**Write an Ansible Playbook to install and configure DNS on RHEL 9 Guide**

**Install the Required Ansible Collection**

**Run this command on your control machine (where you run Ansible):**

# ansible-galaxy collection install ansible.posix

**Add to requirements.yml (for consistency)**

**Create a file called requirements.yaml:**

# vim requirements.yaml

collections:

- name: ansible.posix

Then install it with:

# ansible-galaxy collection install -r requirements.yaml

Confirm It Works

After installation, re-run your playbook:

# ansible-playbook install\_dns.yaml

**Create a user hogege and add the sudoers file:**

# useradd hogege; passwd hogege

**Edit sudoers file:**

# vim /etc/sudoers

## Allow root to run any commands anywhere

root ALL=(ALL) ALL

hogege ALL=(ALL) ALL

# su - hogege

# mkdir ansible\_automation; cd ansible\_automation

# sudo vim install\_dns.yaml

---

- name: Install and Configure DNS Server (BIND) on RHEL 9

hosts: dns

become: true

vars:

domain\_name: "henogez.com"

zone\_file: "forward.henogez.com"

dns\_ip: "10.0.0.35" # IP of the DNS server

reverse\_zone\_name: "0.0.10.in-addr.arpa"

reverse\_zone\_file: "reverse.henogez.com"

host\_last\_octet: "35"

tasks:

- name: Install BIND and utilities

dnf:

name:

- bind

- bind-utils

state: present

- name: Enable and start named service

systemd:

name: named

enabled: yes

state: started

- name: Ensure backup directory exists

file:

path: /etc/named.backups

state: directory

mode: '0755'

- name: Backup named.conf with timestamp

copy:

src: /etc/named.conf

dest: "/etc/named.backups/named.conf.{{ ansible\_date\_time.iso8601 }}"

remote\_src: yes

mode: '0644'

- name: Configure main BIND config

copy:

dest: /etc/named.conf

content: |

options {

listen-on port 53 { 127.0.0.1; 10.0.0.35; };

listen-on-v6 port 53 { ::1; };

directory "/var/named";

dump-file "/var/named/data/cache\_dump.db";

statistics-file "/var/named/data/named\_stats.txt";

memstatistics-file "/var/named/data/named\_mem\_stats.txt";

secroots-file "/var/named/data/named.secroots";

recursing-file "/var/named/data/named.recursing";

allow-query { any; };

recursion yes;

dnssec-enable yes;

dnssec-validation yes;

managed-keys-directory "/var/named/dynamic";

pid-file "/run/named/named.pid";

session-keyfile "/run/named/session.key";

include "/etc/crypto-policies/back-ends/bind.config";

};

zone "{{ domain\_name }}" IN {

type master;

file "{{ zone\_file }}";

allow-update { none; };

allow-query { any; };

};

- name: Add reverse zone to named.conf

blockinfile:

path: /etc/named.conf

marker: "# {mark} REVERSE ZONE BLOCK"

block: |

zone "{{ reverse\_zone\_name }}" IN {

type master;

file "{{ reverse\_zone\_file }}";

allow-update { none; };

allow-query { any; };

};

include "/etc/named.rfc1912.zones";

include "/etc/named.root.key";

- name: Create forward zone file

copy:

dest: /var/named/{{ zone\_file }}

owner: named

group: named

mode: '0644'

content: |

$TTL 86400

@ IN SOA dns-01.{{ domain\_name }}. root.{{ domain\_name }}. (

2025060501 ; Serial

3600 ; Refresh

1800 ; Retry

604800 ; Expire

86400 ) ; Minimum TTL

IN NS dns-01.{{ domain\_name }}.

dns-01 IN A {{ dns\_ip }}

www IN A {{ dns\_ip }}

- name: Create reverse zone file

copy:

dest: /var/named/{{ reverse\_zone\_file }}

owner: named

group: named

mode: '0644'

content: |

$TTL 86400

@ IN SOA dns-01.{{ domain\_name }}. root.{{ domain\_name }}. (

2025060501 ; Serial

3600 ; Refresh

1800 ; Retry

604800 ; Expire

86400 ) ; Minimum TTL

IN NS dns-01.{{ domain\_name }}.

{{ host\_last\_octet }} IN PTR dns-01.{{ domain\_name }}.

# - name: Allow DNS through firewalld

# firewalld:

# service: dns

# permanent: true

# state: enabled

# immediate: true

- name: Restart named to apply zone changes

systemd:

name: named

state: restarted

- name: Verify named is running

shell: systemctl is-active named

register: named\_status

changed\_when: false

- name: Show named status

debug:

msg: "named service is {{ named\_status.stdout }}"

# sudo ansible-playbook install\_dns.yaml --syntax-check

# sudo ansible-playbook install\_dns.yaml

To **permanently set the nameserver in /etc/resolv.conf** on RHEL 9 (or any modern Linux using NetworkManager or systemd-resolved), you must configure the **network connection**, not just edit the file manually — because it gets **overwritten on reboot or network changes**.

**Here are the correct methods:**

**Use nmcli (Recommended on RHEL 9)**

**Find your connection name:**

# nmcli con show

# nmcli con mod "ens33" ipv4.dns "10.0.0.35"

# nmcli con mod "ens33" ipv4.ignore-auto-dns yes

# nmcli con down ens33; nmcli con up ens33

**Confirm:**

# cat /etc/resolv.conf

**To confirm that the DNS zone lookup files are free from any syntactical errors, run the commands shown:**

# named-checkconf

# named-checkzone henogez.com /var/named/forward.henogez.com

# named-checkzone 10.0.0.35 /var/named/reverse.henogez.com

**For the changes to be reflected in the system, Restart the Bind DNS server:**

# systemctl restart named

**Run the “nslookup” command to test the Bind DNS server:**

# nslookup dns-01.henogez.com

# nslookup 10.0.0.35

# dig dns-01.henogez.com

**To perform a reverse DNS lookup, use the dig command as shown:**

# dig -x 10.0.0.35