Lietuvos mokslo ir studijų institucijų kompiuterių tinklas LITNET

Vilniaus universitetas

SISTEMINIŲ ŽURNALŲ TERMINUOTO SAUGOJIMO PASLAUGA

Paslaugos administravimo 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

Sistemos sandaros aprašymas

logs-in.tinklas.vu.lt [158.129.159.204]

1. Sisteminių žurnalų įrašų (angl. logs) surinkimo ir saugojimo sistema.
2. Surenka ir pagal nustatytas taisykles rūšiuoja įrašus, užtikrina jų efektyvų saugojimą pagal reikalavimus.
    1. Įrašai rūšiuojami pagal:
        1. serverio (siuntėjo) adresą
        2. metus ir mėnesį
        3. kalendorinę dieną
    2. Log'ai saugomi:
        1. 6 mėnesius
        2. senesi nei 2 mėnesių įrašai saugomi suspaustu formatu
3. Programinė įranga:
    1. Operacinė sistema - CentOS 7 x86_64
    2. Log'ų surinkimas - logstash 2.x+ versija
    3. NFS serveris

logs-t.tinklas.vu.lt [158.129.159.205]

1. Prieigos prie sisteminių žurnalų įrašų aplinka SSH protokolu
2. Įgalina administratorius savarankiškai skaityti žurnalų įrašus failus, pagal jiems suteiktas prieigos teises
3. Programinė įranga:
    1. Operacinė sistema - CentOS 7 x86_64
    2. NFS klientas
    3. SSH serveris

logs-o.tinklas.vu.lt [158.129.159.206]

1. Kritinių įvykių stebėjimo ir informavimo sistema
2. Siunčia pranešimus nurodytiems adresatams (administratoriams) apie konkretaus įrašų siuntėjo (įrenginio) kritinius įvykius.
3. Programinė įranga:
    1. Operacinė sistema - CentOS 7 x86_64
    2. NFS klientas
    3. Postfix MTA

lp-s4a.local.vu.lt [172.16.159.64]

1. Sisteminių žurnalų įrašų indeksavimo serveris
2. Realiu laiku paruošia skirtingų tipų iš įvairių siuntėjų ateinančius įrašus greitai paieškai (klasteris su lp-s4b)
3. Programinė įranga:
    1. Operacinė sistema - CentOS 7 x86_64
    2. Elasticsearch 2.x+

lp-s4b.local.vu.lt [172.16.159.65]

1. Sisteminių žurnalų įrašų indeksavimo serveris
2. Realiu laiku paruošia skirtingų tipų iš įvairių siuntėjų ateinančius log'us greitai paieškai (klasteris su lp-s4a)
3. Programinė įranga:
    1. Operacinė sistema - CentOS 7 x86_64
    2. Elasticsearch 2.x+

logs-v.tinklas.vu.lt [158.129.159.207]

1. Sisteminių žurnalų įrašų paieškos ir vizualizavimo sistema
2. Grafinis Elasticsearch duomenų bazės klientas, leidžiantis naudotojui per naršyklės sąsają atlikti itin greitą paiešką per daugelio sisteminių žurnalų siuntėjų įrašus ir paverčiantis įrašus statistine informacija bei ją atvaizduojantis įvairių tipų grafikais.
3. Programinė įranga:
    1. Operacinė sistema - CentOS 7 x86_64
    2. Kibana 4.x+

logs-pro.tinklas.vu.lt [158.129.159.208]

1. Centralizuota programinės įrangos ir atnaujinimų valdymo sistema
2. Sistema, automatiškai atnaujinanti programinės įrangos saugyklą iš visų sistemose naudojamų šaltinių, suteikianti vieningą prieigą diegti ir atnaujinti visus komponentus.
3. Programinė įranga:
    1. Operacinė sistema - CentOS 7 x86_64
    2. Katello 2.x+

Informacijos saugojimas

Sisteminių žurnalų įrašai saugomi LITNET duomenų centruose – sistemos serveriai ir duomenų saugykla VU duomenų centre, atsarginių kopijų saugykla VGTU duomenų centre.

Prieiga prie sistemų apribota ugniasienėmis ir sisteminėmis prieigos kontrolės priemonėmis (ACL, file permissions, Search Guard).

Administratoriai gali pasiekti tik savo administruojamų sistemų sisteminius įrašus ir tik šifruotais protokolais.

Atsarginės kopijos

Atsarginių kopijų saugykla (158.129.192.215:/SZTSP) primontuota serveryje logs-t.tinklas.vu.lt:

mount -t nfs 158.129.192.215:/SZTSP /mnt/backups

Stebėjimas

Serverių veikimas stebimas iš sistemos https://tss.vu.lt/cacti SNMP protokolu.

Prieigos kontrolė

Prieiga pries sistemos serverių apribota ugniasienės (iptables) taisyklėmis:

 # firewall-cmd --list-all

Priegai prie žurnalų įrašų kontroliuojama naudotojams prisijungus per SSH failinės sistemos teisių ribojimais (ACL ir permissions), o prisijungus per grafinę sąsają – naudojant Elasticsearch įskiepį Search Guard.

LDAP

Paslaugos naudotojų paskyrų duomenys saugomi LDAP duomenų bazėje. LDAP įdiegtas serveryje logs-o.tinklas.vu.lt (ldap://lp-s3.ittc.vu.lt/)

Įrašų suspaudimas ir trynimas

Įrašų suspaudimo ir trynimo skriptai randami kataloge /opt/app/automation/

Įrašų konvertavimas į struktūruotą informaciją

Įrašų sintaksinį apdorojimą ir konvertavimą į struktūruotą informaciją atlieka Logstash įskiepis Grok.

Grok taisyklės randamos logs-in.tinklas.vu.lt kataloge /etc/logstash/conf.d/patterns