HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Implementacija syslog protokola u Windows okruženju

CCERT-PUBDOC-2005-05-120

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 4

2. SYSLOG PROTOKOL 5

2.1. ARHITEKTURA 5
2.2. FORMAT *SYSLOG* PORUKA 5
2.2.1. PRI polje 5
2.2.2. HEADER polje 7
2.2.3. MSG polje 8
2.3. NEDOSTACI SYSLOG PROTOKOLA 8
2.3.1. Neobvezujući format *syslog* poruka 8
2.3.2. Autentičnost poruka 8
2.3.3. Pouzdanost dostave 8
2.3.4. Ostala pitanja 9

3. IMPLEMENTACIJA *SYSLOG* PROTOKOLA U WINDOWS OKRUŽENJU 9

3.1. POSLUŽITELJSKA STRANA – KIWI SYSLOG DAEMON 9
3.1.1. Instalacija 9
3.1.2. Konfiguracija i rad 10
3.1.3. Ocjena paketa 12
3.2. KLIJENTSKA STRANA – NTSYSLOG 13
3.2.1. Instalacija 13
3.2.2. Konfiguracija i rad 13
3.2.3. Ocjena paketa 14
3.3. IMPLEMENTACIJA U STVARNOM OKRUŽENJU 14

4. ZAKLJUČAK 17

5. REFERENCE 17

1. Uvod

Nadzor i bilježenje aktivnosti u informacijskom sustavu vrlo su važni elementi u svakom sustavu za upravljanje sigurnošću. Aktivnosti se mogu bilježiti na razne načine, ovisno o elementu informacijskog sustava na kojem se provode određene aktivnosti ili mu se pristupa.

Kod tehničkih komponenti informacijskog sustava kao što su operacijski sustavi ili aplikacije na radnim stanicama i poslužiteljima ili mrežni uređaji (preklopnici, usmjerivači, vatrozidi i sl.), uobičajeno je bilježenje aktivnosti u tzv. *log* datoteke.

Načini bilježenja, informacije koje se bilježe, razina detaljnosti, format vremenskih znački i drugi parametri bilježenja vrlo često se razlikuju od implementacije do implementacije, a pregledavanje višestrukih *log* datoteka u velikim i/ili heterogenim sustavima postaje potpuno nepraktično, pa čak i nemoguće.

U složenim informacijskim sustavima, a posebno u onima kod kojih postoje formalni sustavi za upravljanje sigurnošću, od ključne je važnosti da se bilježenje svih aktivnosti važnih za ispravno i sigurno funkcioniranje sustava provodi kontrolirano. Sustavi za centralizirano bilježenje, koji se najčešće koriste u takvim okruženjima, omogućavaju jednostavnije ručno ili automatizirano pregledavanje *log* zapisa, te njihovo arhiviranje u skladu s definiranom sigurnosnom politikom.

Osim toga, korištenjem takvih sustava osigurava se dodatna razina sigurnosti na sustavima koji udaljeno šalju zabilježene aktivnosti, pošto u slučaju njihove kompromitacije od strane neovlaštenih korisnika sve aktivnosti koje su se događale prije kompromitacije ostaju zabilježene na centralnom sustavu, a zlonamjerni korisnik nema mogućnost njihove naknadne promjene u cilju uklanjanja tragova svojih aktivnosti.

U korporativnim okruženjima, korištenjem sustava za centralizirano/udaljeno bilježenje aktivnosti moguća je i efikasna separacija dužnosti, gdje osobe koje su zadužene za administraciju pojedinog sustava nemaju ovlasti nadzora nad zabilježenim aktivnostima na tom sustavu.

Syslog protokol predstavlja jednu od mogućnosti uspostave centraliziranog sustava za bilježenje aktivnosti. Na Unix/Linux sustavima njegova uporaba je sasvim uobičajena, a uglavnom je podržan i od proizvođača mrežne opreme. *Syslog* protokol (BSD *syslog* protokol) standardiziran je RFC dokumentom "The BSD syslog protocol" [1].

Za razliku od spomenutih sustava, Windows platforme same po sebi ne podržavaju *syslog* protokol, već je za njegovu podršku potrebna instalacija komponenti trećih strana koje Windows *Event Log*-u ili drugim *log* sustavima omogućavaju *syslog* funkcionalnost.

Ovaj dokument opisuje syslog protokol i mogućnost njegove primjene na Windows platformama. Prvi dio dokumenta opisuje *syslog* protokol, te daje osvrt na neke funkcionalne i sigurnosne nedostatke protokola, dok je u drugom dijelu opisan način implementacije *syslog* funkcionalnosti na Windows platformama korištenjem *freeware* programskih komponenti.

2. Syslog protokol

Syslog je *de facto* standard za bilježenje aktivnosti na većini sustava. RFC dokument 3164, "The BSD syslog protocol" opisuje komunikacijsku komponentu, odnosno *syslog* protokol, za slanje *syslog* poruka. Također, u dokumentu su opisana ograničenja i sigurnosni nedostaci protokola.

Obzirom na raznolikost zahtjeva i načina bilježenja aktivnosti, odnosno generiranja poruka kod različitih aplikacija, operacijskih sustava i uređaja, *syslog* protokol prvenstveno osigurava fleksibilnost.

Različite aplikacije mogu generirati poruke koje u sebi sadrže različite informacije, poruke jezgri operacijskih sustava također mogu biti raznolike. Nadalje, uređaji nemaju internu mogućnost bilježenja (pisači, preklopnici i sl.) mogu imati mogućnost generiranja poruka. Poželjno je da takve poruke sadrže generalne informacije kao što su:

- vremenska značka događaja ili vrijeme generiranja poruke,
- ime aplikacije ili uređaja koji je generirao događaj,
- razina ozbiljnosti događaja.

Obzirom da zbog različitosti načina i razloga generiranja poruka u različitim sustavima te poruke ne sadrže nužno neke od tih informacija, *syslog* protokol je definiran tako ne nameće nikakva ograničenja na sadržaj poruka, niti uključuje obvezna polja.

Nadalje, poruke raznih aplikacija i različitih razina ozbiljnosti mogu, na temelju sigurnosne politike ili drugih zahtjeva, biti prikazivane na konzoli, zapisane u datoteci na lokalnom računalu, poslane na udaljeno centralno mjesto za bilježenje aktivnosti ili na različita mjesta, ovisno o ozbiljnosti ili izvoru poruke. *Syslog* je zamišljen tako da osigurava sve navedene funkcionalnosti.

2.1. Arhitektura

Arhitektura *syslog* protokola vrlo je jednostavna i sastoji se od sljedeća tri entiteta:

- **uređaja** (eng. *device*) – predstavlja uređaj (ili servis ili aplikaciju pokrenutu na uređaju) koji je generator *syslog* poruke,
- tzv. ***syslog relay* uređaja** koji prima i prosljeđuje syslog poruke i
- ***syslog* poslužitelja**, odnosno kolektora (eng. *collector*) koji isključivo prima *syslog* poruke.

Prilikom komunikacije *syslog* protokolom uređaj je isključivo pošiljatelj poruka, syslog poslužitelj je isključivo primatelj poruka, dok *syslog relay* predstavlja entitet koji je i primatelj i pošiljatelj. Bilo koji pošiljatelj može slati poruke višestrukim primateljima, a *syslog relay* može generirati i vlastite poruke (u tom slučaju on predstavlja samo uređaj).

Slika 1 prikazuje neke od mogućih *syslog* arhitektura. U praksi najviše se koristi arhitektura prikazana u prvom primjeru (1), no i druge mogućnosti imaju svoju primjenu. Također, podrazumijeva se da višestruki uređaji mogu prosljeđivati poruke istim *syslog relay* i *syslog* poslužitelj entitetima.

2.2. Format *syslog* poruka

Format syslog poruka nije striktno definiran što omogućava prihvaćanje poruka generiranih na različite načine, ali dovodi i do nekih nekonzistentnosti. Generalno, svaki UDP paket s odredišnim portom 514 treba se tretirati kao *syslog* poruka. Ukupna duljina paketa može biti maksimalno 1024 okteta, a minimalna duljina nije definirana, iako je slanje prazne *syslog* poruke besmisleno.

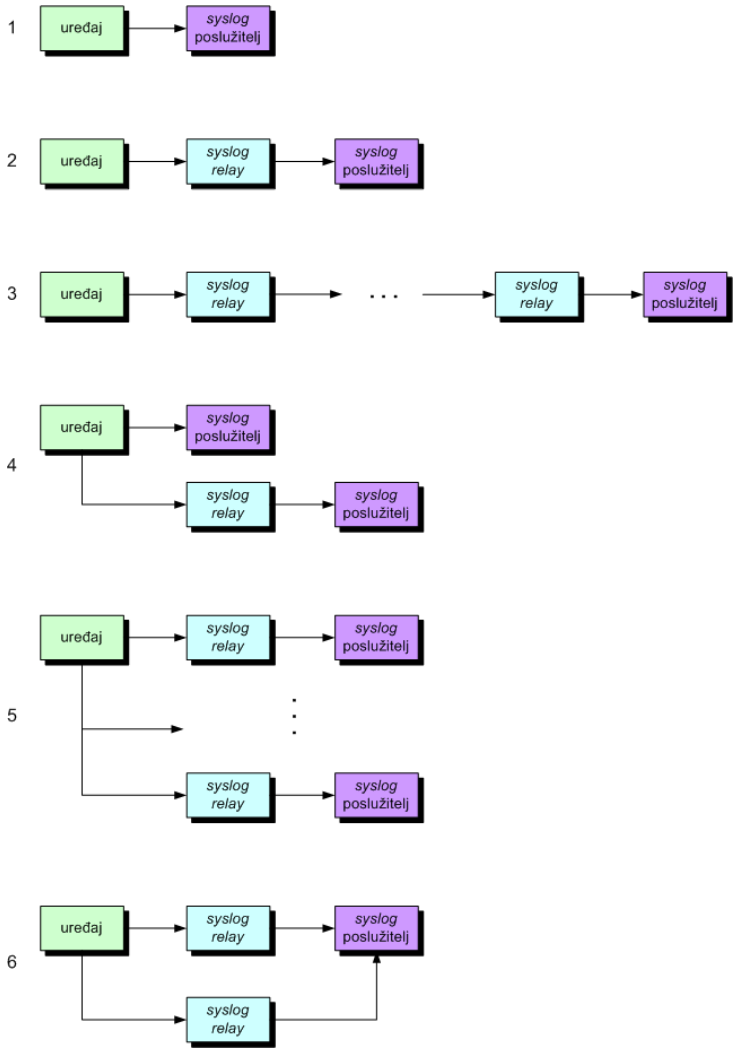
Syslog poruka trebala bi biti sadržana u podatkovnom dijelu UDP paketa i trebala bi se sastojati od sljedeća tri polja:

- `PRI`,
- `HEADER` i
- `MSG`.

2.2.1. PRI polje

`PRI` polje mora se sastojati od tri, četiri ili pet ASCII znakova. `PRI` polje počinje s "<" znakom (ASCII kod `0x3C`), a završava s ">" znakom (ASCII kod `0x3E`). Broj sadržan između znakova "<" i ">" može imati jednu, dvije ili tri znamenke u ASCII obliku koje mogu poprimiti vrijednosti od "0" (ASCII kod

0x30) do "9" (ASCII kod 0x39), a označava prioritet i predstavlja kodove koji označavaju izvor koji je generirao poruku (eng. *facility*) i razinu ozbiljnosti poruke (eng. *severity*).



Slika 1: Neke od mogućih syslog arhitektura

Protokol definira kodove izvora koji generiraju poruke (*Tablica 1*) i razine ozbiljnosti poruka (*Tablica 2*). Procesi i servisi koji nisu eksplicitno definirani kao izvori poruka mogu koristiti bilo koji kod rezerviran za lokalnu uporabu (kodovi 17 do 23) ili kod namijenjen korisničkim porukama (kod 1).

Kod	Izvor poruke
0	jezgra operacijskog sustava (eng. *kernel messages*)
1	korisničke poruke (eng. *user-level messages*)
2	e-mail sustav (eng. *mail system*)
3	sistemski servisi (eng. *system daemons*)
4	sigurnosne/autentikacijske poruke (eng. *security/authorization messages*)
5	poruke generirane interno od *syslogd* servisa
6	linijski pisač (eng. *line printer subsystem*)
7	*network news* sistem
8	UUCP sistem
9	sistemski sat (eng. *clock daemon*)
10	sigurnosne/autentikacijske poruke

Kod	Izvor poruke
11	Poruke FTP servisa
12	Poruke NTP servisa
13	log zapisi (eng. *log audit*)
14	log zapisi
15	sistemski sat (eng. *clock daemon*)
16	Lokalna uporaba (eng. *local use 0*)
17	Lokalna uporaba (eng. *local use 0*)
18	Lokalna uporaba (eng. *local use 0*)
19	Lokalna uporaba (eng. *local use 0*)
20	Lokalna uporaba (eng. *local use 0*)
21	Lokalna uporaba (eng. *local use 0*)
22	Lokalna uporaba (eng. *local use 0*)

Tablica 1: Kodovi koji označavaju izvor poruke

Kodovi 4, 10, 13 i 14 označavaju iste izvore poruka (sigurnosne i autentikacijske poruke) iz razloga što različiti sustavi za istu ili sličnu namjenu koriste te (različite) kodove. Slično, za sistemski sat rezervirani su kodovi 9 i 15. Na temelju eksplicitno definiranih izvora poruka, uočljivo je da je *syslog* protokol izvorno zamišljen za Unix sustave.

Kod	Razina ozbiljnosti
0	izvanredno stanje: sustav nije funkcionalan (eng. *emergency: system unusable*)
1	uzbuna: nužna trenutna akcija (eng. *alert: action must be taken immediately*)
2	kritična (eng. *critical: critical conditions*)
3	pogreška (eng. *error: error conditions*)
4	upozorenje (eng. *warning: warning conditions*)
5	opomena (eng. *notice: normal but significant condition*)
6	informacije (eng. *informational: informational messages*)
7	debug informacije (eng. *debug: debug-level messages*)

Tablica 2: Kodovi koji označavaju ozbiljnost poruke

Vrijednost PRI polja računa se na sljedeći način:

```
"<" + integer_to_ASCII(izvor*8 + ozbiljnost) + ">"
```

Na primjer vrijednost PRI polja za kritičnu poruku jezgre operacijskog sustava bila bi sljedeća:

```
"<" + integer_to_ASCII(0*8 + 2) + ">" = <2>
```

Na isti način bi vrijednost PRI polja za informativnu poruku FTP servisa bila:

```
"<" + integer_to_ASCII(11*8 + 6) + ">" = <94>
```

2.2.2. HEADER polje

HEADER polje sastoji se od dva podpolja:

- TIMESTAMP – označava vremensku značku (eng. *timestamp*) i
- HOSTNAME – označava IP adresu ili ime uređaja koji je generirao *syslog* poruku.

U HEADER polju dozvoljena je uporaba vidljivih ASCII znakova i praznine (od 0x21 do 0x7E i 0x20), a ono se nastavlja odmah nakon ">" znaka PRI polja TIMESTAMP poljem koje označava lokalno vrijeme i mora biti oblika:

```
Mmm dd hh:mm:ss
```

gdje Mmm označava mjesec (moguće vrijednosti: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec), dd označava dan u mjesecu, a hh:mm:ss označava sate, minute i sekunde.
Nakon toga obvezno slijedi praznina (ASCII kod 0x20), te zatim HOSTNAME polje nakon kojega ponovno slijedi praznina. HOSTNAME polje može predstavljati IP adresu uređaja ili ime uređaja, a ne smije sadržati praznine.

Slijedi primjer ispravnih HEADER polja:

```
Jan 31 23:48:55 192.168.1.3
Feb 01 01:03:34 host.local.ad[192.168.1.3]
```

Za razliku od toga, sljedeća HEADER polja su neispravna i biti će krivo protumačena od strane *syslog relay*-a ili *syslog* poslužitelja:

```
Jan 31 23:48:55 192.168.1.3 GMT+1 192.168.1.3
Jan 31 23:48:55 192.168.1.3 host.local.ad [192.168.1.3]
```

2.2.3. MSG polje

Nakon PRI i HEADER polja, MSG polje odnosi se na ostatak UDP paketa. MSG, isto kao i HEADER polje, smije sadržavati samo vidljive ASCII znakove i prazninu (od 0x21 do 0x7E i 0x20), a sastoji se od dva podpolja:

- TAG – označava ime programa ili procesa koji je generirao poruku i
- CONTENT – sadrži detaljne informacije o razlogu generiranja poruke.

TAG polje je maksimalne duljine 32 znaka, a smije se sastojati samo od alfanumeričkih ASCII znakova (0-9, A-Z i a-z). Bilo koji nealfanumerički znak biti će protumačen kao početak CONTENT polja. Za odvajanje TAG i CONTENT polja uobičajeno je korištenje znakova "]", ":" ili praznine.

2.3. Nedostaci syslog protokola

2.3.1. Neobvezujući format *syslog* poruka

Iako protokol definira polja koja *syslog* poruka treba imati, takav format poruke, odnosno paketa nije obvezan, nego je samo preporuka. To znači da *syslog* poruke ne moraju nužno biti oblikovane tako da sadrže sva tri (PRI, HEADER i MSG) polja definirana protokolom.

Prema protokolu, *syslog relay* uređaji trebali bi prilikom prosljeđivanja poruka oblikovati njihov sadržaj tako da odgovaraju preporukama protokola. Detaljne informacije o konvencijama koje se pri tom koriste dane su u samoj specifikaciji protokola [1].

Također, neke implementacije *syslog* uređaja (*relay* uređaja i *syslog* poslužitelja) bile su osjetljive na pogrešno oblikovane pakete (standardna polja, dozvoljeni skup ASCII znakova) ili pakete čija je duljina bila veća od 1024 okteta.

2.3.2. Autentičnost poruka

Mehanizam *syslog* protokola ne zahtijeva nikakvu provjeru autentičnosti *syslog* poruka. Npr. primatelj *syslog* poruke ne uspoređuje adresu u IP zaglavlju *syslog* paketa s HOSTNAME vrijednošću u HEADER polju. Zbog karakteristika samog oblika tog polja (nije nužno navesti niti IP adresu niti FQDN ime pošiljatelja), u nekim slučajevima takvu usporedbu ne bi ni bilo moguće napraviti.

Nedostatak autentikacije poruka omogućava napade kao što su umetanje lažiranih poruka (eng. *injection*) ili ponavljanje (eng. *replaying*) prethodno presretnutih poruka koje se mogu lažirati prema potrebi (eng. *message forgery*). Kombinacijom ovih nedostataka potencijalni napadač ima priličan broj mogućnosti zavaravanja ili prikrivanja svojih aktivnosti, unatoč tome što napadnuti uređaj ili mreža koriste neovisne *syslog* poslužitelje.

2.3.3. Pouzdanost dostave

Syslog protokol za slanje paketa koristi UDP protokol. Inherentni nedostatak UDP protokola jest nedostatak potvrde prijema od strane primatelja. Zbog jednostavnosti *syslog* protokola i prirode informacija koje sadrže *syslog* paketi, odbacivanje tih paketa (bilo zbog zagušenja mreže ili oštećenja) vrlo lako može proći nezapaženo na strani *syslog* poslužitelja.

Isto tako, niti uređaj koji je generirao paket, odnosno pošiljatelj *syslog* poruke ne može biti siguran da je *syslog* poruka uspješno primljena od strane *syslog* poslužitelja, ili da je *syslog* poslužitelj uopće u funkciji (što ipak donekle može biti provjereno korištenjem posrednih metoda – npr. slanjem odgovarajućih ICMP paketa).

Nadalje, *syslog* protokol ne osigurava pravilan redoslijed dostave paketa. Moguće je da primatelj *syslog* poruke ne dobiva poruke onim redoslijedom kojim ih pošiljatelj šalje, što može uzrokovati probleme u kasnijoj interpretaciji *syslog* zapisa.

2.3.4. Ostala pitanja

Zbog nepostojanja nikakvog kontrolnog mehanizma, ispravnost konfiguracije *syslog* sustava potpuno je ovisna o ljudskom faktoru. Može se dogoditi da pošiljatelj zbog pogrešne konfiguracije šalje podatke krivom primatelju koji uopće nije konfiguriran da prima *syslog* poruke.
Također, neispravno konfiguriranje *relay* uređaja u složenijim konfiguracijama (*Slika 1*) može uzrokovati generiranje beskonačne petlje.
Na kraju, na strani *syslog* poslužitelja potrebno je ispravno dimenzionirati diskovni prostor, pošto *syslog* bilježenje može biti vrlo intenzivno. U suprotnom, vrlo lako se mogu, namjerno – od strane zlonamjernih korisnika ili nenamjerno, ostvariti DoS (eng. *denial of service*) uvjeti.

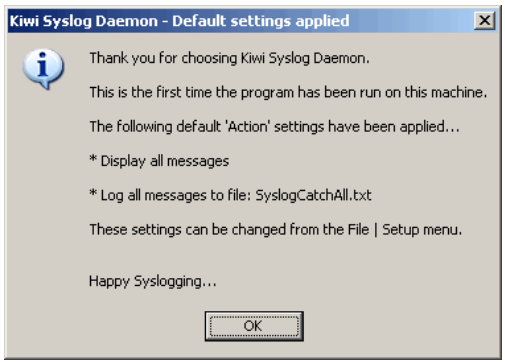
3. Implementacija *syslog* protokola u Windows okruženju

3.1. Poslužiteljska strana – Kiwi Syslog Daemon

Kiwi Syslog Daemon (http://www.kiwisyslog.com) najpoznatiji je *syslog* poslužitelj za Windows 9x/Me/NT/2000/XP/2003 sustave, a postoji u komercijalnoj i *freeware* inačici. Već i *freeware* inačica sadrži sve potrebne funkcionalnosti *syslog* poslužitelja, a osim toga ima i brojne druge mogućnosti.
Standardna *syslog* funkcionalnost omogućava Kiwi Syslog Daemon-u da funkcionara kao *syslog* poslužitelj ili kao *syslog relay*. *Syslog relay* prosljeđivanje moguće je definirati na temelju razine ozbiljnosti i drugih parametara.
Sve primljene poruke mogu se bilježiti, arhivirati i prikazivati u stvarnom vremenu. Također, omogućeno je generiranje uzbuna u slučaju pojedinih događaja. Na temelju primljenih poruka Kiwi Syslog omogućava i generiranje statistika i grafičkih prikaza. Konačno, osim standardne UDP komunikacije, Kiwi Syslog također podržava TCP i SMNP komunikaciju.

3.1.1. Instalacija

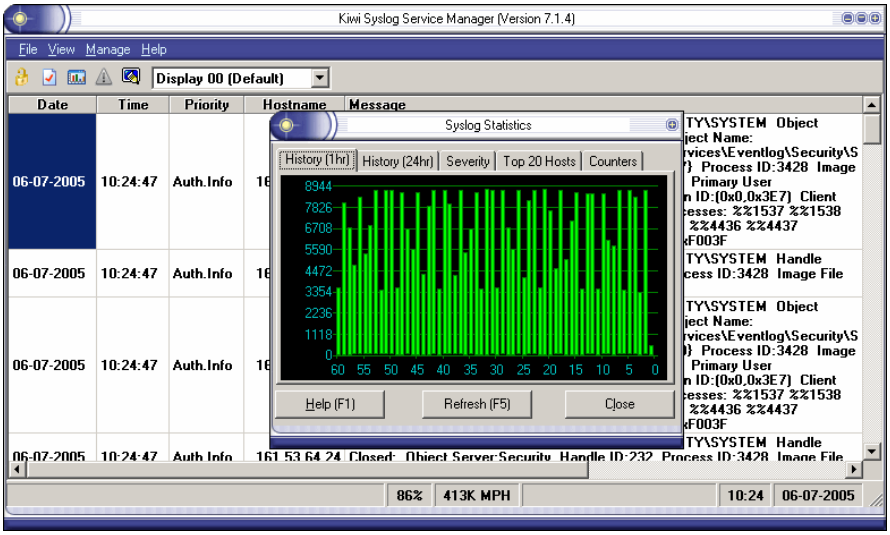
Freeware inačicu Kiwi Syslog Daemon paketa moguće je dohvatiti na stranici http://www.kiwisyslog.com/software_downloads.htm, s koje se mogu dohvatiti inačice paketa koje funkcioniraju kao aplikacija ili kao servis (isključivo za NT-bazirane sustave).
Nakon pokretanja dohvaćene *installer* datoteke pokreće se postupak instalacije u kojem je potrebno prihvatiti uvjete licence, način instalacije (*normal*, *normal with shortcuts* ili *custom*), te ciljnu mapu, nakon čega se instalira Kiwi Syslog Daemon servis koji funkcionira s *LocalSystem* ovlastima. Po završetku instalacije moguće je odmah pokrenuti servis, nakon čega korisnik dobiva osnovne informacije o parametrima s kojima je servis pokrenut (*Slika 2*).



Slika 2: Kiwi Syslog Daemon moguće je pokrenuti neposredno nakon instalacije

3.1.2. Konfiguracija i rad

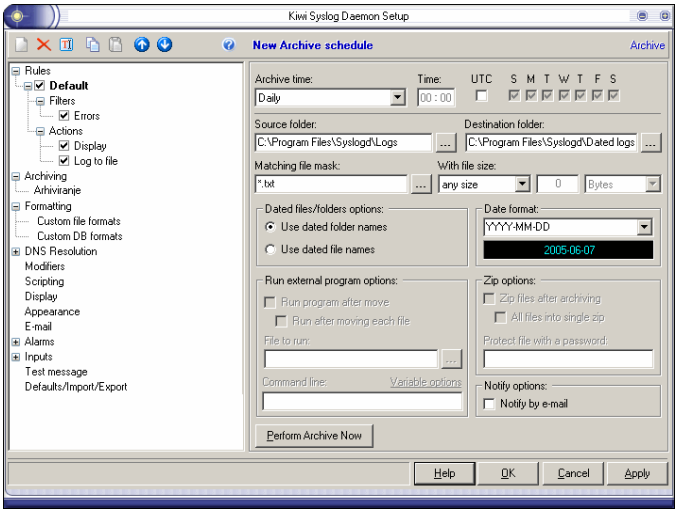
Grafičko sučelje Kiwi Syslog Daemon ima velik broj elemenata pomoću kojih je moguće podešavati različite parametre poslužitelja i nadzirati njegov rad (*Slika 3*). Za inicijalnu konfiguraciju najvažnije je podesiti postavke poslužitelja, što se čini kroz izbornik *File*, naredba *Setup*.



Slika 3: Kiwi Syslog Daemon konzola

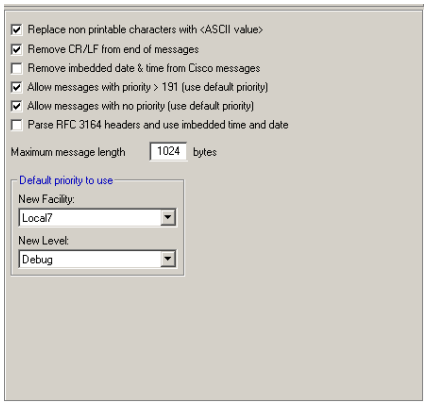
Odabirom te naredbe otvara se novi prozor u kojem je moguće podesiti sve postavke bitne za rad *syslog* poslužitelja. Korisnik može konfigurirati sljedeće postavke i grupe postavki:

- *Rules* – omogućava podešavanje pravila. Pravila se definiraju podešavanjem filtara (*Filters*) prema prioritetima, IP adresama, imenima računala, tekstu poruka, vremenskim značkama i brojčanim veličinama, te akcija (*Actions*) koje mogu biti prikaz na ekranu, zapisivanje u log datoteku, prosljeđivanje na drugi (*syslog*) poslužitelj, zvukovno upozorenje, izvršavanje proizvoljnog programa, slanje e-mail poruke, slanje *syslog* poruke, zapisivanje u ODBC bazu, zapisivanje u Windows *Event log*, slanje SNMP trap-a, izvršavanje skripte, te slanje ICQ ili NotePager poruke.
- *Archiving* – omogućava arhiviranje (*Slika 4*). Arhiviranja je moguće provoditi vremenskim zakazivanjem. Prilikom toga je moguće i izvršavanje vanjskih programa, slanje e-mail poruka, a arhivirane datoteke moguće je automatski komprimirati u `.zip` datoteke.



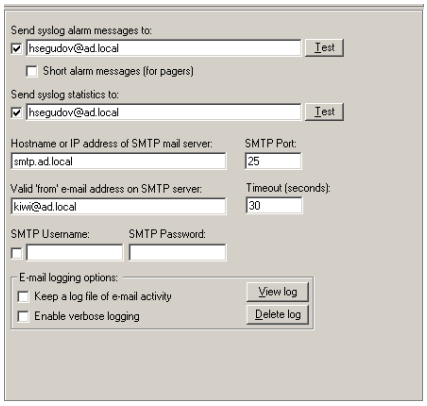
Slika 4: Funkcija arhiviranja omogućava kvalitetan backup syslog informacija

- *Formatting* – omogućava podešavanje formata zapisivanja u datoteke (*Custom File Formats*) i baze (*Custom DB Formats*).
- *DNS Resolution* – omogućava podešavanje parametara uz DNS rezoluciju. Ovdje je moguće podesiti i modifikaciju teksta *syslog* poruka u skladu s provedenom DNS rezolucijom (npr. dodavanje DNS imena uz IP adresu).
- *Modifiers* – omogućava modifikaciju nekih elemenata primljenih poruka. Npr. moguće je odbacivati nevidljive ASCII znakove, CR/LF oznake na kraju poruke, ograničiti maksimalne duljine poruke i sl. (*Slika 5*).



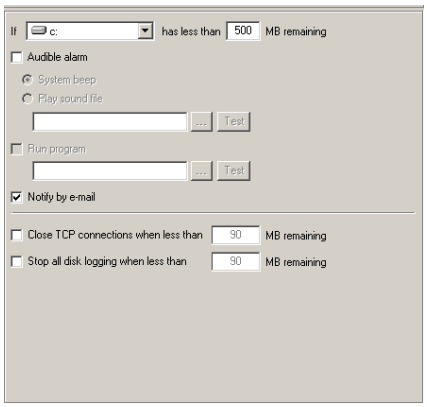
Slika 5: Mogućnosti modifikacije primljenih poruka

- *Scripting* – omogućava korištenje do 16 statičkih varijabli za generiranje korisničkih statistika koje se mogu koristiti u skriptama.
- *Display* – omogućava podešavanje opcija grafičkog prikaza *syslog* poruka.
- *Appearance* – omogućava podešavanje izgleda konzole.
- E-*mail* – omogućava podešavanje e-mail postavki za slanje *syslog* upozorenja i *syslog* statistika (*Slika 6*).



Slika 6: E-mail postavke moguće je podesiti za slanje syslog upozorenja i syslog statistika

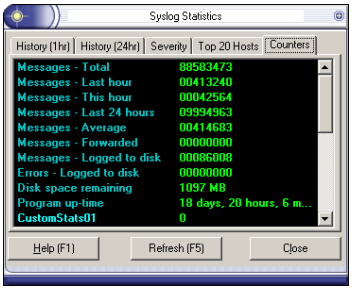
- *Alarms* – omogućava generiranje upozorenja prema minimalnom i maksimalnom broju poruka primljenih u zadanom vremenskom roku, te prema raspoloživom diskovnom prostoru na poslužitelju.



Slika 7: Nadziranje količine slobodnog diskovnog prostora vrlo je važno kod syslog poslužitelja

- *Input* – omogućava podešavanje osnovne funkcionalnosti. Kiwi Syslog Daemon može primati UDP i TCP *syslog* poruke na proizvoljnom portu, te SNMP trap poruke.
- *Test Message* – omogućava slanje test poruke. Koristi se za dijagnostiku.
- *Defaults/Import/Export* – omogućava učitavanje predefiniranih postavki ili pohranu/učitavanje parametara programa.

Neki od opisanih konfiguracijskih parametara su onemogućeni u *freeware* inačici, ali to vrlo malo utječe na efikasnost kompletnog paketa.
Osim konfiguracijskih postavki, Kiwi Syslog Daemon sučelje podijeljeno u traku s izbornicima i traku s alatima omogućava i podešavanje drugih postavki, te interaktivni rad u konzoli.
Izbornik *File*, osim konfiguracijskih postavki omogućava čišćenje raznih datoteka (e-mail log zapisi, log zapisi o pogreškama itd.), ispravljanje problema u radu (*Debug*), kopiranje ekrana ili dijela ekrana u Windows *Clipboard*, pohranu konfiguracije u `.ini` datoteku, te slanje *syslog* test poruke.
Izbornik *View* omogućava podešavanje načina ekranskog pregleda (brisanje, odabir fonta), pregled e-mail log datoteka i log datoteka s pogreškama, te prikaz statistike (*Slika 8*).



Slika 8: Prikaz osnovnih statističkih podataka

Izbornik *Manage* omogućava pokretanje i zaustavljanje servisa, prikaz stanja servisa, ispravljanje problema u radu servisa, te uklanjanje servisa s računala.
Konačno, izbornik *Help* omogućava pomoć pri radu s Kiwi Syslog Daemon paketom.

3.1.3. Ocjena paketa

Kiwi Syslog Daemon odličan je *syslog* poslužitelj. Servis nadilazi osnovne *syslog* funkcionalnosti, pa osim UDP *syslog* poruka može primati i TCP *syslog* poruke, isto kao i pratiti SNMP trap-ove. Korištenjem filtara, pravila, mogućnosti arhiviranja, generiranja upozorenja i drugih opcija moguće je vrlo kvalitetno podešavanje bilježenja i izolacija bitnih događaja, što je od presudne važnosti prilikom pregleda generiranih *syslog* zapisa.
Korištenjem i dobrom konfiguracijom Kiwi Syslog Daemon može se koristiti kao *syslog* poslužitelj čak i u većim tvrtkama, odnosno mrežnim okruženjima, dok je za manja okruženja već i mali dio opcija koje pruža dovoljan za kvalitetno i pouzdano bilježenje.

3.2. Klijentska strana – NTSyslog

NTSyslog (http://ntsyslog.sourceforge.net) je *freeware syslog* klijent za Windows NT/2000/XP/2003 sustave koji ima mogućnost presretanja i prosljeđivanja svih događaja koji se bilježe u standardnim Windows *Application*, *Security* i *System* logovima. Ukoliko se radi o poslužitelju, NTSyslog može pratiti i druge specifične log zapise: npr. *DNS Server*, *Directory Service* i sl.

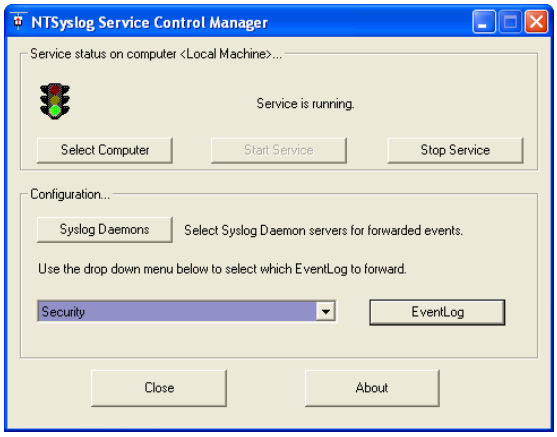
3.2.1. Instalacija

NTSyslog moguće ga je dohvatiti na stranici http://sourceforge.net/projects/ntsyslog s koje se mogu dohvatiti `.zip` datoteke s izvršnom datotekom koju je potrebno ručno instalirati ili gotovi *installer* paket.

Instalacija korištenjem *installer* paketa je jednostavna, a korisnik u nekoliko koraka mora prihvatiti uvjete licence, odabrati ciljnu mapu, komponente koje će instalirati (*full*, *compact* ili *custom* instalacija), te ime programske mape u *Programs* izborniku. Nakon toga NTSyslog se instalira kao servis na ciljnom računalu. Predefinirano NTSyslog radi s *LocalSystem* korisničkim ovlastima, no može raditi pod bilo kojim drugim korisničkim računom, pod uvjetom da ima sljedeće ovlasti na lokalnom računalu:

- *Logon as a service* i
- *Manage auditing and security log*,

što se može podesiti kroz *Group policy* snap-in (lokalno ili unutar domene).



Slika 9: Grafičko sučelje NTSyslog servisa

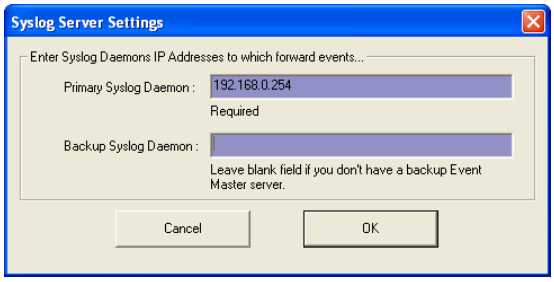
3.2.2. Konfiguracija i rad

Korištenje NTSyslog grafičkog sučelja (*Slika 9*) vrlo je jednostavno, dok istovremeno osigurava svu potrebnu *syslog* funkcionalnost. Prozor sučelja podijeljen je u dva dijela:

- statusni dio i
- konfiguraciju.

U statusnom dijelu moguće je vidjeti trenutno stanje servisa (da li je pokrenut ili ne), te izvršiti pokretanje (*Start Service*) ili zaustavljanje (*Stop Service*) NTSyslog servisa. Također, pritiskom na *Select Computer* gumb unutar statusnog dijela, moguće je administrirati i NTSyslog servise na udaljenim računalima, pod uvjetom da korisnički račun pod kojim je pokrenut NTSyslog ima administrativne ovlasti na udaljenom računalu. Ova opcija olakšava rad i konfiguraciju NTSyslog servisa u složenijim mrežnim okruženjima.

Konfiguracija NTSyslog klijenta svodi se na podešavanje *syslog* poslužitelja koje se provodi pritiskom na *Syslog Daemons* gumb, nakon čega se otvara novi prozor u kojem se mogu podesiti IP adrese primarnog i eventualnog *backup syslog* poslužitelja (*Slika 10*).



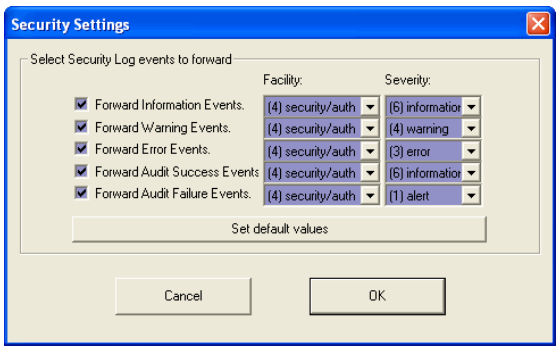
Slika 10: Podešavanje syslog poslužitelja

Osim podešavanja *syslog* poslužitelja, potrebno je podesiti i način transpozicije Windows log zapisa u *syslog* format. Način transpozicije može se definirati posebno za sve logove koji postoje na lokalnom računalu.

Odabirom željenog loga iz padajućeg izbornika i pritiskom na *EventLog* gumb moguće je podesiti:

- Koji će se Windows događaji prosljeđivati (*information*, *warning*, *error*, *audit success* i *audit failure*),
- Kako će se interpretirati izvor poruke. NTSyslog podržava sve kodove izvora specificiranih *syslog* protokolom (*Tablica 1*),
- Kako će se transponirati odgovarajuća razina ozbiljnosti događaja. NTSyslog podržava sve razine ozbiljnosti specificiranih *syslog* protokolom (*Tablica 2*).

Slika 11 prikazuje moguću konfiguraciju transpozicije Windows *Security loga* u *syslog* format. Obzirom da *syslog* protokol i Windows sustavi ne koriste isti sustav za klasifikaciju razina ozbiljnosti događaja, konkretna konfiguracija ovisi o potrebama i zahtjevima pojedinog sustava. Isto se može reći i za izvore poruka, iako bi se npr. događaji iz *Security* loga pravilno trebali transponirati u *syslog* kodove 4, 10, 13 ili 14 (poglavlje 2.2.1).



Slika 11: Moguća konfiguracija transpozicije Windows Security loga u syslog zapise

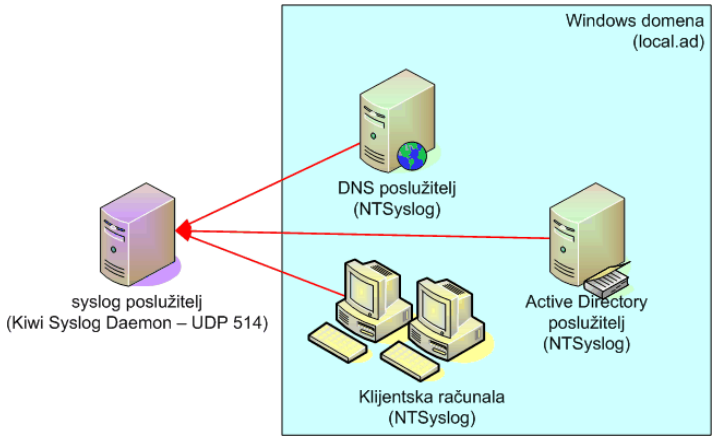
3.2.3. Ocjena paketa

NTSyslog se u radu pokazao stabilnim i pouzdanim, a grafičko sučelje je jednostavno i pregledno. Vrlo je korisna i mogućnost udaljene administracije postojećih NTSyslog servisa, čime se olakšava konfiguracija u mrežnom okruženju. Jedini nedostatak paketa jest nemogućnost ručnog podešavanja UDP porta na koji se šalju *syslog* poruke, ukoliko je odgovarajući *syslog* poslužitelj podešen tako da osluškuje *syslog* poruke na nestandardnom portu.

3.3. Implementacija u stvarnom okruženju

Korištenjem opisanih poslužiteljskih (Kiwi Syslog Daemon) i klijentskih (NTSyslog) komponenti implementirano je bilježenje u jednostavnom domenskom okruženju. *Slika 12* prikazuje logičku shemu implementacije *syslog* bilježenja u Windows okruženju. U mrežnom okruženju postoji Windows 2003 domena (`local.ad`), koja se sastoji od *Active Directory* poslužitelja (Windows Server 2003), DNS poslužitelja (Windows Server 2003) i Windows 2000/XP klijentskih radnih stanica. Na svim

poslužiteljima i radnim stanicama u domeni instaliran je NTSyslog servis koji se administrira korištenjem NTSyslog konzole s *Active Directory* poslužitelja.
Također, na Windows Server 2003 poslužitelju koji nije dio domene, već je samostalni poslužitelj (eng. *standalone server*) instaliran je Kiwi Syslog Daemon poslužitelj. Syslog poslužitelj implementiran je izvan Windows domene da bi se osigurala efikasna separacija dužnosti, odnosno da domenski administrator ne bi imao pravo pristupa, odnosno promjene zabilježenih podataka (domenski administrator i dalje ima ovlasti zaustavljanja NTSyslog servisa na domenskim poslužiteljima).



Slika 12: Logička shema implementacije syslog protokola

Točne konfiguracije NTSyslog parametara na klijentskim računalima i poslužiteljima dane su u nastavku. Transpozicija Windows poruka u *syslog* poruke napravljena je tako da se na središnjem *syslog* poslužitelju mogu jednostavnije identificirati poruke pojedinih servisa. *Tablica 3* daje konfiguraciju NTSyslog-a na *Active Directory* poslužitelju. Poruke imeničkog servisa na *Active Directory* poslužitelju transponiraju se kao lokalni izvor poruka (*local 0*). Niti jedan drugi servis na drugim računalima nije podešen da se transponira kao *local 0* izvor. Također servis za replikaciju datoteka (*File Replication Service*) transponiran je kao uucp (8) izvor (izvorno *unix-to-unix copy* protokol).

Syslog poslužitelji		
Primarni syslog poslužitelj	192.168.0.254	
Backup syslog poslužitelj	-	
Syslog transpozicije		
Application log	**izvor poruke (eng. facility)**	**razina ozbiljnosti (eng. *severity*)**
Error	(18) local 2	(1) alert
Warning	(18) local 2	(4) warning
Information	(18) local 2	(6) information
Security log		
Success	(4) security/auth	(6) information
Failure	(4) security/auth	(1) alert
System log		
Error	(3) system	(0) emergency
Warning	(3) system	(4) warning
Information	(3) system	(6) information
Directory service log		
Error	(16) local 0	(0) emergency
Warning	(16) local 0	(4) warning
Information	(16) local 0	(6) information
File Replication Service log		
Error	(8) uucp	(1) alert
Warning	(8) uucp	(4) warning

Information	(8) uucp	(6) information

Tablica 3: Konfiguracija NTSyslog-a na Active Directory poslužitelju

Tablica 4 daje konfiguraciju NTSyslog-a na DNS poslužitelju. Poruke DNS servisa na ovom poslužitelju transponiraju se kao lokalni izvor poruka (*local 1*). Niti jedan drugi servis na drugim računalima nije podešen da se transponira kao *local 1* izvor.

Syslog poslužitelji		
Primarni syslog poslužitelj	192.168.0.254	
Backup syslog poslužitelj	-	
Syslog transpozicije		
Application log	**izvor poruke (eng. facility)**	**razina ozbiljnosti (eng. *severity*)**
Error	(18) local 2	(1) alert
Warning	(18) local 2	(4) warning
Information	(18) local 2	(6) information
Security log		
Success	(4) security/auth	(6) information
Failure	(4) security/auth	(1) alert
System log		
Error	(3) system	(0) emergency
Warning	(3) system	(4) warning
Information	(3) system	(6) information
DNS server log		
Error	(17) local 1	(0) emergency
Warning	(17) local 1	(4) warning
Information	(17) local 1	(6) information

Tablica 4: Konfiguracija NTSyslog-a na DNS poslužitelju

Također, na oba poslužitelja aplikacijske, sigurnosne i sistemske poruke transponiraju se identično, što znači da ih na syslog poslužitelju razlikuje samo HOSTNAME polje.

Tablica 5 prikazuje postavke na klijentskim računalima. Može se uočiti da je za sigurnosne poruke odabran drugi *syslog* izvor, da bi se te poruke što lakše odvojile od poruka koje se generiraju na poslužiteljima. Također, transpozicija razine ozbiljnosti je ublažena u odnosu na poslužitelje, a isto tako bilježe se samo najvažniji događaji, za razliku od poslužitelja gdje se bilježe svi događaji. Na taj način štedi se diskovni prostor na *syslog* poslužitelju i smanjuje broj nepotrebnih poruka.

Syslog poslužitelji		
Primarni syslog poslužitelj	192.168.0.254	
Backup syslog poslužitelj	-	
Syslog transpozicije		
Application log	**izvor poruke (eng. facility)**	**razina ozbiljnosti (eng. *severity*)**
Error	(19) local 3	(3) error
Security log		
Failure	(10) security/auth	(3) error
System log		
Error	(1) user	(3) error
Warning	(1) user	(4) information

Tablica 5: Konfiguracija NTSyslog-a na klijentskim računalima

Tablica 6 prikazuje konfiguraciju implementiranog Kiwi Syslog Daemon poslužitelja. Pravila su podešena tako da se događaji koje generiraju različiti servisi izoliraju, prikazuju na različitim zaslonima (eng. *display*) i bilježe u posebne datoteke. Sve poruke klijentskih računala pohranjuju se u istu datoteku, isto kao i aplikacijske, sistemske i sigurnosne poruke koje generiraju poslužitelji. E-mail upozorenje šalje se ukoliko se detektira bilo koji događaj razina ozbiljnosti 0 ili 1. Sve datoteke arhiviraju se na dnevnoj ili tjednoj bazi. Ovakvu konfiguraciju vrlo je jednostavno podesiti korištenjem

raspoloživih pravila i filtara. Jedino ograničenje u *freeware* inačici jest nemogućnost definiranja filtriranja IP adresa, no pošto su klijentske syslog transpozicije definirane tako da se ne poklapaju s poslužiteljskim, pravilnim odabirom izvora poruka to ograničenje *freeware* inačice Kiwi Syslog Daemon poslužitelja može se zaobići (umjesto ranga IP adresa `192.168.0.100-192.168.0.200`, potrebno je uključiti izvore 1, 10 i 19).

Parametar	**Vrijednost**
Primanje poruka	syslog, 514-UDP
Upozorenja	diskovni prostor < 500MB, e-mail
E-mail	upozorenja, statistike
Pravila	
Default	svi događaji, display 0, datoteka SyslogCatchAll.txt
E-mail alert	događaji emergency (0), alert(1)
Active Directory log	izvor: (16) local 0, display 1, datoteka: SyslogAD.txt
File Replication log	izvor: (8) uucp, display 2, datoteka SyslogFR.txt
DNS log	izvor: (17) local 1, display 2, datoteka: SyslogDNS.txt
Servers: Security log	izvor: (4) security/auth, display 3 datoteka: SyslogSecServer.txt
Server: System log	izvor: (3) system, display 4 datoteka: SyslogSysServer.txt
Servers: App log	izvor: (18) local 2, display 5, datoteka: SyslogAppServer.txt
Clients log	IP:192.168.0.100-192.168.0.200, display 6, datoteka:SyslogCli.txt
Arhiviranje	
SyslogAD.txt	dnevno
SyslogFR.txt	tjedno
SyslogDNS.txt	dnevno
SyslogSecServer.txt	tjedno
SyslogSysServer.txt	dnevno
SyslogAppServer.txt	dnevno
SyslogCli.txt	tjedno

Tablica 6: Konfiguracija syslog poslužitelja

4. Zaključak

Korištenjem *freeware* komponenti moguće je vrlo lako uspostaviti *syslog* funkcionalnost u Windows okruženju. Opisane programske komponente (NTSyslog i Kiwi Syslog Daemon) vrlo su jednostavne za konfiguraciju, što se pogotovo odnosi na klijentski NTSyslog servis. Uvjetni nedostatak prilikom implementacije na klijentskoj strani (NTSyslog) jest nemogućnost podešavanja slanja *syslog* poruka na drugi UDP port, ili pak slanje TCP *syslog* poruka, čime bi se osigurala pouzdanost dostave. Za razliku od tih, manjih nedostataka na klijentskoj strani, na poslužiteljskoj strani (Kiwi Syslog Daemon) nisu uočeni nikakvi problemi niti nedostaci. Naprotiv, mogućnosti konfiguracije koje Kiwi Syslog Daemon pruža nadilaze zahtjeve koje je bilo potrebno ispuniti za opisani testni sustav. Implementirani *syslog* poslužitelj bi uz mala podešavanja konfiguracijskih parametara mogao vrlo lako poslužiti i kao *syslog* poslužitelj u heterogenim mrežnim okruženjima (Windows, Unix, Linux), a mogao bi bilježiti i događaje koje generiraju mrežni uređaji, bilo *syslog* porukama, bilo korištenjem SNMP-a.

5. Reference

[1] The BSD syslog protocol, IETF, August 2001, http://www.ietf.org/rfc/rfc3164.txt