4.6.3. Setting up a reverse zone on a BIND primary server

Reverse zones map IP addresses to names. For example, if you are responsible for IP range 192.0.2.0/24, you can set up a reverse zone in BIND to resolve IP addresses from this range to hostnames.

**Note**

If you create a reverse zone for whole classful networks, name the zone accordingly. For example, for the class C network 192.0.2.0/24, the name of the zone is 2.0.192.in-addr.arpa. If you want to create a reverse zone for a different network size, for example 190.0.2.0/28, the name of the zone is 28-2.0.192.in-addr.arpa.

**Prerequisites**

* BIND is already configured, for example, as a caching name server.
* The named or named-chroot service is running.

**Procedure**

1. Add a zone definition to the /etc/named.conf file:
2. **zone "*2.0.192.in-addr.arpa*" {**
3. **type master;**
4. **file "*2.0.192.in-addr.arpa.zone*";**
5. **allow-query { *any;* };**
6. **allow-transfer { *none;* };**

**};**

These settings define:

* + This server as the primary server (type master) for the 2.0.192.in-addr.arpa reverse zone.
  + The /var/named/2.0.192.in-addr.arpa.zone file is the zone file. If you set a relative path, as in this example, this path is relative to the directory you set in directory in the options statement.
  + Any host can query this zone. Alternatively, specify IP ranges or BIND access control list (ACL) nicknames to limit the access.
  + No host can transfer the zone. Allow zone transfers only when you set up secondary servers and only for the IP addresses of the secondary servers.

1. Verify the syntax of the /etc/named.conf file:

# **named-checkconf**

If the command displays no output, the syntax is correct.

1. Create the /var/named/2.0.192.in-addr.arpa.zone file, for example, with the following content:
2. **$TTL *8h***
3. **@ IN SOA *ns1.example.com.* *hostmaster.example.com.* (**
4. ***2022070601*** **; serial number**
5. ***1d*** **; refresh period**
6. ***3h*** **; retry period**
7. ***3d*** **; expire time**
8. ***3h*** ) **; minimum TTL**
9. **IN NS** **ns1.example.com.**
10. **1** **IN PTR** **ns1.example.com.**

**30** **IN PTR** **www.example.com.**

This zone file:

* + Sets the default time-to-live (TTL) value for resource records to 8 hours. Without a time suffix, such as h for hour, BIND interprets the value as seconds.
  + Contains the required SOA resource record with details about the zone.
  + Sets ns1.example.com as an authoritative DNS server for this reverse zone. To be functional, a zone requires at least one name server (NS) record. However, to be compliant with RFC 1912, you require at least two name servers.
  + Sets the pointer (PTR) record for the 192.0.2.1 and 192.0.2.30 addresses.

1. Set secure permissions on the zone file that only allow the named group to read it:
2. # **chown root:named /var/named/*2.0.192.in-addr.arpa.zone***

# **chmod 640 /var/named/*2.0.192.in-addr.arpa.zone***

1. Verify the syntax of the /var/named/2.0.192.in-addr.arpa.zone file:
2. # **named-checkzone *2.0.192.in-addr.arpa* */var/named/2.0.192.in-addr.arpa.zone***
3. zone *2.0.192.in-addr.arpa/IN*: loaded serial *2022070601*

OK

1. Reload BIND:

# **systemctl reload named**

If you run BIND in a change-root environment, use the systemctl reload named-chroot command to reload the service.

**Verification**

* Query different records from the reverse zone, and verify that the output matches the records you have configured in the zone file:
* # **dig +short @*localhost* -x *192.0.2.1***
* ns1.example.com.
* # **dig +short @*localhost* -x *192.0.2.30***

www.example.com.

This example assumes that BIND runs on the same host and responds to queries on the localhost interface.

<https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/deploying_different_types_of_servers/assembly_setting-up-and-configuring-a-bind-dns-server_deploying-different-types-of-servers>