KAUNO TECHNOLOGIJOS UNIVERSITETAS

INFORMATIKOS FAKULTETAS

KOMPIUTERIŲ KATEDRA

Waldemar Wołyniec

Grid monitoringo sistema

Magistro darbas

Darbo vadovas

doc. dr. G. Vilutis

Kaunas, 2010

KAUNO TECHNOLOGIJOS UNIVERSITETAS

INFORMATIKOS FAKULTETAS

KOMPIUTERIŲ KATEDRA

Waldemar Wołyniec

Grid monitoringo sistema

Magistro darbas

Recenzentas

doc. dr. Gediminas Činčikas

2010-05-26

Vadovas

doc. dr. G. Vilutis

2010-05-26

Atliko

IFN-8/3 gr. stud.

Waldemar Wołyniec

2010-05-26

Kaunas, 2010

Turinys

Įvadas

Sparčiai plintant *GRID* tinklui labai svarbiu aspektu tampa informacijos perdavimo *GRID* tinkle saugumas ir jo užtikrinimo būdai. Informacijos perdavimo srautas kai kuriose sistemose užtikrinamas panaudojant autentifikaciją ir autorizaciją, tačiau norint saugiai naudotis *GRID* tinklo teikiamomis galimybėmis itin svarbu yra pasirinkti tinkamą, stabilumu pasižyminčią ir turinčią visas reikalingas savybes monitoringo sistemą.

GRID monitoringo sistemų paskirtis - pateikti vartotojui konkrečią informaciją apie *GRID* tinklo veiklą bei parodyti atliekamų darbų skaičių ir laukiančių eilėje darbų skaičių, klasterio atminties užimtumą ir laisvumą bei daugelį kitokių parametrų. Šie parametrai turi būti parodyti vaizdžiai ir aiškiai. Vartotojui svarbu, kad jo užduotis *GRID* tinkle būtų atlikta greitai bei užtikrintų duomenų saugumą (t.y. kad jo duomenys nebūtų prarasti, neteisėtai pasisavinti ar sugadinti). Monitoringo sistemos pagalba vartotojas gali sužinoti, kuris klasteris jo užduotį atliks greičiau. *GRID* monitoringo sistemos funkcionalumas priklauso nuo to, kokius parametrus ji vaizduoja. Kuo daugiau reikalingų parametrų monitoringo sistema parodo, tuo vartotojui lengviau teisingai pasirinkti *GRID* tinklą ar klasterį, kuris jo užduotį atliks greičiausiai.

Sukurta daug LAN/WAN monitoringo sistemų, tačiau tik dalis yra skirtos būtent *GRID* tinklui. *GRID* monitoringo sistemos nuo tinklo parametrų stebėjimo sistemų skiriasi tuo, kad *GRID* monitoringo sistemai aktualūs ne tik tinkliniai parametrai, bet ir aparatūrinės įrangos apkrovimas, resursų būklė ir t.t. Dauguma tinklo stebėjimui sukurtų sistemų to padaryti negali. Iš *GRID* tinklui skirtų naudoti monitoringo sistemų bus apžvelgtos *MonALISA, Ganglia, GridIce, GridView* bei *Nagios* sistemos. Šių monitoringo sistemų pasirinkimą lėmė, kad tai vienos iš plačiausiai naudojamų monitoringo sistemų *GRID* tinkluose.

Darbo objektas ir sritis

Magistriniame darbe ištirti *GRID* monitoringo sistemų pažeidimai, atsiradę dėl naudojamų technologijų trūkumų. Taip pat pateikiama sistemų struktūros analizė, nurodomi trūkumai ir privalumai bei trūkumų pašalinimo būdai.

Darbo objektas – informacinių sistemų saugumo technologijos, kurios naudojamos stebėjimo sistemose. Aptariamos esamų *GRID* monitoringo sistemų panaudotų saugumo elementų privalumai ir trūkumai.

Darbo tikslas ir uždaviniai

Darbo tikslas - panaudoti tinkamus metodus, kurių dėka galima sukurti saugią *BalticGrid* monitoringo sistemą, užtikrinančią informacijos autentiškumą, vientisumą bei konfidencialumą. Itin svarbu įsisavinti žinias apie naudojamus saugumo standartus bei pakelti kuriamos monitoringo sistemos saugumą. Magistrinio darbo praktinė užduotis - sukurti saugią *BalticGrid* tinklo monitoringo sistemą.

Uždaviniai:

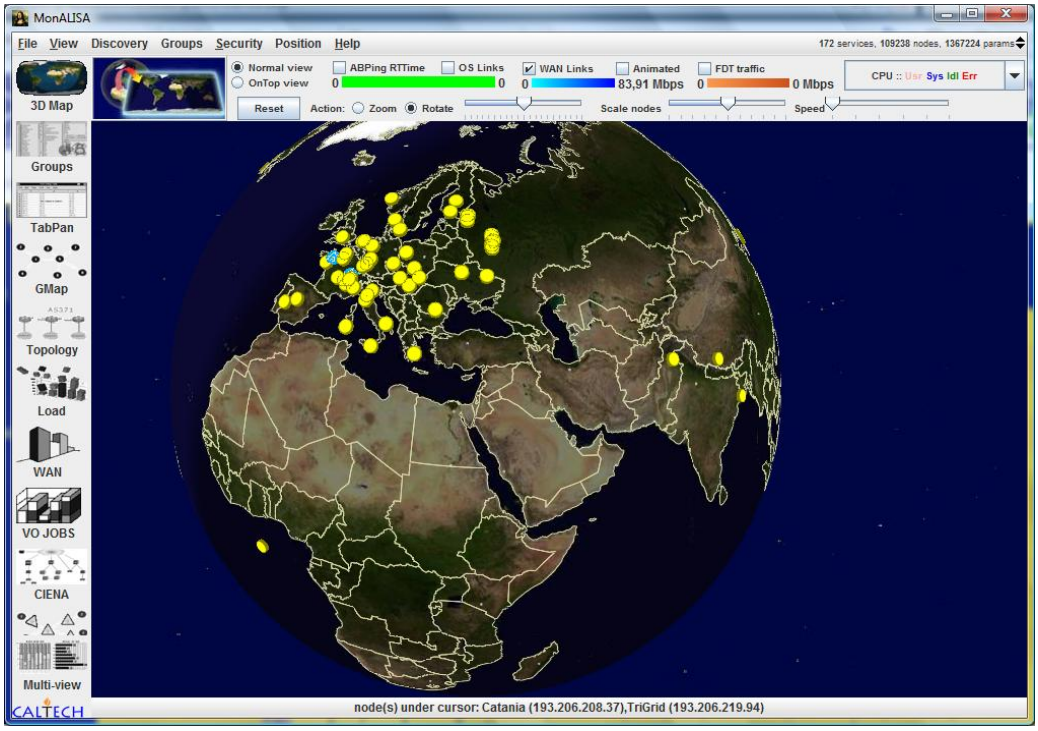
- apžvelgti esamas *GRID* monitoringo sistemas saugumo atžvilgiu, nurodyti jų privalumus ir trūkumus;
- išsiaiškinti būtinus saugumo kriterijus, kurie turi būti taikomi monitoringo sistemose;
- aptarti sistemų architektūras ir pasiūlyti tinkamiausią architektūrą šiuolaikiniam *GRID* tinklo stebėjimui;
- sukurti saugią *BalticGrid* tinklo parametrų stebėjimo sistemą;
- nustatyti, ar kinta sistemos veikimas, naudojant saugumo priemones.

1. *GRID* monitoringo sistemų analizė

Analizės dalyje aptariamos populiariausios *GRID* monitoringo sistemos. Pagrindinis dėmesys skiriamas saugumo nustatymui, sistemų architektūrų pristatymui bei vaizduojamų parametrų analizei.

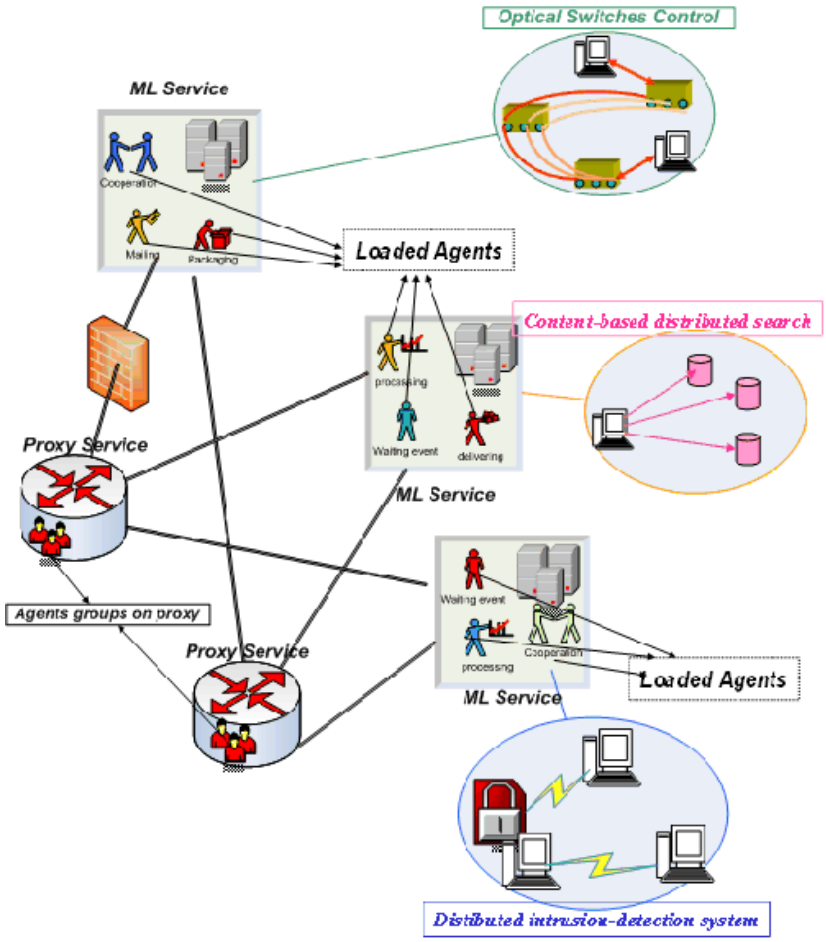
1.1. Populiariausios GRID tinkluose naudojamos monitoringo sistemos

Pačios populiariausios ir turinčios daugiausiai galimybių *GRID* tinklo stebėjimo sistemos yra šios: *MonALISA, Ganglia, GridIce, GridView* bei *Nagios (1,3,5,7,9 pav.).*



1 pav. MonALISA stebėjimo sistema

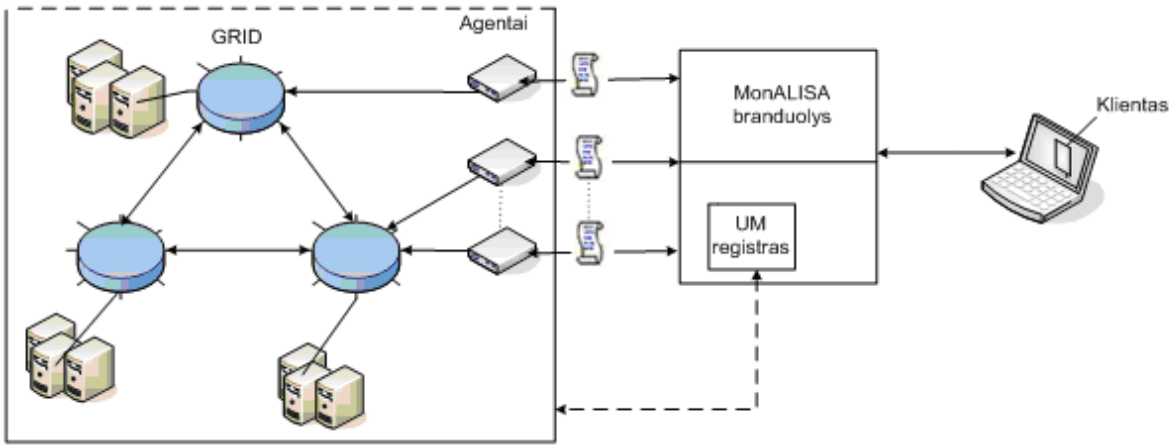
MonALISA stebėjimo sistema (1 pav.) skirta stebėti realiu laiku vykstančius procesus *GRID* tinkle ir matyti esamą *GRID* tinklo situaciją, resursų parametrus. Naudojant šią stebėjimo sistemą patogu lyginti skirtingų klasterių parametrų reikšmes, nes šiam tikslui specialiai įdiegtas įrankis. Siekiant patobulinti plačiai išdėstytų realaus laiko aplikacijų veikimą, *MonALISA* užduočių atlikimui naudoja specialius agentus. Šie agentai komunikuoja žinutėmis, naudodami greitą, patikimą, keičiamo dydžio ir saugią agentų platformą, integruotą su *MonALISA* konstrukcija (framework) (2 pav.) [1]. Nauji agentai, kurie apdoroja monitoringo paslaugos sukauptą informaciją, gali būti lengvai sukuriami ir įdiegti į paskirstytą sistemą. TCP susijungimai tarp monitoringo paslaugų ir visų proxy paslaugų sudaro sąlygas patikimam komunikavimui tarp agentų.



2 pav. MonALISA Agentų Platformų Komunikacija

Agentai yra išdėstomi pagal monitoringo paslaugas ir identifikuojami pagal jų vardus. Jie komunikuoja naudodami TCP susijungimus tarp proxy ir monitoringo paslaugų. *MonALISA* sistemos agentai yra klasifikuojami į grupes. Šį klasifikavimą valdo proxy paslauga. Agentai gali būti grupuojami pagal aplikaciją, kurią jie bando pasiekti.

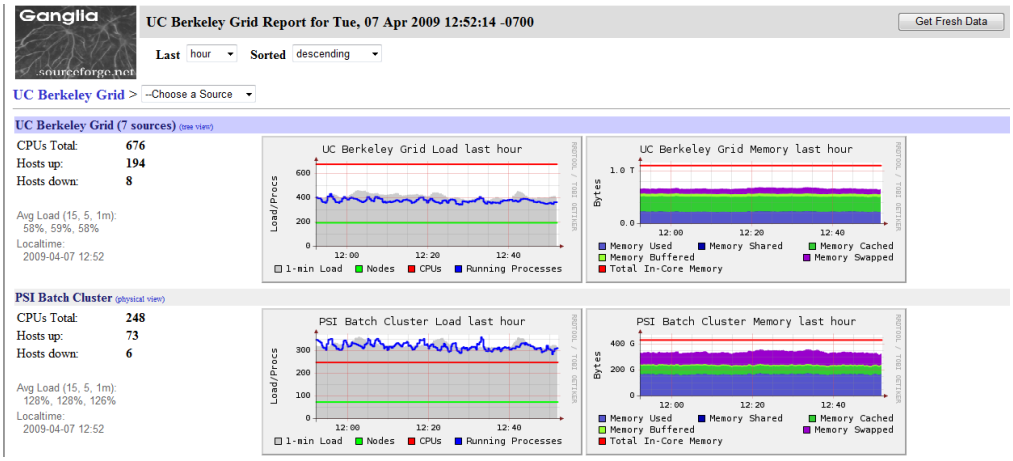
MonALISA stebėjimo sistemos trūkumas tas, kad matomi tik savaitės senumo duomenys.



3 pav. MonALISA architektūra

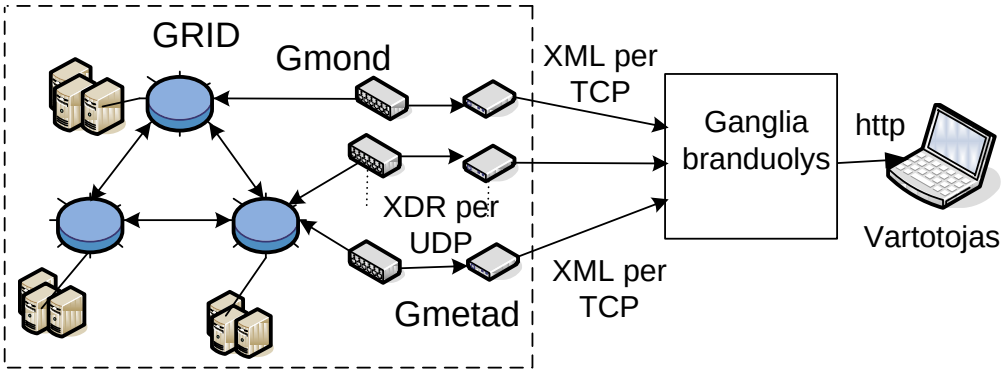
Pagal pateiktą *MonALISA* architektūrą (3 pav.) matome, kad *MonALISA* branduolys su agentais jungiasi saugiu ryšiu, panaudojant sertifikatus. Agentai komunikuoja su *GRID* tinklo klasteriais, iš kurių paima ir pateikia vartotojui visus tinklo parametrus.

Ganglia [2] stebėjimo sistema (4 pav.) skirta stebėti kompiuterių tinklo bei jo mazgų parametrus. Jos pagalba matomi tinklo mazgų esamų resursų parametrai, jų apkrova bei kiti istoriniai techninių parametrų duomenys.



4 pav. Ganglia stebėjimo sistema

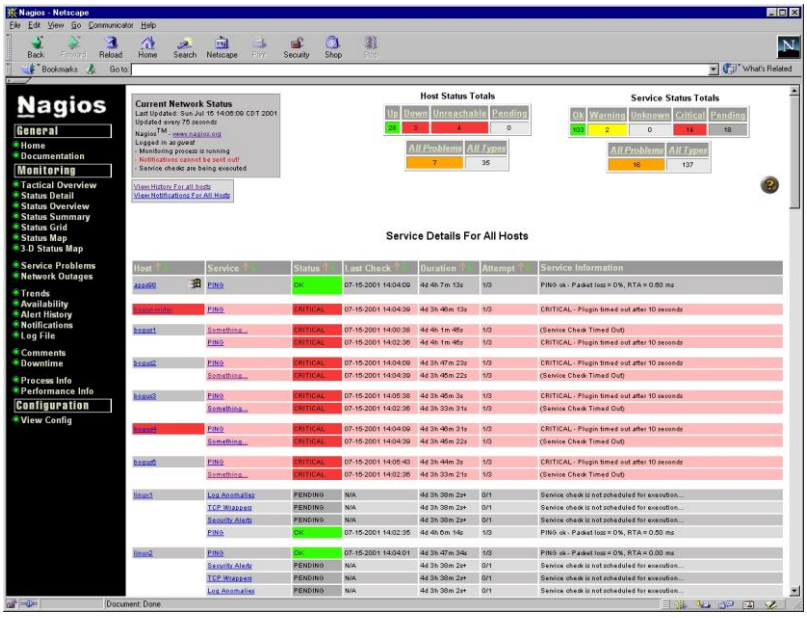
Ganglia vaizduoja svarbiausius parametrus: procesorių spartą, tinklo apkrovą, disko talpą ir pan. *Ganglia* taip pat suteikia informaciją apie operacines sistemas ir kompiuterinę įrangą. *Ganglia* monitoringo sistemoje stebėjimą galima pradėti nuo sistemos paleidimo iki to momento, kada buvo atidarytas monitoringo sistemos langas, ar iki momento, kol buvo įjungti duomenų rinkimo moduliai. Taigi, sistema suteikia galimybę stebėti viso duomenų kaupimo laikotarpio duomenis. Keletas *Ganglia* privalumų: ji jau įdiegta klasteriuose kaip klasterių paskirstymo dalis, lengvai atliekama priežiūra, yra intuityvi tinklo sąsaja ir sąveika su MDS (Monitoring and Discovery Service). *Ganglia* trūkumas yra tas, kad šioje sistemoje nėra daviklio valdymo ir saugumo. *Ganglia* naudojama kaip pavienė sistema ir integruojama su MDS. Ji naudoja standartines technologijas, tokias kaip XML – duomenų pavaizdavimui, XDR – kompaktiškam, kilnojamam informacijos transportavimui ir RRD (Round Robin Database) įrankį - informacijos saugojimui ir vaizdavimui.



5 pav. Ganglia architektūra

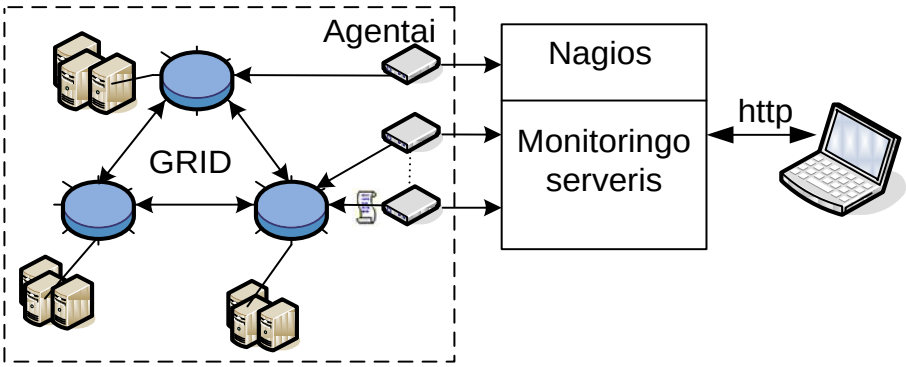
Pateiktoje (5 pav.) Ganglia architektūroje matome, jog sistemos branduolys su *GRID* tinklu komunikuoja neapsaugotu ryšiu. *GRID* tinklo parametrai perduodami XML dokumentais nesaugiu TCP protokolu.

Nagios [3] stebėjimo sistema (6 pav.) skirta stebėti kompiuterių tinklo bei jo mazgų parametrus. Jos pagalba stebimi tinklo mazgų esamų resursų parametrai, jų apkrovų bei kitų techninių parametrų istoriniai duomenys, pavyzdžiui: procesorių sparta, tinklo apkrova, disko talpa ir pan.



***6* pav. Nagios stebėjimo sistema**

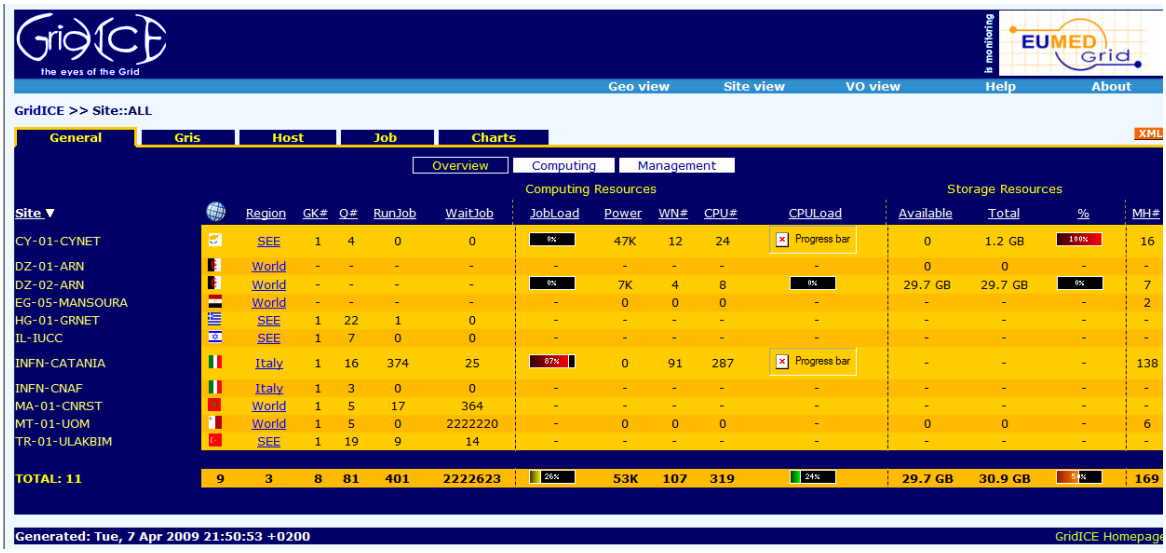
Šioje monitoringo sistemoje taip pat kaupiami visi istoriniai duomenys, pradedant tuo momentu, kuomet sistema buvo paleista.



7 pav. Nagios architektūra

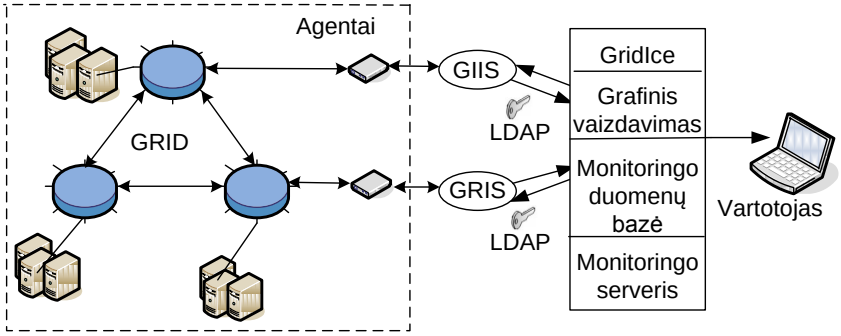
Nagios monitoringo sistema yra atviro kodo, vartotojai patys gali prisitaikyti sistemą savo poreikiams. Norint apsaugoti taip pat galima nustatyti norimą saugumo būdą.

GridIce [4] (8 pav.) stebėjimo įrankis suprojektuotas atsižvelgiant į reikalavimus, kuriuos pateikė įvairių tipų vartotojai, dirbantys skirtinguose *GRID* abstrakcijos lygmenyse: virtualios organizacijos, *GRID* operacijų centro, puslapio administravimo ir galutinio vartotojo.



8 pav. GridIce stebėjimo sistema

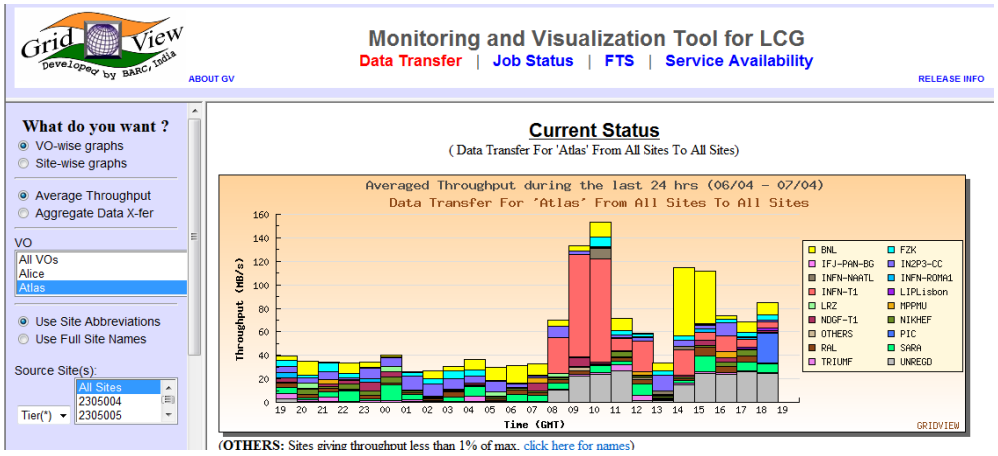
GridIce kaupia istorinius duomenis nuo pat sistemos paleidimo pradžios (8 pav.), taigi vartotojas gali apžvelgti visus sistemoje sukauptus istorinius duomenis.



9 pav. GridIce architektūra

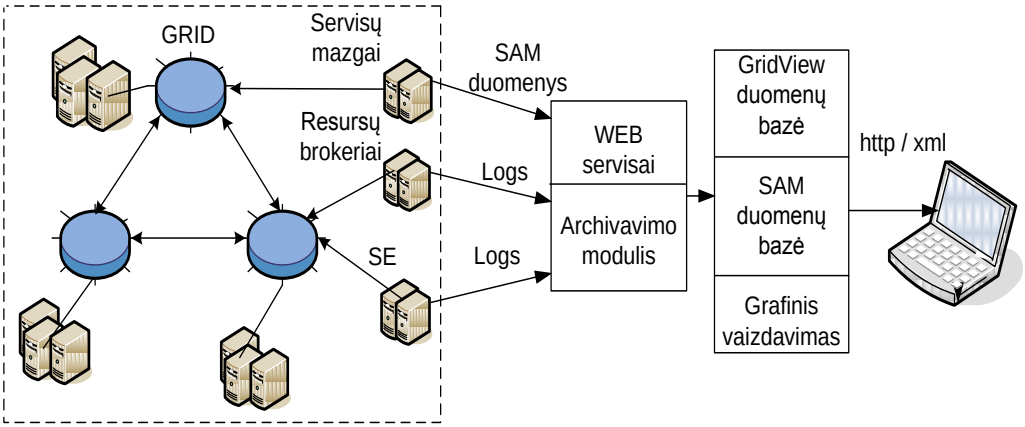
Gridlce sistema prie GRID tinklo jungiama per GIIS ir GRIS servisus. Servisai su sistema bendrauja LDAP protokolu, kuris užtikrina duomenų saugumą.

GridView [5] - tai keičiamo masto, įvairiarūšė ir dinaminė *GRID* monitoringo sistema. Ji turi daug privalumų: išsamų skaičiavimo pajėgumo modelį, masinių duomenų valdymo mechanizmus ir masinių duomenų vizualizacijos techniką. *GridView* (10 pav.) yra *GRID* monitoringo sistema, kuri renka informaciją apie naudojamus išteklius iš įvairių *GRID* mazgų. *GridView* projektas neskirtas veikti su kitomis programomis. Vaizdiniam informacijos pateikimui *GridView* naudoja masinių duomenų vizualizacijos techniką ir pateikia keturis vaizdų tipus: statinius, dinaminius, paskirstytus ir duomenų palyginimo.



10 pav. GridView stebėjimo sistema

Šioje sistemoje taip pat kaupiami duomenys nuo sistemos gyvavimo pradžios stebimame tinkle, tačiau maksimalus laikotarpis, kurį vienu metu gali apžvelgti vartotojas, yra 900 valandų.



11 pav. GridView architektūra

GridView sistemos architektūra pavaizduota 11 pav. *GRID* tinklo duomenys į sistemą perduodami iš WEB servisų arba archyvavimo modulio. Duomenis surenka Resursų brokeriai. Duomenų perdavimo saugumas nėra užtikrintas.

1.2. Sistemų aptarimas ir palyginimas

Visos aptariamos sistemos sudarytos panašiu architektūriniu principu. Vartotojas jungiasi prie centrinio serverio, kuriame kaupiami istoriniai ar realaus laiko duomenys. Centrinis serveris jungiasi prie agentų arba *GRID* informacijos servisų, kad rinktų ir kauptų duomenis. Labiausiai iš šių sistemų veikimo principo išsiskiria tik *MonALISA*. Jei nori prie jos prisijungti, vartotojas privalo atsisiųsti į savo naršyklę vartotojo sąsają. Šios sistemos veikimas paremtas „storo kliento“ (*angl. fat client*) modeliu. Tai turi ir savų pliusų - šis veikimo modelis nuolat atnaujina ryšį su centriniu serveriu ir vartotojo matomą informaciją realiu laiku. Šios galimybės neturi kitos aptariamos sistemos. Išskirtinis bruožas tas, kad *MonALISA* pati pasirūpina saugiu ryšiu tarp vartotojo sąsajos ir centrinio serverio, nes duomenys iš kliento į sistemą keliauja koduotu *X.509* protokolu. Skirtingai nei *MonALISA*, tačiau labai panašiai, tarpusavyje „plono kliento“ modeliu (*angl. thin client*) veikia *Ganglia, Nagios, GridView* ir *GridIce*. Vartotojas per naršyklę jungiasi prie centrinio web serverio, kuris sugeneruoja vartotojo sąsają. Kitas žingsnis - *Ganglia* ir *MonALISA* centriniai serveriai jungiasi prie agentų, kurie šioms sistemoms teikia informaciją, *Nagios* agentai patys siunčia informaciją į centrinį serverį, o agentai jungiasi prie *GRID* mazgų ir renka jų duomenis. *GridView* sistema jungiasi prie *webserviso*, kuris iš duomenų archyvo pasiima jai reikalingą informaciją, o duomenų archyvavimo modulis renka informaciją iš resursų brokerio bei *GRID* mazgų. *GridIce* centrinis serveris naudodamasis *LDAP* protokolu jungiasi prie *GRIS* (*Grid Resource Information Service*) ir *GIIS* (*Grid Index Information Service*). Šiose dviejose -*GIIS* ir *GRIS* - sistemose pateikiama pagrindinė GRID informacija, kurią vartotojui ir pateikia *GridIce.*

Kadangi dėl klasterių ir teikiamų duomenų įvairovės sunku sukurti vieningą duomenų perdavimo struktūrą, *GridView* pritaiko perdavimą tarp klasterio informacijos tinklo sąsajos sluoksnio ir *GRID* informacijos valdymo sluoksnio *XML* standartu.

Įmanoma būtų sukurti stebėjimo sistemą, kuri iš *Ganglia, Nagios, GridView* ir *GridIce* rinktų ir saugotų teikiamą informaciją pas save. Tai galima atlikti dėl to, kad šios sistemos veikia „plono kliento“ modeliu, tačiau *MonALISA* stebėjimo sistemos duomenų taip rinkti nepavyktų, nes, kaip aptarėme anksčiau, ji veikia „storo klieno“ modeliu, ir centrinis serveris nesuteikia vartotojui ar sukurtai sistemai galutinai sugeneruoto rezultato.

Saugumo atžvilgiu *MonALISA* - viena iš labiausiai į saugumą orientuotų monitoringo sistemų. Į vartotojo kompiuterį atsiųsta vartotojo sąsaja sukuria su centriniu serveriu saugų ryšį, pagrįstą sertifikatais ir X.509 [6] protokolu. Tokį pat saugų koduotą ryšį centrinis serveris palaiko ir su agentais, kurie renka informaciją iš *GRID* mazgų. Tokiu būdu *MonALISA* visiškai apsaugota nuo pašalinių vartotojų ar programinės įrangos įsiterpimo tarp vartotojo ir monitoringo duomenų. *Nagios*, kaip ir *Ganglia* ar *GridView*, nenaudoja saugių ryšių, išskyrus atvejus, kai naudojami

vartotojo sukurti specialūs „įskiepiai“ į agentus, kai stebimi parametrai (tokie kaip uždavinių eilės klasteryje, laisvi resursai ir t.t.), kuriems reikalinga *GRID* autentifikacija. *Ganglia* agentai TCP tinklu transliuoja informaciją XML formatu, kurią gali rinkti ne tik *Ganglia* sistema, bet ir kitos programos ar vartotojai. Užtenka sukurti programinę įrangą, kuri kreiptųsi į *Ganglia* agentus tam tikrais *Ganglia* naudojamais prievadais, ir agentai pateiktų visus, išskyrus istoriją, *Ganglia* sistemai skirtus duomenis. Tokiu būdu šie parametrai galėtų būti kaupiami ir kitos sistemos, kuriai neskirti duomenys, ar *Ganglia* sistemai galėtų būti retransliuojami pakeisti duomenys. *Nagios* nenaudoja saugių sesijų tarp vartotojo ir sistemos. Agentai, kurie teikia informaciją sistemai, gali naudoti autentifikuotus prisijungimus prie *GRID*, kad galėtų rinkti specifinius parametrus, kurie neteikiami viešai. Ilgiau stebint tinklą (pvz.: *snifer* ir panašiomis programomis), nesudėtinga perimti teikiamo agento paslaugas ir teikti centriniam serveriui neteisingą informaciją. *GridIce* vartotojai prie sistemos jungiasi nesaugiu ryšiu, tačiau sistema, jungdamasi prie *GRID* informacijos rinkimui, naudojasi *LDAP* protokolu, kuriame dažniausiai autentifikavimas nėra vykdomas, nors galimas. Šis būdas apsaugotų informaciją nuo trečiųjų asmenų ar programinės įrangos įsiterpimo tarp teisingos informacijos ir vartotojo.

Straipsnyje „CRO-GRID *Grid Monitoring Architecture”* [2] aptariami *GRID* tinklo standartai, reikalavimai monitoringo sistemoms bei sistemų architektūra. Apžvelgiamos populiariausios monitoringo sistemos, tokios kaip *Ganglia, NWS, MonALISA* ir kt. Straipsnyje nurodyta sistemos architektūra parodo, kokie elementai yra būtini kuriant saugią *GRID* monitoringo sistemą.

Straipsnyje trumpai pateikiamos nagrinėjamų sistemų saugumo užtikrinimo galimybės, išryškinami kiekvienos sistemos privalumai ir trūkumai, tinkamumas konkrečioms sąlygoms.

Nors egzistuoja daug gerai apgalvotų sistemų, tačiau nė viena iš jų neturi tokio sprendimo, kuris patenkintų visus reikalavimus, būtinus efektyviam Grid monitoringui. Straipsnio tikslas - nurodyti Grid monitoringo architektūras, kurios atitinka CRO-GRID reikalavimus. Šiuo straipsniu autoriai siekia supažindinti su esamų sistemų integravimu, priemonėmis monitoringo komponentų valdymui, integruojant ir praplečiant duomenų archyvavimo galimybes bei kuriant tinklo sąsają, skirtą valdymui.

Po išsamios daugelio *GRID* monitoringo sistemų peržiūros, straipsnio autoriai išrinko sistemas, kurios patogiausios reikalingos informacijos naudojimui ir pateikimui. Tinkamiausios *GRID* monitoringo sistemos yra: *Ganglia, NWS, INCA ir MDS*. Vienas iš *Ganglia* privalumų, kad ji jau įdiegta klasteriuose kaip klasterių paskirstymo dalis, lengvai prižiūrima, turinti intuityvią tinklo sąsają ir sąveiką su *MDS* (Monitoring and Discovery Service). Įdiegta centrinė Gmetad, todėl naudojama tinklo sąsaja ir duomenų archyvavimas. *Ganglia* trūkumas tas, kad šioje sistemoje nėra

daviklio valdymo ir saugumo. *Ganglia* naudojama kaip pavienė sistema ir integruojama su *MDS*. *NWS* privalumams priskiriamas daviklių valdymas, interneto monitoringas, elgsenos prognozės bei integravimas su vykdomąja valdymo sistema. Šiuo metu *NWS* naudojama kaip pavienė sistema, nes vykdymo valdymas negali jos panaudoti kaip *MDS* dalies. Ateityje planuojama ją visiškai integruoti į *MDS*. *INCA* leidžia patikrinti programinės įrangos instaliavimą ir *GRID* vidinių sluoksnių paslaugas. *MDS* yra faktinė standartinė informacijos valdymo sistema. *MDS* privalumai: hierarchinis informacijos valdymas, išplėstinumas ir integravimas su daugeliu monitoringo sistemų bei Globus GSI saugumo sistema. Tačiau *MDS* turi efektyvumo problemų, pavyzdžiui, ji turi būti apdairiai sukonfigūruota - tokiu būdu, kad būtų pateikiami tik naujausi duomenys. Duomenų apibūdinimui *MDS* planuojama panaudoti *GLUE* informacijos schemą.

Straipsnyje siekiama aprašyti, kokios yra tinkamiausios *GRID* monitoringo sistemos, ir supažindinti, kokius saugumo metodus naudoja ir ar naudoja skirtingos monitoringo sistemos. Straipsnyje aiškiai išvardinti sistemų privalumai, taip pat surasti trūkumai bei įvardinti siekiai, kuriuos bandoma įgyvendinti.

Kitas straipsnis „*GridView: A Dynamic and Visual Grid Monitoring System*“ [5] aprašo pagrindinius *GridView* monitoringo sistemos elementus. Pateikiama sistemos architektūra, kuri suskirstyta į atskirus sluoksnius. Pavaizduoti ir aprašyti duomenų rinkimo, informacijos kaupimo, duomenų atvaizdavimo bei klasterio informacijos sluoksniai. Straipsnyje pateikta ne tik *GridView,* bet ir *Ganglia* monitoringo sistemų duomenų perdavimo standartai bei naudojami protokolai.

Šio straipsnio tikslas - trumpai supažindinti skaitytoją su *GRID* veikimo principais. Taip pat argumentuojamas *GridView* sistemos pasirinkimas aprašomai sistemai.

GRID tinklas sudarytas iš įvairių geografiškai išskirstytų išteklių dideliame virtualiame kompiuteryje ir turi galimybę dalintis ištekliais, kaip skaičiavimo, saugojimo, informacijos ar žinių. *GRID* tikslas – leisti vartotojams skaidriai naudotis išteklių rinkiniais bei lengvai ir efektyviai gauti norimą informaciją. Šiam tikslui plačiai naudojami „gridai“: skaičiavimo *GRID*, duomenų *GRID* ir informacijos *GRID*.

GRID sėkmė daugiausiai priklauso nuo efektyvaus šių išteklių panaudojimo. *GRID* tinklui monitoringas yra būtinas. Kai kurios monitoringo sistemos jau gali rinkti informaciją, jos yra efektyvios, keičiamo dydžio ir žemo poveikio. Bet daugelis jų neatsižvelgia į dinamiškas ir didelio masto charakteristikas. Šių aspektų nagrinėjimas ir tampa pagrindine problema.

Šiame darbe pristatomas *GridView*, kuris gali stebėti ir kaupti informaciją bei įgyti prisijungusių išteklių statusą. *GridView* - tai keičiamo masto, įvairiarūšė ir dinaminė *GRID* monitoringo sistema. Ji turi ir daugiau savybių, pavyzdžiui, išsamus skaičiavimo pajėgumo modelis, masinių duomenų valdymo mechanizmas ir masinių duomenų vizualizacijos technika.

GridView yra *GRID* monitoringo sistema, kuri renka informaciją apie naudojamus išteklius ir įvairių *GRID* mazgų konfigūraciją iš žemo lygio duomenų rinkimo sistemų. Šiame darbe pateikiama jos architektūra bei įdiegimas, kurį sudaro informacijos suradimo sąsajos lygis, blokinio informacijos tinklo sluoksnis, *GRID* informacijos valdymo sluoksnis ir *GRID* vaizdo sluoksnis. Pateikiami keli projektavimo klausimai, įskaitant keturių pakopų struktūrą, išsamų skaičiavimo pajėgumo modelį, masinių duomenų valdymo mechanizmą bei masinių duomenų vizualizacijos techniką.

GridView projektas nėra skirtas veikti su kitomis programomis. Vaizdiniam informacijos pateikimui ir lengvam norimos informacijos perdavimui administratoriui *GridView* naudoja masinių duomenų vizualizacijos techniką ir pateikia keturis vaizdus: statinius, dinaminius, paskirstytus ir duomenų palyginimo vaizdus.

Straipsniu siekiama, kad skaitytojas galėtų lengviau nuspręsti rinkdamasis monitoringo sistemą, žinotų kriterijus, pagal kuriuos verta nagrinėti sistemos tinkamumą konkrečiu atveju. Straipsnio autoriai gerai paaiškino *GRID* tinklo veikimo principus ir pateikė *GridView* monitoringo sistemos galimybes, veikimą bei duomenų vaizdavimo būdus.

Straipsnyje *„List of Quality Attributes for Grid Monitoring Tools”* [7] aptariami ir palyginami devyni *GRID* monitoringo įrankiai. Iš jų 5 neatitinka aukščiausios kokybės reikalavimų.

1 lentelė. Kokybės užtikrinimo parametrai

Nr.	QA\kokybės užtikrinimas	Ganglia	Kadmin	RMT	Parmon	HBM	AV	G&P	NWS	Net Logger
1.	Prieinamumas	+								
2.	Išplečiamumas	+	+	-	+					
3.	Perkeliamumas	+			-					
4.	Patikimumas	*			*	+			+	-
5	Modifikavimas	+						+		
6.	Saugumas						+			
7	Tinkamumas		-				+			

- neigiamas ženklas rodo, kad šio įrankio kokybės užtikrinimas neturi tikslaus pagrindimo architektūriniu požiūriu;

\+ reiškia, jog įrankio visi teiginiai apie kokybės užtikrinimą yra tinkamai įgyvendinti architektūroje;

* reiškia, kad kokybės užtikrinimas yra architektūroje, bet neturi tikslaus apibūdinimo.

Parmon teigia, kad perkeliamumas pasiekiamas Java programinės kalbos dėka. Tai nėra pats geriausias būdas kokybei užtikrinti. Kokybės užtikrinimo architektūra turėtų būti sluoksniuota,

duomenų patikimumas turėtų būti užtikrinamas stebint informaciją skirtinguose *GRID* hierarchijos lygiose: node, grupėje ir klasteryje.

Ganglia patikimumas priklauso nuo klasterio vidinio stebėjimo. Protokolo įdiegimas nėra ryškiai matomas jungties konfigūracijoje.

RAMT yra specifiškai suprojektuotas stebėjimui, sekimui ir klaidų atpažinimui. *RMT* vykdo išplėtimą vadovo/agento pagrindu. Ši architektūra yra analogiška klientui/serveriui.

Kadmin projektas buvo pradėtas norint ištobulinti įrankį, kuris naudotų jau esančius įrankius. *Kadmin* duomenų pateikimui naudoja XML, kad užtikrintų tinkamumą kitai sistemai.

Net Logger teikia duomenų prieinamumą tinkamu lygiu. Prieinamumas glaudžiai susijęs su duomenų patikimumu. Stambūs duomenys yra generuojami host sensorių pagalba ir kaupiami vietiniame diske.

Pagal pateiktus duomenis matome, kad monitoringo sistemos tik iš dalies atitinka šiuolaikinius kokybės užtikrinimo reikalavimus. Kiekviena sistema turi savo privalumų ir trukumų, reikalauja patobulinimų. Kuriant naują sistemą, būtina atsižvelgti į kokybės reikalavimus, kad ta sistema atitiktų kuo daugiau reikalavimų, paminėtų 1 lentelėje.

Reikia pabrėžti, kad parametrai pavieniui nenurodo bendro monitoringo sistemos kokybės lygio, todėl būtina atsižvelgti į kokybinių parametrų visumą, nes tik tada galime daryti išvadas apie sistemos pranašumą kitų sistemų atžvilgiu.

Prieinamumo parametras padeda nustatyti, kaip dažnai šis resursas buvo prieinamas pasirinktu laikotarpiu. Tai leidžia vartotojui sužinoti, kurie resursai yra dažniausiai prienami ir yra pasiruošę atlikti užduotį. (Šį parametrą sugeba parodyti tik *Ganglia* monitoringo sistema). Tuo tarpu išplečiamumo parametras parodo sistemos sugebėjimą surasti naujus resursus ir automatiškai pradėti jų stebėjimą. (Šia savybe pasižymi *Ganglia, Kadmin* bei *Parmon* monitoringo sistemos). Kitas - perkeliamumo parametras - apibūdina sistemos savybę stebėti specifinius resursų tipus ir taip palaikyti jų matomumą *GRID* tinkle. Kiekvienai monitoringo sistemai labai svarbus yra patikimumo parametras, kuris apskaičiuoja tikimybę, kad komponentas atliks jam numatytą užduotį per nustatytą laiką esant tam tikroms aplinkybėms. Jeigu sistemoje dažnai atliekami pakeitimai, svarbus yra modifikavimo parametras, kuris nurodo sistemos galimybę atlikti vienų komponentų pakeitimus taip, kad tie pakeitimai neįtakotų kitų komponentų veikimo. Vienas iš svarbiausių yra saugumo parametras, nusakantis sistemos sugebėjimą apsaugoti laikomus, apdorojamus ir perduodamus duomenis. Visų operacijų, susijusių su saugiais duomenimis, metu būtina laikytis autentiškumo, konfidencialumo ir vientisumo principų. Darbo su tiriama sistema patogumą nurodo tinkamumo parametras. Šie parametrai nurodo svarbiausias savybes, kuriomis turėtų pasižymėti gera ir patikima monitoringo sistema.

1.3. Naudojamos platformos

Skirtingos *GRID* monitoringo sistemos naudoja skirtingas platformas. *Ganglia* monitoringo sistema naudoja gmond ir gmetad demonus duomenų rinkimui, kurie veikia OSX 10.5 platformoje. *Ganglia* galima paleisti daugelyje operacinių sistemų. *Nagios* tai pat naudoja OSX platformą. Nors *Nagios* buvo suprojektuotas veikti Linux operacinėje sistemoje, bet taip pat veikia ir kitose sistemose. *GridIce* [8] naudoja gLite 3.1, Scientific Linux 4 (i386) platformą. *MonALISA* monitoringo sistema naudoja java platformą ir puikiai veikia Windows ir Linux sistemose.

Apžvelgus straipsnius, susijusius su *GRID* monitoringo sistemomis, ir išanalizavus pačias sistemas, pastebėta, kad skirtingos *GRID* monitoringo sistemos stebi ir vaizduoja skirtingus parametrus. Populiariausių monitoringo vaizduojami parametrai pateikti 2 lentelėje.

2 lentelė. Grid monitoringo parametrai

GridView	MonAlisa	GridIce	Ganglia	Nagios
- data transfer	- TabPan	-Region	- CPU total	- Hosts status totals
- jobs	*a) Regional center*	-RunJob	- Hosts Up	*a) Up b) down*
a) VO\State	*b) Hostname*	-WaitJob	- Hosts down	*c) unrachable*
b) Submitted	*c) Local time*	-JobLoad	-Nodes	*d) pending*
c) Waiting	*d) Group*	-WN	- Running processes	*e) All problems*
d) ready	*e) UpTime*	-CPU	- Memory used	*f) All types*
e) Scheduled	*f) Total params*	-CPULoad	- Memory shared	- Service status totals
f) running	*g) CPUTime*	-Available	- Memory cached	*a) Ok b) warrning*
g) done	*h) Master Load*	- Total	- Memory buffered	*c) Unknown d) critical*
h) Aborted	*k) CollectedParams*	-MinSlotFree	- Memory swapped	*e) Pending f) all types*
k) cancelled	*l) Database*	-MaxSlotFree	- Total in-core memory	*g) All problems*
l) NewSumbmitted		-StorageAvailable		- Service status details for all hosts
m) lost		-StorageTotal		*a) Host b) service*
n) total		- StorageLoad		*c) Status d) last check*
				e) Duration f) attemps
				g) Status information

GRID tinklui svarbiausi parametrai, parodantys tinklo galingumą: procesorių skaičius, laisvų ir užimtų procesorių skaičius, atminties kiekis ir paleistų bei laukiančių užduočių skaičius. Šiuos parametrus vaizduoja visos *GIRD* monitoringo sistemos.

1.4. Grid monitoringo saugą galinčios užtikrinti priemonės ir technologijos

GRID monitoringo sistema *MonALISA* vienintelė iš visų stebimų sistemų naudoja saugumo sertifikatus. Šioje sistemoje taikomas sertifikatas X.509 [6] naudoja asimetrinį šifravimą. Sertifikatai naudingi, kai yra būtinybė patvirtinti, jog vartotojas tinkle yra būtent tas, kuo prisistato. Daugelyje kitų sistemų vartotojų sąsajų pasitikima paprastu autentifikavimu įvedant slaptažodį. X.509 leidžia šifruotą abipusę autentifikaciją, remiasi šifravimo raktais, komunikavimo ir vidinio laukų rinkinio, saugančio informaciją apie sertifikato naudotoją. X.509 sertifikatai sukurti taip, kad

juos galima modifikuoti, išplėsti, naudoti esant įvairioms sąlygoms ir saugumo lygiams. Kiekviena X.509 aplikacija gali apimti skirtingus laukus ar priskirti jiems skirtingas reikšmes.

Akivaizdu, kad X.509 sertifikatas nėra tobulas būdas spręsti *GRID* saugumo problemas. Daugelis vartotojų gali norėti prisijungti prie *GRID* paslaugų iš skirtingų vietų, todėl X.509 sertifikatas turėtų būti įdiegtas visuose kompiuteriuose, kuriais vartotojas naudojasi, tačiau tai mažina saugumą. Sertifikatai naudojami, kad sumažintų vartotojų ratą, sistemos duomenimis naudotis gali tik organizacijai priklausantys vartotojai.

1.4.1. Autentifikavimo metodai

Autentifikuodamiesi legalūs vartotojai gauna teisę prisijungti prie tinklo, o nelegalūs – neįleidžiami. Autentifikavimosi būdai:

- autentifikuodamasis vartotojas prisijungia naudodamasis slaptažodžiu ar iš anksto sutarta abiems žinoma informacija;
- autentifikuodamasis vartotojas parodo unikalų fizinį daiktą, pvz., elektromagnetinę kortelę;
- autentifikuodamasis vartotojas identifikuojasi piršto antspaudu, akies rainele ar kita biometrine informacija, saugoma tikrinančiojo duomenų bazėje.

Autentifikavimo algoritmus butų galima suskirstyti į septynis skirtingus metodus:

- *Paprastas slaptažodis* yra paprasčiausias būdas autentifikuoti vartotoją. Klientas neapsaugotu kanalu serveriui pateikia vartotojo vardą ir slaptažodį (pvz., TCP/IP protokolu). Serveris, gavęs šią informaciją, palygina ją su atitikmenimis savo duomenų bazėje ir sutapimo atveju vartotojas autentifikuojamas ir gali prisijungti prie sistemos. Jei serveris vartotojų slaptažodžius laiko nešifruotus, piktavaliams yra paprasta gauti prieigą prie visų vartotojų prisijungimo duomenų, todėl serveryje saugoma informacija koduojama „hash“ algoritmu ir informacija trečiosioms šalims yra neprieinama. Serveris įvedamą vartotojo slaptažodį konvertuoja pagal slaptą „hash“ funkciją ir duomenų bazėje ieško atitikmens.

Toks autentifikavimosi metodas naudojamas be papildomų saugumo priemonių yra labai pažeidžiamas. Yra galimybė „klausytis“ nešifruojamo duomenų srauto, keliaujančio tarp vartotojo ir serverio, arba spėliojimo būdu atsekti slaptažodį.

- *Vienkartinis slaptažodis* iš tiesų yra slaptažodžių sąrašas, iš kurių kiekvienas gali būti panaudotas tik vieną kartą. Šią funkciją gali atlikti ir procesorius ar netgi SecureID kortelė, generuojantys slaptažodžius pagal tam tikrą algoritmą. Šie slaptažodžiai naudojami tik kartą, tad juos saugu siųsti neapsaugotais kanalais. Autentifikavimo serveris, saugodamas paskutinį gautą vartotojo slaptažodį bei kitą to paties vartotojo slaptažodį, „hash“ algoritmo pagalba perskaičiuoja

naują turėtos reikšmės reikšmę, palygindamas ją su gautąja. Reikšmių sutapimo atveju vartotojas autentifikuojmas ir serverio duomenų bazėje senasis slaptažodis pakeičiamas nauju.

- *Užklausos* – atsakymo autentifikavimo būdas, paremtas tuo, kad vartotojas generuoja atsakymą tinklui pasinaudodamas savo slaptažodžiu ar kita informacija. Užklausa paprastai būna atsitiktinė nesikartojanti reikšmė ir yra persiunčiama vartotojui, kuris atsako užklausos ir bendro rakto funkcijos apskaičiuota reikšme. Šis metodas pasižymi tokiomis pačiomis saugumo spragomis, kaip ir paprastojo slaptažodžio metodas.
- Norint padidinti saugumą visų trijų metodų atvejais, galima naudotis *anonimišku raktų apsikeitimu*. Paprastojo slaptažodžio saugumą galima padidinti užšifruojant ir apsaugant nuo pranešimų turinio pakeitimo autentifikacijos duomenų kanalą. Šifravimo raktus abiejoms ryšio seanso dalyvių pusėms nesaugiu kanalu saugiai galima perduoti naudojantis viešo rakto kriptografija. Ryšio seanso pradžioje vartotojas ir serveris apsikeičia viešaisiais raktais ir jais užkoduoja pranešimus. Atkoduodami juos privačiaisiais raktais, ryšio seanso dalyviai neidentifikuoja vienas kito ir neapsaugo nuo apsimetimo kitu vartotoju.
- *Slapto slaptažodžio patvirtinimo* būdas dažniausiai naudojamas vienam ryšio seanso dalyviui siekiant įrodyti savo autentiškumą kitam seanso dalyviui, neišduodant slaptažodžio. Tai padaroma nesaugiu kanalu vietoj paprasto slaptažodžio siunčiant ilgą dvejetainį skaičių. Taip paslepiamas tikrasis slaptažodis nuo jo gavėjo (serverio) ir pastarasis turi pateikti savo slaptažodžio versiją. Abiejų ryšio seansų dalyvių dvejetainių skaičių sutapimo atveju kliento autentifikamasis patvirtinamas.
- *Serverio sertifikatų ir vartotojo autentifikacijos* būdu abu ryšio sesijos dalyviai gali pradėti saugų vienakryptį autentifikavimo kanalą, autentifikuojantis tik vienam dalyviui, o antrasis ryšio dalyvis per saugų ryšio kanalą autentifikuojasi pateikdamas savo oficialų sertifikatą. Tolimesniame etape sukuriamas saugus ryšio kanalas serveris-vartotojas ir vartotojas autentifikuojamas serveriui.
- *Abipusio viešų raktų autentifikavimo* metode vartotojas ir serveris turi oficialius sertifikatus. Serveris ir klientas turi privačius raktus, susietus su jų sertifikatais, todėl nenaudojami slaptažodžiai. Autentifikuotis gali net iki tol nekontaktavę vartotojai. Viešojo rakto autentifikacijos metodu serveris sužino tik vartotojo viešą raktą, o ne slaptažodį. Tai labai padidina saugumą.

1.4.2. Autorizavimo metodas

Autorizacija užtikrina, kad kiekvienas turintis teisę prisijungti prie tinklo, galės atlikti tik jam numatytus veiksmus. Be prieigos prie katalogų, failų ir spausdintuvo vartotojų teisių sutikimo

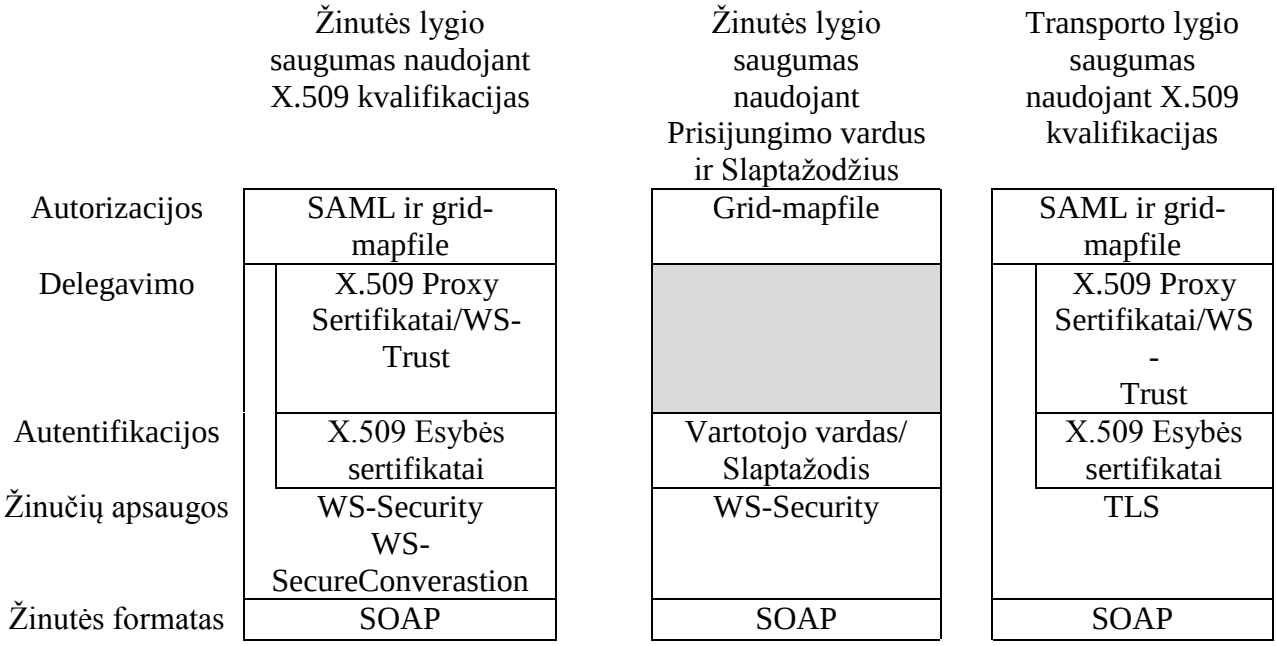
autorizacijos sistema gali kontroliuoti vartotojų galimybę atlikti įvairias sistemines funkcijas, tokias kaip lokali prieiga prie serverių, sisteminio laiko nustatymas, duomenų rezervinių kopijų sukūrimas, serverio išjungimas ir pan. *GRID* technologijų [9] ir web paslaugų susiliejimas pristato naujas galimybes ir naujus iššūkius *GRID* saugumui. Šios specifikacijos suteikė standartinius ir kartu veikiančius *GRID* saugumo užtikrinimo metodus. Tačiau siekiant sukurti autorizacijos mechanizmą, tinkamą *GRID* skaičiavimams, šios specifikacijos turi būti išplėstos ir pakeistos, nes „gridai“ turi savo aplikacijų reikalavimus. *GRID* sistemoje kiekvienas domenas turi savo saugumo politiką, tokią kaip ACL (Access Control List), CAS (Code Access Security), SAML (Security Assertion Markup Language), autorizacijos sprendimų pareiškimus ir XAML (eXtensible Access Control Markup Language*)* politikos nuostatas. Tačiau *Globus Toolkit 4.0* autorizacijos karkasas turi palaikyti keletą saugumo politikų ir turi būti lankstus, kad jį būtų galima lengvai pakeisti skirtingoms aplinkoms.

1.5. Esamų problemų sprendimai

GRID monitoringo sistemose saugumui užtikrinti naudojamas Globus Toolkit 4.0 [10] įrankių rinkinys, kuris suteikia vartotojams galimybę autentifikuotis su prisijungimo vardu ir slaptažodžiu. GT4 saugumas leidžia apsaugoti SOAP (*Simple Object Access Protocol)* žinutes, naudojant Transporto Lygio Saugumą (TLS) arba WS-Security standartais. TLS autentifikacija yra vykdoma naudojant X.509 kvalifikacijas arba neautentifikuotoje (anonimo) būsenoje. Šioje būsenoje autentifikavimas gali būti atliktas pasinaudojant vartotojo vardu ir slaptažodžiu iš SOAP žinutės. Tačiau keletas sertifikatų yra palaikomi žinutės lygio saugume. Dėl to, kad ji naudojasi žiniatinklio paslaugų standartais, tokiais kaip WS-Security ir WS-SecureConversation, ji yra neutrali specifiniams sertifikatų tipams, naudojamiems įgyvendinti šį saugumą. Žiniatinklio paslaugų standartai leidžia GSI (*Grid Security Infrastructure*) ir GT4, naudoti vartotojo vardą ir slaptažodį kaip priedą prie skaitmeninių sertifikatų. GT4 naudoja du mechanizmus, skirtus apsaugoti SOAP žinutes, siunčiamas skirtingų komponentų, t.y. transporto lygio saugumo ir žinutės lygio saugumo. Transporto lygio saugumas apsaugo transporto lygio saugumo perduodamą informaciją, naudojantis tokiais standartais, kaip TLS. Žinutės lygio saugumas veikia aukštesniame lygyje ir naudoja žiniatinklio paslaugomis grįstus standartus, tokius kaip WS-Security, WS-SecureConversation ir kt., apsaugant SOAP žinutes, kurios perduodamos transportiniu kanalu. Kiekvienas iš šių sistemos komponentų suteikia atitinkamą saugumo lygį. *MonALISA* ir *Ganglia* saugumui užtikrinti pasirinkta GSI saugumo infrastruktūra. GSI [11] galima laikyti susidedančia iš keturių atskirų funkcijų: žinučių apsaugos, autentifikacijos, delegavimo ir autorizacijos.

Skirtingų standartų įgyvendinimai naudojami suteikti kiekvieną iš šių funkcijų:

- TLS (transporto lygio) ar WS-Security ir WS-SecureConversation (žinutės lygio) yra naudojami kaip žinutės apsaugos mechanizmai, kartu veikiantys su SOAP;
- X.509 Esybės Sertifikatai ar Vartotojo vardas ir Slaptažodis yra naudojami kaip autentifikavimo kvalifikacijos;
- X.509 Proxy Sertifikatai ir WS-Trust yra naudojami delegavimui;
- SAML pareiškimai yra naudojami autorizacijai.



GT4 Grid saugumo infrastruktūros ir standartų, naudojamų skirtingoms funkcijoms, apžvalga. Pateikiamas transporto lygio saugumo ir žinutės lygio saugumo metodo apibudinimas.

Saugumo funkcijos skirtinguose lygiuose vykdomos skirtingais metodais. Autorizacijos ir žinutės lygio bei transporto lygio funkcijose, kur naudojamos X.509 klasifikacijos, naudojamas SAML ir grid-mapfile, tačiau naudojant prisijungimo vardą ir slaptažodį, SAML nėra naudojamas. Delegavimo ir autetifikacijos funkcijos lygiuose, kur naudojamos X.509 klasifikacijos yra vykdomos vienodai, tai reiškia panaudojant X.509 proxy ir esybės sertifikatus bei WS-trust. Žinučių apsaugos visuose lygiose atliekamos skirtingomis funkcijomis, o žinučių formatas visose lygiuose yra SOAP.

1.5.1. Transporto lygio saugumas

Transporto lygio saugumas[10] nustato SOAP žinutes perduodamas per tinklo prisijungimą, apsaugotą TLS. TLS šifruojant suteikia vientisumo apsaugą ir privatumą. Transporto lygio saugumas yra palaikomas kaip aukštesnio našumo alternatyva, daugiau standartais besinaudojančiu žinutės lygio saugumu. Jeigu žinutės lygio saugumas tampa spartesnis, naudojant įgyvendinimo ir specifikacijos faktorių kombinaciją, tikimasi laipsniško transporto lygio saugumo vertės sumažėjimo. Transporto lygio saugumas naudojamas sujungiant su X.509 autentifikacijos sertifikatu, bet taip pat gali būti naudojamas be tokių sertifikatų, siekiant suteikti žinutės apsaugą be autentifikacijos. Tai vadinama „anoniminiu transporto lygio saugumu“. Šioje veikimo būsenoje autentifikacija gali būti atlikta skirtingu lygiu, pvz., įvedus vartotojo vardą ir slaptažodį SOAP žinutėje arba komunikacija gali būti visai neautentifikuota.

1.5.2. Žinutės lygio saugumas

SOAP [10] žinutė suteikia galimybę išgauti pritaikymui tinkamą sistemos apkrovos dalį iš bet kurio saugumo - skaitmeninio parašo, vientisumo apsaugos ar šifravimo,- pritaikomo tai apkrovos daliai, leidžiant pritaikyti GSI saugumą nuosekliai per SOAP žinutes bet kuriai GT4 žiniatinklio paslaugomis paremtai programai ar komponentui. GSI įgyvendina WS-Security standartą ir WS-SecureConversation patikslinimą, kad SOAP žinutėms suteiktų apsaugą. WS-SecureConversation yra IBM ir Microsoft pasiūlytas standartas, leidžia pradinį apsikeitimą žinutėmis, siekiant sukurti saugų kontekstą, kuris gali būti naudojamas apsaugoti einančias vėlesnes žinutes mažiau kompiuterinių resursų viršijimo reikalaujančiu būdu. WS-Security ir WS-SecureConversation yra numatytos būti neutralios tam tikriems sertifikatų tipams, kurie naudojami įgyvendinti šią saugą. GSI leidžia X.509 viešojo rakto sertifikato ir vartotojo vardo bei slaptažodžio kombinacijos panaudojimą šiai saugai. GSI naudojamas arba su vartotojo vardo/slaptažodžio, arba su X.509 kvalifikacijomis. Naudoja WS-Security standartą leisti autentifikuoti, tai reiškia, gavėjas gali patikrinti duomenų siuntėjo tapatybę.

1.5.3. Autentifikavimas ir delegavimas

GSI tradiciškai palaiko autentifikavimą ir delegavimą per X.509 sertifikatą ir viešojo rakto naudojimą. Kaip nauja GT4 savybė GSI taip pat palaiko autentifikavimą per paprastą vartotojo vardą ir slaptažodį. GSI naudoja X.509 esybės sertifikatus (EEC *end entity certificates*) [12] identifikuoti pastovias esybes, tokias kaip vartotojai ir paslaugos. X.509 EEC suteikia kiekvienai esybei unikalų identifikatorių (pvz. išskirtinį vardą) ir būdą patvirtinti tą identifikatorių kitai pusei

per asimetrinio rakto poros panaudojimą sertifikatui. *GRID* išdėstymas visame pasaulyje naudoja pačių susikurtas sertifikavimo valdybas, paremtas trečiosios pusės programine įranga, kuri išleidžia X.509 EEC sertifikatus naudojimui su GSI ir Globus Toolkit. GSI taip pat palaiko delegavimą ir paprastą prisijungimą naudojant X.509 standarto Proxy sertifikatus. Proxy sertifikatai leidžia X.509 EEC informacijos pernešėjams laikinai perduoti savo privilegijas kitai esybei. Autentifikavimo ir autorizavimo tikslais GSI naudoja EEC ir Proxy sertifikatus vienodai. GT4 palaiko delegavimo paslaugą, kuri suteikia sąsają, leidžiančią klientams deleguoti (arba atnaujinti) X.509 Proxy sertifikatus paslaugai. Šios paslaugos sąsaja yra pagrįsta WS-Trust [13] specifikacijos. Autentifikacija su X.509 sertifikatais gali būti įvykdyta arba per TLS (transporto lygio saugumo atveju) arba parašu kaip nurodyta WS-Security (žinutės lygio saugumo atveju).

1.5.4. Vartotojo vardas ir slaptažodis

GSI gali naudoti WS-Security su tekstiniais vartotojo vardais ir slaptažodžiais, kaip nurodyta WS-Security standarte. Šis mechanizmas suteikia galimybes palaikyti elementaresnes žiniatinklio paslaugų programas atitinkant WS-I (*Web Services Interoperability*). Naudojant vartotojo vardus ir slaptažodžius, priešingai nei X.509 sertifikatus, GSI suteikia tik autentifikaciją ir nepažangias saugumo savybes, tokias kaip delegavimą, konfidencialumą, vientisumą ir pakartojimo apsaugą.

1.5.5. GRID saugos rezultatai

GRID saugumas [14] paveikia daugelį sistemos sričių, nuo tų, kurioms yra leidžiama gauti prieigą prie *GRID* tinklo, iki tų *GRID* mašinų, kurios gali atlikti skirtingas operacijas. Yra įvairių saugumo problemų *GRID* aplinkoje - nuo priėjimo saugos iki duomenų saugos.

Gali būti suskirstytos į:

- Saugumo lygio sauga - ji šalina problemas dėl vykdytų svetimų programų, tokių kaip virusai, kirminai, kenkėjiškas kodas ir t.t.;
- Architektūrinio lygio sauga - ji dirba su *GRID* sistemos saugumo infrastruktūros kūrimu, t.y. autentifikacija, autorizacija ir konfidencialumu *GRID* aplinkoje;
- Bendrasis veikimas - jis valdo heterogeninę saugumo infrastruktūrą skirtingo saugumo priemonių terminais, pvz., autorizacija, autentifikavimas, ir t.t. tarp keleto domenų organizacijoje ar didesniame tinkle.

1.5.6. GRID saugumą užtikrinantys būdai

Yra daug *GRID* saugumą užtikrinančių būdų, tokių kaip autentifikavimas, autorizavimas, konfidencialumas, vienas prisijungimas, delegavimas, neatsisakymas veikti, auditavimas, apskaita ir integralumas.

Kai vartotojas nori gauti prieigą prie *GRID* tinklo, jis turi prisijungti autentifikuodamas save.

Autentifikavimas - informacijos dalis, naudojama įrodyti subjekto tapatybę (pvz., paliudijimas) [15]. Yra daug metodų, skirtų vartotojų ar sistemų autentifikavimui. Dar kartą aptariami trys pagrindiniai paliudijimo modeliai:

a) Viešojo rakto infrastruktūra (PKI)

Viešojo rakto infrastruktūra susideda iš dviejų raktų. Pirmasis yra Privatusis Raktas (kuris neturėtų būti išduodamas jokiu būdu) ir kitas yra Viešasis raktas. Siuntėjas šifruoja savo žinutę savo Privačiuoju raktu ir siunčia ją gavėjui. Antrasis raktas, t.y. Viešasis raktas, yra siunčiamas gavėjui, kad jis galėtų iššifruoti siuntėjo užšifruotą žinutę. Raktams patikrinti parenkamas patikimas asmuo, kuris yra atsakingas už komunikavimui naudojamų raktų sertifikavimą. Šis asmuo vadinamas Sertifikavimo Valdyba (CA), kuri, savo ruožtu, yra registruojama Registravimo Valdybai (RA). Visas šis CA validavimo pas RA procesas ir tolimesnių vartotojo raktų validavimas pas CA vykdomas PKI infrastruktūroje.

b)Kerberos

Kerberos yra paskirstytoji autentifikavimo paslauga, leidžianti procesui (klientui), veikiančiam vartotojo vardu, patvirtinti jo tapatybę tikrintojui (aplikacijų serveriui ar paprastam serveriui) be informacijos siuntimo per visą tinklą, kas vėliau galėtų leisti atakuotojui ar tikrintojui apsimesti valdžia. Kerberos pagal pageidavimą suteikia vientisumą ir konfidencialumą informacijai, siunčiamai tarp kliento ir serverio.

c) Saugus Apvalkalas (Shellas)

Saugus apvalkalas yra protokolas, suteikiantis galimybę saugiam komunikavimui tinkle[16]. Saugus apvalkalas suteikia tris pagrindines galimybes, atveriančias duris daugeliui kūrybingų saugumo sprendimų:

- Saugus komandinis apvalkalas leidžia nuotolinį prisijungimą ir suteikia vartotojui galimybę autentifikuotis ir atjungti vartotoją, jei jis bando pakenkti sistemai.
- Saugus failų perdavimas naudojamas su Saugaus Failų Perdavimo Protokolu (SFTP) saugiam failų perdavimui.
- Portų nukreipimas suteikia galimybę lengvai „tuneliuoti“ duomenis, apsaugant siunčiamą informaciją.

Labiausiai tinkama autentifikavimui yra *Viešojo rakto infrastruktūra (PKI).* Tai geriausias būdas vartotojo tapatybei patikrinti. Vartotojas, norėdamas prisijungti prie sistemos, turi gauti *BalticGrid* arba *LitGrid* sertifikatą. Sertifikatui gauti turi pateikti sertifikatų išdavimo organizacijai atitinkama prašymą, bet prieš tai turėtų susigeneruoti Viešą ir Privatų raktą. Tik pateikus reikalingus dokumentus ir Viešąjį raktą, išduodamas sertifikatas.

Autorizavimas

Autorizavimo procesas nustato, ar vartotojas arba sistema gali įvykdyti pageidaujamą operaciją. Yra keletas autorizacijos įgyvendinimo būdų:

a) Prisijungimo kontrolės sąrašas (ACL)

Prisijungimo kontrolė [17] yra mechanizmas, leidžiantis resursų savininkams apibūdinti, valdyti ir paskatinti prisijungimo sąlygas, galiojančias kiekvienam resursui.

b) Rolėmis pagrįsta prisijungimo kontrolė (RBAC)

RBAC plėtojimas sutampa su korporacijų intranetų pasirodymu. Korporacijos yra paprastai hierarchiškai struktūrizuotos, ir prisijungimo leidimai priklauso nuo vartotojo pozicijos hierarchijoje. Rolės yra esybių rinkiniai ir prisijungimo teisės, sugrupuotos remiantis jų atliekamomis sistemos aplinkoje skirtingomis užduotimis.

c) Paskirstytoji autorizacija

Sistemos yra išdėstytos skirtinguose administravimo domenuose, kur kiekviena organizacija turi tam tikrą sistemos naudojimo kontrolės politiką [18]. Prisijungimo Politikos prisijungimui prie tam tikro resursų rinkinio yra valdomos skirtingų administratorių.

d) Bendruomenės autorizavimo paslauga (CAS)

CAS [19] komponentai leidžia resursų teikėjams nustatyti apytiksles prisijungimo kontrolės politikas bendruomenių visumos terminais, deleguojant tiksliai nustatytą prisijungimo kontrolės politikos valdymą pačiai bendruomenei. Resursų teikėjai palaiko pagrindinę savo resursų valdžią (įtraukiant vartotojų kontrolę ir auditavimą), apsieinant be daugelio kasdienių politikos administravimo užduočių (pvz., pridėjimo ir vartotojų pašalinimo iš grupių, vartotojų privilegijų koregavimo).

Autorizavimas yra vykdomas pagal vartotojų tipą. Privilegijuoti vartotojai turi visiškas monitoringo teises, administratorius turi teisę pašalinti nepageidaujamus vartotojus, o paprasti vartotojai gali tik paskaityti informaciją apie *GRID* tinklus. Visi vartotojų veiksmai yra registruojami veiksmų registre, tai leidžia nustatyti, kokius veiksmus atlieka atskiri vartotojai.

Konfidencialumas

Informacijos pasiekimas yra saugus ir nepažeidžiamas atakomis. Yra du populiarūs konfidencialumo modeliai. Kai raktai turi būti perduodami tarp siuntėjo ir gavėjo, Viešojo Rakto kriptografijos modelis yra naudojamas komunikavimui ar žinutės perdavimui arba yra naudojamas Slaptojo Rakto modelis žinutės perdavimui.

a) Slaptojo rakto kriptografija

Ši kriptografija naudojasi simetriniu šifravimu [20].

- Abi pusės naudojasi ta pačia rakto reikšme šifruojant aiškų tekstą į šifrą ir iššifruojant šifrą atgal į aiškų tekstą;
- Simetrinis raktas padeda apsikeisti slaptais raktais pusėms, kurios nepasitiki viena kita, pvz., internete;
- Vartotojų grupėms su n vartotojų raktų skaičius yra K= n(n-1)/2 (1).

b)Viešojo rakto kriptografija

Viešojo rakto kriptografijoje šifravimas ir dešifravimas yra atliekami naudojant porą raktų, tokių, kai vieno iš jų žinojimas nesuteikia žinių apie kitą poros raktą. Vienas raktas yra paviešinamas ir vadinamas viešuoju raktu, o kitas raktas yra saugomas slaptai ir yra vadinamas privačiuoju raktu (neturėtų būti maišomas su slaptuoju raktu, kuris yra pasidalinamas tarp pusių bendravimui įprastoje kriptosistemoje). Viešojo rakto kriptografija turi keletą privalumų prieš įprastinę kriptografiją, kai naudojama autentifikavimui. Jie turi natūralesnį palaikymą keleto gavėjų autentifikacija, palaikymą apsaugos nuo neatpažinimo (dėl to, kad patvirtinantysis nežino privačiojo rakto, sistema gali sugeneruoti žinutę, kuri gali apsimesti esanti iš autentifikuotos valdžios), ir eleminavimą slapto šifravimo raktų ir centrinio autentifikavimo serverio. Pasirašymas yra šifravimo procesas su privačiuoju raktu. Verifikavimas yra procesas šifravimo su viešuoju raktu.

Konfidencialumui užtikrinti naudojama *Viešojo rakto kriptografija*. Klasterio duomenis vartotojas gali išsaugoti į PDF failą, kuris pasirašomas elektroniniu parašu.

1.6. Sprendimo kūrimo metodai ir priemonės

Ganglia [21] sistema stebi klasterius ir klasterių junginius, renka sistemų statuso informaciją (gali būti pateikta XML dokumente arba grafiškai naudojantis žiniatinklio sąsaja). Siekiama paprastumo ir kokybės, tad galėtų stebėti tūkstančius sistemų. *Ganglios* pateikta informacija gali naudotis ir *MonALISA* monitoringo sistema. *Ganglia* monitoringo sistema naudoja GMOND „deamoną“, kuris veikia kiekvienoje stebimoje sistemoje. Jis renka standartinį informacijos rinkinį, o jo konfigūraciniame faile yra nurodyta, kada rinkti informaciją ir kada ją siųsti. Remiantis laiku ar

būsenos pokyčiu galima nurodyti, kam siųsti ir kam leisti atsiųsti užklausą. Kitas Ganglia „demonas“ yra GMETRIC. Ši programa suteikia nustatomą informaciją Gangliai (pvz. CPU temperatūrą, užduočių eilės ilgį ir pan.). Gmetric naudoja Gmond konfigūracijos failą, kad sužinotų, kam siųsti informaciją. Dar vienas „demonas“, veikiantis Ganglia sistemoje, yra GMETAD. Jis segreguoja informaciją iš „gmondų“. Konfigūracijos faile nurodyta, iš kurių „gmondų“ rinkti informaciją (pasinaudojant TCP protokolu).

Kitaip realizuota yra *MonALISA* [22] GRID parametrų stebėjimo sistema. Ji realizuota JAVA kalba. *MonALISA* nustato paslaugas ir komunikavimą, kaupia informaciją iš kitų sistemų (SNMP, Ganglia ir kt.). *MonALISA* naudoja klientus, kurie suranda ir užsako paslaugas, teikiančias monitoringo informaciją. Taip pat klientai grafiškai vaizduoja informaciją per žiniatinklio sąsają. *MonALISA* teikia autonomines paslaugas. Kiekviena monitoringo sistema saugo informaciją reliacinėje duomenų bazėje, automatiškai atnaujina monitoringo paslaugas, ieško paslaugų.

Kitokius kūrimo metodus ir priemones naudoja *Nagios* stebėjimo sistema. Ji yra konfigūruojama ir gali būti išplėsta. Ji turi platų funkcijų spektrą, palaiko paskirstytą monitoringą, gali atlikti kai kurias korekcijas sistemų nustatymuose reaguodamas į monitoringo duomenis. Grafinėje sąsajoje galima stebėti esamą būklę grafikais. Gali bandyti išspręsti problemas, pvz., perkrauti daemon‘ą. Jei problema pasikartoja daug kartų, gali imtis nurodytų veiksmų.

Prisijungimui prie naujai sukurtos BalticGrid monitoringo sistemos reikalingas specialus sertifikatas. Duomenys, kaip ir kitose sistemose, vaizduojami grafiškai bei lentelėje. Galima pasirinkti tikslų stebėjimo laikotarpį. Kaip jau minėta anksčiau, skirtingai nei kitose monitoringo sistemose, naujai sukurtoje BalticGrid monitoringo sistemoje stebimus duomenis galima išsaugoti PDF faile, kuris pasirašomas elektroniniu parašu.

1.7. Išvados

- pagal suformuluotus kriterijus tirtos populiariausios *GRID* monitoringo sistemos. Nustatyta, kad į saugumą labiausiai orientuota yra MonALISA monitoringo sistema, kitų sistemų saugumas užtikrintas silpniau;

- palyginus sistemas bei aptarus moksliniuose straipsniuose nagrinėjamas *GRID* monitoringo sistemas, galima daryti išvadą, jog nėra tokios sistemos, kuri pateiktų visus svarbius parametrus bei visiškai užtikrintų duomenų saugumą;

- išnagrinėjus *GRID* monitoringo saugą užtikrinančias priemones ir technologijas, nuspręsta magistriniame darbe naudoti *Viešojo rakto infrastruktūrą* vartotojų autentifikavimui; autorizavimui

naudojamas prieigos kontrolės sąrašas (*ACL)*, o duomenų konfidencialumą užtikrina *Viešojo rakto kriptografija;*

- atsižvelgus į esamų problemų sprendimus *GRID* monitoringe bei sprendimo kūrimo metodus ir priemones, nuspręsta naujoje sistemoje prisijungimui naudoti sertifikatą, o duomenis vaizduoti ne tik grafiškai, bet ir lentelėse, taip pat užtikrinti galimybę išsaugoti juos PDF faile.

2. BalticGrid monitoringo sistemos projektas

Projekto tikslas - sukurti BalticGrid tinklui saugią monitoringo sistemą. Sistema turi būti skirta uždaram vartotojų ratui, vadinasi prieigą prie jos turės tik vartotojai, turintys atitinkamą sertifikatą.

2.1. Projekto reikalavimai

a) funkciniai:

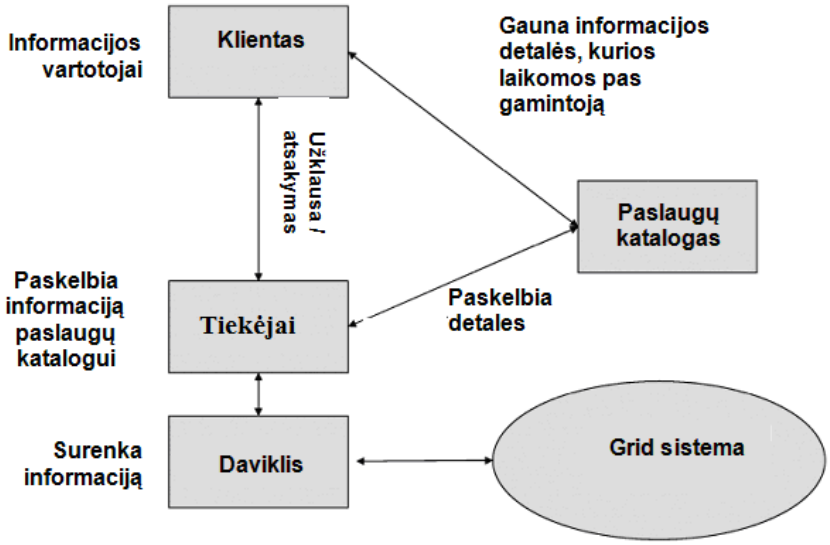
- monitoringo sistema turi talpinti informaciją apie *GRID* tinklus ir stebėti klasterių parametrus;
- klasterio duomenys turi būti vaizduojami lentelėje ir grafiškai;
- grafikas turi būti interaktyvus, su kursoriumi galima nustatinėti rėžius, pagal kuriuos galima stebėti parametrus pasirinktam laikotarpyje;
- prisijungimui prie sistemos reikia turėti BalticGrid arba LitGrid sertifikatą;
- klasterių parametrus galima išsaugoti PDF faile, kuris pasirašytas elektroniniu parašu;
- vartotojų stebėjimui turi būti sistemos vartotojų veiksmų įrašų sistema;

b) nefunkciniai:

- reikalingas *msql* ir *apache* serveris;
- interneto naršyklė;
- prisijungimo sertifikatas;
- PDF dokumentų skaitymo programa.

2.2. Rekomenduojama Grid monitoringo architektūra

GRID monitoringo architektūrą [23] (GMA) pagal rekomendaciją *GRID* sistemai sukūrė Global Grid Forum (GGF). Būtina pažymėti, kad ji nėra standartinė, todėl ji dar diskutuotina, įgyvendinama tikintis rezultatų. 12 pav. nurodyta *GRID* monitoringo architektūros komponentai. GMA sudaryta iš daviklių, tiekėjų, klientų ir paslaugų katalogo. Šie komponentai yra sutinkami daugelyje *GRID* monitoringo sistemų architektūrose, naujai kuriamoje BalticGrid monitoringo sistemoje komponentai suskirstyti skirtingais sluoksniais.



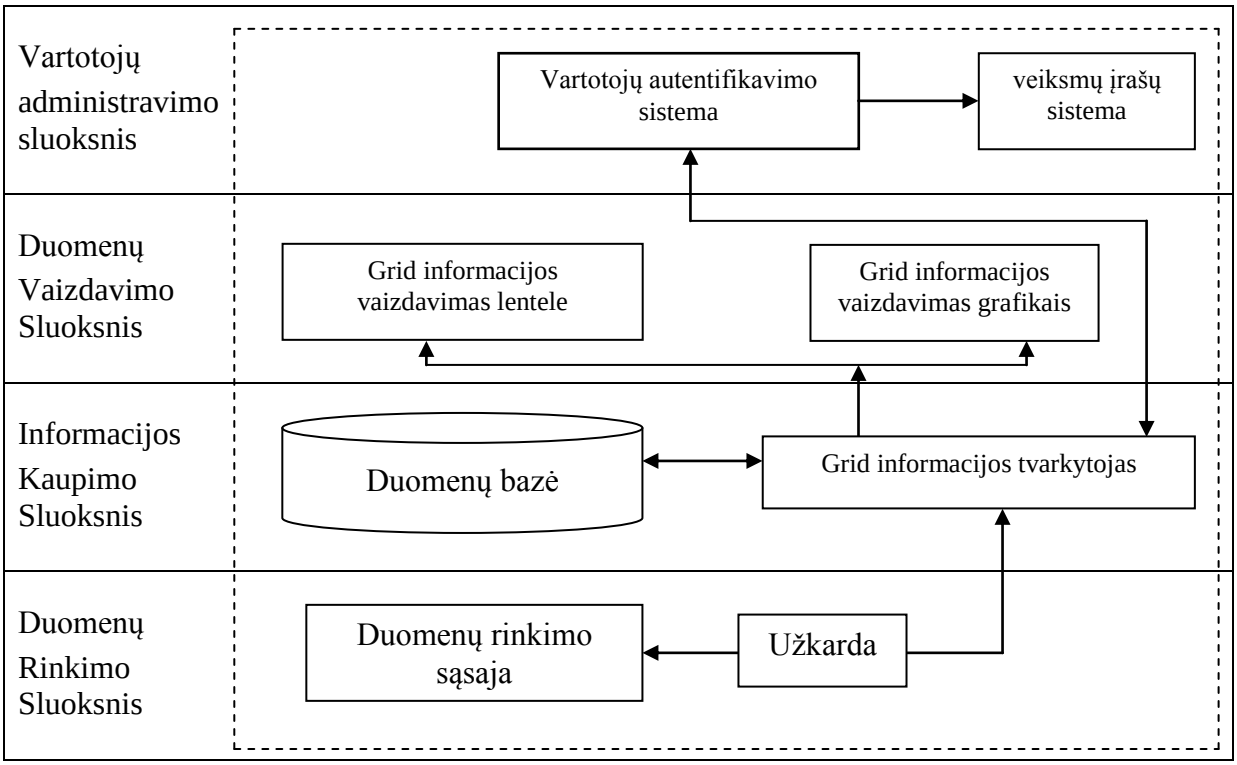
12 pav. GGF Rekomenduojama architektūra

- **Davikliai (Sensors).** Davikliai - tai duomenų monitoringo šaltinis, atsakingas už duomenų surinkimą iš parskirstytos *GRID* sistemos. Jie taip pat atsakingi už įvykius, atsiradusius pagal matuojamus duomenis. Architektūra gali būti supaprastinta įvedus daviklius pas klientus arba vartotojus.
- **Tiekėjai (Producer).** *GRID* monitoringo architektūroje tiekėjai atsakingi už įsiregistravimą paslaugų kataloge. Jie taip pat privalo pateikti norimos perduoti *GRID* tinklui informacijos tipą ir struktūrą. Kažkuria prasme tiekėjai yra daviklių vadybininkai, nes sprendžia kokio tipo ir kiekio informacija bus naudinga klientams.
- **Paslaugų katalogas (Directory Service) arba Registras.** Paslaugų katalogas (vadinamas registru) atsakingas už įvykių tipo ir atitinkamų gamintojų paskelbimą. Klientai susisiekia su registru norėdami sužinoti prieinamos informacijos tipą bei surasti gamintoją, kuris tą informaciją tiekia.
- **Vartotojai (Consumer).** Tai monitoringo duomenų vartotojai. Klientai patiekia paslaugų katalogui užklausą ir gauna informaciją apie gamintojus. Kai informacija gaunama, klientas tiesiogiai susisiekia su paslaugų katalogu dėl jam reikiamos informacijos.

2.3. Monitoringo sistemos architektūra

Naujai kuriamos BalticGrid monitoringo sistemos architektūra pavaizduota 13 pav. Kaip ir rekomenduojamoje architektūroje, žemiausias sluoksnis yra „Duomenų rinkimo sluoksnis“. Kitas sluoksnis yra „Informacijos kaupimo sluoksnis“, jame yra duomenų bazė ir *GRID* informacijos tvarkytojas, kuris pateikia reikalingą vartotojui informaciją, vadinasi atlieka „tiekėjo“ funkcijas. Už

informacijos pateikimą yra atsakingas „duomenų vaizdavimo sluoksnis“. Šiame sluoksnyje kaip ir „Paslaugų kataloge“ keliais būdais yra pateikiama vartotojui reikalinga informacija apie *GRID* tinklą. Vartotojas duomenis gali peržiūrėti interaktyvių grafikų pagalba arba duomenys yra pateikiami lentelėje. Lentelėje pateiktus duomenis, galima išsisaugoti PDF faile. Norint užtikrinti PDF failo autentiškumą, jis yra pasirašomas elektroniniu parašu. Viršutiniame sluoksnyje yra „vartotojų administravimo sluoksnis“. Vartotojai norėdami sužinoti informaciją apie *GRID* tinklą pirmiausia turi gauti BalticGrid arba LitGrid sertifikatą ir prisiregistruoti prie sistemos.

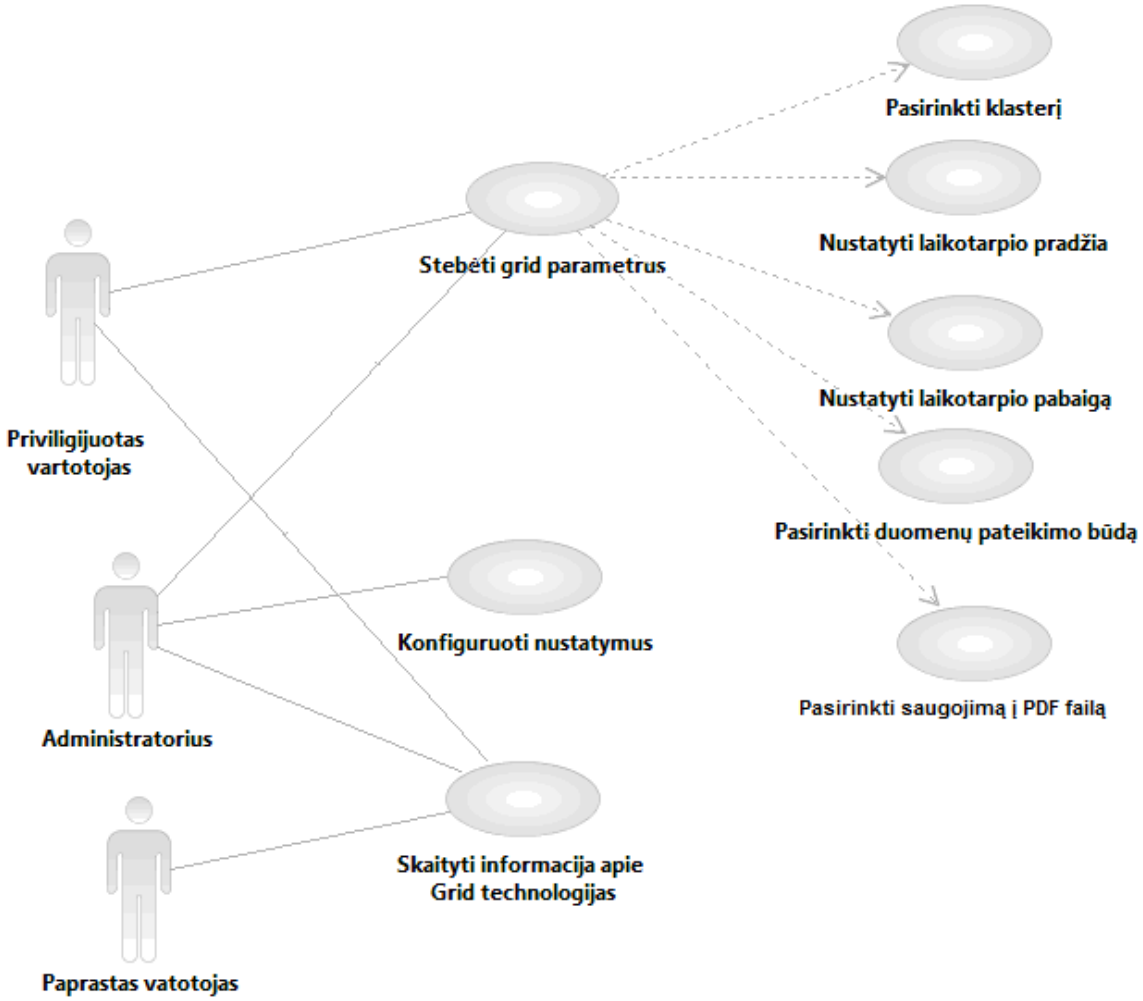


13 pav. Kuriamos monitoringo sistemos architektūra

Kuriama sistema atitinka rekomenduojamos *GRID* monitoringo architektūros komponentus bei tenkina būtinus saugumo reikalavimus, todėl yra tinkama naudoti *GRID* tinkluose, kuriuose dirbama su svarbiais ir slaptumo reikalaujančiais duomenimis. Vartotojai, norintys prisijungti prie sistemos, turi įsigyti specialų sertifikatą. Kiekvieno vartotojo prisijungimai yra saugomi prisijungimų registre. Tai leidžia lengvai nustatyti, kada ir kuris vartotojas bando neteisėtai naudotis sistema. Sistemoje yra naudojamos ugniasienės, kurios blokuoja neteisėtą prisijungimą prie duomenų rinkimo sluoksnio. Ši architektūra yra pakankamai saugi bei patikima, jos struktūra sugeba patenkinti daugelį keliamų reikalavimų.

2.4. Monitoringo sistemos galimybės

Vartotojų poreikiai kuriamam produktui panaudojimo atvejų diagrama



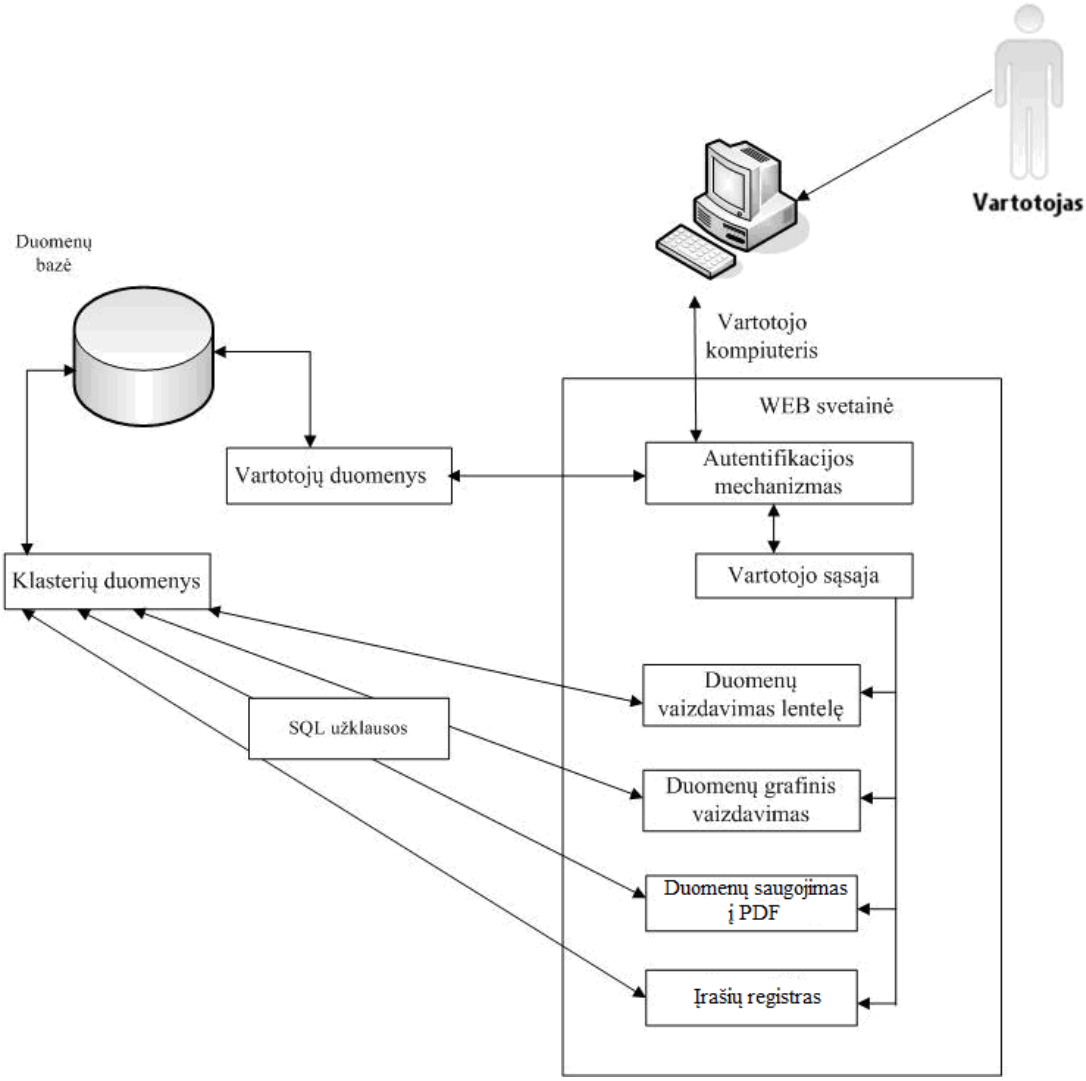
14 pav. Panaudojimo atvejų diagrama

Panaudojimo atvejų diagrama parodo, kokius veiksmus gali atlikti atskiro lygio vartotojas. Pateiktoje diagramoje (14 pav.) brūkšniuota linija detalizuoja, ką konkrečiai gali peržiūrėti vartotojas, paspaudęs nurodytą komponentą. Paprastas vartotojas gali tik pasiskaityti informacija apie *GRID* tinklus. Kad galėtų stebėti klasterių veikimo rezultatus, būtinai turi prisiregistruoti prie sistemos. Prisiregistravęs tampa privilegijuotu vartotoju. Privilegijuotas vartotojas gali dviem būdais peržiūrėti klasterių parametrus: lentele ir grafiku, duomenis gali taip pat išsaugoti PDF faile. Stebėdamas parametrus lentelės pavidale vartotojas gali nusistatyti laikotarpį, nuo kada iki kada rezultatai jį domina, pažymėti parametrus, kurių reikšmes nori stebėti bei gali nurodyti ribą, kuri tenkina jo reikalavimus. Tokiu būdu gaus informaciją, kokiomis dienomis klasteris veikė pagal nurodyta ribą. Parenkant grafinį duomenų stebėjimą galimybės yra kur kas didesnės. Grafike vaizdžiai matomi visi parametrai. Nurodžius tenkinamą ribą, matoma skirtingom spalvom, kada parametrai tenkina vartotojo poreikius, kada yra žemiau ribos bei kada kerta nustatytą ribą. Pasirinkus grafinį stebėjimą galima palyginti pasirinktus parametrus arba palyginti pasirinktus klasterius. Kad palygintų norimus parametrus, viename grafike yra braižomos kreivės skaičiuojant

procentines reikšmes, o palyginant klasterius, parenkama norimi klasteriai bei parametras ir kreivėmis palyginama klasterių veikimas nustatytam laikotarpiui.

2.5. Apibendrintas monitoringo sistemos modelis

Monitoringo sistemos modelio komponentai ir ryšiai tarp jų.

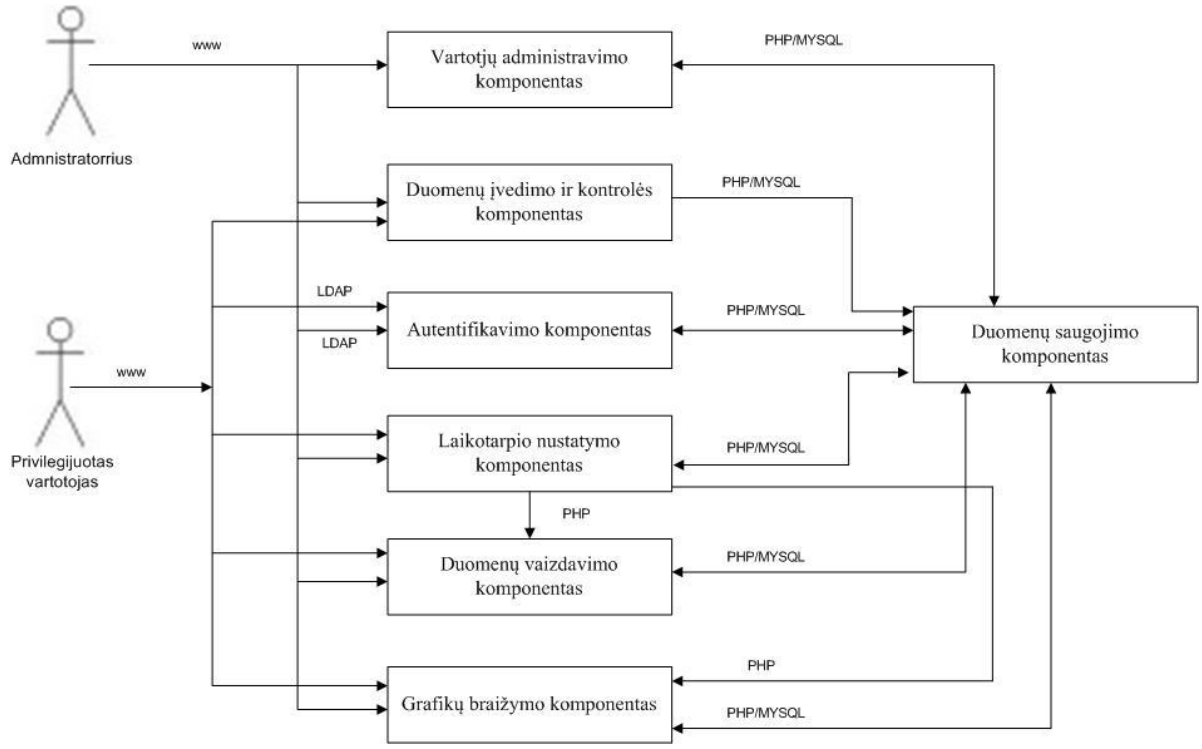


15 pav. Apibendrintas sukurtos sistemos modelis

Apibendrintame sukurtos sistemos modelyje (15 pav.) pavaizduota programos sudėtis, jos veikimo principas bei santykis su programos veikimo kontekstu. Modelyje pavaizduota komponentai, iš kurių susideda visą sistema bei parodyta, iš kur imami duomenys. Visi reikalingi duomenys yra talpinami į duomenų bazę, o priėjimą prie jų turi tik prisiregistravę vartotojai.

2.6. Sistemos komponentų modelis

Sistemos komponentų modelyje (16 pav.) pavaizduoti sistemą sudarantys komponentai, vartotojai bei jų tarpusavio ryšiai, nurodant technologijas, kuriomis šie ryšiai yra paremti.



16 pav. Sistemos komponentų modelis

Sistemos komponentų modelis parodo, kokius veiksmus gali atlikti administratorius ir privilegijuotas vartotojas. Atliekamos funkcijos yra labai panašios, administratorius papildomai gali administruoti vartotojus. Turi teisę pašalinti vartotoją iš sistemos, taip pat mato kiekvieno vartotojo atliekamus veiksmus sistemoje.

2.7. Išvados

- projektinėje dalyje pateikti funkciniai ir nefunkciniai sistemos reikalavimai, kurie turi būti įgyvendinti realizacijos dalyje;
- išanalizuota sistemos rekomenduojama architektūra bei pasiūlyta nauja BalticGrid monitoringo architektūra;
- schemomis pavaizduotos sistemos galimybės, monitoringo sistemos bei komponentų modeliai, šios schemos padeda lengviau suprasti sistemos veikimą.

3. BalticGrid monitoringo sistemos realizacija

Realizacijos dalyje nagrinėjamos BalticGrid monitoringo sistemos projektavimo ir kūrimo detalės. Konkretizuojami priimti sprendimai, pateikiamos sistemos komponentų architektūros ir duomenų vaizdavimo būdai.

3.1. Monitoringo sistemos kūrimo pagrindimas

Magistrinio darbo tikslas - sukurti monitoringo sistemą BalticGrid tinklui. Sistema turi vaizdžiai ir aiškiai vartotojui pateikti tinklo parametrus, turėti parametrų bei klasterių palyginimą. Didelis dėmesys skiriamas saugumui bei duomenų vientisumui, todėl reikia užtikrinti saugų vartotojų prisijungimą prie sistemos ir patikimą parametrų nuskaitymą.

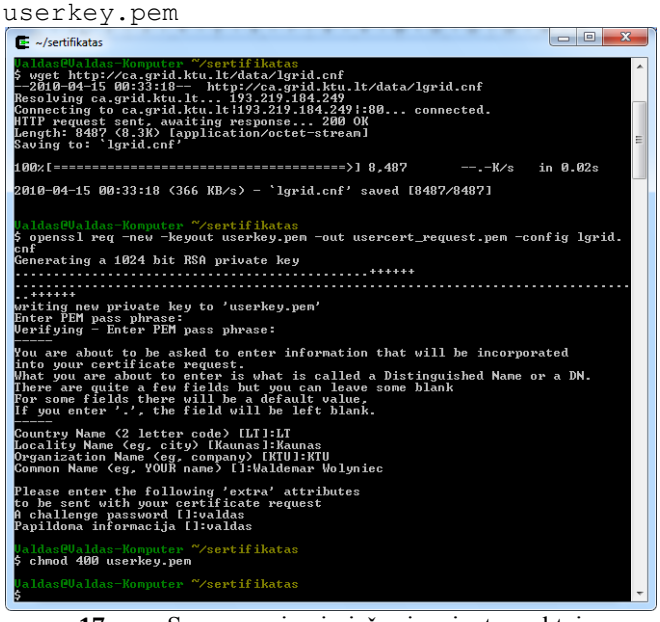
3.2. Saugumo užtikrinimas

Monitoringo sistema naudotis gali tik registruoti vartotojai. Norit stebėti BalticGrid tinklo parametrus, reikia įsigyti BalticGrid arba LitGrid sertifikatą. Sertifikatą įsigyti gali tik mokslinių įstaigų nariai. Sertifikato gavimui reikia susigeneruoti sertifikato užklausą, asmeniškai susitikti su LitGrid CA arba BalticGrid įgaliotu atstovu ir pateikti popierinę užklausos kopiją, Jūsų tapatybę patvirtinantį dokumentą ir įrodymą, kad dirbate/mokotės Lietuvos akademinėje įstaigoje. Tik patvirtinus tapatybės duomenis yra suteikiama teisė naudotis monitoringo sistema. Toks būdas apsaugo nuo nepageidautinų vartotojų naudojimosi sistema.

3.3. Sertifikato gavimo ir įdiegimo eiga

Sugeneruojami userkey.pem ir usercert_request.pem failai.

```
$ wget http://ca.grid.ktu.lt/data/lgrid.cnf
$ openssl req -new -keyout userkey.pem -out usercert_request.pem -config
lgrid.cnf
$ chmod 400 userkey.pem
```



17 pav. Sugeneruojami viešas ir privatus raktai

Viešas raktas siunčiamas sertifikavimo centrui.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBtjCCAR8CAQAwSDELMAkGA1UEBhMCTFQxDzANBgNVBAcMBkthdW5hczEMMAoG
A1UECgwDS1RVMRowGAYDVQQDDBFXYWxkZW1hciBXb2x5bmllYzCBnzANBgkqhkiG
9w0BAQEFAAOBjQAwgYkCgYEAr7cTGARP0FaJHLD1FGCh+3ZH5i+WVd555IrUqWxO
4SjcPKi2Ko4UliF6L3KQ/ofnWB8XoXXFConKWBNIwCjQgbv4qHS7OILotwCJ/BZZ
TF8RUUAy6XoAHJkz4ZUnd5yOJVXRcFoYg3DjIiYC7P+bSuMUhF7p2FT+e0pO/RcH
qF0CAwEAAaAuMBUGCSqGSIb3DQEJAjEIDAZ2YWxkYXMwFQYJKoZIhvcNAQkHMQgM
BnZhbGRhczANBgkqhkiG9w0BAQUFAAOBgQCLn94oauJsX5N2Qi6MWzZgKQ2k2g0S
N3iw989BzPCzBT9SDCjcCD5yQTKxUstdymeq+Xi53qSlWBU8SI9TH1+vaF4PHlYz
C5QGk3Ywh2sZI5iGrAiKwwST/EfBkUHNHrKoVMDh75v5gyZUj+6/pHzHdnxFrVvD
qfuYvIF0WizneQ==
-----END CERTIFICATE REQUEST-----
```

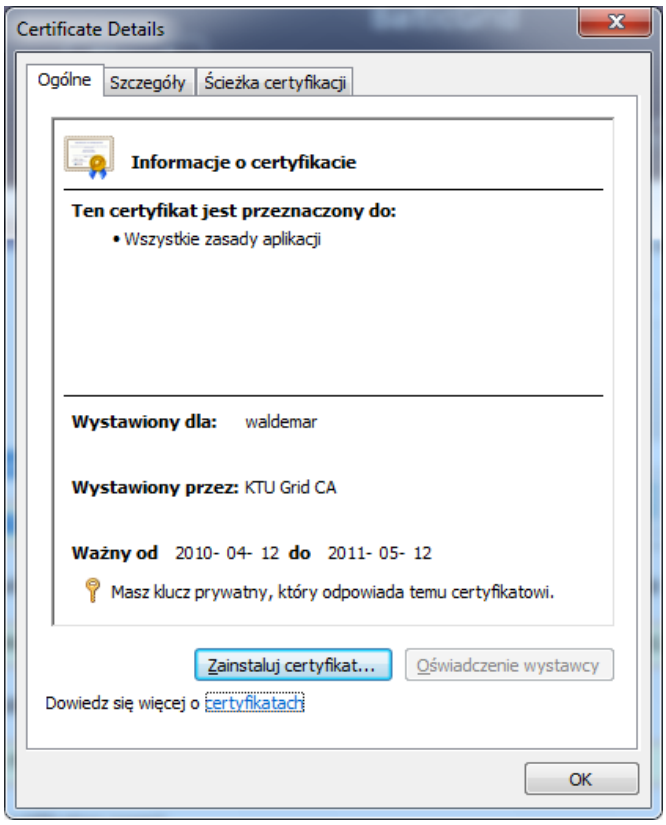
18 pav. Viešas raktas

Sertifikavimo centrui pateikus asmens tapatybės patvirtinančius dokumentus gaunamas reikalingas sertifikatas. Gautą sertifikatą reikia konvertuoti į PKCS#12 formatą (19 pav.), perkonvertavus galima į naršyklę įdiegti reikalingą sertifikatą (20 pav.).

```
openssl pkcs12 -export -in usercert.pem -inkey userkey.pem -out certificate.p12
```

19 pav. Konvertavimo į PKCS#12 užklausa

Tik perkonverguotas ir priskirtas prie patikimų sertifikatų BalticGrid arba LitGrid sertifikatas leis vartotojui prisijungti prie stebėjimo sistemos.

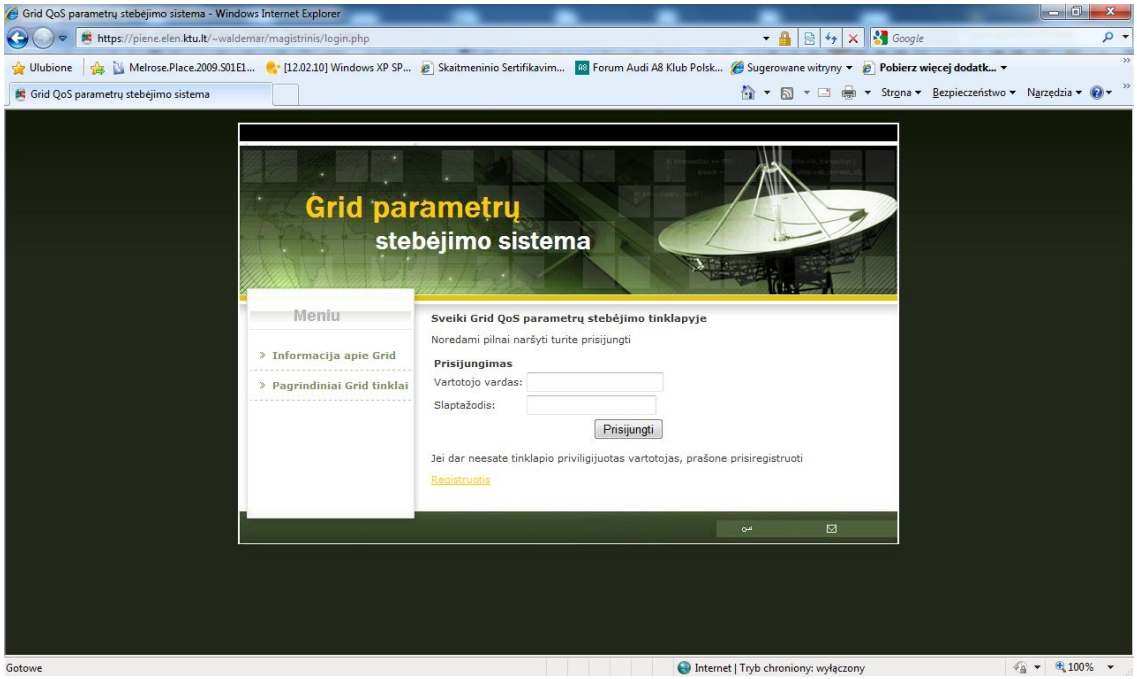


20 pav. LitGrid sertifikatas

3.4. Sistemos naudojimas

Vartotojai, neturintys reikalingo sertifikato, bandydami jungtis prie sistemos, gauna pranešimą, kad sistema nepasiekiama.

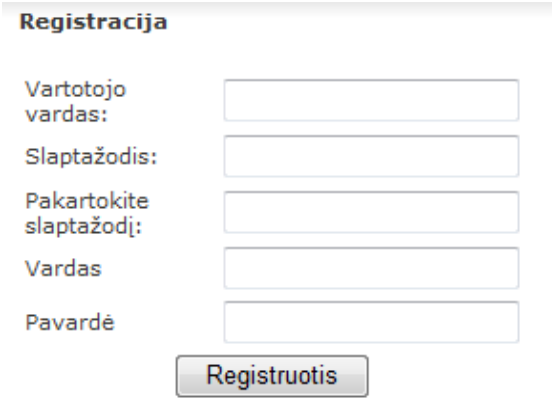
Vartotojas, turintis LitGrid arba BalticGrid sertifikatą, suvedus prisijungimo adresą https://piene.elen.ktu.lt/~waldemar , prijungiamas prie sistemos.



21 pav. Prisijungimas prie sistemos

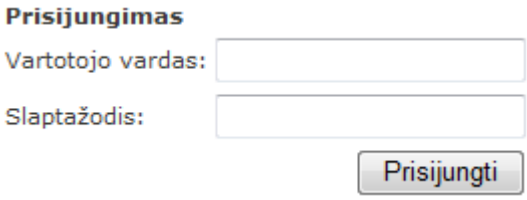
3.5. Sistemos komponentų architektūra

Vartotojų registracijos komponente (22 pav.) vaizduojama, kaip vartotojas turi prisiregistruoti prie sistemos. Suvedinėjant vartotojo vardą, sistema tikrina, ar tokio vartotojo sistemoje dar nėra, o rašant slaptažodį yra tikrinama, ar abu laukai parašyti vienodai.



22 pav. Registracijos komponentas

Prisiregistravus prie sistemos vartotojas turi prie jos prisijungti. Tai padaroma suvedant prisijungimo duomenis į prisijungimo langelius. (23 pav.).

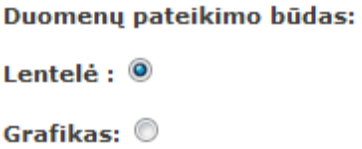


23 pav. Prisijungimo komponentas

Atlikus registracijos ir prisijungimo procedūras, vartotojas gali visiškai naudotis sistemos galimybėmis. Klasterių stebėjimui pirmiausia reikia nustatyti laikotarpį ir klasterį, kurio duomenys domina. Šie nustatymai atliekami (24 pav.) pavaizduotame komponente.

24 pav. Klasterio ir laikotarpio nustatymo komponentas

Nustačius visus tenkinančius parametrus, prieinama prie duomenų stebėjimo. Galima pasirinkti vieną iš kelių klasterių duomenų vaizdavimų. Duomenis galima matyti lentelėje arba kelių tipų grafikuose. Lentelėje duomenys vaizduojamas klasterio parametrų reikšmių kitimas laike (parenkama pagal datą). Grafinis vaizdavimas yra kelių rūšių, apie tai parašyta žemiau. Stebėjimo būdo parinkimas pavaizduotas (25 pav.). Pasirenkant stebėjimo būdą galima nustatyti norimą ribą, pagal kurią paryškinami vartotoja tenkinantys parametrai.



25 pav. Parametrų vaizdavimo būdo nustatymo komponentas

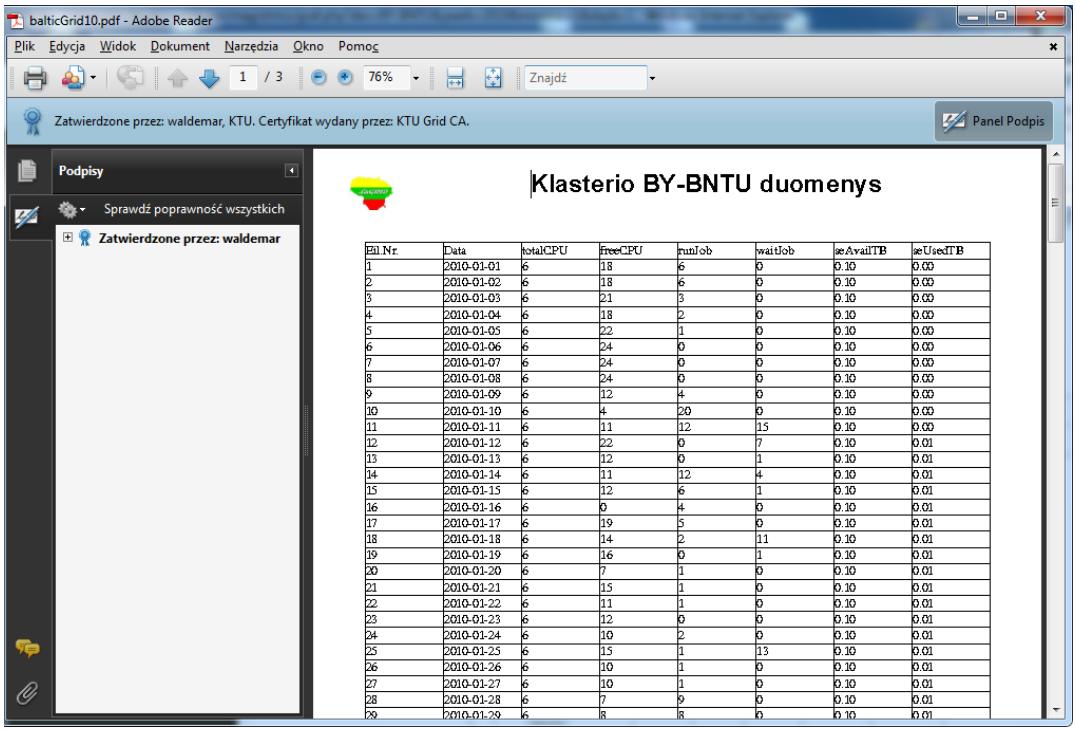
Duomenų stebėjimui reikia parinkti parametrus, kuriuos norima matyti. Tai padaroma (26 pav.) pažymėtame komponente. Kaip jau buvo minėta, grafinis vaizdavimas yra kelių būdų. Pažymėjus dominančius parametrus, galima juo išvysti atskiruose grafikuose vieną po kitu arba visus parametrus viename grafike. Pasirinkus vaizdavimą viename grafike, visi pažymėti parametrai yra lyginami tarpusavy. Skaičiuojama yra procentinės parametrų vertės. Didžiausia reikšmė duotame laikotarpyje yra prilyginama 100%, o visos kitos atitinkamai mažesnės, tokiu būdu matomas klasterio parametrų palyginimas.

26 pav. Vaizduojamų parametrų pasirinkimo komponentas

Vaizdavimui galima pasirinkti tokius parametrus, kaip bendras CPU skaičius, laisvų CPU skaičius. Galima matyti, kiek yra vykdoma užduočių ir kiek yra laukiančių eilėje. Taip pat galima sužinoti, kiek kalsteryje yra laisvos vietos ir kiek jau panaudota.

3.6. Duomenų išsaugojimas PDF faile

Klasterių duomenis galima ne tik stebėti, bet taip pat galima išsisaugoti PDF faile. Išsaugotą failą galima pateikti *GRID* tinklo tiekėjui tuo atveju, kai turima kažkokių nusiskundimų dėl klasterio veikimo sąlygų. Kaip ir visų paslaugų vartotojai, taip ir *GRID* tinklo vartotojas, besinaudojantis *GRID* tinklu, turi teisę reikalauti iš tiekėjo paslaugų patikimumo ir stabilumo. Pastebėjus, kad naudojamas klasteris neveikia arba neatlieka tiek užduočių, kiek buvo pasirašyta sutartyje, vartotojas, pateikęs monitoringo duomenis, gali pareikšti tiekėjui priekaištus. Tiekėjui pateikus monitoringo duomenis, reikia užtikrinti, kad tie jie yra tikri, tam tikslui reikia, jog PDF failas butų pasirašytas elektroniniu parašu.



Eil.Nr.	Data	totalCPU	freeCPU	runJob	waitJob	seAvailTB	seUsedTB
1	2010-01-01	6	18	6	0	0.10	0.00
2	2010-01-02	6	18	6	0	0.10	0.00
3	2010-01-03	6	21	3	0	0.10	0.00
4	2010-01-04	6	18	2	0	0.10	0.00
5	2010-01-05	6	22	1	0	0.10	0.00
6	2010-01-06	6	24	0	0	0.10	0.00
7	2010-01-07	6	24	0	0	0.10	0.00
8	2010-01-08	6	24	0	0	0.10	0.00
9	2010-01-09	6	12	4	0	0.10	0.00
10	2010-01-10	6	4	20	0	0.10	0.00
11	2010-01-11	6	11	12	15	0.10	0.00
12	2010-01-12	6	22	0	7	0.10	0.01
13	2010-01-13	6	12	0	1	0.10	0.01
14	2010-01-14	6	11	12	4	0.10	0.01
15	2010-01-15	6	12	6	1	0.10	0.01
16	2010-01-16	6	0	4	0	0.10	0.01
17	2010-01-17	6	19	5	0	0.10	0.01
18	2010-01-18	6	14	2	11	0.10	0.01
19	2010-01-19	6	16	0	1	0.10	0.01
20	2010-01-20	6	7	1	0	0.10	0.01
21	2010-01-21	6	15	1	0	0.10	0.01
22	2010-01-22	6	11	1	0	0.10	0.01
23	2010-01-23	6	12	0	0	0.10	0.01
24	2010-01-24	6	10	2	0	0.10	0.01
25	2010-01-25	6	15	1	13	0.10	0.01
26	2010-01-26	6	10	1	0	0.10	0.01
27	2010-01-27	6	10	1	0	0.10	0.01
28	2010-01-28	6	7	9	0	0.10	0.01
29	2010-01-29	6	8	8	0	0.10	0.01

27 pav. Klasterio duomenys pdf formate

PDF failo suformavimui naudojama TCPDF biblioteka. Sukuriamas PDF formavimo objektas, sudedami reikalingi nustatymai: šriftas, antraštės, paraštės, tada surenkami klasterių duomenys, sugeneruojamas html tekstas ir jis paduodamas PDF formavimui. Gavus visus duomenis kreipiamasi į metodą, kuris suformuoja pasirašyta elektroniniu parašu PDF failą.

3.7. Veiksmų įrašų sistema

Veiksmų įrašų sistema - tai būdas saugumui pagerinti. Kiekvienas vartotojo atliktas veiksmas išsaugojamas šioje sistemoje.

data	veiksmas	vartotojas
2010-04-21 18:46:25	Užkrautas 'grafikas.php'	valdas
2010-04-21 23:12:25	Užkrautas 'graf.php'	valdas
2010-04-21 23:33:54	Užkrautas 'graf.php'	valdas
2010-04-21 23:44:21	Užkrautas 'graf.php'	valdas
2010-04-21 23:46:17	Užkrautas 'graf.php'	valdas
2010-04-21 23:46:23	Užkrautas 'graf.php'	valdas
2010-04-21 23:50:50	Užkrautas 'graf.php'	valdas
2010-04-21 23:51:00	Užkrautas 'klasteris.php'	valdas
2010-04-21 23:51:07	Užkrautas 'QoS.php'	valdas
2010-04-21 23:51:09	Užkrautas 'klasteris.php'	valdas
2010-04-25 21:29:55	Užkrautas 'priv.php'	valdas
2010-04-25 21:29:56	Užkrautas 'graf.php'	valdas
2010-04-25 21:30:16	Užkrautas 'graf.php'	valdas
2010-04-25 23:36:45	Užkrautas 'priv.php'	valdas
2010-04-25 23:36:47	Užkrautas 'graf.php'	valdas
2010-04-25 23:36:56	Užkrautas 'graf.php'	valdas
2010-04-25 23:45:46	Užkrautas 'priv.php'	valdas
2010-04-25 23:45:47	Užkrautas 'graf.php'	valdas
2010-04-25 23:54:54	Užkrautas 'pdf sukurimas'	valdas

28 pav. Veiksmų įrašų sistema

„Veiksmų įrašų sistema“ - tai geras būdas atsekti, koks vartotojas buvo paskutinis prisijungęs ir kokius veiksmus atliko.

3.8. Parametrų vaizdavimo pavyzdys

Nustatytų parametrų atvaizdavimas lentele. Pagal datą pateikiami pasirinkti klasterio duomenys.

Duomenų atvaizdavimo lentelių pagalba pavyzdys:

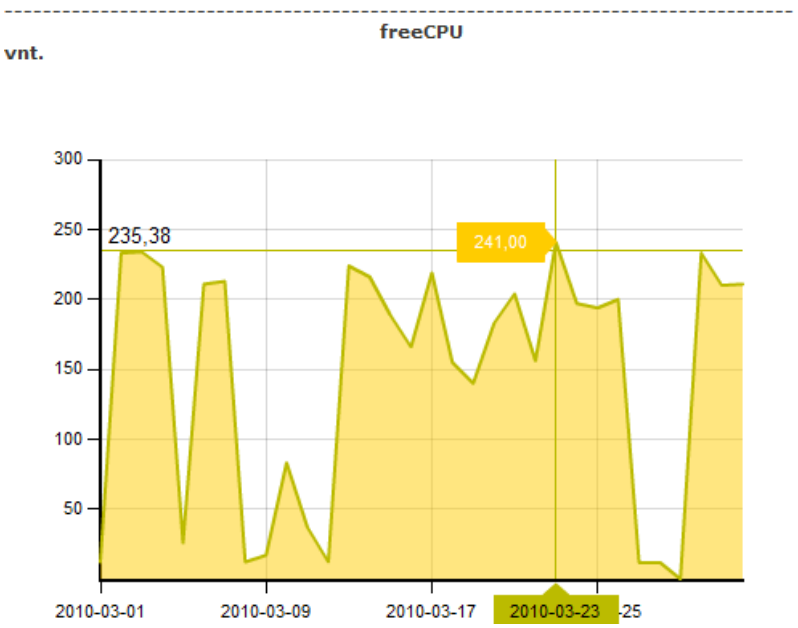
Eil. Nr.	Data	totalCPU	freeCPU	runJob	waitJob
1	2010-03-01	63	12	275	291
2	2010-03-02	63	233	54	0
3	2010-03-03	63	234	53	0
4	2010-03-04	63	223	64	0
5	2010-03-05	63	26	261	0
6	2010-03-06	63	211	76	0
7	2010-03-07	63	213	74	0
8	2010-03-08	63	12	275	794
9	2010-03-09	63	17	270	0
10	2010-03-10	63	83	204	0
11	2010-03-11	63	37	250	0
12	2010-03-12	63	12	275	29
13	2010-03-13	63	224	63	0
14	2010-03-14	63	216	71	0
15	2010-03-15	63	189	98	0
16	2010-03-16	63	166	121	0
17	2010-03-17	63	219	68	0
18	2010-03-18	63	155	132	0
19	2010-03-19	63	140	147	0
20	2010-03-20	63	183	104	0
21	2010-03-21	63	204	83	0
22	2010-03-22	63	156	131	0
23	2010-03-23	63	241	46	0
24	2010-03-24	63	197	90	0
25	2010-03-25	63	194	93	0

29 pav. T2_Estonia klasterio duomenys

Klasterių duomenys vaizduojami lentelėje, kurioje pateikiami nustatyti stebėjimui parametrai bei stebėjimo laikotarpis. Vaizduojami pasirinkti parametrai dienos tikslumu.

Grafinio vaizdavimo pavyzdys:

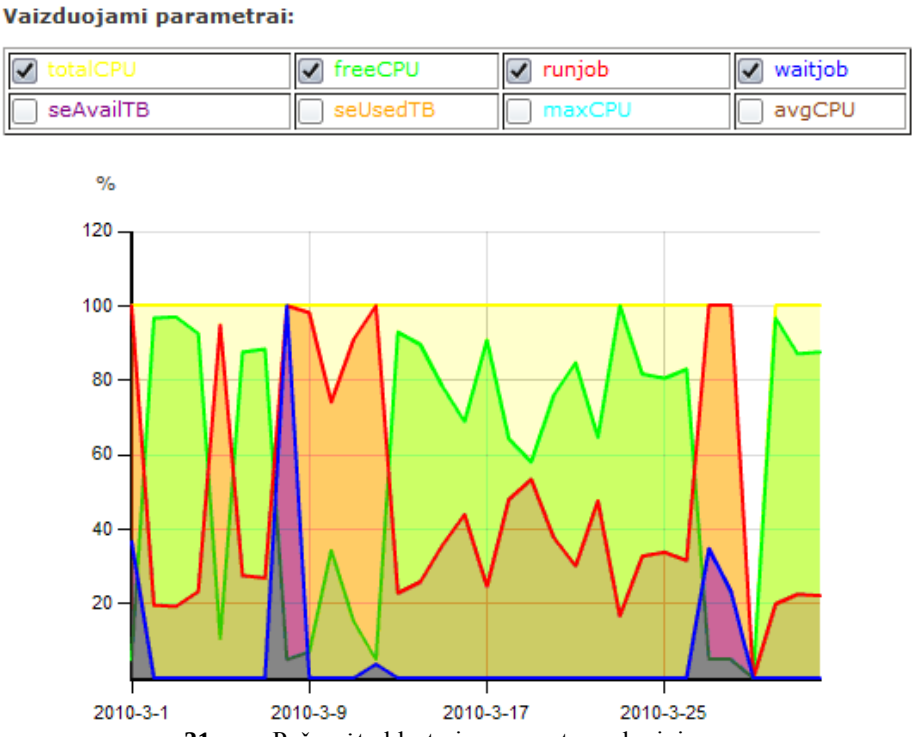
Vaizdžiam parametrų peržiūrėjimui naudojamas grafinis pateikimo būdas.



30 pav. T2_Estonia klasterio duomenys

Nustatytus parametrus galima pasižiūrėti interaktyvių grafikų pagalba. Grafiką pele galima išsididinti ir peržiūrėti tas dienas, kurios domina vartotoją didesniu tikslumu.

Klasterio parametrų palyginimas

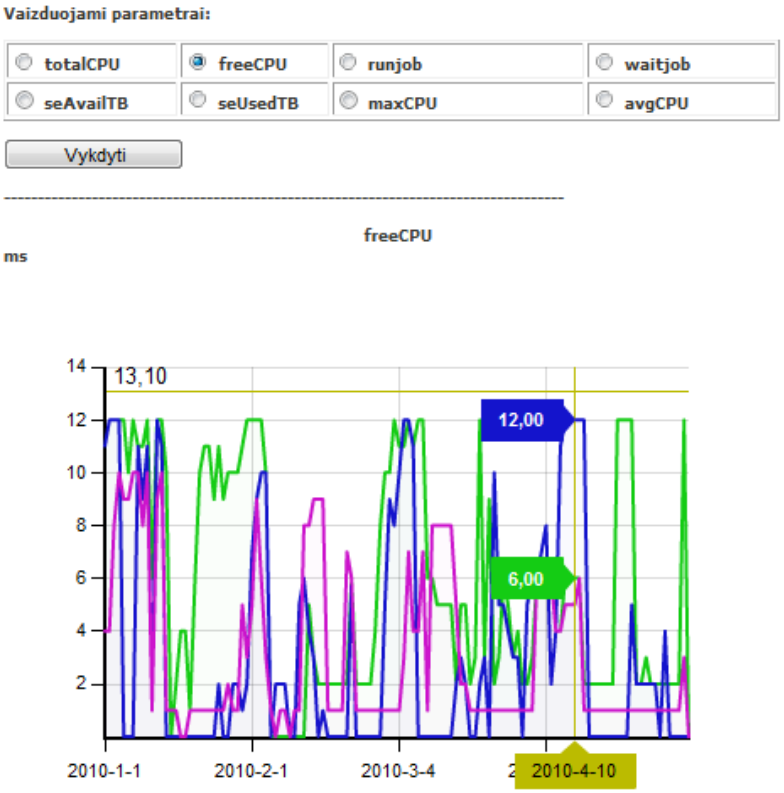


31 pav. Pažymėtų klasterio parametrų palyginimas

Klasterių parametrų palyginimo grafikas (31 pav.) procentais, skirtingomis spalvomis palygina klasterio parametrus duotu laikotarpiu.

Klasterių palyginimas

Klasterių palyginimas greitai suteikia informaciją, kuomet klasteris atlieka daugiau užduočių, turi laisvos vietos ar laisvų CPU.



32 pav. Pažymėtų klasterių palyginimas

Kalsterių palyginimas - tai patogus būdas sužinoti, kurį klasterį naudoti, kad vartotojo pateikta užduotis butų atlikta per trumpesnį laiką.

3.9. Išvados

- realizacijos dalyje pateiktos visos sistemos galimybės; pagal jau esančias sistemas duomenys pateikiami dviem būdais: lentele ir grafikais;
- prisijungimas prie sistemos yra išskirtinai apsaugotas specialiu sertifikatu, tokio saugumo nėra kitose sistemose;
- kaip naujovė, palyginus su kitomis sistemomis, yra parametrų išsaugojimas PDF faile, kuris duomenų autentiškumą užtikrina elektroniniu parašu.

4. Eksperimentas ir testavimas

Sukūrus naują BalticGrid monitoringo sistemą, reikia atlikti testavimą ir palyginimą su kitomis sistemomis. Pirmoje eksperimento dalyje palyginama naujai sukurta sistema su jau esančiomis populiariausiomis monitoringo sistemomis. Testavimo etape, atliekamas matavimas, kiek laiko yra formuojamas PDF failas. Tiriama, koks laiko skirtumas yra formuojant paprastą PDF failą, o kiek užtrunka formuojant pasirašytą PDF failą elektroniniu parašu. Duomenų išsaugojimas PDF faile yra naujovė monitoringo sistemose. Dar nė viena sistema neleidžia duomenų saugoti faile ir tuo labiau jokia sistema nepatvirtina elektroniniu parašu.

Pirmoji eksperimento dalis yra palyginimas *GRID* monitoringo sistemų pagal jų atliekamas funkcijas.

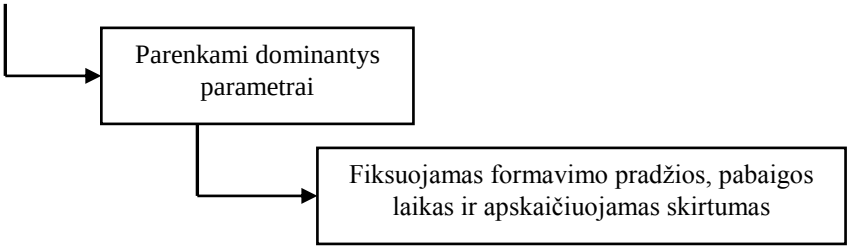
3 lentelė. Monitoringo sistemų atliekamos funkcijos

Funkcijos	MonALISA	Ganglia	Nagios	GridView	GridIce	BalticGrid
Duomenų vaizdavimas lentele	+		+		+	+
Duomenų vaizdavimas grafikais	+	+		+	+	+
Prisijungimui naudojama registracija					+	+
Prisijungimui naudojami sertifikatai						+
Galimas duomenų išsaugojimas į failą	+	+		+		+
Pasirašytas el. parašu duomenų išsaugojimas						+
Saugumui užtikrini naudojama veiksmų įrašų sistema						+
Galimas parametrų palyginimas						+
Galimas klasterių palyginimas	+					+

Kaip matome lentelėje, skirtingos monitoringo sistemos turi skirtingas galimybes. Dauguma parametrus vaizduoja lentelėse, taip pat beveik visos sistemos vaizdą pateikia grafiškai. Kai kurios leidžia parametrus išsaugoti faile, tačiau tik naujai sukurta BalticGrid monitoringo sistema išsaugotus duomenis pasirašo elektoriniu parašu. Parametrų palyginimą vaizduoja tik *MonALISA* sistema ir BalticGrid. Saugumo atžvelgiu jungiantis prie sistemos registruotų vartotojų reikalauja tik *GridIce*, bet taip pat ne visais atvejais. Lengvai galima pastebėti, kad naujai sukurta BalticGrid sistema yra efektinga vaizduojant, palyginant klasterių duomenis bei taip pat yra užtikrinti pagrindiniai saugumo elementai.

Kitas eksperimento etapas yra paskaičiavimas per kiek laiko yra suformuojamas PDF failas. Kreipiamas dėmesys kiek užtrunka suformuoti PDF failą su elektroniniu parašu ir kiek be jo.

Nustatomas klasteris ir vaizdavimo laikotarpis



333 pav. PDF formavimo schema

Eksperimentas atliktas su skirtingais duomenų ir lapų skaičiais. Pirmas bandymas atliktas su dviem parametrais ir 1, 2, 3, 4, 5, 10, 15, 20, 25, 30 puslapiais. Žemiau pateikiama lentelės, kur nurodomas P – formavimo pradžios laikas, G – formavimo pabaigos laikas ir S – laikas per kiek suformuojamas PDF failas.

4 lentelė. PDF be elektroninio parašo

data	veiksmas	vartotojas
2010-05-15 13:42:33	PDF formavimas(nepasirasytas) P: 13-42-31; G: 13-42-33; S: 2.8369160079956s.	valdas
2010-05-15 13:44:03	PDF formavimas(nepasirasytas) P: 13-43-57; G: 13-44-03; S: 5.8183990001678s.	valdas
2010-05-15 13:45:19	PDF formavimas(nepasirasytas) P: 13-45-11; G: 13-45-19; S: 8.7680941390991s.	valdas
2010-05-15 13:46:35	PDF formavimas(nepasirasytas) P: 13-46-24; G: 13-46-35; S: 11.724236898422s.	valdas
2010-05-15 13:48:42	PDF formavimas(nepasirasytas) P: 13-48-27; G: 13-48-42; S: 15.67844004631s.	valdas
2010-05-15 13:50:45	PDF formavimas(nepasirasytas) P: 13-50-16; G: 13-50-45; S: 29.492618942261s.	valdas
2010-05-15 13:53:49	PDF formavimas(nepasirasytas) P: 13-53-06; G: 13-53-49; S: 43.81058713913s.	valdas
2010-05-15 13:56:46	PDF formavimas(nepasirasytas) P: 13-55-47; G: 13-56-46; S: 59.174006109238s.	valdas
2010-05-15 14:01:18	PDF formavimas(nepasirasytas) P: 14-00-04; G: 14-01-18; S: 74.358201913834s.	valdas
2010-05-15 14:04:20	PDF formavimas(nepasirasytas) P: 14-02-52; G: 14-04-20; S: 90.102496156693s.	valdas

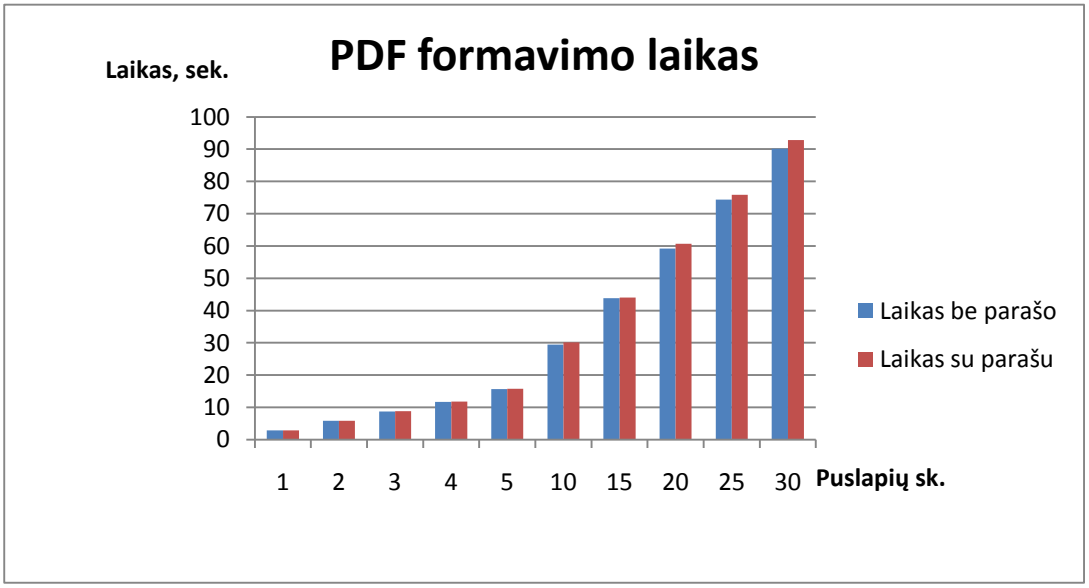
Atlikus testavimą, galima pastebėti, kad suformuoti 1 lapo PDF failą reikia apie 3 sekundžių, kiekvienas kitas lapas formavimo laiką pratęsė maždaug 3 sekundes. 4 lentelėje pateikiami laikai formuojant PDF failą be elektorinio parašo.

Failo formavimas su elektroniniu parašu užtrunka kiek ilgiau – mažiau nei sekundę. Testavimo duomenys pateikiami 5 lentelėje.

5 lentelė. PDF su elektroniniu parašu

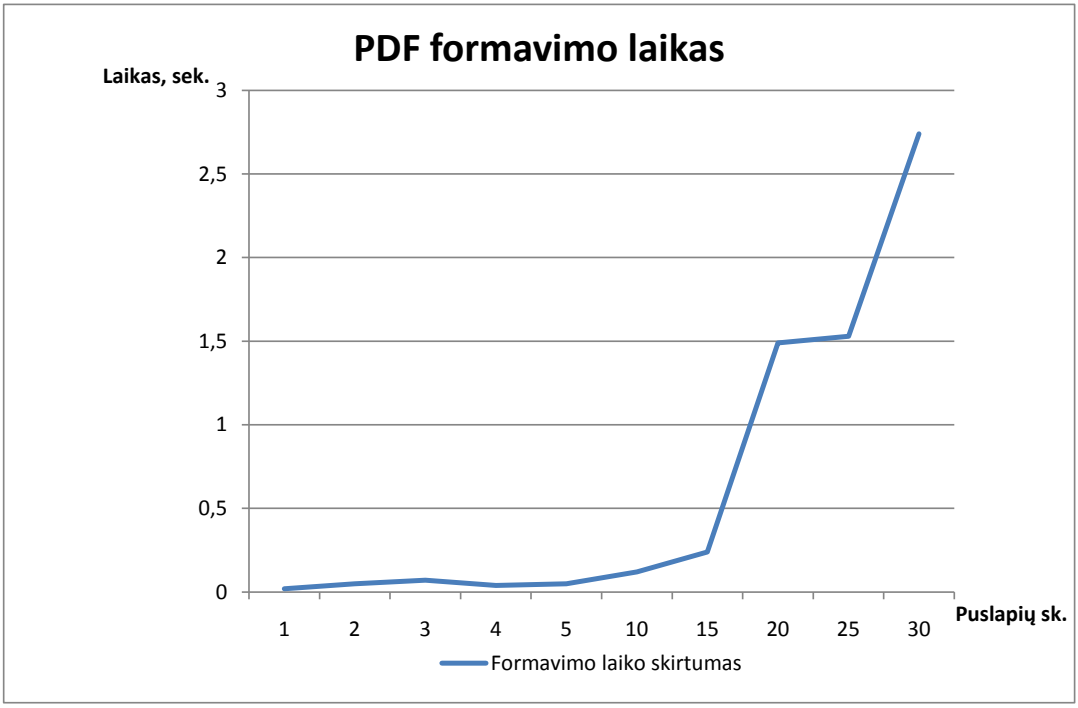
data	veiksmas	vartotojas
2010-05-15 14:16:01	PDF formavimas(pasirasytas) P: 14-15-58; G: 14-16-01; S: 2.8506270122528s.	valdas
2010-05-15 14:17:41	PDF formavimas(pasirasytas) P: 14-17-35; G: 14-17-41; S: 5.8628180885315s.	valdas
2010-05-15 14:20:35	PDF formavimas(pasirasytas) P: 14-20-26; G: 14-20-35; S: 8.8394668102264s.	valdas
2010-05-15 14:24:24	PDF formavimas(pasirasytas) P: 14-24-09; G: 14-24-24; S: 11.767242937088s.	valdas
2010-05-15 14:28:39	PDF formavimas(pasirasytas) P: 14-28-25; G: 14-28-39; S: 15.726662187576s.	valdas
2010-05-15 14:52:34	PDF formavimas(pasirasytas) P: 14-52-04; G: 14-52-34; S: 29.615616874695s.	valdas
2010-05-15 14:54:59	PDF formavimas(pasirasytas) P: 14-54-15; G: 14-54-59; S: 44.057330951691s.	valdas
2010-05-15 14:58:23	PDF formavimas(pasirasytas) P: 14-57-23; G: 14-58-23; S: 60.66842795372s.	valdas
2010-05-15 15:00:59	PDF formavimas(pasirasytas) P: 14-59-45; G: 15-00-59; S: 75.884227056503s.	valdas
2010-05-15 15:06:21	PDF formavimas(pasirasytas) P: 15-04-51; G: 15-06-21; S: 92.846750955582s.	valdas

Pateikta diagrama (34 pav.) parodo, kiek laiko trunka suformuoti PDF failą, pasirašytą elektroniniu parašu, bei kiek užtrunka tokį patį failą suformuoti be elektroninio parašo.



34 pav. PDF formavimo laikas

Iš diagramos matome, jog formuojant PDF failą su parašu laiko skirtumas yra tik šimtosios sekundės dalys. Toliau pateikiama diagrama (35 pav.) su kreive aiškiai parodo tikslų laikų skirtumą.



35 pav. PDF formavimo laiko skirtumas

Iš diagramos matome, jog laiko skirtumas yra praktiškai nepastebimas, su mažu duomenų kiekiu skiriasi tik sekundės šimtosiomis dalimis. Esant didesniam duomenų kiekiui, formavimo laikas prasitęsia beveik iki 3 sekundžių.

Toks pats eksperimentas buvo atliktas su didesniu kiekiu parametrų. Pirmi skaičiavimai (nurodyta 4 ir 5 lentelėse) buvo vykdomi su 2 parametrais, o antri skaičiavimai (nurodyta 6 ir 7 lentelėse) - su 4 parametrais. Nors puslapių kiekis tas pats, tačiau formuojant PDF su didesniu parametrų kiekiu laiko atžvilgiu užtrunkama ilgiau. Vieno lapo duomenų suformavimas užtrunka daugiau kaip 4 sekundes. 6 lentelėje pateikiami formavimo laikai nepasirašyto failo.

6 lentelė. PDF 4 parametrų be elektroninio parašo

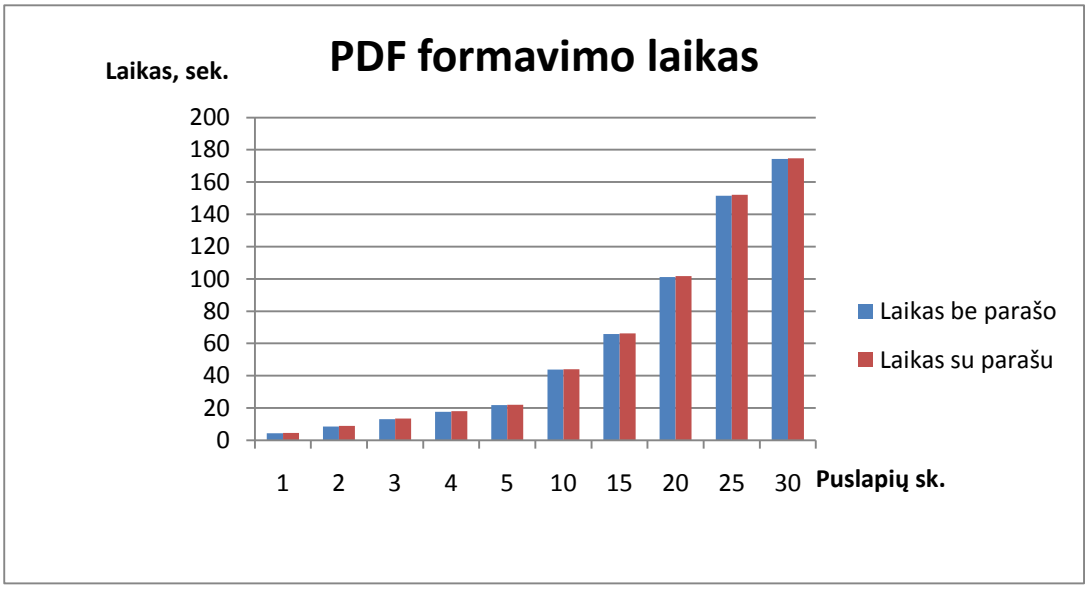
data	veiksmas	vartotojas
2010-05-18 01:01:14	PDF formavimas(nepasirasytas) P: 01-01-09; G: 01-01-14; S: 4.3401038646698s.	valdas
2010-05-18 01:02:10	PDF formavimas(nepasirasytas) P: 01-02-01; G: 01-02-10; S: 8.5276759719849s.	valdas
2010-05-18 01:02:57	PDF formavimas(nepasirasytas) P: 01-02-43; G: 01-02-57; S: 13.055463933945s.	valdas
2010-05-18 01:04:33	PDF formavimas(nepasirasytas) P: 01-04-15; G: 01-04-33; S: 17.641764879227s.	valdas
2010-05-18 01:05:27	PDF formavimas(nepasirasytas) P: 01-05-05; G: 01-05-27; S: 21.777957201004s.	valdas
2010-05-18 01:07:16	PDF formavimas(nepasirasytas) P: 01-06-32; G: 01-07-16; S: 43.777952194214s.	valdas
2010-05-18 01:09:22	PDF formavimas(nepasirasytas) P: 01-08-16; G: 01-09-22; S: 65.84486413002s.	valdas
2010-05-18 01:11:56	PDF formavimas(nepasirasytas) P: 01-10-13; G: 01-11-56; S: 101.09078407288s.	valdas
2010-05-18 01:17:49	PDF formavimas(nepasirasytas) P: 01-15-17; G: 01-17-49; S: 151.52087402344s.	valdas
2010-05-18 01:19:12	PDF formavimas(nepasirasytas) P: 01-16-17; G: 01-19-12; S: 174.28407502174s.	valdas

7 lentelėje pateikiami pasirašytų failų formavimo laikai. Nors palyginus su dviejų parametrų formavimu, trukmė yra beveik 2 sekundėmis ilgesnė, tačiau parašo padėjimo laikas nuo parametrų kiekio nepriklauso.

7 lentelė. PDF 4 parametrų su elektroniniu parašu

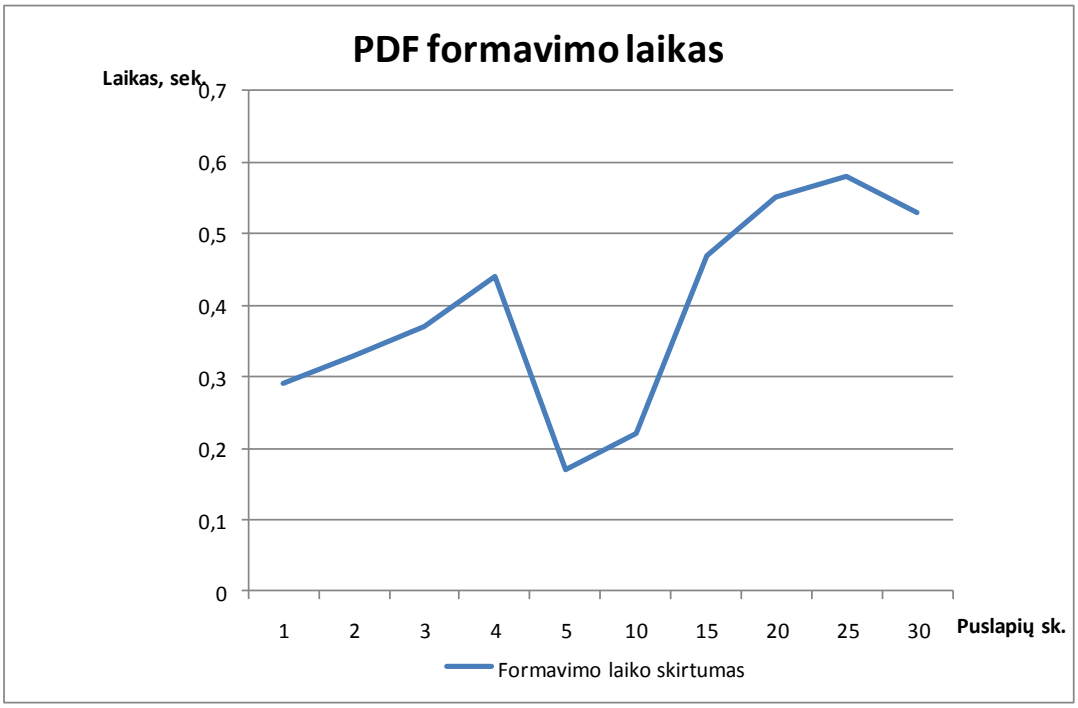
data	veiksmas	vartotojas
2010-05-17 23:40:50	PDF formavimas(pasirasytas) P: 23-40-46; G: 23-40-50; S: 4.6334621906281s.	valdas
2010-05-17 23:41:48	PDF formavimas(pasirasytas) P: 23-41-39; G: 23-41-48; S: 8.8565681934357s.	valdas
2010-05-17 23:43:00	PDF formavimas(pasirasytas) P: 23-42-47; G: 23-43-00; S: 13.427853870392s.	valdas
2010-05-17 23:44:36	PDF formavimas(pasirasytas) P: 23-44-18; G: 23-44-36; S: 18.080350160599s.	valdas
2010-05-17 23:45:34	PDF formavimas(pasirasytas) P: 23-45-11; G: 23-45-34; S: 21.943113994598s.	valdas
2010-05-17 23:47:55	PDF formavimas(pasirasytas) P: 23-47-11; G: 23-47-55; S: 43.99281001091s.	valdas
2010-05-17 23:49:13	PDF formavimas(pasirasytas) P: 23-48-06; G: 23-49-13; S: 66.317378044128s.	valdas
2010-05-17 23:51:49	PDF formavimas(pasirasytas) P: 23-50-07; G: 23-51-49; S: 101.64304804802s.	valdas
2010-05-17 23:57:39	PDF formavimas(pasirasytas) P: 23-55-07; G: 23-57-39; S: 152.1003370285s.	valdas
2010-05-17 23:59:06	PDF formavimas(pasirasytas) P: 23-56-10; G: 23-59-06; S: 174.81870999336s.	valdas

PDF failo formavimo laikus su 4 parametrais parodo 36 pav. Matyti aiškus laiko skirtumas ypač su didesniu duomenų kiekiu. Suformuoti 30 lapų užtrunka net apie 3 minutes.



36 pav. PDF formavimo laikas su 4 parametrais

Kaip jau anksčiau buvo minėta, nors failo formavimas užtrunka ilgiau, tačiau skirtumas tarp pasirašytų elektroniniu parašu failų yra labai mažas (mažiau nei 1 sekundė). Skirtumą iliustruoja 37 pav. pavaizduota kreivė.



37 pav. PDF formavimo laiko skirtumas 4 parametrų

Laiko skirtumų kreivė parodo, kad duomenų kiekis ne visada lemia elektroninio parašo pasirašymo laiką. Kartais, nors duomenų ir daugiau, tačiau pasirašymas įvyksta labai greitai. PDF failo formavimo greitį taip pat lemia serverio apkrautumas.

4.1. Išvados

- atlikus eksperimentą įsitikinta, jog naujai sukurta BalticGrid sistema atlieka daugiau funkcijų nei jau esančios;
- testavimo metu atliktas laiko matavimas formuojant pasirašytą elektroniniu parašu arba nepasirašytą PDF failą, pastebėta, kad pasirašymo laikas užima mažiau nei sekundę;
- atlikus matavimus pastebėta, jog PDF failo formavimas priklauso tik nuo duomenų kiekio, o ne nuo to, ar failas pasirašomas ar nepasirašomas elektroniniu parašu.

Išvados

1. Apžvelgus *GRID* monitoringo sistemas, pastebėta, kad nėra tokios sistemos, kuri užtikrintų duomenų saugumą bei konfidencialumą, todėl naujoje BalticGrid sistemoje duomenys patvirtinami elektroniniu parašu.
2. Monitoringo sistemų saugumui užtikrinti yra taikomos priemonės: Viešojo rakto infrastruktūra, ACL būdas ir viešojo rakto kriptografija. Šios priemonės patikimai užtikrina monitoringo sistemos saugumą.
3. Apžvelgus monitoringo sistemų architektūras bei atsižvelgus į rekomenduojamą architektūrą, sukurta nauja sistemą atitinkanti architektūra pagal saugumo bei funkcionalumo reikalavimus.
4. Pritaikius papildomus saugumo kriterijus, sukurta nauja BalticGrid monitoringo sistema. Sistemos saugumą užtikrina prisijungimo sertifikatas, veiksmų įrašų registras bei duomenų autentiškumui ir konfidencialumui garantuoti formuojamas pasirašytas elektroniniu parašu PDF failas.
5. Eksperimento metu pagrįsta, jog naudojant saugumo priemones, tokias kaip sertifikatas ir elektroninis parašas, sistemos veikimas laiko požiūriu kinta labai mažai - 1-3 sekundes.

Literatūra

1. *MonALISA* agentų platforma. Prieiga per Internetą: <http://monalisa.caltech.edu/monalisa__System_Design__agents_system.html >
2. Imamagic, E.; Radic, B.; Dobrenic D.; 2005; *CRO-GRID Grid Monitoring Architecture* University Computing Centre, University of Zagreb, Croatia Prieiga per Internetą:< http://ieeexplore.ieee.org/xpl/RecentCon.jsp?punumber=9984 >
3. Casey, J.; Imamagic, E.; Neilson, I.; 2008; *Advances in Monitoring of Grid Services in WLCG,* International Conferenceon Computingin High Energyand Nuclear Physics (CHEP'07);
4. Andreozzi, S.; Fattibene, E.; Misurelli, G.; Rubini, L. G.; 2005 *GridICE: Requirements, Architecture and Experience of a Monitoring Tool for Grid Systems;*
5. Ni Guangbao, Ma Jie, Li Bo,; 2004; *GridView: A Dynamic and Visual Grid Monitoring System,* Institute of Computing Technology, Chinese Academy of Sciences Prieiga per Internetą: <http://ieeexplore.ieee.org/xpl/RecentCon.jsp?punumber=9244 >
6. Lock R.; Sommerville I,; 2002; *Grid Security and its use of X.509 Certificates* Department of Computer Science Lancaster University;
7. Imtiaz, A.; Sajid and Dr. Arshad; A. Shahid; *List of Quality Attributes for Grid Monitoring Tools;* FAST-National University of Computer and Emerging Sciences, Islamabad, Pakistan;
8. GridIce platforma. Prieiga per Internetą: < http://www.italiangrid.org/middleware/gridice >
9. Lang B.; Foster I.; Siebenlist F.; Ananthakrishnan R.; Freeman T.; 2006; *A Multipolicy Authorization Framework for Grid Security,* Mathematics and Computer Science Division; psl. 269 – 272 ;
10. Anirban Chakrabarti; 2007; *Grid computing security;* ISBN 978-3-540-44492-3 Springer Berlin Heidelberg New York;
11. Volpato G.; Grimm Ch.; 2004; *Definition of Security Levels;* Chapter 3 of the Mental Health (Care and Treatment) (Scotland);
12. Welch, V., Foster I., Kesselman, C., Mulmo O., 2004; *X.509 Proxy Certificates for Dynamic Delegation;* National Center for Supercomputing Application,University of Illionois;
13. Andreson S; Bohren J.; Chanliau M; 2005; *Web Services Trust Language (WS-Trust);* Actional Corpoation, BEA Systems, Inc.;

14. Foster I.; Kesselman C.; 2004; *The Grid 2: Blueprint for a New Computing Infrastructure;* Elsevier, San Francisco; ISBN: 1558609334;
15. Esteban Talavera González, 2007; *Credential Mapping in Grids*, Center for Parallel Computers (PDC) Royal Institute of Technology (KTH) Stockholm;
16. Van Dyke J.; 2006; *An Overview of Secure Shell*, Innovative Solutions International;
17. Xiaopeng W.; Junzhou L.; Aibo S.; Teng M.; 2005; *Semantic Access Control in Grid Computing*, Proceedings of the 2005 11th International Conference on Parallel and Distributed Systems;
18. Hoon Wei Lim, PhD, 2006; *On the Application of Identity-Based Cryptography in Grid Security*, Information Security Group, Department of Mathematics Royal Holloway, University of London;
19. Ali Nasrat Haidar, 2003; *Critical Evaluation of Current Approaches to Grid Security* MSc Secure Electronic Commerce Royal Holloway, University of London;
20. Gollman D.; 1999; *Computer Security*, John Wiley Publishers; ISBN:0-471-97844-2; psl. 320;
21. Ganglia [žiūrėta: 2009 m. birželio 12d.]. Prieiga per Internetą: <http://ganglia.sourceforge.net>
22. MonALISA [žiūrėta: 2009 m. birželio 12d.]. Prieiga per Internetą: <http://monalisa.cacr.caltech.edu>
23. Anirban Chakrabarti; 2007; *Grid computing security;* ISBN 978-3-540-44492-3 Springer Berlin Heidelberg New York

Summary

This research paper deals with security technologies used in monitoring systems. As *GRID* network is developing rapidly, secure information transfer in *GRID* network still remains as one of the most crucial aspects. For this reason, the main aim of this paper is to adopt the most effective methods in order to create secure *BalticGrid* monitoring system that will ensure authenticity, integrity and confidentiality of information. First of all, the vulnerabilities of existing monitoring systems were examined. Further, the main safety criteria for monitoring systems were stated. Later, the analysis of architectures used in monitoring systems was performed and, accordingly, the most suitable architecture for modern Grid monitoring network was suggested. Finally, *BalticGrid*, a secure system designed to monitor network parameters, was created. Its security is ensured by the fact that it can be approached only by users possessing either *BalticGrid* or *LitGrid* certificates. Additionally, the event register is enabled; its function is to store information about all actions that each user has performed in the system. A special feature of *BalticGrid* includes saving cluster's parameters in PDF file format signed with electronic signature. In this situation, electronic signature ensures complete confidentiality of data.

Santrumpų sąrašas

ACL *(Access Control List)* – prieigos kontrolės sąrašas

CA *(Certificate Authority)* – sertifikatus išduodanti organizacija

CAS *(Code Access Security)* – Kodo prieigos saugumas

EEC *(End Entity Certificate)* – galinio vartotojo sertifikatas išduotas CA.

GIIS *(Grid Index Information Service)* – GRID indekso informacijos paslauga

GLUE *(Grid Laboratory for a Uniform Environment)* – GRID laboratorija universaliajai aplinkai

GMA *(grid monitoring architecture)* – *GRID* monitoringo architektūra

GMETAD *(Ganglia Meta Daemon)* – Ganglia duomenų daimonas

GMOND *(Ganglia Monitoring Daemon)* – Ganglia monitoringo daimonas

GRID – tai sistema, kuri integruoja ir valdo resursus, kuriuos kontroliuoja įvairūs domenai ir sujungti kompiuteriniai tinklai.

GRIS *(*Grid Resource Information Service*)* – GRID išteklių informacijos paslauga

GSI *(Globus Security Infrastructure)* **–** GRID saugumo infrastruktūra

GT4 *(Globus Toolkit 4.0)* - tai „atviro kodo“ įrankis skirtas Globus Alliance išrastų ir pateiktų GRID kūrimui

LAN *(Local Area Network)* – uždarasis tinklas, aptarnaujantis mažoje teritorijoje esančius vienos organizacijos vartotojus

LDAP *(Lightweight Directory Access Protocol)* – protokolas naudojamas kataloginių duomenų priėjimui

PKI *(Public Key Infrastructure)* – privataus rakto infrastruktūra

RBAC *(Role-based Access Control)* – vaidmenimis paremta prieigos kontrolė

RRD *(Round Robin Database)* – įrankių rinkinys duomenų bazėms valdyti

SAML *(Security Assertion Markup Language)* – XML paremtas standartas skirtas autentifikacijos ir autorizacijos duomenų apsikeitimui tarp domenų.

SFTP *(SSH File Transfer Protocol)* – klientas-serveris tipo protokolas, leidžia siųsti failus iš ir į serverį panaudojant TCP/IP

SNMP *(Simple Network Management Protocol)* – tinklo protokolų rinkinys, naudojamas tinklo įrenginių valdymui

SOAP (*Simple Object Access Protocol*) – protokolas, naudojamas visokių tipų duomenų tarp programų siuntimui.

TCP *(Transmission Control Protocol)* – vienas iš pagrindinių protokolų, esančių *Internetinių protokolų rinkinyje,* tarpinis lygis tarp IP ir aplikacijos bei priklausantis transportavimo lygmeniui

TCPDF – tai PDF dokumentų generavimo PHP klasė

TLS *(Transport Layer Security)* **–** TLS protokolas užtikrina slaptumą ir integralumą siunčiant duomenis

WAN *(wide area network)* – ryšio kanalais sujungtų mažesnių tinklų visuma

WS-I (*Web Services Interoperability*) – tai pramoninis konsorciumas, kuriam suteikta privilegija skatinti veiksnumą tarp daugybės tinklo paslaugų specifikacijų. WS-I nenustato tinklo paslaugų standartų, jis pateikia nurodymus ir išbando jų tarpusavio veiksnumą

WS-SecureConversation – tai tinklo paslaugos specifikacija, kurią sukūrė IBM ir kiti. Ji veikdama kartu su WS-Security (WS-Saugumu), WS-Trust (WS-Patikimums) ir WS-Policy (WS-Politika) leidžia kurti ir dalintis saugumo kontekstais

WS-Security *(Web Services Security)* – internetinių paslaugų sauga

X.509 – sertifikatas, aprašantis asimetrinių kriptografinių algoritmų naudojimą pasirašant elektroniniu parašu

XAML (eXtensible Access Control Markup Language*)* – XML paremta sąsajų aprašomoji kalba

XML (Extensible Markup Language) – rekomenduojama bendros paskirties duomenų struktūrų bei jų turinio aprašomoji kalba

Paveikslų sąrašas

Lentelių sąrašas

Priedai

„MOKSLAS – LIETUVOS ATEITIS“. 2009, Nr. 2 (2)
INFORMATIKA
Mokslinių straipsnių rinkinys ISSN 2029-2341 (print) / ISSN 2029-2252 (online)

GRID MONITORINGAS UŽTIKRINANT DUOMENŲ SAUGUMĄ

Kęstutis Paulikas[1], Donatas Sandonavičius[2], Gytis Vilutis[3], Waldemar Wolyniec[4]
[1,3]docentas, [2]doktorantas, [4]magistrantas
Kauno technologijos universitetas,
el. p. [4]waldemar.wolyniec@gmail.com

Anotacija. Aptartos populiariausios *Grid* monitoringo sistemos, pateikta aiški jų architektūrų analizė, išryškinti kiekvienos sistemos privalumai, bei trūkumai. Paaiškinti monitoringo sistemų veikimo principai, atsižvelgiant į duomenų saugumo užtikrinimą juose bei vartotojo sąsajos patogumą, paaiškinta stabilumo svarba. Aprašytos kai kuriose sistemose panaudojamos technologijos, aprašoma tokio pasirinkimo nauda. Akcentuojamos priemonės, kuriomis užtikrinamas kiekvienos sistemos vartotojų saugumas. Paaiškinta kuo monitoringo sistemos skiriasi tarpusavyje, kokios jų populiarumo priežastys, išskirtos skirtingos panaudojimo sritys, kuriose kiekviena konkreti sistema yra labiausiai tinkama. Pateikiama kiekvienos sistemos grafinė sąsaja.

Reikšminiai žodžiai: *GRID* monitoringas, saugumas, MonAlisa, Ganglia, GridView, GridIce, Nagios.

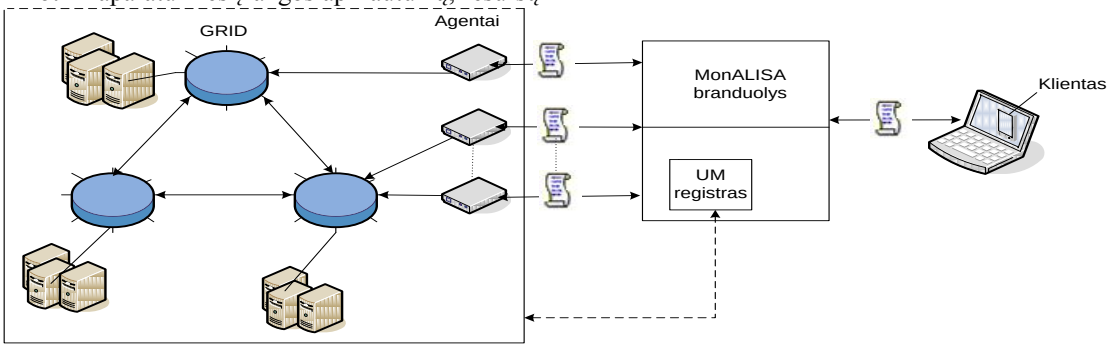
Įvadas

Sparčiai plintant *GRID* tinklui vis svarbiau tampa užtikrinti informacijos keliavimo tinkle saugumą. Informacijos priėjimo srautas kai kuriose sistemose užtikrinamas panaudojant autentifikaciją ir autorizaciją. Norint saugiai naudotis *GRID* tinklo teikiamomis galimybėmis, itin svarbu yra pasirinkti tinkamą monitoringo sistemą, turinčią visas reikalingas savybes ir pasižyminčią stabilumu.

Sukurta daug monitoringo sistemų, tačiau dirbama *GRID* tinkle ir aktualios tos monitoringo sistemos, kurias galima pritaikyti arba jos sukurtos būtent *GRID* tinklui. *GRID* monitoringo sistemos nuo tinklo parametrų stebėjimų sistemų skiriasi tuo, kad *GRID* monitoringo sistemai aktualūs ne tik tinkliniai parametrai. *Gride* aktualu žinoti ir aparatūrinės įrangos apkrautumą, resursų stovį ir t.t. Dauguma tinklui stebėti sukurtų sistemų to negali. Iš *GRID* tinklui skirtų naudoti monitoringo sistemų apžvelgsime *MonALISA, Ganglia, GridIce, GridView* bei *Nagios.* Šios monitoringo sistemos parinktos, todėl, kad tai vienos iš plačiausiai naudojamų (ne mažiau kaip 10 žinomų *GRID* tinklų) *GRID* tinkluose monitoringo sistemų.

Populiariausios GRID tinkluose naudojamos monitoringo sistemos

GRID tinklo stebėjimo sistemų yra gana daug. Pačios populiariausios ir turinčios daugiausia galimybių yra: *MonALISA, Ganglia, GridIce, GridView* bei *Nagios (1,3,5,7,9 pav.).*



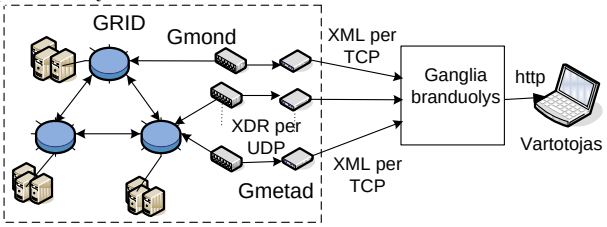
1 pav. MonALISA architektūra

Trumpai apie šias sistemas:

MonALISA stebėjimo sistema (1 pav.) skirta stebėti realiu laiku vykstančius procesus *GRID* tinkle, matyti esamą *GRID* tinklo situaciją, resursų parametrus. Taip pat naudojant šią stebėjimo sistemą patogu lyginti skirtingų klasterių parametrų reikšmes, tam specialiai įdiegtas įrankis. Tačiau, MonALISA stebėjimo sistemoje (2 pav.) matomi duomenys yra ne senesni kaip savaitės senumo.

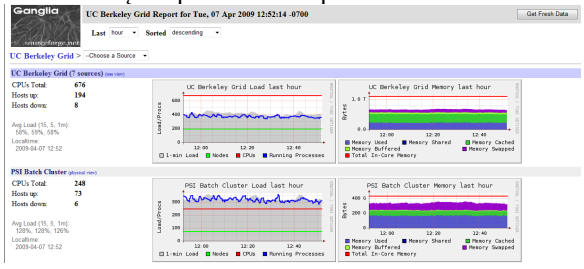
2 pav. MonALISA stebėjimo sistema

Ganglia (*Imamagic, Radic, Dobrenic; 2005*) stebėjimo sistema (3 pav.) skirta stebėti kompiuterių tinklo bei jo mazgų parametrams. Joje galima stebėti tinklo mazgų esamų resursų parametrų, jų apkrovų bei kitų techninių parametrų istorinius duomenis.



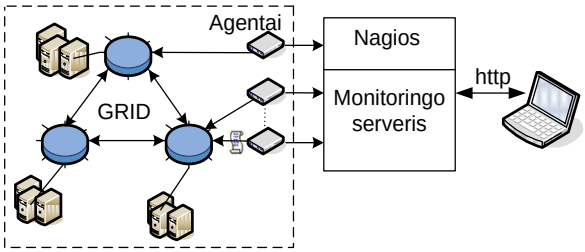
3 pav. Ganglia architektūra

Kaip pvz.: procesorių spartą, tinklo apkrovą, disko talpą ir pan. Taip pat *Ganglia* suteikia informaciją apie operacines sistemas ir kompiuterinę įrangą. Ganglia monitoringo sistemoje (4 pav.) galima stebėti nuo sistemos paleidimo, iki to momento, kada buvo atidarytas monitoringo sistemos langas, ar iki momento, kol buvo išjungti duomenų rinkimo moduliai. Taigi, galima stebėti viso duomenų kaupimo laikotarpio duomenis.



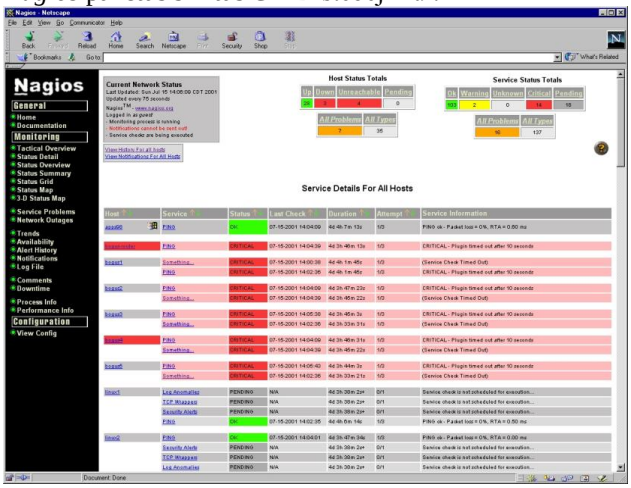
4 pav. Ganglia stebėjimo sistema

Nagios (*Casey, Imamagic, Neilson, 2008*) stebėjimo sistema (5 pav.) skirta stebėti kompiuterių tinklo bei jo mazgų parametrams. Joje galima stebėti tinklo mazgų esamų resursų parametrų, jų apkrovų bei kitų techninių parametrų istorinius duomenis. Kaip pvz.: procesorių sparta, tinklo apkrovą, disko talpą ir pan.



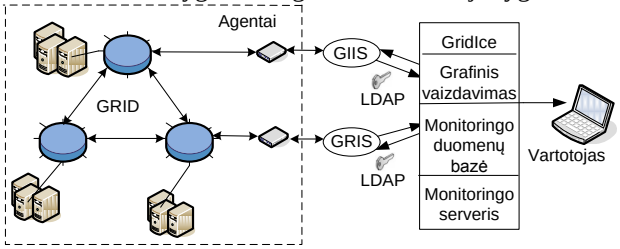
5 pav. Nagios architektūra

Šioje monitoringo sistemoje (6 pav.) taip pat kaupiami visi istoriniai duomenys, nuo to momento, kuomet sistema buvo paleista. *gLite* gamintojai ruošia *Nagios* paketus skirtus *GRID* stebėjimui.



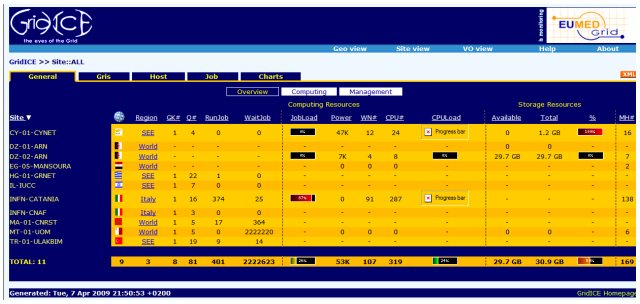
6 pav. Nagios stebėjimo sistema

GridIce (*Andreozzi, Fattibene, Misurelli, Rubini, 2005*) (7 pav.) stebėjimo įrankis suprojektuotas atsižvelgiant į reikalavimus, kuriuos pateikė įvairių tipų vartotojai, kur kiekvienas iš jų dirba skirtinguose *GRID* abstrakcijos lygmenyse, tokiuose kaip virtualios organizacijos lygmuo, *GRID* operacijų centro lygmuo, puslapio administravimo lygmuo, ir galutinio vartotojo lygmuo.



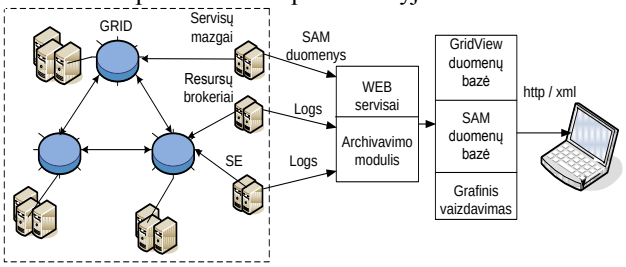
7 pav. GridIce architektūra

GridIce kaupia istorinius duomenis nuo pat sistemos paleidimo pradžios (8 pav.), taigi vartotojas gali peržvelgti, visus sistemoje sukauptus istorinius duomenis.



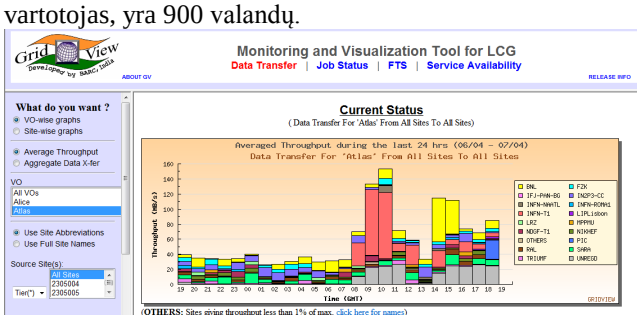
8 pav. GridIce stebėjimo sistema

GridView (*Guangbao, Jie, Bo; 2004*) kuriamas tam, kad kauptų informaciją heterogeninių šaltinių panaudojimui ir paskirstytųjų resursų *GRID* aplinkoje konfigūracijos informaciją. Sistemos veikimo architektūra pavaizduota 9 paveikslėlyje.



9 pav. GridView architektūra

Šioje sistemoje kaupiami duomenys (10 pav.) taip pat nuo sistemos gyvavimo pradžios stebimame tinkle, tačiau maksimalus rėžis, kurį vienu metu gali apžvelgti vartotojas, yra 900 valandų.



10 pav. GridView stebėjimo sistema

Visas aptariamos sistemos sudarytos panašiu architektūriniu principu. Vartotojas jungiasi prie centrinio serverio, kuriame kaupiami istoriniai ar realaus laiko duomenys. Centrinis serveris jungiasi prie agentų arba GRID informacijos servisų, kad rinktų ir kauptų duomenis. Labiausiai iš šių sistemų veikimo principu išsiskiria tik *MonALISA*. Kad galima būtų prie jos prisijungti, vartotojas privalo parsisiųsti į savo naršyklę vartotojo sąsają. Ši sistema veikia storo kliento (*angl. fat client*) modeliu. Tačiau tai turi ir savų pliusų, šis veikimo modelis pastoviai atnaujina ryšį su centriniu serveriu ir atnaujina vartotojo matomą informaciją realiu laiku. Šia galimybe negali pasigirti kitos aptariamos sistemos. Taip pat pati sistema pasirūpina saugiu ryšiu tarp vartotojo sąsajos ir centrinio serverio, nes duomenys iš kliento į sistemą keliauja koduotu *X.509* protokolu. Skirtingai nei *Monalisa*, tačiau labai panašiai tarpusavyje, plono kliento modeliu (*angl. thin client*), veikia *Ganglia*, *Nagios*, *GridView* ir *GridIce*. Vartotojas per naršyklę jungiasi prie centrinio web serverio, kuris sugeneruoja vartotojo sąsają. Sekantis žingsnis, *Ganglia* ir *MonALISA* centriniai serveriai jungiasi prie agentų, kurie šioms sistemoms teikia informaciją, *Nagios* agentai patys siunčia informaciją į centrinį serverį, o agentai jungiasi prie *GRID* mazgų ir renka nuo jų duomenis. *GridView* sistema jungiasi prie *webserviso*, kuris iš duomenų archyvo pasiima jai reikalingą informaciją, o duomenų archyvavimo modulis renka informaciją iš resursų brokerio, bei *GRID* mazgų. *GridIce* centrinis serveris naudodamasis *LDAP* protokolu jungiasi prie *GRIS* (*Grid Resource Information Service*) ir *GIIS* (*Grid Index Information Service*). Šiuose dviejose *GIIS* ir *GRIS* sistemose pateikiama pagrindinė GRID informacija, kurią vartotojui ir pateikia *GridIce*.

Dėl klasterių ir teikiamų duomenų įvairovės, sunku sukurti vieningą duomenų perdavimo struktūrą, tam tikslui *GridView* pritaiko perdavimą *XML* standartu tarp klasterio informacijos tinklo sąsajos sluoksnio ir *GRID* informacijos valdymo sluoksnio.

Galima sukurti stebėjimo sistemą, kuri iš *Ganglia*, *Nagios*, *GridView* ir *GridIce* rinktų teikiamą informaciją ir saugotų pas save, tai galima atlikti dėlto, kad šios sistemos veikia plono kliento modeliu, tačiau MonALISA stebėjimo sistemos duomenų taip rinkti nepavyktų, nes kaip ir aptarėme anksčiau, ji veikia storo klieno modeliu, ir centrinis serveris nesuteikia vartotojui ar sukurtai sistemai galutinai sugeneruoto rezultato.

Saugumo atžvilgiu *MonALISA* viena iš labiausiai į saugumą orientuota monitoringo sistema. Į vartotojo kompiuterį parsiųsta vartotojo sąsaja sukuria su centriniu serveriu saugų ryšį pagrystą sertifikatais ir X.509 (Lock, Sommerville; 2002) protokolu. Tokį pat saugų koduotą ryšį centrinis serveris palaiko ir su agentais, kurie renka informaciją iš *GRID* mazgų. Tokiu būdu *MonALISA* pilnai apsaugota nuo pašalinių vartotojų ar programinės įrangos įsiterpimo tarp vartotojo ir monitoringo duomenų. *Nagios*, kaip ir *Ganglia* ar *GridView*, nenaudoja saugių ryšių, išskyrus atvejus, kai naudojami vartotojo sukurti specialūs įskiepiai į agentus kai stebimi parametrai (tokie kaip uždavinių eilės klasteryje, laisvi resursai ir t.t.), kuriems reikalinga *GRID* autentifikacija. *Ganglia* agentai *TCP* tinklu transliuoja *XML* formatu informaciją, kurią gali rinkti ne tik *Ganglia* sistema, bet ir kitos programos ar vartotojai. Užtenka sukurti programinę įrangą kuri kreiptųsi į *Ganglia* agentus tam tikrais *Ganglia*

naudojamais prievadais, ir agentai pateikia visus, išskyrus istoriją, *Ganglia* sistemai skirtus duomenis, tokiu būdų šie parametrai gali būti kaupiami ir kitos sistemos, kuriai neskirti duomenys, ar *Ganglia* sistemai retransliuojami pakeisti duomenys. *Nagios* nenaudoja saugių sesijų, tarp vartotojo ir sistemos, agentai, kurie teikia informaciją sistemai, gali naudoti autentifikuotus prisijungimus prie *GRID*, kad galėtų rinkti specifinius parametrus, kurie neteikiami viešai. Ilgiau pastebėjus tinklą (pvz.: *snifer* ir panašiomis programomis), nesudėtinga perimti teikiamo agento paslaugas ir teigti centriniam serveriui neteisingą informaciją. *GridIce* vartotojai prie sistemos jungiasi nesaugiu ryšiu, tačiau sistema jungdamasi prie *GRID* rinkti informaciją, naudojasi *LDAP* protokolu, kuriame dažniausiai nėra vykdomas autentifikavimas, tačiau galimas, ir šis būdas apsaugotų informaciją nuo trečiųjų asmenų ar programinės įrangos įsiterpimo tarp teisingos informacijos ir vartotojo.

Išvados

1. Iš apžvelgtų sistemų labiausiai į saugumą orientuota *MonALISA* stebėjimo sistema, dėlto, kad ji nuo pat vartotojo iki agento naudojasi saugiais koduotais protokolais.

2. Pakankamai saugi *GridIce* stebėjimo sistema, nes ji pasirūpintų autentifikuotu ryšiu tarp sistemos ir *GRID* informacijos servisų, jei *LDAP* protokole sistemos administratorius įjungtų autentifikaciją.

3. Atlikus analizę pastebėta, kad iš vartotojo perspektyvos MonALISA stebėjimo sistema tinka tik realiu momentu ar labiau trumpo laikotarpio tinklo informacijos stebėjimui. Todėl norint kaupti duomenis pačioje sistemoje rekomenduojama būtų rinktis Ganglia, Nagios, GridView ar GridIce, kurios skirtos statistinių duomenų rinkimui.

4. MonALISA, GridView ir GridIce sistemos sukurtos specialiai GRID tinklui stebėti, o Nagios ir Ganglia tai universalios sistemos, ir GRID tinklui pritaikomos tiek, kiek ją diegiantis asmuo sugeba patobulinti, kad joje būtų matomas kuo didesnis kiekis specifinės GRID tinklo informacijos. Dažniausiai jos naudojamos standartiškai pateikti tipinius paskirstyto tinklo mazgų parametrus.

5. Daugumoje monitoringo sistemų nenaudojamos tokios saugumo priemonės, kaip autentifikacija, sertifikatai, duomenų kodavimas ir kitos. Todėl jas diegiant į GRID tinklą būtina pasirūpinti saugų sistemos darbą užtikrinančiais techniniais sprendimais.

Literatūra

Andreozzi, S.; Fattibene, E.; Misurelli, G.; Rubini, L. G.; 2005 *GridICE: Requirements, Architecture and Experience of a Monitoring Tool for Grid Systems*

Casey, J.; Imamagic, E.; Neilson, I.; 2008; *Advances in Monitoring of Grid Services in WLCG*, International Conferenceon Computingin High Energyand Nuclear Physics (CHEP'07)

Ganglia, 2009 [žiūrėta: 2009 m. balandžio 02d.]. Prieiga per Internetą: < http://ganglia.info >

Lock R.; Sommerville I,; 2002; *Grid Security and its use of X.509 Certificates* Department of Computer Science Lancaster University

Imamagic, E.; Radic, B.; Dobrenic D.; 2005; *CRO-GRID Grid Monitoring Architecture* University Computing Centre, University of Zagreb, Croatia

MonALISA, 2009 [žiūrėta: 2009 m. kovo 29d.]. Prieiga per Internetą: < http://monalisa.caltech.edu/monalisa.htm >

Nagios, 2009 [žiūrėta: 2009 m. balandžio 01d.]. Prieiga per Internetą: < http://www.nagios.org/ >

Ni Guangbao, Ma Jie, Li Bo,; 2004; *GridView: A Dynamic and Visual Grid Monitoring System*, Institute of Computing Technology, Chinese Academy of Sciences

GRID MONITORING ENSURING INFORMATION SECURITY

K. Paulikas, D. Sandonavičius, G. Vilutis, W. Wolyniec

Summary

The most popular Grid monitoring systems, their architecture and advantages, as well as disadvantages have been discussed. The working tenets of these systems were presented with regard to the security of the data and user's connection comfort. It was explained by the importance of stability. The description of some technologies that are used in the certain systems and the benefits of such choices were presented. The specific means, which help to achieve the security of each system user, are emphasized. The differences between the monitoring systems were given. The reasons of their popularity were presented together with the distinction of specific areas of usage, in which each particular system is the most suitable one. GUI of each system is provided.

GRID PROGRAMINĖS ĮRANGOS PRITAIKYMO VARTOTOJŲ POREIKIAMS ANALIZĖ

Gytis Vilutis, Kęstutis Paulikas, Waldemar Wołyniec, Rasa Mažutienė
Kauno technologijos universitetas, walwoly@stud.ktu.lt

Anotacija. Aptarti populiariausia Grid programinė įranga. Išnagrinėtos jų pagrindinės savybės, o vartotojo sąsaja vertinama patogumo naudotis atžvilgiu. Aptarti taip pat pagrindiniai programinės įrangos įrankiai, kurie buvo sukurti vartotojams. Nemažai dėmesio skiriama ir informacijos gavimui ir monitoringui. Aptariamas taip pat ir programinės įrangos integralumas su kitomis operacinėmis sistemomis bei įvairiomis programomis.

Įvadas

Išpopuliarėjus Grid tinklų technologijoms, buvo pradėta kurti įvairi programinė įranga. Kiekviena iš jų turi savo privalumų ir trūkumų. Grid sąvoka jau yra pakankamai sena. Pažymima (Bala, Pytlinski, Nazaruk,M 2002), kad Gridai leidžia daugelio įvairių geografiškai išmėtytų resursų apjungimą, bei leidžia paskirstytų resursų pažymėjimą ir agregavimą tarp kelių organizacijų, siekiant išspręsti didelio masto skaičiavimais, bei dideliu duomenų kiekiu pasižyminčias mokslo problemas.

Kitur apibrėžiama, kad bendrame Grid skaičiavimų darbo scenarijuje įtrauktas dinaminis “virtualių organizacijų” formulavimas, susidedantis iš atskirų ir susietų resursų ir paslaugų, apjungtų bendro tikslo, bet išdėstytų ne viename administravimo vienete (Welch, Siebenlist, Foster, Bresnahan, Czajkowski, 2003). Pagrindinis uždavinys Gride – užtikrinti prieigą prie resursų. Kadangi Gride resursai paskirstyti, šį uždavinį sprendžia speciali programinė įranga, vadinama servisais.

Kai kuriami Grid tinklai, pasirenkant jų programinę įrangą būtina atsižvelgti į tai, kokias jie turės turėti savybes. Vienas iš svarbiausių Grid savybes lemiančių veiksnių yra jo architektūra. SOA (angl. Service Oriented Architecture) (Thimas, 2005) yra technologija, skirta sujungti verslo ir skaičiavimo resursus, reikalingus pasiekti galutinių vartotojų pageidaujamus rezultatus. Visi SOA specifiniai architektūriniai principai sistemos ir paslaugų aprašymui susitelkia ties specifinėmis temomis, kurios įtakoja vidinį sistemos elgesį ir jo projektavimo būdą, jos detaliai aprašytos (Newcomer, Lomow, 2004) literatūros šaltinyje. Teigiama (Arsanjani, Liang-Jie, Ellis, Allam, Channabasavaiah, 2007), kad būtent SOA leidžia lengvai lygiagretini IT funkcijas ir verslo procesus bei tikslus. SOA mažina išlaidas, pagreitina užduočių gavimą bei organizacijų bendradarbiavimą ir integraciją. Tikslus SOA architektūros apibrėžimas 9 sluoksniuose pateiktas Service oriented Solution Stack (S3) modelyje, kuriame kiekvienas sluoksnis atsakingas už atskiras funkcijas. Šiame straipsnyje didžiausias dėmesys skirsiu plačiausiai naudojamai Grid programinei įrangai: Globus Toolkit, Unicore, GRASP, gLite, Nordu Grid, kiti.

Populiariausia programinė įranga

Globus pagrindinės paslaugos, sąsaja ir protokolai leidžia vartotojams pasiekti nutolusius resursus, tuo pačiu metu išsaugant vietinę resursų kontrolę. Jame išvystyta monitoringo sistema leidžia sekti vartotojų užduočių Gride būsenas bei kaip keliauja jų duomenų srautai. Nepriklausoma resursų kontrolė yra labai naudinga kompiuterių, kurie atlieka skaičiavimus, administratoriams, nes jie gali palaikyti savo organizacijai priimtiną tvarka. Atviras sistemos kodas yra kitas privalumas, nes vartotojai, norėdami panaikinti esamus trukumus gali pakoreguoti programų kodus.

Abipusė Unicore autentifikacija leidžia vartotojui būt užtikrintam, duomenų integralumu bei autorizuotu jų naudojimu, tai užtikrinama X.509 sertifikato naudojimu. Santykinai paprastas klientinių programinės įrangos įdiegimo procesas, o vartotojo grafinės sąsajos būvimas žymiai palengvina vartotojo darbą ir taupo laika.

GRASP‘e (Oh-Kyoung, Jaegyoon, Sangwan, Jongsuk, 2004) vartotojas gali stebėti, bei kontroliuoti visą darbą. Surandami vartotojo poreikius atitinkantys resursai. Atliekama tarpininkavimo funkcija tarp vartotojo pateiktos resurso charakteristikos bei resurso savininko sukurtos darbo politikos.

EGEE Grid vartotojai gali nesunkiai prieiti prie atminties ir skaičiavimo resursų. Jie gali stebėti resursus, informuoti apie vykstančius nesklandumus. Vartotojai, norėdami susipažinti su šios sistemos galimybėmis, tai gali padaryti nuėję http://public.eu-egee.org/test/ adresu, gali taip pat susiinstaliuoti jos klientą savo kompiuteryje.

NorduGrid vartotojai sistemoje, kuri veikia ARC programinės įrangos pagrindu, gali patys keisti atliekamų skaičiavimų paskirstymą. ARC užtikrina: informacines paslaugas, resursų paiešką, stebėjimą bei užduočių valdymą. Pavieniam klientui prieinama daugybė taikomųjų paketų, palengvinančių darbą šia programine įranga. Serverio instaliavimui nereikia pilno pakartotino konfigūravimo, tai supaprastina sistemos administratorių darbą.

Plačiausiai naudojami programinės įrangos įrankiai

Praktiškai kiekviena Grid programinė įranga turi vartotojų naudojimui skirtus specifinius įrankius. Čia aptarsime šiuos bendresnius vartotojų įrankius, kurie gali būti naudojami skirtinguose programinėse įrangose: Migrating Desktop, Zeus toolkit, Ganga, P-GRADE, GPDK. Šių įrankių pagalba paprasčiau gauti įvairius duomenis, stebėti užduočių atliekamo darbo būsenas ir t.t.

Migruojančio darbastalio užduotis – suteikti mokslininkams aplinką, kuri paslepia Grid paslaugų detales ir leidžia nustatyti, bei interaktyviu būdu kontroliuoti sudėtingas sistemas. Pateikia grafinę vartotojo sąsają, kuri apjungia ir naudoja keletą programinės įrangos įrankių, kurie leidžia vartotojui bendrauti su taikomąja programa. Vartotojas šio įrankio pagalba gali: patogiai naudotis Grid resursais, paleisti interaktyvią programą, vykdyti jos stebėjimą ir vizualizaciją bei duomenų valdymą.

Pagrindinė Zeus Grid Toolkit programinės įrangos užduotis – atskirti kliento/vartotojo sąsajos nuo konkrečios programinės įrangos. Šis paketas tai įrankių sąsaja, kuris įgalina naudotis tais pačiais skriptais skirtinguose programinėse įrangose. Vartotojo patogumui, jeigu įsivelia klaida ar viršijamas nustatytas neveiklumo laikas, kliento aplinka leidžia vartotojui pakartoti komanda, o tai yra ypač patogu. Galima greitai ir nevarginant vartotojo sukurti darbo aprašymą, darbo atlikimą, stebėti jo vykdymą, atnaujinti rezultatus, jei reikia, nutraukti darbą.

Ganga sukurtas norint patenkinti Atlas ir LHCb poreikį vartotojų interfeisui. Jame įdiegtas vartotojui palengvinimas konfigūravimui ir programų paleidimui, kurie sukurti pagal Gaudi/Athena struktūra.

Ganga leidžia atlikti perėjimus iš vietinių paketų sistemų į didesnius apdorojimus Gridu resursuose.

Ganga sistema leidžia vartotojui mažiau rūpintis užduoties įvykdymu ir sistemos stabilumo problemomis. Konfigūravimas atliekamas pakankamai patogiai ir lengvai, vartotojui nesunku paleisti programas.

P-GRADE Grid Portalas yra oficialus visų vartotojų bendrijų portalas ir serveris. Jis plačiai naudojamas: mokant tarptautinių Grid projektų, norint parodyti Grido infrastruktūros galimybes bei Grid programos plėtimo sąvokas.

P-GRADE Grid Portalas suteikia vartotojui abstraktų Grido kompiuterinės įrangos ir laikmenų resursų vaizdą. Tai patogus įrankis kiekvienam norinčiam didelėje pateiktoje Grido aplinkoje išspręsti kompiuterinės įrangos arba duomenų problemas.

P-GRADE sistema paslepia žemo lygio Grido priėjimo mechanizmus, panaudodamas aukšto lygio grafinius interfeisus, o tai leidžia net ne Grido ekspertams suformuluoti ir naudoti pateiktas programas daugybės institucijų kompiuterinėje įrangoje. Nustatyti darbo srautai ir darbo srauto tyrimai yra kilnojami Grido platformose be papildomo naujos sistemos mokymosi ar programos kodo keitimo. Vartotojai gali naudotis vienu metu keletu Gridų, o tai leidžia paskirstyti sudėtingas programas keletui platformų ir pagreitinti rezultatų gavimą.

Grid Portal Development Kit (GPDK) yra sukurtas suteikti priėjimą prie Grid paslaugų naudojantis Java Server Pages (JSP) ir Java Beans. GPDK įrankis leidžia valdyti Tomcat, atviro kodo tinklo paslaugų serverį, sukurtą Sun microsystems, kaip vėliausią Java Servlets v2.2 ir Java Server Pages v1.1 charakteristikų patobulinimą.

GPDK nėra iki galo išbaigtas įrankis. Tai iš tiesų yra komponentų rinkinys GRID‘o uždavinių valdymui. Sistemoje, naudojantis tinklo naršykle, galima prieiti prie nutolusių resursų iš bet kur, nereikalaujant sertifikatų ar privatumo raktų saugojimo tame pačiame įrenginyje. Tai itin patogu vartotojams, kurie savo užduotis valdo ne iš vieno kompiuterio. Myproxy serveris yra atsakingas už proxy sertifikatų palaikymo servisą, kuris leidžia saugiai atkurti sertifikatus tolimesniam naudojimui. Tinklo paslauga gali būti lengvai supakuota ir išskleista kaip Java klases turintis Web programų archyvo failas. Tai yra itin patogu perduodant programą per tinklą i kitus kompiuterius.

Išvados

1. Apžvelgti pagrindiniai GRID tinkluose naudojama programinė įranga, kiekvienas iš jų buvo kuriamas su labai konkrečiais tikslais, todėl jie nėra lankstūs platesnio vartotojų uždavinių rato požiūriu.

2. Kuriant papildomus vartotojų sąsajos įrankius programinei įrangai, stengiamasi daliniai kompensuoti pačios programinės įrangos neišbaigtumą.

3. Iš pateiktų programinės įrangos savybių aprašymo galime teigti, jog prieš pasirenkant konkrečia programinę įrangą ar jo įrankį būtina gerai apgalvoti kuriamo GRID ir teikiamų servisų architektūrą.

Literatūra

Arsanjani, A.; Liang-Jie Zhang; Ellis, M.; Allam, A.; Channabasavaiah, K.; *A Service-Oriented Reference Architecture*, IT Professional Volume 9, Issue *3*, May-June 2007 Page(s):10 – 17

Bala, P.; Pytlinski, J.; Nazaruk, M.; *BioGRID - An European Grid for molecular biology.* High Performance Distributed Computing, 2002. HPDC-11 2002. Proceedings. 11th IEEE International Symposium on 23-26 July 2002 Page(s):412

Eric Newcomer, Greg Lomow. *Understanding SOA with Web Services. Independent Technology Guides*, 2004. Pages 444

Oh-Kyoung Kwon, Jaegyoon Hahm, Sangwan Kim, Jongsuk Lee, *GRASP: A Grid Resource Allocation System based on OGSA*, High performance Distributed Computing, 2004. Proceedings. 13th IEEE International Symposium on Volume, Issue, 4-6 June 2004

Thimas Erl. *Service-Oriented Architecture. Concepts, Technology and Design.* Prantice Hall, Profesional Technical Reference, 2005. Pages 760.

Welch, V.; Siebenlist, F.; Foster, I.; Bresnahan, J.; Czajkowski, K.; *Security for Grid services.* High Performance Distributed Computing, 2003. Proceedings. 12th IEEE International Symposium on 22-24 June 2003 Page(s):48 - 57

THE ANALYSIS OF GRID'S MIDDLEWARE ADAPTATION TO USER‘S NEEDS

G. Vilutis, K. Paulikas, W. Wołyniec, R. Mažutienė

Summary

The most popular GRID middleware has been reviewed. Their main characteristics have been presented. The user interfaces have been analyzed from the point of view of convenience. The main tools of middleware designed for users have been discussed. Much attention has been paid to the ways of receiving information for monitoring. The integrity of middleware with operating systems and various program products have been discussed.