Lietuvos mokslo ir studijų institucijų kompiuterių tinklas LITNET

Vilniaus universitetas

SISTEMINIŲ ŽURNALŲ TERMINUOTO SAUGOJIMO PASLAUGA

Paslaugos naudojimo instrukcija

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

Vilnius

2018

Paslaugos naudojimo sąlygos

- Sisteminių žurnalų terminuoto saugojimo paslaugos naudotoju gali būti tik LITNET tinklo administratoriai.
- Sisteminiai įrašai į surinkimo serverį turi būti siunčiami syslog formatu.
- Sisteminiai įrašai saugomi 6 mėnesius.
- Paslaugos naudotojas gali peržiūrėti ir gauti pranešimus tik apie jo administruojamų įrenginių atsiųstus įrašus.
- Paslaugos administratorius ir paslaugos naudotojas įsipareigoja laikytis LITNET Tinklo naudojimo taisyklių (https://www.litnet.lt/index.php/lt/tnt).

Instrukcijos paslaugos naudotojui

Paslaugos užsakymas

Sisteminių žurnalų terminuoto saugojimo paslaugą galima užsakyti užpildant elektroninę formą adresu https://info.tinklas.vu.lt/zurnalai/ .

Gavę užsakymo duomenis, sisteminių žurnalų terminuoto saugojimo paslaugos administratoriai patikrina pateiktus duomenis, su užsakovais suderina įrašų struktūravimo ir pranešimų formatus bei suteikia tinkamas prieigos teises.

Įrašų siuntimas į sisteminių įrašų surinkimo serverį

Administratoriai turi nukreipti savo administruojamų įrenginių sisteminius įrašus į įrašų surinkimo serverį logs-in.tinklas.vu.lt (158.129.159.204) į standartinį syslog portą UDP 514.
Dėl įrenginių įvairovės bei skirtingų poreikių įrašų nurkreipimo konfigūracijos atskiruose įrenginiuose skiriasi, todėl toliau pateikiami tik keletas tipinių sistemų konfigūravimo pavyzdžių:

Linux OS konfigūravimas

Linux operacinės sistemos faile /etc/rsyslog.conf nurodoma sisteminius įrašus siųsti į įrašų surinkimo serverį logs-in.tinklas.vu.lt (158.129.159.204) į standartinį syslog portą UDP 514.

Atidaromas konfigūravimo failas:
$ vi /etc/rsyslog.conf

Įrašomas nustatymas:
**.* @158.129.159.204:514*

Perkraunamas rsyslog tarnyba:
$ sudo service rsyslog restart

Išbandymui galima sukurti sisteminį įrašą, kuris tuoj pat turi būti nusiunčiamas į sisteminių įrašų serverį:
$ logger "Įrašų siuntimas sukonfigūruotas"

Cisco IOS konfigūravimas

Cisco įrenginyje įjungiamas globalaus konfigūravimo režimas:
Router# configure terminal

Nurodomas sisteminių įrašų surinkimo serveris:
Router(config)# logging host 158.129.159.204

Nustatoma, kokio svarbumo įrašai siunčiami (šiuo atveju *notifications* lygmens):
Router(config)# logging trap notifications

Išeinamas konfigūravimo režimas su komanda End ir peržiūrima konfigūracija:
Router(config)# End
Router# show logging

Įrašų peržiūra SSH protokolu

Užsakius paslaugą (žiūrėti Paslaugos užsakymas) ir gavus prisijungimo duomenis, į sisteminių įrašų surinkimo serverio atsiųstus įrašus galima peržiūrėti ir analizuoti prisijungus prie paslaugos SSH protokolu:
$ ssh naudotojo-vardas@logs-t.tinklas.vu.lt

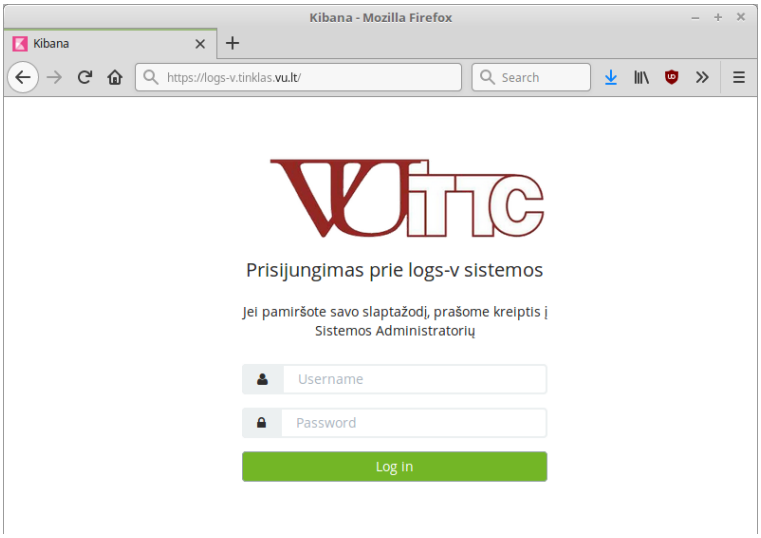
Naudotojui leidžiama peržiūrėti tik savo administruojamų sistemų įrašus. Jie randami kataloge /logs/ . Sisteminiai įrašai skaidomi į atskirus katalogus pirmiausia pagal IP adresą, vėliau pagal metus, mėnesius ir dienas, pavyzdžiui:
/logs/172.0.0.13/2018/2018-01/2018-10/2018-01-20_172.0.0.13.log

Daugiau kaip 2 mėnesių senumo įrašai saugomi suspaustu formatu ir taip pat yra prieinami administratoriams.

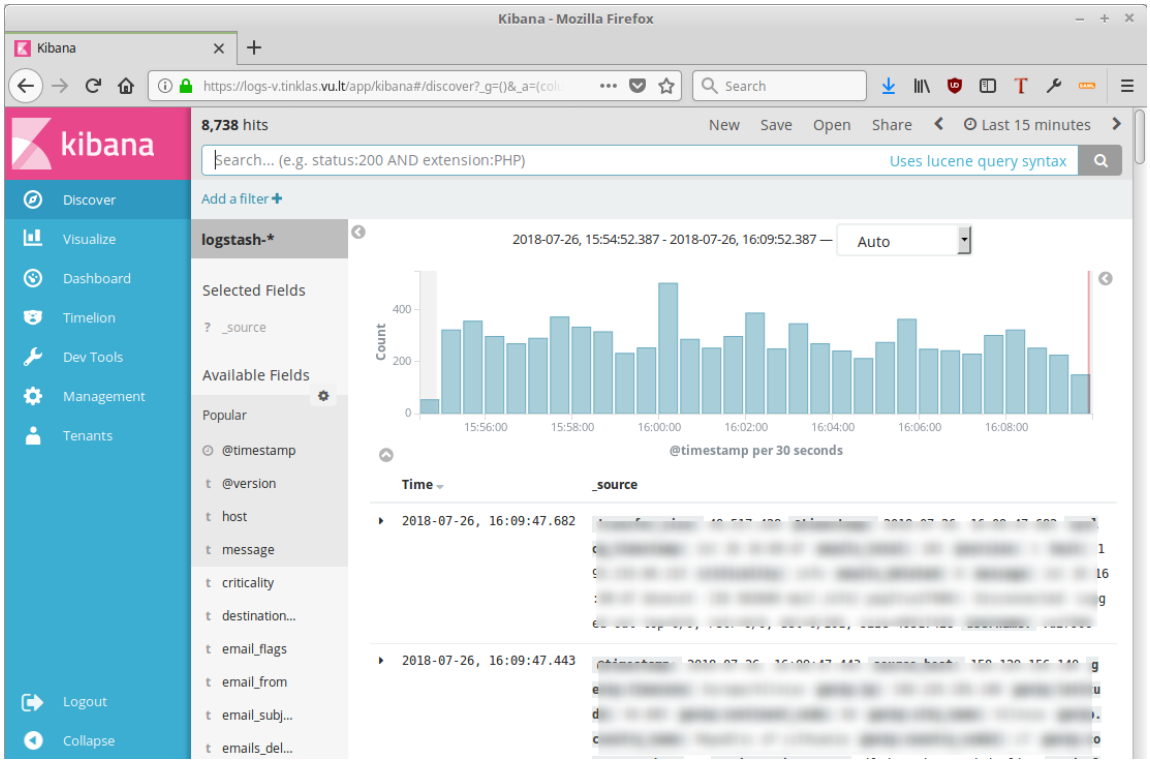
Įrašų peržiūra naudojant grafinę sąsają

Užsakius paslaugą (žiūrėti Paslaugos užsakymas) ir gavus prisijungimo duomenis, sisteminių įrašų surinkimo serverio gautus įrašus galima peržiūrėti ir analizuoti naudojant grafinę sąsają – per naršyklę prisijungus šifruotu HTTPS protokolu adresu https://logs-v.tinklas.vu.lt. Grafinės sąsajos atvaizdavimui įdiegtas atviro kodo įrankis Kibana.

Prie sistemos prisijungęs (1 pav.) naudotojas gali atlikti tik jo administruojamų sistemų siųstų įrašų paiešką ir peržiūrą norimame laiko intervale (2 pav.). Naudotojas iš struktūruotos informacijos gali išsirinkti ir atvaizduoti tik jam norimas informacijos dalis. Naudotojo surasti įrašai atvaizduojami ne tik tekstinių reikšmių pavidalu (2 pav. užtušuoti regionai), bet ir parodomi įrašų skaičiaus kitimas laiko skalėje.

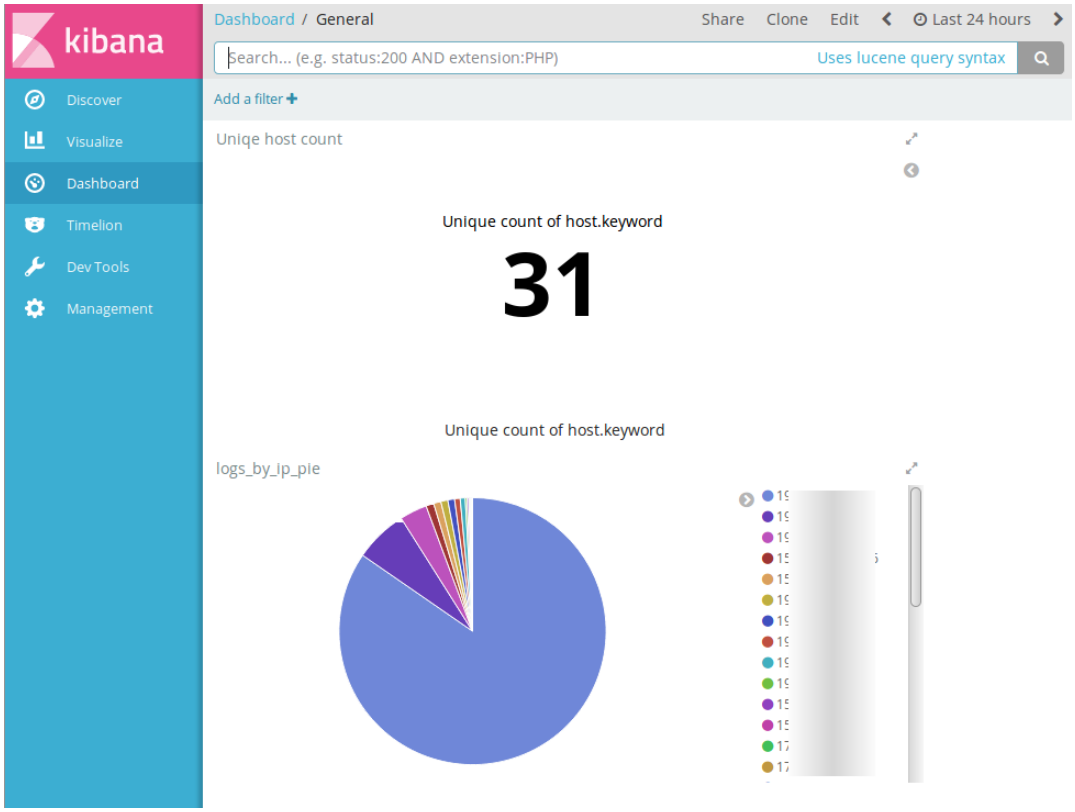


1 pav. logs-v.tinklas.vu.lt prisijungio langas

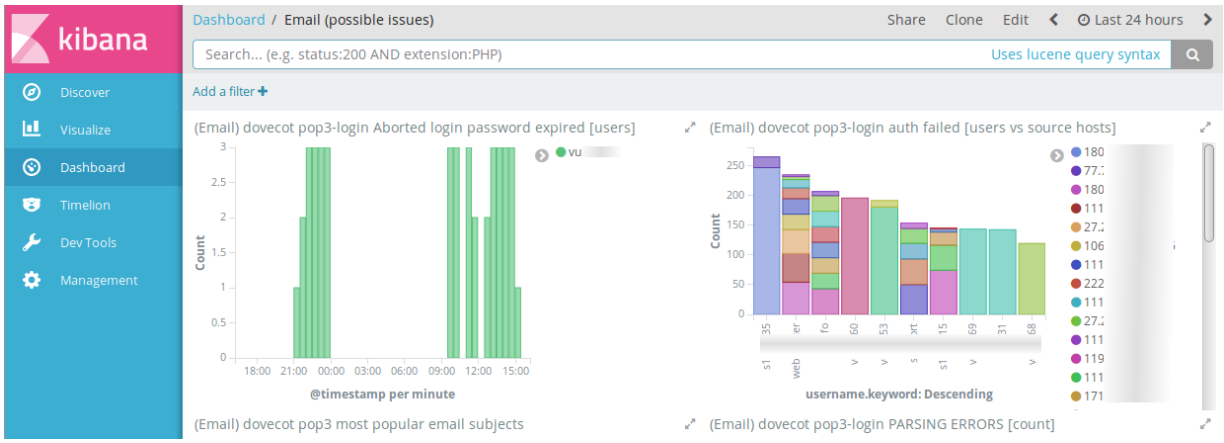


2 pav. įrašų paieškos langas

Kibana įrankis leidžia administratoriui pagal savo poreikius susiformuoti svarbios informacijos atvaizdavimo pultą (angl. Dashboard), sudarytą iš įvairių informacijos atvaizdavimo skydelių (angl. Panel). Skydeliai gali būti atvaizduoti įvairiais grafikais, lentelėmis ir skaitinėmis reikšmėmis (3 ir 4 pav.)



3 pav. Pulto pavyzdys



4 pav. Pulto pavyzdys