

Creating Forward Lookup Zones

LPIC-2: Linux Engineer (202-450)

Objectives:

At the end of this episode, I will be able to:

1. Describe the function of a forward lookup zone.
2. Create and enable a forward lookup zone in BIND.
3. Create A, AAAA, MX, NS, and CNAME records in a zone.

Additional resources used during the episode can be obtained using the download link on the overview episode.

- Forward Lookup Zones
 - Contain DNS records for a domain
 - Makes the DNS server authoritative for the domain
 - Can be public or private
 - Public requires use of a registrar
- Zone files
 - Usually there are none by default
 - File extensions (not required)
 - Creating a zone file
 - `sudoedit /etc/bind/lab.itpro.tv.dns`
- Required Records
 1. TTL
 2. SOA
 3. NS
- Time to live
 - Defines the default time a record is allowed to be cached
 - Standard is 7 days
 - Defined in seconds
 - `$TTL 604800`
- Start of authority
 - Contains administrative info for the zone
 - `@ IN SOA dns1.lab.itpro.tv. admin.lab.itpro.tv. (`
 - `1; Serial Number`
 - `86400; DNS Secondary Refresh Interval`
 - `7200; DNS Secondary Retry Interval`
 - `57600; DNS Secondary Expire Interval`
 - `3600); Domain Cache TTL`
- Name server records
 - Define authoritative DNS servers for the zone
 - `@ IN NS dns1.lab.itpro.tv.`
- Host records
 - Identify resources on the network
 - `dns1 IN A 10.0.222.51`
 - `@ IN A 10.0.222.100`
 - `webserv01 IN A 10.0.222.100`
 - `IN AAAA 2001:1234::ABCD:1`
 - `mail1 IN A 10.0.222.101`
 - `mail1 IN A 10.0.222.102`
 - `mail2 IN A 10.0.222.103`
 - `www IN CNAME webserv01.lab.itpro.tv.`
 - `@ IN MX 10 mail1.lab.itpro.tv.`

- @ IN MX 20 mail2.lab.itpro.tv.
- Activating a Zone
 - Zone files must be defined in *named*'s config
 - `sudoedit /etc/bind/named.conf.local`
 - Add to the bottom
 - `zone "lab.itpro.tv" IN { type master; file "/etc/bind/lab.itpro.tv.dns"; };`
 - BIND only reads config files when it starts
 - Verify the config before restarting
 - `named-checkzone lab.itpro.tv /etc/bind/lab.itpro.tv.dns`
- Restart BIND
 - When adding new zones
 - `sudo rndc reconfig`
 - When modifying a zone
 - `sudo rndc reload lab.itpro.tv`
 - Full restart
 - `systemctl restart named.service`

Example Forward Lookup Zone

```
$TTL 604800
@ IN SOA dns1.lab.itpro.tv. admin.lab.itpro.tv. (
    1      ; Serial
    86400 ; Refresh
    7200  ; Retry
    57600 ; Expire
    3600) ; Negative Cache TTL

lab.itpro.tv. IN NS      dns1.lab.itpro.tv.

dns1          IN A        10.0.222.51
websrv01      IN A        10.0.222.100
              IN AAAA    2001:1234::ABCD:1
@             IN A        10.0.222.100
*            IN A        10.0.222.100
mail1        IN A        10.0.222.101
mail1        IN A        10.0.222.102
mail2        IN A        10.0.222.103
www          IN CNAME   websrv01.lab.itpro.tv.
@            IN MX      10 mail1.lab.itpro.tv.
@            IN MX      20 mail2.lab.itpro.tv.
```