Lietuvos mokslo ir studijų institucijų kompiuterių tinklas LITNET

VYTAUTO DIDŽIOJO UNIVERISTETAS

PASLAUGŲ IŠPLĖTIMAS APIMANT NAUJUS ŽURNALŲ SAUGOJIMO RESURSUS

2.3.2

Paslauga sukurta vykdant Europos socialinio fondo finansuojamą projektą „Mokslo ir studijų institucijoms LITNET teikiamų IT paslaugų plėtra“ Nr. 09.3.3-ESFA-V-711-01-0003

Kuriame Lietuvos ateitį

2014–2020 metų Europos Sąjungos fondų investicijų veiksmų programa

Kaunas

2019 m.

TURINYS

1. ĮVADAS

Esamos standartinės paslaugos bus išplėstos, realizuojant didelės apimties žurnalų saugojimą ir analizę projekto dalyvio infrastruktūroje. Realizuojant paslaugą, paaiškėjo, kad norint užtikrinti efektyvų įvykių žurnalų saugojimą, būtina paskirstyta saugojimo sistema, ir vieninga koreliacijos sistema, galinti apibendrinti informaciją iš skirtingų saugojimo vietų. Neįgyvendinus šios paslaugos plėtros, projekte numatyta paslaugos realizacija liks tik dalinė, nebus galimybės užtikrinti vienodos paslaugos kokybės visiems Lietuvos mokslininkams ir tyrėjams.

IT administratoriaus darbe didelę darbo dalį sudaro tinklinės aparatūros (komutatoriai, maršrutizatoriai) bei serverių darbo analizė, gedimų šalinimas. Serveriai, dažniausia, saugo informaciją apie darbą žurnaluose (log file) lokaliniuose diskuose, informaciją iš kurių, žurnalus galima nuskaityti net įvykus serverio trikiui.

Kompiuterijoje trikio apibrėžimas yra sekantis: tai įvykiai, kurie pažeidžia normalų tinklo veikimą, prieštarauja tinklo saugumo taisyklėms. Trikis – realų ar potencialiai nepageidaujamą poveikį kompiuterių tinklo veiklai turintis įvykis, kurio rezultatas – apgaulė, nuostoliai ar piktnaudžiavimas, grėsmė informacijai, informacijos nuosavybės praradimas ar žala jai.

Tačiau tinklinės aparatūros atveju tai atlikti negalima, kadangi žurnalų failai saugojami konkrečios įrangos atmintyje, ir, po aparatūros trikio (persikrovimo, atakos, trumpalaikio elektros sutrikimo ar kitokio trikio), jie susinaikina ir nuskaityti žurnalų failų negalima. Kiekvienas serveris ar komutatorius per dieną generuoja apie 1 MB apimties žurnalo failą. Tačiau, įvykus kokiam nors trikiui ar gedimui, žurnalo failo apimtis drastiškai išauga ir gali pasiekti kelis GB (jei yra tam diskinės vietos). Todėl greitam reagavimui į IT infrastruktūros sutrikimus pageidautina centralizuota žurnalų saugojimo sistema į kurią, realiu laiku, suplauktų visi žurnalai iš serverių ir tinklines aparatūros, kol jie dar yra veiksnus. Įvertinus tai, kad VDU IT infrastruktūroje yra apie 160 komutatorių bei 100 serverių ir saugojimo trukmę bent 30 kalendorinių dienų, informacijos apimtis gali siekti šimtus GB. Operatyviai juos galima išanalizuoti tik tada, jei visa informacija bus patalpinta duomenų bazėje, saugoma ir reikalui esant pasiekiama analizei.

Atlikti įvykių analizę iš surinktų duomenų, galima tiktai tada, kuomet visi žurnaluose užregistruoti įvykiai bus atspindėti tikslai pagal laiką, tai yra nebus pažeistas jų nuoseklumas. Tam būtina, kad visi įrenginiai būtų tiksliai sinchronizuoti laike – tai yra. visi įrenginiai privalo būti sinchronizuoti laike pagal vieną ir tą patį laiko šaltinį. Tik esant vieningam, sinchronizuotam laikui, apjungus visus duomenis iš skirtingų įrenginių žurnalų, galima žiūrėti kaip konkrečiu laiku atsiradęs trikis įtakojo visą tinklo darbą ir kokių veiksmų reikia imtis, kad ateityje išvengti panašių atvejų ir taip užtikrinti nepertraukiamą tinklo darbą.

2. PASLAUGOS TIKSLAI IR UŽDAVINIAI

Šiai paslaugai buvo iškelti sekantys tikslai:

1. Sukurti vieningą žurnalų arba jų įvykių saugojimo sistemą, į kurią suplauktų realiame laike visi aparatūros įvykiai ir ji būtų tinkama ir patogi įvykių analizei.

2. Sinchronizuoti pagal vieną laiko šaltinį visus serverius bei tinklinę aparatūrą.

Bei buvo suformuluoti sekantys uždaviniai:

- Sukurti įvykių saugojimo duomenų bazę, kurioje būtų saugojami visi įrašai iš įrenginių žurnalų, skirtų įvykių analizei.
- Sinchronizuoti visų įrenginių laiką pagal vieną ir tą patį laiko šaltinį.
- Nukreipti visus reikiamus įvykius į žurnalų duomenų bazę iš karto, kai jis (įvykis) įvyko.
- Sukurti analizės procedūras, kurių rezultatų pagalba galima būtų šalinti gedimus bei numatyti prevencinius veiksmus.

3. PASLAUGOS REALIZACIJA

Pirmajam uždaviniui spręsti buvo sukurta centralizuota MySQL duomenų bazė dedikuotame virtualiame serveryje. Aplinka kurioje buvo patalpinta duomenų bazė buvo kuriama taip, kad esant poreikiui ar pritrukus resursų juos lanksčiai galima būtų praplėsti.

Antrajam uždaviniui spręsti buvo įdiegtas vidinis laiko serveris, kuris sinchronizuoja laiką pagal lt.pool.ntp.org. turimą laiką. Visų serverių bei tinklinės aparatūros laikas buvo nustatytas taip, kad jis (laikas) būtų sinchronizuotas pagal šį VDU infrastruktūroje sukurtą laiko serverį.

Trečiam uždaviniui spręsti visuose įrenginiuose buvo sukonfigūruoti žurnalų nukreipimai į centralizuotą žurnalų saugyklą ir įrašomi į MySQL duomenų bazę. Tam pasinaudota įdiegiant ir sukonfigūruojant rsyslog (v5) programą.

Ketvirtajam uždaviniui nuspręsta įdiegti MS Windows darbinę stotį su Microsoft Access programine įranga. Buvo sukurtos parametrizuotos SQL procedūros darbui su prijungtomis lentelėmis iš centrinės žurnalų saugyklos.

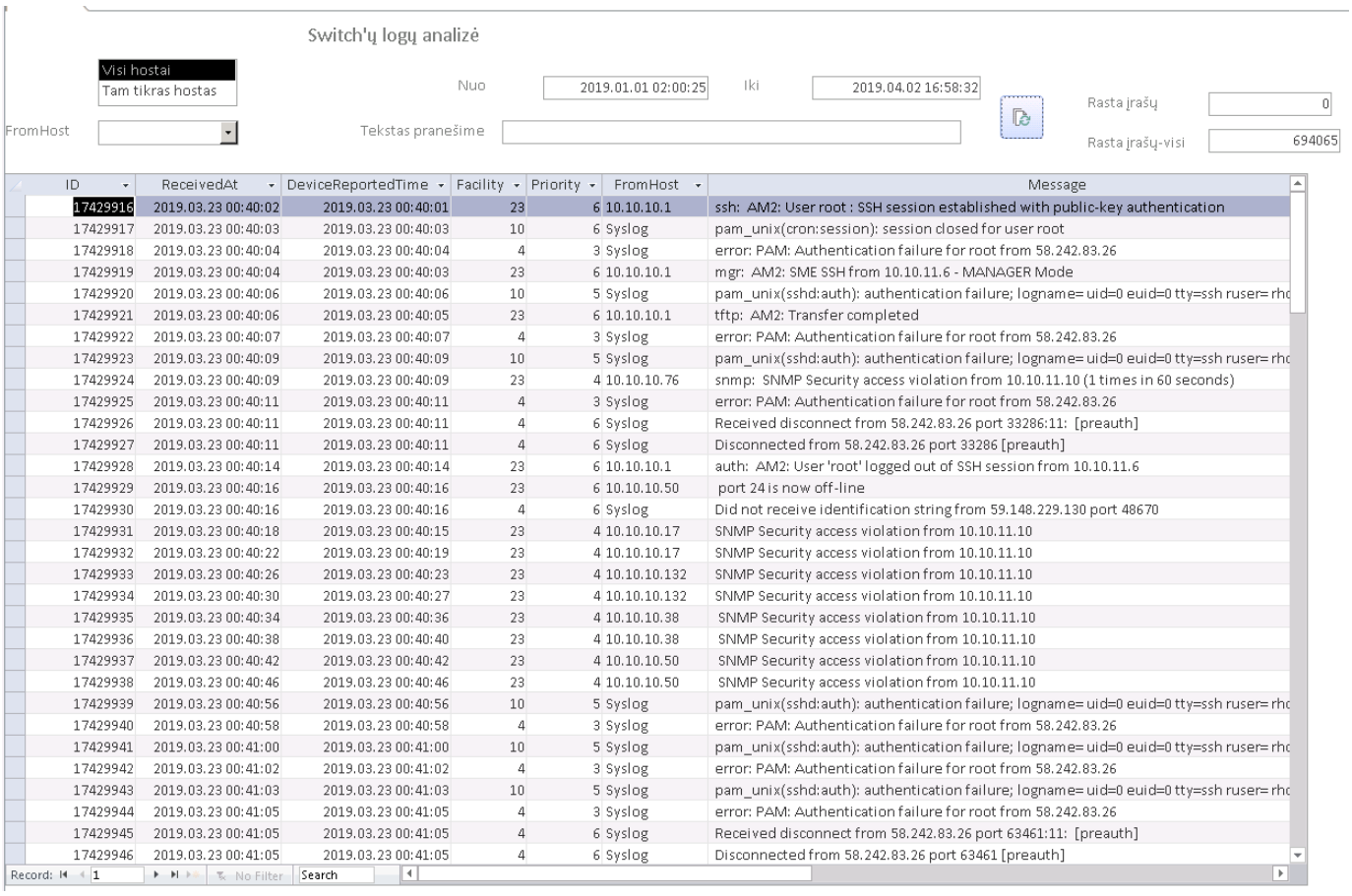
4. PASLAUGOS NAUDOJIMAS

Paslauga gali naudotis VDU tinklo administratoriai, turintis teisę pasiekti valdymo potinklį iš savo darbinės stoties.

Norint pradėti naudotis paslauga, reikia darbinėje stotyje paleisti Microsoft Access failą syslog-syslog.accdb. Atsidaryti formą Form1. Pradinės (startinės) formos vaizdas pateikiamas paveikslėlyje 1.1.

Paveikslėlis 1.1

Pradinė (startinė) forma



ID	ReceivedAt	DeviceReportedTime	Facility	Priority	FromHost	Message
17429916	2019.03.23 00:40:02	2019.03.23 00:40:01	23	6	10.10.10.1	ssh: AM2: User root : SSH session established with public-key authentication
17429917	2019.03.23 00:40:03	2019.03.23 00:40:03	10	6	Syslog	pam_unix(cron:session): session closed for user root
17429918	2019.03.23 00:40:04	2019.03.23 00:40:04	4	3	Syslog	error: PAM: Authentication failure for root from 58.242.83.26
17429919	2019.03.23 00:40:04	2019.03.23 00:40:03	23	6	10.10.10.1	mgr: AM2: SME SSH from 10.10.11.6 - MANAGER Mode
17429920	2019.03.23 00:40:06	2019.03.23 00:40:06	10	5	Syslog	pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhc
17429921	2019.03.23 00:40:06	2019.03.23 00:40:05	23	6	10.10.10.1	tftp: AM2: Transfer completed
17429922	2019.03.23 00:40:07	2019.03.23 00:40:07	4	3	Syslog	error: PAM: Authentication failure for root from 58.242.83.26
17429923	2019.03.23 00:40:09	2019.03.23 00:40:09	10	5	Syslog	pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhc
17429924	2019.03.23 00:40:09	2019.03.23 00:40:09	23	4	10.10.10.76	snmp: SNMP Security access violation from 10.10.11.10 (1 times in 60 seconds)
17429925	2019.03.23 00:40:11	2019.03.23 00:40:11	4	3	Syslog	error: PAM: Authentication failure for root from 58.242.83.26
17429926	2019.03.23 00:40:11	2019.03.23 00:40:11	4	6	Syslog	Received disconnect from 58.242.83.26 port 33286:11: [preauth]
17429927	2019.03.23 00:40:11	2019.03.23 00:40:11	4	6	Syslog	Disconnected from 58.242.83.26 port 33286 [preauth]
17429928	2019.03.23 00:40:14	2019.03.23 00:40:14	23	6	10.10.10.1	auth: AM2: User 'root' logged out of SSH session from 10.10.11.6
17429929	2019.03.23 00:40:16	2019.03.23 00:40:16	23	6	10.10.10.50	port 24 is now off-line
17429930	2019.03.23 00:40:16	2019.03.23 00:40:16	4	6	Syslog	Did not receive identification string from 59.148.229.130 port 48670
17429931	2019.03.23 00:40:18	2019.03.23 00:40:15	23	4	10.10.10.17	SNMP Security access violation from 10.10.11.10
17429932	2019.03.23 00:40:22	2019.03.23 00:40:19	23	4	10.10.10.17	SNMP Security access violation from 10.10.11.10
17429933	2019.03.23 00:40:26	2019.03.23 00:40:23	23	4	10.10.10.132	SNMP Security access violation from 10.10.11.10
17429934	2019.03.23 00:40:30	2019.03.23 00:40:27	23	4	10.10.10.132	SNMP Security access violation from 10.10.11.10
17429935	2019.03.23 00:40:34	2019.03.23 00:40:36	23	4	10.10.10.38	SNMP Security access violation from 10.10.11.10
17429936	2019.03.23 00:40:38	2019.03.23 00:40:40	23	4	10.10.10.38	SNMP Security access violation from 10.10.11.10
17429937	2019.03.23 00:40:42	2019.03.23 00:40:42	23	4	10.10.10.50	SNMP Security access violation from 10.10.11.10
17429938	2019.03.23 00:40:46	2019.03.23 00:40:46	23	4	10.10.10.50	SNMP Security access violation from 10.10.11.10
17429939	2019.03.23 00:40:56	2019.03.23 00:40:56	10	5	Syslog	pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhc
17429940	2019.03.23 00:40:58	2019.03.23 00:40:58	4	3	Syslog	error: PAM: Authentication failure for root from 58.242.83.26
17429941	2019.03.23 00:41:00	2019.03.23 00:41:00	10	5	Syslog	pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhc
17429942	2019.03.23 00:41:02	2019.03.23 00:41:02	4	3	Syslog	error: PAM: Authentication failure for root from 58.242.83.26
17429943	2019.03.23 00:41:03	2019.03.23 00:41:03	10	5	Syslog	pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhc
17429944	2019.03.23 00:41:05	2019.03.23 00:41:05	4	3	Syslog	error: PAM: Authentication failure for root from 58.242.83.26
17429945	2019.03.23 00:41:05	2019.03.23 00:41:05	4	6	Syslog	Received disconnect from 58.242.83.26 port 63461:11: [preauth]
17429946	2019.03.23 00:41:05	2019.03.23 00:41:05	4	6	Syslog	Disconnected from 58.242.83.26 port 63461 [preauth]

Record: 1 No Filter Search

Startinė forma užpildyta pagal sekančias taisykles:

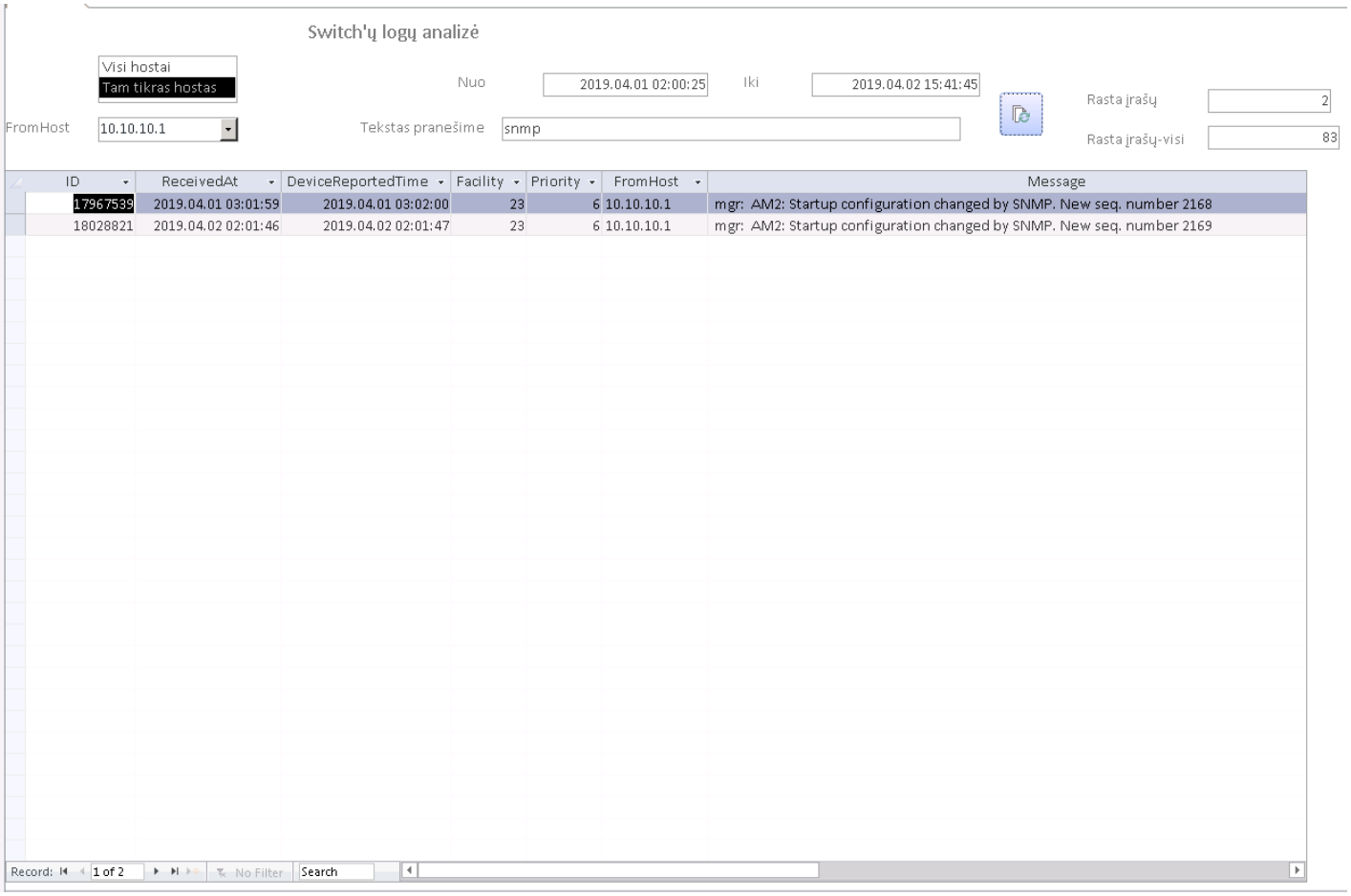
1. Rodomi visų hostų sukaupti įrašai nuo **Nuo** lauke įrašytos datos iki **Iki** lauke įrašytos datos.
2. Starto metu **Nuo** lauke automatiškai įrašoma anksčiausio rasto įrašo data.
3. Starto metu **Iki** lauke automatiškai įrašoma dabartinis laikas ir data.
4. **FromHost** lauke automatiškai surenkami visi hostai. Starto metu nustatoma reikšmė-*Visi hostai*

Jei reikia rasti tam tikro hosto, tam tikram laike su tam tikra fraze įrašus, užpildomi laukai From Host, Nuo, Iki laukai ir Tekstas pranešime.

Pvz., reikia rasti hosto 10.10.10.1 įrašus laike tarp 2019.04.01 02:00:25 ir 2019.04.02 15:41:45 turinčius frazę snmp pranešime. Formos užpildymas ir gauti rezultatai pateikti paveikslėlyje 1.2 .

Paveikslėlis 1.2

Rezultatų forma



Čia lauke Rasta įrašų rodoma bendras rastų įrašų skaičius, lauke Rasta įrašų-visi -bendras įrašų skaičius be frazes snmp.

Įrašai duomenų bazėje saugomi 6 mėn., po to automatiškai trinami. Šį parametrą pagal poreikius galima laisvai keisti.

5. PASIEKTI REZULTATAI

Veikla buvo išplėsta, realizuojant didelės apimties žurnalų saugojimą MySQL duomenų bazėje. Sukonfigūruoti 30 serverių bei 160 tinklinės aparatūros vienetų (sinchronizuotas laikas, centralizuotas žurnalų nukreipimas į duomenų bazę). Buvo sukurtus procedūros bei valdymo forma, leidžiančios

analizuoti ir apibendrinti informaciją iš skirtingų hostų. To pasėkoje, reakcijos laikas į kritinius tinklo infrastruktūros įvykius buvo sutrumpintas, padidintas IT infrastruktūros darbingumas/stabilumas. Taip pat šių žurnalų duomenų analizavimas įgalins pateikti rekomendacijas tinklo infrastruktūros prevenciniams veiksmams atlikti bei tiksliau nustatyti silpnas tinklo vietas. Tai leis užtikrinti MSI mokslininkams ir tyrėjams stabilesnį tinklo paslaugų veikimą.