**Tugas Day 7**

Instalasi & Konfigurasi DNS server

pada sistem operasi CentOS

**Intro**

*Domain Name System* atau DNS merupakan sebuah entitas dari arsitektur jaringan yang dianalogikan sebagai sebuah “buku telepon” internet yang menyimpan informasi tentang nama *host* maupun nama *domain* dalam bentuk basis data tersebar (distributed database). Dengan kata lain, sistem ini memungkinkan adanya proses translasi dan identifikasi alamat komputer dalam suatu jaringan melalui proses pemetaan alamat IP berdasarkan *domain name* yang bersesuaian.

**Spesifikasi Client & Server**

Pada proses instalasi DNS server ini akan dilakukan skenario pada *client-server* sebagai berikut:

Server

|  |
| --- |
| Operating system : CentOS 8 minimal server (Docker container) Hostname : mfaqih.com IP Address : 192.168.88.1/24  Service : HTTP (Port 80) |

Client

|  |
| --- |
| Operating system : Ubuntu 18.10 Desktop (Host) IP Address : 192.168.88.55/24 |

**Persiapan Docker Container**

Pada tahap ini, dilakukan proses pembuatan image CentOS dengan **Dockerfile** yang selanjutnya dijalankan dengan commandsebagai berikut

|  |
| --- |
| FROM centos/systemd  RUN yum -y install httpd vim bind bind-utils net-tools; yum clean all; systemctl enable httpd.service  EXPOSE 80  CMD ["/usr/sbin/init"] |

|  |
| --- |
| $ docker build --rm --no-cache -t dns-server .  $ docker run --privileged --name dns-server -v /sys/fs/cgroup:/sys/fs/cgroup:ro -p 1337:80 -d dns-server  $ docker exec -it CONTAINER\_ID bash |

**Instalasi DNS server**

Sebelum melakukan konfigurasi DNS server, dilakukan proses instalasi aplikasi manajemen DNS server terlebih dahulu dengan perintah sebagai berikut

|  |
| --- |
| $ sudo yum install bind bind-utils -y |

**Konfigurasi DNS server**

1. **BIND setup**

Pada proses ini akan dilakukan modifikasi *BIND options* pada file **/etc/named.conf** dengan menambahkan alamat IP server pada argumen **listen-on port, allow-query,** dan **allow-query**-**cache** sehingga diperoleh hasil sebagai berikut

|  |
| --- |
| // // named.conf // options {  listen-on port 53 { 127.0.0.1; **192.168.88.1;** };  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.recursing";  secroots-file "/var/named/data/named.secroots";  allow-query { localhost; **192.168.88.1; any;** };  allow-query-cache { localhost; **192.168.88.1; any;** }; |

1. **Define Forward Zone**

Selanjutnya pada file **/etc/named.conf** akan dilakukan pendefinisian **DNS *forward-zone*** sebagai berikut

|  |
| --- |
| zone "mfaqih.com" {  type master;  file "/etc/named/mfaqih.com.zone"; }; |

Barulah kemudian dilakukan pengisian *basic* **DNS records** pada file **/etc/named/mfaqih.com.zone**

|  |
| --- |
| **$TTL 86400 @ IN SOA mfaqih.com. root.mfaqih.com. (  2018092501 ;Serial  3600 ;Refresh  1800 ;Retry  604800 ;Expire  86400 ;Minimum TTL )   @ IN NS ns1.mfaqih.com. @ IN NS ns2.mfaqih.com. @ IN A 192.168.88.1 ns1 IN A 192.168.88.1 ns2 IN A 192.168.88.1 www IN CNAME mfaqih.com.** |

1. **Define Reverse Zone**

Selanjutnya pada file **/etc/named.conf** akan dilakukan pendefinisian **DNS reverse*-zone***dengan membalik oktet dari alamat IP server sebagai berikut

|  |
| --- |
| zone "88.168.192.in-addr.arpa" IN {  type master;  file "/etc/named/88.168.192.rev"; }; |

Barulah kemudian dilakukan pengisian *basic* **DNS records** pada file **/etc/named/88.168.192.rev**

|  |
| --- |
| **$TTL 86400 @ IN SOA mfaqih.com. root.mfaqih.com. (  2018092501 ;Serial  3600 ;Refresh  1800 ;Retry  604800 ;Expire  86400 ;Minimum TTL )   IN NS ns1.mfaqih.com.  IN NS ns2.mfaqih.com. @ IN A 192.168.88.1 ns1 IN A 192.168.88.1 ns2 IN A 192.168.88.1 50 IN PTR mfaqih.com.** |

Setelah beberapa modifikasi tersebut file **/etc/named.conf** akan terlihat sebagai berikut

|  |
| --- |
| // // named.conf // // Provided by Red Hat bind package to configure the ISC BIND named(8) DNS // server as a caching only nameserver (as a localhost DNS resolver only). // // See /usr/share/doc/bind\*/sample/ for example named configuration files. // // See the BIND Administrator's Reference Manual (ARM) for details about the // configuration located in /usr/share/doc/bind-{version}/Bv9ARM.html  options {  listen-on port 53 { 127.0.0.1; **192.168.88.1;** };  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.recursing";  secroots-file "/var/named/data/named.secroots";  allow-query { localhost; **192.168.88.1; any;** };  **allow-query-cache { localhost; 192.168.88.1; any; };**   /\*   - 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 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 "mfaqih.com" {  type master;  file "/etc/named/mfaqih.com.zone"; };  zone "88.168.192.in-addr.arpa" IN {  type master;  file "/etc/named/88.168.192.rev"; };**  zone "." IN {  type hint;  file "named.ca"; };  include "/etc/named.rfc1912.zones"; include "/etc/named.root.key"; |

**Aktivasi *named DNS service***

Dari sini kita lakukan aktivasi *named service* untuk menjalankan DNS server dengan konfigurasi yang telah dilakukan sebelumnya

|  |
| --- |
| $ sudo systemctl enable named  $ sudo systemctl restart named |
|  |

**DNS Resolver Assignment**

Setelah itu dilakukan penambahan *nameserver* pada file **/etc/resolv.conf** dengan alamat IP DNS server yang telah dibuat

|  |
| --- |
| **# This file is managed by man:systemd-resolved(8). Do not edit.** **#** **# This is a dynamic resolv.conf file for connecting local clients directly to** **# all known uplink DNS servers. This file lists all configured search domains.** **#** **# Third party programs must not access this file directly, but only through the** **# symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a different way,** **# replace this symlink by a static file or a different symlink.** **#** **# See man:systemd-resolved.service(8) for details about the supported modes of** **# operation for /etc/resolv.conf.**  **search mfaqih.com nameserver 192.168.88.1** nameserver 192.168.0.1 |

**DNS Server Testing**

1. **Server**

Untuk memverifikasi kevalidan dari konfigurasi DNS server yang dibuat, kita dapat melakukan pengecekan sebagai berikut

|  |
| --- |
| $ nslookup mfaqih.com |
|  |

|  |
| --- |
| $ dig mfaqih.com |
|  |

**Web Server Deployment Test**

Selain itu, kita juga dapat melakukan pengujian akses *domain name* dari sebuah *HTTP Request* dengan melakukan instalasi web server terlebih dahulu

|  |
| --- |
| $ sudo yum install httpd $ sudo systemctl enable httpd $ sudo systemctl start httpd |

Kemudian melakukan inisialisasi **index.html** pada directory **/var/www/html**

|  |
| --- |
| <!DOCTYPE html> <**html**> <**head**>  <**title**>It works!</**title**> </**head**> <**body**>  <**h1**>It works!</**h1**> </**body**> </**html**> |

|  |
| --- |
| $ sudo chmod 755 /var/www/html/index.html $ curl mfaqih.com |
|  |

**Firewall Configuration**

Untuk mengizinkan akses dns beserta web server kepada pihak client, dilakukan penambahan *inbound* rule pada **UDP Port 53**  & **TCP Port 80**

|  |
| --- |
| firewall-cmd --add-service=dns --permanent firewall-cmd --add-service=http --permanent firewall-cmd --reload |

1. **Client**

Setelah melakukan konfigurasi DNS server beserta firewall pada komputer server, tiba saatnya untuk melakukan pengujian pada komputer client. Untuk itu dilakukan DNS resolver assignment dengan memasukkan alamat IP server

|  |
| --- |
| **# This file is managed by man:systemd-resolved(8). Do not edit.** **#** **# This is a dynamic resolv.conf file for connecting local clients to the** **# internal DNS stub resolver of systemd-resolved. This file lists all** **# configured search domains.** **#** **# Run "resolvectl status" to see details about the uplink DNS servers** **# currently in use.** **#** **# Third party programs must not access this file directly, but only through the** **# symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a different way,** **# replace this symlink by a static file or a different symlink.** **#** **# See man:systemd-resolved.service(8) for details about the supported modes of** **# operation for /etc/resolv.conf.**  nameserver 192.168.88.1 nameserver 127.0.0.53 options edns0 |

Barulah dilakukan pengujian sebagaimana yang kita lakukan sebelumnya pada komputer server. Berikut ini merupakan cuplikan dari komparasi pengujian pada komputer **client**-**server**



