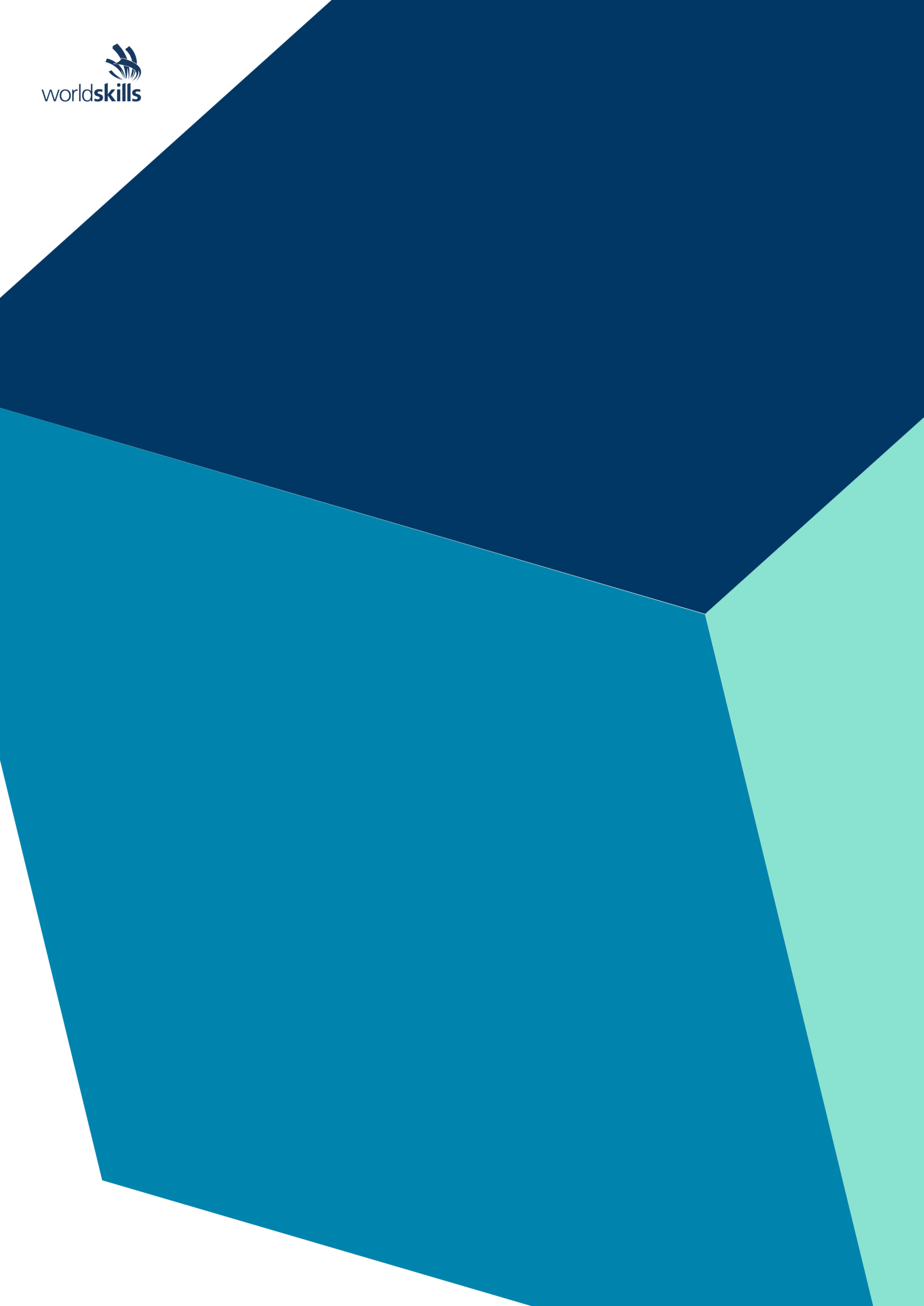
Test Project



*IT Network Systems Administration Module D – Linux Environment*

### Submitted by: ITNSA-ID Team

LKSN2019\_ITNSA

**Contents**

[INTRODUCTION 3](#_bookmark0)

[PART I BASIC CONFIGURATION 4](#_bookmark1)

[PART II (CLOUD) 4](#_bookmark2)

[PART III (EDGE) 6](#_bookmark3)

[PART IV (INTERNAL & CLIENT) 7](#_bookmark4)

[APPENDIX 8](#_bookmark5)

[SPECIFICATION 8](#_bookmark6)

[NETWORK DIAGRAM 11](#_bookmark7)

**Introduction to Test Project**

## This Test Project proposal consists of the following document/file:

* LKSN2019\_ITNETWORK\_MODUL-D.pdf

# Introduction

The competition has a fixed start and finish time. You must decide how to best divide your time. Please carefully read the following instructions!

When the competition time ends, please leave your station in a running state.

#### PHYSICAL MACHINE (HOST) FOLDER PATHS

Virtual Machines : D:\KOMPETISI\VM ISO Images : D:\KOMPETISI\ISO

Password for VMs Pre-Install: Skill39

Note: Please use the default configuration if you are not given details.

# PART I BASIC CONFIGURATION

## WORK TASK ALL VMs.

#### INSTALL SYSTEM TOOLS

* Install **smbclient**, **curl**, **lynx**, **dnsutils**, **ldap**-**utils**, **ftp**, **lftp**, **wget**, **ssh**, **nfs**-**common**, **rsync**, **telnet**, **traceroute** on **all VMs**.

#### CONFIGURE LOGIN BANNER

* Must be shown before the login prompt. Must appear for local and network(ssh) logins with message below without double quote and change Hostname accordingly.

“Welcome to [Hostname] - SMK Hebat”

* Example:

Welcome to lks-lb - SMK Hebat

Manual

|  |
| --- |
| # apt install -y smbclient curl lynx dnsutils ldap-utils ftp lftp wget ssh nfs-common rsync telnet traceroute  # hostnamectl set-hostname lks-lb  # nano /etc/hosts  127.0.0.1 localhost  127.0.1.1 lks-lb.itnsaskills.cloud lks-lb |

Automation

|  |
| --- |
| Node Host |
| root@node:~# apt install -y ssh  root@node:~# nano /etc/ssh/sshd\_config; service ssh restart  ......  ...  PermitRootLogin yes  ...  ...... |
| Ansible Host |
| root@ansible:~# ssh-keygen  root@ansible:~# ssh-copy-id root@node  root@ansible:~# apt install -y ansible sshpass  root@ansible:~# nano /etc/ansible/hosts  ......  ...  [node-lks]  lks-i-srv ansible\_host=10.2.2.10 ansible\_user=root  lks-lb ansible\_host=10.1.1.10 ansible\_user=root  lks-srv1 ansible\_host=10.1.1.20 ansible\_user=root  lks-srv2 ansible\_host=10.1.1.30 ansible\_user=root  lks-internal-edge ansible\_host=172.17.1.254 ansible\_user=root  lks-cloud-edge ansible\_host=172.17.1.253 ansible\_user=root  root@ansible:~# nano basic\_configuration.yml  ---  - name: Basic Configuration  hosts: node-lks  tasks:  - name: Install Tools  shell: "echo 'samba-common samba-common/workgroup string WORKGROUP' | debconf-set-selections;echo 'samba-common samba-common/dhcp boolean true' | debconf-set-selections;echo 'samba-common samba-common/do\_debconf boolean true' | debconf-set-selections;apt install -y smbclient curl lynx dnsutils ldap-utils ftp lftp wget ssh nfs-common rsync telnet traceroute"  - name: Configure Hostname  hostname:  name="{{ inventory\_hostname }}"  - name: Configure /etc/issue  lineinfile:  path: /etc/issue  regexp: '^Debian'  line: Welcome to {{ inventory\_hostname }} - SMK Hebat  - name: Configure Banner  lineinfile:  path: /etc/ssh/sshd\_config  regexp: '^#Banner'  line: Banner /etc/issue  - name: Restarting SSH  service:  name: ssh  state: restarted |

#### CONFIGURE THE HOSTNAME, USER CREATION AND IP ACCORDING TO APPENDIX.

# PART II (CLOUD)

## WORK TASK SERVER LKS-LB

#### DNS (bind9)

* Configure a forward zone called “**itnsaskills.cloud**”
* Create for each host an A record to the respective IP in the **cloud zones**.
* Create a CNAME record for ‘**www**’ that point to the appropriate host that serves websites for all clients.
* Create A record for ‘**mail**’ that points to the mail server.
* Create the appropriate **MX** records.
* Configure a reverse zone for each host defined for network **10.1.1.0/24**.
* Configure multiple views DNS for external and internal client, with the specification below:
* External client will resolve [**www.itnsaskills.cloud**](http://www.itnsaskills.cloud/) to **172.17.1.253**.
* Internal client will resolve [**www.itnsaskills.cloud**](http://www.itnsaskills.cloud/) to **10.1.1.10**.

|  |
| --- |
| root@lks-lb:~# cat /etc/bind/rndc.key >> /etc/bind/named.conf.local |
| db.itnsaskills-int |
| ;  ; BIND data file for local loopback interface  ;  $TTL 604800  @ IN SOA itnsaskills.cloud. root.itnsaskills.cloud. (  2 ; Serial  604800 ; Refresh  86400 ; Retry  2419200 ; Expire  604800 ) ; Negative Cache TTL  ;  @ IN NS itnsaskills.cloud.  @ IN A 10.1.1.10  @ IN MX 10 mail  lks-lb IN A 10.1.1.10  lks-srv1 IN A 10.1.1.20  lks-srv2 IN A 10.1.1.30  lks-cloud-edge IN A 10.1.1.254  mail IN A 10.1.1.20  www IN CNAME lks-lb |
| db.itnsaskills-ext |
| ;  ; BIND data file for local loopback interface  ;  $TTL 604800  @ IN SOA itnsaskills.cloud. root.itnsaskills.cloud. (  2 ; Serial  604800 ; Refresh  86400 ; Retry  2419200 ; Expire  604800 ) ; Negative Cache TTL  ;  @ IN NS itnsaskills.cloud.  @ IN A 192.168.1.15  lks-cloud-edge IN A 192.168.1.15  www IN CNAME lks-cloud-edge |
| db.10 |
| ;  ; BIND reverse data file for local loopback interface  ;  $TTL 604800  @ IN SOA itnsaskills.cloud. root.itnsaskills.cloud. (  1 ; Serial  604800 ; Refresh  86400 ; Retry  2419200 ; Expire  604800 ) ; Negative Cache TTL  ;  @ IN NS itnsaskills.cloud.  10.1.1 IN PTR lks-lb.itnsaskills.cloud.  20.1.1 IN PTR lks-srv1.itnsaskills.cloud.  30.1.1 IN PTR lks-srv2.itnsaskills.cloud.  254.1.1 IN PTR lks-cloud-edge.itnsaskills.cloud. |
| named.conf.local |
| acl internal\_network { 10.1.1.0/24; 10.2.2.0/24; 10.2.3.0/24; };  key "itnsaskills" {  algorithm hmac-md5;  secret "rWJPyivsgOas6XJj2hUf8g==";  };  view "internal" {  match-clients { internal\_network; };  zone "itnsaskills.cloud" {  type master;  file "/var/cache/bind/db.itnsaskills-int";  allow-update { key itnsaskills; };  };  zone "10.in-addr.arpa" {  type master;  file "/var/cache/bind/db.10";  allow-update { key itnsaskills; };  };  };  view "external" {  match-clients { any; };  zone "itnsaskills.cloud" {  type master;  file "/var/cache/bind/db.itnsaskills-ext";  };  }; |
| named.conf |
| // This is the primary configuration file for the BIND DNS server named.  //  // Please read /usr/share/doc/bind9/README.Debian.gz for information on the  // structure of BIND configuration files in Debian, \*BEFORE\* you customize  // this configuration file.  //  // If you are just adding zones, please do that in /etc/bind/named.conf.local  include "/etc/bind/named.conf.options";  include "/etc/bind/named.conf.local";  // include "/etc/bind/named.conf.default-zones"; |

#### Load balancer (HAProxy)

* Configure HTTP & HTTPS load balancer for [**www.itnsaskills.cloud**,](http://www.itnsaskills.cloud/) which is hosted by lks-srv1 and lks-srv2.
* Use roundrobin as algorithm.

|  |
| --- |
| /etc/bind/haproxy.cfg |
| ......  ....  frontend http\_frontend  bind \*:80  bind \*:443 ssl crt /etc/ssl/private/server.pem  default\_backend http\_backend  backend http\_backend  balance roundrobin  option forwardfor  option httpclose  server lks-srv1 10.1.1.20:443 ssl verify none  server lks-srv1 10.1.1.30:443 ssl verify none |

#### SSH

* Use key based for SSH authentication.
* Disable root login.
* Create a new Local User named “cloudops” with password: Skill39.
* Install sudo and then add Local User named “cloudops” to sudo group.
* Change SSH port default to 2019.
* Make sure user “competitor” in lks-i-client and lks-e-client can SSH to user “cloudops” in lks-lb without password.

|  |
| --- |
| lks-lb |
| root@lks-lb:~# apt install -y ssh sudo  root@lks-lb:~# adduser cloudops  Adding user `cloudops’ ...  Adding new group `cloudops’ (1001) ...  Adding new user `cloudops’ (1001) with group `cloudops’ ...  Creating home directory `/home/cloudops’ ...  Copying files from `/etc/skel’ ...  New password: \*fill Skill39  Retype new password: \*fill Skill39  ...  ......  root@lks-lb:~# usermod -aG sudo cloudops  root@lks-lb:~# nano /etc/ssh/sshd\_config; service ssh restart  ......  ....  Port 2019  ....  PermitRootLogin no  ....  ...... |
| lks-i-client and lks-e-client as competitor user |
| competitor@lk-client:~$ ssh-keygen  Generating public/private rsa key pair.  Enter file in which to save the key (/home/competitor/.ssh/id\_rsa): (just enter)  Created directory ‘/home/competitor/.ssh’.  Enter passphrase (empty for no passphrase): (just enter)  Enter psame passphrase again: (just enter)  ......  ....  ..  competitor@lks-client:~$ ssh-copy-id cloudops@lks-lb |

## WORK TASK SERVER LKS-SRV1

#### LDAP (OPENLDAP)

* + Configure the directory service of **itnsaskills.cloud**
  + Create users with OU and password specified in the appendix
  + Mail services should be available for LDAP users.

|  |
| --- |
| root@lks-srv1:~# apt install -y slapd ldapscripts  Configuring slapd  Administrator password: |
| +-----------------------------| Configuring slapd |---------------------------+  | Please enter the password for the admin entry in your LDAP directory. |  | |  | Administrator password: |  | |  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  | |  | <Ok> |  +-----------------------------------------------------------------------------+ |
| +-----------------------------| Configuring slapd |---------------------------+  | Please enter the admin password for your LDAP directory again to verify |  | that you have typed it correctly. |  | |  | Confirm password: |  | |  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  | |  | <Ok> |  +-----------------------------------------------------------------------------+ |
| root@lks-srv1:~# dpkg-reconfigure slapd |
| +-----------------------------| Configuring slapd |---------------------------+  | If you enable this option, no initial configuration or database will be |  | created for you. |  | |  | Omit OpenLDAP server configuration? |  | |  | <Yes> <No> |  +-----------------------------------------------------------------------------+ |
| +-----------------------------| Configuring slapd |---------------------------+  | The DNS domain name is used to construct the base DN of the LDAP directory |  | For example, ‘foo.example.org’ will create the directory with |  | ‘dc=foo, dc=example, dc=org’ as base DN. |  | |  | DNS domain name: |  | |  | itnsaskills.cloud\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  | |  | <Ok> |  +-----------------------------------------------------------------------------+ |
| +-----------------------------| Configuring slapd |---------------------------+  | Please enter the name of the organization to use in the base DN of your | | LDAP directory. |  | |  | Organization name: |  | |  | itnsaskills.cloud\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  | |  | <Ok> |  +-----------------------------------------------------------------------------+ |
| +-----------------------------| Configuring slapd |---------------------------+  | Please enter the password for the admin entry in your LDAP directory. |  | |  | Administrator password: |  | |  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  | |  | <Ok> |  +-----------------------------------------------------------------------------+ |
| +-----------------------------| Configuring slapd |---------------------------+  | Please enter the admin password for your LDAP directory again to verify |  | that you have typed it correctly. |  | |  | Confirm password: |  | |  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  | |  | <Ok> |  +-----------------------------------------------------------------------------+ |
| +-----------------------------| Configuring slapd |---------------------------+  | HDB and BDB use similar storage formats, but HDB adds support for subtree |  | renames. Both support the same configuration options. |  | |  | ........ |  | |  | ...... |  | |  | Database backend to use: |  | |  | BDB |  | HDB |  | MDB |  | |  | <Ok> |  +-----------------------------------------------------------------------------+ |
| +-----------------------------| Configuring slapd |---------------------------+  | |  | |  | Do you want the database to be removed when slapd is purged? |  | |  | <Yes> <No> |  +-----------------------------------------------------------------------------+ |
| +-----------------------------| Configuring slapd |---------------------------+  | There are still ............... |  | |  | Move old database? |  | |  | <Yes> <No> |  +-----------------------------------------------------------------------------+ |
| root@lks-srv1:~# apt install -y libpam-ldapd |
| +-----------------------------| Configuring nslcd |---------------------------+  | Please enter the ............... |  | |  | ............... |  | |  | .................... |  | |  | LDAP server URI: |  | |  | ldap://ip\_address\_lks-srv1/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  | |  | <Ok> |  +-----------------------------------------------------------------------------+ |
| +-----------------------------| Configuring nslcd |---------------------------+  | Please enter the ............... |  | |  | LDAP server search base: |  | |  | dc=itnsaskills,dc=cloud\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  | |  | <Ok> |  +-----------------------------------------------------------------------------+ |
| +--------------------------| Configuring libnss-ldapd |-----------------------+  | For this package to work ....... |  | |  | ............... |  | |  | Name services to configure: |  | |  | [\*] passwd |  | [\*] group |  | [ ] shadow |  | [ ] hosts |  | [ ] networks |  | ..... |  | <Ok> |  +-----------------------------------------------------------------------------+ |
| root@lks-srv1:~# nano /etc/ldapscripts/ou.ldif  dn: ou=VPN,dc=itnsaskills,dc=cloud  objectclass: organizationalUnit  dn: ou=MAIL,dc=itnsaskills,dc=cloud  objectclass: organizationalUnit  dn: ou=MISC,dc=itnsaskills,dc=cloud  objectclass: organizationalUnit  dn: cn=Users\_VPN,ou=VPN,dc=itnsaskills,dc=cloud  objectclass: posixGroup  gidnumber: 500  dn: cn=Users\_MAIL,ou=MAIL,dc=itnsaskills,dc=cloud  objectclass: posixGroup  gidnumber: 501  dn: cn=Users\_MISC,ou=MISC,dc=itnsaskills,dc=cloud  objectclass: posixGroup  gidnumber: 502  root@lks-srv1:~# ldapadd -xD cn=admin,dc=itnsaskills,dc=cloud -w Skill39 -f /etc/ldapscripts/ou.ldif  root@lks-srv1:~# nano /etc/ldapscripts/ldapscripts.conf  .....  .......  SERVER=”ldap://localhost”  ..........  ....  USUFFIX=”ou=VPN”  ..........  BINDDN=”cn=admin,dc=itnsaskills,dc=cloud”  ........  #BINDPWDFILE=”......”  ...............  BINDPWD=”Skill39”  ............  USHELL=”/bin/bash”  UHOMES=”/home/%u”  CREATEHOMES=”yes”  ..........  PASSWORDGEN=”echo Skill39”  ............  root@lks-srv1:~# nano /etc/ldapscripts/users\_VPN.sh  #!/bin/bash  for x in `se 1 10`  do  ldapadduser vpnuser$x Users\_VPN  done  root@lks-srv1:~# nano /etc/ldapscripts/users\_MAIL.sh  #!/bin/bash  for x in `se 11 20`  do  ldapadduser mailuser$x Users\_MAIL  done  root@lks-srv1:~# nano /etc/ldapscripts/users\_MISC.sh  #!/bin/bash  for x in `se 21 99`  do  ldapadduser localuser$x Users\_MISC  done  root@lks-srv1:~# sh /etc/ldapscripts/users\_{VPN,MAIL,MISC}.sh  Successfully added user vpnuser1 to LDAP  Successfully set password for user vpnuser1  Successfully added user vpnuser1 to LDAP  Successfully set password for user vpnuser2  Successfully added user vpnuser1 to LDAP  Successfully set password for user vpnuser3  .....  ....... |

#### Mail (POSTFIX, DOVECOT)

* + Configure SMTPS (TCP 465) and IMAPS (TCP 993) server for “**itnsaskills.cloud**” domain using certificates issued by lks-i-srv.
  + Configure mail directory in “**/home/[user]/Maildir**”
  + Authentication has to be done through LDAP.
  + Make sure that the corresponding local user do not exist and make sure LDAP user cannot login locally.
  + Limit mailbox for each user to 5 MB.

|  |
| --- |
| root@lks-srv1:~# apt install -y dovecot-core dovecot-pop3d dovecot-imapd postfix |
| // Installnya ngertilah harus kayak gimana  root@lks-srv1:~# dpkg-reconfigure postfix  // Ngerti jugalah harus gimana  root@lks-srv1:~# nano /etc/postfix/main.cf  ......  ....  smtpd\_tls\_cert\_file=/etc/ssl/private/server.pem  smtpd\_tls\_key\_file=/etc/ssl/private/server.key  smtpd\_use\_tls=yes  ...  myhostname = srv1.itnsaskills.cloud  .....  mydestination = srv1.itnsaskills.cloud, itnsaskills.cloud  ........  mailbox\_size\_limit = 5120000  message\_size\_limit = 5120000  .....  home\_mailbox = Maildir/  smtpd\_sasl\_type = dovecot  smtpd\_sasl\_path = private/auth  smtpd\_sasl\_auth\_enable = yes  broken\_sasl\_auth\_clients = yes  root@lks-srv1:~# nano /etc/postfix/master.cf  .....  smtps inet n - y - - smtpd  -o syslog\_name=postfix/smtps  -o smtpd\_tls\_wrappermode=yes  # .....  # ..  root@lks-srv1:~# nano /etc/dovecot/conf.d/10-{auth,master,mail,ssl}.conf  /etc/dovecot/conf.d/10-auth.conf file  ##  ## Authentication processes  ##  ...  .....  disable\_plaintext\_auth = no  ..  .....  auth\_mechanism = plain login  /etc/dovecot/conf.d/10-master.conf file  #default\_process\_limit = 100  #default\_client\_limit = 1000  ..  ....  service imap-login {  inet\_listener imap {  port = 143  }  inet\_listener imaps {  port = 993  ssl = yes  }  ..  }  service pop3-login {  inet\_listener imap {  port = 110  }  inet\_listener pop3s {  port = 995  ssl = yes  }  ..  }  service auth {  ..  # Postfix smtp-auth  unix\_listener /var/spool/postfix/private/auth {  mode = 0666  user = postfix  group = postfix  }  }  /etc/dovecot/conf.d/10-mail.conf file  ##  ## Mailbox locations and namespaces  ##  ...  .....  mail\_location = maildir:~/Maildir  .......  # mail\_location = mbox:~/mail:INBOX=/var/mail/%u  /etc/dovecot/conf.d/10-ssl.conf file  ##  ## SSL settings  ##  ..  ...  # SSL/TLS support: yes, no, required. <doc/wiki/SSL.txt>  ssl = yes  .....  ssl\_cert = </etc/ssl/private/server.pem  ssl\_key = </etc/ssl/private/server.key  root@lks-srv1:~# systemctl restart postfix dovecot |

## WORK TASK SERVER LKS-SRV1 AND LKS-SRV2

#### WEB SERVER (Apache)

* + The website page should display the following message:
  + “Welcome to ITNSA cloud on [Hostname]”
  + Add the Hostname dynamically with PHP.
  + Disable HTTP and Enable HTTPS only for both sites.
  + Use certificate signed by CA in lks-i-srv.
  + Make sure no certificate warning is shown.
  + Add the HTTP header “**X-Served-By**” with the server Hostname as the value.
  + Make sure PHP script can be run.
  + Create php info page with the filename **info.php**.
  + Install and configure **rsync** on lks-srv1 and synchronize **/var/www** directory (recursive) from lks-srv1 to lks-srv2.
  + Configure crontab to automatically synchronize for every minute.

|  |
| --- |
| lks-srv1 and lks-srv2 |
| root@server:~# apt install -y apache2 php  root@server:~# nano /var/www/html/index.php; rm /var/www/html/index.html  <?php  header(“X-Served-By: ”.gethostname());  echo “Welcome to ITNSA cloud on ”.gethostname();  ?>  root@server:~# nano /etc/apache2/ports.conf  ..  ....  # Listen 80  ..  root@server:~# cp /etc/apache2/sites-available/default-ssl.conf /etc/apache2/sites-available/itnsa-ssl.conf  .....  ..  SSLEngine on  .....  SSLCertificateFile /etc/ssl/private/server.pem  SSLCertificateKeyFile /etc/ssl/private/server.key  ....  root@server:~# a2enmod ssl; a2ensite itnsa-ssl.conf; a2dissite 000-default.conf  root@server:~# service apache2 restart  root@server:~# nano /var/www/html/info.php  <?php  phpinfo();  ?> |
| lks-srv2 |
| root@lks-srv2:~# apt install -y ssh  // Allow SSH root access |
| lks-srv1 |
| root@lks-srv1:~# ssh-keygen  // Enter enter aja gak usah masukin password atau apa udah  root@lks-srv1:~# ssh-copy-id 10.1.1.30  ..  ....  root@lks-srv1:~# crontab -e  no crontab for root – using an empty one  Select an editor. To change later, run ‘select-editor’.   1. /bin/nano <---- easiest 2. /usr/bin/vim.tiny   Choose 1-2 [1]: 1  .....  \* \* \* \* \* rsync -av –delete /var/www/ root@10.1.1.30:/var/www/ |

Reference:

<https://crontab.guru/>

# PART III (EDGE)

## WORK TASK LKS-INTERNAL-EDGE & LKS-CLOUD-EDGE

#### ROUTING

* + Enable routing to forward IPv4 packet.
  + Consider the different VLANs on the **lks-internal-edge**.

|  |
| --- |
| lks-internal-edge and lks-cloud-edge |
| root@router:~# nano /etc/sysctl.conf  .....  net.ipv4.ip\_forward=1  root@router:~# sysctl -p |
| lks-internal-edge |
| // Untuk VLAN saya pernah melakukan lab dimana hanya dapat dilakukan di ESXi. Ketika saya coba di VMWare Workstation konektivitas tidak berjalan.  root@lks-internal-edge:~# nano /etc/network/interfaces  ..  .....  auto ens32  iface ens32 inet static  address 172.17.1.254/24  auto ens160.20  iface ens160.20 inet static  address 10.2.2.254/24  auto ens160.30  iface ens160.30 inet static  address 10.2.3.254/24 |

#### SITE TO SITE VPN (OPENVPN)

* + Configure site-to-site VPN between **lks-internal-edge** and **lks-cloud-edge**.
  + Use **tun0** interface with IP: **10.0.0.1** for **lks-internal-edge** and **10.0.0.2** for **lks-cloud-edge**.
  + Use port **1194** for both.
  + Traffic from **internal server network** to **cloud network** and vice versa should use the VPN (static route via IP tun0).
  + Site to site VPN connection should be established automatically and be always on.

|  |
| --- |
| lks-internal-edge and lks-cloud-edge |
| root@router:~# apt install -y openvpn  root@lks-internal-edge:~# nano /etc/openvpn/s2s.conf  remote 172.17.1.253  dev tun  port 1194  ifconfig 10.0.0.1 10.0.0.2  route 10.1.1.0 255.255.255.0  // Config file s2s.conf pada lks-cloud-edge hanya tinggal dirubah menyesuaikan saja  root@router:~# systemctl restart openvpn@s2s; systemctl enable openvpn@s2s |

#### FIREWALL (IPTABLES) ON CLOUD EDGE

* + Configure default policy for the **INPUT** & **FORWARD** chains should be drop.
  + Make sure that firewall operates in stateful mode.
  + Configure DNAT for **DNS**, **HTTPS**, **SSH** (TCP 2019) to **lks-lb** using IP external of **lks-cloud-edge**.
  + Configure DNAT for **IMAPS** (TCP 993) and **SMTPS** (TCP 465) to **lks-srv1** using IP external of **lks- cloud-edge.**
  + Configure **INPUT** chain to allow **ICMP**, **DNS**, **HTTPS**, **SSH** (TCP 2019), **IMAPS** (TCP 993), SMTPS (TCP 465), **LDAP**, **VPN** traffic.
  + Configure FORWARD chain to allow the following traffic from any network to the IP of lks-lb & lks- srv1:

###### ICMP

###### DNS

###### HTTPS

###### SSH

###### IMAPS

###### SMTPS

###### LDAP

* + All other traffic should be prohibited.

|  |
| --- |
| lks-cloud-edge |
| root@lks-cloud-edge:~# iptables -P INPUT DROP  root@lks-cloud-edge:~# iptables -t nat -A PREROUTING -d 172.17.1.253 -p udp --dport 53 -j DNAT --to 10.1.1.10  root@lks-cloud-edge:~# iptables -A INPUT -p icmp -m state –-state NEW, ESTABLISHED -j ACCEPT  root@lks-cloud-edge:~# iptables-save > /root/iptables; nano /root/iptables  # .....  \*filter  :INPUT DROP [0:0]  :FORWARD DROP [0:0]  :OUTPUT ACCEPT [0:0]  -A INPUT -p icmp -m state --state NEW,ESTABLISHED -j ACCEPT  -A INPUT -p udp -m udp --dport 53 -m state --state NEW,ESTABLISHED -j ACCEPT  -A INPUT -p tcp -m tcp --dport 443 -m state --state NEW,ESTABLISHED -j ACCEPT  -A INPUT -p tcp -m tcp --dport 2019 -m state --state NEW,ESTABLISHED -j ACCEPT  -A INPUT -p tcp -m tcp --dport 993 -m state --state NEW,ESTABLISHED -j ACCEPT  -A INPUT -p tcp -m tcp --dport 465 -m state --state NEW,ESTABLISHED -j ACCEPT  -A INPUT -p tcp -m tcp --dport 389 -m state --state NEW,ESTABLISHED -j ACCEPT  -A INPUT -p udp -m udp --dport 1194 -m state --state NEW,ESTABLISHED -j ACCEPT  -A INPUT -p udp -m udp --dport 1195 -m state --state NEW,ESTABLISHED -j ACCEPT  -A FORWARD -d 10.1.1.10 -p icmp -m state --state NEW,ESTABLISHED -j ACCEPT  -A FORWARD -d 10.1.1.10 -p udp -m udp --dport 53 -m state --state NEW,ESTABLISHED -j ACCEPT  -A FORWARD -s 10.1.1.10 -p udp -m udp --dport 53 -m state --state NEW,ESTABLISHED -j ACCEPT  -A FORWARD -d 10.1.1.10 -p tcp -m tcp --dport 443 -m state --state NEW,ESTABLISHED -j ACCEPT  -A FORWARD -s 10.1.1.10 -p tcp -m tcp --dport 443 -m state --state NEW,ESTABLISHED -j ACCEPT  -A FORWARD -d 10.1.1.10 -p tcp -m tcp --dport 2019 -m state --state NEW,ESTABLISHED -j ACCEPT  -A FORWARD -d 10.1.1.20 -p tcp -m tcp --dport 993 -m state --state NEW,ESTABLISHED -j ACCEPT  -A FORWARD -s 10.1.1.20 -p tcp -m tcp --dport 993 -m state --state NEW,ESTABLISHED -j ACCEPT  -A FORWARD -d 10.1.1.20 -p tcp -m tcp --dport 465 -m state --state NEW,ESTABLISHED -j ACCEPT  -A FORWARD -s 10.1.1.20 -p tcp -m tcp --dport 465 -m state --state NEW,ESTABLISHED -j ACCEPT  -A FORWARD -d 10.1.1.20 -p tcp -m tcp --dport 389 -m state --state NEW,ESTABLISHED -j ACCEPT  -A FORWARD -s 10.1.1.20 -p tcp -m tcp --dport 389 -m state --state NEW,ESTABLISHED -j ACCEPT  COMMIT  # Completed on Thu Jun 24 08:24:57 2021  # Generated by xtables-save v1.8.2 on Thu Jun 24 08:24:57 2021  \*nat  :PREROUTING ACCEPT [0:0]  :INPUT ACCEPT [0:0]  :POSTROUTING ACCEPT [0:0]  :OUTPUT ACCEPT [0:0]  -A PREROUTING -d 172.17.1.253/32 -p udp -m udp --dport 53 -j DNAT --to-destination 10.1.1.10  -A PREROUTING -d 172.17.1.253/32 -p tcp -m tcp --dport 443 -j DNAT --to-destination 10.1.1.10  -A PREROUTING -d 172.17.1.253/32 -p tcp -m tcp --dport 2019 -j DNAT --to-destination 10.1.1.10  -A PREROUTING -d 172.17.1.253/32 -p tcp -m tcp --dport 993 -j DNAT --to-destination 10.1.1.20  -A PREROUTING -d 172.17.1.253/32 -p tcp -m tcp --dport 465 -j DNAT --to-destination 10.1.1.20  COMMIT  root@lks-cloud-edge:~# iptables-restore < /root/iptables |

#### FIREWALL (IPTABLES) ON INTERNAL EDGE

* + Configure default policy for the INPUT & FORWARD chains should be drop.
  + Make sure that firewall operates in stateful mode.
  + Configure INPUT chain to allow VPN traffic.
  + Configure FORWARD chain to allow all traffic from internal client & VPN network to all networks.

##### Configure source NAT for internet access from internal client network only.

* + All other traffic should be prohibited.

|  |
| --- |
| lks-internal-edge |
| root@lks-internal-edge:~# iptables -P INPUT DROP  root@lks-internal-edge:~# iptables -A INPUT -p udp --dport 1194 -m state –-state NEW, ESTABLISHED -j ACCEPT  root@lks-internal-edge:~# iptables -A INPUT -p udp --dport 1195 -m state –-state NEW, ESTABLISHED -j ACCEPT  root@lks-internal-edge:~# iptables -A FORWARD -s 10.2.2.0/24 -m state –-state NEW, ESTABLISHED -j ACCEPT  root@lks-internal-edge:~# iptables -A FORWARD -s 10.2.3.0/24 -m state –-state NEW, ESTABLISHED -j ACCEPT  root@lks-internal-edge:~# iptables -A FORWARD -s 10.20.30.0/24 -m state –-state NEW, ESTABLISHED -j ACCEPT  root@lks-internal-edge:~# iptables -t nat -A POSTROUTING -s 10.2.3.0/24 -j SNAT –to 172.17.1.254 |

#### REMOTE ACCESS VPN (OPENVPN) ON INTERNAL EDGE.

* + Configure VPN access to Internal networks (server and client).
  + Use port **1195** for VPN server.
  + Configure **lks-e-client** as VPN client.
  + Use password with certificates for authentication
  + Use LDAP user with OU “VPN” for OpenVPN client login.
  + Use certificate signed by **lks-i-srv** for data encryption.
  + Network Remote Access **10.20.30.0/24**
  + Make sure default gateway is interface **tun0**

|  |
| --- |
| root@lks-internal-edge:~# apt install -y openvpn-auth-ldap; cp /usr/share/doc/openvpn-auth-ldap/examples/auth-ldap.conf /etc/openvpn/  root@lks-internal-edge:~# cp /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz /etc/openvpn/  root@lks-internal-edge:~# gunzip /etc/openvpn/server.conf.gz; nano /etc/openvpn/server.conf  .....  port 1195  ....  ca cacert.pem  cert server.pem  key server.key  ...  dh dh2048.pem  .....  ;server 10.8.0.0 255.255.255.0  Server 10.20.30.0 255.255.255.0  ....  push “redirect-gateway def1 bypass-dhcp”  ...  #tls-auth ta.key 0  .....  comp-lzo  ....  plugin /usr/lib/openvpn/openvpn-auth-ldap.so /etc/openvpn/auth-ldap.conf  root@lks-internal-edge:~# nano /etc/openvpn/auth-ldap.conf  <LDAP>  # LDAP server URL  URL ldap://10.1.1.20/  # Bind DN (If your LDAP server doesn't support anonymous binds)  BindDN cn=admin,dc=itnsaskills,dc=cloud  # Bind Password  Password Skill39  # Network timeout (in seconds)  Timeout 15  # Enable Start TLS  # TLSEnable yes  # Follow LDAP Referrals (anonymously)  FollowReferrals yes  # TLS CA Certificate File  # TLSCACertFile /usr/local/etc/ssl/ca.pem  # TLS CA Certificate Directory  # TLSCACertDir /etc/ssl/certs  # Client Certificate and key  # If TLS client authentication is required  # TLSCertFile /usr/local/etc/ssl/client-cert.pem  # TLSKeyFile /usr/local/etc/ssl/client-key.pem  # Cipher Suite  # The defaults are usually fine here  # TLSCipherSuite ALL:!ADH:@STRENGTH  </LDAP>  <Authorization>  # Base DN  BaseDN "ou=VPN,dc=itnsaskills,dc=cloud"  # User Search Filter  # SearchFilter "(&(uid=%u)(accountStatus=active))"  SearchFilter "(&(uid=%u))"  # Require Group Membership  # RequireGroup false  # Add non-group members to a PF table (disabled)  #PFTable ips\_vpn\_users  # <Group>  # BaseDN "ou=Groups,dc=example,dc=com"  # SearchFilter "(|(cn=developers)(cn=artists))"  # MemberAttribute uniqueMember  # # Add group members to a PF table (disabled)  # #PFTable ips\_vpn\_eng  # </Group>  </Authorization>  root@lks-internal-edge:~# systemctl restart openvpn |

# PART IV (INTERNAL & CLIENT)

## WORK TASK LKS-I-SRV

#### CA (openssl)

* + Configure as CA using OpenSSL.
  + Use “/etc/ca” as the CA root directory.
  + Create a CA private named cakey.pem, save it in the /etc/ca/private/, key should have minimal permission.
  + CA attributes should be set as follows:
  + Country code is set to ID.
  + Organization is set to LKSNSMK.
  + The common name is set to “LKSNSMK CA”.
  + Create a root CA certificate named cacert.pem, save it in the /etc/ca/
  + All certificates required in the test project should be published by CA.

|  |
| --- |
| root@lks-i-srv:~# mkdir -p /etc/ca/private/  root@lks-i-srv:~# nano /etc/ssl/openssl.cnf  ......  [ req\_distinguished\_name ]  countryName = Country Name (2 letter code)  countryName\_default = ID  countryName\_min = 2  countryName\_max = 2  #stateOrProvinceName = State or Province Name (full name)  #stateOrProvinceName\_default = Some-State  #localityName = Locality Name (eg, city)  0.organizationName = Organization Name (eg, company)  0.organizationName\_default = LKSNSMK  # we can do this but it is not needed normally :-)  #1.organizationName = Second Organization Name (eg, company)  #1.organizationName\_default = World Wide Web Pty Ltd  #organizationalUnitName = Organizational Unit Name (eg, section)  #organizationalUnitName\_default =  commonName = Common Name (e.g. server FQDN or YOUR name)  commonName\_max = 64  commonName\_default = LKSNSMK CA  #emailAddress = Email Address  #emailAddress\_max = 64  ....  root@lks-i-srv:~# cd /etc/ca  root@lks-i-srv:/etc/ca# openssl genrsa -out private/cakey.pem  Generating RSA private key, 2048 bit long modulus (2 primes)  ..................................................................................................................................................................+++++  ..+++++  e is 65537 (0x010001)  root@lks-i-srv:/etc/ca# chmod 400 private/cakey.pem  root@lks-i-srv:/etc/ca# openssl req -new -x509 -key private/cakey.pem -out cacert.pem  You are about to be asked to enter information that will be incorporated  into your certificate request.  What you are about to enter is what is called a Distinguished Name or a DN.  There are quite a few fields but you can leave some blank  For some fields there will be a default value,  If you enter '.', the field will be left blank.  -----  Country Name (2 letter code) [ID]:  Organization Name (eg, company) [LKSNSMK]:  Common Name (e.g. server FQDN or YOUR name) [LKSNSMK CA]:  root@lks-i-srv:/etc/ca# openssl genrsa -out server.key  root@lks-i-srv:/etc/ca# openssl req -new -key server.key -out server.csr  root@lks-i-srv:/etc/ca# openssl x509 -req -in server.csr -CA cacert.pem -CAkey private/cakey.pem -CAcreateserial -out server.pem  // Configure SAN if needed |

#### DHCP

* + Create DHCP for internal client with the following requirement below:

o Range: **10.2.3.100** – **10.2.3.200**

* + - Netmask: **/24**

o Gateway **10.2.3.254**

o DNS: **10.1.1.10**

* + The clients should automatically register their name with the DNS server after they have been assigned with an IP address by the DHCP server.

|  |
| --- |
| lks-i-srv |
| root@lks-i-srv:~# apt install -y isc-dhcp-server  root@lks-i-srv:~# scp root@10.1.1.10:/etc/bind/rndc.key /etc/dhcp/  root@lks-i-srv:~# cd /etc/dhcp/; cat rndc.key >> dhcpd.conf; nano dhcpd.conf  .....  key "itnsaskills" {  algorithm hmac-md5;  secret "AoEJw8QI0rv/ALfDcqCauQ==";  };  ...  ddns-update-style interim;  ddns-domainname "itnsaskills.cloud";  ddns-rev-domainname "10.in-addr.arpa";  ......  subnet 10.2.3.0 netmask 255.255.255.0 {  range 10.2.3.100 10.2.3.200;  option domain-name-servers 10.1.1.10;  option domain-name “itnsaskills.cloud”;  option routers 10.2.3.254;  option broadcast-address 10.2.3.255;  default-lease-time 600;  max-lease-time 7200;  zone itnsaskills.cloud {  primary 10.1.1.10;  key itnsaskills;  }  zone 10.in-addr.arpa {  primary 10.1.1.10;  key itnsaskills;  }  } |

## WORK TASK LKS-I-CLIENT

* + Make sure LDAP user in OU “MISC” can login locally.
  + Make sure the ca certificate is installed.
  + Install & configure Icedove mail client using smtps & imaps for user mailuser11

## WORK TASK LKS-E-CLIENT

* + Make sure lks-e-client can access http or https:/[www.itnsaskills.cloud.](http://www.itnsaskills.cloud/)
  + Make sure lks-e-client can access to lks-lb (via IP of lks-cloud-edge)
  + Make sure VPN connection can be established using Openvpn GUI.
  + Make sure the ca certificate is installed.
  + Client certificate for authentication VPN must be store /home/competitor/vpn.pem
  + Install & configure Icedove mail client using smtps & imaps for user mailuser12

Testing purpose ¯\\_(ツ)\_/¯

# APPENDIX

## LDAP USERS

|  |  |  |  |
| --- | --- | --- | --- |
| **Username** | **OU** | **password** | **Domain** |
| vpnuser1 – vpnuser10 | VPN | Skill39 | itnsaskills.cloud |
| mailuser11 – mailuser20 | MAIL | Skill39 | itnsaskills.cloud |
| localuser21 – localuser99 | MISC | Skill39 | itnsaskills.cloud |

# SPECIFICATION

## LKS-LB

|  |  |
| --- | --- |
| Operating System | Linux Debian 9.6 |
| FQDN: | lks-lb.itnsaskills.cloud |
| Root Password | Skill39 |
| Local Username: | competitor |
| User Password: | Skill39 |
| Network Adapter 1: | 10.1.1.10/24 |

## LKS-SRV1

|  |  |
| --- | --- |
| Operating System | Linux Debian 9.6 |
| FQDN: | lks-srv1.itnsaskills.cloud |
| Root Skill39 | Skill39 |
| Local Username: | competitor |
| User Password: | Skill39 |
| Network Adapter 1: | 10.1.1.20/24 |

## LKS-SRV2

|  |  |
| --- | --- |
| Operating System | Linux Debian 9.6 |
| FQDN: | lks-srv2.itnsaskills.cloud |
| Root Password | Skill39 |
| Local Username: | competitor |
| Local User Password: | Skill39 |
| Network Adapter 1: | 10.1.1.30/24 |

## LKS-CLOUD-EDGE

|  |  |
| --- | --- |
| Operating System | Linux Debian 9.6 |
| FQDN: | lks-cloud-edge.itnsaskills.cloud |
| Root Password: | Skill39 |
| Local Username: | competitor |
| Local User Password: | Skill39 |
| Network Adapter 1: | 172.17.1.253/24 |
| Network Adapter 2: | 10.1.1.254/24 |

## LKS-I-SRV

|  |  |
| --- | --- |
| Operating System | Linux Debian 9.6 |
| FQDN: | lks-i-srv.itnsaskills.cloud |
| Root Password: | Skill39 |
| Local Username: | competitor |
| Local User Password: | Skill39 |
| Network Adapter 1: | 10.2.2.10/24 |

## LKS-INTERNAL-EDGE

|  |  |
| --- | --- |
| Operating System | Linux Debian 9.6 |
| FQDN: | lks-internal-edge.itnsaskills.cloud |
| Root Password: | Skill39 |
| Local Local Username: | competitor |
| Local User Password: | Skill39 |
| Network Adapter 1: | 172.17.1.254/24 |
| Network Adapter 2 VLAN 20: | 10.2.2.254/24 |
| Network Adapter 2 VLAN 30: | 10.2.3.254/24 |

## LKS-I-CLIENT

|  |  |
| --- | --- |
| Operating System | Linux Debian 9.6 (GUI) |
| FQDN: | lks-i-client.itnsaskills.cloud |
| Root Password: | Skill39 |
| Local Local Username: | Competitor |
| Local User Password: | Skill39 |
| Network Adapter 1: | DHCP |

## LKS-E-CLIENT

|  |  |
| --- | --- |
| Operating System | Linux Debian 9.6 (GUI) |
| FQDN: | lks-e-client.itnsaskills.cloud |
| Root Password: | Skill39 |
| Local Local Username: | Competitor |
| Local User Password: | Skill39 |
| Network Adapter 1: | 172.17.1.10/24 |

Internal

Port-Group: Clients

VLAN: 30

-Server services testing

k

Port-Group: Servers

VLAN: 20

vSwitch-Internal

lks-i-srv

(10.2.2.10/24)

lks-i-client

(IP: DHCP)

* CA
* DHCP

Client

Server

CLOUD

Port-Group: Cloud

vSwitch-Cloud

* Load Balancer
* DNS
* SSH

lks-cloud-edge

(172.17.1.253/24),

(10.1.1.254/24)

lks-lb

(10.1.1.10/24)

lks-srv1

(10.1.1.20/24)

* Web Server 1
* MAIL
* LDAP

- Web Server 2

lks-srv2

(10.1.1.30/24)

* Firewall
* Router
* VPN

# NETWORK DIAGRAM

Port-Group: Internet

Port-Group: Internet

vSwitch-Internet

-Server services testing

lks-e-client

(172.17.1.10/24)

Port-Group: Internet

Port-Group: Trun

* Firewall
* Router
* VPN

VLAN: 4095

lks-internal-edge

(172.17.1.254/24),

(10.2.2.254/24),

(10.2.3.254/24)