Nr. 2R-26(2024)

Vidiniam naudojimui

TVIRTINU:

Valstybės skaitmeninių sprendimų agentūros direktorius

Tomas Misevičius

2024 m. rugsėjo 19 d.

VALSTYBĖS HIBRIDINĖS DEBESIJOS PASLAUGŲ TEIKIMO IT INFRASTRUKTŪROS ARCHITEKTŪRA

TURINYS

Derinimas

Data	Aprašymas	Suderino
2024-09-12	Derinimas su Valstybės skaitmeninių sprendimų agentūros atsakingais darbuotojais	Algirdas Puodžiūnas - VSSA Valstybės informacinių technologijų departamento Naujų klientų migravimo skyriaus vedėjas Marius Dubrickas – VSSA Valstybės informacinių technologijų departamento Pagalbos ir konsultavimo skyriaus antro lygio specialistas – sis. administratorius Vidas Sadauskas – VSSA Valstybės informacinių technologijų departamento Pagalbos ir konsultavimo skyriaus antro lygio specialistas – vyr. analitikas, atliekantis KSS vedėjo funkcijas Arūnas Oškutis - VSSA Valstybės informacinių technologijų departamento Kompiuterinių darbo vietų priežiūros skyriaus vedėjas Jurgita Jazgevičienė - VSSA Valstybės informacinių technologijų departamento Projektų valdymo skyriaus vedėja Dimitrian Kondrašov – VSSA Valstybės informacinių technologijų departamento Techninės infrastruktūros skyriaus vedėjas Vitalijus Gorkovčiukas – VSSA Valstybės informacinių technologijų departamento Projektų valdymo skyriaus vyriausiasis specialistas Juzef Statkevič – VSSA Valstybės informacinių technologijų departamento Pagalbos ir konsultavimo skyriaus vedėjas, atliekantis departamento direktoriaus funkcijas
2024-08-08	Informacinės visuomenės plėtros komitetas (nuo 2024-08-14 Valstybės skaitmeninių sprendimų agentūra, sutr. VSSA) 2024-07-19 raštu Nr. S-323(2024) kreipėsi į EIMIN, KAM, NKSC ir KVTC įstaigas „Dėl valstybės hibridinės debesijos paslaugų teikimo IRT infrastruktūros architektūros dokumento suderinimo“ (toliau –	Lietuvos Respublikos krašto apsaugos ministerija Nacionalinis kibernetinio saugumo centras Kertinis valstybės telekomunikacijos centras

	Architektūros dokumentas). Lietuvos Respublikos krašto apsaugos ministerija atsakydama į 2024-07-19 raštą Nr. S-323(2024) informavo ir pateikė 2024-08-08 raštu G-677(2024) rekomendacijas Architektūros dokumentui.	
2024-07-22	Informacinės visuomenės plėtros komitetas (nuo 2024-08-14 Valstybės skaitmeninių sprendimų agentūra) 2024-07-19 raštu Nr. S-323(2024) kreipėsi į EIMIN, KAM, NKSC ir KVTC įstaigas „Dėl valstybės hibridinės debesijos paslaugų teikimo IRT infrastruktūros architektūros dokumento suderinimo“ (toliau – Architektūros dokumentas). Lietuvos Respublikos ekonomikos ir inovacijų ministerija atsakydama į 2024-07-19 raštą Nr. S-323(2024) el. paštu pateikė rekomendacijas Architektūros dokumentui.	Lietuvos Respublikos ekonomikos ir inovacijų ministerija

Lentelė Nr. 1 Derinimas

Versijavimas

Versija	Data	Aprašymas	Parengė
1.0	2024-08-30	Parengtas dokumentas (galutinė versija)	Dimitrian Kondrašov – VSSA Valstybės informacinių technologijų departamento Techninės infrastruktūros skyriaus vedėjas (techninis projekto vadovas) Vitalijus Gorkovčiukas – VSSA Valstybės informacinių technologijų departamento Projektų valdymo skyriaus vyriausiasis specialistas (Projekto vadovas)
0.4	2024-08-30	Dokumento tikslinimas ir papildymas atsižvelgiant į EIMIN, KAM, KVTC, NKSC pateiktas pastabas bei rekomendacijas	Dimitrian Kondrašov – VSSA Valstybės informacinių technologijų departamento Techninės infrastruktūros skyriaus vedėjas Vitalijus Gorkovčiukas – VSSA Valstybės informacinių technologijų departamento Projektų valdymo skyriaus vyriausiasis specialistas Juzef Statkevič – VSSA Valstybės informacinių technologijų departamento Pagalbos ir konsultavimo skyriaus vedėjas, atliekantis departamento direktoriaus funkcijas

0.3	2024-07-15	Dokumento tikslinimas ir papildymas	Juzef Statkevič – VSSA Valstybės informacinių technologijų departamento Pagalbos ir konsultavimo skyriaus vedėjas, atliekantis departamento direktoriaus funkcijas
0.2	2024-07-08	Dokumento struktūros peržiūra, keitimas ir papildymas Dokumento turinio redagavimas ir stiliaus sutvarkymas	Dimitrian Kondrašov – VSSA Valstybės informacinių technologijų departamento Techninės infrastruktūros skyriaus vedėjas Vitalijus Gorkovčiukas – VSSA Valstybės informacinių technologijų departamento Projektų valdymo skyriaus vyriausiasis specialistas
0.1	2024-06-17	Naujas dokumentas	Dimitrian Kondrašov – VSSA Techninės infrastruktūros skyriaus vedėjas Andrius Simanynas – VSSA Valstybės informacinių technologijų departamento Techninės infrastruktūros skyriaus vyriausiasis specialistas Artūr Zima – VSSA Valstybės informacinių technologijų departamento Techninės infrastruktūros skyriaus vyriausiasis specialistas Simonas Mockus – VSSA Valstybės informacinių technologijų departamento Techninės infrastruktūros skyriaus vyriausiasis specialistas Vytautas Kelmelis – VSSA Valstybės informacinių technologijų departamento Techninės infrastruktūros skyriaus specialistas Kiti specialistai (dalyviai)

Lentelė Nr. 2 Versijavimas

ĮVADAS

Įgyvendinus „Valstybės debesijos paslaugų teikimo infrastruktūros sukūrimas“ projektą, vadovaujantis „Logine debesijos paslaugų teikimo ir infrastruktūros architektūra“ yra sukurta ir įdiegta valstybės debesijos paslaugų teikimo veiklai reikalinga informacinių technologijų (toliau – IT) infrastruktūros platforma, kuri skirta teikti valstybės debesijos paslaugas. Taip pat, yra suformuoti reikiami žmogiškieji ir informaciniai ištekliai, reikalingi valstybės debesijos IT paslaugų teikimo organizacijos veiklai vykdyti ir valstybės debesijos paslaugoms teikti. IT paslaugų teikimą vykdo Valstybės skaitmeninių sprendimų agentūra (toliau – VSSA).

Vienas iš pagrindinių VSSA 2024-2028 metų tikslų yra užtikrinti tinkamą centralizuotai teikiamų IT paslaugų teikimą ir plėtrą. Šiam tikslui įgyvendinti yra numatyti veiksmai, susiję su hibridinės debesijos (angl. *Hybrid-Cloud*) paslaugomis, kurios bus teikiamos Valstybės debesijos platformoje ir viešosios debesijos platformose, toliau kartu – Valstybės hibridinės debesijos (toliau – VHD) platforma:

- Vadovaujantis patvirtintu naujo VHD modeliu ir parengtą VHD paslaugų teikimo ir IT infrastruktūros architektūrą atlikti paruošiamuosius darbus, įgalinančius VHD IT infrastruktūros įdiegimą ir IT paslaugų teikimą (IT infrastruktūros įrangos pirkimas, viešosios debesijos paslaugų pirkimas, VSSA ir IT paslaugų gavėjų darbuotojų mokymai, migravimas į naujus valstybinius duomenų centrus (toliau – DC);
- Įdiegti VHD IT platformą;
- Teikti VHD IT paslaugas.

Šio dokumento paskirtis:

- Numatyti ir apibrėžti priemones VHD IT paslaugų teikimo ir IT infrastruktūros architektūros įgyvendinimui.

Dokumento tikslai:

- Parengti (aprašyti) detalią VHD paslaugų teikimo IT infrastruktūros realizacijos architektūrą;
- Parengti VHD IT paslaugų teikimo ir IT infrastruktūros įgyvendinimo planą.

Pagrindiniai uždaviniai:

- **Uždavinys/Etapas Nr. 1** – kritinių valstybės informacinių sistemų, aplikacijų ir registrų (toliau – IS) papildomų rezervinių duomenų kopijų (angl. *Backup*) už Lietuvos Respublikos ribų užtikrinimas. Atsižvelgiant į tai, kad papildomų rezervinių duomenų kopijų saugojimas už Lietuvos Respublikos ribų yra prioritetinė kryptis;
- **Uždavinys/Etapas Nr. 2** – kritinių valstybės IS nepertraukiamos veiklos tęstinumo atstatymo užtikrinimas karo, nepaprastos padėties ir kitų ekstremalių situacijų atveju, užtikrinant susietų IT paslaugų atstatymą (angl. *Disaster Recovery*). Atsižvelgiant į tai, kad šios užduoties įgyvendinimui būtina daugiau laiko, papildomų techninių sprendimų bei aplikacijų modifikavimo *(angl. Refactoring)*;
- **Uždavinys/Etapas Nr. 3** – Valstybės informacinių išteklių valdymo įstatymo (sutr. VIIVĮ, aktuali redakcija) nuostatų, leidžiančių institucijoms savo valdomus mažos ir vidutinės svarbos VII laikyti privačiuose duomenų centruose, įgyvendinimas. Viešosios debesijos inovatyvių ir modernių technologijų naudojimas kuriant naujas ir modernizuojant esamas Valstybės informacines sistemas ir registrus (toliau – IS) (angl. *Cloud Ready, Refactoring*);
- **Uždavinys/Etapas Nr. 4** – VHD IT infrastruktūros veikimo ir plėtros užtikrinimas naudojant viešosios debesijos resursus ir (ar) paslaugas.

1. ESAMO SPRENDIMO ARCHITEKTŪROS APRAŠYMAS

Esamas ir nuo 2020 m. gegužės mėn. veikiantis Valstybės debesijos (angl. *G-Cloud)* paslaugų teikimo IT architektūros sprendimas aprašytas „Loginėje debesijos paslaugų teikimo IT infrastruktūros architektūroje" (versija v9.0):

Loginė_Debesijos_paslaugų_teikimo_IT_infrastruktūros_architektūra.pdf (lrv.lt)

1.1. Valstybės debesijos paslaugų teikimo IT infrastruktūros paslaugos

Visos Valstybės debesijos paslaugų teikėjo (toliau – VDPT) platformos IT paslaugos (skaičiavimo resursų, įvairių duomenų saugyklų, rezervinio kopijavimo ir t.t.) yra tiekiamos ir pasiekiamos IT infrastruktūroje, kuri yra įdiegta ir veikia dvejose valstybiniuose duomenų centruose ir užsienio duomenų centre, esančiame NATO valstybėje.

VDPT IT paslaugų sąrašas:

Paslaugos kodas	Paslaugos pavadinimas
D1	Techninės įrangos talpinimas duomenų centruose
I1	Standartinių parametrų virtualios mašinos (toliau – VM)
I2	Nestandartinių parametrų virtualios mašinos
I3	Didelio našumo dubliuojami diskai
I4	Didelio našumo diskai
I21	S3 objektinės saugyklos didelės talpos diskai
I6	Saugykla rezervinėms duomenų kopijoms valstybiniai duomenų centrai
I6.1	Saugykla rezervinėms duomenų kopijoms – ne Lietuvos teritorijoje esantys duomenų centrai
I7	SAN (angl. *Storage Area Network*) jungtys
I10	Srauto apsauga nuo nepageidaujamo turinio (angl. *AntiSpam*)
I11	Tinklo ugniasienė
I12	Internetinių programų ugniasienė
I13	Srauto apkrovos paskirstymo paslauga (LB/ADC)
I14	Papildomi saugumo elementai (IPS/UTM/SSO/MFA)
I16	Virtualus privatus ryšys (VPN)
I17	Antivirusinė srauto apsauga (angl. *AntiVirus*)
I18-F	Tarpinis serveris (angl. *forward proxy*)
I18-R	Atvirkštinis tarpinis serveris (angl. *Reverse proxy*)
I19	Paslaugos gavėjo tinklas
I20	LAN (angl. *Local Area Network*) jungtys
P1	Duomenų bazių valdymo sistema Microsoft SQL Server
P2	Duomenų bazių valdymo sistema Oracle Database Server
P6	Konteinerių valdymo platforma (Tanzu)
P6.1	Konteinerių valdymo platforma (OpenShift)
P7	Taikomųjų programų serveriai (angl. *middleware*)
P3	Duomenų bazių valdymo sistema PostgreSQL
S1	Failų serveris
S2	Kompiuterinės darbo vietos programinė įranga

S3	Elektroninis paštas
A1	Operacinių sistemų priežiūros paslauga
A2	Duomenų bazių valdymo sistemos priežiūros paslauga
A8	Lokalių tinklų priežiūros paslauga
B2	Rezervinis kopijavimas
B7	Debesijos (virtualizacijos) platformos valdymo portalas
B1	Stebėsena (angl. *Monitoring*)
B6	Pagalbos tarnyba (angl. *Helpdesk* arba *Service Desk*)
A5	Konsultavimo paslauga
A3	IRT projektavimo, migravimo paslauga
A4	Kompiuterių darbo vietų priežiūros paslauga
A6	Kompiuterinės darbo vietos įranga
A7	Spausdinimo paslauga
I22	Standartinių parametrų didelio našumo VM – pridėta nauja paslauga;
S5	Programinio kodo saugykla – pridėta nauja paslauga;

Lentelė Nr. 3 VDPT teikiamų paslaugų sąrašas

Papildomai naudojamas trečias duomenų centras (nutolęs už Lietuvos ribų, NATO valstybėje) teikiantis tik rezervinių kopijų saugojimo paslaugas.

1.2. Sprendimo architektūra

VDPT sprendimas veikia VMware Cloud Suite bei VMware vCloud Director programinių sprendimų pagrindu. Remiantis viešosios debesijos paslaugų gamintojo geriausiomis praktikomis sprendimas yra segmentuotas į tris saugumo zonas:

- DCIM – duomenų centrų įrangos valdymo zoną.
- VIM – virtualios infrastruktūros ir platformos valdymo zoną.
- VI – Kliento paslaugoms skirtos virtualios infrastruktūros valdymo zona.

Visos trys saugumo zonos realizuojamos VMware vSphere virtualizacijos platformos pagrindu bei naudoja VMware NSX-T tinklo paslaugų virtualizacijos sprendimą.

VIM ir VI saugumo zonų realizavimui naudojami dedikuoti LAN fabriko segmentai (leaf komutatoriai).

DCIM naudojama dedikuota LAN tinklo įranga.

Visos trys saugumo zonos naudoja bendrą SAN tinklo bei duomenų saugyklų infrastruktūrą yra simetriškai išdėstytos abiejuose duomenų centruose.

1.2.1 DCIM zona

Aukščiausio saugumo DCIM zona yra skirta fizinės duomenų centrų įrangos valdymui:

- LAN ir SAN infrastruktūros konfigūravimui;
- Serverių OOB (Out of Band prieigai);
- Saugyklų valdymo sąsajų prieigai.

Dalis VDPT sprendimo įrangos dėl konkretaus sprendimo specifikos ir apribojimų yra valdoma iš VIM platformos.

DCIM platforma realizuota dedikuotu vSphere 7.x virtualizacijos klasteriu su dedikuotu valdymo tašku (vCenter) bei dedikuota NSX-T 3.2.x implementacija.

Platformoje veikia paslaugos ir servisai reikalingi platformos funkcionavimui bei kitų platformų paruošimui bei valdymui:

- Autentifikavimo paslaugos (MS AD);
- Vidinė sertifikatų infrastruktūra (MS CA);
- Platformos valdymo prieigos serveriai (jump/bastion host);
- Tinklo paslaugos:
    - DHCP;
    - DNS;
    - NTP;
    - SMTP;
    - NSX-T tinklo virtualizacijos komponentai.
- Platformos valdymo įrankiai:
    - VMware vCenter;
    - VMware Aria for Logs – skirtas platformos bei tinklo infrastruktūros logų rinkimui;
    - Cisco DCNM;
    - Lenovo & Dell serverių valdymo bei stebėjimo įrankiai;
    - IBM Spectrum Control.

Didžioji dalis paslaugų įdiegtos padidinto pasiekiamumo režimu, užtikrinančiu atitinkamos paslaugos prieinamumą vieno duomenų centro netekimo atveju.

1.2.2 VIM zona

VIM zona skirta virtualios platformos (VI zona) valdymo paslaugų bei įrankių diegimui.

VIM platforma realizuota dedikuotu vSphere 7.x virtualizacijos klasteriu su dedikuotu valdymo tašku (vCenter) bei dedikuota NSX-T 3.2.x implementacija.

Platformoje veikia paslaugos ir servisai reikalingi VI platformos funkcionavimui bei tenantams skirtų platforminių paslaugų valdymui:

- Autentifikavimo paslaugos (MS AD);
- Vidinė sertifikatų infrastruktūra (MS CA);
- Platformos valdymo prieigos serveriai (jump/bastion host);
- Tinklo paslaugos:
    - DHCP;
    - DNS;
    - NTP;
    - SMTP;
    - NSX-T tinklo virtualizacijos (VIM platforma) komponentai;
    - NSX-T tinklo virtualizacijos (VI platforma) komponentai.
- Platformos valdymo įrankiai (neapsiribojant, galimi ir kiti alternatyvūs sprendimai):
    - VMware vCenter – skirtas VIM platformos valdymui (veikia padidinto pasiekiamumo konfigūracijoje);

    - VMware vCenter – skirtas VI platformos valdymui (veikia padidinto pasiekiamumo konfigūracijoje);
    - VMware CloudDirector – PĮ skirta tenantų izoliacijos realizavimui bei valdymui (VI platforma);
    - VMware Aria for Logs – skirtas platformos bei tinklo infrastruktūros logų rinkimui;
    - VMware vRealize Operations Manager – skirta VIM bei VI virtualizacijos platformų stebėjimui ir analizei;
    - Platformos infrastruktūros bei tenantų paslaugų stebėjimo infrastruktūros veikiančios Zabbix PĮ pagrindu.
- Rezervinio kopijavimo sprendimo infrastruktūra veikianti Veeam PĮ pagrindu;
- Objektinės duomenų saugyklos paslauga bei jos valdymo įrankiai.

Visos paslaugos įdiegtos padidinto pasiekiamumo režimu, užtikrinančiu atitinkamos paslaugos prieinamumą vieno duomenų centro netekimo atveju.

1.2.3 VI zona

Tenantų uždavinių zona. Realizuota keleto vSphere klasterių pagrindu, leidžiančiu optimaliai valdyti trečiųjų šalių PĮ licencijų panaudojimą tokių kaip:

- MS Windows Server;
- RedHat Linux Server;
- Oracle Database Enterprise Edition (įskaitant papildinius);
- Oracle Database Standard Edition;
- Oracle Middleware;
- MS SQL Server Enterprise Edition;
- vSphere Tanzu;
- RedHat OpenShift;
- GPU procesorių virtualizavimui.

Platforma realizuota vSphere 7.x virtualizacijos klasterių pagrindu su dedikuotu valdymo tašku (vCenter) bei dedikuota NSX-T 3.2.x implementacija. Tenantų bei jų resursų valdymas atliekamas VMware Cloud Director 10.4.x priemonėmis.

Kubernečių paslauga teikiama virtualizacijos platformos pagrindu ir yra realizuota VMware Tanzu bei RedHat Openshift priemonėmis (atskiri, izoliuoti resursų telkiniai).

Papildomai šiai zonai priklauso Oracle KVM pagrindu veikianti platforma skirta senų (legacy) Oracle PĮ (nepatenkančių į aukščiau išvardintą sąrašą) pagrindu veikiančių sprendimų veikimui.

1.2.4 Duomenų saugyklos

Visų platformų duomenų saugojimui naudojamos 4 tipų duomenų saugyklos:

1. *Lokalios blokinės saugyklos*. Tai SAN tipo duomenų saugyklos veikiančios SSD NVMe diskų pagrindu. Naudojamos tame duomenų centre esančių sprendimų (tiek platforminių, tiek tenantų uždavinių) duomenų saugojimui. Skirtos produkcinių sprendimų duomenų saugojimui kuomet sprendimas palaiko aplikacijos lygio padidinto pasiekiamumo funkcionalumą, taip pat ne produkcinių uždavinių duomenų saugojimui. Saugyklos (ar duomenų centro) gedimo atveju – duomenys tampa nepasiekiami. Naudojamos IBM Storwize v5100 bei IBM FS7300 duomenų saugyklos. Bendra saugyklų talpa ~260 TiB per duomenų centrą. Duomenys saugyklose nėra dubliuojami. Talpinamos

kritinės informacinės sistemos aplikacijų lygyje naudojančios aukšto pasiekiamumo sprendimus, neišleistos į gamybą testinės aplinkos, mažos svarbos informacinės sistemos.

2. *Virtualizuotos blokinės saugyklos.* Tai SAN tipo duomenų saugyklos veikiančios SSD NVMe diskų pagrindu. Šio tipo saugykla užtikrina duomenų pasiekiamumą dviejuose duomenų centruose (virtualaus ar fizinio serverio atžvilgiu matoma kaip viena loginė saugykla). Skirtos produkcinių uždavinių, kuriems padidintas pasiekiamumas turi būti užtikrinamas platformos lygmenyje, duomenų saugojimui. Duomenų centro gedimo atveju loginė saugykla bei joje saugomi duomenys pasiekiami išliekančiame duomenų centre. Naudojamos IBM Storwize v5100, IBM FS7300 duomenų saugyklos bei IBM SVC saugyklų virtualizacijos kontroleriai. Bendra saugyklų talpa ~2 PiB duomenų dubliuotų per du duomenų centrus. Duomenys saugykloje yra dubliuojami. Talpinamos kritinės informacinės sistemos, kurios aplikacijų lygyje nenaudoja aukšto pasiekiamumo.

3. *Lokalios NL tipo blokinės saugyklos.* Tai SAN tipo duomenų saugyklos veikiančios NL SAS diskų pagrindu. Naudojamos įvairiems rezervinio kopijavimo sprendimų uždaviniams spęsti. Saugyklos (ar duomenų centro) gedimo atveju – duomenys tampa nepasiekiami. Naudojamos IBM v5030E bei Dell ME5084 duomenų saugyklos. Bendra saugyklų talpa – ~2.5 PiB. Duomenys saugyklose nėra dubliuojami. Talpinamos kritinės informacinės sistemos aplikacijų lygyje naudojančios aukšto pasiekiamumo sprendimus, neišleistos į gamybą testinės aplinkos, mažos svarbos informacinės sistemos.

4. *Objektinių duomenų saugyklos.* S3 protokolo pagrindu veikianti saugykla skirta nestruktūrizuotų duomenų saugojimui. Saugyklos resursai prienami tiek konkretaus duomenų centro ribose, tiek padidinto pasiekiamumo formatu, kuomet duomenys dubliuojami per du duomenų centrus. Šioje duomenų saugykloje saugomiems duomenims nėra daromos rezervinės kopijos. Duomenų apsauga (nuo sugadinimo/praradimo/užšifravimo) turi būti užtikrinama šią paslaugą naudojančios aplikacijos architektūros (duomenų dubliavimas) bei S3 protokolo standartinių funkcijų (object versioning, object lock ir t.t.) pagalba. Paslauga teikiama Dell ECS objektinės duomenų saugyklos pagrindu. Saugyklos talpa ~3 PiB per duomenų centrą. Duomenys saugykloje yra dubliuojami per du duomenų centrus (aplikacijos lygio nustatymai).

1.2.5 Duomenų perdavimo infrastruktūra

Duomenų perdavimo infrastruktūra apima kelias sritis:

- Duomenų perdavimo duomenų centruose bei tarp jų užtikrinimas (DC infrastruktūra);
- Ryšio su tenantų infrastruktūromis užtikrinimas;
- Interneto ryšio paslaugos.

1.2.6 DC ryšio infrastruktūra

Duomenų centrų ryšio infrastruktūra apima 3 (tris) paslaugų blokus:

1. Ryšio tarp duomenų centrų užtikrinimas (DWDM paslaugos).
2. Tinklo infrastruktūra (LAN fabrikas).
3. Duomenų saugyklų tinklo infrastruktūra (SAN fabrikas).

1.2.7 DWDM infrastruktūra

Duomenų centrų apjungimui fiziniame lygyje naudojami 2 (du) sprendimai:

1. DCIM zonai priklausančiam įrangos valdymo tinklui apjungti naudojamos optinės skaidulos (dark fiber) – po vieną porą einančią skirtingais keliais.
2. LAN bei SAN fabrikų apjungimui naudojama DWDM technologija. Sujungimui naudojamos optinių skaidulų poros – po 2 einančias skirtingais keliais (viso 4 skaidulų poros). Sprendimas realizuotas įrangos pagrindu ir fabrikų lygmenyje užtikrinamas 8x 100GbE (LAN) ir 8x 32Gb (SAN) sujungimai.

1.2.8 LAN infrastruktūra

VDPT platformos LAN tinklas realizuotas dviem lygiais: fizinis ir virtualus. Fizinį LAN tinklą galima suskaidyti į tris dalis: Cisco technologijomis realizuotas duomenų centrų fabrikas, DCIM platformai skirti klasikiniai komutatoriai ir OOB tinklas. Virtualus tinklas realizuotas VMware NSX-T technologijų pagrindu. Tinklo perimetro apsauga rūpinasi KVTC 9jeigu yra KVTC kientas, o tuo atveju, jeigu nėra – VSSA). VDPT platformoje papildomai fizinių ugniasienių pagalba realizuotas tinklo perimetro saugumo sluoksnis, kuriame nustatomos bendrinės taisyklės visiems tenantams. Tenantų saugumo sprendimai realizuoti naudojant VMware NSX-T technologijas.

1.2.9 SAN infrastruktūra

Projektuojant VDPT sprendimą buvo pasirinkta skaičiavimo resursų bei duomenų saugojimo infrastruktūros atskyrimo strategija nes jis leidžia lanksčiau valdyti bei planuoti atitinkamų resursų telkinių plėtrą. Jų apjungimui panaudota FC SAN infrastruktūra.

Remiantis geriausiomis SAN dizaino praktikomis, SAN infrastruktūra realizuota 2 pilnai izoliuotų SAN fabrikų principu, kuomet sukuriami du izoliuoti SAN tinklai. Visi jų vartotojai (serveriai) bei paslaugų tiekėjai (duomenų saugyklos) jungiami prie abiejų SAN infrastruktūrų mažiausiai 1 jungtimi.

SAN infrastruktūra realizuota Director klasės SAN komutatorių pagalba (naudojama Cisco MDS 9700 tipo moduliniai komutatoriai, 240 32 Gb FC SAN jungčių, per komutatorių), po 2 per duomenų centrą, apjungtų DWDM pagalba (4x 32Gb FC sujungimai per SAN fabriką).

1.2.10 Ryšio su tenantų infrastruktūromis užtikrinimas

Tenantai su VDPT platforma sujungiami KVTC tvarkomu Saugiuoju tinklu. Išskirtiniais atvejais sujungimas gali būti realizuotas naudojant site-to-site VPN tunelius. Šiuo atveju tunelis terminuojamas VDPT platformoje ir tenanto infrastruktūroje. Interneto ryšio paslaugos ir saugos priemonės

VDPT platformos veikimui reikalingą viešojo interneto ryšį užtikrina KVTC Ryšio patikimumu ir saugumu rūpinasi KVTC. KVTC užtikrina AntiDDoS (L3) kibernetinio saugumo paslaugos centralizuotą teikimą, netinkamo turinio filtravimą pasitelkdama atitinkamas interneto ryšio saugos priemones.

1.2.11 Rezervinio kopijavimo infrastruktūra

Platformos lygio rezervinio kopijavimo bei atstatymo paslaugas teikianti infrastruktūra realizuota VIM platformoje. Sprendimas veikia Veeam PĮ pagrindu. Visi sprendimo valdymo komponentai (Veeam Backup&Recovery (VBR) serveriai, jiems skirti duomenų bazių serveriai (MS SQL), Veeam One serveriai, centralizuoto sprendimo valdymo (Veeam Enterprise Manager) serveriai) veikia virtualių serverių formatu. Duomenų perdavimo infrastruktūros komponentai yra tiek virtualūs (Veeam proxy server (HotAdd tipo kopijavimas per LAN), tiek fiziniai (atlieka tiek fizinio Veeam proxy rolę kopijavimui per SAN tinklą), tiek duomenų saugyklos (Veeam Gateway for dedup storage) rolę.

Duomenų saugojimui naudojamos HPE StoreOnce 5650 bei Dell ME5084 duomenų saugyklos.

Visa duomenų perdavimo infrastruktūra išdėstyta simetriškai per duomenų centrus. Papildomai nutolusiame NATO duomenų centre yra įdiegta HPE StoreOnce 5650 saugykla bei papildomi serveriai su Veeam Gateway role taip įgalinant turėti kritinių duomenų kopijas ne Lietuvos teritorijoje.

Sprendimas užtikrina rezervinių kopijų atlikimą bei saugojimą pagal VSSA nustatytus paslaugos RPO bei RTO reikalavimus.

1.2.12 Platformos ir paslaugų stebėjimo infrastruktūra

Platformos ir paslaugų stebėjimo infrastruktūros sprendimas realizuotas VIM platformoje. Sprendimas veikia Zabbix PĮ pagrindu ir jį sudaro dvi atskiros infrastruktūros – viena skirta platformos ir jos komponentų stebėjimui, prieinama tik VDPT operatoriui, bei antra – skirta tenantų paskyrose veikiančių uždavinių bei paslaugų stebėjimui. Pastaroji yra prieinama visiems tenantų administratoriams (konkretaus tenanto kontekste).

1.2.13 Privilegijuotų paskyrų valdymo sprendimas

Privilegijuotų paskyrų valdymo sprendimas realizuotas CyberArc PĮ pagrindu ir skirtas kontroliuoti privilegijuotų paskyrų naudojimą DCIM, VIM bei VI platformose (tenantų administratoriai). Sprendimas įdiegtas VIM platformoje.

Sprendimas naudojamas prisijungimo prie įrangos bei serverių valdymo sąsajų atsekamumui bei privilegijuotų vartotojų slaptažodžių valdymui.

1.2.14 Saugos įvykių surinkimo bei analizės sprendimas

Saugos įvykių surinkimo ir analizės sistema realizuota IBM QRadar PĮ pagrindu ir įdiegta VIM platformoje. Sprendimas renka ir analizuoja saugumo informaciją iš aparatinės bei programinės įrangos komponentų DCIM, VIM bei VI (dalinė tenantų integracija) platformose.

2. VIEŠOSIOS DEBESIJOS PASIRINKIMO PRINCIPAI

2.1 Viešosios debesijos paslaugų gamintojo platformos pasirinkimo pagrindiniai kriterijai

Kiekvienas viešosios debesijos paslaugų gamintojas turi savo architektūros principus, ir jais pagrįstus valdymo ir audito įrankius. Praktiškai visi viešosios debesijos paslaugų gamintojai valdo tik savo platformoje esančius resursus ir paslaugas, pritaiko saugumo ir kitas politikas tik savo debesijos platformos resursams. Iš IT paslaugų valdymo pusės, viešosios debesijos paslaugų gavėjui yra optimaliausia konsoliduoti tarpusavyje priklausančias IT paslaugas arba IS vieno iš pasirinktų viešosios debesijos paslaugų gamintojo platformoje. Tokiu būdu atsiranda naudos:

- mažinami IT paslaugų priežiūros kaštai;
- užtikrinama vieninga IT paslaugų priežiūra ir auditas;
- užtikrinama komponentų tarpusavio integracija;
- užtikrinamas ryšio saugumas, nes duomenys lieka to paties viešosios debesijos paslaugų gamintojo atsakomybės perimetre;
- sumažinami duomenų siuntimo kaštai.

Atskirais atvejais, tam tikros Paslaugos gali būti teikiamos keleto viešosios debesijos paslaugų gamintojų. Pasirinkimas naudoti vieną ar kitą viešosios debesijos paslaugų gamintojo platformą priklauso nuo:

- ar IT paslaugų kataloge leidžiama pasirinkti viešosios debesijos paslaugų gamintoją;
- ar IT paslaugų kataloge yra nustatyti ribojimai, kurie įtakoja paslaugos užsakymą ir (ar) realizavimą;
- ar IT paslaugų kataloge viešosios debesijos Gamintojas palaiko licencijavimą (pvz., Azure viešosios debesijos platforma prioriteto tvarka (natūraliai) palaiko Microsoft gamintojo programų ir serverių licencijas, o kiti viešosios debesijos Gamintojai Microsoft komponentus palaiko fragmentiškai. Pasirenkami tie viešosios debesijos paslaugų Gamintojai, kurie užtikrina IT paslaugų priežiūrą ir licencijų palaikymą);
- ar IT paslauga yra priklausoma nuo kitos paslaugos, kuri jau realizuota viešojoje debesijoje (ar yra priklausomybė IT paslaugą talpinti toje pačioje viešosios debesijos platformoje – pvz., reikalavimai duomenų vėlinimui, arba reikalavimai šifravimo raktų pasiekiamumui). Šiuo atveju IT paslauga yra diegiama toje viešosios debesijos platformoje, kurioje jau yra realizuoti priklausomybę formuojantys komponentai ir paslaugos.

Taip pat, viešosios debesijos platformos pasirinkimas priklauso ne tik nuo tenanto *Disaster Recovery* sprendimo realizavimo kainos, bet ir naudojamos technologijos.

2.2 Saugumo sprendimai

Viešosios debesijos paslaugų gamintojo platforma ir teikiamos paslaugos turi atitikti šiuos reikalavimus (sąrašas nėra baigtinis, gali būti papildytas pagal aktualumą, pateikti ir kiti lygiaverčiai susiję reikalavimai):

- turi būti sertifikuotos ISO 27001;
- turi atitikti duomenų apsaugos reikalavimus, nustatytus ISO 27018:2014;
- turi atitikti Bendrojo duomenų apsaugos reglamento (toliau – BDAR) reikalavimus;
- turi galėti pateikti trečių šalių paslaugų kontrolės audito ataskaitas, tokias kaip SOC1 ir SOC2;

- turi atitikti ENISA Cloud Computing Information Assurance Framework reikalavimus (daugiau apie tai galima susipažinti čia: Cloud Computing Information Assurance Framework);
- kiti galimai taikytini privačių ir užsienio duomenų centrų, kuriuose talpinami valstybės informaciniai ištekliai, vietovės, įrengimo, fizinės apsaugos ir kiti techniniai ir organizaciniai reikalavimai (pvz., viešosios debesijos paslaugų gamintojo duomenų centro infrastruktūrai ir pan.).

Detali informacija apie pagrindinių viešosios debesijos paslaugų gamintojų platformos atitikimą IT standartams:

AWS viešosios debesijos gamintojo taikomų sistemų (programų) ir standartų sąrašas: https://aws.amazon.com/security/
Google viešosios debesijos gamintojo taikomų sistemų (programų) ir standartų sąrašas: https://cloud.google.com/security/compliance/offerings
Microsoft Azure viešosios debesijos gamintojo taikomų sistemų (programų) ir standartų sąrašas: https://learn.microsoft.com/en-us/azure/compliance/
Oracle Cloud viešosios debesijos gamintojo taikomų sistemų (programų) ir standartų sąrašas: https://www.oracle.com/corporate/cloud-compliance/
IBM Cloud viešosios debesijos gamintojo taikomų sistemų (programų) ir standartų sąrašas: https://www.ibm.com/cloud/compliance

Lentelė Nr. 4 Viešosios debesijos paslaugų Gamintojų saugumo standartai

Viešosios debesijos atsakomybių modelis remiasi bendrojo veikimo modelio (angl. *Shared Operating Model*) principu ir IT paslaugų gavėjui (Klientui) tenka svarbi atsakomybė užtikrinant saugą savo atsakomybės ribose.

Viešosios debesijos paslaugų gamintojas yra visiškai atsakingas už viešosios debesijos platformos veikimą bei, priklausomai nuo paslaugos tipo, atsakingi už:

- „Infrastruktūra kaip paslauga“ (IaaS) atveju, viešosios debesijos paslaugų gamintojas yra atsakingas už fizinę infrastruktūrą, Paslaugos pirkėjas (Klientas) arba IT paslaugų gavėjas (Užsakovas) atsakingas už operacines sistemas, duomenų bazes, sistemas (aplikacijas) jų saugumą, atnaujinimus, konfigūravimą ir pan.;
- „Platforma kaip paslauga“ (PaaS) atveju, viešosios debesijos paslaugų gamintojas atsakingas ir už fizinę infrastruktūrą, ir už platformą, t. y. atsakingas už operacinių sistemų, duomenų bazių ir kt. saugumą ir naujinimus. Paslaugų pirkėjas (Klientas) arba IT paslaugų gavėjas (Užsakovas)atsakingas už viešosios debesijos platformoje esančias sistemas, jų saugumą, atnaujinimus, konfigūravimą ir pan.;
- „Sistema kaip paslauga“ (SaaS) atveju, viešosios debesijos paslaugų gamintojas yra atsakingas ir už fizinę infrastruktūrą, už platformą, už sistemas, jų saugumą, atnaujinimus, konfigūravimą ir pan.;
- Viešosios debesijos paslaugų gamintojas taip pat yra atsakingas už viešosios debesijos visos infrastruktūros ir teikiamų viešosios debesijos paslaugų atestavimą bei sertifikavimą;

- Viešosios debesijos paslaugų Pirkėjas arba IT paslaugų gavėjas (Užsakovas) yra atsakingas už duomenis, kurių yra valdytoju arba tvarkytoju ir jų nustatytą konfigūraciją viešoje debesijoje.

Viešosios debesijos platformos saugumo užtikrinimo pagrindiniai principai:

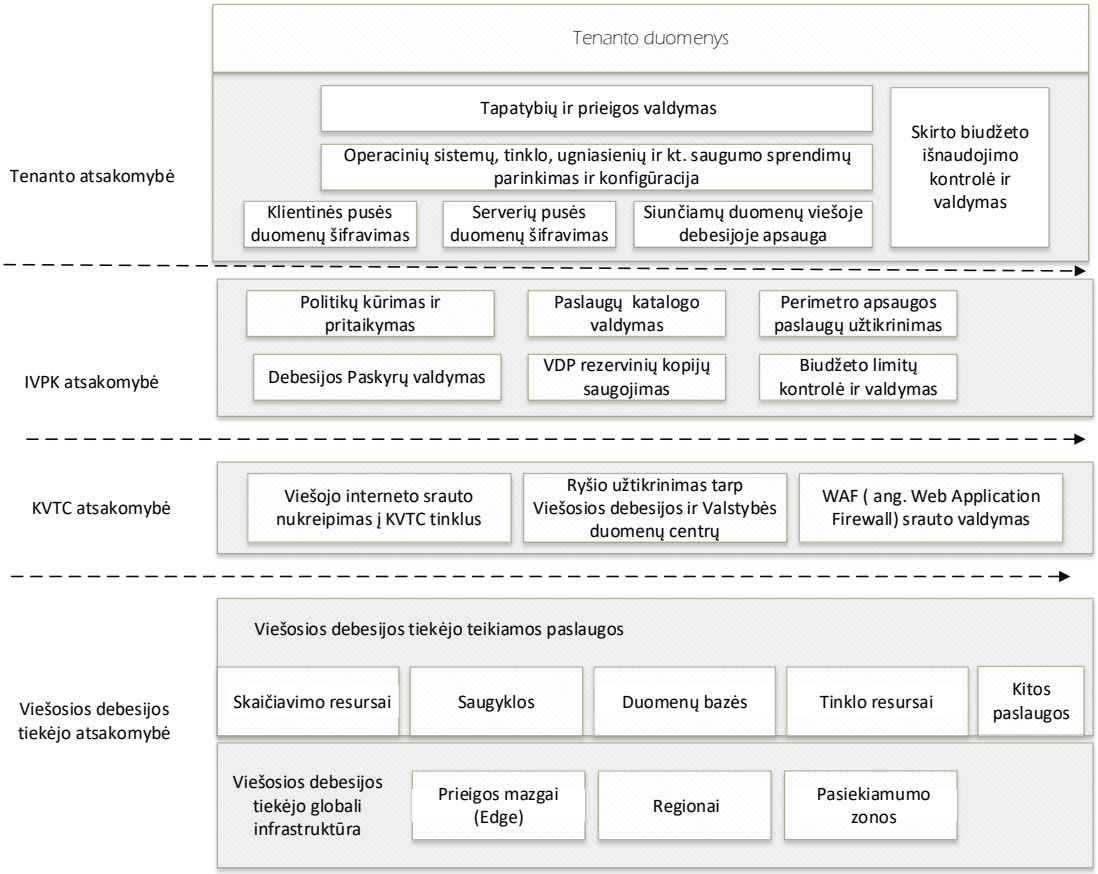
- Nulinio pasitikėjimo modelis – organizacijos turi „nepasitikėti“ sistemomis ir naudotojais vien dėl to, kad jie yra organizacijos tinklo perimetro viduje. Saugumo kontrolės mechanizmai turi būti taikomi kiekviename lygyje, nepriklausomai nuo lokacijos ir konteksto;
- Geriausių saugumo praktikų įgyvendinimas – sistemų (aplikacijų) saugumo, tinklo saugumo, duomenų saugumo, naudotojų ir teisių saugumo, saugumo kontrolės mechanizmų geriausių praktikų taikymas;
- Rizikų vertinimas ir valdymas – įtraukia rizikų atpažinimą, įvertinimą ir sprendimą viešoje debesijoje.

Viešosios debesijos platformos papildomos saugumo užtikrinimo priemonės:

- Prieigos prie viešosios debesijos paslaugų kontrolės ribojimas iš patikimų IP adresų, reikalaujant MFA autentifikavimo;
- AntiDDoS, netinkamo turinio filtravimas
- Tinklo segmentų ir prenumeratų izoliavimas, užtikrinantys, kad saugumo incidento atveju bus paveiktas nedidelis izoliuotas viešosios debesijos platformos segmentas;
- Duomenų srautų valdymas, užtikrinant, kad srautas tarp viešosios debesijos paslaugų vyktų tik viešosios debesijos Gamintojo tinklo viduje;
- Centralizuotas žurnalinių įrašų kaupimas ir saugojimas;
- Duomenų ir duomenų srautų šifravimas;
- Sistemų (aplikacijų) sertifikatų, slaptažodžių ir prisijungimo informacijos saugojimas, pagal sistemas (aplikacijas) segmentuotose seifuose ir (ar) slaptažodžių saugyklose;
- Rezervinių kopijų saugojimas, panaudojant backup technologiją, užtikrinančią, kad kopijos nebus sunaikintos arba pakeistos;
- Infrastruktūros stebėjimo politikų ir automatinių pranešimų siuntimas;
- Keitimų (atnaujinimų, konfigūracijų ir pan.) valdymo procesai, užtikrinantys, kad naudojamos naujausios ir saugiausios versijos;
- Infrastruktūros auditai, užtikrinantys, kad konfigūracija nebuvo pakeista ir atitiktų naujausias saugumo rekomendacijas;
- Valdymo politikos, kurios kontroliuoja, kokie ir kaip resursai yra kuriami ir naudojami.

KVTC, teikdama interneto ryšio ar kitas susijusias paslaugas, sprendimus taikys Lietuvos Respublikos teisės aktų, kurios reglamentuoja KVTC veiklą, tvarka. KVTC Saugiuoju tinklu teikiamų interneto ryšio paslaugų parametrai bei saugos sprendimai patvirtinti Lietuvos Respublikos krašto apsaugos ministro 2019 m. liepos 2 d. įsakymu Nr. V-583 „Dėl saugiojo valstybinio duomenų perdavimo tinklo veiklą užtikrinančių dokumentų patvirtinimo“ (aktuali redakcija, V-583 Dėl Saugiojo valstybinio duomenų perdavimo tinklo veiklą užtikrinančių dokumentų patvirtinimo (lrs.lt)).

3. ATSAKOMYBIŲ PASIDALINIMAS VIEŠOSIOS DEBESIJOS GAMINTOJO APLINKOJE



Pav. 1 Atsakomybių pasidalinimas viešosios debesijos paslaugų gamintojo aplinkoje

3.1 Viešosios debesijos paslaugų gamintojo atsakomybė

Viešosios debesijos paslaugų gamintojas yra atsakingas už viešosios debesijos paslaugų gamintojo platformos veikimą, kokybiškų paslaugų teikimą ir informacijos saugumą tiek kiek tai apima platformą ir teikiamas paslaugas. Viešosios debesijos platforma ir paslaugos remiasi infrastruktūros ir paslaugų sprendimais.

Viešosios debesijos paslaugų gamintojas yra atsakingas už viešosios debesijos paslaugų gamintojo platformos visą infrastruktūrą:

- Pastatus, ir jiems reikalingus išteklius: elektra, aušinimas, fizinė apsauga, informacijos saugumas (kibernetinis saugumas, asmens duomenų apsauga, elektroninės informacijos sauga) ir t.t.;
- Pasiekiamumo zonas – didelio patikimumo ir rezervinę įrangą, aptarnaujamus mazgus, kurie veikia nepriklausomai vienas nuo kito ir užtikrina, kad vieno mazgo gedimas vienoje pasiekiamumo zonoje neįtakoja kito mazgo skirtingoje pasiekiamumo zonoje veikimo;
- Resursų pasidalinimą skirtinguose regionuose: užtikrina, jog infrastruktūra skirtinguose regionuose būtų nepriklausoma, infrastruktūros gedimas viename regione neįtakotų infrastruktūros kitame regione veikimo. Jei nepasakyta kitaip, užtikrina, kad duomenys, žurnalų duomenys, metrikos liktų pasirinktame regione.
- Prieigos mazgus – užtikrina galimybę jungtis prie viešosios debesijos ir užtikrina prieigos mazgų apsaugą.

Priklausomai nuo paslaugos modelio (IaaS, PaaS, SaaS) viešosios debesijos paslaugų gamintojas yra atsakingas už teikiamas paslaugas:

- Skaičiavimo resursus;
- Duomenų saugyklas;
- Duomenų bazes;
- Tinklo resursus;
- Paskyrų biudžeto limitavimo kontrolę (angl. *Chargeback*);
- Paslaugos pirkėjo arba Kliento konsultavimą ir pagalbą;
- Ir kt.

„Infrastruktūra kaip paslauga“ (IaaS) atveju, viešosios debesijos paslaugų gamintojas viešosios debesijos paslaugoms teikti yra atsakingas už fizinę infrastruktūrą, o Paslaugos pirkėjas (Klientas) ir IT paslaugų gavėjas (Užsakovas) yra atsakingi už operacines sistemas, duomenų bazes, sistemas (aplikacijas), jų saugumą, atnaujinimus, konfigūravimą) ir pan.

„Platforma kaip paslauga“ (PaaS) atveju, viešosios debesijos paslaugų gamintojas viešosios debesijos paslaugoms teikti yra atsakingas už fizinę infrastruktūrą ir už platformą, t. y. atsakingas už operacinių sistemų, duomenų bazių ir kt. įrangos saugumą, atnaujinimus, konfigūravimą ir pan. Paslaugos pirkėjas ir IT paslaugų gavėjas (Užsakovas arba Klientas) yra atsakingi už sistemas (aplikacijas), jų saugumą, atnaujinimus, konfigūravimą ir pan.

„Sistema kaip paslauga“ (SaaS) atveju, viešosios debesijos paslaugų gamintojas viešosios debesijos paslaugoms teikti yra atsakingas už fizinę infrastruktūrą, platformą, ir sistemas (aplikacijas), jų saugumą, atnaujinimus, konfigūravimą ir pan.

Viešosios debesijos paslaugų gamintojas taip pat yra atsakingas už infrastruktūros ir teikiamų viešosios debesijos paslaugų atestavimą bei sertifikavimą.

3.1 KVTC atsakomybių gairės

KVTC yra atsakingas už jungiantį:

- Valstybės įstaigas ir (ar) institucijas (Saugiojo tinklo naudotojus);
- Valstybės įstaigas (įtrauktas į Saugiojo tinklo naudotojų sąrašą) ir Valstybės duomenų centrus;
- Viešosios debesijos duomenų centrus ir Valstybės duomenų centrus;
- Viešojo interneto srauto nukreipimą per WAF (angl. *Web Application Firewall*) į viešosios debesijos resursus.

3.2 VSSA atsakomybių gairės

VSSA yra atsakingas už viešosios debesijos paslaugų teikimo organizavimą, koordinavimą ir administravimą:

- Viešosios debesijos organizacijos medžio, paskyrų sukūrimą ir valdymą, išorinių paskyrų valdymą;
- Saugumo, išteklių, politikų kūrimą ir valdymą;
- IT paslaugų katalogo valdymą;
- Paskyrų biudžeto limitavimą ir paskirstymą (angl. *Chargeback*);
- Rezervinių kopijų saugojimą;

- Tais atvejais, kai naudojamos bendros viešosios debesijos paslaugų gamintojo platformos paslaugos perimetro apsaugai, VSSA yra atsakinga už perimetro apsaugą (pvz., WAF).

3.3 Tenanto (Kliento, IT paslaugų gavėjo arba Užsakovo) atsakomybių gairės

Viešosios debesijos paslaugų Klientas atsakingas:

- už savo duomenis viešoje debesijoje. Kiekvieno viešosios debesijos Kliento atsakomybė yra užtikrinti savo duomenų apsaugą:
    - Iš Kliento pusės duomenų šifravimą, kai šifravimą atlieka Klientas lokaliai, apsaugant duomenis siuntimo metu ir esant jiems saugykloje. Tokiu būdu užšifruoti duomenys yra apsaugoti nuo trečiųjų šalių prieigos. Klientas valdo šifravimo raktą ir saugo jį savo nuožiūra parinktoje saugykloje.
    - Serverių pusės duomenų šifravimą, kai šifravimą atlieka gavusi duomenis paskirties aplikacija. Jei aplikacija teikia tokias šifravimo paslaugas, Klientas yra atsakingas už tokio šifravimo paslaugų tinkamą konfigūraciją ir įjungimą.
    - Siunčiamų duomenų apsaugą;
    - Viešosios debesijos Klientas yra pilnai atsakingas už suteikto biudžeto viešojoje debesijoje išnaudojimą, valdymą ir priežiūrą (angl. *Showback*).
- Priklausomai nuo užsakyto viešosios debesijos paslaugos modelio (IaaS, PaaS, SaaS), Klientas atsakingas už operacinių sistemų, programų, tinklo, ugniasienių ir kitų saugumo sistemų parinkimą, konfigūravimą, atnaujinimą ir apsaugą;
- Viešosios debesijos Klientas yra atsakingas už atitikimą pritaikytoms politikoms;
- Viešosios debesijos Klientas yra atsakingas už jo diegiamos / kuriamos / naudojamos IS saugumą / priežiūrą ir kodo rašymo gerąsias praktikas viešosios debesijos platformoje.

3.4 Viešosios debesijos dalyvių atsakomybė skirtinguose hibridinės debesijos diegimo etapuose

Pirmas etapas – kritinių valstybės IS papildomų rezervinių duomenų kopijų (angl. *Backup*) už Lietuvos Respublikos ribų užtikrinimas naudojant viešosios debesijos platformų paslaugas.

Viešosios debesijos paslaugų gamintojas yra atsakingas už viešosios debesijos visą infrastruktūrą: platformos veikimą, kokybiškų paslaugų teikimą ir informacijos saugumą tiek kiek tai apima platformą ir teikiamas paslaugas.

- Konsoliduotoms organizacijoms:
    - VSSA atsakingas už rezervinių kopijų duomenų papildomos kopijos saugojimą ir esant poreikiui rezervinės kopijos atstatymą;
    - KVTC atsakingas už ryšio suteikimą ir jo apsaugą ugniasienėmis ir kitais ryšio saugumo sprendimais;
    - Klientas atsakingas už rezervinių kopijų poreikio nustatymą ir reikalavimų konfigūravimą. Už savo IS veiklos atkūrimo planą ir atstatymą. Už suteikto biudžeto viešojoje debesijoje išnaudojimą, valdymą ir priežiūrą (angl. *Showback*).
- Nekonsoliduotoms organizacijoms:
    - Klientas atsakingas už rezervinių kopijų poreikio nustatymą ir reikalavimų konfigūravimą, rezervinių kopijų duomenų papildomos kopijos iškėlimą, saugojimą, rezervinės kopijos atstatymą, paskyros biudžeto išnaudojimo priežiūrą, saugumo nustatymų, politikų ir t.t. vykdymą.

- KVTC atsakingas už saugaus ryšio suteikimą ir jo apsaugą ugniasienėmis ir kitais ryšio saugumo sprendimais.
- VSSA gali teikti rekomendacijas dėl hibridinės debesijos paslaugų architektūros, debesijos paskyros sukūrimo, biudžeto, saugumo nustatymų ir politikų valdymo.

Antras etapas – kritinių valstybės IS nepertraukiamos veiklos tęstinumo atstatymo užtikrinimas karo, nepaprastos padėties ir kitų ekstremalių situacijų atveju, užtikrinant susietų IT paslaugų atstatymą (angl. *Disaster Recovery*).

Viešosios debesijos paslaugų gamintojas yra atsakingas už viešosios debesijos visą infrastruktūrą: platformos veikimą, kokybiškų paslaugų teikimą ir informacijos saugumą tiek kiek tai apima platformą ir teikiamas paslaugas.

- Konsoliduotoms organizacijoms:
  - VSSA atsakingas už tenanto modelio parinkimą ir sukūrimą Klientui.
  - KVTC atsakingas už saugaus ryšio suteikimą ir jo apsaugą ugniasienėmis ir kitais ryšio saugumo sprendimais.
  - Klientas atsakingas už savo aplikacijų konfigūravimą. Už savo IS veiklos atkūrimo planą ir atstatymą. Už suteikto biudžeto viešojoje debesijoje išnaudojimą, valdymą ir priežiūrą (angl. *Showback*).
- Nekonsoliduotoms organizacijoms:
  - VSSA gali teikti rekomendacijas dėl hibridinės debesijos paslaugų architektūros. Nurodo reikalavimus politikoms, kurios bus pritaikytos valdymo struktūroje.
  - KVTC atsakingas už saugaus ryšio suteikimą ir jo apsaugą ugniasienėmis ir kitais ryšio saugumo sprendimais.
  - Klientas pilnai atsakingas už savo tenanto organizacijos struktūros ir paskyrų valdymą, tenanto platforminių paslaugų ir aplikacijų diegimą, konfigūravimą ir valdymą, duomenų saugumo reikalavimų vykdymą ir auditą, biudžeto valdymą ir tinkamą naudojimą.

Trečias etapas – Valstybės informacinių išteklių valdymo įstatymo (sutr. VIIVĮ, aktuali redakcija) nuostatų, leidžiančių institucijoms savo valdomus mažos ir vidutinės svarbos VII laikyti privačiuose duomenų centruose, įgyvendinimas. Viešosios debesijos inovatyvių ir modernių technologijų naudojimas kuriant naujas ir modernizuojant esamas Valstybės IS (angl. *Cloud Ready, Refactoring*).

Viešosios debesijos paslaugų gamintojas yra atsakingas už viešosios debesijos visą infrastruktūrą: platformos veikimą, kokybiškų paslaugų teikimą ir informacijos saugumą tiek kiek tai apima platformą ir teikiamas paslaugas.

- Konsoliduotoms organizacijoms:
  - VSSA atsakingas už tenanto modelio parinkimą ir sukūrimą Klientui.
  - KVTC atsakingas už saugaus ryšio suteikimą ir jo apsaugą ugniasienėmis ir kitais ryšio saugumo sprendimais.
  - Klientas atsakingas už savo IS (aplikacijų) konfigūravimą, veiklos atkūrimo planą ir atstatymą. Už suteikto biudžeto viešojoje debesijoje išnaudojimą, valdymą ir priežiūrą (angl. *Showback*).

4. HIBRIDINĖS DEBESIJOS DIEGIMO ETAPAI

Be tipinių resursų talpos plėtros bei platformos palaikymo (techninės bei programinės įrangos atnaujinimas) valdymo uždavinių, numatomi 3 pagrindiniai hibridinės debesijos diegimo etapai:

1. Valstybės kritinių IS (registrų bei sistemų) rezervinių kopijų duomenų papildomos kopijos iškėlimas saugojimui į viešųjų debesijos paslaugų platformas.
2. Valstybės kritinių IT paslaugų (resursų) veiklos tęstinumo realizavimas viešosios debesijos platformose.
3. Nekritinių IS veikimas viešosios debesijos platformose.

5. PIRMAS ETAPAS. Valstybės kritinių IS (registrų bei sistemų) rezervinių kopijų duomenų papildomos kopijos iškėlimas saugojimui į viešųjų debesijos paslaugų platformas

Papildomos rezervinės duomenų kopijos iškėlimas į viešosios debesijos platformas yra pirmas žingsnis link hibridinės debesijos veiklos modelio. Tikslas turėti valstybės kritinių IS duomenų kopiją už Lietuvos ribų, vieno ar keleto viešosios debesijos paslaugų platformose. Planuojama integruoti viešosios debesijos objektinių duomenų saugyklų paslaugas į VDPT naudojamą rezervinio kopijavimo sprendimą, tuo pačiu užtikrinant maksimalią duomenų apsaugą. Įskaitant duomenų perdavimo kanalo saugumo užtikrinimą, duomenų šifravimą bei šifravimo raktų valdymą, objektinėse duomenų saugyklose esančių duomenų apsaugą nuo modifikavimo/piktybiško užšifravimo/sunaikinimo.

Rezervinio duomenų kopijavimo sprendimų į viešosios debesijos platformas realizavimas atskiriamas į dvi dalis:

1. Valstybės įstaigos, kurios nesinaudoja konsoliduota VDPT platforma, šį funkcionalumą turės realizuoti pačios pasinaudojant hibridinės debesijos veiklos modeliu bei jų naudojamos rezervinio kopijavimo PĮ priemonėmis.
2. Valstybės įstaigos, kurios naudojasi konsoliduota VDPT platforma rezervinio kopijavimo sprendimu į viešosios debesijos platformas galės naudotis kaip platformos lygio paslauga, valdoma VDPT operatoriaus. Rezervinės duomenų kopijos iškėlimas į viešosios debesijos platformas užtikrina papildomą duomenų apsaugą bei leidžia atstatyti tenantų duomenis VDPT platformoje arba bet kurioje kitoje VDPT operatoriaus kontroliuojamoje platformoje (Lietuvoje esančių duomenų centrų praradimo atveju).

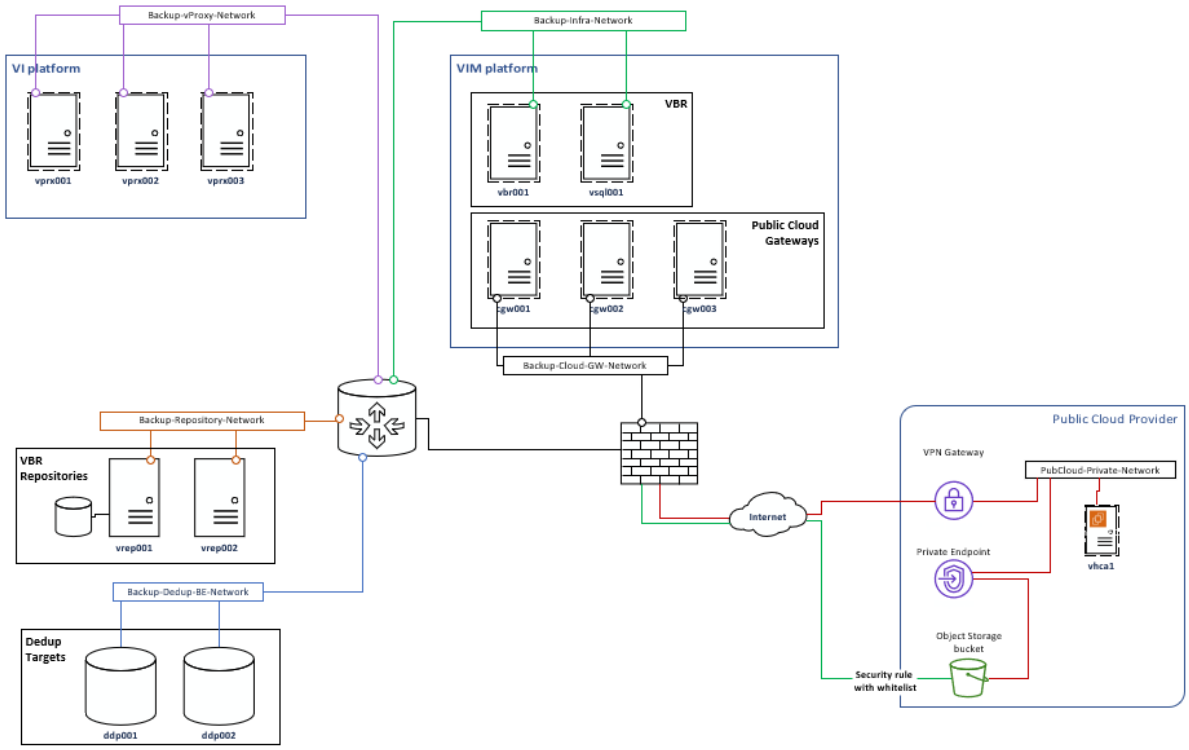
5.1 VDPT platformos rezervinio kopijavimo į viešosios debesijos paslaugas sprendimo architektūra

Rezervinio kopijavimo į viešosios debesijos paslaugų gamintojo siūlomas objektinių saugyklų paslaugas sprendimo architektūra. Tam tikslui kuriama dedikuota hierarchija su mažiausiai trimis organizaciniais vienetais (OU), bei atitinkamais paskyros konteineriais:

1. Saugos OU su įrašų archyvų bei audito paskyromis.
2. Platformos paslaugų OU su tinklo paslaugų paskyra (skirta VPN tunelio su VDPT infrastruktūra realizavimui).
3. Aplikacijų OU su rezervinio kopijavimo sprendimui skirta paskyra, kurioje kuriamos objektinės saugyklos resursai bei skaičiavimo resursai reikalingi rezervinių kopijų integralumo tikrinimui. Šio OU lygyje konfigūruojamos saugumo politikos nustatančios

saugumo parametrus, tokius kaip draudimas nustatyti objektinės saugyklos resursams galimybę viešai prieigai ir pan.

5.2 VBR sprendimo architektūra



Pav. 2 Rezervinio kopijavimo į viešosios debesijos paslaugas sprendimo architektūra

Rezervinių duomenų kopijų kopijavimui į viešosios debesijos paslaugų gamintojo objektinių saugyklų paslaugas esama VDPT rezervinio kopijavimo platforma išplečiama viešosios debesijos prieigos komponentais – Veeam šliuzais (angl. *gateway*), kurie konfigūruojami darbui su atitinkamo viešosios debesijos paslaugų gamintojo objektinių saugyklų paslaugų viešosios prieigos taškais (angl. *public endpoints*).

Viešosios debesijos paslaugų gamintojo pusėje atitinkamoje paskyroje sukuriami objektinių saugyklų resursai ir privatus tinklas, bei jam skirtos saugumo taisyklės. Planuojama, jog šiame tinkle bus automatiškai inicijuojami skaičiavimo resursai reikalingi rezervinių kopijų integralumo patikrinimui. Objektinių saugyklų resursų kūrimo metu planuojama įjungti apsaugą nuo duomenų sugadinimo/ištrynimo bei duomenų šifravimas su Kliento valdomais šifravimo raktais.

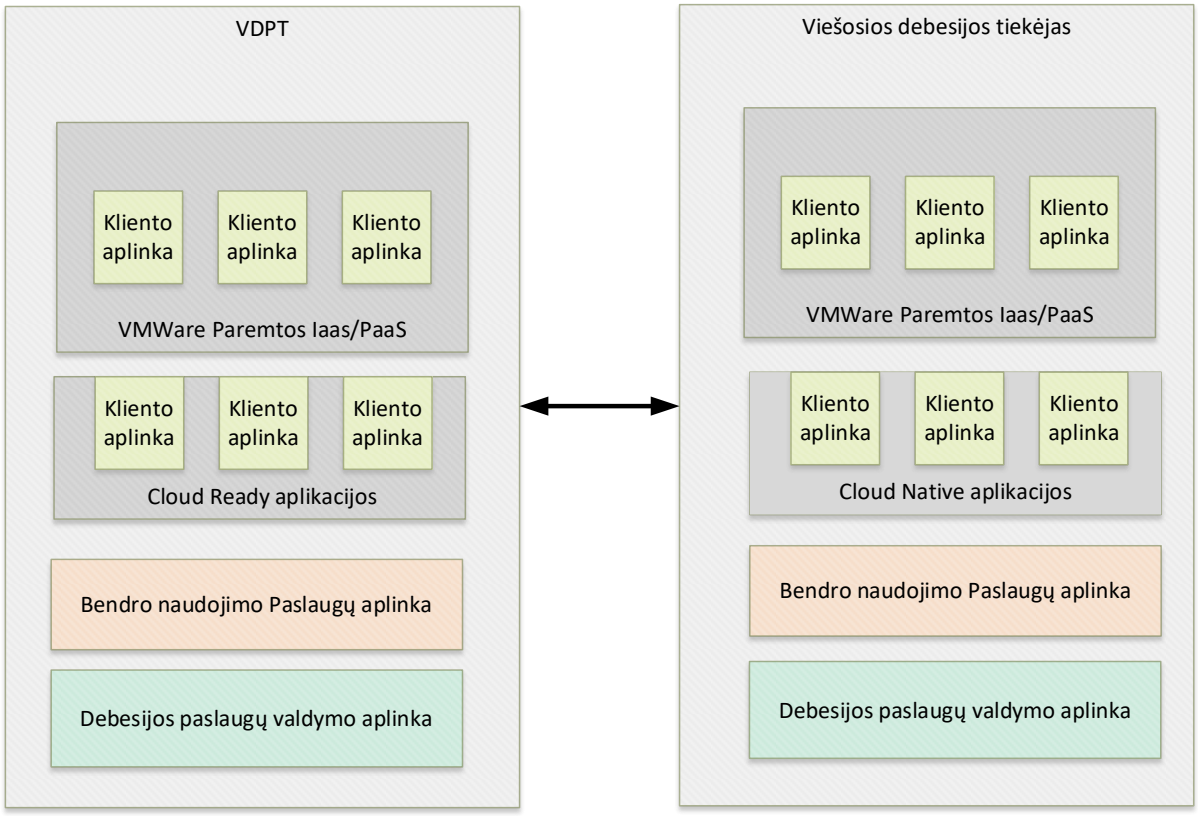
Duomenų kopijavimas iš VDPT infrastruktūros į viešosios debesijos paslaugų gamintojo objektinių saugyklų resursus planuojama bus vykdomas per viešosios prieigos taškus (angl. *public endpoints*). Visos duomenų kopijavimo užduotys privalo naudoti Veeam lygmens arba saugyklos lygmens duomenų šifravimą.

Tam kad šis procesas galėtų vykti sklandžiai, VBR serveris privalo apsikeisti šifravimo raktais su integralumo tikrinimą atliekančiu virtualiu serveriu. Ši komunikacija privalo būti vykdoma privačiais tinklais, todėl turi būti užtikrintas tinklų sujungimas tarp VDPT infrastruktūros ir atitinkamo viešosios debesijos paslaugos gamintojo. Įvertinus duomenų srautą šiam tikslui gali būti naudojamas VPN sujungimas (*site to site* VPN). VDPT infrastruktūroje esantys VBR infrastruktūros serveriai turėtų būti sukonfigūruoti duomenų apsikeitimui naudojant privačius tinklus – standartiškai tai atliekama per viešuosius tinklus. Objektinių saugyklų resursų turinį serveriai atliekantys integralumo patikrinimą pasiekia per privačius tinklus panaudojant privačios prieigos taškus (angl. *private endpoints*).

6. ANTRAS ETAPAS. Veiklos tęstinumo realizavimas viešosios debesijos platformose

Antrasis hibridinės debesijos sprendimo realizavimo etapas apima tenantų valdomų informacinių sistemų veiklos tęstinumo realizavimą pasirinkto viešosios debesijos paslaugų gamintojo platformoje.

Numatoma, jog šio etapo vykdymas bus atliekamas kiekvienos informacinės sistemos apimtyje atskirai, išanalizuojant jos struktūrą, komponentų sąryšius, ryšius su kitomis informacinėmis sistemomis, pagal poreikį adaptuojant informacinę sistemą darbui viešosios debesijos paslaugų gamintojų platformose, paruošiant veiklos tęstinumo planus bei aktyvavimo procedūras, įdiegiant *disaster recovery* sistemos komponentus pasirinktoje viešosios debesijos platformoje, bei užtikrinant informacinės sistemos duomenų bei rezervinių kopijų nuolatinį atnaujinimą. Visa tai realizuojama užtikrinant maksimalų duomenų perdavimo kanalų ir duomenų saugojimo bei apdorojimo resursų saugumą.



Pav. 3 Numatoma Disaster Recovery sprendimo principinė schema

Priklausomai nuo IS paslaugoms keliamų reikalavimų galimi 3 veiklos tęstinumo platformos resursų naudojimo modeliai:

1. *Hot stand-by* – IS reikalingi skaičiavimo bei duomenų saugojimo resursai yra pilnai dedikuoti ir aktyvūs visą laiką – tai pilnavertė nuolatos veikianti produkcinės IS infrastruktūros kopija, kuri, kaip ir produkcinė aplinka turi būti palaikoma. Tai maksimalaus funkcionalumo, greičiausio aktyvavimo bet ir maksimalios resursų kainos variantas.
2. *Warm stand-by* – IS yra dedikuoti minimalūs funkcionalumui bei duomenų sinchronizavimui užtikrinti skaičiavimo bei duomenų saugojimo resursai. Dalis resursų gali būti paruošti tačiau laikomi išjungtoje būsenoje. Platformos neveikimo atveju galimas IS komponentų resursų padidinimas, bei trūkstamų komponentų paleidimas. Tai optimalaus resursų naudojimo, vidutinio aktyvavimo greičio bei vidutinės (optimalios) kainos variantas.

3. *Cold stand-by* – yra paruošti IS reikalingi loginiai komponentai reikalingi IS komponentų tarpusavio komunikacijai, bei komunikacijai su išore, tačiau nėra dedikuoti ir aktyviai naudojami skaičiavimo bei duomenų saugojimo resursai. Aktyviai naudojami tik rezervinio kopijavimo sprendimo komponentams reikalingi resursai. Platformos neveikimo atveju visi IS komponentai yra atstatomi iš rezervinių kopijų. Tai minimalių resursų, ilgo aktyvavimo laiko bei mažiausios kainos variantas.

Priklausomai nuo pasirinkto modelio galimi 3 pagrindiniai duomenų replikavimo tarp produkcinių ir DR platformų sprendimai:

1. Duomenų bazės / aplikacijos lygio duomenų replikavimas. Taikytinas duomenų bazių bei kitų *stateful* aplikacijų turinčių nuosavus duomenų integralumą užtikrinančius duomenų replikavimo mechanizmus.
2. Trečių šalių replikavimo sprendimai (rezervinio kopijavimo bei kitų PĮ tiekėjų siūlomi snapshot based arba *Continuous Data Protection* sprendimai).
3. Rezervinio kopijavimo valdoma duomenų kopija į DR platformą.

Veiklos tęstinumo platformos modelių palyginimas:

	Hot stand-by	**Warm stand-by**	**Cold standby**
RTO ir RTO	Trumpiausias atstatymo laikas Tiesiogiai priklauso nuo IS sudėtingumo ir kritiškumo	Vidutinis atstatymo laikas Tiesiogiai priklauso nuo IS sudėtingumo ir kritiškumo	*Vidutinis arba Didelis atstatymo laikas* *Tiesiogiai priklauso nuo IS sudėtingumo*
Aktyviai naudojami resursai	• Skaičiavimo resursai • Duomenų saugojimo resursai • Rezervinio kopijavimo saugyklos resursai	• Skaičiavimo resursai (daliniai) • Duomenų saugojimo resursai • Rezervinio kopijavimo saugyklos resursai	• Rezervinio kopijavimo saugyklos resursai
Naudotini duomenų replikavimo sprendimai	• DB/Aplikacijos lygio replikavimas	• DB/Aplikacijos lygio replikavimas • VM replika/CDP sprendimai • Atstatymas iš rezervinės kopijos	• Atstatymas iš rezervinės kopijos
Resursų kaina	●●●	●●	●
DR sprendimo priežiūros kaštai	●●●	●●	●

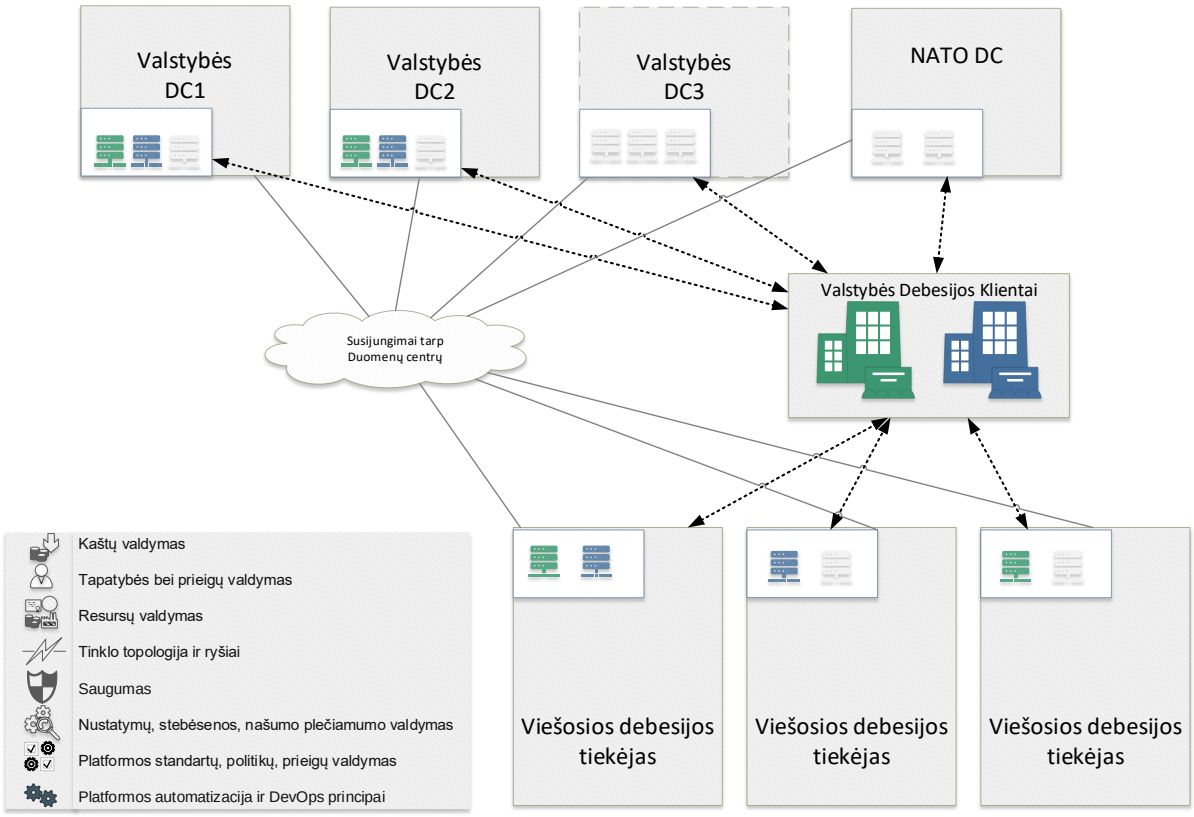
Lentelė Nr. 5 Veiklos tęstinumo platformos modelių palyginimas

7. TREČIAS ETAPAS. Viešosios debesijos paslaugų naudojimas nekritinėms informacinėms sistemoms

Nekritinės valstybės IS gali būti diegiamos viešosios debesijos platformose. Anksčiau minėtų sistemų diegimui turi būti naudojamos VSSA teikiamos paslaugos. IS įdiegtų viešosios debesijos platformose kopijos privalo būti saugomos bent viename Valstybės duomenų centre. Numatoma, jog detalūs reikalavimai nekritinių valstybės IS diegimui viešosios debesijos platformose bus aprašyti atskirame dokumente.

7.1 Hibridinės debesijos platformos architektūros gairės

Šiame skyriuje aprašoma išplėstos viešosios debesijos sprendimais VDPT platformos architektūra (toliau – Hibridinės debesijos platforma). Hibridinės debesijos platformos architektūra suprojektuota atsižvelgiant į anksčiau išdėstytas VDPT platformos vystymo kryptis. Esminis architektūros tikslas – identiškas tenantų valdymo technologinis sprendimas turi būti taikomas visuose VDPT platformos vystymo etapuose.



Pav. 4 Hibridinio debesijos modelio architektūra (iliustracinis modelis bendram supratimui)

Esminiai siūlomo sprendimo architektūros principai:

- Esami Valstybės duomenų centrai saugiai (pvz., naudojant dedikuotus sujungimus) sujungiami su pasirinktais viešosios debesijos paslaugų gamintojais;
- Operatyviam valstybės kritinių IS ir registrų darbingumo atstatymui realizuojami DR sprendimai į viešosios debesijos platformas;
- Valstybės kritinėms IS ir registrams kurie naudoja legacy technologijas sudaroma galimybė naudoti šiuo metu valstybės IT paslaugų tiekėjo naudojamos IRT infrastruktūros

virtualizacijos platformos pagrindu realizuotą darbingumo atstatymo platformą veikiančią viešosios debesijos paslaugų gamintojo duomenų centruose;

- Modernių IS ir registrų valdytojams/tvarkytojams DR sprendimus numatoma realizuoti kiek įmanoma daugiau naudojant *Native* technologijas ir CI/CD procesus.

Viešosios debesijos platformos architektūra paremta geriausiomis pasaulio praktikomis ir viešosios debesijos Gamintojų rekomendacijomis, kuriomis remiantis rekomenduojama diegti ir valdyti visą infrastruktūrą debesijoje. Pamatiniai principai :

- Kaštų valdymas;
- Tapatybės bei prieigų valdymas;
- Resursų valdymas;
- Tinklo topologija ir ryšių valdymas;
- Saugumo užtikrinimas;
- Nustatymų, stebėsenos, našumo plečiamumo, valdymas;
- Platformos standartų, politikų, prieigų valdymas;
- Platformos automatizacijos užtikrinimas.

Šie architektūros dizaino principai leidžia užtikrinti saugumą bei centralizuotai ir sklandžiai valdyti, plėsti, migruoti ar kurti aplikacijas ir visą reikalingą palaikymo infrastruktūrą naudojant pačias geriausias praktikas ir patirtis. Detaliau:

https://docs.aws.amazon.com/wellarchitected/latest/framework/definitions.html

https://cloud.google.com/architecture/framework/system-design/principles

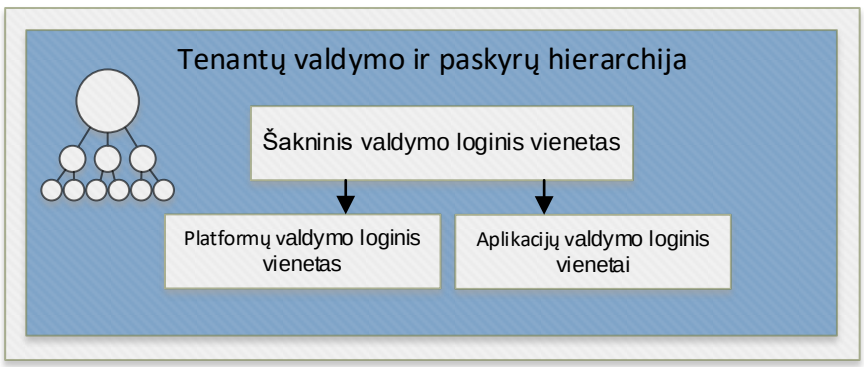
https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/landing-zone/design-principles

Aprašyti viešosios debesijos architektūros principai gali būti taikomi pagrindinėms viešosios debesijos platformoms, bet priklausomai nuo platformos gali skirtis įgyvendinimo priemonės.

7.2 Hibridinės debesijos tenantų valdymo principai

Architektūra realizuojama diegiant valdymo loginius vienetus taip išskaidant ir atskiriant debesijoje naudojamus resursus pagal jų pobūdį, funkcijas, valdymą ar kitus poreikius. Principai naudojant skirtingas viešosios debesijos paslaugų gamintojų platformas gali skirtis.

Valdymo loginiai vienetai yra kertiniai visos architektūros pamato elementai, kuris išlaiko hierarchiją ir gali atspindėti organizacijos struktūrą. Valdymo loginiai vienetai leidžia naudoti centrinį politikų taikymo modelį. Valdymo loginiai vienetai taip pat leidžia pritaikyti rolėmis pagrįstą prieigos kontrolę, valdyti teises vartotojams, grupėms ir kitiems objektams paskyrų lygyje.



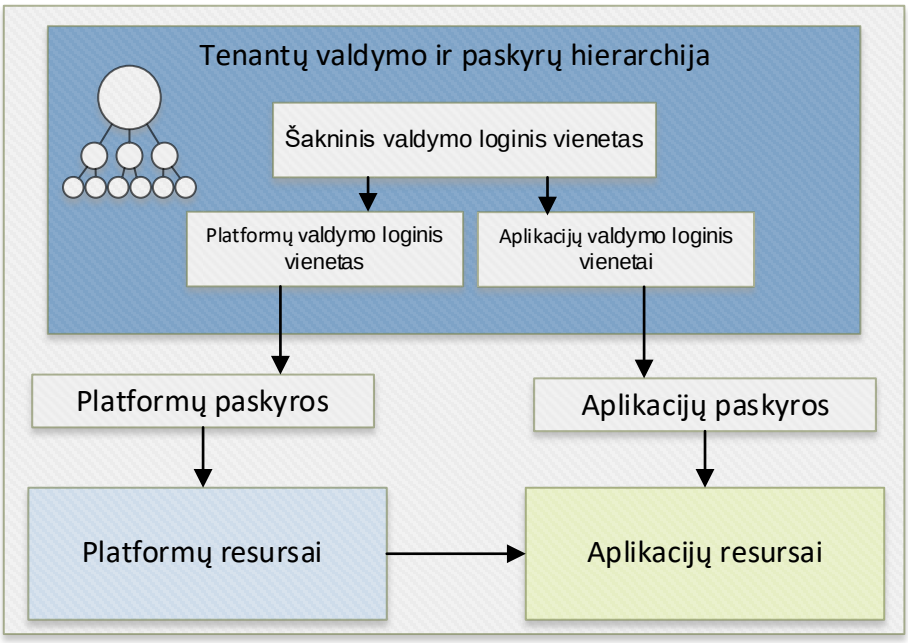
Pav. 5 Tenantų valdymo ir paskyrų hierarchija

Valdymo loginių vienetų kūrimo principai:

- Paskyra gali priklausyti tik vienam loginiam valdymo vienetui;
- Loginių valdymo vienetų hierarchija turi ribotą gylį;
- Loginių valdymo vienetų hierarchija priklausomai nuo poreikio gali grupuoti paskyras pagal organizaciją, organizacijos struktūrą, aplinką, tipą, aplikaciją arba kitą bendrą kriterijų.

7.3 Hibridinės debesijos paskyrų valdymo principai

Platformai valdyti naudojami dedikuoti loginio valdymo vienetai (platforminiai arba bendrintų paslaugų), kuriuose talpinamos dedikuotos paskyros, su platformai arba bendrintos paslaugos dedikuoti resursai. Aplikacijoms ir jos resursams dedikuojami atskiri loginio valdymo vienetai, kuriose talpinamos aplikacijų paskyros ir aplikacijų resursai. Principai naudojant skirtingas viešosios debesijos paslaugų gamintojo platformas gali skirtis.



Pav. 6 Hibridinės debesijos paskyrų valdymo principai

Paskyrų kūrimo principai:

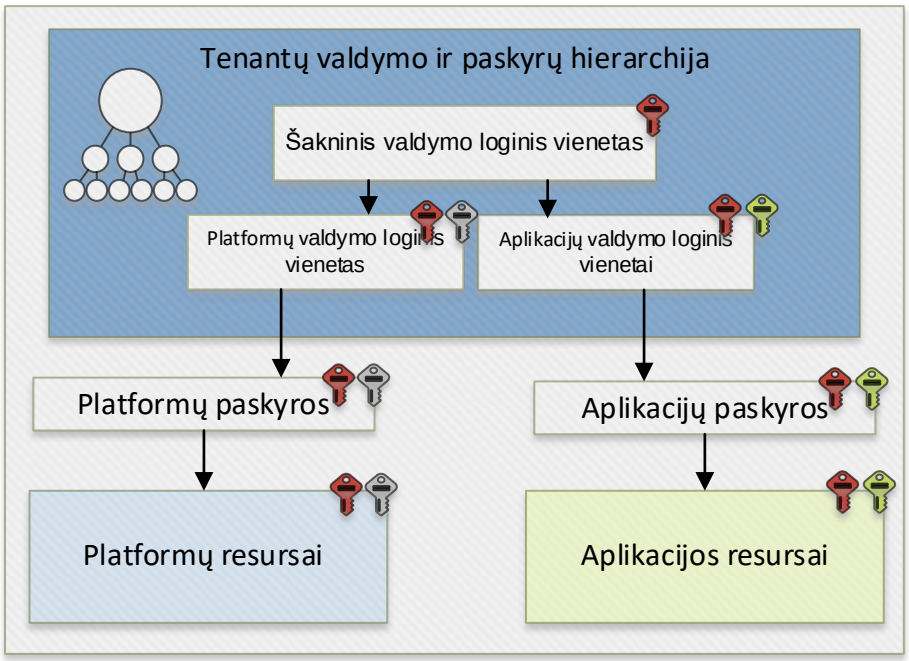
- Paskyra gali priklausyti tik vienam loginiam valdymo vienetui;
- Platforminės arba bendrintų paslaugų paskyros privalo būti izoliuotos nuo aplikacijų paskyrų, toki būdu užtikrinat prieigos ir atsakomybių atskyrimą bei galimybė pridėti arba šalinti paskyras neįtakojant esamos infrastruktūros.

7.4 Hibridinės debesijos paslaugų valdymo principai

Paslaugoms valdyti taikomos centralizuotos valdymo politikos, kurios užtikrina nuoseklių ir saugų išteklių valdymą, saugumo reguliavimo standartų laikymąsi, resursus, kaštų kontrolę, taip pat leidžia kategorizuoti bei žymėti resursus įvairiais pjūviais. Politikos taikomos pagal numatytą valdymo loginių vienetų struktūrą. Principai naudojant skirtingas viešosios debesijos paslaugų gamintojo platformas gali skirtis.

Numatoma, jog viešojoje debesijoje bus naudojami šie politikų tipai:

- Resursų politikos nustatys viešosios debesijos sąrašą leidžiamų resursų, kuriuos tenantai galės diegti ir naudoti savo paskyrose, bei užtikrins, kad resursai diegiami tik patvirtintuose viešosios debesijos regionuose;
- Resursų konfigūravimo politikos leis stebėti ir kontroliuoti tam tikrų resursų konfigūraciją – draus netinkamą konfigūraciją, arba leis konfigūraciją, bet informuos apie ją politikos valdytojui;
- Kaštų stebėjimo politikos leis stebėti tenantui priskirto biudžeto naudojimą.
- Tapatybės valdymo politikos leis užtikrinti atitikmenį saugaus prisijungimo ir valdymo standartams;
- Vardinimo politikos leis užtikrinti nuoseklumą ir aiškumą resursų pavadinimuose.
- Rakinimo politikos leis apsaugoti kritinius viešosios debesijos resursus nuo atsitiktinio arba nesankcionuoto ištrynimo arba modifikavimo.
- Žymų valdymo politikos leis užtikrinti, kad vis resursai turi žymes, pagal kurias galima identifikuoti resurso savininką, priklausomybę aplikacijai arba sistemai ir aplinką.
- Saugos atitikties politikos leis patikrinti atitikimą IT saugos standartams, pvz. CIS rekomendacijomis[1].



Pav. 7 Hibridinės debesijos paslaugų valdymo principai

Politikų taikymo principai:

- Politikos gali būti pritaikytos šakniniame lygyje, loginiame lygyje arba tiesiai paskyroms;

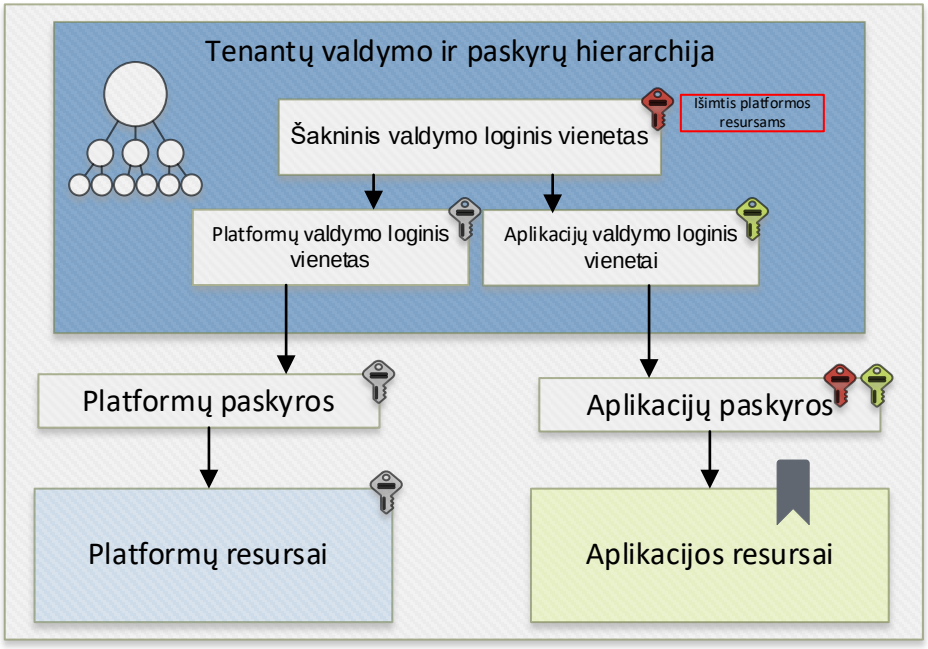
[1] CIS (Center for Internet Security) yra ne pelno siekianti organizacija, kuri teikia kibernetinio saugumo geriausiąsias praktikas, įrankius ir išteklius įvairioms pramonės šakoms ir sektoriams. Jos tikslas yra padėti organizacijoms apsaugoti savo IT sistemas nuo kibernetinių grėsmių. Šios organizacijos veikla yra pagrįsta bendruomenės sukurtomis rekomendacijomis, kurios padeda stiprinti saugumą ir sumažinti kibernetinių atakų riziką. CIS teikia daugiau nei 100 konfigūracijos gairių, apimančių daugiau nei 25 tiekėjų produktų šeimas, tokias kaip debesys, konteineriai, duomenų bazės ir mobiliajame įrenginyje naudojama programinė įranga.

- Politikos yra paveldimos: šakniniame lygyje pritaikytos politikos galioja visiems loginiams valdymo lygiams bei paskyroms, loginiams valdymo lygiams pritaikytos politikos galioja visoms paskyroms;
- Draudžiančios politikos turi viršenybę prieš leidžiančias politikas;
- Visada galioja labiausiai ribojanti politika, nepriklausomai nuo pritaikymo lygio.

Politikų išimčių taikymo principai:

Kad politika pradėtų galioti ją reikia paskirti valdymo grupei arba paskyrai. Paskyrimo metu gali būti nurodyta išimtis kokioms paskyroms arba resursams (nurodant resurso identifikacijos numerį) politika nėra taikoma. Paskyrimas po politikos paskyrimo gali būti keičiamas.

Lanksčiam politikų išimčių valdymui viešojoje debesijoje išimtys gali būti taikomos žymų pagalba. Toks taikymo būdas leidžia pritaikyti išimtį ne nenurodant galutinio resursų identifikacijos numerį, o priskiriant resursui nustatytą žymę. Tokia žyma pažymėtiems resursams politika nebus taikoma. Tokioms žymoms pridėti prie išteklių turi būti sukuriama atskira rolė, kurios teises valdytų, ir ją priskirtų Viešosios debesijos paslaugų valdytojas. Įprasti administratoriai neturi turėti teisės priskirti žymas, kurios išskirtų resursus iš politikų taikymo.

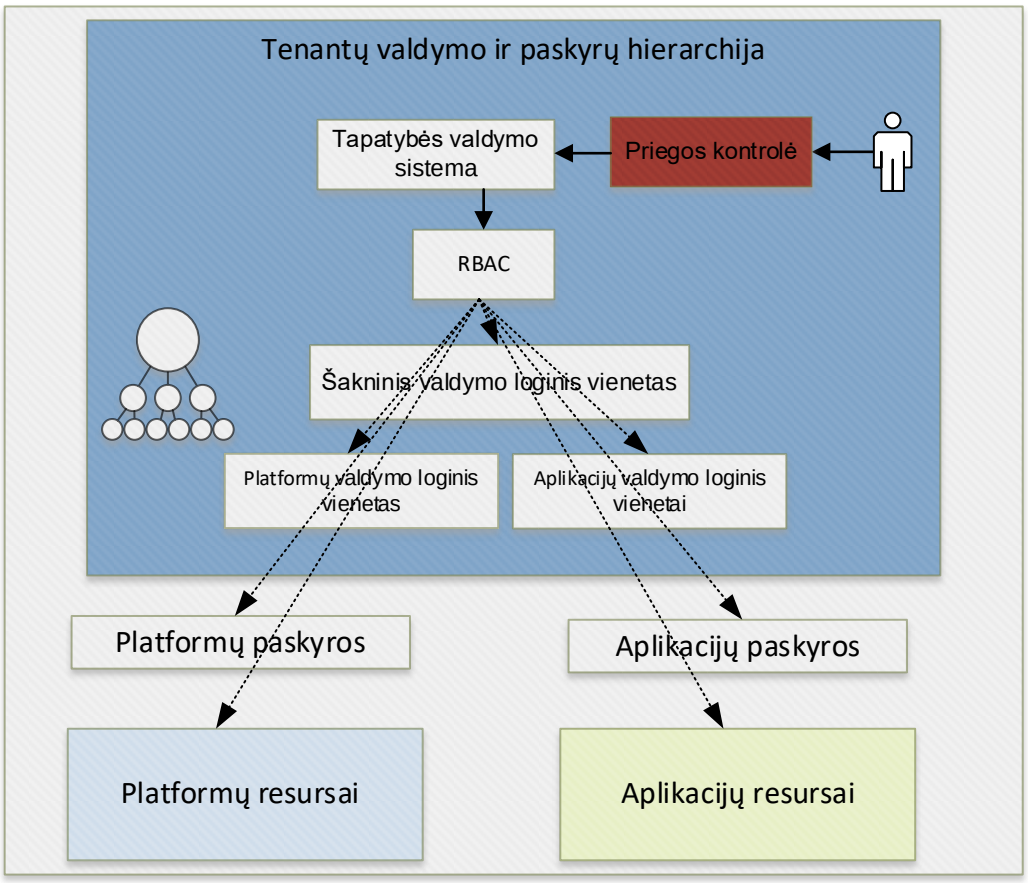


Pav. 8 Pavyzdinė politika su išimtimi

Visos politikų išimtys, ištekliai su išskiriančiomis žymomis, turėtų būti stebimos ir audituojamos.

7.5 Hibridinės debesijos tapatybės ir prieigos valdymo principai

Rekomenduojama, jog Viešosios debesijos tapatybės valdymui būtų naudojamos platformos tapatybės valdymo priemonės susidedančios iš tapatybės valdymo sistemos, prieigos kontrolės priemonių ir rolėmis paremtos prieigos valdymo. Tapatybės valdymo sistemoje bus kuriamos vartotojų, grupių ir techninės paskyros. Prieigos kontrolės priemonės užtikrins, kad prieiga prie viešosios debesijos galima tik patvirtinus tapatybę naudojant kelių faktorių autentifikavimą ir tik iš patvirtintų viešų IP adresų sąrašo. Rolėmis paremtos prieigos valdymas leis tiksliai apibrėžti, kas ir kur ir kokius resursus gali pasiekti ir kokius veiksmus jais gali atlikti. Principai naudojant skirtingas viešosios debesijos paslaugų gamintojo platformas gali skirtis.



Pav. 9 Tapatybės valdymo modelis

Tapatybės valdymo principai:

- Tiesos šaltinis (angl. *Source of truth*) viešosios debesijos paslaugų gamintojo IAM (angl. *Identity and Access Management*);
- Paskyros yra atskirtos ir izoliuotos nuo valdymo ir administravimo paskyrų;
- Prieiga suteikiama tik tam tikriems resursams ir tik apibrėžtiems veiksmams;
- Prieiga prie debesijos IAM galima tik patvirtinus tapatybę būtinu papildomu autentifikavimosi faktoriumi ir tik iš patvirtintų viešų IP adresų sąrašo;
- Galimybę kurti vartotojus viešosios pačioje debesijos IAM, sinchronizuoti vartotojus į viešosios debesijos IAM iš įvairių šaltinių (On-Premise Active Directory, Microsoft Entra ID, kt.);
- Galimybę autentifikuoti vartotojus į viešosios debesijos IAM iš įvairių šaltinių (On-Premise Active Directory, Microsoft Entra ID, kt.) bei autentifikuoti moderniais ir klasikiniais protokolais (OAuth 2.0, OpenID Connect, SAML, Kerberos);
- Modelis turi turėti palaikyti automatizuotas vartotojų kūrimo priemones (pvz. Terraform, Pulumi, Okta, etc.).

7.6. Valstybės hibridinės debesijos platformos naudotojų tapatybės ir prieigos valdymo principai

Įvertinus realius hibridinės debesijos platformos poreikius identifikuotos dvi potencialių naudotojų grupės: į VDPT sukonsoliduotos / konsoliduojamos valstybės įstaigos ir įstaigos, nepatenkančios į konsoliduojamų įstaigų sąrašą. Atsižvelgiant į paslaugų poreikį nuspręsta projektuoti platformą taip, kad būtų galima hibridinės debesijos platformos paslaugas teikti abiejų tipų naudotojų grupėms. Principai naudojant skirtingas viešosios debesijos paslaugų gamintojo platformas gali skirtis.

Turi būti galimybė sinchronizuoti vartotojus į viešosios debesijos IAM iš įvairių šaltinių (On-Premise Active Directory, Microsoft Entra ID, Google identity ir kt.).

7.6.1 Įstaigų/organizacijų atskyrimo ir valdymo modeliai

Įstaigos, nepatenkančios į konsoliduojamų įstaigų sąrašą **valdomos Organizacijos lygyje**. Kiekviena organizacija turi savo dedikuotas bendrų pagrindinių servisų (platformines) paskyras (Management, Network, Identity, Security ir pan.). Aplikacijos ar kiti loginiai vienetai atskiriami į atskiras zonas. Organizacija eksploatuoja debesijos paslaugas maksimaliai realizuojant nurodytą architektūrą.

Pliusai:

a) **Organizacijos lygio izoliacija.** Kiekviena organizacija turi dedikuotą tiek bendrų tiek dedikuotų servisų, resursų zoną.

b) **Detaliausiai pritaikytos politikos.** Kiekviena organizacija turi kontrolę visuose lygiuose, tiek valdymo, tiek saugumo, tinklo ar aplikacijų ir pan. lygiuose.

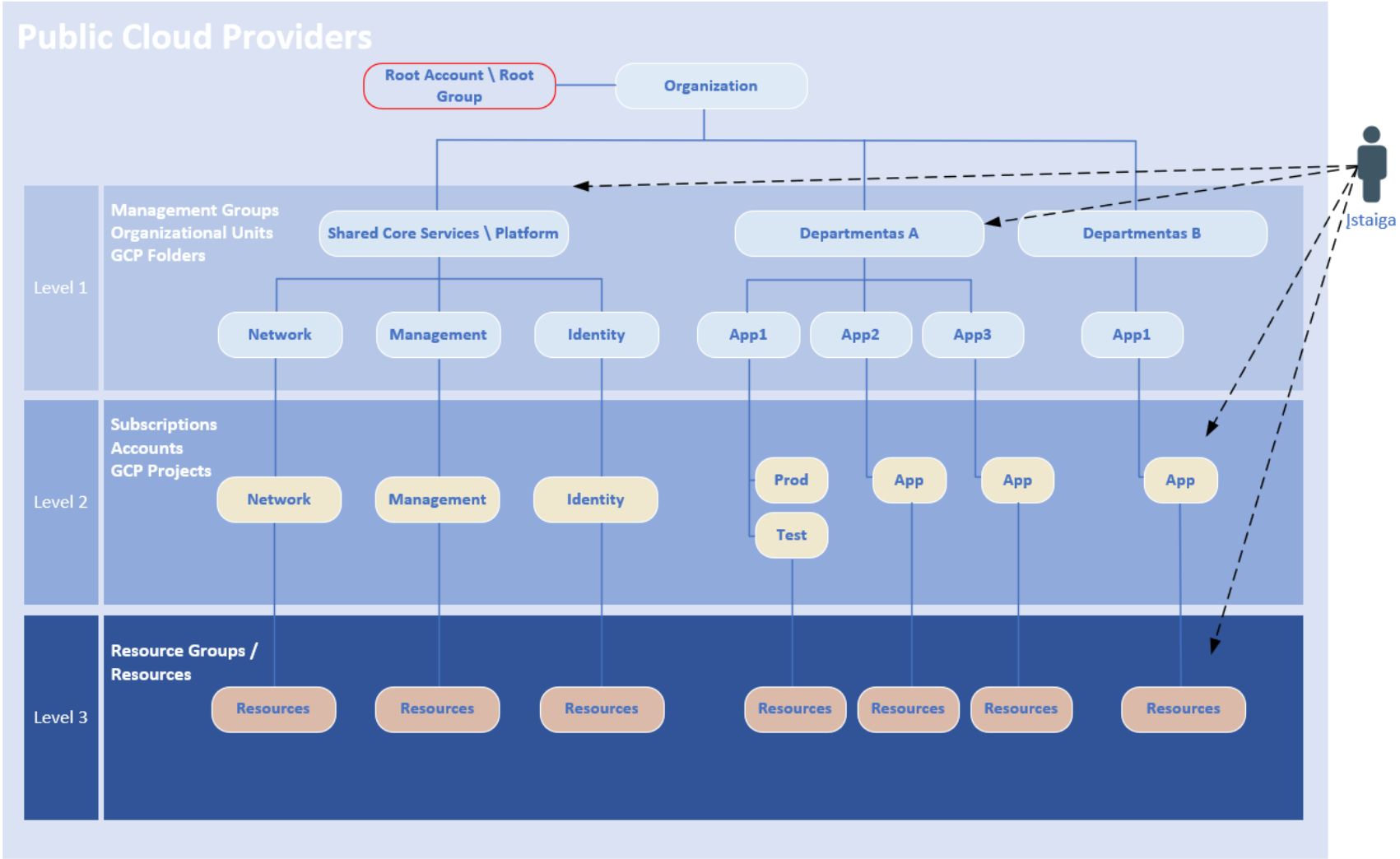
c) **Sumažinta saugumo rizika.** Tokio lygios izoliacija ir atskyrimas maksimaliai sumažina rizikas cross-tenant prieigų, aplinkų, resursų pasiekiamumui, kurios gali atsirasti dėl nenumatytų klaidų vykdant įvairias kasdienes operacijas.

Minusai:

a) **Padidėjęs valdymo kompleksiškumas**. Valdyti daug Organizacijų su daug paskyrų Organizaciniame lygyje yra ganėtinai sudėtinga, nes Įstaiga tokiu atveju turi maksimaliai kompleksišką infrastruktūros apimtį.

b) **Didesnės išlaidos priežiūrai.** Turint atskiras Organizacijas atskirtas tokiame lygyje maksimaliai išauga jų valdymo bei debesijos resursų kaštai, kurie kitais atvejais būtų naudojami daugiau negu vienai įstaigai.

Įstaigos prieigos valdymas dedikuotų tenantų valdymo modeliui:



Pav. 10 Įstaigos prieigos valdymas dedikuotų tenantų valdymo modeliui (schema naudojant skirtingas viešosios debesijos paslaugų gamintojo platformas gali skirtis).

Sukonsoliduotos / konsoliduojamos valstybės įstaigos galėtų būti **valdomos valdymo loginio vieneto lygyje** – Level 1 lygyje. Tokios įstaigos naudotųsi bendromis pagrindinių servisų paskyromis (Management, Network, Identity, Security ir pan.). Tokiu atveju kiekviena atskira įstaiga galėtų būti kuriama kaip atskira dedikuota zona tik tai įstaigai. O įstaiga gautų priėjimą arba Level 2 arba Level 3 lygyje, t.y. turėtų prieigą tik prie paskyros arba tik prie savo paskyros resursų.

Pliusai:

a) **Centralizuotas lengvesnis valdymas.** Valdytojas turi galimybę centralizuotai valdyti įstaigas paskyrų lygyje, taikyti joms politikas vienos dedikuotos zonos apimtyje.

b) **Resursų pasidalinimas.** Bendri kertiniai servisai (platforminiai) ir resursai naudojami visų šioje organizacijoje talpinamų įstaigų, todėl tiek jų valdymas tiek kaštai pasidalintų.

c) **Įdiegimo greitis ir kontrolė.**

Minusai:

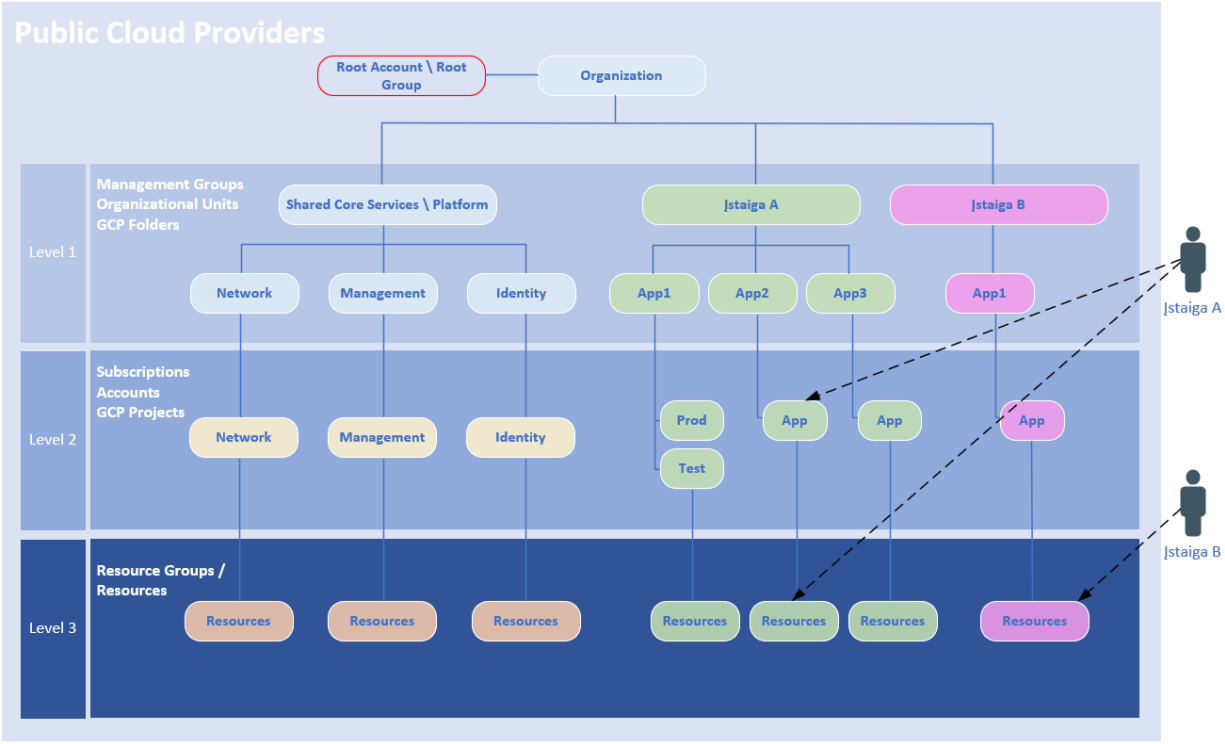
a) **Apribota izoliacija**. Įstaigų resursai būtų valdomi tos pačios Organizacijos (tenant) lygyje, todėl atsiranda tam tikros ribos kaip stipriai galime atskirti atskiras įstaigas, bei rizika dėl atskirų įstaigų duomenų atskirties.

b) **Politikų kompleksiškumas.** Teisių bei politikų valdymas tarp skirtingų įstaigų vienos organizacijos apimtyje gali tapti sudėtingas bei keliantis problemų ypač jeigu skirtingų įstaigų poreikiai iš esmės skiriasi.

c) **Priklausomybių rizika.** Kadangi visos įstaigos naudotų bendrus kertinius (platforminius) servisus, tai sutrikus jų veiklai poveikis būtų jaučiamas ne vienos įstaigos bet visų įstaigų esančių po viena organizacija lygyje.

d) **Reikalinga nuolatinė priežiūra ir palaikymo veikla, vykdant naujus įdiegimus ir atnaujinant esamus.**

Įstaigos prieigos valdymas bendro naudojimo tenantų valdymo modeliui:



Pav. 11 Įstaigos prieigos valdymas bendro naudojimo tenantų valdymo modeliui (schema naudojant skirtingas viešosios debesijos paslaugų gamintojo platformas gali skirtis).

8. VIEŠOSIOS DEBESIJOS PASLAUGŲ TENANTO ARCHITEKTŪRA

8.1 Viešosios debesijos paslaugų tenantų modeliai

Viešojoje debesijoje dominuoja į aplikacijas orientuota architektūra. Aplikacijų kūrimui, veikimui, palaikymui, stebėjimui ir apsaugai viešoje debesijoje yra naudojamos platformų paslaugos. Į platformines paslaugas įtraukiamos ir ryšių, saugumo, tapatybių valdymo, stebėjimo ir auditavimo paslaugos.

Kaip minėta anksčiau, aplikacijų platformų paslaugų valdymui yra dedikuojamos pagrindinės (platforminės arba bendrintų paslaugų) zonos, kurių kiekviena naudoja dedikuotą paskyrą. Toje paskyroje talpinami platformų paslaugų resursai.

Priklausomai nuo Tenanto dydžio ir resursų dalinimosi modelio, planuojami keturi tenanto architektūros modeliai:

- standartinio tenanto architektūra;
- midi tenanto architektūra;
- mini tenanto architektūra;
- mikro tenanto architektūra.

Tenanto pasirinkimas priklausys nuo organizacijos ir aplikacijos dydžio, platforminių resursų poreikio ir galimybės dalintis resursais ir paslaugomis, kad optimizuoti Viešosios debesijos kaštus.

- *Standartinio tenanto architektūra* – tai atskiro tenanto architektūra, kai organizacija valdo savo Platforminę ir Aplikacijų zoną. Tenantų komponentai yra visiškai nepriklausomi nuo kitų Tenantų komponentų. Platforminiai Resursai tarp tenantų nedalinami. Standartinio tenanto Platformų zonoje įgyvendinamas platformų tinklas, kuris be kitų būtinų komponentų talpina dedikuotus ryšio išteklius ir įgalina sujungimą tarp kitų tenantų, bendrintų paslaugų ir kitų Organizacijos tinklų. Perimetro apsaugos paslaugos yra dedikuotos tenantui. Architektūra skirta didelei įstaigai.

- *Midi tenanto architektūra* – tai atskiro tenanto architektūra, kuri labai panaši į Standartinio tenanto architektūrą. Skirtumas tarp Midi tenanto ir Standartinio tenanto toks, kad Midi tenantas nenaudoja dedikuotų išorinio perimetro apsaugos paslaugų, o dalinasi jomis su kitais tenantais – tokias paslaugas teikia VSSA. Architektūra skirta didelei ir vidutinei įstaigai, kai norima optimizuoti platforminių paslaugų kaštus.

- *Mini tenanto standartinė architektūra* – tai architektūra, kai platforminių resursų funkcionalumas yra dalinamas tarp tenantų, o platforminių paslaugų zonų resursai priklauso viešosios debesijos platformos valdytojui – VSSA. Aplikacijos zona tokiems tenantams yra dedikuota. Šio modelio architektūra turi tam tikrus ribojimus, nes atsiranda priklausomybės tarp tenantų. Numatomi veiksniai:
  - skirtinga IP komponentų adresacija;
  - įstaigų tinklų atskyrimas.

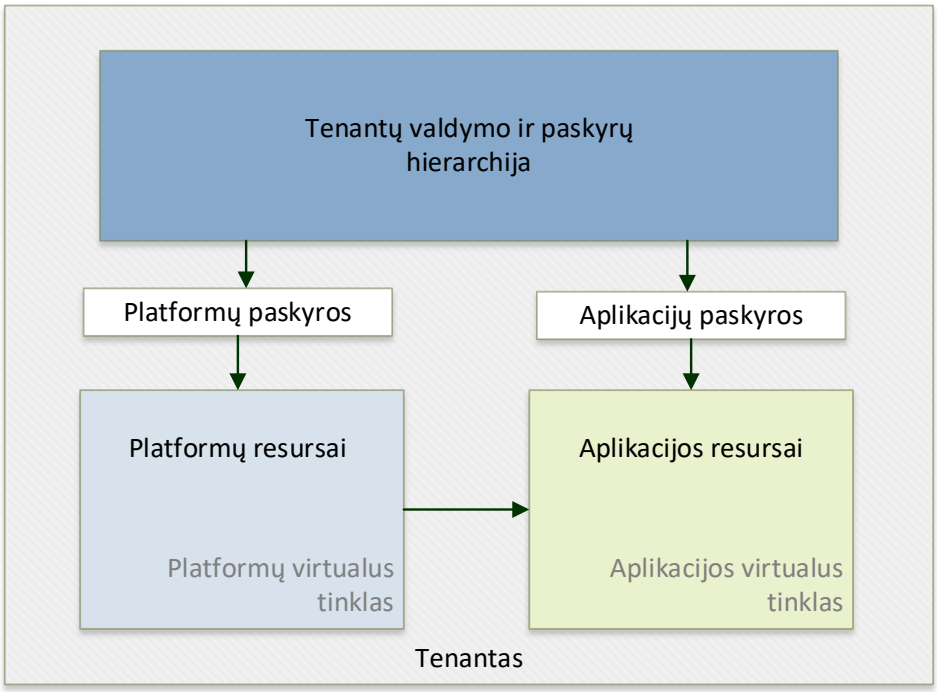
- *Mikro tenanto architektūra* – tai architektūra, kai tenantai turi tik WEB aplikaciją. Platforminių resursų funkcionalumas yra dalinamas tarp tenantų. Aplikacijų *Cloud-Native* komponentai – yra naudojamas grupės tenantų, bet valdomas viešosios debesijos platformos valdytojo. Panaudojant šį tenanto realizacijos modelį yra optimizuojami operaciniai kaštai. Šio tenanto architektūra yra skirta labai mažai įstaigai ar aplikacijai, kurios neturi savo dedikuotų platforminių išteklių.

Keičiant tenanto modelį iš vieno į kitą, gali prireikti resursų migracijos organizacijų valdymo medyje, ir, priklausomai nuo tenanto, migracijos iš vieno ryšio tinklo į kitą.

8.1.1 Viešosios debesijos paslaugų Standartinio tenanto architektūra

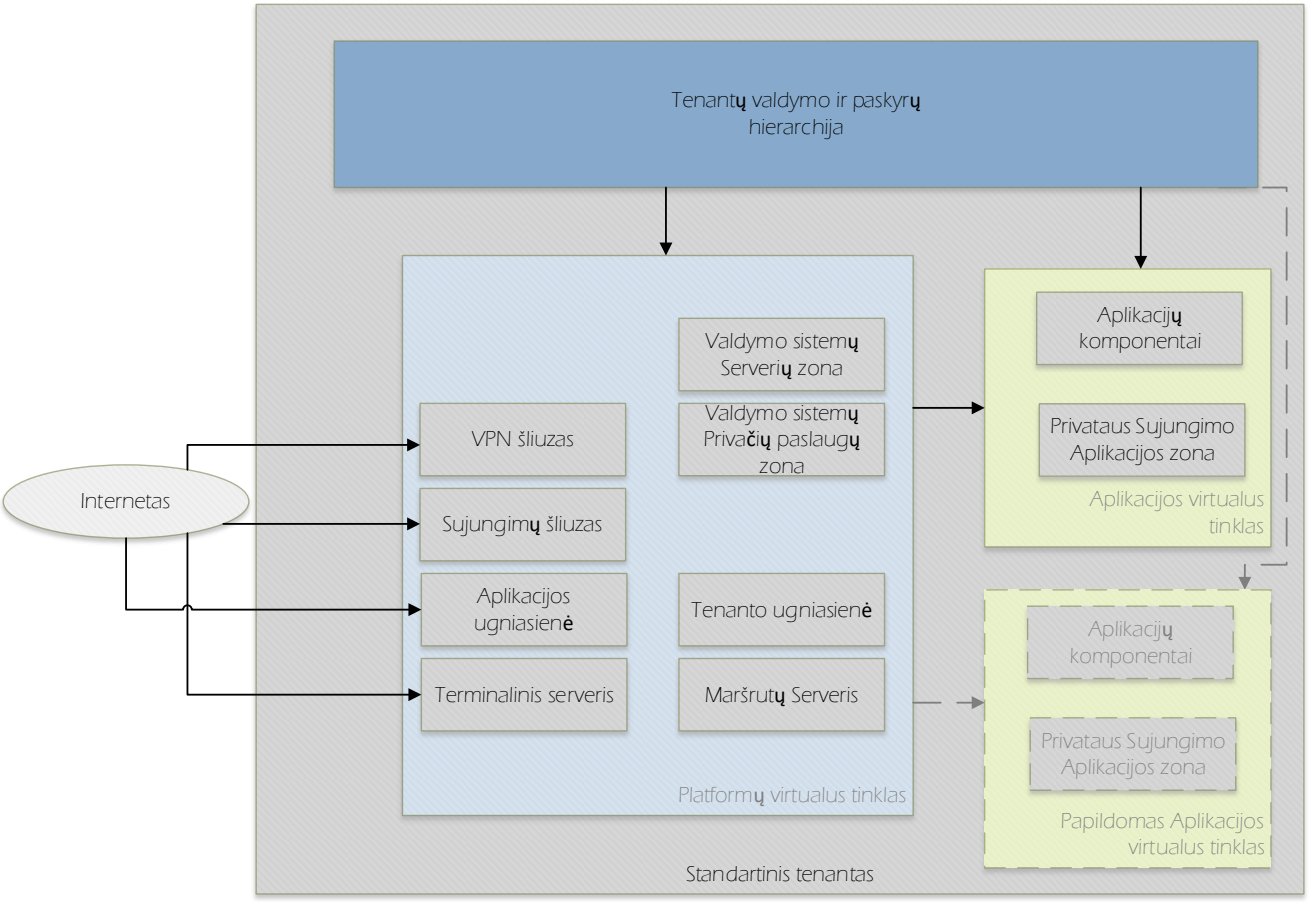
Standartinio tenanto architektūrą sudaro dvi dalys, kur viena skirta platformos resursams, kita – aplikacijos resursams. Įstaiga valdo tenanto platformines ir aplikacines paslaugų dalis.

Kiekvienai paskyrų grupei planuojamas virtualaus tinklo sukūrimas. Standartinio tenanto architektūrą sudaro 2 virtualūs tinklai. Esant poreikiui, plečiant tenanto infrastruktūrą, gali būti prijungiami daugiau aplikacijų virtualių tinklų.



Pav. 12 Galima standartinio tenanto principinė schema

Platformų ir Aplikacijų tinklai talpina skirtingus komponentus. Žemiau išvardintų komponentų grupės reikalingos viešosios debesijos paslaugų funkcijų užtikrinimui – stebėsenos, atitikimo standartams, saugumo ir ryšio užtikrinimui. Pačių komponentų, resursų kiekis ir turinys gali kisti priklausomai nuo tenanto modelio, dalinimosi ištekliais būdo, viešosios debesijos paslaugų gamintojo bei jo platformos ir galimų paslaugų pasiūlos.



Pav. 13 Galima standartinio tenanto architektūra

Platformų tinklo komponentai:

- VPN šliuzas – komponentas, skirtas IPSEC VPN tunelio sujungimams. Galimi sujungimų variantai Taškas-Tinklas, Tinklas-Tinklas ir kt.;
- Sujungimų šliuzas – komponentas, įgalinantis L3 tipo maršrutizuojamą sujungimą tarp skirtingų tenantų arba su Viešųjų paslaugų tenantu. Planuojama, kad šis komponentas gali būti naudojamas tik išimtiniais atvejais. Informacinės sistemos tarpusavyje turėtų bendrauti per aplikacijų programavimo sąsają (angl. *application programming interface, API*);
- Aplikacijos ugniasienė – komponentas, užtikrinantis Aplikacijos perimetro apsaugą nuo grėsmių. Priklausomai nuo aplikacijos poreikių, gali būti taikomi tokie apsaugos komponentai – DDoS apsauga, WAF – Web Application Firewall – Interneto WEB aplikacijų apsauga, IPS – įsilaužimų prevencijos apsauga ir kitos;
- Valdymo sistemų serverių zona – tai komponentas, įgalinantis veikti platforminių paslaugų servisus. Zonoje gali būti talpinami valdymo, stebėsenos (monitoring), įrašų kaupimo (logging), saugumo, tapatybės nustatymo ir kitas paslaugas teikiantys serveriai;
- Valdymo sistemų privačių paslaugų zona – tai komponentas, leidžiantis pasiekti viešąsias paslaugas naudojant „privatų sujungimą“ (Private link). Privatus sujungimas tai yra viešosios debesijos paslaugų gamintojo paslauga, kai tarp tenantų bendrintos paslaugos ir viešosios paslaugos gali būti saugiai pasiekiamos vidiniais viešosios debesijos paslaugų gamintojo tinklais;

- Tenanto Ugniasienė – tai komponentas, užtikrinantis duomenų srautų valdymą tenanto tinklo viduje;
- Maršrutų serveris – komponentas, užtikrinantis maršrutų apsikeitimą tarp Aplikacijų tinklų ir Platformų tinklų potinklių ir komponentų, kaip Ugniasienės ir šliuzai;
- Terminalinis serveris – komponentas, leidžiantis jungtis iš Tenanto tinklo į Aplikacijų ir kitus serverius jų valdymui.

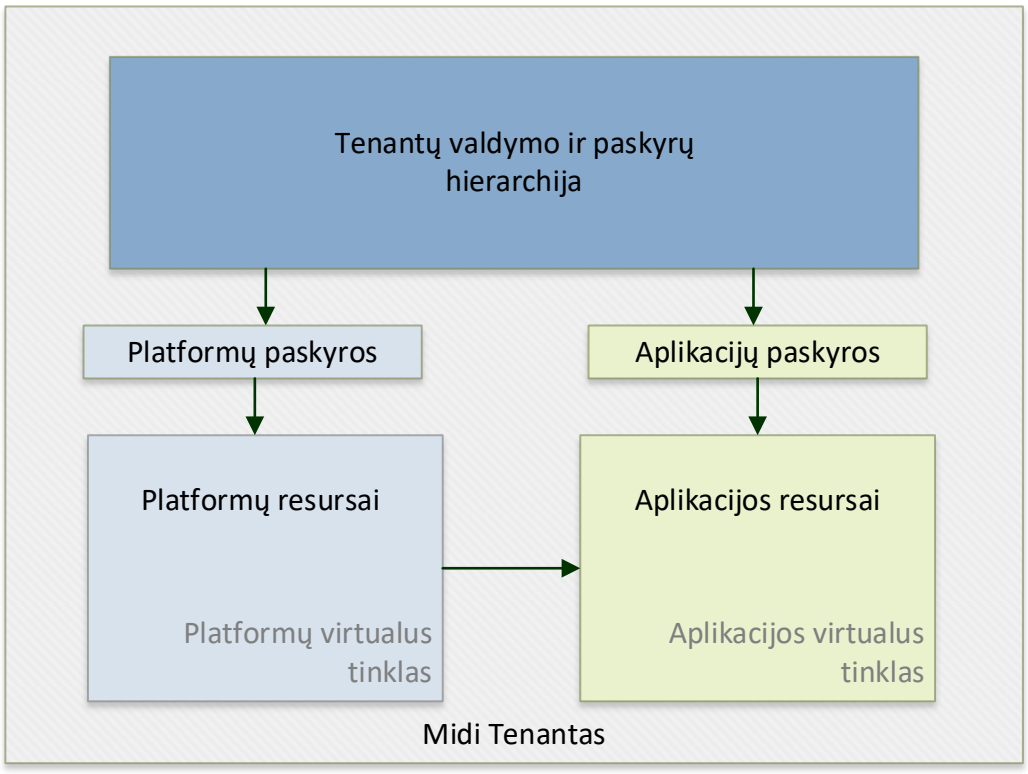
Aplikacijų tinklo komponentai:

- Aplikacijų komponentai – viešosios debesijos komponentai, užtikrinantys WEB aplikacijos veikimą ir jos paslaugos panaudojimą. Abstrakcija apima aplikacijos įgyvendinimą skirtingais būdais – be serverių komponentų, su serveriais – Windows/Linux, su VMWare komponentais, ir kita;
- Privataus sujungimo aplikacijos zona – tai komponentai, leidžiantys aplikacijai sukurti privataus sujungimo galimybę (Private Endpoint). Privatus sujungimas tai yra pačios viešosios debesijos paslaugų gamintojo įgalinta paslauga, kai bendros tarp tenantų ir viešosios paslaugos gali būti saugiai pasiekiamos vidiniais viešosios debesijos paslaugų gamintojo tinklais.

Aukščiau išvardinti komponentai sudaro Standartinio tenanto architektūrą. Naudojamų komponentų skaičius priklausomai nuo organizacijos dydžio gali skirtis. Kiti tenantų modeliai nebūtinai naudos visus aukščiau išvardintus, arba dalį aukščiau išvardintų platforminių ir aplikacijos komponentų.

8.1.2 Viešosios debesijos paslaugų Midi tenanto architektūra

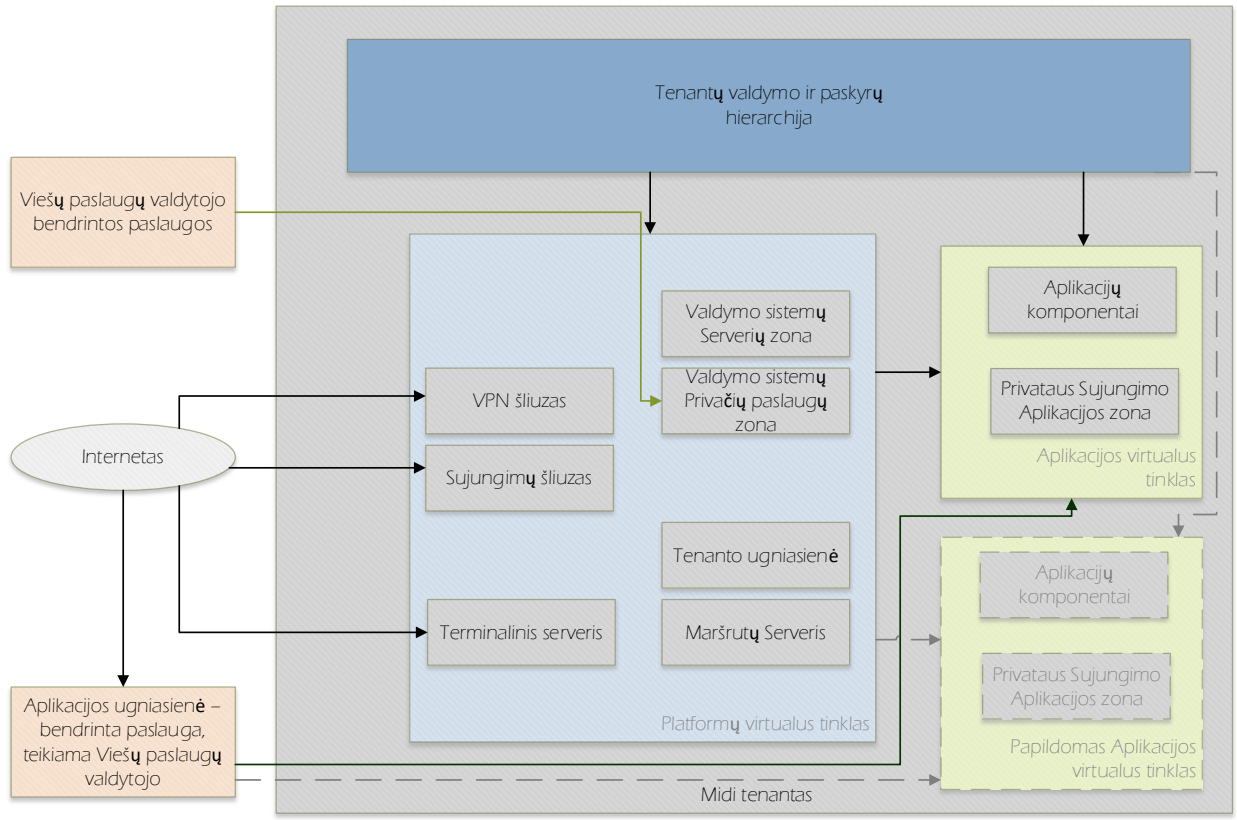
Ši architektūra panaši į Standartinio tenanto architektūrą, kai Įstaigos valdo ir platforminius ir aplikacijos resursus. Tačiau siekiant optimizuoti kaštus, bendrai naudoja VSSA teikiamas perimetro apsaugos (jeigu nėra KVTC klientas) ir kitas Edge paslaugas. Tokios sukonsoliduotos/konsoliduojamos valstybės įstaigos galėtų būti valdomos valdymo loginio vieneto lygyje – Level 1 lygyje.



Pav. 14 Midi tenanto principinė schema

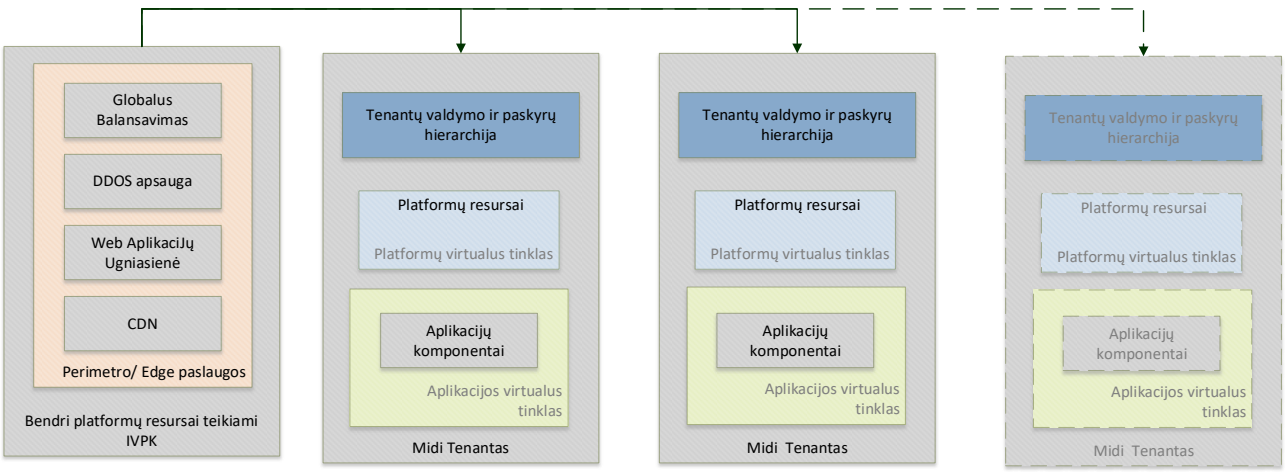
Šioje architektūroje Perimetro/Edge paslaugų funkcionalumas yra dalinamas tarp tenantų. Palyginus su Mini ir Mikro tenantų modeliu, Midi tenanto architektūrai nebūtinas tiesioginio tinklo susijungimas su Bendrų paslaugų valdytojo – VSSA – tenantu, kad panaudoti bendrintas paslaugas.

Platformų ir Aplikacijų tinklai talpina skirtingus komponentus. Žemiau išvardintų komponentų grupės reikalingos Viešosios debesijos paslaugų funkcijų užtikrinimui – stebėsenos, atitikimo standartams, saugumo ir ryšio užtikrinimui, ir t.t. Tačiau pačių komponentų, resursų kiekis ir turinys gali kisti priklausomai nuo tenanto modelio, dalinimosi ištekliais būdo, viešosios debesijos paslaugų gamintojo ir galimų paslaugų pasiūlos.



Pav. 15 Midi tenanto architektūra

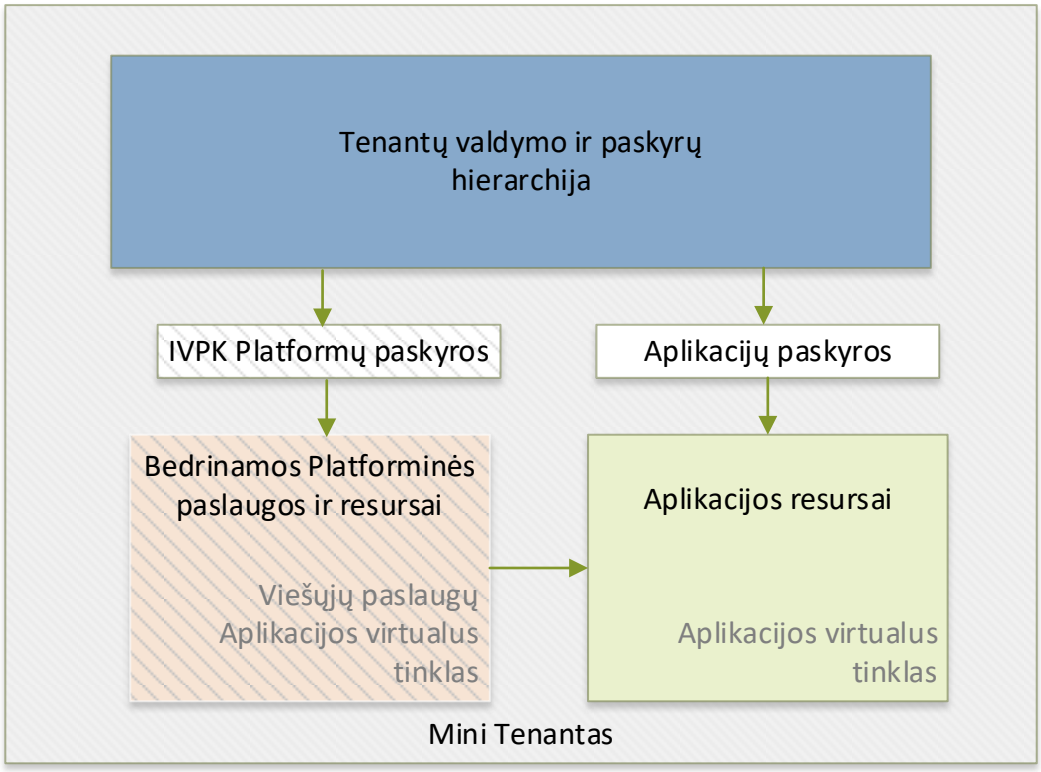
Midi tenantui gali būti teikiamos Viešų paslaugų valdytojo – VSSA - bendrintos paslaugos, kaip stebėjimo įrašų saugojimas, tapatybių valdymo, saugumo audito ir kt.



Pav. 16 Bendrintų Edge paslaugų teikimas Midi tenantams

8.1.3 Viešosios debesijos paslaugų Mini tenanto architektūra

Šioje architektūroje Platforminių resursų funkcionalumas yra dalinamas tarp tenantų. Platforminiai resursai priklauso Viešosios debesijos platformos valdytojui. Tenanto Aplikacijų resursus valdo Įstaiga. Šio modelio architektūra turi tam tikrus ribojimus, nes atsiranda priklausomybės tarp tenantų – Tenantų Aplikacijų komponentų IP adresacija turi būti skirtinga, yra limitų tenanto ryšio komponentams, priklausomai nuo viešosios debesijos paslaugų gamintojo.

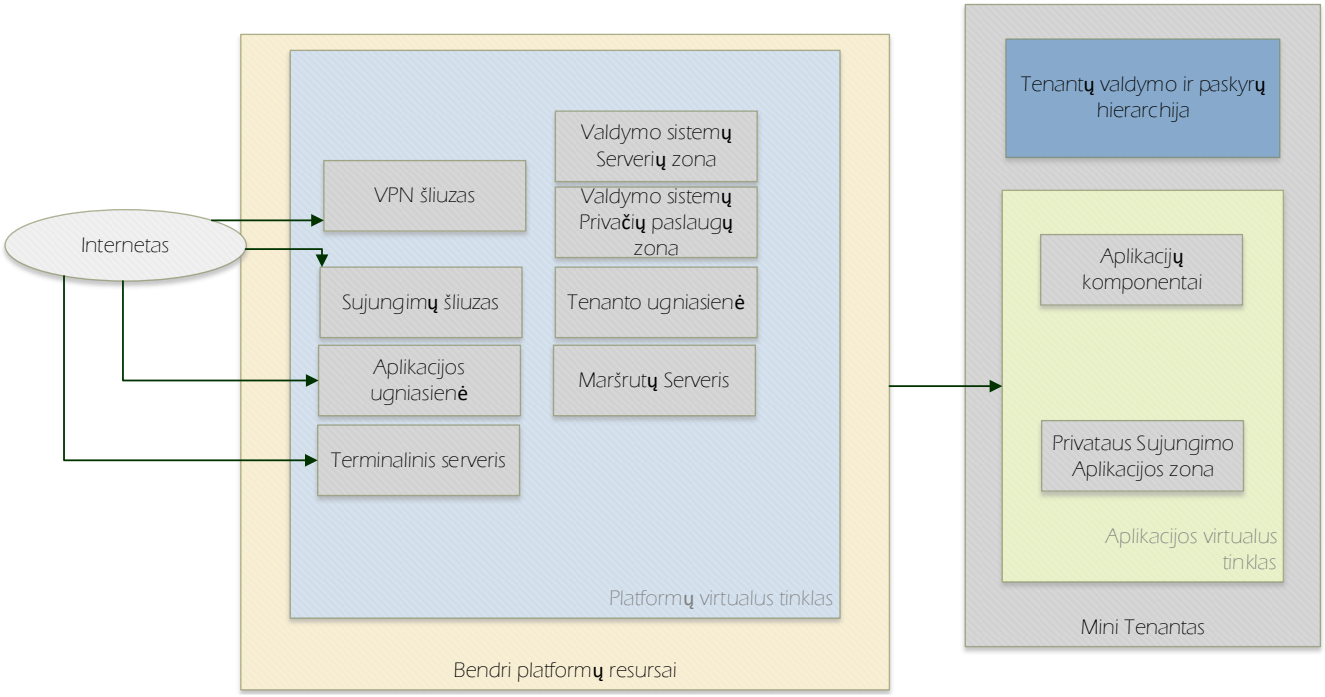


Pav. 17 Mini tenanto principinė schema

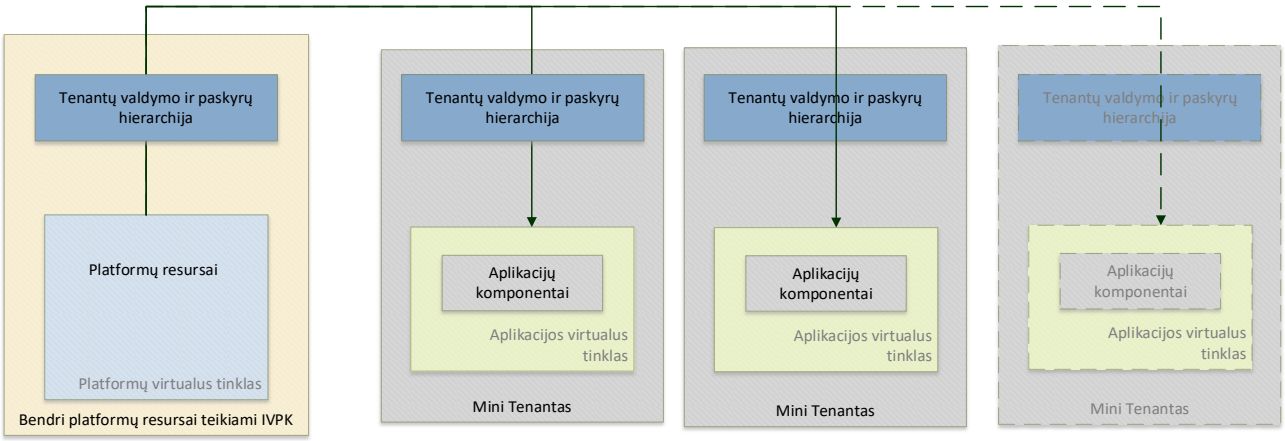
Platformų tinklo ir Aplikacijų tinklo komponentai gali būti tie patys, kaip ir standartinio modelio architektūros. Dalis ar visi platformos komponentai yra teikiami VSSA tenanto, ir tų komponentų funkcionalumas yra bendrinamas tarp kitų mini tenantų.

Tokiam platforminių paslaugų bendrinimui rekomenduotinas tiesioginis tinklų sujungimas tarp Viešų paslaugų valdytojo – VSSA tenanto ir Mini tenantų tinklų. Šiam modeliui rekomenduotina nepersidengiančios IP adresacijos tarp tenantų tinklų. Skirtingos įstaigos ir organizacijos gali turėti persidengiančią IP adresaciją savo biuruose ir duomenų centruose.

Platformų ir Aplikacijų tinklai talpina skirtingus komponentus. Žemiau išvardintų komponentų grupės reikalingos Viešosios debesijos paslaugų funkcijų užtikrinimui – stebėsenos, atitikimo standartams, saugumo ir ryšio užtikrinimui, ir t.t. Tačiau pačių komponentų, resursų kiekis ir turinys gali kisti priklausomai nuo tenanto modelio, dalinimosi ištekliais būdo, viešosios debesijos paslaugų gamintojo ir galimų paslaugų pasiūlos.



Pav. 18 Mini tenanto architektūra

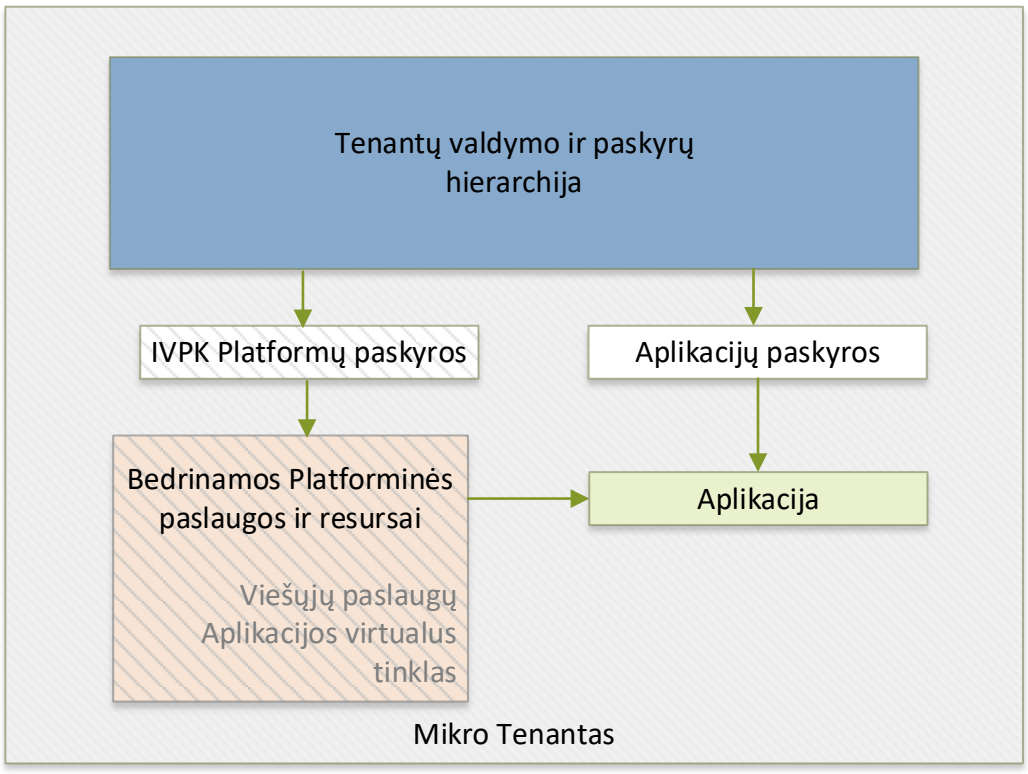


Pav. 19 Bendrintų paslaugų teikimas Mini tenantams

8.1.4 Viešosios debesijos paslaugų Mikro tenanto architektūra

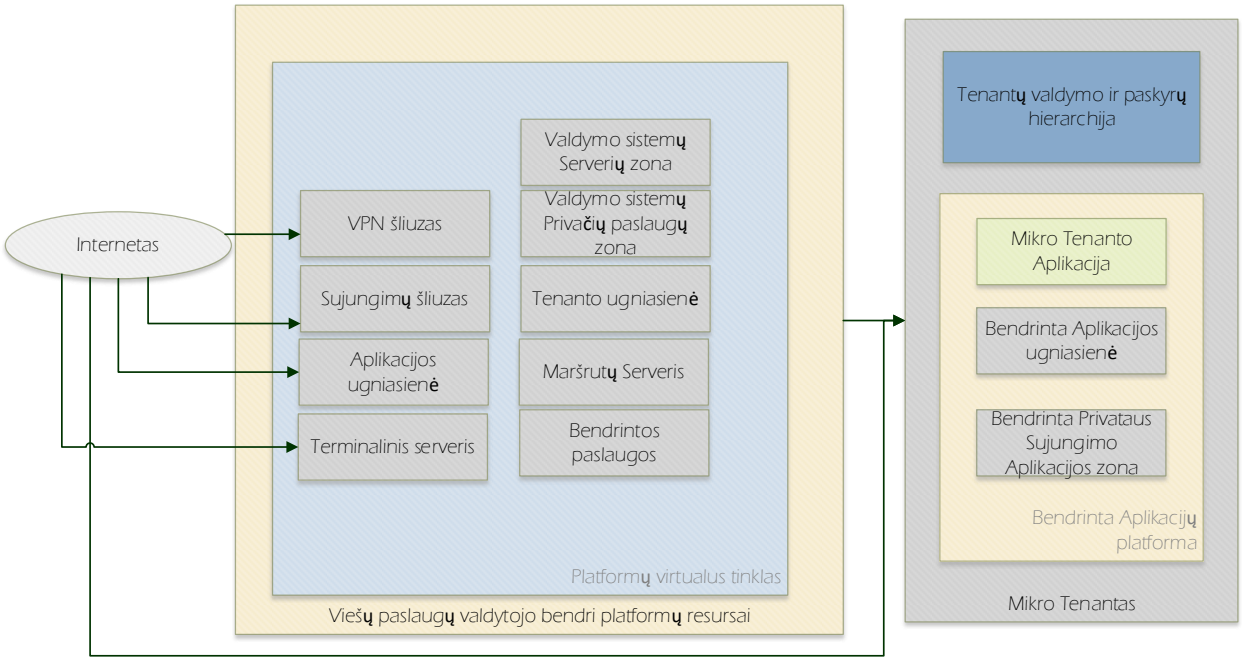
Šioje architektūroje tenantai turi tik WEB aplikaciją. Platforminių resursų funkcionalumas ir aplikacijų platformos resursai yra dalinami tarp tenantų.

Platforminių resursų funkcionalumas yra dalinamas tarp tenantų. Platforminiai resursai priklauso Viešosios debesijos platformos valdytojui - VSSA. Aplikacijų Cloud-Native komponentas – yra naudojamas grupės tenantų, o valdomas Viešosios debesijos platformos valdytojo. Šiuo būdu operaciniai kaštai yra optimizuojami labiausiai. Šiam architektūros modeliui Tenantų aplikacijos komponentai neturi sujungimo galimybės su įstaigų ar tenantų tinklais, tik su Viešosios debesijos platformos valdytojo – VSSA tinklais.



Pav. 20 Mikro tenanto principinė schema

Šiame modelyje Platformų ir Aplikacijų komponento resursus valdo Viešosios debesijos platformos valdytojas. Tenantas galėtų valdyti tik pačios Aplikacijos konfigūraciją.



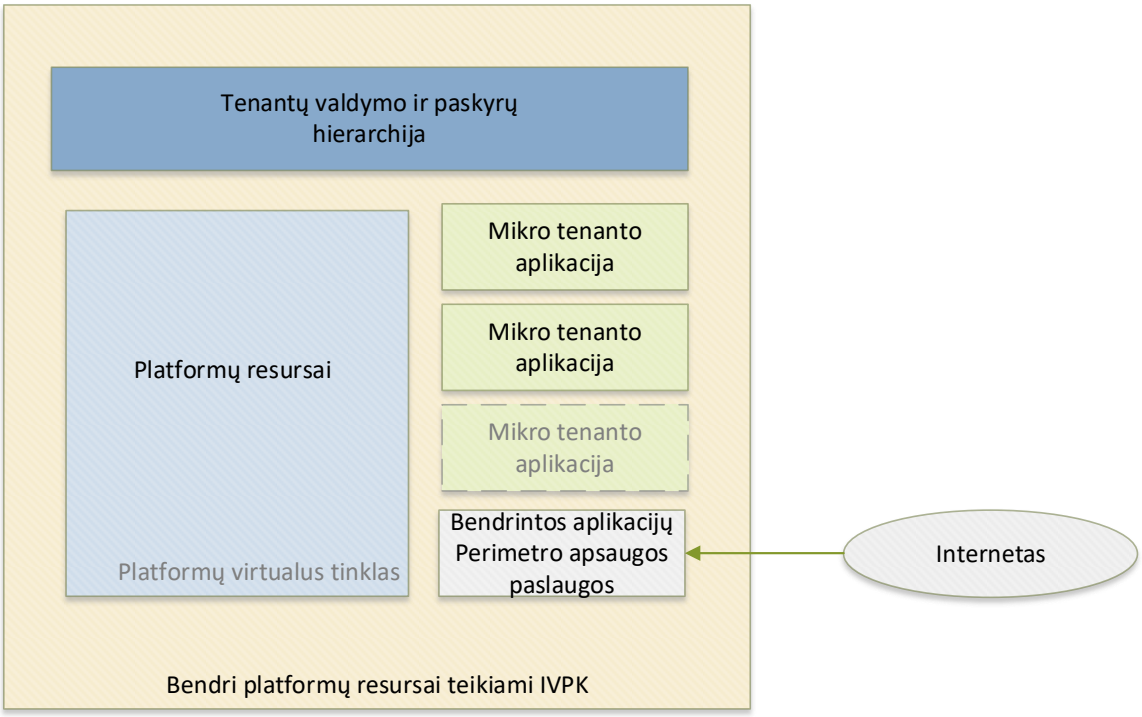
Pav. 21 Mikro tenanto architektūra

Platforminiai resursai šiame modelyje skiriasi tuo, kad, priklausomai nuo Aplikacijų komponento, Interneto ryšys ir aplikacijų apsauga galimai būtų taikoma su aplikacija susijusiais

komponentais, o ne platforminiame tinkle. Priklausomai nuo Aplikacijų komponento poreikių, platforminių komponentų gali mažėti.

Aplikacijų tinklo komponentai:

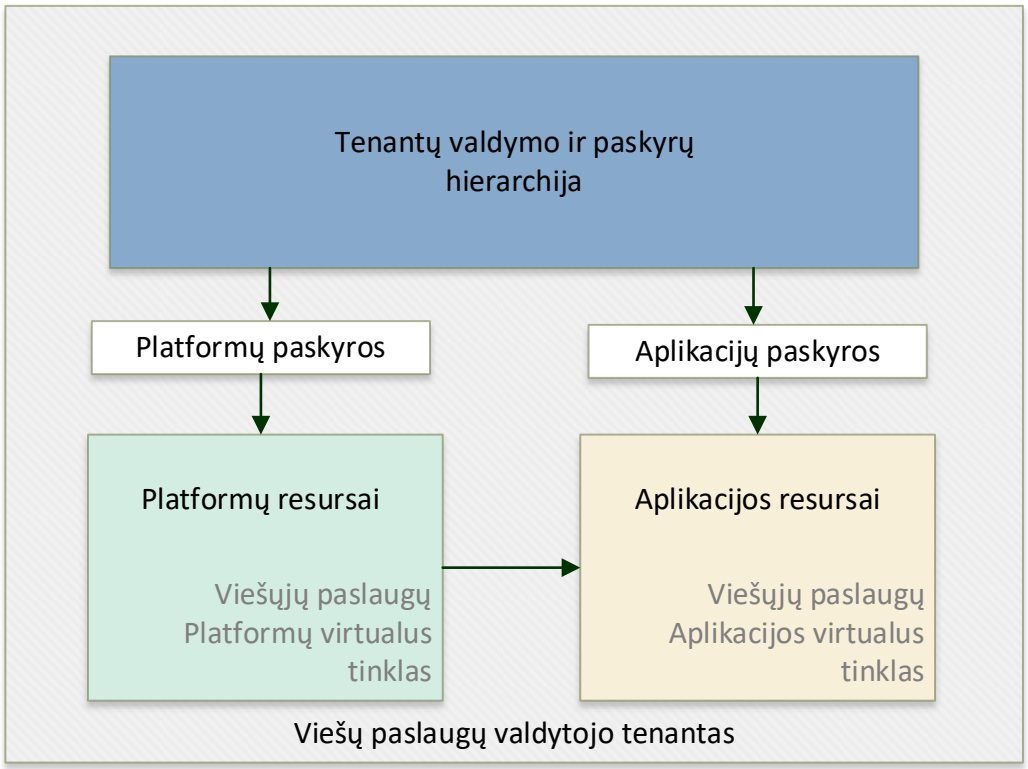
- Aplikacijų komponentai – viešosios debesijos komponentai, užtikrinantys WEB aplikacijos veikimą ir jos paslaugos panaudojimą naudojant Cloud Native priemones.
- Aplikacijos ugniasienė – komponentas, užtikrinantis aplikacijos perimetro apsaugą nuo grėsmių. Priklausomai nuo aplikacijos poreikių, gali būti taikomi tokie apsaugos komponentai – DDoS apsauga, WAF – Web Application Firewall – Interneto WEB aplikacijų apsauga, IPS – įsilaužimų prevencijos apsauga ir kitos. Viešosios debesijos paslaugų gamintojas yra atsakingas už savo aplikacijų ugniasienes, jų savalaikį atnaujinimą ir prisiimti pasekmes bei atsakomybę, įvykus platformos saugumo pažeidimui.



Pav. 22 Mikro tenantų aplikacijų modelis

8.1.5 Viešosios debesijos paslaugų Bendrų (viešų) paslaugų Valdytojo tenanto architektūra

Viešų paslaugų valdytojo – VSSA – tenanto architektūra atitinka standartinio tenanto architektūrą. Ją sudaro valdymo vienetų ir paskyrų hierarchija, ir dvi paskyrų grupės, kur viena skirta platformos resursams, kita – aplikacijos resursams. Kiekvienai paskyrai sukuriamas virtualus tinklas. Tenanto architektūrą sudaro 2 virtualūs tinklai. Esant poreikiui, plečiant tenanto infrastruktūrą, gali būti prijungiami daugiau aplikacijų virtualių tinklų.



Pav. 23 Viešų paslaugų valdytojo - VSSA - tenanto principinė schema

Platformų ir Aplikacijų tinklai talpina skirtingus komponentus. Žemiau išvardintų komponentų grupės reikalingos Viešosios debesijos paslaugų funkcijų užtikrinimui – stebėsenos, atitikimo standartams, saugumo ir ryšio užtikrinimui, ir t.t. Tačiau pačių komponentų, resursų kiekis ir turinys gali kisti priklausomai nuo tenanto modelio, dalinimosi ištekliais būdo, viešosios debesijos paslaugų gamintojo ir galimų paslaugų pasiūlos.

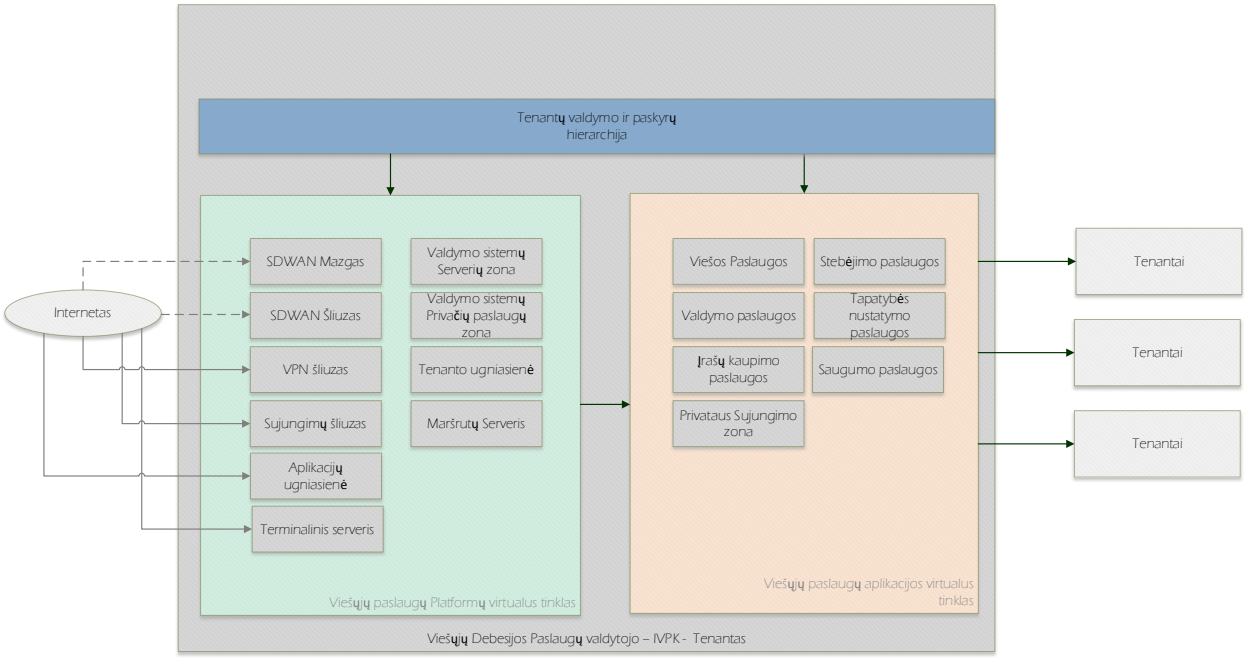
Platformų tinklo komponentai:

- SDWAN mazgas – komponentas, skirtas užtikrinti SDWAN tinklo veikimą jei nebus pasiekiami lokalūs Valstybės debesijos duomenų centrai, ir juose esantys SDWAN mazgai. Komponento būtinumas bus sprendžiamas įgyvendinimo metu;
- SDWAN šliuzas – Komponentas, skirtas susijungti su Viešų paslaugų valdytojo tenanto virtualiu tinklu, kuriuo galima pasiekti tenanto aplinkas Valstybės debesijoje arba tenanto biurą. Komponento būtinumas bus sprendžiamas įgyvendinimo metu;
- VPN šliuzas – komponentas, skirtas prisijungti prie tenanto IPSEC VPN pagalba. Sujungimai gali būti Taškas-Tinklas arba Tinklas-Tinklas;

- Sujungimų šliuzas – komponentas, įgalinantis L3 tipo maršrutizuojamą sujungimą tarp skirtingų tenantų;
- Aplikacijos ugniasienė – komponentas, užtikrinantis Viešų paslaugų valdytojo aplikacijų ir paslaugų apsaugą nuo grėsmių. Priklausomai nuo aplikacijos poreikių, gali būti taikomi tokie apsaugos komponentai – DDoS apsauga, WAF – Web Application Firewall – Interneto WEB aplikacijų apsauga, IPS – įsilaužimų prevencijos apsauga ir kitos;
- Valdymo sistemų serverių zona – tai komponentas, įgalinantis veikti platforminių paslaugų servisus. Zonoje gali būti talpinami valdymo, stebėsenos (angl. *monitoring*), įrašų kaupimo (logging), saugumo, tapatybės nustatymo ir kitas paslaugas teikiantys serveriai;
- Valdymo sistemų privačių paslaugų zona – tai komponentas, leidžiantis pasiekti viešąsias paslaugas naudojant „privatų sujungimą“ (angl. *Private link*). Privatus sujungimas tai yra pačios viešosios debesijos paslaugų gamintojo įgalinta paslauga, kai tarp tenantų bendrintos paslaugos ir viešosios paslaugos gali būti saugiai pasiekiamos vidiniais viešosios debesijos gamintojo tinklais;
- Tenanto ugniasienė – tai komponentas, užtikrinantis duomenų srautų valdymą tenanto viduje;
- Maršrutų serveris – komponentas, užtikrinantis maršrutų apsikeitimą tarp aplikacijų tinklų ir platformų tinklų potinklių ir komponentų, kaip ugniasienės ir šliuzai;
- Terminalinis serveris – komponentas, leidžiantis jungtis iš tenanto tinklo į aplikacijų tinklą ir kitus serverius jų valdymui.

Aplikacijų tinklo komponentai, paslaugų komponentai, kuriomis teikiamos bendro naudojimo paslaugos, teikiamos kitiems tenantams:

- Valdymo – talpinamos valdymo sistemos, kaip ugniasienių valdymo, Operacinių sistemų atnaujinimo ir pan.;
- Stebėjimo – talpinama serverių, paslaugų ir komponentų stebėjimo infrastruktūra;
- Tapatybės nustatymo – talpinamos tapatybės nustatymo sistemos, teisių ir prieigos sistemos
- Įrašų kaupimo – talpinamos Įrašų kaupimo sistemos ir komponentai;
- Saugumo – talpinamos audito sistemos, politikų ir valdymo sistemos, kitos sistemos;
- Privataus sujungimo zona – tai komponentai, leidžiantys aplikacijai sukurti privataus sujungimo galimybę. Privatus sujungimas tai yra pačios viešosios debesijos paslaugų gamintojo įgalinta paslauga, kai bendros tarp tenantų ir viešosios paslaugos gali būti saugiai pasiekiamos vidiniais viešosios debesijos paslaugų gamintojo tinklais. Jei viešosios valdytojo paslaugos yra pasiekiamos privataus sujungimo pagalba, išsprendžiami vienodų / persidengiančių IP adresų klausimai.

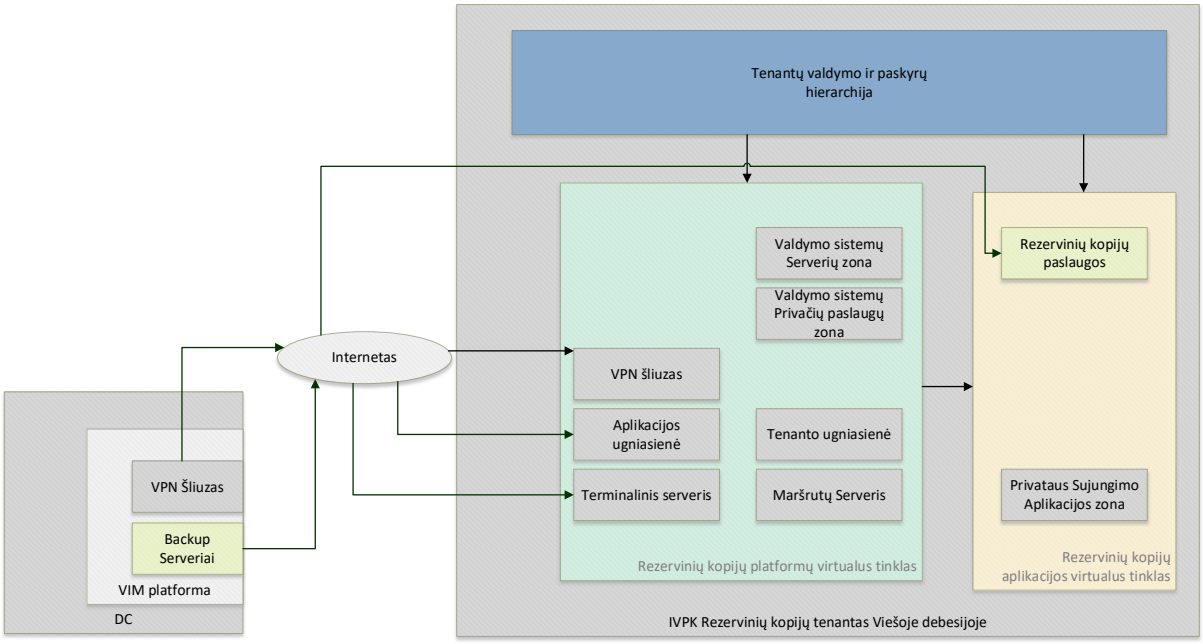


Pav. 24 Viešų debesijos paslaugų valdytojo - VSSA - tenanto architektūra

Visų viešosios debesijos tenanto architektūros komponentų reikalingumas bus sprendžiamas įgyvendinimo analizės metu.

8.1.6 Viešosios debesijos rezervinių kopijų tenanto architektūra

Rezervinių kopijų tenantą valdys Viešosios debesijos valdytojas – VSSA. Šiai tenanto architektūrai skiriami platforminiai ir aplikaciniai resursai.

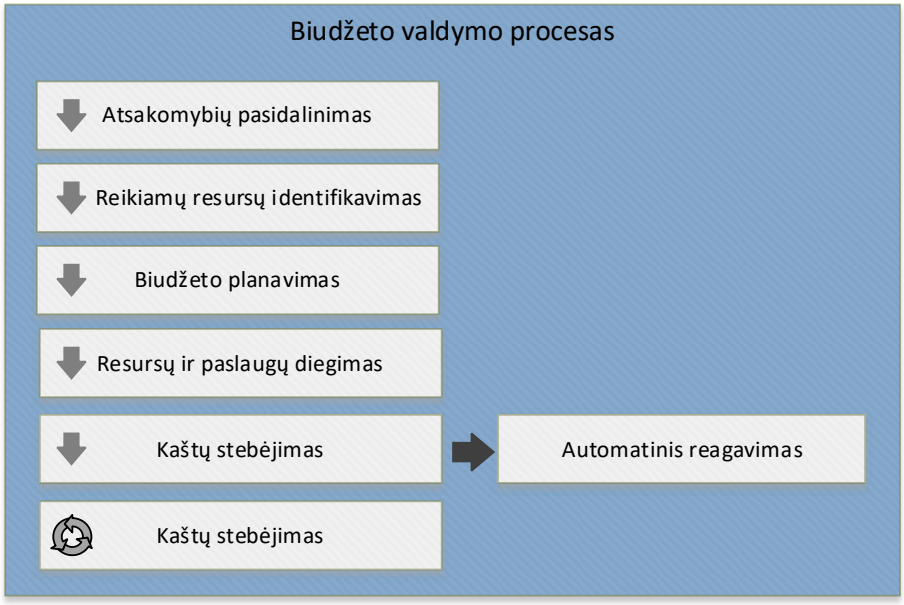


Pav. 25 Rezervinių kopijų tenanto architektūra

Platforminiai resursai sutampa su Mini tenanto platforminiais resursais, o aplikacijos resursų grupė talpina rezervinių kopijų serverius. Potinkliai priklauso Viešų paslaugų valdytojui, tinklai dedikuoti tik rezervinio kopijavimo funkcijai atlikti. VIM platforma yra pasiekiama per VPN tinklus. Rezervinių kopijų saugykla viešoje debesijoje gali būti pasiekiama ir per internetą.

9. HIBRIDINĖS DEBESIJOS BIUDŽETO VALDYMO PRINCIPAI

Rekomenduojama, jog viešosios debesijos kaštų valdymo arba valdymo politikų priemonėmis paskyroms būtų nustatytas sutartas kaštų limitas, bei įgyvendintas stebėsenos modelis stebintis sąnaudas realiuoju laiku bei siunčiantis įspėjimo pranešimus. Pranešimų siuntimas numatytas realizuoti tokiu būdu, kad pranešimai Klientui pasiekus 60% išnaudojimą būtų siunčiami kas 10 procentų nustatyto kaštų limito išnaudojimo, taip užtikrinat, kad stebimas ne tik viršijimas bet ir išnaudojimo dinamika. Papildomai gali būti sukonfigūruoti automatiniai veiksmai, kurie bus vykdomi tuo atvejui, kai limitas viršijamas ir galės sustabdyti suderintas paslaugas arba resursus.



Pav. 26 Hibridinės debesijos biudžeto valdymo procesas

Siekiant užtikrinti efektyvų biudžeto valdymą būtina sukurti procesus kuriuo metu būtų užtikrinama kad:

- Paskirti atsakingi darbuotojai iš VSSA, kurie bus atsakingi už biudžeto limitų valdymą;
- Kliento pusėje turi būti paskirti atsakingi darbuotojai, kurie bus atsakingi už efektyvų ir optimalų gauto biudžeto panaudojimą ir stebėjimą;
- Apribota galimybė, be papildomo patvirtinimo diegti nestandartinius arba didelius kaštus turinčius resursus ir paslaugas;
- Užsakant paslaugas Klientas atsakingas, kad resursai neturi būti pertekliniai ir būtų didinami tik esant realiam poreikiui;
- Svarstoma galimybė vietoje klasikinių sprendimų, naudoti viešosios debesijos *native* arba *serverless* sprendimus arba dinaminį resursų išskyrimą priklausomai nuo momentinio poreikio;
- Planuojama, kad visi resursai turės žymas, kurių pagalba galima identifikuoti resurso ir paslaugos savininką, priklausomybę aplinkai ir aplikacijai;
- Sutartos ir suderintos atsakomybės ir veiksmų planas, nustatyto limito viršijimo atvejui;

- Politikų diegimas, resursų optimizacija, veiksmų automatizavimas.

Papildomai privalo būti sukurtos ir realizuotos procedūros užtikrinančios, kad sąnaudos yra stebimos ir optimizuojamos, jų metu įvertinus kaštus turi būti atliekami šie veiksmai:

- Koreguojamas esamas kaštų limitas, jį didinat arba mažinat, kad informavimo pranešimai būtų savalaikiai ir neklaidinantys;
- Analizuoja priežastis kodėl kaštai auga;
- Analizuojamos brangiausių viešosios debesijos resursų arba paslaugų optimizavimo galimybės;
- Analizuojamos galimybės testavimo ir vystymo aplinkoms pritaikyti politikas automatu stabdančias resursų naudojimą ne darbo metu;
- Esant poreikiui resursams taikomos rezervacijos arba taupymo planai;
- Identifikuojami nenaudojami arba pertekliniai resursai ir imamasi priemonių juos panaikinti.
- Esant resursų ir biudžeto naudojimo piktnaudžiavimams Kliento resursai būtų stabdomi.

10. VIEŠOSIOS DEBESIJOS PASLAUGŲ TENANTŲ RYŠIAI IR TINKLŲ APJUNGIMAS

10.1. Viešosios debesijos tenantų susijungimo būdai

Pagrindiniai būdai kaip sujungti skirtingų organizacijų tinklus vienoje viešosios debesijos aplinkoje yra šie:

1. VPC (angl. *Virtual Private Clouds*) Peering (lt. apjungimas) viešosios debesijos tinklų apjungimo technologijų (pvz. VPC Peering, Virtual Network Peering) pagalba. Toks metodas leidžia užtikrinti tiesioginį ryšio kanalą vieno viešosios debesijos paslaugų gamintojo ribose. Pagrindiniai privalumai: saugumas, mažas tinklo vėlinimas, konfigūravimo paprastumas. Pagrindiniai trūkumai: negali būti pasikartojančių IP adresų rėžių, kiekviena VPC pora turėtų būti sujungiama atskirai, gali būti taikomi limitai sujungimų skaičiui.

2. Debesijos maršrutizatorius (pvz. AWS Transit Gateway). Kiekvienas viešosios debesijos paslaugų gamintojas turi savo debesijos maršrutizatoriaus įgyvendinimą, kuris smarkiai skiriasi tarpusavyje. Visų maršrutizatorių galimybės skirtingos, ir ypač gebėjime apsikeisti virtualių maršrutų lentelėmis (VRF) su persidengiančiais IP adresais. Norint taikyti vieningą architektūrą visiems viešosios debesijos sprendimams šis būdas gali apsunkinti įgyvendinimą. Šis susijungimo būdas gali būti naudojamas, jei išpildomos visos saugaus susijungimo sąlygos.

3. Privatus debesijos (angl. *Private Link, Private endpoint*) sujungimo būdas. Šis būdas tinkamas tuo, kad išsprendžia Debesijos maršrutizatoriaus problemą dėl maršrutų apsikeitimo, ir persidengiančių IP adresų problemą. Kiekvieno viešosios debesijos paslaugų gamintojo sprendimas kiek skiriasi ir tokie Privatūs sujungimai gali būti pasiekiami tik vieno viešosios debesijos gamintojo tinkle. Papildomai, šiam sprendimui veikti reikalingi papildomi komponentai, kaip DNS zonų konfigūravimas.

4. Virtualaus privataus tinklo (angl. *Virtual Private Network*) sujungimas (pvz. VPN IPsec). Šis sprendimas gali padidina kaštus, sumažinti tinklo greitaveiką dėl saugumo algoritmų ir naudojamas priklausomai nuo scenarijaus.

5. Yra galimybė vienam tenantui pasiekti kito tenanto išteklių per internetą. Viešinama tenanto paslauga tampa pasiekiama kitų tenantų per internetą ir iš visų viešosios debesijos paslaugų gamintojų. Priklauso nuo informacinės sistemos paskirties ir funkcionalumo.

6. Ryšio paslaugas tenantams teikia ir administruoja KVTC:

Susijungimo būdas	**Ar galimas IP adresų persidengimas tarp tenantų**	**Ar veikia iš kitų viešosios debesijos paslaugų gamintojų tinklų**	**Ar ryšio kanalas papildomai šifruojamas***	**Ar duomenys siunčiami Viešosios debesijos paslaugų gamintojo vidiniais tinklais**	**Ar duomenys siunčiami per internetą**
VPC Peering	Ne	Ne	Ne	Taip	Ne
Debesijos maršrutizatorius	Ne	Priklauso nuo viešosios debesijos paslaugų gamintojo	Ne	Taip	Ne

Privatūs sujungimai	Taip	Ne	Ne	Taip	Ne
Virtualūs privatūs tinklai	Taip	Taip	Taip	Taip	Taip
Paslauga viešinama per internetą	Taip	Taip	Ne	Ne	Taip

Lentelė Nr. 6 Galimi tenantų sujungimo būdai viešojoje debesijoje

PASTABA:

* Ryšio kanalas gali būti papildomai šifruojamas, kai duomenys jau šifruoti tinklo protokolo pagalba (pvz., TLS).

** KVTC, teikdama interneto ryšio ar kitas susijusias paslaugas, vadovausis veiklą reglamentuojančiais Lietuvos Respublikos teisės aktais. KVTC Saugiuoju tinklu teikiamų interneto ryšio paslaugų parametrai bei saugos sprendimai patvirtinti Lietuvos Respublikos krašto apsaugos ministro 2019 m. liepos 2 d. įsakymu Nr. V-583 „Dėl saugiojo valstybinio duomenų perdavimo tinklo veiklą užtikrinančių dokumentų patvirtinimo“ (aktuali redakcija, V-583 Dėl Saugiojo valstybinio duomenų perdavimo tinklo veiklą užtikrinančių dokumentų patvirtinimo (lrs.lt)).

Pagrindiniai būdai kaip sujungti skirtingų organizacijų tinklus tarp skirtingų viešosios debesijos paslaugų gamintojų arba sujungti vidinį tinklą su pasirinktu viešosios debesijos:

1. Tiesioginis tinklų sujungimas (angl. *Direct Connect*), kuris užtikrina aukštą tinklo greitaveiką (angl. *High Bandwidth and Low Latency*), saugumą ir patikimumą. .

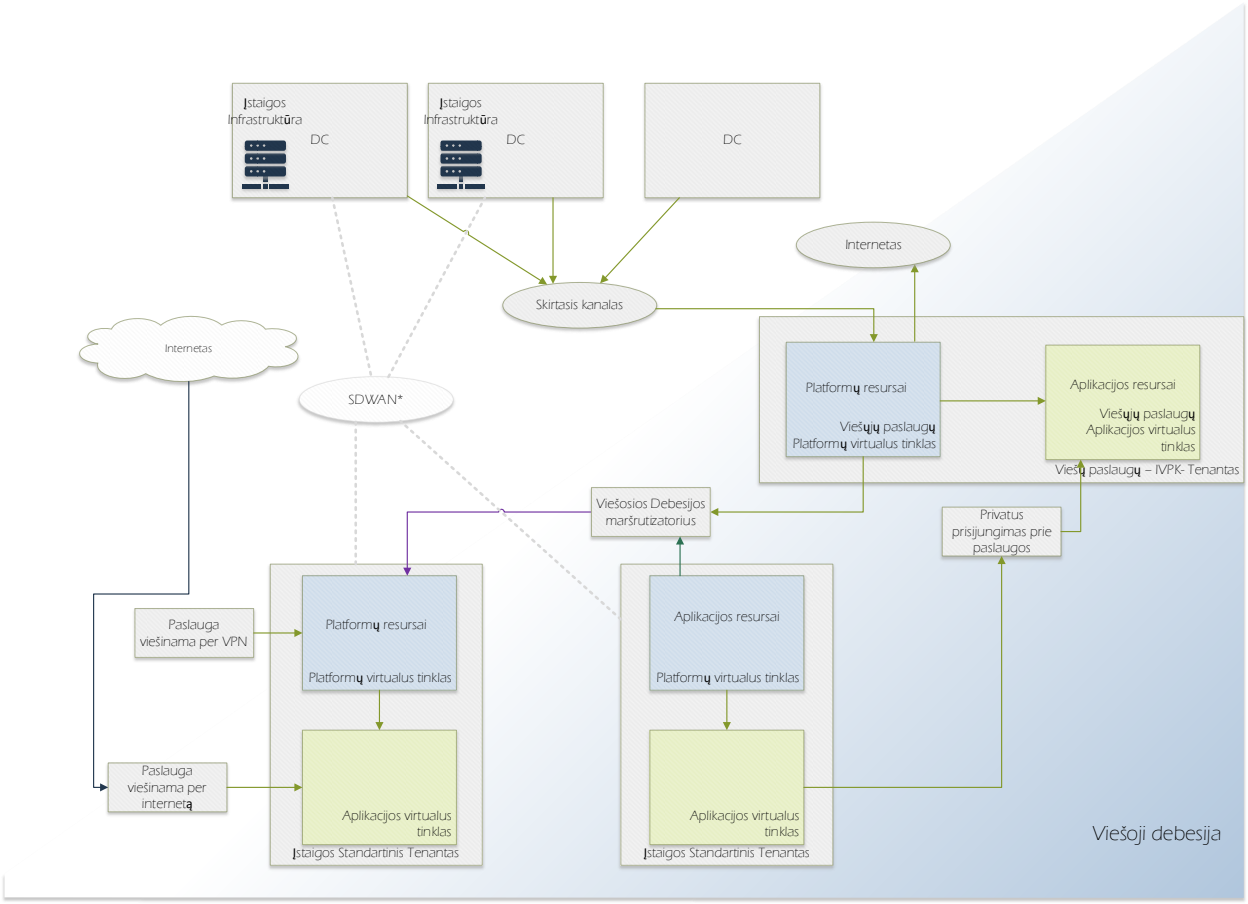
2. VPN (angl. *Virtual Private Network*) virtualaus privataus tinklo sujungimas. Nereikalauja fizinės infrastruktūros, lanksčiai konfigūruojamas. Priklausomai nuo pasirinktų saugumo užtikrinimo būdų gali turėti žemesnę greitaveiką.

Tinklų sujungimo sąsajos su aplikacijomis:

1. Informacinės sistemos kuriamos viešojoje debesijoje turėtų bendrauti tarpusavyje https protokolu API lygyje nenaudojant aukščiau paminėtų sujungimo būdų.

2. Duomenų apsikeitimui rekomenduojama naudoti kitas viešosios debesijos priemones (angl. *S3 bucket sharing*).

Kaip papildomą sujungimo priemonę galima naudoti SDWAN komponentus prioritetą teikiant aukščiau išvardintiems sujungimo būdams.



Pav. 27 Tenantų tinklų sujungimo pavyzdys

10.2. Viešųjų paslaugų valdytojo – VSSA – tenanto ryšiai

Debesijos tenantų tinklai turi būti segmentuoti ir atskirti vienas nuo kito. Tam KVTC tinkle ir Valstybės debesijos platformoje naudojami VRF – virtualios maršrutų lentelės, užtikrinančios segmentaciją. Šis sprendimas leidžia tenantų potinklių IP adresacijai persidengti – kadangi tinklai visiškai segmentuoti vienas nuo kito, vienas tinklas nedaro jokios įtakos kitam tinklui.

Viešosios debesijos paslaugų gamintojų tinkluose tenantų atskyrimas pirmiausiai numatytas virtualaus tinklo pagalba. VRF nepalaikomi. Dėl to viešosios debesijos paslaugų gamintojai rekomenduoja nedubliuoti tinklų adresacijos, kitaip atsiranda problema transportuoti tokių tinklų maršrutus.

Prisijungimas iš įstaigos tenanto į Viešų paslaugų VSSA tenantą gali būti vykdomas dviem būdais: – per Debesijos maršrutizatorių – apsikeičiant maršrutais, arba pasinaudojant Debesijos vidine paslauga – per privačius sujungimus. Privatus sujungimas – kai sujungimas tarp teikiamų viešosios debesijos paslaugų vykdomas viešosios debesijos ribose ir į viešąjį internetą nėra išleidžiamas. Pastaroji paslauga naudinga tuo, kad viešas resursas gali būti pasiekiamas iš tenantų, kurių IP adresacija vienoda. Šis prisijungimo prie VSSA tenanto būdas yra rekomenduojamas.

Ryšio kokybei, vėlinimo ir paketų sklaidos sumažinimui su kiekviena iš naudojamų Viešųjų debesijų gali būti diegiamas skirtosios linijos ryšio kanalas. Skirtuoju kanalu duomenys mažiau įtakojami paketų sklaidos ir jų vėlinimas mažiausias. Skirtosios linijos ryšio kanalas terminuojamas viešosios debesijos paslaugų gamintojo tenante.

Viešų paslaugų valdytojo – VSSA – maršrutų apsikeitimui tarp viešosios ir VHD panaudojamas debesijos maršrutizatoriaus komponentas. Kaip minėta aukščiau, kiekvienas viešosios debesijos paslaugų gamintojas turi savo debesijos maršrutizatoriaus konfigūraciją.

Skirtoji linija naudinga, kai yra reikalavimai mažam duomenų siuntimo vėlinimui, arba mažai paketų sklaidai, arba tais atvejais, kai papildomas šifravimas ir tuneliavimas įtakoja tenanto ryšį. Kitais atvejais, galima užtikrintini ryšį per Internetą panaudojant tunelius.

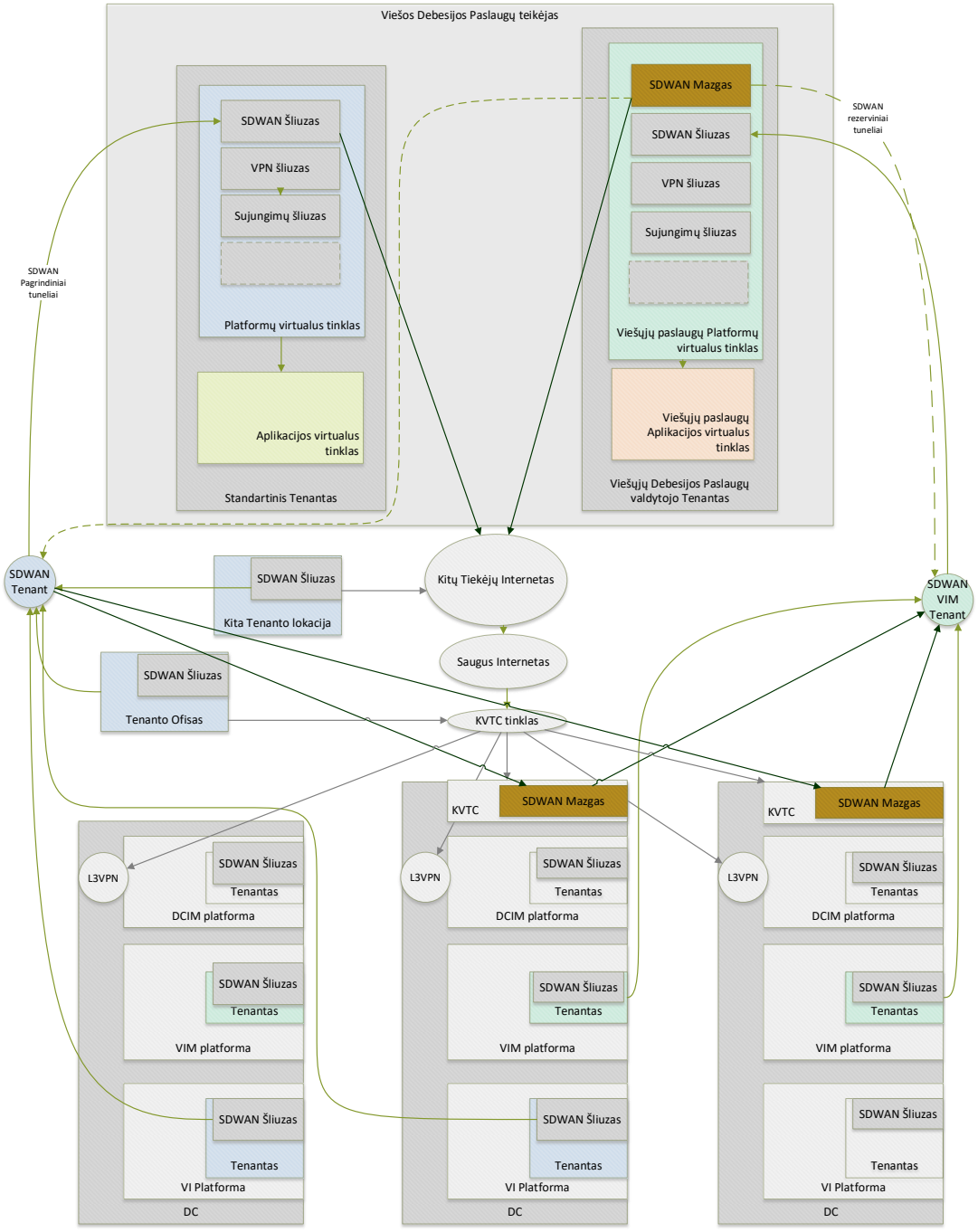
10.3 Papildoma apjungimo galimybė SDWAN tinklu

Ši technologija leistų užtikrinti ryšį iki viešosios debesijos paslaugų gamintojo SDWAN tinklu. Apjungimo galimybė gali būti naudojama didžiausioms organizacijoms, kurie jau naudoja šią technologiją savo vidiniuose tinkluose. Saugiais šifruotais ryšio būtų užtikrinama prieiga tarp VHD Klientų biurų, VHD Klientų resursų duomenų centre ir viešosios debesijos paslaugų gamintojo.

SDWAN šifruotus tunelius sukurtų SDWAN šliuzai, kurie būtų įdiegti tik didelių Klientų, naudojančių SDWAN technologiją savo vidiniuose tinkluose, taškuose, kurie reikalauja prieigos prie viešosios debesijos paslaugų gamintojo.

SDWAN tinklo veikimą užtikrina SDWAN mazgai. Vienas mazgas būtų įdiegtas VHD prieigose ir prižiūrimas VHD Viešų paslaugų valdytojo – VSSA kitas rezervinis SDWAN mazgas būtų diegiamas viešosios debesijos paslaugų gamintojo prieigose – viešosios debesijos paslaugų gamintojo viešųjų paslaugų valdytojo tenante ir prižiūrimas viešųjų debesijos paslaugų valdytojo – VSSA. Ryšys, reikalingas SDWAN tinklo veikimui, būtų teikiamas ir prižiūrimas KVTC.

SDWAN technologija būtų planuojama naudoti tik didžiausiems Klientams.

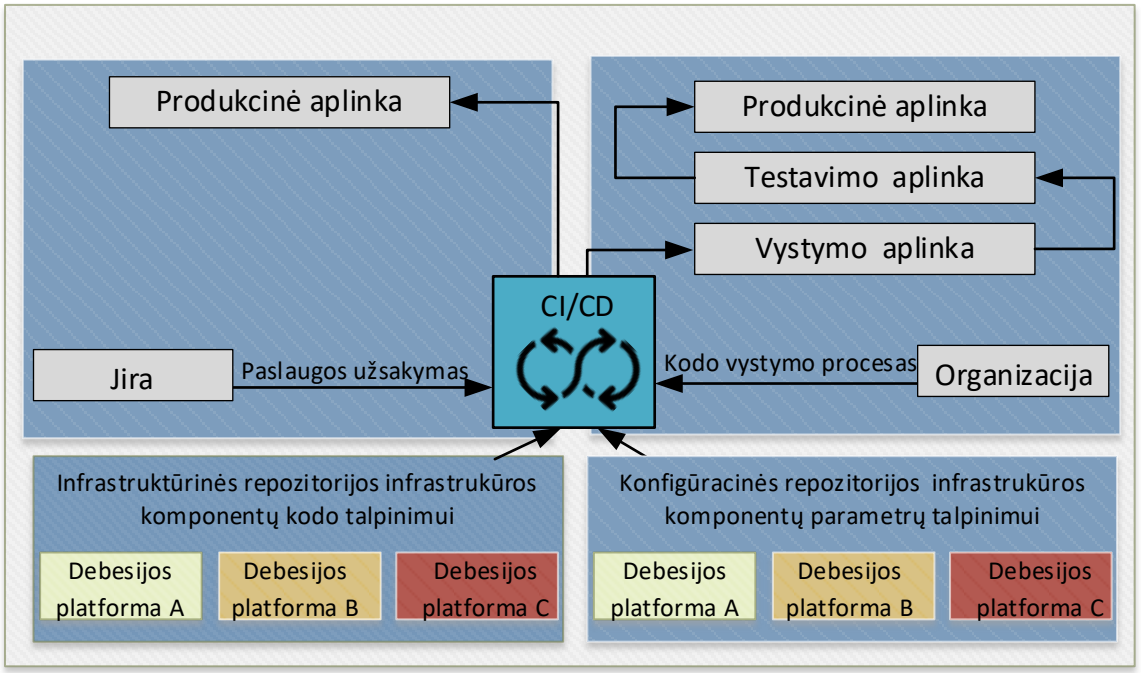


Pav. 28 Viešosios debesijos SDWAN sujungimo pavyzdys. Punktyrinėmis linijomis parodyti ryšiai iki rezervinių SDWAN mazgų

11. HIBRIDINĖS DEBESIJOS AUTOMATIZACIJOS ĮRANKIAI

11.1. Paslaugų užsakymo sistema

Siūloma viešosios paslaugos debesijos užsakymus, gautus iš Klientų, vykdyti automatizuotu keliu Klientui suformavus ir užpildžius atitinkamai paruoštą užsakymo formą. Užpildytos ir patvirtintos formos duomenys atkeliauja tiesiai iš paslaugų užsakymo sistemos (JIRA) į GIT sistemą (būtų išnaudojamas GIT REST API). GIT (kodo valdymo sistema) ir GIT Workflow (nepertraukiamo diegimo sistema CI/CD) gavus Kliento duomenis pagal juos suformuoja užsakymą atitinkančią **konfigūracinio** kodo saugykla (angl. *Repository*).



Pav. 29 Procesų automatizacija

Konfigūracinio kodo saugyklai susikūrus, automatiškai pasileidžia nepertraukiamo diegimo procesas, kuris sukurs bei sukonfigūruos Kliento užsakytus Viešosios debesijos paslaugos resursus.

11.2. Automatizacijos įrankių panaudojimo privalumai

Atsižvelgiant į tai, kad viešosios debesijos paslaugų gamintojai (AWS, Azure, Google Cloud ir kt.) nuolatos naujina, gerina ir vysto savo paslaugų pasiūlą rinkai – o rinka iš savo pusės proaktyviai reaguoja į šiuos pakeitimus dėl atnešamų naudų ir rinkos poreikius tenkinančių paslaugų už nuolatos per optimizacijas mažėjančią kainodarą, siūloma:

- Išnaudoti viešosios debesijos paslaugų gamintojo suteikiamas infrastruktūros valdymo galimybes, kurias suteikia Infrastruktūros kaip kodas (angl. *Infrastructure as a Code*, toliau – IAC) technologijos. Infrastruktūros kodą planuojama aprašyti rinkoje paplitusiomis *Terraform (alternatyva OpenTofu)* technologijomis kartu panaudojant viešosios debesijos IAAS kodui aprašyti skirtas priemones: pvz. *AWS CloudFormation, Azure Bicep, Google Deployment Manager*.

```
  network_rules {
    default_action             = "Deny"
    ip_rules                   = ["78.61.196.174", "78.63.76.116", "88.119.94.17", "77.90.72.
    virtual_network_subnet_ids = [azurerm_subnet.cluster.id, azurerm_subnet.vm.id]
  }
}
```

Pav. 30 Terraform kodo pavyzdys. Tinklo IP adresai, kuriems draudžiamas prisijungimas prie tinklo

- Pageidaujant daugiau lankstumo, platesnių galimybių ir laisvės valdant Infrastruktūrą – *Terraform* kodas galėtų būti toliau naudojamas kartu su *Terragrunt*. Plečiantis *Terraform* repozitorijai, *Terragrunt* įvedimas ženkliai sutaupo *Terraform* kodo valdymo, vystymo ir priežiūros kaštus, įvesdamas daugiau lankstumo.
- Sujungiant daugiau viešosios debesijos paslaugų gamintojų (pvz. AWS, Azure, Google Cloud), kodo valdymui ir optimizavimui išnaudoti *Terramate* produktą.
- Išnaudoti Git kodo versijavimo sistemų suteikiamas galimybes kodui, bei „iš kodo“ sukompiliuotai (angl. *compiled from code*) infrastruktūrai, saugiai bei efektyviai valdyti, vystyti ir prižiūrėti kodo ir jo konfigūracijos repozitorijos pakeitimus viso kodo gyvavimo ciklo (angl. *Release Lifecycle*) metu. Šios galimybės patenkina sekančius poreikius:
    - kodo versijavimas;
    - kodo versijų kontrolė;
    - kodo pakeitimų testavimas ir validavimas prieš diegimą;
    - kodo patvirtinimas (*approval*) bei sujungimas (*merge*) visų suinteresuotų šalių per *Pull Request*'us;
    - kodo istorija ir auditas;
    - kodo atskyrimas git'o atšakomis (branching).
    - efektyvų komandos veikimą, kuomet prižiūrimą infrastruktūrą per kodą valdo ne vienas žmogus – o žmonių komanda.

```
kvm985@KVM985XM1 MINGW64 ~/OneDrive - Telia Company/Documents/git/lt-sap-terraform-multienv (main)
$ git branch -a
* main
  qa
  qa-terraform-bogus-update
  remotes/origin/HEAD -> origin/main
  remotes/origin/dev
  remotes/origin/edmcck-test
  remotes/origin/main
  remotes/origin/prod
  remotes/origin/qa
```

Pav. 31 Git atšakų pavyzdys

- IAC pritaikymą vykdyti moderniu automatizuotu principu, kuris IT industrijoje yra vadinamas „Nepertraukiamu Tiekimu“ (angl. *Continuous Delivery*). Continuous Delivery (CD) koncepcija remiasi mokslu apie *tiekimo grandines*. Iš Nepertraukiamo tiekimo (CD) įrankių ir technologijų yra siūloma rinktis Git technologijas.

11.3. Kodo valdymas ir būtini kodo repozitorijų tipai

Rekomenduojama, jog kodo valdymui būtų naudojami tokie repozitorijų tipai (neapsiribojant tik jomis) kaip: infrastruktūros, konfigūracijų, Klientų aplikacijų.

Infrastruktūros kodo repozitorijos aprašo bendrus resursus pagal suderintą architektūrą.

- Infrastruktūros kodo repozitorijos, kuriose laikomas bei tobulinamas infrastruktūrinis kodas. Infrastruktūrinis kodas atitinkamai būtų paskirstytas pagal didžiausius viešosios debesijos paslaugų gamintojus:
    - AWS;
    - Azure;
    - Google;
    - Kt.
- Kiekvienam viešosios debesijos paslaugų gamintojui planuojama naudoti atskirą infrastruktūros repozitorija;
- IaC Terraform kalbos pagalba būtų aprašyti tokie servisai:
    - Loginiai resursai (virtualios mašinos, duomenų laikmenos, virtualūs tinklai, ugniasienės ir t.t.) pagal suderintą ir „landing zone“ principus;
    - Standartiniai saugumo ir valdymo politikų rinkiniai;
    - Autentikavimo ir autorizacijos mechanizmai;
    - Resursų stebėsena;
    - Biudžetavimo stebėsena;
    - Auditavimui ir įrašų failams skirti resursai.
- Infrastruktūros kodo repozitorija turės savo nepertraukiamos integracijos/nepertraukiamo tiekimo grandinę (angl. *CI/CD*) tam, kad repozitorijos pakeitimai galėtų būti testuojami bei diegiami automatizuotu būdu.
- Pilnai ištestavus bei patikrinus naują infrastruktūros versiją, ją bus galima diegti į Kliento aplinką.

IaC kodo repozitorijos – yra lygiagrečių kodo šakų (angl. *multibranch*) repozitorijos, kuriose gali būti saugoma:

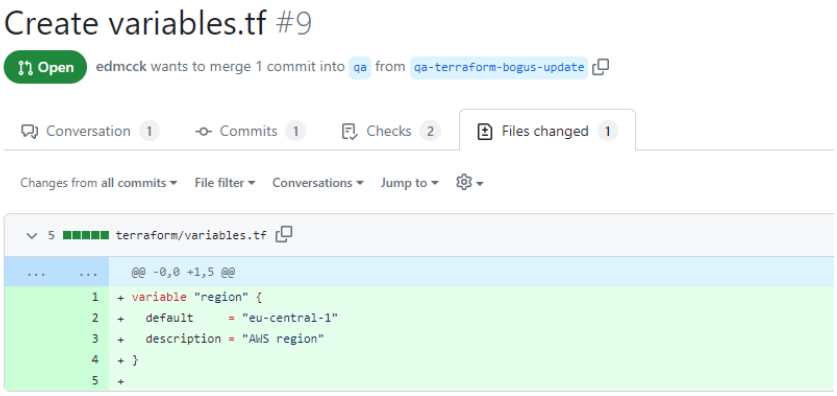
- Konfigūraciniai failai, kuriuose aprašyti naudojamų resursų tipai (pvz., virtualių mašinų CPU, RAM dydžiai) ir t.t.;
- Tinklų IP adresaciją;
- Papildomos saugumo ir valdymo politikos;
- Ugniasienių praleidimai;
- Svarbūs Klientui unikalūs duomenis: Kliento pavadinimas, atstovo vardas ir pavardė ir t.t.
- Stebėsenos konfigūracijos (threshold‘ų nustatymai);
- Biudžeto stebėsenos konfigūracija.

Galimos IaC kodo repozitorijos šakos:

- **sandbox** – testams, bandymams skirti resursai;
- **dev** – development aplinkos resursai;
- **prod** – produkcinių aplinkų resursai;
- **main** – management aplinkos resursai;
- **conn** – sujungimų (connectivity, vnet, vpc peering) resursai.

Įvertinus Kliento pageidavimus aplinkų gali būti ir daugiau: integration (sit arba int), user acceptance testing (uat).

Pagal Kliento poreikius sandbox, development aplinkų infrastruktūrinių resursų valdymui galima suteikti daugiau teisių. Pavyzdžiui, suteikti prieigas bei leisti repozitorijų pakeitimus, kuriuos per Pull Request patvirtins paskyros administratoriai.



Pav. 32 Pakeitimų įkėlimas bei patvirtinimo procesas per Pull Request'ą

11.4. IaC Kodo skirtumai skirtingose aplinkose

Kūrimo (angl. *Development*) aplinkose gali būti priimtina, kad aprašytas kodas skiriasi nuo produkcinės (angl. *roduction*) aplinkos programinio kodo. Skirtumai tarp kodo repozitorijų Klientų paskyrose turėtų būti reguliariai stebimi bei šalinami. IaC kodo skirtumų valdymui turėtų būti taikomas konfigūracijos poslinkio (angl. *Configuration drift*) principas, kuris nusako, kad laikui bėgant, konfigūracija, kurią aprašėte kode, gali skirtis nuo konfigūracijos veikiančioje sistemoje. CI/CD metodika padeda suvaldyti šiuos kodo repozitorijų skirtumus.