

# 1. DNS lab introduction

This lab is an introduction to DNS, the Domain Name System. The goal is to learn how to configure, set up and troubleshoot DNS servers. More specifically, you will get a basic understanding of the BIND DNS software and the “dig” lookup tool.

You will also learn about various types of data stored in DNS, the caching system, and master-slave relationships for redundant servers.

The lab assumes basic knowledge about virtualization and Linux, including how logging is done and how services are used. You also should have some familiarity with Linux command line tools, and with editing text files using a screen-oriented text editor such as "vi" and "nano".

Moreover, the lab relies heavily on the "git" version-control system and you will hand in your solution by uploading it to [KTH GitHub \(https://gits-15.sys.kth.se\)](https://gits-15.sys.kth.se).

## Assessment

This assignment is graded Pass/Fail. It consists of many parts. **In order to get a passing grade, you need to complete all parts before the deadline.** More specifically, this is what you need to do:

1. Pass the DNS lab quizzes in Section 4 – 7 of the first part of the lab.
2. Answer the questions in Section 8 – 10 of the second part, and submit your answers to your git repository on KTH GitHub.
3. Submit a working DNS server configuration to your git repository on KTH GitHub.
4. Inform us that you are done with the lab, by submitting the URL for your KTH GitHub repository to the DNS lab submission here in Canvas.

The first part (DNS lab quizzes) gets graded as you attempt, and you can attempt as many times as you like until you pass.

## 2. DNS lab organization

### Overview

This lab is done in groups of two students. Follow the instructions for creating lab groups: [Sign up for DNS lab groups and supervision](https://canvas.kth.se/courses/41496/pages/sign-up-for-dns-lab-groups-and-supervision) (<https://canvas.kth.se/courses/41496/pages/sign-up-for-dns-lab-groups-and-supervision>). (<https://canvas.kth.se/courses/41496/pages/sign-up-for-the-dns-lab-instructions>) You do the lab on your own computer, at a time that you decide (as long as it is before the deadline, of course).

### Organization

The lab is organized as assignments in two parts. You do the lab by answering questions in the assignments, and creating a set of DNS configuration files. The assignments also give background and explain the basic concepts in DNS.

The first part of the lab consists of four quizzes intended to give background and prepare you for solving the tasks that come in the second part. In fact, the first part gives an overview of DNS, so it can also help you to prepare for the exam. The quizzes in the first part are automatically graded, and you will see your score as soon as you have completed each quiz. You need to reach a certain number of points to pass a quiz. *The quizzes in the first part are done individually, so both members in a group need to submit answers to the quizzes.*

The second part is about setting up a DNS server, and you will be working with DNS software. The assignments give instructions for you what to do, step by step. This part is manually graded by the teaching staff. *The second part is done groupwise, and the two members in a group make a joint submission.* See [Sign up for DNS lab groups and supervision](https://canvas.kth.se/courses/41496/pages/sign-up-for-dns-lab-groups-and-supervision) (<https://canvas.kth.se/courses/41496/pages/sign-up-for-dns-lab-groups-and-supervision>).

In order to complete the lab, you need to pass all assignments, **both the automatically graded individual quizzes and the manually graded group assignment.**

### Supervision and Guidance

Login ([https://app.kth.se/kpm/auth/login?nextUrl=https://canvas.kth.se/courses/41496/pages/2-dns-lab-organization?module\\_item\\_id=700416](https://app.kth.se/kpm/auth/login?nextUrl=https://canvas.kth.se/courses/41496/pages/2-dns-lab-organization?module_item_id=700416)) during supervision slots to help you with the lab. Follow the instructions for booking supervision in Zoom: [Sign up for DNS lab groups and supervision \(https://canvas.kth.se/courses/41496/pages/sign-up-for-dns-lab-groups-and-supervision\)](https://canvas.kth.se/courses/41496/pages/sign-up-for-dns-lab-groups-and-supervision).

There is also a Canvas discussion topic reserved for this lab: [DNS Lab Discussion Forum \(https://canvas.kth.se/courses/41496/discussion\\_topics/319054\)](https://canvas.kth.se/courses/41496/discussion_topics/319054). If you have questions, get stuck, or have experiences or tips that you want to share with other students, please feel free to use this discussion topic. The teaching staff monitors this discussion topic, but we also encourage students to help and discuss with each other.

## Environment

This lab requires system privileges, and uses the BIND software for DNS, which may not be that easy to run directly on your computer. We have therefore prepared a virtual machine configured with the software that you need. The virtual machine is for the VirtualBox hypervisor, which you need to download and install prior to doing the lab. It is straightforward to install – just follow the instructions.

For the purpose of easing the process of downloading and installing the virtual machine, we have made the virtual machine image as small as possible. Hence, it does not come with a GUI, and it probably lacks quite a few other features. If you follow the suggestions in the lab instructions, this should not be much of a problem for you. Should you run into problems, please feel free to use [DNS Lab Discussion Forum \(https://canvas.kth.se/courses/41496/discussion\\_topics/319054\)](https://canvas.kth.se/courses/41496/discussion_topics/319054) to get help, or book a supervision slot in Zoom.

## Submission

When you are done, you submit the work in two ways:


1. Submit your files by pushing them to your git repository on KTH GitHub (more about this later)
2. Submit the URN for your KTH GitHub repository in the DNS lab submission assignment in Canvas (this will tell the teaching staff that your submission is ready for grading.)

## 3. DNS lab software – VirtualBox, shell, git and BIND

This section describes the main software components in the DNS lab:

- Oracle VM VirtualBox hypervisor for running the lab virtual machine
- SSH and Linux shell for executing commands on the virtual machine
- The git distributed version-control system
- The BIND DNS software with the "named" DNS server

### Oracle VirtualBox

This lab runs on a virtual machine in Oracle VirtualBox. VirtualBox is installed on the computers in the computer rooms that we use for this lab. You can also download and install VirtualBox on your own computer, and do the lab there: <https://www.virtualbox.org>  (<https://www.virtualbox.org>).

### Installing the virtual machine

Once you have a computer with VirtualBox installed, the first step is to download and import the virtual machine image for the lab. You can find a link to the OVF file among the resources in the DNS lab module. Once downloaded, simply double-click to run the installer and then follow the instructions (you do not need to change any settings, just use the defaults).

Your virtual machine needs to connect to our infrastructure in order for you to proceed with this lab. For this, you need to sign up for group and get a group number. See [Sign up for DNS lab groups and supervision \(https://canvas.kth.se/courses/41496/pages/sign-up-for-dns-lab-groups-and-supervision\)](https://canvas.kth.se/courses/41496/pages/sign-up-for-dns-lab-groups-and-supervision).

Now that you know your group number, start your virtual machine. In the console window, edit the two lines in the file `/home/tc/ovpnclient/login.conf`. On both lines, replace the `X` with your group number. Then uncomment both lines by removing the `#` character at the beginning. Save and exit.

**Note:** you need system privileges to edit this file. But that is easy: just type “sudo” before the edit command. So if you use “nano” to edit, type:

```
$ sudo nano /home/tc/ovpnclient/login.conf
```

**Note:** the dollar sign “\$” represents the shell prompt. You don't type that. You type what comes after the prompt. Also, the prompt may vary depending on your shell settings. The default in the lab virtual machine is to use a more elaborated prompt, something like `tc@box:~ $`. In these instructions, we will just be using a plain “\$” sign instead.

nextUrl=https://canvas.kth.se/courses/41496/pages/3-dns-lab-software-virtualbox-shell-git-and-bind?module\_item\_id=700417)

group42  
IK2218-group42

After editing the file, reboot your virtual machine. Once it boots up again, you should see something like this in your console window:

```
Mon Sep 19 07:44:48 2016 /usr/local/sbin/ip route add 192.16.125.104/32 via 10.0.2.2
Mon Sep 19 07:44:48 2016 /usr/local/sbin/ip route add 0.0.0.0/1 via 192.16.127.129
Mon Sep 19 07:44:48 2016 /usr/local/sbin/ip route add 128.0.0.0/1 via 192.16.127.129
Mon Sep 19 07:44:48 2016 Initialization Sequence Completed
```

If you see the message “Initialization Sequence Completed”, that means your virtual machine is up and running and you are ready to proceed with the lab.

**NOTE:** it is a good practice to verify that the VM has IP reachability in both directions. You can do this by trying to ping a known Internet host, such as a google DNS server with IP address 8.8.8.8, and ping your lab VM (IP address 192.16.127.X, where X is your group number) from another device.

## Running commands

As you have already noticed, the virtual machine does not come with a desktop interface. It has a console window. Instead of typing your commands directly into the console window, we recommend that you login to your virtual machine from your computer using SSH. As part of the VM installation, your computer has been configured to redirect TCP port 2222 on your computer to port 22 on the virtual machine – the SSH server port. Therefore, to login on your virtual machine, you can simply run SSH with the following parameters:

<b>Hostname</b>	localhost
<b>Port</b>	2222
<b>User</b>	tc
<b>Password</b>	IK2218dns

You can use any SSH client of your choice. On Windows, PuTTY

(<https://www.chiark.greenend.org.uk/~sgtatham/putty/>)

(<https://www.chiark.greenend.org.uk/~sgtatham/putty/>) is a popular choice, while on a Mac or a Linux computer you can just open a Terminal window and run SSH like this:

```
$ ssh -p 2222 tc@localhost
```

Some commands require superuser privileges. Use the “sudo” program to run a command with superuser privileges. Be careful – you can do a lot of damage if you make mistakes as superuser!

**Login** (<https://app.kth.se/kpm/auth/login?>

nextUrl=https://canvas.kth.se/courses/41496/pages/3-dns-lab-software-virtualbox-shell-git-good-idea-to-keep-an-eye-on-the-system-log-file-while-you-are-working-we-recommend-that-you-have-one-window-with-an-ssh-session-where-you-run-your-commands-and-a-second-ssh-window-where-you-keep-an-eye-on-the-log-file

good idea to keep an eye on the system log file while you are working. we recommend that you have one window with an SSH session where you run your commands, and a second SSH window where you keep an eye on the log file:

```
$ sudo tail -f /var/log/messages
```

## Editing

During the lab, you will mostly be editing files. You will have to master a screen-based text editor. There are two editors available in the virtual machine: "vi" and "nano". If you haven't used any of them before, you may find "nano" easier to work with.

## Git Version Control and GitHub

The purpose of this lab is set up a DNS name server, which you do by creating a number of name server configuration files. Initially you get a basic, rudimentary server configuration packaged as a *git repository*. This repository is stored on a git management server, [KTH GitHub \(https://gits-15.sys.kth.se\)](https://gits-15.sys.kth.se). This repository is created automatically (but with some delay) when you have formed a student group with two members in it. See [Sign up for DNS lab groups and supervision \(https://canvas.kth.se/courses/41496/pages/sign-up-for-dns-lab-groups-and-supervision\)](https://canvas.kth.se/courses/41496/pages/sign-up-for-dns-lab-groups-and-supervision).

Your task consists of copying (or *cloning*, in git terminology) your group's repository to your virtual machine, making changes to the files on your virtual machine, and then submitting your changes by copying (or *pushing*) your changes back to your group's repository on KTH GitHub.

For an introduction to git, see:

- [Ric Glassey, DD1301 & DD1337, Managing Work with GitHub \(https://canvas.kth.se/courses/3050/files/344542/download?wrap=1\)](https://canvas.kth.se/courses/3050/files/344542/download?wrap=1).

You can also find plenty of tutorials and documentation for git on-line.

Git comes pre-installed on the lab virtual machine. In order to create a local repository on your virtual machine, you need to do the following steps:

1. Start the virtual machine (see above)
  2. Create SSH keys on the *virtual machine*, and install the keys on your KTH GitHub account. See [this ↗ \(https://www.youtube.com/watch?v=Sp5AASmX4no&list=PLZtN6QLX2rBA\\_gL6zs-gijlDihx-p2tO8\)](https://www.youtube.com/watch?v=Sp5AASmX4no&list=PLZtN6QLX2rBA_gL6zs-gijlDihx-p2tO8) series for how to set this up, or the guides ([Generating a new SSH key ↗ \(https://help.github.com/en/articles/generating-a-new-ssh-key-and-adding-it-to-the-ssh-agent\)](https://help.github.com/en/articles/generating-a-new-ssh-key-and-adding-it-to-the-ssh-agent)), [Adding a new SSH key to your GitHub account ↗ \(https://help.github.com/en/articles/adding-a-new-ssh-key-to-your-github-account\)](https://help.github.com/en/articles/adding-a-new-ssh-key-to-your-github-account)) on GitHub.
  3. Clone the repository from GitHub into the home directory of the "tc" user *on the virtual machine*. You can find the name of the repository via your [KTH GitHub \(https://gits-15.sys.kth.se\)](https://gits-15.sys.kth.se) account, and the URL you should use to clone the repository. Assuming that two
- Login (https://app.kth.se/kpm/auth/login?)

nextUrl=<https://canvas.kth.se/courses/41496/pages/3-dns-lab-software-virtualbox-shell-git-something-like-umc@kth-se-13-sys-kth-se-DNSlab21/ezra-bridger-bind> and bind:module\_new\_id=700417)

command will then create a directory called "bind" in the current directory. *Make sure to run the command in the home directory of the "tc" user! That is where the name server expects to find its configuration files. Also note that the third (last) argument should be "bind", to tell git that the new repository should be in a directory called "bind".*

```
$ git clone git@gits-15.sys.kth.se:DNSlab21/ezra-bridger-bind bind
```

4. Verify that you now have created a directory called "bind" in the home directory of the user "tc":

```
$ pwd
/home/tc
$ ls
bind/          ovpnclient/
```

Git is a powerful and very useful version-control system. You should make use of it as a tool to manage your files and keep track of your changes while you are working on the lab. So make it a habit to store the changes you make to the configuration files into your local repository ("git add" and "git commit"), and to keep your local repository in sync with the remote repository on KTH GitHub ("git push" and "git pull").

## BIND and named

The BIND DNS software is pre-installed in the lab virtual machine. The DNS server in BIND is a program called "named". It is a daemon program, which means that it runs in the background without connection to a terminal. Therefore, it does not print any output to the terminal window; the output goes to the system log file "/var/log/messages".

You start/stop/restart named using the "bind9" command:

```
$ sudo /etc/init.d/bind9 start
$ sudo /etc/init.d/bind9 stop
$ sudo /etc/init.d/bind9 restart
```


Named is configured through a config file, which in the virtual machine is the file "bind/named.conf" located in the home directory of the "tc" user. The config file specifies, among other things, what zones are controlled by this name server, and what the names are of the corresponding zone files.

Once named is up and running, it can be controlled by a separate program called "rndc". In particular, when you change a zone file, you need to tell named to reload the content to update its zone information:

```
$ sudo rndc reload
```

When you do this, remember to check /var/log/messages for error messages.

Login (<https://app.kth.se/kpm/auth/login?>

nextUrl=https://canvas.kth.se/courses/41496/pages/3-dns-lab-software-virtualbox-shell-git-  
if-a-dns-zone-is-working-correctly. This tool can be accessed at <https://zonemaster.iis.se/>   
(<https://zonemaster.iis.se/>). The goal with the lab is to pass all its tests. But you can also use it  
intermediately as a debugging tool.



## 8. Create your own zone

Now you will start working with your name server in the virtual machine. So if you haven't set up your virtual machine environment yet with BIND and named, now is the time to do it. Follow the instructions: [3. DNS lab software – VirtualBox, shell, git and BIND](https://canvas.kth.se/courses/41496/pages/3-dns-lab-software-virtualbox-shell-git-and-bind) (<https://canvas.kth.se/courses/41496/pages/3-dns-lab-software-virtualbox-shell-git-and-bind>).

Once you have your environment in place, the next step is to set up the zone file. You will create the zone file with some initial resource records, and tell named to read the zone information from the file.

Follow the instructions below to create your own zone file. Also write down the answers to the questions. The answers are submitted in the file "bind/report.txt" which is located together with your configuration files in your git repository.

### 8.1 Create the zone file

You have been given the task to take care of the DNS zone "groupX.ik2218.ssvl.kth.se.", where X is your group number. So if you are group number 26, your zone is "group26.ik2218.ssvl.kth.se." (without the quotation marks).

First you need to tell named that there is a new zone, and where its zone file is. Add a new zone entry to the named config file "bind/named.conf". Don't make any other changes. A zone entry is a line in the configuration file that starts with the "zone" keyword. Specify the domain name (FQDN!) for the zone, and the name of the zone file (as an absolute file path). You also need to give the *zone type*. There are several to choose from; find it out for yourself what the type should be.

**IMPORTANT:** You must write the zone entry in one line. Otherwise, your named config file may not be parsed properly since the grading script assumes each zone entry is in one line (i.e., no line break).

It is a good practice to verify that the named config file that you have just updated contains no syntax error using the command below:

```
$ named-checkconf /home/tc/bind/named.conf
```

If there is no error, the command terminates without any output and you can proceed. Otherwise, you need to troubleshoot and fix the error accordingly.

The next step is to create a zone file. Create the new zone file in the "bind/" directory by copying the template file named "db.empty". The new zone file must be named: **db.groupX** where **X** is your group number. This file is a forward-mapped zone file for the domain groupX.ik2218.ssvl.kth.se.

To get a working zone file, you need to have (at least) the following entries in the zone file:

- A \$TTL – use a low value in the order of a few minutes
- A \$ORIGIN macro with the domain name of your zone (FQDN)
- A SOA record (see examples in the preparations). Use a low refresh value.
- An NS entry pointing at the name server for the zone (that is, the name server that you are creating right now). If your group number is X, the name server must be called "ns.groupX.ik2218.ssvl.kth.se" – because this is the name that the delegating name server refers to.
- An A record for the name server for the zone matching the name server's IP address
  - This is the IP address of the "tap0" interface on your virtual machine – use "ifconfig tap0" to see the IP address.

After completing the zone file, you will verify that it has no syntax error using the command below: You need to replace the <ZONENAME> and <FILENAME> with the new zone and the zone file that you just created, respectively.

```
$ named-checkzone <ZONENAME> <FILENAME>
```

If there is no error, you will see that the zone is loaded and an "OK" in the last line of the output. Otherwise, you need to troubleshoot and fix the error accordingly.

## 8.3 Load and verify the zone file

First make sure that you have started named properly – see [3. DNS lab software – VirtualBox, shell, git and BIND \(https://canvas.kth.se/courses/41496/pages/3-dns-lab-software-virtualbox-shell-git-and-bind\)](https://canvas.kth.se/courses/41496/pages/3-dns-lab-software-virtualbox-shell-git-and-bind). If named has already been started, you can reload the configuration file with the command below:

```
$ sudo rndc reload
```

You know that your zone file has been correctly loaded when named reports into the log file that the zone with the file's current serial number has been loaded (the serial number is in the SOA record, remember?).

You can also run the command below to check the status of the name server:

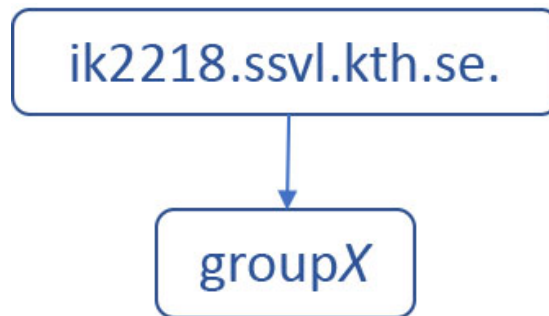
```
$ sudo /etc/init.d/bind9 status
```

The last line of the output should show "server is up and running". Otherwise, you must troubleshoot, fix the problem, and start the name server.

While you are working with your name server configuration files, make sure to commit your changes to the local git repository ("git add" and "git commit")! You should also synchronise your changes ("git push") to the remote repository at KTH GitHub.

*Delegation* is a central issue in DNS. For your zone to be tied to the global DNS tree, someone else needs to delegate the zone to you.

You are responsible for the zone "groupX.ik2218.ssvl.kth.se.", where X is your group number. This means that "ik2218.ssvl.kth.se." has delegated the zone named "groupX" to you:



Use dig to verify that there is indeed a delegation for your zone from "ik2218.ssvl.kth.se.". To do this, think about what it means to delegate, and how you can see a delegation in place. What DNS queries can you use? What should you ask for, and who should you ask? You should be able to do this on any computer connected to the Internet (not only on your virtual machine).

**Question 8.1:** What dig command you must use to verify that there is a delegation path for your zone from the root name servers?

**Question 8.2:** What DNS record type is shown in the output when you run the dig command in Question 8.1?

**Question 8.3:** What primary name server for the new zone is shown in the output when you run the dig command in Question 8.1?

You can also verify that the IP address of the "tap0" interface on your virtual machine is mapped to your name server for the new zone by running the command below, where <IP\_ADDRESS\_TAP0> is the IP address of the "tap0" interface on your virtual machine:

```
$ dig -x <IP_ADDRESS_TAP0>
```

**Question 8.4:** What DNS record type is shown in the output when you run the dig -x command above?

**Question 8.5:** When you run the dig -x command above, you should get an FQDN in the answer. What FQDN should you get as an answer?

## 8.5 Caveats

Things to think about when editing the zone file:

- Named is quite picky about spaces and newlines in the zone file. Follow the examples.
- Increment the serial number each time you update the zone file.

from the previous line, and is therefore position-dependent. So if you move a line with a blank name, it may get a different meaning.

- Run “rndc reload” after each change and check the logfile for error messages.
- Are you using the correct IPv4 address? Use “ifconfig” to check.
- Does “bind/named.conf” really contain the name of the correct zone file?
- Are you using the correct zone name (e.g. "group42.ik2218.ssvl.kth.se")?
- Do you have a glue record (an A record) with the IPv4 address corresponding to your NS record?
- Sometimes (if nothing else helps) you can try to restart named and check with “rndc status”.

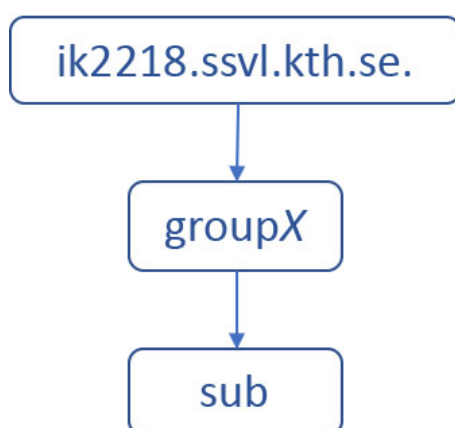
## 9. Subzones and delegations

It is common practice to distribute the responsibility for a zone to several servers, by dividing a zone into subzones and delegating the responsibilities for the subzones to other servers. There are many advantages with this in terms of, for example, performance, reliability, and ease of administration. Here you will create zone files for several subzones, delegate subzones to other servers, and receive delegations for subzones from other servers.

Follow the instructions below to set up subzones and their delegations. Also write down the answers to the questions.

### 9.1 Create a subzone

Now you should create a subzone named "sub.groupX.ik2218.ssvl.kth.se.", for which your name server will be responsible.



You create the subzone simply by creating a new zone file named "**db.sub.groupX**" where **X** is your group number in the "bind/" directory and adding a corresponding zone entry to your "named.conf" configuration file.

- Make sure that the SOA record matches the new zone. Although the subzone hosts on the same physical server as the groupX.ik2218.ssvl.kth.se zone, it is a best practice to name the primary name server for the subzone as ns.sub.groupX.ik2218.ssvl.kth.se. In this way, the name can remain the same even when the service is moved to another physical server with a different IP address.
- Add an NS record for the subzone.
- Add a TXT record for the subzone, with a text string: "groupX subzone", where X is your group number. For example, group1 should use the text string "group1 subzone".
- Add an A record for the name server for the subzone using the IP address of the "tap0" interface on your virtual machine.

Verify that the name server configuration file has no error with the following command:

Login ([https://app.kth.se/kpm/auth/login?nextUrl=https://canvas.kth.se/courses/41496/pages/9-subzones-and-delegations?module\\_item\\_id=700427](https://app.kth.se/kpm/auth/login?nextUrl=https://canvas.kth.se/courses/41496/pages/9-subzones-and-delegations?module_item_id=700427))

Verify that the zone file has no error with the following command, where the <ZONENAME> and <FILENAME> are the new zone and the zone file that you just created, respectively:

```
$ named-checkzone <ZONENAME> <FILENAME>
```

If there is no error, you can proceed to reload the named configuration:

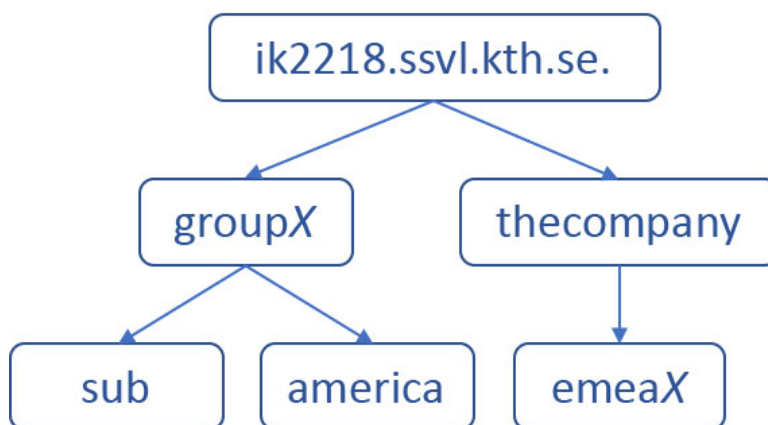
```
$ sudo rndc reload
```

Check the log file for error messages. Use dig to verify that the subzone appears in the global DNS tree. And don't forget to commit your changes to the git repository!

**Question 9.1:** What dig command do you use to verify that there is a delegation path for the subzone from the root name servers?

## 9.2 Subzone organization

Your group is involved in the IT operations of a renowned organization called TheCompany. For this task, the parent (the name server for "ik2218.ssvl.kth.se.") has already delegated the subzone "thecompany.ik2218.ssvl.kth.se" to another nameserver (see figure below). This other nameserver has everything pre-configured for you to be able to carry out the following tasks. **For brevity, the zone names below are given relative to the parent zone, and not as FQDNs (i.e. "america.groupX" instead of "america.groupX.ik2218.ssvl.kth.se."). Keep in mind though that you need to use FQDNs when configuring and testing.**



### 9.2.1 Delegate a subzone

The background here is that IT operations of "groupX" in America have grown substantially and therefore its management decided that America should have its own sub-domain. You, as the groupX DNS administrator, are given the task to delegate the zone "america.groupX" to the nameserver "ns.america.groupX" with IP address 192.16.125.106.

The DNS administrator for "america.groupX" has already configured its name server to accept the delegation.

Login ([https://app.kth.se/kpm/auth/login?nextUrl=https://canvas.kth.se/courses/41496/pages/9-subzones-and-delegations?module\\_item\\_id=700427](https://app.kth.se/kpm/auth/login?nextUrl=https://canvas.kth.se/courses/41496/pages/9-subzones-and-delegations?module_item_id=700427))

The NS record is a delegation while the A record is a glue record for the subzone. As described in [6. Define resource records \(https://canvas.kth.se/courses/41496/quizzes/49965\)](https://canvas.kth.se/courses/41496/quizzes/49965), a glue record is an address record that provides IP addresses for the authoritative name server in the delegation, which is needed to address a circular dependency.

Verify that the configuration is correct before you proceed. You should be able to resolve the IP addresses that those records point to if your configuration is correct.

The DNS administrator for "america.groupX" has also created records for "us.america.groupX", "canada.america.groupX" and "brazil.america.groupX".

**Question 9.2:** What are the IPv4 addresses for "us.america.groupX"?

**Question 9.3:** What are the IPv4 addresses for "brazil.america.groupX"?

**Question 9.4:** What is the TXT record for "canada.america.groupX"?

**NOTE:** You may wonder why the subzone you created in Section 9.1 seems to work even though you have not added a glue record in your groupX zone file. It works when the query goes to the primary name server (ns.groupX.ik2218.kth.se), to which the groupX zone and the subzone are delegated. However, it does not work due to the circular dependency problem when the query goes to the secondary name server (ns2.groupX.ik2218.ssvl.kth.se). You can verify this by using a dig command to look up your subzone on different servers.

## 9.2.2 Accept a delegated subzone

As the DNS administrator for "groupX", you are given the task to take over the EMEA IT operations of TheCompany. TheCompany's DNS administrator has delegated the zone "emeaX.thecompany" to your nameserver, and your task is to accept this delegation by configuring your DNS server accordingly.

For your server to be able to answer queries for the zone, you must accept the delegation by creating a zone file for "emeaX.thecompany" named "**db.emeaX.thecompany**" where **X** is your group number in the "bind/" directory. Add NS and A records to this file, as well as a TXT record containing your unique message. Remember to add the corresponding zone file entry to "bind/named.conf".

Now that you are in charge of "emeaX.thecompany", the network administrators of the Sweden, Turkey and Qatar branches contacted you and made the following requests.

- "sweden.emeaX.thecompany" shall resolve to the IP address 1.2.3.4
- "turkey.emeaX.thecompany" shall resolve to the IP address 5.6.7.8
- "qatar.emeaX.thecompany" shall resolve to the IP address 9.10.11.12

Verify that the delegation works by running "dig +trace". Also check that you can resolve the above records for Sweden, Turkey and Qatar from a public nameserver. (And, finally, remember to store your changes with git!)

# 10. Replication – masters and slaves

All zones and sub-zones you have configured so far are on your server; if your server goes down, the zone information becomes unavailable. A DNS server can replicate its data to other DNS servers via so called *zone transfers*, which are essential for redundancy and load balancing in DNS. In this task, you will 1) configure your master (or primary) server to replicate its information to a slave (or secondary) server so that the secondary server can answer queries for records in your zone, and 2) configure your server as a secondary for another primary server so that your server can respond to queries for the zone hosted by the primary.

Follow the instructions below to configure your server as primary and secondary. Also write down the answers to the questions. Towards the end of the lab, you will submit your answers.

Note: the terminology can be a bit confusing. The terms "primary name server" and "secondary name server" are the original ones, but BIND 8 changed this and called them "master name server" and "slave name server" instead. There is no difference, though. "Primary" means the same thing as "master", and "secondary" is the same as "slave". In this document, we will stick to the traditional terminology – "primary" and "secondary".

For brevity, the zone names below are given relative to the parent zone, and not as FQDNs (i.e. "groupX" instead of "groupX.ik2218.ssvl.kth.se."). **Keep in mind though that you need to use FQDNs when configuring and testing.**

## 10.1 Primary server

The "groupX" management has purchased another server to be configured as a secondary for your zone. Your colleague has already configured the secondary and informed you that its IP address is 192.16.125.106.

For your server to act as a primary in this replication, you must:

1. Declare the secondary as an authoritative server for the zone "groupX" in the zone file (the name of the secondary is "ns2.groupX").
2. Tell named that the secondary is allowed to initiate zone transfers from your primary. You declare this in "named.conf".
3. Amend your "groupX" zone definition in "named.conf" so that named will send DNS NOTIFY messages about zone changes to your secondary.

Make the necessary changes to the zone file and named configuration file, and restart named. Now the secondary should be able to return answer queries for the records in the "groupX" zone.

To verify that the zone transfer has taken place, and that the secondary can answer queries for records in your primary domain, use dig to query for records in your zone explicitly against the "ns2.groupX" server.



**Question 10.1:** What dig command do you use to verify that the secondary can answer a lookup query for the address of the primary server of your domain?

## 10.2 Secondary server

An organization called "GreenWorldX" (X is your group number) has signed an agreement with "groupX" for improving DNS availability. Per requirement, you are expected to configure your server as a secondary for the primary "ns.greenworldX" with IP address 192.16.125.106. They have already configured the primary to replicate the "greenworldX" zone to your server, with an NS record for "ns2.greenworldX" pointing at your server's IP address.

For your server to act as a secondary of this replication, you must:

1. Create a zone definition in named.conf with the appropriate zone type.
2. Specify the primary name server for this zone in the zone definition.
3. In the zone definition, set a new zone file named "**db.greenworldX**" where **X** is your group number zone file in the "bind/" directory, which the server will populate automatically. (The name server process should create this file automatically for you. You cannot, and should not, read/write the file.)

Once you complete the configuration and restart named, your nameserver should be able to answer queries for records in the "greenworldX" zone. (And don't forget to commit!)

**Question 10.2:** Use dig to query *your name server* for the IP addresses of "china.greenworldX", what dig command do you use?


**Question 10.3:** Use dig to query *your name server* for the IP addresses of "china.greenworldX", what is the IP address in the response?

**Question 10.4:** Use dig to query *your name server* for the IP addresses of "russia.greenworldX", what dig command do you use?

**Question 10.5:** Use dig to query *your name server* for the IP addresses of "russia.greenworldX", what is the IP address in the response?

**Question 10.6:** What is the TXT record for "themessage.greenworldX"?

# 11. Verifying your configuration

You must verify that your DNS setup passes the test at <http://zonemaster.iis.se/>  (<http://zonemaster.iis.se/>). Use this tool to verify groupX.ik2218 and greenworldX.ik2218 domains and correct any errors that show up.

Note that Zonemaster may cache your results for 5 minutes, so if you run the tool again for the same zone you may get the same report again. It could also be the case that your browser may return a cached response, use an incognito tab every time you run the test.

Zonemaster results for all your zones should not be reporting any errors or warnings, except the two warnings below:

- **Connectivity:** *AS Diversity*. All authoritative nameservers have the IPv4 addresses in the same AS (8973).
- **Zone:** *SOA 'expire' minimum value*. SOA 'expire' value (XX) is less than the recommended one (604800).

The final proof is to verify that everything is OK with your server configurations and report. From the terminal of the name server virtual machine, run the check script with the command below, replacing <GROUP\_NO> with your group number:

```
$ /home/tc/scripts/check_dns_lab.sh <GROUP_NO>
```

If you see an ERROR in the output, you must troubleshoot and fix it. If the output shows OK on all lines, then you have successfully completed the DNS lab and can submit it.

**IMPORTANT:** Sometimes, DNS cache may cause an error due to outdated records. Thus, you may want to run the check script again to verify that the error persists. If the error is due to the DNS cache, you will not see the error in the second run. Otherwise, you are likely to have an error in your configuration.

Login ([https://app.kth.se/kpm/auth/login?nextUrl=https://canvas.kth.se/courses/41496/pages/11-verifying-your-configuration?module\\_item\\_id=700429](https://app.kth.se/kpm/auth/login?nextUrl=https://canvas.kth.se/courses/41496/pages/11-verifying-your-configuration?module_item_id=700429))