HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Analiza Nagios alata

CCERT-PUBDOC-2006-03-152

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Programski paket Nagios (TM) spada u kategoriju alata za nadgledanje i analizu rada računalnih mreža i mrežnih servisa. Od ostalih programa slične namjene izdvaja se zbog svoje fleksibilne arhitekture i visokog stupnja prilagodljivosti.

Najznačajnije mogućnosti alata odnose se na provjeravanje statusa računala i njihovih servisa. Na temelju povratnih rezultata Nagios može poduzeti određene korake kako bi spriječio neželjene pojave, ispravio nastale nepravilnosti u radu te po potrebi obavijestio nadležnog administratora o neregularnosti unutar mreže (putem elektroničke pošte, SMS poruka ili na neki drugi korisnički definirani način). Program je u stanju nadzirati raznovrsna računala i servise koji se mogu izvoditi na različitim operacijskim sustavima. To ga u kombinaciji s modularnom arhitekturom čini primjenjivim u gotovo svakom mrežnom okruženju, koliko god ono bilo specifično. Osim toga, napisan u programskom jeziku C, Nagios se distribuira pod GNU GPL licencom i kao takav pogodan je za mnoge namjene kada komercijalni alati nisu prihvatljivi.

Dokument opisuje princip rada Nagios programa, instaliranje i konfiguriranje programa te web administracijsko sučelje.

Slika 1: Prikaz administracijskog sučelja Nagios alata

2. Princip rada

Postoje dva osnovna zadataka koji se stavljaju pred programe za nadzor računalnih mreža:

- centralizirano nadgledanje svih potrebnih uređaja i servisa prisutnih u mrežnom okruženju, i
- pravovremeno prijavljivanje detektiranih poremećaja unutar mreže i pregledno prezentiranje dobivenih rezultata.

Nagios uspješno ispunjava navedene zadatke, a posjeduje i mogućnost definiranja okolnosti u kojima nastupa opterećenje sustava te uslijed kojih program, shodno obrađenim rezultatima, šalje upozorenje administratoru. Također, ukoliko Nagios nije u mogućnosti obavijestiti sistemskog administratora, program posjeduje mogućnost automatskog rješavanja definiranog problema tokom rada putem konfiguracijskih skripti.

Nagios omogućava nadgledanje dostupnosti nekih od mrežnih servisa kao što su ICMP, DNS, HTTP, SSH, SMTP, POP3, IMAP… Osim nadgledanja servisa omogućeno je i nadgledanje sistemskih resursa na računalima kao što su recimo opterećenje procesora, iskoristivost radne memorije, opterećenje diskova, stanje mrežnih sučelja kao i sve podatke važne sistemskim administratorima, koje im omogućavaju da što kvalitetnije pronađu prirodu greške u radu sistema.

Specifičnost Nagios alata je i to što korisniku pruža mogućnost da sam razvija pomoćne programe kojima je u mogućnosti nadgledati specifične servise. Omogućeno je i istovremeno nadgledanje više vrsta servisa što omogućava provjeravanje i razlikovanje statusa računala. Računala mogu biti dostupna, nedostupna ili loše konfigurirana zbog nepravilno podešene mreže. U slučaju bilo kakvih nepravilnosti Nagios posjeduje mogućnost izvještavanja o pogrešci u radu na više načina (elektroničkom poštom, SMS-om ili pak nekom drugom metodom koju je odredio korisnik).

Prednost Nagios alata je i to što podržava tzv. *event handler*-e. Time je korisniku omogućeno proaktivno rješavanje problema u radu, jer se korištenjem *event handler* mehanizma unaprijed definiraju procedure koje se trebaju izvoditi u slučaju nepravilnosti u radu.

Jedna od dodatnih prednosti Nagios alata je i njegova mogućnost nadgledanja redundantnih poslužitelja i prikupljanja informacija na temelju kojih se određuje izvođenje potrebnih radnji. Ovaj mehanizam moguć je zahvaljujući činjenici što Nagios podržava i distribuirano nadgledanje mreže preko web administracijskog sučelja unutar kojeg su na istom mjestu prikazani tekući status mreže, poslana obavještenja, povijest problema, sve relevantne log datoteke, itd… Korištenjem web administracijskog sučelja moguće je na vrlo jednostavan način kontrolirati i definirati relevantne informacije.

2.1. Arhitektura alata

Kao što je u uvodu naglašeno Nagios se temelji na jednostavnoj modularnoj arhitekturi. Osnovu mu čini jezgra koja se izvršava u obliku servisa (eng. *daemon)* i sama za sebe nije u stanju obavljati nikakav oblik mrežnog nadzora. Tu funkcionalnost postiže u sprezi s pomoćnim programima (eng. *plugins*) koji obavljaju zadaću ispitivanja stanja određenog mrežnog resursa te po završetku ispitivanja šalju rezultate jezgri na analizu. Jezgra alata je u stanju dobivene rezultate obraditi i prezentirati u smislenom obliku. Osim toga, moguće je definirati i niz postupaka koji će se pokrenuti ukoliko dođe do određenog stanja (eng. *event handlers*) te o tome informirati nadležnu osobu.

Nagios omogućava kontroliranje različitih lokalnih ili udaljenih servisa i resursa. Kada se javi potreba za ispitivanjem nekog parametra, jezgra pokreće pomoćni program zadužen za tu provjeru. U tom kontekstu jezgru Nagiosa moguće je shvatiti kao okruženje (eng. *framework*) unutar koga se izvršavaju raznovrsni namjenski alati čiji predmet ispitivanja može biti bilo što (uređaj ili servis) ukoliko je u stanju odgovoriti na primljeni zahtjev.

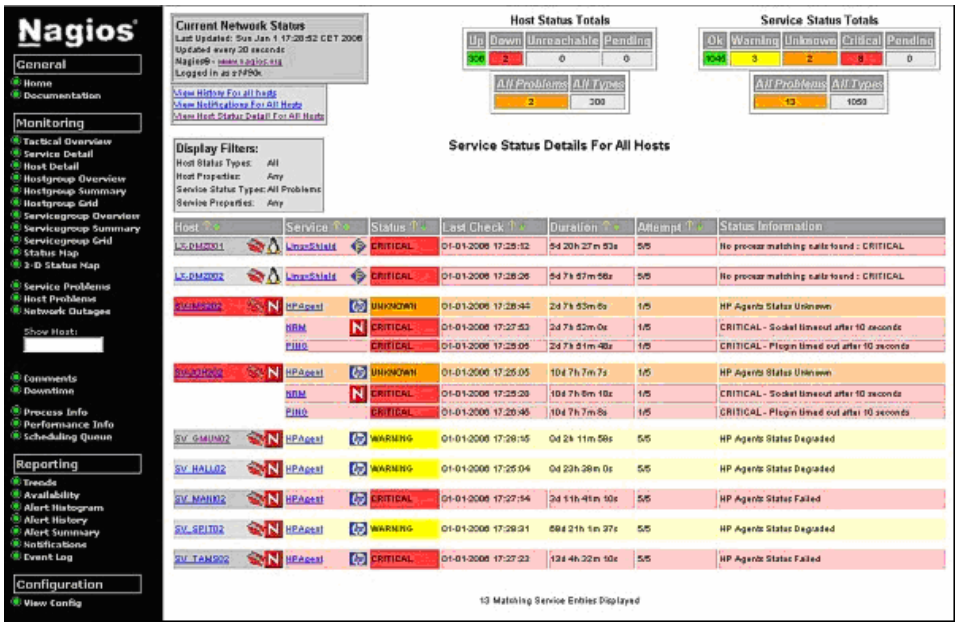
2.2. Pomoćni programi

Specifičnost Nagios alata je što je zasnovan na jednostavnoj arhitekturi. Procesi se mogu odvijati interno u jezgri programa ili pak eksterno pomoću pomoćnih programa (eng. *plugins*) koji dohvaćaju podatke i predaju ih jezgri Nagios alata na analizu. Pomoćni programi obavljaju uobičajene zadaće nadgledanja mrežne infrastrukture. Oni su dostupni na web stranicama Nagios projekta. Uz njih na raspolaganju su i mnogi dodatni pomoćni programi kao dio Nagios Exchange projekta koji ima svrhu nadograđivanje Nagios alata. Ipak, ono čime se odlikuje arhitektura Nagios alata i što ga čini izrazito moćnim jest mogućnost kreiranja vlastitih pomoćnih programa. I ukoliko je korisniku potreban neki

specifični pomoćni program ili mu postojeća rješenja nisu dovoljno dobra, korisnik ima mogućnost programiranja vlastitog alata ili skripte koji će obavljati definirane zadatke.
Pomoćni programi se u radu uglavnom koriste za nadgledanje procesa. Zbog toga je alat vrlo fleksibilan i moguće ga je veoma lako povezati s drugim *open source* programima. Stoga se Nagios može koristiti i kao centralna konzola za nadgledanje statusa mreža, koju je moguće povezati s drugim programima za nadzor mreže te iz jednog sučelja nadgledati i kontrolirati sve važne podatke. Smisao pomoćnih programa je u tome da izvršavaju radnje koje im je Nagios povjerio te rezultate vraćaju Nagios programu koji na osnovu njih odlučuje hoće li na odgovarajući način obavijestiti administratora o problemu na mreži ili će pak pokrenuti izvršavanje *event handler*-a, tj. unaprijed definiranih procedura koje otklanjaju problem. Ovim načinom ostvaruje se gotovo neograničena mogućnost automatiziranog nadgledanja. S Nagios alatom standardno dolaze neki pomoćni programi koji provjeravaju uobičajene servise, a pod tim se podrazumijevaju TCP/UCP portovi, opterećenje procesora, slobodan prostor na disku, brzina odziva na komandu PING, SNMP promet, itd…
Ukoliko nisu dostupni pomoćni programi za neki specifični servis koji je potrebno nadgledati, isti je moguće napisati. Ipak, pretpostavka za ispunjenje toga je dobro poznavanje programskog jezika C. Prednost ovakve arhitekture s pomoćnim programima je što Nagios ne zna što kontrolira – on samo prati vrijednosti i na osnovu njih generira grafički prikaz, ili šalje upozorenje administratoru ukoliko je neka vrijednost izvan uobičajenih granica. Većinu poslova obavljaju pomoćni programi i oni znaju što točno nadgledaju.

2.3. Aktivni i pasivni način rada

Lokalni parametri vezani uz pojedino računalo, poput temperature procesora, iskorištenja diskovnog prostora i sl. nisu javno dostupni na mreži. Stoga nije moguće ispitivati njihovo stanje na daljinu uobičajenim metodama. Ipak, Nagios posjeduje mogućnost rješavanja i takvih situacija korištenjem pomoćnog programa `check_nrpe` i dodatka u obliku NRPE (eng. *Nagios Remote Plugin Executor*) paketa. NRPE predstavlja dodatak za Nagios alat koji je namijenjen izvršavanju na udaljenim računalima u obliku pozadinskog procesa koji se aktivira u trenutku kada primi zahtjev od `check_nrpe` pomoćnog programa. Nakon što primi zahtjev, NRPE lokalno izvede potrebne naredbe te njihov rezultat proslijedi `check_nrpe` pomoćnom programu, koji primljene podatke prosljeđuje do jezgre Nagios-a gdje se oni obrađuju. Cijeli postupak je potpuno transparentan za korisnika, stoga nije narušena ideja centraliziranog mrežnog nadzora.
Prethodno opisana metoda rada Nagios alata, tzv. aktivni način rada, odnosi se na uobičajenu metodu pokretanja pomoćnih programa u trenucima kada je potrebno ispitati stanje nekog servisa ili računala. Uz taj način rada postoji i tzv. pasivni način koji se izvršava na principu davanja podataka jezgri u slučajevima kada program procjeni da je to potrebno. Za obavljanje spomenute zadaće koristi se NSCA (eng. *Nagios Service Check Acceptor*) paket. NSCA predstavlja dodatak za Nagios alat koji šalje jezgri Nagios alata potrebne informacije bez primljenog zahtjeva za istima. Prema definiranim uputama klijentski program preko NSCA javlja jezgri da je došlo do promjene unutar mreže i jezgra tada obrađuje podatke na uobičajeni način.
Generalno gledajući, Nagios može raditi u 2 načina rada, aktivnom i pasivnom. Aktivni se još naziva i *Pull* način rada jer u tom radu centralna aplikacija, tj. Nagios dohvaća informacije o statusu nadgledane mreže. U pasivnom načinu rada koji se još naziva i *Push* način rada, informacije o statusu mreže bivaju dohvaćene pomoću pomoćnih agentskih programa te se njihovi rezultati obrade predaju jezgri Nagios programa na obradu. Specifičnost ovog načina je što pomoćni agentski programi imaju određenu inteligenciju odlučivanja o tome kada je potrebno jezgri Nagios programa slati podatke. U suprotnom bi mreža bila obasuta redundantnim podacima.
U praksi je moguća situacija gdje je korištenjem Nagios alata potrebno nadgledati velik broj sistemskih parametara koji mogu zagušiti sistem zbog velike količine podataka ili pak zbog prevelikog opterećenja procesora računala na kojem se nalazi Nagios. Zbog toga nije moguće kvalitetno pratiti što se doista događa na sustavu. Manjkavost aktivnog načina rada očituje se u količini prenesenih podataka koji u velikim okruženjima mogu predstavljati znatno opterećenje za mrežu. S druge strane, nedostatak pasivnog načina je smanjena pouzdanost koja proizlazi iz činjenice da se ispitivanje ne vrši u frekventnim vremenskim intervalima.



Slika 2: Prikaz *Service Detail* sučelja s izdvojenim detaljima za grupu poslužitelja pod alarmom

2.4. Izvještavanje

Nagios posjeduje opciju slanja obavijesti o stanju računala i servisa definiranim korisnicima. Također, ukoliko Nagios detektira problematičan rad nekog servisa, korisniku je pružena mogućnost definiranja oblika izvještavanja. Sam mehanizam je dosta složen i da bi se poslala obavijest o problemu u radu, ona mora proći kroz određene filtre i kontrole. Korisniku je tako omogućeno da definira više scenarija izvještavanja za svaki problem u mreži. U praksi se može dogoditi da nije moguće poslati SMS poruku zbog nedostupnosti telefonskog aparata pa se u tom slučaju nastavlja s izvještavanjem korištenjem elektroničke pošte ili na neki drugi zamjenski način koji je korisnik definirao. Sam broj mogućih scenarija je praktički neograničen i neovisan o nadgledanim procesima. Prednost takvog sustava izvještavanja je što korisnik može definirati za sebe najpogodniji način izvještavanja o problemima u radu.

Host	Service	Type	Time	Contact	Notification Command	Information
bogus1	N/A	HOST UNREACHABLE	01-15-2006 14:46:47	jdoe	host-notify-by-email	CRITICAL - Plugin timed out after 10 seconds
bogus5	N/A	HOST UNREACHABLE	01-15-2006 14:45:57	jdoe	host-notify-by-email	CRITICAL - Plugin timed out after 10 seconds
bogus3	N/A	HOST UNREACHABLE	01-15-2006 14:45:57	jdoe	host-notify-by-email	CRITICAL - Plugin timed out after 10 seconds
bogus2	N/A	HOST UNREACHABLE	01-15-2006 14:45:47	jdoe	host-notify-by-email	CRITICAL - Plugin timed out after 10 seconds
bogus4	N/A	HOST DOWN	01-15-2006 14:45:47	jdoe	host-notify-by-email	CRITICAL - Plugin timed out after 10 seconds
bogus-router	N/A	HOST DOWN	01-15-2006 14:19:58	jdoe	host-notify-by-email	CRITICAL - Plugin timed out after 10 seconds
bogus1	N/A	HOST UNREACHABLE	01-15-2006 14:16:47	jdoe	host-notify-by-email	CRITICAL - Plugin timed out after 10 seconds
bogus5	N/A	HOST UNREACHABLE	01-15-2006 14:15:57	jdoe	host-notify-by-email	CRITICAL - Plugin timed out after 10 seconds
bogus3	N/A	HOST UNREACHABLE	01-15-2006 14:15:57	jdoe	host-notify-by-email	CRITICAL - Plugin timed out after 10 seconds
bogus2	N/A	HOST UNREACHABLE	01-15-2006 14:15:47	jdoe	host-notify-by-email	CRITICAL - Plugin timed out after 10 seconds
bogus4	N/A	HOST DOWN	01-15-2006 14:15:47	jdoe	host-notify-by-email	CRITICAL - Plugin timed out after 10 seconds

Slika 3: Prikaz *Notifications* izvještaja s obavijestima o ugašenim i nedostupnim računalima

3. Instalacija i konfiguracija

Programski paket Nagios je izvorno razvijan za Linux operacijske sustave, ali uspješno se izvodi i na ostalim sličnim platformama kao što su AIX, Solaris, Unix i sl. Kao što je u uvodu spomenuto, distribuira se pod uvjetima GNU GPL licence i kao takav dostupan je za slobodno preuzimanje sa službenih web stranica.

Sklopovski preduvjeti, u obliku radne memorije i tvrdog diska, koji su potrebni za normalan rad Nagios programa, variraju zavisno o proporcijama mreže koja se prati i količini te kompliciranosti pomoćnih programa koji se koriste.
Prije samog procesa instalacije Nagios paketa, potrebno je obaviti određene pripreme. Cijeli postupak zahtjeva administratorske (*root*) privilegije, a drugi zahtjev odnosi se na stvaranje posebnog korisnika i korisničke grupe u kontekstu koje će se Nagios izvršavati. Za to se koriste standardne naredbe:

```
# useradd -m nagios
# groupadd nagios
```

Nakon toga, preporuča se kreiranje direktorija u koji će se alat instalirati. U primjeru je odabran direktorij `/usr/local/nagios`, ali isto tako može se koristiti bilo koje drugo kazalo. Odgovarajućem direktoriju potom se pridaju ovlasti prethodno definiranog korisnika i grupe.

```
# mkdir /usr/local/nagios
# chown nagios.nagios /usr/local/nagios
```

Kako bi Nagios-ovo web sučelje ispravno funkcioniralo potrebno mu je osigurati odgovarajuće konfiguriran web poslužitelj. U ovom primjeru će se, zbog svoje raširenosti, podrazumijevati Apache web poslužitelj, ali analogna procedura vrijedi za bilo koji drugi web server. Naredbom

```
# grep "^User" /.../httpd.conf
```

Može se saznati pod kojim korisničkim imenom se Apache poslužitelj izvršava. To je najčešće '`wwwrun`' ili '`apache`'. U nastavku ovog opisa pretpostavljeno je korištenje potonjeg.
Nakon toga kreira se još jedna grupa korisnika koju sačinjavaju korisnik pod kojim se izvršava Nagios te korisnik pod čijim imenom je utvrđeno da se izvršava aktivni web poslužitelj.

```
# groupadd nagcmd
# usermod -G nagcmd apache
# usermod -G nagcmd nagios
```

Budući da se web sučelje Nagios alata potpuno oslanja na svoje CGI skripte nužno je dopuniti konfiguracijsku datoteku `httpd.conf` kako bi im web poslužitelj mogao pristupati. Uz to, definira se i zamjensko ime (eng. *alias*) za HTML stranice što omogućava pristup web sučelju i dokumentaciji korištenjem adrese `http://ime_računala/nagios/`.
U tu svrhu, potrebno je otvoriti datoteku `httpd.conf` i dopisati u nju sljedeći sadržaj:

```
ScriptAlias /nagios/cgi-bin /usr/local/nagios/sbin

<Directory "/usr/local/nagios/sbin">
    AllowOverride AuthConfig
    Options ExecCGI
    Order allow,deny
    Allow from all
</Directory>

Alias /nagios /usr/local/nagios/share

<Directory "/usr/local/nagios/share">
    Options None
    AllowOverride AuthConfig
    Order allow,deny
    Allow from all
</Directory>
```

Slijedi ponovno podizanje Apache web poslužitelja kako bi se primijenile nastale promjene. Za to se koristi naredba oblika:

```
# /usr/sbin/apachectl graceful
# /usr/sbin/apache2ctl graceful  // za Apache2
```

Prije instalacije potrebno je osigurati da na sistemu budu instalirane slijedeće biblioteke:

- png biblioteka (http://prdownloads.sourceforge.net/libpng/),
- jpeg bibilioteka (http://www.ijg.org/files/) te
- Boutell gd bibilioteka (http://www.boutell.com/gd/).

Spomenute biblioteke Nagios koristi kako bi mogao grafički prikazivati stanje unutar mreže.

3.1. Instalacija

Korištenje instalacijskog programskog paketa prilično je jasno i intuitivno te će stoga u ovom postupku biti objašnjena samo instalacija pomoću izvornog koda. Pod pretpostavkom da su preuzete datoteke Nagios jezgre i Nagios pomoćnih programa smještene u radnom direktoriju, standardnim naredbama raspakiravaju se iz arhive:

```
# tar -xvzf nagios-2.0.tar.gz
# tar -xvzf nagios-plugins-1.4.1.tar.gz
```

Postupak instalacije jezgre započinje '`configure`' naredbom sukladno podacima iz prethodnih postupaka, a završava instalacijom oglednih konfiguracijskih datoteka.

```
# cd nagios-2.0
# ./configure --prefix=/usr/local/nagios
    --with-cgiurl=/nagios/cgi-bin
    --with-htmurl=/nagios --with-nagios-user=nagios
    --with-nagios-group=nagios --with-command-group=nagcmd
# make all
# make install
# make install-init
# make install-commandmode
# make install-config
```

Naredba '`configure`' kao parametre prima:

- `prefix` - stvoreni instalacijski direktorij,
- `cgiurl` - adresa koja će se koristiti za pristupanje CGI skriptama (u skladu s direktivom ScriptAlias koja je prethodno definirana u `httpd.conf` datoteci),
- `htmurl` - adresa koja će se koristiti za pristupanje HTML dokumentima sučelja i dokumentaciji,
- `nagios-user` - korisničko ime na sustavu koje ima dozvolu vlasnika nad instaliranim programskim datotekama,
- `nagios-group` - korisnička grupa na sustavu koja ima dozvolu vlasnika nad instaliranim datotekama programa i
- `command-group` - korisnička grupa na sustavu koja ima dozvolu izvršavanja web servera.

Ovime je instalacija Nagios jezgre privedena kraju. Važno je istaknuti da je pristup web sučelju Nagios paketa i CGI skriptama u ovom trenutku dostupan svima koji imaju mogućnost korištenja usluge konkretnog web poslužitelja. Stoga je potrebno uvesti neki od oblika autentifikacije, zavisno o odabranom web poslužitelju.

Da bi Nagios bio potpun i da bi se funkcionalno iskorištavale njegove mogućnosti nužno ga je povezati s različitim pomoćnim programima (eng. *plugins*). Instalacija kolekcije pomoćnih programa koja je dostupna na web stranicama Nagios programa prati već poznatu proceduru konfiguracije:

```
# cd .../nagios-plugins-1.4.1
# ./configure --prefix=/usr/local/nagios
    --with-nagios-user=nagios
    --with-nagios-group=nagios
```

```
# make
# make install
```

Po završetku instalacije svi instalirani pomoćni programi bit će smješteni u kazalo `/libexec` osnovnog direktorija Nagios paketa.

3.2. Konfiguracija

Postoje četiri osnovne i nekoliko pomoćnih konfiguracijskih datoteka koje određuju ponašanje Nagios alata. Svi parametri koji utječu na rad programa podešavaju se unutar sučelja Nagiosa te je stoga vrlo važno upoznati se s njihovom strukturom.
Alat prilikom instalacije kreira nekoliko primjera tih konfiguracijskih datoteka koje svojim primjerom olakšavaju izradu pravih konfiguracijskih datoteka. Uobičajeni direktorij u koji se smještaju konfiguracijske datoteke Nagios paketa je `/usr/local/nagios/etc`, ali to može biti i neko drugo kazalo, poput `/etc/nagios`, ako je alat instaliran u sklopu neke distribucije. Da bi se iz predefiniranih konfiguracijskih datoteka stvorile stvarne potrebno ih je preimenovati:

```
# cd /usr/local/nagios/etc
# cp nagios.cfg-sample nagios.cfg
# cp cgi.cfg-sample cgi.cfg
# cp resource.cfg-sample resource.cfg
# cp minimal.cfg-sample minimal.cfg
# cp misccommands.cfg-sample misccommands.cfg
# cp checkcommands.cfg-sample checkcommands.cfg
# mkdir ./samples ; mv *.cfg-sample ./samples/*
```

Posljednjom naredbom premještamo predefinirane datoteke u zaseban direktorij kako se ne bi miješale s aktivnim konfiguracijskim datotekama:

- `nagios.cfg` - glavna konfiguracijska datoteka koja određuje adresu ostalih konfiguracijskih datoteka i direktorija, log zapisa, korisnika pod čijim se nalogom Nagios izvršava i sl.,
- `resource.cfg` - određuje različite makro upute korištene u drugim konfiguracijskim datotekama, a pošto CGI skripte nemaju potrebne ovlasti za pristup ovoj datoteci moguće ju je iskoristiti kod definiranja nekih sigurnosno osjetljivih parametara,
- `cgi.cfg` - konfiguracijska datoteka CGI web sučelja koja određuje adresu CGI skripti i HTML datoteka, dozvole pristupa pojedinim elementima web sučelja i sl.,
- `minimal.cfg` - datoteka koja na temelju predložaka opisuje kako se definiraju pojedina računala, servisi, kontakt osobe te komande koje je potrebno izvršiti te je stoga od velike koristi novim korisnicima jer ih kroz primjere uvodi u konfiguraciju alata (opširnija varijanta ove datoteke nalazi se pod imenom `bigger.cfg`),
- `misccommands.cfg` – dodatna datoteka koja sadrži naredbe koje nisu izvorno vezane na Nagios jezgru i
- `checkcommands.cfg` – dodatna datoteka koja sadrži naredbe za provjeru koje su korištene od strane drugih konfiguracijskih datoteka.

U nastavku dokumenta opisane su ukratko datoteke `nagios.cfg`, `resource.cfg` i `cgi.cfg` te dijelovi `minimal.cfg` konfiguracijske datoteke koja je za potrebe ovog dokumenta razdijeljena u tri datoteke: `hosts.cfg`, `services.cfg` i `contacts.cfg`.

3.2.1. `nagios.cfg` datoteka

Kao primjer će poslužiti prva direktiva koja se odnosi na smještaj log zapisa, a ima slijedeći oblik:

```
log_file=/usr/local/nagios/var/nagios.log
```

Ovom se direktivom Nagios paketu definira u koje kazalo i pod kojim imenom treba pohranjivati log zapise. Preporuča se da upravo ta direktiva bude prva definirana unutar `nagios.cfg` datoteke kako

bi program mogao u nju zabilježiti sve pogreške i nepravilnosti na koje naiđe pri daljnjem čitanju ostalih parametara.
Važno je naglasiti da je većina direktiva intuitivno imenovana te ukratko opisana unutar same konfiguracijske datoteke te stoga niti manje iskusni korisnici ne bi trebali imati problema sa snalaženjem i razumijevanje njihova djelovanja.
Slijedeća bitna skupina direktiva odnosi se na adrese ostalih konfiguracijskih datoteka kojima se alat služi. Primjer jedne od njih:

```
cfg_file=/usr/local/nagios/etc/minimal.cfg
```

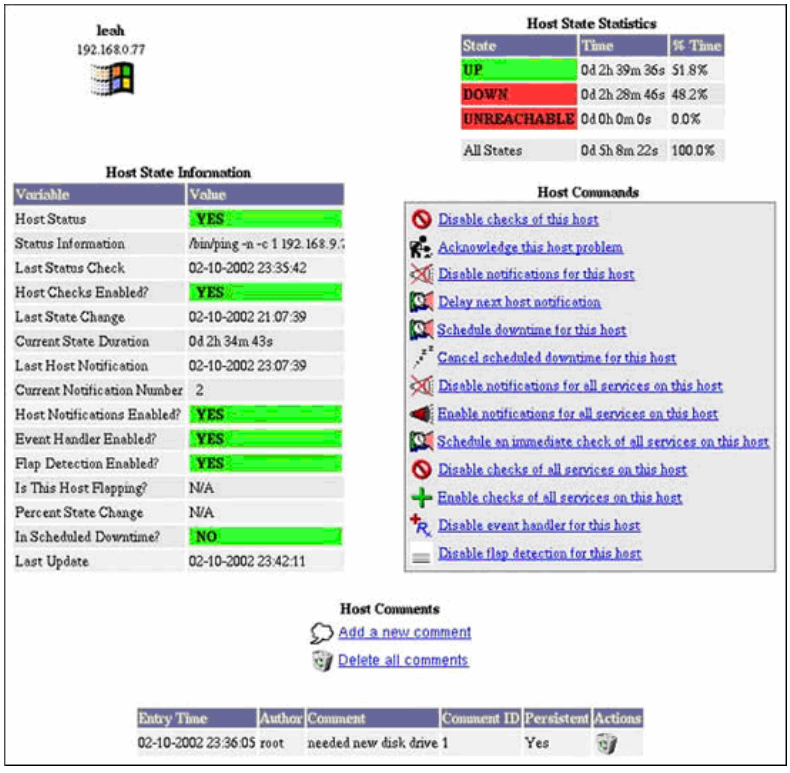
Tim zapisom Nagios paketu definiramo postojanje dodatne konfiguracijske datoteka čiji sadržaj treba uzeti u obzir. Na ovaj se način može napraviti podjela konfiguracijskih parametara u više datoteka prema vlastitim potrebama čime se olakšava organizacija sustava.
Da bi se omogućilo stvaranje novih konfiguracijskih datoteka u kojima se definiraju računala koja se nalaze u mreži koju Nagios nadgleda potrebno je navesti sljedeću direktivu:

```
cfg_file=/usr/local/nagios/etc/hosts.cfg
```

Nagios posjeduje jednu funkcionalnost koja je povezana s pojavom tzv. '*flapping*', sindroma koji se događa ukoliko neki uređaj ili servis naizmjenično mijenja svoje stanje. Npr. kada servis uredno odgovori na nekoliko ispitivanja, a zatim na sljedećih nekoliko prijavi pogrešku, a potom se opet pokaže ispravnim, itd… U cilju smanjenja suvišnih obavijesti Nagios će, ukoliko je ova mogućnost uključena, privremeno prestati slati obavijesti o promjeni statusa sve dok '*flapping*' ne prestane. Za aktiviranje ove mogućnosti potrebno je direktivi `enable_flap_detection` promijeniti stanje iz nule u jedinicu:

```
enable_flap_detection=1
```

Dodatna pojašnjenja i upute vezane uz glavnu konfiguracijsku datoteku mogu se naći na web,adresi: http://nagios.sourceforge.net/docs/2_0/configmain.html.



Slika 4: Prikaz detaljnih informacija o računalu

Stavka	Značenje
Disable checks of this host	Prestaje s nadgledanjem računala
Acknowledge this host problem	Izvještava o problemu na hostu
Disable notifications for this host	Ne šalju se upozorenja ukoliko računalo nije dostupno
Delay next host notification	Odgađa slanje obavijesti o idućem upozorenju s računala
Schedule downtime for this host. Cancel scheduled downtime for this host	Definira se period u kojem se ne izvještavaju problemi u radu ukoliko je računalo nedostupno
Disable/Enable notifications for all services on this host.	Ne šalje se upozorenje ukoliko je računalo nedostupno
Schedule an immediate check of all services on this host	Provjerava sve servise žurno
Disable checks of all services on this host Enable checks of all services on this host	Uključuju se ili isključuju provjere svih servisa na računalu
Disable event handler for this host	Sprječava se izvršavanje korektivnih skripti ukoliko se dogodi nelogičnost u radu računala
Disable flap detection for this host	Ne izvršava se detekcija „*flap*“ aktivnosti za određeno računalo

Tablica 1: Pojašnjenje stavki raspoloživih za definiranje praćenja jednog računala

3.2.2. `resource.cfg` datoteka

Ova datoteka određuje različite makro upute korištene u drugim konfiguracijskim datotekama. Primjer definiranja postavki za spajanje na bazu podataka:

```
xsddb_host=localhost
xsddb_port=3060
xsddb_database=nagios
xsddb_password=password_set_above_in_mysql
xsddb_optimize_data=1
xsddb_optimize_interval=3600
```

Uređivanjem svake stavke datoteke `resource.cfg` možemo podesiti više parametara kao što je to dano za prethodni primjer:

- '`xsddb_host`' - služi za određivanje računala na kojem se nalazi baza,
- '`xsddb_port`' - označava port na kojem se baza nalazi,
- '`xsddb_database`' - određuje naziv baze podataka koju Nagios koristi,
- '`xsddb_password`' - određuje ukoliko je potrebno koristiti lozinku za pristup bazi,
- '`xsddb_optimize_data`' - korisna stavka čijim korištenjem se postiže veća brzina obrade podataka jer uz tu uključenu opciju Nagios optimizira status tablica u određenim intervalima i
- '`xsddb_optimize_interval`' – određuje interval optimiziranja.

3.2.3. `cgi.cfg` datoteka

Ova datoteka određuje adresu CGI skripti i HTML datoteka te dozvole pristupa pojedinim elementima web sučelja. Primjer definiranja postavki:

```
main_config_file=sysconfdir/nagios.cfg
```

```
physical_html_path=datadir
url_html_path=htmurl
use_authentication=1
authorized_for_system_information=nagiosadmin
authorized_for_configuration_information=nagiosadmin
authorized_for_system_commands=nagiosadmin
authorized_for_all_services=nagiosadmin
authorized_for_all_hosts=nagiosadmin,nagiosuser
authorized_for_all_service_commands=nagiosadmin
authorized_for_all_host_commands=nagiosadmin
```

Pojašnjenje pojedninih naredbi za dani primjer:

- 'main_config_file' - služi za određivanje pozicije glavne konfiguracijske datoteke,
- 'physical_html_path' - označava poziciju HTML datoteka,
- 'url_html_path' – označava URL poziciju HTML datoteka,
- 'use_authentication' - određuje ukoliko je potrebno koristiti autentifikaciju za administriranje Nagios alata i prikazivanje statusnih informacija (može biti 1 ili 0),
- 'authorized_for_' – naredbe koje započinju navedenim nizom određuju koji korisnici imaju pravo pristupa sistemskim informacijama, konfiguracijskim informacijama, mijenjanju sistemskih postavki, pristupa informacijama o računalima i servisima te mijenjanju istih.

Unutar cgi.cfg datoteke moguće je odrediti i grafički model prikaza računala i servisa kao i zvukove koji opisuju pojedina stanja računala i servisa.

3.2.4. hosts.cfg datoteka

Ova datoteka zamišljena je kao centralno mjesto za definiranje svih uređaja koje je potrebno nadgledati pomoću Nagios programa. Naravno, čitav ili samo dio njezinog sadržaja može se nalaziti unutar neke druge konfiguracijske datoteke no tada ovakva podjela gubi smisao. S druge strane, dozvoljeno je definiranje više različitih konfiguracijskih datoteka u kojima ćemo odvojeno definirati grupe računala. Pri tome je bitno da se svaka novonastala datoteka pravilno uključi u konfiguraciju cfg_file direktivom, odnosno da se izuzme ukoliko određeni segment mreže iz nekog razloga nije potrebno nadgledati.
Sintaksa prema kojoj se definira pojedino računalo raspoloživo je u minimal.cfg datoteci. Primjer definiranja jednog računala:

```
define host{
       use                     generic-host
       host_name               localhost
       alias                   localhost
       address                 127.0.0.1
       check_command           check-host-alive
       max_check_attempts      10
       notification_interval   120
       notification_period     24x7
       notification_options    d,r
       contact_groups          admins
}
```

Definicija računala sastoji se od sljedećih elemenata:

- 'host_name' - definira ime pod kojim će se uređaj raspoznavati unutar sustava,
- 'alias' – koristi se kao opširnije ime ili opis,
- 'address' - obično sadrži IP adresu uređaja, ali može se zadati i FQDN (eng. *Fully Qualified Domain Name*) no u slučaju otkazivanja DNS servera neće se moći provesti provjera na udaljenom uređaju,
- 'check_command' - definira koja naredba će se koristiti pri ispitivanju dostupnosti računala,
- 'max_check_attempts' – definira koliko puta će se provjera dostupnosti računala provesti prije nego se računalo proglasi nedostupnim,

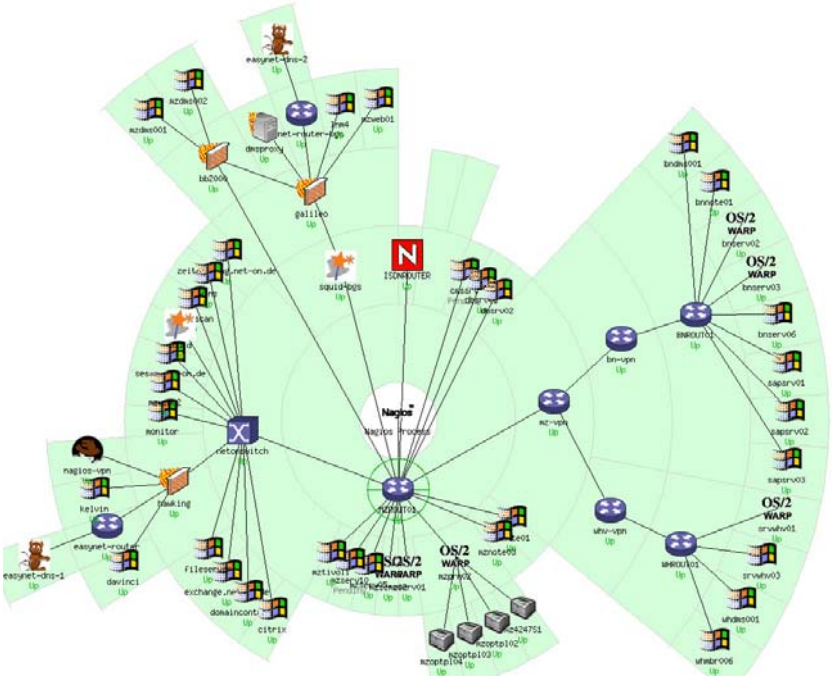
- 'notification_interval' - definira nakon koliko vremenskih jedinica će alat ponovo obavijestiti nadležnu osobu o postojećim problemima,
- 'notification_period' - definira u kojim vremenskim razdobljima će se obavijesti slati nadležnim osobama (npr. 24x7 - bilo koji sat svakog dana; vremenska jedinica je u danom primjeru standardno minuta, no taj se parametar može promijeniti),
- 'notification_options' - definira u kojim situacijama će se obavijesti slati nadležnim osobama; (d - *down*, r – *recovery*; *Down* je period u kojem računalo ne radi, dok je *recovery* vrijeme koje je potrebno da se računalo dovede u prethodno operativno stanje) i
- 'contact_groups' - navodi imena grupa korisnika koji će primati obavijesti u slučaju da konkretno računalo prijavi nepravilnosti u radu. Grupu čini više korisnika koji su nadležni za isti segment mreže.

Svaka konfiguracijska datoteka može sadržavati neograničeno mnogo definicija računala. Jedno od praktičnih rješenja koje Nagios pruža je mogućnost definiranja grupe računala. Na taj način moguće je više uređaja koji čine svojevrsnu cjelinu nadgledati paralelno. Općeniti oblik objekta:

```
define hostgroup{
    hostgroup_name    <ime_grupe>
    alias             <opis_grupe>
    members           <prvi_član,drugi_član,...>
}
```

Definicija grupe računala sastoji se od sljedećih elemenata:

- 'hostgroup_name' - određuje jedinstveno ime koje će identificirati konkretnu grupu,
- 'alias' - sadrži njezino opširnije ime ili opis i
- 'members' - direktiva definira sve članove grupe koristeći se njihovim imenima (zadana 'host_name' direktivom iz prethodnog primjera).



Slika 5: Vizualni prikaz mreže i njenih servisa

3.2.5. `services.cfg` datoteka

Ovo je još jedna korisnički definirana datoteka čija je svrha objedinjavanje svih zadataka koje se pred Nagios postave. Definiranje tih zadataka (eng. *services*), kao i u svim dosada spomenutim konfiguracijskim datotekama, prati određenu konvenciju. U ovom slučaju ona izgleda ovako:

```
define service{
    use                     generic-service
    host_name               localhost
    service_description     Current Users
    is_volatile             0
    check_period            24x7
    max_check_attempts      4
    normal_check_interval   5
    retry_check_interval    1
    contact_groups          admins
    notification_options    w,u,c,r
    notification_interval   960
    notification_period     24x7
    check_command           check_local_users!20!50
}
```

Gornji primjer ponovo je preuzet iz `minimal.cfg` datoteke. Kao u slučaju definicije računala i ovdje nailazimo na direktive:

- 'use' - povezuje konkretnu definiciju s općenitim predloškom (u ovom primjeru ime predloška je 'generic-service'),
- 'host_name' - definira ime pod kojim će se uređaj raspoznavati unutar sustava,
- 'service_description' - definira opis servisa,
- 'is_volatile' – vrijednost koja može se postaviti u 0 ili 1, ovisno o tome da li je potrebno zadaću koju definiramo proglasiti promjenjivom-učestalo mijenja stanje iz nule u 1 pa ju ne promatramo kao konstantu,
- 'check_period' - definira u kojim će se vremenskim razdobljima provjeravanje provoditi,
- 'max_check_attempts' ima istu ulogu kao istoimena direktiva u definiciji računala.
- 'normal_check_interval' i 'retry_check_interval' - određuju vremenski interval u kome će se ponoviti provjera statusa ukoliko je prethodno stanje bilo ispravno, odnosno ukoliko je provjera detektirala nepravilnost,
- 'notification_interval', 'notification_period' i 'notification_options' - definiraju uvjete u kojima će Nagios ponovo obavijestiti nadležnu osobu o postojećim problemima na isti način kako je to opisano u prethodnom poglavlju i
- 'check_command' - definira koju naredbu će alat pozvati kako bi obavio konkretnu zadaću.

3.2.6. `contacts.cfg` datoteka

Ova datoteka služi za definiranje svih kontakt osoba kojima se šalju obavijesti o statusu računala i servisa. Ukoliko se na korisnike primjenjuju ista pravila, korisnici se mogu grupirati u grupe. Sintaksa prema kojoj se definira pojedino računalo raspoloživo je u `minimal.cfg` datoteci. Primjer definiranja jedne kontakt osobe:

```
define contact{
   contact_name                  naziv
   alias                         nadimak
   service_notification_period   24x7
   host_notification_period      24x7
   service_notification_options  w,u,c,r
   host_notification_options     d,u,r
   service_notification_commands notify-by-email,notify-by-epager
   host_notification_commands    host-notify-by-email,host-notify-by-epager
   email                         email@adresa.hr
   pager                         38598999999
}
```

Definicija korisnika sastoji se od sljedećih elemenata:

- 'contact_name' - definira ime pod kojim će se kontakt osoba raspoznavati unutar sustava,

- 'alias' – sadrži opširniji naziv ili nadimak,
- 'service_notification_period' – određuje period u kojem se korisniku šalje obavijest o stanju servisa,
- 'host_notification_period' – određuje period u kojem se korisniku šalje obavijest o statusima računala,
- 'service_notification_options' – definira situacije u kojima se korisniku šalje obavijest o stanju servisa,
- 'host_notification_options' – definira situacije u kojima se korisniku šalje obavijest o statusima računala,
- 'service_notification_commands' - određuje načine obavještavanja korisnika o stanju servisa,
- 'host_notification_commands' - određuje načine obavještavanja korisnika o statusima računala,
- 'email' – definira adresu elektroničke pošte na koju se šalju obavijesti i
- 'pager' – definira broj mobitela ili pager-a na koji se šalje obavijest.

Svaka konfiguracijska datoteka može sadržavati neograničeno mnogo definicija pojedinih kontakt podataka kao i grupa kontakt osoba. Primjer grupe korisnika:

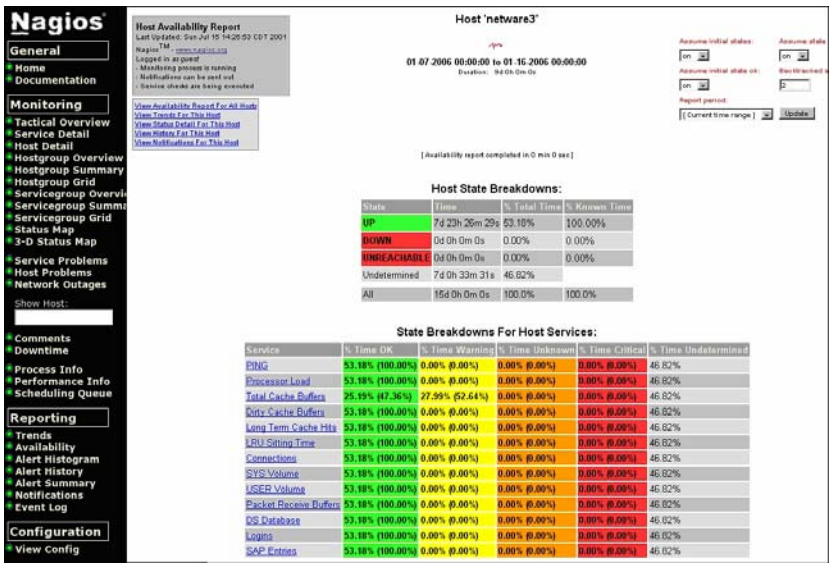
```
define contactgroup{
    contactgroup_name       naziv_grupe
    alias                   nadimak_grupe
    members                 korisnik1,korisnik2
}
```

Definicija grupe korisnika sastoji se od sljedećih elemenata:

- 'contactgroup_name' - određuje jedinstveno ime koje će identificirati konkretnu grupu,
- 'alias' - sadrži njezino opširnije ime ili nadimak i
- 'members' - direktiva definira sve članove grupe koristeći se njihovim imenima.

4. Web administracijsko sučelje

Specifičnost Nagios alata je mogućnost pregledavanja svih relevantnih informacija putem web sučelja. Time korisnici mogu administrirati Nagios alatom s bilo koje lokacije.



Slika 6: Web administracijsko sučelje: prikaz dostupnosti jednog računala

Sučelje je podijeljeno u 4 različite grupe izbornika gdje se dobivaju različite sistemske informacije:

- *General* – pruža osnovne informacije o programu i pripadajućoj dokumentaciji.

- *Monitoring* – pruža mogućnost odabira poslužitelja ili klijenata te njihovih servisa koje je potrebno nadgledati. Izbornik se sastoji od više manjih podizbornika:
  - *Tactical overview* - glavna stranica koja omogućava sumarni prikaz svih računala i servisa,
  - *Service detail* - pruža detalje vezane uz neki servis na računalu: stanja mogu biti: ispravno, upozorenje nad servisom, nedostupan servis.
  - *Host detail* - pruža detaljne informacije o računalu (prikazuje informacije o IP adresi računala, usmjerivačima na koji je spojen, broju dostupnih servisa, itd…),
  - *Hostgroup overview* - prikazuje slične informacije kao prethodna stavka, ali za grupu računala, te
  - *Hostgroup summary* - omogućuje sažeti prikaz za grupu računala. Ukoliko se povežu u grupu ili tzv polje (eng. *grid*) računala, tada Nagios prikazuje podatke o grupi računala.

  Isti načini izvješćivanja je primijenjen i za servise:
  - *Servicegroup overview* - prikazuje status za grupu servisa,
  - *Servicegroup summary* - omogućava skupno izvješćivanje za grupu servisa koji se izvode na računalima,
  - *Servicegroup grid* - prikazuje status o grupi servisa udruženih u tzv. *grid*,
  - *Service problems* - izbornik koji administratori najčešće koriste jer se na ovom mjestu prikazuju sve greške vezane uz servise,
  - *Host problems* - slično prethodnom izborniku služi za prikaz problema u radu računala i
  - *Network outages* - služi prikazivanju svih problema ili opterećenja mreže.
- *Reporting* izbornik pruža razne mogućnosti vizualnog prikaza prikupljenih informacija. Ali ukoliko nije potreban grafički prikaz, u ovoj cjelini se mogu pročitati i dnevnički zapisi (eng. *log*) bez grafičkog prikaza:
  - *Trends* - prikazuje usporedbe podataka za proteklo razdoblje s mogućnošću predviđanja problema u radu,
  - *Availability* - prikazuje dostupnost poslužitelja na mreži,
  - *Alert histogram* - grafičkim putem prikazuje greške u radu,
  - *Alert history* - prikazuje povijest grešaka u radu za računalo ili servis,
  - *Alert summary* - prikazuje sažetak grešaka za grupu računala ili servisa,
  - *Notifications* - prikazuje sve prikazane obavijesti i
  - *Event log* - prikazuje sve informacije o greškama u radu.
- *Configuration* - omogućava centralizirano konfiguriranje Nagios alata.

5. Zaključak

Nagios je koristan program sistemskim administratorima koji pruža uvid u cjelokupnu statistiku prometa na mreži uz mogućnost izvještavanja o nepravilnostima u radu. Korištenjem Nagios alata moguće je specificirati poslužitelje koje je potrebno pratiti, u kojem intervalu te definirati način izvještavanja o pogrešci s detaljnim objašnjenjem. Osnovna distribucija dolazi sa setom pomoćnih programa, ali moguće je izraditi i svoje što administratorima pruža neograničene mogućnosti. Glavni nedostatak programa je kompliciranа konfiguracija, osobito prilikom prve instalacije programa kad se od korisnika zahtjeva podešavanje brojnih sistemskih parametara. Ipak, to je potrebno s razlogom kreiranja kvalitetnijih izvješća o pogreškama

6. Reference

[1] Alat Nagios http://www.nagios.org/
[2] Alata CGI wrap http://cgiwrap.unixtools.org/
[3] Biblioteka PNG grafika za Nagios http://prdownloads.sourceforge.net/libpng/
[4] Biblioteke za JPG kompresiju slika http://www.ijg.org/files/
[5] Alat za generiranje dinamične grafike http://www.boutell.com/gd/
[6] Milenković Z.: Nadzor i upravljanje računalnim mrežama pomoću open source paketa Nagios, studeni 2004.