DETALIOS LOGINĖS DEBESIJOS PASLAUGŲ TEIKIMO IT INFRASTRUKTŪROS ARCHITEKTŪROS PARENGIMO IR TECHNINĖS IR PROGRAMINĖS ĮRANGOS REIKALAVIMŲ PARENGIMO PASLAUGA

PRIE 2019-01-14 sutarties Nr: 6F-1

LOGINĖ DEBESIJOS PASLAUGŲ TEIKIMO IT INFRASTRUKTŪROS ARCHITEKTŪRA

Versija: 6.0.0

Data: 2019.04.26

Būklė: Patvirtintas

Ekonomikos ir inovacijų viceministras
Elijus Čivilis
2019-04-26

Ekonomikos ir inovacijų ministerijos
Skaitmeninės darbotvarkės departamento
direktorius
Arūnas Cijūnaltis
2019-04-26

Turinys

1 Bendroji dalis

1.1 Dokumento tikslas

Šiame dokumente pateikta Loginė Debesijos paslaugų teikimo IT infrastruktūros architektūra, apimanti:

- virtualizuotų tarnybinių stočių architektūros modelį;
- virtualizuotų duomenų talpyklų architektūros modelį;
- duomenų perdavimo tinklų fizinės bei loginės tinklo topologijos architektūros modelį;
- saugos sprendimo modelį;
- rezervinio kopijavimo sistemų veiklos modelį.

1.2 Tvirtinimo forma

Pareigos	Vardas, pavardė	Parašas	Data
Perkančioji organizacija:			
IVPK Projekto vadovas	Andžej Trachimovič		2019-04-26
IVPK Techninės grupės vadovas	Jonas Ignatavičius		2019-04-26
Tiekėjas:			
Telia Lietuva projekto vadovas	Mindaugas Zlatarinskas		2019-04-26

1.3 Derinimo forma

Pareigos	Vardas, pavardė	Parašas	Data
Perkančioji organizacija:			
IVPK techninės įrangos administratorius	Vilmantas Povilaitis		2019-04-26
IVPK techninės įrangos administratorius	Vygintas Čiurlionis		2019-04-26
IVPK techninės įrangos administratorius	Artūras Lisauskas		2019.04.26
IVPK techninės įrangos administratorius	Dimitrian Kondrašov		2019.04.26
IVPK techninės įrangos administratorius	Justinas Mačionis		2019-04-26

NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS
PRIE KRAŠTO APSAUGOS MINISTERIJOS

Informacinės visuomenės plėtros komitetui

2019-03- Nr.
Į 2019-03-15 Nr. S-150

DĖL DETALIOS LOGINĖS DEBESIJOS PASLAUGŲ TEIKIMO IT INFRASTRUKTŪROS ARCHITEKTŪROS DERINIMO

Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos, išnagrinėjęs Informacinės visuomenės plėtros komiteto 2019 m. kovo 15 d. raštu Nr. S-150 „Dėl detalios loginės debesijos paslaugų teikimo it infrastruktūros architektūros derinimo“ pateiktą pagal paslaugų pirkimo sutartį Nr. 6F-1 su AB Telia Lietuva parengtą detalios loginės debesijos paslaugų teikimo IT infrastruktūros architektūros aprašymą, esminių pastabų ir pasiūlymų neturi. Architektūros aprašymą laikome suderintu.

Direktorius dr. Rytis Rainys

Remigijus Zakarauskas, tel. 8 706 79 607, el. p. remigijus.zakarauskas@kam.lt

DETALŪS METADUOMENYS	
Dokumento sudarytojas (-ai)	Nacionalinis kibernetinio saugumo centras prie KAM 191630942, Vilnius, Gedimino pr. 40
Dokumento pavadinimas (antraštė)	DĖL DETALIOS LOGINĖS DEBESIJOS PASLAUGŲ TEIKIMO IT INFRASTRUKTŪROS ARCHITEKTŪROS DERINIMO
Dokumento registracijos data ir numeris	2019-03-21 Nr. (4.2 E) 6K-200
Dokumento gavimo data ir dokumento gavimo registracijos numeris	2019-03-21 Nr. G-443
Dokumento specifikacijos identifikavimo žymuo	ADOC-V1.0
Parašo paskirtis	Pasirašymas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	RYTIS RAINYS, Direktorius, Vadovybė
Sertifikatas išduotas	RYTIS,RAINYS LT
Parašo sukūrimo data ir laikas	2019-03-21 09:45:46 (GMT+02:00)
Parašo formatas	XAdES-T
Laiko žymoje nurodytas laikas	2019-03-21 09:46:05 (GMT+02:00)
Informacija apie sertifikavimo paslaugų teikėją	EID-SK 2016, AS Sertifitseerimiskeskus EE
Sertifikato galiojimo laikas	2019-01-11 10:20:06 – 2024-01-10 23:59:59
Informacija apie būdus, naudotus metaduomenų vientisumui užtikrinti	"Registravimas" paskirties metaduomenų vientisumas užtikrintas naudojant "RCSC IssuingCA, VI Registru centras - i.k. 124110246 LT" išduotą sertifikatą "Dokumentų valdymo sistema DokVIS, Lietuvos Respublikos krašto apsaugos ministerija, į.k.188602751 LT", sertifikatas galioja nuo 2018-12-27 13:53:48 iki 2021-12-26 13:53:48 "Gauto dokumento registravimas" paskirties metaduomenų vientisumas užtikrintas naudojant "RCSC IssuingCA, VI Registru centras - i.k. 124110246 LT" išduotą sertifikatą "Dokumentų valdymo sistema Avilys, Informacinės visuomenės plėtros komitetas, į.k.188772433 LT", sertifikatas galioja nuo 2019-02-19 08:15:45 iki 2022-02-18 08:15:45
Pagrindinio dokumento priedų skaičius	–
Pagrindinio dokumento pridedamų dokumentų skaičius	–
Pridedamo dokumento sudarytojas (-ai)	–
Pridedamo dokumento pavadinimas (antraštė)	–
Pridedamo dokumento registracijos data ir numeris	–
Programinės įrangos, kuria naudojantis sudarytas elektroninis dokumentas, pavadinimas	Dokumentų valdymo sistema Avilys, versija 3.5.1
Informacija apie elektroninio dokumento ir elektroninio (-ių) parašo (-ų) tikrinimą (tikrinimo data)	Atitinka specifikacijos keliamus reikalavimus. Visi dokumente esantys elektroniniai parašai galioja (2019-03-21 11:13:30)
Paieškos nuoroda	–
Papildomi metaduomenys	Nuorašą suformavo 2019-03-21 11:13:30 Dokumentų valdymo sistema Avilys

1.4 Dokumento istorija

Rev.	Data	Autorius	Pakeitimai
1	2019.01.16	Robertas Balkys	Sukurtas dokumentas
2	2019.02.18	Antanas Vainauskas	Aprašytas tinklo sprendimas
3	2019.02.18	Justinas Balčiūnas	Aprašyta konteinerių platforma
4	2019.02.18	Darius Klepšys	Aprašyta serverių, saugyklų ir rezervinio duomenų kopijavimo architektūra
5	2019.02.18	Robertas Balkys	Aprašytas paslaugų krepšelis ir valdymo sluoksnis
6	2019.02.18	Mindaugas Zlatarinskas	Aprašytas paslaugų krepšelis bei kiti infrastruktūros elementai
7	2019.02.18	Vilija Bakutienė	Dokumentas pakoreguotas pagal IVPK pastabas
8	2019.02.19	Agnė Nairanauskaitė	Dokumento rašybos ir stilistikos korekcijos
9	2019.02.22	Mindaugas Zlatarinskas	Dokumentas pakoreguotas pagal IVPK pastabas. Suformuota galutinė dokumento versija tvirtinimui
10	2019.03.27	Mindaugas Zlatarinskas	Dokumento korekcijos atsižvelgus į rinkos dalyvių pastabas

1.5 Konfidencialumas

Šiame dokumente aprašytas sprendimas (toliau - Sprendimas) bei visa su juo susijusi dokumentacija, atskiros sprendimo dalys yra laikoma konfidencialia informacija, kaip tai numatyta pagrindinėje Sutartyje Nr. 6F-1 (toliau - Sutartis).

Sutarties Šalys stengsis visomis galimomis priemonėmis užtikrinti, kad konfidenciali informacija nebūtų atskleista ir platinama šalių darbuotojų ar agentų, pažeidžiant Sutarties ir jos priedų sąlygas.

Sutarties Šalys įsipareigoja konfidencialią viena kitos informaciją saugoti šios Sutarties galiojimo laikotarpiu ir 10 metų po jo pasibaigimo.

Šalys supranta, kad toks sukurtas Sprendimas yra skirtas išimtinai šios Sutarties vykdymui. Jeigu Perkančioji organizacija šios Sutarties galiojimo laikotarpiu vienašališkai ir iš esmės pakeičia suderintą ir patvirtintą Sprendimą, AB Telia Lietuva neprisiima atsakomybės už galutinio Sprendimo veikimą.

1.6 Sąvokų žodynas

Nr.	Sąvokos / Trumpiniai	Aprašymas

1	AaaS	Automatizavimas kaip paslauga
2	ADC	Application Delivery Controller – srauto balansavimo įrenginys
3	ADG	Active data guard
4	Affinity rules	Taisyklės, suteikiančios galimybę apriboti virtualių tarnybinių stočių veikimą skirtingose fizinėse tarnybinėse stotyse
5	AntiDDoS	Įranga apsaugai nuo DDoS atakų
6	AntiSpam	Apsauga nuo nepageidaujamų laiškų
7	AntiVirus	Įranga apsaugai nuo virusų
8	API	Aplikacijos programavimo interfeisas
10	BACKUP	Atsarginė duomenų kopija
11	CPU	Procesorius
12	DC	Duomenų centras (patalpa ar grupė patalpų, skirti centralizuotam informacinių technologijų ir tinklo įrangos, skirtos reikiamo patikimumo ir saugumo lygio duomenų saugojimo, apdorojimo ir perdavimo paslaugų teikimui, kartu su infrastruktūra ir įrenginiais, skirtais elektros maitinimui ir aplinkos palaikymui)
13	DCaaS	Techninės įrangos talpinimo duomenų centro patalpose paslauga (angl. *Data Centre as a Service – DCaaS*)
14	DCI	Duomenų centrų sujungimas
15	DG	Data guard
16	DR	Disaster recovery – veiklos atkūrimas
17	DWDM	Dense Wavelength Division Multiplexing
18	Edge	Prieiga prie tinklo
19	EE	Enterprise edition
20	FWaaS	Ugniasienė kaip paslauga
21	HA	Aukštas prieinamumas
22	HC	HyperConverged technologija – specializuoti sprendimai, apimantys visus klasikinės architektūros elementus vienoje platformoje
24	IaaS	Techninė įranga kaip paslauga (angl. *Infrastructure as a Service – IaaS*)
25	IDS	Įsilaužimų aptikimo sistema
26	IS	Informacinė sistema
27	Investicijų projektas	„Valstybės debesijos paslaugų teikimo infrastruktūros sukūrimas“ investicijų projektas
28	IO	Input / Output
29	IOPS	Input / Output operacijos per sekundę
30	IPaaS	Infrastruktūra kaip programinis kodas
31	IPS	Įsilaužimų prevencijos sistemos

32	IRT	Informacinės ir ryšių technologijos
33	LAN	Local area network – vietinis kompiuterinis tinklas
34	LB	Srauto balansavimas
37	MaaS	Stebėjimas kaip paslauga
38	MFA	Daug faktorių autentifikacija
39	NMS	Tinklo valdymo sistema
40	OS	Operacinė sistema
41	OSI	Open Systems Interconnection Reference Model – abstraktus ryšio protokolų, naudojamų ryšio ir kompiuteriniuose tinkluose, aprašymas
42	PaaS	Programinės įrangos platforma kaip paslauga (angl. *Platform as a Service – PaaS)*
43	Patches	Pataisos
44	PDU	Power distribution unit
45	PĮ	Programinė įranga
46	PĮK	Programinės įrangos konteineriai
47	Proxy	Tarpinis serveris
48	PTL	Paslaugų teikimo lygiai. PTL=SLA
50	RAM	Operatyvinė atmintis
51	RPO	Laikotarpis, kurio duomenis galima prarasti
52	RTO	Laikas, apibrėžiantis kiek gali neveikti sistema
53	SaaS	Programinė įranga kaip paslauga (angl. *Software as a Service – SaaS*)
54	SAN	Angl. storage area network – tinklas, apjungiantis duomenų saugyklas
55	SDN	Software Defined Network
56	SDS	Duomenų saugojimo sprendimas
57	SE	Standart edition
58	SIEM	Saugos informacijos ir įvykių valdymo sistema
59	SIEMaaS	Saugos informacijos ir įvykių valdymo sistema kaip paslauga
60	SPOF	Single point of failure
61	SSO	Single sign - on – prieigos kontrolė, kuri leidžia su vienu vartotojo vardu ir slaptažodžiu prieiti prie skirtingų sistemų
62	SVDPT	Saugusis valstybinis duomenų perdavimo tinklas (Saugusis tinklas) – valstybės valdomas specialiuosius organizacinius ir techninius reikalavimus atitinkantis ir nuo viešųjų elektroninių ryšių tinklų nepriklausomas elektroninių ryšių tinklas.
63	Tenantas	Tenantas – izoliuota loginė skaičiavimo / saugyklų / tinklo / saugumo paslaugų resursų aibė, priskiriama vienai įstaigai / organizacijai.
64	ToR	Top of Rack

65	Updates	Atnaujinimai
66	vCPU	Virtualios tarnybinės stoties procesorius
67	VDPT	Valstybės debesijos paslaugų teikėjas (VDPT=VITC)
68	VITC / Valstybės informacinių technologijų centras	Biudžetinė įstaiga Valstybės informacinių technologijų centras, kuri vykdys Valstybės IRT paslaugų teikėjo funkcijas bei kitas teisės aktų nustatytas funkcijas (VITC=VDPT)
69	VPN	Virtualus privatus ryšys
70	VPNaaS	Virtualus privatus ryšys kaip paslauga
71	WAF	Internetinių / taikomųjų programų lygmens ugniasienių sistema

2 Įvadas

Platforma projektuojama atsižvelgiant į naujausias tendencijas, geriausias pasaulines praktikas, standartus, teisės aktų reikalavimus ir Telia kompanijos sukauptą patirtį kuriant bendro naudojimo (angl. public) debesijos sprendimus, virtualizuojant tinklo elementus ir paslaugas, automatizuojant paslaugų teikimą, užsakymų vykdymą.

Vertinant naujausių IT sprendimų praktinį pritaikymą debesijos platformose buvo analizuojami Microsoft Azure Stack, HPE Helion/Hybrid Cloud solutions, OpenStack, VMware, Nutanix, Dell EMC VxRail ir kiti rinkoje siūlomi specializuoti debesijos sprendimai, jų architektūros bei naudojimo ypatybės.

Sprendimų projektavimui planuojami naudoti technologiniai elementai, įrankiai, jų rinkiniai buvo vertinami platesnės ekosistemos kontekste apimant, bet neapsiribojant, žemiau įvardintų gamintojų produktus ir sprendimus:

- A10 Networks;
- AMD;
- Bitdefender;
- Check Point Software Technologies;
- Cisco;
- Commvault;
- Dell EMC;
- Elastic Stack;
- F5 Networks;
- Fortinet;
- Gigamon;
- Hitachi;
- HPE;
- IBM;
- Intel;
- Juniper Networks;
- Lenovo;
- McAfee;
- Microsoft;
- nCipher Security;
- NetApp;
- Nuage Networks;
- Nutanix;
- Oracle;
- Palo Alto Networks;
- Pivotal Software;

- Rancher;
- Red Hat;
- RSA Security;
- Symantec;
- Splunk Technology;
- Veeam;
- Veritas;
- VMware;
- Zabbix.

Atsižvelgiant į konsolidacijos mastą, esamų sistemų specifiką ir debesijos principais paremtus valdymo poreikius buvo pasirinktas hibridinės infrastruktūros architektūros variantas iš tinkamiausių komponentų: klasikiniai virtualizuotų tarnybinių stočių ir duomenų saugyklų sprendimai bei vieni moderniausių virtualizuotų tinklų ir tinklo saugos funkcijų sprendimai. Sprendimo apimtyje be kitų modernių technologijų, nuspręsta panaudoti vieną iš šiuo metu labiausiai besivystančių – HyperConverge technologiją, – specializuotus sprendimus, apimančius visus klasikinės architektūros elementus vienoje platformoje. Sprendimas projektuojamas taip, kad ateityje, kai įstaigų informacinės sistemos ir registrai bus kuriami pasitelkiant modernias technologijas bei metodus, būtų galima infrastruktūrą plėsti naudojant pagrindinių gamintojų sertifikuotus, plačiausiai naudojamus debesijos sprendimus arba dalį infrastruktūros migruoti į viešuosius debesijos sprendimus (angl. Public cloud).

3 Esamos situacijos analizė

Šiame dokumento skyriuje detalizuojami, su IVPK atstovais suderinti, numatomų teikti Debesijos paslaugų keliami tikslai, užduotys, galimi panaudojimo scenarijai, diegimo etapų apimtys, rizikos ir apribojimai.

3.1 Keliami tikslai

Investicijų projekto tikslas yra sukurti ir įdiegti valstybės debesijos paslaugų teikimo veiklai reikalingą IRT infrastruktūrą.

Darbo grupėje detalizuoti tikslai:

- planuojama infrastruktūra turi leisti konsoliduoti viešojo sektoriaus įstaigų IRT ūkį (pagal patvirtintą sąrašą);
- planuojama infrastruktūra turi leisti teikti debesijos paslaugas viešojo sektoriaus įstaigoms.

3.2 Užduotis

Patvirtinti uždaviniai:

- Parengti virtualizuotų tarnybinių stočių architektūros modelį;
- Parengti virtualizuotų duomenų talpyklų architektūros modelį;
- Parengti duomenų perdavimo tinklų fizinės bei loginės tinklo topologijos architektūrų modelius;
- Parengti rezervinio kopijavimo sistemų veiklos modelį;
- Parengti ir su II, III etapais atnaujinti techninės įrangos reikalavimus;
- Parengti ir suderinti su Nacionaliniu kibernetinio saugumo centru saugos sprendimo modelį, suderinti loginės Debesijos paslaugų teikimo IT infrastruktūros architektūros sprendimą;
- Pateikti pasiūlymus, skaičiavimus ir pagrindimus dėl Debesijos numatomų teikti paslaugų galimų ir efektyviausių architektūrinių sprendimų įgyvendinimo I,II ir III etapui.

3.3 Dokumentų analizė

Projekto komanda išanalizavo žemiau išvardintus dokumentus:

- „Investicijų projektas Valstybės debesijos paslaugų teikimo infrastruktūros sukūrimas“;
- pirkimo dokumentuose pateiktą fizinę aukšto lygio tinklo apjungimo schemą;
- fizinių techninės įrangos komponentų schemą;
- techninės įrangos skaičiuoklę, kurioje yra pateiktas techninės įrangos įsigijimo ir įdiegimo pradinis modeliavimas, montuojamų spintų komplektacija atskiruose duomenų centruose;
- IVPK atstovų pateiktus duomenis apie šiuo metu įstaigų naudojamą infrastruktūrą, turimas licencijas, informacines sistemas ir t.t;
- Pirkimo dokumentuose įvardintus teisės aktus.

3.4 Numatytų etapų apimtis, reikalavimai projektavimui

I etapas

Esminės prielaidos I etapo infrastruktūros projektavimui:

VDPT infrastruktūra, infrastruktūros talpa (su 30 - 40% rezervu) ir bazinis paslaugų krepšelis planuojami atsižvelgiant į numatytų konsoliduoti 7 pilotinių įstaigų (Ekonomikos ir inovacijų ministerija, Informacinės visuomenės plėtros komitetas, Energetikos ministerija, Susisiekimo ministerija, Sveikatos apsaugos ministerija (be E-sveikata informacinės sistemos IRT infrastruktūros), Valstybinė mokesčių inspekcija, Muitinės informacinių sistemų centras) ir įstaigų, kurios pagal 2 bei 10 prioritetų investicinius projektus šiuo metu kuria informacines sistemas, kurių diegimas numatytas iki 2020 m. I ketv., pateiktus pradinius resursų poreikius diegimui / konsolidacijai. Resursų valdymo automatizavimas nebus diegiamas arba bus diegiamas minimalia apimtimi. Planuojama naudoti 2 vnt. duomenų centrų Vilniaus regione (vėlinimas tarp DC matuojant į abi puses iki 1ms, atstumas iki 30 km matuojant trasomis) + Backup infrastruktūrai DC Kaune + NATO duomenų centre diskinė erdvė kritinių duomenų kopijoms talpinti.

II etapas

Išplečiama talpa konsolidacijai ir debesijos paslaugų teikimui. Sukuriamos papildomos debesijos paslaugos paslaugų krepšelyje. Automatizuojamas resursų valdymas.

III etapas

Išplečiama talpa konsolidacijai, naujų informacinių sistemų talpinimui ir debesijos paslaugų teikimui. Paslaugų krepšelis išplečiamas papildomomis paslaugomis.

Iki 2021 m. planuojama pilnai įrengti papildomus du duomenų centrus (arba vieną DC su dviem nepriklausomomis serverinėmis) Kauno regione (vėlinimas tarp DC matuojant į abi puses iki 1ms, atstumas iki 30 km matuojant trasomis). Šiame etape VDPT infrastruktūros talpinimui planuojama naudoti 2 vnt. duomenų centrų Vilniaus regione (vėlinimas tarp DC matuojant į abi puses iki 1ms, atstumas iki 30 km matuojant trasomis) + 2 vnt. duomenų centrų (arba vienas DC su dviem nepriklausomomis serverinėmis) Kauno regione + NATO duomenų centre diskinė erdvė kritinių duomenų kopijoms talpinti.

Tolimesni etapai

Hibridiniai sprendimai su kitais debesijos tiekėjais (pvz.: Microsoft, Amazon, Google) ir organizacijomis.

Tolimesnė PaaS / SaaS, automatizacijos ir savitarnos plėtra.

Įrangos gyvavimo ciklo valdymas ir savalaikė platformos plėtra.

3.5 Rizikos

Esminė rizika – suprojektuota VDPT infrastruktūra gali nepilnai atitikti IVPK ir migruojamų įstaigų ar organizacijų poreikius.

Argumentai šios rizikos iškėlimui:

1. Bendrinė konsoliduota informacija apie institucijų naudojamus technologinius resursus neatspindi informacinių sistemų faktinės konfigūracijos su visais programiniais komponentais, sąsajomis ir resursų naudojimo intensyvumu. Tokia informacija turės būti tikslinama ir pakartotinai vertinama prieš pradedant migruoti konkrečią informacinę sistemą;
2. Įstaigų pateikta informacija gali būti netiksli, pateikta nepilna apimtimi ir detalumu;
3. Infrastruktūros valdymo atsakomybių pasiskirstymo tarp KAM, VDPT ir įstaigų pokyčiai.

Rizikos mažinimo priemonė – platforma projektuojama taip, kad esant poreikiui būtų galima nesudėtingai išplėsti 3 - 4 kartus.

3.6 Apribojimai

Infrastruktūros projektavimas neapima debesijos paslaugų valdymo projektavimo ir platformos įdiegimo, debesijos paslaugų sukūrimo, debesijos paslaugų teikėjo žmogiškųjų išteklių bei jų kompetencijos suformavimo, esamų sistemų migracijos projektavimo ir migracijos. Šios sutarties apimtyje nebus teikiamos šios paslaugos:

- Sukurti ir įdiegti Debesijos paslaugų teikimo valdymo platformą ir Debesijos paslaugų teikimui reikalingas priemones;
- Techninės įrangos ir saugos sprendimo techninių priemonių debesijos paslaugų teikimui įsigijimas ir parengimas;
- VDPT organizacijos siekiamo IT veiklos valdymo bei veiklos planavimo ir valdymo reglamentavimo ir jo įgyvendinimo priemonių (politikų, procesų, procedūrų), būtinų sėkmingam infrastruktūros konsolidavimui ir numatytiems rezultatams pasiekti, parengimas / atnaujinimas;
- Valstybės informacinių išteklių infrastruktūros debesijos paslaugų teikimo IT infrastruktūroje, įgalinant jų veikimą ir tvarkymą naudojant debesijos paslaugas, talpinimo;
- VDPT organizacijos institucinių ir žmogiškųjų išteklių žinių, gebėjimų bei kompetencijų, reikalingų teikti Debesijos paslaugas ir valdyti VDPT organizaciją vadovaujantis pasaulyje pripažintomis metodikomis ir gerosiomis praktikomis suteikimo ir sustiprinimo;
- Priemonių Projekto įgyvendinimui ir tęstinumui užtikrinti parengimo.

3.7 Esamos situacijos įvertinimas

Perkančioji organizacija įvardino tokius VDPT platformos panaudojimo scenarijus:

- institucijų esamo IRT ūkio perkėlimas į konsoliduotą infrastruktūrą (pilnai arba dalinai);
- naujai įsteigiamų institucijų IRT ūkio diegimas konsoliduotoje infrastruktūroje;
- esamų informacinių sistemų perkėlimas be esminio programinio kodo pakeitimo į konsoliduotą infrastruktūrą (pilnas arba dalinis);
- naujai kuriamų informacinių sistemų diegimas konsoliduotoje infrastruktūroje.

Projektuojamas sprendimas turi atsižvelgti į tai, kad sprendimo priežiūra reikalautų kaip įmanoma mažiau žmogiškųjų ir finansinių resursų.

Projektuojant sprendimą galima tikslinti (didinti arba mažinti) investicijų projekte numatytus DC spintų kiekius. Sprendimo architektūros dokumente turi būti įvardinta, koks bendras spintų kiekis reikalingas (per visus numatomus DC).

Fizinės įrangos talpinimo duomenų centre paslaugos neprojektuojamos. Paslaugų kataloge ši paslauga įtraukiama kaip galima. Projektuojant infrastruktūrą reikia atsižvelgti į tai, kad dalis klientų gali užsakinėti ne tik debesijos paslaugas, bet ir fizinės įrangos talpinimo duomenų centre paslaugą.

Projektuojant bendrą infrastruktūros architektūrą reikia atsižvelgti į tai, kad infrastruktūros resursus būtų galima plėsti bent 3 - 4 kartus, naudojant skirtingų gamintojų įrangą.

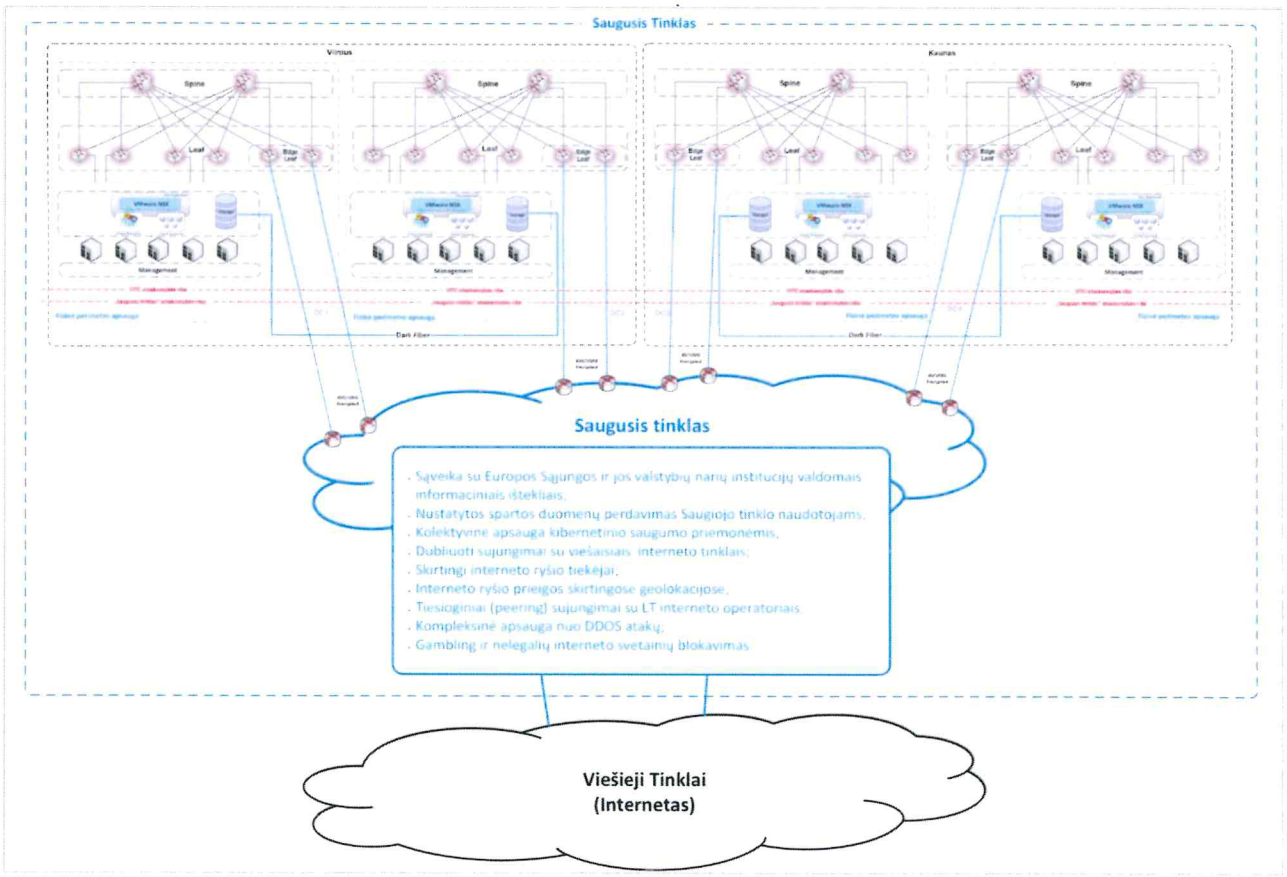
IVPK atstovai patvirtino, kad pagal šiai dienai turimą informaciją, planuojamos migruoti sistemos nėra pritaikytos modernioms debesijos platformoms. Dauguma naudojamų informacinių sistemų suprojektuotos ir realizuotos naudojant klasikinės architektūros principus. Pirmos ir antros kategorijos valstybės informacinės sistemos bei valstybės registrai naudoja Oracle, Microsoft SQL, SAP HANA duomenų bazes. Aukšto pasiekiamumo užtikrinimui naudojami klasikiniai klasterizavimo mechanizmai. Dalis sprendimų įdiegta per du nepriklausomus duomenų centrus. Naudojami saugyklų lygio arba duomenų bazių lygio sinchroninio duomenų replikavimo sprendimai. VMI ir VRM naudoja saugyklų virtualizacijos technologijas. Dauguma serverių virtualizuoti. Dažniausiai naudojama Vmware virtualizavimo platforma, mažiau Microsoft Hyper-V ir kitos virtualizacijos platformos. Įstaigos, kurias planuojama migruoti pirmame etape, naudoja savo IRT infrastruktūrą, t. y. turi savo įrengtus duomenų centrus, perka ir prižiūri įstaigos poreikiams reikalingą IRT infrastruktūrą. Įstaigose dirba IT specialistai, kurie prižiūri naudojamą infrastruktūrą. Dalį sprendimų diegimo ir priežiūros paslaugų perka iš privačių įmonių. Naudojama įvairių gamintojų įranga. Standartizacijos tarp įstaigų nėra. Konsolidavimo metu neplanuojama sistemų perkurti naudojant debesijos aplinkoms pritaikytas technologijas. Dalis informacinių sistemų suprojektuotos taip, kad IP adresų keitimas gali pareikalauti programinio kodo keitimo, todėl labai svarbu projektuojant naujus sprendimus numatyti galimybę įstaigoms išlaikyti šiuo metu naudojamus IP adresus. Kuriant naujas informacines sistemas bandoma reikalauti iš tiekėjų, kad būtų naudojamos debesijos aplinkoms pritaikytos technologijos, tačiau susiduriama su situacija, jog dažniausiai tiekėjų darbuotojai apie tokias technologijas žino, tačiau realiai jų nenaudoja. Keliant reikalavimus tiekėjams naujas sistemas kurti naudojant debesijos technologijas, tokių sistemų sukūrimo kaina kyla eksponentiškai.

Organizacijos, kurias planuojama migruoti, naudoja WAF, srauto balansavimo, tinklo ugniasienių, IDS, IPS, SSO, MFA VPN ir Proxy sprendimus. Naudojami sprendimai yra skirtingų gamintojų arba naudojamas skirtingas analogiškų sprendimų funkcionalumas. Daugumoje įstaigų dirbantys IT specialistai prižiūri šiuos sprendimus. Dalis priežiūros ir diegimo paslaugų perkama iš privačių įmonių.

Interneto, sujungimų tarp DC, sujungimų tarp institucijos padalinių paslaugas teikia ryšio paslaugų teikėjai. Kai kurios įstaigos naudoja AntiDDoS sprendimus. Šiuos sprendimus taip pat teikia ryšio paslaugų teikėjas. Dažniausia šias paslaugas teikia VĮ Infostruktūra, kita dalis įstaigų analogiškas paslaugas perka iš privačių ryšio paslaugų teikėjų. Be anksčiau minėtų paslaugų, įstaigos naudoja Saugaus valstybinio duomenų perdavimo tinklo ir saugaus sujungimo su kitomis Europos sąjungos valstybėmis sprendimus. Šiuos sprendimus įstaigoms teikia VĮ Infostruktūra ir kitos teisės aktuose numatytos įstaigos ir organizacijos.

Atsižvelgiant į tai, kad planuojamas tinklo paslaugų valdymo automatizavimas, debesijos paslaugų platformos priemonėmis visus VITC DC vidinius tinklus valdys ir

aptarnaus VITC. Ryšio paslaugų teikėjas BĮ „Saugusis tinklas“ teiks fizinius sujungimus tarp DC, užtikrins centralizuotą tinklo monitoringą bei teiks kitas, paslaugų krepšelyje numatytas tinklo paslaugas (AntiDDos, Internetas, SVDPT ir kt.). VITC ir KAM suderintų ir patvirtintų atsakomybių ribų schema pateikiama žemiau (pav. 3-1 Atsakomybių ribų schema)



pav. 3-1 Atsakomybių ribų schema

SAN tinklo kontekste ryšio paslaugų teikėjas irgi teiks tik fizinius sujungimus. Visa VITC SAN tinklo infrastruktūra projektuojama šio projekto apimtyje.

Šio projekto apimtyje įranga gali būti įsigyjama tik kaip ilgalaikis turtas. Nuomos ir panašios paslaugos negali būti naudojamos.

3.8 Duomenų centrai

Darbo grupės posėdžiuose nutarta, kad vėlinimas tinkle gali turėti esminės įtakos greitaveikai. Sprendimams, kurie reikalaus duomenų sinchroninės replikacijos, vėlinimas, didesnis kaip 1ms, – nepriimtinas. Atsižvelgiant į tai, svarstyti žemiau įvardinti variantai:

- Naudoti du duomenų centrus Vilniuje, nutolusius vienas nuo kito iki 30 km matuojant trasomis ir trečią duomenų centrą Kaune (rezervinėms duomenų kopijoms laikyti);
- Naudoti vieną duomenų centrą su dviem nepriklausomomis serverinėmis Vilniuje ir antrą duomenų centrą Kaune (rezervinėms duomenų kopijoms laikyti);

- Naudoti du duomenų centrus Vilniuje, nutolusius vienas nuo kito iki 30 km ir du duomenų centrus Kaune, nutolusius vienas nuo kito iki 30 km;
- Naudoti vieną duomenų centrą su dviem nepriklausomomis serverinėmis Vilniuje ir vieną duomenų centrą su dviem nepriklausomomis serverinėmis Kaune;
- Aptartos ir kitos anksčiau minėtų variantų kombinacijos.

Priimti sprendimai dėl duomenų centrų išsidėstymo:

- Pirmame etape bus 2 vnt. DC Vilniuje (iki 30 km atstumu) + rezerviniai DC Kaune ir NATO;
- Iki 2021 m. planuojama įrengti papildomus 2 vnt. DC Kaune (arba dvi atskirtos DC patalpos tame pačiame pastate).

Sprendimai turi būti projektuojami taip, kad aukštas prieinamumas (angl. HA) būtų užtikrinamas miesto (regiono) lygyje. Veiklos atkūrimo (angl. DR) atveju sistemos būtų atstatomos į kito miesto (regiono) duomenų centrus.

3.9 Prielaidos, kuriomis remiantis projektuojamas sprendimas

Šiame skyriuje aprašomos prielaidos, kuriomis remiantis projektuojamas sprendimas:

- Infrastruktūra turi būti suprojektuota taip, kad esant poreikiui jos talpą (išteklių resursus) būtų galima nesudėtingai plėsti bent 3 - 4 kartus;
- Infrastruktūros skaičiavimo telkiniai turi būti realizuojami x86 procesorių architektūros pagrindu;
- Infrastruktūra turi būti suprojektuota taip, kad atitiktų šiuo metu įstaigų daugiausiai naudojamos programinės įrangos gamintojų taikomas licencijavimo taisykles;
- Infrastruktūra turi būti suprojektuota taip, kad valdymas būtų kaip įmanoma labiau centralizuotas;
- Infrastruktūra turi būti suprojektuota taip, kad jos valdymas būtų kaip įmanoma paprastesnis;
- Infrastruktūra turi būti suprojektuota taip, kad veiktų kaip įmanoma stabiliau;
- Infrastruktūros našumas, talpa, patikimumas ir kiti parametrai turi būti projektuojami pagal analizės etape darbo grupės pateiktus duomenis;
- Techninės įrangos skaičiuoklėje (pirkimo dokumentų Priedas Nr. 3) pateikta informacija I etapo projektavimui gali būti tikslinama;
- Infrastruktūra turi būti suprojektuota taip, kad pirmajame projekto įgyvendinimo etape į ją būtų galima sumigruoti analizės etape įvardintų įstaigų naudojamas IS bei diegti naujai kuriamas IS. IS planuojama migruoti virtualių serverių, duomenų bazių ir pan. lygyje, t. y. šiuo metu įstaigų naudojama fizinė įranga nebus vežama į centralizuotus duomenų centrus infrastruktūros konsolidavimo tikslais. Fizinės įrangos vežimas galimas tik labai išskirtiniais atvejais;
- Infrastruktūra turi būti suprojektuota taip, kad kiekviena įstaiga galėtų valdyti tik jai priskirtus resursus, t. y. nebūtų galimybės peržiūrėti ar valdyti kitoms įstaigoms priskirtų resursų;
- Infrastruktūra turi būti suprojektuota taip, kad II-III projekto įgyvendinimo etapuose būtų galima nesudėtingai įdiegti automatizavimo įrankius;

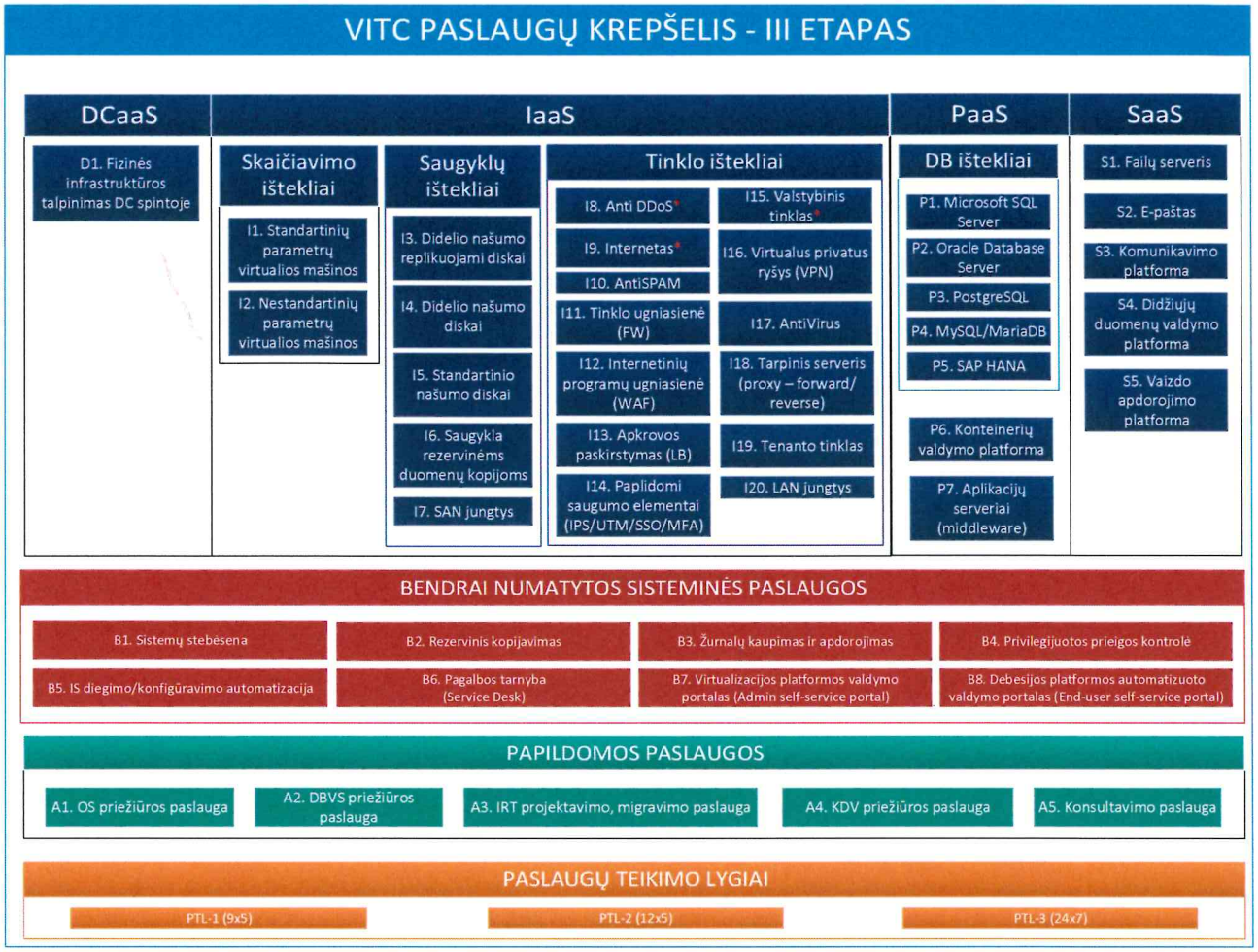
- Infrastruktūra turi būti suprojektuota taip, kad visiems komponentams įrangos pasiūlymus galėtų pateikti bent trys skirtingi įrangos gamintojai;
- Infrastruktūra turi būti suprojektuota taip, kad užtikrintų kaip įmanoma didesnį saugumo lygį;
- Infrastruktūra turi būti suprojektuota taip, kad leistų skirtingoms įstaigoms naudoti tas pačias vidinių IP adresų aibes;
- Infrastruktūra turi būti suprojektuota taip, kad leistų esant poreikiui migruojamiems serveriams išlaikyti IP adresus;
- Infrastruktūra turi būti suprojektuota taip, kad serverius migruojant tarp duomenų centrų būtų galima išlaikyti IP adresus, ugniasienių taisykles ir kitus nustatymus nepriklausomai nuo to, kuriame duomenų centre konkrečiu laiko momentu yra serveris;
- Infrastruktūra turi būti suprojektuota taip, kad esant poreikiui įstaigoms komunikuoti tarpusavyje tinklo lygyje, komunikacija vyktų per ugniasienes pagal iš anksto suderintas taisykles;
- Infrastruktūra turi būti suprojektuota taip, kad leistų įstaigai segmentuoti savo valdomą tinklą į norimą segmentų kiekį ir kontroliuoti duomenų srautus tarp segmentų;
- Infrastruktūra turi būti suprojektuota taip, kad atitiktų KAM keliamus reikalavimus;
- Infrastruktūra turi būti suprojektuota taip, kad būtų galimybė kaip įmanoma didesnį informacinės sistemos pasiekiamumą užtikrinti platformos lygyje;
- Infrastruktūra turi būti suprojektuota taip, kad užtikrintų analizės etape įvardinto duomenų kiekio nepertraukiamą pasiekiamumą fizinės saugyklos gedimo atveju. Fizinės saugyklos gedimo atveju įtakos duomenų pasiekiamumui neturi būti, t. y. trūkis 0 s. Procesai turi būti pilnai automatizuoti;
- Kritinėms sistemos (pvz. I-II lygio IS ir registrai) projektuojama infrastruktūra vieno regiono lygyje (Vilniaus arba Kauno) turi užtikrinti RPO – 0 s., RTO – iki 10 min;
- Turi būti galimybė užtikrinti kritinių sistemų (pvz. I-II lygio IS ir registrai) veikimo atstatymą tarp regionų (Vilniaus – Kauno) užtikrinant RPO – 15 min., RTO – iki 1 val. Sprendimas gali būti užtikrinamas duomenų bazių asinchroninio replikavimo priemonėmis (pvz. Oracle DG/ADG, Microsoft SQL AlwaysOn ir t.t.);
- Infrastruktūros projektavimas turi apimti ir stebėsenos sistemą, skirtą infrastruktūros komponentų veikimo stebėsenai;
- I projekto įgyvendinimo etape rezervinio duomenų kopijavimo ir atstatymo sprendimas turi būti suprojektuotas taip, kad rezervinio duomenų kopijavimo ir atstatymo sprendimo priežiūrą vykdytų projektuojamos infrastruktūros administratoriai. Naudotojai pagal suderintus procesus galės užsakyti norimą duomenų kopijavimo planą ir esant poreikiui užsisakyti duomenų atstatymą iš rezervinių kopijų.
- Paslaugos pasiekiamumo laikai skaičiuojami vieno duomenų centro praradimo atveju t. y. laikas (išreikštas procentais), per kurį paslaugos pasiekiamumas būtų atstatomas, praradus vieną iš duomenų centrų.
- NKSC nustatė saugumo reikalavimus, apibrėžė prieigas į VDPT.

4 Debesijos paslaugų krepšelis ir paslaugų atributai

Įvertinus analizės etape surinktus duomenis, bei IVPK įvardintus reikalavimus, suformuotas VDPT/VITC paslaugų krepšelis I - III projekto įgyvendinimo etapams. Paslaugų krepšelis pateiktas schemose žemiau.

pav. 4-1 I etapo VITC paslaugų krepšelis

pav. 4-2 II etapo VITC paslaugų krepšelis



pav. 4-3 III etapo VITC paslaugų krepšelis

Ruošiant paslaugų krepšelį orientuojamasi į detalų pradiniame projekto etape planuojamų realizuoti paslaugų aprašymą. Tolimesniuose etapuose planuojamos diegti paslaugos bus suprojektuotos kituose sutarties įgyvendinimo etapuose, atsižvelgiant į realius IVPK poreikius.

Naudojant šiame dokumente aprašomas paslaugas galima suprojektuoti ir įdiegti informacines sistemas, kurios atitiks šiuos reikalavimus:

- I – II lygio IS ir registrai, kurie veikia Active - Active režimu Vilniaus arba Kauno regiono duomenų centruose; RPO – 0 s., RTO – 10 min.;
- I – II lygio IS ir registrai, kurie veikia Active – Passive režimu (Disaster Recovery sprendimas) tarp Vilniaus – Kauno arba Kauno – Vilniaus duomenų centrų; RPO – 15 min., RTO – 1 val. Taikoma IS, kurios turi būti asinchroniškai replikuojamos ir operatyviai atstatomos sutrikus pagrindiniams DC;
- I – IV lygio IS ir registrų standartinis rezervinis kopijavimas; RPO – 15 min., RTO – 8 val. Taikoma esant poreikiui atstatyti duomenis iš rezervinės kopijos;
- I lygio IS ir duomenų atstatymui iš NATO DC; RPO – 7 d., RTO – 60 d.;
- Aplikacijų serveriams; RPO – 24 val., RTO – 8 val.

Paslaugų krepšelio elementams aprašyti bus naudojama Paslaugos kortelės aprašo forma (pateikta žemiau). Tokia aprašo forma leidžia lengviau paruošti paslaugas valdymui ir automatizacijai.

Paslaugos kortelės aprašas

Laukas	Reikšmė
Kodas	Paslaugos kodas sutartu formatu.
Pavadinimas	Paslaugos pavadinimas.
Kategorija	Paslaugų kategorija, kuriai aprašoma paslauga priskiriama.
Aprašas	Pateikiamas paslaugos aprašas, kuris paaiškina kokia tai paslauga, kur ji gali būti naudojama, kokie dažniausi panaudojimo atvejai ir pan.
Technologinis aprašas	Pateikiami technologiniai paslaugos teikimo parametrai, galimos konfigūracijos bei kiti reikšmingi aspektai.
Tiesioginis teikimas	Ar šią paslaugą galima naudoti kaip galutinį produktą? Galimos reikšmės – Taip / Ne.
Naudojimas kitų paslaugų teikimui	Ar ši paslauga gali būti kitų paslaugų sudėtine dalimi? Galimos reikšmės – Taip / Ne.
Privalomų paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	Išvardinti paslaugų, kurios privalomos šiai paslaugai teikti, kodus, o jeigu tokių nėra – nurodyti „Nėra“.
Pasirinktinių paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	Išvardinti paslaugų, kurios gali būti pasirinktos teikiant šią paslaugą, kodus, o jeigu tokių nėra – nurodyti „Nėra“.

4.1 Paslaugų teikimo lygiai

Šiame dokumento skyriuje aprašomi sistemų komponentų paslaugų teikimo lygiai, taikomi sistemų komponentų priežiūros paslaugoms.

PTL-1 (angl. SLA1) – aptarnavimas darbo valandomis pirmadieniais – penktadieniais nuo 8.00 val. iki 17.00 val., išskyrus švenčių dienas.

PTL-2 (angl. SLA2) – aptarnavimas prailgintomis valandomis pirmadieniais – penktadieniais nuo 8.00 val. iki 24.00 val., išskyrus švenčių dienas.

PTL-3 (angl. SLA3) – aptarnavimas visą parą pirmadieniais – sekmadieniais nuo 0.00 val. iki 24.00 val. bei švenčių dienomis.

Paslaugos pateikiamumas	PTL-1	PTL-2	PTL-3
Aptarnavimo laikas	9x5	16x5	24x7
Reakcijos į incidentą laikas	iki 1 val.	iki 1 val.	iki 1 val.
Incidento sprendimo laikas (žemas)	iki 8 val.	iki 8 val.*	iki 8 val.*
Incidento sprendimo laikas (vidutinis)	iki 6 val.	iki 6 val.	iki 6 val.
Incidento sprendimo laikas (aukštas)	iki 4 val.	iki 4 val.	iki 4 val.
Reakcijos į užklausą laikas	iki 8 val.	iki 4 val.*	iki 4 val.*
Užklausos išsprendimo laikas	Priklauso nuo sudėtingumo		

*Žemo prioriteto incidentai ir užklausos aptarnaujami pirmadieniais – penktadieniais nuo 8.00 val. iki 17.00 val., išskyrus švenčių dienas.			
	Aptarnavimo prioritetas pagal poreikį		
	Nėra tiesioginio poveikio veiklai	Apribotos vartotojų galimybės, rizika patirti finansinius praradimus	Vartotojai negali dirbti, tiesioginė įtaka veiklai
Paveiktas vienas vartotojas	Žemas	Žemas	Vidutinis
Paveikta dalis vartotojų (iki 10)	Žemas	Vidutinis	Aukštas
Paveikti visi vartotojai	Vidutinis	Aukštas	Aukštas

Atsižvelgiant į realius organizacijų poreikius, užsakovas šiame skyriuje įvardintus parametrus gali koreguoti pagal poreikį.

4.2 DCaaS

4.2.1 Fizinės infrastruktūros talpinimas DC spintoje

Kodas	D1
Pavadinimas	Fizinės infrastruktūros talpinimas DC spintoje
Kategorija	DCaaS
Aprašas	Paslauga apima fizinės infrastruktūros elementų talpinimą duomenų centrų infrastruktūroje (spintoje). Norint naudotis šia paslauga talpinama įranga turi atitikti duomenų centrų valdytojo keliamus reikalavimus.
Technologinis aprašas	Šio projekto apimtyje paslauga detaliau neprojektuojama. Duomenų centrų valdytojo keliami reikalavimai turi apimti: • Reikalavimus aušinimui; • Reikalavimus elektros jungtims; • Reikalavimus įrangos tvirtinimui ir kt.
Tiesioginis teikimas	Taip
Naudojimas kitų paslaugų teikimui	Nėra
Paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	Nėra
Pasirinktinių paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	Nėra

4.3 IaaS

4.3.1 Skaičiavimo ištekliai

Šiame skyriuje yra aprašomos IAAS tipo skaičiavimų išteklių paslaugos.

4.3.1.1 Standartinių parametrų virtualios mašinos

Kodas	I1
Pavadinimas	Standartinių parametrų virtualios mašinos
Kategorija	IaaS skaičiavimo ištekliai
Aprašas	Šia paslauga suteikiama iš anksto numatytų, standartinių parametrų virtuali mašina. Užsakant šią paslaugą bus sudaryta galimybė užsakyti Windows arba

<table>
<tr><td></td><td>Linux operacinės sistemos licencijas. OS versijų pasirinkimo sąrašas bus pateiktas užsakymo metu. Užsakymo metu bus galimybė pasirinkti resursų naudojimo modelį – dinaminio, pilnai rezervuoto, dalinai išskirto.
I etape paslaugos suteikime dalyvauja VDPT administratoriai.

Virtualių mašinų parametrai bus suderinti infrastruktūros diegimo etape.</td></tr>
<tr><td>Technologinis aprašas</td><td>Užsisakius šią paslaugą klientui suteikiamas prisijungimas prie Debesijos platformos valdymo portalo (I projekto etape šios paslaugos užsakymas bus vykdomas neautomatizuotomis priemonemis. Automatizuotai paslauga bus tiekiama II-III projekto etapuose). Debesijos platformos valdymo portalo funkcionalumas aprašomas šios paslaugos apraše. Užsakant paslaugą būtina nurodyti konkrečius standartinių parametrų virtualių mašinų kodus per platformos resursų telkinius.

Pradiniame etape projektuojami žemiau įvardinti resursų telkiniai / konsolidavimo platformos:
• Oracle PĮ pagrindu veikiančių uždavinių – skirta virtualiems serveriams, kurie naudojami Oracle Database EE/SE duomenų bazių valdymo sistemoms, Oracle WebLogic Suite, bei Oracle SOA Suite for Oracle Middleware programinei įrangai;
• MS SQL PĮ pagrindu veikiančių uždavinių konsolidavimo platforma – skirta virtualiems serveriams, kurie naudojami MS SQL Server Enterprise Edition duomenų bazių valdymo sistemoms;
• Konteinerių technologijų pagrindu veikiančių uždavinių – skirta programinei įrangai, veikiančiai konteinerių pagrindu;
• Bendrų uždavinių – resursų telkinys, skirtas virtualiems serveriams, kurie nenaudoja anksčiau minėtos programinės įrangos.

Standartizuoti parametrai yra vCPU ir RAM kiekio kombinacija. Galimos vCPU ir RAM kiekio kombinacijos Oracle PĮ išteklių telkinyje:
<table>
<tr><th>Kodas</th><th>vCPU (vnt.)</th><th>RAM (GB)</th></tr>
<tr><td>ORA1.VM1</td><td>4</td><td>16</td></tr>
<tr><td>ORA1.VM2</td><td>4</td><td>32</td></tr>
<tr><td>ORA1.VM3</td><td>8</td><td>32</td></tr>
<tr><td>ORA1.VM4</td><td>8</td><td>64</td></tr>
<tr><td>ORA1.VM5</td><td>16</td><td>128</td></tr>
<tr><td>ORA1.VM6</td><td>16</td><td>256</td></tr>
</table>
Galimos vCPU ir RAM kiekio kombinacijos Microsoft SQL PĮ išteklių telkinyje:
<table>
<tr><th>Kodas</th><th>vCPU (vnt.)</th><th>RAM (GB)</th></tr>
<tr><td>SQL1.VM1</td><td>2</td><td>8</td></tr>
<tr><td>SQL1.VM2</td><td>4</td><td>16</td></tr>
<tr><td>SQL1.VM3</td><td>4</td><td>32</td></tr>
<tr><td>SQL1.VM4</td><td>8</td><td>32</td></tr>
<tr><td>SQL1.VM5</td><td>8</td><td>64</td></tr>
<tr><td>SQL1.VM6</td><td>16</td><td>128</td></tr>
<tr><td>SQL1.VM7</td><td>16</td><td>256</td></tr>
</table>
Galimos vCPU ir RAM kiekio kombinacijos bendrų uždavinių išteklių telkinyje:
<table>
<tr><th>Kodas</th><th>vCPU (vnt.)</th><th>RAM (GB)</th></tr>
<tr><td>BA1.VM1</td><td>1</td><td>2</td></tr>
<tr><td>BA1.VM2</td><td>2</td><td>4</td></tr>
<tr><td>BA1.VM3</td><td>2</td><td>8</td></tr>
<tr><td>BA1.VM4</td><td>4</td><td>8</td></tr>
</table>
</td></tr>
</table>

	<table><tr><td>BA1.VM5</td><td>4</td><td>16</td></tr><tr><td>BA1.VM6</td><td>4</td><td>32</td></tr><tr><td>BA1.VM7</td><td>8</td><td>32</td></tr><tr><td>BA1.VM8</td><td>8</td><td>64</td></tr><tr><td>BA1.VM9</td><td>8</td><td>128</td></tr><tr><td>BA1.VM10</td><td>16</td><td>128</td></tr><tr><td>BA1.VM11</td><td>16</td><td>192</td></tr><tr><td>BA1.VM12</td><td>16</td><td>256</td></tr></table> Šakninio disko dydis yra konfigūruojamas parametras, tačiau turintis numatytąją reikšmę, kurios dydis yra 50 GB. Papildomai prijungiamų virtualių diskų dydis yra neribojamas. Paslaugos pasiekiamumas – 99,99%. RPO – netaikoma – paslauga neapima atminties (RAM) turinio ir procesorių (vCPU) komandų / registrų duomenų replikavimo ir rezervinio kopijavimo. RTO (skaičiavimo išteklių numatytajai talpai atstatyti) – 3 min. Virtualių serverių diskų RPO/RTO nusako atitinkamų Saugyklų išteklių (I3-I6) paslaugų lygiai. Detaliau resursų telkinių / konsolidavimo platformų techninė realizacija aprašyta infrastruktūros architektūroje.
Tiesioginis teikimas	Taip
Naudojimas kitų paslaugų teikimui	Taip
Paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	Debesijos platformos valdymo portalas, saugyklų ištekliai (I3-I6)), tinklo ištekliai (I19)
Pasirinktinių paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	Nėra

4.3.1.2 Nestandartinių parametrų virtualios mašinos

Kodas	I2
Pavadinimas	Nestandartinių parametrų virtualios mašinos
Kategorija	IaaS skaičiavimo ištekliai
Aprašas	Šia paslauga suteikiama nestandartinių parametrų virtuali mašina. Paslauga skirta talpinti šiuo metu naudojamiems ir į VDPT perkeliamiems skaičiavimo ištekliams arba specifiniams bei technologiškai pagrįstiems nestandartiniams poreikiams, kurie negali būti realizuojami naudojantis paslauga I1. Užsakant šią paslaugą bus sudaryta galimybė užsakyti Windows arba Linux operacinės sistemos licencijas. OS versijų pasirinkimo sąrašas bus pateiktas užsakymo metu. I etape paslaugos suteikime dalyvauja VDPT administratoriai.
Technologinis aprašas	Užsisakius šią paslaugą klientui suteikiamas prisijungimas prie Debesijos platformos valdymo portalo (I projekto etape šios paslaugos užsakymas bus vykdomas neautomatizuotomis priemonemis. Automatizuotai paslauga bus tiekiama II-III projekto etapuose). Debesijos platformos valdymo portalo funkcionalumas aprašomas šios paslaugos apraše. Užsakant paslaugą būtina nurodyti konkretų pageidaujamų resursų (vCPU, RAM) kiekį per platformos resursų telkinius. Pradiniame etape projektuojami žemiau įvardinti resursų telkiniai / konsolidavimo platformos: • Oracle PĮ pagrindu veikiančių uždavinių – skirta virtualiems serveriams, kurie naudojami Oracle Database EE/SE duomenų bazių

	valdymo sistemoms, Oracle WebLogic Suite, bei Oracle SOA Suite for Oracle Middleware programinei įrangai; • MS SQL PĮ pagrindu veikiančių uždavinių konsolidavimo platforma – skirta virtualiems serveriams, kurie naudojami MS SQL Server Enterprise Edition duomenų bazių valdymo sistemoms; • Konteinerių technologijų pagrindu veikiančių uždavinių – skirta programinei įrangai, veikiančiai konteinerių pagrindu; • Bendrų uždavinių – resursų telkinys, skirtas virtualiems serveriams, kurie nenaudoja anksčiau minėtos programinės įrangos. Paslaugos suteikimo ribojimai: • vCPU kiekis gali būti tik sveikasis skaičius, kuris yra dalus iš 2 be liekanos, išskyrus vienintelį atvejį, kai vCPU kiekis lygus vienetui; • RAM kiekis nurodomas gigabaitais kaip sveikasis skaičius, kuris yra dalus iš 2 be liekanos, išskyrus vienintelį atvejį, kai RAM kiekis gigabaitais lygus vienetui. Paslaugos pasiekiamumas – 99,99%. RPO – netaikoma. Paslauga neapima atminties (RAM) turinio ir procesorių (vCPU) komandų / registrų duomenų replikavimo ir rezervinio kopijavimo. RTO (skaičiavimo išteklių numatytajai talpai atstatyti) – 3 min. Virtualių mašinų diskų RPO/RTO nusako atitinkamų Saugyklų išteklių (I3-I6) paslaugų lygiai. Detaliau resursų telkinių / konsolidavimo platformų techninė realizacija aprašyta infrastruktūros architektūroje.
Tiesioginis teikimas	Taip
Naudojimas kitų paslaugų teikimui	Taip
Paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	Debesijos platformos valdymo portalas, saugyklų ištekliai (I3-I6), tinklo ištekliai (I19)
Pasirinktinių paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	Nėra

4.3.2 Saugyklų ištekliai

Šiame skyriuje yra aprašomos IAAS tipo saugyklų išteklių paslaugos.

4.3.2.1 Didelio našumo replikuojami diskai

Kodas	I3
Pavadinimas	Didelio našumo replikuojami diskai
Kategorija	IaaS saugyklų ištekliai
Aprašas	Šia paslauga suteikiami pasirinkto dydžio didelio našumo replikuojami loginiai diskai. Šie diskai ypač tinkami didelio kritiškumo ir didelių apkrovų duomenų bazėms, o taip pat taikomajai programinei įrangai, kuri reikalauja labai intensyvių skaitymo ir rašymo operacijų bei minimalaus vėlinimo. Užsakant paslaugą būtina nurodyti konkretų pageidaujamų resursų kiekį duomenų saugyklose (kiekis vnt., GB/TB). I projekto etape SAN tipo duomenų saugyklos replikuojamos regiono ribose. Paslaugos pasiekiamumas – 99,99%. RPO – 0 min.

	RTO – 0 min. Pastaba: Užsakant šią paslaugą privalomai suteikiama Rezervinio duomenų kopijavimo paslauga.
Technologinis aprašas	Duomenų saugojimo sluoksnio techninė realizacija aprašyta infrastruktūros architektūroje.
Tiesioginis teikimas	Taip
Naudojimas kitų paslaugų teikimui	Taip
Paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	B2
Pasirinktinių paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	Nėra

4.3.2.2 Didelio našumo diskai

Kodas	I4
Pavadinimas	Didelio našumo diskai
Kategorija	IaaS saugyklų ištekliai
Aprašas	Šia paslauga suteikiama pasirinkto dydžio didelio našumo nereplikuojami loginiai diskai nurodytame duomenų centre. Šie diskai ypač tinkami didelių apkrovų duomenų bazėms bei taikomajai programinei įrangai, kuri reikalauja labai intensyvių skaitymo ir rašymo operacijų bei minimalaus vėlinimo. Užsakant paslaugą būtina nurodyti konkretų pageidaujamų resursų kiekį duomenų saugyklose (kiekis vnt., GB/TB). Pradiniame etape naudojamos lokalios (vieno DC ribose) SAN tipo duomenų saugyklos. Paslaugos pasiekiamumas – 99,5%. RPO/RTO – pagal Rezervinio kopijavimo paslaugos apimtyje suderintus parametrus. Pastabos: Užsakant šią paslaugą privalomai suteikiama Rezervinio duomenų kopijavimo paslauga. Informacinių sistemų, duomenų bazių, taikomosios programinės įrangos pasiekiamumas turi būti užtikrinamas ne infrastruktūros priemonėmis.
Technologinis aprašas	Duomenų saugojimo sluoksnio techninė realizacija aprašyta infrastruktūros architektūroje.
Tiesioginis teikimas	Taip
Naudojimas kitų paslaugų teikimui	Taip
Paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	B2
Pasirinktinių paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	Nėra

4.3.2.3 Standartinio našumo diskai

Kodas	I5
Pavadinimas	Standartinio našumo diskai

Kategorija	IaaS saugyklų ištekliai
Aprašas	Šia paslauga suteikiama pasirinkto dydžio standartinio našumo nereplikuojami loginiai diskai nurodytame duomenų centre. Šie diskai skirti ne produkcinių aplinkų duomenų bazėms bei taikomajai programinei įrangai, kuri nereikalauja minimalaus vėlinimo. Užsakant paslaugą būtina nurodyti konkretų pageidaujamų resursų kiekį duomenų saugyklose (kiekis vnt., GB/TB). Pradiniame etape naudojamos lokalios (vieno DC ribose) SAN tipo duomenų saugyklos. Paslaugos pasiekiamumas – 99,5%. RPO/RTO – pagal Rezervinio kopijavimo paslaugos apimtyje suderintus parametrus. Pastabos: Užsakant šią paslaugą privalomai suteikiama Rezervinio duomenų kopijavimo paslauga. Informacinių sistemų, duomenų bazių, taikomosios programinės įrangos pasiekiamumas turi būti užtikrinamas ne infrastruktūros priemonėmis.
Technologinis aprašas	Duomenų saugojimo sluoksnio techninė realizacija aprašyta infrastruktūros architektūroje.
Tiesioginis teikimas	Taip
Naudojimas kitų paslaugų teikimui	Taip
Paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	B2
Pasirinktinių paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	Nėra

4.3.2.4 Saugykla rezervinėms duomenų kopijoms

Kodas	I6
Pavadinimas	Saugykla rezervinėms duomenų kopijoms
Kategorija	IaaS saugyklų ištekliai
Aprašas	Šia paslauga suteikiama pasirinkto dydžio saugykla rezervinėms duomenų kopijoms saugoti. Paslauga skirta įstaigoms / organizacijoms, kurių tarnybinės stotys yra ne VDPT infrastruktūroje. Užsakant paslaugą būtina nurodyti konkretų pageidaujamų resursų kiekį saugykloje (GB/TB), kuris bus prijungtas prie atskirai užsakomos standartinių parametrų virtualios mašinos. Saugyklos erdvė bus pasiekiama su užsakovu suderintais protokolais (pvz. NFS, CIFS). Pradiniame etape naudojama lokali SAN tipo duomenų saugykla viename DC. Paslaugos pasiekiamumas – 98%. RPO– netaikoma. Papildomos rezervinės duomenų kopijos nebus kuriamos. Sugedus saugyklai duomenys gali būti prarasti. RTO – 24 val. Taikoma paslaugos veikimo atstatymui.
Technologinis aprašas	Duomenų saugojimo sluoksnio techninė realizacija aprašyta infrastruktūros architektūroje.
Tiesioginis teikimas	Ne
Naudojimas kitų paslaugų teikimui	Ne
Paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	I1, I8-I19

Pasirinktinių paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	Nėra

4.3.2.5 SAN jungtys

Kodas	I7
Pavadinimas	SAN jungtys
Kategorija	IaaS saugyklų ištekliai
Aprašas	Šia paslauga suteikiamos dvi 8G/16G/32G FC SAN jungtys, kurių kiekviena yra fiziškai atskiruose komutatoriuose. Naudojantis FC SAN jungčių paslauga įstaiga / organizacija galės užsakyti saugyklos išteklių paslaugas I3-I6.
Technologinis aprašas	Dviejuose bendro naudojimo fiziškai atskiruose SAN FC komutatoriuose yra išskiriama po vieną 8G/16G/32G FC jungtį, prie kurių OM3 LC MM kabeliu yra prijungiamas infrastruktūros elementas, atskirtas į izoliuotą loginę SAN FC zoną.
Tiesioginis teikimas	Taip
Naudojimas kitų paslaugų teikimui	Taip
Paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	Nėra
Pasirinktinių paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	Nėra

4.3.3 Tinklo ištekliai

Šiame skyriuje aprašomos VDPT planuojamos teikti tinklo ir saugumo paslaugos (tinklo ištekliai).

4.3.3.1 AntiDDoS

Kodas	I8
Pavadinimas	AntiDDoS paslauga
Kategorija	IaaS tinklo ištekliai
Aprašas	Šio projekto apimtyje AntiDDoS paslauga neprojektuojama. AntiDDoS paslaugą projektuojamos infrastruktūros naudotojai galės užsisakyti, tačiau ji bus technologiškai teikiama ryšio paslaugų teikėjo. Šios paslaugos funkcionalumas ir kiti atributai bus pateikti ryšio paslaugų teikėjo teikiamos paslaugos aprašyme.
Technologinis aprašas	Technologinis šios paslaugos aprašymas pateikiamas ryšio paslaugų teikėjo dokumentacijoje.
Tiesioginis teikimas	Taip
Naudojimas kitų paslaugų teikimui	Taip
Privalomų paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	Internetas (I9)
Pasirinktinių paslaugų, kuriomis naudojamasi	Nėra

teikiant šią paslaugą, kodai	

4.3.3.2 Internetas

Kodas	I9
Pavadinimas	Interneto ryšys
Kategorija	IaaS tinklo ištekliai
Aprašas	Šio projekto apimtyje interneto paslauga neprojektuojama. Interneto paslaugą projektuojamos infrastruktūros naudotojai galės užsisakyti, tačiau ji bus technologiškai teikiama ryšio paslaugų teikėjo. Šios paslaugos funkcionalumas ir kiti atributai bus pateikti ryšio paslaugų teikėjo teikiamos paslaugos aprašyme.
Technologinis aprašas	Technologinis šios paslaugos aprašymas pateikiamas ryšio paslaugų teikėjo dokumentacijoje.
Tiesioginis teikimas	Taip
Naudojimas kitų paslaugų teikimui	Taip
Privalomų paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	AntiDDoS (I8)
Pasirinktinių paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	Nėra

4.3.3.3 AntiSpam

Kodas	I10
Pavadinimas	Srauto apsauga nuo nepageidaujamo turinio (angl. AntiSpam)
Kategorija	IaaS tinklo ištekliai
Aprašas	Ši paslauga skirta VDPT infrastruktūroje esančių el. pašto serverių apsaugai nuo nepageidaujamų laiškų. Paslaugą rekomenduojama užsisakyti toms įstaigoms, kurios VDPT infrastruktūroje planuoja talpinti el. pašto serverius. Aptikus, kad laiškas galimai yra brukalas, turi būti galimybė atlikti šias funkcijas: • Laišką persiųsti toliau; • Laišką atmesti; • Laišką pažymėti „spam" žyme; • Koreguoti laiško antraštę, pridedant „spam" žymę. Antispam taisykles rekomenduojama automatiškai atnaujinti iš gamintojo duomenų bazės. Paslaugos pasiekiamumas – 99,99%.

Technologinis aprašas	Paslauga skirta gaunamo ir siunčiamo elektroninio pašto srauto apsaugojimui nuo nepageidaujamų el. laiškų (angl. Spam). Užsisakius šią paslaugą galima naudotis žemiau įvardintais funkcionalumais:
	• Prie gaunamo arba siunčiamo nepageidaujamo laiško antraštės galima pridėti žymą arba laiškus nukreipti į karantiną;
	• Nepageidaujamų laiškų atpažinimui bus naudojamos šios technologijos:
	  ○ juodasis IP sąrašas (IPBlackList),
	  ○ laiške ieškomos nuorodos į tam tikrus internetinius puslapius (SURL),

	○ suminis bitų kiekis (Checksum), ○ siuntėjų tikrinimas žinomose duomenų bazėse; • Return e-mail DNS check – el. laiškai, kuriuose randamos neaiškios ar potencialiai pavojingos tinklalapių nuorodos, taip pat gali būti žymimi kaip nepageidaujami (angl. AntiPhishing); • Laiškų filtravimui naudojami metodai: ○ IP adresų nepatikimų / patikimų siuntėjų sąrašai, ○ filtravimas pagal elektroninio pašto adresus – siuntėjas / gavėjas, ○ filtravimas pagal nurodytus žodžius ir frazes, ○ elektroninio pašto tikrinimas pasaulinėje gamintojo duomenų bazėje.
Tiesioginis teikimas	Taip
Naudojimas kitų paslaugų teikimui	Ne
Privalomų paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	I9, I11
Pasirinktinių paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	I15

4.3.3.4 Tinklo ugniasienė(FW)

Kodas	I11
Pavadinimas	Tinklo ugniasienė (FW)
Kategorija	IaaS tinklo ištekliai
Aprašas	Tai saugumo paslauga, kuri apsaugo nuo bazinių įsilaužimų į sistemas iš interneto arba vidinio tinklo. Paslaugos pasiekiamumas – 99,99%.
Technologinis aprašas	Tinklo ugniasienės paslauga yra skirta apsaugoti duomenų centro naudotojus nuo išorinių bei vidinių grėsmių. Paslauga realizuojama dedikuotų organizacijai arba DC bendro naudojimo, specializuotų ugniasienių funkcijoms užtikrinti skirtais įrenginiais. Ugniasienių funkcijoms užtikrinti naudojami įrenginiai atlieka šias funkcijas: • maršrutizuoja ir apsaugo srautą tarp skirtingų tinklo zonų ir uždarų organizacijos tarnybinių stočių zonų; • maršrutizuoja ir apsaugo srautą tarp išorinių resursų (SVDPT, Internetas, VPN) ir išorinės zonos organizacijos tarnybinių stočių; • atlieka išorinių IP adresų NAT transliacijas; • atlieka mikrosegmentaciją – leidžia arba draudžia komunikaciją tarp bet kurių dviejų virtualių mašinų, tarp virtualios mašinos ir fizinės mašinos vidinėje arba išorinėje saugumo zonose; • apsaugo duomenų srautą tarp bet kurių dviejų virtualių mašinų arba tarp virtualios mašinos ir fizinės mašinos vidinėje arba išorinėje saugumo zonose; • Atlieka srauto valdymą (angl. *traffic shapping*).
Tiesioginis teikimas	Taip
Naudojimas kitų paslaugų teikimui	Taip
Privalomų paslaugų, kuriomis naudojamasi	I9, I15

teikiant šią paslaugą, kodai	
Pasirinktinių paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	I19

4.3.3.5 *Internetinių programų ugniasienė (WAF)*

Kodas	I12
Pavadinimas	Internetinių programų ugniasienė
Kategorija	IaaS tinklo ištekliai
Aprašas	Internetinių / taikomųjų programų lygmens ugniasienių sistema (angl. Web application firewall – WAF) skirta apsaugoti internetu teikiamoms e-paslaugoms. WAF įgyvendina apsaugą nuo galimų pažeidimų, išnaudojančių WEB paslaugas teikiančių portalų saugumo spragas. Paslaugos pasiekiamumas – 99,99%.
Technologinis aprašas	WAF sistema kontroliuoja užklausų, siunčiamų į e-paslaugų portalus, atitikimą standartams, nustatytiems reikalavimams, stebi bandymus įsilaužti, bandymus siųsti virusus, įkelti kenksmingus programinius kodus. WAF - tarpinė kontroliuojanti sistema tarp vartotojų ir WEB paslaugas teikiančių sistemų. Naudojant WAF vartotojų užklausos yra siunčiamos į WAF, o ne į realius WEB serverius tikrinant užklausas ir persiunčiant į WEB paslaugas teikiančias sistemas. WAF funkcionalumas: • automatinio apsimokymo funkcija (ugniasienė stebėdama komunikaciją tarp vartotojo ir WEB serverio nustato leistinos elgsenos modelį ir pagal tai sukuria saugumo taisykles); • nuolat atnaujinama įsilaužimo bei kitų WEB grėsmių aprašų bazė; • SSL ir TLS duomenų srautų dešifravimas ir siunčiamos informacijos patikra; • integracija su HSM įrenginiais saugiam privačių raktų saugojimui ir panaudojimui duomenų srauto dešifravimui / šifravimui; • galimybę aptikti ir apsaugoti nuo aplikacijų lygmens DoS atakų, taip užtikrinant nenutrūkstamą WEB paslaugų teikimą; • galimybę apsaugoti nuo jautrios informacijos nutekėjimo (asmens duomenys, socialiniai draudimo numeriai, t.t.) iškerpant jautrią informaciją iš duomenų srauto ar ją maskuojant; • galimybę modifikuoti / slėpti WEB serverių grąžinamą informaciją apie vartotojų užklausų klaidas, kuri gali būti panaudota identifikuoti naudojamai WEB serverių programinei įrangai ir tos įrangos žinomiems pažeidžiamumams atskleisti; • ataskaitų formavimas.
Tiesioginis teikimas	Taip
Naudojimas kitų paslaugų teikimui	Ne
Privalomų paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	I9, I19
Pasirinktinių paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	I15

4.3.3.6 Apkrovos paskirstymas(LB/ADC)

Kodas	I13
Pavadinimas	Srauto apkrovos paskirstymo paslauga (angl. LB/ADC)
Kategorija	IaaS tinklo ištekliai
Aprašas	Apkrovos paskirstymo paslauga (angl. *Load balancing – LB, Application Delivery Controller - ADC*) yra skirta duomenų srauto ir aplikacijų užklausų paskirstymui tarp taikomųjų programų tarnybinių stočių. Duomenų srauto ir aplikacijų užklausų paskirstymas tarp aplikacijų tarnybinių stočių leidžia kurti aukšto pasiekiamumo ir didelio našumo aplikacijų sprendimus. Paslaugos pasiekiamumas – 99,99%.
Technologinis aprašas	Ši paslauga gali būti naudojama išorinių naudotojų kreipinių paskirstymui į informacinės sistemos portalui aptarnauti skirtus serverius. Paslauga taip pat gali būti naudojama portalų serverių kreipinių paskirstymui į aplikacijų serverius ir kitiems analogiško principo sprendimams. LB sprendimas gali paskirstyti L4 lygmens (pagal OSI modelį) duomenų srautą. Esant poreikiui užtikrinamas duomenų srauto simetriškumas, naudojant šaltinio adreso transliavimą (anglų k. source network address translation - SNAT). Duomenų srauto simetriškumo užtikrinimas yra svarbus kai apkrovos paskirstymo paslauga yra naudojama aplinkose su tinklo ir taikomųjų programų ugniasienėmis bei panašiomis paslaugomis. Paslauga išmaniai paskirsto duomenų srautą ir aplikacijų užklausas atsižvelgiant į įvairius duomenų srauto (L3/L4 lygmenys) ir aplikacijų užklausų (L7 lygmens) atributus bei užtikrina, kad egzistuojančios aplikacijų sesijos visada būtų nukreipiamos į sesiją, aptarnaujančią tarnybinę stotį (anglų k. session persistence). LB paslauga geba įvairiais išmaniais zondais (angl. *probe*) stebėti tarnybinių stočių pasiekiamumą ir aplikacijų veikimą. LB paslauga geba iššifruoti SSL ir TLS duomenų srautus.
Tiesioginis teikimas	Taip
Naudojimas kitų paslaugų teikimui	Ne
Privalomų paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	I19
Pasirinktinių paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	I9, I15

4.3.3.7 Papildomi saugumo elementai (IPS/UTM/SSO/MFA)

Kodas	I14
Pavadinimas	Papildomi saugumo elementai (IPS/UTM/SSO/MFA)
Kategorija	IaaS tinklo ištekliai
Aprašas	Kompleksinė saugumo paslauga, kurią sudaro apsauga nuo įsilaužimų ir nuo pavojingų interneto nuorodų. Apsauga vykdoma nuo kenkėjiškų programų ar web portalų stebint duomenų srautą nuo IP iki aplikacinio lygmens. Paslauga apima įsibrovimų prevencijos sistemą (angl. Intrusion prevention system) ir įsibrovimų aptikimo sistemą (angl. Intrusion detection system). Šios paslaugos apimtyje bus realizuojami dviejų faktorių autentifikacijos sprendimai. Paslaugos pasiekiamumas – 99,99%.

Technologinis aprašas	Paslauga skirta apsaugoti kritines sistemas ir aplikacijas nuo grėsmių ir atakų, kurios nukreiptos į klientus. Naudojami sprendimai turi leisti persidengti atskirų organizacijų VLAN numeriams ir IP adresams. Sprendimo funkcionalumai: • Maršrutizuoti ir apsaugoti srautą tarp skirtingų zonų; • Atlikti išorinių IP adresų NAT transliacijas; • Atlikti IPS arba IDS funkcijas; • Atlikti antiviruso funkcijas FTP, HTTP ir pašto protokolams; • Atlikti antispam funkcijas pašto protokolams; • Atlikti mikrosegmentaciją – leisti arba drausti komunikaciją tarp bet kurių dviejų virtualių mašinų arba tarp virtualios mašinos ir fizinės mašinos vidinėje arba išorinėje saugumo zonose; • Apsaugoti duomenų srautą tarp bet kurių dviejų virtualių mašinų arba tarp virtualios mašinos ir fizinės mašinos vidinėje arba išorinėje saugumo zonose; • Turi būti galimybė skirtingoms organizacijoms pasiekti viena kitos resursus naudojantis vidiniais duomenų centrų komutavimo, maršrutizavimo, proxy ir saugumo resursais. Pasiekiamumas tarp organizacijų turi būti privalomas per išorines arba vidines ugniasienes, priklausomai nuo to, kurioje saugumo zonoje yra serveriai, tarp kurių vyksta komunikacija; • Užtikrinti dviejų faktorių autentifikavimą, padidinant naudojamų sprendimų saugumą, naudojant prisijungimo vardą ir slaptažodį bei su vartotoju susietą autentifikavimo mechanizmą. MFA sprendime antras autentifikavimo faktorius gali būti realizuojamas mobilaus telefono aplikacijoje, fiziniame raktų generatoriuje arba fiziniame USB rakte.
Tiesioginis teikimas	Taip
Naudojimas kitų paslaugų teikimui	Ne
Privalomų paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	I19
Pasirinktinių paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	I9, I15

4.3.3.8 Valstybinis tinklas

Kodas	I15
Pavadinimas	Saugus valstybinis duomenų perdavimo tinklas (SVDPT)
Kategorija	IaaS tinklo ištekliai
Aprašas	Šio projekto apimtyje Valstybinio tinklo paslauga neprojektuojama. Valstybinio tinklo paslaugą projektuojamos infrastruktūros naudotojai galės užsisakyti, tačiau ji bus technologiškai teikiama ryšio paslaugų teikėjo. Šios paslaugos funkcionalumas ir kiti atributai bus pateikti ryšio paslaugų teikėjo teikiamos paslaugos aprašyme.
Technologinis aprašas	Technologinis šios paslaugos aprašymas pateikiamas ryšio paslaugų teikėjo dokumentacijoje.
Tiesioginis teikimas	Taip

Naudojimas kitų paslaugų teikimui	Ne
Privalomų paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	Nėra
Pasirinktinių paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	Nėra

4.3.3.9 Virtualus privatus ryšys (VPN)

Kodas	I16
Pavadinimas	Virtualus privatus ryšys
Kategorija	IaaS tinklo ištekliai
Aprašas	Paslauga skirta saugiam nuotoliniam vartotojų prijungimui prie įstaigos debesijos resursų ir sistemų. Ši paslauga taip pat gali būti naudojama saugiam sujungimui tarp įstaigos debesijos resursų / sistemų ir išorinių įstaigų / įmonių.
Technologinis aprašas	SSL VPN paslauga įgalina vartotojus nuotoliniu būdu prisijungti prie duomenų centre esančių resursų šifruotu kanalu iš bet kurios interneto vietos. Naudojant SSL VPN, vartotojai gali prisijungti prie VPN įrenginio naudodamiesi standartiniu HTTPS prievadu 443. Site-to-site VPN – saugus nuotolinis ryšys tarp dviejų lokacijų (angl. site-to-site VPN) įgalinantis nutolusios lokacijos vartotojus pasiekti duomenų centro resursus saugiu šifruotu tuneliu. Šis tunelis yra užmezgamas tarp dviejų įrenginių arba jų telkinių. Vartotojai gali naudotis saugiu ryšiu ir pasiekti reikiamus resursus nekurdami atskiros dedikuotos VPN sesijos. Paslaugos pasiekiamumas – 99,99%.
Tiesioginis teikimas	Taip
Naudojimas kitų paslaugų teikimui	Ne
Privalomų paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	I9
Pasirinktinių paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	I15

4.3.3.10 AntiVirus

Kodas	I17
Pavadinimas	Antivirus srauto apsauga (angl. AntiVirus)
Kategorija	IaaS tinklo ištekliai
Aprašas	Tikrinimas ir apsauga nuo kenksmingo turinio duomenų sraute. Ugniasienės antiviruso funkcionalumas leidžia patikrinti vartotojų siunčiamus failus ar jie nėra kenkėjiški. Tokį patikrinimą ugniasienė geba atlikti jei ja keliauja ne šifruotas duomenų srautas protokolu, kuriuo gali būti siunčiami failai (pvz.: pašto protokolai, HTTP, FTP). Paslaugos pasiekiamumas – 99,99%.

Technologinis aprašas	Antiviruso funkcionalumas aptinka įvairaus tipo kenkėjiškas programas: botnet, spyware, malware, ranasomware virusus. Visų šių virusų aprašus rekomenduojame automatiškai atnaujinti iš gamintojo duomenų bazės. Realiuoju laiku skanuojamas įeinantis ir išeinantis interneto srautas nuo virusų, trojan'ų, kirminų, šnipinėjimo ir reklaminių programų. Skanuojama visa siunčiama ir gaunama informacija šiais protokolais: HTTP, FTP, SMTP, POP3, IMAP, NNTP. Rekomenduojama tikrinti visų plėtinių bylas, kurių dydis yra pakankamai mažas – pvz. iki 5 MB. Blokuojamos Grayware, Adware, Ransomware tipo virusų atakos: Dialer, Toolbar, Keylogger, Spyware, RAT, Hijacker, CryptoWall. Virusų atpažinimo įrašai atnaujinami nedelsiant, kai atsiranda papildymai paslaugą palaikančio teikėjo duomenų bazėje.
Tiesioginis teikimas	Taip
Naudojimas kitų paslaugų teikimui	Ne
Privalomų paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	I9, I11
Pasirinktinių paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	I15

4.3.3.11 *Tarpinis serveris (angl. forward proxy, reverse proxy)*

Kodas	I18-F
Pavadinimas	Tarpinis serveris (angl. forward proxy)
Kategorija	IaaS tinklo ištekliai
Aprašas	Tarpinės stoties (angl. proxy server) užduotis yra persiųsti gavėjo tarnybinei stočiai siuntėjo užklausas. Ši paslauga apsaugo vidinius vartotojus nuo grėsmių kreipiantis į interneto resursus tiesiogiai. Paslaugos pasiekiamumas – 99,99%.
Technologinis aprašas	Tarpinės stoties apsauga yra realizuojama perimant siuntėjo užklausas ir jas siunčiant pačios tarpinės stoties vardu. Tokiu būdu ne tik yra paslepiama vartotojo tapatybė, tačiau yra atliekamos papildomos saugumo patikros. Tarpinės stoties funkcionalumas: • Terminuoti HTTP/HTTPS web naršymo protokolą; • Terminuoti bet kokius TCP/UDP protokolus; • Terminuoti vartotojų užklausas tiesiogiai arba jas periminėti tinkle (angl. transparent mode); • Tikrinti siunčiamas bylas; • Riboti greitaveiką; • Dinamiškai atnaujinti web puslapių klasifikavimą; • Dinamiškai atnaujinti antivirusų duomenų bazę; • Riboti web puslapių naršymą naudojant puslapių klasifikavimo grupes; • Autentifikuoti naudotojus; • Matyti SSL šifruotą srautą.
Tiesioginis teikimas	Taip
Naudojimas kitų paslaugų teikimui	Ne
Privalomų paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	I19

Pasirinktinių paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	Nėra

Kodas	I18-R
Pavadinimas	Atvirkštinis tarpinis serveris (anglų k. Reverse proxy)
Kategorija	IaaS tinklo ištekliai
Aprašas	Atvirkštinis tarpinis serveris (anglų k. Reverse proxy) – įrenginys arba paslauga, skirta apsaugoti internetu prieinamoms aplikacijoms ir jų tarnybinėms stotims. Be šios, internetu pasiekiamų aplikacijų ir jų tarnybinių stočių apsaugos, gali kilti grėsmė konfidencialumui (duomenų perėmimas), integralumui (duomenų manipuliacija), pasiekiamumui. Paslaugos pasiekiamumas – 99,99%.
Technologinis aprašas	Atvirkštinis tarpinis serveris turi veikti paprasto persiuntimo režimu (anglų k. forwarding) arba aktyviai dalyvauti priimant įeinančias užklausas iš naudotojų į aplikacijas ir užmezgant sesijas į aplikacijų tarnybines stotis klientų vardu (anglų k. full reverse proxy). Pilno režimo atvirkštinis tarpinis serveris įgalina pažangesnes apsaugos priemones. Priimamos SSL/TLS užklausos gali būti iššifruotos, patikrinamos, papildomai autentifikuojamos / autorizuojamos ir vėl šifruojamos. Užklausų iš aplikacijos kliento ir atsakymų iš tarnybinių stočių matomumas leidžia naudoti išmanius duomenų srauto paskirstymo metodus bei aplikacijų lygmens saugumo priemones. SSL/TLS duomenų srautų iššifravimas ir šifravimas leidžia užtikrinti, kad internetu perduodamų duomenų šifravimui būtų naudojami saugiausi algoritmai, nepriklausomai nuo to, kokius algoritmus palaiko aplikacijų ir WEB/API tarnybinės stotys. Būtina integracija su HSM saugiam privačių raktų saugojimui ir naudojimui, duomenų srauto iššifravimui / šifravimui. Atvirkštinis tarpinis serveris turi būti išplečiamas naudojant programinius kodus leidžiančius su duomenų srautu atlikti tam tikrus veiksmus, kurie nebuvo numatyti gamintojo.
Tiesioginis teikimas	Taip
Naudojimas kitų paslaugų teikimui	Ne
Privalomų paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	I19
Pasirinktinių paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	I15

4.3.3.12 Tenanto tinklas

Kodas	I19
Pavadinimas	Tenanto tinklas
Kategorija	IaaS tinklo ištekliai
Aprašas	Įstaigos / organizacijos – tenanto tinklas VDPT aplinkoje / platformoje Paslaugos pasiekiamumas – 99,99%.
Technologinis aprašas	Tenanto tinklas yra tinklo infrastruktūros VDPT platformoje dalis. Tenanto tinklą sudaro konfigūracinių vienetų, nustatymų ir taisyklių aibė VDPT fizinėje

	ir virtualioje aplinkoje. Tenanto tinklas leidžia įstaigai / organizacijai saugiai ir patikimai pasiekti leistinus resursus.
Tiesioginis teikimas	Taip
Naudojimas kitų paslaugų teikimui	Taip
Privalomų paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	I15
Pasirinktinių paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	I9

4.3.3.13 LAN jungtys

Kodas	I20
Pavadinimas	LAN jungtys
Kategorija	IaaS tinklo ištekliai
Aprašas	Šia paslauga suteikiamos dvi 1G/10G/25G LAN jungtys, kurių kiekviena yra fiziškai atskiruose komutatoriuose. Naudojantis LAN jungčių paslauga, įstaiga / organizacija galės fizinę įrangą sujungti su virtualiais resursais, patalpintais VDPT virtualizacijos platformoje LAN tinklo lygyje. Paslaugos pasiekiamumas – 99,95% (priklausomai nuo konfigūracijos gali kisti).
Technologinis aprašas	1G LAN paslaugai teikti naudojami bendro naudojimo komutatoriai. Fiziniai įrenginiai prie bendro naudojimo komutatorių jungiami RJ45 tipo jungtimis. Kiekvieną įrenginį būtina jungti ne mažiau kaip 2 portais į nepriklausomus fizinius komutatorius, išskyrus atvejus, kai portas naudojamas valdymo interfeiso prijungimui. 10G/25G LAN paslaugai teikti naudojami bendro naudojimo LAN komutatoriai. Fiziniai įrenginiai prie bendro naudojimo komutatorių jungiami LC MM tipo jungtimis. Kiekvieną įrenginį būtina jungti ne mažiau kaip 2 portais į atskirus fizinius komutatorius.
Tiesioginis teikimas	Taip
Naudojimas kitų paslaugų teikimui	Taip
Paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	D1
Pasirinktinių paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	Nėra

4.4 PaaS

Šiame skyriuje yra aprašomos PaaS tipo paslaugos.

4.4.1 Microsoft SQL Server

Kodas	P1
Pavadinimas	Microsoft SQL Server DBVS
Kategorija	PaaS

Aprašas	Šia paslauga suteikiama pasirinktos versijos Microsoft SQL Server duomenų bazių valdymo sistema.
Technologinis aprašas	Paslauga realizuojama virtualių mašinų priemonėmis, jas kuriant ir palaikant tam numatytuose Microsoft SQL PĮ skaičiavimo išteklių telkiniuose. Teikiamos SQL Server versijos: • SQL Server 2012 • SQL Server 2014 • SQL Server 2016 • SQL Server 2017 Pastaba: tikslios SQL Server versijos bus suderintos infrastruktūros diegimo etape.
Tiesioginis teikimas	Taip
Naudojimas kitų paslaugų teikimui	Ne
Paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	I1, I2
Pasirinktinių paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	I3-I5

4.4.2 Oracle Database Server

Kodas	P2
Pavadinimas	Oracle Database Server DBVS
Kategorija	PaaS
Aprašas	Šia paslauga suteikiama pasirinktos versijos Oracle Database Server duomenų bazių valdymo sistema.
Technologinis aprašas	Paslauga realizuojama virtualių mašinų priemonėmis, jas kuriant ir palaikant tam numatytuose Oracle PĮ skaičiavimo išteklių telkiniuose. Teikiamos Oracle Database versijos: • Oracle Database 12c Release 2 • Oracle Database 18c Pastaba: tikslios Oracle DB versijos bus suderintos infrastruktūros diegimo etape.
Tiesioginis teikimas	Taip
Naudojimas kitų paslaugų teikimui	Ne
Paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	I1, I2
Pasirinktinių paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	I3-I5

4.4.3 PostgreSQL

Kodas	P3
Pavadinimas	PostgreSQL
Kategorija	PaaS

Aprašas	Šia paslauga suteikiama pasirinktos versijos PostgreSQL duomenų bazių valdymo sistema.
Technologinis aprašas	Paslauga realizuojama virtualių mašinų priemonėmis, jas kuriant ir palaikant tam numatytuose bendrų uždavinių skaičiavimo išteklių telkiniuose. Pastaba: Tikslios PostgreSQL versijos bus suderintos infrastruktūros diegimo etape.
Tiesioginis teikimas	Taip
Naudojimas kitų paslaugų teikimui	Ne
Paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	I1, I2
Pasirinktinių paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	I3-I5

4.4.4 MySQL/MariaDB

Kodas	P4
Pavadinimas	MySQL/MariaDB
Kategorija	PaaS
Aprašas	Šia paslauga suteikiama pasirinktos versijos MySQL/MariaDB duomenų bazių valdymo sistema.
Technologinis aprašas	Paslauga realizuojama virtualių mašinų priemonėmis, jas kuriant ir palaikant tam numatytuose bendrų uždavinių skaičiavimo išteklių telkiniuose. Pastaba: Tikslios MySQL/MariaDB versijos bus suderintos infrastruktūros diegimo etape.
Tiesioginis teikimas	Taip
Naudojimas kitų paslaugų teikimui	Ne
Paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	I1, I2
Pasirinktinių paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	I3-I5

4.4.5 SAP HANA

Kodas	P5
Pavadinimas	SAP HANA DB
Kategorija	PaaS
Aprašas	Šia paslauga suteikiama pasirinktos versijos SAP HANA duomenų bazių valdymo sistema. Pastaba: Pirmame projekto įgyvendinimo etape paslauga nerealizuojama.
Technologinis aprašas	Paslauga realizuojama virtualių mašinų arba didesnių fizinių tarnybinių stočių priemonėmis. Teikiamos SAP HANA DB versijos, papildomi infrastruktūros konfigūracijos reikalavimai ir diegimo procedūros bus projektuojamos prieš pradedant įgyvendinti tolimesnius projekto etapus, atsižvelgiant į realius poreikius.

Tiesioginis teikimas	Taip
Naudojimas kitų paslaugų teikimui	Ne
Paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	I1, I2
Pasirinktinių paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	I3-I5

4.4.6 Konteinerių valdymo platforma

Kodas	P6
Pavadinimas	Konteinerių valdymo platforma
Kategorija	PaaS
Aprašas	Šia paslauga teikiami Kubernetes ir Docker technologijomis realizuoti programinės įrangos konteineriai. Paslaugos pasiekiamumas – 99,95%.
Technologinis aprašas	Paslauga realizuojama virtualių mašinų priemonėmis, jas kuriant ir palaikant tam numatytuose bendrų uždavinių skaičiavimo išteklių telkiniuose. Docker konteineriai veikia valdomi Kubernetes telkinio. Programinės įrangos konteinerių sprendimas integruotas į bendrą platformą ir naudoja bendrus išteklius, valdymo, autentifikacijos bei autorizacijos priemones. Detaliau techninė realizacija aprašyta infrastruktūros architektūroje.
Tiesioginis teikimas	Taip
Naudojimas kitų paslaugų teikimui	Ne
Paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	I1, I2
Pasirinktinių paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	I3-I5

4.4.7 Aplikacijų serveriai (middleware)

Kodas	P7
Pavadinimas	Aplikacijų serveriai (middleware)
Kategorija	PaaS
Aprašas	Šia paslauga suteikiamas pageidaujamų pajėgumų Oracle WebLogic Server 12c aplikacijų serveris.
Technologinis aprašas	Paslauga realizuojama virtualių mašinų priemonėmis, jas kuriant ir palaikant tam numatytuose Oracle PĮ skaičiavimo išteklių telkiniuose. Teikiamos Oracle WebLogic Server versijos: • Oracle WebLogic Server 12c. Pastaba: Tikslios Oracle WebLogic Server versijos bus suderintos infrastruktūros diegimo etape.
Tiesioginis teikimas	Taip
Naudojimas kitų paslaugų teikimui	Ne

Paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	I1, I2
Pasirinktinių paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	I3-I5

4.5 SaaS

Šiame skyriuje yra aprašomos SaaS tipo paslaugos.

4.5.1 Failų serveris

Kodas	S1
Pavadinimas	Failų serveris
Kategorija	SaaS
Aprašas	Šia paslauga suteikiamas pageidaujamos talpos failų serveris įstaigos / organizacijos vartotojams. Paslaugos pasiekiamumas – 99,75%.
Technologinis aprašas	Paslauga realizuojama virtualių mašinų priemonėmis, jas kuriant ir palaikant tam numatytuose bendrų uždavinių skaičiavimo išteklių telkiniuose. Failų serveris bus integruojamas su įstaigos / organizacijos tapatybės valdymo sistema. Pastaba: Failų serverio parametrai, nustatymai ir integracijos bus suderintos infrastruktūros diegimo etape.
Tiesioginis teikimas	Taip
Naudojimas kitų paslaugų teikimui	Ne
Paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	I1, I2, I8-I19
Pasirinktinių paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	I3-I5

4.5.2 E-paštas

Kodas	S2
Pavadinimas	E-paštas
Kategorija	SaaS
Aprašas	Šia paslauga suteikiama pageidaujamos talpos ir pašto dėžučių skaičiaus elektroninio pašto serveris įstaigos / organizacijos vartotojams. Paslaugos pasiekiamumas – 99,75%.
Technologinis aprašas	Paslauga realizuojama virtualių mašinų priemonėmis, jas kuriant ir palaikant tam numatytuose bendrų uždavinių skaičiavimo išteklių telkiniuose. Elektroninio pašto serveris gali būti integruojamas su įstaigos / organizacijos tapatybės valdymo sistema. Pastaba: Pašto serverio parametrai, nustatymai ir integracijos bus suderinta infrastruktūros diegimo etape.
Tiesioginis teikimas	Taip

Naudojimas kitų paslaugų teikimui	Ne
Paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	I1, I2, I8-I19
Pasirinktinių paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	I3-I5

4.5.3 Komunikavimo platforma

Kodas	S3
Pavadinimas	Komunikavimo platforma
Kategorija	SaaS
Aprašas	Platforma skirta įstaigų komunikavimui tarpusavyje. Komunikacija gali vykti integruojant vaizdo, balso, telefonijos, dokumentų apsikeitimo ir kitas priemones.
Technologinis aprašas	Paslauga bus projektuojama prieš pradedant įgyvendinti tolimesnius projekto etapus, atsižvelgiant į realius poreikius.
Tiesioginis teikimas	Taip
Naudojimas kitų paslaugų teikimui	Ne
Paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	I1, I2
Pasirinktinių paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	I3-I5

4.5.4 Didžiųjų duomenų valdymo platforma

Kodas	S4
Pavadinimas	Didžiųjų duomenų valdymo platforma
Kategorija	SaaS
Aprašas	Platfoma skirta duomenų saugojimui, apdorojimui ir analizei.
Technologinis aprašas	Paslauga bus projektuojama prieš pradedant įgyvendinti tolimesnius projekto etapus, atsižvelgiant į realius poreikius.
Tiesioginis teikimas	Taip
Naudojimas kitų paslaugų teikimui	Ne
Paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	I1, I2
Pasirinktinių paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	I3-I5

4.5.5 Vaizdo apdorojimo platforma

Kodas	S5
Pavadinimas	Vaizdo apdorojimo platforma

Kategorija	SaaS
Aprašas	Vaizdo apdorojimo platforma skirta vaizdo įrašų saugojimui, apdorojimui ir analizei.
Technologinis aprašas	Paslauga bus projektuojama prieš pradedant įgyvendinti tolimesnius projekto etapus, atsižvelgiant į realius poreikius.
Tiesioginis teikimas	Taip
Naudojimas kitų paslaugų teikimui	Ne
Paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	I1, I2
Pasirinktinių paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	I3-I5

4.6 Bendrai numatytos sisteminės paslaugos

Šiame skyriuje yra aprašomos bendrai numatytos sisteminės paslaugos.

4.6.1 Sistemų stebėsena

Kodas	B1
Pavadinimas	Sistemų stebėsena (angl. monitoring)
Kategorija	Bendrai numatytos sisteminės paslaugos
Aprašas	Paslauga bus teikiama: 1. Paslauga privalomai bus teikiama visiems VITC platformos komponentams pagal VITC apibrėžtus šablonus. 2. Paslauga privalomai suteikiama visiems VITC platformoje talpinamiems virtualiems serveriams ir tinklo įrenginiams pagal VITC apibrėžtus šablonus. 3. Papildomų sistemų stebėsenos paslauga gali būti atskirai užsisakoma visų debesijos paslaugų platformos naudotojų (pagal poreikį). Stebimi parametrai suderinami užsakymo metu. Pagal nustatytas prieigos teises paslaugų gavėjui suteikiama prieiga prie sistemų stebėsenos programinės įrangos. Sistemų stebėsenos programinė įranga leidžia stebėti užsakovo pasirinktų įrenginių suderintų parametrų reikšmes, gauti automatinius pranešimus pasiekus parametro nustatytą reikšmę, užsisakyti papildomų parametrų stebėjimą ir pan. Paslaugos pasiekiamumas – 99,99%.
Technologinis aprašas	Stebėsenos sistemos funkcionalumas: • stebėjimo agentų ir (arba) tarnybų diegimas bei konfigūravimas; • standartinių stebėjimo šablonų pradinis konfigūravimas ir sukonfigūruotų parametrų stebėjimas; • papildomai pasirinktų sričių ar būsenų stebėjimas; • automatinis stebėjimo sistemų pranešimų siuntimas.
Tiesioginis teikimas	Taip
Naudojimas kitų paslaugų teikimui	Taip
Privalomų paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	I19, I1, I2
Pasirinktinių paslaugų, kuriomis naudojamasi	Nėra

teikiant šią paslaugą, kodai	

4.6.2 Rezervinis kopijavimas

Kodas	B2
Pavadinimas	Rezervinis kopijavimas
Kategorija	Bendrai numatytos sisteminės paslaugos
Aprašas	VDPT infrastruktūroje esančių resursų rezervinis kopijavimas. Šia paslauga suteikiama galimybė užsakyti VM, OS, failų, DB, aplikacijų rezervinį kopijavimą ir rezervinių kopijų valdymą. Paslaugos pasiekiamumas – 99%.
Technologinis aprašas	Sistemų ir programų duomenų atsarginės kopijos kuriamos pagal paslaugų gavėjo pasirinktą atsarginių kopijų kūrimo parametrų rinkinį. Atsarginių kopijų kūrimo tvarka nustatoma naudojant rezervinio kopijavimo programinę įrangą. Preliminarūs atsarginių kopijų kūrimo planai[1] 1. Aplikacijų serverių kopijavimui skirtas planas. Dalinės atsarginės kopijos kuriamos kiekvieną dieną. Pilnos atsarginės virtualių serverių kopijos kuriamos kas 7 dienas. Maksimalus duomenų praradimo laikas (angl. RPO) – 24 val., RTO – 8 val. Operatyvinės duomenų kopijos saugomos 1 mėnesį. 2. Duomenų bazių kopijavimui skirtas planas. Duomenų bazių logų rezervinės kopijos kuriamos kartą per valandą. Pilna DB kopija kuriama kartą per parą. Maksimalus duomenų praradimo laikas (angl. RPO) – 1 val., RTO – 8 val. Operatyvinės rezervinės kopijos saugomos 1 mėnesį. 3. Ilgalaikėms duomenų kopijoms saugoti skirtas planas. RPO – 24 val., RTO – 8 val. Duomenų kopijos saugomos 6 mėnesius. Jei paslaugų gavėjas neišreiškia specifinių reikalavimų atsarginių kopijų kūrimui, bus pritaikyti aukščiau įvardinti atsarginių kopijų kūrimo planai.
Tiesioginis teikimas	Taip
Naudojimas kitų paslaugų teikimui	Ne
Privalomų paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	I1-I2, I3-I6
Pasirinktinių paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	I19

4.6.3 Žurnalų kaupimas ir apdorojimas, SIEM

Kodas	B3
Pavadinimas	Žurnalų kaupimas ir apdorojimas, SIEM
Kategorija	Bendrai numatytos sisteminės paslaugos
Aprašas	Paslauga apima tinkle esančių IT įrenginių žurnalų analizę, saugojimą ir koreliaciją, saugumo incidentų generavimą. Paslaugos pasiekiamumas – 99,99%.

[1] Įvardinti parametrai (atsarginių kopijų kūrimo planai) bus derinami konkrečios informacinės sistemos diegimo / migravimo etape.

Technologinis aprašas	Paslaugos realizacija aprašyta infrastruktūros architektūroje. Paslaugos parametrai, nustatymai ir integracijos bus suderinta infrastruktūros diegimo etape.
Tiesioginis teikimas	Ne
Naudojimas kitų paslaugų teikimui	Taip
Paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	I1-I20
Pasirinktinių paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	P1-P7, S1-5

4.6.4 Privilegijuotos prieigos kontrolė

Kodas	B4
Pavadinimas	Privilegijuotos prieigos kontrolė (angl. PAM)
Kategorija	Bendrai numatytos sisteminės paslaugos
Aprašas	PAM atlieka vartotojų (administratorių) kontrolės funkciją, kuri užtikrina vartotojų prisijungimų kontrolę prie resursų bei saugų slaptažodžių maskavimą ir valdymą. Paslaugos pasiekiamumas – 99.99%.
Technologinis aprašas	Paslaugos realizacija aprašyta infrastruktūros architektūroje. Paslaugos parametrai, nustatymai ir integracijos bus suderinta infrastruktūros diegimo etape.
Tiesioginis teikimas	Taip
Naudojimas kitų paslaugų teikimui	Taip
Paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	Nėra
Pasirinktinių paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	Nėra

4.6.5 IS diegimo ir konfigūravimo automatizacija

Kodas	B5
Pavadinimas	IS diegimo ir konfigūravimo automatizacija
Kategorija	Bendrai numatytos sisteminės paslaugos
Aprašas	IS diegimo ir konfigūravimo automatizavimo paslauga apima automatizuotą resursų išskyrimą, reikiamų serverių sukūrimą, standartinės programinės įrangos įdiegimą bei suderintų specifinės programinės įrangos komponentų įdiegimą.
Technologinis aprašas	Paslauga bus projektuojama prieš pradedant įgyvendinti tolimesnius projekto etapus, atsižvelgiant į realius poreikius.
Tiesioginis teikimas	Taip
Naudojimas kitų paslaugų teikimui	Taip
Paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	I1-I20

Pasirinktinių paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	P1-P7, S1-5

4.6.6 Pagalbos tarnybos (Service Desk)

Kodas	B6
Pavadinimas	Pagalbos tarnyba (angl. Service Desk)
Kategorija	Bendrai numatytos sisteminės paslaugos
Aprašas	Pagalbos tarnybos paslauga apimanti ne mažiau kaip šias sritis: • Kreipinių valdymas; • Incidentų valdymas; • Problemų valdymas; • Pakeitimų valdymas; • Versijų valdymas; • Konfigūracijų valdymas; • Paslaugų lygio valdymas; • Žinių bazė ir jos valdymas; • Skambučių centras.
Technologinis aprašas	Šio projekto apimtyje pagalbos tarnybos paslauga detaliau neprojektuojama. Pagalbos tarnybos paslaugos bus projektuojamos, diegiamos ir dokumentuojamos atskiro projekto (10 prioriteto investicijų projekto) apimtyje.
Tiesioginis teikimas	Taip
Naudojimas kitų paslaugų teikimui	Ne
Paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	Nėra
Pasirinktinių paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	Nėra

4.6.7 Virtualizacijos platformos valdymo portalas (Admin self service portal)

Kodas	B7
Pavadinimas	Virtualizacijos platformos valdymo portalas (Admin self-service portal)
Kategorija	Bendrai numatytos sisteminės paslaugos
Aprašas	Pagal nustatytas prieigos teises, paslaugų gavėjui suteikiama prieiga prie Debesijos platformos valdymo portalo, kuriame galima kurti, valdyti ir naudoti skaičiavimo, saugyklų ir tinklo išteklius.
Technologinis aprašas	Debesijos platformos valdymo portalo būtinas funkcionalumas: • pilnas resursų valdymo atskyrimas organizacijų lygyje; • visiškas resursų ir tinklų izoliavimas organizacijų lygyje; • galimybė naudoti resursus iš skirtingų resursų telkinių; • galimybė integruoti su išoriniu tapatybės informacijos šaltiniu (angl. Identity integration – LDAP, other); • galimybė apriboti virtualių tarnybinių stočių veikimą tarp skirtingų fizinių tarnybinių stočių (angl. affinity rules). Asmeniui, atsakingam už organizacijos resursų valdymą, turi būti galimybė atlikti šiuos veiksmus priskirtų resursų aibėje: • kurti, stabdyti, perkrauti, ištrinti virtualias tarnybines stotis;

	• keisti visus virtualios tarnybinės stoties parametrus: vCPU, RAM, HDD; • virtualiai tarnybinei stočiai priskirti ne mažiau kaip 2 (du) virtualius tinklo adapterius; • kurti virtualias tarnybines stotis iš paruoštų šablonų; • kurti virtualias tarnybines stotis, pasinaudojant virtualiais atvaizdais; • kurti ir saugoti momentines virtualių tarnybinių stočių kopijas (angl. Snap Shots); • turi būti galimybė pasinaudojant platformos valdymo portalu prisijungti prie virtualios tarnybinės stoties, nenaudojant papildomų programinių įrankių. Virtuali tarnybinė stotis turi būti pasiekiama ir tuo atveju, kai jai nėra prijungtas ar suteiktas virtualus tinklo adapteris ar IP adresas; • priskirti reikiamą VLAN konkrečiam virtualiam serveriui. Organizacijos atsakingam asmeniui turi būti leidžiama peržiūrėti ir valdyti tik savo organizacijos VLAN.
Tiesioginis teikimas	Taip
Naudojimas kitų paslaugų teikimui	Taip
Paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	Nėra
Pasirinktinių paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	Nėra

4.6.8 Debesijos platformos automatizuoto valdymo portalas (End user self service portal)

Kodas	B8
Pavadinimas	Debesijos platformos automatizuoto valdymo portalas (end user self-service portal)
Kategorija	Bendrai numatytos sisteminės paslaugos
Aprašas	Debesijos platformos automatizuoto valdymo portalas suteikia galimybę naudotojams savarankiškai užsisakyti pageidaujamas paslaugas, valdyti resursus, stebėti resursų naudojimo statistiką, valdyti užsakymų ir atsiskaitymo informaciją. Portalas bus integruojamas su Service Desk programine įranga, automatizavimo ir monitoringo įrankiais.
Technologinis aprašas	Paslauga bus projektuojama prieš pradedant įgyvendinti tolimesnius projekto etapus, atsižvelgiant į realius poreikius. Paslauga bus projektuojama ir diegiama atskiro projekto apimtyje.
Tiesioginis teikimas	Taip
Naudojimas kitų paslaugų teikimui	Ne
Paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	I1-I20
Pasirinktinių paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	P1-P7, S1-5

4.7 Papildomos paslaugos

Šiame skyriuje aprašomos VDPT planuojamos teikti informacinių sistemų (toliau – IS) infrastruktūros priežiūros, IRT projektavimo bei migravimo, KDV priežiūros ir konsultavimo paslaugos. VDPT klientai, užsisakydami IS infrastruktūros priežiūros paslaugas, kiekvienai IS gali pasirinkti vieną iš trijų paslaugų teikimo lygių (toliau – PTL).

4.7.1 OS priežiūros paslauga

Kodas	A1
Pavadinimas	OS priežiūros paslauga
Kategorija	Papildomos paslaugos
Aprašas	Microsoft Windows bei Linux šeimos (CentOS ir kitų distribucijų) operacinių sistemų priežiūros paslauga pagal užsakovo pasirinktą paslaugų teikimo lygį. Operacinių sistemų priežiūros paslaugos apima: • Operacinės sistemos diegimą iš gamintojo pateikiamų šaltinių; • Operacinės sistemos nustatymų konfigūravimą; • Papildomų tarnybų (angl. roles) diegimą ir konfigūravimą (pagal apibrėžtą ir suderintą poreikį); • Vartotojų ir administratorių teisių konfigūravimą; • Operacinės sistemos stebėjimo agentų diegimą, konfigūravimą pagal Paslaugos teikėjo poreikius; • Standartinių stebėjimo šablonų pradinį konfigūravimą priklausomai nuo OS ir veikiančių serverio tarnybų; • Incidentų sprendimą, operacinės sistemos veikimo užtikrinimą; • Operacinės sistemos darbingumo atstatymą po aparatinio ar programinio gedimo; • Problemų analizę ir gerinimo veiksmų inicijavimą; • Operacinės sistemos įvykių žurnalo peržiūrą, klaidų įrašų analizę bei klaidų priežasčių panaikinimą; • Atnaujinimų (angl. Updates) bei pataisų (angl. Patches) diegimą tos pačios operacinės sistemos versijos ribose.
Technologinis aprašas	Šio projekto apimtyje operacinių sistemų priežiūros paslauga detaliau neprojektuojama. Priežiūros paslaugos bus projektuojamos atskiro projekto apimtyje.
Tiesioginis teikimas	Taip
Naudojimas kitų paslaugų teikimui	Nėra
Paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	DCaaS, IaaS, B1-B8
Pasirinktinių paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	Nėra

4.7.2 DBVS priežiūros paslauga

Kodas	A2
Pavadinimas	DBVS priežiūros paslauga
Kategorija	Papildomos paslaugos
Aprašas	Oracle, Microsoft SQL, MySQL/MariaDB, PostgreSQL ir SAP HANA duomenų bazių valdymo sistemų priežiūros paslauga pagal užsakovo pasirinktą paslaugų teikimo lygį. Duomenų bazių valdymo sistemų priežiūros paslaugos gali būti užsakomos tik tuo atveju, jeigu yra užsakyta konkretaus

	serverio operacinės sistemos priežiūros paslauga. Duomenų bazių valdymo sistemų priežiūros paslauga apima: • Duomenų bazių valdymo sistemos programinės įrangos diegimą iš gamintojo pateikiamų šaltinių; • Duomenų bazių valdymo sistemos nustatymų konfigūravimą; • Duomenų bazių sukūrimą ir paleidimą (pagal apibrėžtą ir suderintą poreikį); • Duomenų bazių konfigūravimą, vartotojų ir administratorių teisių konfigūravimą; • Duomenų bazių atsarginių kopijų vykdymo plano suderinimą ir konfigūravimą; • Duomenų bazių valdymo platformos stebėjimo agentų diegimą ir konfigūravimą pagal Paslaugos teikėjo poreikius; • Standartinių stebėjimo šablonų pradinį konfigūravimą; • Duomenų bazių naikinimą (pagal apibrėžtą ir suderintą poreikį); • Incidentų sprendimą ir duomenų bazių veikimo užtikrinimą; • Duomenų bazių darbingumo atstatymą po aparatinio ar programinio gedimo; • Problemų analizę ir gerinimo veiksmų inicijavimą; • Duomenų bazių valdymo platformos įvykių žurnalo peržiūrą, klaidų įrašų analizę bei klaidų priežasčių panaikinimą; • Atnaujinimų (angl. Updates) bei pataisų (angl. Patches) diegimą tos pačios duomenų bazės versijos ribose.
Technologinis aprašas	Šio projekto apimtyje DBVS sistemų priežiūros paslauga detaliau neprojektuojama. Priežiūros paslaugos bus projektuojamos atskiro projekto apimtyje.
Tiesioginis teikimas	Taip
Naudojimas kitų paslaugų teikimui	Nėra
Paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	DCaaS, IaaS, P1-P5, B1-B8
Pasirinktinių paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	Nėra

4.7.3 IRT projektavimo, migravimo paslauga

Kodas	A3
Pavadinimas	IRT projektavimo, migravimo paslauga
Kategorija	Papildomos paslaugos
Aprašas	IRT projektavimo ir migravimo paslauga leidžia organizacijoms / įstaigoms suprojektuoti bei tinkamai įdiegti naujas informacines sistemas arba išmigruoti esamas IS į VDPT infrastruktūrą.
Technologinis aprašas	Paslauga apima: • Informacinių sistemų infrastruktūros projektavimą pagal užsakovo poreikius; • Virtualių serverių diegimą ir konfigūravimą pagal užsakovo poreikius; • Tinklo elementų konfigūravimą pagal užsakovo poreikius; • Duomenų bazių valdymo sistemų diegimą ir konfigūravimą pagal užsakovo poreikius; • Saugumo elementų konfigūravimą pagal užsakovo poreikius. Šio projekto apimtyje paslauga detaliau neprojektuojama. Paslauga bus projektuojamos atskiro projekto apimtyje.

Tiesioginis teikimas	Taip
Naudojimas kitų paslaugų teikimui	Taip
Paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	Nėra
Pasirinktinių paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	Nėra

4.7.4 KDV priežiūros paslauga

Kodas	A4
Pavadinimas	KDV priežiūros paslauga
Kategorija	Papildomos paslaugos
Aprašas	Kompiuterinių darbo vietų priežiūros paslauga.
Technologinis aprašas	Šio projekto apimtyje paslauga detaliau neprojektuojama. Paslauga bus projektuojamos atskiro projekto apimtyje.
Tiesioginis teikimas	Taip
Naudojimas kitų paslaugų teikimui	Nėra
Paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	Nėra
Pasirinktinių paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	Nėra

4.7.5 Konsultavimo paslauga

Kodas	A5
Pavadinimas	Konsultavimo paslauga
Kategorija	Papildomos paslaugos
Aprašas	Konsultacijos debesijos platformos naudojimo klausimais.
Technologinis aprašas	Konsultacijos debesijos platformos naudojimo klausimais apima: • Konsultacijas paslaugų krepšelio naudojimosi klausimais; • Konsultacijas virtualių serverių diegimo, konfigūravimo ir veikimo klausimais; • Konsultacijas tinklo elementų konfigūravimo ir veikimo klausimais; • Konsultacijas duomenų bazių valdymo sistemų konfigūravimo ir veikimo klausimais; • Konsultacijas saugumo elementų konfigūravimo ir veikimo klausimais. • Konsultacijos kitais VITC kuruojamais klausimais (KDV priežiūra, IS steigimas, dokumentacijos rengimas ir kt. Technologinis šios paslaugos aprašymas pateikiamas atskirame dokumente. Šio projekto apimtyje paslauga detaliau neprojektuojama. Paslauga bus projektuojama atskiro projekto apimtyje.
Tiesioginis teikimas	Taip
Naudojimas kitų paslaugų teikimui	Nėra

Paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	Nėra
Pasirinktinių paslaugų, kuriomis naudojamasi teikiant šią paslaugą, kodai	Nėra

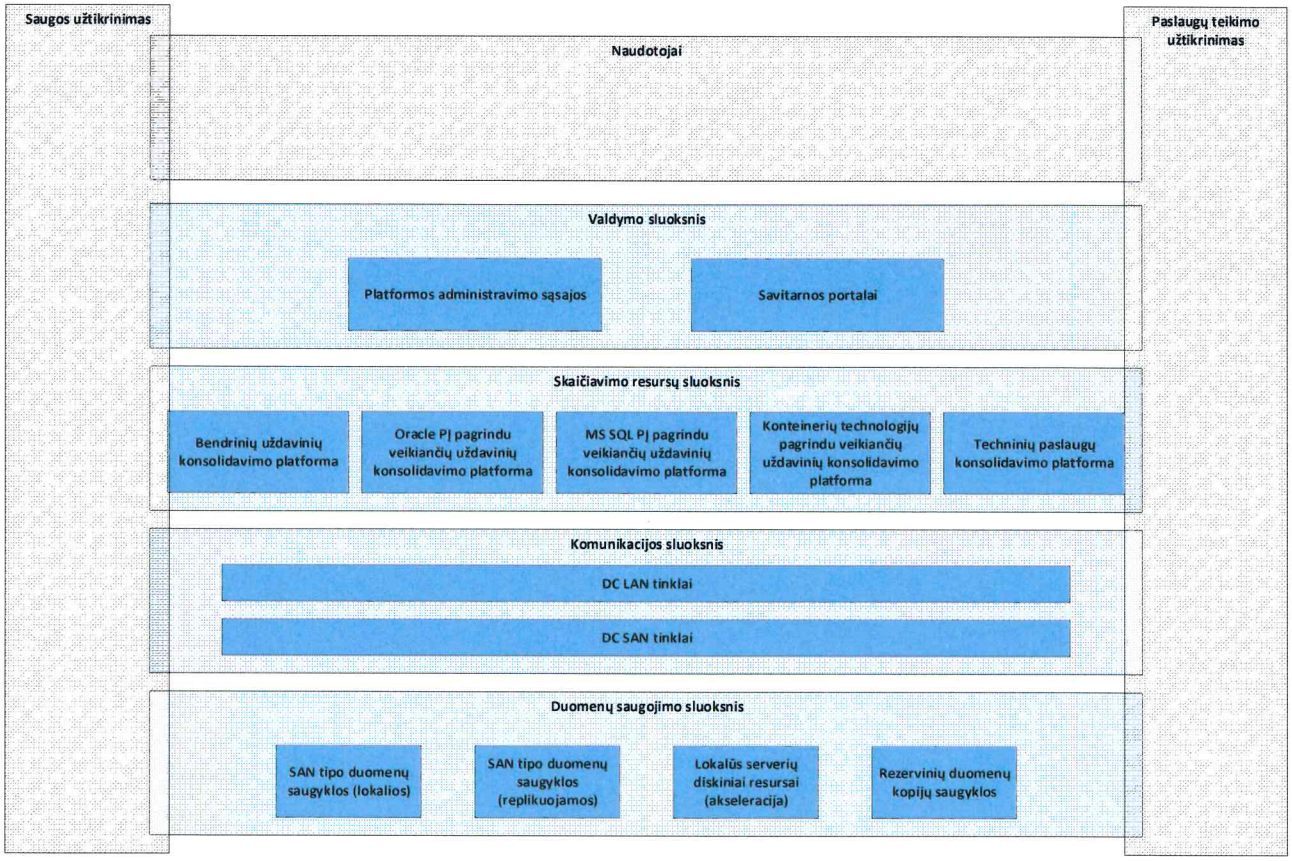
4.8 Tolimesnių etapų paslaugos

Atsižvelgiant į tai, kad potencialūs projektuojamos platformos naudotojai neturi pakankamai patirties naudojantis debesijos technologijomis, didžioji dalis šiuo metu naudojamų informacinių sistemų nėra pritaikytos naudoti debesijos sprendimus, bei tai, kad pirmame projekto etape vyks tik pradinis platformos diegimas, šiame dokumente detaliai neprojektuojamos tolimesnių projekto įgyvendinimo etapų paslaugos. Šiame dokumento skyriuje įvardinamos paslaugos, kurios buvo identifikuotos analizės etape (pagal šiuo metu turimą informaciją), tačiau priimtas sprendimas pirmame projekto įgyvendinimo etape jų nerealizuoti. Šiame dokumento skyriuje įvardintos paslaugos bus projektuojamos prieš pradedant įgyvendinti tolimesnius projekto etapus, atsižvelgiant į realius poreikius.

5 Bendra sprendimo architektūra

5.1 Apibendrinta sprendimo vizija

Remiantis geriausiomis konsoliduotų platformų kūrimo praktikomis siūlomame sprendime išskiriama 3 bendrinės sritys ir 4 infrastruktūros sluoksniai (pav. 5-1 Apibendrinta sprendimo vizija).



pav. 5-1 Apibendrinta sprendimo vizija

Bendrinės sritys:

1. Naudotojai.
2. Saugos užtikrinimas.
3. Paslaugų teikimo užtikrinimas.

Infrastruktūros sluoksniai:

1. Valdymo sluoksnis.
2. Skaičiavimo resursų (angl. compute) sluoksnis.
3. Komunikacijos sluoksnis.
4. Duomenų saugojimo sluoksnis.

5.1.1 Naudotojai

Įstaigų / organizacijų / VDPT administratoriai, valdantys debesijos resursus, paslaugų valdytojai, galutiniai debesijos paslaugų naudotojai, galintys turėti tiesioginę ir netiesioginę prieigą prie debesijos paslaugų krepšelio resursų bei debesijos platformos. Netiesioginė prieiga realizuojama praplečiant esamus arba kuriant naujus valstybės institucijų portalus / svetaines, integruotus su VDPT išteklių lygmens valdymo savitarnos elementais.

5.1.2 Saugos užtikrinimas

Saugumo užtikrinimas apima:

- VDPT paslaugų krepšelio tinklo – saugos išteklius: AntiDDoS, VPN, AntiSPAM, AntiVirus, skirtingo lygio ugniasienes, internetinių programų ugniasienes (WAF), IDS/IPS/UTM;
- tinklo mikrosegmentacijos ir loginės izoliacijos sprendimus;
- saugos informacijos ir įvykių valdymo sistemą (angl. SIEM);
- tinklo stebėjimo įrankius;
- saugaus ryšio, šifravimo raktų valdymo priemones;
- prisijungimų valdymą (vartotojų identifikavimas ir autentifikavimas, autorizacija ir prieigos taisyklių valdymas).

5.1.3 Paslaugų teikimo užtikrinimas

VDPT platformos paslaugų užtikrinimas apima:

- duomenų centrų valdymą;
- tinklų nuo VDPT iki galutinio naudotojo valdymą;
- virtualizuotų išteklių (skaičiavimo, saugyklų, tinklo) konfigūravimą ir valdymą;
- platformos resursų, paslaugų krepšelio išteklių stebėseną (angl. monitoring) ir kontrolę;
- pagalbos tarnybos veiklą.

5.1.4 Valdymo sluoksnis

Valdymo sluoksnis apima platformos valdymo įrankius, naudojamus platformos administratorių bei savitarnos portalus, skirtus galutinių platformos resursų naudotojams (įstaigų / institucijų administratoriams).

5.1.5 Skaičiavimo resursų sluoksnis

Skaičiavimo resursų sluoksniui priklauso tarnybinių stočių resursai, kurie pagal analizės etape identifikuotus technologinius / licencinius ir kitus apribojimus yra skirstomi į keletą pagrindinių resursų grupių:

1. Bendrinių uždavinių konsolidavimo platforma. Skirta virtualiems serveriams, veikiantiems MS Windows ar Linux operacinių sistemų pagrindu ir neturinčių sudiegtų PĮ komponentų, kuriems galioja licenciniai apribojimai (Oracle ar MS SQL produktai).
2. Oracle PĮ pagrindu veikiančių uždavinių konsolidavimo platforma, kuri skirta virtualiems serveriams, naudojantiems Oracle PĮ. Platforma diferencijuojama pagal naudojamus produktus, siekiant optimalaus licencijų panaudojimo.
3. MS SQL PĮ pagrindu veikiančių uždavinių konsolidavimo platforma. Ši platforma skirta virtualiems serveriams, veikiantiems MS Windows pagrindu bei naudojantiems MS SQL programinę įrangą.
4. Konteinerių technologijų pagrindu veikiančių uždavinių konsolidavimo platforma. Skirta naujos kartos sprendimų kūrimui, naudojant modernias debesijos technologijas.
5. Techninių paslaugų konsolidavimo platforma. Skirta virtualiems serveriams, užtikrinantiems įvairias platformos technines funkcijas (valdymo, autentifikacijos, rezervinio kopijavimo ir kita).

5.1.6 Komunikacijos sluoksnis

Komunikacijos sluoksnis apima duomenų centrų LAN ir SAN įrangą.

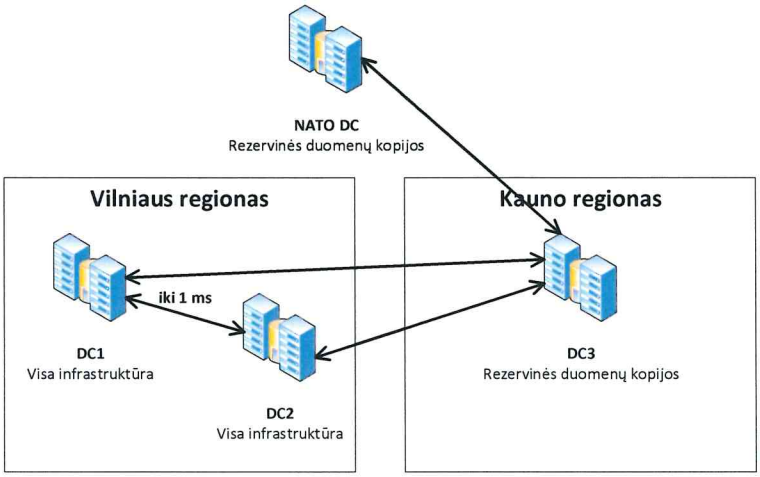
5.1.7 Duomenų saugojimo sluoksnis

Duomenų saugojimo sluoksnis apima skirtingus duomenų saugojimo sprendimus:

1. Lokalios (duomenų centro lygmenyje) SAN tipo duomenų saugyklos, skirtos žemesnio kritiškumo ar išskleistų (angl. distributed) sprendimų duomenų saugojimui.
2. SAN tipo duomenų saugojimo sprendimai, veikiantys virtualizacijos pagrindu bei užtikrinantys sinchroninę duomenų repliką dviejuose duomenų centruose. Sprendimas skirtas kritinių sistemų, reikalaujančių aukšto patikimumo bei minimalaus atstatymo laiko, duomenų saugojimui.
3. Lokalūs serverių diskiniai resursai (NVMe technologijos pagrindu). Sprendimas orientuotas į konteinerių technologijos pagrindu veikiančias sistemas.
4. Rezervinio kopijavimo duomenų saugyklos. Sprendimas, užtikrinantis rezervinių kopijų saugojimą pagal nustatytus reikalavimus.

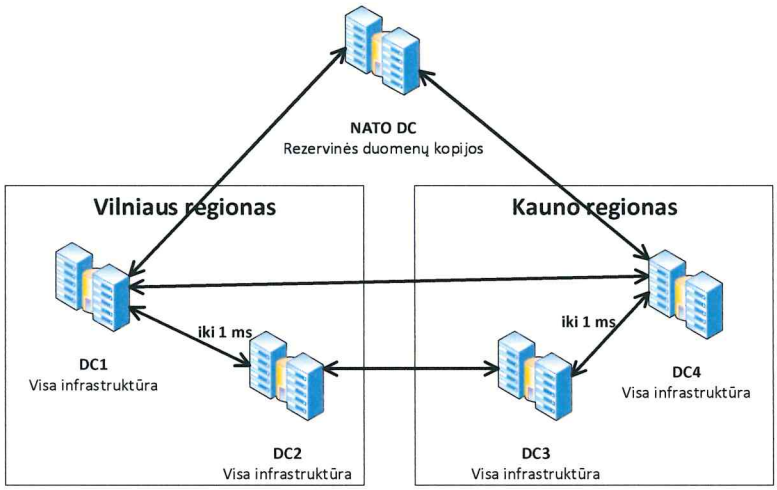
5.2 Duomenų centrai

Įvertinus nacionalinio saugumo interesus bei kitus teisinius aspektus nuspręsta, kad duomenų centrai, kuriuose bus diegiama projektuojama infrastruktūra, geografiškai turi būti nutolę bent 100 kilometrų atstumu vienas nuo kito. Šio projekto analizės etape nustatyta, kad konkrečių sprendimų realizacijai bus būtina sinchroninė duomenų replikacija tarp duomenų centrų. Dauguma gamintojų rekomenduoja, kad sinchroninės replikacijos atveju vėlinimas, skaičiuojant į abi puses, būtų iki 1 mili sekundės, - jeigu norima, kad greitaveikos įtaka nebūtų juntama galutiniams naudotojams. Atsižvelgiant į tai, kad vėlinimas stikle 100 kilometrų atstumu apytiksliai lygus 1 mili sekundei, realus atstumas tarp duomenų centrų gali būti iki 30 kilometrų (0,3 ms į vieną pusę, 0,3 ms grįžimas ir iki 0,4 ms aktyvinės įrangos vėlinimas). Įvertinus realią duomenų centrų bei kitos infrastruktūros situaciją Lietuvoje, teisės aktų reikalavimus bei nacionalinio saugumo interesus, nuspręsta, kad šiai platformai bus naudojami keturi duomenų centrai Lietuvoje ir rezervinėms kritinių duomenų kopijoms skirta infrastruktūra NATO duomenų centre. Atsižvelgiant į tai, kad šiuo metu valstybės įstaigos neturi keturių laisvų duomenų centrų bei tai, kad pirmąjį šio projekto etapą planuojama įvykdyti 2019 metais, nuspręsta pirmajame projekto įgyvendinimo etape platformą realizuoti dviejuose duomenų centruose Vilniaus regione, atsargines kopijas saugoti Kauno regione esančiame duomenų centre, o kritinių duomenų kopijas saugoti NATO duomenų centre. Koncepcinė pirmojo šio projekto įgyvendinimo etapo duomenų centrų schema pateikiama žemiau (pav. 5-2 Duomenų centrai 2019-2020).



pav. 5-2 Duomenų centrai 2019-2020

2021 metais planuojama Kauno regione įrengti papildomą duomenų centrą su dviem nepriklausomomis serverinėmis. Koncepcinė duomenų centrų schema, įrengus Kauno regiono duomenų centrus, pateikiama žemiau (pav. 5-3 Duomenų centrai 2021).

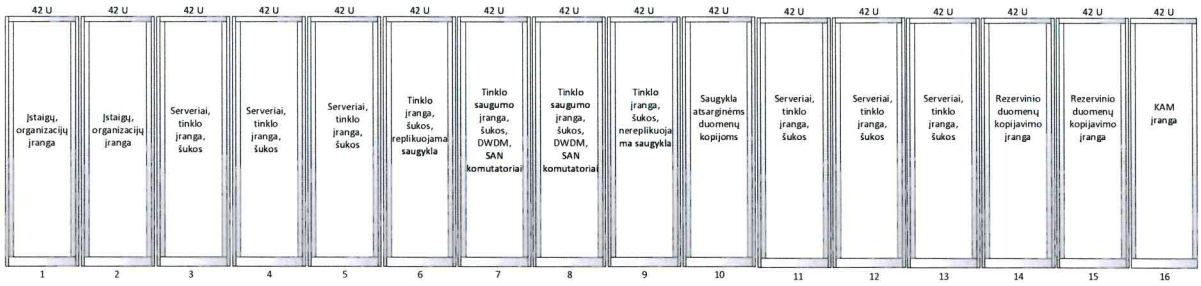


pav. 5-3 Duomenų centrai 2021

5.3 Įrangos išdėstymas duomenų centruose

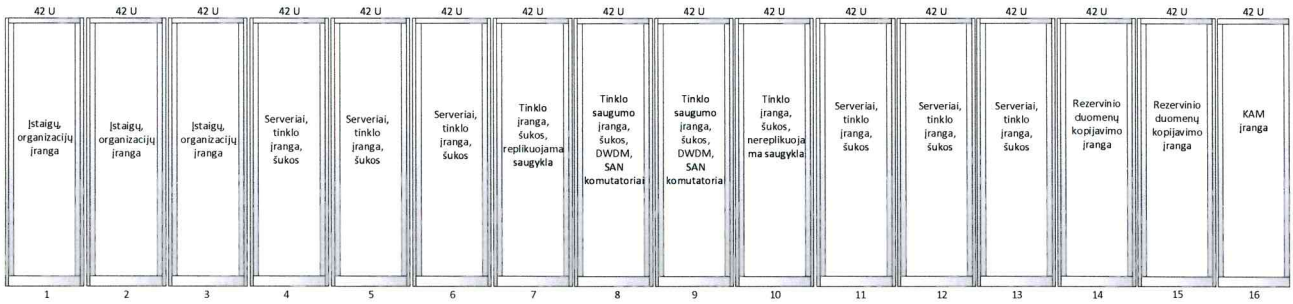
I projekto įgyvendinimo etape įranga bus talpinama dviejuose Vilniaus regiono duomenų centruose, Kauno duomenų centre ir NATO duomenų centre. Duomenų centruose bus naudojamos standartinės 42 RU aukščio spintos. Vilniaus regiono duomenų centruose planuojama naudoti po 16 spintų. Kauno duomenų centre bus naudojamos 4 – 5 spintos priklausomai nuo įsigytos įrangos. NATO duomenų centre įrangą planuojama talpinti į 2 spintas.

Koncepcinė įrangos išdėstymo Vilniaus regiono pirmame duomenų centre schema pateikiama žemiau (pav. 5-4 Vilniaus regiono duomenų centro (DC1) įrangos išdėstymo koncepcinė schema).



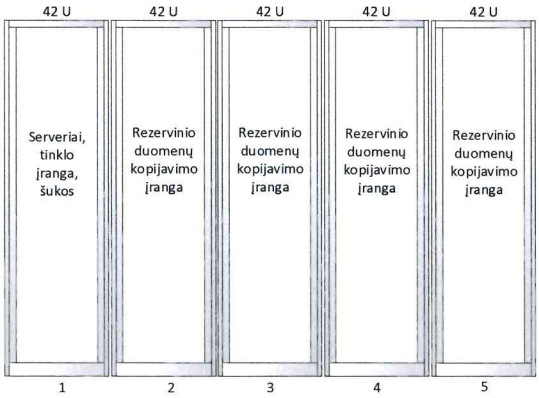
pav. 5-4 Vilniaus regiono duomenų centro (DC1) įrangos išdėstymo koncepcinė schema

Koncepcinė įrangos išdėstymo Vilniaus regiono antrame duomenų centre schema pateikiama žemiau (pav. 5-5 Vilniaus regiono duomenų centro (DC2) įrangos išdėstymo koncepcinė schema).



pav. 5-5 Vilniaus regiono duomenų centro (DC2) įrangos išdėstymo koncepcinė schema

Koncepcinė įrangos išdėstymo Kauno duomenų centre schema pateikiama žemiau (pav. 5-6 Kauno regiono duomenų centro (DC3-rezervinių duomenų kopijų) įrangos išdėstymo koncepcinė schema).



pav. 5-6 Kauno regiono duomenų centro (DC3-rezervinių duomenų kopijų) įrangos išdėstymo koncepcinė schema

Koncepcinė įrangos išdėstymo NATO duomenų centre schema pateikiama žemiau (pav. 5-7 NATO duomenų centro įrangos išdėstymo koncepcinė schema).

pav. 5-7 NATO duomenų centro įrangos išdėstymo koncepcinė schema

Įrangos išdėstymo duomenų centruose schemos bus patikslintos kai bus aiškūs planuojamos montuoti įrangos modeliai.

Atsižvelgiant į tai, kad projektuojamos įrangos elektros galia nebus koncentruota, planuojama, kad maksimali elektros galia vienai spintai bus apie 10 kW. Vertinant tai, kad infrastruktūra suprojektuota taip, kad gali būti plečiama 3-4 kartus, preliminariais skaičiavimais būtina užtikrinti:

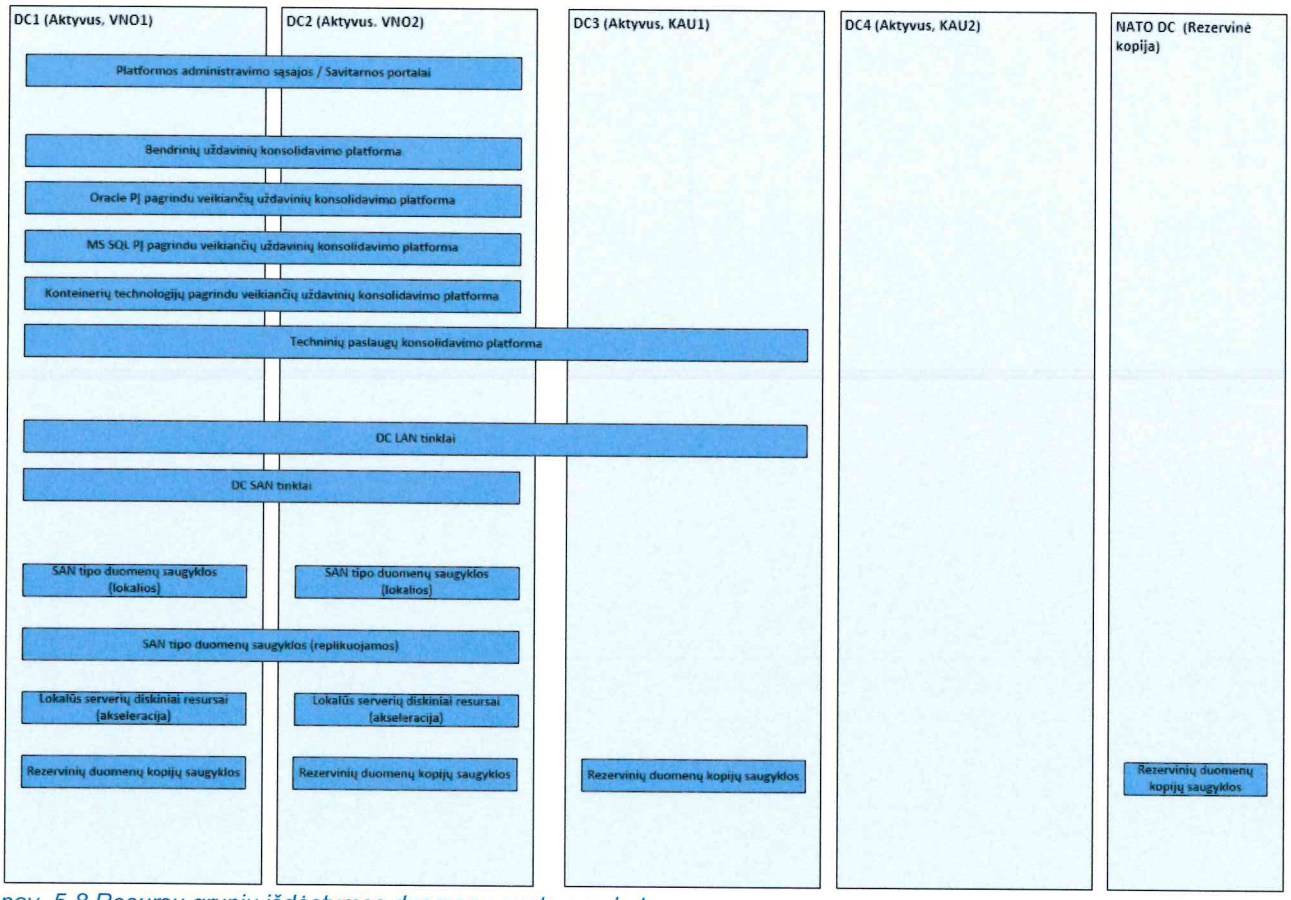
- I etapas: po 16 spintų (I etape bus naudojama apie 12 spintų priklausomai nuo pasiūlytos įrangos) ir po 160 kW elektros įvadų galingumo kiekvienam Vilniaus regiono duomenų centrui (DC1 ir DC2), 5 spintas ir 50 kW elektros įvadų galingumo Kauno rezervinio kopijavimo duomenų centre (DC3-rezervinių duomenų kopijų), 2 spintas ir 20 kW elektros įvadų galingumo NATO duomenų centre;
- II etapas: po 16 spintų (II etape numatoma panaudoti visas spintas) ir 160 kW elektros įvadų galingumo kiekvienam Vilniaus regiono duomenų centrui (DC1 ir DC2), 5 spintas ir 50 kW elektros įvadų galingumo Kauno rezervinio kopijavimo duomenų centre (DC3-rezervinių duomenų kopijų), 3 spintas ir 30 kW elektros įvadų galingumo NATO duomenų centre;
- III ir vėlesni etapai: po 16 spintų ir po 160 kW elektros įvadų galingumo kiekvienam Vilniaus regiono duomenų centrui (DC1 ir DC2) bei po 30 spintų ir po 300 kW elektros įvadų galingumo kiekvienam Kauno regiono duomenų centrui (DC3 ir DC4)[2], 4 spintas ir 40 kW elektros įvadų galingumo NATO duomenų centre.

[2] Kauno rezervinio kpijavimo duomenų centro (DC3- rezervinių duomenų kopijų) įrangą bus perkeltą į naujai įrengtus Kauno duomų centrus (DC3 ir DC4).

III projekto įgyvendinimo etape naujai įrengtuose Kauno regiono duomenų centruose bus talpinama papildomai įsigyta įranga, skirta infrastruktūros plėtrai. Vilniaus regiono duomenų centruose bus talpinama rezervinio duomenų kopijavimo įranga, skirta Kauno DC duomenų kopijoms saugoti, o Kauno regiono duomenų centruose bus talpinama (perkelta) rezervinio duomenų kopijavimo įranga, skirta Vilniaus DC duomenų kopijoms saugoti. Koncepcinė III projekto etapo įrangos išdėstymo schema bus pateikta pilnai suprojektavus III projekto etapo infrastruktūrą.

5.4 Sprendimo dalių išdėstymas duomenų centruose

Remiantis 5.2 Duomenų centrai dalyje pateikta duomenų centrų pasirinkimo informacija, sprendimą sudarančias logines dalis pirmame projekto etape siūlome išdėstyti taip (pav. 5-8 Resursų grupių išdėstymas duomenų centruose I etape):



pav. 5-8 Resursų grupių išdėstymas duomenų centruose I etape

Vilniaus duomenų centrai (2 vnt., nutolę ne daugiau nei 30 km vienas nuo kito). Juose diegiama (esminiai akcentai):

- Vartotojams skirtų resursų grupių serveriai;
- DC SAN tinklai. Abiejų duomenų centrų SAN tinklai apjungiami į vieningus SAN fabrikus (2, nepriklausomus, izoliuotus);

- Aukšto patikimumo duomenų saugyklų sprendimas (replikuotas);
- Lokalios SAN tipo duomenų saugyklos bei rezervinių kopijų saugyklos, diegiamos kiekviename duomenų centre.

Per visus 3 duomenų centrus diegiama:

- Techninių paslaugų konsolidavimo platformos serveriai, užtikrinantys ir valdymo sluoksnio funkcijų (platformos administravimo įrankiai bei savitarnos portalai) pasiekiamumą. Kauno DC naudojama SDS (Software Defined Storage) tipo duomenų saugykla;
- DC LAN tinklai;
- Rezervinio kopijavimo sprendimo komponentai (serveriai bei saugyklos).

Antrame projekto etape (pav. 5-9 Resursų grupių išdėstymas duomenų centruose II etape (nuo 2021 m.)) infrastruktūra išplečiama dviejuose Kauno regiono duomenų centuose.

pav. 5-9 Resursų grupių išdėstymas duomenų centruose II etape (nuo 2021 m.)

Papildomai Kauno regiono DC diegiama:

- Vartotojams skirtų resursų grupių serveriai;
- Aukšto patikimumo duomenų saugyklų sprendimas (replikuotas);

- Lokalios SAN tipo duomenų saugyklos bei rezervinių kopijų saugyklos, diegiamos kiekviename duomenų centre.

Keičiama DC tinklų konfigūracija:

- Išplečiami LAN tinklų sujungimai į ketvirtą duomenų centrą;
- Papildomai įdiegus SAN komutatorius Kauno regiono DC, perkonfigūruojami SAN tinklai, sukuriant vieningą konfigūraciją, apimančią 4 duomenų centrus (2 nepriklausomi SAN fabrikai).

6 Virtualizuotų tarnybinių stočių architektūros modelis

6.1 Skaičiavimo resursų sluoksnio realizacija

6.1.1 Serverių standartizacija

Platformose projektuojamiems serverių telkiniams nuspręsta naudoti standartizuotus x86 architektūros serverius. Kriterijai, kurių pagrindu parinkti serveriai:

1. Serverių korpusas. Sprendimui naudojami ne daugiau 2U aukščio serveriai, nes būtent šis serverio formatas leidžia užtikrinti optimalų serverio IO posistemių išdėstymą (2 ir daugiau PCIe jungčių per procesorių) bei aušinimą. Modulinių serverių (blade) naudojimo atsisakyta dėl keleto faktorių:
    a. Privalomo aktyvios įrangos įvedimo (LAN ir SAN komutatoriai ar jų funkcijas atliekantys įrenginiai) į LAN ir SAN infrastruktūras. Atsiranda papildomi suderinamumo reikalavimai bei neigiamas poveikis į našumą orientuotiems duomenų perdavimo tinklams (maksimaliai plokščios architektūros, daugiau detalių pateikta skyriuje 7.1 Komunikacijos sluoksnio realizacija);
    b. Moduliniuose serveriuose esantys riboti PCIe jungčių kiekiai;
    c. Vertinant ilgalaikę perspektyvą bei tikimybę, kad skirtinguose projekto etapuose gali būti diegiama skirtingų gamintojų įranga, – būtent modulinių serverių atveju iškiltų atskirų fizinės įrangos telkinių apjungimo bei suderinamumo problemos. Rack tipo serveriai šiuo atveju yra standartiniai bei unifikuoti visų gamintojų kontekste.
2. Procesorius. Parenkant pagrindinius procesorius vertinta bendra keleto kriterijų įtaka:
    a. Procesoriaus techniniai parametrai – branduolių skaičius bei taktinis dažnis;
    b. Procesoriaus palaikomas atminties kiekis;
    c. MS Windows Server 2016 licenciniai kaštai (analizės etape nustatyta, kad virš 50% konsoliduojamų uždavinių veikia MS Windows Server pagrindu, likę uždaviniai veikia įvairių Linux distribucijų pagrindu (dalis su gamintojų palaikymu)). Licencijuojama per branduolį (komercinių Linux distribucijų atveju dažniausiai licencijuojama per procesorių (socket));
    d. Konsoliduojamų duomenų bazių valdymo sprendimų (Oracle DB, MS SQL) licenciniai apribojimai (licencijuojama daugeliu atveju per branduolį, žemesnio funkcionalumo lygio produktai – per procesorių (socket)).

    Analizei buvo naudojami pagrindinių procesorių gamintojų produktai (Intel Xeon Scalable Gold bei Platinum procesoriai, AMD EPIC procesoriai). Įvertinus pradinę

konsoliduojamų uždavinių imtį nustatyta, jog patvirtinama bendra praktika, kuomet ne CPU resursai, o atmintis yra ribojantis faktorius. Kadangi atminties kiekis nuo naudojamo procesoriaus to paties modelio serveryje iš esmės nepriklauso, naudoti procesorius su ypač dideliu branduolių skaičiumi (atitinkamai aukštesnė kaina) yra neracionalu.

Atsižvelgiant į anksčiau minėtas priežastis, nuspręsta naudoti 2 procesorių pagrindu komplektuojamus standartinius serverių modelius:

a. 18 branduolių, aukšto dažnio (3 ir daugiau GHz) procesorius serveriuose, skirtuose bendrinių uždavinių konsolidacijos platformai bei duomenų bazių valdymo ar kitai specifinei PĮ, licencijuojamai procesoriaus (socket) pagrindu.
b. 8 branduolių, aukšto dažnio (3 ir daugiau GHz) procesorius serveriuose, skirtuose duomenų bazių valdymo bei kitų uždavinių, licencijuojamų branduolio (core) pagrindu, konsolidacijai.

3. Atmintis. Kadangi konsolidacijos uždaviniuose dažniausiai pasitaikantis ribojantis faktorius yra serverio atminties kiekis, nuspręsta komplektuoti serverius su maksimalia, ekonomiškai pagrįsta konfigūracija. Šiuo metu tai 24 vnt. 64GB LRDIMM atminties konfigūracija, suteikianti ne mažiau nei 1536GB atminties per serverį. Šio tipo atminties (LRDIMM) naudojimas taip pat užtikrina, kad atminties posistemė išlaiko maksimalų darbinį dažnį net prie maksimalios konfigūracijos, kuomet visi atminties lizdai yra užpildyti.
4. IO plokštės. Visi serveriai privalo užtikrinti dubliuotą prijungimą prie duomenų centrų LAN ir SAN tinklų. Prijungimai dubliuojami PCIe jungčių (IO plokščių lygyje), todėl kiekviename serveryje diegiama ne mažiau kaip:
   a. 4 vnt. 25 GbE tinklo jungčių, veikiančių Mellanox ConnectX-4 Lx arba lygiaverčio procesoriaus pagrindu bei realizuotų ne mažiau kaip 2 atskirų tinklo plokščių pagalba. Atskiros tinklo plokštės reikalingos HA užtikrinimui vienos iš tinklo plokščių ar PCI jungties gedimo atveju;
   b. 2 vnt. 32 GB FC SAN jungčių, realizuotų 2 atskirų tinklo plokščių pagalba. Atskiros tinklo plokštės reikalingos HA užtikrinimui vienos iš tinklo plokščių ar PCI jungties gedimo atveju.

Remiantis šiais argumentais nuspręsta konsolidacijos platformas kurti 3 serverių tipų pagrindu:

- A tipo serveris – 2 CPU su 36 branduolių (3+ GHz), 1.5TB RAM, 2 x 32Gb FC HBA, 4x 25GbE LAN;
- B tipo serveris – 2 CPU su 16 branduolių (3+ GHz), 1.5TB RAM, 2 x 32Gb FC HBA, 4x 25GbE LAN;
- C tipo serveris – 2 CPU su 36 branduolių (3+ GHz), 512GB RAM, 2 x 32Gb FC HBA, 4x 25GbE LAN[3].

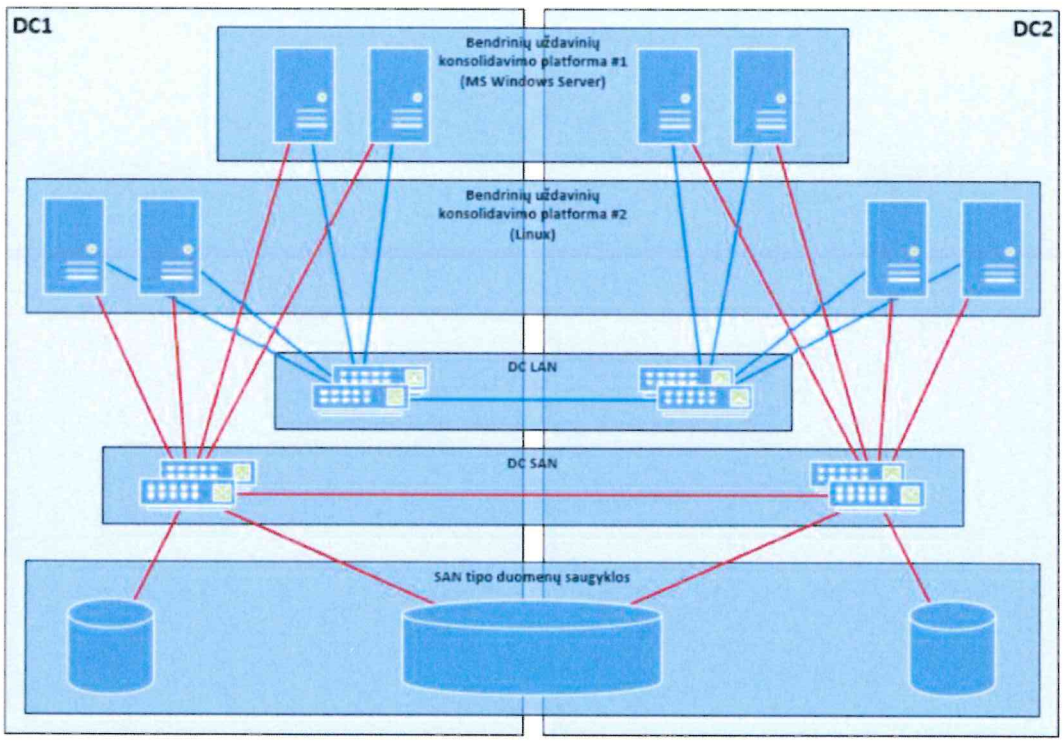
[3] Atsižvelgiant į SDN tinklo realizacijos specifiką gali būti naudojamos kitos konfigūracijos LAN tinklo adaptateriai (pvz. 4x10GbE, 2x100 GbE ar pan.).

6.1.2 Bendrinių uždavinių konsolidavimo platforma

Bendrinių uždavinių konsolidavimo platformai nuspręsta naudoti A tipo serverius. Jų pagrindu būtų formuojami virtualizacijos platformos serverių klasteriai. Siekiant efektyvaus OS licencijų panaudojimo bei paprastesnio valdymo, siūloma uždavinius, veikiančius MS Windows Server OS pagrindu, konsoliduoti viename klasteryje, o veikiančius Linux OS pagrindu – kitame. Priklausomai nuo naudojamų komercinių Linux distribucijų kiekio, licencijų valdymą galima atlikti virtualizacijos platformos priemonėmis arba suformuoti atskirą virtualizacijos platformos klasterį (esant dideliam konkrečios komercinės distribucijos paplitimui). Koncepcinė sprendimo schema pateikta (pav. 6-1 Bendrinių uždavinių konsolidavimo platformos principinė schema).

II projekto etape (2 DC Kaune) analogiška konfigūracija diegiama Kaune. Serverių kiekiai klasteriuose parenkami pagal migruotinų institucijų bei organizacijų poreikius.

Sprendimo plėtimas ateityje vykdomas papildomai įtraukiant serverius į atitinkamus klasterius.



pav. 6-1 Bendrinių uždavinių konsolidavimo platformos principinė schema

6.1.3 Oracle PĮ pagrindu veikiančių uždavinių konsolidavimo platforma[4]

Oracle PĮ pagrindu veikiantys uždaviniai gali būti klasifikuojami pagal produktų grupes bei licencijavimo principus. Šiai daliai siūlomos platformos turi būti izoliuotos nuo visų likusių (licenciniai Oracle reikalavimai) bei viena nuo kitos (licencijų panaudojimo optimizavimas).

Pradinės informacijos analizės metu išryškėjo poreikis 4 skirtingoms konsolidavimo platformoms:

1. Oracle DB Enterprise Edition PĮ pagrindu veikiantiems uždaviniams;
2. Oracle DB Standard Edition (2) PĮ pagrindu veikiantiems uždaviniams;
3. Oracle WebLogic PĮ pagrindu veikiantiems uždaviniams;
4. Kitos Oracle PĮ pagrindu veikiantiems uždaviniams.

6.1.3.1 Oracle DB Enterprise Edition uždaviniams skirta platforma

Oracle DB EE PĮ licencijuojama branduolių pagrindu, papildomas funkcionalumas bazinio produkto kainą gali ženkliai padidinti. Remiantis anksčiau įvardintu teiginiu, šią platformą realizuoti nuspręsta naudojant B tipo serverius (nedidelis aukšto dažnio branduolių kiekis minimizuoja Oracle PĮ licencinius kaštus bei minimizuoja neefektyvų resursų panaudojimą nepakankamos apkrovos atveju, o didelis atminties kiekis (GB/branduolį) paprastai teigiamai veikia duomenų bazių našumą).

Įvertinus analizės etape surinktą informaciją, I projekto etape nuspręsta naudoti 6 vnt. B tipo serverių, išskleistų per 2 DC klasterį (pav. 6-2 Oracle DB EE PĮ pagrindu veikiančių uždavinių konsolidavimo platforma). Visi naudojamų serverių procesorių branduoliai licencijuojami pagrindiniu Oracle DB EE PĮ bei papildomų komponentų paketu:

- Oracle Database Enterprise Edition
- Papildomi komponentai:
  - Oracle Active Data Guard;
  - Partitioning;
  - Diagnostic pack;
  - Tuning pack;
  - Database Lifecycle Management Pack;
  - Advanced Security.

Pagal Oracle licencijavimo taisykles, serveriai licencijuojami per fizinius branduolius. x86 architektūros procesorius naudojantiems serveriams taikomas 0,5 koeficientas. Platformoje bus naudojami 6 serveriai, kurių kiekvienas turės po 16 branduolių, todėl bendras platformos branduolių kiekis bus 96 vnt. Įvertinus Oracle taikomą 0,5 koeficientą gauname, kad pagal Oracle licencijavimo taisykles šiai platformai reikia 48 vnt. licencijų rinkinių.

[4] Siūloma architektūra suderinta su Oracle Lietuva atstovybe

Prieš migruojant sprendimus, kurie naudoja papildomus Oracle DB EE PĮ komponentus, rekomenduojama įvertinti jų naudojimo būtinumą. Esant galimybei rekomenduojama papildomų komponentų naudojimo atsisakyti. Jeigu jų atsisakyti nepavyksta, reikėtų įvertinti galimybę įsigyti papildomus komponentus visai platformai arba formuoti atskirą telkinį, kuris bus licencijuojamas reikiamais komponentais.

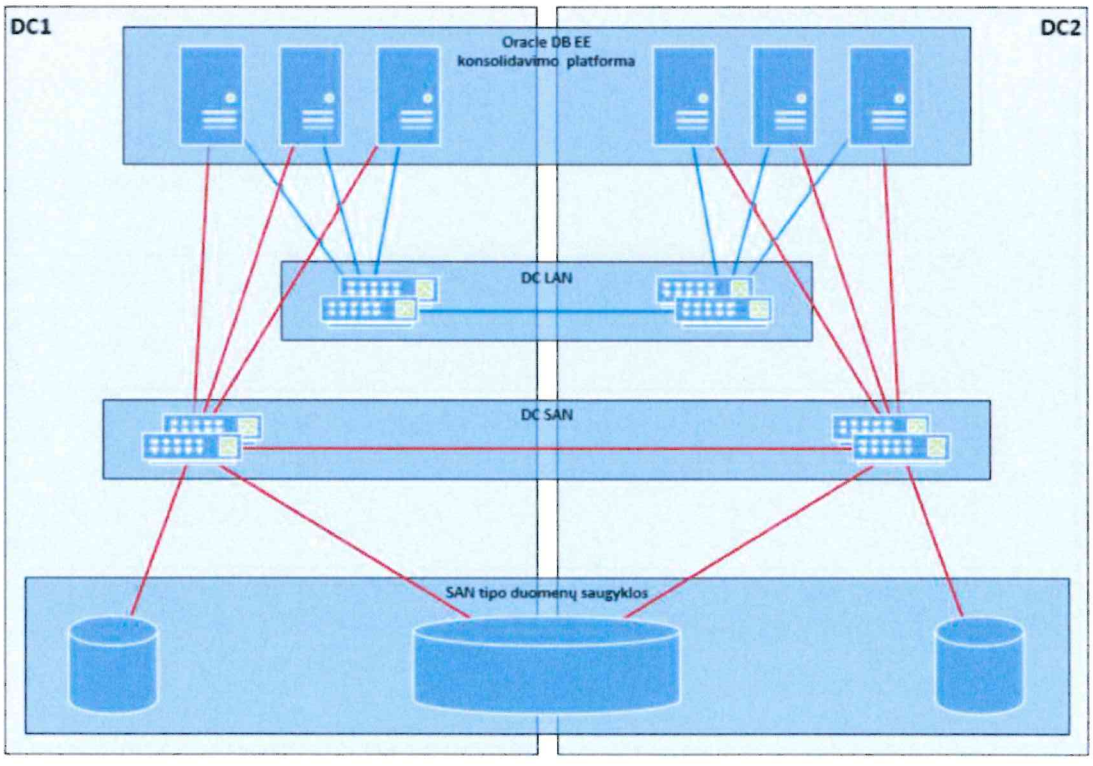
Duomenų saugojimo kontekste nuspręsta naudoti 2 tipų duomenų saugyklas:

1. Lokalias duomenų centro duomenų saugyklas;
2. Virtualizuotas (replikuotas per 2 duomenų centrus) duomenų saugyklas.

Oracle DB uždavinių pasiekiamumą rekomenduojama užtikrinti 2 būdais:

1. Pavieniams uždaviniams pasiekiamumas užtikrinamas platformos lygmenyje naudojant virtualizuotas duomenų saugyklas;
2. Uždaviniams, jau naudojantiems padidinto pasiekiamumo sprendimus (Oracle DG/ADG), pasiekiamumą būtų galima užtikrinti išlaikant esamą technologiją. Virtualūs serveriai būtų diegiami lokaliose duomenų saugyklose taip išlaikant nepriklausomus duomenų rinkinius, sinchronizaciją tarp jų paliekant Oracle technologijų kontrolėje.

Naudoti Oracle RAC sprendimų nerekomenduojama, nes jiems yra reikalingas papildomas prieigos lygis prie duomenų saugyklų, kas apsunkintų platformos ir sprendimų administravimą.



pav. 6-2 Oracle DB EE PĮ pagrindu veikiančių uždavinių konsolidavimo platforma

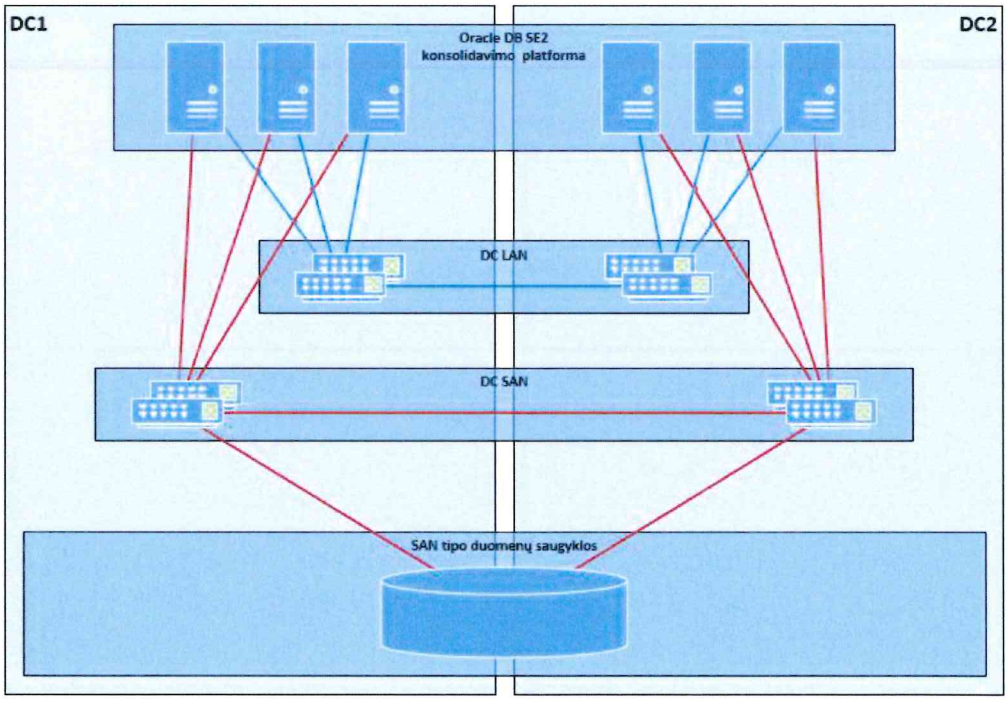
II projekto etape (2 DC Kaune), analogiška konfigūracija diegiama Kaune. Serverių kiekiai klasteriuose parenkami pagal migruotinų institucijų bei organizacijų poreikius.

Sprendimo plėtimas tolimesniuose projekto etapuose būtų atliekamas prijungiant prie esamų klasterių papildomus B tipo serverius bei papildomai įsigyjant licencijų paketą pridedamų branduolių kiekiui.

6.1.3.2 Oracle DB Standard Edition uždaviniams skirta platforma

Oracle DB Standard Edition 2 PĮ licencijuojama procesoriaus lizdo (socket) pagrindu. Taip pat egzistuoja papildomi apribojimai – fizinis serveris negali turėti daugiau nei 2 procesorius bei Oracle DB uždavinys negali naudoti daugiau nei 16 branduolių. Tačiau konsolidacijos kontekste tai nedraudžia naudoti procesorių su didesniu branduolių skaičiumi. Remiantis tuo, šią platformą realizuoti nuspręsta naudojant A tipo serverius (didesnis aukšto dažnio branduolių kiekis minimizuoja Oracle PĮ licencinius kaštus bei leidžia pasiekti aukštesnį konsolidacijos lygį (šią PĮ versija naudojantys sprendimai dažniausiai nėra didelės apimties)).

Įvertinus analizės etape surinktą informaciją, I projekto etape nuspręsta naudoti 6 serverių, išskleistų per 2 DC, klasterį (pav. 6-3 Oracle DB SE2 PĮ pagrindu veikiančių uždavinių konsolidavimo platforma). Visi naudojamų serverių procesorių lizdai dengiami Oracle DB SE2 licencijomis.



pav. 6-3 Oracle DB SE2 PĮ pagrindu veikiančių uždavinių konsolidavimo platforma

Duomenų saugojimui nuspręsta naudoti virtualizuotas (replikuotas per 2 duomenų centrus) duomenų saugyklas.

Šio tipo PĮ naudojantiems duomenų bazių valdymo uždaviniams pasiekiamumas būtų užtikrinamas platformos lygmenyje. DB sistemos turėtų būti konfigūruojamos kaip pavieniai virtualūs serveriai. Oracle RAC technologijos naudoti nerekomenduojame dėl papildomų prieigos prie duomenų saugyklos reikalavimų, kas apsunkintų platformos ir sprendimų administravimą. Jei sprendimui reikalingas aukštesnis pasiekiamumo lygis, rekomenduojama svarstyti jo perkėlimą į Oracle DB Enterprise Edition uždaviniams skirtą platformą.

II projekto etape (2 DC Kaune) analogiška konfigūracija diegiama Kaune. Serverių kiekiai klasteriuose parenkami pagal migruotinų institucijų bei organizacijų poreikius.

Platformos plėtimas tolimesniuose projekto etapuose būtų atliekamas į atitinkamus klasterius įtraukiant papildomus A tipo serverius bei įsigyjant papildomas Oracle DB SE2 licencijas.

6.1.3.3 Oracle WebLogic Suite bei Oracle SOA Suite for Oracle Middleware uždaviniams skirta platforma

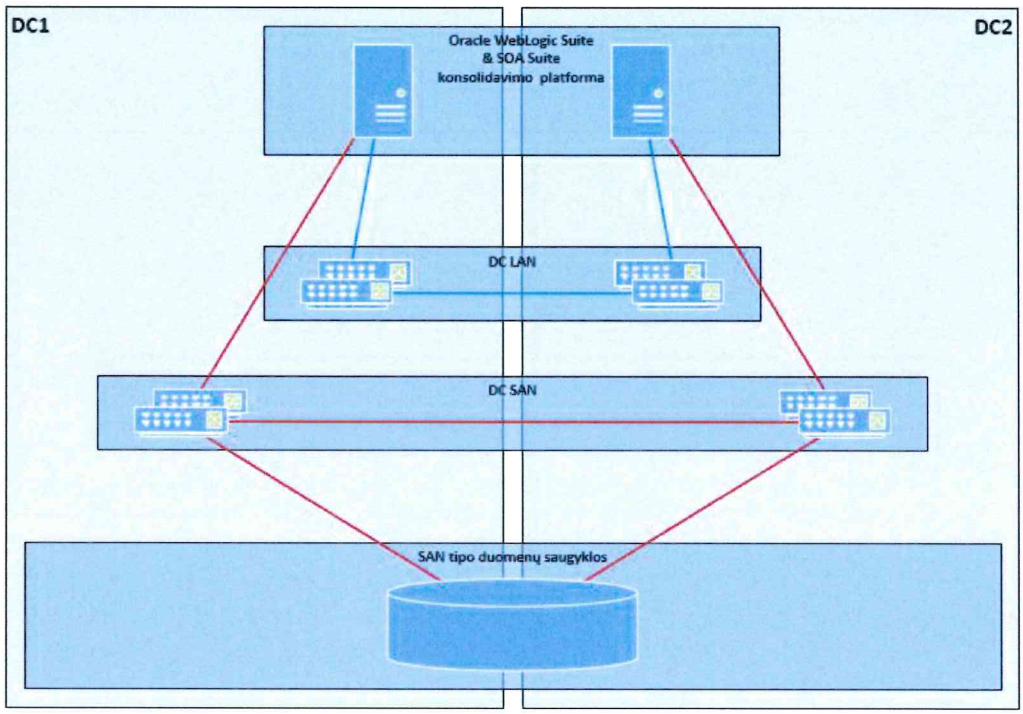
Iš pradinei analizei pateiktų duomenų matyti, kad iš Oracle Middleware produktų grupės galima išskirti Oracle WebLogic Suite bei Oracle SOA Suite for Oracle Middleware, kurių pagrindu veikiantys sprendimai yra naudojami ne vienoje valstybės institucijoje ar organizacijoje. Būtent šių PĮ paketų kombinaciją siūloma naudoti kaip atskirą konsolidacijos platformą, siekiant optimizuoti PĮ licencijavimo kaštus bei sistemų utilizaciją. Šie paketai yra licencijuojami procesoriaus branduolio lygmenyje.

Įvertinus analizės etape surinktą informaciją, I projekto etape nuspręsta naudoti 2 vnt. B tipo serverių, išskleistų per 2 DC klasterį (pav. 6-4 Oracle WebLogic Suite bei Oracle SOA Suite for Oracle Middleware PĮ pagrindu veikiančių uždavinių konsolidavimo platforma). Visi naudojamų serverių procesorių branduoliai licencijuojami pagrindiniu Oracle WebLogic Suite bei Oracle SOA Suite for Oracle Middleware licencijomis.

2 vnt. B tipo serverių atveju būtų reikalinga 16 licencijų komplektų (2 serveriai su 16 branduolių kiekvienas, 0.5 licencijų faktorius x86 serverių atveju).

Duomenų saugojimui yra nuspręsta naudoti virtualizuotas (replikuotas per 2 duomenų centrus) duomenų saugyklas.

Šio tipo PĮ naudojantiems uždaviniams pasiekiamumas būtų užtikrinamas platformos lygmenyje. Aplikacijų serveriai turėtų būti konfigūruojami kaip pavieniai virtualūs serveriai. Esant poreikiui gali būti naudojamos kitos priemonės (pvz. srauto balansavimo įrenginiai ir pan.) tam, kad būtų pakeltas virtualių serverių teikiamų paslaugų pasiekiamumo lygis.



pav. 6-4 Oracle WebLogic Suite bei Oracle SOA Suite for Oracle Middleware PĮ pagrindu veikiančių uždavinių konsolidavimo platforma

II projekto etape (2 DC Kaune) analogiška konfigūracija diegiama Kaune. Serverių kiekiai klasteriuose parenkami pagal migruotinų institucijų bei organizacijų poreikius.

Plėtimas tolimesniuose projekto etapuose būtų atliekamas plečiant klasterį B tipo serveriais bei papildomai įsigyjant licencijų komplektą naujų procesoriaus branduolių kiekiui.

Taip pat tolimesniuose projekto etapuose gali atsirasti ekonominis pagrindimas atskirai įdiegti tik Oracle WebLogic Suite licencijomis dengtą platformą.

6.1.3.4 Kitos Oracle PĮ pagrindu veikiantiems uždaviniams skirta platforma

Ne visi Oracle PĮ pagrindu veikiantys ir šiuo metu valstybės institucijų bei organizacijų naudojami IT sprendimai gali būti sumigruoti į aukščiau aprašytas platformas. Tam gali būti kelios priežastys:

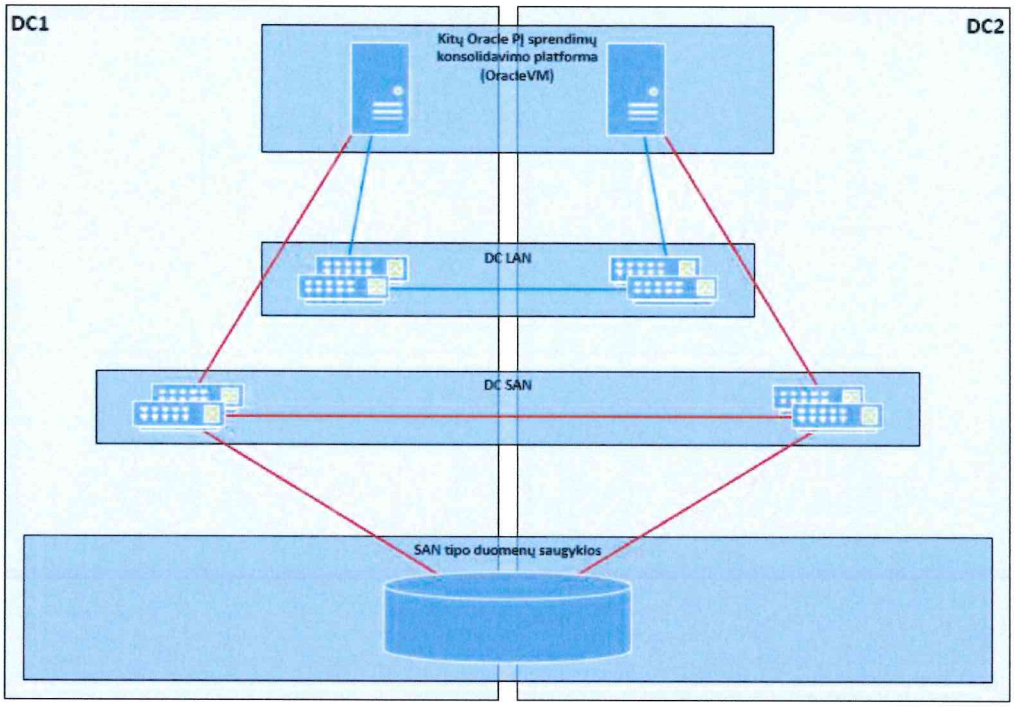
- Naudojami kiti Oracle produktai, netinkami konsoliduotoms platformoms;
- Naudojama konsolidacijai tinkančių produktų netinkama privalomų komponentų kombinacija (licenciniai sąryšiai tarp Oracle produktų gali būti labai sudėtingi);
- Per maži licencijų kiekiai atskiros produktų grupės konsolidacijos platformos kūrimui.

Tokių sprendimų konsolidavimui siūlomas OracleVM pagrindu veikiantis konsolidacijos sprendimas. OracleVM pasirinktas kaip vienintelė Oracle pripažįstama platforma, leidžianti sumažinti licencinius kaštus (licencijuoti reikia tik konkrečiam Oracle produktui išskiriamus procesoriaus resursus (lizdus / branduolius), o ne visus fiziniame serveryje esančius).

Technologiniai šio spendimo apribojimai, atsirandantys siekiant minimizuoti Oracle PĮ licencinius kaštus:

- Privalomas procesoriaus branduolių priskyrimas konkrečiam uždaviniui (angl. Core locking / pinning).
- Draudžiama naudoti platformos lygio padidinto pasiekiamumo technologijas (DRS, HA, DPM), t.y.: virtualus serveris tampa „pririštu“ prie fizinio serverio. Padidinto pasiekiamumo sprendimai galimi tik aplikacijos lygmenyje.

Įvertinus analizės etape surinktą informaciją, I projekto etape yra nuspręsta naudoti 2 vnt. A tipo serverių, išskleistų per 2 DC klasterį (pav. 6-5 Kitų Oracle PĮ pagrindu veikiančių uždavinių konsolidavimo platforma). Visi naudojamų serverių procesorių lizdai (socket) dengiami Oracle VM licencijomis. Platformoje leidžiamų uždavinių Oracle PĮ licencijos perkamos / perkeliamos diegimo / migracijos metu.



pav. 6-5 Kitų Oracle PĮ pagrindu veikiančių uždavinių konsolidavimo platforma

Duomenų saugojimui nuspręsta naudoti virtualizuotas (replikuotas per 2 duomenų centrus) duomenų saugyklas.

II projekto etape (2 DC Kaune) analogiška konfigūracija diegiama Kaune. Serverių kiekiai klasteriuose parenkami pagal migruotinų institucijų bei organizacijų poreikius.

Plėtimas tolimesniuose projekto etapuose būtų atliekamas plečiant klasterį A tipo serveriais bei papildomai įsigyjant Oracle VM licencijas.

6.1.4 MS SQL Server PĮ pagrindu veikiančių uždavinių konsolidavimo platforma

Microsoft pateikia keletą MS SQL Server versijų (editions) su skirtingomis licencijavimo taisyklėmis. MS SQL Server Enterprise Edition (licencijavimo pagrindas – serverio procesoriaus branduoliai) komplektuojama su naujumo garantijos teise (Software Assurance) suteikia teisę naudoti neribotą virtualių serverių kiekį licencijuotoje platformoje (licencijuojami visi fizinio serverio procesoriaus branduoliai). Taip pat ši versija suteikia teisę

naudotis visomis padidinto serviso pasiekiamumo bei našumo optimizavimo galimybėmis. Būtent šios versijos pagrindu kuriama konsolidavimo platforma.

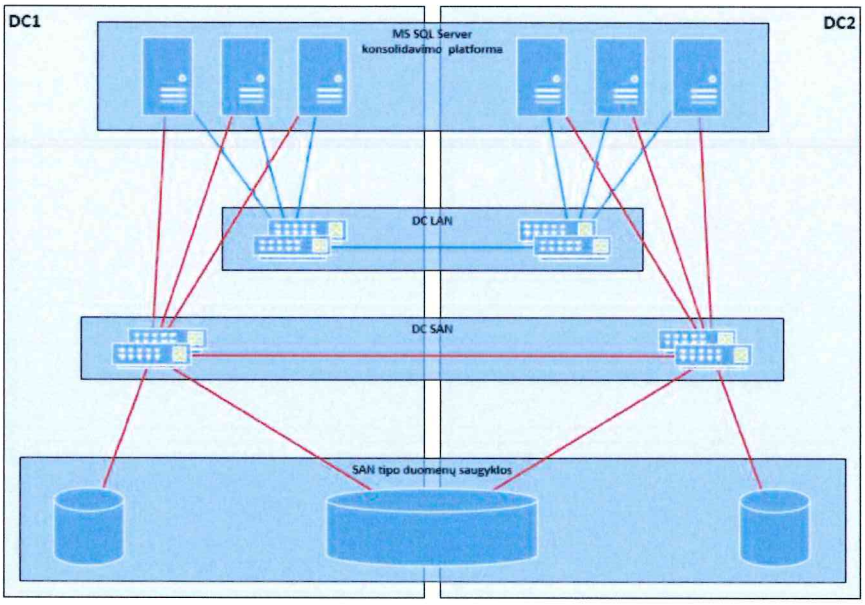
Įvertinus analizės etape surinktą informaciją, I projekto etape siūloma naudoti 6 vnt. B tipo serverių, išskleistų per 2 DC klasterį (pav. 6-6 MS SQL Server PĮ pagrindu veikiančių uždavinių konsolidavimo platforma). Visi naudojamų serverių procesorių branduoliai dengiami MS SQL Server Enterprise Edition licencijomis su naujumo garantijos teise.

Duomenų saugojimui siūlome naudoti 2 variantus:

1. Pavieniams virtualiems serveriams, kuriems padidintas pasiekiamumas užtikrinamas platformos lygmenyje, naudoti virtualizuotas saugyklas;
2. Sprendimams, naudojantiems MS SQL serverio padidinto pasiekiamumo technologijas (Always - On, Log shipping ir pan.), siūlome naudoti lokalias duomenų centro saugyklas (2 nepriklausomi duomenų komplektai).

II projekto etape (2 DC Kaune) analogiška konfigūracija diegiama Kaune. Serverių kiekiai klasteriuose parenkami pagal migruotinų institucijų bei organizacijų poreikius.

Sprendimo plėtimas tolimesniuose projekto etapuose būtų atliekamas prijungiant prie esamų klasterių papildomus B tipo serverius bei papildomai įsigyjant licencijas pridedamų branduolių kiekiui.



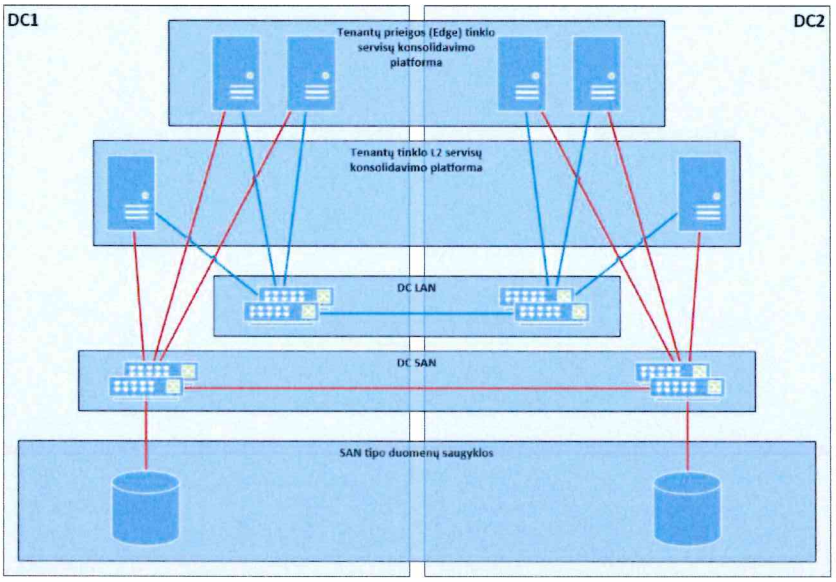
pav. 6-6 MS SQL Server PĮ pagrindu veikiančių uždavinių konsolidavimo platforma

6.1.5 Tinklo paslaugų konsolidavimo platforma

Remiantis duomenų centrų LAN tinklo dizainu, aprašytu skyriuje 7.1.3 LAN fizinės bei loginės tinklo topologijos architektūros modelis, yra kuriamos 2 tenantams skirtos tinklo paslaugų konsolidavimo platformos (pav. 6-7 Tenantų tinklo servisų konsolidacijos platformos):

1. Tenantų prieigos (edge) tinklo paslaugų konsolidavimo platforma skirta prieigos zonoje esančioms paslaugoms (prieigos maršrutizatoriai (edge routers), srautų balansavimo įrenginiai, perimetro ugniasienės) teikti. Platforma realizuojama 4 serverių telkinio, išskleisto per 2 duomenų centrus pagrindu, bei užtikrina paslaugų pasiekiamumą duomenų centro lygyje. Esant poreikiui užtikrinti padidintą paslaugų pasiekiamumą tarp duomenų centrų, šios paslaugos turėtų būti realizuotos panaudojant išskleistos architektūros (multiinstance) bei aplikacijos lygio padidinto pasiekiamumo principus. Duomenų saugojimui naudojamos lokalios duomenų centrų saugyklos.

2. Tenantų tinklo L2 paslaugų konsolidavimo platforma skirta virtualiems paslaugų serveriams, atsakingiems už sprendime naudojamų virtualių tinklų bei tenantų naudojamų fizinių tinklų sujungimą (L2 bridging). Platforma realizuojama dviejų serverių telkinio, išskleisto per 2 duomenų centrus, pagrindu. Tenantų paslaugų pasiekiamumas užtikrinamas aplikacijos lygmenyje (paslaugos tiekimui naudojami 2 virtualių serverių komplektai). Duomenų saugojimui naudojamos lokalios duomenų centrų saugyklos.



pav. 6-7 Tenantų tinklo servisų konsolidacijos platformos

Tolimesniuose projekto etapuose analogiška konfigūracija diegiama Kauno duomenų centruose. Taip pat, esant poreikiui, atitinkami klasteriai plečiami į juos įtraukiant naujas paslaugas.

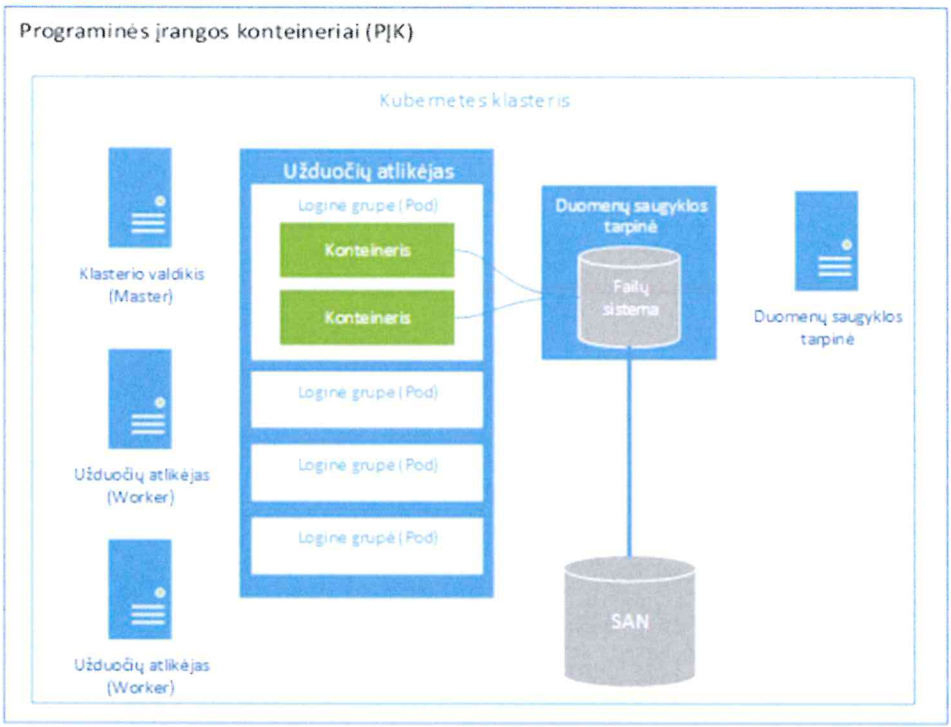
6.1.6 Konteinerių technologijų konsolidavimo platforma

Poreikių analizės metu buvo išreikštas poreikis suprojektuoti konteinerizuotai programinei įrangai tinkamą platformą, todėl bendroje platformos architektūroje šio reikalavimo įgyvendinimas yra numatytas.

Lyginant su tradicine virtualizacija, programinės įrangos konteinerizacija turi akivaizdų pranašumą tais atvejais, kai konteinerizuojama programinė įranga yra pritaikyta veikti konteineriuose, taikoma mikropaslaugų architektūra. Nepaisant to, atkreipiamas dėmesys, kad šiuo metu, dėl technologijos naujumo, produkcinėse aplinkose esančių diegimų skaičius yra vis dar pakankamai mažas. Kita vertus, yra pagrindo manyti, jog tokio tipo programinės įrangos kiekis ateityje didės [1,2,3].

1. Gartner, Four Key Container Deployment Considerations for I&O Leaders. https://www.gartner.com/doc/reprints?id=1-51KVQ88&ct=180531&st=sb
2. Diamanti, 2018 CONTAINER ADOPTION BENCHMARK SURVEY. https://diamanti.com/wp-content/uploads/2018/07/WP_Diamanti_End-User_Survey_072818.pdf
3. Pivotal Software, Inc. , What are Cloud - Native Applications? https://pivotal.io/cloud-native

Debesijos paslaugų teikimo platformoje rekomenduojama realizuoti Kubernetes ir Docker technologijomis grįstą programinės įrangos konteinerių (toliau – PĮK) sprendimą, kuris būtų integruotas į bendrą platformą ir naudotų bendras išteklių, valdymo, autentifikacijos bei autorizacijos priemones. Manoma, kad pradiniame etape PĮK gali būti realizuojami naudojant virtualias mašinas. Tačiau didėjant PĮK poreikiui, tolimesniuose etapuose produkcinėje aplinkoje veikiančius PĮK būtų prasminga perkelti į šiai funkcijai dedikuotus fizinius serverius.



pav. 6-8 Programinės įrangos konteinerių Kubernetes principinė veikimo schema

Tradicinį Kubernetes konteinerių telkinį sudaro kelios rolės: telkinio valdiklis (master), užduočių atlikėjas (worker) ir duomenų saugyklos tarpinė:

- Telkinio valdiklis suteikia priemones valdyti PĮK telkinį – stebi veikiančių konteinerių būseną, paleidžia ar sustabdo konteinerius užduočių atlikėjuose, plečia ar sutraukia nurodytos aplikacijos replikas ir pan.;

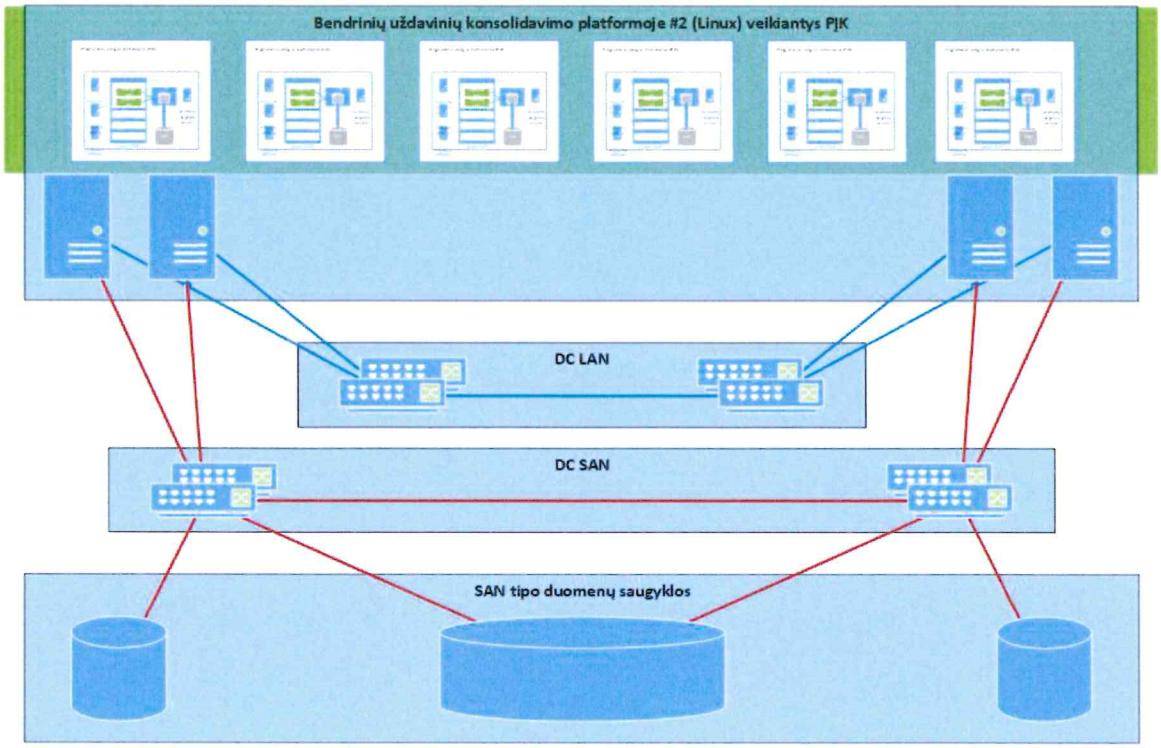
- Užduočių atlikėjo rolė atlieka konteinerių vykdymo funkciją. Atkreipiamas dėmesys, kad konteineriai gali būti grupuojami į logines grupes, kurios yra skirtos apjungti konteinerius, atliekančius panašias užduotis, kurios yra vienos funkcinės paslaugos dalis (pvz., duomenų bazė, internetinės vartotojo prieigos portalas ir pan.) ar turi dalintis bendrais ištekliais (pvz., nutolusia duomenų saugykla);
- Duomenų saugyklos tarpinė PĮK suteikia prieigą prie nutolusios duomenų saugyklos per failų sistemos protokolus (pvz., NFS, GlusterFS) kaupiamiems duomenims saugoti. Ši rolė būtina norint užtikrinti, kad būtų išsaugomi duomenys nepriklausomai nuo PĮK gyvavimo ciklo.

Kubernetes PĮK klasterių architektūra, technologinio realizavimo aprašas ir administravimo bei konfigūravimo gairės šiame dokumente nėra pateikiamos. Dokumente pateikiama bendriniai Kubernetes PĮK aspektai, galiojantys visoms Kubernetes distribucijoms ir nėra specifiniai šiam konkrečiam projektui. Detaliau apie PĮK: https://kubernetes.io/docs/concepts/.

Debesijos paslaugų teikimo platformos paslaugomis besinaudojančios organizacijos galės PĮK klasterius diegti bei valdyti nepriklausomai nuo kitų platformą naudojančių organizacijų, t.y. bus išlaikomas resursų izoliacijos ir nepriklausomo valdymo principas.

PĮK funkcionalumas turi būti realizuotas taip, kad konteinerių naudojami skaičiavimo, duomenų saugyklų bei tinklo ištekliai būtų integruoti į bendrą virtualaus duomenų centro išteklių telkinį. Atsižvelgiant į tai, kad Kubernetes klasteriuose veikiantys Docker technologijos konteineriai vykdomi išimtinai tik Linux OS, PĮK klasteriai projektuojami veikti Bendrinių uždavinių konsolidavimo platformoje #2 (Linux) (pav. 6-9 Programinės įrangos konteinerių principinė realizavimo schema bendroje platformoje).

Atkreipiamas dėmesys į tai, kad augant platformoje eksploatuojamų PĮK kiekiui (daugiau nei 500), esant sudėtingesnių tinklo funkcionalumo sprendimų poreikiui, siekiant standartizuoto PĮK naudojimo ir gyvavimo ciklo valdymo (įskaitant ir PĮK veikiančios programinės įrangos diegimo ir atnaujinimo būdus) standartinis Kubernetes technologijos funkcionalumas gali būti nepakankamas. Minėti uždaviniai sprendžiami naudojant Kubernetes distribucijas, kurios turi specializuotas funkcijas minėtiems uždaviniams spręsti. Šiuo metu dominuoja Red Hat OpenShift ir Pivotal CloudFoundry platformos.



pav. 6-9 Programinės įrangos konteinerių principinė realizavimo schema bendroje platformoje

Realizuojant PĮK sprendimą turi būti numatyta integracija su PĮK šablonų šaltiniais ir galimybė paleisti konteinerius naudojant šiuos šablonus.

Pažymima, kad PĮK klasteriai turi išlaikyti debesijos paslaugų teikimo platformos paslaugų gavėjų virtualių duomenų centrų nepriklausomumo principą, t. y., kiekvienas platformos paslaugų gavėjas gali laisvai ir nepriklausomai nuo kitų paslaugų gavėjų diegti ir eksploatuoti PĮK klasterius. Tokių klasterių diegimas ir valdymas turi būti įmanomas trimis būdais:

Prieigos būdas	**Paskirtis**
Grafinė vartotojo sąsaja (GUI)	Interaktyvi, per interneto naršyklę realizuojama prieiga PĮK platformos ar joje esančių išteklių valdymui.
Komandinės eilutės klientas (CLI)	PĮK platformos ar joje esančių išteklių valdymas naudojant pagalbines programėles (skriptus) ar vartotojui vykdant užklausas iš komandinės eilutės.
API (REST arba SOAP)	PĮK platformos integracijai su monitoringo, automatizavimo ar kitos paskirties sistemomis.

Taip pat būtina užtikrinti PĮK platformos vartotojų privilegijų kontrolę taikant prieigos kontrolės mechanizmus, suteikiant vartotojams skirtingas roles, priklausomai nuo jų atliekamų užduočių:

Prieigos rolė	**Paskirtis**
PĮK platformos administratorius (super administrator)	Ši rolė atlieka visos PĮK išteklių platformos diegimą, administravimą ir kitą bendros platformos valdymą.

Debesijos paslaugų teikimo platformos paslaugų gavėjo administratoriaus rolė (tenant administrator)	Ši rolė atlieka konkretaus debesijos paslaugų teikimo platformos paslaugų gavėjo PĮK klasterių diegimą, administravimą bei kitokį valdymą.
PĮK klasterio vartotojas (tenant user)	Ši rolė naudoja PĮK klasterio išteklius per Kubernetes API ir/ar kubectl komandinės eilutės klientą.

Atkreipiamas dėmesys, kad PĮK telkinių naudojimas eksploatuojant programinę įrangą skiriasi nuo tradicinių būdų tai darant fiziniuose arba virtualiuose serveriuose, todėl rekomenduojama, kad taikoma PĮK veikiančios programinės įrangos gyvavimo ciklo politika būtų suderinama su PĮK specifika ir būtų atsižvelgiama į šios technologijos privalumus, tačiau taip pat būtų įvertinti ir skirtumai lyginant su tradiciniais ir nusistovėjusiais programinės įrangos sprendimų, platformų ir sistemų eksploatavimo būdais.

Rekomenduojame, kad pokyčiai, diegiami informacinėse sistemose ar platformose, naudojant PĮK, taikytų pažangius programinės įrangos diegimo ir atnaujinimo būdus, kurie leidžia pasiekti aukštą sistemų pasiekiamumą ir patikimumą, bei leistų pokyčius realizuoti prognozuojamu ir saugiu būdu. Šiuo metu dažniausiai yra naudojami trys PĮK veikiančios programinės įrangos diegimo ir atnaujinimo būdai, apibūdinami lentelėje žemiau.

Diegimo ir atnaujinimo būdas	**Aprašymas**
Green - blue	Šis būdas realizuojamas turint dvi identiškas aplinkas, kurių viena yra vadinama „žalia“ (angl. green), o kita – „mėlyna“ (angl. blue). Kreipiniai į sistemą yra aptarnaujami arba žalios, arba mėlynos aplinkos, o tai, kuri aplinka aptarnauja užklausas, valdoma tinklo apkrovos balansavimo priemonėmis (angl. load balancer). Taikant šį būdą, pakeitimai diegiami aplinkoje, kuri tuo metu užklausų neaptarnauja ir, įsitikinus, kad pakeitimai įdiegti sėkmingai ir veikia korektiškai, visi kreipiniai peradresuojami iš aktyvios aptarnaujančios aplinkos į tą, kurioje buvo ką tik sudiegti pakeitimai. Didžiausias šio būdo privalumas – nulinė prastova, tačiau jis reikalauja dvigubai daugiau resursų ir perjungimo metu bus neišvengiamai prarastos jau veikiančios sesijos į aktyvią aplinką. Vis dėlto, eksploatuojant kritines sistemas šis būdas yra taikomas dažniausiai.
Canary	Šis būdas pasižymi tuo, kad pakeitimai diegiami pamažu, ribota apimtimi ir yra pasiekiami tik ribotam vartotojų skaičiui. Įsitikinus, kad pakeitimai veikia korektiškai, jų diegimo intensyvumas yra didinamas, diegiant jį vis didesniame veikiančių PĮK kiekyje. Šio būdo privalumas yra tai, kad pakeitimai ir jų poveikis realioje, produkcinėje aplinkoje yra pamatomas iš karto, tačiau riboto vartotojų skaičiaus, tokiu būdu sumažinant neigiamų pasekmių riziką. Kita vertus, šis būdas reikalauja nemažai kontrolės mechanizmų ir gali būti netinkamas kritinėms sistemoms eksploatuoti.
Rolling	Šis būdas yra panašus į Canary būdą, tačiau skirtumas yra tas, kad funkcionalumas diegiamas į naujus konteinerius, pamažu užkeičiančius senuosius, kurie yra išjungiami ir vėliau pašalinami. Taigi, naujai įdiegtas funkcionalumas ar kiti pakeitimai tampa prieinami visiems vartotojams, kurių užklausos būna aptarnaujamos naujų konteinerių. Šis būdas yra labai efektyvus, gali būti tinkamas kritinėms sistemoms eksploatuoti, tačiau būtina užtikrinti labai aiškiai apibrėžtą ir parametrizuotą kokybės kontrolę, kuria remiantis būtų priimami sprendimai kada naujai įdiegti konteineriai taptų prieinami vartotojams.

Papildomai pažymima, kad PĮK naudojimas dažnai taikomas su pažangiais, moderniais ir automatizuotais tęstinės integracijos / tęstinio diegimo, TI/TD (angl. continuous integration / continuous delivery, CI/CD) metodais bei priemonėmis, kurių parinkimas negali būti universalus, t. y., TI/TD metodai ir taikomos technologinės priemonės bei įrankiai priklauso nuo konkretaus produkto, paslaugos, sistemos ar platformos realizacijos, veikimo, eksploatavimo ir naudojimo specifikos, vidinių organizacijos ir su ja susijusių asmenų (pvz., rangovų) veiklos procesų.

Projektuojant ir diegiant informacines sistemas, programinės įrangos komponentus, svarbu įvertinti jų eksploatacijos, aptarnavimo specifiką, tinkamus sprendimus rezerviniam kopijavimui, įvykių žurnalų kaupimui ir t.t. .

Rezervinis kopijavimas ir atstatymas Kubernetes kontekste yra realizuojamas atliekant PĮK klasterio konfigūracijos, jame veikiančių konteinerių ir konteineriams pateiktų duomenų saugyklų išteklių (angl. persistent volumes) rezervinį kopijavimą ir atstatymą. Rezervinė kopija turi apimti tokius PĮK klasterio elementus: etcd duomenis, API objektus, konteinerių registrą ir konteinerinius loginius diskus (angl. volumes) bei juose esančius duomenis.

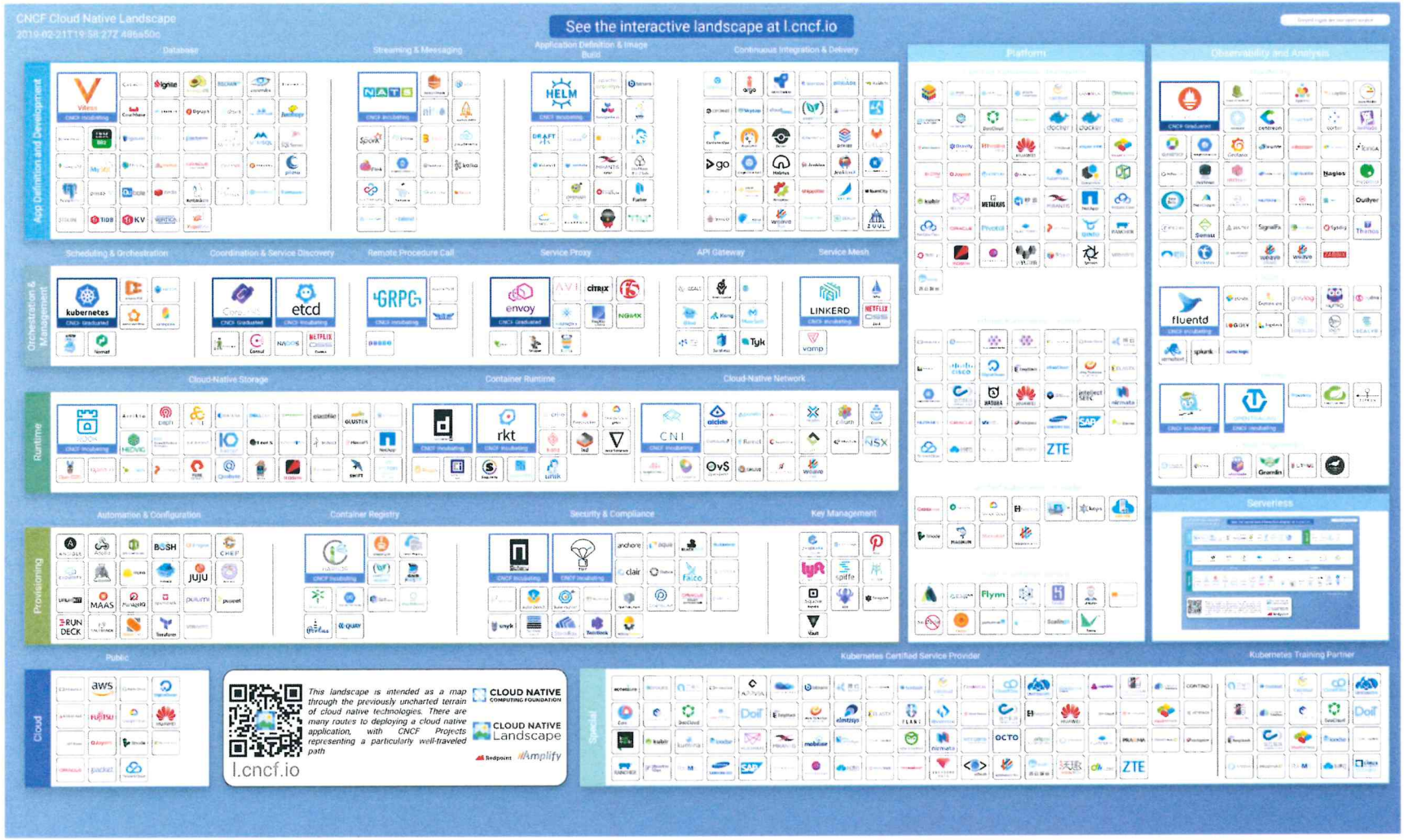
Dažniausiai rezervinio kopijavimo ir atstatymo užduotys PĮK kontekste yra atliekamos į Kubernetes distribuciją (Red Hat OpenShift, Rancher, Pivotal CloudFoundry ir kt.) integruotomis priemonėmis. Jeigu Kubernetes distribucija nėra naudojama arba jeigu ji neturi integruotų rezervinio kopijavimo priemonių, turi būti naudojami specialiai paruošti ir pritaikyti skriptai arba trečiųjų šalių pateikiama specializuota programinė įranga, skirta PĮK rezerviniam kopijavimui, tokia kaip Heptio Velero, anksčiau žinoma Ark pavadinimu (https://github.com/heptio/velero), kuri užtikrina PĮK ir susijusių elementų rezervinį kopijavimą, gali migruoti PĮK tarp skirtingų klasterių, replikuoti PĮK aplinkas viena į kitą (pvz., produkcinę aplinką į vystymo, testavimo ar DR).

Informacinių sistemų, programinės įrangos įvykių žurnalų kaupimas yra svarbi programinės įrangos sudedamoji funkcinė dalis, kuri turi būti numatoma projektavimo, kūrimo etapuose. Realizacija tokio funkcionalumo dažniausiai nesiskiria ar programinė įranga veiks fizinėje aplinkoje (pvz. tarnybinėje stotyje), ar virtualioje (pvz. virtualioje mašinoje, programinės įrangos konteineryje). Pavyzdžiui, duomenų bazių valdymo sistema fizinėje ar virtualioje / konteinerių aplinkoje gali įvykius fiksuoti failų sistemoje arba siųsti į kitą specializuotą nuotolinę žurnalų valdymo sistemą. Pastebima, kad debesijos technologijų vystymo bendruomenė teikia rekomendacijas žurnalizavimo principams (pvz. pateiktas nuorodoje https://kubernetes.io/docs/concepts/cluster-administration/logging) ir moderniems papildomiems įrankiams (pvz.: Prometheus, fluentd ir t.t., naujausia versija prieinama žiniatinklio adresu https://raw.githubusercontent.com/cncf/trailmap/master/CNCF_TrailMap_latest.png).

Technologijų, kurios laikomos tikrąja debesijoje veikiančia programine įranga, matrica yra pateikiama žemiau (pav. 6-10 Modernių debesijos technologijų, technologinių priemonių

žemėlapis). Naujausia šios matricos versija yra prieinama šiuo žiniatinklio adresu: https://landscape.cncf.io/

Analitinė kompanija Gartner pateikia gaires, rekomendacijas ir praktines įžvalgas, kurios gali būti naudingos debesijos paslaugų teikimo platformos operatoriui ir šios platformos naudotojams pasirenkant TI/TD, technologinius sprendimus ir priemones bei integruojant šią metodiką veiklos procesuose (licencijuojamas turinys): https://www.gartner.com/doc/3857563/guidance-framework-continuous-integration-continuous



pav. 6-10 Modernių debesijos technologijų, technologinių priemonių žemėlapis

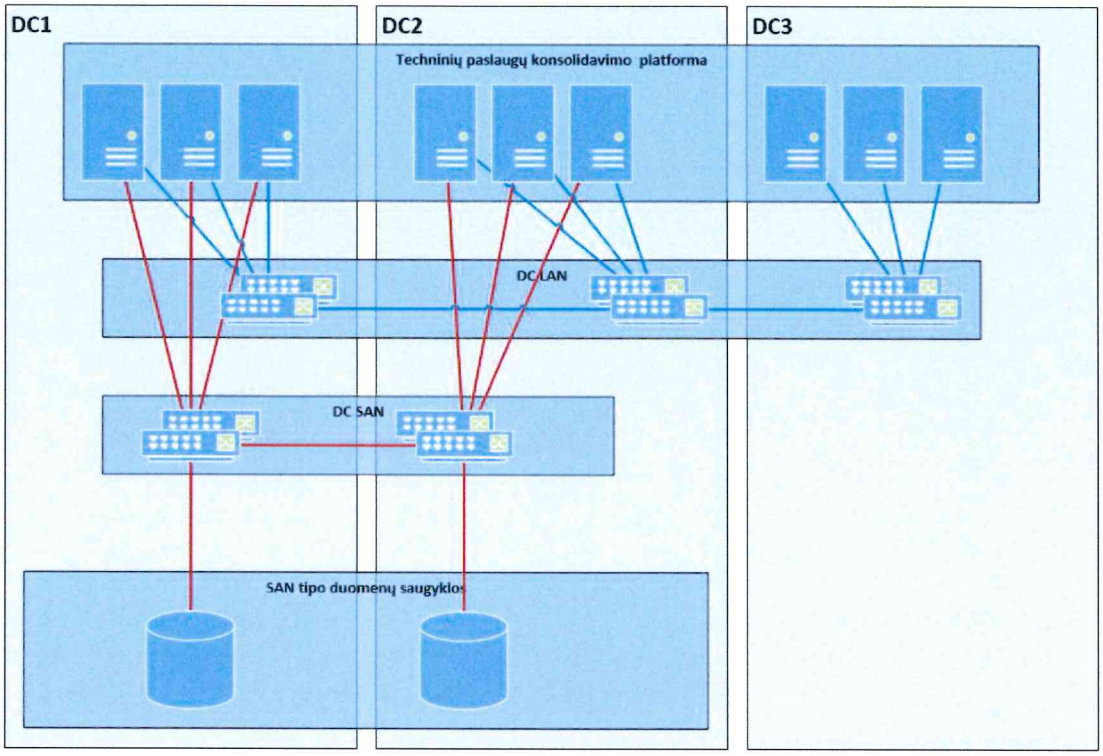
6.1.7 Technologinių paslaugų konsolidavimo platforma

Ši platforma yra skirta įvairių technologinių servisų bei valdymo komponentų diegimui. Platformoje bus diegiama serverių ir tinklo virtualizacijos platformos valdymo komponentai, tinklo virtualizacijos valdymo komponentai, rezervinio kopijavimo infrastruktūros serveriai, įvairūs saugumo sprendimų komponentai ir pan.,- t. y.,- visi servisai reikalingi užtikrinti korektiškam sprendimo veikimui.

I projekto etape diegiamas atskiras C tipo serverių klasteris, kuris yra išskleistas per Vilniaus 2 duomenų centrus. Reikalingas serverių kiekis bus patikslintas detalaus servisų projektavimo stadijoje.

Duomenų saugojimui naudojamos lokalios duomenų centrų saugyklos. Techninių servisų padidintas pasiekiamumas duomenų centro ribose būtų užtikrinamas platformos lygyje. Esant techninėms galimybėms technologinių paslaugų servisų padidintas pasiekiamumas tarp duomenų centrų turėtų būti užtikrinamas konkretaus serviso standartinėmis PĮ priemonėmis.

Papildomai I etape, Kauno DC, diegiamas izoliuotas HCI technologijų pagrindu veikiantis klasteris. Numatyta - klasterio duomenų saugojimo efektyvi talpa 20TiB (saugant mažiausiai 2 kopijas). Dėl nedidelės šio duomenų centro skaičiavimo ir duomenų saugojimo resursų poreikio apimties naudoti pagrindiniuose Vilniaus duomenų centruose taikomas SAN pagrindu veikiančias duomenų saugojimo technologijas bei standartizuotus serverius yra neracionalu. Reikalingas HCI sprendimo serverių kiekis bei jų parametrai bus patikslinta detalaus servisų projektavimo stadijoje. I projekto etape ši platforma taip pat (esant poreikiui) bus naudojama tenantų technologinių servisų (tokių kaip klasterių arbitratoriai) veikimo užtikrinimui.



pav. 6-11 Technologinių paslaugų konsolidavimo platforma

6.2 Valdymo sluoksnio realizacija

6.2.1 Valdymo atsakomybių ir funkcijų pasiskirstymas

Analizės etape nustatyta, kad projektuojamos platformos resursų valdymą atliks dviejų tipų administratoriai – platformos ir tenantų (įstaigų / organizacijų).

Platformos administratorių pagrindinės funkcijos[5]:

- Užtikrinti korektišką platformos veikimą;
- Užtikrinti naujų paslaugų gavėjų (įstaigų / organizacijų) paruošimą platformos naudojimui;
- Užtikrinti bendrinį platformos valdymą ir priežiūrą;
- Teikti konsultacijas integruojant su paslaugų gavėjų esama infrastruktūra;
- Užtikrinti korektišką resursų atskyrimą tarp įstaigų / organizacijų;
- Išskirti reikiamus resursus įstaigoms / organizacijoms;
- Inicijuoti savalaikę platformos plėtrą / atnaujinimą;
- Formuoti, prijungti, atjungti, keisti išteklių telkinius;
- Diegti, konfigūruoti, naujinti papildomus platformos valdymo, saugumo ir stebėsenos įrankius;
- Kurti, publikuoti ir vystyti tipinių platformos paslaugų / išteklių katalogą;
- Kurti ir administruoti paslaugų teikėjo vartotojus, vartotojų prieigas ir jų teises;
- Kurti ir administruoti paslaugų gavėjo pagrindinius vartotojus ir jų teises;
- Užtikrinti platformos tinklo ir saugumo valdymą;

[5] Funkcijos bus detalizuotos kituose etapuose

- Paaiškinti įstaigų / organizacijų administratoriams kaip reikia diegti informacines sistemas ir kitą programinę įrangą projektuojamoje platformoje;
- Esant poreikiui ir galimybėms suprojektuoti informacinės sistemos infrastruktūros architektūrą esamos platformos kontekste;
- Užtikrinti suderintos technologinės integracijos su VĮ Infrastruktūra, NKSC ir kitais paslaugų teikėjais veikimą.

Tenantų administratorių pagrindinės funkcijos[6]:

- Infrastruktūros, skirtos informacinėms sistemoms ir kitai programinei įrangai, projektavimas ir diegimas;
- Įstaigos / organizacijos vartotojų kūrimas, jų prieigų ir teisių valdymas;
- Virtualių serverių, duomenų bazių, programinės įrangos ir įstaigai / organizacijai dedikuotų tinklo sprendimo komponentų priežiūra;
- Informacinių sistemų migravimo į paslaugų teikėjo platformą kuravimas ir valdymas;
- Paslaugų pokyčių valdymas;
- Paslaugų gavėjo uždaro paslaugų / išteklių katalogo formavimas ir valdymas;
- Įstaigos / organizacijos tinklo resursų konfigūravimas ir prieigos valdymas;
- Paslaugų gavėjo stebėsenos sistemų priežiūra ir valdymas;
- Paslaugų gavėjo integracinių sąsajų konfigūravimas ir valdymas.

6.2.2 Valdymo sluoksnio loginiai sąryšiai su ištekliais

Projektuojama virtualizacijos ir valdymo platforma suteiks galimybę platformos administratoriams atskirti konkrečiai įstaigai / organizacijai išskirtus išteklius į vieną loginį vienetą. Naujai suformuotas loginis vienetas šio projekto apimtyje bus vadinamas Tenantu (angl. *tenant*). Platformos administratorius suteiks prieigas tenanto administratoriams, kurie galės valdyti savo įstaigos / organizacijos išteklius. Tenantų apimtyje užtikrinama išteklių izoliacija.

Atsižvelgiant į tai, kad projektuojama infrastruktūra diegiama keturiuose duomenų centruose, siekiant sudaryti galimybes užtikrinti reikiamą informacinių sistemų, registrų ir kitos programinės įrangos patikimumo lygį, labai svarbu įstaigos / organizacijos administratoriui teisingai išdėstyti atskirus informacinės sistemos / registro komponentus fizinių duomenų centrų, platformų atžvilgiu. Šio poreikio įgyvendinimui nuspręsta virtualizacijos ir valdymo platformoje įvesti tenanto virtualaus duomenų centro (Tenant vDC) ir paslaugų teikėjo virtualaus duomenų centro (Provider vDC) sąvokas.

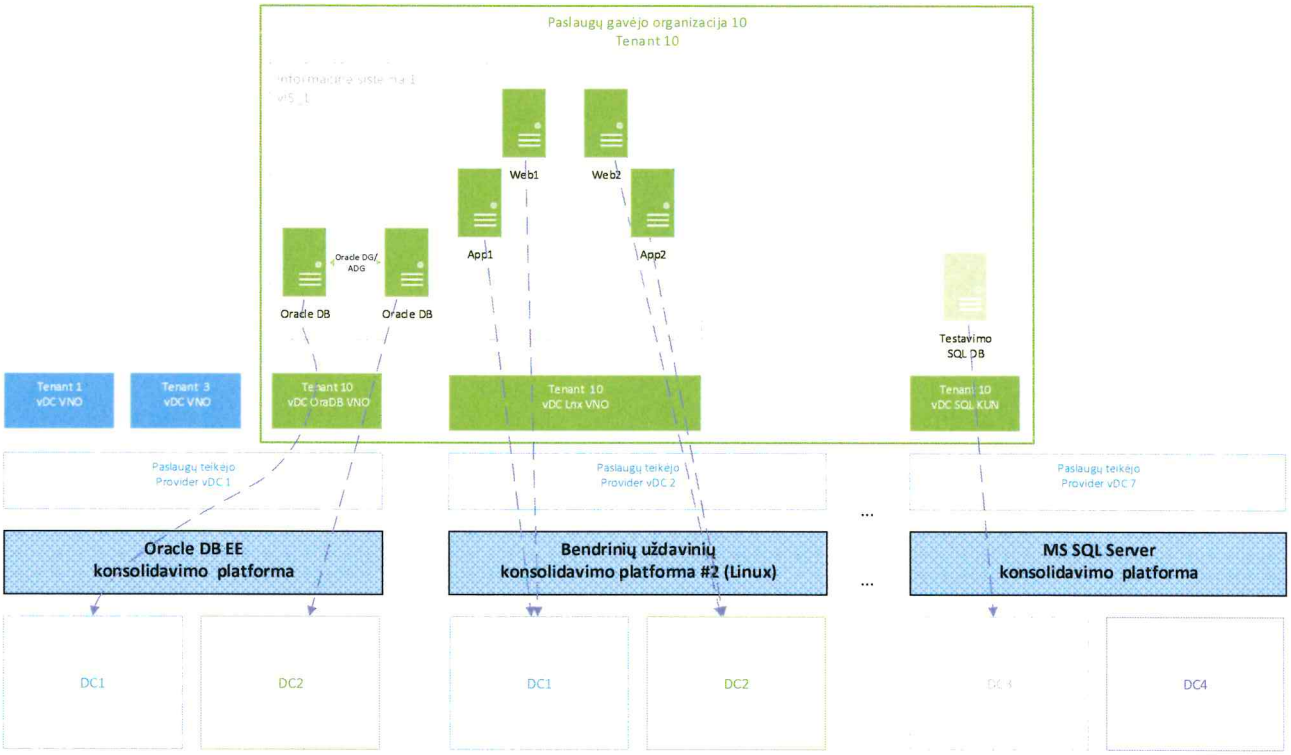
Skirtingų virtualizacijos telkinių / konsolidavimo platformų ištekliai priskiriami vienam arba keliems paslaugų teikėjo virtualiems duomenų centrams (Provider vDC). Teikėjo virtualus duomenų centras šiuo atveju atspindi fizinę konkrečių resursų lokaciją pasirinktos konsolidavimo platformos (pvz. Linux, Windows, Oracle ir t.t.) rėmuose. Kai vienas ar kitas virtualizacijos / resursų telkinys prijungiamas prie valdymo platformos, jis tampa kontroliuojamas ir valdomas valdymo platformos.

[6] Funkcijos bus detalizuotos kituose etapuose

Savo ruožtu teikėjo sukurtas loginis sluoksnis (Provider vDC) leidžia toliau paskirstyti išteklius įstaigų / organizacijų (tenantų) virtualiems duomenų centrams (Tenant vDC). Virtuali organizacija – tenantas – gali turėti kelis įstaigos / organizacijos virtualius duomenų centrus (Tenant vDC), naudojančius resursus iš skirtingų platformų skirtinguose lokacijose (fiziniuose duomenų centruose).

Provider vDC ir Tenant vDC loginiai lygiai užtikrina teisių ir funkcijų segregaciją tarp paslaugų teikėjo ir paslaugų gavėjų administratorių.

Žemiau yra vizualizuoti galimi sąryšiai tarp resursų telkinių / platformų, fizinių DC, virtualių DC, virtualių serverių, informacinių sistemų (vIS) ir paslaugų gavėjų (organizacijų / tenantų) (pav. 6-12 Resursų telkinių/platformų, virtualių DC, virtualių serverių ir organizacijų/tenantų sąryšiai).



pav. 6-12 Resursų telkinių/platformų, virtualių DC, virtualių serverių ir organizacijų/tenantų sąryšiai

Priklausomai nuo paslaugų gavėjo organizacijos poreikių, dinamikos ir paslaugų teikėjo galimybių, virtualizacijos valdymo platforma kiekvienam įstaigos / organizacijos (tenanto) virtualiam duomenų centrui (Tenant vDC) gali turėti vieną iš trijų išteklių naudojimo / vartojimo modelių:

- dinaminio (angl. pay as you go) – išteklių ribos nematomos paslaugų gavėjui, ištekliai mažinami arba didinami paslaugų gavėjo pagal poreikį. Modelis dažniausiai pasirenkamas trumpalaikių poreikių įgyvendinimui;
- pilnai rezervuoto – ištekliai priskiriami / rezervuojami 100%. Modelis dažniausiai pasirenkamas darbinių aplinkų su griežtais našumo reikalavimais įgyvendinimui;
- dalinai išskirto – išteklių užtikrinimas su maksimalia viršutine riba. Modelis dažniausiai pasirenkamas projektinių veiklų / sistemų be didelių įsipareigojimų įgyvendinimui.

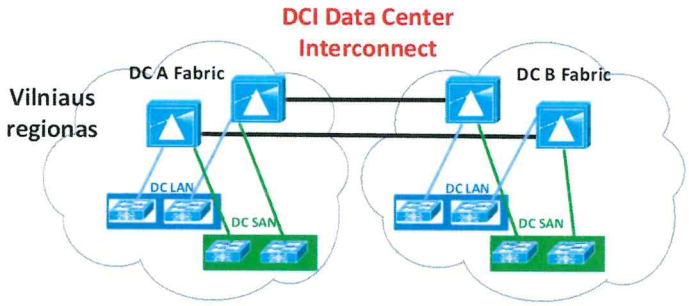
Valdymo sluoksnio valdančios ir kontroliuojančios programinės įrangos komponentai bus talpinami technologinių paslaugų konsolidavimo platformoje.

7 Duomenų perdavimo tinklų fizinės bei loginės tinklo topologijos architektūros modelis

7.1 Komunikacijos sluoksnio realizacija

7.1.1 Duomenų centrų apjungimas fiziniame tinklo lygyje[7]

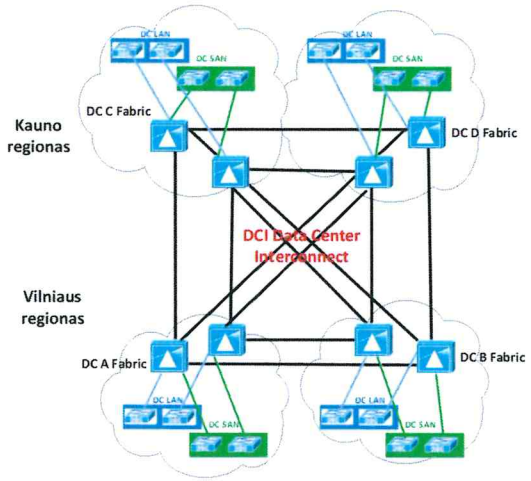
Duomenų centrų apjungimas fiziniame lygyje realizuojamas fiziškai apjungiant duomenų centrus DWDM (angl. Dense Wavelength Division Multiplexing) pagalba. Pirmame etape Vilniaus regiono duomenų centrai tarpusavyje apjungiami dubliuotais, skirtingais keliais einančiais sujungimais (pav. 7-1 DWDM sprendimo schema (I etapas)). Bendra sujungimo greitaveika tarp gretimų duomenų centrų – 8x100G (LAN lygyje) ir 8x32G (SAN lygyje). Sujungimo realizavimui kiekvienu keliu reikalingos 2 skaidulos (viso 4 skaidulos).



pav. 7-1 DWDM sprendimo schema (I etapas)

Antrame projekto etape analogiškas sprendimas diegiamas Kauno regiono DC. Vilniaus ir Kauno regionų duomenų centrai tarpusavyje sujungiami dubliuotais, skirtingais keliais einančiais sujungimais. Bendra sujungimo greitaveika tarp gretimų duomenų centrų – 8x100G (LAN lygyje) ir 8x32G (SAN lygyje). Koncepcinė sprendimo schema pateikta (pav. 7-2 DWDM sprendimo schema (II etapas). Sujungimo realizavimui kiekvienu keliu reikalingos 2 skaidulos (4 skaidulos regiono ribose ir 16 skaidulų apjungimui tarp regionų). Prieš pradedant realizuoti antro etapo sprendimą, rekomenduojama įvertinti realų sujungimų poreikį, atsižvelgiant į pirmame projekto įgyvendinimo etape įsigytas ir naudojamas technologijas.

[7] Kai bus patvirtinti duomenų centrų adresai, duomenų centrų apjungimo fiziniame tinklo lygyje sprendimas gali keistis atsižvelgiant į Saugiojo tinklo operatoriaus technines galimybes (už duomenų centrų apjungimą fiziniame tinklo lygyje atsakingas Saugiojo tinklo operatorius).

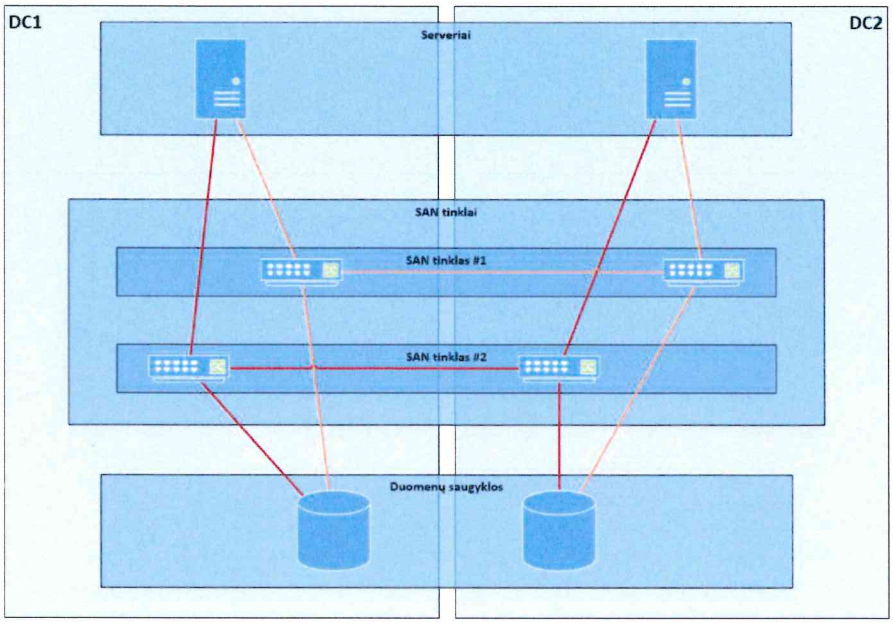


pav. 7-2 DWDM sprendimo schema (II etapas)

7.1.2 Duomenų centrų SAN tinklai

Duomenų perdavimui tarp serverių ir duomenų saugyklų sujungimui bus naudojamas SAN tinklas, realizuojamas remiantis geriausiomis SAN tinklų kūrimo praktikomis, – sukuriant 2 nepriklausomus SAN tinklus (SAN fabric) (pav. 7-3 Koncepcinė I etapo SAN tinklų schema). SAN komutatoriai sujungiami į 2 nepriklausomas grupes taip užtikrinant galimų problemų izoliavimą. Tiek serveriai, tiek duomenų saugyklos jungiami prie abiejų SAN tinklų (pagal poreikį daugiau nei 1 jungtimi).

Pagal pradinių duomenų analizės rezultatus matoma, kad I projekto etape planuojamas SAN jungčių skaičius viename duomenų centre viršija 250 vnt. (daugiau nei 125 vnt. per SAN tinklą viename duomenų centre). Įvertinus infrastruktūros plėtimo reikalavimus ir siekiant išlaikyti kiek galima paprastesnę SAN tinklų architektūrą bei valdymą, siūloma sprendimo diegimui naudoti modulinius Director klasės SAN komutatorius su 192 vnt. 32GB FC jungčių I etape bei galimybe išplėsti komutatorius, įdiegiant papildomus jungčių modulius (maksimalus jungčių skaičius ne mažiau nei 300 vnt.) tolimesniuose projekto etapuose.



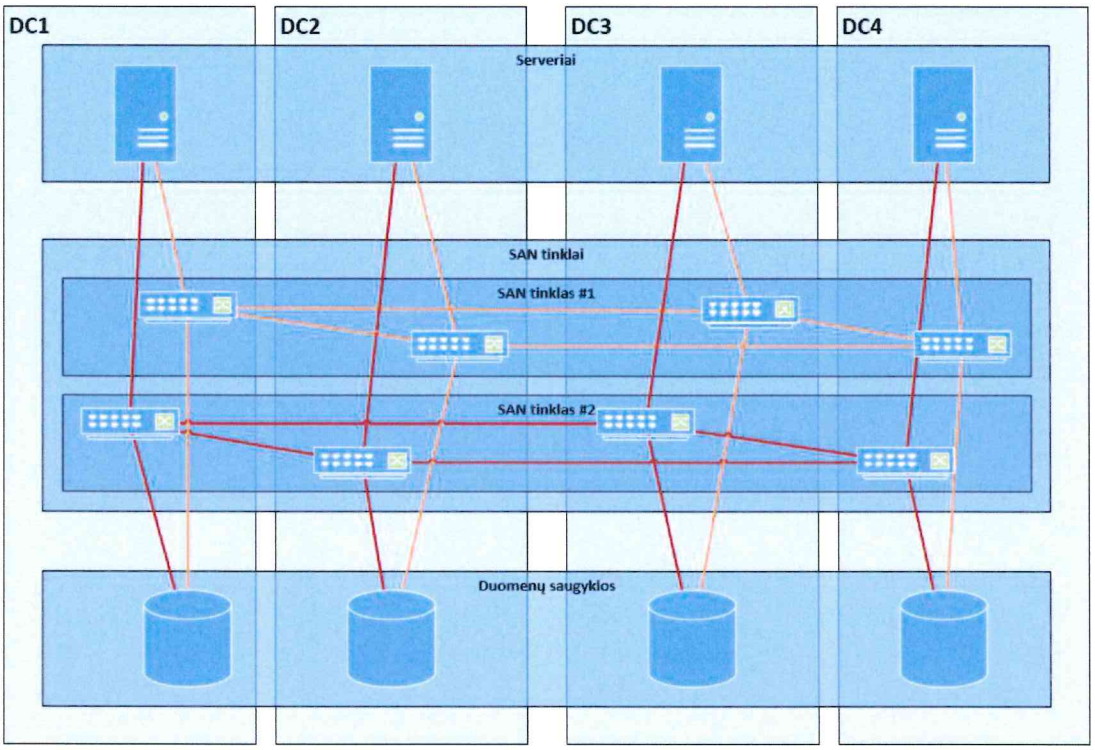
pav. 7-3 Koncepcinė I etapo SAN tinklų schema

SAN tinklų sujungimui tarp skirtinguose duomenų centruose esančių komutatorių naudojamas DWDM (angl. Dense Wavelength Division Multiplexing) sprendimas. SAN tinklų sujungimams pateikiama greitaveika – 32Gbps.

I projekto etape naudojami 8 sujungimai tarp Vilniaus duomenų centruose įdiegtų komutatorių (po 4 per fizinį SAN tinklą).

Tolimesniuose projekto etapuose – analogiškas sprendimas diegiamas duomenų centruose Kaune, išplečiant esamus SAN tinklus į 4 duomenų centrus. Sujungimas tarp Vilniaus ir Kauno duomenų centrų realizuojamas 8 sujungimų pagalba. Šį sujungimą planuojama naudoti serverių ir duomenų migracijoms tarp regionų bei kitiems poreikiams. Koncepcinė šio etapo SAN tinklų schema pavaizduota (pav. 7-4 Koncepcinė 4 duomenų centrų SAN tinklų schema). Prieš pradedant realizuoti antro etapo sprendimą, rekomenduojama įvertinti realų sujungimų poreikį, atsižvelgiant į pirmame projekto įgyvendinimo etape įsigytas ir naudojamas technologijas.

Esant poreikiui didinti SAN jungčių skaičių duomenų centruose į komutatorius diegiami papildomi jungčių moduliai.



pav. 7-4 Koncepcinė 4 duomenų centrų SAN tinklų schema

7.1.3 LAN fizinės bei loginės tinklo topologijos architektūros modelis

Vadovaujantis teisės aktų reikalavimais bei įgyvendinant tarpžinybinius susitarimus nuspręsta, kad duomenų centrų apjungimui reikiamus sprendimus projektuos ir realizuos VĮ Infostruktūra. Šio projekto apimtyje turi būti įvardinti reikalavimai sujungimams. Nuspręsta, kad VĮ Infostruktūra projektuojamos platformos naudotojams teiks Interneto, AntiDDoS ir Saugaus valstybinio duomenų perdavimo tinklo paslaugas. Šios paslaugos projekto apimtyje nėra projektuojamos. Suderinami tik paslaugų teikimui reikiami sujungimo mechanizmai.

7.1.3.1 Bendroji tinklo architektūra

Duomenų perdavimo tinklo struktūrizavimas – tinklas skaidomas į atskirus segmentus, kur kiekvienas segmentas nusako tam tikro lygio tinklą.

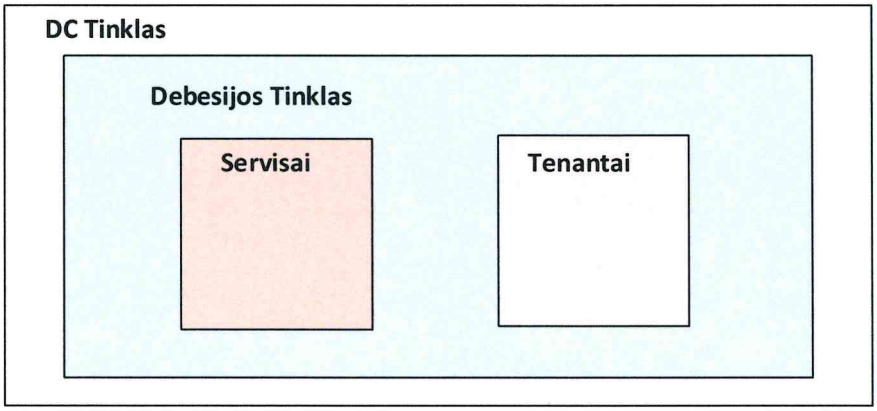
Horizontaliai tinklas skaidomas į tris sluoksnius – duomenų centrų tinklas, debesijos tinklas ir organizacijų / įstaigų tinklas. Visi šie tinklai sudaro bendrą loginį tinklą, kur kiekvienas aukštesniame loginio tinklo sluoksnyje esantis komponentas naudojasi žemesniame sluoksnyje esančio komponento teikiamomis paslaugomis.

Duomenų centrų tinklas – fizinis duomenų centrų tinklas, skirtas apjungti duomenų centruose esančią infrastruktūrą. DC tinklas projektuojamas kaip duomenų centrų fabrikai, apjungti į vieną paskirstytą fabriką, išsidėsčiusį per keturis fizinius duomenų centrus skirtingose lokacijose.

Debesijos tinklas – virtualus duomenų centrų tinklas, naudojamas kaip technologinis tinklas organizacijų tinklui. Debesijos tinklas projektuojamas kaip vientisas virtualus tinklas per keturis fizinius duomenų centrus, grįstas SDN (angl. Software Defined Network) technologijų pagrindu. Korektiškam debesijos tinklo veikimui reikalinga suprojektuoti duomenų centrų tinklą, kuris atliks fizinio apjungimo funkciją.

Įstaigų / organizacijų tinklas – konkrečios įstaigos, organizacijos arba jos padalinio atskiras virtualus arba hibridinis (virtualus ir fizinis) tinklas, kuris naudojasi DC ir debesijos tinklo paslaugomis. Naudojant organizacijų tinklą apjungiami organizacijos IT infrastruktūros įrenginiai (serveriai, saugumo įrenginiai ir t.t.) į vieną homogeninį tinklą.

Bendroji tinklo architektūra pateikta (pav. 7-5 Bendroji tinklo architektūros schema).



pav. 7-5 Bendroji tinklo architektūros schema

Duomenų centrų tinklo rolės:

- transportuoti duomenų srautus tarp duomenų centrų bei išorinių tinklų;
- būti pagrindu organizacijų tenantų tinklams, kuriuose talpinami organizacijų IT infrastruktūros elementai.

Duomenų centro tinklo ir debesijos tinklo kontroliniai valdymo mazgai (Control plane) turi būti nepriklausomi, atskiri ir negali būti bendrame duomenų centro ir debesijos tinklų kontroliniame, valdymo (Control plane) mazge. Toks sprendimas užtikrina tinklų nepriklausomumą, patikimumą ir panaikina arba maksimaliai minimizuoja pilnutinio duomenų centrų praradimo arba užvaldymo rizikas. Tinklų izoliavimas taip pat leidžia atskirti tinklų valdymo komandas ir minimizuoti žmogiškųjų klaidų įtaką.

Vertikaliai bendras duomenų perdavimo tinklas skirstomas į keturias sritis / domenus, atsakingus už atskiras duomenų perdavimo tinklo funkcijas. Projektuojamame tinkle bus šie domenai:

- Paslaugų – pagrindinis domenas, apibrėžiantis teikiamas tinklo paslaugas ir jas sudarančius elementus;
- Prieigos – domenas, apibrėžiantis tinklo komunikaciją su išoriniais tinklais;
- Valdymo – domenas, apibrėžiantis kaip konkrečiame tinklo sluoksnyje esantis įrenginys yra valdomas ir stebimas. Domenas taip pat atsakingas už automatizavimą, orkestravimą ir programavimą;

- Patikimumo – domenas, apibrėžiantis kompiuterinio tinklo patikimumo realizaciją. Tinklas projektuojamas sluoksniais kai aukščiau esantis sluoksnis naudojasi žemiau esančio sluoksnio paslaugomis ir manoma, kad žemiau esančio sluoksnio paslaugos teikiamos patikimai.

Bendrą projektuojamo tinklo architektūrą galima atvaizduoti matrica. Matricos eilutės atitinka sluoksnius, o stulpeliai – domenus.

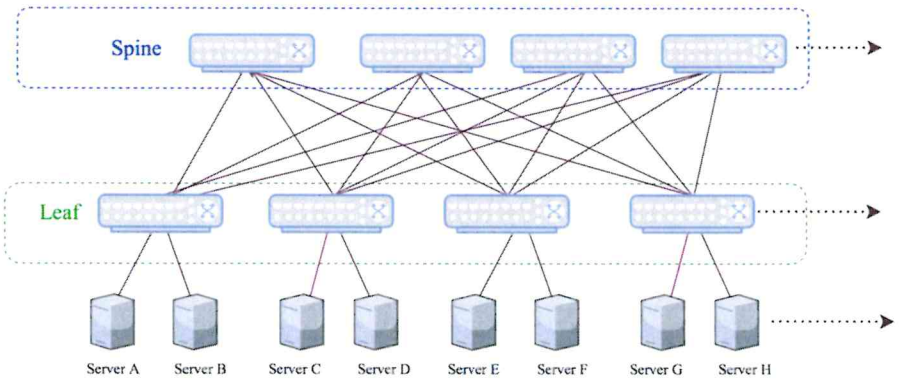
Tinklas \ Domenas	Paslaugų	Prieigos	Valdymo	Patikimumo
Duomenų centrų	Komutavimo, maršrutizavimo, saugumo	Internetas, WAN, nutolęs valdymas	Stebėjimas, automatizavimas, orkestravimas, programavimas	Patikimumas, pasiekiamumas
Debesijos	Komutavimo, maršrutizavimo, saugumo	Internetas, WAN, nutolęs valdymas	Stebėjimas, automatizavimas, orkestravimas, programavimas	Patikimumas, pasiekiamumas
Organizacijų \ Tenantų	Komutavimo, maršrutizavimo, saugumo	Internetas, WAN, nutolęs valdymas	Stebėjimas, automatizavimas, orkestravimas, programavimas	Patikimumas, pasiekiamumas

7.1.3.2 Duomenų centro tinklas

Duomenų centro tinklas – fizinis duomenų centrų tinklas, skirtas apjungti duomenų centruose esančią IT infrastruktūrą, taip pat užtikrinti fizinius sujungimus tarp duomenų centrų ir išorinių tinklų.

7.1.3.2.1 Bendra duomenų centrų tinklo architektūra

Duomenų centrų tinklas projektuojamas kaip duomenų centrų fabrikai, esantys skirtinguose fiziniuose duomenų centruose, apjungti į vieną bendrą fabriką. Bendras fabrikas projektuojamas remiantis CLOS architektūros pagrindu. CLOS topologiją sudaro du sluoksniai – Spine ir Leaf. Serveriai ir tinkliniai įrenginiai jungiami į Leaf komutatorius (Top of Rack – ToR), kur kiekvienas iš Leaf sujungtas su visais Spine. Šioje topologijoje nėra tiesioginių sujungimų Leaf – su – Leaf arba Spine – su - Spine. Esminiai tokio sprendimo privalumai – nesvarbu kur tinkle prijungtas serveris, saugykla ir / arba tinklinis įrenginys, jis kitą tinkle esantį įrenginį pasieks per 2 tinklinius segmentus. Naudojant šį sprendimą gaunamas stabilus, valdomas vėlinimas tinkle nepriklausomai nuo to, kur serveriai prijungti tinkle vienas kito atžvilgiu.



pav. 7-6 Bendra duomenų centrų tinklo topologijos schema

CLOS topologija plečiama horizontaliai, kas užtikrina efektyvų kaštų panaudojimą ir tinklo plečiamumą nekeičiant tinklo architektūros. Pralaidumas plečiamas prijungiant daugiau Spine komutatorių į Leaf komutatorius.

7.1.3.2.2 Duomenų centrų fabrikas

Duomenų centro fabrikas projektuojamas remiantis CLOS Leaf ir Spine topologija ir VXLAN MP-BGP EVPN technologijų pagrindu. Fabrikas projektuojamas kaip maršrutizuojamas L3 tinklas (pagal OSI modelį).

Duomenų centrų fabriko maršrutizavimas L3 lygyje (pagal OSI modelį) vyksta naudojant VXLAN MP – BGP EVPN technologiją. Fabrikas projektuojamas iš dviejų nepriklausomų sluoksnių – fabriko pamato (angl. *underlay)* ir fabriko transporto (angl. *overlay)*. Fabriko pamato (angl. *underlay)* sluoksnis užtikrina sklandų pasiekiamumą tarp skirtingų fabriko elementų. Fabriko transportas *Overlay* konstruojamas kaip tunelių L2/ L3 rinkinys, kurie skirti realiems kliento duomenų srautams transportuoti. Pasirinktas sprendimas leidžia atskirti virtualius ir fizinius tinklus. Atskyrimas leidžia užtikrinti maksimalų DC tinklo ir Debesijos tinklo stabilumą, nepriklausomumą, skirtingus tinklų gyvavimo ciklus, neturėti technologinių ribojimų, kurie kyla bandant sujungti virtualius ir fizinius tinklus. Leidžia atskirti valdymo funkcijas: fizinis tinklas – DC tinklas – transportas. Virtualus tinklas – tenantų tinklas. Loginiame lygyje fabriką segmentuojame į penkis segmentus:

- Skaičiavimo (Compute) segmentas – šiame segmente talpinami serveriai, kuriuose talpinama tenantų stuburinė dalis;
- Tenanto paslaugų (Tenat service) segmentas – šiame segmente talpinami fiziniai tinkliniai įrenginiai – saugumo (ugniasienės, aplikacijų ugniasienės (WAF), įsilaužimo aptikimo / prevencijos sistemų, balansavimo ir t.t.), saugyklos, veikiančios IP protokolu, taip pat talpinami virtualių tinklų sujungimo mazgai su fiziniais įrenginiais. Fiziniai įrenginiai gali būti lokalūs, esantys duomenų centre, arba nutolę, esantys nutolusiame duomenų centre;
- Prieigos lokalus (Edge) segmentas – šiame segmente talpinami įrenginiai – perimetro ugniasienės, perimetro saugumo įrenginiai, serveriai, kuriuose talpinama tenantų prieigos dalis, skirta sujungimams su išoriniais tinklais, tokiais kaip WAN, nutolę LAN, internet, partnerių tinklai;
- Prieigos nutolęs (Edge) segmentas – šis segmentas yra integracinis mazgas organizacijų esamiems duomenų centrams integruoti;
- Valdymo (Managment) segmentas – šiame segmente talpinami serveriai ir tinkliniai įrenginiai skirti infrastruktūrų valdymui.

Vieno duomenų centro fabriko segmentų loginė schema pateikta žemiau (pav. 7-7 Duomenų centro fabriko segmentų loginė schema). Visi duomenų centrų fabrikai segmentuojami į tuos pačius segmentus.

pav. 7-7 Duomenų centro fabriko segmentų loginė schema

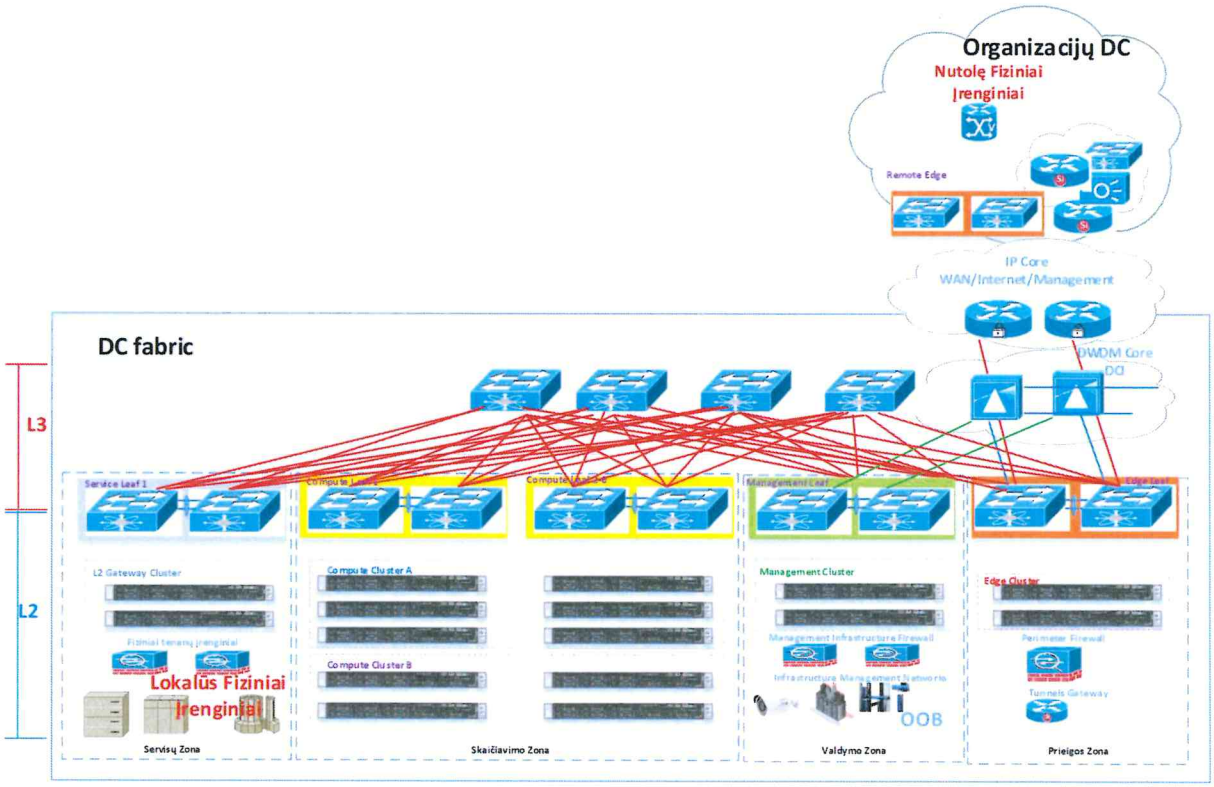
Fiziškai fabrikas – nepriklausomų komutatorių rinkinys, sujungtų į vieną tinklą. Leaf komutatoriai šiuo atveju atlieka ToR komutatorių funkcijas. ToR komutatoriuose terminuojami L2 segmentai. Kiekvienas duomenų centro fabrikas – atskiras, nepriklausomas fabrikas. Visi duomenų centrai sujungiami į vieningą duomenų centrų tinklą, kuris sujungia skirtingus fabrikus. Kiekvieno duomenų centro tinklas projektuojamas iš:

- Spine tipo komutatorių – 4 vnt. Spine tipo komutatorių. Kiekvienas Spine komutatorius – aukšto našumo fizinis komutatorius, palaikantis VXLAN MP – BGP EVPN technologiją;
- Virtualių Leaf tipo komutatorių – 12 vnt. virtualių Leaf tipo komutatorių. Kiekvienas virtualus Leaf – sudarytas iš dviejų fizinių 10/25 Gbps spartos aukšto našumo komutatorių, palaikančių VXLAN MP – BGP EVPN technologiją ir dviejų 1 Gbps spartos aukšto našumo komutatorių. Virtualūs Leaf komutatoriai segmentų atžvilgiu pasiskirstę:

Segmentas	**Leaf virtualus komutatorius**	**Leaf fizinis aukšto našumo 10/25 Gbps spartos komutatorius**	**Leaf fizinis aukšto našumo 1 Gbps spartos komutatorius**
Skaičiavimo (Compute)	6	12	12
Paslaugų (Service)	2	4	4
Prieigos lokalus (Edge) segmentas	1	2	2
Prieigos nutolęs (Edge) segmentas	2	4	4
Valdymo (Management)	1	2	2
Viso	12	24	24

Sujungimai tarp Spine ir Leaf projektuojami 100Gbps pralaidumo ir MM (Multi Mode) tipo jungtimis. Pralaidumas bus patikslintas detalaus projektavimo stadijoje.

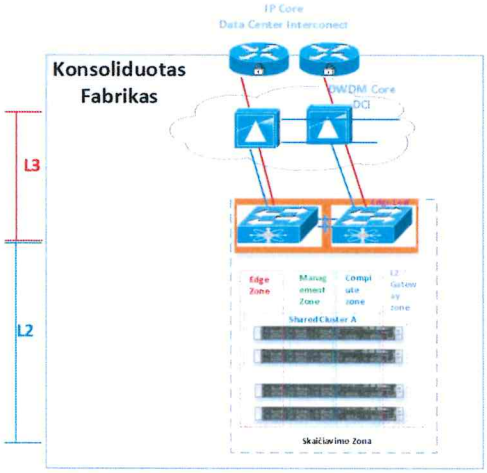
Vieno duomenų centro fabriko logika pavaizduota žemiau (pav. 7-8 Duomenų centro fabriko schema)



pav. 7-8 Duomenų centro fabriko schema

7.1.3.2.3 Konsoliduotas duomenų centrų fabrikas

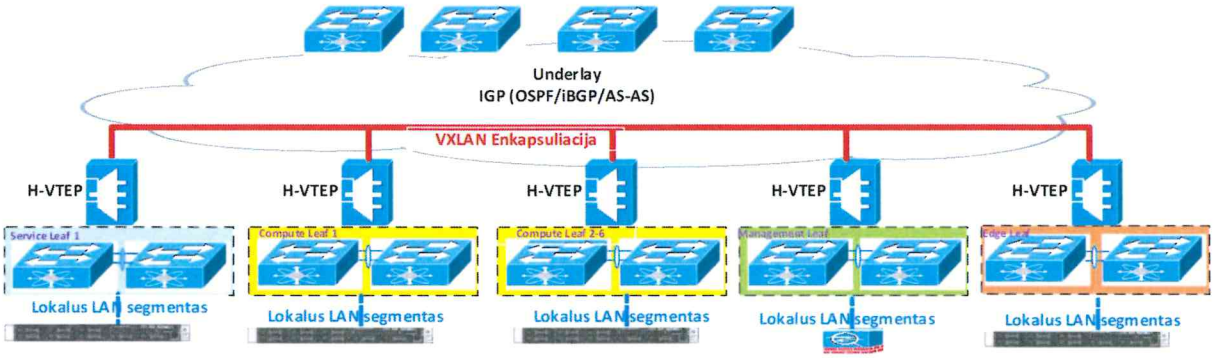
Konsoliduotas duomenų centrų fabrikas – fabriko modelis, kuriame tinklo ir skaičiavimo funkcijos apjungiamos į bendrus komutatorius. Mažiausioje konfigūracijoje du komutatoriai atlieka Spine ir Leaf funkcijas bei juose konsoliduojamos skaičiavimo, Edge, valdymo ir tinklo paslaugų zonos. Šiose zonose esančios virtualios mašinos talpinamos į vieną skaičiavimo telkinį. Šis modelis taikomas nutolusiems duomenų centrams, kur pilną fabriką laikinai ar dėl kitų priežasčių yra netikslinga naudoti. Konsoliduotas fabrikas pavaizduotas žemiau (pav. 7-9 Konsoliduotas duomenų centrų fabrikas schema).



pav. 7-9 Konsoliduotas duomenų centrų fabrikas schema

7.1.3.2.4 Duomenų centrų fabriko pamato architektūra

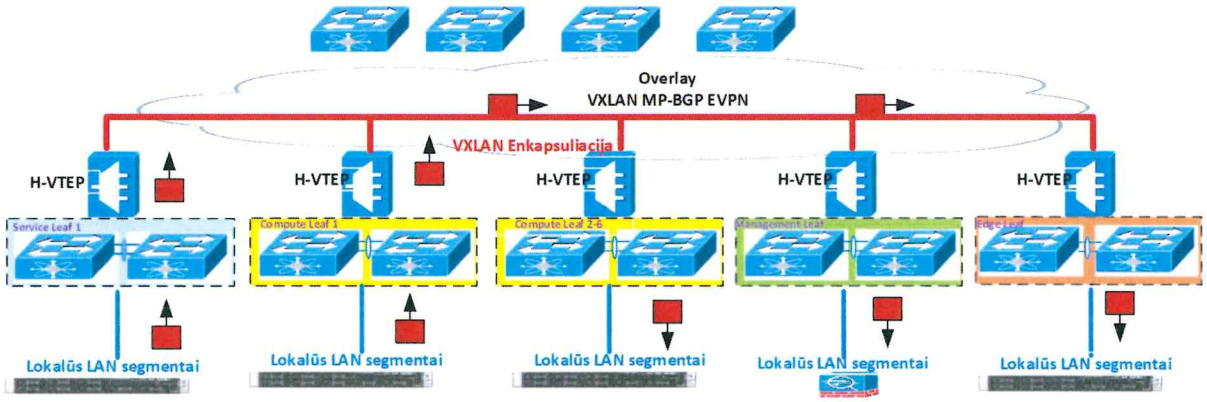
Pagrindinis fabriko pamato (UNDERLAY) tikslas – užtikrinti pasiekiamumą tarp fizinių virtualių tunelio interfeisų (Hardware Virtual Tunnel End Points (H-VTEPs)) ir BGP sujungimų (BGP peering) IP adresų. Analogiška architektūra taikoma visiems duomenų centrų tinklams, kuriuose bus diegiama debesijos platforma. Duomenų centrų fabriko pamato architektūra pavaizduota žemiau (pav. 7-10 Duomenų centrų fabriko pamato architektūros schema).



pav. 7-10 Duomenų centrų fabriko pamato architektūros schema

7.1.3.2.5 Duomenų centrų fabriko transporto architektūra

Fabriko transportas (OVERLAY) – dinaminių L2/ L3 (pagal OSI modelį) tunelių rinkinys, transportuojantis paketus tarp dviejų tinklo virtualių Leaf komutatorių. OVERLAY projektuojamas naudojant VXLAN MP – BGP EVPN technologijas. Analogiška architektūra taikoma visiems duomenų centrams, kuriuose bus diegiama debesijos platforma. Duomenų centrų fabriko transporto architektūra pavaizduota žemiau (pav. 7-11 Duomenų centrų fabriko transporto architektūros schema).



pav. 7-11 Duomenų centrų fabriko transporto architektūros schema

7.1.3.2.6 Duomenų centrų tinklo paslaugų domenas

Duomenų centrų tinklo paslaugų domeną sudaro dvi paslaugų grupės – transporto ir saugumo.

7.1.3.2.6.1 Duomenų centrų tinklo paslaugų domeno transporto paslaugos

Duomenų centrų tinklo paslaugų domeno transporto (maršrutizavimo ir komutavimo) paslaugos realizuojamos duomenų centrų fabriko transporto (OVERLAY) pagrindu. Transporto (OVERLAY) lygyje projektuojami L2/ L3 tuneliai (pagal OSI modelį). Tuneliai gali būti projektuojami vieno duomenų centro fabriko ribose arba tarp duomenų centrų atsižvelgiant į konkretų poreikį.

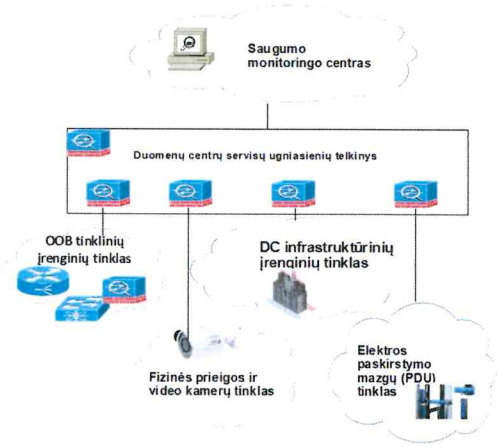
7.1.3.2.6.2 Duomenų centrų tinklo paslaugų domeno saugumo paslaugos

Duomenų centrų tinklo paslaugų domeno saugumo paslaugos užtikrina saugumo funkcijas. Šios paslaugos skirtos apsaugoti duomenų centruose esančią infrastruktūrą.

Duomenų centrų tinklo saugumo paslaugos projektuojamos naudojant duomenų centrų tinklo paslaugų ugniasienių telkinį (klasterį), esantį duomenų centruose. Ugniasienių telkinio resursus daliname į virtualias ugniasienes, skirtas apsaugoti žemiau išvardintus tinklo segmentus:

- Tinklo įrenginių valdymo – tinklinių įrenginių valdymo segmentas (out-of-band arba OOB) skirtas valdyti tinklinius įrenginius įvykus kritinėms situacijoms;
- DC infrastruktūros įrenginių valdymo – duomenų centruose esantiems šaldymo įrenginiams, elektros generatoriams ir kitiems duomenų centrų infrastruktūros įrenginiams valdyti skirtas segmentas;
- Elektros paskirstymo valdymo įrenginių (power distribution unit (PDU)) – duomenų centruose esančių elektros paskirstymo valdymo įrenginių stebėjimui, valdymui ir suvartotos elektros energijos apskaitai skirtas segmentas;
- Fizinės saugos prieigos ir vaizdo stebėjimo įrenginių – duomenų centruose esančių fizinės prieigos kontrolės ir vaizdo stebėjimo įrenginių segmentas.

Duomenų centrų tinklo saugumo segmentai pavaizduoti žemiau (pav. 7-12 Duomenų centrų tinklo saugumo segmentų schema).



pav. 7-12 Duomenų centrų tinklo saugumo segmentų schema

7.1.3.2.7 Duomenų centrų tinklo prieigos domenas

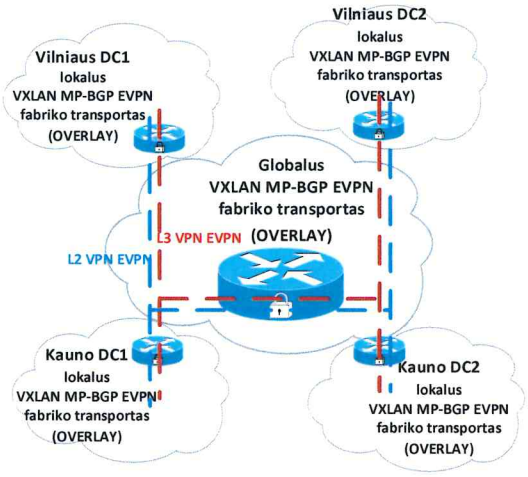
Duomenų centrų prieigos domenas apibrėžia duomenų centro fabriko sujungimus su išoriniais tinklais ir skirtinguose duomenų centruose esančių fabrikų sujungimus tarpusavyje.

7.1.3.2.7.1 Duomenų centrų sujungimas

Duomenų centrų sujungimo (Data Center Interconnect – DCI) logika realizuota dviem lygiais sujungiant duomenų centrų tinklus – fiziškai ir logiškai.

7.1.3.2.7.1.1 Duomenų centrų sujungimas loginiame tinklo lygyje

Duomenų centrų sujungimas loginiame lygyje realizuojamas sujungiant duomenų centruose suprojektuotus fabrikus į vieną globalų duomenų centrų fabriką OVERLAY lygyje. Toks sprendimas leidžia transportuoti paketus iš vieno duomenų centro į visus likusius duomenų centrus. Sprendimo schema pateikta žemiau (pav. 7-13 Duomenų centrų sujungimo loginiame tinklo lygyje schema).

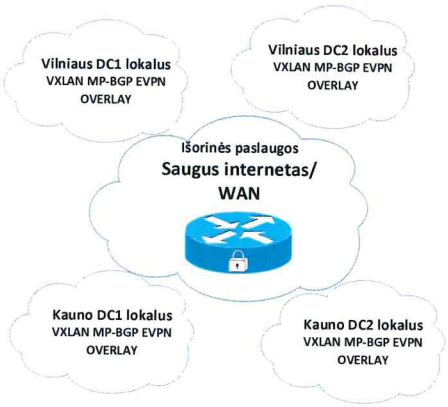


pav. 7-13 Duomenų centrų sujungimo loginiame tinklo lygyje schema

7.1.3.2.7.2 Išorinių paslaugų prijungimas

7.1.3.2.7.2.1 Išorinių paslaugų prijungimas loginiame lygyje

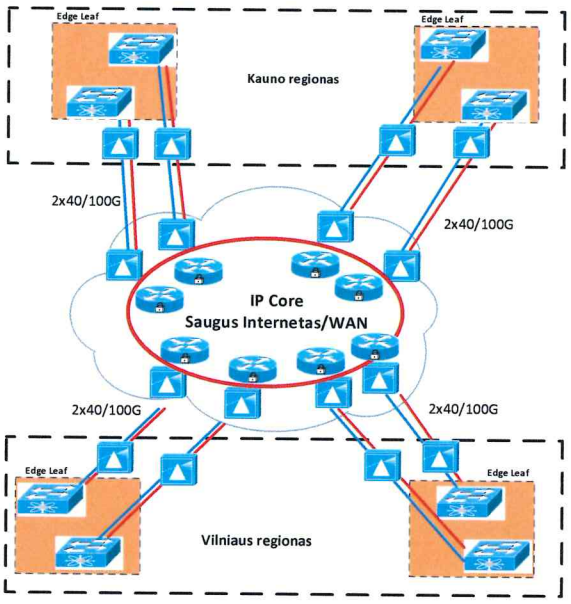
Išorinės duomenų centrų paslaugos bus teikiamos vieno ryšio paslaugų teikėjo. Šiam tikslui visi duomenų centrai bus sujungti su ryšio paslaugų tiekėjo stuburiniu tinklu, iš kurio gaus saugų internetą ir L2/L3 (pagal OSI modelį) VPN paslaugas, kurių pagalba duomenų centrai susisiekia su išoriniais tinklais, tokiais kaip Europos Sąjungos institucijos, organizacijų nutolę padaliniai ir pan. Koncepcinė sprendimo schema pateikta žemiau (pav. 7-14 Išorinių paslaugų prijungimo loginiame lygyje schema).



pav. 7-14 Išorinių paslaugų prijungimo loginiame lygyje schema

7.1.3.2.7.2.2 Išorinių paslaugų prijungimas fiziniame lygyje

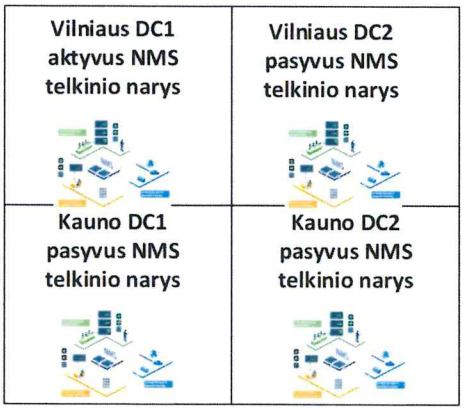
Visi duomenų centrai prie ryšio paslaugų tiekėjo stuburinio tinklo prijungiami dedikuotais dubliuotais sujungimais, kurių sparta 2x40Gbps arba 2x100Gbps. Greitaveika pasirenkama priklausomai nuo stuburinio tinklo tiekėjo techninių galimybių. Sprendimo schema pateikiama žemiau (pav. 7-15 Išorinių paslaugų prijungimo fiziniame lygyje schema).



pav. 7-15 Išorinių paslaugų prijungimo fiziniame lygyje schema

7.1.3.2.8 Duomenų centrų valdymo paslaugų domenas

Duomenų centrų tinklas projektuojamas taip, kad būtų valdomas kaip vienas loginis vienetas, sudarytas iš keturių nepriklausomų duomenų centrų. Kiekviename iš duomenų centrų bus diegiami duomenų centrų valdymo sprendimo (Network Managment System – NMS) komponentai, veikiantys viename telkinyje active / pasive rėžimu. Įprastomis sąlygomis duomenų centrų tinklas valdomas iš to duomenų centro, kuriame yra aktyvus telkinio narys. Sutrikus įprastomis sąlygomis naudojamam sprendimui bus aktyvuotas kitame duomenų centre esantis tinklo valdymo telkinio narys. Duomenų centrų valdymo schema pavaizduota žemiau (pav. 7-16 Duomenų centrų valdymo schema).



pav. 7-16 Duomenų centrų valdymo schema

7.1.3.2.9 Duomenų centrų patikimumo paslaugų domenas

Duomenų centrų fabrikas projektuojamas vadovaujantis pilnutiniu visų komponentų dubliavimu, t. y., nepaliekant nei vieno duomenų centro tinklo komponento nedubliuoto (single point of failure – SPOF).

Spine tipo komutatoriai – sprendimas suprojektuotas taip, kad vienu metu sugedus trims 3 Spine tipo komutatoriams, duomenų centro tinklo funkcionalumas nesutriktų.

Leaf tipo komutatoriai – sprendimas suprojektuotas taip, kad sugedus bet kuriam iš Leaf tipo komutatorių, duomenų centro tinklo funkcionalumas nesutriktų.

Edge tipo komutatoriai – sprendimas suprojektuotas taip, kad sugedus bet kuriam iš Edge tipo komutatorių, duomenų centro tinklo funkcionalumas nesutriktų.

7.1.3.3 Debesijos tinklas

Debesijos tinklas – virtualus duomenų centrų tinklas, naudojamas kaip technologinis tinklas organizacijų tinklui. Debesijos tinklas projektuojamas kaip vientisas virtualus tinklas per keturis fizinius duomenų centrus. Šis tinklo sluoksnis projektuojamas SDN (angl. Software Defined Network) technologijų pagrindu. Debesijos tinklas naudojasi bendro loginio duomenų centrų tinklo paslaugomis.

7.1.3.3.1 SDN tinklas

Debesijos tinklo architektūros pagrindą sudaro SDN (Software Definet Network). SDN sudaro šie sluoksniai:

- Valdymo (Management plane) – sluoksnį sudaro SDN tinklo vieningas API, kuris yra centrinis SDN tinklo valdymo komponentas. Naudojantis anksčiau minėtu API atliekami SDN tinklo konfigūracijos pakeitimai bei realizuojama SDN tinklo valdymo sąsaja (interfeisas). SDN tinklo valdymo sąsaja įprastai būna trijų tipų – grafinė, komandinės eilutės ir REST API;

- Kontrolės (Control plane) – šis sluoksnis kontroliuoja SDN tinklo vykdymą, pagal valdymo sluoksnyje suvestą konfigūraciją. Funkcija realizuojama SDN tinklo kontroleriais;
- Transporto (Data Plane) – sluoksnis atlieka realų paketų transportavimą ir / arba transformavimą pagal lenteles, kurias formuoja ir kontroliuoja kontrolės sluoksnis. Funkcija realizuojama SDN tinklo virtualiais įrenginiais (maršrutizatoriai, komutatoriai ir ugniasienės).

SDN tinklo architektūra pavaizduota žemiau (pav. 7-17 SDN tinklo architektūra schema).

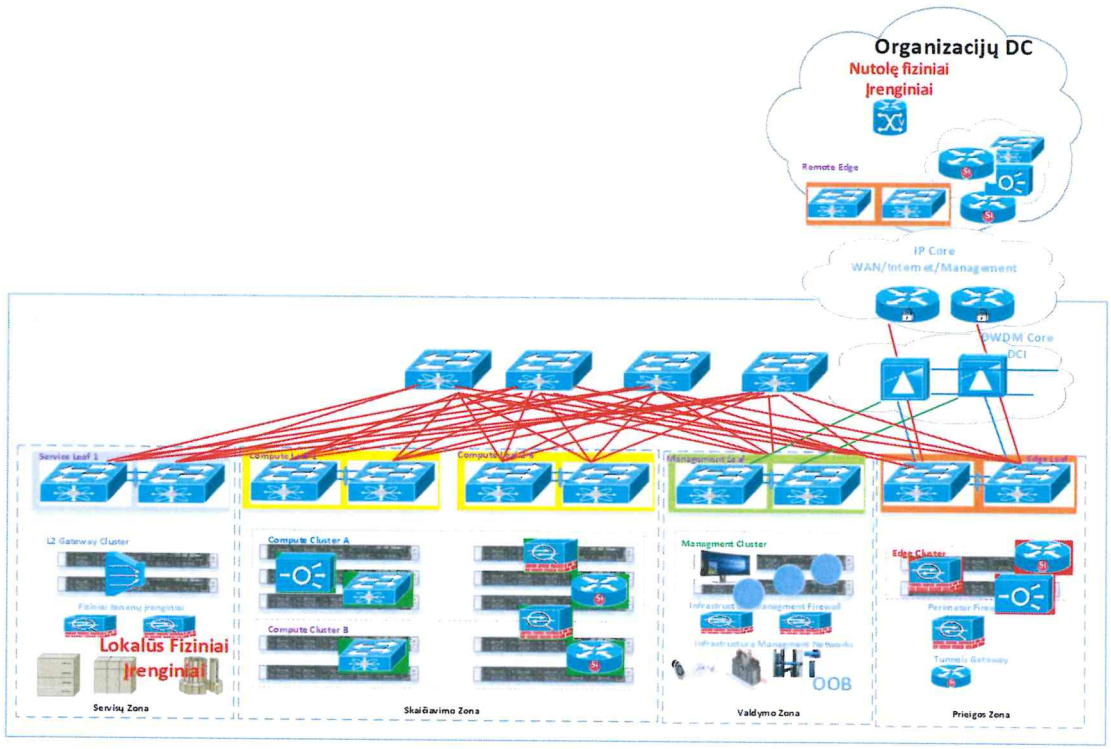
pav. 7-17 SDN tinklo architektūra schema

7.1.3.3.1.1 SDN tinklo komponentai

Visi SDN tinklo komponentai yra virtualūs ir talpinami fiziniuose serveriuose. Fiziniai serveriai grupuojami į keturias telkinių grupes:

- Valdymo (Management Cluster) – fizinių serverių telkiniai, kuriuose įdiegti valdymo ir kontrolės sluoksnių komponentai bei SDN tinklo valdymo sąsaja ir kontroleriai;
- Prieigos (Edge Cluster) – fizinių serverių telkiniai, kuriuose įdiegti virtualūs, prieigos valdymui skirti, tinkliniai įrenginiai (prieigos maršrutizatoriai (edge routers), srautų balansavimo įrenginiai, perimetro ugniasienės);
- Organizacijų (Compute Cluster) – fizinių serverių telkiniai, kuriuose įdiegti virtualūs organizacijų tinkliniai įrenginiai (organizacijų maršrutizatoriai (tenant routers), organizacijų srautų balansavimo įrenginiai, organizacijų tinklų segmentacijos ir mikrosegmentacijos ugniasienės).
- Paslaugų (Service Cluster) – fizinių serverių telkiniai, kuriuose įdiegti tenantų fizinių ir virtualių segmentų susiejimo mazgai. Pagrindinis šių mazgų tikslas išplėsti tenanto virtualaus tinklo segmentus fiziniais įrenginiais, tokiais kaip ugniasienės arba duomenų bazės, įdiegtos fiziniuose serveriuose.

SDN komponentų talpinimas telkiniuose pavaizduotas žemiau (pav. 7-18 SDN komponentų talpinimo schema).



pav. 7-18 SDN komponentų talpinimo schema

7.1.3.3.1.2 Telkinių sujungimai

Valdymo, prieigos ir organizacijų telkiniai į duomenų centrų tinklą jungiami pagal universalią serverių prijungimo schemą.

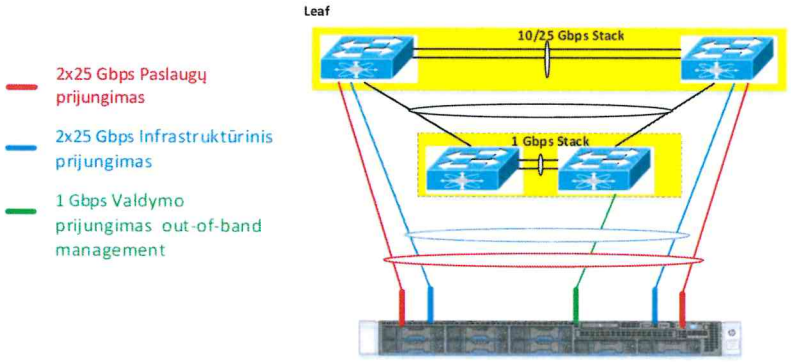
Fiziniai serveriai į duomenų centrų tinklą jungiami naudojant Multi – Chassis Link Aggregation Group (MLAG or MCLAG) virtualizavimo technologiją. Ši technologija leidžia serverius prijungti prie dviejų ToR komutatorių, sudarančių vieną DC tinklo Leaf. Šio sprendimo privalumai – patikimumas ir našumas. Našumas išgaunamas užtikrinant srautų balansavimą. Patikimumas išgaunamas serverius lygiagrečiai prijungiant prie dviejų komutatorių.

Serveriai fiziškai prie komutatorių jungiami:

- Paslaugos – 2x25Gbps[8] portais, sujungtais į vieną virtualų, naudojant MLAG technologiją;
- Infrastruktūrinis – 2x25Gbps portais, sujungtais į vieną virtualų, naudojant MLAG technologiją;
- Valdymo – nedubliuotais 1x1Gbps sujungimais. Jungiami serverių valdymo interfeisai (out-of-band – OOB).

Tipinė serverių prijungimo prie duomenų centrų tinklo schema pateikta žemiau (pav. 7-19 Telkinių sujungimų schema).

[8] Atsižvelgiant į SDN tinklo realizacijos specifiką gali būti naudojamos kitos konfigūracijos LAN tinklo adaptateriai (pvz. 4x10GbE, 2x100 GbE ar pan.).

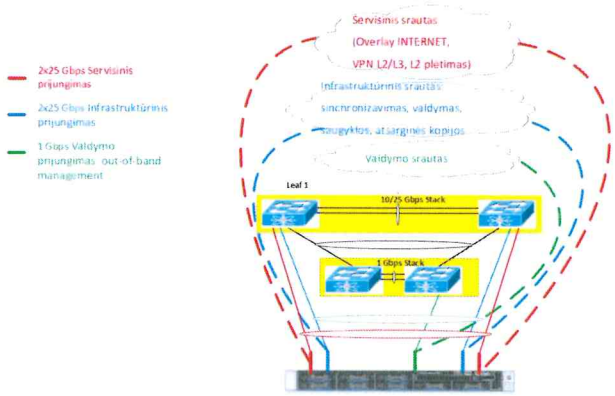


pav. 7-19 Telkinių sujungimų schema

Loginis serverių prijungimas realizuojamas klasifikuojant srautus pagal jų paskirtį. Suklasifikuoti srautai nukreipiami per konkrečius portus:

- Paslaugų srautas – šis srautas apima Overlay ir išorinių sujungimų (interneto, WAN L2/L3 VPN, L2 plėtimas į išorines infrastruktūras) srautus. Paslaugų srautams naudojami paslaugų portai;
- Infrastruktūrinis srautas – šis srautas apima sinchronizavimo, valdymo ir rezervinio duomenų kopijavimo srautus. Infrastruktūriniam srautui naudojami infrastruktūriniai portai;
- Valdymo srautas – šis srautas apima fizinės įrangos išorinių OOB valdymo interfeisų srautus. Valdymo srautui naudojami valdymo portai.

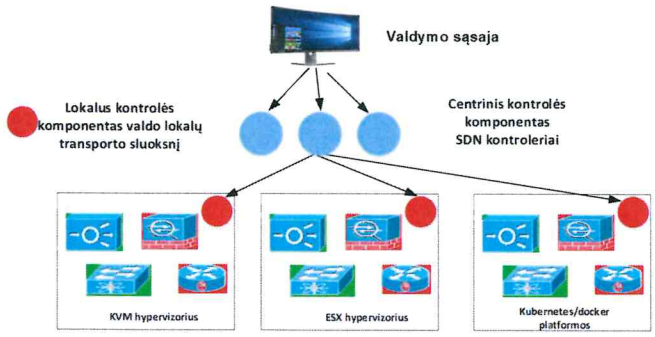
Tipinė telkinių sujungimų ir srautų schema pateikta žemiau (pav. 7-20 Telkinių sujungimų ir srautų schema).



pav. 7-20 Telkinių sujungimų ir srautų schema

7.1.3.3.1.3SDN heterogeniškumas

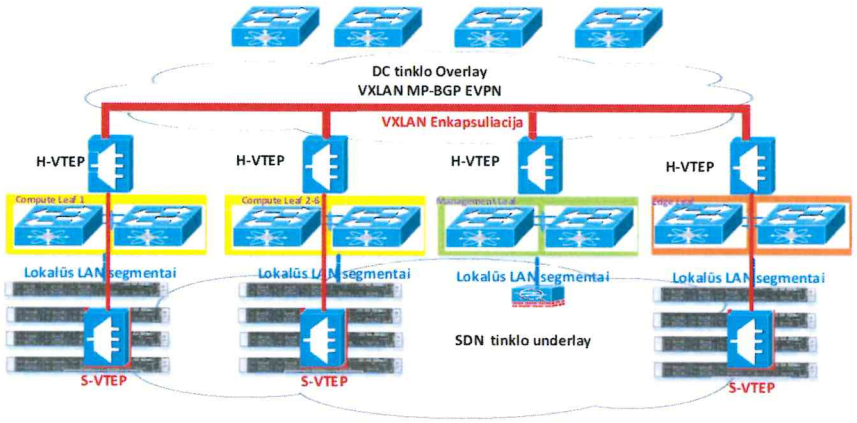
SDN kaip vieningas tinklas dirba heterogeninėse aplinkose ir nepriklauso nuo skaičiavimo aplinkų. SDN tinklas – vieningas universalus tinklas, apimantis šias aplinkas: ESX, KVM, OpenStack, Kubernetes, ir Docker. Sprendimo schema pavaizduota žemiau (pav. 7-21 SDN heterogeninių aplinkų tinklas).



pav. 7-21 SDN heterogeninių aplinkų tinklas

7.1.3.3.1.4 SDN underlay architektūra

SDN Underlay užtikrinamas duomenų centrų tinklo Overlay. Maršrutizavimo / komutavimo paslaugomis realizuojamas pasiekiamumas tarp virtualių tunelio interfeisų (Software Virtual Tunnel End Points (S-VTEPs)). Koncepcinė sprendimo schema pavaizduota žemiau (pav. 7-22 SDN Underlay architektūros schema).



pav. 7-22 SDN Underlay architektūros schema

7.1.3.3.1.5 SDN overlay architektūra

SDN overlay – dinaminių L2/L3 (pagal OSI modelį) tunelių rinkinys, transportuojantis paketus tarp dviejų S-VTEP, esančių skirtinguose serveriuose. SDN overlay konstruojamas VXLAN arba GENEVE technologijos pagrindu.

7.1.3.3.2 Paslaugų domenas

Paslaugų domeną sudaro trys paslaugų grupės – transporto, saugumo ir stebėjimo.

7.1.3.3.3 SDN transporto servisai

Transporto (maršrutizavimo / komutavimo) paslaugos realizuojamos SDN overlay technologijomis. Šiuo atveju neprojektuojami dedikuoti tuneliai (priešingai nei duomenų centrų tinklų atveju) realizuojami paskirstytais tinkliniais sprendimais. Paskirstyti tinkliniai sprendimai – paskirstytas maršrutizatorius ir paskirstytas komutatorius.

7.1.3.3.4 SDN Saugumo paslaugų plėtimas

SDN saugumo paslaugos ugniasienes, realizuojančias L2-L4 (pagal OSI modelį) kontrolės mechanizmų funkcionalumą, išplečiame L7 (pagal OSI modelį) kontrolės mechanizmu ir papildomais funkcionalumais (įsilaužimų aptikimų / prevencijos sistemomis (IDS ir IPS)).

7.1.3.3.5 SDN stebėjimo paslaugų plėtimas

SDN stebėjimo paslaugos funkcionalumas išplečiamas specifiniais monitoringo sprendimais, orientuotais į pilną SDN tinklų matomumą ir kontrolę. Šie sprendimai plačiau detalizuojami prie organizacijų tinklo stebėjimo ir valdymo sprendimų.

7.1.3.3.6 SDN paslaugų optimizavimas

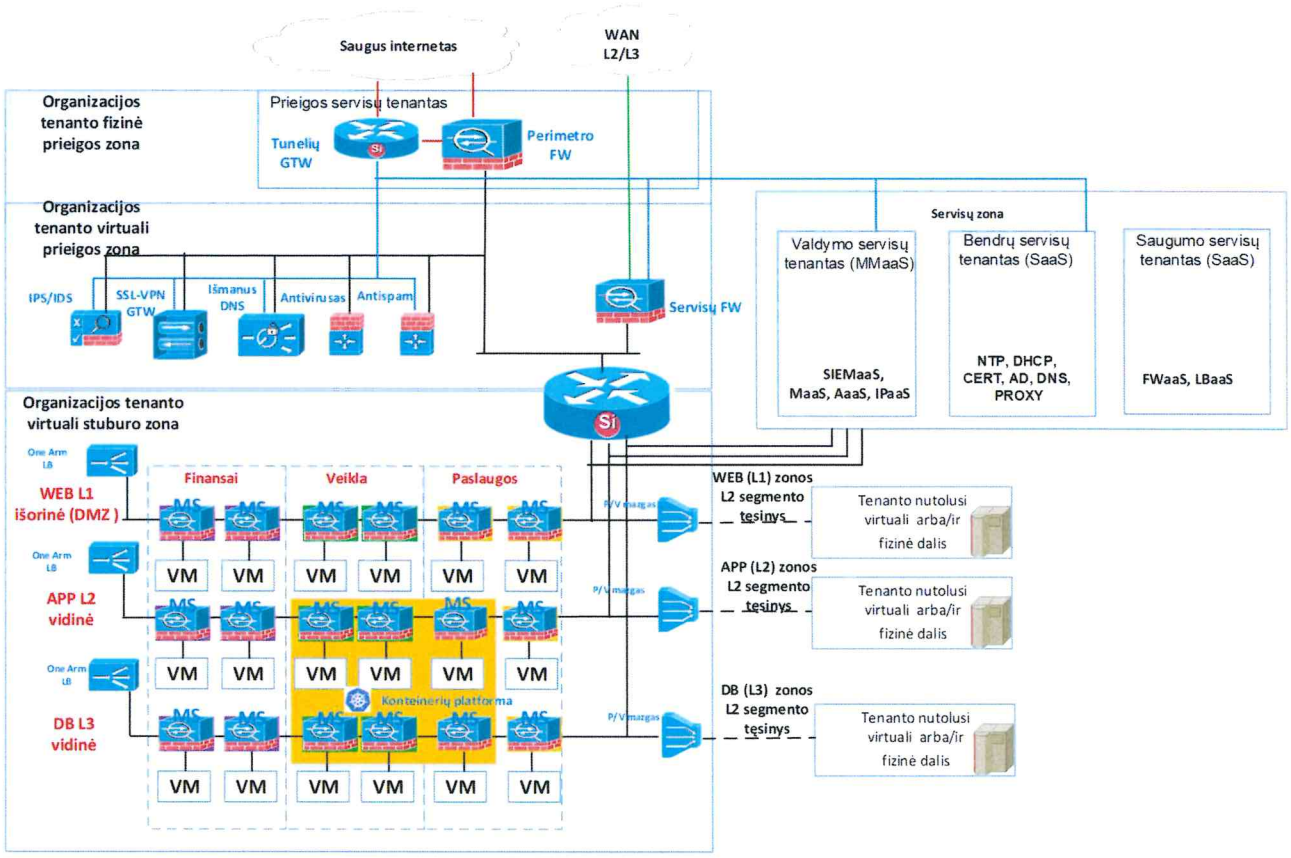
Siekiant užtikrinti SDN tinklo transporto ir saugumo paslaugų pakankamą našumą, nuspręsta šias paslaugas vykdyti ant specialių dedikuotų procesorių, o ne ant centrinio fizinio serverio procesoriaus. Dedikuoti procesoriai įprastai įmontuojami į serverių tinklines sąsajas. Tokiuose sprendimuose didžiausias našumas išgaunamas naudojant paskirstytų funkcijų vykdymo technologijas (SR-IOV (Single Root I/O Virtualization) arba ASAP (Accelerated Switching and Packet Processing)), kurių esmė SDN tinklo funkcijas vykdyti naudojant specifinius įrenginius. Šį sprendimą planuojama naudoti VXLAN enkapsuliacijai / dekapsuliacijai, paketų klasifikavimui pagal L2-L4 antraščių (Header) atributus, Quality of service (QoS) ir Access Control List (ACL).

7.1.3.4 Organizacijų tinklas

Organizacijų tinklas – konkrečios įstaigos, organizacijos arba jos padalinio atskiras virtualus arba hibridinis (virtualus ir fizinis tinklas) tinklas, kuris naudojasi DC ir debesijos tinklo paslaugomis. Naudojant organizacijų tinklą sujungiami organizacijos IT infrastruktūros įrenginiai (serveriai, saugumo įrenginiai ir t.t.) į vieną homogeninį tinklą.

7.1.3.4.1 Organizacijų tinklo architektūra

Organizacijų tinklu vadinamas organizacijos vidinis tinklas, kuris sujungia organizacijos IT infrastruktūros elementus į bendrą loginį vienetą. Bendroji organizacijos tinklo architektūra pateikta žemiau (pav. 7-23 Bendroji organizacijos tinklo architektūros schema).



pav. 7-23 Bendroji organizacijos tinklo architektūros schema

7.1.3.4.2 Organizacijos tinklo zonos

Išorinių paslaugų atžvilgiu organizacijos tinklas dalinamas į dvi zonas – prieigos ir stuburo.

7.1.3.4.2.1 Organizacijos tinklo prieigos zona

Prieigos zona skirta talpinti tinklo elementus, kurie tiesiogiai bendrauja su išoriniais servisais, esančiais išoriniuose tinkluose. Atsižvelgiant į tinklinių įrenginių tipą (virtualūs ar fiziniai), prieigos zona skirstoma į organizacijos fizinę prieigos zoną ir organizacijos virtualią prieigos zoną.

Organizacijos fizinės prieigos zonai priklausantys tinkliniai įrenginiai tiesiogiai jungiami į duomenų centrų tinklą pagal bendrą tinklo įrenginių prijungimo modelį. Šioje zonoje talpinami žemiau nurodomi tinklo elementai:

- Perimetro ugniasienė – skirta apsaugoti organizacijas nuo išorinių grėsmių / įsilaužimų;
- Tunelių koncentratorius – skirtas terminuoti IPsec ir GRE tunelius.

Organizacijos virtualioje prieigos zonoje priklausantys tinkliniai įrenginiai, virtualizuojantys tinklo funkcijas NFV (Network Function virtualization) virtualiose mašinose. Šioje zonoje talpinami žemiau nurodomi tinklo elementai:

- SSL VPN koncentratorius – IT administratorių prisijungimo taškas, terminuojantis SSL sesijas;
- Išmanus DNS – tikrina aplikacijų gyvybingumą;
- AntiVirus sprendimas – apsaugo organizacijos įrenginius nuo virusų;
- AntiSpam sprendimas – apsaugo nuo spam laiškų;
- IPS/IDS sprendimas – įspėja arba apsaugo organizaciją nuo įsilaužimų.

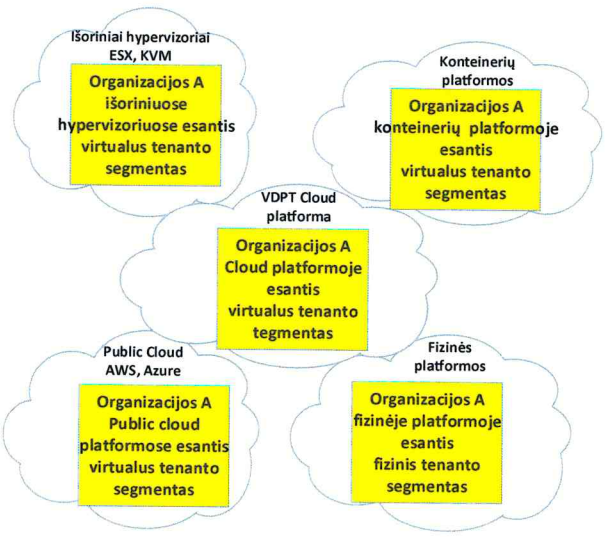
7.1.3.4.2.2 Organizacijos tinklo stuburo zona

Organizacijos tinklo stuburo zona skirta talpinti tinklo elementus, kurie tiesiogiai nebendrauja su išorinėmis paslaugomis, esančiomis išoriniuose tinkluose, o realizuoja organizacijos vidines funkcijas, kitaip tariant, skirta organizacijai priklausančias aplikacijas sujungti lokaliu tinklu. Organizacijos tinklo stuburo zona pagal serverių funkcijas skirstoma į išorinę ir vidinę. Išorinėje zonoje talpinami serveriai, kurie suteikia vartotojams sąsajas. Vidinėje zonoje talpinami serveriai, kurie atlieka realią aplikacijų logiką ir talpina duomenis. Tinklo lygyje išorinė ir vidinė zona realizuojamos identiškai. Skirtumas išorinių srautų atžvilgiu – išoriniai srautai gali patekti tik į stuburo zonos išorinę zoną. Stuburo zonoje talpinami žemiau nurodomi tinklo elementai:

- Tenanto ugniasienės – skirtos apsaugoti virtualius serverius nuo vidinių grėsmių. Realizuoja mikrosegmentacijos modelį, kur kiekvieno serverio apsauga realizuota individuliai atsižvelgiant į aplikacijų srautų logiką;
- Srautų balansavimo įrenginiai – skirti virtualizuoti serverių vykdomas funkcijas ir balansuoti srautus tarp serverių.

7.1.3.4.3 Organizacijos tinklo heterogeniškumas

Organizacijos tinklo heterogeniškumas suprantamas kaip organizacijos tinklo pasiskirstymas įvairiose vykdymo platformose (fizinė įranga, hypervizoriai (ESX, KVM), konteineriai, Public Cloud AWS, Azure). Organizacijos tinklo heterogeniškumas pateiktas žemiau (pav. 7-24 Heterogeniško organizacijos tinklo architektūros schema).



pav. 7-24 Heterogeniško organizacijos tinklo architektūros schema

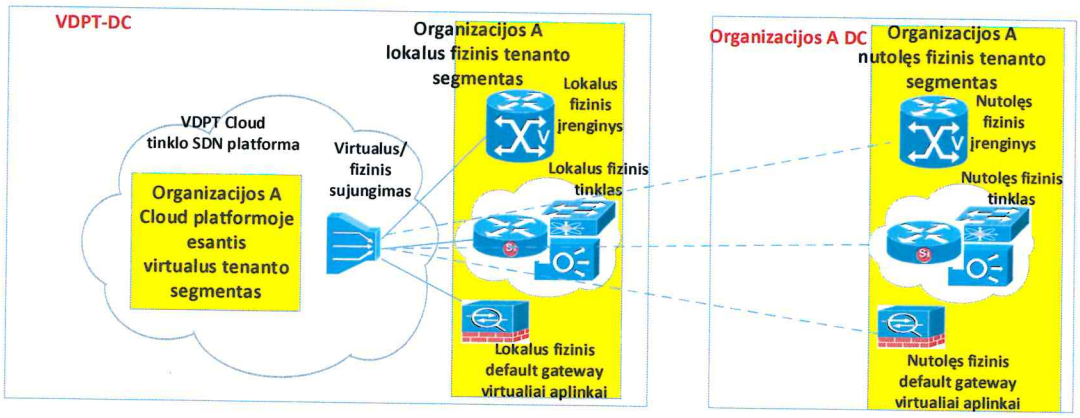
7.1.3.4.4 Organizacijos tinklo sujungimas su fizinėmis platformomis

Virtuali organizacijos tinklo dalis, esanti VDPT platformoje, gali būti sujungta su fizine platforma, kuri savo ruožtu galėtų būti lokaliame DC fabriko tinkle arba nutolusiame organizacijos padalinyje.

Išoriniai įrenginiai organizacijos tinklo atžvilgiu gali atlikti šias funkcijas:

- Default Gateway – organizacijos tam tikro tinklo segmento default gateway, skirtas segmentui bendrauti su išore;
- Lokalus ir / arba nutolęs fizinis tinklas – visas tinklas, prie kurio prijungti fiziniai įrenginiai, reikalingi organizacijos tinklui funkcionuoti;
- Organizacijos fizinis įrenginys – organizacijos tinklui funkcionuoti reikalingas fizinis įrenginys.

Koncepcinė šios sprendimo dalies schema pateikiama žemiau (pav. 7-25 Organizacijos tinklo sujungimo su fizinėmis platformomis architektūros schema).



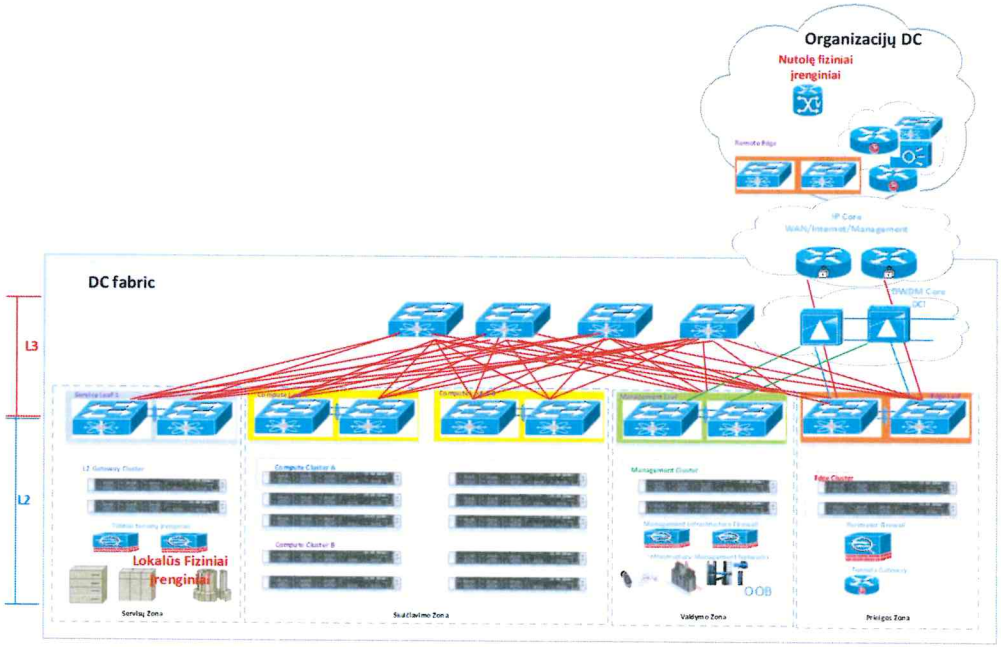
pav. 7-25 Organizacijos tinklo sujungimo su fizinėmis platformomis architektūros schema

7.1.3.4.5 Organizacijos lokalaus fizinio segmento talpinimas DC

Organizacijos lokalūs fiziniai įrenginiai debesijos duomenų centre traktuojami kaip paslaugos ir talpinami paslaugų zonoje. Fiziniai organizacijų įrenginiai jungiami į dedikuotus paslaugų zonos komutatorius ir per virtualių / fizinių sujungimų komponentus fiziniai įrenginiai prijungiami prie virtualaus organizacijos segmento.

Virtualus / fizinis sujungimo komponentas yra sąsaja tarp fizinių įrenginių ir virtualaus organizacijos tinklo. Komponentas projektuojamas pagal aukšto patikimumo sprendimų projektavimo principus, kad vieno fizinio įrenginio gedimo atveju organizacijos tinklo veikimui įtakos nebūtų.

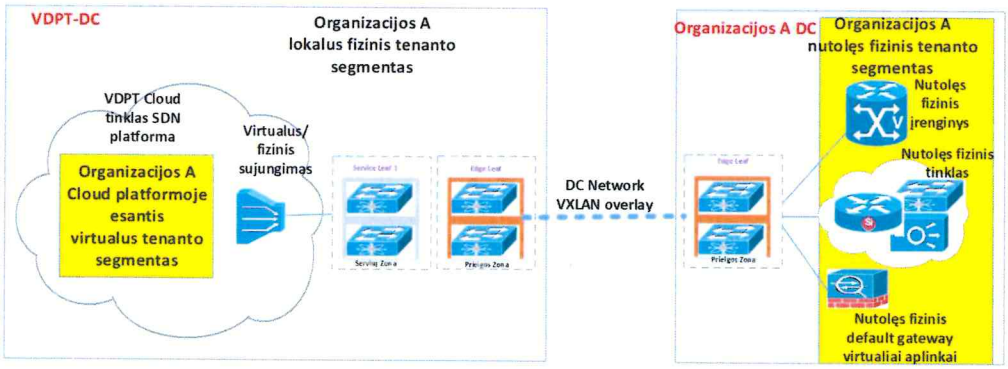
Organizacijos lokalaus fizinio segmento talpinimas DC pateiktas žemiau (pav. 7-26 Organizacijos lokalaus fizinio segmento talpinimo DC schema).



pav. 7-26 Organizacijos lokalaus fizinio segmento talpinimo DC schema

7.1.3.4.6 Organizacijos nutolusio fizinio segmento prijungimas duomenų centre

Organizacijos nutolę fiziniai įrenginiai prijungiami pasinaudojus DC tinklu. Šiam tikslui organizacijos DC diegiame DC prieigos (edge) sprendimą, kuris užtikrina VXLAN Overlay tarp VDPT DC ir organizacijos DC. Šio Overlay pagalba yra ištęsiamas virtualus organizacijos segmentas. Organizacijos nutolusio fizinio segmento prijungimas pateiktas žemiau (pav. 7-27 Organizacijos nutolusio fizinio segmento prijungimo duomenų centre schema).

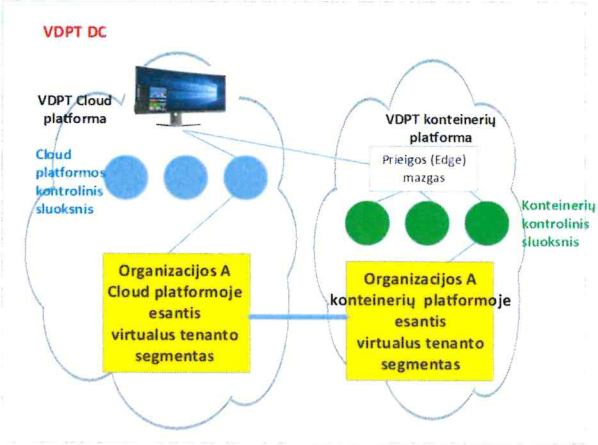


pav. 7-27 Organizacijos nutolusio fizinio segmento prijungimo duomenų centre schema

7.1.3.4.7 Organizacijos tinklo sujungimas su konteinerių platformomis

Virtualus organizacijos tinklo segmentas, esantis VDPT platformoje, gali būti sujungtas su organizacijos segmentu, realizuotu konteinerių platformoje. Integracija realizuojama diegiant VDPT platformos prieigos (Edge) komponentą, kuris įgalina VDPT platformos valdymo elementus valdyti konteinerių tinklus kaip savo nuosavus. Realizavus šį sprendimą VDPT platformos valdymo elementai gali kurti virtualius tinklus, saugumo politikas bei realizuoti srautų balansavimą konteinerių platformoje. Organizacijos tinklo sujungimas su

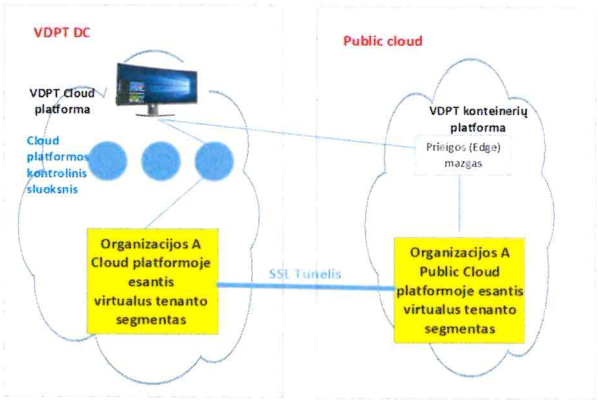
konteinerių platforma pateiktas žemiau (pav. 7-28 Organizacijos tinklo sujungimo su konteinerių platformomis schema).



pav. 7-28 Organizacijos tinklo sujungimo su konteinerių platformomis schema

7.1.3.4.8 Organizacijos tinklo sujungimas su public cloud platformomis

Virtualus organizacijos tinklo segmentas, esantis VDPT platformoje, gali būti sujungtas su organizacijos tinklo segmentu, realizuotu public cloud platformoje. Integracija realizuojama diegiant VDPT platformos prieigos (Edge) komponentą PSG, kuris įgalina VDPT platformos valdymo elementams valdyti public cloud tinklus, kaip savo nuosavus. Realizavus šį sprendimą VDPT platformos valdymo elementai gali kurti virtualius tinklus, valdyti saugumo politikas bei realizuoti srautų balansavimą public cloud platformose. Organizacijos tinklo sujungimas su public cloud platforma pateiktas žemiau (pav. 7-29 Organizacijos tinklo sujungimo su public cloud platformomis schema).



pav. 7-29 Organizacijos tinklo sujungimo su public cloud platformomis schema

7.1.3.4.9 Prieigos paslaugų organizacijos tinklas

Prieigos (Edge) paslaugų organizacijos tinklas skirtas talpinti prieigos paslaugoms, kurias sudaro žemiau nurodyti elementai:

- Ugniasienės paslauga (FWaaS – Firewall as a Service) – ši paslauga suprojektuota iš perimetro fizinės multitenant ugniasienės. Fizinės ugniasienės virtualios

ugniasienės sudaro organizacijų tinklų fizinės prieigos zoną, kurioje atliekama prieigos kontrolės funkcija. Ši paslauga teikiama dviem modeliais – dedikuotu ir bendro naudojimo (shared). Dedikuotas modelis – fizinės ugniasienės viena (arba daugiau) virtuali ugniasienė dedikuota organizacijai. Bendro naudojimo (shared) modelis – fizinės ugniasienės viena virtuali ugniasienė naudojama keletui organizacijų;
- VPN paslauga (VPNaaS – VPN as a Service) – ši paslauga suprojektuota specializuoto aukšto našumo maršrutizatoriaus pagrindu, kuriame atliekamas organizacijos GRE ir IPsec tunelių terminavimas.

7.1.3.4.10 Bendrų paslaugų tenantas

Bendrų paslaugų organizacijos tinklas skirtas talpinti debesijos platformos infrastruktūrines paslaugas ir naudoti jų funkcionalumą debesijos platformos veiklai užtikrinti. Tam tikros paslaugos, pvz. kaip NTP, galės būti naudojamos ir skirtingų tenantų poreikiams. Šiame tinkle talpinamos žemiau nurodomos paslaugos:

- NTP – tikslaus laiko sinchronizavimo paslauga, skirta, kad visi IT įrenginiai turėtų vienodai tikslų laiką;
- DHCP – automatinė IP adresų dalinimo ir valdymo paslauga;
- CERT – automatinė sertifikatų dalinimo, valdymo ir saugojimo paslauga;
- AD – direktorijų, tapatybių valdymo paslauga;
- DNS – domenų vardų sistemos paslauga.

7.1.3.4.11 Valdymo paslaugų tenantas

Valdymo paslaugų segmentas skirtas talpinti organizacijų valdymo, stebėjimo, automatizavimo, programavimo įrankius ir teikti jų funkcionalumą kaip multitenant paslaugas organizacijoms. Šiame segmente talpinamos žemiau nurodomos paslaugos:

- Organizacijų saugumo paslauga (SIEMaaS (SIEM Security Information and Event Management)) – apimanti organizacijos tinkle esančių IT įrenginių saugumo žurnalų analizę, saugojimą ir koreliaciją, saugumo incidentų generavimą;
- Organizacijų stebėjimo paslauga (MaaS (Monitoring as a Service)) – apimanti organizacijos tinkle esančių IT įrenginių gyvybingumo stebėseną bei infrastruktūrinių incidentų generavimą;
- Organizacijų automatizacijos paslauga (AaaS (Automation as a Service)) – apimanti organizacijos tinklų sukūrimą bei valdymą taikant standartinius sprendimus bei gerąsias praktikas;
- Organizacijų tinklų programavimo paslauga (IPaaS Infrastructure programing as a Service) – apimanti organizacijos tinklų sukūrimą bei valdymą taikant standartinius sprendimus, laikant, kad organizacija arba jos dalis yra infrastruktūra kaip programinis kodas.

7.1.3.4.12 Saugumo paslaugų tenantas

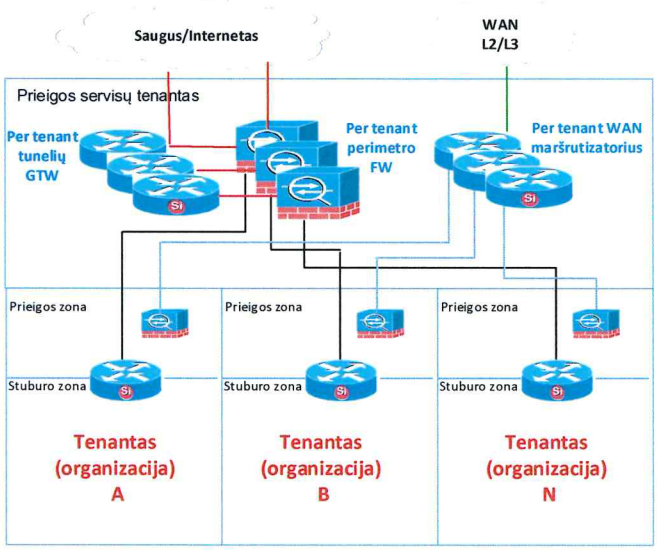
Tinklo saugumo paslaugų tenantas skirtas talpinti bendro naudojimo tinklo saugumo sprendimus. Šios paslaugos teikiamos skirtingų organizacijų tenantams, kaip bendro naudojimo paslaugos, t.y. tą patį tinklo saugumo įrenginį naudoja daugelis organizacijų. Šiame tenante talpinamos šios tinklo saugumo paslaugos:

- Ugniasienė kaip paslauga – suprojektuota iš virtualios ugniasienės. Paslauga teikiama bendru (shared) modeliu – kaip virtuali ugniasienė talpinanti keletą organizacijų;
- Srautų balansavimo paslauga – suprojektuota iš virtualaus srautų balansavimo įrenginio ir teikiama tenantams kaip paslauga, įgalinanti balansuoti tenanto srautus.

7.1.3.4.13 Multitenant architektūra

VDPT platforma konstruojama kaip Multitenant Cloud paslaugų tiekėjas, teikiantis paslaugas Vilniaus ir Kauno regionuose.

Vieno duomenų centro multitenantų architektūra pateikiama žemiau (pav. 7-30 Duomenų centro multitenant architektūros schema).



pav. 7-30 Duomenų centro multitenant architektūros schema

7.1.4 Tinklo valdymo architektūra

Bendras tinklas susideda iš trijų sluoksnių, kur kiekvieną sluoksnį sudaro atskiras nepriklausomas tinklas. Suprojektuoti šie tinklai: duomenų centrų, debesijos ir organizacijų / tenantų. Tinklai vienas nuo kito nepriklausomi, todėl kiekvieno sluoksnio valdymui projektuojami nepriklausomi sprendimai. Visi tinklų valdymo įrankiai talpinami specialiame valdymo tenante „Valdymo servisų tenantas“. Prieiga prie tinklo valdymo įrankių kontroliuojama PAM sprendimu, kuris užtikrina prieigos prie resursų kontrolę ir prisijungimo slaptažodžių valdymą.

Valdymo įrankiai ir tinklo segmentai pateikti lentelėje žemiau:

Tinklas	Įrankiai	Administratoriaus rolė
Duomenų centrų	Duomenų centrų tinklų – fabriko valdymo, automatizavimo įrankiai	DC tinklo fabriko tinklų administratoriai
Debesijos	SDN tinklo valdymo, automatizavimo įrankiai	SDN tinklo administratoriai

Organizacijų / Tenantų	Organizacijų / Tenantų tinklų automatizavimo ir valdymo	Tenantų tinklo administratoriai

Detaliau tinklų valdymo sprendimai aprašyti prie kiekvieno tinklo valdymo paslaugų domeno.

7.1.4.1 Duomenų centrų tinklo valdymo architektūra

Duomenų centrų tinklas yra fizinis tinklas, kuris atlieka transporto rolę debesijos tinklui. Duomenų centrų tinklo valdymui ir monitoringui projektuojami du tinklai: avarinio valdymo tinklas (OOB out-of-band managment network) ir darbinio valdymo tinklas (IB in-band). Kiekvienas duomenų centre esantis tinklinis įrenginys turi avarinio ir darbinio pajungimo įvadus. Tinklinio įrenginio avarinio pajungimo įvadas prijungtas į avarinį tinklą, o darbinio tinklo įvadas, dažniausiai virtualus, prijungtas į darbinio valdymo tinklą.

7.1.4.1.1 Duomenų centrų tinklo avarinio valdymo tinklas

Avarinio valdymo tinklas (OOB out-of-band managment network) skirtas avariniam prisijungimui prie tinklo, esant duomenų centro fabriko overlay tinklo sutrikimams.

Avarinio valdymo tinklas susideda iš trijų komponentų: ugniasienės, komutavimo tinklo ir avarinio valdymo modulio.

Avarinio tinklo ugniasienė – kiekviename duomenų centre esantis avarinio prisijungimo tinklas, ginamas dedikuotu ugniasienių klasteriu. Šis klasteris turi galimybę pasinaudojus GSM jungtimi „išeiti“ į internetą (tam, kad nutolusiems gamintojo palaikymo serviso konsultantams būtų suteikta prieiga prie duomenų centrų fabriko įrangos). Šis prisijungimo būdas naudojamas tik visišku duomenų centrų fabriko overlay sugedimo atveju pagal patvirtintą ir suderintą procedūrą.

Komutavimo tinklas – tinklas, jungiantis tinklinių prietaisų avarinio prisijungimo įvadus, per kuriuos galima pasijungti prie tinklinių prietaisų esant duomenų centro fabriko gedimui.

Avarinio valdymo modulis – avarinio valdymo modulis susideda iš įrankių rinkinio, skirto valdyti duomenų centrų tinklus esant avarinei situacijai.

7.1.4.1.2 Duomenų centrų tinklo darbinio valdymo tinklas

Duomenų centrų darbinio valdymo tinklas (IB in-band) skirtas darbiniams, kasdieniniams duomenų centro tinklo administravimo darbams. Šiuo tinklu naudojasi tinklo administratoriai, monitoringo, valdymo ir automatizavimo sistemos.

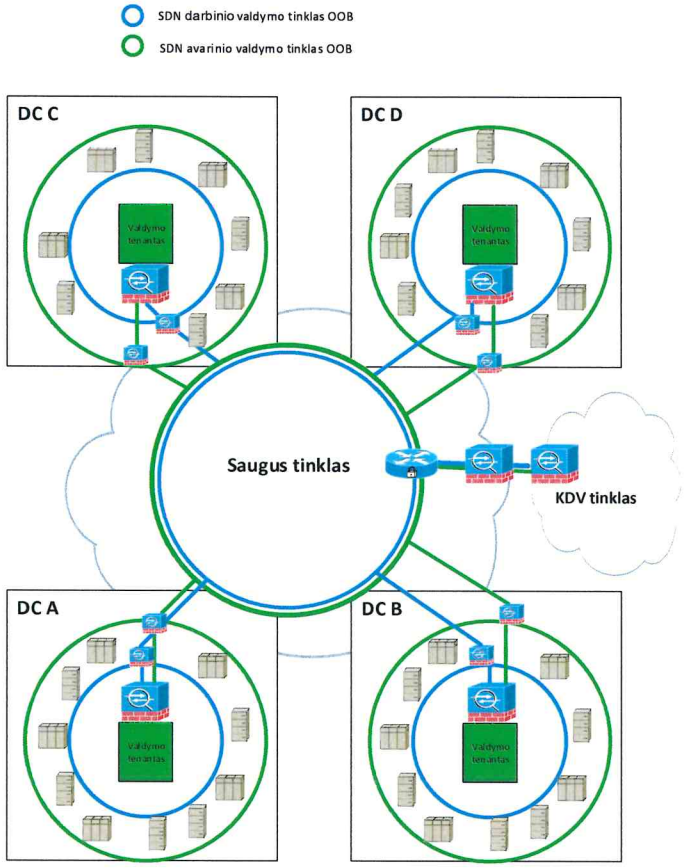
Darbinio valdymo tinklas susideda iš trijų komponentų: ugniasienės, darbinio virtualaus valdymo tinklo ir valdymo tenanto.

Darbinis virtualus valdymo tinklas – apjungiantis tinklinių prietaisų valdymą į virtualų vieningą tinklą, kurio dėka galima realizuoti kasdienines tinklo valdymo funkcijas.

Valdymo tenantas – talpinantis tinklų valdymo, monitoringo, automatizavimo, programavimo įrankius, kurių dėka realizuojama kasdieninės tinklo valdymo funkcijos.

Darbinio valdymo tinklo ugniasienė – kiekviename duomenų centre esantis darbinio valdymo tinklas, ginamas dedikuotu ugniasienių klasteriu, kuris kontroliuoja prieigą prie darbinio valdymo tinklo.

Duomenų centrų tinklo valdymo architektūra pateikta žemiau (pav. 7-31 Duomenų centrų tinklo valdymo architektūros schema).



pav. 7-31 Duomenų centrų tinklo valdymo architektūros schema

7.1.4.2 Debesijos tinklo valdymo architektūra

Debesijos tinklo valdymui ir monitoringui projektuojami du tinklai – avarinio valdymo tinklas (OOB out-of-band managment network) ir darbinio valdymo tinklas (IB in-band). Kiekvienas duomenų centre esantis SDN platformos serveris turi avarinio ir darbinio prijungimo įvadus. SDN platformos avarinio prijungimo įvadas prijungtas į debesijos avarinį tinklą, o darbinio tinklo įvadas į darbinio valdymo tinklą. Priešingai nei duomenų centrų tinklo atžvilgiu, debesijos avarinio ir darbinio valdymo tinklai yra virtualūs, ir suprojektuoti duomenų centrų fabriko technologijomis.

7.1.4.2.1 Debesijos SDN infrastruktūros avarinio valdymo tinklas

Avarinio valdymo tinklas (OOB out-of-band managment network) skirtas avariniam prisijungimui prie SDN infrastruktūros serverių OOB įvadų. Debesijos avarinio valdymo tinklas susideda iš trijų komponentų: ugniasienės, avarinio virtualaus valdymo tinklo, ir valdymo tenanto.

Debesijos avarinis virtualus valdymo tinklas – apjungiantis SDN infrastruktūros serverių OOB įvadų valdymą į virtualų vieningą tinklą.

Debesijos avarinio virtualus valdymo tinklo ugniasienė - kiekviename duomenų centre esantis debesijos avarinis valdymo tinklas ginamas ugniasienių klasteriu, kuris kontroliuoja prieigą prie debesijos avarinio valdymo tinklo.

Valdymo tenantas – talpinantis SDN infrastruktūros valdymo, monitoringo, automatizavimo ir programavimo įrankius, kurių dėka realizuojamos specializuotos SDN infrastruktūros valdymo funkcijos.

7.1.4.2.2 Debesijos SDN infrastruktūros darbinio valdymo tinklas

Debesijos SDN infrastruktūros darbinio valdymo tinklas (IB in-band) skirtas darbiniams, kasdieniams SDN infrastruktūros administravimo darbams. Šiuo tinklu naudojasi SDN infrastruktūros administratoriai, monitoringo, valdymo ir automatizavimo sistemos.

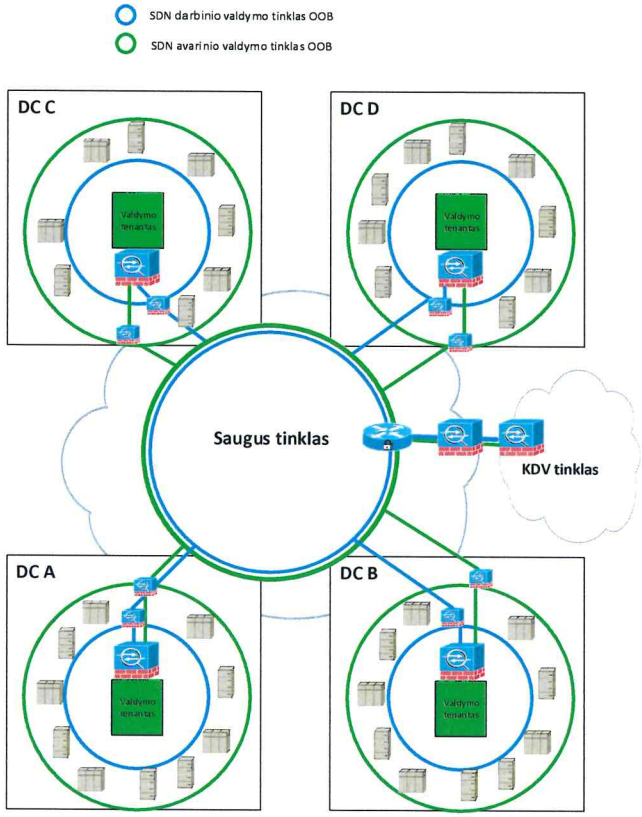
Debesijos SDN infrastruktūros darbinio valdymo tinklas susideda iš trijų komponentų: ugniasienės, darbinio virtualaus valdymo tinklo ir valdymo tenanto.

Debesijos SDN infrastruktūros darbinis virtualus valdymo tinklas – apjungiantis SDN infrastruktūros valdymą į virtualų vieningą tinklą, kurio dėka galima realizuoti kasdienines debesijos SDN infrastruktūros valdymo funkcijas.

Valdymo tenantas – talpinatis debesijos SDN infrastruktūros valdymo, monitoringo, automatizavimo, programavimo įrankius, kurių dėka realizuojama kasdieninės Debesijos SDN infrastruktūros valdymo funkcijos.

Debesijos SDN infrastruktūros darbinio valdymo tinklo ugniasienė – kiekviename duomenų centre esantis debesijos SDN infrastruktūros darbinio valdymo tinklas, ginamas dedikuotu ugniasienių telkiniu, kuris kontroliuoja prieigą prie debesijos SDN infrastruktūros darbinio valdymo tinklo.

Debesijos tinklo valdymo architektūra pateikta žemiau (pav. 7-32 Debesijos tinklo valdymo architektūros schema).



pav. 7-32 Debesijos tinklo valdymo architektūros schema

7.1.4.3 Organizacijų (tenantų) tinklo valdymo architektūra

Tenantų valdymo architektūra suprantama kaip debesijos platformos teikiamų valdymo paslaugų rinkinys. Šis paslaugų rinkinys realizuotas SaaS modeliu. Kiekviena tenato valdymo paslauga yra debesijos platformos teikiamas servisas.

8 Virtualizuotų duomenų talpyklų architektūros modelis

8.1 Duomenų saugojimo sluoksnio realizacija

Atlikus analizę paaiškėjo, kad didelė dalis I etape konsoliduojamų sistemų yra sukurtos senos kartos enterprise lygio technologijomis (Oracle ir MS DBVS sprendimai, skirtingų gamintojų Middleware sprendimai), kurios nėra pritaikytos veikimui debesijos aplinkoje, tačiau joms būtinas didelis pasiekiamumas bei duomenų apsauga. Siekiant aukšto pasiekiamumo ir poreikio duomenų saugos sprendimus užtikrinti platformos lygyje, nuspręsta duomenų saugojimui naudoti SAN tipo duomenų saugyklas. Šiam tikslui pasiekti naudojami žemiau įvardinti technologiniai sprendimai:

1. Virtualizuotos SAN tipo duomenų saugyklos, užtikrinančios vieningos loginės saugyklos resursų pateikimą serveriams dviejuose duomenų centruose (I etape tik Vilniaus regiono duomenų centruose, II – nepriklausomas sprendimas Kauno regiono DC);

2. Lokalios (duomenų centro apimtyje) SAN tipo duomenų saugyklos;
3. Lokalūs (NVMe technologijos pagrindu veikiantys) serverių diskiniai resursai, skirti konteinerių technologijų pagrindu veikiantiems sprendimams.

Įvertinus analizės etape pateiktus konsoliduojamų įstaigų / organizacijų duomenis, planuojamus naujų informcinių sistemų resursų poreikius, naujausias technologijas ir pasaulines praktikas, nuspręsta visoms duomenų saugykloms, skirtoms produkcinių duomenų saugojimui, naudoti 0,5 PiB naudingos talpos saugyklas. Siekiant optimalaus našumo bei resursų panaudojimo, saugykla atitiks tokius našumo reikalavimus – ne mažiau nei 300000 IOPS (apkrovos pobūdis – 8K blokas, 60/40 skaitymas / rašymas) atsako laikui neviršijant 1 ms. Atsižvelgiant į viešojo sektoriaus informacinių sistemų ir/arba registrų duomenų svarbą bei saugumo reikalavimus, numatoma, kad duomenų saugyklose duomenys bus saugomi užšifruoti (data at rest encryption), todėl visos duomenų saugyklos turi turėti galimybę palaikyti tiek lokalų, tiek centralizuotą šifravimo raktų valdymą.

Visos produkcinių duomenų saugojimui skirtos saugyklos projektuojamos SSD/NVMe diskų pagrindu. Mechaninių diskų pagrindu (HDD) veikiančių saugyklų nuspręsta nenaudoti dėl šių priežasčių:

- Tokių saugyklų našumas bus ženkliai mažesnis;
- Sprendimai užims daugiau vietos duomenų centruose bei naudos ženkliai didesnius elektros kiekius nei SSD/NVMe sprendimai;
- Sprendimuose nerekomenduojama naudoti duomenų optimizavimo sprendimų (deduplikacija ir / arba kompresija) dėl įtakos našumui;
- Konsolidacijai tinkamų sprendimų (su adekvačiais našumo reikalavimais) kaina, įskaitant įrangos palaikymo kaštus 5 metams, nuo SSD/NVMe pagrindu veikiančių sprendimų skiriasi iki 20%.

Rezervinių kopijų saugyklos – atskira duomenų saugojimo sprendimo dalis. Naudojamos technologijos detalizuotos rezervinio kopijavimo sprendimo dalyje.

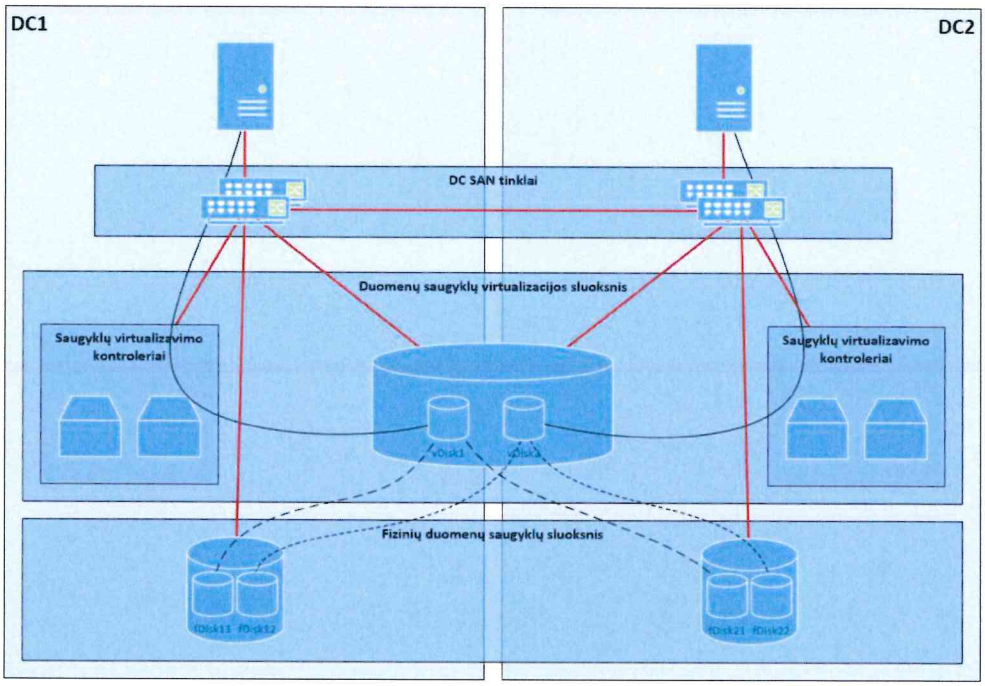
8.1.1 Virtualizuotos SAN tipo duomenų saugyklos

Aukšto patikimumo reikalaujantiems uždaviniams (ypač pavieniams (single instance) duomenų bazių ar kritinių aplikacijų diegimams) nuspręsta naudoti virtualizuotas duomenų saugyklas (pav. 8-1 Virtualizuoto duomenų saugojimo sluoksnio schema). Šis sprendimas būtų diegiamas per 2 duomenų centrus ir būtų sudarytas iš keleto principinių blokų:

1. Saugyklų virtualizavimo kontrolerių (priklausomai nuo gamintojo tai gali būti arba papildoma įranga, arba PĮ diegiama / aktyvuojama duomenų saugyklų kontroleriuose);
2. Duomenų saugyklų, esančių konkrečiuose duomenų centruose (backend). Priklausomai nuo resursų bei našumo poreikio gali būti naudojama daugiau nei 2 duomenų saugyklos.

Pagrindiniai veikimo principai:

- Saugyklų virtualizacijos kontroleriai sujungiami į išskleistą telkinį (distributed/stretched cluster);
- Virtualizacijos kontroleriai naudoja bendrą spartinančiąją atmintį (shared cache);
- Serveriai virtualizacijos telkinį traktuoja kaip vieną loginę duomenų saugyklą, tokiu būdu įgalinant diegti per kelis duomenų centrus išskleistus serverių tekinius, tradiciškai veikiančius vieno duomenų centro lygyje, nenaudojant jokių papildomų integracinių komponentų (supaprastintas sprendimo valdymas);
- Loginių diskų resursai iš saugyklų pateikiami (presented) ne tiesiogiai serveriams, bet virtualizaciją atliekantiems kontroleriams;
- Virtualizacijos kontroleriai suformuoja diskinės talpos telkinį, iš kurio pateikiami loginiai diskai serveriams;
- Kiekvienas serveriui pateikiamas diskas saugomas 2 galutinėse duomenų saugyklose (backend), tokiu būdu užtikrinant 2 nepriklausomų duomenų komplektų buvimą fiziniame duomenų saugyklų lygmenyje bei sistemų veikimą vieno duomenų centro praradimo atveju;
- Virtualizacijos sprendimai paprastai naudoja papildomas arbitravimo technologijas, jog būtų išvengta klasterio padalinimo pusiau scenarijaus;



pav. 8-1 Virtualizuoto duomenų saugojimo sluoksnio schema

Pagal pradinės konsoliduojamų sistemų imties duomenų kiekių analizės rezultatus šis sprendimas turi pateikti 1 PiB naudingos talpos.

8.1.2 Lokalios SAN tipo duomenų saugyklos

Sprendimams, nereikalaujantiems padidinto pasiekiamumo užtikrinimo per 2 duomenų centrus platformos lygyje, siūloma naudoti lokalias duomenų centrų SAN tipo duomenų saugyklas.

Pagal pradinės konsoliduojamų sistemų imties duomenų kiekių analizės rezultatus šis sprendimas turi pateikti 1 PiB naudingos talpos per duomenų centrą.

8.1.3 Lokalūs serverių diskiniai resursai

Lokalūs (NVMe technologijos pagrindu veikiantys) serverių diskiniai resursai skirti konteinerių technologijų pagrindu veikiantiems sprendimams.

I projekto etape šio tipo duomenų saugojimo sprendimo naudoti neplanuojama, nes nebus diegiama atskira konteinerių pagrindu veikiantiems sprendimams skirta platforma. Tolimesniuose projekto etapuose vystant konteinerių pagrindu veikiančius sprendimus ši technologija gali būti naudojama.

9 Saugos sprendimo modelis

Debesijos platformos saugumo architektūrą sudaro saugaus tenanto architektūra, debesijos saugumo servisai, saugumo monitoringo centras ir saugaus priėjimo architektūra.

Architektūra projektuojama nagrinėjant kibernetines atakas ir konstruojant atakų prevencijos sprendimus, kurie grįsti paslaugų modeliu, kai kiekvienas sprendimas realizuojamas kaip debesijos tinklo paslauga.

9.1 Atakos atakų vektoriai ir prevencijos sprendimai

Debesijos platformos saugumo architektūra nusako, kokia ji turėtų būti kibernetinių atakų atžvilgiu. Sąryšis tarp atakų, atakų vektorių, grėsmių, saugumo sprendimų ir saugumo servisų pavaizduotas žemiau esančioje lentelėje.

Atakos vektorius	Atakos vektoriaus aprašymas	Grėsmė	Saugumo sprendimas	Saugumo paslauga
Naudotojai	Darbuotojai, trečiosios šalys, klientai, administratoriai	Atakuotojai pasieks konfidencialią informaciją	Tapatybės nustatymu paremtos prieigos	Prieigos teisių valdymas
Tinklas	Fizinė, virtualaus tinklo infrastruktūra - maršrutizatoriai, komutatoriai, naudojami prieigos, paskirstymo, pagrindinio tinklo paslaugų sluoksnių sujungimui. (angl. Physical, virtual network infrastructure; routers, switches, used to connect access, distribution, core, and	Neautorizuota prieiga ir piktybiškai transformuoti paketai duomenų centruose ir tarp jų. (angl. Unauthorized accessand malformed packetsbetween and within the data center.)	Nusakomos būsenos sesijų, protokolų filtravimas ir tikrinimas tarp segmentų duomenų centre. (angl. Stateful filtering and protocol inspection between segments in the data center.	Duomenų centro perimetro ugniasienė, Tenantų segmentų ugniasienė, Tenantų mikrosegmentacijos ugniasienės. (angl. DC Edge firewall, Tenant Segment Firewall, Tenant insegment microsegmentation firewall)
		Išpuoliai naudojant kirminus, virusus ar kitus metodus. (angl. Attacks using	Įsibrovimo prevencija: užpuolimų blokavimas parašais ir anomalijų analizė. (angl. Intrusion Prevention:Blocking of attacks by signatures and anomaly analysis.)	Duomenų centro perimetro ugniasienė (angl. DC Edge firewall)

	services layers together.)	worms, viruses, or other techniques.)		
		Neteisėta prieiga ir kenkėjiškas srautas tarp segmentų. (angl. Unauthorized access and malicious traffic between segments.)	Žymėjimas: programinės įrangos segmentavimas naudojant VLAN (angl. Tagging:Software-basedsegmentation using VLANs)	Duomenų centro Tenanto ugniasienė (angl. DC Tenant firewall)
		Kenkėjiškų programų platinimas tinkluose arba tarp serverių ir įrenginių. (angl. Malware distribution across networks or between servers and devices.)	Kenkėjiškų programų blokavimo programinė įranga: nustato, blokuoja, analizuoja kenkėjiškus failus ir jų perdavimą. (angl. Anti-Malware: Identify, block, and analyze malicious files and transmissions)	Ugniasienės su kenkėjiškų programų filtravimu.
		Kenkėjiškos programos ir atakos, kurioms nėra sukurtos įrangos gamintojų apsaugos priemonės (angl. Zero-day malware and attacks.)	Intelektualus grėsmių aptikimas: kontekstinės žinios esamų ir atsirandančių pavojų. (angl. Threat Intelligence: Contextual knowledge of existing and emerging hazards.)	
		Srauto, telemetrijos ir duomenų eksfiltracijos iš sėkmingų atakų. (angl. Traffic, telemetry, and data exfiltration from successful attacks.)	Srauto analizė: tinklo srauto metaduomenys nusakantys saugumo incidentus (angl. .Flow Analytics: Networktraffic metadata identifying security incidents.)	Tinklo matomumo įrankiai (angl. Network visibility tools)
Aplikacijos	Valdymo serveriai, duomenų bazės, srauto balansavimo įrenginiai	Neteisėtos prieigos ir neteisingai suformuoti paketai jungiantis prie paslaugų. (angl. Unauthorized access and malformed packets connecting to services.)	Aplikacijų matomumo kontrolė: tinklo komunikacijos tikrinimas. (angl. Application Visibility Control: Inspects network communications.)	

		Esminis tikslas - visiška įstaigos kontrolė ir įmonės žlugdymas. (angl. Single target for complete company control and destruction.)	Centralizuotas valdymas: valdymo, stebėsenos ir kontrolės mechanizmai visos įmonės mastu. (angl. Central Management: Company-wide management, monitoring, and controls.)	
		Kenkėjiškos programos ir atakos, kurioms nėra sukurtos įrangos gamintojų apsaugos priemonės (angl. Zero-day malware and attacks.)	Kenkėjiškų programų aptikimo aplinka: tikrina ir analizuoja įtartinus failus. (angl. Malware Sandbox: Inspects and analyzes suspicious files.)	
		Nešifruoto srauto vagystė. (angl. Theft of unencrypted traffic.)	Spartesnis TLS šifravimas perteikiant funkcijas specializuotiems įrenginiams, mikroschemoms. angl. TLS Encryption Offload: Accelerated encryption of data services.)	SSL VPN vartotojams Site-to-site IPsec
		Atakos į menkai išvystytų taikomųjų programų ir interneto svetainių pažeidžiamumus. (angl. .Attacks against poorly developed applications and website vulnerabilities.)	Žiniatinklio taikomųjų programų ugniasienė: išplėstinė aplikacijų kontrolė ir stebėjimas. (angl. Web Application Firewalling: Advanced application inspection and monitoring.)	WAF
Duomenų saugyklos	Duomenų laikmenos, duomenų bazės, tinklinės duomenų saugyklos.	Nešifruotų duomenų vagystė.	Duomenų šifravimas	Šifravimo raktai ir jų saugaus saugojimo priemonės (pvz. HSM).
Serveriai		Kenkėjiškų programų sklidimas tarp serverių. (angl. Malware distribution across servers.)	Nustatyti, blokuoti ir analizuoti kenkėjiškus failus ir duomenų perdavimą. (angl. Anti-Malware: Identify, block, and analyze malicious files and transmissions.)	
		Virusai sistemose.	Anti-Virus	Anti-Virus
		Neteisėtos prieigos ir	Serverio lygio ugniasienė: užtikina	Mikrosegmentacija

		neteisingai suformuoti paketai besijungiant prie serverių. (angl. Unauthorized access and malformed packets connecting to servers.)	mikrosegmentaciją. (angl. Host-based Firewall: Provides microsegmentation)	
		Žinomi pažeidžiamumai – atakos kryptis. (angl. Targeted attacks taking advantage of known vulnerabilities.)	Padėties vertinimas: serverio atitikties patikra, autorizacijos ir pataisymų diegimas. (angl. Posture Assessment: Server compliance verification, authorization, and patching.)	
		Įvairiapusės ir polimorfinės atakos. (angl. Diverse and polymorphic attacks.)	Analizė / koreliacija: realaus laiko informacijos saugos įvykių valdymas. (angl. Analysis/Correlation: Security event management of real-time information.)	SIEM
		Kirminų duomenų srautas demonstruojantis tinklo skenavimą. (angl. Worm traffic that exhibits scanning behavior.)	Anomalijos aptikimas: užsikrėtusių kompiuterių aptikimas pagal bandymą skenuoti kitus kompiuterius (angl. Anomaly Detection: Identification of infected hosts scanning for other vulnerable hosts.)	
		Esminis tikslas - visiška įmonės kontrolė ir įmonės žlugdymas. (angl. Single target for complete company control and destruction.)	Tapatybė / autorizacija: centralizuota tapatybės ir administravimo politika. (angl. Identity/Authorization: Centralized identity and administration policy.)	
		Neautorizuota tinklo prieiga ir konfigūracijos valdymas. (angl. Unauthorized network access or configuration.)	Žurnalizavimas / ataskaitos: centralizuotas įvykių informacijos rinkimas. (angl. Logging/Reporting: Centralized event information collection.)	
		Srauto, telemetrijos ir duomenų eksfiltracija iš	Stebėsena: tinklo srauto tikrinimas. (angl. Monitoring: Network traffic	

		sėkmingų atakų. (angl. Traffic, telemetry, and data exfiltration from successful attacks.)	inspection.)	
		Infrastruktūros arba įrenginių užgrobimas. (angl. Seizure of infrastructure or devices.)	Politika / konfigūracijos: vieningas infrastruktūros valdymas ir atitikties patikros. (angl. Policy/Configuration: Unified infrastructure management and compliance verification)	
		Klaidingas atakų interpretavimas ir neteisingos koreliacijos.	Laiko sinchronizacija	Centrinės NTP tarnybos.
		Kenkėjiški įrenginiai infrastruktūroje.	Pažeidžiamumų valdymas: nuolatinis infrastruktūros skenavimas, pataisymų diegimas ir ataskaitų teikimas.	

9.2 Saugaus tenanto servisai

Saugaus tenanto servisai – debesijos servisai, skirti apsaugoti tenantą nuo kibernetinių atakų. Paslaugos gali būti dviejų tipų – dedikuotos (dedicated) arba bendro naudojimo (shared).

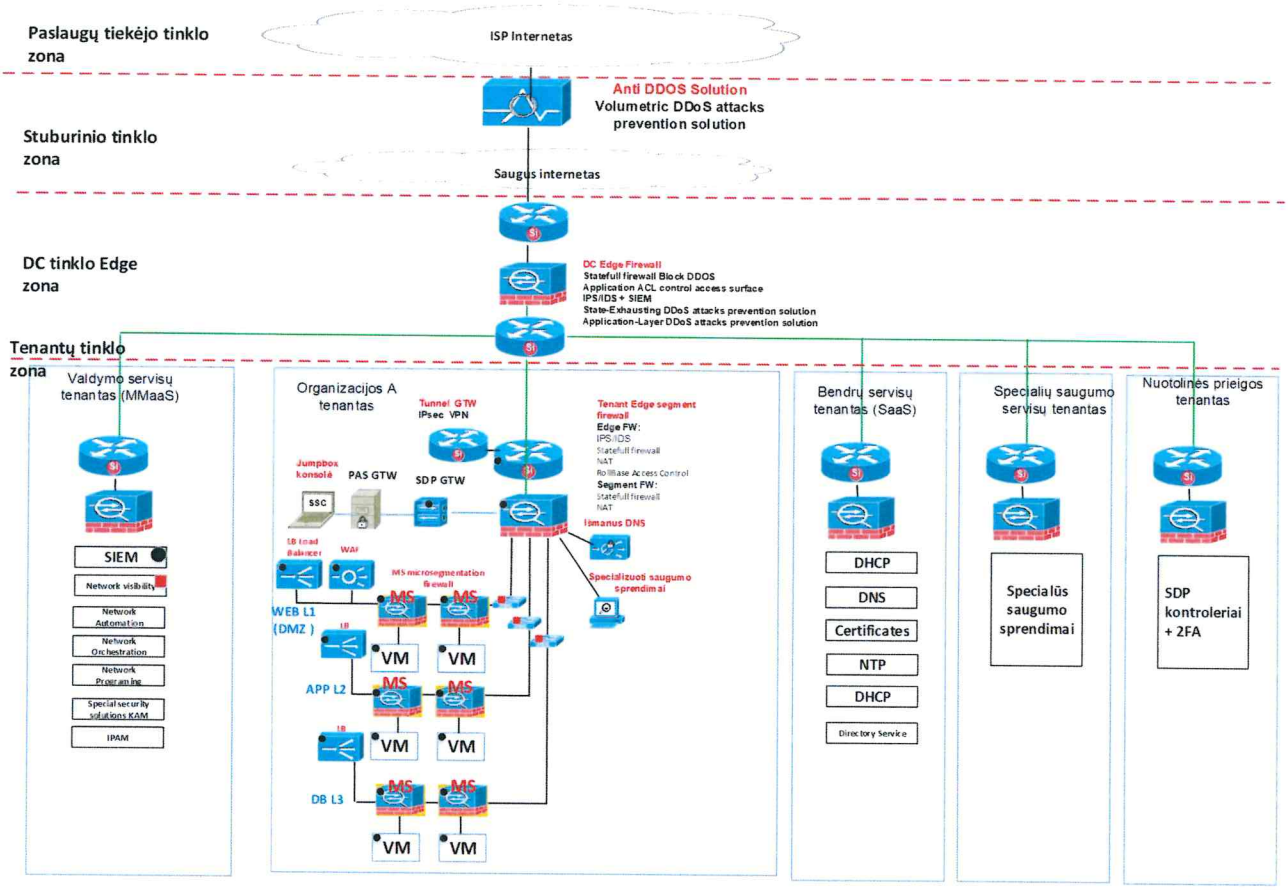
Debesijos saugumo servisai pateikti žemiau esančioje lentelėje.

Servisas	Aprašas	Realizavimo vieta
AntiDDOS Volumetric-attacks prevention soliution	AntiDDOS sprendimas, skirtas apginti tenantus nuo DDOS volumetrinių atakų	Saugaus tinklo operatorius
AntiDDOS State-Exhausting Security devices attacks prevention soliution	AntiDDOS sprendimas, skirtas apsaugoti tenantų Statefull įrenginius nuo „DDOS State-Exhausting Security“ atakų	Duomenų centro tinklo operatorius
AntiDDOS Application-Layer DDoS attacks soliution	AntiDDOS sprendimas skirtas apsaugoti tenantų Statefull įrenginius nuo „DDOS Application-Layer“ atakų	Duomenų centro tinklo operatorius
NAT	Tinklo adresų transliavimo sprendimas	Tenantų Edge ugniasienė
WAF	WEB aplikacijų ugniasienė	Tenantų WEB ugniasienė
Išmanus DNS	Aplikacijų pasiekiamumo sprendimas	Tenantų specializuotas įrenginys
PAM (privilefe access managment)	Privilegijuotų vartotojų pareigos kontrolės sprendimas	Tenantų servisas
MFA (Multi factor authentificationj)	Keletos faktorių autentifikacijos mechanizamas	Tenantų servisas
Edge (Perimeter) Firewall	Tenantų perimetro ugniasienė	Tenantų servisas

Tenant (Segment based) Firewall	Tenantų perimetro ugniasienė	Tenantų servisas
Tenant Microsegmantetion firewall l2-l7 for E-W traffic	Tenantų mikrosegmentacijos ugniasienės	Tenantų servisas
IPAM	IP adresų valdymo sprendimas	Tenantų servisas
Antivirus	Antiviruso valdymo sprendimas	Tenantų servisas
Antispam	Elektroninių laiškų saugumo sprendimas	Tenantų servisas
IPS	Įsilaužimų prevencijos saugumo sprendimas	Tenantų servisas
Network visibility	Tinklo matomumo sprendimas	Tenantų servisas
IPsec VPN	IPsec VPN sprendimas	Tenantų servisas
SSL VPN	SSL VPN sprendimas	Tenantų servisas
SIEM	Saugumo incidentų ir įvykių valdymo sprendimas	Tenantų servisas
KEY management	Šifravimo raktų valdymo sprendimas	Tenantų servisas

9.3 Saugaus tenanto architektūra

Saugaus tenanto architektūra nusako, kaip turi būti konstruojami tenantai, t.y. kokius saugumo servisus naudoti, kaip juos tarpusavyje sujungti tam, kad būtų atremtos kibernetinės atakos. Saugaus tenanto architektūra pateikta žemiau (pav. 9-1 Saugaus tenanto architektūros schema).



pav. 9-1 Saugaus tenanto architektūros schema

9.4 Saugaus priėjimo architektūra

Saugaus priėjimo architektūra nusako saugaus priėjimo prie tenanto modelį. Prie tenanto galima prisijungti pasinaudojus saugaus tinklo paslaugomis per privačius tinklus ir per viešą tinklą Internet.

9.4.1 Saugaus priėjimo per privačius tinklus architektūra

Šiame skyriuje aprašomas nuotolinio prisijungimo per privačius tinklus sprendimas. Šis sprendimas skirtas organizacijos darbuotojams ir administratoriams prisijungti prie organizacijų / tenantų tinklo.

9.4.1.1 Nuotolinio prisijungimo per privačius tinklus sprendimo komponentai

Nuotolinio prisijungimo per privačius tinklus sprendimas susideda iš tokių komponentų:

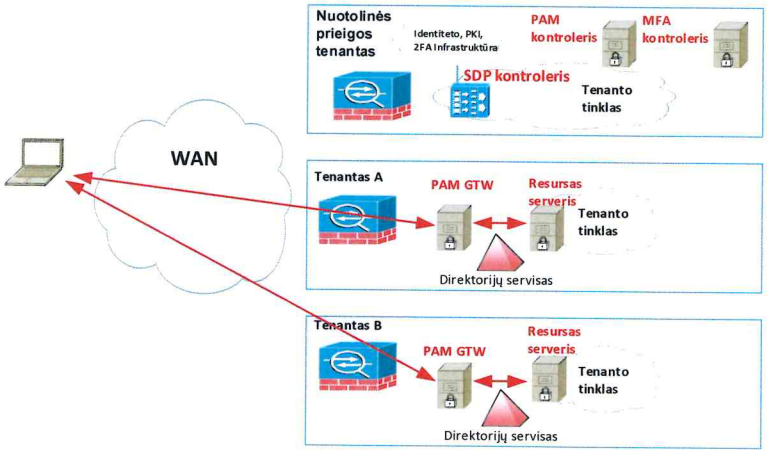
- PAM sprendimas (PAM (Privileged Access Management)) – atlieka vartotojų kontrolės funkciją, kuri užtikrina vartotojų prisijungimų kontrolę prie resursų bei saugų slaptažodžių maskavimą ir valdymą;
- MFA Sprendimas (MFA Multi-factor authentication) – realizuoja keleto faktorių autentifikavimo sprendimą.

9.4.1.2 Nutolusio prisijungimo per privačius tinklus scenarijus

Klientas jungiasi į PAM serverį, kur esant sėkmingai autentifikacijai, autorizacijai ir priėjimo kontrolei, ir yra automatiškai prijungiamas į norimą serverį. Kitas scenarijus, kai klientas jungiasi į PAM serverį, ir portale pasirenka norimą serverį.

Taip yra projektuojama priėjimo prie resursų kontrolė, saugus sesijų valdymas bei sesijų įrašymas.

Nutolusio prisijungimo per privačius tinklus scenarijus pateikta žemiau (pav. 9-2 Nutolusio prisijungimo per privatų tinklą architektūros schema).



pav. 9-2 Nutolusio prisijungimo per privatų tinklą architektūros schema

9.4.2 Saugaus priėjimo per viešuosius tinklus architektūra

Šiame skyriuje aprašomas nuotolinio prisijungimo per viešuosius tinklus sprendimas. Šis sprendimas skirtas darbuotojams, administratoriams, konsultantams ir trečioms šalims prisijungimui prie organizacijų / tenantų tinklo.

Nuotolinio prisijungimo architektūra per viešuosius tinklus grįsta SDP - Software Defined Perimeter saugumo modeliu. SDP saugumo modelio pagrindinis tikslas apsisaugoti nuo tokių tinklų atakų kaip DDoS, Man-in-the-Middle, Server Query (OWASP10) ar Advanced Persistent Threat (APT).

Architektūros skiriamasis požymis – naudojami atskiri kontrolės ir duomenų sluoksniai, leidžiantys išvengti tiesioginio atakų vektoriaus į VPN tunelio paslaugas.

9.4.2.1 Nuotolinio prisijungimo per viešuosius tinklus sprendimo komponentai

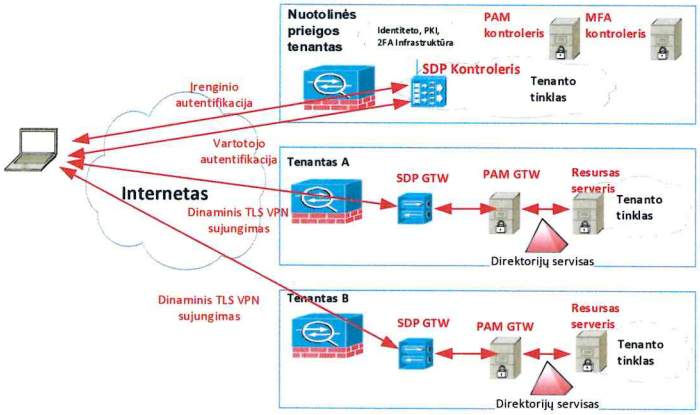
Nuotolinio prisijungimo sprendimas susideda iš žemiau išvardintų komponentų:

- SDP klientas (SDP client) – autorizuotas ir autentifikuotas SDN kontroleris, kuris užmezga VPN TLS tunelį su SDP serveriu. SDP klientas atlieka organizacijos / tenanto saugumo politikų taikymo mazgo funkcijas;
- SDP kontroleris (SDP controller) – funkcionuoja kaip tarpininkas tarp SDP kliento ir identiteto, PKI (Public Key Infrastructure), 2FA (Two-factor authentication) infrastruktūrų, kurių pagalba SDP klientas autentifikuojamas ir autorizuojamas. SDP kontroleris užmezga tunelį tarp SDP kliento ir SDP serverio;
- SDP serveris (SDP Gateway) – terminavimo taškas TLS VPN tunelio iš SDP kliento;
- PAM ir MFA sprendimai aprašyti Nutolusio prisijungimo per viešus tinklus scenarijus skyriuje.

9.4.2.2 Nutolusio prisijungimo per viešus tinklus scenarijus

Klientas jungiasi į SDP kontrolerį, kuris autentifikuoja, autorizuoja ir užmezga VPN TLS tunelį su organizacijos / tenanto tinkle esančiu SDP serveriu. Užmegztu VPN TLS tuneliu klientas jungiasi į PAM serverį, kuris prijungia arba suteikia galimybę prisijungti prie resursų serverio. Resursų serverio prisijungimo atributai valdomi PAM sprendime.

Nutolusio prisijungimo architektūra pateikta žemiau (pav. 9-3 Nutolusio prisijungimo per viešą tinklą architektūros schema).



pav. 9-3 Nutolusio prisijungimo per viešą tinklą architektūros schema

9.5 Saugaus valdymo architektūra

Saugumo valdymo architektūra projektuojama kaip saugumo operacijų centras (SOC Security operation center), kurio pagrindinės funkcijos valdyti tenantų saugumo sprendimus ir incidentus.

Saugumo operacijų centras tai centrinis taškas, į kurį suplaukia su saugumu susijusi informacija iš visų saugumo sprendimų. Čia saugumo informacija normalizuojama, koreliuojama, ir kaip rezultatas generuojami saugumo incidentai.

10 Rezervinio kopijavimo sistemų veiklos modelis

Šiame skyriuje aprašomas rezervinio kopijavimo sistemų veiklos modelis.

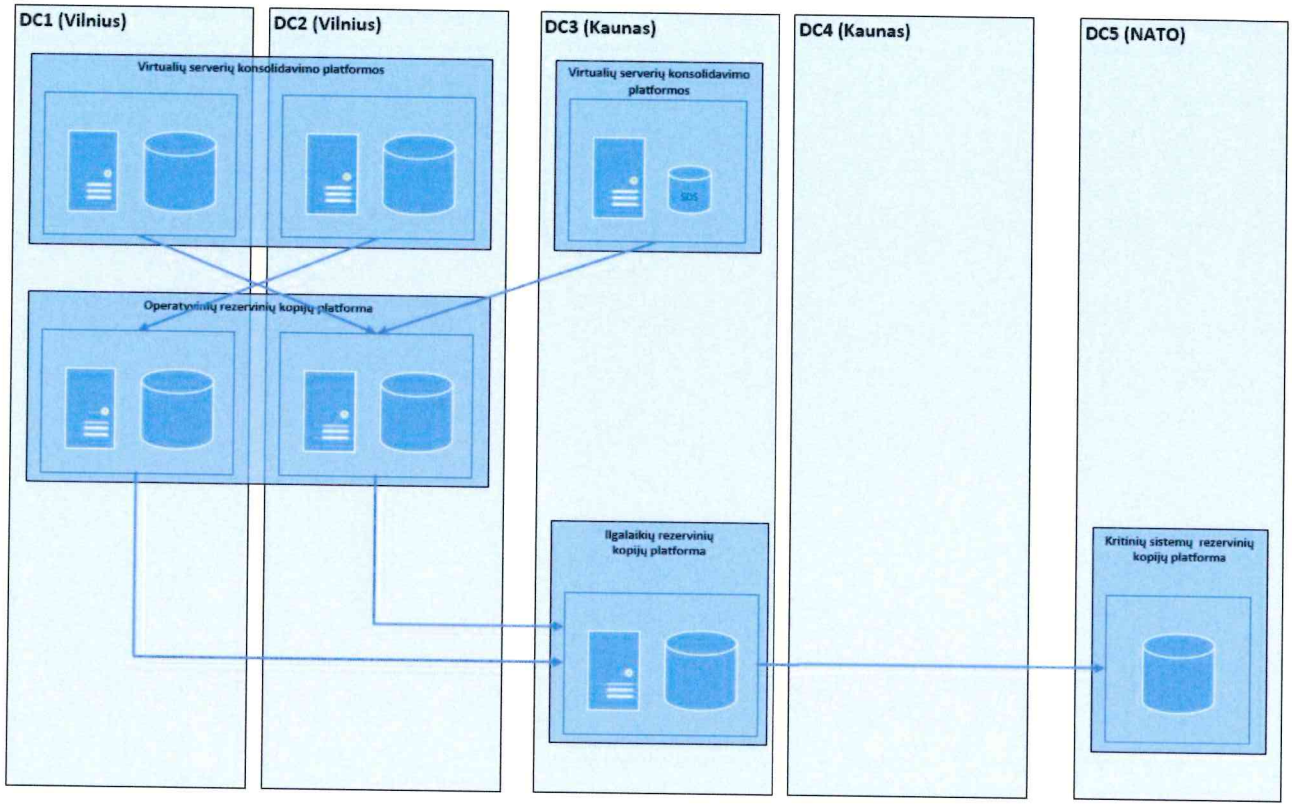
Rezervinio duomenų kopijavimo ir atstatymo sprendimo projektavimui taikomos šios prielaidos:

- Serveriai / duomenys bus klasifikuojami pagal duomenų keitimosi dažnumą, t. y. aplikacijų serveriai, kuriuose duomenys praktiškai nekinta, bus priskiriami vienai kategorijai, o DB duomenys, kurie nuolat keičiasi – kitai ir pan.;
- Turi būti galimybė nuolat besikeičiančius duomenis (pvz.: DB log failus) kopijuoti minimaliu periodiškumu, pvz. kas 15 min. (atstatymo iš rezervinės kopijos RPO – 15 min., RTO – 8 val.);
- Serveriai, kuriuose duomenys praktiškai nekinta, standartiškai bus kopijuojami kartą per parą (atstatymo iš rezervinės kopijos RPO – 24 val.; RTO – 8 val.).;
- Operatyvines duomenų kopijas planuojama saugoti 1 mėn., ilgalaikes – 6 mėn.;
- Turi būti galimybė saugoti ilgalaikes duomenų kopijas, pvz.: mėnesio, metų ir pan. Apie 10 – 20 proc. visų duomenų bus reikalingos ilgalaikės duomenų kopijos;
- Duomenų kopijavimo greitis – ne mažiau kaip 120 TB per valandą;
- 10 proc. duomenų bus kritiniai ir juos reikės saugoti visuose duomenų centruose. Likusių duomenų rezervines kopijas reikia saugoti priešingame regiono DC negu yra operatyviniai duomenys ir kito regiono viename iš DC;
- Apie 10 proc. duomenų reikės saugoti NATO DC (DR atstatymo iš rezervinės kopijos RPO – 1-7 d. RTO – iki 60 d.);

- Atsižvelgiant į viešojo sektoriaus informacinių sistemų ir/arba registrų duomenų svarbą bei saugumo reikalavimus, numatoma, kad rezervinių kopijų saugojimo įrenginiuose duomenys bus saugomi užšifruoti (data at rest encryption), todėl rezervinių duomenų kopijų saugojimo sprendimas turi turėti galimybę palaikyti tiek lokalų, tiek centralizuotą šifravimo raktų valdymą. Papildomų specifinių reikalavimų rezervinio duomenų kopijavimo ir atstatymo įrangai nėra. Juostinių įrenginių naudoti neplanuojama;
- Pirmajame projekto etape neplanuojamas rezervinių duomenų kopijų išnešimas į nepriklausomas patalpas, tačiau rezervinės kopijos turi būti saugomos kitame DC nei yra saugomi pagrindiniai duomenys;
- Programinei įrangai specifinių apribojimų nėra. Sprendimas turi būti projektuojamas taip, kad sprendimą būtų galima realizuoti bent 3 skirtingų gamintojų programine įranga;
- Pirmame projekto įgyvendinimo etape vienkartinio įrašymo technologijos be galimybės duomenis ištrinti ar kitaip modifikuoti naudoti neplanuojama;
- Turi būti galimybė užsisakyti rezervinių duomenų kopijavimą VM'o lygyje;
- Turi būti galimybė rezervines duomenų kopijas kurti standartinėmis programinės įrangos priemonėmis, pvz.: Oracle RMAN, MS SQL, SAP HANA;
- Turi būti galimybė kurti virtualių serverių grupių rezervines kopijas bei jas atstatyti;
- Rezervinio kopijavimo sprendimo įranga projektuojama visiems duomenų centrams (įtraukiant NATO DC);
- Archyvavimo sprendimai I etape neprojektuojami;
- I etape viename iš Vilniaus regiono DC projektuojama 500TB rezervinio kopijavimo duomenų saugykla įstaigoms, kurių informacinės sistemos neperkeltos į VDPT. Saugykla turi priimti (įrašyti) po 2TB duomenų iš ne mažiau kaip 10 įstaigų (sumoje 20TB per parą);

10.1 Rezervinio duomenų kopijavimo sprendimo aprašymas

Rezervinio kopijavimo sprendimų realizacija gana ženkliai skiriasi priklausomai nuo pasirinktų PĮ įrangos tiekėjų (dėl naudojamų skirtingų būdų tiek informacijos paėmimui iš produkcinių duomenų saugyklų, tiek perdavimui, tiek saugojimui galutinėje rezervinių kopijų saugykloje). Atsižvelgiant į tai, šiame skyriuje pateikiama tik rezervinio kopijavimo sistemų veiklos modelis.



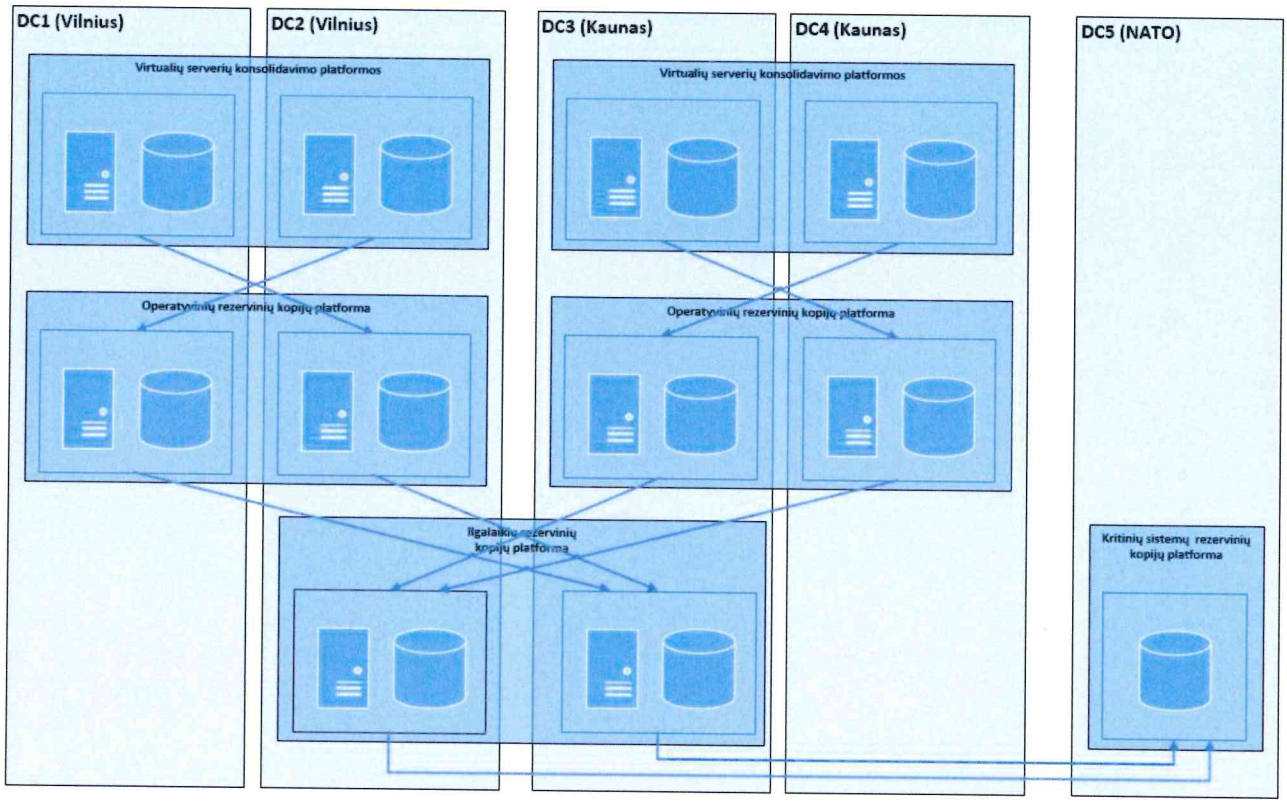
pav. 10-1 Rezervinio kopijavimo sistemų veiklos modelis (I etapas)

I projekto etape diegiamame sprendime (pav. 10-1 Rezervinio kopijavimo sistemų veiklos modelis) operatyvinės rezervinės kopijos saugomos priešingame regiono (Vilnius) duomenų centre. Tokiu būdu įvykus pilnam duomenų centro gedimui, išliekančiame DC yra galimybė atstatyti sistemas iš rezervinės kopijos. Kauno DC esanti ir technologiniams uždaviniams skirta platforma taip pat kopijuojama į vieną iš Vilniaus duomenų centrų.

Operatyvinių rezervinių kopijų sistemos visus duomenis privalomai replikuoja į Kauno DC, kuriame įdiegta pagrindinė (šiam etapui) rezervinių kopijų saugojimo sistema. Papildomai kritinių sprendimų duomenys replikuojami į nutolusį DC (NATO).

Praradus vieną iš Vilniaus duomenų centrų, duomenų atstatymas gali būti atliekamas iš išliekančio aktyvaus Vilniaus DC arba tiesiai iš Kauno DC (tinklo sujungimai nėra ribojantis faktorius duomenų siuntimui).

II projekto etape analogiškas sprendimas diegiamas Kauno duomenų centruose (pav. 10-2 Rezervinio kopijavimo sistemų veiklos modelis).



pav. 10-2 Rezervinio kopijavimo sistemų veiklos modelis (II etapas)

Šiame etape Kauno DC serverių operatyvinės rezervinės kopijos taip pat saugomos priešingame regiono DC, o pagrindinė rezervinių kopijų saugykla diegiama viename iš Vilniaus DC. Papildomai kritinių sistemų duomenys kopijuojami į nutolusį (NATO) DC.

Priklausomai nuo sprendime naudojamų rezervinio kopijavimo sistemų parametrų bei prijungimo sąsajų reikalavimų, pagrindinės rezervinių kopijų saugyklos regionams gali būti realizuotos per abu priešingo regiono duomenų centrus siekiant išlaikyti balansą duomenų centrų fizinės talpos lygmenyje.

Programinės įrangos kontekste, taip pat, priklausomai nuo gamintojo, pilnas rezervinio kopijavimo bei atstatymo funkcionalumas gali būti realizuotas keleto produktų pagalba.

Rezervinio kopijavimo sprendimas užtikrins kopijų atlikimą virtualizacijos platformos (virtualaus serverio) lygmenyje pagal konkretiems sprendimams taikomus RPO/RTO reikalavimus. Duomenų bazių valdymo sistemoms (MS SQL, Oracle) sprendimas atliks rezervinį kopijavimą išlaikant reikiamą duomenų integralumo lygį (application consistent backups) bei keliamus RPO/RTO reikalavimus.

Remiantis konsolidacijos platformų duomenų saugyklų architektūros duomenimis (žr. skyrių 8.1 Duomenų saugojimo sluoksnio realizacija), rezervinio kopijavimo sprendimas užtikrins iki 3 PiB duomenų rezervinį kopijavimą (I projekto etapas) su numatomu kasdieniu duomenų kitimu iki 10% duomenų bazėms bei iki 5% kitoms sistemoms, bei kopijavimui skirtu 8-12h ilgio langu (priklausomai nuo sistemų). Šių reikalavimų tenkinimui, operatyvinių

rezervinių kopijų sistemos užtikrins ne mažesnį nei 120TiB/h suminį duomenų įrašymo srauto pralaidumą (data ingestion rate).

10.1.1 Rezervinio kopijavimo saugyklos paslauga

Rezervinio kopijavimo saugyklos kaip paslaugos (skirtos antrinės / nutolusios kopijos saugojimui) sprendimas realizuojamas dviejų dedamųjų pagrindu:

1. SAN tipo duomenų saugykla komplektuojama NL (nearline) diskais bei prijungta prie SAN tinklo viename iš Vilniaus regiono duomenų centrų. Bendra naudinga erdvė – 500 TiB;
2. Tenanto erdvėje veikiantis virtualus serveris (izoliacijos užtikrinimui), pateikiantis saugyklos erdvę reikiamais protokolais.

Tolimesniuose etapuose, esant poreikiui, sprendimas plečiamas prijungiant papildomas šio tipo saugyklas.

11 Suprojektuoto sprendimo apimtis, diegimas ir integravimas

Siekiant įgyvendinti konsolidavimo projekto numatytus tikslus ir uždavinius, VDPT sprendimas buvo projektuojamas taip, kad atitiktų aukšto našumo, patikimumo bei greitaveikos reikalavimus, o taip pat, atsižvelgiant į viešojo sektoriaus įstaigų informacinių sistemų bei registrų svarbą, užtikrintų optimalų bei kaip įmanoma greitesnį įstaigų (ypatingai pilotinių) IRT infrastruktūros migravimo į VDPT procesą. Projektuojant sprendimą buvo atsižvelgta į viešojo sektoriaus naudojamų IS technologijų specifiką, o taip pat į viešojo sektoriaus darbuotojų turimas IRT kompetencijas, reikalingas administruoti bei plėsti įdiegtą VDPT infrastruktūrą. Sprendimas suprojektuotas taip, kad jį būtų galima nesudėtingai išplėsti bent 3-4 kartus. Įvertinus IVPK pateiktus poreikius bei reikalavimus, buvo parinkti suprojektuotos infrastruktūros realizavimui reikalingos įrangos modeliai. Siekiant kaip įmanoma efektyviau išnaudoti įsigyjamą įrangą bei optimizuoti įrangos eksploatavimo kaštus (gamintojų garantijas, palaikymą ir t.t.), šiame dokumente numatytų etapų įranga gali būti įsigyjama / užsakoma mažesnėmis apimtimis (pvz. perkama / užsakoma 50 proc. šio dokumento I etape numatytos įrangos ir pan.).

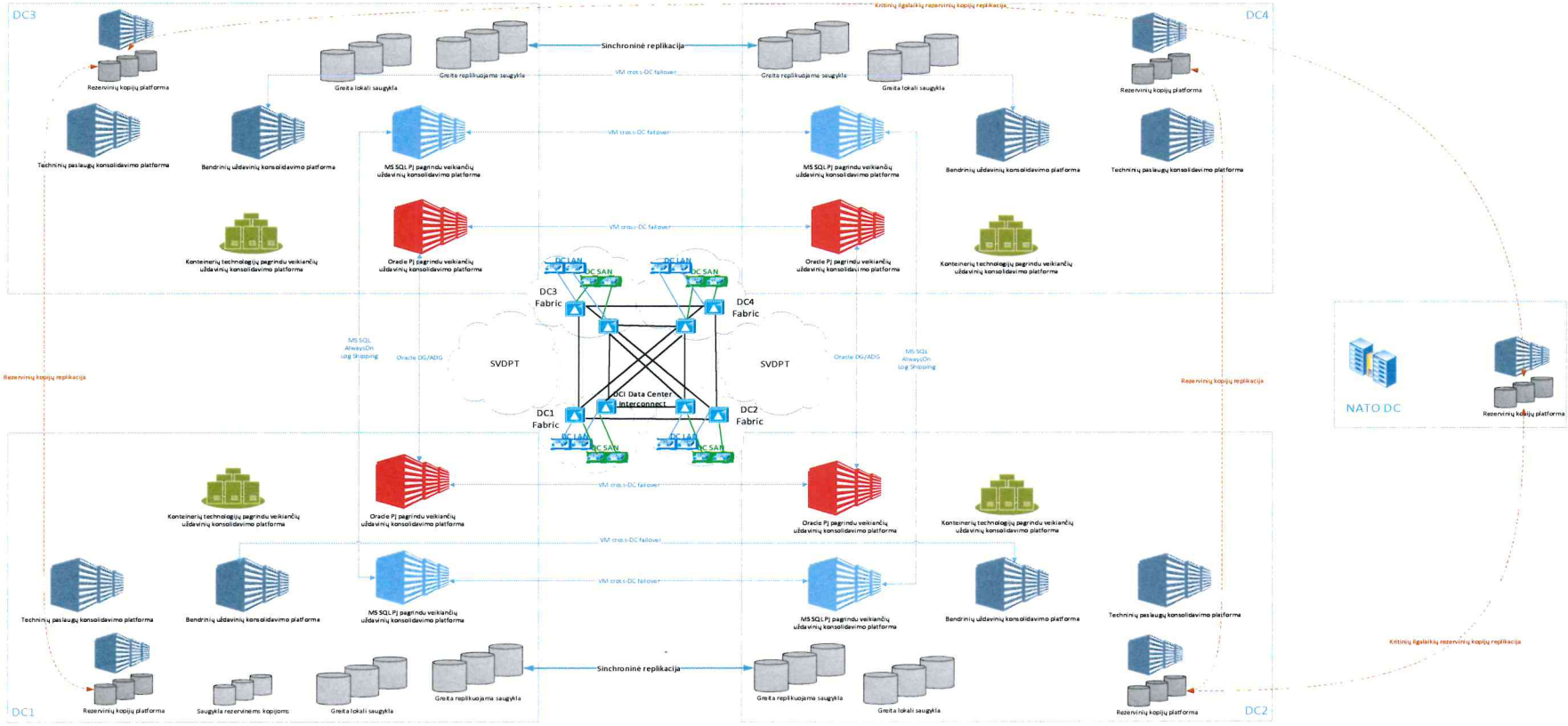
Norint užtikrinti kaip įmanoma didesnę rinkos konkurenciją, nuspręsta suprojektuoto sprendimo įgyvendinimui būtiną techninę ir programinę įrangą įsigyti atskirais pirkimais / dalimis, atsižvelgiant į galimas integracijas ir komponentų suderinamumą (pvz. visi komutatoriai bus perkami vienu pirkimu siekiant užtikrinti kaip įmanoma geresnį tarpusavio suderinamumą bei centralizuoto valdymo galimybes ir pan.). Atsižvelgiant į tai, kad suprojektuotas sprendimas turės veikti kaip viena visuma, o įranga bus perkama atskirais pirkimais / dalimis (potencialiai galimi skirtingi tiekėjai / gamintojai), nuspręsta papildomu viešuoju pirkimu įsigyti sprendimo įdiegimo bei integravimo paslaugas. Diegimo paslaugų teikėjas, bendradarbiaudamas su įrangos tiekėjais, gamintojais, bei IVPK atstovais, privalės pilna apimtimi užtikrinti korektišką ir galutinį suprojektuoto sprendimo įdiegimą, integravimą bei pridavimą eksploatacijai.

12 Priedai

1. Priedas Nr. 1 Bendra infrastruktūros architektūros schema
2. Priedas Nr. 2 Virtualizuoto duomenų saugojimo sluoksnio sprendimo schema
3. Priedas Nr. 3 Organizacijos tinklo architektūros schema
4. Priedas Nr. 4 Rezervinio kopijavimo sistemos schema
5. Priedas Nr. 5 Tinklo saugos architektūros schema

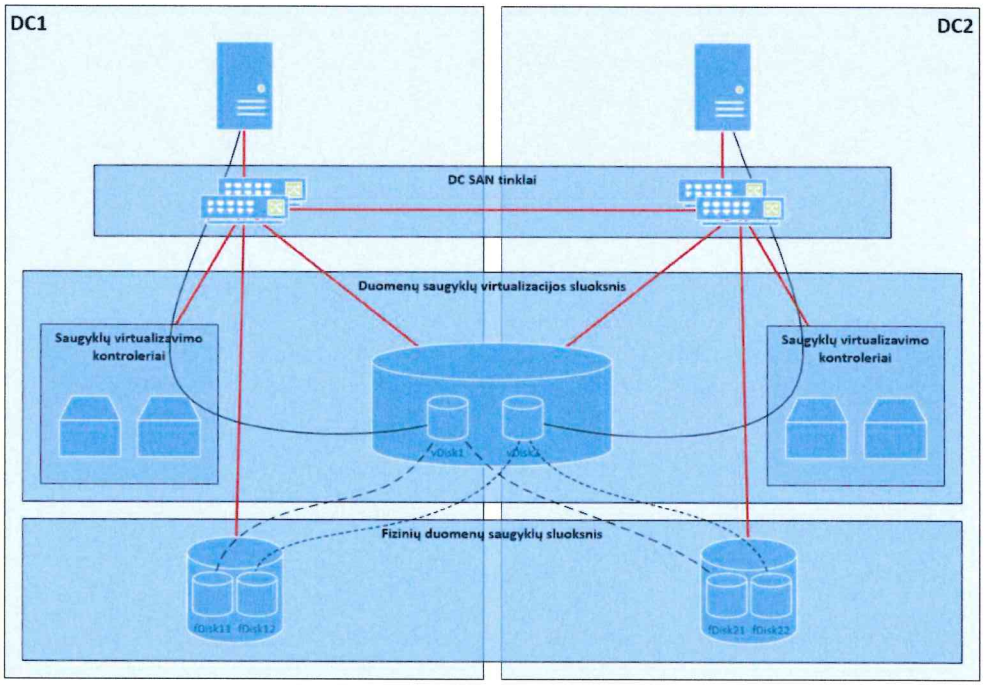
Priedas Nr. 1

Bendra infrastruktūros architektūros schema



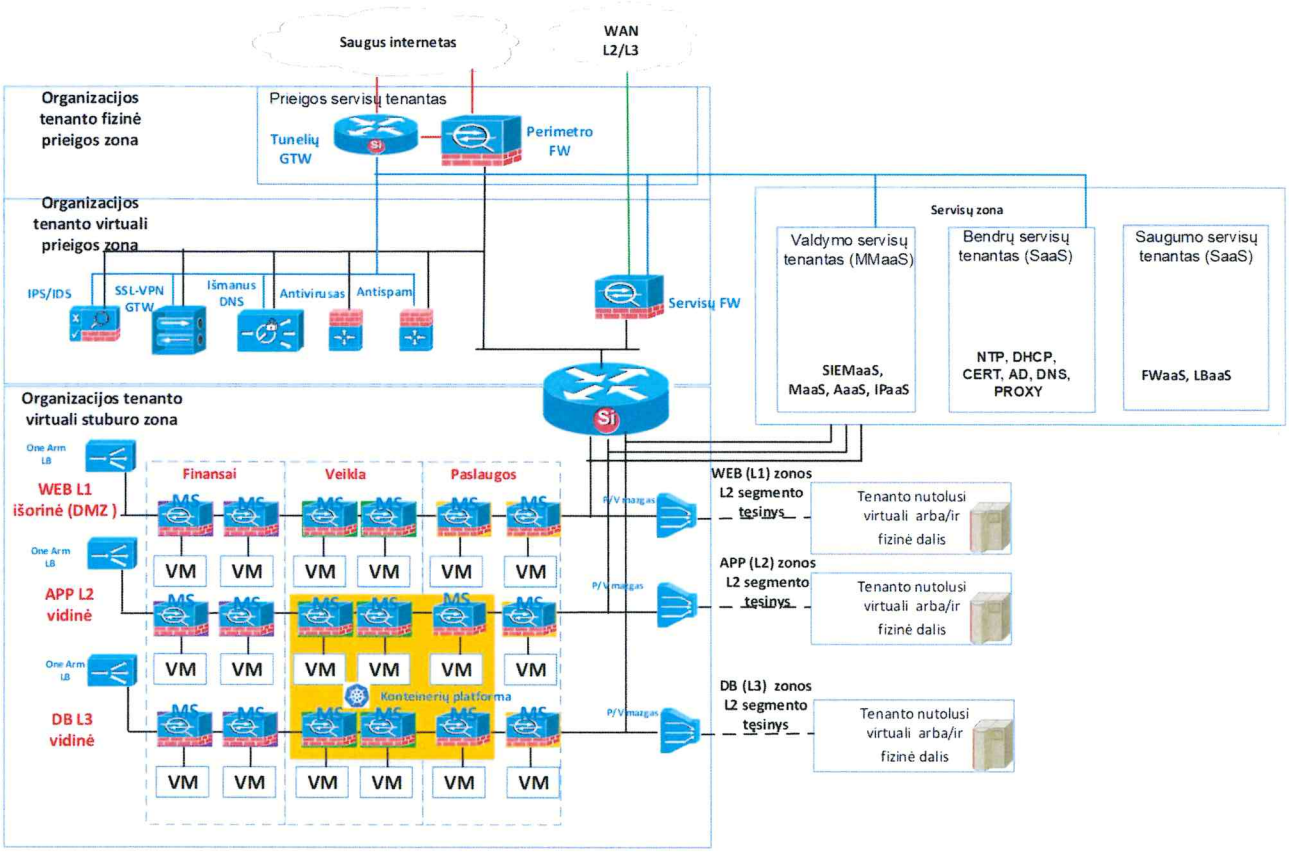
Priedas Nr. 2

Virtualizuoto duomenų saugojimo sluoksnio sprendimo schema



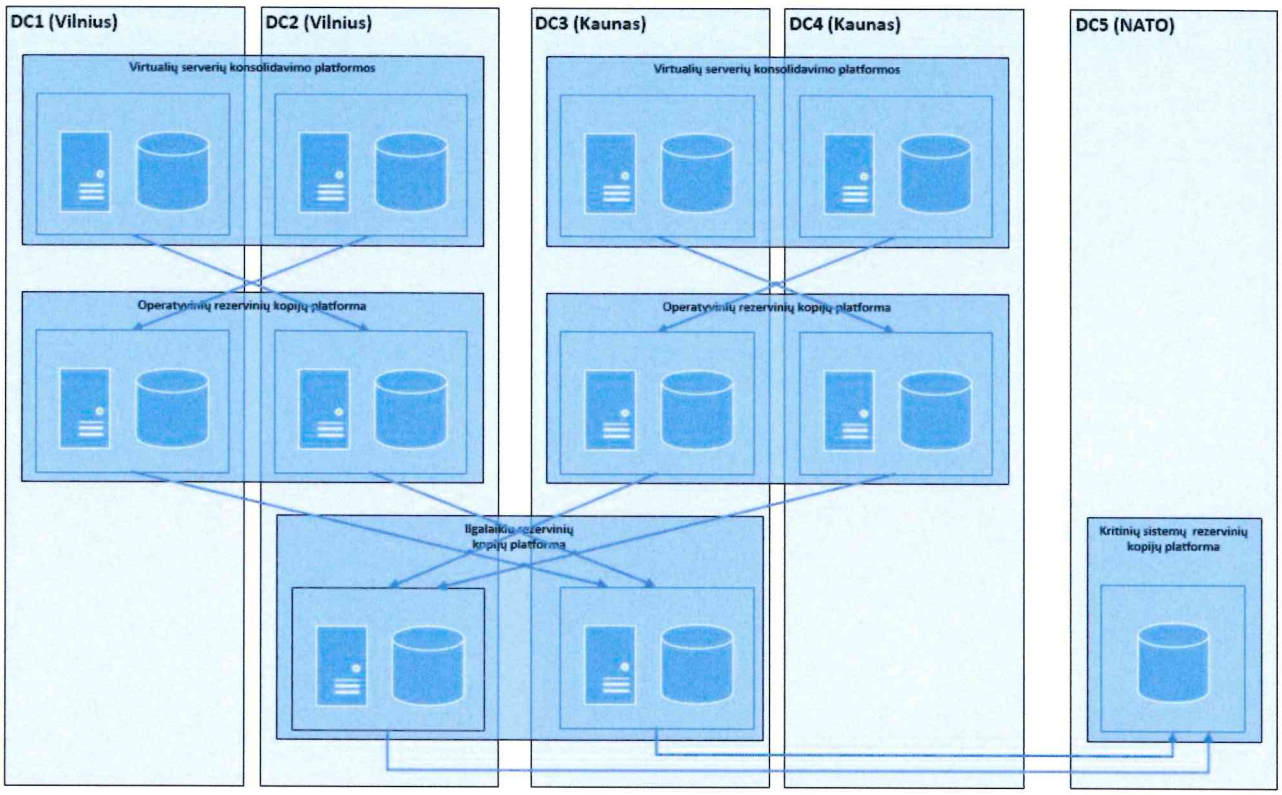
Priedas Nr. 3

Organizacijos tinklo architektūros schema



Priedas Nr. 4

Rezervinio kopijavimo sprendimo schema



Priedas Nr. 5

Tinklo saugos architektūros schema