Domain Name System

KTH NS-Lab

Standalone VM version

Group Nr	
Name1	
Name2	
Date	
Grade	
Instructor's Signature	

Table of Contents

1 Goals

This lab is an introduction to the Domain Name System. The goal is to give you knowledge so that you can configure, setup and troubleshoot DNS systems. More specifically, you will get a basic understanding of the dns system BIND and the dns lookup tool DIG.

The lab will also introduce the various types of data stored in DNS, the caching system and master-slave relationships for redundant servers.

The lab assumes basic knowledge of virtualization and UNIX style systems, including how logging is done and how services are used. It is also absolutely necessary to be able to edit text files using a standard text editor.

At every milestone you are expected to call a lab assistant, show your work and get a signature, and only then proceed with the following task. So please print this instructions document before you come to lab.

2 Preparing the lab environment

You are going to perform this lab on a virtual machine (VM) of your own. First step is to download and import the OVF template for the VM into Oracle VirtualBox. You can find the download link to the VM in course Canvas, Files -> DNS Lab folder. (IK2218DNS VM). Once downloaded, simply double-click it and follow the instructions below.

Your VM needs to connect to our infrastructure in order for you to proceed with this lab. For this, you need to know your group number, please refer to the DNS module in Canvas for finding it out.

Now that you know your group number, start your VM and edit the file */home/tc/ovpnclient/login.conf* Replace the *X* with your group number in both lines, then uncomment both lines by removing the # character at the beginning of each line. Save and exit, then reboot the VM.

Once your VM boots up, you are expected to see something like the following screen at your VM console.

```
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 192.16.127.1
29
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 VM is ready to proceed with the lab.

For your convenience (i.e. keyboard language, multiple shells), we recommend you to SSH to your VM. Because the VM NIC is configured in NAT mode and necessary ports are already forwarded, you should SSH to **the IP address of your host machine (lab computer) and not the VM IP.** For convenience, use the *localhost* as your destination.

SSH Destination: localhost SSH Port: 2222
Username: tc
Password: IK2218dns

Use Xterm as your terminal client (Putty if you are using Windows) to SSH into your VM.

For your convenience, enter the `sudo su` command to enter root privileges. Also we recommend you to establish two SSH sessions to the VM where you perform configurations at one and read the logs at the other.

At this stage, your VM has automatically been delegated the zone group**X**.ik2218.ssvl.kth.se where **X** is your group number. The name server (your VM) IP to which this zone delegated to is the IP that your tap0 interface obtained. Run the command *ifconfig tap0* to find it out.

During the lab, you will mostly be editing files. You will have to master a text editor. There are two text editors available, vi and nano. The most intuitive is nano.

Your DNS zone:_____.ik2218.ssvl.kth.se (fill in x)

Your partner's DNS zone:_____.ik2218.ssvl.kth.se (fill in y of another group)

Init seq completed & delegated zone is identified

Milestone 1: Lab env Signature: _____

3 Using dig to explore the DNS system

Dig is a tool for sending queries to DNS servers and view the results. Typical output from Dig looks like this:

```
# dig www.kth.se
; <<>> DiG 9.9.4 <<>> www.kth.se
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39398
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL:
1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.kth.se.                    IN      A

;; ANSWER SECTION:
www.kth.se.             74      IN      A       130.237.28.40

;; Query time: 4 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Wed Aug 24 14:11:13 UTC 2016
;; MSG SIZE  rcvd: 55
```

Make sure you understand the status and flags fields. They are as important as the records returned. Reference the questions above.

Dig is a powerful tool to explore the DNS system. Use Dig to answer the following questions:

What is the IPv4 address of ns.ik2218.ssvl.kth.se?

What is the IPv6 address of ipv6.google.com?

What data is stored in the TXT record of ik2218.ssvl.kth.se?

Use the trace flag to do an iterative lookup for ik2218.ssvl.kth.se. List the servers queried and what record is used from each server:

Dig can also do reverse DNS, mapping IP addresses to DNS name. This is done by doing a query for the PTR records of a specially formed DNS name. Use dig with the trace flag to get the DNS name of 130.237.28.40. Use the returned data to illustrate how reverse lookups are done in DNS.

You can request to ask a specific nameserver in DIG. How is this done?

How do you query for a zone transfer? Try to get all records from ik2218.ssvl.kth.se.

Exploring DNS system

Milestone 2: Dig Signature: _____

4 Setting up BIND

Bind is a daemon program (actually called "named"), which means it runs in the background most of the time. It will not give you any direct output but syslogs its output. Interaction with bind is done through the system log, zone files, the configuration files and the rndc client.

In the VM you work, bind is not configured to start automatically on boot. Syntax for interacting with the service is below (mind the # prompt, use sudo if you are in $ prompt).

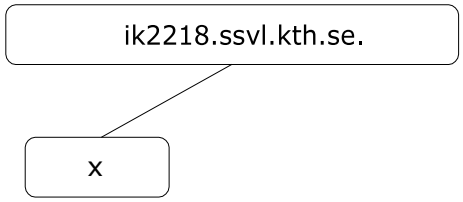
```
# /etc/init.d/bind9 {start|stop|restart}
```

You configure bind by editing `/etc/bind/named.conf`
Operation of named can be controlled by the program rndc (eg `rndc reload` after zone changes). Always check the syslog for errors after changes (rndc might report success even if parts of the configuration contain errors). We recommend you to open up a second SSH window and use it as a live monitor for logs via the following command.

```
# tail -f /var/log/messages
```

IIS has a tool that lets you verify if a DNS zone is working correctly. This tool can be accessed on http://dnscheck.iis.se/. The goal of the complete lab is to pass all its tests. But you can use it intermediately as a debugging tool.

5 Accepting the zone delegation



A central issue with DNS is that of delegation. In order to be tied to the global DNS tree, someone else needs to delegate a zone to you.

You have been given the DNS zone <x>.ik2218.ssvl.kth.se. This means that ik2218.ssvl.kth.se has delegated the <x> zone to you. In the delegation there is also a secondary nameserver allocated, but you can ignore this until Section 8.

Verify the delegation from ik2218.ssvl.kth.se using dig! How is this done?

Your task is to accept this delegation by configuring a DNS server to answer for zone <x>. You do this by creating a zone file containing a SOA record matching the zone and adding your zone to the bind configuration file. In /etc/bind folder, there exists a zone file template named db.empty. You can copy this template to create your zones.

Getting the files right

Add a new zone entry to the `/etc/bind/named.conf` file. Don't make any other changes. Create a new zone file in `/etc/bind/`. When you cd into /etc/bind, shell prompt may show as /home/tc/bind# and that is OK.
When you make changes to /etc/bind/named.conf and your zone file, reload named and *always* check for any error messages prompted to shell by rndc.

```
# rndc reload
```

Meanwhile, observe your second SSH window where you monitor the logs live and verify that the correct zone file is found and loaded.

Edit the zone file

To get a working zone file you need to specify (at least) the following records:

- Specify $TTL using a low value
- The $ORIGIN macro should be the absolute name of your zone (trailing dot)
- A SOA record (see examples in the preparations). Use a low refresh value.
- An NS entry pointing at the nameserver for the zone. This should be the specific host ns.<x>.ik2218.ssvl.kth.se.
- An A record matching the name-server's IP address

You will know that you have the correct *syntax* of your zone file when bind reports into the log file you are monitoring that the file is loaded correctly with a new serial number.

Then you can verify that your server is part of the DNS tree by using dig. For example:

```
dig @<your ip address> ns.<x>.ik2218.ssvl.kth.se dig
<x>.ik2218.ssvl.kth.se
dig ns.<x>.ik2218.ssvl.kth.se
dig ns.<x>.ik2218.ssvl.kth.se +trace
```

Things to think about when editing the zone file:
- The zone file is quite picky about spaces and newlines. Write as it looks in the examples.
- Increment the serial number each time you save the zone file.
- *Avoid* blank names (lines starting with space): they represent repetitions. If you move a line with a blank name, it may get a different name, making the order significant.
- Make rndc reload after every change and check your second SSH window where you monitor the logs.
- Do you use the correct IPv4 address?
- Does /etc/bind/named.conf really contain the name of the correct zone file?
- Are you using the correct zone name (e.g. a1.ik2218.ssvl.kth.se)?
- Do you have an A record for your NS record?
- Sometimes (when nothing else helps) you just have to restart named and check with "rndc status". This happens now and then if named got into a strange state.

6 Adding records to your zone

A zone is rather uninteresting unless there is some data in it. Therefore you should add the following records to your zone:

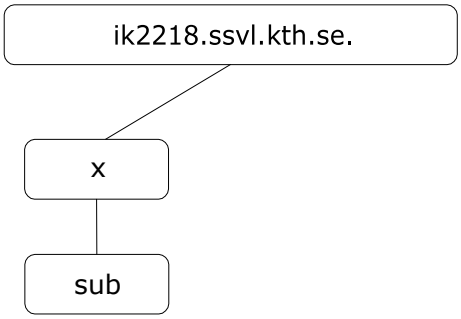
- A CNAME for your server
- A TXT record with your name or some other unique text which you can use when debugging.

Check the new records with dig.

Setting up BIND and configuring your zone

Milestone 3: BIND Signature: _____

7 Creating a sub-zone

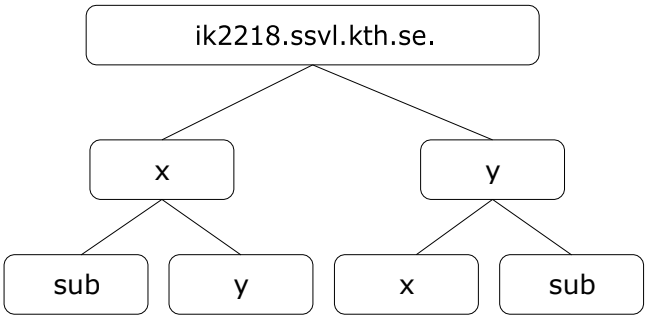


It is common for the same DNS server to answer for several zones. In this case you will create a subzone named sub.<x>.ik2218.ssvl.kth.se. You do this simply by creating a new zone file and adding the zone to your bind config. Make sure you add NS and A records to the zone.

Verify that you can reach the zone.

Define a different TXT file for the sub-zone.

8 Delegating a sub-zone



Frequently you wish to delegate a sub-zone to another server (and administrator). For example ssvl.kth.se. delegates ik2218. ssvl.kth.se. to the lab. You should now do a delegation to one of the other groups. Assuming the other group is *y* you should delegate <y>.<x>.ik2218.ssvl.kth.se to the other group.

For the delegation to work correctly you need to add two records (NS and A) to your zone file. These are called glue records.

Why are glue records needed?

_____

When you delegate, you should assume that the nameserver in the delegated zone is called ns.<y>.<x>.ik2218.ssvl.kth.se.

Which are your glue records?

_____

_____

The glue records breaks one important principle in DNS. What is that?

_____

Once you have done the delegation, make sure your partner group delegates <x>.<y>. ik2218.ssvl.kth.se. to you in return.

For your server to answer for the zone you must accept the delegation by creating a Zone file matching <x>.<y>. ik2218.ssvl.kth.se. Add NS and A records to this file.

Also add a TXT records to so you can demonstrate that it works correctly.

To complete this milestone you should have:
1: dig +trace'es showing your zones working
2: dig's illustrating the data in your zones

Milestone 4: Sub-zone Signature: _____

9 Masters and slaves, replication

At this point your DNS infrastructure is very vulnerable as the failure of a single server would make it all stop working. The way DNS solves this problem is through replication of the data over several redundant servers.

Replication requires several steps:

1. All nameservers for a zone must be listed in the zonefile (and in the delegation)
2. The master must send notify messages and accept zone transfers to the slaves
3. The slave must accept notify messages, initiate zone transfers and respond for the zone.

The parent zone, ik2218.ssvl.kth.se has been setup to return two separate nameservers for your zone: Your nameserver (ns.<x>) and your partner's nameserver IP (ns2.<x>). This means that your zone currently has a secondary nameserver which does not respond correctly.

To replicate your zone to your partner's nameserver you must:

1. List his nameserver among the authoritative nameservers in your zonefile for <x>
2. Add a "also-notify" entry to your bind configuration for the zone
3. Ask your neighbor to add a slave entry for the zone, with your server as the master.

To act as a slave for your neighbor you must:

1. Configure named to be a slave of <y>. Specify /etc/bind as the directory for the file.

Use rndc (or restart bind) to get bind to notify your slave of the zone and initiate a zone transfer. You can check the syslog to see if the zone transfer was successful. After that you can use "dig <x> @ns.<y>" to check that your neighbor answers correctly for your zone.

10 Verification of zones

The final proof of your DNS setup is to pass the IIS test at http://dnscheck.iis.se/. Use this tool to verify all your zones and correct any errors that show up.

Note that DNSCheck will cache your results for 5 minutes, so if you run the tool again on the same zone you will just get the same report again.

To complete this milestone you should have

1. dig +trace results illustrating how the two nameservers answers to queries and
2. DNSCheck results for all your zones, without any errors

Milestone 5: Working, redundant DNS! Signature: _____

References

[1] Forouzan, "TCP/IP protocol Suite", Chapter 17 Domain name System (DNS)
[2] P. Mockapetris, "RFC 1034", Domain Names – Concepts and Facilities, IETF, 1987
[3] P. Mockapetris, "RFC 1035", Domain Names – Implementations and Specifications, IETF, 1987

[4] Bind 9 administrator reference manual on the web. Chapter 3: Nameserver configuration provides some examples of zone files and how to use dig and rndc.