```
# curl --doh-url https://doh.local www.iiref.in
```

VI. Install dnslookup tool for verifying DoH and DoT working

1) Download and install dnslookup using SNAP

```
# snap install dnslookup
```

2) Query DoH and DoT [Here, a public DoH/DoT is being used.]

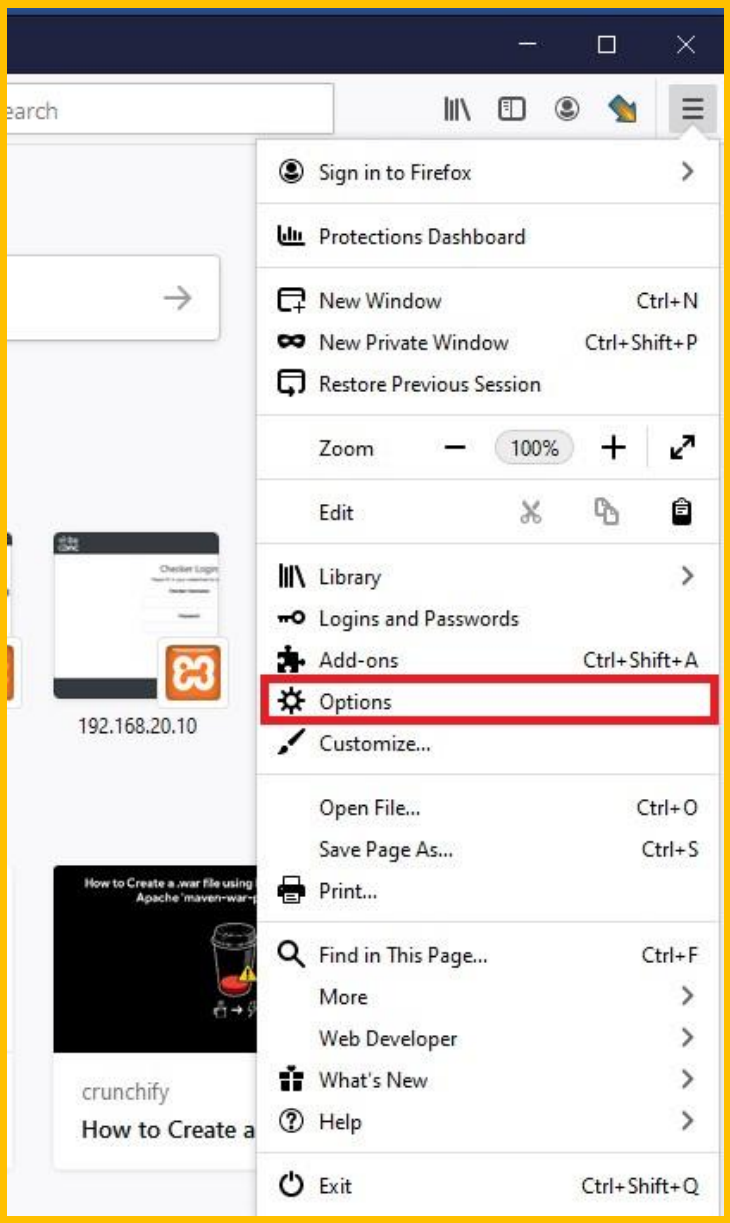
# dnslookup www.cdac.in https://doh.iiref.in	[Public DoH Sever]
# dnslookup www.cdac.in tls://doh.iiref.in	[Public DoT Sever]
#VERIFY=0 dnslookup www.cdac.in tls://doh.local	[To disable certificate check]

```
root@ubuntu:/opt# dnslookup www.cdac.in https://doh.iiref.in
dnslookup 1.3.0-5472
dnslookup result:
;; opcode: QUERY, status: NOERROR, id: 65327
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.cdac.in.   IN       A

;; ANSWER SECTION:
www.cdac.in.    1200    IN      CNAME   cdac.in.
cdac.in.        1200    IN      A       196.1.113.45

root@ubuntu:/opt# dnslookup www.cdac.in tls://doh.iiref.in
dnslookup 1.3.0-5472
dnslookup result:
;; opcode: QUERY, status: NOERROR, id: 61686
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.cdac.in.   IN       A

;; ANSWER SECTION:
www.cdac.in.    1192    IN      CNAME   cdac.in.
cdac.in.        1192    IN      A       196.1.113.45
```

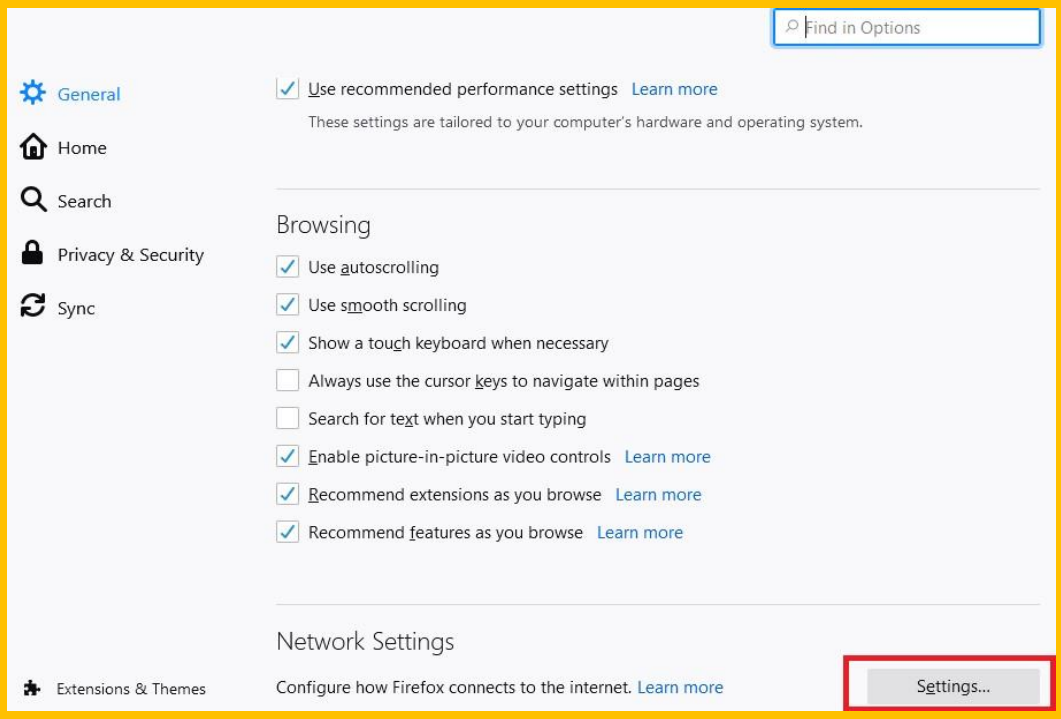
VII. Enabling DoH in Firefox *[Only if the DoH server has a valid domain name and TLS certificate]*

The Firefox browser should be updated to the latest version (currently 73.0+)

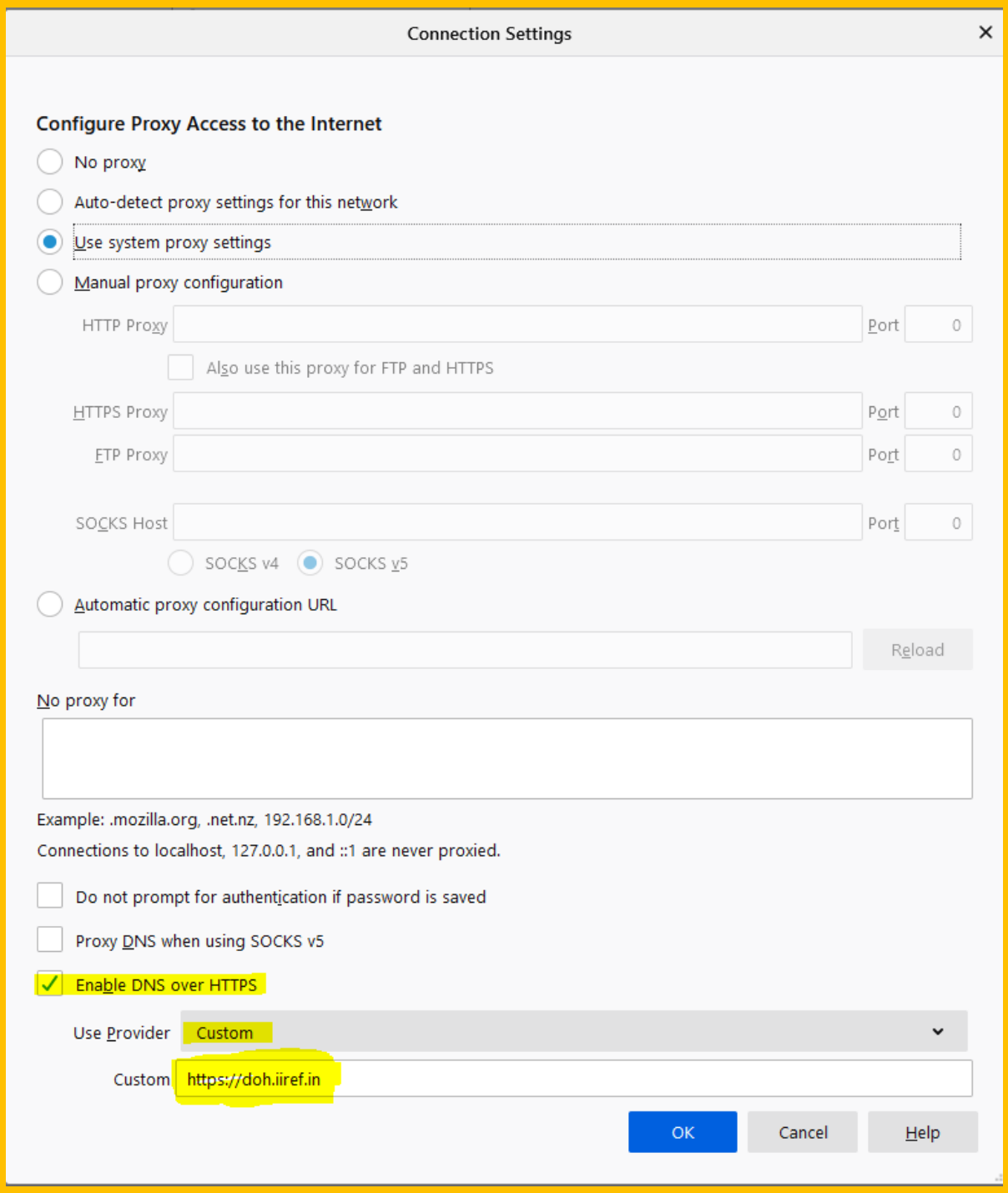
1) **To enable DoH, click the three horizontal bars in the top-right corner of Firefox and then select the "Options" button.**



2) **Search for Network Settings (usually at the bottom of the page) and click on the button.**



3) **Scroll to the bottom of the wizard, click on Enable DNS over HTTPS checkbox, select custom provider and type the URL of the DoH server.**


Connection Settings
Configure Proxy Access to the Internet
No proxy
Auto-detect proxy settings for this network
Use system proxy settings
Manual proxy configuration
HTTP Proxy
Port
0
Also use this proxy for FTP and HTTPS
HTTPS Proxy
Port
0
FTP Proxy
Port
0
SOCKS Host
Port
0
SOCKS v4
SOCKS v5
Automatic proxy configuration URL
Reload
No proxy for
Example: .mozilla.org, .net.nz, 192.168.1.0/24
Connections to localhost, 127.0.0.1, and ::1 are never proxied.
Do not prompt for authentication if password is saved
Proxy DNS when using SOCKS v5
Enable DNS over HTTPS
Use Provider
Custom
Custom
https://doh.iiref.in
OK
Cancel
Help

VIII. Enable logging in Bind 9

1) Open bind configuration file

```
# nano /etc/bind/named.conf
```

Append the following line

```
include "/etc/bind/named.conf.logging";
```

2) Open named options file and enable querylog

```
# nano /etc/bind/named.conf.options

querylog yes;
```

```
root@dns:/home/anoopmis# cat /etc/bind/named.conf.options
options {
        directory "/var/cache/bind";

        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacing
        // the all-0's placeholder.

        // forwarders {
        //      0.0.0.0;
        // };

        //========================================================================
        // If BIND logs error messages about the root key being expired,
        // you will need to update your keys.  See https://www.isc.org/bind-keys
        //========================================================================
        dnssec-validation auto;

        querylog yes;

        listen-on-v6 { any; };
};
```

3) Create logging configuration file and add the following

```
# nano /etc/bind/named.conf.logging

logging {
```

```
    channel querylog {
        file "/var/cache/bind/querylog";
        severity debug 3;
        print-time yes;     // Print timestamp on logs
    };
    category queries { querylog; };
};
```

4) Create querylog file and change ownership

```
# touch /var/cache/bind/querylog
# chown bind.bind /var/cache/bind/querylog
```

5) Restart Bind

```
# systemctl restart bind
```


Acknowledgements:

We express our sincere thanks to Internet Governance Division of Ministry of Electronics & Information Technology (MeitY) and National Internet Exchange of India (NIXI).