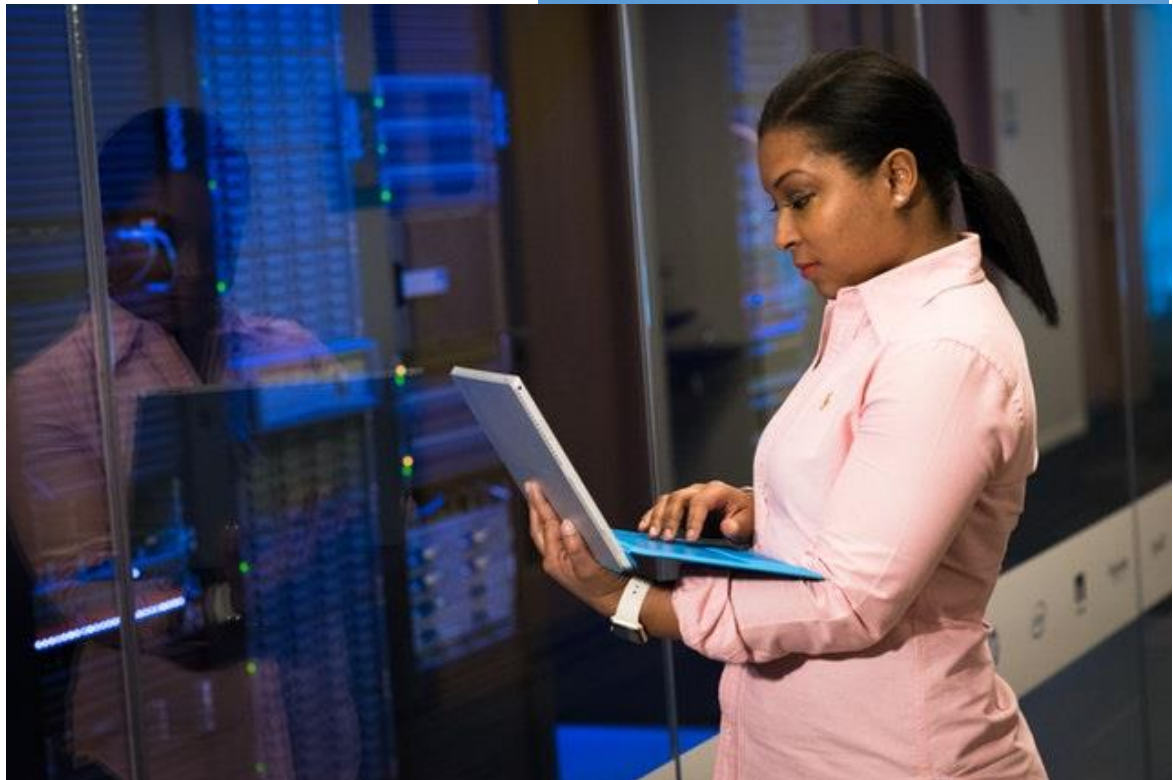


Linux Module

LKS

Information Technology Network Systems Administration



Juri LKS Provinsi 2019

Dinas Pendidikan Prov. Kepulauan Riau

November 12, 2019

Table of Contents

PART I BASIC CONFIGURATION	2
WORK TASK ALL VMs	2
PART II (CLOUD)	2
WORK TASK SERVER LKS-LB	2
WORK TASK SERVER LKS-SRV1	3
WORK TASK SERVER LKS-SRV1 AND LKS-SRV2	3
PART III (EDGE)	4
WORK TASK LKS-INTERNAL-EDGE & LKS-CLOUD-EDGE	4
PART IV (INTERNAL & CLIENT).....	5
WORK TASK LKS-I-SRV	5
WORK TASK LKS-I-CLIENT	5
WORK TASK LKS-E-CLIENT	5
APPENDIX.....	6
SPECIFICATION.....	6
NETWORK	8

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, nmap 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

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 to 172.17.1.253.
 - Internal client will resolve www.itnsaskills.cloud to 10.1.1.10.

Load balancer (HAProxy)

- Configure HTTP & HTTPS load balancer for www.itnsaskills.cloud, which is hosted by lks-srv1 and lks-srv2.
- Use roundrobin as algorithm.

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 “disdikkepri” in lks-i-client and lks-e-client can SSH to user “cloudops” in lks-lb without password

WORK TASK SERVER LKS-SRV1

LDAP (OPENLDAP)

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

Mail (POSTFIX, DOVECOT)

- Configure SMTPS (TCP 465) and IMAPS (TCP 993) server for “itsaskills.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.

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.
- 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.
- Create a profile page with the filename myprofile.php, using this script.

```
<?php
    echo “Name: [Your Name]”;
    echo “School: [Your School]”;
    echo "Today is " . date("Y-m-d") . "<br>";
?>
```
- Make sure to disable Trace HTTP Request
- Make sure to disable Server Signature, so Apache do not reveal its version.
- Make sure to make apache to only return Apache in the Server header, returned on every page request.
- Make sure to hide php version in response header.

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.

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.

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 lkscld-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 & lkssrv1:
 - ICMP
 - DNS
 - HTTPS
 - SSH
 - IMAPS
 - SMTPS
 - LDAP
- All other traffic should be prohibited.

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.

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

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 LKSPROVSMK.
- The common name is set to “LKSPROVSMK 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.

DHCP

- Create DHCP for internal client with the following requirement below:
 - Range: 10.2.3.100 - 10.2.3.200
 - Netmask: /24
 - Gateway 10.2.3.254
 - 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.

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 mailuser15

WORK TASK LKS-E-CLIENT

- Make sure lks-e-client can access http or https://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/disdikkepri/vpn.pem
- Install & configure Icedove mail client using smtps & imaps for user mailuser16

APPENDIX

LDAP USERS

Username	OU	Password	Domain
vpnuser1 - vpnuser10	VPN	!Password123	itnsaskills.cloud
mailuser11 - mailuser20	MAIL	!Password123	itnsaskills.cloud
localuser21 - localuser50	MISC	!Password123	itnsaskills.cloud

SPECIFICATION

LKS-LB

Operating System	Debian 9.6 (CLI)
FQDN	lks-lb.itnsaskills.cloud
Root Password	!Password123
Local User Username	disdikkepri
User Password	!Password123
Network Adapter 1	10.1.1.10/24

LKS-SRV1

Operating System	Debian 9.6 (CLI)
FQDN	lks-srv1.itnsaskills.cloud
Root Password	!Password123
Local User Username	disdikkepri
User Password	!Password123
Network Adapter 1	10.1.1.20/24

LKS-SRV2

Operating System	Debian 9.6 (CLI)
FQDN	lks-srv2.itnsaskills.cloud
Root Password	!Password123
Local User Username	disdikkepri
User Password	!Password123
Network Adapter 1	10.1.1.30/24

LKS-CLOUD-EDGE

Operating System	Debian 9.6 (CLI)
FQDN	lks-cloud-edge.itnsaskills.cloud
Root Password	!Password123
Local User Username	disdikkepri
User Password	!Password123
Network Adapter 1	172.17.1.253/24
Network Adapter 2	10.1.1.254/24

LKS-I-SRV

Operating System	Debian 9.6 (CLI)
FQDN	lks-i-srv.itnsaskills.cloud
Root Password	!Password123
Local User Username	disdikkepri
User Password	!Password123
Network Adapter 1	10.2.2.10/24

LKS-INTERNAL-EDGE

Operating System	Debian 9.6 (CLI)
FQDN	lks-internal-edge.itnsaskills.cloud
Root Password	!Password123
Local User Username	disdikkepri
User Password	!Password123
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	Debian 9.6 (GUI)
FQDN	lks-i-client.itnsaskills.cloud
Root Password	!Password123
Local User Username	disdikkepri
User Password	!Password123
Network Adapter 1	DHCP

LKS-E-CLIENT

Operating System	Debian 9.6 (GUI)
FQDN	lks-e-client.itnsaskills.cloud
Root Password	!Password123
Local User Username	disdikkepri
User Password	!Password123
Network Adapter 1	172.17.1.10/24

NETWORK

