

Uzlabojumi “E-veselība”

Projektam piesaistītā ekspertu grupa



Eksperti

Piesaistītie eksperti:

- Uģis Bērziņš, Santa Monica Networks valdes priekšsēdētājs
- Roman Yashin, Santa Monica Networks experts
- Uldis Miķelsons, Analytica experts
- Pēteris Erbs, Nacionālais veselības dienests

Prezentācijas struktūra

**INFRASTRUKTŪRA
UN TĪKLI**

**APKALPOŠANA UN
PĀRVALDĪBA**

**PROGRAMMATŪRA
UN TĀS
KONFIGURĀCIJA**

**DROŠĪBAS UN
PAKALPOJUMU
PIEEJAMĪBAS
ELEMENTI**

Statuss iesaistoties projektā

Statuss iesaistoties projektā

Šajā sadaļā aplūkojam situāciju, kādu to konstatējām, iepazīstoties ar sistēmu

- Ekspertu komanda uzsāka darbu 2018.05.03;
- Cilvēki, kuri nebija iesaistīti projekta realizācijā - svaigs skats no malas;
- Kopējās sistēmas ekspluatācijas problēmas;
- Kompetences ietvaros uzaicinājums izvērtēt infrastruktūras darbību, tās ietekmi uz sistēmas pieejamību un veiktspēju;
- Izvērtās no tehniskas ekspertīzes projekta par vairākdimensionālu projektu, piesaistot kolēģus arī citās zināšanu sfērās;
- SMN atbildības sfēra - infrastruktūra un tīkli.

Infrastruktūra un tīkli

- Tīkli un infrastruktūra ir papildināta laika gaitā un tās arhitektūras plānošanā ir ieguldīts būtiski mazāk laika un resursu kā programmatūrā;
- Nav homogēns risinājums;
- Nav ņemts vērā apjoma pieaugums, un tehnoloģisko risinājumu attīstības faktors;
- Veidots vēsturiski dažādās organizācijās (no 2011.gada NVD) un dažādos laika posmos;
- Dažādu virtualizācijas, operētājsistēmu, datubāžu, u.c risinājumu izmantošanas izraisītās sekas.

Infrastruktūra un tīkli - DC tīkls

- Lielākā daļa infrastruktūras elementu iegādāta 2011. un 2015.gadā;
- Tīklam nav bijusi veidota atbilstoša arhitektūra, lai nodrošinātu Datu Centru līmeņa augstu pieejamību;
- Nav izvērtēta sasaiste starp dažādiem infrastruktūras līmeņiem - “labākais” katrā līmenī ne vienmēr ir labākais kopumā;
- Tā vietā ir trīs dažādu paaudžu komutatori, kuru vienīgais kopīgais izmantojamais protokols augstas pieejamības nodrošināšanai ir Spanning Tree Protocol;
 - STP protokola topoloģijas izmaiņas nozīmē to, ka ir iespēja portam pārtraukt raidīšanu uz 30 sekundēm, kas nav pieņemami izmantotajam nākamā līmeņa DC augstas pieejamības klāsteru risinājumam.

Infrastruktūra un tīkli - Tīkla Drošības sistēmas

- Drošības sistēmas darbojas uz viena pāra drošības ierīcēm, kuras nodrošina “visu”:
 - Iekšējo apakštīklu savstarpējo maršrutēšanu;
 - Iekšējo drošības zonējumu;
 - Ārējo aizsardzību ienākošajiem savienojumiem;
 - Ārējo aizsardzību izejošajiem savienojumiem;
- Šīs ierīces ir noslogotas vairāk nekā tām pienāktos;
- Kaut arī tehniski iekārtas ir “ļoti labas”, drošības risinājums nav paredzēts rezervētu Datu Centru izveidei;
- Tām ir sava vieta drošības arhitektūrā, bet tā būtu būtiski jāpapildina.

Infrastruktūra un tīkli - Serveru infrastruktūra

- Serveru infrastruktūra ir vairākās paaudzēs veidota;
- Ieviešanā ir izmantoti daudzi risinājumi, kas paši par sevi ir labi, bet kopumā no elastības viedokļa ir suboptimāli;
- Piemēram, virtualizācijā izmatotie virtuālo mašīnu diski ir izvietoti uz viena LUN:
 - Ērti, kad ir viena sistēma, optimāli izmanto diska vietu, neprasa papildus administrēšanas resursus;
 - Tomēr, neelestīgi, ja nepieciešams ko mainīt, pārnest daļu no sistēmām vai atsevišķas datu bāzes uz citu infrastruktūras daļu;
 - Kopīgi resursi: nav iespējas vai ļoti apgrūtināti detalizēti redzēt, ko katrs atsevišķs sistēmas elements patērē

Infrastruktūra un tīkli

- Kopumā infrastruktūra ir veidota, lai pārciestu viena elementa bojājumu;
- Tomēr, sistēma nav toleranta vienlaicīgu problēmu gadījumā;
- Sistēma nav paredzēta rezervētu Datu Centru ekspluatācijai;
- Noslodzes mērīšanas sistēmas pašas rada slodzi;
- No 2018.gada viedokļa sistēmas arhitektūra nenodrošina 24x7 ekspluatācijas režīmu ar spēju apkalpot lietotājus:
 - plānotās dīkstāves laikā - sistēmas modernizācija, apkalpošana,
 - būtiskos neplānotās dīkstāves gadījumos - avārijas.

Apkalpošana

- Programmatūrai ir beidzies garantijas uzturēšanas līgums;
- Uzsākot darbu, identificēts, ka nav cilvēkresursu, kas būtu piesaistīti tikai E-veselība projektam (NVD IT departaments atbild par daudz dažādām sistēmām un lietotāju atbalstu);
- NVD pusē bija daudz neaizpildītu lomu (vakanču), liela kadru mainība;
- Nav precīzu apkalpošanas procedūru (izmaiņu vadības, apziņošanas, incidentu apstrādes ir daļēji):
 - Incidentu gadījumā trūkst resursu veikt cēloņu analīzi
 - Ierobežotas iespējas veikt uzlabojumus

Drošība / pakalpojuma pieejamība

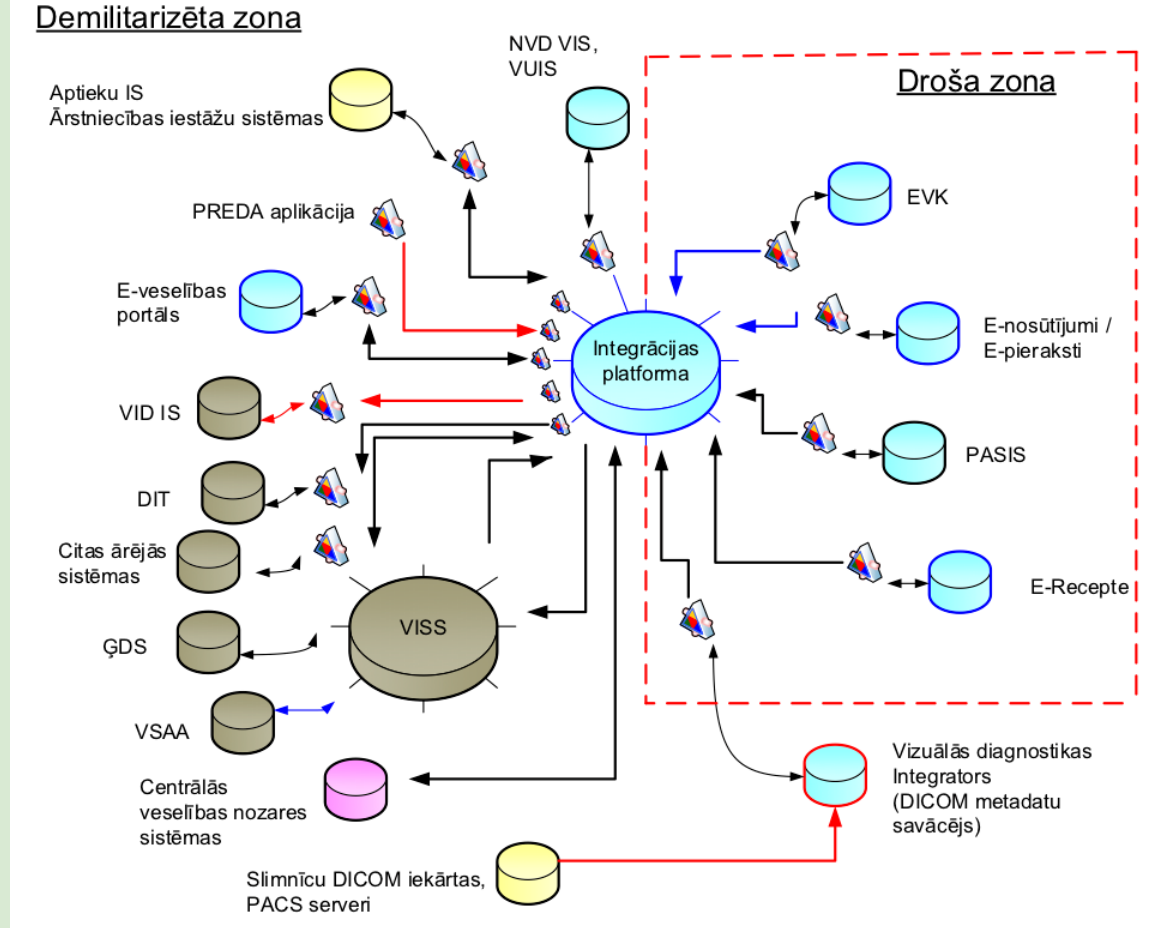
- Identificētas nepieciešamība uzlabot drošības pārvaldību
- Nepieciešama auditācijas kārtības uzlabojumi (šobrīd auditācijas pierakstu skaits un apjoms pārsniedz sistēmas datus)
- Pakalpojuma pieejamības riski
 - Izmantojamo resursu novecošanas riski
 - Resursu nodalījuma riski
 - Tehnisko resursu nepietiekamības riski
- Darbinieku pieejamība

Programmatūra un konfigurācija

- Pārejas periods programmatūras uzturēšanā no sākotnējiem izstrādātājiem:
 - Nepieciešami papildus resursi NVD pusē problēmu detalizētai identifikācijai;
 - Realizētā konfigurācija pret piegādāto dokumentāciju nepietiekami dokumentēta;
- Testa vidē nav iespējams veikt uz produkcijas veikspēju attiecināmus testus;
- Ļoti ilgs piegādes process (testēšana manuāla, nepilnīgi dokumentēti scenāriji):
 - Izmaiņas vienā sadaļā var iespaidot funkcionalitāti citās;
- Produkcijā ir komponentes, kas ir *EoL* un *EoS* (bija aktuālas piegādes brīdī).

Arhitektūra

- Ir arhitektūras elementi, kuru dīkstāves aptur visas sistēmas darbību;
- Ir atkarības no 3.pusēm (piemēri: VRAA koplietošanas komponentes, ārējie reģistri: VSAA, PMLP IeR)
- Visas darbības realizētas tiešsaistē, t.sk. Integrētās sistēmas



Būtiskākie novērojumi - KOPSAVILKUMS

- Resursu trūkums sākotnēji (faktiski NVD pusē nebija “TIKAI EVeselībai” nozīmētas komandas):
 - Darba organizācija 5x8 režīmā, kamēr sistēmas darbība 7x24;
 - Liels skaits IKT vakanču, kas aizpildītas tikai pēdējo 2 mēnešu laikā.
- Aparatūras vecums, atbalsts un kapacitāte;
- Veiktspējas prasību sistēmai definējums nav izvirzījis darbībai būtisku parametru pārbaudi;
- Sistēmas uzlabojumu procesa “lēnums”

Kas ir izdarīts un
kas ir sasniegts
kopš 2018.05.03. ?

Esošās prioritātes uzsākot projektu

1. Stabilitāte
2. Darbības caurspīdīgums un monitorings
 - a. Uzsākusies pāreja no kopējām sistēmas problēmām uz individuālu incidentu izpēti (no 2018.05.23)
3. Veiktspēja
 - a. Uzsākta vairāklīmeņu monitoringa pilnveidošana, kas ļauj sniegt detalizētu informāciju par pieprasījumu izpildes laikiem
4. Sadarbība ar 3.pusēm
 - a. Tiek apzinātas būtiskākās problēmsituācijas un uzlabota integrācijas risinājumu darbību analīze/monitorings

Infrastruktūra un tīkli

Kas ir izdarīts

- Veikta infrastruktūras analīze ar mērķi apzināt veiktspējas un pieejamības jautājumus;
- Identificētas būtiskākās lietas, kas darbojas suboptimāli;
- Apzinātas lietas, kas darbojas optimāli;
- Veiktas konsultācijas ar infrastruktūras piegādātāju un ražotāju speciālistiem.

Infrastruktūra un tīkli

Kas tiek darīts:

- Tiek sakārtotas lietas, kas neprasa papildus ieguldījumus;
- Tiek iegādātas minimāli nepieciešamās iekārtas, lai ar minimāliem ieguldījumiem panāktu esošo iekārtu maksimālu atdevi veiktspējas un pieejamības ziņā;
- Tiek iesaistīti “Subject Matter Experts” sarežģītāku jautājumu risināšanā.

Infrastruktūra un tīkli

- Šobrīd ir 2018.gads.
- 10 gadus atpakaļ lietotājiem bija citas prasības.
- Arī daudzas lietas IT pasaulē tolaik darīja citādi:
 - Ir mainījušās Datu Centru tehnoloģijas, cita ātrdarbība, citi augstas pieejamības risinājumi.
 - Ir parādījušies jauni drošības riski un veidi kā tos mazināt.
 - Ir mainījies veids kā ekspluatēt 24x7 sistēmas, izpratne par plānotajām dīkstāvēm “always on-line” laikmetā.
- “Divu DC” princips ir kļuvis par nepieciešamību.

Infrastruktūra un tīkli - DC tīkls (A)

- DC tīkls ir savākts no trīs dažādu tehnoloģiju komutatoriem, saslēgtiem divos apļos ar šķērssavienojumiem, miksēti 1G un 10G savienojumi aplī. Iekārtas iegādātas 2011. un 2015.gadā asmeņserveru sastāvā, lai nodrošinātu minimālu tīkla atbalstu.
- Acīmredzami, tīkla arhitektūra nav plānota pirms iegādes, un savienojumi ir veidoti, izmantojot pieejamos portus tām iekārtām, kas ir nopirktas, tā, lai veidotos vismaz kaut kāda tīkla rezervācija.

Infrastrukturā un tīkli - DC tīkls (A)

- Tīkla rezervācijas protokols ir Spanning Tree Protocol. Tas nav savietojams ar MS Cluster mehānismiem - STP pārejas procesi var bloķēt portus uz 30 sekundēm, kuru laikā Cluster mehānismi detektē tīkla nepieejamību un izraisa pārejas procesus uz Cluster dalībniekiem, kas rada lielas dīkstāves, izraisot līdz pat vairāku stundu garu pilnīgas pārlādes procesu.
- Asmeņserveru savienojumos disparitāte 10G servera interfeisiem ar 1G asmeņietvaru komutatoru interfeisiem.

Infrastruktūra un tīkli - DC tīkls (A)

Kas tiek darīts:

- Tiek modernizēti pāris ar asmeņserveru komutatoriem:
 - Iegādes procesam jānoslēdzas šodien;
- Pēc piegādes - notiks pāreja uz “2015.gada līmeni”:
 - Izslēgts STP;
 - Izvedoti jauni tīkla rezervācijas mehānismi, salāgoti ar citiem DC līmeņiem;
 - Pirmais solis ceļā uz “Divu DC” arhitektūru.

Infrastruktūra un tīkli - DC tīkls (B)

Kas tiek darīts:

- Tiek veidots ārjoslas pārvaldības tīkls, lai nodrošinātu piekļuvi pie visu iekārtu, tai skaitā tīkla iekārtu, pārvaldības portiem avārijas situācijās.
- Tas būtiski uzlabo reakcijas laiku, ietaupa vismaz stundu, lai inženieriem nav jādodas uz datu centru, bet nekavējoši var uzsākt darbus.
- Šādi ārjoslas pārvaldības tīkli ir jāveido visos datu centros, kuri atrodas attālināti no inženieru atrašanās

Infrastruktūra un tīkli - DC tīkls (C)

- Tīkla maršrutēšana tiek veikta uz tīkla drošības iekārtām.
- Izmantotā serveru IP adresācija ir suboptimāla, jo nenodrošina iespēju serverus nodalīt atsevišķos IP apakštīklos, kas ir pamatu pamats augstas pieejamības nodrošināšanai;
- Esošā tīkla arhitektūra nav paplašināma uz “Diviem DC” bez būtiskām izmaiņām un papildinājumiem.

Kas tiek darīts: ir nosprausti tīkla arhitektūras pamatprincipi, izveidots tīkla dizaina variants pārejai uz “Divu DC” risinājumu.

Tīkla arhitektūra vēl ir jāpielāgo programmatūras arhitektūrai.

Infrastruktūra un tīkli - Serveri

- Analizējot tīkla veiktspēju tika atklāti ārkārtīgi lieli pakešu zudumi hipervizoros.

Kas tiek darīts: Veikta sākonējā analīze, iesaistīts MS atbalsta dienests.

Rezultātā ir secināts, ka visā sistēmā ir izslēgta IPv6 protokola darbība, kas ir ražotāja neatbalstīts risinājums MS Cluster vidē. Ieslēgt IPv6 atpakaļ pilnīgi visos serveros, tai skaitā virtuālajos, ir potenciāli bīstams darbs, kurš ir rūpīgi jāplāno un jāveic ārpus pamata darba laika, kā arī jāērēķinās ar iespējamu sistēmas nepieejamību daudzu stundu garumā.

Infrastruktūra un tīkli - Serveri

- Analizējot serveru veiktspēju tika konstatēta pazemināta veiktspēja, saistīta ar procesoru darbības režīmiem, analizēts procesoru resursu un atmiņas resursu sadalījums NUMA arhitektūras griezumā serveros ar 4 procesoru ligzdām, īpaši izpaužas specifiskai Intel procesoru paaudzei;

Kas tiek darīts:

- Veiktas izmaiņas, kas dod būtiskāko ieguldījumu veiktspējas palielināšanā;
- Tiek turpināts darbs pie detalizētākas analīzes virtuālo serveru līmenī, specifiski uz tiem darbojošos aplikāciju griezumā.

Infrastruktūra un tīkli - Serveri

- Eošā serveru infrastruktūra ir būtiski noslogota, nav resursu manevriem;
- Pārvaldības rīki, kas mēra sistēmas veiktspēju ir izvietoti pašā sistēmā un ietekmē mērījumus.

Kas tiek darīts:

- Testa nolūkiem un mērījumu veikšanai rasta iespēja uz laiku nodrošināt nepieciešamos resursus;
- Piemēram, mērījumu veikšanai izvietot atsevišķas sistēmas komponentes, lai noskaidrotu to reālo resursu patēriņu un veiktspēju, kura nav ietekmēta no blakus procesiem.

Infrastruktūra un tīkli - TĪKLA DROŠĪBAS SISTĒMAS

Kas tiek darīts:

- Nekavējoši - izmantot cita Latvijas valsts uzņēmuma resursus DDoS aizsardzībā, atslogojot esošās tīkla drošības iekartas no ārējo ienākošo savienojumu aizsardzības slodzes.

Infrastruktūra un tīkli - TĪKLA DROŠĪBAS SISTĒMAS

Kas tiek darīts:

- Ilgtermiņā - jāveido jaunu ienākošo savienojumu aizsardzības sistēmu, kura ir paredzēta, atšķirībā no esošās, nodalītu un savstarpēji rezervējošu datu centru aizsardzībai - “Divi DC”. Sistēmai ir jābūt spējīgai strādāt neatkarīgi un paralēli, nevis viena klāstera variantā.
- Jāveido sintētisks monitorings, kurš integrētā veidā ar tīkla drošības sistēmu veic “end-to-end” testus un novirza datu plūsmas uz darbaspējīgu DC “Divu DC” arhitektūrā.

Infrastruktūra un tīkli - ILGTERMIŅA SOĻI

- Sagatavot DC tīklu sistēmas ekspluatācijai rezervētos datu centros - “Divu DC” risinājums;
- Arhitektūra, dizains, iekārtu iegāde, tīkla migrācija.
- Tīkla arhitektūra, tai skaitā FC starpsavienojumu nepieciešamība, ir atkarīga no programmatūras arhitektūras attīstības un datu replikācijas mehānismiem.
- Serveru migrācija rezervētos datu centros nozīmē jaunas paralēlas serveru sistēmas instalāciju, maksimāli izmantojot esošo serveru aparatūru.

APKALPOŠANA

- Reorganizēts NVD IT nodaļas darbs
 - Tikai uz E-veselība atbalstu norīkota daļa cilvēku
 - leviesti Agile procesi un "war room" režīms
- Būtiski samazināts "nekontrolētu izmaiņu" skaits, t.sk.konfigurācijās
- Uzsākts darbs pie piegādes procesu optimizēšanas un sakārtošanas (labojumi programmatūrā un jaunās funkcionalitātes)
- Darbības pārtraukumu gadījumā daudz ātrāka spēja atjaunot darbību (t.sk. pamanīt)



PROGRAMMATŪRA UN KONFIGURĀCIJAS

- Sasniegtais
 - Veicot procesu analīzi identificēti līdz šim problēmsituācijas izraisošās sistēmas komponentes
 - Kur iespējams ir veikta problēmsituācijas izraisošo komponentu uzlabošana, kur nepieciešama papildus izstrāde, tā ir uzsākta.
- Īstermiņa plāni
 - Veik sistēmas stabilitāti ietekmējošo procesu “uzkopšanu”, un identificēto programmatūras kļūdu novēršanu
- Ilgtermiņa plāni
 - Papildus jauno funkcionalitāšu integrācija - veidā, kas minimāli iespaido esošos lietotājus
 - Arhitektūras paplašināšana ar mērogojamiem elementiem (konteinerizācija jaunajiem elementiem un jauno elementu efektīva mijiedarbība ar esošajām saskarnēm)
 - Pakāpeniska pāreja integrācijas risinājumu piegādātājiem uz REST asinhroniem servisiem

PROGRAMMATŪRA UN KONFIGURĀCIJA GALA LIETOTĀJIEM

- Sasniegtais
 - Iespēja identificēt individuālas problēmas (labojumi un jau sākotnēji piegādāto rīku efektīva izmantošana)
- Īstermiņa plāni
 - Fokuss uz plānotajām papildus funkcionalitātēm un to, lai tās minimāli iespaidotu pieejamību un veiktspēju
- Ilgtermiņa plāni
 - Minimāls jauninājumu iespaids uz stabilitāti
 - Spēja identificēt lietotāju darbības un veidot izmaiņas balstoties uz lietotāju paradumiem

DROŠĪBA

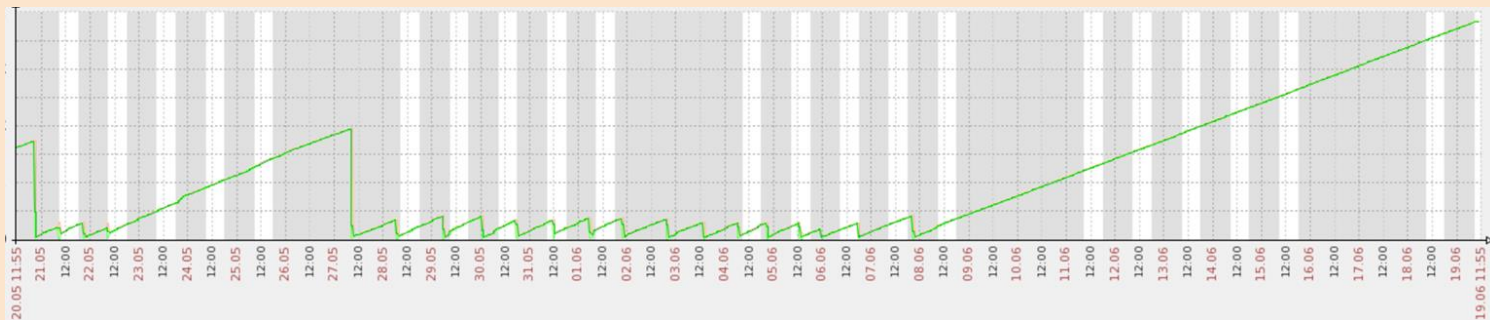
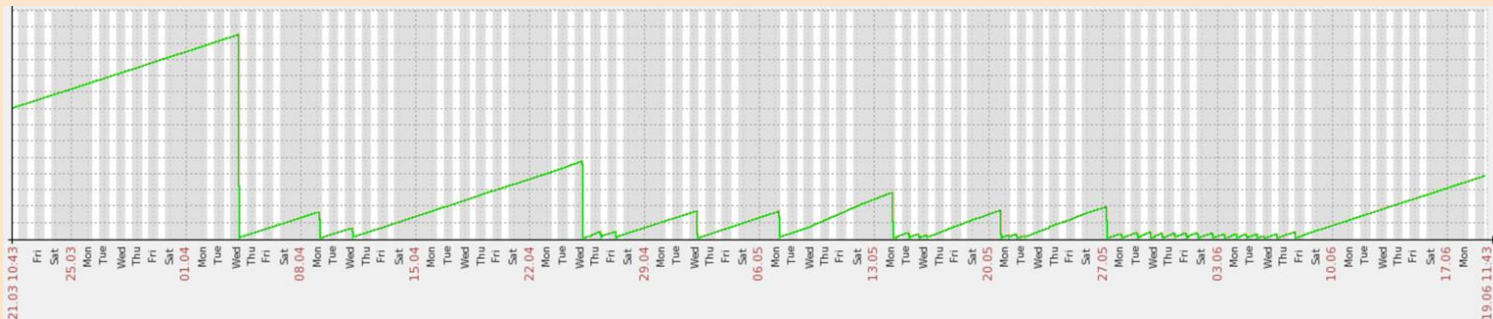
- Izdarītais
 - Regulāri drošības auditi (šobrīd arī notiek visaptveroša drošības pārbaude sistēmām)
 - Auditācijas pierakstu alternatīva ievākšana (t.sk.par administratoru un citām darbībām)
- Īstermiņā plānotais
 - Drošības vadības centrs, kas fokusējas tikai uz drošības procesiem un notikumiem
- Ilgtermiņā plānotais
 - Informācijas drošības pārvaldības sistēma NVD pusē (ISO 27001 balstīta)

Rezultāti

- Integrācijas platformas stabilitātes uzlabošanās
- Lietotāju atbalsta pieprasījumu skaita samazināšanas
- Veiktspējas uzlabošanās dati pa datumiem

Rezultāti - stabilitātes uzlabojums

- Integrācijas platformas komponentes darbības (stabilitātes) atainojums



Rezultāti - Lietotāju atbalsta zvanu skaits

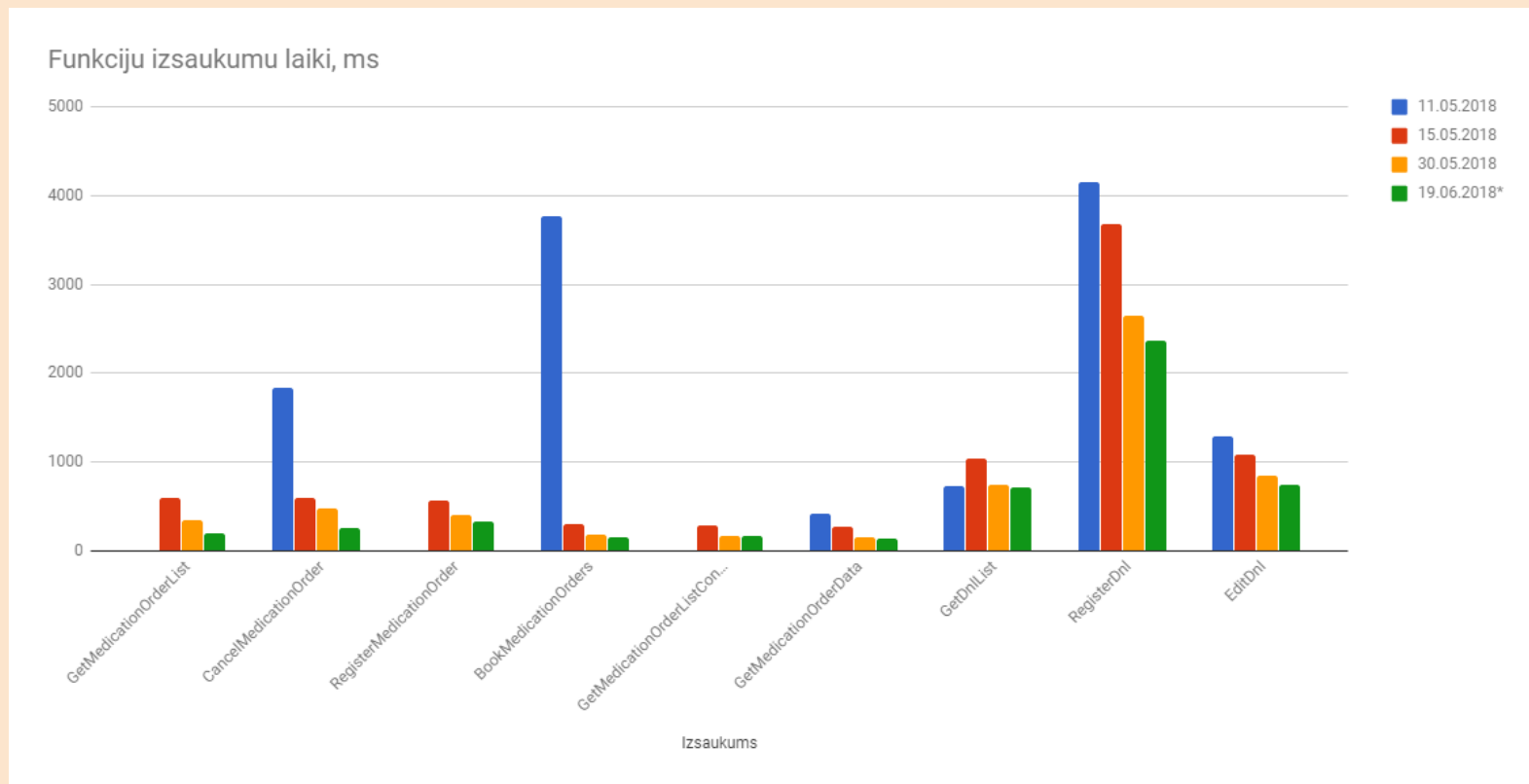
Mēnesis	Marts	Aprīlis	Maijs	Jūnijs*
Zvanu skaits	3977	4551	3647	1261

* Laika posmā no 1. līdz 18. Jūnijam

Rezultāti - veikspējas uzlabojumi

Izsaukums	11.05.2018	15.05.2018	30.05.2018	19.06.2018*
GetMedicationOrderList	-	597 msec	349 msec	197 msec
CancelMedicationOrder	1 sec 832 msec	587 msec	479 msec	258 msec
RegisterMedicationOrder	-	568 msec	407 msec	334 msec
BookMedicationOrders	3 sec 770 msec	301 msec	186 msec	147 msec
GetMedicationOrderListContinuation	-	276 msec	160 msec	165 msec
GetMedicationOrderData	418 msec	263 msec	152 msec	130 msec
GetDnlList	727 msec	1 sec 33 msec	734 msec	705 msec
RegisterDnl	4 sec 156 msec	3 sec 674 msec	2 sec 643 msec	2 sec 363 msec
EditDnl	1 sec 293 msec	1 sec 82 msec	849 msec	744 msec

Rezultāti - veikspējas uzlabojumi, grafiski



Secinājumi

Būtiskākie secinājumi

- Kaut arī sistēmas arhitektūra nav atbilstoša moderniem lielas veiktspējas sistēmas principiem, to ir iespējams pakāpeniski pielāgot, turpinot izmantot lielu daļu esošo elementu un datu struktūru:
 - Argumenti:
 - Izstrādātāju jau esošās saskarnes datu nodošanai;
 - Pamatdatu turpmāka uzkrāšana EVK ir iespējama;
- Lai nodrošinātu augstu pakalpojuma pieejamību nepieciešamas papildus investīcijas. Ne tikai infrastruktūrā. Šobrīd riski ir “vadīti”, taču ir nepieciešams pārskatīt prasību prioritātes;
- Nepieciešami programmatūras uzlabojumi, lai tie atbalstītu apstrādājamo datu apjoma pieaugumu un arī citas prasības;
- Strādājošu sistēmu rekomendēts attīstīt labojot sākotnēji neparedzētās lietas vai trūkumus

Atgādinājumi

1. Pieteikumi uz helpdesk
 - a. Gala lietotājiem: atbalsts@eveseliba.gov.lv
 - b. Izstrādātājiem: help@eveseliba.gov.lv
2. Lūgums integrāciju izstrādātājiem atbildēt uz izsūtīto incidentu un pieteikumu aktualizācijas e-pastu.