Report Manager 1.6.0

Dokumentacja techniczna

Katarzyna Władyszewska, Hadden Sp.J.

Report Manager 1.6.0: Dokumentacja techniczna

by Katarzyna Władyszewska

Data wydania Kwiecień 2010

Spis treści

1. Konwencje typograficzne 1
2. Informacje ogólne o systemie David 2
    2.1. Charakterystyka ogólna 2
    2.2. Architektura systemu David 3
3. Terminologia 6
    3.1. Autoryzacja dokonywana przez moduły systemu David 6
    3.2. Terminy używane w systemie David i jego dokumentacji 6
4. Instalacja 8
    4.1. Główny plik konfiguracyjny systemu David 8
    4.2. Dedykowane konto dla obsługi systemu David 8
    4.3. Układ katalogów systemu David 9
    4.4. Konfiguracja demon-a syslogd 9
5. Wymagania dla Report Manager-a 10
6. Instalacja 11
    6.1. Instalacja z pakietu RPM 11
    6.2. Instalacja za pomocą skryptu 11
7. Informacje ogólne 12
    7.1. Funkcjonalność 12
    7.2. Opis działania 12
    7.3. Tematy pokrewne 12
8. Zarządca Raportów (dreportd) 13
    8.1. Opis ogólny 13
    8.2. Składnia 13
    8.3. Znaczenie opcji w programie dreportd 13
    8.4. Opis działania 14
        8.4.1. Przetwarzanie filtrów dotyczących wpisów SNMP Trap 14
        8.4.2. Przetwarzanie filtrów dotyczących wpisów o prowadzonych sprawach (cases) 15
        8.4.3. Przetwarzanie filtrów dotyczących wpisów o monitorowanych obiektach 15
    8.5. Tematy pokrewne 15
9. Przyciski najczęściej występujące w aplikacjach WWW 16
    9.1. Znaczenie przycisków 16
10. Konfigurator Zarządcy Raportów (Report Manager Configurator) 18
    10.1. Opis ogólny 18
    10.2. Opis działania 18
        10.2.1. Widok domyślny aplikacji 18
        10.2.2. Edycja filtrów dotyczących wpisów SNMP Trap 19
        10.2.3. Edycja filtrów dotyczących wpisów o prowadzonych sprawach (cases) 21
        10.2.4. Edycja filtrów dotyczących wpisów o monitorowanych obiektach 23
    10.3. Tematy pokrewne 24
11. Przeglądarka Raportów (Report Browser) 25

11.1. Opis ogólny 25
11.2. Opis działania 25
11.2.1. Widok domyślny aplikacji 25
11.2.2. Widok działania pojedynczego filtra 26
11.2.3. Widok działania pojedynczego filtra pokazujący podzakresy 27
11.3. Tematy pokrewne 28

Spis tabel

1.1. Konwencje typograficzne użyte w dokumencie 1
2.1. Produkty wchodzące w skład systemu David 3
8.1. Znaczenie opcji w programie dreportd 13
9.1. Przyciski najczęściej występujące w aplikacjach WWW 16
11.1. Przeglądarka Raportów - obiekty paska narzędziowego 26

Rozdział 1. Konwencje typograficzne

Następujące konwencje typograficzne są użyte w niniejszym dokumencie:

Tabela 1.1. Konwencje typograficzne użyte w dokumencie

Czcionka	Znaczenie	Przykład
Kursywa	Nazwy zmiennych środowiskowych	Nazwa pliku przechowywana jest w zmiennej środowiskowej *$DAVIDPRIVDIR*...
Kursywa	Opcje składni.	[*-l,--log-facility log_facility*]
Pogrubiona	Nazwy programów, aplikacji i produktów.	Program **damcsud** jest częścią **Operation Manager-a**.
`Rozstrzelona`	Nazwy opcji i menu	W menu `View` znajduje się także opcja `Show tool bar`.
`Rozstrzelona`	Nazwy plików i katalogów.	... czyta swój plik konfiguracyjny `.damadbudrc`.
`Rozstrzelona`	Nazwy okienek i pól w okienkach dialogowych.	W okienku `A sessions property` w polu `Sticking string` podaje się tekst...
`Rozstrzelona`	Nazwy przycisków.	Przez naciśnięcie przycisku `Tab` z klawiatury możesz uzyskać focus.
`Rozstrzelona pogrubiona`	Wzory matematyczne.	**`exp( -x ), gdy a = 0 1 / pow( a , a ) * pow( x , a ) * exp( -x + a ), gdy a > 0`**.
`Rozstrzelona pogrubiona`	Terminy użyte w terminologii systemu David.	**`SNMP Data`** - rodzaj danych występujących...
`Rozstrzelona pogrubiona`	Zawartość plików konfiguracyjnych.	**`action`** **`{`** `...` **`}`**

Rozdział 2. Informacje ogólne o systemie David

2.1. Charakterystyka ogólna

System David to system zarządzania siecią komputerową. Jest on pakietem programów (modułów) pozwalającym zdalnie, tzn. poprzez rozległą sieć komputerową (np.: Internet), monitorować i zarządzać, w czasie rzeczywistym, urządzeniami pracującymi w sieciach komputerowych. Jedynym warunkiem, jakie muszą spełniać urządzenia jest, aby pracował na nich agent SNMP (Simple Network Management Protocol). Wobec faktu, że SNMP jest najbardziej rozpowszechnionym protokołem zarządzania na świecie, wymaganie to nie jest szczególnie trudne do spełnienia. Wiele urządzeń posiada oprogramowanie, które pozwala się z nimi komunikować poprzez protokół SNMP. Do urządzeń tych należą m.in.:

- routery IP,
- switche ATM-owe,
- zarządzalne switche ethernetowe,
- UPS-y wyposażone w adaptery SNMP,
- modemy telewizyjnych sieci kablowych pozwalające pracować urządzeniom IP w sieciach telewizji kablowej,
- stacje komputerowe.

Jedną z głównych cech **systemu David** jest fakt, że jest on złożony z wysoce konfigurowalnych i dalece niezależnych od siebie modułów. Staranność o utrzymanie takiego sposobu projektowania systemu jest widoczna od początku jego powstania. W konsekwencji, z tych samych modułów, można zbudować istotnie różniące się w działaniu konfiguracje **systemu David**. Jako jego główne cechy można więc wymienić:

- ogólność w podejściu do sterowania przepływem informacji wynikająca z wysokiej niezależności od siebie modułów systemu,
- wysoka konfigurowalność wszystkich modułów systemu pozwalająca maksymalnie zbliżyć się do oczekiwanego rezultatu podczas konfigurowania pracy systemu,
- skalowalność systemu, tzn. system można łatwo rozbudować dodając kolejne moduły, nawet nie wchodzące w skład **systemu David**, a także bez trudu można poszerzać listę monitorowanych urządzeń,
- wykorzystanie skryptów shell'owych w strumieniu przepływu informacji pozwala w łatwy sposób

formatować i wpływać na przetwarzane informacje,

- wszystkie pliki konfiguracyjne **systemu David**, a także pliki z danymi wejściowymi jak i wyjściowymi, pliki z istotnymi dla systemu komunikatami (log files), są plikami tekstowymi,
- komunikacja z monitorowanymi urządzeniami poprzez protokoły SNMPv1, SNMP 2C i SNMPv3.

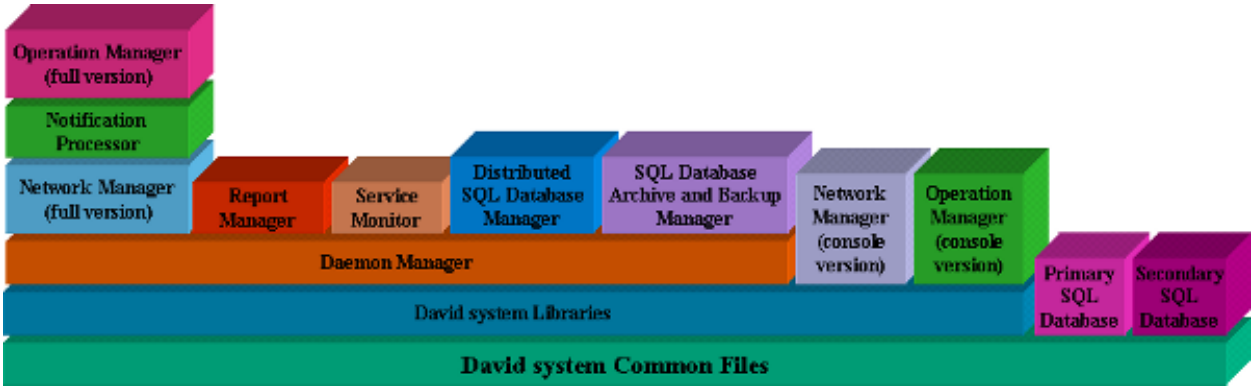
2.2. Architektura systemu David

Tabela 2.1. Produkty wchodzące w skład systemu David

Nazwa produktu	Opis
David system Common Files	Produkt podczas instalacji przygotowuje układ katalogów dla innych produktów **systemu David**. Zawiera też kilka podstawowych plików dla wszystkich innych produktów. Jest to podstawowy produkt **systemu David** wymagany przez resztę jego produktów.
Primary SQL Database	Produkt instaluje podstawową SQL-ową bazę danych **systemu David**. Każda instalacja **systemu David** musi mieć tylko jedną podstawową bazę danych.
Secondary SQL Database	Produkt instaluje dodatkową SQL-ową bazę danych **systemu David**. Może istnieć wiele dodatkowych baz danych w jednej instalacji **systemu David**. Pozwala to rozpraszać bazę danych **systemu David** na wiele serwerów.
David system Libraries	Dostarcza biblioteki **systemu David** potrzebne aplikacjom systemu. Produkt ten jest wymagany przez wiele innych produktów **systemu David**.
Daemon Manager	Zajmuje się uruchamianiem i zatrzymywaniem demonów **systemu David** oraz monitorowaniem ich pracy.
Network Manager (full version)	Produkt poprzez wykorzystanie protokołu SNMP umożliwia wizualizację topologii monitorowanych sieci i automatyczne odkrywanie urządzeń w zarządzanych sieciach. Wizualizacji podlega także stan monitorowanych obiektów. Produkt zajmuje się także zbieraniem danych dotyczących pracy monitorownych urządzeń, wykorzystując do tego celu protokół SNMP oraz pozwala administrować kontami użytkowników.
Network Manager (console version)	Produkt poprzez graficzną aplikację umożliwia wizualizację topologii monitorowanych sieci oraz stanu monitorowanych obiektów. Pozwala także sterować pracą demonów monitorujących oraz kolekcjonujących dane. Obecnie większość funkcji tej aplikacji jest dostępna także poprzez aplikacje webowe.
Notification Processor	Zajmuje się głównie obsługą komunikatów typu SNMP Trap nadchodzących do stacji zarządzających od monitorowanych urządzeń. Otrzymane komunikaty mogą podlegać dowolnemu formatowaniu do

Nazwa produktu	Opis
	postaci czytelnej dla człowieka, a następnie mogą być rejestrowane. Przetworzone w ten sposób komunikaty mogą być również przekazywane do dalszego przetwarzania.
Operation Manager (full version)	Na podstawie przekazywanych mu danych może on uruchamiać wyspecyfikowane akcje. Skomplikowany często sposób oceny sytuacji, dokonywany m.in. na podstawie otrzymywanych sygnałów od innych produktów **systemu David** wraz z ich korelacją, ma na celu, w sposób nieco bardziej inteligentny niż tylko prosta reakcja na nie, generowanie informacji dla operatora w odpowiedzi na zaistniałe zdarzenia. Graficzna aplikacja wyświetla powiadomienia o zdarzeniach oraz umożliwia odtwarzanie plików dzwiękowych oraz odczytywanie komunikatów przez zewnętrzny syntezator mowy.
Operation Manager (console version)	Produkt zawiera graficzną aplikację wyświetlającą powiadomienia o zdarzeniach oraz umożliwiającą odtwarzanie plików dzwiękowych oraz odczytywanie komunikatów przez zewnętrzny syntezator mowy.
Report Manager	Zajmuje się przetwarzaniem zarejestrowanych komunikatów SNMP Trap, wpisów o toczących się sprawach oraz wpisów dotyczących zmiany stanów monitorowanych obiektów (obiektów pingowanych, interfejsów sieciowych i sąsiadów BGP) i generuje na tej podstawie dane do raportów. Wizualizacja wygenerowanych raportów dokonywana jest przez aplikację webową.
Service Monitor	Monitoruje wskazane serwisy sieciowe na poziomie warstwy aplikacyjnej. W tym celu monitoruje wskazane porty TCP wyspecyfikowanych hostów. Sprawdza zarówno dostępność portów jak i poprawność reakcji dla kilku wybranych protokołów sieciowych (HTTP, SMTP, FTP). Może także weryfikować poprawność pracy serwisów poprzez weryfikację danych od nich uzyskanych. Wyniki jego pracy w postaci raportów i wykresów prezentuje aplikacja webowa.
SQL Database Archive and Backup Manager	Zajmuje się archiwizowaniem danych przechowywanych w SQL-owej Bazie Danych, z których korzystają aplikacje **systemu David**.
Distributed SQL Database Manager	Pozwala podzielić bazę danych **systemu David** na jedną bazę podstawową oraz wiele baz dodatkowych. Pozwala to zwiększyć szybkość pracy systemu poprzez rozproszenie obciążenia na wiele serwerów. Proces migracji odbywa się podczas normalnej pracy systemu a podział bazy danych może być modyfikowany wielokrotnie.

Zależności pomiędzy poszczególnymi produktami **systemu David** przedstawia poniższy schemat.



Funkcjonalność **systemu David** może być bardzo szeroka i w ogromnym stopniu zależy od konkretnej konfiguracji. Najważniejsze funkcje jakie system może dostarczać to:

- odkrywanie i wizualizacja topologii monitorowanych sieci wraz z wizualizacją stanów poszczególnych węzłów sieci;
- formatowanie i rejestrowanie komunikatów typu SNMP-Trap nadsyłanych przez monitorujące urządzenia;
- automatyczne reagowanie na wybrane komunikaty typu SNMP-Trap nadsyłane przez monitorowane urządzenia;
- możliwość identyfikacji operatora odbierającego od systemu zgłoszenie o problemie (awarii);
- kolekcjonowanie danych dotyczących pracy monitorowanych urządzeń;
- automatyczne reagowanie na wykryte podczas kolekcjonowania danych nieprawidłowe wartości danych;
- prowadzenie ewidencji aktualnych spraw prowadzonych przez system powstałych jako reakcja na zdarzenia mające miejsce w zarządzanej sieci i wykrytych przez system;
- monitorowanie serwisów sieciowych warstwy aplikacji.

Rozdział 3. Terminologia

3.1. Autoryzacja dokonywana przez moduły systemu David

Moduły pracujące w ramach systemu David, które potrzebują dokonywać autoryzacji nadawców wiadomości (np. **damsnmpdaud**, **dnmmsd**, **dgnsd**), korzystają z biblioteki, która sprawdza, czy adres IP nadawcy pasuje do jakiegokolwiek wpisu w pliku `.known.host`. Biblioteka spodziewa się, że plik ten znajduje się w podkatalogu `.sec` katalogu, którego nazwa wskazywana jest przez zmienną *confdir* w pliku `/etc/system-david.conf`.

Wpisy w pliku `.known.host` mają postać wyrażeń regularnych specyfikujących adresy IP, które mają być akceptowane.

3.2. Terminy używane w systemie David i jego dokumentacji

Poniżej znajduje się wyjaśnienie części terminów, które są używane przez system David oraz w dokumentach opisujących jego pracę:

- **wiadomości (informacje)** - najczęściej są to dane otrzymywane przez interfejsy **Operation Manager-a**, jego analizatory danych oraz **Jednostkę Tworzącą Bazę Danych Aktywnych Spraw** należącą do tego produktu;
- **komunikaty** - termin ten występuje głównie w produktach: **Notification Processor**, **Operation Manager** i **Report Manager**; najczęściej są to dane, których źródłem są agenci SNMP pracujący na monitorowanych urządzeniach sieciowych;
- **zdarzenia (events)** - termin ten występuje najczęściej w produktach takich jak: **Operation Manager** i **Report Manager**; określa byt, którego źródłem jest pojedyncza dana typu SNMP Trap lub SNMP Data; **zdarzenie** zawsze wchodzi w skład **sprawy**;
- **sprawy (cases)** - termin ten występuje najczęściej w produktach takich jak: **Operation Manager** i **Report Manager**; określa zbiór zdarzeń skojarzonych ze sobą; w skład sprawy musi wchodzić przynajmniej jedno **zdarzenie**;
- **SNMP Trap** - rodzaj danych występujących w produkcie **Operation Manager**, których źródłem są komunikaty otrzymywane od agentów SNMP; komunikaty te nie są odpowiedzią na prośby wysyłane przez stację zarządzającą, lecz są samoistnie wysyłane przez agentów zarządzających urządzeniami sieciowymi i przetwarzane przez produkt **Notification Processor**;

- **`SNMP Data`** - rodzaj danych występujących w produkcie **Operation Manager**, których źródłem są odpowiedzi otrzymywane od agentów SNMP na prośby, wysyłane do nich przez stację zarządzającą za pomocą produktu **Network Manager**.

Rozdział 4. Instalacja

4.1. Główny plik konfiguracyjny systemu David

Podstawowy plik konfiguracyjny systemu David to `/etc/david-system.conf`. Zawiera on wpisy konfiguracyjne jako pary: klucz = wartość. Poza wpisem `default_email_recipient` w zasadzie żadna inna pozycja nie musi być modyfikowana ręcznie. Wszystkie konieczne modyfikacje dokonywane są podczas instalowania poszczególnych produktów systemu David. Poniżej znajduje się lista możliwych wpisów wraz z ich opisem.

- `user` - nazwa użytkownika z prawami którego pracują demony systemu David;
- `default_email_recipient` - domyślny adres e-mail, gdzie są wysyłane wiadomości od aplikacji systemu David;
- `bindir` - katalog z aplikacjami systemu David (domyślnie: /usr/bin/david-system);
- `libdir` - katalog z bibliotekami systemu David (domyślnie: /usr/lib/david-system);
- `incdir` - katalog z plikami nagłówkowymi systemu David (domyślnie: /usr/include/david);
- `confdir` - katalog z plikami konfiguracyjnymi systemu David (domyślnie: /etc/david-system);
- `logdir` - katalog, gdzie są tworzone logi aplikacji systemu David (domyślnie: /var/log/david-system);
- `sharedir` - katalog z różnymi plikami (obrazki, pliki audio, serwis webowy itd.) systemu David (domyślnie: /usr/share/david-system);
- `docdir` - katalog z dokumentacją systemu David (domyślnie: /usr/share/doc/david-system);
- `vardir` - katalog z archiwami bazy SQL-owej systemu David (domyślnie: /var/lib/david-system);
- `is_sqldb_installed` - flaga, czy SQL-owa baza systemu David została zainstalowana.

4.2. Dedykowane konto dla obsługi systemu David

Nie ma potrzeby, aby jakikolwiek moduł systemu David pracował z prawami superużytkownika (zazwyczaj konto o nazwie `root` i UID równym 0). Nawet, jeśli dany daemon systemu David wymaga w chwili uruchomienia praw superużytkownika, to zawsze istnieje możliwość wyspecyfikowania jako argumentu uruchomienia demona nazwy użytkownika, którego prawa ma przyjąć.

Najwygodniej jest dodać nowego użytkownika do systemu operacyjnego, pod którego kontrolą ma

pracować system David.

4.3. Układ katalogów systemu David

Układ katalogów i ich zawartość może być zależna od konkretnej konfiguracji systemu David. W standardowej konfiguracji systemu poszczególne katalogi zawierają:

- `/usr/bin/david-system` - pliki binarne i skrypty;
- `/etc/david-system` - pliki konfiguracyjne;
- `/usr/share/doc/david-system` - dokumentację systemu David;
- `/usr/share/david-system` - pliki graficzne, dźwiękowe, portal webowy;
- `/usr/include/david` - pliki nagłówkowe systemu David;
- `/usr/lib/david-system` - biblioteki systemu David;
- `/var/log/david-system` - pliki z logami;
- `/var/lib/david-system` - archiwa bazy SQL-owej systemu David.

4.4. Konfiguracja demon-a syslogd

Moduły systemu David wykorzystują standardowy podsystem `syslog` dostępny na platformach UNIX-owych. Domyślne ustawienia modułów systemu David powodują, że informacje są przesyłane jako typ (`facility`) local6. Ustawienia te można oczywiście zmienić w momencie uruchamiania danego modułu. W związku z tym dobrym pomysłem wydaje się takie skonfigurowanie demona `syslogd`, aby wszystkie informacje przesyłane od modułów systemu David znalazły się w jednym miejscu (w jednym lub kilku plikach o charakterystycznej nazwie np.: david.log).

Rozdział 5. Wymagania dla Report Manager-a

Platforma zarządzania, na której ma pracować **Report Manager** musi spełniać następujące wymagania:

- posiadać zainstalowaną kompatybilną wersję **Daemon Manager-a**.

Rozdział 6. Instalacja

6.1. Instalacja z pakietu RPM

Instalacja produktu wymaga uruchomienia przez użytkownika posiadającego prawa `root-a`. Poniżej znajdują się kolejne kroki typowej instalacji:

- Zainstaluj produkt:

```
rpm -i david-xxx-rm-yyy.rpm
```

6.2. Instalacja za pomocą skryptu

Instalacja produktu wymaga uruchomienia przez użytkownika posiadającego prawa `root-a`. Poniżej znajdują się kolejne kroki typowej instalacji:

- Rozkompresuj i rozpakuj archiwum:

```
gunzip david-xxx-rm-yyy.i386.tar.gz
tar xf david-xxx-rm-yyy.i386.tar
```

  Operacje te spowodują utworzenie katalogu david-xxx-rm-yyy.i386 w bieżącym katalogu

- Zmień swój bieżący katalog na david-xxx-rm-yyy.i386:

```
cd david-xxx-rm-yyy.i386
```

- Przczytaj plik LICENSE z bieżącego katalogu i KONTYNUUJ INSTALACJĘ TYLKO WTEDY, KIEDY AKCEPTUJESZ WARUNKI TAM ZAWARTE.

- Uruchom skrypt instalacyjny:

```
./install
```

Rozdział 7. Informacje ogólne

7.1. Funkcjonalność

Report Manager umożliwia:

- automatyczne generowanie godzinnych raportów na podstawie, zdefiniowanych przez użytkownika, filtrów komunikatów SNMP Trap;
- automatyczne generowanie godzinnych raportów na podstawie, zdefiniowanych przez użytkownika, filtrów zarejestrowanych spraw (cases);
- automatyczne generowanie godzinnych raportów na podstawie, zdefiniowanych przez użytkownika, filtrów elementów podlegających monitorowaniu: obiektów pingowanych, interfejsów sieciowych i sąsiadów BGP;
- wizualizację wygenerowanych godzinnych raportów w postaci graficznych raportów dziennych, miesięcznych i rocznych.

7.2. Opis działania

Report Manager zajmuje się przetwarzaniem zarejestrowanych komunikatów SNMP-Trap, wpisów o toczących się sprawach oraz wpisów dotyczących zmiany stanów monitorowanych obiektów (obiektów pingowanych, interfejsów sieciowych i sąsiadów BGP) i generuje na tej podstawie dane do raportów.

Generowanie danych jest dokonywane na podstawie konfiguracji filtrów zdefiniowanej przez użytkownika.

Wizualizacja wygenerowanych raportów dokonywana jest przez aplikację WWW i polega głównie na filtrowaniu i łączeniu danych w większe raporty obejmujące swoim zasięgiem dłuższe odcinki czasu.

7.3. Tematy pokrewne

Zarządca Raportów (dreportd)

Konfigurator Zarządcy Raportów (Report Manager Configurator)

Przeglądarka Raportów (Report Browser)

Rozdział 8. Zarządca Raportów (dreportd)

8.1. Opis ogólny

Program **dreportd** jest **Zarządcą Raportów** i jest częścią **Report Manager-a**. Jest to proces daemon, który pracuje bez przerwy w czasie działania systemu i co godzinę dokonuje przetwarzania zachowanych danych w celu wygenerowania raportu obejmującego ostatnią godzinę. Przetwarzanie danych odbywa się zgodnie z konfiguracją filtrów zdefiniowanych przez użytkownika za pomocą Konfiguratora Zarządcy Raportów.

8.2. Składnia

Program **dreportd** można uruchomić z następującymi opcjami: [*-P,--pid-file filename*] [*-l,--log-facility log_facility*] [*-L,--log-level log_level*] [*-u,--run-as-user username*] [*--reports-since date*] [*--background*] [*-v,--version*] [*-h,--help*]

8.3. Znaczenie opcji w programie dreportd

Tabela 8.1. Znaczenie opcji w programie dreportd

Nazwa opcji	Opis
-P,--pid-file filename	Zapisz swój PID w wyspecyfikowanym pliku.
-l,--log-facility log_facility	Wybierz typ logowania (log facility) do syslogd: daemon | user | local0 | ... | local7 (domyślnie: local6).
-L,--log-level log_level	Wybierz poziom logowania (na standardowe wyjście błędów i do daemona syslogd), tzn. będą wypisywane komunikaty wybranego poziomu oraz komunikaty poziomów ważniejszych: emerg | alert | crit | err | warning | notice | info | debug0 | ... | debug2 (domyślnie: notice).
-u,--run-as-user username	Zrezygnuj z praw root'a i uruchom serwer z prawami podanego użytkownika.
--reports-since date	Generuj raport od podanej daty, jeśli żadne raporty nie zostały jeszcze wygenerowane (format daty: 'rrrr/mm/dd gg').
--background	Rozpocznij pracę w tle po uruchomieniu.
-v,--version	Wypisz numer wersji na swoje standardowe wyjście błędów i zakończ.
-h,--help	Wypisz komunikat o użyciu na swoje standardowe wyjście błędów i zakończ.

8.4. Opis działania

Po uruchomieniu program sprawdza, czy nie ma do zrobienia zaległych raportów. Jeśli tak to będzie je sukcesywnie wykonywał. Jeśli nie to wykona zwyczajny raport za bieżącą godzinę.

Zaległe raporty mogą być wykonywane w kilku przypadkach. Program stara się odnaleźć ostatni poprawnie zakończony raport. Jeśli nie znajdzie go za ostatnią godzinę, to zacznie wykonywać raporty za kolejne okresy, począwszy od ostatniego poprawnie zakończonego raportu. Jeśli nie znajdzie żadnego raportu, to wykona raport za bieżącą godzinę. Jeśli natomiast został uruchomiony z opcją --reports-since odnoszącą się do przeszłości, to zacznie wykonywać raporty od podanego momentu.

Po wykonaniu wszystkich ewentualnych zaległych raportów, **dreportd** przystępuje do normalnej pracy. Oczekuje on na upływ kolejnej pełnej godziny (np. 15:00, 18:00 itp.) i wykonuje raport za ostatnią, pełną godzinę. W pierwszej kolejności generowane są raporty dotyczące wpisów SNMP Trap, następnie wpisów o prowadzonych sprawach (cases), a na końcu o monitorowanych obiekatach (obiekty pingowane, interfejsy sieciowe, sąsiedzi BGP).

Generowanie raportów każdorazowo zakończone jest potwierdzeniem poprawnego zakończenia wykonania raportu. Tylko takie raporty są traktowane jako poprawne.

8.4.1. Przetwarzanie filtrów dotyczących wpisów SNMP Trap

Na podstawie filtrów zdefiniowanych przez użytkownika budowane są zapytania SQL, których wynik działania jest następnie odpowiednio interpretowany. Każde zapytanie generowane jest na podstawie pojedynczego filtra. W pierwszej kolejności, podczas budowania zapytania, przetwarzane są wpisy z grupy `Group by` Konfiguratora Zarządcy Raportów zgodnie z kolejnością wpisów podaną w konfiguracji. Do dalszej budowy zapytania używane są wpisy z grupy `Custom filters`, zaś na końcu dodawane są warunki z grupy `Rules`. Kolumny `Field` dla wszystkich trzech grup zawierają listę pól charakteryzujących wpisy o komunikatach SNMP Trap.

Po zbudowaniu zapytania jest ono wykonywane, a każdy wiersz jego wyniku jest interpretowany przy pomocy wpisów z grup `Group by` i `Custom filters`. Na początku dokonuje się interpretacja przy pomocy wpisów a grupy `Group by`. Każdy wpis tej grupy odpowiada pojedynczej kolumnie wyniku zapytania, której zawartość jest interpretowana zgodnie ze specyfikacją pól `Treat as` i `Show` danego wpisu.

Pole `Treat as` może przyjmować następujące wartości: `BGPPEER`, `NETINTERFACE`, `OBJECT`, `PINGOBJECT`. Pole to może być też puste (wartość `--skip--` Konfiguratora Zarządcy Raportów). Wartości te wskazują jak zawartość kolejnych kolumn rezultatu zapytania, powstałych poprzez działanie wpisów z grupy `Group by`, ma być interpretowana i tym samym tłumaczona na nazwy monitorowanych obiektów (np.: na nazwy urządzeń, opisy interfejsów sieciowych, wpisy sąsiadów BGP).

Pole `Show` może przyjmować następujące wartości: `Yes`, `No`, `When others failed`, `If success`. Wartości te wskazują jak zawartość kolejnych kolumn rezultatu zapytania, powstałych poprzez działanie wpisów z grupy `Group by`, ma być interpretowana i tym samym, czy ma się znaleźć

w końcowym rezultacie przetwarzania wiersza wyniku. Wartości `Yes` i `No` nie wymagają wyjaśnienia. Wartość `If success` oznacza, że wartość ma być brana pod uwagę, jeśli nie będzie pusta, zaś wartość `When others failed` oznacza, że będzie użyta tylko wtedy, gdy wartości dla wszystkich wpisów grupy `Group by` są puste. Wpis ten pełni, więc rolę wpisu awaryjnego.

Interpretacja wyniku zapytania przy pomocy wpisów z grupy `Custom filters` dokonywana jest poprzez pola `Filter` i `Result`. Zawartość odpowiedniej kolumny wyniku zapytania, powstałej poprzez działanie danego wpisu z grupy `Custom filters`, jest parsowana zgodnie z zawartością pola `Filter` i tłumaczona na napis zgodnie z zawartością pola `Result`.

8.4.2. Przetwarzanie filtrów dotyczących wpisów o prowadzonych sprawach (cases)

Przetwarzanie filtrów dotyczących prowadzonych spraw dokonywane jest analogicznie jak przetwarzanie filtrów dla wpisów SNMP Trap. Jedyną różnicą jest zawartość kolumn `Field` dla kolejnych trzech grup każdego filtra. W tym przypadku kolumny `Field` zawierają bowiem listę pól odnoszących się do wpisów o toczących się sprawach.

8.4.3. Przetwarzanie filtrów dotyczących wpisów o monitorowanych obiektach

Przetwarzanie wpisów dotyczących monitorowanych obiektów dokonuje się na podstawie filtrów zdefiniowanych przez administratora. Każdy filtr zawiera pole określające rodzaj obiektu, którego dotyczy. Na podstawie tego pola **dreportd** wie, gdzie szukać wpisów dotyczących tego typu obiektów. Każdy filtr może zawierać listę dopuszczalnych rodzajów urządzeń, których ma dotyczyć. Dzięki temu można ograniczyć dopływ zbędnych informacji, jakie powstałyby w wyniku przetwarzania danego filtra (obecnie ma to znaczenie tylko w przypadku interfejsów sieciowych). Użytkownik może dokonać specyfikacji dozwolonych urządzeń w grupie `Allowed devices` Konfiguratora Zarządcy Raportów.

8.5. Tematy pokrewne

Konfigurator Zarządcy Raportów (Report Manager Configurator)

Przeglądarka Raportów (Report Browser)

Rozdział 9. Przyciski najczęściej występujące w aplikacjach WWW

9.1. Znaczenie przycisków

W poniższej tabeli zostały zebrane przyciski, które w aplikacjach WWW występują najczęściej. Ich funkcja w poszczególnych aplikacjach jest zbliżona, a czasem nawet identyczna. Niektóre z nich mogą jednak pełnić dodatkowe funkcje, które przy okazji omawiania poszczególnych aplikacji.

Tabela 9.1. Przyciski najczęściej występujące w aplikacjach WWW

Przycisk	Opis
	Powoduje powrót do widoku poprzedniej strony.
	Generalnie powoduje usunięcie elementu tzn. np: powoduje zamknięcie sprawy (case), ustawienie zdarzenia (event) w stan pasywny itp.
	Podwoduje przejście do edycji danego elementu.
	Najczęściej oznacza zatwierdzenie operacji i przejście do jej wykonania (np.: wygenerowanie raportu używając wybranych kryteriów).
	Powoduje przejście do widoku szczegółowego.
	Pozwala przejść do wyższego poziomu w hierarchii elementów.
	Otwiera nowe okno z danymi przygotowanymi do wydruku.
	Powoduje przejście do prezentacji wykresu z danymi dla danego elementu (Przeglądarka Kolekcji).
	Odświeża widok strony.
	Powoduje akceptację zmienionych wartości jako aktualnych.

Przycisk	Opis
	Powoduje przejście do raportu dla danego elementu (Przeglądarka Raportów o Węzłach).
	Powoduje przejście do przeglądarki raportów o Trapach dla danego elementu (Przeglądarka Trapów).
	Powoduje przejście do przeglądarki raportów o sprawach (cases) dla danego elementu (Przeglądrka Zarejestrowanych Spraw).
	Zachowuje zmiany dokonane przez użytkownika.

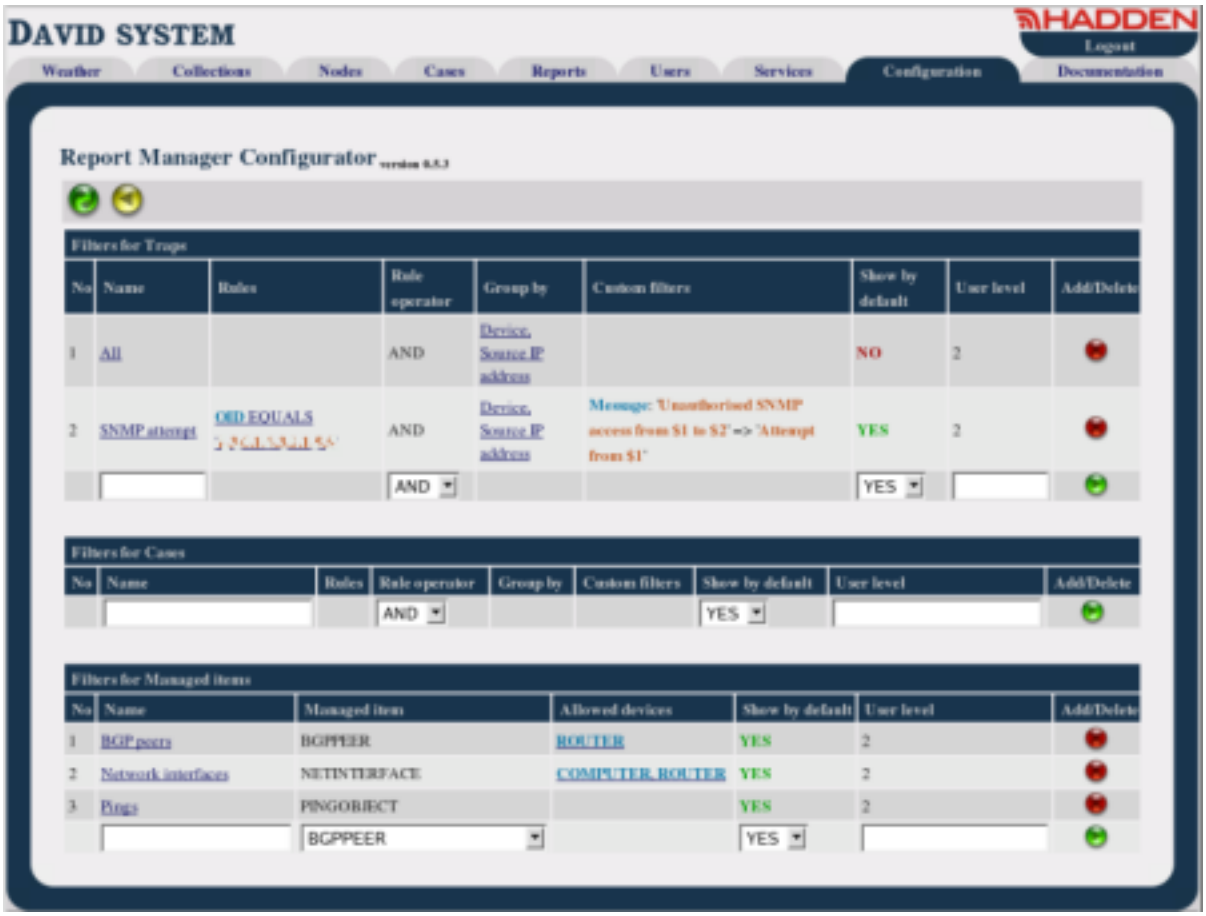
Rozdział 10. Konfigurator Zarządcy Raportów (Report Manager Configurator)

10.1. Opis ogólny

Konfigurator Zarządcy Raportów jest aplikacją WWW i wchodzi w skład **Report Manager-a**. Konfigurator pozwala sterować pracą Zarządcy Raportów (dreportd) poprzez definiowanie filtrów służących do generowania raportów.

10.2. Opis działania

10.2.1. Widok domyślny aplikacji



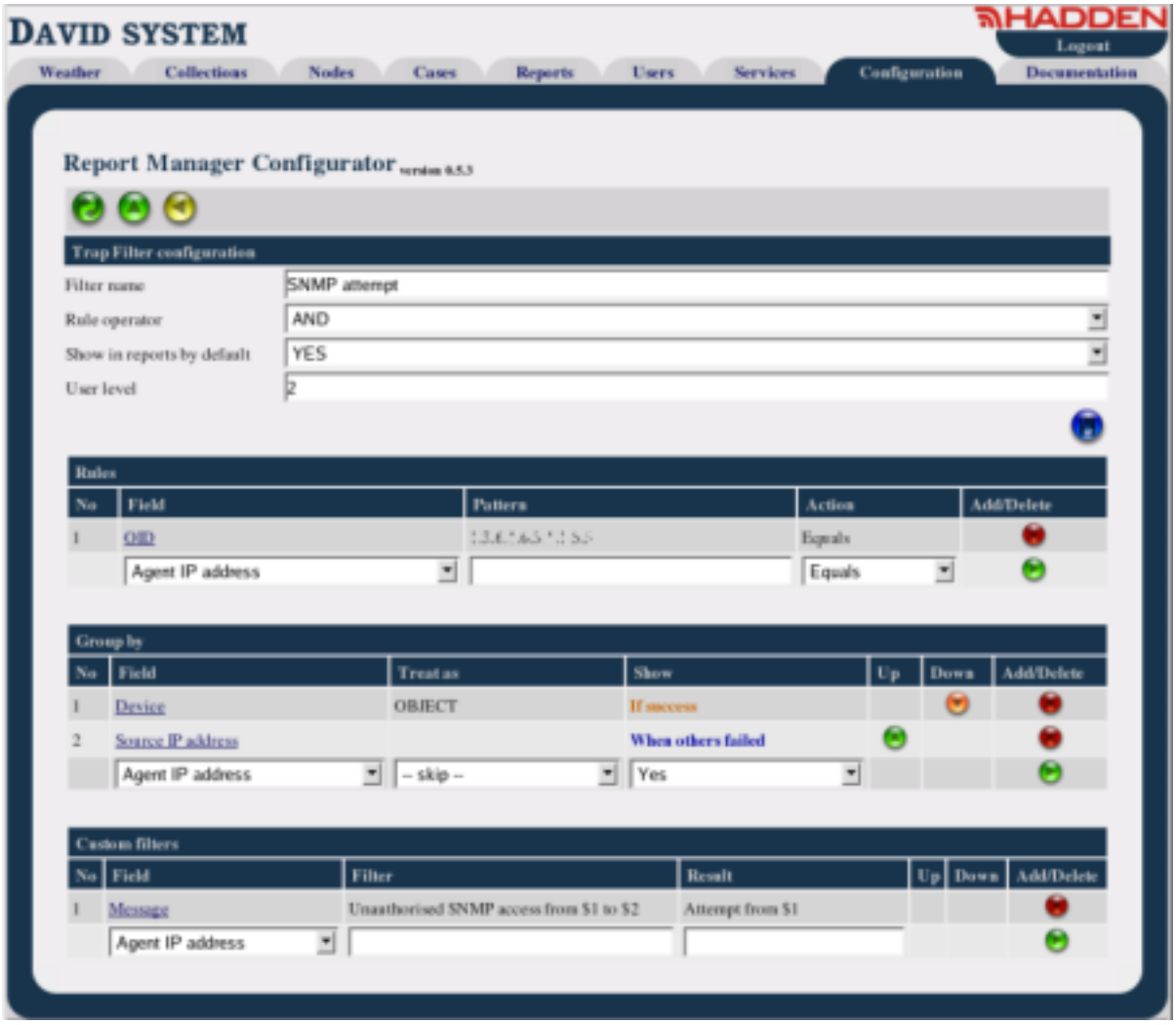
Konfigurator Zarządcy Raportów to jedna z aplikacji dostępnych w zakładce `Configuration`. Główny widok aplikacji prezentuje listę wszystkich zdefiniowanych filtrów poszczególnych typów. Dostępne są trzy typy filtrów: dotyczące danych SNMP Trap, dotyczące zarejestrowanych wpisów o

prowadzonych sprawach oraz dotyczące wpisów o monitorowanych obiektach. Lista każdego typu jako ostatni swój wiersz zawiera pola edycyjne pozwalające wyspecyfikować nowy jej element i dodać go do listy. Pola te różnią się w zależności od typu filtra, którego nowy element definiujemy. Znaczenie poszczególnych kolumn dla różnych typów filtrów zostały omówione szczegółowo w części dokumnetu dotyczącej Zarządcy Raportów.

Trzy kolumny opisane poniżej są wspólne dla wszystkich typy filtrów. Są to: `Show by default` - wskazuje, czy wyniki działania filtra mają być domyślnie prezentowane przez Przeglądarkę Raportów , `User level` - minimalny poziom użytkownika wymagany do edycji filtra oraz `Add/Delete` - pozwala dodać nowy i usunąć istniejący filtr.

Linki w poszczególnych kolumnach pozwalają przejść do edycji wybranego filtra.

10.2.2. Edycja filtrów dotyczących wpisów SNMP Trap



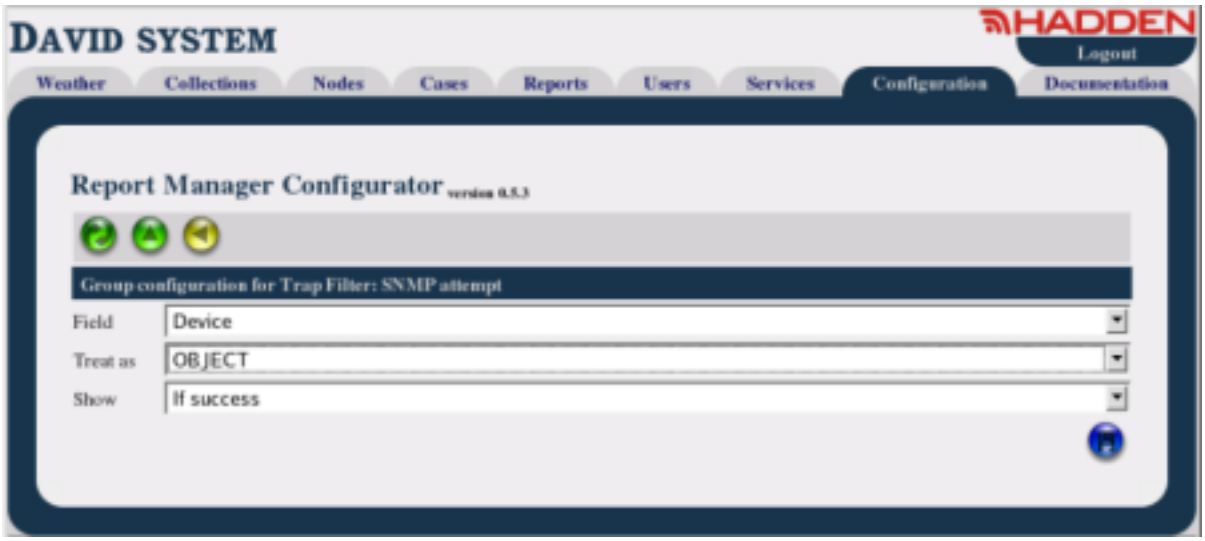
Górną część aplikacji zajmują pola edycyjne pozwalające zmienić nazwę filtra, rodzaj operacji logicznej (AND lub OR) występującej pomiędzy wpisami w grupie `Rules`, warunek, czy wyniki działania filtra są prezentowane domyślnie przez Przeglądarkę Raportów, minimalny poziom użytkownika wymagany do

edycji filtra.

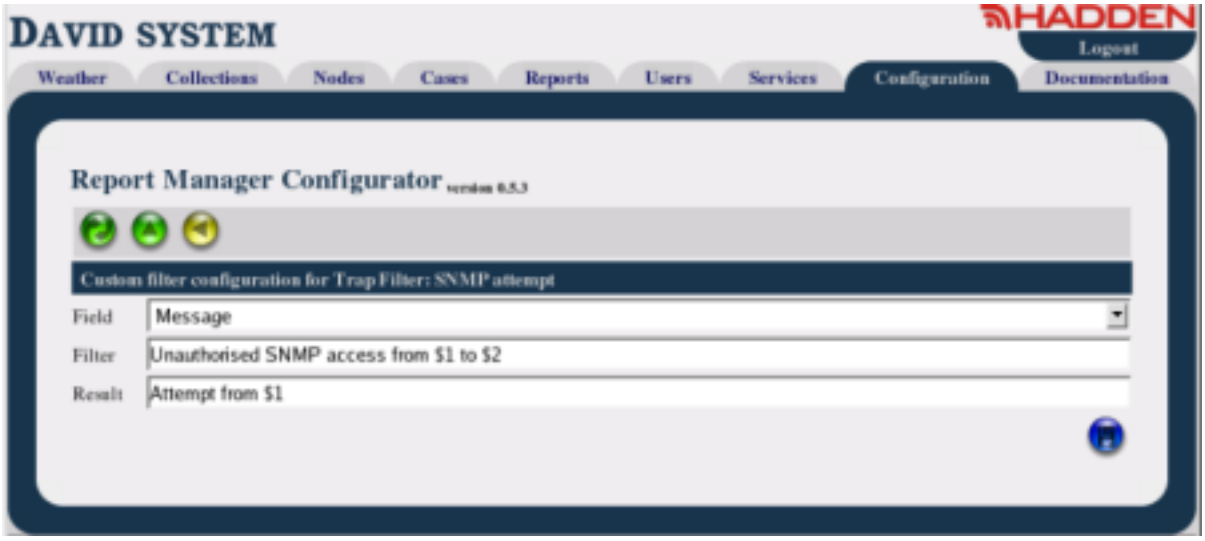
Poszczególne grupy wpisów definiujące dany filtr zawierają charakterystyczne dla siebie kolumny. Dodatkowo każda z nich zawiera kolumnę `Add/Delete` zawierają przyciski pozwalające dodać nowy lub usunąć istniejący wpis. Grupa `Group by` zawiera dwie dodatkowe kolumny `Up` i `Down` pozwalające przesuwać względem siebie poszczególne wpisy.

Każda grupa w ostatnim wierszu zawiera pola pozwalające dodać nowy wpis do grupy. Kolumny `Field` zawierają linki pozwalające na edycję poszczególnych wpisów.

Edycja grupy `Rule` sprowadza się do specyfikacji zawartości pól: `Field`, `Pattern` i `Action`. Ich znaczenie zostało opisane w części dokumnetu dotyczącej Zarządcy Raportów.



Edycja grupy `Group by` sprowadza się do specyfikacji zawartości pól: `Field`, `Treat as` i `Show`. Ich znaczenie zostało opisane w części dokumnetu dotyczącej Zarządcy Raportów.



Edycja grupy `Custom filter` sprowadza się do specyfikacji zawartości pól: `Field`, `Filter` i `Result`. Ich znaczenie zostało opisane w części dokumnetu dotyczącej Zarządcy Raportów.

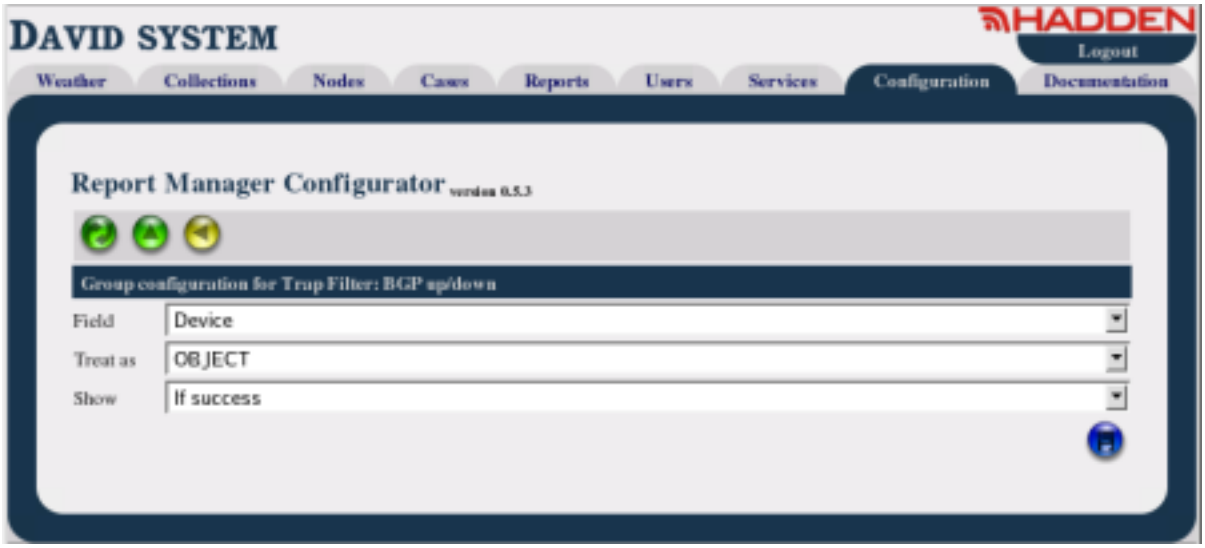
10.2.3. Edycja filtrów dotyczących wpisów o prowadzonych sprawach (cases)

Górną część aplikacji zajmują pola edycyjne pozwalające zmienić nazwę filtra, rodzaj operacji logicznej (AND lub OR) występującej pomiędzy wpisami w grupie `Rules`, warunek, czy wyniki działania filtra są prezentowane domyślnie przez Przeglądarkę Raportów, minimalny poziom użytkownika wymagany do edycji filtra.

Poszczególne grupy wpisów definiujące dany filtr zawierają charakterystyczne dla siebie kolumny. Dodatkowo każda z nich zawiera kolumnę `Add/Delete` zawierają przyciski pozwalające dodać nowy lub usunąć istniejący wpis. Grupa `Group by` zawiera dwie dodatkowe kolumny `Up` i `Down` pozwalające przesuwać względem siebie poszczególne wpisy.

Każda grupa w ostatnim wierszu zawiera pola pozwalające dodać nowy wpis do grupy. Kolumny `Field` zawierają linki pozwalające na edycję poszczególnych wpisów.

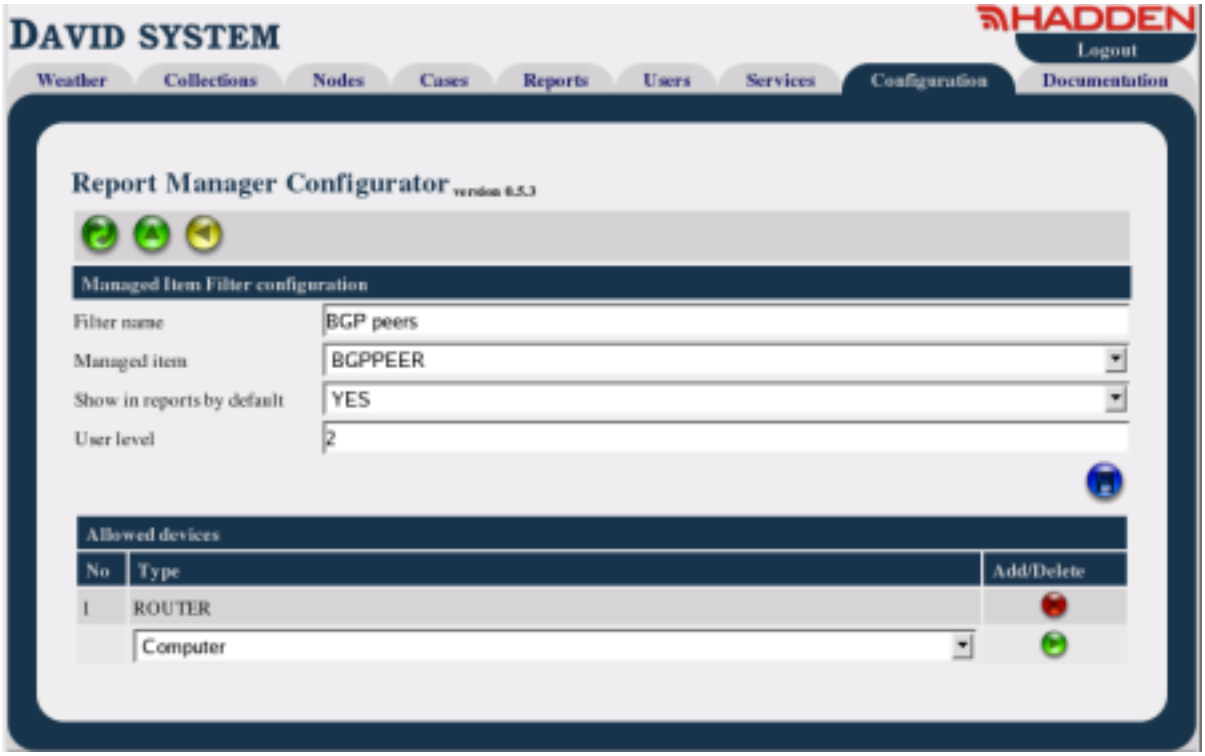
Edycja grupy `Rule` sprowadza się do specyfikacji zawartości pól: `Field`, `Pattern` i `Action`. Ich znaczenie zostało opisane w części dokumnetu dotyczącej Zarządcy Raportów.



Edycja grupy `Group by` sprowadza się do specyfikacji zawartości pól: `Field`, `Treat as` i `Show`. Ich znaczenie zostało opisane w części dokumnetu dotyczącej Zarządcy Raportów.

Edycja grupy `Custom filter` jest identyczna jak w przypadku edycji tej grupy dotyczącej wpisów SNMP Trap. W tym przypadku jest ona jednak rzadziej wykorzystywana.

10.2.4. Edycja filtrów dotyczących wpisów o monitorowanych obiektach



Górną część aplikacji zajmują pola edycyjne pozwalające zmienić nazwę filtra, typ obiektu monitorowanego, którego filtr dotyczy, warunek, czy wyniki działania filtra są prezentowane domyślnie przez Przeglądarkę Raportów, minimalny poziom użytkownika wymagany do edycji filtra.

Dolną część aplikacji zajmuje lista typów urządzeń objętych działaniem filtra. Ostatnia kolumna listy zawiera przyciski pozwalające dodać nowy typ urządzenia lub usunąć istniejący. Pusta lista oznacza, że filtr dotyczy wszystkich typów urządzeń.

10.3. Tematy pokrewne

Zarządca Raportów (dreportd)

Przeglądarka Raportów (Report Browser)

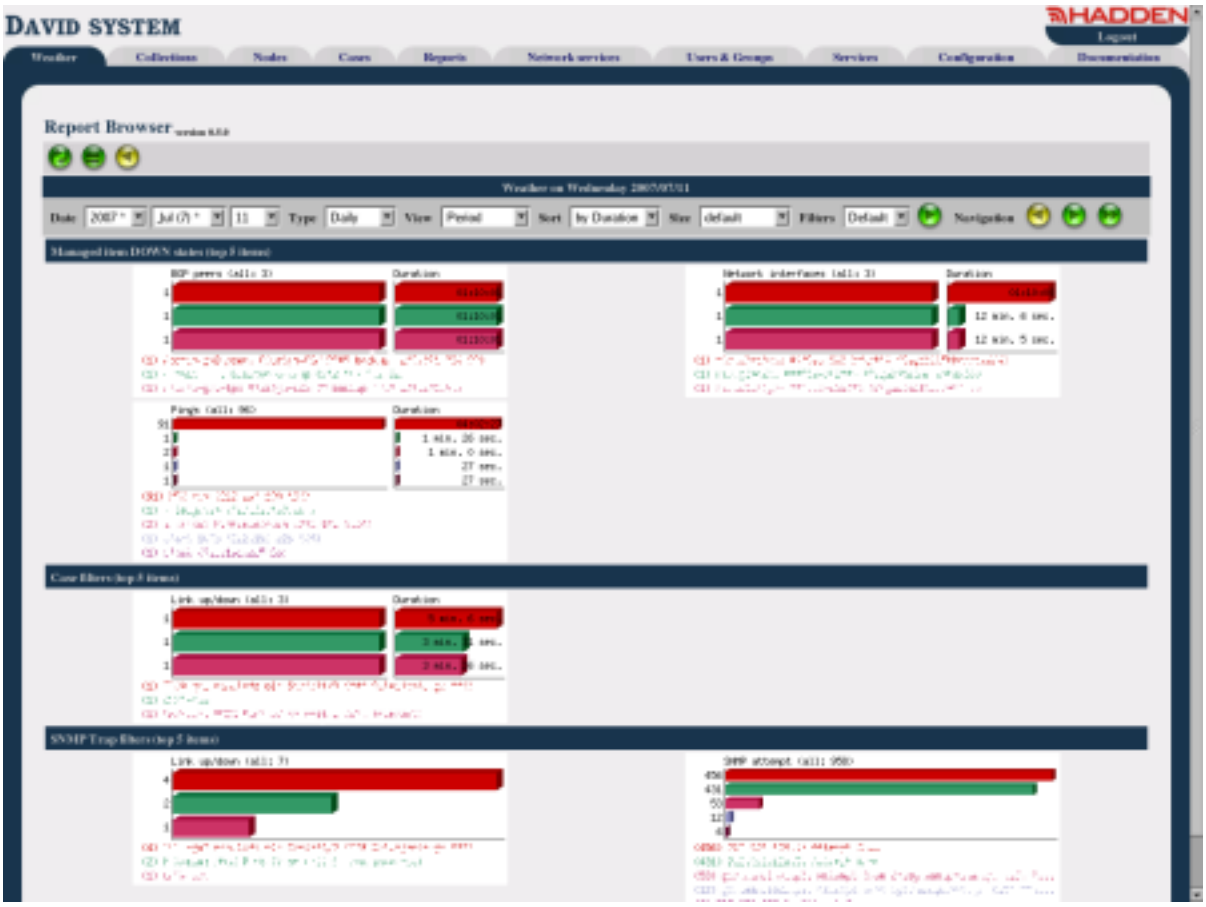
Rozdział 11. Przeglądarka Raportów (Report Browser)

11.1. Opis ogólny

Przeglądarka Raportów jest aplikacją WWW oraz częścią **Report Manager-a**. Pozwala ona przeglądać dzienne, miesięczne i roczne raporty wygenerowane na podstawie danych będących wynikiem pracy Zarządcy Raportów.

11.2. Opis działania

11.2.1. Widok domyślny aplikacji



Przeglądarka Raportów jest dostępna poprzez zakładkę `Weather`. Górną część aplikacji zajmuje pasek narzędziowy charakterystyczny dla wszystkich aplikacji WWW. Pod nim znajduje się pasek narzędziowy z obiektami definiującymi rodzaje prezentowanych danych. Znaczenie poszczególnych pól prezentuje poniższa tabela:

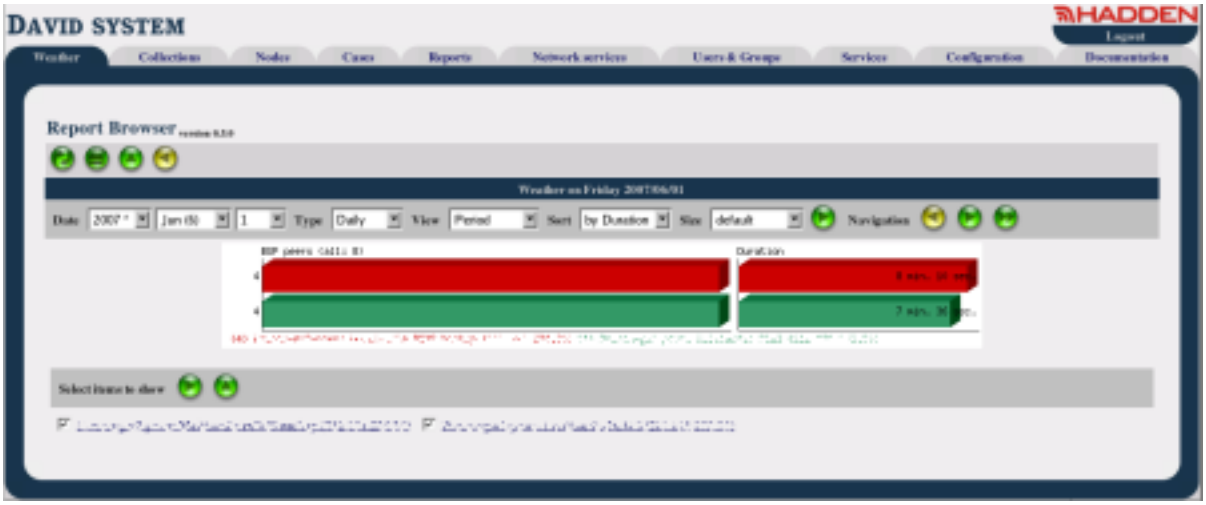
Tabela 11.1. Przeglądarka Raportów - obiekty paska narzędziowego

Obiekt	Znaczenie
Date	Data, której ma dotyczyć raport. Dla raportu miesięcznego dzień nie ma znaczenia, zaś dla rocznego nie ma znaczenia także miesiąc.
Type	Typ raportu definiujący jego zakres czasowy. Możliwe są następujące wartości: dzienny, miesięczny i roczny.
View	Określa, czy ma być pokazywany raport podsumowujący wybrany odcinek czasu, czy też raport ma pokazywać podzakresy (np.: dla raportu dziennego podzakresami są godziny, zaś dla miesięcznego są to dni).
Sort	Definiuje typ sortowania wyników działania każdego filtra. Typ `by Result` sortuje wyniki malejąco według liczby wystąpień poszczególnych wyników. Typ `by Duration` sortuje wyniki według czasu trwania poszczególnych wpisów.
Size	Zależnie od kontekstu ustawia szerokość lub wysokość wykresów.
Filters	Rodzaj pokazywanych wyników filtrów (domyślne filtry lub wszystkie). Pole to ma znaczenie tylko w przypadku pokazywania grup filtrów, a nie wybranego filtra.

Generowanie raportu, zgodnie z wybranymi wartościami pól, odbywa się za pomocą wciśnięcia przycisku  . Na końcu paska narzędziowego znajdują się przyciski nawigacyjne pozwalające przeglądanie wyników raportu w kolejnych odcinkach czasu (np.: dniach).

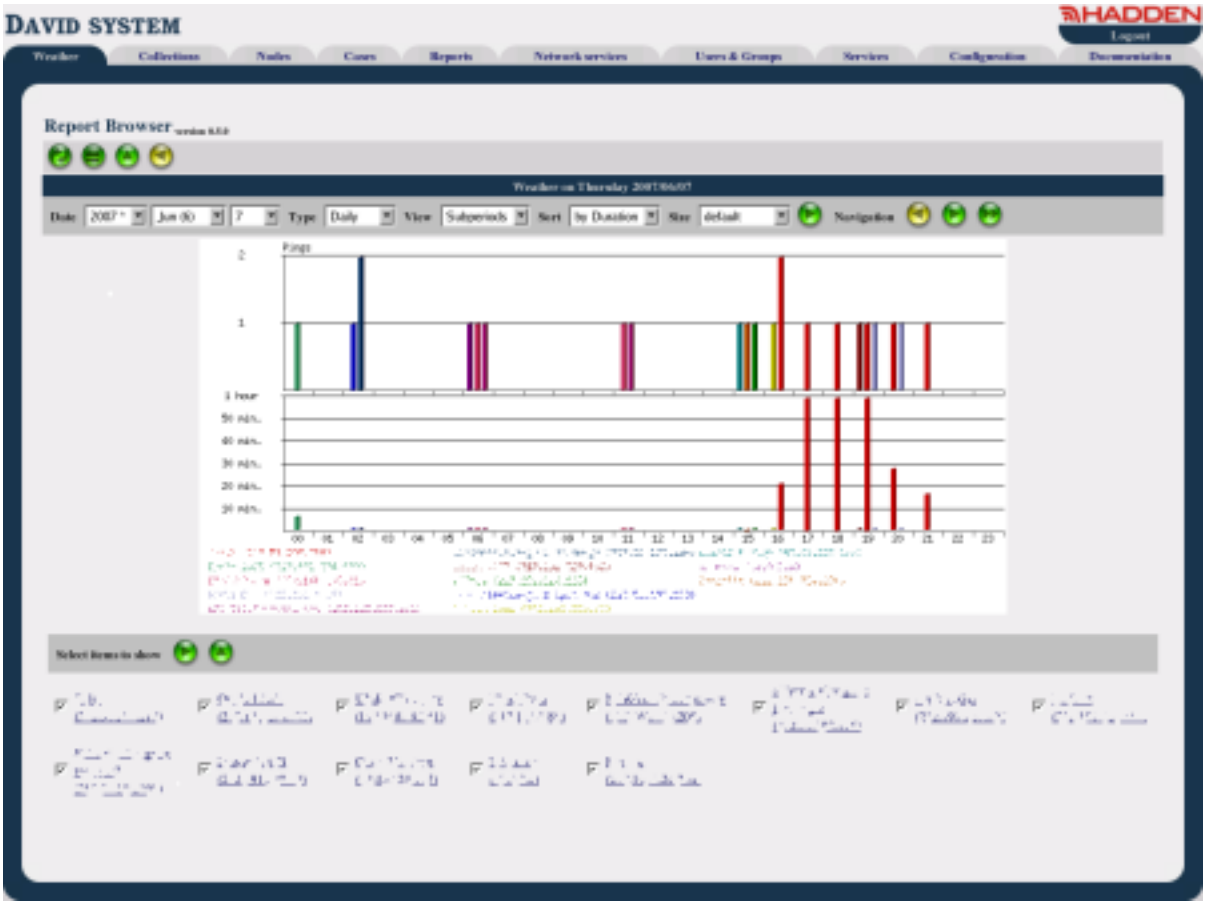
Kliknięcie na słupek wykresu powoduje przejście do obiektu, którego dotyczy za pomocą **Przeglądarki Węzłów**. Dla wyników filtrów dotyczących monitorowanych obiektów, kliknięcie na słupek spowoduje przejście do raportu na temat wskazanego obiektu za wybrany odcinek czasu, za pomocą **Przeglądarki Raportów o Węzłach**. Kliknięcie poza obszarem słupków wykresu powoduje przejście do widoku działania pojedynczego filtra.

11.2.2. Widok działania pojedynczego filtra



Widok ten pokazuje wyniki działania pojedynczego filtra, a nie ich grupy. Wiele operacji jest jednak analogicznych jak przypadku widoku grupy filtrów. Poniżej wykresu dodatkowo umieszczony jest wykaz wszystkich wygenerowanych wyników dla tego filtra z zaznaczonymi pozycjami prezentowanymi na wykresie. Dzięki temu można wybierać pozycje, które chcemy umieścić na wykresie. Przycisk  przywraca wybór domyślnych pozycji.

11.2.3. Widok działania pojedynczego filtra pokazujący podzakresy



Jedyną różnicą w porównaniu z całościowym raportem prezentującym wyniki działania pojedynczego filtra jest inny typ wykresu. Pokazuje on wyniki podzielone na podzakresy wybranego okresu czasowego.

11.3. Tematy pokrewne

Konfigurator Zarządcy Raportów (Report Manager Configurator)

Zarządca Raportów (dreportd)

Network Manager Przeglądarka Węzłów

Network Manager Przeglądarka Raportów o Węzłach