

DNS and BIND Deep Dive

Course Navigation

Introduction

Section 1

DNS Fundamentals

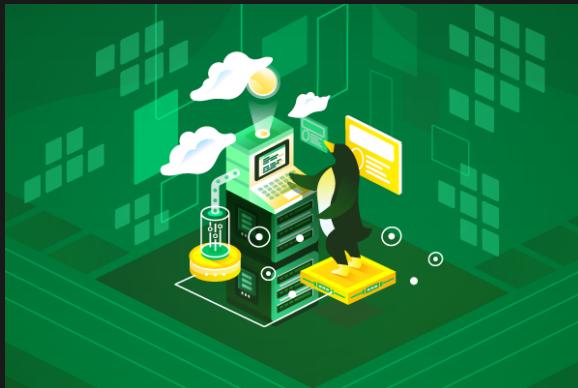
Section 2

DNS Configuration

Section 3

DNS Server Security

Section 4



Linux Academy

Course Navigation

Introduction

Section 1

Getting Started

Course Introduction

About the Training Architect

How to Use the Cloud Playground for This Course

DNS Fundamentals

Section 2

DNS Configuration

Section 3

DNS Server Security

Section 4

Select one of the items below to get started:

[Course Introduction](#)

[About the Training Architect](#)

[How to Use the Cloud Playground for This Course](#)

Next

[Back to Main](#)

[Next Section](#)



Linux Academy

Introduction

Getting Started

Course Navigation

Introduction

Section 1

Getting Started

Course Introduction

About the Training Architect

How to Use the Cloud Playground for This Course

DNS Fundamentals

Section 2

DNS Configuration

Section 3

DNS Server Security

Section 4



Dear Students.

Welcome to the Linux Academy **DNS and BIND Deep Dive** course. This course is intended for students with a good understanding of the Linux operating system. Students should be able to perform tasks such as running basic commands, editing text files, moving around in the filesystem structure, and installing packages. Students should also have some basic configuration skills.

This is a deep dive course and will cover the components of BIND as well as basic and advanced DNS configuration. We will also discuss configurations for added security. I will be using Red Hat Enterprise Linux 7 for all demonstrations.

Thank you for taking this course from Linux Academy. Let's get started!

Cara Nolte
Linux Training Architect

Back

[Back to Main](#)

[Next Section](#)



Linux Academy

Course Navigation

Introduction

Section 1

Getting Started

Course Introduction

About the Training Architect

How to Use the Cloud
Playground for This
Course

DNS Fundamentals

Section 2

DNS Configuration

Section 3

DNS Server Security

Section 4

About the Training Architect



Cara Nolte

Linux Training Architect

- Red Hat Certified Engineer
(RHCE)
- Almost **20 years** of experience
in Information Technology
- Previous Experience Includes:
 - **Sys Admin**
 - **Sys Eng**
 - **PM**
 - **TAM**
 - **TA**

Back

[Back to Main](#)

[Next Section](#)



Linux Academy

Introduction

Section 1

Getting Started

Course Introduction

About the Training Architect

How to Use the Cloud Playground for This Course

DNS Fundamentals

Section 2

DNS Configuration

Section 3

DNS Server Security

Section 4

How to Use the Cloud Playground for This Course



- The **Cloud Playground** is a feature that is available with your subscription. It's a hands-on environment that will help you learn more effectively. You will want to use the Cloud Playground to get the most out of your learning experience. It isn't just for following along in courses. You can set up real **Linux** servers and try things out. Please utilize them.
- The Cloud Playground servers do not allow root logins. You can access the root shell by using the command `sudo -i`. If the instructor is running commands using the root user, you must run `sudo -i` first in order to follow along, or you will receive a permissions error.
- To access the **Graphical User Interface** (for distributions with this feature), from the server configuration drop down, select *Actions & Graphical Shell*. Please be aware that you cannot access the GUI with a VNC client as port 5901 is blocked.

[Back](#)

[Back to Main](#)

[Next Section](#)



Linux Academy

DNS Fundamentals

Introduction to DNS and BIND

Course Navigation

Introduction

Section 1

DNS Fundamentals

Section 2

Introduction to DNS and BIND

DNS Types Overview

DNS Concepts - Terms and Definitions

Zones and Domains

DNS Configuration

Section 3

DNS Server Security

Section 4

Select on the items below to an introduction to DNS and BIND:

DNS Types Overview

DNS Concepts - Terms and Definitions

Zones and Domains

Next

[Back to Main](#)

[Next Section](#)



Linux Academy

Introduction

Section 1

DNS Fundamentals

Section 2

Introduction to DNS and BIND**DNS Types Overview**

DNS Concepts - Terms and Definitions

Zones and Domains

DNS Configuration

Section 3

DNS Server Security

Section 4

DNS - Domain Name System

The **Domain Name System**, or **DNS**, is a hierarchical name service that acts as a directory for networked hosts and resources. In addition to mapping names to IP addresses, the DNS also maps other data which is stored in resource records.

BIND - Berkeley Internet Name Domain

BIND, or **Berkeley Internet Name Domain** is the most commonly used **DNS** service on the Internet, and is the de facto standard on Unix-like operating systems.

**Types of Name Servers****Authoritative Name Server**

An **authoritative name server** is one that is configured to answer queries using its own data without needing to query other servers. This category also includes **primary and secondary name servers**, which are also known as master and slave name servers.

Recursive Name Server**Non-Authoritative Name Server or Caching Name Server**

These offer resolution services, but they are not authoritative. This means that the name server will start an iterative process called recursion. It will query servers listed in the `/etc/resolv.conf` file, in order, until it gets an answer or runs out of servers. It will then store responses received, (following the referrals from authoritative servers) in memory and reuse them in order to **reduce network traffic and improve system performance**.

Back**Back to Main****Next Section****Linux Academy**

DNS Fundamentals

DNS Concepts - Terms and Definitions

Course Navigation

Introduction

Section 1

DNS Fundamentals

Section 2

Introduction to DNS and BIND

DNS Types Overview

DNS Concepts - Terms and Definitions

Zones and Domains

DNS Configuration

Section 3

DNS Server Security

Section 4

Configuration

/etc/resolv.conf

The resolver configuration file used to configure a DNS server

/etc/named.conf

The main configuration file for BIND

Definitions

Zone File

Zone files contain the zone records for a domain or sub-domain.

Forward DNS Lookup

This returns the IP address for any given name.

Reverse DNS Lookup

Returns the name for any given IP address.

Domain

Any tree or subtree within a domain namespace.

Records

Records are used to **map an IP address to a hostname**, as well as other data. There are many record types including the following:

- **A** (address record): this is the most basic record type and points a domain to an IP address
- **NS** (name server): Identifies the authoritative DNS server for a zone
- **MX** (mail exchanger): Specifies a mail server for the zone
- **CN** (canonical name): Specifies an alias for another name
- **PTR** (pointer): A reverse DNS record, resolving an IP to a fully qualified host name
- **SOA** (start of authority): Stores information about DNS zones and zone records

Back

Back to Main

Next Section



Linux Academy

DNS Fundamentals

Zones and Domains

Course Navigation

Introduction

Section 1

DNS Fundamentals

Section 2

Introduction to DNS and BIND

DNS Types Overview

DNS Concepts - Terms and Definitions

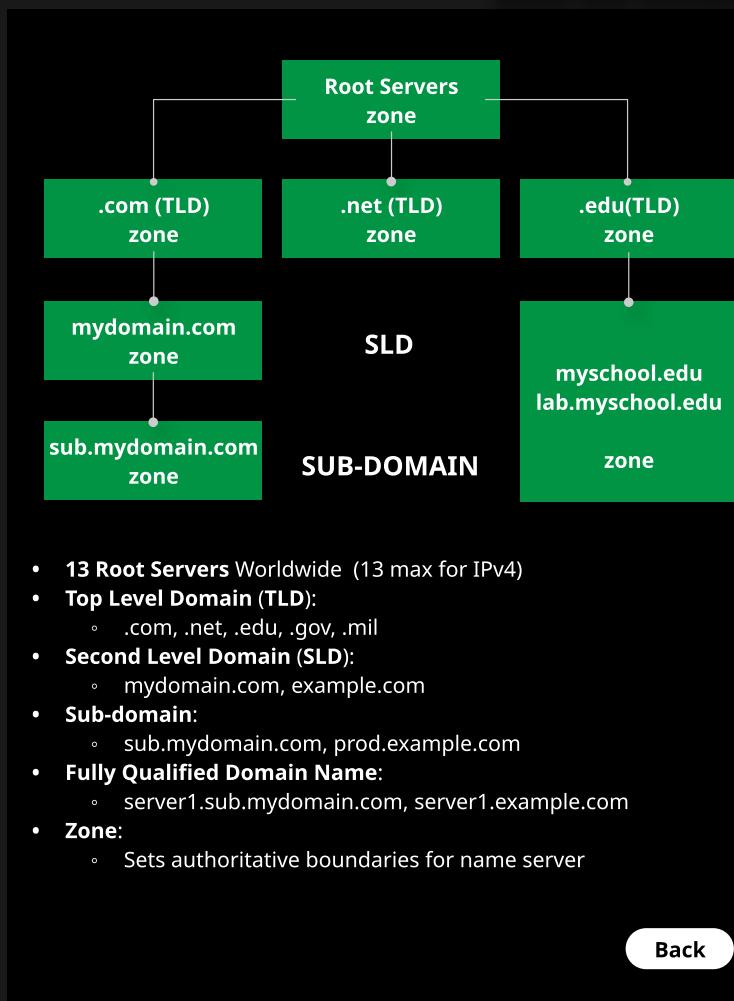
Zones and Domains

DNS Configuration

Section 3

DNS Server Security

Section 4



Back

[Back to Main](#)

[Next Section](#)



Linux Academy

DNS Configuration

Basic DNS Server Configuration

DNS Configuration

Section 3

Basic DNS Server Configuration

- DNS Configuration
- Configure a Caching Name Server
- Named Service and RNDC Keys
- RNDC Configuration
- Using the dig Command
- DNS and BIND: Create a Caching Name Server
- DNS and BIND: Working with RNDC Keys
- Working with DNS Zones
- Configuring for Zones
- Zone Files and Record Types - Start of Authority
- Zone Files and Record Types - Common Record Types
- Zone File Validity
- Creating Reverse Zone Files
- Hosing Multiple Domains
- Multiple Master DNS Servers
- DNS Master and Replication Slave

DNS Server Security

Section 4

Select the items below to review a basic DNS server configuration:

DNS Configuration

Configure a Caching Name Server

Named Service and RNDC Keys

RNDC Configuration

Using the dig Command

Next

DNS Configuration

DNS Configuration

Course Navigation

DNS Configuration

Section 3

Basic DNS Server Configuration

DNS Configuration

Configure a Caching Name Server

Named Service and RNDC Keys

RNDC Configuration

Using the dig Command

DNS and BIND: Create a Caching Name Server

DNS and BIND: Working with RNDC Keys

Working with DNS Zones

Configuring for Zones

Zone Files and Record Types - Start of Authority

Zone Files and Record Types - Common Record Types

Zone File Validity

Creating Reverse Zone Files

Hosing Multiple Domains

Multiple Master DNS Servers

DNS Master and Replication Slave

DNS Server Security

Section 4

Basic DNS Configuration

\$ yum provides nslookup

The provides option will list all of the packages in all of the configured repos that contain nslookup.

\$ yum install bind-utils -y

Install the bind-utils package

\$ cat /etc/resolv.conf

This resolver configuration file used to configure a DNS server.

Primary file to configure your server to translate names to routable IPs.



\$ nslookup www

This is a non-qualified query, as no domain is specified. It will search the domains specified in the /etc/resolv.conf file.

\$ nslookup www.google.com

This is a fully-qualified domain name and will search the dns servers specified in the /etc/resolv.conf file and then follow the recommendations from the queried servers all the way to the root servers.

\$ cat /var/named/named.ca

This is the configuration file that contains the list of root servers. You will not edit this file. The file is configured with updates from the package.

Back

Back to Main



Linux Academy

DNS Configuration

Section 3

Basic DNS Server Configuration

DNS Configuration

Configure a Caching Name Server

Named Service and RNDC Keys

RNDC Configuration

Using the dig Command

DNS and BIND: Create a Caching Name Server

DNS and BIND: Working with RNDC Keys

Working with DNS Zones

Configuring for Zones

Zone Files and Record Types - Start of Authority

Zone Files and Record Types - Common Record Types

Zone File Validity

Creating Reverse Zone Files

Hosing Multiple Domains

Multiple Master DNS Servers

DNS Master and Replication Slave

DNS Server Security

Section 4

[Back to Main](#)

DNS Configuration

Configure Caching Name Server

```
// named.conf
//
options {
    listen-on port 53 { 127.0.0.1; };
    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";
    recursing-file "/var/named/data/named.recurse";
    secopts-file  "/var/named/data/named.secopts";
    allow-query { localhost; };

/*
    - If you are building an AUTHORITATIVE DNS server, do NOT enable recursion.
    - If you are building a RECURSIVE (caching) DNS server, you need to enable recursion.
    - If your recursive DNS server has a public IP address, you MUST enable access control to limit queries to your legitimate users. Failing to do so will cause your server to become part of large-scale DNS amplification attacks. Implementing BCP38 within your network would greatly reduce such an attack surface.
*/
recursion yes;
dnssec-enable yes;
dnssec-validation yes;
/* Path to ISC DLV key */
bindkeys-file "/etc/named.root.key";
managed-keys-directory "/var/named/dynamic";
pid-file "/run/named/named.pid";
session-keyfile "/run/named/session.key";
};

logging {
    channel default_debug {
        file "data/named.run";
        severity dynamic;
    };
};
zone "." IN {
    type hint;
    file "named.ca";
};
include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
}

"/etc/named.conf"
```



named.conf

[Back](#)



Linux Academy

DNS Configuration

Named Service and RNDC Keys

DNS Configuration

Section 3

Basic DNS Server Configuration

[DNS Configuration](#)[Configure a Caching Name Server](#)[Named Service and RNDC Keys](#)[RNDC Configuration](#)[Using the dig Command](#)[DNS and BIND: Create a Caching Name Server](#)[DNS and BIND: Working with RNDC Keys](#)[Working with DNS Zones](#)[Configuring for Zones](#)[Zone Files and Record Types - Start of Authority](#)[Zone Files and Record Types - Common Record Types](#)[Zone File Validity](#)[Creating Reverse Zone Files](#)[Hosing Multiple Domains](#)[Multiple Master DNS Servers](#)[DNS Master and Replication Slave](#)

DNS Server Security

Section 4

RNDC

BIND includes the **rndc** utility which, allows control of the name server. The **rndc** utility connects to the name server over port 53, sending commands authenticated with digital signatures.



RNDC Auto Key Generation

\$systemctl start named

- Start the named service. This will automatically create the `/etc/rndc.key` file and attach it to the configuration.

\$systemctl enable named

- Enable the service so it is persistent upon reboot. A symbolic link to the service will be copied to the startup directory.

\$cat /etc/rndc.key

- Verify that the key was created and there is hashed MD5 data in the key file.

[Back](#)[Back to Main](#)

Linux Academy

DNS Configuration

Section 3

Basic DNS Server Configuration

DNS Configuration

Configure a Caching Name Server

Named Service and RNDC Keys

RNDC Configuration

Using the dig Command

DNS and BIND: Create a Caching Name Server

DNS and BIND: Working with RNDC Keys

Working with DNS Zones

Configuring for Zones

Zone Files and Record Types - Start of Authority

Zone Files and Record Types - Common Record Types

Zone File Validity

Creating Reverse Zone Files

Hosing Multiple Domains

Multiple Master DNS Servers

DNS Master and Replication Slave

DNS Server Security

Section 4

RNDC Manual Key Generation

\$rm /etc/rndc.key

Remove the auto-generated key file.

\$rndc reload

Reload the configuration. This command results in error because there is no key file or configuration.

\$systemctl stop named

Stop the named service.

\$rndc-confgen -r /dev/urandom > /etc/rndc.conf

Creates a key file and the configuration file for the key.

\$cat /etc/rndc.conf

Copy the section regarding using the key in the **named.conf** file and paste into **/etc/named.conf**, before the **Include** statement, and uncomment the section.

\$chgrp named /etc/rndc.conf

Change the group of the file to named.

\$chmod 640 /etc/rndc.conf

Change the permissions to remove read access from Other.

\$systemctl start named

Start named.

\$rndc reload

You will get an error stating there is a configuration file and a key, so the default is to use the configuration file. To remove this message, simply remove the **rndc.key** file and reload the configuration.

Back

Back to Main



Linux Academy

DNS Configuration

Section 3

Basic DNS Server Configuration

DNS Configuration

Configure a Caching Name Server

Named Service and RNDC Keys

RNDC Configuration

Using the **dig** Command

DNS and BIND: Create a Caching Name Server

DNS and BIND: Working with RNDC Keys

Working with DNS Zones

Configuring for Zones

Zone Files and Record Types - Start of Authority

Zone Files and Record Types - Common Record Types

Zone File Validity

Creating Reverse Zone Files

Hosing Multiple Domains

Multiple Master DNS Servers

DNS Master and Replication Slave

DNS Server Security

Section 4

Using the **dig** Command

The **dig** (Domain Information Groper) utility was developed by BIND to query name servers. The **dig** command will enable you to perform any DNS query, most commonly:

- A (Address Record)
- NS (Name Server)
- MX (Mail Exchange)
- CN (Canonical Name or Alias)



The Name Resolution Process

1. DNS client **queries the resolver** for the google.com address.
2. The resolver queries the **root server** for www.google.com.
3. The root server refers your resolver to the **.com Top-Level Domain (TLD)** authoritative server.
4. Your resolver queries the .com TLD authoritative server for www.google.com.
5. The .com TLD authoritative server refers your resolver to the authoritative servers for the google.com domain.
6. Your resolver queries the authoritative servers for www.google.com and receives the IP address as the answer.
7. Your resolver caches the answer for the duration of the **time-to-live (TTL)** specified on the record, and the answer is returned it to you.

Back

Back to Main



Linux Academy

DNS Configuration

Section 3

Basic DNS Server Configuration

[DNS Configuration](#)[Configure a Caching Name Server](#)[Named Service and RNDC Keys](#)[RNDC Configuration](#)[Using the dig Command](#)

DNS and BIND: Create a Caching Name Server

[DNS and BIND: Working with RNDC Keys](#)[Working with DNS Zones](#)[Configuring for Zones](#)[Zone Files and Record Types - Start of Authority](#)[Zone Files and Record Types - Common Record Types](#)[Zone File Validity](#)[Creating Reverse Zone Files](#)[Hosing Multiple Domains](#)[Multiple Master DNS Servers](#)[DNS Master and Replication Slave](#)

DNS Server Security

Section 4

DNS Configuration

DNS and BIND: Create a Caching Name Server

Select the items below to review DNS zones:

[DNS and BIND: Working with RNDC Keys](#)[Working with DNS Zones](#)[Configuring for Zones](#)[Zone Files and Record Types - Start of Authority](#)[Zone Files and Record Types - Common Record Types](#)[Creating Forward Zone Files](#)[Next](#)[Back to Main](#)

Linux Academy

DNS Configuration

Section 3

Basic DNS Server Configuration

[DNS Configuration](#)[Configure a Caching Name Server](#)[Named Service and RNDC Keys](#)[RNDC Configuration](#)[Using the dig Command](#)

DNS and BIND: Create a Caching Name Server

DNS and BIND: Working with RNDC Keys

[Working with DNS Zones](#)[Configuring for Zones](#)[Zone Files and Record Types - Start of Authority](#)[Zone Files and Record Types - Common Record Types](#)[Zone File Validity](#)

Creating Reverse Zone Files

[Hosing Multiple Domains](#)[Multiple Master DNS Servers](#)[DNS Master and Replication Slave](#)

DNS Server Security

Section 4

named.conf

```
zone "mylabserver.com" {  
    type master;  
    file "fwd.mylabserver.com.db";  
};
```

```
zone "xx.xx.xxx.in-addr.arpa" {  
    type master;  
    file "xx.xx.xxx.db";  
};
```

[Back](#)[Back to Main](#)

Linux Academy

DNS Configuration

Section 3

Basic DNS Server Configuration

DNS Configuration

Configure a Caching Name Server

Named Service and RNDC Keys

RNDC Configuration

Using the dig Command

DNS and BIND: Create a Caching Name Server

DNS and BIND: Working with RNDC Keys

Working with DNS Zones

Configuring for Zones

Zone Files and Record Types - Start of Authority

Zone Files and Record Types - Common Record Types

Zone File Validity

Creating Reverse Zone Files

Hosing Multiple Domains

Multiple Master DNS Servers

DNS Master and Replication Slave

DNS Server Security

Section 4

zone

Start of Authority (SOA) Record

```
@ttl 86400
```

```
@ IN SOA nameserv.mylabserver.com.  
root.mylabserver.com. (  
    000001      ; serial number  
    172800      ; refresh  
    900         ; update retry  
    1209600     ; expiry  
    86400       ; min TTL
```

[Back to Main](#)



Linux Academy

DNS Configuration

Section 3

Basic DNS Server Configuration

DNS Configuration

Configure a Caching Name Server

Named Service and RNDC Keys

RNDC Configuration

Using the dig Command

DNS and BIND: Create a Caching Name Server

DNS and BIND: Working with RNDC Keys

Working with DNS Zones

Configuring for Zones

Zone Files and Record Types - Start of Authority

Zone Files and Record Types - Common Record Types

Zone File Validity

Creating Reverse Zone Files

Hosting Multiple Domains

Multiple Master DNS Servers

DNS Master and Replication Slave

DNS Server Security

Section 4

Back

Back to Main



Linux Academy

DNS Configuration

Section 3

Basic DNS Server Configuration

DNS Configuration

Configure a Caching Name Server

Named Service and RNDC Keys

RNDC Configuration

Using the dig Command

DNS and BIND: Create a Caching Name Server

DNS and BIND: Working with RNDC Keys

Working with DNS Zones

Configuring for Zones

Zone Files and Record Types - Start of Authority

Zone Files and Record Types - Common Record Types

Zone File Validity

Creating Reverse Zone Files

Hosting Multiple Domains

Multiple Master DNS Servers

DNS Master and Replication Slave

DNS Server Security

Section 4

DNS Configuration

Zone Files and Record Types - Start of Authority

Forward

namserver.mylabserver.com xxx.xx.xx

zone

```
@ttl 86400
@ IN SOA nameserver.mylabserver.com.
root.mylabserver.com. (
    000001      ; serial number
    172800      ; refresh
    900         ; update retry
    1209600     ; expiry
)
; name server
@           IN NS nameserver.mylabserver.com.
; host records
nameserver   IN A  xxx.xx.xx
mailserver   IN A  xxx.xx.xx
mailbackup   IN A  xxx.xx.xx
```

Back

Back to Main



Linux Academy

DNS Configuration

Section 3

Basic DNS Server Configuration

DNS Configuration

Configure a Caching Name Server

Named Service and RNDC Keys

RNDC Configuration

Using the dig Command

DNS and BIND: Create a Caching Name Server

DNS and BIND: Working with RNDC Keys

Working with DNS Zones

Configuring for Zones

Zone Files and Record Types - Start of Authority

Zone Files and Record Types - Common Record Types

Zone File Validity

Creating Reverse Zone Files

Hosing Multiple Domains

Multiple Master DNS Servers

DNS Master and Replication Slave

DNS Server Security

Section 4

DNS Configuration

Zone Files and Record Types - Common Record Types

nameserver.mylabserver.com

Reverse

xxx.xx.xx

zone

```
@ IN SOA nameserver.mylabserver.com.  
root.mylabserver.com. (  
    000001 ; serial number  
    172800 ; refresh  
    900 ; update retry  
    1209600 ; expiry  
    86400 ; min TTL  
; name server  
@ IN NS nameserver.mylabserver.com.  
; pointer records  
xx IN PTR nameserver.mylabserver.com.  
xx IN PTR mailprod.mylabserver.com.  
xx IN PTR mailbackup.mylabserver.com.
```

Back

Back to Main



Linux Academy

DNS Configuration

Section 3

Basic DNS Server Configuration

DNS Configuration

Configure a Caching Name Server

Named Service and RNDC Keys

RNDC Configuration

Using the dig Command

DNS and BIND: Create a Caching Name Server

DNS and BIND: Working with RNDC Keys

Working with DNS Zones

Configuring for Zones

Zone Files and Record Types - Start of Authority

Zone Files and Record Types - Common Record Types

Zone File Validity

Creating Reverse Zone Files

Hosting Multiple Domains

Multiple Master DNS Servers

DNS Master and Replication Slave

DNS Server Security

Section 4

zone

named-checkconf

named-checkzone {zonename} {filename}



Back to Main

Back



Linux Academy

DNS Configuration

Advanced DNS Configuration

DNS Configuration

Section 3

Basic DNS Server Configuration

[DNS Configuration](#)[Configure a Caching Name Server](#)[Named Service and RNDC Keys](#)[RNDC Configuration](#)[Using the dig Command](#)

DNS and BIND: Create a Caching Name Server

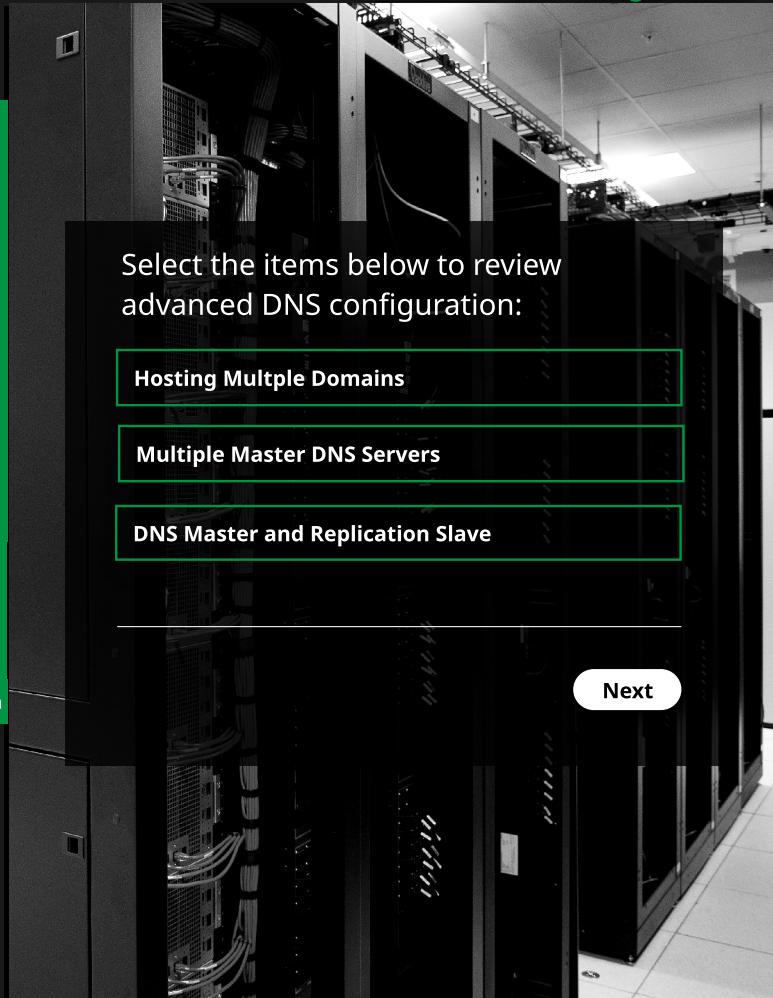
[DNS and BIND: Working with RNDC Keys](#)[Working with DNS Zones](#)[Configuring for Zones](#)[Zone Files and Record Types - Start of Authority](#)[Zone Files and Record Types - Common Record Types](#)[Zone File Validity](#)

Advanced DNS Configuration

[Hosing Multile Domains](#)[Multiple Master DNS Servers](#)[DNS Master and Replication Slave](#)

DNS Server Security

Section 4



Select the items below to review advanced DNS configuration:

[Hosting Multiple Domains](#)[Multiple Master DNS Servers](#)[DNS Master and Replication Slave](#)[Next](#)[Back to Main](#)**Linux Academy**

DNS Configuration

Hosting Multiple Domains

DNS Configuration

Section 3

Basic DNS Server Configuration

- DNS Configuration
- Configure a Caching Name Server
- Named Service and RNDC Keys
- RNDC Configuration
- Using the dig Command
- DNS and BIND: Create a Caching Name Server**
- DNS and BIND: Working with RNDC Keys
- Working with DNS Zones
- Configuring for Zones
- Zone Files and Record Types - Start of Authority
- Zone Files and Record Types - Common Record Types
- Zone File Validity

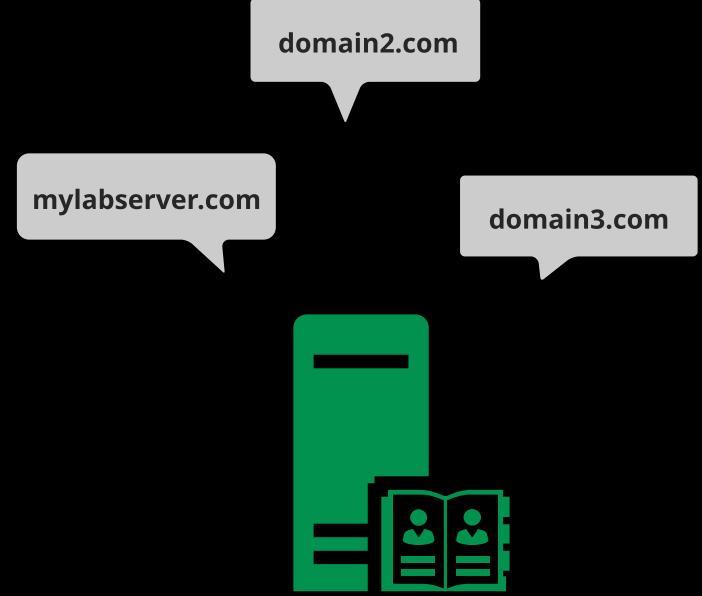
Advanced DNS Configuration

Hosting Multiple Domains

- Multiple Master DNS Servers
- DNS Master and Replication Slave

DNS Server Security

Section 4



mylabserver.com

domain2.com

domain3.com



Name Server

DNS Configuration

Multiple Master DNS Servers

DNS Configuration

Section 3

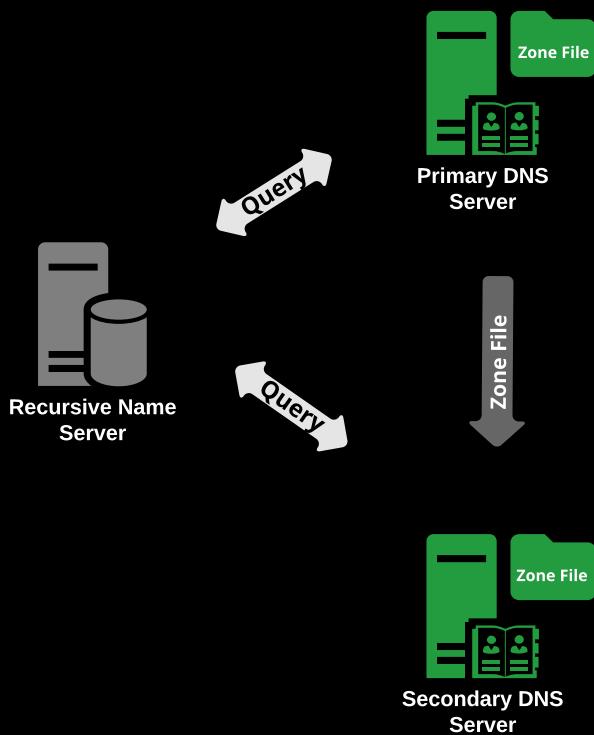
Basic DNS Server Configuration

- DNS Configuration
- Configure a Caching Name Server
- Named Service and RNDC Keys
- RNDC Configuration
- Using the dig Command
- DNS and BIND: Create a Caching Name Server**
- DNS and BIND: Working with RNDC Keys
- Working with DNS Zones
- Configuring for Zones
- Zone Files and Record Types - Start of Authority
- Zone Files and Record Types - Common Record Types
- Zone File Validity
- Advanced DNS Configuration**
- Hosting Multiple Domains
- Multiple Master DNS Servers**

DNS Master and Replication Slave

DNS Server Security

Section 4



DNS Configuration

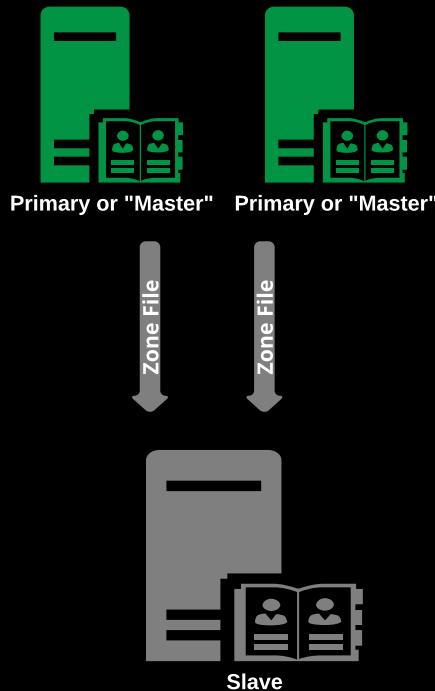
DNS Master and Replication Slave

DNS Configuration

Section 3

Basic DNS Server Configuration

- DNS Configuration
 - Configure a Caching Name Server
 - Named Service and RNDC Keys
 - RNDC Configuration
 - Using the dig Command
 - DNS and BIND: Create a Caching Name Server**
 - DNS and BIND: Working with RNDC Keys
 - Working with DNS Zones
 - Configuring for Zones
 - Zone Files and Record Types - Start of Authority
 - Zone Files and Record Types - Common Record Types
 - Zone File Validity
- #### Advanced DNS Configuration
- Hosting Multiple Domains
 - Multiple Master DNS Servers
 - DNS Master and Replication Slave**



DNS Server Security

Section 4

[Back to Main](#)

Linux Academy

DNS Server Security

Securing a DNS Server

Course Navigation

Introduction

Section 1

DNS Fundamentals

Section 2

DNS Configuration

Section 3

DNS Server Security

Section 4

Securing a DNS Server

Split DNS Configuration for Security

Running BIND in a Chroot Jail

DNS Security Tools - Keys and Signing a Zone File

DANE and TLSA Records

Final Steps

What's Next?

Select the items below to review securing a DNS server:

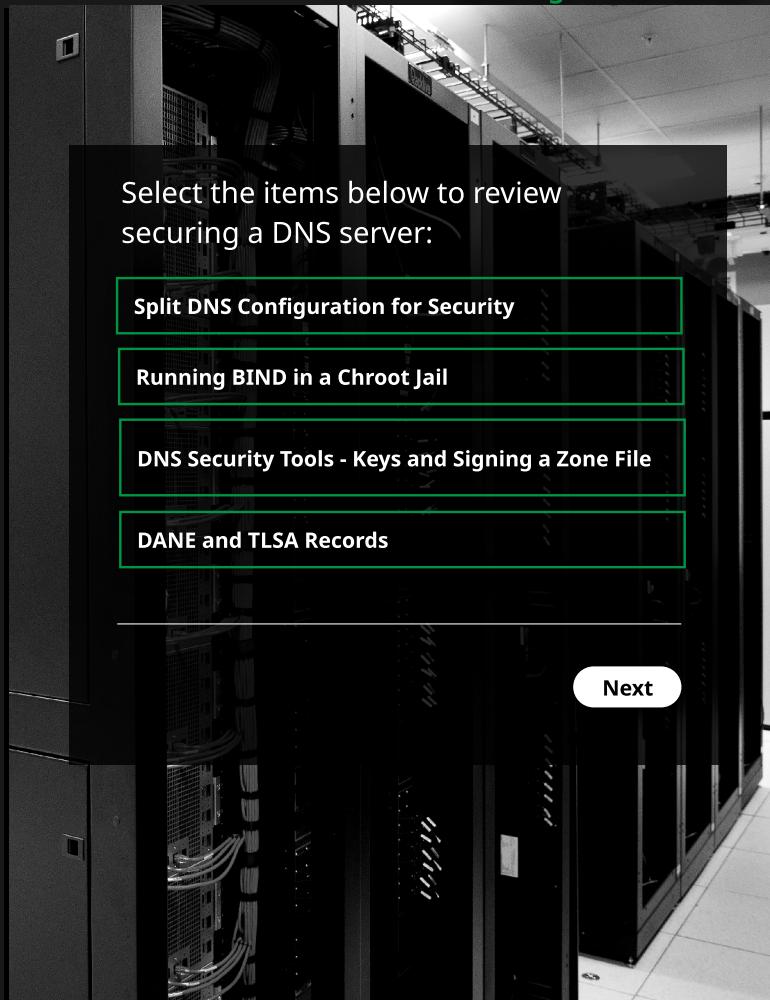
Split DNS Configuration for Security

Running BIND in a Chroot Jail

DNS Security Tools - Keys and Signing a Zone File

DANE and TLSA Records

Next



[Back to Main](#)



Linux Academy

Introduction

Section 1

DNS Fundamentals

Section 2

DNS Configuration

Section 3

DNS Server Security

Section 4

Securing a DNS Server**Split DNS Configuration for Security**

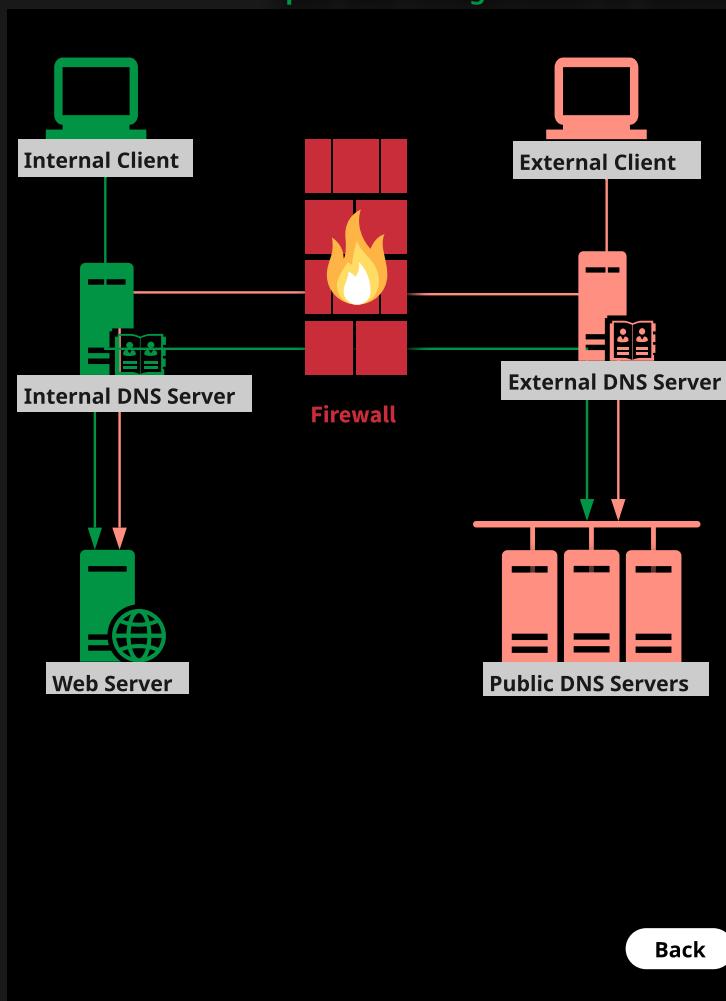
Running BIND in a Chroot Jail

DNS Security Tools - Keys and Signing a Zone File

DANE and TLSA Records

Final Steps

What's Next?

**Back****Back to Main****Linux Academy**

Introduction

Section 1

DNS Fundamentals

Section 2

DNS Configuration

Section 3

DNS Server Security

Section 4

Securing a DNS Server

Split DNS Configuration for Security

Running BIND in a Chroot Jail

DNS Security Tools - Keys and Signing a Zone File

DANE and TLSA Records

Final Steps

What's Next?



```
$ mkdir /chroot  
$ mkdir -p /chroot/named  
$ mkdir -p /chroot/named/dev  
$ mkdir -p /chroot/named/etc  
$ mkdir -p /chroot/named/var/named/  
$ mkdir -p /chroot/named/var/run
```

Introduction

Section 1

DNS Fundamentals

Section 2

DNS Configuration

Section 3

DNS Server Security

Section 4

Securing a DNS Server

Split DNS Configuration for Security

Running BIND in a Chroot Jail

DNS Security Tools - Keys and Signing a Zone File

DANE and TLSA Records

Final Steps

What's Next?

DNS Server Security

DNS Security Tools - Keys and Signing a Zone File

`named.conf`

```
zone "mylabserver.com" {  
    type master;  
    file "fwd.mylabserver.com.db.signed";  
};
```

Back

Back to Main



Linux Academy

Introduction

Section 1

DNS Fundamentals

Section 2

DNS Configuration

Section 3

DNS Server Security

Section 4

Securing a DNS Server

Split DNS Configuration for Security

Running BIND in a Chroot Jail

DNS Security Tools - Keys and Signing a Zone File

DANE and TLSA Records

Final Steps

What's Next?

DNS-based Authentication of Named Entities (DANE)

TLSA Record

_443._tcp.dane.mylabserver.com. IN TLSA 3 1 1
0d6fce3320315023ff499a3f3de1c362c88f8380311ac
8c036890dab13243aa7

Back

Back to Main



Linux Academy

DNS Server Security

Final Steps

Course Navigation

Introduction

Section 1

DNS Fundamentals

Section 2

DNS Configuration

Section 3

DNS Server Security

Section 4

Securing a DNS Server

Split DNS Configuration for Security

Running BIND in a Chroot Jail

DNS Security Tools - Keys and Signing a Zone File

DANE and TLSA Records

Final Steps

What's Next?

Select the items below to review the final steps:

What's Next?

Back

Back to Main



Linux Academy

Introduction

Section 1

DNS Fundamentals

Section 2

DNS Configuration

Section 3

DNS Server Security

Section 4

Securing a DNS Server

Split DNS Configuration for Security

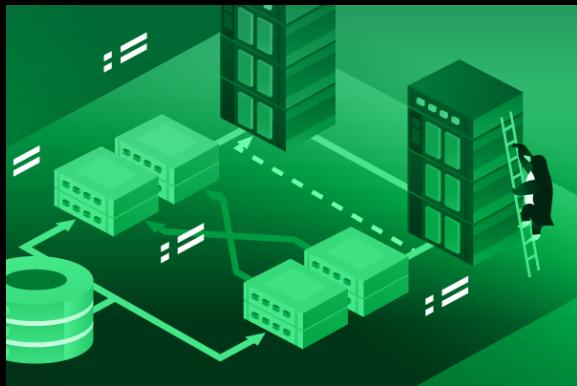
Running BIND in a Chroot Jail

DNS Security Tools - Keys and Signing a Zone File

DANE and TLSA Records

Final Steps

[What's Next?](#)



Linux Certification Prep Courses

Red Hat Certified Systems Administrator - RHCSA (EX200) Exam Prep

Red Hat Certified Engineer (RHCE) Prep Course (EX300)

Linux Foundation Certified SysAdmin (LFCS)

Linux Foundation Certified Engineer

LPIC-1 (Linux Professional Institute Certification) System Administrator Exam Prep for 101 and 102 Exams

LPIC-2 (Linux Professional Institute Certification) Linux Engineer Exam Prep for 201 and 202 Exams

Security Courses

Red Hat Certified Specialist in Security Exam Prep

Beginner Cloud Courses

Serverless Concepts

CompTIA's Cloud Essentials

[Back](#)

[Back to Main](#)



Linux Academy