KIWI SYSLOG SERVER

System zarządzania dziennikami zdarzeń dla systemu Windows

Wykonali:
Sławomir Adamus 143684
Sebastian Bugała 143693

Spis treści

1. Wprowadzenie

Program Kiwi Syslog Server stanowi narzędzie do zarządzania logami pochodzącymi z routerów, switchów, hostów, serwerów i innych urządzeń sieciowych posiadających syslog.

Jego podstawowe funkcjonalności to:

otrzymywanie komunikatów
wyświetlanie wiadomości
logowanie
archiwizowanie wiadomości
powiadamianie o zdarzeniach (np. e-mail)
przekazywanie komunikatów syslog (forwarding)

Przeglądanie logów odbywa się w czytelnej graficznej formie z kolorowaniem wg rodzaju, można również generować wykresy ze statystykami. Program może automatyczne dzielić logi wg priorytetu lub przedziału czasowego i przekazywać dalej wiadomości spełniające określone kryteria.

2. Schemat klasyfikacji komunikatów

Komunikaty demona syslog posiadają przypisane źródło komunikatu oraz priorytet:

Pochodzenie komunikatów (facility):

Nazwa	Opis
user	różnorodne programy zwykłych użytkowników
mail	komunikaty podsystemu poczty elektronicznej
daemon	różne demony systemowe
auth, authpriv	bezpieczeństwo (autoryzacja użytkowników)
syslog	syslog
lpr	drukarka
news	system grup dyskusyjnych (Usenet)
uucp	podsystem UUCP
cron	demony zegarowe: AT, CRON
ftp	serwer FTP
local0 - local7	uniwersalne źródła lokalne, możliwe do dowolnego zastosowania przez administratora

Priorytety (level):

Nazwa	Opis
emerg	system już nie nadaje się do użytku
alert	poważna awaria - należy podjąć natychmiastową akcję
crit	zdarzenie krytyczne
err	błędy
warning	ostrzeżenia
notice	ważne zdarzenia
info	informacje
debug	dodatkowe informacje - przydatne przy odpluskwianiu

3. Konfiguracja źródeł komunikatów

Źródłem komunikatów dla Kiwi mogą być wszystkie urządzenia używające do logowania zdarzeń demona syslog, czyli wszystkie hosty i serwery Linuksowe i Uniksowe, a ponadto switche zarządzalne, routery (sprzętowe i programowe), itp...

Poniżej przedstawione są mechanizmy konfiguracyjne umożliwiające wysyłanie logów do centralnego serwera logów.

3.1. Vyatta VC6.0

Zakładając, że mamy poprawnie skonfigurowane interfejsy sieciowe, uruchomienie wysyłania logów odbywa się wg następującego algorytmu:

1. Logujemy się do routera podając login i hasło

```
Welcome to Vyatta - VyattaKruchy tty1

VyattaKruchy login: kruchy
Password:
Last login: Fri Jul  9 11:27:29 GMT 2010 on tty1
Linux VyattaKruchy 2.6.31-1-586-vyatta #1 SMP Fri Mar 19 12:15:52 PDT 2010 i686
Welcome to Vyatta.
This system is open-source software. The exact distribution terms for
each module comprising the full system are described in the individual
files in /usr/share/doc/*/copyright.
kruchy@VyattaKruchy:~$ _
```

2. Wchodzimy do powłoki konfiguracyjnej poleceniem *configure*

```
kruchy@VyattaKruchy:~$ configure
[edit]
kruchy@VyattaKruchy# _
```

3. Włączamy logowanie do serwera poleceniem:

set system syslog host <a> facility <b> level <c>

gdzie w miejscu znacznika <a> wstawiamy adres serwera logów
<b> wybieramy pochodzenie komunikatu
<c> priorytet komunikatu

Przykładowo wysyłanie wszystkich komunikatów z priorytetem „info” do serwera pod adresem 192.168.5.27 definiujemy poleceniem:

```
kruchy@VyattaKruchy# set system syslog host 192.168.5.27 facility all level info

[edit]
kruchy@VyattaKruchy# _
```

4. Zatwierdzamy ustawienia poleceniem *commit*

```
kruchy@VyattaKruchy# commit
Reloading system log daemon....
[edit]
kruchy@VyattaKruchy#
```

5. Zapisujemy konfigurację routera poleceniem *save*

```
kruchy@VyattaKruchy# save
Saving configuration to '/opt/vyatta/etc/config/config.boot'...
Done
[edit]
kruchy@VyattaKruchy# _
```

6. Wychodzimy z powłoki konfiguracyjnej poleceniem *exit* i następnie wylogowujemy się poleceniem *logout*.

3.2. Syslog (Debian)

Umożliwia rejestrowanie zdarzeń zachodzących w systemie przy pomocy scentralizowanego mechanizmu. Pozwala na rejestrowanie informacji pochodzących z źródeł: zgłoszeń przekazywanych przez bibliotekę systemową oraz informacji pochodzących od jądra systemu. Program ten działający w tle dokonuje sortowania wpisów i decyduje co zrobić z informacją, stosując dwa kryteria przy podjęciu decyzji: priorytet i źródło komunikatu.

Konfiguracja programu odbywa się za pomocą pliku /etc/syslog.conf.
Schemat tworzenia nowego odbiorcy logów wygląda następująco:

```
facility.level @adres_ip
```

gdzie w miejsce *facility* wstawiamy odpowiednią nazwę źródła (wg rozdz. 2), a w miejsce *level* odpowiedni priorytet logów (wg rozdz. 2)

Aby zdefiniować wysyłanie wszystkich logów na serwer o adresie 192.168.5.27 wystarczy dodać do pliku następującą linię:

```
*.*  @192.168.5.27
```

Następnie należy wyedytować plik */etc/default/syslogd* i zmienić w nim linię *SYSLOGD=""* na następującą:

```
SYSLOGD="-r"
```

Na koniec należy przeładować demona syslog poleceniem konsolowym:

```
sudo /etc/init.d/syslogd restart
```

Sprawdzenia poprawności konfiguracji możemy dokonać wysyłając komunikat testowy poleceniem logger wg schematu:

```
logger -p facility.level "Treść wiadomości"
```

np.:

```
logger -p cron.info "wiadomosc testowa"
```

Przykłady bardziej rozbudowanych plików konfiguracyjnych z opisami można znaleźć np. na:
http://www.softpanorama.org/Logs/Syslog/syslog_configuration_examples.shtml

3.3. Syslog-ng (Ubuntu 10.04)

Syslog-ng (syslog - new generation) zajął miejsce syslogd. Jest to program o bogatych opcjach konfiguracji, zapewniający większą pewność działania, a co za tym idzie większe bezpieczeństwo logów.

Większe bezpieczeństwo zapewnia możliwość użycia protokołu TCP w komunikacji z tzw. loghostem, aby jednak korzystać z dobrodziejstw tego protokołu na obu maszynach musi być użyty demon "nowej generacji". Możliwa jest także komunikacja z klasycznym syslogiem, w tym wypadku musimy użyć protokołu UDP i portu 514 (wartość domyślna dla syslog-ng).

Jeśli w systemie nie ma zainstalowanego demona syslog-ng, należy go doinstalować poleceniem:

```
sudo apt-get install syslog-ng
```

Całą konfigurację umieszczamy w jednym pliku: /etc/syslog-ng/syslog-ng.conf.

- Źródła - definiujemy je następująco:
  ```
  source $nazwa { $źródło($opcje); };
  ```
  przykłady:
  ```
  source  src  { internal(); };
  source  udp  { udp(); };
  source  tcp  { tcp(ip(192.168.1.5) port(1999) max-
  connections(20)); };
  ```

  Pierwszy z przykładów jest źródłem komunikatów syslog-a.
  Drugi tworzy źródło komunikatów wysyłanych z dowolnej maszyny w sieci - nasłuch na domyślnym porcie (514 UDP).
  Trzeci oczekuje komunikatów od komputera 192.168.1.5 na porcie 1999 z ograniczeniem do 20 połączeń.

- Filtry:
  ```
  filter $nazwa { $rodzaj($wartość); };
  ```
  rodzaje:
  - facility - pochodzenie zdarzenia: cron, daemon, mail, ... - szczegóły w dodatku
  - level - priorytet: emerg, alert, crit, ... - szczegóły w dodatku
  - host - filtrowane po nazwie hosta z użyciem wyrażeń regularnych
  - program - filtrowane po nazwie programu z użyciem wyrażeń regularnych

  przykłady:
  ```
  filter f_emergency { level(emerg); };
  filter f_daemon    { facility(daemon); };
  ```

  Pierwszy przykładowy filtr przepuszcza jedynie powiadomienia o najpoważniejszych błędach.
  Drugi zdarzenia pochodzące od demonów.

- Cele - ogólna definicja:
  ```
  destination $nazwa { $cel($miejsce); };
  ```
  najpopularniejsze cele:
  - file - plik tekstowy / urządzenie znakowe (/dev/)
  - usertty - ekran terminala wskazanego użytkownika
  - tcp - komunikaty do loghosta (TCP)
  - udp - komunikaty do loghosta (UDP)

  przykłady:
  ```
  destination  kernel       { file("/var/log/kernel"); };
  destination  root         { usertty("root"); };
  destination  loghost      { udp("10.0.0.1"); };
  ```

  W pierwszym przykładnie komunikaty są kierowane do pliku /var/log/kernel.
  Drugi cel spowoduje wyświetlanie komunikatu na ekranie terminala użytkownika root.
  Trzeci obiekt pozwoli na wysyłanie komunikatów do loghosta o adresie IP 10.0.0.1 (uwaga na zgodność protokołów TCP/UDP u nadawcy i odbiorcy).

- Regułki - budujemy je na samym końcu, kiedy mamy już zdefiniowane źródła, filtry i cele:
  ```
  log { source($źródło); destination($cel); };
  ```

```
log { source($źródło); filter($filtr1); filter($filtr2);
destination($cel); };
```

np.:

```
log { source(src);  destination(console_all); };
log { source(src);  filter(f_emergency); destination(loghost);
};
```

Przykładowy plik konfiguracyjny wysyłający na host 192.168.5.27 wszystkie wiadomości z sysloga:

```
source s_all {
     internal();
};
destination kiwisyslog {
     udp("192.168.5.27");
};
log {
        source(s_all);
        destination(kiwisyslog);
};
```

Aby zmiany weszły w życie oraz utworzone zostały nowe pliki dzienników, należy ponownie uruchomić demona:

```
     service syslog-ng reload
```

Sprawdzenia poprawności konfiguracji możemy dokonać wysyłając komunikat testowy poleceniem logger wg schematu:

```
     logger -p facility.level "Treść wiadomości"
```

np.:

```
     logger -p cron.info "wiadomosc testowa"
```

3.4. Urządzenia CISCO

Logujemy się do urządzenia i przechodzimy do trybu konfiguracji (znak zachęty: `(config)#)`, a następnie:

1. Podwyższamy poziom logowania do info:
   `logging trap informational`

2. Dodajemy znacznik czasowy do komunikatów
   `logging timestamp`

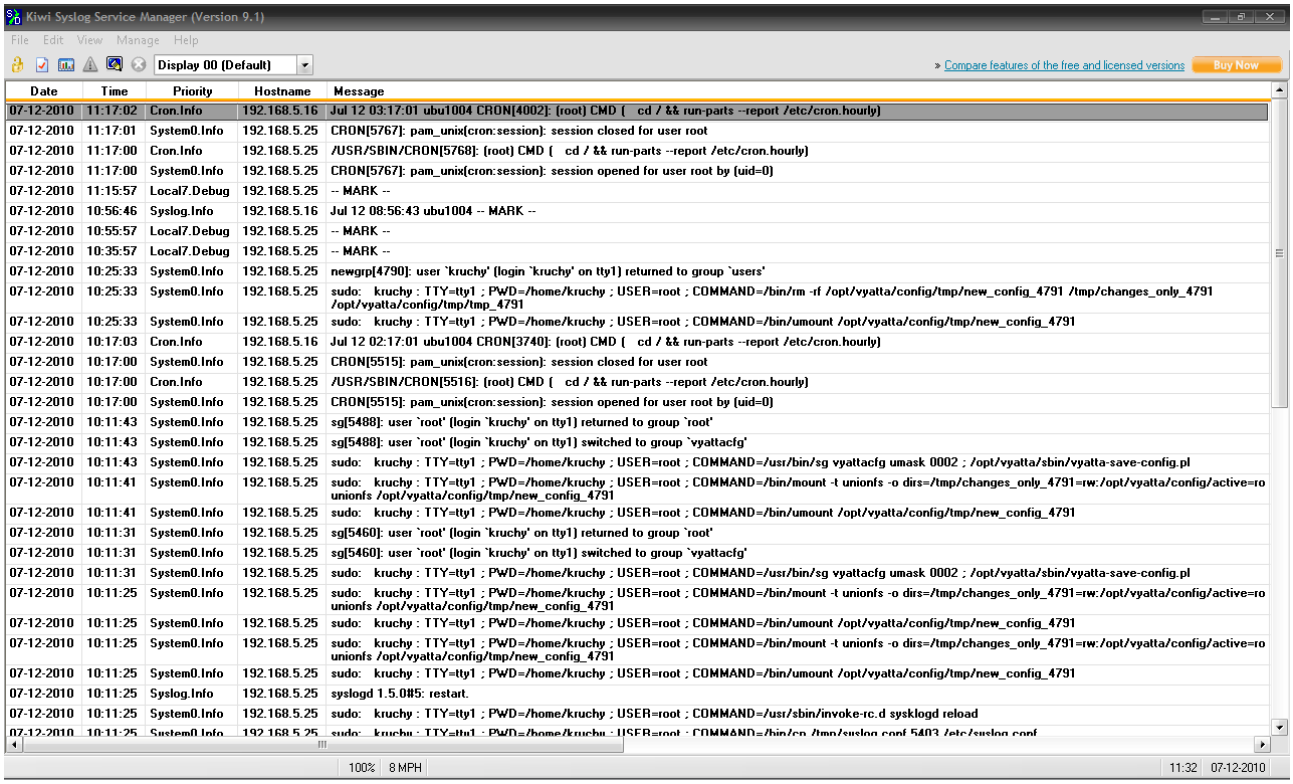
3. Ustawiamy adres serwera syslog
   `logging host 192.168.5.27`

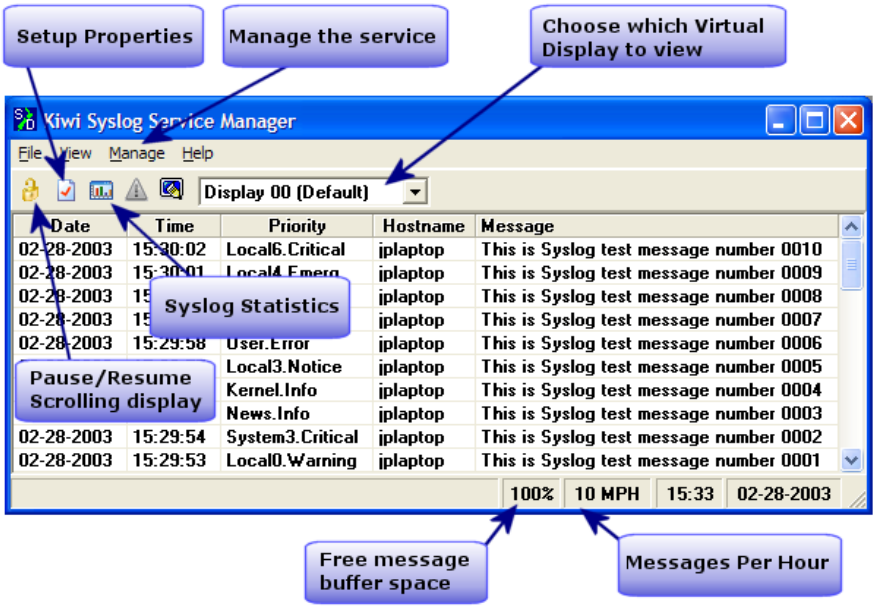
4. Uruchamiamy wysyłanie logów
   `logging enable`

5. Zapisujemy konfigurację urządzenia
   `copy running-config startup-config`

4. Podstawowa obsługa Kiwi Syslog Server

Po uruchomieniu programu wita nas główne okno programu Kiwi Syslog:

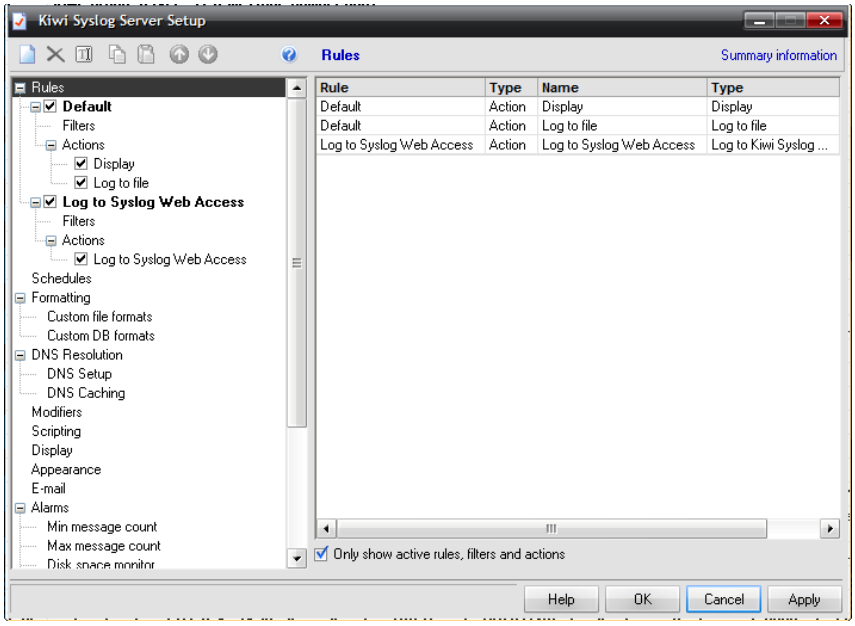




4.1. Menu FILE

- Setup

  Otwiera okno konfiguracji programu



- Send Test message to localhost

  Opcja ta umozliwia wysyłanie testowej wiadomości sysloga protokołem UDP na localhost (127.0.0.1) w celu sprawdzenia poprawności działania programu. Wiadomość wysyłana jest na ten sam port, na którym nasłuchuje syslog (domyślnie 514). Aby przeprowadzić testy połączenia TCP należy użyć narzędzia SyslogGen dostępnego na stronie www.kiwisyslog.com.

  Przykładowa wiadomość testowa wygląda następująco:

  Kiwi Syslog Server – Test message number 0001

  Cyfra na końcu komunikatu jest inkrementowana przy każdorazowym wywołaniu testu.

- Purge

  Umożliwia wyczyszczenie zawartości poszczególnych plików logów:

  - Purge e-mail log file
  - Purge error log file
  - Purge message queue
  - Purge mail queue
  - Purge failed MIB lookup file
  - Purge database cache

- Import setting from INI file

  Umożliwia zaimportowanie ustawień programu z pliku *.ini

- Export setting to INI file

  Eksportuje ustawienia do pliku *.ini

- Create Tech-Support File (ZIP)

  Opcja tworzy archiwum ZIP z plikami konfiguracyjnymi i opcjonalnie logami, które można wysłać do producenta programu – SolarWinds – w celach diagnostycznych

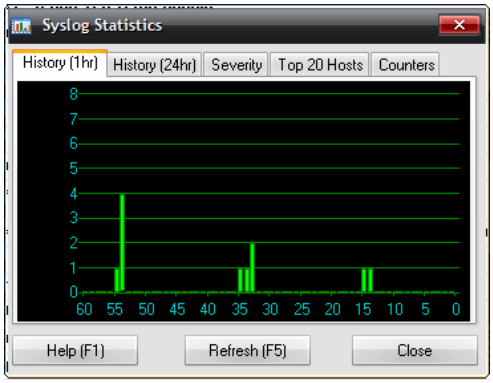
- Exit

Wyjście z programu

4.2. Menu VIEW

- View Syslog Statistics

  Wyświetla okno ze statystykami i wykresami ilości otrzymywanych komunikatów/



- View e-mail log file

  Wyświetla liste wysłanych wiadomości e-mail (InstallPath/SendMailLog.txt)

- View error log file

  Wyświetla zawartość pliku zawierającego błedy logowania (InstallPath/Errorlog.txt)

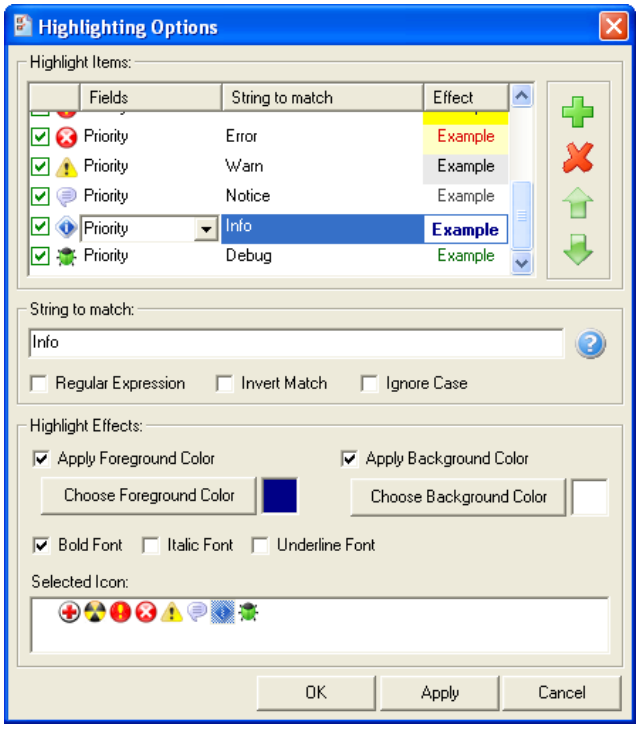
- Adjust width to fit screen

  Dopasowuje szerokość głównego okna do szerokości ekranu

- Highlight options

  Opcja dostępna tylko w płatnej wersji Kiwi Syslog.

Umożliwia kolorowanie komunikatów w zależności od źródła komunikatu, priorytetu czy na podstawie porównywania treści komunikatów do wyrażeń regularnych.



Dostępne efekty podkreślania komunikatów:

- Apply foreground color – zmiana koloru czcionki
- Apply background color – zmiana koloru tła komunikatu
- Bold Font – pogrubienie czcionki
- Italic Font – pochylenie czcionki
- Underline font – podkreślenie czcionki
- Selected icon – przypisanie ikony do odfiltrowanego komunikatu

- Clear display

  Usuwa wszystkie wiadomości z aktualnego ekranu

- Choose font

  Umożliwia zmianę czcionki komunikatów

- Show/Hide Columns

  Umożliwia dostosowanie wyświetlanych wiadomości poprzez pokazywanie/ukrywanie poszczególnych kolumn

4.3. Menu MANAGE

- Start the Syslogd service

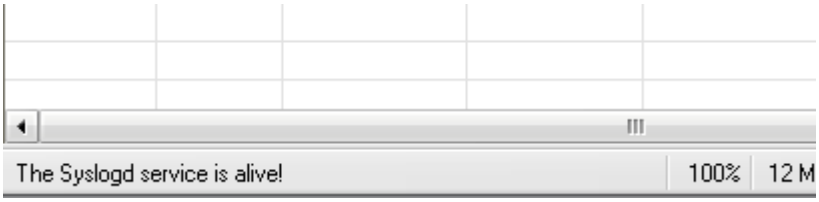
  Uruchamia usługę systemowa syslogd – kiedy usługa jest uruchomiona działa odbieranie, logowanie i przekazywanie komunikatów.

- Stop the Syslogd service

  Zatrzymuje działanie usługi Syslogd

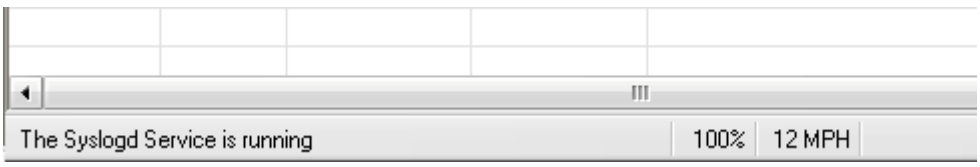
- Ping the Syslogd service

  Sprawdza działanie usługi Syslogd – wynik badania jest wyświetlany w lewym dolnym rogu okna.



- Show the Syslogd Service state

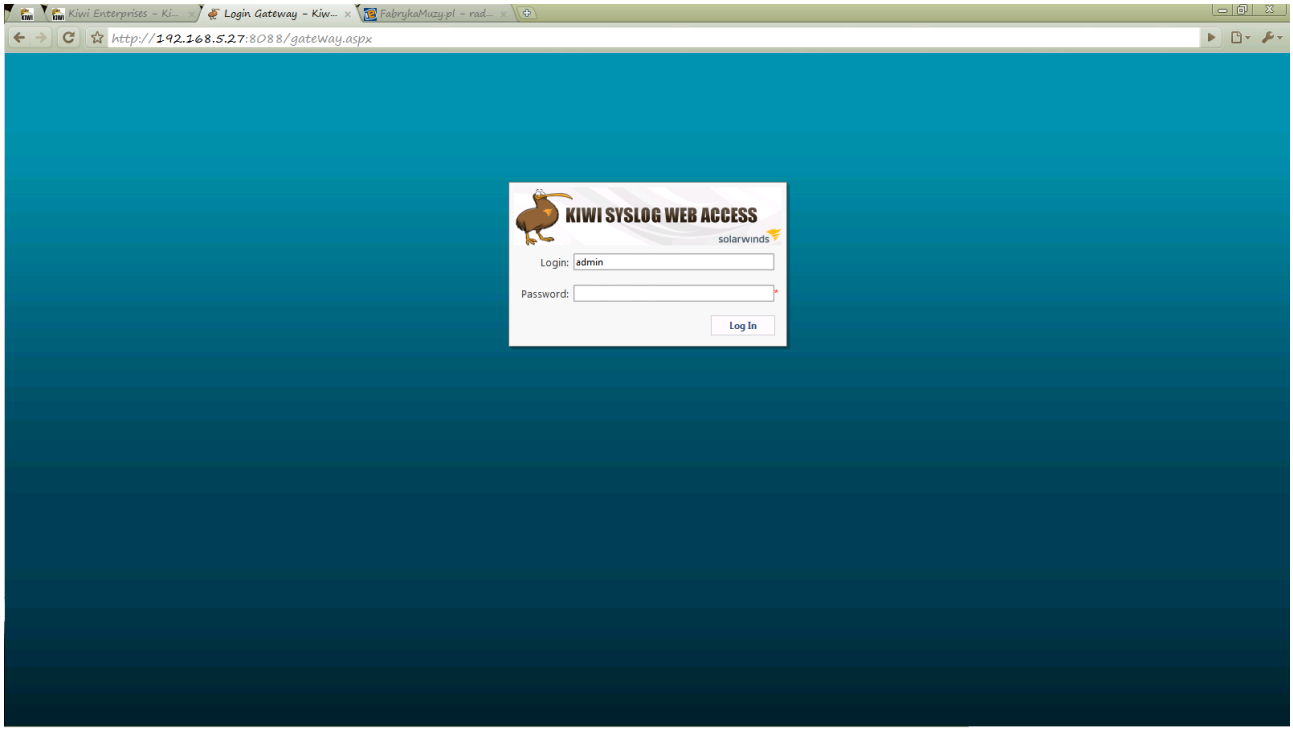
  Sprawdza stan działania usługi. Dostępne stany: Uninstalled, Running, Stopped i Not responding



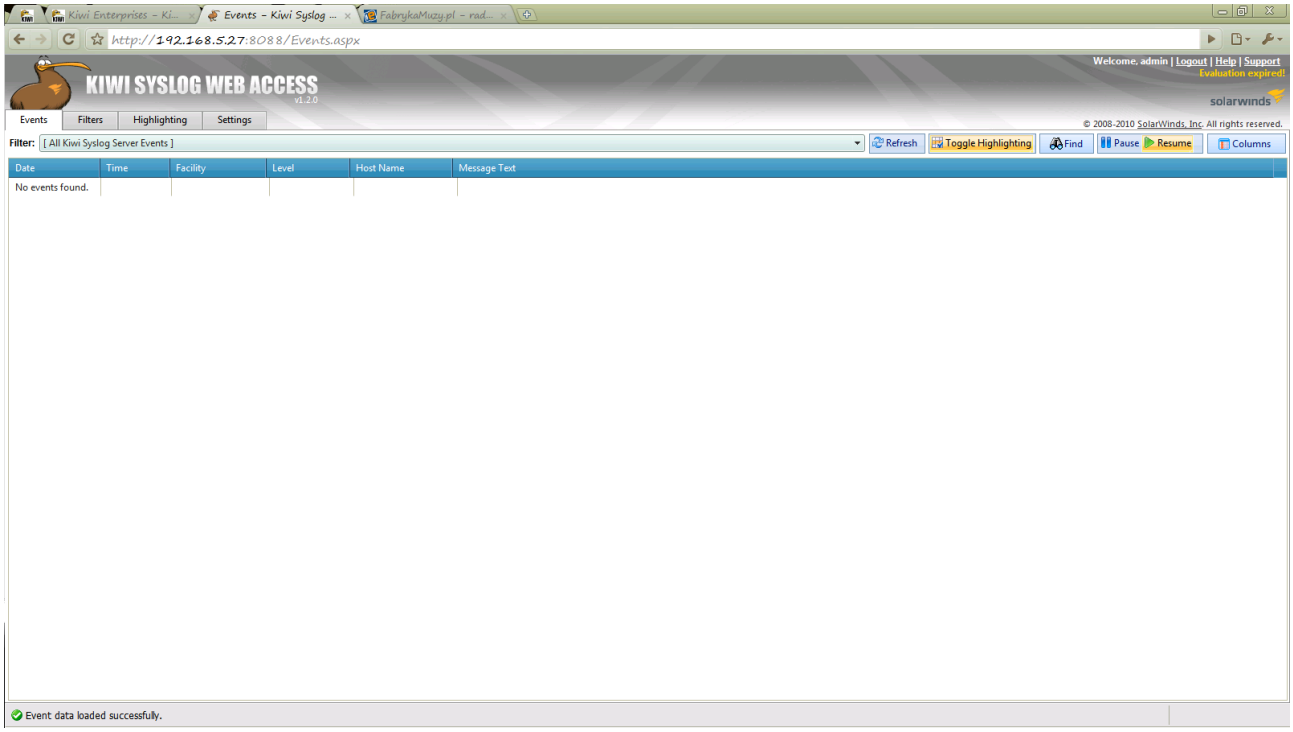
4.4. Dostęp przez WWW

Kiwi umożliwia dostęp do interfejsu administracyjnego poprzez przeglądarkę www.

Aby dostać się w ten sposób do interfejsu należy wejść na stronę http://adres_serwera:8088/, np.: http://192.168.5.27:8088/



Po zalogowaniu dostajemy dostęp do dziennika zdarzeń:



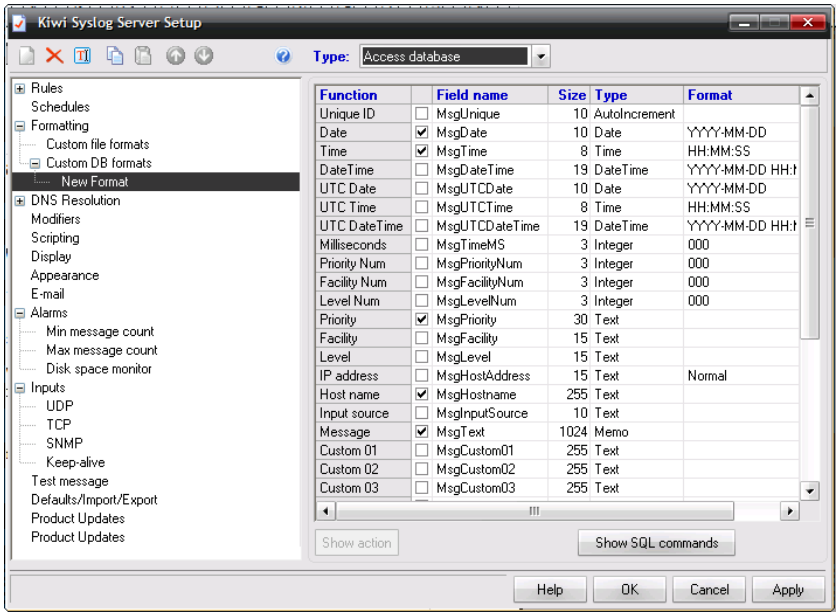
5. Zaawansowana konfiguracja

Konfigurację zaawansowaną przeprowadza się w oknie File->Setup (Ctrl + P).

5.1. Zapis komunikatów do bazy danych (MS Access, Oracle, MySQL, SQL)

Zapis komunikatów do bazy danych możliwy jest poprzez stworzenie własnego formatu bazy danych. W tym celu:

1. Wchodzimy do okna konfiguracji (ctrl + P)
2. W grupie „Formatting" klikamy prawym przyciskiem myszy na „Custom DB Formats" i wybieramy „Add new custom DB format"

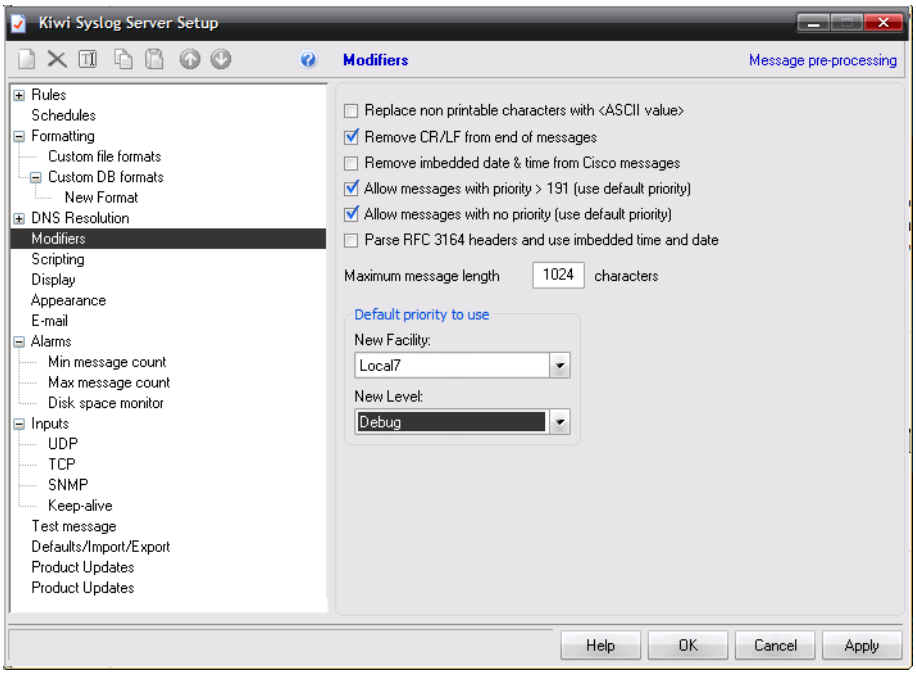


3. W górnym polu „Type" wybieramy rodzaj naszej bazy danych:
   - MS Access
   - SQL
   - MySQL
   - Oracle
   - inne bazy danych
4. W dolnej części okna można dokonać modyfikacji struktury tabeli w bazie danych (nazwy kolumn, typ danych, rozmiar danych i format zapisywanych danych).
5. Podgląd zapytań do bazy danych możliwy jest pod przyciskiem „Show SQL commands"
6. Zapytania zatwierdzamy przyciskiem OK.

5.2. Modyfikatory treści

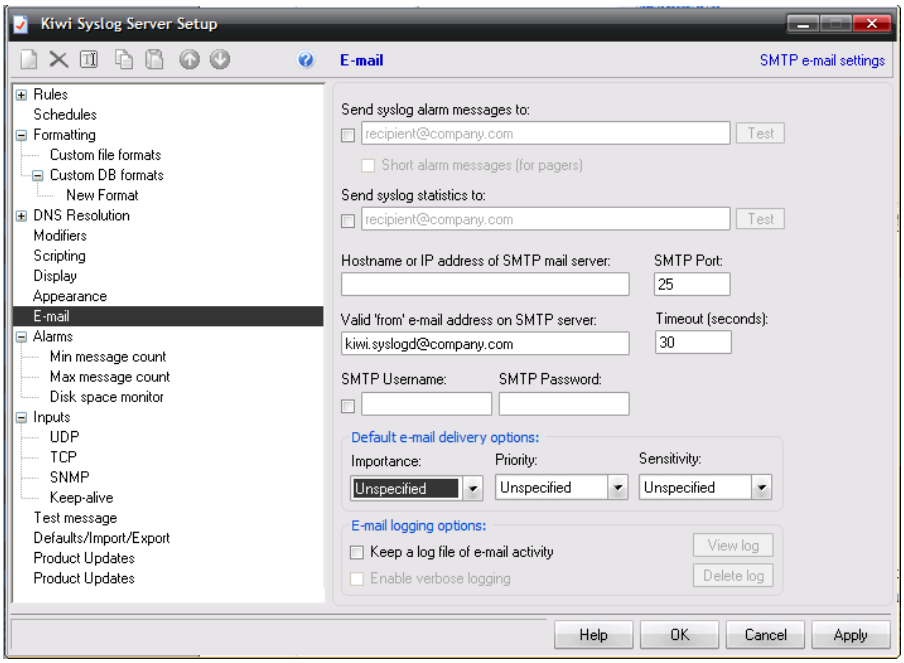
Na przychodzących komunikatach mogą zostać przeprowadzone modyfikacje w celu dostosowania ich do naszych wymagań. Można w ten sposób zredukować długość komunikatu, zmienić priorytet komunikatu, zamienić znaki niedrukowane na kody ASCII czy np. usunąć znacznik czasowy z komunikatów generowanych przez urządzenia CISCO.

Wybór modyfikatorów jest możliwy w oknie File → Setup → Modifiers



5.3. Konfiguracja e-mail

Kiwi posiada możliwość wysyłania logów na skrzynki pocztowe z wykorzystaniem protokołu SMTP. Konfigurację tej funkcjonalności można popełnić w oknie File → Setup → E-mail.



Pierwsza opcja umożliwia wysyłanie wszystkich komunikatów sysloga na zdefiniowaną skrzynkę pocztową.

Opcja druga wysyła na skrzynkę statystyki sysloga.

Niżej należy wypełnić pola konfiguracyjne serwera pocztowego (adres IP, port, login i hasło, wartość pola „from” w nagłówku smtp)

5.4. Alarmy

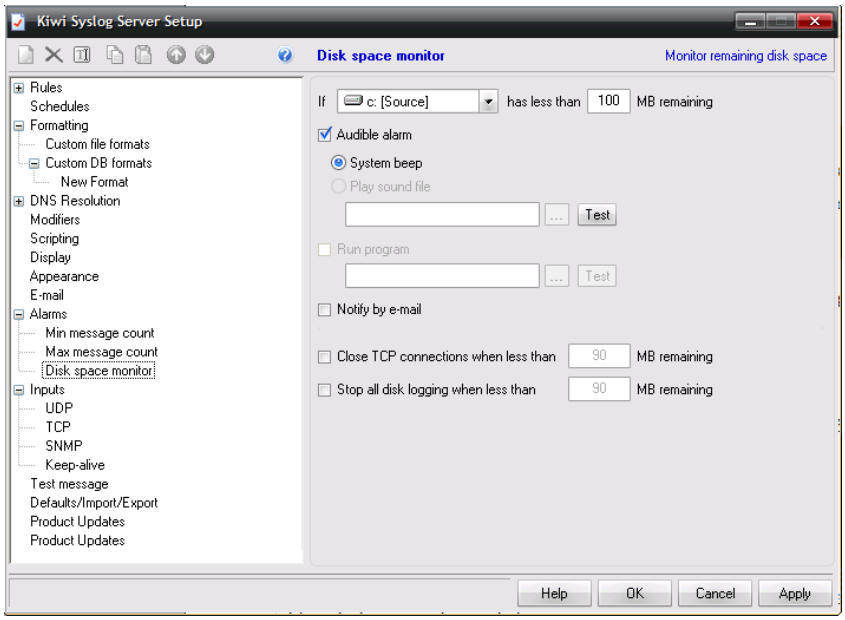
Kiwi umożliwia wyzwalanie alarmów przy 3 rodzajach zdarzeń:

- za mało komunikatów syslog (możliwe np. fizyczne uszkodzenie medium transmisyjnego)
- za dużo komunikatów (standardowo powyżej 3000 kom. na godzinę)
- kończące się miejsce na dysku, na którym zapisywane są logi

Do każdego rodzaju alarmu możliwe jest podjęcie 3 działań:

- Alarm dźwiękowy (buzzer lub dźwięk z zewnętrznego pliku)
- Uruchomienie programu zewnętrznego
- powiadomienie e-mailowe

Dodatkowo przy kończącym się miejscu na dysku można rozłączyć wszystkie przychodzące połączenia TCP oraz zatrzymać logowanie komunikatów do pliku.



5.5. Konfiguracja protokołów sieciowych

W oknie File → Setup → Input można przeprowadzić modyfikację konfigurajci protokołów z których zbierane są komunikaty.

W standardowej konfiguracji włączony jest wyłącznie nasłuch protokołu UDP na porcie 514.

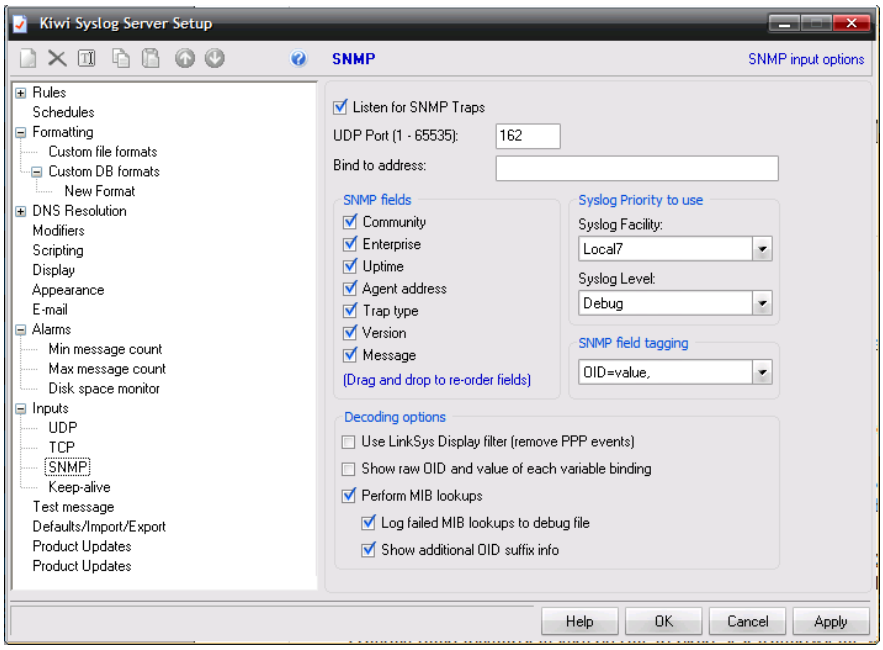
Poza tą opcją można uruchomić nasłuch dla protokołu TCP – wykorzystywany jest on m.in. przez niektóre firewalle do wysyłania komunikatów (np.. Cisco PIX wysyła komunikaty na TCP 1468).

Kolejną opcją jest umożliwienie nasłuchu komunikatów SNMP – Kiwi obsługuje komunikaty w standardzie 1 i 2c SNMP. Standardowy nasłuch dla komunikatów jest prowadzony

na porcie 162 UDP.

Ostatnią funkcjonalnością jaką oferuje to okno, jest ustanowienie wysyłania komunikatów keep-alive. Są to komunikaty sysloga wysyłane do siebie samego (na localhost). Mechanizm ten umożliwia wykrocie awarii serwera syslog czy okresowe uruchamianie skryptów. Można również komunikaty keep-alive przekazywać do innego serwera i w przypadku braku komunikatów przez okreslony czas podnieść alarm o uszkodzeniu serwera z Kiwi.

Okno do konfiguracji pułapek SNMP:



5.6. Modyfikacja wyglądu

Istnieje możliwość modyfikacji wyglądu w zakresie zmiany skórek interfejsu oraz dodania tekstur pod menu. Modyfikacje można przeprowadzić w oknie File → Setup → Appearance