REPUBLIKA SLOVENIJA
MINISTRSTVO ZA IZOBRAŽEVANJE, ZNANOST IN ŠPORT

CPI
CENTER RS ZA POKLICNO IZOBRAŽEVANJE

EVROPSKA UNIJA
EVROPSKI SOCIALNI SKLAD
NALOŽBA V VAŠO PRIHODNOST

Projekt vzpostavitve IKT-sistema v podjetju

CreditBank d.d.

SloveniaSkills 2024 – IKT
18.–22. september 2024

worldskills Slovenia

Izvajalec: ConfigIT

CONFIGIT
CONFIGURING TOMORROWS NETWORK TODAY

Avtorji:

Jan Kovič, NIL d.o.o., jkovic@nil.com – Linux
Luka Filipič, NIL d.o.o., lfilipic@nil.com – Cisco
Tomaž Prezelj, NIL d.o.o., tprezelj@nil.com – Windows

UVOD

Podjetje ConfigIT d.o.o. je podjetje z vrhunskimi strokovnjaki s področja IKT tehnologij. Specializirano je za rešitve s področja telekomunikacij, natančneje načrtovanja, vzpostavitve in upravljanja omrežnih rešitev proizvajalca Cisco, ter za strežniške sisteme in končne naprave s področja Microsofta in odprtokodnih rešitev, ki temeljijo na operacijskih sistemih Linux. Podjetje se pri vseh korakih − od načrtovanja, preko vzpostavitve in vzdrževanja – drži priporočil dobrih praks v skladu z razvojem sodobnih IKT-sistemov.

Podjetje ConfigIT je ravnokar sklenilo pogodbo za načrtovanje, vzpostavitev in upravljanje omrežja ene izmed večjih bank v regiji z imenom CreditBank d.d., ki ponuja svojim strankam na slovenskem in tudi tujem tržišču raznovrstna bančne storitve.

Vaša naloga v sklopu projekta je priprava, vzpostavitev in vzdrževanje IKT-infrastrukture za novonastalo družbo v skladu z naročnikovimi željami in potrebami. V vseh fazah izdelave IKT-rešitve upoštevajte naslednja načela: varnost (ang. security), zanesljivost (ang. redundancy), razširljivost (ang. scalability) in enostavnost (ang. simplicity).

NAČIN DELA

Projekt je zasnovan za izvedbo v dveh tekmovalnih dneh. Tekmovalna naloga se deli v dva logično zaključena sklopa − A in B. Sklop A predstavlja izdelavo in konfiguracijo telekomunikacijskega omrežja s pomočjo opreme proizvajalca Cisco. V sklopu B pa je treba zgraditi strežniški sistem, zasnovan na programski opremi proizvajalcev Microsoft in Linux. Prvi tekmovalni dan polovica sodelujočih ekip izvaja naloge iz sklopa A in druga polovica iz sklopa B. Naslednji tekmovalni se vloge ekip obrnejo.

Dostop do interneta je med tekmovanjem (ne pa npr. med kosilom) strogo prepovedan. Tekmovalci nimate dostopa do komunikacijskih naprav, ki bi bile povezane v zunanje omrežje. Svoje naprave, ki bi bile tega zmožne, morate pred začetkom tekmovanja pustiti v za to namenjenih garderobah. Na tekmovališče vam ni dovoljeno prinašati ničesar. Kar potrebujete, je zagotovljeno na tekmovališču.

Projekt je zastavljen tako, da določi cilje vsakega dne, a hkrati prepusti vam, katere izmed njih boste glede na svoje zmožnosti uresničili.

Namen projekta je simulirati življenjski scenarij, vsakdanje delo normalnega podjetja, kolikor je to le mogoče. Naš namen NI zavajanje, ustvarjanje dodatnih trikov ali poustvarjanje situacij, ki so v produkcijskem okolju skoraj nemogoče. Vsekakor obstaja več možnih poti do končne rešitve.

OPREMA

STROJNA OPREMA:

- 5 x usmerjevalnik Cisco 892,
- 2 x stikalo Cisco C3650,
- 2 x stikalo Cisco C2960s,
- 1 x strežnik
    - 32 GB RAM
    - 1 TB SSD
    - CPU TBD
    - 2x NIC 1 GB
- 2 x prenosni računalnik (Windows 10 build 21H2),
- 2 x Cisco konzolni kabel in pretvornik RS232-USB.

PROGRAMSKA OPREMA:

- Operacijski sistem Linux CentOS (version 8 Minimal Install)
    - Na voljo tudi Full ISO za namestitev opcijskih paketov
- Operacijski sistem MS Windows Server 2022 21H2 Datacenter (OS Build vsaj 20348.1668)
- Operacijski sistem Windows 11 Enterprise 23H2
- VMware vSphere ESXi version 7.x
- Cisco IOS/IOS XE verzije:
    - C3650: IOS XE 16.12.11
    - C2960: IOS 15.2(2)E9
    - 892: IOS 15.7(3)M4a (Feature Set: adventerprisek9)

TRAJNOST

V skladu s sodobnimi smernicami trajnosti boste uporabili minimalno število fizičnih naprav, ki jih bomo nadomestili s platformo virtualizacije. Tako bodo na strežniku prednastavljene naslednje virtualne naprave:

- WIN-AD01,
- WIN-AD02,
- WIN-ROOTCA,
- WIN-SUBCA,
- WIN-CRLCA,
- WIN-W11CL,
- WIN-DHCP,
- lin-node1,
- lin-node2.

NAVODILA ZA TEKMOVALCE

V nalogi uporabljajte naslednja uporabniška imena in gesla brez navednic:

- Cisco: uporabniško ime: »netadmin«, geslo/enable: »SuperGeslo@2024«
- Windows: uporabniško geslo: »SuperGeslo@2024«
- Linux: uporabniško geslo: »SuperGeslo@2024«

Če sodniška ekipa ne more dostopati do naprav/strežnikov v IKT-sistemih, tekmovalna ekipa prejme nič (0) točk.

Kjerkoli v nalogi najdete namesto zapisane številke spremenljivko »X« (npr. IP- naslovi), na tem mestu vnesite številko svojega delovnega mesta. Številka posamezne ekipe je napisana na tekmovališču. Delajte, kot da je vaša oprema dejansko povezana v internet. V tem duhu izvedite potrebne varnostne ukrepe, da ne bi kdo, pomotoma ali ne, vdrl v vašo opremo (komunikacija med tekmovalci s stališča omrežja ni blokirana).

Sodniška ekipa pri ocenjevanju naloge ocenjuje delovanje in pravilnost same konfiguracije kot celote.

PODJETJE CreditBank d.d.

Z najavo prihoda podjetja CreditBank na slovensko tržišče prinaša nove storitve iz področja bančništva, ki olajša poslovanjem njihovim uporabnikom.

Njihovo omrežje je sestavljeno iz centralne lokacije (v nadaljevanju CL) in trenutno ene (1) oddaljene poslovne enote (v nadaljevanju PE). S povečanjem uspešnosti poslovanja ni izključena možnost odpiranja in dodajanja dodatnih PE v omrežje. Zaposleni v oddaljeni PE morajo imeti omogočen enak dostop do storitev v omrežju podatkovnega centra kot zaposleni na CL. Oddaljeni dostop je zagotovljen preko dveh različnih ponudnikov storitev (v nadaljevanju ISP), ki omogočata vsak svoj način povezovanja. Oddaljeni dostop mora biti varen in nam mora omogočati podvojenost v primeru izpada posameznega robnega usmerjevalnika na centralni lokaciji oz. povezave posameznega ponudnika storitve.

Jedrno omrežje je sestavljeno iz dveh centralnih stikal in zagotavlja popolno delovanje omrežja v primeru izpada posameznega stikala. Namesto trinivojske arhitekture samega omrežja je uporabljena dvonivojska, t. i. »collapsed core«. Stikali predstavljata mejo med L2 in L3 delom omrežja.

Centralni stikali zagotavljata povezave do robnih usmerjevalnikov, lokalnega omrežja in omrežja podatkovnega centra (v nadaljevanju DC).

Dostopovno omrežje je trenutno sestavljeno iz dveh (2) dostopnih stikal, saj še zadostuje trenutnim potrebam po priklopu končnih naprav. Konfiguracija naj vsebuje primer dobrih praks zaščite na dostopovne plasti (ang. Layer 2) pred morebitnimi napadi oz. napačnim priklopom končnih naprav.

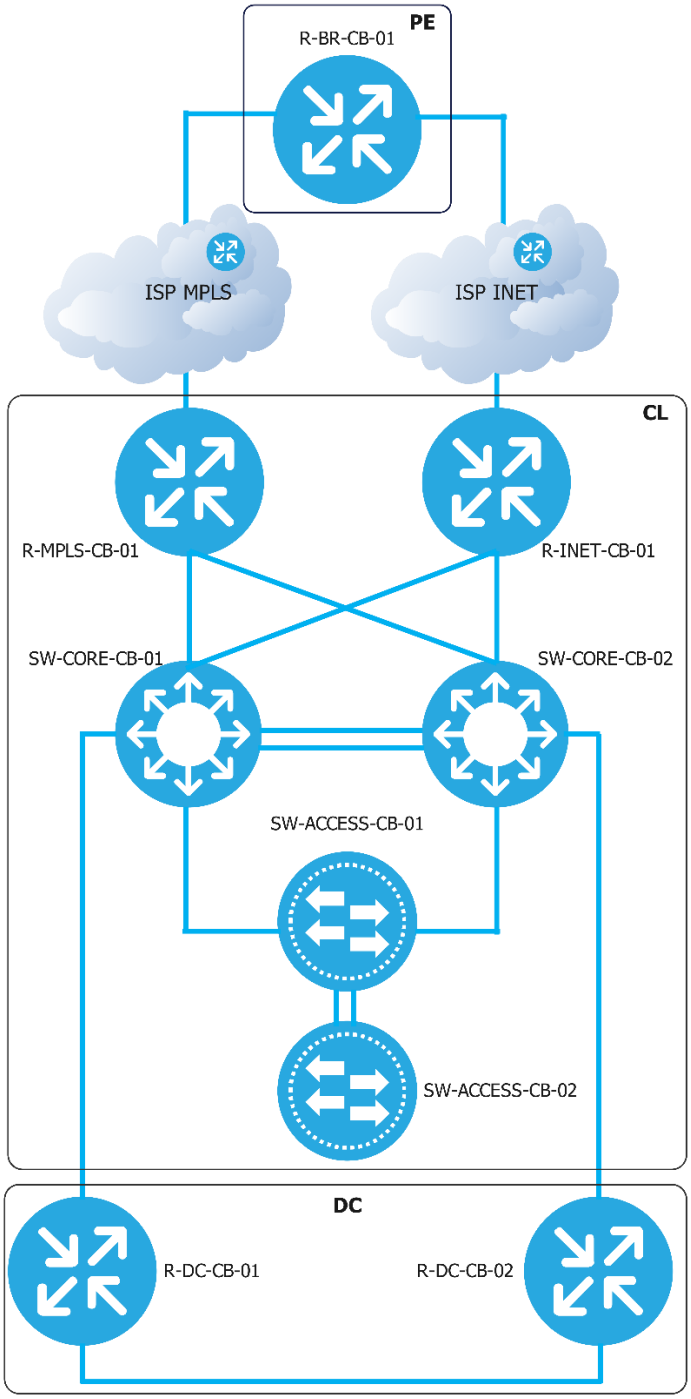
Strežniško okolje Windows je sestavljeno iz sedmih virtualnih strežnikov in enega virtualnega odjemalca.
WIN-AD01 ter WIN-AD02 sta v vlogi domenska krmilnika, kjer je nameščen Aktivni Imenik ter storitev DNS.
Na WIN-DHCP bomo imeli DHCP strežnik, ki bo podeljeval naslove IP Linux mrežnemu delu in delu, kjer bodo Windows odjemalci.
WIN-ROOT, WIN-SUBCA ter WIN-CRLCA pa so namenjeni PKI okolju, kjer bomo zgradili dvonivojsko okolje za izdajanje certifikatov Active Directory Certificate Services.
WIN-W11CL je končna uporabniška naprava.

Strežniško okolje Linux je sestavljeno iz dveh virtualnih strežnikov z imenoma lin-node1 in lin-node2.

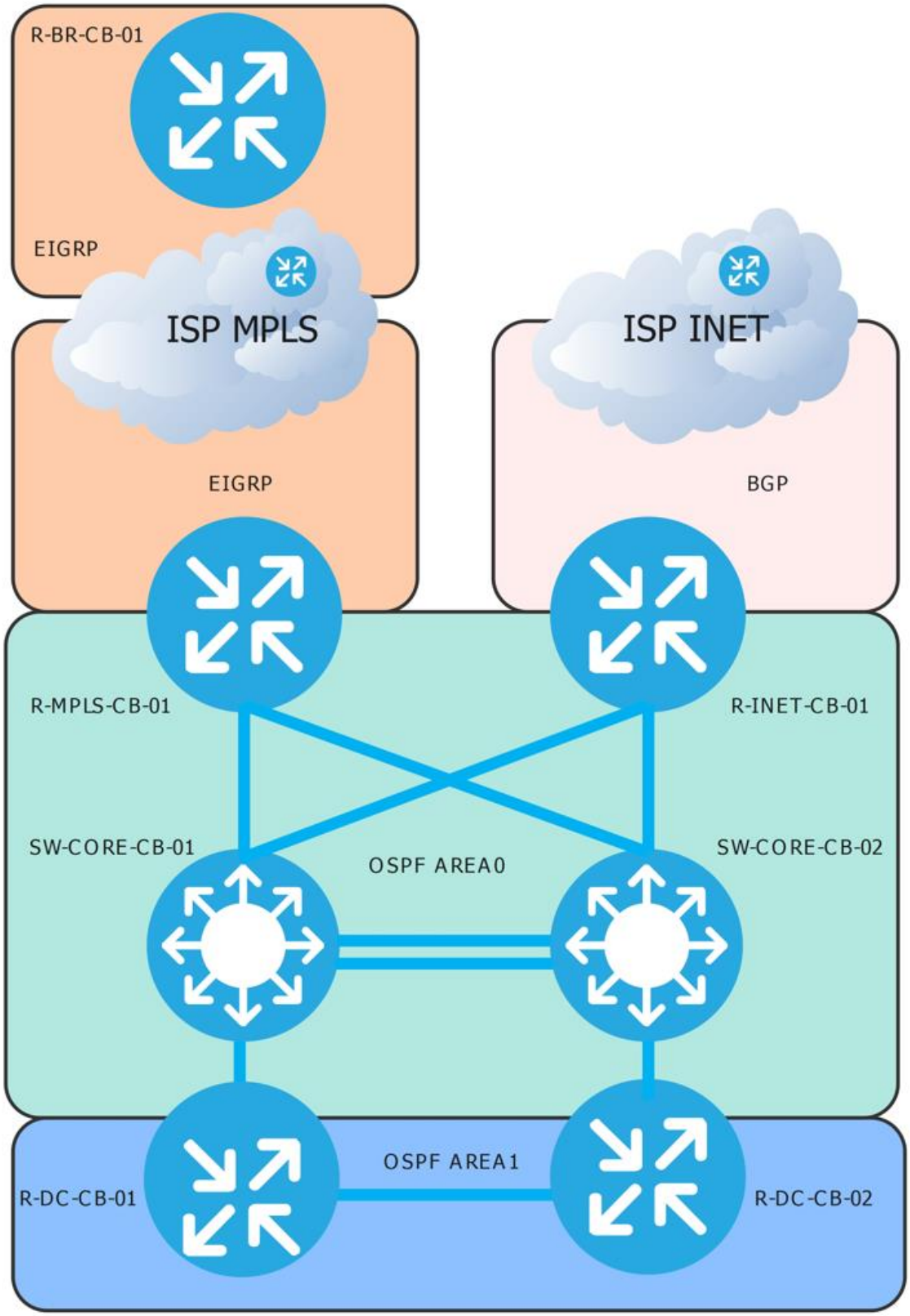
Lin-node1 ima vlogo centralnega strežnika Rsyslog in nadzornega sistema Zabbix. Strežnik je dodan v domeno in potrebno je pripraviti primerni skupini za administrativne uporabnike in navadne domenske uporabnike. Zabbix sistem deluje v okolju Podman sestavljen iz skupine štirih zabojnikov (ang. containers).

Lin-node2 ima vlogo aplikacijskega strežnika, na katerem živi aplikacija VaultWarden in spletna stran v jeziku PHP. Aplikacija je povezana z bazo SQL in prikazuje podatke iz tabele. Storitev VaultWarden deluje v okolju Podman, in sicer v obliki zabojnika kot servis s pravicami lokalnega uporabnika.

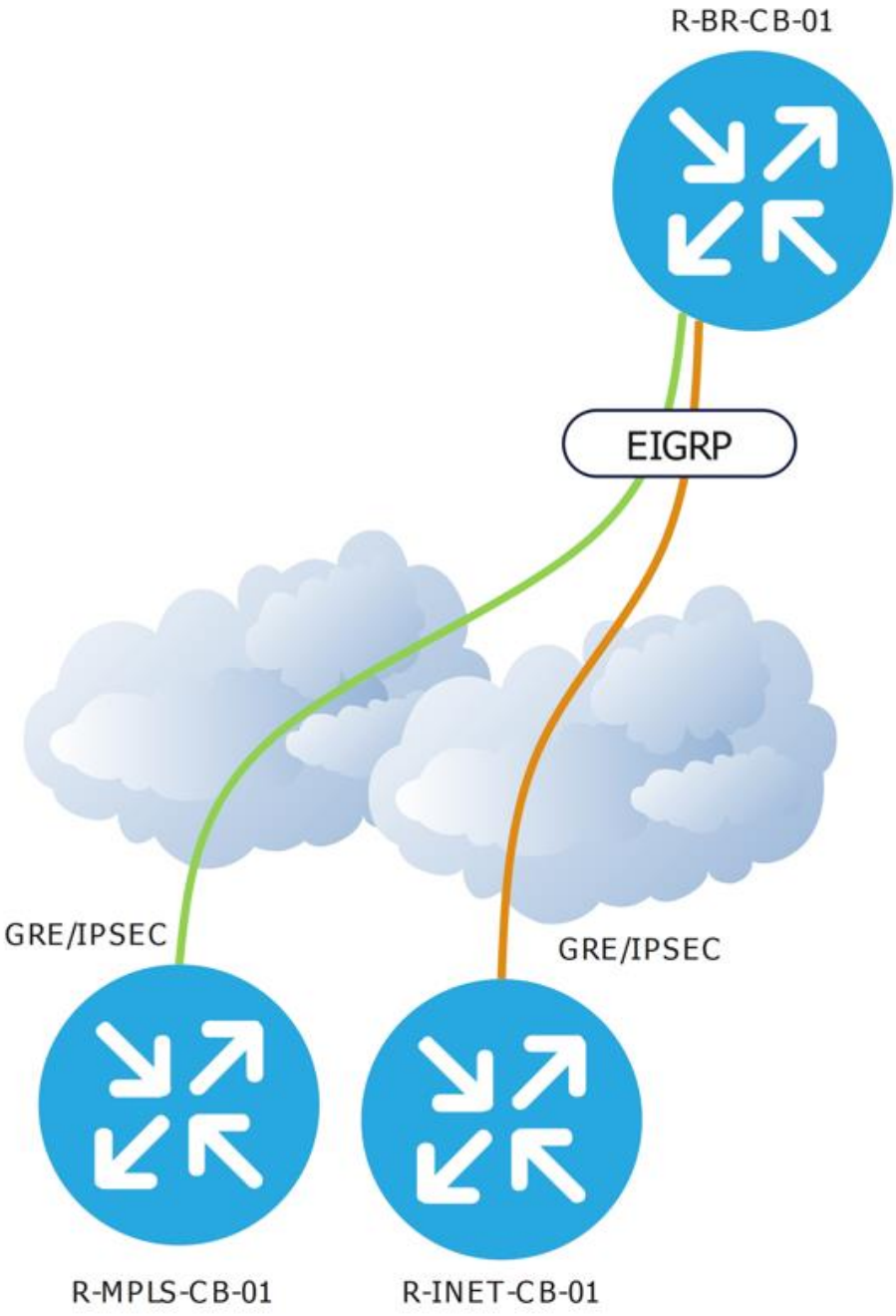
TOPOLOGIJA – SKLOP A



Slika 1: Topologija omrežja - Sklop A

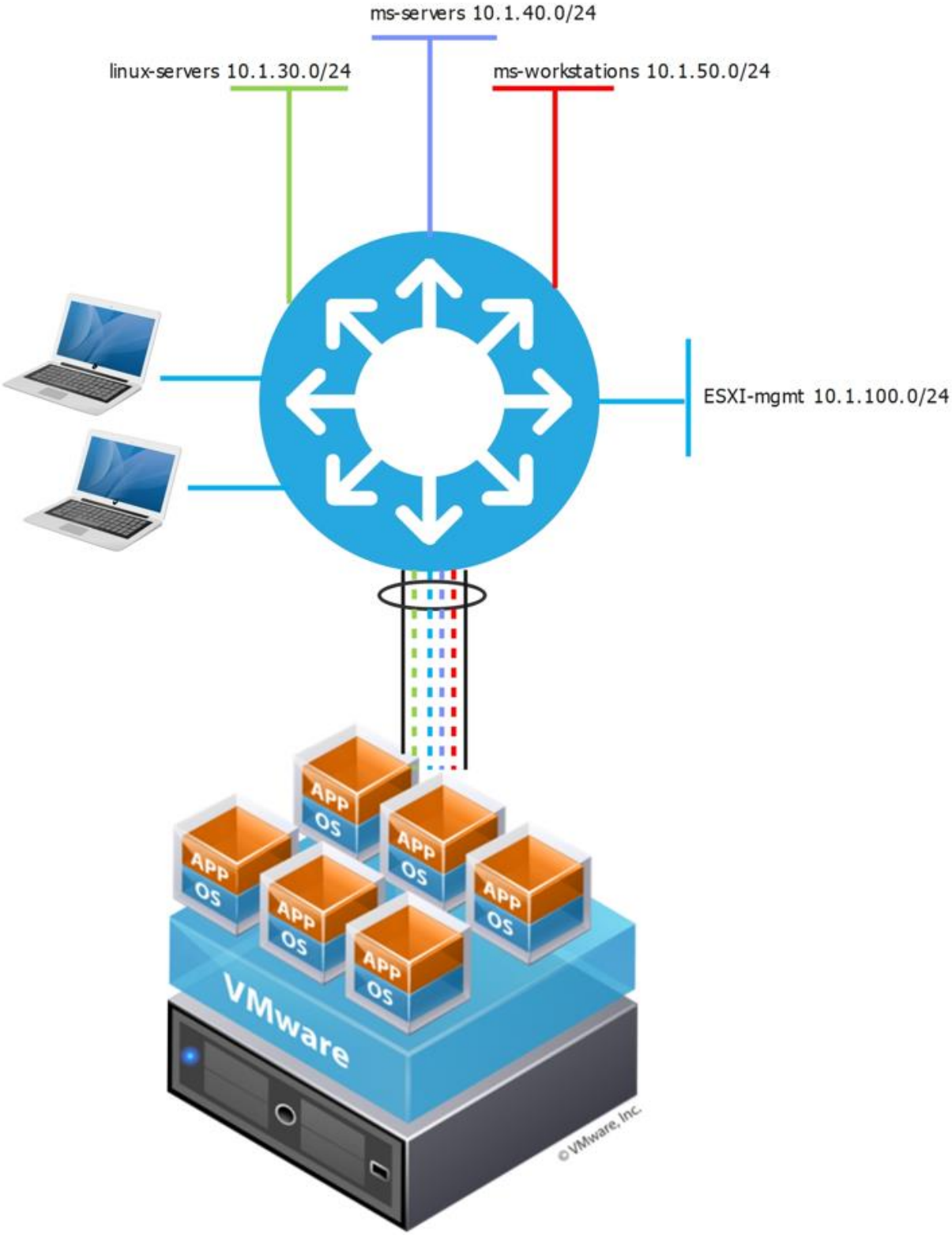


Slika 2: Usmerjevalni protokoli BGP, OSPF in EIGRP



Slika 3:Povezave med lokacijama CL in PE

TOPOLOGIJA – SKLOP B



Slika 4: IP naslavljanje - Sklop *B*

IP NASLAVLJANJE – SKLOP A

Spodnje tabele prikazujejo seznam in vrednosti IP-naslovnega prostora, VLAN L2, ASN in imena naprav.

Ime VLAN	VLAN ID	IP segment
Uporabniki	110	10.1.10.0/24
Gosti	120	10.1.20.0/24
MGMT	130	10.1.30.0/24
Alarm	140	10.1.40.0/24
Strezniki_DC	250	10.1.250.0/24
DEMO_OKOLJE	251	10.1.251.0/24
Zaposleni_PE	100	10.10.100.0/24
MPLS-01_CORE-01	101	Tabela 6
MPLS-01_CORE-02	102	Tabela 6
INET-01_CORE-01	201	Tabela 6
INET-01_CORE-02	202	Tabela 6

Tabela 1: Seznam L2/L3 VLAN

Naslovni prostor	IP segment
Loopback vmesniki	192.[2-4].1.0/24
Tunelski vmesnik 1	192.1.2.0/24
Tunelski vmesnik 2	192.1.3.0/24

Tabela 2: Seznam naslovnih prostorov za vmesnike Loopback in Tunnel

Ime naprave	Loopback 0	Tunelski vmesnik
R-INET-CB-01	192.2.1.11/32	Tu1: 192.1.2.11
R-MPLS-CB-01	192.2.1.12/32	Tu2: 192.1.3.12
SW-CORE-CB-01	192.2.1.21/32	N/A
SW-CORE-CB-02	192.2.1.22/32	N/A
SW-ACCESS-CB-01	192.2.1.31/32	N/A
SW-ACCESS-CB-02	192.2.1.32/32	N/A
R-DC-CB-01	192.3.1.41/32	N/A
R-DC-CB-02	192.3.1.42/32	N/A
R-BR-CB-01	192.4.1.100/32	192.1.2.100, 192.1.3.100

Tabela 3: Imena in IP-naslovi vmesnikov Loopback in Tunnel

Ime naprave	Usmerjevalni protokol	OSPF AREA	ASN BGP	ASN WAN	ASN MPLS
R-INET-CB-01	OSPF/EIGRP/BGP	Area0	6450x	6500x	N/A
R-MPLS-CB-01	OSPF/EIGRP	Area0	N/A	6500x	6450x
SW-CORE-ZM-01	OSPF	Area0/Area1	N/A	N/A	N/A
SW-CORE-ZM-02	OSPF	Area0/Area1	N/A	N/A	N/A
R-DC-CB-01	OSPF	Area1	N/A	N/A	N/A
R-DC-CB-02	OSPF	Area1	N/A	N/A	N/A
R-BR-CB-01	EIGRP	N/A	N/A	6500x	6450x

Tabela 4: Usmerjevalni protokoli in podatki o vrednosti ASN/AREA

Ime naprave A	Vmesnik naprave A	Vmesnik naprave B	Ime naprave B
R-INET-CB-01	Fas 0	Gig 1/0/2	SW-CORE-CB-01
R-INET-CB-01	Fas 1	Gig 1/0/2	SW-CORE-CB-02
R-MPLS-CB-01	Fas 0	Gig 1/0/1	SW-CORE-CB-01
R-MPLS-CB-01	Fas 1	Gig 1/0/1	SW-CORE-CB-02
R-INET-CB-01	Gig0	N/A	ISP
R-MPLS-CB-01	Gig0	N/A	ISP
SW-CORE-CB-01	Gig 1/0/23	Gig 1/0/23	SW-CORE-CB-02
SW-CORE-CB-01	Gig 1/0/24	Gig 1/0/24	SW-CORE-CB-02
SW-CORE-CB-01	Gig 1/0/3	Gig0	R-DC-CB-01
SW-CORE-CB-02	Gig 1/0/3	Gig0	R-DC-CB-02
R-DC-CB-01	Fas 0	Fas 0	R-DC-CB-02
SW-CORE-CB-01	Gig 1/0/21	Gig 1/0/23	SW-ACCESS-CB-01
SW-CORE-CB-02	Gig 1/0/21	Gig 1/0/24	SW-ACCESS-CB-01
SW-ACCESS-CB-01	Gig 1/0/1	Gig 1/0/1	SW-ACCESS-CB-02
SW-ACCESS-CB-01	Gig 1/0/2	Gig 1/0/2	SW-ACCESS-CB-02
R-BR-CB-01	Gig0	N/A	ISP
R-BR-CB-01	Fas 8	N/A	ISP

Tabela 5: Seznam fizičnih povezav med napravami

Ime naprave A	IP naprava A	IP naprava B	Ime naprave B
R-INET-CB-01	172.1.1.1/30	172.1.1.2/30	SW-CORE-CB-01
R-INET-CB-01	172.1.5.1/30	172.1.5.2/30	SW-CORE-CB-02
R-MPLS-CB-01	172.1.9.1/30	172.1.9.2/30	SW-CORE-CB-01
R-MPLS-CB-01	172.1.12.1/30	172.1.12.2/30	SW-CORE-CB-02
SW-CORE-CB-01	172.1.16.1/30	172.1.16.2/30	R-DC-CB-01
SW-CORE-CB-02	172.1.20.1/30	172.1.20.2/30	R-DC-CB-02

Tabela 6: IP-naslovi povezovalnih segmentov

Ime naprave	MGMT IP naslov
R-INET-CB-01	N/A
R-INET-MPLS-01	N/A
R-BR-ZM-01	N/A
SW-CORE-CB-01	10.1.30.2/24
SW-CORE-CB-02	10.1.30.3/24
SW-ACCESS-CB-01	10.1.30.31/24
SW-ACCESS-CB-02	10.1.30.32/24

Tabela 7: MGMT IP-naslovi

Ekipa	Omrežni segment ISP lokacija CL	Omrežni segment ISP lokacija PE
Ekipa 1	198.51.100.0/29	198.51.100.128/30
Ekipa 2	198.51.100.8/29	198.51.100.132/30
Ekipa 3	198.51.100.16/29	198.51.100.136/30
Ekipa 4	198.51.100.24/29	198.51.100.140/30

Tabela 8: Javni IP naslovni prostor

Ekipa	Omrežni segment MPLS lokacija CL	Omrežni segment MPLS lokacija PE
Ekipa 1	172.17.100.0/29	172.17.100.224/29
Ekipa 2	172.17.100.8/29	172.17.100.232/29
Ekipa 3	172.17.100.16/29	172.17.100.240/29
Ekipa 4	172.17.100.24/29	172.17.100.248/29

Tabela 9: MPLS IP naslovni prostor

IP-NASLAVLJANJE – SKLOP B

Spodnje tabele prikazujejo seznam in vrednosti IP naslovnega prostora, VLAN L2, itd.

Ime VLAN	VLAN ID	IP segment
linux-servers	30	10.1.30.0/24
ms-servers	40	10.1.40.0/24
ms-workstations	50	10.1.50.0/24
ESXI-mgmt	100	10.1.100.0/24

Tabela 10: Seznam L2/L3 VLAN - Sklop B

Ime naprave A	IP naslov
VMware ESXi	10.1.100.100/24
WIN-AD01	10.1.40.10/24
WIN-AD02	10.1.40.11/24
WIN-ROOTCA	10.1.40.12/24
WIN-SUBCA	10.1.40.13/24
WIN-CRLCA	10.1.40.14/24
WIN-DHCP	10.1.40.15/24
WIN-W11CL	DHCP
lin-node1	DHCP
lin-node2	DHCP

Tabela 11: Seznam IP-naslovov naprav v sklopu B

SKLOP A – Izdelava omrežja z opremo Cisco (8 ur)

Dokumentacija
Stikala 3650

Stikala 2960

Usmerjevalniki 892

1. **Osnovne nastavitve in upravljanje (vsi usmerjevalniki in stikala):**
    a. Na vseh omrežnih napravah nastavite imena naprav, kot narekuje Tabela 3, stolpec 1.
    b. Na vseh omrežnih napravah nastavite logične vmesnike Loopback, kot narekuje Tabela 3, stolpec 2.
    c. Na vseh napravah omogočite zgolj in samo varen oddaljen dostop preko protokola SSHv2. Prijava naj bo mogoča samo z lokalnim uporabnikom na prvih pet (5) navideznih terminalnih povezav. Uporabite domeno *cbank.local*.
    d. Na vseh omrežnih napravah preprečite prijavo brez vnosa lokalnega uporabniškega imena in gesla. Vsa gesla naj bodo šifrirana. Vsi lokalno definirani uporabniki naj imajo polne pravice dostopa.
    e. Na vseh omrežnih napravah ustvarite dodatno uporabniško ime z imenom »*urgent*« in mu dodelite lokalno politiko gesel s sledečimi zahtevami:
        i. minimalna dolžina gesla deset (10) znakov,
        ii. en (1) poseben znak,
        iii. en (1) velik znak,
        iv. en (1) mali znak in
        v. življenjska doba gesla šest (6) mesecev.
        vi. Ime politike naj bo »*CB-URGENT«.* Lokalno geslo je poljubno v skladu s pripadajočo politiko.
    f. Na vseh napravah nastavitev pravilen časovni pas (CET/CEST) glede na lokacijo Ljubljana z upoštevanjem spremembe zimskega in poletnega časa.
    g. Na vseh napravah pred vse dnevniške zapise tipa *»log«* in *»debug«* zagotovite pripis točnega časa z natančnostjo na milisekundo in vključenost lokalnega časa skupaj s časovnim pasom in letom.
    h. Na vseh omrežnih napravah nastavite sporočilo dneva po lastni izbiri.
    i. Povečajte velikost dnevniških zapisov na 200 000 vrstic.

2. **Osnovna povezljivost omrežnih naprav:**
    a. Omrežno opremo fizično povežite skladno s podatki, ki jih predstavlja Tabela 5.
    b. Na fizičnih povezavah med napravama SW-CORE-CB-01 in SW-CORE-CB-02 ter SW-ACCESS-CB-01 in SW-ACCESS-CB-02 uporabite protokol za združevanje fizičnih povezav v eno logično. Sledite spodnjim zahtevam:
        i. Protokol naj bo nelastniški (ang. non-proprietary) in tisti, ki ima zaščito pred napačno povezanimi kabli.
        ii. Zagotovite pošiljanje kontrolnih paketov vsako sekundo, kjer je to mogoče.
        iii. Oznaka združene povezave naj bo deset (10).
    c. Na stikalih SW-CORE-CB-01, SW-CORE-CB-02, SW-ACCESS-CB-01 in SW-ACCESS-CB-02 vklopite protokol VTP s spodnjimi zahtevami:
        i. Verzija protokola naj bo tri (3), domena »*cbank*«, geslo »*cbank@123*«
        ii. Stikalo SW-CORE-CB-01, naj ima vlogo primarnega strežnika za razširjanje VLAN-ov in MST nastavitev na ostala stikala znotraj CL.
        iii. Ostala stikala naj imajo vlogo klienta za MST in VLAN.
    d. Pri nastavljanju L2 VLAN vrednosti na napravah SW-CORE-CB-01, SW-CORE-CB-02, SW-ACCESS-CB-01 in SW-ACCESS-CB-02 naj vam bo v pomoč Tabela 1, stolpca 1 in 2.
    e. Na vseh fizičnih in/ali logičnih povezavah dovolite zgolj in samo nujno potrebne VLAN-e.
    f. Na stikalih SW-CORE-CB-01, SW-CORE-CB-02, SW-ACCESS-CB-01 in SW-ACCESS-CB-02 zagotovite delovanje protokola MST v skladu s spodnjimi in predhodno podanimi zahtevami:
        i. Ime domene »*cbank*«, instanca 1 naj vsebuje VLAN-e 1, 110, 120, instanca 2 naj vsebuje VLAN-a 130 in 140.
        ii. Centralno stikalo SW-CORE-CB-01 naj bo vedno vrh vpetega drevesa za instanco 1.
        iii. Centralno stikalo SW-CORE-CB-02 naj bo vedno vrh vpetega drevesa za instanco 2.
        iv. Vrh drevesa naj bo določen oz. izvoljen na podlagi atributa »bridge priority«.
    g. Med usmerjevalnikoma R-DC-CB-01 in R-DC-CB-02 zagotovite ustrezno povezljivost za lokalno definirane VLAN-e.

3. **Osnovna IP-povezljivost:**
    a. Tabela 7 naj vam bo v pomoč pri nastavljanju upravljavskih IP-naslovov na stikalih centralne lokacije.
    b. Uredite ustrezno IP-povezljivost med usmerjevalnikoma in stikaloma na lokaciji CL in povezavi med lokacijo CL in DC (Tabela 6, Tabela 7).
    c. Stikali SW-CORE-CB-01 in SW-CORE-CB-02 naj zagotavljata privzete prehode (L3 VLAN) za vsa lokalno definirana omrežja v sklopu s spodnjimi zahtevami:
        i. Uporabite prvi prosti IP-naslov iz segmenta za privzeti prehod in naslednja dva prosta IP-naslova za vmesnika. Nižji naslov IP naj bo na stikalu z nižjo številko v imenu stikala.
        ii. Uporabite protokol vedno aktivnega privzetega prehoda (ang. FHRP), in omogočite šifrirano komunikacijo z mehanizmom MD5.
        iii. Številka skupine naj bo enaka vrednosti VLAN ID.
        iv. Uporablja naj MAC naslove med *0000.0c9f.f000* in *0000.0c9f.ffff*.
        v. Vloga aktivnega stikala mora biti deterministično določena in naj se ne zanaša na samodejno dodeljevanje vloge aktivnega in pasivnega stikala. Stikalo SW-CORE-CB-01 naj ima privzete prehode za VLAN-e 110 in 120, stikalo SW-CORE-CB-02 pa za VLAN-e 130 in 140.
        vi. Vključen naj bo mehanizem za povrnitev prvotnega stanja v aktivno vlogo v primeru izpada aktivnega vmesnika.
    d. Usmerjevalnika R-DC-CB-01 in R-DC-CB-01 naj zagotavljata naj zagotavljata privzete prehode (L3 VLAN) za vsa lokalno definirana omrežja v sklopu s spodnjimi zahtevami:
        i. Uporabite prvi prosti IP-naslov iz segmenta za privzeti prehod in naslednja dva prosta IP-naslova za vmesnika. Nižji naslov IP naj bo na usmerjevalniku z nižjo številko v imenu stikala.
        ii. Uporabite protokol vedno aktivnega privzetega prehoda (ang. FHRP) in omogočite šifrirano komunikacijo z mehanizmom MD5.
        i. Številka skupine naj bo enaka vrednosti VLAN ID.
        iii. Uporabite nelastniški protokol.
        iv. Vloga aktivnega usmerjevalnika mora biti deterministično določena in naj se ne zanaša na samodejno dodeljevanje vloge aktivnega in pasivnega usmerjevalnika. Usmerjevalnik R-DC-CB-01 naj ima privzete prehode za VLAN-e 250 in 251.
    e. Uredite povezljivost obeh robnih usmerjevalnikov na lokaciji CL. V pomoč naj vam bosta Tabela 8 in Tabela 9:
        v. Na napravah R-INET-CB-01 in R-MPLS-CB-01 uporabite prvi prosti naslov IP iz vašega omrežja.
    f. Uredite povezljivost usmerjevalnika na lokaciji PE:
        vi. Na napravi R-BR-CB-01 uporabite prvi prosti naslov IP iz vašega omrežja.

4. **Napredna IP povezljivost in usmerjanje:**
    a. Zagotovite izmenjavo usmerjevalnih poti s protokolom OSPF med naslednjimi napravami SW-CORE-CB-01, SW-CORE-CB-02, R-INET-CB-01 in R-MPLS-CB-01 po spodnjih zahtevah:
        i. Uporabite vrednost procesa 1 in vrednost area 0.
        ii. Sosedstvo se lahko vzpostavi zgolj in samo na fizičnih L3 povezavah med napravami in konfiguracija naj bo izvedena na vmesnikih.
        iii. Vsi povezovalni segmenti OSPF so tipa točka-točka.
        iv. Zagotovite oglaševanje vmesnikov Loopback v protokol OSPF.
        v. Preprečite samodejno vzpostavljanje sosedstva OSPF oz. oglaševanja IP-omrežij na novo dodanih IP-vmesnikih, razen če to ni eksplicitno dovoljeno.
        vi. Zagotovite, da se omrežja IP, dodeljena vmesnikom SVI, na napravah SW-CORE-ZM-01 in SW-CORE-ZM-02 vidijo v usmerjevalnih tabelah robnih usmerjevalnikov.
    b. Zagotovite izmenjavo usmerjevalnih poti s protokolom OSPF med naslednjimi napravami SW-CORE-CB-01, SW-CORE-CB-02, R-DC-CB-01 in R-DC-CB-02 po spodnjih zahtevah:
        i. Uporabite vrednost procesa 1 in vrednost area 1.
        ii. Sosedstvo se lahko vzpostavi zgolj in samo na fizičnih L3 povezavah med napravami in konfiguracija naj bo izvedena na vmesnikih.
        iii. Vsi povezovalni segmenti OSPF so tipa točka-točka.
        iv. Zagotovite oglaševanje vmesnikov Loopback v protokol OSPF.
        v. Preprečite samodejno vzpostavljanje sosedstva OSPF oz. oglaševanja IP-omrežij na novo dodanih IP-vmesnikih, razen če to ni eksplicitno dovoljeno.
        vi. Zagotovite, da se omrežja IP, dodeljena vmesnikom SVI, na napravah R-DC-CB-01 in R-DC-CB-02 vidijo v usmerjevalnih tabelah centralnih stikal.
        vii. Vzpostavitev OSPF sosedstva naj bo šifrirana po sledečih zahtevah:
            1. ime: *»DC«*,
            2. zaporedna številka ključa ena (1),
            3. vrednost ključa *»cbank@2024«* in
            4. uporaba šifrirnega algoritma hmac-sha-512.

c. Med odsotnostjo vam je sodelavec, ki zelo dobro pozna usmerjevalni protokol BGP, v pomoč za dokončanje dodeljenih zahtev pripravil spodnjo predlogo. Dopolnite manjkajoče parametre in jo uporabite. Zagotovite sosedstvo BGP med vašim robnim usmerjevalnikom in ISP po spodnjih zahtevah:

   i.

router bgp <ASN>
! Vrednost router ID – nastavi glede na vrednost javnega naslova IP
bgp router-id 192.2.1.11
! eBGP seja proti ISP
neighbor <IP-naslov> remote-as 64496
neighbor <IP-naslov> update-source <fizični vmesnik>

d. Podjetje vas je ravnokar poslalo na izobraževanje glede usmerjevalnega protokola EIGRP. V vaše zapiske ste si zapisali sledeče nastavitve, ki so vam lahko v pomoč pri izpolnjevanju naslednjih zahtev:

   i.

router eigrp <IME>
!
address-family ipv4 unicast autonomous-system <ASN>
!
af-interface default

exit-af-interface
! !
topology base
exit-af-topology
network <OMREŽNI NASLOV + WILDCARD>
exit-address-family

   ii. Nastavite usmerjevalni protokol EIGRP na povezavah med napravami R-MPLS-CB-01 – ISP – R-BR-CB-01.
   iii. Ime procesa naj bo »MPLS«, vzpostavitev sosedstev naj bo omogočeno na minimalnem številu fizičnih povezav, na vseh ostalih naj bo privzeto onemogočeno, v proces oglašujte samo povezovalne segmente med napravami s pripadajočo nadomestno masko.

e. Na stikalih SW-CORE-CB-01 in SW-CORE-CB-02 zagotovite, da se omrežni segmenti 10.1.[1-4]0.0/24 v podatkovnem centru vidijo kot združena usmerjevalna pot z najboljšim ujemanjem.

5. **Zagotavljanje varne povezljivosti med lokacijama CL in PE:**
    a. Zagotovite varno povezljivost med oddaljeno in CL lokacijo v skladu z zahtevami:
        i. Povezava mora omogočati prenos tipov prometa: unicast, multicast, broadcast.
        ii. PE obvezno potrebuje podvojeno pot do CL, ki mora zagotavljati delovanje vseh storitev s centralne lokacije v primeru izpada posameznega robnega usmerjevalnika naenkrat.
        iii. IP-naslavljanje naj bo v skladu s podatki, predstavljenimi v Tabela 3.
    b. Za zagotavljanje dosegljivosti usmerjevalnih poti med lokacijami naj skrbi protokol EIGRP z imenom procesa »WAN«:
        i. Primarna pot naj bo jasno določena z atributom v vrednosti 1024 Kb in naj bo tista, ki ima nižji IP-naslov tunelskega vmesnika na strani usmerjevalnika lokacije PE. Sekundarna pa naj ima vrednost istega atributa 512 Kb.
        ii. Sosedstvo se lahko vzpostavi samo na nujno potrebnih vmesnikih in to upoštevajte pri konfiguraciji vmesnikov, sodelujočih v procesu EIGRP.
        iii. Povezava poteka preko transportnih omrežij, tako da jih ustrezno zaščitite pred morebitnimi napadalci. Uporabite tehnologijo IKEv2 z naslednjimi zahtevami:
            1. Ime konstrukta »proposal« naj bo »IKEv2_PROPOSAL« z algoritmi DH14, šifriranje aes-cbc-256 in integriteto sha256.
            2. Ime politike »IKEv2_POLICY«.
            3. Ime konstrukta »keyring« naj bo »IKEv2_KEYRING«.
            4. Uporabite dva profila, eden naj služi šifriranju povezave preko omrežja Internet z imenom »IKEv2_PROFILE_INET«, drugi pa povezavi preko omrežja MPLS z imenom »IKEv2_PROFILE_MPLS«.
            5. Konstrukt »transformset« naj bo poimenovan »TRANSFORM_SET« s sledečimi algoritmi esp-sha-hmac.
            6. Profile za šifriranje druge faze naj bo poimenovan »IPSEC_PROFILE«.
        iv. Na strani centralnih usmerjevalnikov izvedite redistribucijo usmerjevalnih poti med protokoloma OSPF in EIGRP z imenom »WAN« v obe smeri in pri tem lahko uporabite poljubne vrednosti metrike.

6. **Varnost in upravljanje**
    a. Usmerjevalnika R-INET-CB-01 in R-MPLS-CB-01 naj služita kot NTP strežnika STRATUM 1 v podvojeni postavitvi eden drugemu. Za konfiguracijo uporabite njun vmesnik Loopback. Vse ostale naprave Cisco naj sinhronizirajo svoj čas na njiju, vendar prednostno na R-INET-CB-01.
    b. Na vmesnikih stikal SW-CORE-CB-01 in SW-CORE-CB-02 vklopite varnostni mehanizem, da ostala stikala ne morejo postati vrh vpetega drevesa.
    c. Končne vmesnike na napravah SW-ACCESS-CB-01 in SW-ACCESS-CB-02 nastavite v skladu s spodnjimi zahtevami:
        i. Vmesniki v načinu »access« ne sodelujejo v procesu »Proposal/Agreement«.
        ii. Vklopljena naj bo zaščita proti priklopu naprave s podporo STP protokola na uporabniška vrata.
        iii. Vklopljena naj bo mehanizem proti poplavljanju multicast in broadcast okvirjev v vrednosti 50 % kapacitete vmesnika. Ob kršitvi naj se generira dnevniški zapis.
        iv. Vklopljena naj bosta mehanizma overjanja 802.1x in MAB.
        v. Časovni interval osveževanja števcev naj bo nastavljen na 30 sekund.
        vi. Opis vmesnika naj bo »UPORABNIK PC«.
        vii. Uporabite predlogo z imenom »UPORABNIK«.
    d. Vklopite mehanizme zaščite na stikalih SW-ACCESS-CB-01 in SW-ACCESS-CB-02 proti nepooblaščenim DHCP strežnikom po sledečih zahtevah:
        i. Vklopljen naj bo za VLAN-e 110 in 120.
        ii. Avtorizirani DHCP strežniki se nahajajo v VLAN250 na naslovu 10.1.250.10 in 10.1.250.20. Temu primerno uredite konfiguracijo fizičnih vmesnikov in privzetih prehodov za VLAN 110 in 120.
    e. Na fizičnih povezavah med usmerjevalnikoma v DC in jedrnima stikaloma centralne lokacije omogočite protokol dvosmernega zaznavanja s poljubnimi vrednostnimi intervala in njegovega večkratnika. Protokol naj bo omogočen za usmerjevalni protokol OSPF.

SKLOP B – Izdelava IKT-sistema z opremo proizvajalcev Windows in Linux (8 ur)

OKOLJE MICROSOFT WINDOWS

Dokumentacija:

Windows Server documentation | Microsoft Learn

Active Directory Domain Services Overview | Microsoft Learn

Windows LAPS overview | Microsoft Learn

Domain Name System (DNS) | Microsoft Learn

Dynamic Host Configuration Protocol (DHCP) | Microsoft Learn

Active Directory Certificate Services documentation | Microsoft Learn

1. **Aktivni imenik**
   a. Nastavi maksimalno velikost dnevniškega zapisa Security na 4 GB na vseh domenskih krmilnikih.
   b. Na strežniku nastavi časovni pas na UTC+1.
   c. Namesti Active Directory Domain Services. Ime domene naj bo creditbank.local, NetBIOS ime naj bo CREDITBANK. DSRM geslo si izmisli sam.
   d. Naredi novega domenskega uporabnika »adm.jnovak« in naj ima vlogo domenskega administratorja. Geslo si izmisli. Od te točke dalje za vsa administrativna opravila uporabljaj ta račun.
   e. Ponastavi geslo za vgrajenega domenskega administratorja.
   f. Omogoči »koš« (Recycle bin) aktivnega imenika.

2. **DNS**
   a. Dodaj primarne cone IPv4 Reverse Lookup za omrežja 10.1.30.0/24, 10.1.40.0/24 in 10.1.50.0/24. Cone naj bodo integrirane z Aktivnim Imenikom in morajo dovoljevati samo varno dinamično posodabljanje zapisov (angl. secure dynamic updates). Replicira naj se na vse domenske krmilnike znotraj »foresta« creditbank.local.
   b. Na vseh conah nastavi parametra »aging« in »scavenging« zastarelih zapisov po 14 dneh.

3. **Struktura AD**
   a. Naredi nov glavni Organization Unit, znotraj njega pa kreiraj sledeče OU-je:
      - Administrators,
      - Computers,
      - Groups,
      - Servers (pod OU dodaj še 2 OU-ja):
        - Windows,
        - Linux,
      - Service accounts,
      - Users.

      Na koncu naloge naj bodo vsi objekti pod svojim OU. Torej, če bo dodan server Windows, mora biti v OU-ju Windows, znotraj OU Servers. Če boš kreiral novo grupo naj bo pod Groups, itd. Domenski krmilniki naj ostanejo v svojem OU.

   b. V domeni kreiraj naslednje uporabnike:
      - Janez Novak,
      - Miha Novak,
      - Tina Vodopivec,
      - Lara Pirih.

      Nastavi spremembo gesla ob prvi prijavi, uporabniška imena v domeni pa naj imajo v obliki »ime.priimek«.

4. **Nov domenski krmilnik na WIN-AD02**
   a. Strežnik pridruži domeni. Konfiguriraj ga kot nov domenski krmilnik. Geslo DRSM si izmisli in ga shrani.
   b. DNS-strežnika naj imata kot »Primary DNS« nastavljena svoj lasten naslov IP, kot alternativnega pa naslov IP drugega DNS-strežnika. Vsi ostali strežniki naj imajo vpisana naslove IP obeh DNS-strežnikov.

5. **GPO**
   a. Nastavi privzeto politiko za gesla na glavno domensko politiko. Pravila naj bodo:
      - največja veljavnost gesla 180 dni,
      - najkrajša dolžina gesla 12 znakov,
      - najmanjša veljavnost gesla 1 dan,
      - omogoči kompleksnost gesla,
      - račun se zaklene po 5 napačnih poizkusih,
      - v kolikor se račun zaklene, se odklene ponovno po 30 minutah,
      - števec napačnih vnosov gesla naj se ponastavi po 30 minutah.

b. Kreiraj GPO za upravljanje z gesli lokalnega »built-in« administratorja na delovnih postajah (Windows Laps).
   Politika gesla naj bo:
   - Geslo naj se shranjujejo v AD.
   - Kompleksnost gesla: velike, male črke, številke, specialni znaki.
   - Dolžina gesla: vsaj 14 znakov.
   - Geslo naj se menja na 30 dni.
   - Geslo naj se šifrira, preden klient pošlje geslo v AD.
   - V AD naj bodo shranjena zadnja tri gesla za vsakega klienta.

c. Kreiraj lokalno politiko, ki na delovnih postajah (Computers) omogoči požarno pregrado (»Firewall«) za vse tri profile ter za »inboud« in »outbound« pravila uporabi priporočene nastavitve. Lokalna pravila pa naj se ne upoštevajo.

d. Omogoči RDP na strežnikih in delovnih postajah. Omogoči le povezavo preko NLA.

6. DHCP / strežnik WIN-DHCP

a. Strežnik pridruži domeni. Nanj namesti vlogo DHCP in ga avtoriziraj.

b. Kreiraj naslednje IPv4 območja:
   - Ime: »Računalniki«; za omrežje 10.1.50.1/24 naj deli naslove od 10.1.50.50 do 10.1.50.100.
   - Ime: »Linux«; za omrežje 10.1.30.1/24 naj deli naslove od 10.1.30.50 do 10.1.30.100.
   - Uporabi nastavitve DNS vseh DNS-strežnikov. Vsako območje naj ima privzeti prehod svojega omrežja. Nastavi parameter DHCP lease na 14 dni za vsa območja.

c. Na WIN-CL11 preveri, če je dobil IP ter prave nastavitve. Klienta tudi dodaj v domeno.

7. Postavitev infrastrukture javnih ključev (PKI)

a. Domenske strežnike, ki jih boš uporabil za PKI, premakni pod OU Server in OU PKI.

b. PKI-okolje sestavljeno iz treh strežnikov in uporablja dvonivojsko PKI hierarhijo.

c. WIN-ROOTCA bo nedomenski strežnik in bo na koncu tudi izklopljen. Tu bo nastavljen t. i. »offline root certification authority«.

d. Za izdajanje certifikatov bo uporabljen strežnik WIN-SUBCA. Njegova vloga je »enterprise subordinate certification authority«.

e. WIN-CRLCA bo služil za t. i. »Certification Revocation List Distribution point«.

8. **WIN-ROOTCA**
    a. Namesti vlogo Active Directory Certificate Services. Nastavi korenskega izdajatelja (»Root CA«) z naslednjimi lastnostmi:
        - CA Type: Standalone CA.
        - Cryptographic provider: RSA Microsoft Software KSP.
        - Key length: 4096.
        - Hash algorithm: SHA256.
        - Ime korenskega certifikata nastavi na CREDITBANK-ROOT-CA.
        - Veljavnost korenskega certifikata naj bo 12 let.
        - CA naj izdaja certifikate veljavne za obdobje 5 let.
        - CRL naj se izdaja na pol leta, Delta CRL ne rabimo.
        - Za lokacijo o informaciji CRL in AIA Extension uporabi spodnjo lokacijo (razdelek WIN-CRLA), ki jo boš vpisal v DNS. Lokacijo podobno sestavi kakor je v primeru.
    b. ROOT certifikat dodaj preko orodja certutil tudi v aktivni imenik (preko AD strežnika), da se bo avtomatsko namestil na kliente.

9. **WIN-SUBCA**
    a. Namesti vlogo Active Directory Certificate Services. Uporabi CApolicy.inf., ki je na lokaciji C:\SloSkills. Lastnosti podrejenega CA:
        - CA Type: Enterprise Subordinate CA.
        - Cryptographic provider: RSA Microsoft Software KSP.
        - Key length: 4096.
        - Hash algorithm: SHA256.
        - Ime: CREDITBANK-ENTERPRISE-CA.
        - Za lokacijo o informaciji CRL in AIA Extensiona uporabi spodnjo lokacijo (razdelek WIN-CRLA), ki jo boš vpisal v DNS.
        - CRL naj se izdaja tedensko, delta CRL pa dnevno. Certifikati, ki jih izda Enterprise CA, morajo vedno dostopati do osveženih CRL, zato poskrbi, da bodo CRL vedno avtomatsko izdani tudi na server WIN-CRLCA, lokacija C:\CRL.

10. WIN-CRLCA

a. Namesti IIS in v DNS vpiši zapis CNAME »pki.creditbank.com«, ki kaže na strežnik WIN-CRLCA. V vse nadaljnje CRL-je in ostale potrebne certifikate skopiraj v lokalno mapo C:\CRL. IIS virtualna mapa pa naj kaže na to lokacijo.
b. Deli mapo in dodaj nanjo ustrezne pravice za obstoječo domensko skupino »Cert Publishers«. Člani te skupine morajo imeti pravice spreminjanja na to mapo. Onemogoči dedovanje pravic. Na IIS za virtualno mapo »crl« nastavi tudi »double escaping«. Uporabi datoteko »web.config«, ki jo dobiš na C:\SloSkills.
    1. (Nasvet: z orodjem pkiview preveri, da je vse pravilno nastavljeno).

11. PKI – konfiguracija predlog

a. Kreiraj naslednje predloge (»Template«), ki so edine na voljo za izdajanje certifikatov:
    - Creditbank User,
    - Creditbank Workstation,
    - Creditbank Web,
    - Creditbank Domain Controller Authentication (Kerberos).

b. Nastavitve vseh predlog:
    - Veljavnost 1 leto, čas za obnovitev 6 tednov.
    - Compatibility: Windows 10/Windows Server 2016 in novejši operacijski sistemi.
    - Key length 2048 bitov.
    - Algoritm: RSA.
    - Category provider: Key Storage provider.
    - Hash algorithm: SHA256.
    - Certifikata ne bomo shranjevali v AD.

c. Dodatno po predlogah nastavi sledeče:
    a. Creditbank User:
        - Izvoz privatnega ključa ni možen.
        - Zahtevek lahko uporabi kriptografska ponudnika »Microsoft Software Key Storage Provider« ali »Microsoft Platfrom Crypto Provider«.
        - Domenski uporabniki lahko poleg branja tudi oddajo zahtevek za nov certifikat. Certifikati se lahko samodejno obnavljajo.
        - »Subject Name« naj se zgradi iz informacij, ki jih zahtevek dobi iz AD-ja (Subject name format = CN; Alternate subject name = UPN).

b. Creditbank Workstation:
   - Izvoz privatnega ključa ni možen.
   - Zahtevek lahko uporabi kriptografska ponudnika »Microsoft Software Key Storage Provider« ali »Microsoft Platfrom Crypto Provider«.
   - Domenski uporabniki lahko poleg branja tudi oddajo zahtevek za nov certifikat. Certifikati se lahko samodejno obnavljajo.
   - »Subject Name« naj se zgradi iz informacij, ki jih zahtevek dobi iz AD-ja (Subject name format = DNS; Alternate subject name = DNS).

c. Creditbank Web:
   - Izvoz privatnega ključa je možen.
   - AD-skupina »PKI – Web servers« ima pravice za branje, kreiranje in samodejno obnavljaje teh certifikatov.
   - »Subject Name« naj bo zgrajen iz informacij, ki jih uporabnik vpiše ob kreiranju novega zahtevka za certifikat.
   - Dovoljen je katerikoli kriptografski ponudnik.

d. Creditbank Domain Controller Authentication (Kerberos):
   - Izvoz privatnega ključa ni možen.
   - »Subject Name« naj se zgradi iz informacij, ki jih zahtevek dobi iz AD-ja (Subject name format = None; Alternate subject name = DNS).
   - Dovoljen je katerikoli kriptografski ponudnik.

d. Uporabi predlogo Creditbank Web in kreiraj certifikat za pki.creditbank.com in ga uporabi na tej spletni strani.

e. PKI - GPO
   Kreiraj naslednje objekte »Group Policy«:
   - Certificate autoenrollment – Domain Controllers:
     - Naj gre samo na domenske kontrolerje.
   - Certificate autoenrollment – Workstations:
     - Gre na vse računalnike, tudi serverje (brez DC).
   - Certificate autoenrollment – Users:
     - Gre na vse domenske uporabnike.

   Za vsak GPO nastavi, da se certifikati sami obnovijo pred potekom in da klient avtomatsko dobi nov certifikat.

f. V kolikor se ne uporablja niti ena uporabniška nastavitev, ta del GPO-ja onemogoči. Enako velja za računalniški del nastavitve.

Preveri izdajanje certifikatov:

g. Z vsemi uporabniki se prijavi v klienta WIN-CL11 in preveri, da so dobili uporabniški certifikat. S skrbniškim računom preveri tudi certifikat računalnika in pravilnost namestitve certifikatov na strežnikih. Nato preveri še na vlogi Certification Authority izdajanje certifikatov.

OKOLJE LINUX

Dokumentacija:

https://www.redhat.com/sysadmin/linux-active-directory

https://www.rootusers.com/how-to-join-centos-linux-to-an-active-directory-domain/

https://access.redhat.com/solutions/1355683

https://www.zabbix.com/documentation/current/en/manual/installation/containers

https://www.zabbix.com/documentation/6.4/

https://rumaisaniazi008.medium.com/how-to-setup-rsyslog-as-a-centralized-logging-server-in-centos-3d2688620101

https://www.redhat.com/sysadmin/container-systemd-persist-reboot

https://access.redhat.com/documentation/en-us

https://github.com/dani-garcia/vaultwarden

https://www.digitalocean.com/community/tutorials/how-to-install-linux-apache-mysql-php-lamp-stack-on-centos-7

https://nginx.org/en/docs/beginners_guide.html

https://www.digitalocean.com/community/tutorials/how-to-install-nginx-on-centos-7

1. Vzpostavitev lokalnih repozitorijev iz ISO – lin-node 1 & lin-nod2

Zaradi omejenega dostopa do spleta je na strežnikih potrebno nastaviti lokalne repozitorije, iz katerih se lahko namestijo dodatni paketi. Lokalne repozitorije vzpostavite na strežnikih lin-node1 in lin-node2.

a. Dodajte lokalni ISO-disk in ga pripnite v direktorij /mnt/ISO. Zagotovite trajno namestitev ISO diska.
b. Onemogočite repozitorije, ki se povezujejo na splet:
    - centos.repo,
    - centos-addons.repo.
c. Kreirajte repozitorije, ki se povezujejo na ISO disk:
    - BaseOS,
    - AppStream.

2. Dodajate strežnik lin-node1 v domeno in pripravite uporabniške račune

Z vzpostavljenim centralnim upravljanjem uporabnikov v Aktivnem imeniku je potrebno urediti tudi dostop za domenske uporabnike za prijavo v strežnik Linux lin-node1.

a. Namestite potrebna orodja za povezavo z domeno:
   - sssd,
   - realmd,
   - oddjob,
   - oddjob-mkhomedir,
   - adcli,
   - samba-common,
   - samba-common-tools,
   - krb5-workstation,
   - openldap-clients.

b. Dodajte strežnik lin-node1 v domeno.
c. Kreirajte lokalnega »sudo« uporabnika credit_admin.
d. Kreirajte domenske uporabnike v AD-ju:
   - Privilegirani uporabniki: nik_adm, katja_adm.
   - Navadni uporabniki: nik, katja, jan.
e. Dodajte AD skupino, ki ima »sudo« (administrativne) pravice lin_sudo_users.
f. Dodajte AD skupino v kateri so navadni uporabniki lin_normal_users.
g. Dodajte SSH dostop za »sudo« in navadne domenske uporabnike.
h. Preprečite SSH povezavo za root uporabnika.

3. Vzpostavite nadzornega sistema Zabbix na strežniku lin-node1

V okolju podjetja Creditbank d.d. je potrebno vzpostaviti tudi spremljanje delovanja in obremenjenosti opreme in strežnikov. Za spremljanje opreme in strežnikov namestite Zabbix nadzorni servis na lin-node1 strežnik.

a. Dodajte ISO disk 3rd_party in ga pripnite v direktorij /mnt/3rd. Zagotovite tudi trajno namestitev ISO diska.
b. Namestite Podman:
   - Pripravite Zabbix podman image v direktorij /var/zabbix/
c. Uvozite in označite Zabbix podman image:
   - mysql,
   - zabbix-java-gateway,
   - zabbix-server-mysql,
   - zabbix-web-nginx-mysql.

d. Kreirajte omrežje za Zabbix v podman-u:
    - Podomrežje: 172.20.0.0/16.
    - Nabor naslovov IP: 172.20.240.0/20.
e. Zaženite Zabbix podman zabojnike iz predlog v sledečem zaporedju:
    - mysql,
    - zabbix-java-gateway,
    - zabbix-server-mysql,
    - zabbix-web-nginx-mysql.
f. Preverite delovanje Zabbix aplikacije.
g. V Zabbix dodajte strežniško opremo prek protokola SNMP.

4. Centralized rsyslog – lin-node1 & lin-node 2

Poleg spremljanja opreme in strežnikov je zahteva podjetja tudi zbiranje dnevniških zapisov iz strežnikov lin-node1 in lin-node2. Vlogo strežnika centralnega zbiralnika dnevniških zapisov ima strežnik lin-node1, strežnik lin-node2 pa ima vlogo odjemalca. Uporabite mehanizem Rsyslog, in sicer na način, da odjemalec pošilja svoje dnevniške zapise centralnemu zbiralniku.

Lin-node1:

a. Namestite rsyslog.
b. Zagotovite samodejno zaganjanje servisa rsyslog.
c. Nastavite rsyslog, da strežnik lin-node1 sprejema sporočila TCP in UDP iz vseh naprav.
d. Dodajte pravila požarne pregrade za rsyslog. Rsyslog naj posluša na vratih:
    - TCP 514,
    - UDP 514.
e. Naredite test pošiljanja sporočil.

Lin-node2:

a. Namestite rsyslog.
b. Zagotovite samodejno zaganjanje servisa rsyslog.
c. Nastavite rsyslog, da strežnik pošilja pakete TCP in UDP na strežnik lin-node1.
d. Dodajte pravila požarne pregrade za rsyslog. Rsyslog pošilja na vratih:
    - TCP 514,
    - UDP 514.
e. Naredite test pošiljanja sporočil.

5. Podman Vaultwarden – node2

Zaradi kompleksnih gesel in potrebe po varnem hranjenju gesel podjetja Creditbank d.d. je v uporabi aplikacija VaultWarden, ki ima vlogo hranilnika gesel. Navodila za vzpostavitev:

a. Dodajanje ISO disk 3rd_party:
    - Disk pripnite na direktorij /mnt/3rd
b. Zagotovite trajno namestitev ISO diska.
c. Kreirajte navadnega lokalnega uporabnika service_vault.
d. Namestite paket Podman.
e. Pripravite VaultWarden podman image v direktoriju /var/vault/
f. Uvozite in označite VaultWarden podman image.
g. Zaženite VaultWarden zabojnik.
h. Preverite delovanje VaultWarden aplikacije.
i. Kreirajte sistemd datoteko za VaultWarden servis.
j. Ugasnite in odstranite VaultWarden zabojnik.
k. Pripravite direktorij ~/.config/systemd/user/ za servis pod lokalnim uporabnikom service_vault.
l. Zaženite VaultWarden servis z lokalnim uporabnikom service_vault.
m. Zagotovite samodejno zaganjanje servisa VaultWarden.
n. Dodajte pravila požarne pregrade za VaultWarden. VaultWarden naj objavlja servis na vratih 8080.
o. Preverite delovanje servisa VaultWarden.

6. Sklad LAMP – node2

Aplikacija ima vlogo ToDo liste, ki predstavlja proceduro vnosa novega zapisa stranke v bazo podatkov za zaposlene.

a. Namestite LAMP stack:
    - httpd,
    - mysql (mariadb),
    - php.
b. Zagotovite samodejno zaganjanje servisov.
c. Kreirajte uporabnika service_mysql.
d. Kreirajte SQL bazo podatkov in dodajte pravice za uporabnika service_mysql:
    - Ime baze: todo_db
    - Ime tabele: todo_table
    - V tabelo todo_table zapišite opravila:
        - ime stranke,
        - število zaposlenih,
        - letni dobiček stranke,
        - letni stroški stranke.
e. Pripravite php spletno aplikacijo, ki prikazuje ToDo list iz baze SQL:
    - php skripta v direktoriju /var/www/html/ z imenom todo_list.php:
        - prebere z uporabnikom service_mysql podatke iz tabele todo_table,
        - podatke iz tabele nato prikaže na spletni strani.