OPS535 Lab 4

Purpose

In this lab, you are going to build a primary name server for your assigned DNS domain using the BIND package on your VM1 running CentOS 7. Primary name server does not depend upon having access to other name servers in order to function.

Once you have your primary name server running, use command line DNS client tool(s) to test the correctness of your Primary DNS server

Then you will configure both zones to support dynamic updates. Dynamic DNS accepts updates from the command line utility “nsupdate”. This lab does not configure the DNS server to use secure channel for the updates.

Pre-Requisites

The pre-lab must be complete so that your virtual machines share access to a private network.

Investigation 1: Primary Name Server

Perform the following steps on vm1

1. Use the skills you learned in previous courses to make your vm1 act as the primary name server for your assigned domain

    - The SOA record should contain the FQDN of your primary DNS server and the email address of the person responsible for managing your DNS domain name space.
    - The NS record(s) should contain the FQDN for your authoritative DNS server(s).
    - Each A record (address record) should contain the FQDN (or host name) of each VM and its corresponding IP address.
    - Each PTR record should contain the FQDN and the corresponding IP address in reverse dotted-decimal notation format (e.g. use 53.99.168.192.in-addr.arpa. for IP address 192.168.99.53)
    - The file for your forward zone should be my-zone.txt, and the file for the reverse zone should be rev-zone.txt.
    - Make sure you configure the following major options:
        - listen-on: port 53 and all network interface
        - directory: /var/named
        - allow-query: any
        - recursion: no
        - dnssec-enable: yes
        - dnssec-validation: no

    - dnssec-lookaside: auto
  - Ensure you service is running, will continue to run past boot, and is accessible by the other machines in your network.
2. Modify your other VMs so that they use your VM1 as their primary server, and your host as a secondary server.
3. Run the appropriate "tcpdump" command on your DNS server to capture all DNS query and response packets to a file and name the tcpdump packet file as dns-packet. While tcpdump is running on your DNS server, repeat all the DNS queries (SOA, NS, A, PTR) on your host.
   - Possible tcpdump command: `tcpdump -i eth0 host 192.168.99.53 and port 53 -w dns-packet`
   - Read the tcpdump file with the "-r" flag to verify that the targeted packets were captured to the file. It should contain queries and answers for each of the records in your domain.

Investigation 2: Dynamic DNS Updates

Perform the following steps on vm1 after you have confirmed that it is providing forward and reverse lookups of all machines in your domain.

1. Add the following line to your forward and reverse zone records

   allow-update { localhost; };

2. Ensure Verify the user owner, group owner, permissions, and SELinux contexts:

```
[root@localhost named]# ls -lZ zone*
-rw-r--r--. named named unconfined_u:object_r:named_zone_t:s0 rev-
zone.txt
-rw-r--r--. named named system_u:object_r:named_zone_t:s0 my-zone.txt
```

   Please note that the SELinux context type for both zone files should be “named_zone_t”. If it is not, you can fixed it by the command “chcon -t named_zone_t <file>”.

3. Set the SELinux boolean to allow named to have write access to your zone files.

   The directory “/var/named” should be writable by named as shown below

```
[root@localhost named]# ls -ld /var/named
drwxrwx---. 6 root named 4096 Nov 10 23:18 /var/named
```

   Check the SELinux runtime setting for named. Run the following command:

```
[root@localhost named]# getsebool -a | grep named
named_tcp_bind_http_port --> off
named_write_master_zones --> off
```

If the “named_write_master_zones” is not “on”, named will not be able to create the “journal” file to update the master zone file. If “named_write_master_zones” is “off”, run the following command to turn it on for good:

```
[root@localhost named]# setsebool -P named_write_master_zones on
```

The “-P” flag make the change permanent and will stay on after a system reboot.

Restart named. If it does not complain, go to step 4, otherwise check the system log file /var/log/messages for error messages. In addition to the debugging messages you may find in the system log file, you can also use the two utilities “named-checkconf” and “named-checkzone” to check for typos or syntax errors in named.conf or your zone files. Please consult the man page for “named-checkconf” and “named-checkzone” for details.

4. Perform dynamic DNS update with nsupdate

Run the following command(s) on your primary DNS server in order to dynamically add a new A record. Note that you will have to fill in information for your own domain

```
[root@localhost named]# nsupdate -d
> server localhost
> update add c7host.pcallagh.ops 300 A 172.16.182.1
> send
Reply from SOA query:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 42401
;; flags: qr aa; QUESTION: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0
;; QUESTION SECTION:
;c7host.pcallagh.ops. IN SOA

;; AUTHORITY SECTION:
ddns.net. 0 IN SOA vm1.pcallagh.ops. root.pcallagh.ops. 20151111 3600
900 259200 600

Found zone name: ddns.net
The master is: vm1.pcallagh.ops
Sending update to 127.0.0.1#53
Outgoing update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id: 25883
;; flags:; ZONE: 1, PREREQ: 0, UPDATE: 1, ADDITIONAL: 0
;; UPDATE SECTION:
c7host.pcallagh.ops. 300 IN A 172.16.99.10

Reply from update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id: 25883
;; flags: qr; ZONE: 1, PREREQ: 0, UPDATE: 0, ADDITIONAL: 0
;; ZONE SECTION:
ddns.net. IN SOA
```

The above “Reply from update query” section indicate that the update was successful with a “NOERROR” status.

All changes made to a zone using dynamic update are stored in the zone's journal file, in this case, the file will be in the /var/named directory and is called “<zonefile>.jnl”. This file is automatically created by the DNS server when the first dynamic update is received. Please note that the name of the journal file is formed by appending the extension “.jnl” to the name of the corresponding zone file. The journal file is in a binary format and can not be edited using a text editor.

The server will occasionally write the updates found in the journal file to its zone file or when a server is restarted after a shutdown.

Go to the /var/named directory and run the command to list the zone file and its journal file:

```
[root@localhost named]# ls -l my-zone.txt*
-rw-r--r--. 1 named named 306 Nov 10 23:59 my-zone.txt
-rw-r--r--. 1 named named 697 Nov 10 23:47 my-zone.txt.jnl
```

Use the “file” command to check the content type of the zone file and its journal file:

```
[root@localhost named]# file my-zone.txt*
my-zone.txt: ASCII text
my-zone.txt.jnl: data
```

Although you can not view the contents of the journal file using the “cat” command, the command line utility “named-journalprint” from the bind package can be used to print the contents of the journal file:

```
[root@localhost named]# named-journalprint my-zone.txt.jnl
del pcallagh.ops. 300 IN SOA vm1.pcallagh.ops. root.pcallagh.ops.
20151111 3600 900 259200 600
add ddns.net. 300 IN SOA vm1.pcallagh.ops. root.pcallagh.ops.
20151112 3600 900 259200 600
add c7host.pcallagh.ops. 300 IN A 172.16.182.1
```

Run the following command(s) to add an incorrect record to your zone (again filling in your own zone information):

```
[root@localhost named]# nsupdate -d
> server localhost
> update add 100.182.16.172.in-addr.arpa. 7200 PTR c7host.pcallagh.ops.
> send
Reply from SOA query:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 17987
;; flags: qr aa; QUESTION: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0
;; QUESTION SECTION:
100.182.16.172.in-addr.arpa. IN SOA

;; AUTHORITY SECTION:
16.172.in-addr.arpa. 0 IN SOA vm1.pcallagh.ops. root.pcallagh.ops.
20151111 3600 900 259200 600
```

```
Found zone name: 16.172.in-addr.arpa
The master is: vm1.pcallagh.ops
Sending update to 127.0.0.1#53
Outgoing update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id: 25343
;; flags:; ZONE: 1, PREREQ: 0, UPDATE: 1, ADDITIONAL: 0
;; UPDATE SECTION:
100.182.16.172.in-addr.arpa. 7200 IN PTR c7host.pcallagh.ops.

Reply from update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id: 25343
;; flags: qr; ZONE: 1, PREREQ: 0, UPDATE: 0, ADDITIONAL: 0
;; ZONE SECTION:
16.172.in-addr.arpa. IN SOA
```

Check the contents of the files “rev-zone.txt” and “rev-zone.txt.jnl”. Please note that the last octet of the IP address was missed type as “100” instead of “1”. If the contents of the zone file “rev-zone.txt” didn't get updated, restart the named service.

5. Use nsupdate to delete a record from your zones.

   Inevitably, you will need to delete information from a zone at some point. In the previous step, we deliberately added incorrect information in order to delete it in this step. If you do not have an incorrect record, go back and add one before continuing.

   First we will try to delete a record that doesn’t exist.

   Run the following command(s) on your DNS server:

```
[root@localhost named]# nsupdate -d
> server localhost
> update delete 10.182.16.172.in-addr.arpa.
> send
Reply from SOA query:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 17329
;; flags: qr aa; QUESTION: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0
;; QUESTION SECTION:
10.182.16.172.in-addr.arpa. IN SOA

;; AUTHORITY SECTION:
16.172.in-addr.arpa. 0 IN SOA vm1.pcallagh.ops. root.pcallagh.ops.
20151112 3600 900 259200 600

Found zone name: 16.172.in-addr.arpa
The master is: vm1.pcallagh.ops
Sending update to 127.0.0.1#53
Outgoing update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id: 44360
;; flags:; ZONE: 1, PREREQ: 0, UPDATE: 1, ADDITIONAL: 0
;; UPDATE SECTION:
10.182.16.172.in-addr.arpa. 0 ANY ANY

Reply from update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id: 44360
;; flags: qr; ZONE: 1, PREREQ: 0, UPDATE: 0, ADDITIONAL: 0
;; ZONE SECTION:
```

```
16.172.in-addr.arpa. IN SOA
```

There is no complaint from the update query. Check the contents of the journal file. Did the delete record get in to the journal file?

```
[root@localhost named]# named-journalprint rev-zone.txt.jnl
del 16.172.in-addr.arpa. 300 IN SOA vm1.pcallagh.ops.
root.pcallagh.ops. 20151111 3600 900 259200 600
add 16.172.in-addr.arpa. 300 IN SOA vm1.pcallagh.ops.
root.pcallagh.ops. 20151112  3600 900 259200 600
add 100.182.16.172.in-addr.arpa. 7200 IN PTR c7host.pcallagh.ops.
```

Now we will delete a record that actually does exist.

Run the following command(s) on your DNS server:

```
[root@localhost named]# nsupdate -d
> server localhost
> update delete 100.182.16.172.in-addr.arpa.
> send
Reply from SOA query:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55265
;; flags: qr aa; QUESTION: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0
;; QUESTION SECTION:
100.182.16.172.in-addr.arpa. IN SOA

;; AUTHORITY SECTION:
16.172.in-addr.arpa. 300 IN SOA vm1.pcallagh.ops. root.pcallagh.ops.
20151112 3600 900 259200 600

Found zone name: 16.172.in-addr.arpa
The master is: vm1.pcallagh.ops
Sending update to 127.0.0.1#53
Outgoing update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id: 19619
;; flags:; ZONE: 1, PREREQ: 0, UPDATE: 1, ADDITIONAL: 0
;; UPDATE SECTION:
100.182.16.172.in-addr.arpa. 0 ANY ANY

Reply from update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id: 19619
;; flags: qr; ZONE: 1, PREREQ: 0, UPDATE: 0, ADDITIONAL: 0
;; ZONE SECTION:
16.172.in-addr.arpa. IN SOA
```

Check the contents of the zone file and the journal file. Do not restart the DNS server.

The contents of the journal file should look like the following:

```
[root@localhost named]# named-journalprint rev-zone.txt.jnl
del 16.172.in-addr.arpa. 300 IN SOA vm1.pcallagh.ops.
root.pcallagh.ops. 20151111 3600 900 259200 600
add 16.172.in-addr.arpa. 300 IN SOA vm1.pcallagh.ops.
root.pcallagh.ops. 20151112 3600 900 259200 600
add 100.182.16.172.in-addr.arpa. 7200 IN PTR c7host.pcallagh.ops.
```

```
del 16.172.in-addr.arpa. 300 IN SOA vm1.pcallagh.ops.
root.pcallagh.ops. 20151112 3600 900 259200 600
del 100.182.16.172.in-addr.arpa. 7200 IN PTR c7host.pcallagh.ops.
add 16.172.in-addr.arpa. 300 IN SOA vm1.pcallagh.ops.
root.pcallagh.ops. 20151113 3600 900 259200 600
```

Study the contents of the journal file carefully. You should be able to interpret it in order to understand the changes it is making to the zone.

Completing the Lab

You should now have a server providing DNS services for your network. Many other services, and most of your users, will depend on this for translation between hostnames and addresses. You have also configured the service to allow for dynamic updates, though they are limited to the local machine only. In the extension to this lab you may continue this configuration to allow such updates to be made from another machine, though this will require some extra security setup to ensure that only approved machines may make such updates.

Follow the instructions on blackboard to submit the lab.

Exploration Questions

1. Which rpm package provides the “nsupdate” command line utility?
2. What does the “-d” option do for the “nsupdate” command?
3. Which RFC document defines the Dynamic DNS update protocol?
4. Could nsupdate send a dynamic DNS update to a DNS server using a non-standard port? (port 53 is DNS standard port number.)
5. What are the steps using nsupdate to add an “A” record for a host with FQDN “linux.ddns.net” IP address 172.16.101.90 with a TTL of 60 seconds?
6. What are the steps using nsupdate to add a 'PTR” record for the host in question 5?
7. What are the steps using nsupdate to add a “CNAME” record for “gnu.ddns.net” that points to
8. “linux.ddns.net”?
9. What are the steps using nsupdate to delete the “A” record created in question 5?
10. What are the steps using nsupdate to delete the “PTR” record created in question 6?
11. What are the steps using nsupdate to delete the “CNAME” record created in question 7?
12. What would happen if you try to delete a non-existence resource record (PTR, A, CNAME, MX, etc) from a dynamic DNS zone using nsupdate?

13. What would happen if you ry to add a duplicate resource record to a dynamic zone using nsupdate?