Lietuvos mokslo ir studijų institucijų kompiuterių tinklas LITNET

Vilniaus universitetas

Tinklo stebėjimo ir valdymo paslauga

Paslaugos aprašymas

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 centralizuota tinklo stebėjimo ir valdymo sistema. LITNET tinkle taip pat yra institucijų turinčių gana didelį tinklo įrenginių ūkį, kurį patogiausia būtų valdyti centralizuotai.

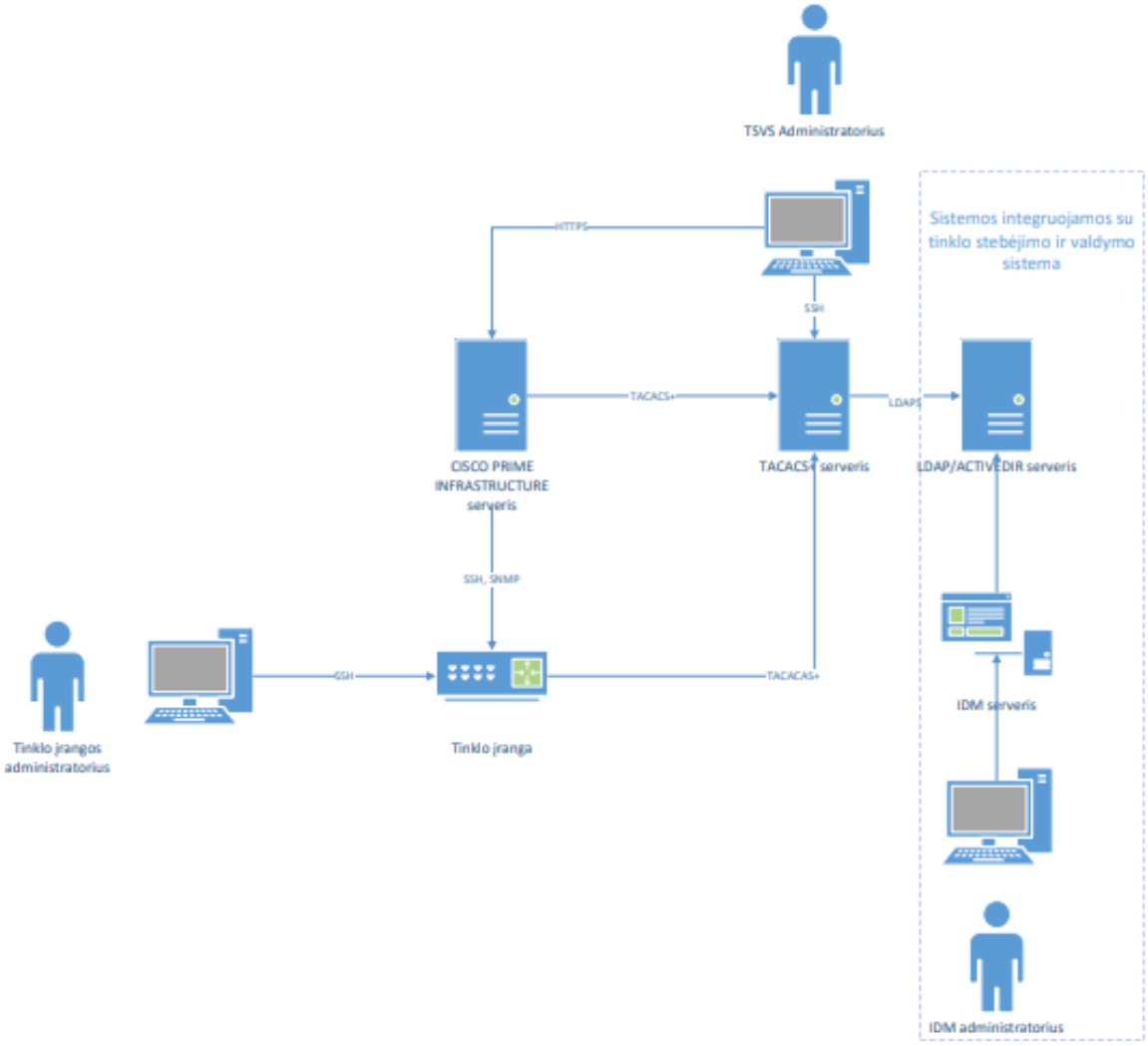
Paslaugos tikslai:

- 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.

Paslaugos platformos architektūra

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 schema

Sistemos komponentų paskirtis ir funkcijos

Tapatybių registravimo sistema skirta LITNET bendruomenės nariams užregistruoti, suteikti prieiga prie el. paslaugų ir jas valdyti.

LDAP/ACTIVEDIR serveris - sistema skirta saugoti el. tapatybės duomenis

Aukščiau aprašytos sistemos yra tik pagalbinės tinklo įrenginių valdymo ir stebėjimo sistemos komponentės, kurios nebuvo sukurtos šiame projekte. Tinklo valdymo ir stebėjimo sistema integruojasi su šiomis sistemomis.

Autentifikacijos, autorizacijos, įvykdytų komandų registravimo sistema TACACS+

Šiame projekte buvo panaudota atviro kodo TACACS+ protokolo realizacija Pro Bono Publico. Operacinė Sistema pasirinkta Ubuntu Linux server.

Šis serveris atlieka tinklo įrenginių administratorių:

- autentifikaciją t.y. patikrina ar suvesti prisijungimo duomenis yra teisingi.
- Autorizacija – patikrina ar šis administratorius turi teises jungtis prie šio įrenginio. Taip pat gali tikrinti, ar jam yra leidžiama atlikti tam tikrą komandą įrenginyje.
- Įvykdytų komandų registravimas. Gali saugoti tinklo įrenginiuose suvestas komandas

Cisco prime infrastructure tinklo stebėjimo ir valdymo sistema.

Pagrindinės šios sistemos funkcijos yra:

- 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 apibendrintos statistikos pateikimas
- Automatinis tinklo topologijos atvaizdavimas
- Tinklo įrenginių konfigūracijų rinkimas ir saugojimas
- Masinis tinklo įrenginių konfigūracijų keitimas
- Centralizuotas tinklo įrenginių programinės įrangos atnaujinimas

Tinklo stebėjimo ir valdymo sistemos veikimas

Registruotam tapatybių valdymo sistemoje tinklo įrenginių administratoriui suteikiamas prisijungimo vardas ir slaptažodis kurį jis gali keisti. Tinklo įrenginio administratorius sukonfigūruoja TACACS+ protokolo naudojimą, SNMP protokolo prisijungimo duomenis savo tinklo įrenginiuose. Po šios procedūros tinklo įrenginių administratorius galės jungtis prie tinklo įrenginių naudodamas tapatybių valdymo sistemos suteiktą vieningą prisijungimo vardą ir slaptažodį. Šie prisijungimo duomenis taip pat bus naudojami jungiantis prie Cisco Prime Infrastructure.

Prieiga prie tinklo įrenginių, komandų autorizacija, ir įvykdytų komandų registravimas pilnai gali būti valdomas TACACS+ serverio. Administratoriui jungiantis tiesiogiai prie tinklo įrenginio SSH protokolu, tinklo įrenginys autentifikuoja naudotoją, autorizuoja vykdomas komandas ir jas registruoja komunikuodamas su TACACS+ serveriu.

TACACS+ serveryje gali būti atlikti tokie nustatymai:

- Administratoriaus paskiros galiojimo pabaigos laikas

- Laikotarpis kurio metu galima jungtis prie įrenginio (pvz., 08:00-17:00)
- Privilegijų lygis (0-15)
- Leidžiamų vykdyti komandų sąrašas
- Pasveikinimo užrašas (sėkmingai prisijungus prie įrenginio)
- Leidžiamų IP adresų sąrašas iš kurių galima prisijungti prie įrenginio
- Įrenginio IP adresas iš kurio jis kreipsis į TACACS+ serverį

Tinklo valdymo ir stebėjimo sistemos Cisco Prime Infrastructure pagrindiniai stebimi parametrai renkami naudojant SNMP protokolą, o įrenginiai valdomi naudojant SSH protokolą. Tinklo įrenginiai gali siųsti savo sisteminius įvykius į tinklo valdymo ir stebėjimo sistemą Syslog formatu, pagal juos tinklo stebėjimo ir valdymo sistema gali generuoti įspėjamuosius pranešimus. Tinklo srautas gali būti stebimas pagal iš įrenginių gaunama NETFLOW informaciją. Prisijungimo duomenis gali naudoti TACACS+ serveryje sukurto vartotojo.

Informacijos saugojimas

Surinkta iš tinklo įrenginių informacija (kokybės parametrai, konfigūracijos, sisteminių žurnalų įrašai, IP paketų statistiniai duomenis) saugomi LITNET VU techninio centro 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.

Paslaugos naudojimo sąlygos

Tinklo stebėjimo ir valdymo paslauga gali naudotis LITNET tinklo administratoriai, savo administruojamuose įrenginiuose sukonfigūravę TACACS+ protokolą autentifikacijai, autorizacijai ir komandų registravimui. Tinklo įrenginyje turi būti nustatyti 2 TACACS+ serveriai: t1.local.vu.lt, t2.local.vu.lt

Paslauga užsakoma užpildant užsakymo elektroninę formą.

Paslaugos administravimas aprašytas dokumente:
„Tinklo stebėjimo ir valdymo paslauga. Paslaugos administratoriaus instrukcija.“

Paslaugos naudojimas aprašytas dokumente:
„Tinklo stebėjimo ir valdymo paslauga. Paslaugos naudotojo instrukcija.“

Paslaugos naudojimo sąlygos:

- Tinklo stebėjimo ir valdymo paslaugos naudotoju gali būti mokslininkai, tyrėjai bei LITNET tinklo administratoriai.
- Tinklo administratoriai turi sukonfigūruoti tacacs+ protokolą savo įrenginiuose
- Tinklo stebėjimo ir valdymo sistemos surinkti tinklo įrenginių duomenys saugomi 6 mėnesius
- Paslaugos naudotojas gali peržiūrėti ir gauti informacija tik apie jo administruojamus įrenginius
- Paslaugos naudotojas įsipareigoja laikytis LITNET Tinklo naudojimo taisyklių (https://www.litnet.lt/index.php/lt/tnt).