Session - 38 Agenda:

1. DNS Configuration Using Ansible

[vikasnehra@ansible-server ~]$ ping node1
PING node1.nehraclasses.local (192.168.229.129) 56(84) bytes of data.
64 bytes from node1.nehraclasses.local (192.168.229.129): icmp_seq=1 ttl=64 time=1.61 ms
64 bytes from node1.nehraclasses.local (192.168.229.129): icmp_seq=2 ttl=64 time=0.529 ms
^C
--- node1.nehraclasses.local ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 0.529/1.071/1.614/0.542 ms

[vikasnehra@ansible-server ~]$ vim dns-server.yml

```
---
- name: Authoritative DNS Server Configuration Playbook
  hosts: node1
  become: true
  tasks:
    - name: Setting up the static hostname in the machine.
      command: hostnamectl set-hostname dns-primary.nehraclasses.edu

    - name: Installing the bind packages in the machine.
      dnf:
        name:
          - bind
          - bind-utils
        state: latest

    - name: Making changes in the /etc/named.conf configuration file. (Comment listen-on port 53 line)
      replace:
        path: /etc/named.conf
        regexp: 'listen-on port 53 { 127.0.0.1; };'
        replace: '//listen-on port 53 { 127.0.0.1; };'

    - name: Making changes in the /etc/named.conf configuration file. (Comment listen-on-v6 port 53 line)
      replace:
        path: /etc/named.conf
        regexp: 'listen-on-v6 port 53 { ::1; };'
        replace: '//listen-on-v6 port 53 { ::1; };'

    - name: Making changes in the /etc/named.conf configuration file. (Modify allow-query line)
      replace:
        path: /etc/named.conf
        regexp: 'allow-query     { localhost; };'
        replace: 'allow-query     { localhost; 192.168.229.0/24; };'

    - name: Making changes in the /etc/named.conf configuration file.
      blockinfile:
        path: /etc/named.conf
        insertafter: EOF
        block: |
          //forward zone
          zone "nehraclasses.edu" IN {
          type master;
          file "nehraclasses.edu.db";
          allow-update { none; };
          allow-query { any; };
          };
```

```
//reverse zone
zone "229.168.192.in-addr.arpa" IN {
type master;
file "nehraclasses.edu.rev";
allow-update { none; };
allow-query { any; };
};


  - name: Creating forward lookup zone file using ansible jinja2 template file.
    template:
      src: forward.j2
      dest: /var/named/nehraclasses.edu.db
      owner: named
      group: named

  - name: Creating reverse lookup zone file using ansible jinja2 template file.
    template:
      src: reverse.j2
      dest: /var/named/nehraclasses.edu.rev
      owner: named
      group: named

  - name: Allowing DNS traffic in the firewall.
    firewalld:
      service: dns
      zone: public
      permanent: true
      immediate: true
      state: enabled

  - name: Starting & enabling the DNS service.
    service:
      name: named
      state: started
      enabled: yes
...

[vikasnehra@ansible-server ~]$ vim forward.j2
$TTL 86400
@ IN SOA dns-primary.nehraclasses.edu. admin.nehraclasses.edu. (
        2020011800 ;Serial
        3600 ;Refresh
        1800 ;Retry
        604800 ;Expire
        86400 ;Minimum TTL
)

;Name Server Information
@ IN NS dns-primary.nehraclasses.edu.
;IP Address for Name Server
dns-primary IN A 192.168.229.129
;Mail Server MX Record
nehraclasses.edu. IN MX 10 mail.nehraclasses.edu.
; A Record for the following hostname
www IN A 192.168.229.50
mail IN A 192.168.229.60
;CNAME Record
ftp IN CNAME www.nehraclasses.edu.
```

[vikasnehra@ansible-server ~]$ vim reverse.j2

```
$TTL 86400
@ IN SOA dns-primary.nehraclasses.edu. admin.nehraclasses.edu. (
        2020011800 ;Serial
        3600 ;Refresh
        1800 ;Retry
        604800 ;Expire
        86400 ;Minimum TTL
)
;Name Server Inforamtion
@ IN NS dns-primary.nehraclasses.edu.
dns-primary IN A 192.168.229.129
;Reverse lookup for name server
129 IN PTR dns-primary.nehraclasses.edu.
;PTR Record IP Address to Hostname
50 IN PTR www.nehraclasses.edu.
60 IN PTR mail.nehraclasses.edu.
```

[vikasnehra@ansible-server ~]$ ansible-playbook dns-server.yml

ERROR! couldn't resolve module/action 'firewalld'. This often indicates a misspelling, missing collection, or incorrect module path.
The error appears to be in '/home/vikasnehra/dns-server.yml': line 69, column 7, but may
be elsewhere in the file depending on the exact syntax problem.
The offending line appears to be:
  - name: Allowing DNS traffice in the firewall.
    ^ here

[vikasnehra@ansible-server ~]$ ansible-galaxy collection install ansible.posix

Starting galaxy collection install process
Process install dependency map
Starting collection install process
Downloading https://galaxy.ansible.com/download/ansible-posix-1.5.4.tar.gz to
/home/vikasnehra/.ansible/tmp/ansible-local-368818mc6rxp3/tmpe022_emi/ansible-posix-1.5.4-94ib36oi
Installing 'ansible.posix:1.5.4' to '/home/vikasnehra/.ansible/collections/ansible_collections/ansible/posix'
ansible.posix:1.5.4 was installed successfully

[vikasnehra@ansible-server ~]$ ansible-playbook dns-server.yml

PLAY [Authoritative DNS Server Configuration Playbook]
****

TASK [Gathering Facts]
****
ok: [node1]

TASK [Setting up the static hostname in the machine.]
****
changed: [node1]

TASK [Installing the bind packages in the machine.]
****
changed: [node1]

TASK [Making changes in the /etc/named.conf configuration file. (Comment listen-on port 53 line)]
****
changed: [node1]

TASK [Making changes in the /etc/named.conf configuration file. (Comment listen-on-v6 port 53 line)]
****
changed: [node1]

TASK [Making changes in the /etc/named.conf configuration file. (Modify allow-query line)]
****
changed: [node1]

TASK [Making changes in the /etc/named.conf configuration file.]
****
changed: [node1]

TASK [Creating forward lookup zone file using ansible jinja2 template file.]
****
changed: [node1]

TASK [Creating reverse lookup zone file using ansible jinja2 template file.]
****
changed: [node1]

TASK [Allowing DNS traffic in the firewall.]
****
changed: [node1]

TASK [Starting & enabling the DNS service.]
****
changed: [node1]

PLAY RECAP
****
node1   : ok=11 changed=10 unreachable=0 failed=0 skipped=0 rescued=0 ignored=0

[vikasnehra@ansible-server ~]$ ansible node1 -m command -a 'sudo systemctl status named'
node1 | CHANGED | rc=0 >>
● named.service - Berkeley Internet Name Domain (DNS)
   Loaded: loaded (/usr/lib/systemd/system/named.service; enabled; vendor preset: disabled)
   Active: active (running) since Fri 2023-07-28 13:06:32 IST; 23s ago
   Process: 21662 ExecStartPre=/bin/bash -c if [! "$DISABLE_ZONE_CHECKING" == "yes"]; then /usr/sbin/named-checkconf -z "$NAMEDCONF"; else echo "Checking of zone files is disabled"; fi (code=exited, status=0/SUCCESS)
   Process: 21713 ExecStart=/usr/sbin/named -u named -c ${NAMEDCONF} $OPTIONS (code=exited, status=0/SUCCESS)
  Main PID: 21750 (named)
   Tasks: 6 (limit: 10804)
   Memory: 24.5M
      CPU: 104ms
   CGroup: /system.slice/named.service
          └─21750 /usr/sbin/named -u named -c /etc/named.conf

[vikasnehra@ansible-server ~]$ nslookup www.nehraclasses.edu
Server: 192.168.229.2
Address: 192.168.229.2#53
** server can't find www.nehraclasses.edu: NXDOMAIN

[vikasnehra@ansible-server ~]$ sudo vim /etc/resolv.conf
 # Generated by NetworkManager
search localdomain nehraclasses.local
nameserver 192.168.229.129

[vikasnehra@ansible-server ~]$ nslookup www.nehraclasses.edu
Server: 192.168.229.129
Address: 192.168.229.129#53
Name: www.nehraclasses.edu
Address: 192.168.229.50

DNS Configuration Using Ansible

By: Er. Vikas Nehra (M. Tech, B. Tech), Experience: 15 + Years

```
[vikasnehra@ansible-server ~]$ nslookup mail.nehraclasses.edu
Server:        192.168.229.129
Address:       192.168.229.129#53
Name:   mail.nehraclasses.edu
Address: 192.168.229.60

[vikasnehra@ansible-server ~]$ nslookup 192.168.229.50
50.229.168.192.in-addr.arpa     name = www.nehraclasses.edu.

[vikasnehra@ansible-server ~]$ nslookup 192.168.229.60
60.229.168.192.in-addr.arpa     name = mail.nehraclasses.edu.

[vikasnehra@ansible-server ~]$ #Our Authoritative DNS Server is Working Perfectly as Expected.#
```

Thank You