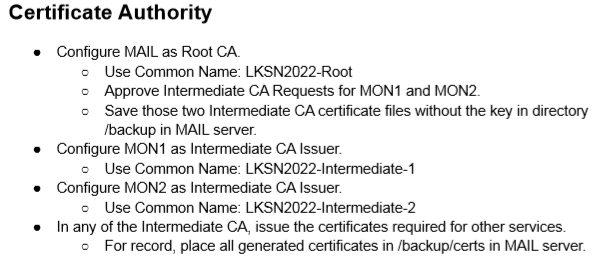
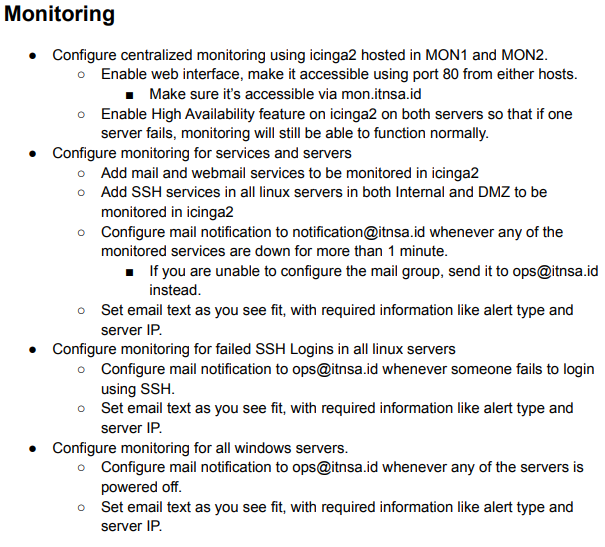
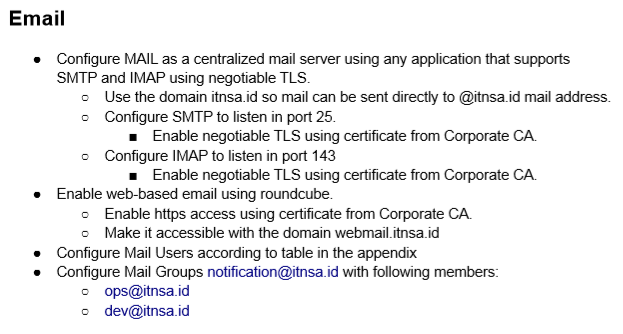
**LKSN 2022**



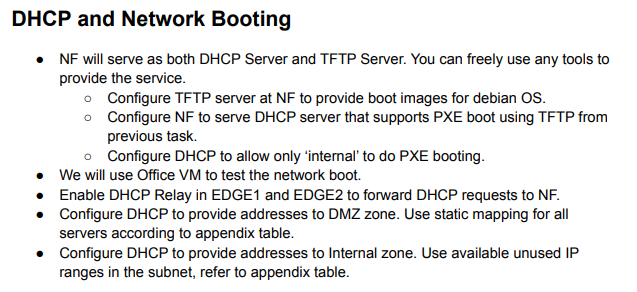
|  |
| --- |
| **Create Root CA pada MAIL**  openssl genrsa -out cakey.pem 2048  openssl req -new -x509 -days 3650 -config openssl.cnf -extensions v3\_ca -key private/cakey.pem -out certs/cacert.pem  **Create Intermediate CA pada MON1 & 2**  pada bagian ini pastikan terlebih dahulu sudah membuat root CA dan tinggal membuat intermediate CA, kita akan mengedit file openssl.cnf dan menyusun struktur directory untuk intermediate untuk meletakkan file key,csr,cert intermediatenya.  Openssl.cnf = /usr/lib/ssl/openssl.cnf  mkdir /root/tls  cd /root/tls  mkdir certs private  echo 01 > serial  touch index.txt  copy file openssl.conf ke /root/tls  edit file openssl sesuai tempat certificate berada  [ CA\_default ]  dir = /root/tls # Where everything is kept  certificate = $dir/certs/cacert.pem # The CA certificate  private\_key = $dir/private/cakey.pem # The private key  policy = policy\_match  [ v3\_intermediate\_ca ]  subjectKeyIdentifier = hash  #authorityKeyIdentifier = keyid:always,issuer (pagarin jika error)  basicConstraints = critical, CA:true, pathlen:0  keyUsage = critical, digitalSignature, cRLSign, keyCertSign  membuat struktur directory intermediate  mkdir /root/tls/intermediate  cd /root/tls/intermediate  mkdir certs csr private  echo 01 > serial  echo 01 > /root/tls/intermediate/crlnumber  cp file openssl.conf ke /root/tls/intermediate  dir = /root/tls/intermediate # Where everything is kept  certificate = $dir/certs/intermediate.cacert.pem # The CA certificate  private\_key = $dir/private/intermediate.cakey.pem # The private key  policy = policy\_anything  openssl.cnf(CA/intermediate)      Openssl.cnf(server/client)      1. Create intermediate CA key  openssl genrsa -out intermediate/private/intermediate.cakey.pem 4096  2. Create intermediate CA Certificate Signing Request (CSR)  openssl req -new -sha256 -config intermediate/openssl.cnf -key intermediate/private/intermediate.cakey.pem -out intermediate/csr/intermediate.csr.pem  3. Sign and generate intermediate CA certificate(gunakan file openssl ca)  openssl ca -config openssl.cnf -extensions v3\_intermediate\_ca -days 2650 -notext -batch -in intermediate/csr/intermediate.csr.pem -out intermediate/certs/intermediate.cacert.pem  cat index.txt  - verify  Openssl verify -CAfile /CAfile/.. /certificate/..  openssl x509 -noout -text -in intermediate/certs/intermediate.cacert.pem  - Membuat certificate yang ditanda tangani oleh intermediate CA  Pada bagian ini perhatikan config openssl.cnf yang digunakan adalah configan openssl yang punya intermediate.  openssl genrsa -out client.key 2048  openssl rsa -in client.key -out client.key  openssl req -new -key client.key -out client.csr  openssl ca -config openssl.cnf -extensions v3\_client\_crt -notext -batch -in client.csr -out client.crt  openssl genrsa -out server.key 2048  openssl rsa -in server.key -out client.key  openssl req -new -key server.key -out server.csr  openssl ca -config openssl.cnf -extensions v3\_server\_crt -notext -batch -in server.csr -out server.crt |



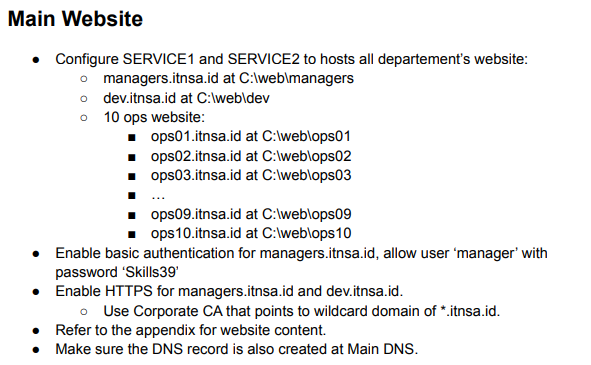
|  |
| --- |
| Pada bagian ini kita akan mengkonfigurasi monitoring dengan icinga2.  File yang akan di konfigurasi adalah membuat 2 database untuk icingamysql dan webnya ada pada file default apache2, edit juga file /etc/icinga2/features-available/ido-mysql.conf   * MON1  1. install icinga2 monitoring-plugins mariadb-server 2. #systemctl start icinga2 3. #systemctl enable icinga2 (harus) 4. create user   mysql -u root –p  create user ‘mon’@’%’ identified by ‘Skills39’;  grant all privileges on \*.\* to ‘mon1’@’%’ identified by ‘Skills39’;   1. apt install icinga2-ido-mysql   Configure Database for Icinga2-ido-mysql  Connect Database for icinga2-ido-mysql Module   1. create database for icinga2   mysql -u root –p  > CREATE DATABASE icinga2;  > GRANT ALL ON icinga2.\* TO 'mon1'@'%' IDENTIFIED BY 'Skills39';  > FLUSH PRIVILEGES;  > EXIT;   1. import file database   mysql -u root -p icinga2 < /usr/share/icinga2-ido-mysql/schema/mysql.sql   1. edit file ido-mysql isi sesuai user dan database yang sudah dibuat   nano /etc/icinga2/features-available/ido-mysql.conf     1. icinga2 feature enable ido-mysql 2. systemctl restart icinga2 3. apt install icingaweb2 apache2 icingacli –y 4. apt install php-gd php-mbstring php-mysqlnd php-curl php-xml php-cli php-soap php-intl php-xmlrpc php-zip php-common php-opcache php-gmp php-imagick php-pgsql -y 5. buat database untuk icingaweb2   > CREATE DATABASE icingaweb2;  > GRANT ALL ON icingaweb2.\* TO ‘mon’@’Skills39’;  > FLUSH PRIVILEGES;  > EXIT;   1. edit file dan ganti sesuai dibawah ini   nano /etc/php/7.4/apache2/php.ini     1. edit file /etc/apache/sites-avalaible/000-default.conf      1. membuat token untuk setup icingaweb2   #icingacli setup token create   1. buka mon.itnsa.id di browser client/ http://<ipadd>/webicinga2/ 2. masukkan token yang sudah didapat pada server tadi 3. pilih monitoring next> next> database next> isi nama databaseweb, user dan pwnya validate dan next 4. next terus sampai bertemu monitoring IDO resourse, isi database icingaido tadi dan isi user dan pw seperti yan sudah dibuat, validate dan next terus 5. local command file> next terus hingga finish 6. pengujian dilakukan dengan login icinga dengan user dan pw yang sudah dibuat tadi  * Pada bagian ini kita akan menambahkan services ssh, http, smtp, imap dan ke monitoring icinga2 pada mon2 dan akan mengedit file services, hosts, dan templates. * Buat template untuk memanggil service yang akan di monitoring oleh icinga2      * Add object host dan object service untuk menentukan target host dan service yang akan di monitoring pada file /etc/icinga2/conf.d/hosts.conf        * Apply service untuk mengapply service http atau webmail pada file /etc/icinga2/conf.d/service.conf |



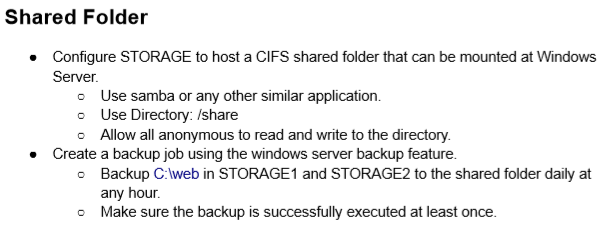
|  |
| --- |
| Pada bagian ini pastikan sudah menggabungkan intermediate ca dan server certificate  Server.crt> intermediate.crt> server.key = allserverinter.pem(penamaan bebas)   1. Apt install postfix & dovecot 2. Maildirmake.dovecot /etc/skel/Maildir 3. tambahkan home\_mailbox = Maildir/ pada /etc/postfix/main.cf 4. dpkg-reconfigure postfix 5. internetsite>mail.domain name> skip>skip>no>tambahkan 0.0.0.0/0> 0> +> ipv4 6. restart postfix dan imap 7. service postfix restart 8. nano /etc/postfix/main.cf      1. nano /etc/postfix/master.cf      1. restart service postfix nya 2. edit file dovecot 3. nano /etc/dovecot/dovecot.conf hapus pagar pada listen \* 4. nano /etc/dovecot/conf.d/10-auth.conf   edit disable\_plaintext\_auth = yes menjadi disable\_plaintext\_auth = no  edit auth\_mechanisms = plain menjadi auth\_mechanisms = plain login   1. nano /etc/dovecot/conf.d/10-mail.conf   beri comment pada mail\_location = mbox:~/mail:INBOX=/var/mail/%u  hilangkan comment mail\_location = maildir:~/Maildir   1. nano /etc/dovecot/conf.d/10-master.conf   # Postfix smtp-auth  unix\_listener /var/spool/postfix/private/auth {  mode = 0666  user = postfix  group = postfix  }   1. nano /etc/dovecot/conf.d/10-ssl.conf     Another way    Server.crt = certificate server  Chained.crt = ca.crt, inter.crt   1. restart dovecot 2. cek dengan   openssl s\_client -connect mail.itnsa.id:143 -starttls imap  openssl s\_client -connect mail.itnsa.id:25 -starttls smtp -tls1\_1  Add User   1. adduser ops 2. isi passwd nya   Add Mail Group   1. sudo nano /etc/aliases 2. notification: ops@itnsa.id, [dev@itnsa.id](mailto:dev@itnsa.id) 3. newaliases 4. sudo service postfix restart 5. coba test send mail kegrup yang sudah dibuat, dan cek email nya.  * Membuat user dan database mysql      1. apt install mariadb-server 2. mysql –u root –p   >CREATE DATABASE roundcube;  >CREATE USER ‘roundcube’@’%’ identified by ‘passwd’;  >GRANT ALL PRIVILAGES ON rouncube.\* to ‘roundcube’@’%’;  >FLUSH PRIVILEGES;   * Konfigurasi Roundcube  1. Apt install roundcube 2. Pilih NO pada bagian pertanyaan konfigurasi database 3. Import terlebih dahulu database yang ada pada /usr/share/roundcube/SQL/mysql.initial.sql ke database roundcube yang sudah kita buat tadi      1. Edit file nano /etc/roundcube/config.inc.php seperti diatas      1. Edit file /etc/roundcube/debian.db.php pastikan semua cocok dengan yang sudah dikonfigurasi      * Membuat vitual host untuk webmail.itnsa.id   1. Edit file /etc/apache2/sites-available/000-default.conf  Tambahkan konfigurasi berikut dipaling bawah, pastikan dokumenrootnya sudah benar    2. Terakhir restart semua service yang berhubungan.   * Pengujian Mail   1. >LNXCLT> Firefox> ketik mail.inaskills2017.com  2. Jika berhasil akan muncul halaman login sepreti ini |



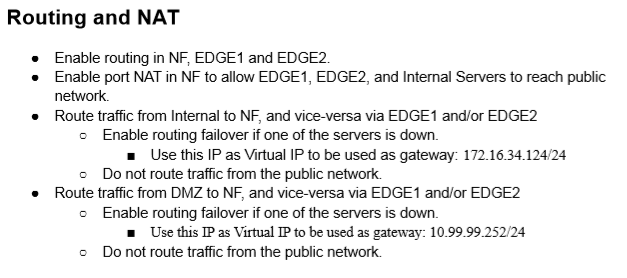
|  |
| --- |
| Pada bagian ini kita akan membuat DHCP dan TFTP server , netboot pada NF dan DHCP Relay pada EDGE 1,2, pastikan gateway yang digunakan pada NF sudah benar yaitu ip virtual EDGE atau yang mengarah pada EDGE.   1. Apt install isc-dhcp-server tftpd-hpa syslinux pxelinux nfs-kernel-server syslinux-utils syslinux 2. Nano etc/dhcp/dhcpd.conf      1. Nano /etc/default/isc-dhcp-server.conf      1. Restart dhcp /etc/init.d/isc-dhcp/server restart 2. Selanjutnya membuat directory untuk tftp 3. Mkdir -p /srv/tftp /srv/nfs1 4. Edit fie /etc/default/tftp-hpa sesuaikan dengan directory yang sudah dibuat.      1. Restart servicenya | systemctl restart tftpd-hpa 2. Siapkan Debian net boot  * wget https://deb.debian.org/debian/dists/bullseye/main/installer-amd64/current/images/netboot/netboot.tar.gz * wget <https://deb.debian.org/debian/dists/bullseye/main/installer-amd64/current/images/netboot/pxelinux.0>  1. cd /srv/tftp 2. tar xzvf ~/netboot.tar.gz 3. cp /usr/lib/syslinux/memdisk /srv/tftp/ 4. ln -s /srv/tftp/debian-installer/amd64/bootnetx64.efi /srv/tftp/   Membuat DHCP Relay pada EDGE 1 & 2   1. Buka server manager> add roles and features> next sampai server roles 2. Pilih remote access      1. Pilih routing pada features 2. Tools> routing and remote access> ipv4> general> new routing protocol> DHCP relay 3. DHCP Relay Agent> klik kanan new Interface> pilih intrerface yang akan menghubungkan DHCP relay> ok 4. DHCP Relay Agent > klik kanan properties> add nf (server address)> ok 5. Pengujian dilakukan pada client, pastikan client berada di interface yang sesuai dan mendapatkan DHCP dan OS dari netboot yang tadi dibuat. |



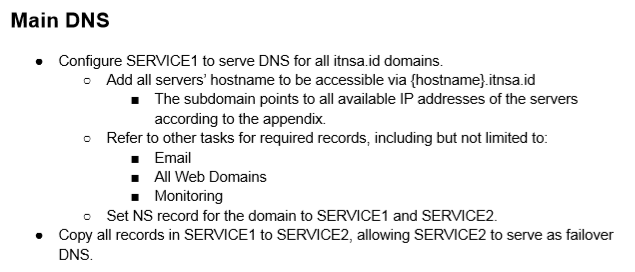
|  |
| --- |
| Pada bagian ini kita akan membuat website secara manual dan dengan menggunakan powershel ise,  Pastikan kamu sudah membuat certificate untuk digunkan pada web https dan membuat user local sesuai permintaan soal  Dan pastikan juga kamu sudah membuat dns record untuk masing’ website yang akan dibuat.  Install IIS   1. Buka server manager 2. Add roles and futures > next 3x> pada bagian server roles pilih web server (IIS)> next 3. Pada bagian role service pilih basicauthentication 4. Next terus sampai install   Add website   1. Buka Server manager> tools 2. Pilih IIS manager 3. Kilk kanan pada sites> add website      1. Isi site name sesuai dengan hostnamenya juga, isi physical path sesuai ketentuan soal> ok 2. Buat file Default.htm didalam masing’ folder sesuai permintaan soal 3. Restart website   Pengujian dilakukan pada edge atau browse nama website yg sudah dibuat  Add website use powershell ise   1. Buka powershell ise   $i=1..25 | foreach {  $j="{0:00}" -f $\_  mkdir C:\web\ops$j­  cd C:\web\ops$j  $k=Get-Location  “isi file html” > $k\Default.htm  }  $i=1..25 | foreach {  $j="{0:00}" -f $\_  "$j"}  foreach ($k in $i) {  New-Website -Name ops$k.itnsa.id -HostHeader ops$k.itnsa.id -port 80 -PhysicalPath C:\web \ops$k  $filter=""system.webserver/defaultdocument/files""  $site=""IIS:\Sites\ops$k.itnsa.is""  Add-WebConfiguration $filter $site -AtIndex 0 -Value @{value=""users.html""}  }  Enable HTTPS  Pastikan sudah mengimport file CA, Intermediate, dan Certificate server ke windows server dalam file .pfx dan sudah ditanda tangani dengan benar dan sesuai.  install file certificate dan import melalui mmc di folder Webhosting.  CA > trusted root cert  Intermediate > intermediate Certification auth  Certificate Server > Webhosting  dan tinggal dipilih di konfigurasi web di iisnya   1. Export cer to pfx in linux   openssl pkcs12 -export -out certificate.pfx -inkey privateKey.key -in certificate.crt  \*note isi password Skills39   1. Kirim certificate ke windows 2. Buka powershell ise   $PlainTextPass = "Skills39"  $pfxpass = $PlainTextPass |ConvertTo-SecureString -AsPlainText -Force  Import-PfxCertificate -FilePath C:\path\to\certificate.pfx -CertStoreLocation Cert:\LocalMachine\My -Password $pfxpass   1. Windows+r > mmc > file> add/remove snap in> certificate>add> computer users> finish> ok 2. Console root> personal>certificate pastikan sertifikat sudah ada disitu 3. Buka server manager> tools> iis manager 4. Klik kanan pada website yang akan menggunakan https > edit bindings> add> ubah type menjadi https, isi hostname dan select ssl certificate > ok   Pengujian dapdat dilakukan dengan cara browse website menggunakan port 443 atau https://  Enable Basic Authentication   1. Diawal kita sudah membuat local user sesuai permintaan soal 2. Klik pada website yang akan enable authnya 3. Pilih authentication 4. Disable anonymous auth 5. Enable basic auth 6. Restart website   Pengujian dapat dilakukan dengan browse website |



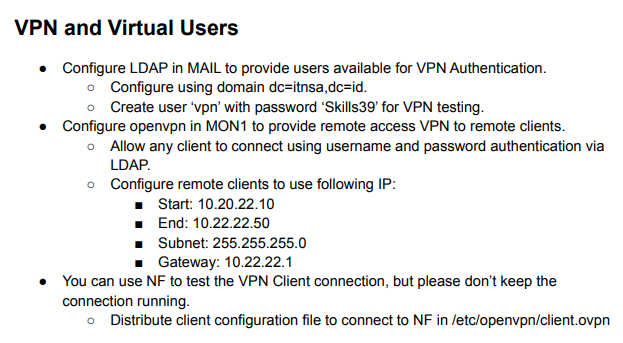
|  |
| --- |
| Pada bagian ini kita akan mengkonfigurasi file smb.conf dan enable logon guest pada windowsnya   * STORAGE  1. Apt install samba cifs-utils 2. Mkdir /share 3. Chmod 777 /share 4. Nano /etc/samba/smb.conf   [shared]  path = /path/to/shared/folder  read only = no  guest ok = yes   1. Systemctl restart smbd  * WINDOWS SERVER  1. On the Windows Server, open the Local Group Policy Editor by typing gpedit.msc in the Run dialog (Win+R). 2. Navigate to Computer Configuration > Administrative Templates > Network > Lanman Workstation. 3. Double-click "Enable insecure guest logons" and select "Enabled". 4. Save and exit the Local Group Policy Editor. 5. On the Windows Server, open the Run dialog (Win+R), type \\debian\_hostname (replace debian\_hostname with the actual hostname or IP address of your Debian machine), and press Enter. 6. The shared folder should now be mounted on the Windows Server and accessible like any other folder.   Create Back up   1. Buka server manager > add roles future 2. Pada bagian features pilih windows server backup 3. Tools> windows server backup 4. Pada section action pilih Backup Schedule 5. Next > isi sesuai keperluan |



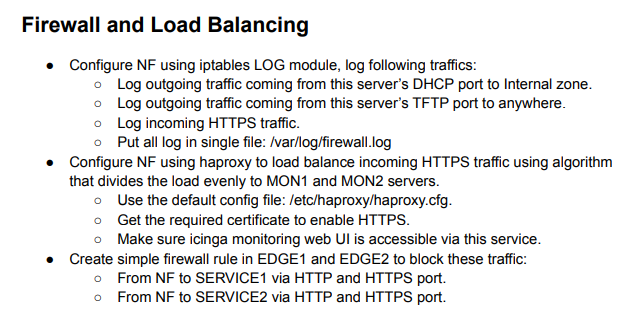
|  |
| --- |
| * NF   enable forward  nano /etc/sysctl.conf  uncomment dan ubah jadi 1 pada line 28  net.ipv4.ip\_forward=1  cek dengann  #sysctl -p   * EDGI 1 & 2   membuat virtual ip biasa   1. windows+r 2. ncpa.cpl > enter 3. pilih interface yang akan dibuat virtual ip nya 4. properties> pilih tcp/ipv4 5. advance> add 6. isi virtual ip dan subnetmask   Membuat virtual ip dan failover dengan cluster  Pada bagian ini kita akan membuat cluster disalah satu edge, lalu connect cluster di edge lainnya,  Pada saat create cluster kita bisa add servernya dengan ip lain (bukan ip interface ataupun vitual ipnya) lalu pada saat membuat role untuk clusternya baru add ipvirtualnya.   1. buka manager server > manage 2. add roles dan futures > next sampai dengan bagian features 3. failover Clustering> next sampai install 4. tools> Cluster-Aware updating> open failover cluster manager 5. create cluster>next 6. pada bagian select server, add hostname server (edge1, edge2)> next 7. pada bagian validation(opsional) 8. pada bagian accesss point for admin cluster beri nama unutuk clusternya, lalu add ip yang bukan ip interface atau pun ip virtual yang akan dibuat nanti 9. next sampai finish   Membuat roles failover untuk cluster   1. klik kanan pada cluster yang sudah dibuat tadi> configure cluster 2. next> generic service> pilih routing dan remote access 3. isi sesuai permintaan soal, buat client access name dan tambahkan ip virutalnya, 4. finish/oke     Lalu pada edge 2 bisa langsung connect cluster yang sudah dibuat tadi  Pengujian dilakukan dengan mendisable interface pada salah satu server dan di ping, jika failover berhasil maka akan tetap berhasil diping. |



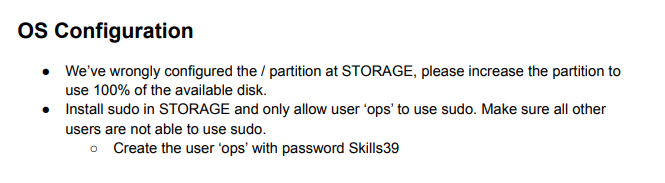
|  |
| --- |
| 1. Buka server manager 2. Tools> pilih DNS      1. Klik kanan pada forward lookup > new zone 2. Klik next dan isi zone name dan yang lainnya sesuai permintaan soal 3. Setelah itu klik kanan pada reverse lookup 4. Pilih ipv4 reverse lookup zone> next 5. Isi network id> next dan isi sesuai permintaan soal   Create sub domain     1. Klik kanan pada file forward yang sudah dibuat 2. Pilih new host (A or AAA) 3. Isi name sesuai sub domain yang diminta 4. Dan isi ip addressnya> add host   Melalui powershell ise  Membuat file csv    Lalu add dns recordnya    For dns failover on service2   1. Install the DNS Server role on both SERVICE1 and SERVICE2:  * Open Server Manager. * Click on "Add roles and features." * Select the appropriate server and click Next. * Choose the "DNS Server" role and complete the installation.  1. Configure DNS on SERVICE1:  * Open DNS Manager. * Expand the server name and select the "Forward Lookup Zones" folder. * Right-click on the zone you want to replicate and select "Properties." * Go to the "Zone Transfers" tab. * Select the option "Allow zone transfers" and choose "To any server" or specify the IP address of SERVICE2. * Click OK to save the changes.  1. Configure DNS on SERVICE2:  * Open DNS Manager. * Right-click on "Forward Lookup Zones" and select "New Zone." * Follow the wizard to create a primary zone with the same name as the zone on SERVICE1. * Once the zone is created, right-click on it and select "Properties." * Go to the "Zone Transfers" tab. * Select the option "Allow zone transfers" and choose "Only to servers listed on the Name Servers tab." * Add the IP address of SERVICE1 to the list of name servers. * Click OK to save the changes.  1. Enable zone transfer on SERVICE1:  * Open DNS Manager. * Expand the server name and select the "Forward Lookup Zones" folder. * Right-click on the zone and select "Properties." * Go to the "Name Servers" tab. * Add the IP address of SERVICE2 to the list of name servers. * Click OK to save the changes.  1. Verify the replication:  * On SERVICE1, make changes to the DNS records in the zone you want to replicate. * Wait for the replication to occur, or you can force it by right-clicking on the zone and selecting "Transfer from Master." * Check the DNS records on SERVICE2 to ensure they have been replicated.     **\*dns primary on service1 && dns secondary on service2** |



|  |
| --- |
| Pada bagian ini pastikan sudah memiliki certificate untuk server dan client, pada soal ini menggunakan CA, intermediate CA, cert server dan client.  Buat file ta.key dan dh dh2048 pada server lalu di copy pada client   * MAIL  1. apt-get install slapd ldap-utils libpam-ldapd libnss-ldapd 2. sudo dpkg-reconfigure slapd 3. nano base.ldif   dn: ou=VPN,dc=itnsa,dc=id  objectclass: organizationalUnit   1. ldapadd -x -D "cn=admin,dc=itnsa,dc=id" -W -f base.ldif 2. nano users.ldif   dn: cn=uservpn1,ou=VPN,dc=itnsa,dc=id  objectclass: posixGroup  gidnumber: 501  another way     1. ldapadd -x -D "cn=admin,dc=itnsa,dc=id" -W -f users.ldif 2. slapcat 3. Lalu edit file nslcd.conf dan ubah suaikan seperti gambar # nano /etc/nslcd.conf Text     Description automatically generated 4. Selanjutnya edit file nsswitch.conf   # nano /etc/nsswitch.conf  Text  Description automatically generated   1. Reboot dan tes login  * MON1   Copy semua ca,intermediate dan certificate server dari MAIL dan sesuaikan peletakkannya agar mudah disesaikan pada file remote   1. apt install openvpn openvpn-auth-ldap -y 2. membuat ta.key   openvpn --genkey – secret ta.key   1. membuat dh dh2048   oenssl dhparam -out dh2048.pem 2048   1. cd /etc/openvpn 3. Cp dulu file remote.conf dari directory diatas 4. nano remote.conf   \  Penjelasan  Jika ingin menggunakan konfigurasi yang menentukan ip pool range dari ip client openvpn  . harus menggunakan dev tab  . tidak boleh menggunakan perintah server 10.22.22.0 255.255.255.0         1. salin template file dari directory diatas 2. nano auth-ldap     \*searchfilter disesuaikan dengan objectclass user.   1. systemctl restart openvpn@remote  * NF   Copy semua ca,intermediate certificate client, ta.key, dh2048 dari MON dan sesuaikan peletakkannya agar mudah disesaikan pada file client.ovpn   1. apt install openvpn -y 2. cd /etc/openvpn 3. nano client.ovpn     Karena di servernya udah pakai dev tap  Maka di clientnya juga pakai dev tap   1. pengujian   openvpn –config client.ovpn  pastikan bisa login auth  (alt+f2) ip a patikan ada tun0      \***note**  objectclass yang bisa untuk login user |



|  |
| --- |
| * iptables  1. nano /etc/rsyslog.d/50-default.conf 2. tambahkan baris berikut   kern.warning /var/log/firewall.log   1. service rsyslog restart 2. create ip tables sesuai permintaan soal:        * Haproxy   Pastikan sudah menggabungkan file kunci,file certificate dan canya pada cert yang akan digunakan.   1. apt install haproxy -y 2. nano /etc/haproxy/haproxy.cfg 3. tambahkan script berikut      1. sudo haproxy -c -f /etc/haproxy/haproxy.cfg 2. sudo systemctl start haproxy   pengujian dilakukan dengan curl atau membuka domain web dan melihat lognya. |



|  |
| --- |
| 1. Check the current partition size and available space using the df command:   #df -h   1. Identify the partition that you want to resize, and note the device name (e.g. /dev/sda1). 2. Use the fdisk command to resize the partition. The exact steps will depend on the current partition layout, but generally you will need to delete the existing partition and create a new one with the desired size.   #fdisk /dev/sda  d # delete the existing partition  n # create a new partition  w # write the changes and exit   1. Reboot the system to ensure that the partition table changes are recognized. 2. Use the resize2fs command to resize the file system to the new partition size. Replace /dev/sda1 with the device name of the partition you resized:   #resize2fs /dev/sda1   1. Check the partition size and available space again using the df command   #df -h   1. Adduser ops 2. Berikan password ‘Skills39’ 3. apt install sudo 4. visudo |