Lietuvos mokslo ir studijų institucijų kompiuterių tinklas LITNET

Vilniaus universitetas

Tinklo stebėjimo ir valdymo paslauga

Paslaugos administratoriaus 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

2019 m.

Turinys

Įvadas

Kompiuterių tinklų stebėjimo paslauga leidžia paslaugos naudotojams (mokslininkams, tyrėjams, kompiuterinių sistemų administratoriams) stebėti ir valdyti jų administruojamą tinklo įrangą, operatyviai gauti pranešimus apie svarbius įvykius tinkle, centralizuotai saugoti kompiuterių tinklo įrenginių konfigūracijas, centralizuotai jas keisti, atnaujinti tinklo įrenginių programinę įrangą. Paslauga taip pat leidžia matyti administruojamo tinklo topologiją, turėti duomenų srautų statistikas, gauti išsamias ataskaitas apie tinkle įvykusius incidentus, gauti atskaitas apie tinkle įvykdytus pakeitimus. Paslaugos naudotojų administravimo priemonės užtikrina galimybę konkretiems naudotojams pasiekti tiktai jiems priskirtus tinklo įrenginius ir gauti tiktai jiems dedikuotą informaciją bei atlikti tik jiems leistus kompiuterių tinklo stebėjimo ir valdymo veiksmus.

Vienas svarbiausių kompiuterių tinklo administravimo uždavinių yra užtikrinti operatyvų tinklo problemų aptikimą, centralizuotai keisti tinklo įrenginių nustatymus ir užtikrinti saugumą suteikiant prieigą prie įrenginių. Su tikslu paaiškinti kompiuterių tinklo valdymo ir stebėjimo sistemos funkcionalumą, šiame dokumente sistema pagal funkcijas išskirstyta į 2 posistemes: kompiuterių tinklo stebėjimo ir valdymo posistemė bei prieigos prie kompiuterių tinklo įrenginių valdymo posistemė. Centralizuota kompiuterių tinklo stebėjimo ir valdymo posistemė užtikrina operatyvų greitaveikos sumažėjimo bei gedimų aptikimą, sutaupo žmogiškuosius resursus naudojant centralizuotą įrenginių konfigūracijų keitimą, saugojimą, programinės įrangos atnaujinimą. Prieigos prie tinklo įrenginių valdymo posistemė užtikrina saugų bei patogų privilegijuotų vartotojų administravimą, atliktų pakeitimų registravimą bei jų saugojimą įvykių žurnaluose.

Paslaugos tikslai

Lietuvos mokslo ir studijų kompiuterių tinkle (toliau – LITNET) yra nemažai institucijų kurių tinklo įrenginių skaičius nėra didelis, o žmogiškųjų resursų tam tinklui administruoti skirta nepakankamai. Taip pat tose institucijose kyla problemų su tinklo administratorių kaita, t. y. išėjus vienam tinklo administratoriui, prisijungimo prie tinklo įrangos duomenys lieka daug laiko nekeičiami, nežinoma kokie, kada ir kokiu tiksliu tinklo įrenginių konfigūracijos pakeitimai buvo atlikti, nebūna išsaugotos konfigūracijų atsarginės kopijos, kartais prisijungimo duomenys prie tinklo įrangos pametami. Visas šias problemas gali išspręsti tinklo stebėjimo ir valdymo sistema. LITNET

tinkle taip pat yra institucijų turinčių gana didėlį tinklo įrenginių ūkį kurį patogiausia būtų valdyti centralizuotai.

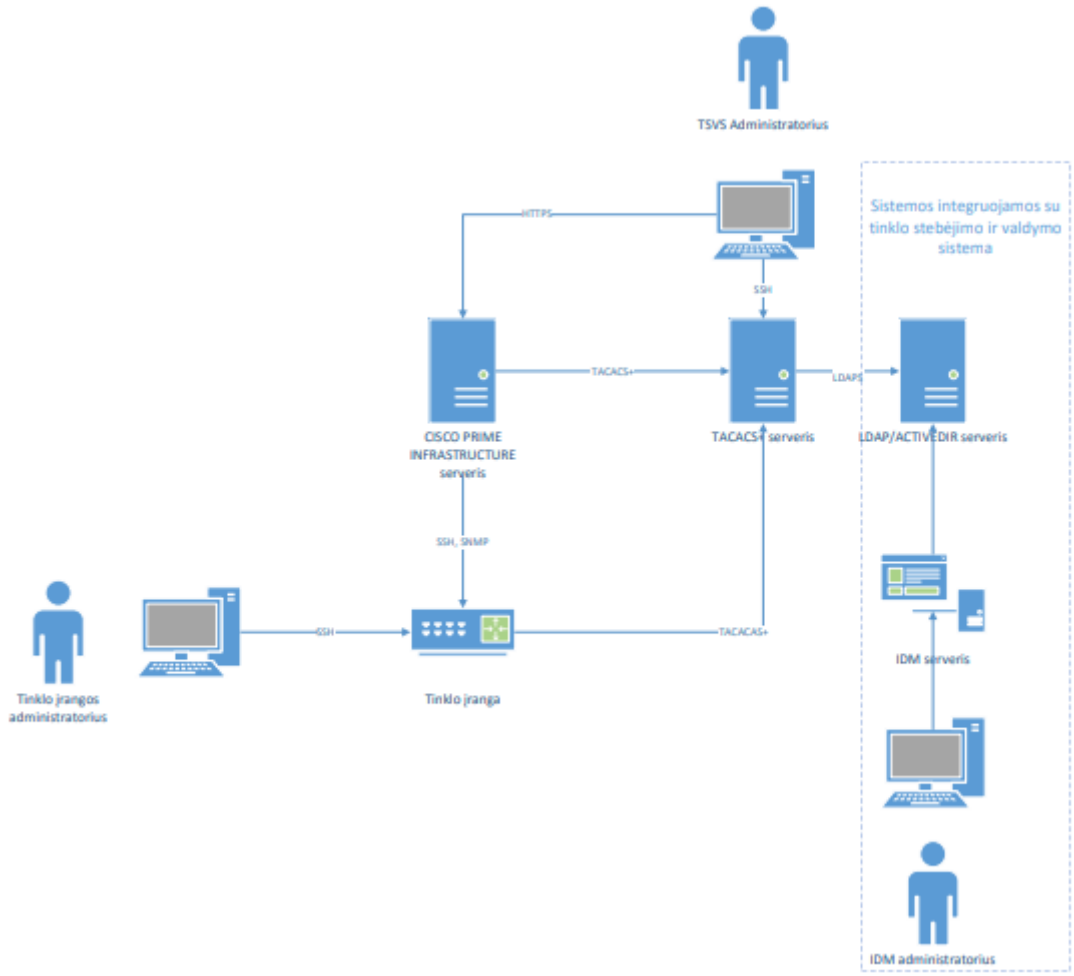
Paslaugos tikslai:

- Suteikti LITNET tinklo administratoriams autentifikuotą prieigą prie jų administruojamų tinklo įrenginių naudojant elektroninės tapatybių valdymo sistemos prisijungimo duomenis
- Registruoti tinklo įrenginiuose vykdomas komandas sisteminiuose įvykių žurnaluose
- Suteikti galimybę LITNET tinklo administratoriams stebėti jų tinklo įrenginių parametrus ir siųsti pranešimus esant įvairiems tinklo parametrų pasikeitimo įvykiams
- Suteikti galimybę LITNET tinklo administratoriams centralizuotai keisti jų administruojamų tinklo įrenginių parametrus, saugoti konfigūracijos failus, atnaujinti programinę įrangą.

Sistemos sandaros aprašymas

Kompiuterių tinklo valdymo ir stebėjimo sistema susideda iš šių komponentų:

- Prieigos prie tinklo įrenginių valdymo posistemė. Autentifikacijos, autorizacijos, įvykdytų komandų registravimo serveris, kuris naudoja TACACS+ protokolą. Ši posistemė gali būti integruojama su centralizuota arba institucijos tapatybių valdymo sistema, kuri naudoja LDAP/ACTIVEDIR serverį tapatybių duomenim saugoti.
- Tinklo stebėjimo ir valdymo sistema Cisco Prime Infrastructure



1 pav. Tinklo stebėjimo ir valdymo sistemos principinė schema

Kompiuterių tinklo valdymo sistema naudoja tokius serverius:

t1.local.vu.lt [172.31.80.132]

- Tinklo įrenginių administratorių autentifikavimo, autorizavimo ir įvykdytų komandų registravimo sistema.
- Autentifikuoja administratorių pagal duomenis gautus iš LDAP/ACTIVEDIR serverio arba pagal duomenis išsaugotus lokaliai sistemoje.
- Autorizavimas atliekamas nustatant privilegijos lygį (0-15) ir nustatant leistinų vykdymui komandų sąrašą.
- Įvykdytų komandas registruoją įrašant į tekstinį failą, kuris saugomas lokaliai sistemoje
- Operacinė sistema - Ubuntu Server 18.

t2.local.vu.lt [172.31.165.15]

- Rezervinė tinklo įrenginių administratorių autentifikavimo, autorizavimo ir įvykdytų komandų registravimo sistema reikalinga aukštam patikimumui užtikrinti, kai t1.local.vu.lt neveikia arba nepasiekiamas.

ciscoprime.tinklas.vu.lt [193.219.80.156]

- Tinklo valdymo ir stebėjimo sistema Cisco Prime Infrastructure 3.4
- Pagrindinės funkcijos:
    - Tinklo įrenginių parametrų rinkimo funkcija
    - Surinktų duomenų agregavimas siekiant sutaupyti diskinę vietą
    - Surinktų duomenų atvaizdavimas grafiniu pavidalu
    - Perspėjimo pranešimų siuntimas tinklo įrenginių administratoriams elektroniniu paštu ir SMS žinutėmis
    - Tinklo įrenginių sisteminių pranešimų žurnalo kaupimas
    - Duomenų srautų statistikų (NetFlow) kaupimas ir analizė
    - Tinklo įrenginių įvykių bei gedimų apibendrintų statistikų pateikimas
    - Automatinis tinklo topologijos atvaizdavimas
    - Tinklo įrenginių konfigūracijų surinkimas
    - Tinklo įrenginių konfigūracijų keitimas
    - Centralizuotas tinklo įrenginių programinės įrangos atnaujinimas
- Naudojamos tarnybos (angl. service):
    - FTP
    - TFTP
    - SSHD
    - SNMP-TRAP
    - HTTPS
    - SYSLOG
    - NETFLOW
- Operacinė sistema Red Hat Linux 7

Techniniai reikalavimai serveriams

Kompiuterių tinklo stebėjimo ir valdymo sistema dirba virtualizuotoje aplinkoje. Minimalūs techniniai reikalavimai virtualioms mašinoms pateikti 1 lentelėje.

1 lentelė. Techniniai reikalavimas virtualioms mašinoms

VM pavadinimas	Procesoriai (vCPU)	Atmintis (RAM), GB	Diskinė vieta
t1.local.vu.lt	1	2	80 GB
t2.local.vu.lt	1	2	80 GB
ciscoprime.tinklas.vu.lt	16	24	1.2 TB
Iš viso:	18	28	1.36 TB

Informacijos saugojimas

Surinkta iš tinklo įrenginių informacija (kokybės parametrai, konfigūracijos, sisteminių žurnalų įrašai, IP paketų statistiniai duomenis) saugomi LITNET VU RC duomenų centre. Prieiga prie sistemų apribota ugniasienėmis ir sisteminėmis prieigos kontrolės priemonėmis. Administratoriai gali stebėti ir valdyti tik savo administruojamus įrenginius. Tinklo valdymo ir stebėjimo sistema pasiekiama šifravimą naudojančiais protokolais.

Įdiegta kompiuterių tinklo stebėjimo ir valdymo sistema naudoja du TACACS serverius ir vieną CPI serverį. Sistemos patikimumo užtikrinimui rekomenduojama naudoti du CPI serverius.