LiNUX+

LiNUX+

NAJWIĘKSZY EUROPEJSKI MAGAZYN O LINUKSIE

NR 6 (156) 2010

PROGRAMOWANIE W QT 4.6 POD UBUNTU

WYSTARTUJ Z TOMCAT. WPROWADZENIE DO ADMINISTRACJI SERWEREM NA LINUXIE

PINGWIN W PUDEŁKU

PENTAHO – OPEN SOURCE DLA BIZNESU

OKIEM W CHMURACH

ZIMBRA COLLABORATION SUITE
PRACA GRUPOWA W OPEN SOURCE
CZ 2.MIGRACJA, KONFIGURACJA URZĄDZEŃ

ROZWIĄZANIA:
OPROGRAMOWANIE OPEN SOURCE WSPOMAGAJĄCE ZARZĄDZANIE SERWERAMI

ZOSTAŃ ADMINISTRATOREM SIECI KOMPUTEROWEJ
CZ 8. BEZPIECZEŃSTWO SIECI BEZPRZEWODOWYCH

Tworzysz aplikacje mobilne?
Wykorzystaj możliwości platformy Samsung bada!

Weź udział w konkursie

badacup

Do wygrania nagrody o wartości

450 000 zł

Podejmij wyzwanie!

Odkryj ocean możliwości, jakie oferuje platforma **Samsung bada** i wygraj. Pula nagród to 450 000 zł.

Zostań przedstawicielem Nowej Ery Aplikacji Mobilnych. Stwórz aplikację, która najlepiej odpowie na potrzeby współczesnych użytkowników telefonów komórkowych. Otwórz ich na zupełnie nowe doznania, wykaż się niestandardowym spojrzeniem na istniejące funkcje telefonu lub stwórz nowe, niepowtarzalne i zaskakujące.
Na Wasze aplikacje czekamy od 30 kwietnia 2010 do 30 lipca 2010 r. pod adresem www.bada.samsung.pl.

www.bada.samsung.pl

SAMSUNG

TURN ON TOMORROW

Potrafisz zaprogramować przyszłość?

Twórz z nami rzeczywistość, którą inni poznają dopiero jutro.

Do końca 2010 roku Tieto zatrudni w Polsce ponad 360 osób.

Zgłoś się do nas i dołącz do grupy wysoko wykwalifikowanych inżynierów kreujących przyszłość IT. Rozpocznij przygodę z innowacyjną technologią 4G w telefonii komórkowej i już dziś rozwijaj technologie, które jutro staną się rzeczywistością.

Tworzymy zespół młodych, zdolnych programistów, doskonale przygotowanych do pracy z jednym z największych światowych dostawców rozwiązań telekomunikacyjnych jutra.

Poszukujemy: programistów C/C++/Java, testerów oprogramowania, kierowników projektu, architektów systemów IT. Interesuje nas każdy poziom doświadczenia.

Dołącz do zespołu 16 000 specjalistów.
Aplikuj na www.tieto.pl/praca

Knowledge. Passion. Results.

tieto

Konferencja Open Source Day 2010

Szanowni Państwo,
Serdecznie zapraszamy na konferencję Open Source Day 2010, która odbędzie się 12 maja w Warszawie, w Pałacu Kultury i Nauki.

Wysłuchaj wykładów światowych liderów otwartego oprogramowania, m.in. Red Hat, JBoss, EnterpriseDB i Zimbra! Dowiedz się więcej o trendach rozwojowych i wpływie Open Source na sytuację ekonomiczną firmy. W programie także wykłady poświęcone m.in. wirtualizacji, bazom danych oraz bezpieczeństwu z SELinuxem.

Każdy uczestnik otrzyma kupon rabatowy na szkolenia certyfikacyjne Red Hat i JBoss.

Największe w Polsce wydarzenie poświęcone technologiom Open Source zostało objęte patronatem Ministerstwa Gospodarki i osobiście Pana Premiera Waldemara Pawlaka, który otworzy konferencję swoim wykładem.

Udział w spotkaniu jest bezpłatny

Zapraszamy do rejestracji: www.opensourceday.pl

Miesięcznik **Linux+** (12 numerów w roku)
jest wydawany przez Software Press Sp. z o.o. SK

Redaktor naczelny:
Tomasz Łopuszański *tomasz.lopuszanski@software.com.pl*

Projekt okładki: Agnieszka Marchocka

Skład i łamanie:
Tomasz Kostro *www.studiopoligraficzne.com*

Kierownik produkcji:
Andrzej Kuca *andrzej.kuca@software.com.pl*

Stali współpracownicy:
Andrzej Jankowski, Roger Zacharczyk, Leszek Konka, Piotr Brzózka, Robert Romaniuk, Sławomir Iwanek

Adres korespondencyjny:
Software Press Sp. z o.o. SK,
ul. Bokserska 1, 02-682 Warszawa, Polska
tel. +48 22 427 36 91, fax +48 22 224 24 59
www.sdjournal.org cooperation@software.com.pl

Dział reklamy: *adv@software.com.pl*

Osoby zainteresowane współpracą prosimy o kontakt:
cooperation@software.com.pl

SPIS TREŚCI

WARSZTATY

PRAKTYKA

ROZWIĄZANIA

SIECI KOMPUTEROWE

Niemcy zaniepokojeni Google Street View

Niemieckim władzom nie podoba się usługa Google Street View. Tym razem nie chodzi o fotografowanie ludzi na ulicach, a dostęp do prywatnych sieci WLAN naszych zachodnich sąsiadów. Zdaniem tygodnika Der Spiegel niemieckie władze chcą przyjrzeć się bliżej zbieraniu materiałów przez firmę Google w ich kraju. Usługa Street View umożliwia użytkownikom Google Maps podgląd ulic czy placów z punktu widzenia zwykłego przechodnia. Obok budynków na zdjęciach widoczni są często zwykli ludzie, przy czym ich twarze są zasłaniane. Według Petera Schaara, Federalnego Komisarza Ochrony Danych i Wolności Informacji, Google oprócz zdjęć może skanować okolicę pod kątem sieci WLAN (także tych prywatnych) i zbierać adresy MAC punktów dostępowych. Schaar podobno dzwonił do przedstawicieli Google'a z prośbą, aby tego rodzaju informacje zostały natychmiast usunięte. Według Der Spiegel, Schaar miał powiedzieć, że jest przerażony możliwościami wykorzystania takich informacji. No właśnie, do czego takie informacje mogą się przydać? Mając bazę sieci bezprzewodowych i ich fizycznych lokalizacji, można zaoferować użytkownikom bardziej trafną usługę geolokalizacji. Wystarczy, że wyślemy do firmy Google adres MAC punktu bezprzewodowego, do którego jesteśmy aktualnie podłączeni, a w odpowiedzi dostaniemy współrzędne geograficzne bliskie naszej aktualnej lokalizacji. Oczywiście jak każde tego typu rozwiązanie, również i to może budzić kontrowersje wśród osób obawiających się o swoją prywatność. Obawy są jednak w dużej mierze nieuzasadnione, bo adres MAC nie jest standardowo wysyłany do serwerów internetowych podczas nawiązywania połączenia, więc użytkownik musiałby samodzielnie poprosić o taką geolokalizację, ewentualnie w jego imieniu mogłoby to zrobić jakieś złośliwe oprogramowanie. To nie pierwsze problemy z usługą Street View. Pod koniec lutego informowaliśmy o apelu Unii Europejskiej, aby firma informowała lokalne władze o zamiarze fotografowania ulic na ich terenie.

iPhone z zainstalowanym Androidem

Do tej pory można było oglądać wiele różnych przeróbek i instalacji mobilnego systemu Google – Android na różnych urządzeniach. Tym razem jednak doszło do czegoś większego Jeden z utalentowanych hackerów iPhone'a, David Wong, zdołał zainstalować Androida na telefonie iPhone 2G – warto nadmienić, że Wang jakiś czas temu uruchomił także Linuksa na iPhonie. System można uruchamiać zamiennie z iPhone OS przy pomocy bootloadera. Wong prezentuje łączenie z siecią Wi-Fi, przeglądanie stron WWW, wysyłanie wiadomości SMS i wykonywanie połączenia. Wong wspomina również, że w podobny sposób można zmodyfikować iPhone'a 3G, ale z wersją 3GS najprawdopodobniej byłoby więcej problemów, z powodu różnic sprzętowych. Jak przyznaje sam autor, system jest dopiero w fazie alfa, jednak główne funkcje działają tak jak powinny. W chwili obecnej system działa wyłącznie na iPhone'ach 2G, jednak zdaniem twórcy przesortowanie go na nowsze wersje powinno być tylko kwestią czasu. Oczywiście używanie "iDroida" nie jest zbyt wygodne i stanowi w zasadzie jedynie ciekawostkę. Jest to jednak czytelny sygnał w stronę Apple o tym, że to użytkownicy powinni decydować o oprogramowaniu zainstalowanym na ich telefonach, a nie korporacje.

Spotkania networkingowe w Twoim mieście.

Lublin, Kielce, Rzeszów, Tarnów, Opole, Łódź to miasta, gdzie w maju Grzegorz Turniak, Prezes BNI Polska, spotka się z przedsiębiorcami i studentami. Wsiądź za stery swojej kariery. Jest to szansa na nawiązanie wyjątkowych kontaktów, gdzie ludzie będą mówili o tym, czym się zajmują, analizując wspólne korzyści. W momencie kiedy jest się w czymś dobrym, ale nie wiadomo, jak to spieniężyć, obowiązkowo trzeba o tym mówić na spotkaniu. Przedsiębiorcy poszukują zazwyczaj młodych talentów oraz partnerów biznesowych. Jest to doskonałe miejsce dla każdego na porozmawianie ze swoim pracodawcą na zasadach partnerskich. Spotkanie kończy się energicznym wykładem Grzegorza Turniaka. Spotkania są organizowane przez Studenckie Forum Business Center Club (*www.sfbcc.org.pl*) oraz BNI Polska (*www.bnipolska.pl*). Weź ze sobą wizytówki i sprawdź koniecznie, gdzie się udać na *www.dnigoscia.pl*

Adobe nie będzie rozwijać produktów dla iPhone oraz iPad

Firma Adobe wstrzymała swoje dążenia do wprowadzenia aplikacji Flash na iPhone'a i iPada. We wtorek Mike Chambers z Adobe poinformował, że firma wstrzymuje inwestycje w narzędzia, które miały umożliwiać portowanie aplikacji pisanych we Flashu na urządzenia Apple. Decyzja jest wynikiem zmian wprowadzonych przez koncern z Cupertino w regułach deweloperskich. Według nowych zasad, każda aplikacja na iPhone'a lub iPada musi być napisana w języku programowania zatwierdzonym przez Apple (np. C++). W tym wypadku, producent telefonu z jabłuszkiem mógłby bez żadnych problemów nie dopuszczać do App Store żadnej aplikacji stworzonej przez Adobe Packager – narzędzia, które w łatwy sposób umożliwia przetłumaczenie aplikacji napisanej we Flash'u, na język obsługiwany przez iPhone'a. Adobe postawione w takiej sytuacji postanowiło wycofać się z projektu Packager dla iPhone'a. Na tym kończy się, przynajmniej na razie, nadzieja na ujrzenie aplikacji pisanych we Flash'u lub zawierających jego elementy na ekranie iPhone'a.

Konferencja meetBSD 2010 - do dzieła !

Od dnia 1 maja 2010 wszyscy miłośnicy systemów uniksowych, a w szczególności z rodziny BSD, mają możliwość zarejestrowania się na VII edycję konferencji z cyklu meetBSD. W tym roku impreza odbędzie się w Krakowie w dniach 2-3 lipca 2010. Podobnie jak w latach ubiegłych, swoje prelekcje poprowadzą osoby należące do oficjalnych grup tworzących systemy BSD, w tym również goście z zagranicy oraz przedstawiciele firm związanych lub współpracujących z opensource'owym środowiskiem deweloperskim. Tegoroczną nowością i uzupełnieniem właściwej części konferencyjnej będzie możliwość uzyskania certyfikatu BSD Certification Group. Konferencja meetBSD jest już cyklicznym spotkaniem poświęconym otwartym systemom uniksowym, głównie systemom z rodziny BSD, projektom i związanym z nimi ludziom, a także tematyce Open Source w ogólności. meetBSD w swoich założeniach ma charakter ściśle techniczny, główny nacisk kładziony jest na bardzo wysoką jakość zawartości merytorycznej. Konferencja dedykowana jest zarówno osobom zawodowo zajmującym się systemami BSD na co dzień, jak również osobom chcącym dopiero rozpocząć przygodę z prawdziwie wolnym światem BSD. Oprócz części merytorycznej, meetBSD to również świetna zabawa i towarzyskie spotkanie, na którym, jak podpowiada historia, wieczory są pełne wrażeń i atrakcji. Zachęcamy do jak najszybszej rejestracji, gdyż konferencja cieszy się ogromną popularnością, a ilość miejsc jest niestety ograniczona. Co roku organizatorzy zamykają wcześniej rejestrację z uwagi na brak miejsc.

Więcej szczegółów o samej konferencji:
http://www.meetBSD.org
Serdecznie wszystkich zapraszamy!
Organizatorzy i współorganizatorzy konferencji meetBSD 2010

Bezprzewodowe wideo Full HD w netbookach już w 2011 r.

Poznaliśmy kolejne szczegóły nt. platformy Cedar-Trail M, o której mieliśmy okazję pisać kilka dni temu. Tym razem mamy okazję poinformować Was, że Cedar-Trail M wspierać będzie funkcję Intel Wireless Display 2.0. Nowa platforma Intela dla netbooków wniesie wiele zmian. Pamiętajmy, że tegoroczna linia procesorów Atom N400 nie różni się wiele od wydanych 2 lata temu układów N200. Przede wszystkim Intel popełnił błąd, pozostawiając bez zmian wydajność i brak wsparcia odtwarzania obrazów wideo w jakości HD. W Cedar-Trail M drugi z problemów zostanie jednak rozwiązany, i to z nawiązką. Nowa generacja energooszczędnej platformy Intela nie tylko poradzi sobie z odtwarzaniem obrazów wideo wysokiej jakości, ale pozwoli nawet przesłać je bezprzewodowo do wyświetlacza. Warto przy tym pamiętać, że cały czas opisujemy tu wideo w jakości 1080p, które wspierane będzie dopiero przez drugą wersję technologii Wireless Display (pierwsza wspiera 720p i wykorzystywana jest przez niektóre notebooki z platformą Calpella). Miejmy tylko nadzieję, że do czasu premiery Cedar-Trail M, adaptery współpracujące z technologią Intel Wireless Display będą łatwiej dostępne niż obecnie, gdzie na rynku mamy zaledwie kilka takich rozwiązań (np. NETGEAR Push2TV Adapter).

12 000 instalacji Ubuntu Enterprise Cloud

Matt Asay z firmy Canonical poinformował, że dystrybucja Ubuntu Enterprise Cloud posiada już ponad dwanaście tysięcy wdrożeń, a każdego dnia przybywa obecnie 200 kolejnych. Liczone są aktywne instalacje, a nie przypadki, gdy ktoś testował dystrybucję przez kilka dni. Dystrybucja UEC jest dostępna od roku i pozwala na tworzenie prywatnych chmur obliczeniowych. Jest interesującym sposobem na optymalne wykorzystanie posiadanej infrastruktury oraz pozwala uniezależnić się od rozwiązań cloud computing takich firm jak Google, Amazon czy Microsoft. Canonical ma nadzieję, że zarobi na dostarczaniu wsparcia dla Ubuntu Enterprise Cloud, a także narzędziach służących do monitorowania i zarządznia. Canonical podkreśla, że przez pierwsze pięć lat działalności nie skupiał się na przynoszeniu zysków. Teraz następuje zmiana nastawienia na bardziej komercyjne.

System informowania o utrudnieniach na drodze – TMC, już w Polsce

Fińska firma Destia Traffic od maja 2010 uruchamia w Polsce system informacji o utrudnieniach drogowych – TMC. Nawigacje współpracujące z systemem TMC będą automatycznie aktualizowały trasę w oparciu o otrzymane dane. TMC z powodzeniem działa u naszych zachodnich sąsiadów (począwszy od Niemiec, kończąc na Hiszpanii). Dostarcza on informacje na temat utrudnień, a nawigacja wylicza nową trasę, omijając np. korek czy też wypadek. System TMC przesyła dane za pomocą fal radiowych. Firma Destia Traffic podpisała umowę z właścicielem stacji RMF-FM i to za ich pomocą będą nadawane informacje. Stacja RMF ma bardzo dobry zasięg w całej Polsce, więc dla kierowców jest to dobra informacja. By korzystać z systemu TMC, wymagana jest nawigacja potrafiąca odbierać fale radiowe, a także posiadać odpowiednie oprogramowanie. Dla użytkowników system ten wydaje się bezpłatny - zazwyczaj wliczony jest w koszt mapy lub urządzenia. Nie wymaga więc kupowania dodatkowego abonamentu.

Pierwsze informacje o Androidzie 2.2

Firma Google testuje już kolejną wersję swojego mobilnego systemu operacyjnego Android oznaczonego numerem 2.2. Najnowsza odsłona systemu, występującego także pod nazwą kodową Froyo, została już dostrzeżona w logach serwerów. Nieoficjalnie mówi się, że Android 2.2 będzie bazował na jądrze Linuksa w wersji 2.6.32, dzięki czemu ma lepiej wykorzystywać dostępną w telefonie pamięć RAM. Ponadto mobilny system Google dorobi się radia FM i nie będzie już miał problemów z ekranem dotykowym. Wśród praktycznych dodatków pojawi się także obsługa multikolorowych trackballi, które poprzez zmianę koloru będą informować użytkownika o różnych wydarzeniach. Z kolei deweloperów tworzących aplikacje dla Androida ucieszy z pewnością obecność kompilatora JIT, Flash Playera 10.1 oraz pełny dostęp do bibliotek OpenGL ES 2.0. Android 2.2 ujrzy światło dzienne prawdopodobnie 19 maja, przy okazji konferencji Google I/O. Nie jest obecnie jasne, które modele telefonów będą mogły być zaktualizowane do tej wersji systemu.

Konferencja Open Surce Day w Warszawie

Serdecznie zapraszamy na konferencję Open Source Day 2010, która odbędzie się 12 maja w Warszawie, w Pałacu Kultury i Nauki. Wysłuchaj wykładów światowych liderów otwartego oprogramowania, m.in. Red Hat, JBoss, EnterpriseDB i Zimbra! Dowiedz się więcej o trendach rozwojowych i wpływie Open Source na sytuację ekonomiczną firmy. W programie także wykłady poświęcone m.in. wirtualizacji, bazom danych oraz bezpieczeństwu z SELinuxem. Każdy uczestnik otrzyma kupon rabatowy na szkolenia certyfikacyjne Red Hat i JBoss. Największe w Polsce wydarzenie poświęcone technologiom Open Source zostało objęte patronatem Ministerstwa Gospodarki i osobiście Pana Premiera Waldemara Pawlaka, który otworzy konferencję swoim wykładem.
Udział w spotkaniu jest bezpłatny
Zapraszamy do rejestracji: *www.opensourceday.pl*

Z kim Google dzieli się swoją wiedzą ?

Nie jest żadną tajemnicą, że polskie oraz zagraniczne służby śledcze bardzo często zdobywają cenne informacje i dowody w wyniku współpracy z korporacjami z branży teleinformatycznej. Nic więc dziwnego, że internetowy gigant z Mountain View otrzymuje co roku od najrozmaitszych rządowych agencji tysiące nakazów udostępnienia danych zgromadzonych przez użytkowników jego rozlicznych usług. Co jednak najciekawsze, amerykański potentat zdecydował się na uruchomienie serwisu prezentującego statystyki tego typu interwencji z podziałem na poszczególne państwa.

Z serwisu Google government requests dowiemy się, jak kształtują się dla poszczególnych państw statystyki żądań kierowanych przez służby do firmy Google w sprawie usunięcia określonych treści lub też udostępnienia danych użytkowników poszczególnych usług. Na chwilę obecną dostępne są jedynie dane z drugiej połowy 2009 roku. Zawartość serwisu ma być jednak co pół roku aktualizowana o kolejne półroczne statystyki. Szczegółowe informacje na temat powstania samych statystyk oraz ich miarodajności można odnaleźć w dołączonym dokumencie FAQ. Google government requests zdradza nam, że w trakcie wspomnianego półrocza, polskie służby państwowe 86-krotnie zwróciły się do amerykańskiego giganta z prośbą o uzyskanie dostępu do prywatnych danych zgromadzonych przez określonych użytkowników. To jednak niewiele w stosunku do czołówki państw zainteresowanych danymi swych obywateli, np. Niemcy. Warto nadmienić, że nowy serwis udostępnia również informacje na temat żądań usunięcia określonych treści przechowywanych w ramach usług Google. Brak jednak takich danych (być może wynika to po prostu z braku tego rodzaju żądań) dla naszego kraju. W przypadku wielu państw, statystki te zostały wzbogacone również o informacje na temat procentowej ilości żądań spełnionych, wraz z rozbiciem na poszczególne usługi firmy Google. Z wpisu na oficjalnym blogu firmy Google możemy się dowiedzieć, że nowy serwis ma być swego rodzaju narzędziem do walki z rosnącymi zapędami wielu rządów do cenzurowania Internetu. Czy jednak rzeczywiście serwis Google government requests może się do tego w jakikolwiek sposób przyczynić?

Niepowodzenie akcji ostrzegającej przed phishingiem

Pod adresem ismycreditcardstolen.com stworzono stronę internetową, która ma ostrzegać internautów przed zagrożeniami atakami z wykorzystaniem phishingu. Niestety akcja edukacyjna tylko początkowo przebiegała zgodnie z planem. Pomysł był dobry. Strona miała udawać serwis sprawdzający, czy karta kredytowa, której numer został wpisany, nie została skradziona. Oczywiście podawanie numeru swojej karty na takiej stronie jest bardzo nierozsądne i właśnie uświadomienie tego internautom było zamierzeniem serwisu. Po wpisaniu danych karty pojawiała się strona wyjaśniająca jakie zagrożenie niesie lekkomyślne podawanie danych swojej karty i w jaki sposób stwierdzić, czy danej witrynie można zaufać. Był też odnośnik do strony Anti-Phishing Working Group. W sumie nie należałoby pisać w czasie przeszłym, gdyż strona działa nadal, jednak pojawił się problem. Edukacyjna witryna tak dobrze udawała stronę phishingową, że trafiła do filtrów antyphishingowych przeglądarek internetowych, w tym Firefoksa.

Skradziono kod uniwersalnego systemu uwierzytelniania Google

Podczas ataku określanego jako atak z wykorzystaniem Aurory lub Chińskiego włamania do Google i innych firm w Grudniu 2009 włamywaczom udało się ukraść kod źródłowy aplikacji umożliwiającej pojedynczą autoryzacje do prawie wszystkich usług webowych giganta, w tym kont poczty Gmail i aplikacji biznesowych. Zgodnie z publikacją "The New York Times" atak "Aurora" zaczął się od kliknięcia w link przesłany (IM) przez Microsoft Messenger do jednego z pracowników Google w Chinach, które doprowadziło do przejęcia komputera tego pracownika. Następnie z tego punktu wejściowego uzyskali dostęp do komputerów krytycznej grupy developerów w kwaterze Mountain View, gdzie uzyskali dostęp do wyżej wymienionego kodu źródłowego funkcjonującego pod nazwą "Gaia". Uzyskali również dostęp do innych wewnętrznych katalogów Google np "Moma", które zawierają informacje o działalności poszczególnych pracowników. Atakujący mieli zadziwiającą wiedzę o twórcach projektu "Gaia" . Mimo tego nie wygląda na to, aby uzyskali dostęp do haseł kont Gmail poszczególnych użytkowników.

Serwisy z linkami i hostingiem są legalne

Ostatnio organizacje mające chronić prawa autorskie wraz z mediami zaczęły kolejną antypiracką nagonkę. Tym razem pisze się o "nielegalnych" serwisach hostingowych i portalach z linkami. Tymczasem nielegalne są zazwyczaj jedynie działania użytkowników, a nie administratorów. To tak, jakby za pobicie kijem baseballowym obwiniać producenta pałki. Ponieważ w epoce Web 2.0 treści na portalach zazwyczaj tworzą użytkownicy i trudno wymagać od administratorów, by monitorowali to, co np. miliony użytkowników zamieszczają lub mogą zamieszczać w ich serwisach, wprowadzono w Polsce (jak i w wielu innych krajach na świecie, w tym w krajach UE i w Stanach Zjednoczonych) odpowiednie przepisy wyłączające odpowiedzialność administratorów (usługodawców udostępniających użytkownikom tylko pewną infrastrukturę) za to, co robią użytkownicy na Portalach. Oczywiście pod pewnymi warunkami. I tak, zgodnie z artykułem 14 ustawy o świadczeniu usług drogą elektroniczną, "nie ponosi odpowiedzialności za przechowywane dane ten, kto udostępniając zasoby systemu teleinformatycznego w celu przechowywania danych przez usługobiorcę, nie wie o bezprawnym charakterze danych lub związanej z nimi działalności, a w razie otrzymania urzędowego zawiadomienia lub uzyskania wiarygodnej wiadomości o bezprawnym charakterze danych lub związanej z nimi działalności niezwłocznie uniemożliwi dostęp do tych danych" (tzw. procedura "notice and takedown").
Z powyższego wynikają m. in. następujące konsekwencje:

1. Usługodawca nie musi prewencyjnie przeglądać czy filtrować zawartości dostarczanych przez usługobiorców;

2. Jest zwolniony z odpowiedzialności za dane przechowywane przez użytkowników – o ile działa zgodnie z powyższą procedurą;
3. Usługodawcy należy wskazać konkretne treści (a nie np. żądać usunięcia wszystkiego, co nielegalne – bo to by niweczyło założenie opisane w punkcie pierwszym.

Microsoft: Android narusza nasze patenty!

Horacio Gutierrez z Microsoftu oświadczył, że Android narusza wiele patentów firmy zarówno w dziedzinie interfejsu użytkownika jak i w "bebechach" systemu operacyjnego. To nic nowego. Android oparty jest przecież na Linuksie, który jak wiadomo narusza 235 patentów firmy z Redmond. Od czasu ogłoszenia tego w 2007 roku producent Windowsa nie wytoczył jednak żadnemu deweloperowi Linuksa czy firmie go wspierającej procesu związanego z własnością intelektualną. Podobnie może być teraz. Gutierrez potwierdził, że Microsoft nie planuje pozywać, chce jednak "rozwiązać problem", bo nie może być tak że "konkurencji żerują na naszych innowacjach". Co ciekawe, informacja o naruszaniu patentów Microsoftu przez Androida pojawiła się tuż po innym niusie, na temat umowy patentowej między Microsoftem a HTC, która ma roztoczyć nad tą drugą firmą wachlarz opieki przed Apple (por. Apple oskarża HTC o naruszenia patentów). Microsoft ma zapewne nadzieję, że strach przed naruszaniem patentów odwróci widoczny od dłuższego czasu trend wybierania przez dystrybutorów systemu Android i rezygnowania z Windows Mobile. Przytakuje temu analityk Gartnera, Ken Dulaney, który uważa, że Google nie posiada wystarczającego portfolio patentowego, aby ochronić HTC przed Apple.

Firma HP kupuje firmę Palm za 1,2 miliarda dolarów.

HP zapowiedziało dzisiejszego wieczora, że do końca lipca sfinalizuje transakcję zakupu firmy Palm, opiewająca na kwotę 1,2 miliarda dolarów. Palm, mający od dłuższego czasu problemy, jest producentem między innymi mobilnego systemu operacyjnego Web OS oraz smartfona Pre. HP zapłaci 5,7 dolara za każdą akcję Palma. Plany największego producenta komputerów zakładają wykorzystanie systemu WebOS do poprawy swojej pozycji na błyskawicznie rozwijającym się rynku urządzeń mobilnych i smartfonów. Gigant z Palo Alto zamierza rozwinąć swoje skrzydła w zakresie wielozadaniowości oraz dzielenia się aktualnymi informacjami poprzez aplikacje.

Będzie App Store dla Mac OS X?

Deweloperzy dostarczający aplikacje dla systemu Mac OS X są zaniepokojeni - oficjalna strona firmy Apple, na której mogli umieszczać swoje programy, najprawdopodobniej zawiesiła działanie. Czy jej miejsce zajmie e-sklep dla aplikacji? Strona Apple Downloads to miejsce, gdzie deweloperzy mogą zamieszczać swoje aplikacje dla systemu Mac OS X. Oprócz programów internauci mogą pobierać widżety, ikonki czy dodatkowe sterowniki. Oczywiście, dostępne są również aplikacje firmy Apple, takie jak przeglądarka Safari, program Aperture do obróbki zdjęć albo iTunes. Dodatkowo z Apple Downloads można pobierać aktualizacje systemu Mac OS X i najnowsze wersje pakietów bezpieczeństwa. Jednak strona nie była aktualizowana od 26 marca. Brakuje nowych programów, a także najnowszej aktualizacji Mac OS X 10.6.3. Pojawiły się przypuszczenia, że Apple może zupełnie zawiesić działalność strony. Byłaby to niemiła wiadomość, bo dzięki niej wielu producentów aplikacji dla Mac OS X wypromowało swoje produkty. Zdaniem serwisu ArsTechnica powodów takiego zachowania może być kilka. Jak przypuszczają niektórzy deweloperzy, być może Apple przygotowuje się do otwarcia e-sklepu na kształt App Store, gdzie udostępnianoby programy dla komputerów Mac. Tyle że z takiego rozwiązania wiele osób nie byłoby zadowolonych. W App Store to Apple decyduje, jakie aplikacje zostają wprowadzone do sklepu. Jeśli podobnie miałoby wyglądać z programami dla Mac OS X, wielu deweloperów nie zostałoby dopuszczonych do sprzedaży swoich produktów. Oczywiście, mogliby nadal udostępniać aplikacje w standardowy sposób, straciliby jednak możliwość ich promowania w e-sklepie. Apple, jak dotąd, nie podał oficjalnych informacji na temat przyszłości swojej strony.

YouTube rozszerza ofertę filmów na żądanie

YouTube znacząco zwiększył ilość tytułów dostępnych w stworzonej przez siebie wypożyczalni wideo, dzięki której za niewielką opłatą można obejrzeć jeden z kilkudziesięciu dostępnych w bazie filmów. Jest to ważny krok w stronę popularyzacji usług wideo na żądanie. Obecnie jednak wypożyczalnia YouTube dostępna jest niestety wyłącznie na terenie USA. YouTube Store pozwala na wypożyczenie wybranego filmu na okres od 24 do 72 godzin. Cena jest uzależniona od konkretnego tytułu i waha się od 0,99 do 3,99 dolarów. Wśród dostępnych w bazie filmów znalazło się wiele głośnych, hollywoodzkich produkcji (Piła, Pan życia i śmierci), japońskich anime, filmów opisujących ciekawe miejsca oraz produkcji naukowych i edukacyjnych. Choć pierwsze próby z płatnym wypożyczaniem wideo miały miejsce w styczniu, dopiero teraz YouTube zdecydował się dodać do swojego sklepu większą liczbę tytułów. Google chwali się, że jego usługa weszła właśnie w etap intensywnego rozwoju i przy jej tworzeniu uczestniczy blisko 500 partnerów. Komentatorzy podkreślają jednak, że YouTube Store wkracza na dość zatłoczony rynek i przyjdzie mu konkurować z podobnymi usługami świadczonymi m.in. przez Netflix i Amazon. Wiele zależy od tego, czy firmie uda się rozszerzyć dostępność wypożyczalni na tyle, by mogli z niej korzystać użytkownicy spoza USA. W wielu krajach rynek płatnego, strumieniowego udostępniania filmów jest jeszcze dość młody i wypożyczalni Google łatwo byłoby odnieść tam sukces. Obecnie firma nie zdradza, w jakim kierunku zamierza rozwijać YouTube Store.

Polscy wydawcy idą na wojnę z Chomikiem

Wydawcy książek skarżą się na praktyki serwisu Chomikuj.pl, w którym jest pełno nielegalnych kopii książek – w tym „Zaginiony symbol", najnowsza powieść Dana Browna, autora „Kodu Leonarda da Vinci". Publikację, na którą polscy internauci czekali ponad cztery lata, tylko z jednego konta pobrano ponad sześć tysięcy razy. Wszystkich użytkowników Chomikuj.pl jest prawie cztery miliony. Łącznie w polskich serwisach, które oficjalnie działają jako zapasowe wirtualne dyski twarde, znaleźć można około dziesięciu tysięcy tytułów. Wydawnictwa uważają, że administratorzy stron łamią prawo. Zasypują „Chomika" skargami i zgłaszają sprawy organom ścigania. Problemem zajął się też Bartłomiej Roszkowski, właściciel serwisu Nexto.pl sprzedającego e-booki i książki w wersji audio. Kilka dni temu wysłał do swoich kontrahentów list. Napisał w nim między innymi: „Zwracam się do Państwa z prośbą, aby zacząć aktywnie walczyć z serwisami udostępniającymi nielegalnie Państwa treści w Internecie. Chcielibyśmy w pierwszej kolejności skierować nasze działania przeciwko serwisowi Chomikuj.pl". Roszkowski powiedział też „Rzeczpospolitej": „Ktoś wreszcie musiał to głośno powiedzieć: Chomikuj.pl, Wiaderko.pl, Peb.pl czy inne podobnie działające serwisy stają się prawdziwą plagą dla wydawców". Ci nieoficjalnie przyznają, że tracą z powodu „piratów" kilka milionów złotych rocznie. Nie biorą oczywiście pod uwagę tego, że większość osób pobierających książki z Sieci nie kupiłaby papierowych wydań. Po prostu nie byłoby ich na nie stać. Straty, o których mówią wydawcy, są na pewno przesadzone, a nawet w pewnym stopniu wydumane. Piotr Hałasiewicz, rzecznik Chomikuj.pl, zapewnia tymczasem, że jego firma reaguje na skargi i usuwa naruszające prawo treści. Nie stosuje jednak prewencyjnej cenzury. Każdy, kto ma jakiekolwiek pojęcie o skali funkcjonowania współczesnych serwisów WWW, musi przyznać, że kontrolowanie wszystkich plików jest po prostu niemożliwe.

Internauci coraz częściej odwiedzają Facebooka

Firma ComScore opublikowała statystyki dotyczące odwiedzin Facebooka. Okazuje się, że popularny serwis społecznościowy jest... bardzo popularny. Średnio w ciągu jednego miesiąca notuje 500 mln unikalnych odwiedzin. Z opublikowanych materiałów, które cytowane są przez TechCrunch, wynika, że w marcu Facebooka odwiedziło 500 mln osób - to jest o 64% więcej, niż w analogicznym okresie w zeszłym roku. Tylko w lutym tego roku w Facebooku zarejestrowało się 22 mln nowych użytkowników. Z kolei według statystyk Facebooka, w serwisie zarejestrowanych jest obecnie ponad 400 mln osób, z czego 100 mln łączy się za pośrednictwem telefonów komórkowych i smartfonów. Prawie 50% spośród użytkowników korzystających z serwisu codziennie loguje się do swojego konta. Różnica między oficjalnymi statystykami Facebooka a tymi podanymi przez ComScore wynika najprawdopodobniej z faktu, że serwis coraz częściej odwiedzają osoby niezarejestrowane na jego stronach. Facebook chce jeszcze bardziej zwiększyć swoją popularność. Podczas konferencji F8 dla deweloperów, która miała miejsce wczoraj, zapowiedziano m.in. rozszerzenie funkcji dostępnych w serwisie na cały Internet. Szef firmy, Mark Zuckerberg, stwierdził, że chciałby, aby internauci mogli korzystać z dodatków społecznościowych podczas surfowania po Sieci. Budujemy Sieć, gdzie społeczność jest domyślna – powiedział.

Prawa autorskie do Uniksa: SCO chce nowego wyroku.

CO Group chce doprowadzić do kolejnego procesu, który miałby rozstrzygnąć, do kogo należą prawa autorskie do Uniksa. W lecie 2007 roku sąd uznał, że ich właścicielem jest Novell. Po wniesieniu odwołania przez SCO sąd apelacyjny zadecydował, że sprawa musi być rozstrzygnięta przez ławę przysięgłych. Ta z kolei przed kilkoma tygodniami potwierdziła prawa Novella. Jak donosi serwis Groklaw, grupa SCO złożyła do sądu wniosek, w którym domaga się uchylenia wyroku ławy przysięgłych i przyznania SCO praw do Uniksa. Proponuje też przeprowadzenie nowego procesu, twierdząc, że ława przysięgłych źle zrozumiała pytanie, czy prawa autorskie zostały przekazane na rzecz SCO na skutek zawarcia umowy z Novellem.

Część I. Programowanie w C++ i Qt pod Ubuntu

Konfiguracja środowiska programistycznego Qt SDK i Eclipse oraz stworzenie prostej aplikacji okienkowej

W części pierwszej artykułu zajmiemy się konfiguracją środowiska programistycznego C++ Qt SDK, Qt Creator i Qt Eclipse Integration jako alternatywnego rozwiązania. Stworzymy również pierwszą prostą aplikację okienkową, korzystając z biblioteki Qt 4.6.

Artykuł ten przeznaczony jest w głównej mierze dla początkujących programistów C++ chcących tworzyć aplikacje komputerowe na systemie Linux w oparciu o dystrybucję Ubuntu, którą można pobrać ze strony *www.ubuntu.pl* – nazwa aktualnej polskiej wersji Ubuntu to Karmelkowy Koliberek. Artykuł został podzielony na kilka części takich jak: „Środowisko programistyczne Qt SDK, Qt Creator", „Integracja Qt z Eclipse" oraz „Pierwsza aplikacja w Qt". Serdecznie zapraszam do artykułu.

Środowisko programistyczne Qt SDK, Qt Creator

W pierwszej kolejności musimy pobrać odpowiednie pakiety instalacyjne pasujące do Twojego systemu. Wybieramy między pakietami dla 64 lub 32 bitowych systemów, w zależności od tego, jaką wersję Ubuntu posiadasz zainstalowaną na swoim komputerze.

Ze strony *qt.nokia.com/downloads* z zakładki *LGPL* pobieramy odpowiednią wersję *Qt SDK*, w skład której wchodzi również *Qt Creator* – doskonale zintegrowane IDE dla biblioteki *Qt*. Następnie, aby zainstalować *Qt SDK*, musimy nadać odpowiednie uprawnienia dla pliku instalacyjnego z końcówką **.bin*, czyli w naszym przypadku *qt-sdk-linux-x86_64-opensource-2010.02.bin*. Możemy do tego celu użyć Terminala (*Programy/Akcesoria/Terminal*) i wydać polecenie:

```
lukasz@IS:~/Pobrane$ chmod +x qt-sdk-linux-x86_64-
                     opensource-2010.02.bin
```

lub też po prostu skorzystać z graficznego interfejsu użytkownika dostępnego z Ubuntu: wtedy należy kliknąć prawym klawiszem myszy na pliku **.bin*, wybrać właściwości i w zakładce uprawnienia zaznaczyć pole *Zezwolić na wykonanie pliku jako programu*. Wpisujemy komendę w konsoli `./qt-sdk-linux-x86_64-opensource-2010.02.bin` i proces instalacji *Qt SDK* się rozpocznie.

Uwaga przed instalacją Qt SDK

Przed rozpoczęciem procesu instalacji Qt SDK należy wykonać następujące polecenia w konsoli:

```
lukasz@IS:~/Pobrane$ sudo apt-get install libglib2.0-
                     dev libSM-dev libxrender-dev
                     libfontconfig1-dev libxext-dev
lukasz@IS:~/Pobrane$ sudo apt-get install libgl-dev
                     libglu-dev
```

Jeśli przy podaniu powyższego polecenia otrzymasz podobną informację jak poniżej:

```
lukasz@IS:~/Pobrane$ sudo apt-get install libgl-dev
                     libglu-dev
Czytanie list pakietów... Gotowe
```

```
Budowanie drzewa zależności
Odczyt informacji o stanie... Gotowe
Pakiet libgl-dev jest pakietem wirtualnym zapewnianym
                    przez:
  nvidia-glx-96-dev 96.43.13-0ubuntu6
  nvidia-glx-185-dev 185.18.36-0ubuntu9
  nvidia-glx-173-dev 173.14.20-0ubuntu5
  libgl1-mesa-dev 7.6.0-1ubuntu4
Należy jednoznacznie wybrać jeden z nich do instalacji.
E: Pakiet libgl-dev nie ma kandydata do instalacji
```

to w takim przypadku należy wybrać odpowiedni pakiet do instalacji zamiast *libgl-dev*, czyli w moim przypadku będzie to *nvidia-glx-185-dev.* Po udanej instalacji wymaganych pakietów przechodzimy do instalacji *Qt SDK*.

Proces instalacji Qt SDK

- Akceptujemy warunki licencji i klikamy *next*.
- Wybieramy katalog instalacji *Qt SDK* – możemy pozostawić domyślny, czyli np. w moim przypadku jest to */home/lukasz/qtsdk-2010.02*.
- W następnym oknie zaznaczamy opcję *Qt Creator* (domyślnie powinno być zaznaczone) i *Qt Development Libraries.*
- Akceptujemy aż do uruchomienia instalatora. Jako że *Qt SDK* waży około 440MB, to proces instalacji może potrwać 2-3 minuty, w zależności od szybkości komputera.
- Po udanej instalacji możemy już uruchomić *Qt Creator.*

Integracja Qt z Eclipse

Ze strony *http://www.eclipse.org/downloads/* pobieramy *Eclipse IDE for C/C++ Developers* dla systemu *Linux* – mamy do wyboru wersję 32 i 64 bitową. Następnie uruchamiamy *eclipse*, wybieramy *Help/Install New Software* i jako nową stronę wpisujemy *http://download.eclipse.org/tools/cdt/releases/galileo,* instalujemy *CDT*. Pobieramy ze strony *http://qt.nokia.com/developer/eclipse-integration qt-eclipse-integration* - mamy do wyboru wersję 32 i 64 – rozpakowujemy archiwum do katalogu *Eclipse,* nadpisując go. Musimy również zainstalować *Qt SDK for Open Source C++ development* dla systemu *Linux* ze strony *http://qt.nokia.com/download/sdk-linux-x11-32bit-cpp* lub *http://qt.nokia.com/download/sdk-linux-x11-64bit-cpp*, w zależności od architektury Twojego systemu. Ostatecznie uruchamiamy *Eclipse* z opcją *-clean*, co zapewni wyczyszczenie *cachu Eclipse*.

Zakończyliśmy proces instalacji *Qt SDK* lub *Qt z Eclipse*. W dalszej części artykułu będziemy tworzyć prostą aplikację, używając środowiska *Qt Creator* dostarczonego razem z *Qt SDK*. Uruchomiamy więc *Qt Creator* (po instalacji powinien być widoczny skrót na pulpicie *Ubuntu*).

Pierwsza aplikacja w Qt

Założenia

Zaczynając tworzenie aplikacji komputerowej, powinnyśmy rozpocząć od zaplanowania aplikacji. Możemy to wykonać przy pomocy specjalnego programu lub po prostu na kartce papieru. Ważne jest, abyś sobie wizualnie uzmysłowił, co chciałbyś uzyskać. Przykład bardzo prostego planu możesz zobaczyć na Rysunku 1.

Listing 1. *Zawartość pliku mainwindow.h po utworzeniu nowego projektu*

```
#ifndef MAINWINDOW_H
#define MAINWINDOW_H

#include <QMainWindow>

namespace Ui {
    class MainWindow;
}

class MainWindow : public QMainWindow {
    Q_OBJECT
public:
    MainWindow(QWidget *parent = 0);
    ~MainWindow();

protected:
    void changeEvent(QEvent *e);

private:
    Ui::MainWindow *ui;
};

#endif // MAINWINDOW_H
```

Listing 2. *Zawartość pliku main.cpp po utworzeniu nowego projektu*

```
#include <QtGui/QApplication>
#include "mainwindow.h"

int main(int argc, char *argv[])
{
    QApplication a(argc, argv);
    MainWindow w;
    w.show();
    return a.exec();
}
```

Nasza aplikacja będzie składała się z menu, głównego okna aplikacji i status bar. Struktura menu będzie następująca:

- Plik
  - Wczytaj zdjęcie (ctrl+w)
  - Separator (linia oddzielająca)
  - Zakończ (ctrl+q)
- Pomoc
  - O programie

Główne okno aplikacji będzie zawierało obszar na zdjęcie, informacje o zdjęciu. Natomiast status bar będzie prezentował dodatkowe informacje w zależności od wykonywanych akcji. Opcja *Wczytaj zdjęcie* będzie mogła wczytać do programu zdjęcie typu *JPG* i żadne inne. W oknie głównym po wczytaniu pliku pojawi się zdjęcie z suwakami, jeśli jego wielkość będzie większa niż zdefiniowany obszar sceny oraz szczegółowe informacje takie jak szerokość i wysokość. Opcja *zakończ* będzie powodować wyjście z programu, natomiast opcja *O programie* wyświetli okienko dialogowe z informacją o wersji programu i autorze.

Listing 3. *Zawartość pliku mainwindow.cpp po utworzeniu nowego projektu*

```
#include "mainwindow.h"
#include "ui_mainwindow.h"

MainWindow::MainWindow(QWidget *parent) :
    QMainWindow(parent),
    ui(new Ui::MainWindow)
{
    ui->setupUi(this);
}

MainWindow::~MainWindow()
{
    delete ui;
}

void MainWindow::changeEvent(QEvent *e)
{
    QMainWindow::changeEvent(e);
    switch (e->type()) {
    case QEvent::LanguageChange:
        ui->retranslateUi(this);
        break;
    default:
        break;
    }
}
```

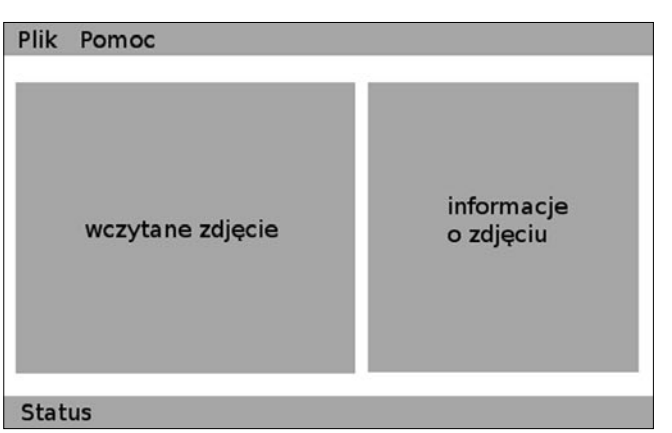
Tworzenie projektu w Qt Creator

Gdy już mamy opisany pomysł aplikacji, możemy zabrać się za programowanie. W tym celu uruchamiamy Qt Creator i tworzymy nowy projekt, wybierając z menu *Plik/Nowy plik lub projekt*, a następnie w oknie wyboru wskazujemy na *Projekty* i *Aplikacja GUI Qt4*. W kolejnym oknie podajemy nazwę projektu, np. *WczytajZdjęcie*, i wybieramy katalog projektu. Dalej mamy możliwość wyboru kilku różnych modułów, które możemy włączyć do projektu, jak np.: QtCore, QtGui, QtNetwork, QtOpenGL, QtSql, QtScript, QtScriptTools, QtSvg, QtWebKit, QtXml, QtXmlPatterns, Phonon, QtMultimedia, Qt3Support, QtTest, QtDBus. Dla naszych celów wystarczą tylko dwa moduły: QtCore i QtGui. Opisem możliwości poszczególnych modułów zajmiemy się w następnym artykule. Na razie skupimy się na tych dwóch modułach, aby przedstawić podstawy projektowania aplikacji w Qt, tak abyś mógł sam zacząć już eksperymentować w oczekiwaniu na kolejny numer Linux+. W następnym oknie możemy ustawić nazwę klasy podstawowej, niech zostanie MainWindow i QmainWindow. Ogólnie pozostawiamy domyślne ustawienia i przechodzimy dalej, a następnie klikamy *zakończ*, co spowoduje stworzenie projektu aplikacji.

Jak pewnie zauważyłeś, zostaliśmy przełączeni od razu na zakładkę *Edycja*. W projekcie *WczytajZdjecie* pojawiły się trzy katalogi: *Formularze*, *Nagłówki* i *Źródła*. W katalogu *Formularze* przechowywane są formatki, u nas *mainwindow.ui*. Katalog *Nagłówki* zawiera pliki nagłówkowe *mainwindow.h* (Listing 1). W katalogu *Źródła* zawarte są pliki źródłowe, właściwie tutaj będziemy programować zachowanie naszej aplikacji. Obecnie są dwa pliki: *main.cpp* (Listing 2) i *mainwindow.cpp* (Listing 3).

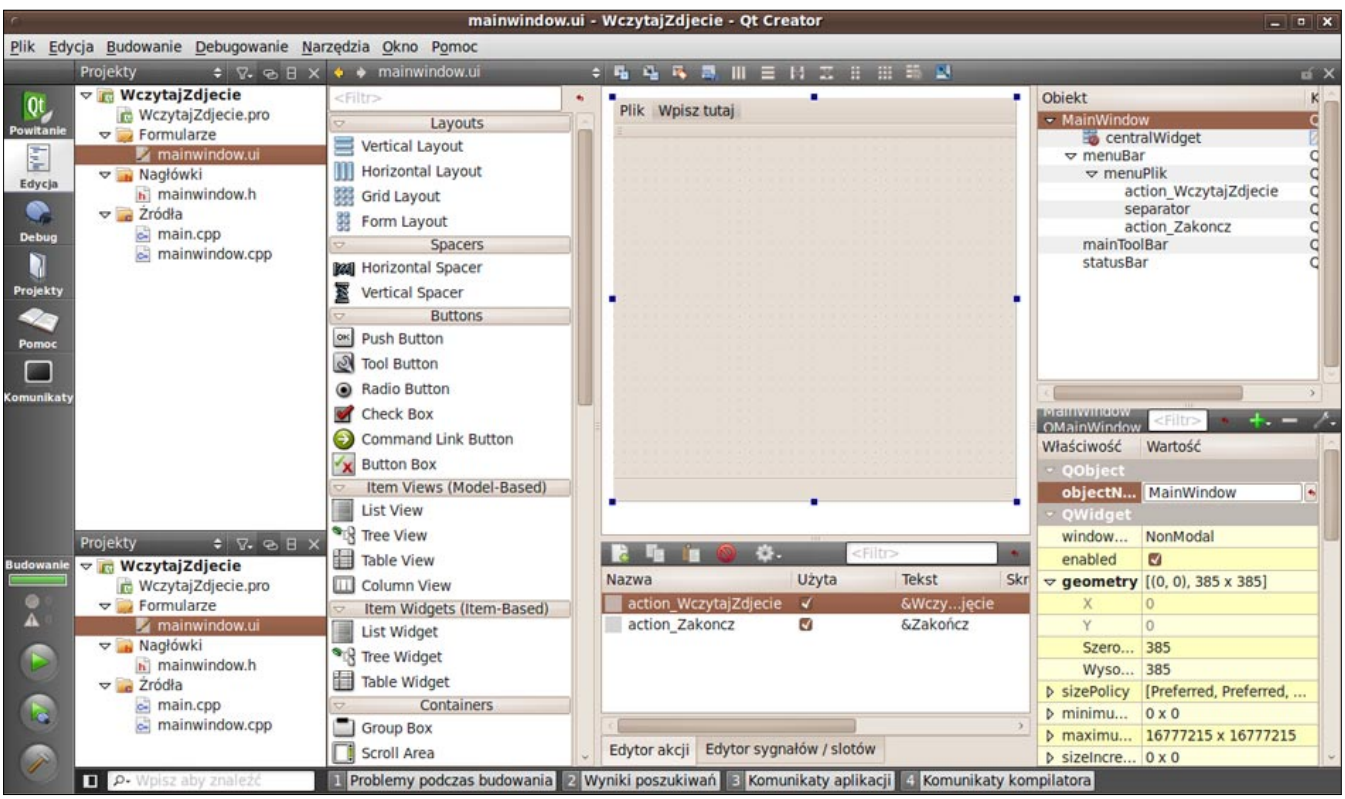
Projektowanie graficznego interfejsu użytkownika

Z katalogu Formularze wybieramy mainwindow.ui (Rysunek 2). Pojawi się okno edycji formatki *MainWindow*. Aby stworzyć strukturę menu, należy klik-



Rysunek 1. *Przykład prostego planu aplikacji komputerowej*

nąć w miejscu *Wpisz tutaj* i wpisać *Plik*, a następnie dodać *&Wczytaj plik*, separator i *&Zakończ*. Znaczek *&* oznacza możliwość wyboru opcji menu poprzez wciśnięcie *W* lub *Z* w celu wywołania danej akcji. Zostały utworzone dwie akcje *action_Wczytaj_plik* i *action_Zako_cz*. Jednakże my te nazwy zmienimy na troszkę ładniejsze. Klikamy w menu rozwijalnym opcję *Wczytaj zdjęcie* i w oknie *QAction* odnajdujemy sekcję *QObject* i pole *objectName*, pole to zmienimy na *action_WczytajZdjecie*. Podobnie w przypadku akcji *Zakończ*, zamieniamy na *action_Zakoncz*. Następnie przypiszemy tym opcjom skróty klawiaturowe. W tym celu należy wybrać z menu *Wczytaj zdjęcie* i w oknie *QAction* odszukujemy opcję *shortcut*, klikamy w pustym polu i wciskamy kombinację klawiszy *CTRL+W*. Podobnie postępujemy w przypadku akcji *Zakończ* (*CTRL+Q*). Dodajemy również główną opcję *Pomoc*, a w niej *O programie*. Zmieniamy również na-



Rysunek 2. *Widok edycji formatki QMainWindow*

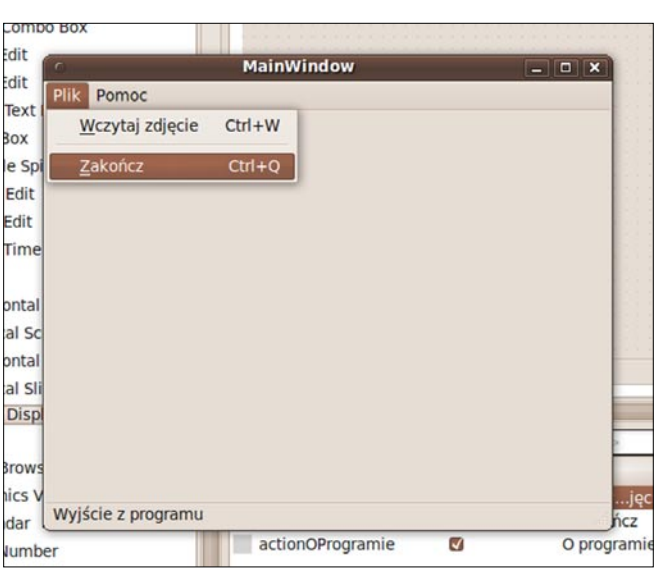
Listing 4. *Metoda WczytajZdjecie_clicked()*

```
void MainWindow::WczytajZdjecie_clicked()
{
    QString fileName = QFileDialog::getOpenFileName(this,"","","Dopuszczalne formaty (*.jpg)");

    QGraphicsScene *scene = new QGraphicsScene();
    QPixmap pix;

    pix.load(fileName);
    scene->addPixmap(pix);

    this->ui->graphicsView->setScene(scene);
    this->ui->graphicsView->show();

    this->ui->labelSzerokosc->setText(QString::number(pix.width()));
    this->ui->labelWysokosc->setText(QString::number(pix.height()));
}
```

zwę obiektu z *action_O_programie* na *action_OProgramie*. Dodamy jeszcze podpowiedzi *StatusTip* do tych opcji, które będą się wyświetlać w trakcie wybierania na listwie *Status Bar*. Przykładowo dla opcji *Wczytaj zdjęcie* odnajdujemy w oknie *QAction* opcję *statusTip*, klikamy na puste pole i wpisujemy *Wczytaj zdjęcie* do programu. Dla opcji *Zakończ* wpisujemy *Wyjście z programu*. Dla ostatniej opcji *O Programie* wpisujemy *Informacje o programie*.

Teraz usuniemy niepotrzebny w naszej aplikacji pasek narzędzi toolBar. W tym celu kliknij na pasku znajdującego się na formatce aplikacji prawym klawiszem myszy i wybierz z menu kontekstowego opcję Usuń pasek narzędzi toolBar. Kolejnym krokiem będzie ustawienie minimalnej szerokości i wysokości okna aplikacji. Zaznaczamy formatkę lewym klawiszem myszy i w oknie *QmainWindow* w sekcji *QWidget* odnajdujemy pole *Szerokość* wpisujemy 485, a w polu *Wysokość* 385. Teraz możemy uruchomić naszą aplikację, aby zobaczyć, jak będzie wyglądała (CTRL+R lub Budowanie/Uruchom). Zobacz Rysunek 3, na którym przedstawiony jest dotychczasowy efekt naszej pracy. Możemy jeszcze zmienić tytuł okna na np. Wczytaj zdjęcie. W tym celu znajdź opcję windowTitle i zmień wartość tego pola.

W części głównej aplikacji dodamy Display Widget o nazwie *Graphics View*. Kliknij, przeciągnij i upuść na formatce w dowolnym miejscu (domyślna nazwa obiektu to *graphicsView*). Następnie w oknie *QGraphicsView* sekcji *GWidget* ustawiamy pole *geometry*, pole *X* ustawiamy na *10*, a pole *Y* na *20*. Pole *Szerokość* ustawiamy na *310*, a *Wysokość* na *300*. Nad Widgetem *Graphics View* dodajemy Widget *Label* o treści *Zdjęcie:*. Możemy również zmienić kolor tego Widgetu poprzez dodanie koloru w oknie *QLabel* sekcji *QWidget* polu *styleSheet*. Klikamy w ikonkę trzech kropek, a następnie w nowym oknie z listy rozwijalnej *Dodaj kolor* wybieramy *background* i ustawiamy interesujący nas kolor. Dodajmy również następny *Widget* typu *Label* na wysokości pierwszego, ale w wolnym miejscu po prawej (zobacz na Rysunku 4). Dodamy jeszcze 4 Widgety typu *Label*. Dwa widoczne i dwa puste dla wartości pobieranych ze zdjęcia. Będą to *Szerokość, Wysokość* i obok



Rysunek 3. *Widok aplikacji z ustawionym menu*

Listing 5. *Metoda Zakoncz_clicked() i OProgramie_clicked()*

```
void MainWindow::Zakoncz_clicked()
{
    QApplication::closeAllWindows();
}

void MainWindow::OProgramie_clicked()
{
    QTextCodec::setCodecForCStrings(QTextCodec::
                    codecForName("utf8"));
    QMessageBox::information(this, "Wczytaj
                    zdjęcie","Prosta aplikacja w
                    Qt\n\nautor: Łukasz Klejnberg,
                    IdealSolutions.pl");
}
```

Listing 6. *Zmiany w pliku mainwindow.h*

```
#ifndef MAINWINDOW_H
#define MAINWINDOW_H

#include <QMainWindow>

namespace Ui {
    class MainWindow;
}

class MainWindow : public QMainWindow {
    Q_OBJECT
public:
    MainWindow(QWidget *parent = 0);
    ~MainWindow();

protected:
    void changeEvent(QEvent *e);

private slots:
    void WczytajZdjecie_clicked();
    void Zakoncz_clicked();
    void OProgramie_clicked();

private:
    Ui::MainWindow *ui;
};

#endif // MAINWINDOW_H
```

Listing 7. *Zmiany w pliku mainwindow.cpp*

```
#include "mainwindow.h"
#include "ui_mainwindow.h"
#include <QFileDialog>
#include <QMessageBox>
#include <QTextCodec>
MainWindow::MainWindow(QWidget *parent) :
    QMainWindow(parent),
    ui(new Ui::MainWindow)
{
    ui->setupUi(this);
    connect(ui->action_WczytajZdjecie, SIGNAL(triggered()), this, SLOT(WczytajZdjecie_clicked()));
    connect(ui->action_Zakoncz, SIGNAL(triggered()), this, SLOT(Zakoncz_clicked()));
    connect(ui->actionOProgramie, SIGNAL(triggered()), this, SLOT(OProgramie_clicked()));
}
MainWindow::~MainWindow()
{
    delete ui;
}
void MainWindow::changeEvent(QEvent *e)
{
    QMainWindow::changeEvent(e);
    switch (e->type()) {
    case QEvent::LanguageChange:
        ui->retranslateUi(this);
        break;
    default:
        break;
    }
}
void MainWindow::WczytajZdjecie_clicked()
{
    QString fileName = QFileDialog::getOpenFileName(this,"","","Dopuszczalne formaty (*.jpg)");
    QGraphicsScene *scene = new QGraphicsScene();
    QPixmap pix;
    pix.load(fileName);
    scene->addPixmap(pix);

    this->ui->graphicsView->setScene(scene);
    this->ui->graphicsView->show();
    this->ui->labelSzerokosc->setText(QString::number(pix.width()));
    this->ui->labelWysokosc->setText(QString::number(pix.height()));
}
void MainWindow::Zakoncz_clicked()
{
    QApplication::closeAllWindows();
}
void MainWindow::OProgramie_clicked()
{
    QTextCodec::setCodecForCStrings(QTextCodec::codecForName("utf8"));
    QMessageBox::information(this, "Wczytaj zdjęcie","Prosta aplikacja w Qt\n\nautor: Łukasz Klejnberg,
                    IdealSolutions.pl");
}
```

nich *labelSzerokosc, labelWysokosc*, które ustawiamy na puste (zobacz na Rysunku 4).

Dodamy teraz możliwość wczytania pliku graficznego o formacie **.jpg* do Widgetu *graphicsView*. Przejdźmy do edycji pliku *mainwindow.h.* W klasie *MainWindow* należy dodać:

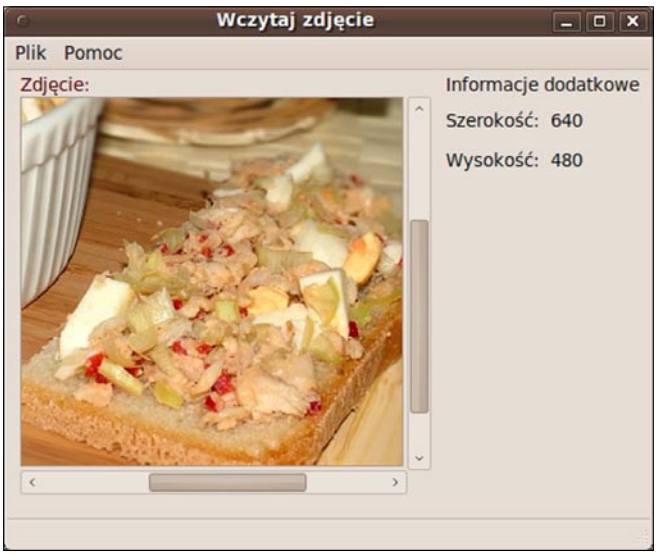
```
private slots:
   void: WczytajZdjecie_clicked();
```

Następnie przechodzimy do edycji pliku *mainwindow.cpp,* gdzie dodamy obsługę wczytania zdjęcia oraz jego szerokości i wysokości. W metodzie *MainWindow* dodajemy sygnał i slot:

```
connect(ui->action_WczytajZdjecie, SIGNAL(triggered()),
                  this, SLOT(WczytajZdjecie_
                  clicked()));
```

Musimy teraz dodać metodę `WczytajZdjecie_clicked()` (Listing 4).

Wiersz zawierający `QString fileName = QFileDialog::getOpenFileName(this,"","","Dopuszczalne formaty (*.jpg)");` deklaruje obiekt `fileName`, który ma ograniczone możliwości wczytywania plików. W naszym przypadku filtrowane są wszystkie pliki oprócz plików *.jpg. Następnie deklarujemy scenę i wczytujemy zdjęcie na scenę. Ostatecznie przy pomocy `this->ui->graphicsView->show();` wyświetlamy zdjęcie. Pozostało jeszcze ustawić szerokość i wysokość etykiet `labelSzerokosc` i `labelWysokosc`. Jest to bardzo proste, jednakże przed zapisaniem danych liczbowych do pola typu string musimy wykonać drobne rzutowanie dzięki



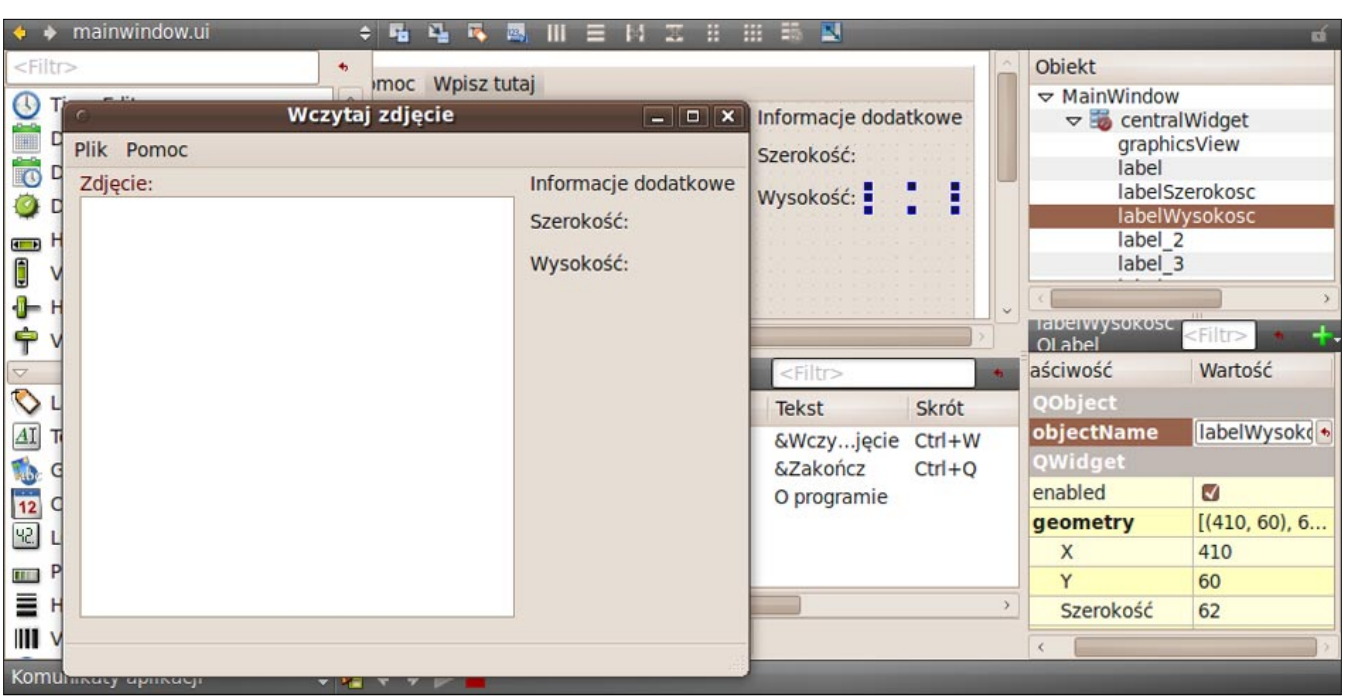
Rysunek 5. *Gotowa aplikacja Wczytaj Zdjęcie*

metodzie `number QString::number(pix.width())`. Właściwie aplikacja jest już gotowa. Musimy dodać jeszcze tylko obsługę akcji *Zakończ* oraz *O programie.* Dodamy dwa nowe sloty w pliku *mainwindow.h*:

```
void Zakoncz_clicked();
void Oprogramie_clicked();
```

Następnie w pliku *mainwindow.cpp* dodajemy dwa sygnały i sloty:

```
connect(ui->action_Zakoncz, SIGNAL(triggered()), this,
                  SLOT(Zakoncz_clicked()));
connect(ui->actionOProgramie, SIGNAL(triggered()),
                  this, SLOT(OProgramie_clicked()));
```



Rysunek 4. *Zawartość głównego okna*

Przydatne adresy

- *http://qt.nokia.com* – serwis www biblioteki *Qt*;
- *http://qt.nokia.com/doc/4.6/index.html* – dokumentacja biblioteki *Qt*;
- *http://doc.qt.nokia.com/4.6/tutorials.html* – przykładowe tutoriale;
- *http://cartan.cas.suffolk.edu/oopdocbook/opensource/* – książka wersji online – *Introduction to Design Patterns in C++ with Qt4*;
- *http://www.pdf-search-engine.com/qt4-pdf.html* – różne przydatne pliki w pdf dotyczące biblioteki *Qt*;

Dodamy teraz dwie metody obsługujące te dwa zdarzenia (Listing 5).

W metodzie `OProgramie_clicked()` została użyta metoda information z klasy `QMessageBox`. Powoduje to wyświetlenie okienka informacyjnego z krótką informacją o programie. Na Listingu 6 i 7 widoczne są pliki *mainwindow.h* i *mainwindow.cpp* po zmianach, które przed chwilą wprowadziliśmy.

Wystarczy teraz przebudować całą aplikację *(Budowanie/Przebuduj wszystko)* i uruchomić (*ctrl+r*). Spróbuj załadować zdjęcie, wynik powinien być podobny jak na Rysunku 5.

Podsumowanie

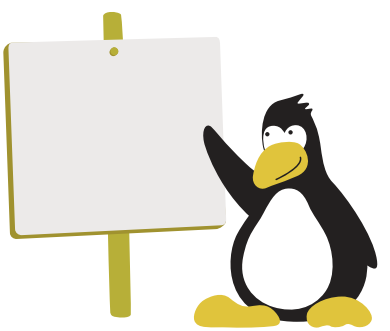
W pierwszej części artykułu przedstawiłem pokrótce zasady tworzenia aplikacji w *Qt Creator*. Jednakże narzędzie *Qt SDK* jest bardzo rozbudowane i w jednym artykule nie dałoby się przedstawić wszystkich jego możliwości. Mam nadzieję, że artykuł zaciekawił Cię do tego stopnia, że spróbujesz napisać aplikację w *Qt*. W następnej części artykułu stworzymy bardziej zaawansowaną aplikację, która będzie korzystała już z innych modułów oprócz standardowych *QtGui* i *QtCore*.

ŁUKASZ KLEJNBERG

Jest właścicielem firmy Ideal Solutions zajmującej się projektowaniem aplikacji internetowych i komputerowych. Komputerami zajmuje się od roku 1989. W zawodzie programisty pracuje od 2000 roku. Także od 2000 roku pracuje nieustannie na systemach Linux: Fedora, Slackware, Debian i Ubuntu. Kontakt z autorem: lukasz.klejnberg@idealsolutions.pl

Pingwin w pudełku

Są trzy podstawowe sposoby na uruchomienie serwera wirtualnego (VPS). Pierwszy z nich to pełna wirtualizacja. Drugi – parawirtualizacja – wymaga modyfikacji goszczonego systemu operacyjnego ale odwdzięcza się wyższą wydajnością. Trzecie podejście zakłada jeszcze bliższe więzy między gospodarzem i gośćmi i jest rozwinięciem znanych od lat środowisk chroot().



Są trzy podstawowe sposoby na uruchomienie serwera wirtualnego (VPS). Pierwszy z nich to pełna wirtualizacja, oferowana przez produkty takie jak qemu, VirtualBox i VMWare. Dają one pełną niezależność goszczonego systemu operacyjnego od platformy gospodarza i pozwalają na uruchomienie dowolnego systemu wspieranego przez procesor. Drugi – parawirtualizacja – wymaga modyfikacji goszczonego systemu operacyjnego, ale odwdzięcza się wyższą wydajnością. Z rozwiązań linuksowych warto tu wymienić projekt Xen i KVM – młody, ale zdobywający coraz większą popularność. Granica między tymi dwoma podejściami powoli zaciera się, między innymi dzięki rozszerzeniom wspomagającym wirtualizację w procesorach kilku ostatnich generacji. Trzecie podejście zakłada jeszcze bliższe więzy między gospodarzem i gośćmi i jest rozwinięciem znanych od lat środowisk chroot(). W tradycyjnym środowisku tego typu główny serwer dzieli z maszynami wirtualnymi jądro systemu operacyjnego, pamięć, sieć i wszystkie inne zasoby poza systemem plików. Ponieważ narzut związany z taką formą wirtualizacji jest minimalny, jest to zdecydowanie najszybsze rozwiązanie. Z drugiej jednak strony, chroot() nie zapewnia wymaganej elastyczności ani dostatecznego bezpieczeństwa. Panaceum na te bolączki obiecuje wirtualizacja oparta o system operacyjny.

Lekka wirtualizacja

Wirtualizacja taka jest dostarczana razem z systemami FreeBSD (jails) i Solaris (zones). Dla Linuksa dostępne są rozwijane od lat projekty OpenVZ i Linux-VServer. Pierwszy z nich stanowi podstawę dla komercyjnego produktu Virtuozzo i odznacza się bogatą funkcjonalnością oraz dopracowaniem. Ma on jednak kilka ograniczeń, które sprawiają, że nie w każdym środowisku sprawdzi się równie dobrze. Wynikają one w dużej mierze z ukierunkowania na RHEL i bliźniacze dystrybucje. Linux-VServer zaś nie ma korporacyjnego zaplecza, a za cel stawia sobie zminimalizowanie uszczerbku na wydajności wywołanego wirtualizacją. Żaden z tych projektów nie jest idealny, dlatego też nie doczekały się włączenia do głównego drzewa jądra Linuksa. Żeby zatem skorzystać z oferowanych przez nie możliwości, trzeba zbudować własne jądro lub skorzystać z dystrybucji, która oferuje odpowiednie pakiety.

Nie oznacza to jednak, że niełatane jądro jest zupełnie nieświadome "lekkiej" wirtualizacji. Od wersji 2.6.19[*] sukcesywnie pojawia się wsparcie dla nowych rodzajów namespace'ów. Są to twory pozwalające na wydzielenie grupy procesów spod normalnego zarządzania jakimś zasobem i stworzenie dla nich specjalnej wersji świata. Najprostszym przykładem jest UTS_NAMESPACE, pozwalający grupie procesów zmienić nazwę systemu, na którym działają, bez wpływu na host-

name widziany przez pozostałe procesy. Bardziej rozbudowany jest namespace identyfikatorów procesów (PIDNS). Pozwala on wydzielić drzewo procesów z własną numeracją, począwszy od pid 1. Numer ten dostaje pierwszy proces w takiej przestrzeni nazw i pełni on rolę identyczną jak prawdziwy init, tj. przechwytuje osierocone procesy. Innym złożonym namespace jest NETNS (przestrzeń nazw dla urządzeń sieciowych). Dzięki niej każdy VPS może mieć własną listę interfejsów sieciowych, zarówno rzeczywistych, jak i wirtualnych. Wśród tych drugich warto zwrócić uwagę na macvlan, czyli klon rzeczywistej karty sieciowej z innym adresem MAC oraz veth, czyli parę interfejsów przekazujących pakiety między sobą nawzajem. Jeden z końców takiej pary można przenieść do środka VPSa, a drugi zostawić w systemie gospodarza, co pozwala na proste zapewnienie łączności VPSa ze światem zewnętrznym. Każdy serwer wirtualny posiada również własną konfigurację firewalla. Wszystkie wspierane obecnie namespace'y były obecne w jądrze 2.6.27, natomiast pełną funkcjonalność osiągnęły w wersji 2.6.29.

Dopełnieniem namespace'ów są control groups (cgroups), które raczej służą ograniczaniu zużycia zasobów przez wybrane grupy procesów niż tworzeniu iluzji niezależnego systemu. Od momentu pojawienia się w wersji 2.6.24 regularnie pojawiają się nowe moduły, rozszerzające funkcjonalność cgroups. Przykładowe moduły pozwalają na: ograniczenie procesorów dostępnych dla grupy, kontrolę nad czasem procesora przydzielonym grupie (aby nie zmonopolizowała CPU), ograniczenie dostępnej pamięci (fizycznej i swap) i udostępnienie tylko wybranych urządzeń (w znaczeniu plików w /dev). Można też cały ruch sieciowy generowany przez grupę odpowiednio otagować na warstwie QoS i ustalić maksymalną przepustowość dysku dostępną dla grupy. Aktualnie rozwijany jest również moduł pozwalający na ograniczenie w obrębie grupy ilości brudnej pamięci (tj. takiej, którą trzeba wkrótce zapisać na dysku). Pozwoli on na jeszcze skuteczniejszą kontrolę wykorzystania dostępnych zasobów. Bardzo ciekawą funkcjonalność otwiera również moduł freezer. Sam w sobie pozwala on jedynie na zatrzymanie wszystkich procesów w grupie (jak hurtowy kill -STOP), ale jest kamieniem węgielnym pod checkpoint/restart. C/R to możliwość zapisania bieżącego stanu grupy procesów i późniejszego jego odtworzenia (np. na innym serwerze fizycznym lub po restarcie gospodarza). Podobna możliwość w ograniczonym zakresie jest obecnie dostępna w OpenVZ. Zestaw łat dla checkpoint/restart jest aktualnie burzliwie rozwijany i ma szansę trafić do jądra 2.6.35.

LXC wkracza na scenę

Połączenie namespace'ów i cgroup, z naciskiem na te pierwsze, określa się jako projekt Linux Containers (LXC). Nie implementuje on całej funkcjonalności OpenVZ i Linux-VServer, jednak obecność w głównej gałęzi jądra oznacza dla LXC duże korzyści. Przede wszystkim oznacza ona dobrą integrację namespace'ów z resztą jądra, jak również poszerza grono developerów uczestniczących w rozwoju kodu, co pozy-

Listing 1. *Konfiguracja interfejsu br0*

```
# tworzymy "switch", do którego podłączony będzie
                    VPS
brctl addbr br0
# nie korzystamy z STP, switch ma przekazywać
                    pakiety od razu
brctl setfd br0 0

# podłączamy system gospodarza do "switcha"
ip link set dev br0 up
ip addr add dev br0 127.17.0.1/24
# i konfigurujemy na nim prosty router z NAT
sysctl -w net.ipv4.ip_forward=1
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
iptables -I FORWARD -i br0 -o eth0 -j ACCEPT
   iptables -I FORWARD -o br0 -i eth0 -j ACCEPT
```

Listing 2. *Plik z konfiguracją VPSa*

```
lxc.utsname = vzcentos
lxc.tty = 4
lxc.network.type = veth
lxc.network.flags = up
lxc.network.link = br0
lxc.network.name = eth0
lxc.network.mtu = 1500
lxc.rootfs = /var/lib/lxc/rootfs.vzcentos
lxc.cgroup.devices.deny = a
# /dev/null and zero
lxc.cgroup.devices.allow = c 1:3 rwm
lxc.cgroup.devices.allow = c 1:5 rwm
# consoles
lxc.cgroup.devices.allow = c 5:1 rwm
lxc.cgroup.devices.allow = c 5:0 rwm
lxc.cgroup.devices.allow = c 4:0 rwm
lxc.cgroup.devices.allow = c 4:1 rwm
# /dev/{,u}random
lxc.cgroup.devices.allow = c 1:9 rwm
lxc.cgroup.devices.allow = c 1:8 rwm
# /dev/pts/*
lxc.cgroup.devices.allow = c 136:* rwm
# rtc
lxc.cgroup.devices.allow = c 254:0 rwm

lxc.pts = 1000
```

tywnie wpływa na jego jakość i stabilność. Zyskuje na tym również OpenVZ, jak i Linux-VServer – w kolejnych wersjach w coraz większym stopniu wykorzystują namespace'y. Kolejną zaletą LXC jest elastyczna architektura, zgodna z założeniami jądra. Namespace'y i cgroups dają określone możliwości, ale nie definiują polityki, która określa, w jaki sposób z nich korzystać. Dzięki temu można dowolnie składać "z klocków" serwery o wymaganym stopniu izolacji, np. z własnym stosem sieciowym, ale wspólnym systemem plików. W porównaniu z OpenVZ, traktującym wirtualizację całościowo, jest to widoczna korzyść i pozwala wykorzystać LXC na różne sposoby, nie polegające na stworzeniu kompletnego VPSa, ale np. na ograniczaniu poszczególnych aplikacji.

Aby od abstrakcyjnej koncepcji namespace'ów przejść do działającego VPSa, potrzebne jest wsparcie w przestrzeni użytkownika. Do tworzenia serwerów wirtualnych i zarządzania nimi służą przede wszystkim dwa projekty. Pierwszy, zwany po prostu lxc, oferuje zestaw narzędzi, takich jak lxc-create, lxc-start, lxc-ps i wiele innych. Stworzenie nowego VPSa polega na ustaleniu zawartości systemu plików (jak w przypadku środowiska chroot()) oraz na utworzeniu prostego pliku konfiguracyjnego, którego format jest opisany w lxc.conf(5). Ze względu na swoją prostotę i ukierunkowanie wyłącznie na Linux Containers, lxc rozwija się równie szybko jak funkcjonalność w jądrze – istnieje już np. eksperymentalne wsparcie dla checkpoint/restart. lxc to optymalny sposób na wypróbowanie możliwości Linux Containers. Nieco inny profil reprezentuje powstały w ramach inicjatywy RedHat Emerging Technologies projekt libvirt. Ma on na celu ujednolicenie zarządzania wszelkimi mechanizmami wirtualizacji. Niezależnie od technologii (KVM, Xen, LXC i inne), libvirt dostarcza jednolity sposób konfiguracji, oparty o pliki XML, oraz jednolity interfejs dla programistów różnych języków. Pomimo swojej nazwy, libvirt to nie tylko biblioteka, ale również zestaw narzędzi o możliwościach porównywalnych do lxc. Sama infrastruktura libvirt umożliwia również zarządzanie VPSami na wielu maszynach z centralnej konsoli. Można się spodziewać, że gdy zestaw łat do checkpoint/restart osiągnie stabilność, w libvirt_lxc pojawi się wsparcie dla migracji działających VPSów między maszynami, analogicznie do np. sterownika do KVM. libvirt to rozwiązanie zdecydowanie warte uwagi przy uruchamianiu większych, produkcyjnych instalacji.

[*] Namespace'y dla systemów plików ("lepszy chroot()") są dostępne od wersji 2.6.14, ale nie były, przynajmniej na początku, tworzone z myślą o bardziej kompletnej wirtualizacji.

Listing 3. *Konfiguracja sieci na VPSie*

```
# etc/sysconfig/network
NETWORKING=yes
HOSTNAME=vzcentos.localdomain

# etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE=eth0
BOOTPROTO=none
IPADDR=172.17.0.2
NETMASK=255.255.255.0
GATEWAY=172.17.0.1

# etc/resolv.conf
nameserver 8.8.8.8
```

Listing 4. *Sprawdzenie stanu startującego VPSa*

```
# lxc-info -n vzcentos
'vzcentos' is RUNNING

# lxc-ps --name vzcentos
CONTAINER    PID TTY          TIME CMD
vzcentos    5432 ?        00:00:00 init
vzcentos    5442 ?        00:00:00 init
vzcentos    5445 ?        00:00:00 rc.sysinit
```

LXC w praktyce

Mimo kilku niedociągnięć, narzędzia LXC pozwalają dość szybko uruchomić pełnowartościowego VPSa. W tym przykładzie podstawowym systemem operacyjnym (gospodarzem) jest Fedora 13, a gościem – CentOS 5. Wymagane niestandardowe pakiety w systemie gospodarza to lxc oraz bridge-utils.

Zacznijmy od podmontowania systemu plików cgroup. Dodajemy do */etc/fstab* wpis:

```
cgroup   /cgroup   cgroup   defaults   0   0
```

a następnie tworzymy katalog i montujemy system plików:

```
mkdir -p /cgroup && mount /cgroup
```

Następnym krokiem będzie konfiguracja sieci. Możemy to zrobić na 2 sposoby: główny interfejs sieciowy gospodarza może być mostkiem przekazującym pakiety do interfejsu VPSa lub routerem dla VPSów.

Dostępne w Internecie opisy z reguły opisują ten pierwszy sposób, dlatego – z przekory – zrobimy to drugim i odizolujemy naszego VPSa maskaradą (NAT). Takie rozwiązanie jest mniej inwazyjne dla systemu gospodarza, gdyż nie wymaga zmiany głównego interfejsu sieciowego na mostek. Urządze-

nie br0 jest w dalszym ciągu konieczne, ale łączy ze sobą tylko VPSy. Możemy je traktować jak switch, do którego są podłączone wirtualne karty sieciowe (Listing 1).

Skorzystamy z obrazu VPSa przygotowanego na potrzeby projektu OpenVZ, do ściągnięcia ze strony projektu:

```
/var/lib/lxc# wget http://download.openvz.org/template/
                    precreated/centos-5-x86.tar.gz
/var/lib/lxc# mkdir rootfs.vzcentos
/var/lib/lxc# cd rootfs.vzcentos
/var/lib/lxc/rootfs.vzcentos# tar xzf ../centos-5-
                    x86.tar.gz
```

Sam obraz systemu to jeszcze za mało, dlatego tworzymy katalog /var/lib/lxc/vzcentos, a w nim plik config o treści (Listing 2).

Określa on podstawowe cechy VPSa, a dokumentacja dostępnych wpisów znajduje się na stronie *manuala lxc.conf*(5).

W tym momencie VPS jest gotowy do uruchomienia, ale nie wystartuje poprawnie, ponieważ parę rzeczy trzeba dostosować do specyfiki LXC. Po pierwsze, wyłączamy udev, dopisując "exit 0" na końcu pliku etc/udev/udev.conf (w katalogu głównym VPSa) – inaczej VPS nie uruchomi się, czekając na zdarzenie, które nigdy nie nadejdzie. Następnie przygotowujemy do działania terminale i pseudoterminale – bez tego nie będzie sposobu na zalogowanie się do VPSa:

```
# drobny błąd w lxc-start powoduje, że ten plik trzeba
                    usuwać przed każdym startem VPSa
                    - lxc-start tworzy go na nowo
/var/lib/lxc/rootfs.vzcentos# rm -f dev/ptmx
# wystarczą zwykłe pliki, lxc-start zajmie się resztą
/var/lib/lxc/rootfs.vzcentos# touch dev/tty{1,2,3,4}
```

Obraz z OpenVZ standardowo zawiera serwer SSH, ale dla celów edukacyjnych dodajmy terminale działające jak standardowa konsola tekstowa. W tym celu do /etc/inittab wewnątrz katalogu VPSa (*/var/lib/lxc/rootfs.vzcentos*) dopisujemy sekcję:

```
# Run gettys in standard runlevels
t1:2345:respawn:/sbin/mingetty /dev/tty1
t2:2345:respawn:/sbin/mingetty /dev/tty2
t3:2345:respawn:/sbin/mingetty /dev/tty3
t4:2345:respawn:/sbin/mingetty /dev/tty4
```

Liczba terminali skonfigurowanych w tym kroku i utworzonych w poprzednim powinna się pokrywać z wartością wpisu "lxc.tty" z pliku konfiguracyjnego.

Tworzymy również pliki z konfiguracją sieci (wszystkie pliki wewnątrz katalogu VPSa) (Listing 3).

Na koniec ustawiamy hasło roota dla VPSa, gdyż domyślnie w wybranym obrazie to konto jest zablokowane:

```
/var/lib/lxc/rootfs.vzcentos# chroot . passwd root
```

W końcu jesteśmy gotowi do uruchomienia VPSa:

```
# lxc-start -n vzcentos -d
```

Opcja -d powoduje start w tle, bez wyświetlania komunikatów skryptów startowych. W obecnych wersjach LXC, jest ona konieczna ze względu na operacje, jakie jądro wykonuje na terminalu, na którym działa `lxc-start` – w telegraficznym skrócie przestaje on działać w pełni poprawnie, np. nie reaguje na kombinację klawiszy *Ctrl-C*. Sprawdzamy, czy wszystko działa (Listing 4).

Widać, że nasz VPS startuje. Jeżeli start się nie powiódł, więcej informacji można uzyskać, dodając do wywołania `lxc-start` parametry `-l DEBUG -o `tty`.` Aby się do niego połączyć, możemy skorzystać ze skonfigurowanych wcześniej terminali (lub ze zwykłego ssh):

```
# lxc-console -n vzcentos
```

Powinniśmy po chwili niezbędnej na dokończenie sekwencji startowej zobaczyć monit z nazwą VPSa:

```
CentOS release 5.4 (Final)
Kernel 2.6.33.2-57.fc13.i686 on an i686
vzcentos login:
```

i móc się zalogować na konto roota z ustawionym hasłem.

Aby wyłączyć VPSa, możemy wydać ze środka polecenie halt. Niestety nie spowoduje to całkowitego wyłączenia VPSa, gdyż nie jest do tego przygotowany standardowy proces init. Musimy jeszcze "nacisnąć przycisk Power":

```
# lxc-stop -n vzcentos
```

Miłej zabawy!

GRZEGORZ NOSEK

Jest programistą i administratorem, sympatykiem Open Source, Perla, Pythona i kotów. Jest współtwórcą MegiTeam. W swojej pracy jako programista stara się, żeby mógł się nudzić jako administrator. Zdarzało mu się zgłaszać błędy i łatki, m.in. w jądrze Linuksa i Linux-VServer. Można go spotkać na konferencjach poświęconych językom programowania. Kontakt z autorem: root@localdomain.pl

Wystartuj z Tomcat

Java jest dzisiaj wiodącą technologią wykorzystywaną przy tworzeniu złożonych serwisów internetowych. Do uruchomienia takich aplikacji konieczny jest odpowiedni serwer i takim właśnie produktem jest powszechnie uznany i stosowany Apache tomcat. Ponieważ linux doskonale sprawdza się jako system operacyjny dla serwerów internetowych, ten artykuł musiał powstać:).

Apache tomcat jest kontenerem aplikacji webowych, umożliwia on więc uruchamianie aplikacji internetowych napisanych w Javie. Oferuje on tak zwaną czystą, referencyjną implementację technologii servletów oraz jsp opublikowaną przez Sun Microsystem. Na samym początku należy jednak podkreślić, że tomcat nie jest serwerem aplikacji J2EE, gdyż nie oferuje wszystkich możliwości określanych przez ten standard. Jest natomiast bardzo często wykorzystywany komercyjnie jako kontener aplikacji napisanych np. z wykorzystaniem popularnego frameworka spring lub w oparciu o klasyczne podejście do technologii servlerów oraz stron jsp. Serwer jest udostępniany na zasadach open source przez powszechnie znaną Apache Software Foundation. Ponieważ jest on napisany w Javie, można go uruchomić na większości platform sprzętowych. Ponadto jest on wykorzystywany w serwerze aplikacji J2EE Apache Geronimo oraz Jboss, możliwa jest również jego integracja z serwerem www Apache.

Tomcat jest bardzo dojrzałym produktem, jego pierwsze wydanie miało miejsce już w 1999 roku. Oferuje znaczną ilość funkcji i możliwości, których tylko niewielka część zostanie opisana w poniższym artykule. Nie będzie on bowiem próbą przedstawienia ich wszystkich, a wprowadzeniem do pracy z tym powszechnie stosowanym produktem. Przedstawiony zostanie proces instalacji serwera, oferowanego przez niego modułu autoryzacji, a następnie połączenia go z bazą danych. Pokazana zostanie również aplikacja umożliwiająca monitorowanie pracy serwera.

Instalacja

Instalacja serwera tomcat zostanie wykonana na komputerze ze świeżo zainstalowanym systemem operacyjnym Linux Debian Lenny. Najprostszą metodą instalacji oprogramowania dla tej wersji linuxa jest skorzystanie z przygotowanych paczek deb. Aby sprawdzić, czy jest dostępna w Debianie paczka deb zawierająca serwer tomcat, wydajmy polecenie:

```
apt-cache search tomcat
```

W wyniku otrzymamy listę paczek skojarzonych z nazwą tomcat, w tym tę zawierającą sam serwer:

```
tomcat5.5 - Servlet and JSP engine.
```

Jak więc widać, najnowszą dostępną wersją sewera tomcat w repozytorium Debiana jest wersja 5.5, natomiast najnowsza opublikowana przez fundację apache wersja posiada numer 6.0.

Jak wspomniano powyżej, najłatwiej zainstalować tomcata w Debianie poprzez użycie przygotowanej paczki z repozytorium. W dalszej części artykułu bazować będziemy jednak na wersji serwera tomcat pobranej z jego internetowej strony domowej. Dzięki temu możliwa będzie bowiem praca na oryginalnych plikach konfiguracyjnych oraz strukturze katalogów serwera, która wyglądać będzie tak samo w większości systemów operacyjnych.

Ponadto będziemy mieli możliwość pobrania najnowszej wersji. Natomiast minusem jest konieczność samodzielnej instalacji wirtualnej maszyny Javy.

Serwer tomcat jest kontenerem aplikacji internetowych Java, sam również jest napisany w tym języku. Tak więc jest oczywiste, że do jego uruchomienia konieczne jest zainstalowanie w systemie operacyjnym wirtualnej maszyny Javy. Zanim to zrobimy, warto sprawdzić, czy jest ona już może zainstalowana:

```
java -version
```

Jeśli w odpowiedzi uzyskaliśmy informację, że wywoływane polecenie jest nieznane, prawdopodobnie nie mamy w systemie dostępnej jvm (wirtualnej maszyny Javy). Należy więc ją zainstalować, tym razem korzystając już z paczki deb:

```
apt-get install openjdk-6-jdk
```

Następnie sprawdźmy, czy działa ona poprawnie. Tym razem w odpowiedzi powinniśmy otrzymać komunikat:

```
java version "1.6.0_0"
OpenJDK  Runtime Environment (build 1.6.0_0-b11)
OpenJDK Client VM (build 1.6.0_0-b11, mixed mode,
                    sharing)
```

Teraz można już przystąpić do pobrania serwera tomcat z sieci. W chwili pisania tego artykułu najnowsza dostępna wersja oznaczona jest numerem 6.0.26. Ze strony *http://tomcat.apache.org/download-60.cgi* pobieramy więc plik *apache-tomcat-6.0.26.tar.gz* do naszego katalogu domowego. Będę wykonywał wszystkie polecenia w systemie jako użytkownik root, choć nie jest to oczywiście zalecane. Moim katalogiem domowym będzie więc */root*, a do rozpakowania paczki tomcata wykorzystamy polecenie:

```
tar xzf  apache-tomcat-6.0.26.tar.gz
```

W wyniku tej operacji powstanie katalog *~/apache-tomcat-6.0.26*. W tej chwili możemy już uruchomić serwer tomcat, aby to zrobić, należy wykonać skrypt:

```
~/apache-tomcat-6.0.26/bin/startup.sh
```

Zostanie uruchomiony serwer tomcat, a system operacyjny wyświetli nam komunikaty:

```
Using CATALINA_BASE:   /root/apache-tomcat-6.0.26
Using CATALINA_HOME:   /root/apache-tomcat-6.0.26
Using CATALINA_TMPDIR: /root/apache-tomcat-6.0.26/temp
Using JRE_HOME:        /usr
Using CLASSPATH:       /root/apache-tomcat-6.0.26/bin/
                    bootstrap.jar
```

Są to bardzo cenne informacje mówiące o wykorzystywanych przez serwer zmiennych środowiskowych. W dalszej części artykułu często będę się odnosił do położenia katalogu określonego przez zmienną `$CATALINA _ HOME`.

Ponieważ każdy z nas posiada wewnętrzną potrzebę małych sukcesów, otwórzmy naszą ulubioną przeglądarkę internetową i wpiszmy adres: *http://192.168.0.68:8080/* (zastępując podany tu adres ip właściwą wartością). Naszym oczom powinno ukazać się powitalne okno tomcata świadczące o zakończeniu sukcesem procesu uruchamiania serwera (Rysunek 1).

Autoryzacja

Autoryzacja jest jedną z podstawowych funkcji aplikacji internetowych. Serwer tomcat posiada wsparcie dla autoryzacji, oferując kilka mechanizmów jej realizacji. War-

Listing 1. *Polecenia sql tworzące tabelę kontaktów*

```
create table t_kontakt(
id_kontakt int identity(1,1) primary key,
opis nvarchar(255));

insert into t_kontakt(opis) values('Adam');
insert into t_kontakt(opis) values('Ania');
insert into t_kontakt(opis) values('Ewa');
insert into t_kontakt(opis) values('Agent
                    Ubezpieczeniowy');
insert into t_kontakt(opis) values('Doradzca
                    Bankowy');
insert into t_kontakt(opis) values('Szef');
insert into t_kontakt(opis) values('Ksiegowa');
insert into t_kontakt(opis) values('Artur');
insert into t_kontakt(opis) values('Monika');
insert into t_kontakt(opis) values('Mama');
```

Listing 2. *Konfiguracja puli połączeń*

```
<Resource name="jdbc/h2"
 auth="Container"
 type="javax.sql.DataSource"
 maxActive="30"
 maxIdle="10"
 maxWait="10000"
 username="sa"
 password=""
 driverClassName="org.h2.Driver"
 url="jdbc:h2:~/test"
 removeAbandoned="true"
 removeAbandonedTimeout="60"
 testOnBorrow="true"
 testOnReturn="true"
 validationQuery="select * from t_kontakt"
 logAbandoned="true" />
```

to zapoznać się z nimi na początku pracy, gdyż dostęp do panelu administracyjnego serwera opiera się właśnie na niej. tomcat może korzystać z różnych baz użytkowników w procesie autoryzacji. My zajmiemy się najprostszym rozwiązaniem, opartym na pliku *$CATALINA_HOME/conf/tomcat-users.xml*, który definiuje użytkowników, ich hasła oraz role. W pierwszym kroku należy dodać nową rolę *manager*, która wymagana jest dla użytkownika konsoli administracyjnej tomcata:

```
<role rolename="manager"/>
```

A następnie dodamy nowego użytkownika, przypisując go do roli manager:

```
<user username="alf" password="szczesciarz"
                roles="manager"/>
```

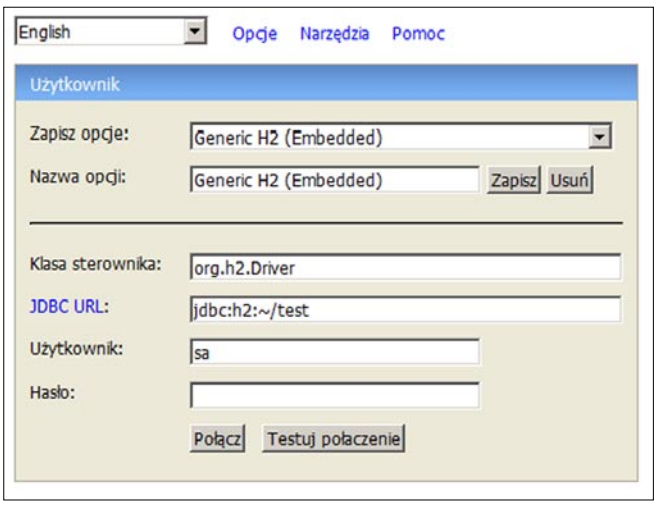
Aby te ustawienia zostały zaakceptowane, konieczne jest zrestartowanie serwera, czyli zatrzymanie serwera oraz ponowne go uruchomienie poleceniami:

```
$CATLINA_HOME/bin/shutdown.sh
```

a następnie

```
$CATLINA_HOME/bin/startup.sh
```

W ten sposób nadaliśmy użytkownikowi alf uprawnienia umożliwiające dostęp do aplikacji Tomcat Web Application Manager, konsoli administracyjnej tomcat. Aby uruchomić tę aplikację, należy kliknąć link *Tomcat Manager* w sekcji *Administration* na stronie głównej tomcata (Rysunek 1). To wszystko!

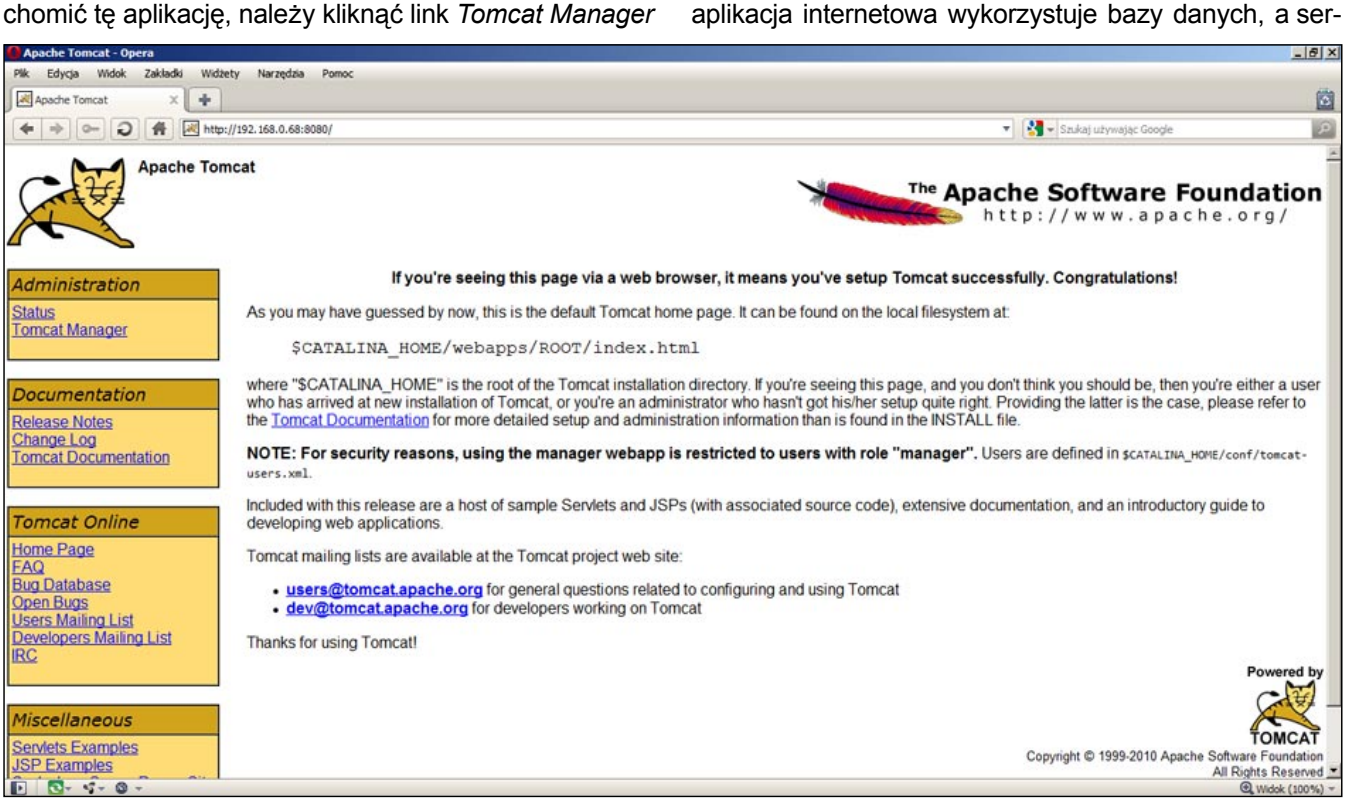


Rysunek 2. *Okno konsoli administracyjnej bazy h2*

Należy podkreślić, że wykorzystaliśmy najprostszy sposób autoryzacji wspomagany przez tomcata. Możliwości są znacznie szersze, m.in. można skorzystać z bazy użytkowników przechowywanych w relacyjnej bazie danych lub usłudze ldap. Funkcjonalności te oferuje mechanizm realm.

Baza danych

Chociaż artykuł ma traktować o kontenerze aplikacji internetowych, to ten podrozdział poświęcony jest uruchomieniu relacyjnej bazy danych h2 oraz utworzeniu prostych struktur danych. Dzisiaj bowiem praktycznie każda aplikacja internetowa wykorzystuje bazy danych, a ser-



Rysunek 1. *Ekran Tomcata po zainstalowaniu*

wer tomcat posiada ku temu odpowiednie wsparcie. Więcej informacji na temat pracy z bazą h2, którą szczerze polecam, można znaleźć w artykule *Baza Danych h2 w praktyce* opublikowanym w kwietniowym numerze Linux+ z roku 2010.

Po pobraniu ze strony *http://www.h2database.com* najnowszej wersji bazy w opcji *All platforms* należy ją rozpakować, a następnie uruchomić poleceniem:

```
java -jar h2-wersja.bazy.jar &
```

Jeśli baza uruchomi się bez problemów, należy otworzyć przeglądarkę internetową oraz wpisać adres *http://localhost:8082/*. Uruchomiona zostanie konsola administracyjna bazy widoczna na Rysunku 2.

Następnie należy się połączyć z bazą danych h2, klikając po prostu *Połącz*. Na potrzeby dalszej pracy z tomcatem utworzymy w bazie prostą tablicę, a następnie wypełnimy ją danymi. W oknie zapytań SQL wykonajmy polecenia z Listingu 1.

W tej chwili należy utworzyć połączenie pomiędzy serwerem tomcat a bazą danych h2. W tym celu skorzystamy z najbardziej uniwersalnego rozwiązania, czyli connection pool. Rozwiązanie to polega na tym, że serwer tomcat tworzy jedno lub więcej połączeń do bazy danych, czyli tzw. pulę połączeń. Następnie kiedy aplikacja internetowa żąda dostępu do bazy danych tomcat, przydziela jej takie połączenie z ustanowionej już puli połączeń do bazy. Tematyka sposobu połączenia aplikacji z bazą danych jest bardzo obszerna i sama w sobie jest materiałem na artykuł, dlatego nie będzie w tym miejscu rozwijana. Podsumowując, stosowanie connection pool ma wiele zalet:

- tomcat sam zarządza ilością aktywnych połączeń, dbając, aby nie było ich zbyt dużo (co nie jest korzystne dla serwera bazy danych), jak również aby ich ilość nie była mniejsza od wymaganej liczby,
- żądanie aplikacji internetowej nie wymaga każdorazowego łączenia się do bazy,
- połączenia nieaktywne mogą być usuwane,
- aplikacja internetowa korzysta z puli połączeń analogicznie jak z bazy danych,
- możliwa jest konfiguracja pracy puli połączeń aby dostosować ją do odpowiednich warunków.

Aby utworzyć pulę połączeń w tomcacie, otwórzmy do edycji plik *$CATALINA_HOME/conf/context.xml*. Mówiąc w dużym skrócie, plik ten umożliwia konfigurację elementów, które następnie będzie można użyć w aplikacji. Dodajmy tam więc wpis przedstawiony na Listingu 2. Najistotniejsze elementy konfigurujące pulę określają:

- `driverClassName`, driver jdbc do bazy danych;
- `url`, ciąg konfigurujący połączenie do bazy danych, analogiczny jak w jdbc;
- `maxActive`, maksymalna liczba aktywnych połączeń;
- `maxIdle`, maksymalna liczba bezczynnych połączeń;
- `maxWait`, określony w milisekundach czas oczekiwania na bazę;
- `testOnBorrow`, czy testować połączenie z bazą przed jego udostępnieniem;
- `testOnReturn`, czy testować połączenie z bazą przed zwróceniem do puli połączeń;
- `validationQuery` – polecenie sql wykorzystywane do testowania połączenia;

Rysunek 3. *Zakładka data sources aplikacji probe*

- `removeAbandoned` – czy usuwać niewykorzystywane połączenia.

Przedstawiona powyżej metoda nie jest najprostszym sposobem konfiguracji puli połączeń w serwerze tomcat. Jest natomiast uniwersalna, można bowiem w prosty sposób zmienić jedynie parametry jdbc (nazwę drivera, ciąg połączenia, nazwę użytkownika i hasło), aby uzyskać dostęp do innej bazy danych, np. oracle czy sql server.

Monitorowanie

W tej chwili mamy już uruchomiony serwer bazy danych h2 oraz kontener aplikacji internetowych tomcat. Dodatkowo skonfigurowaliśmy w tomcacie pulę połączeń do bazy danych, a w bazie utworzyliśmy tabelę zawierającą kontakty do naszych znajomych oraz wypełniliśmy ją przykładowymi danymi. Wykonaliśmy więc kilka czynności, a nie wiemy, jakie są efekty tych działań. O ile serwer tomcat nie zwróci nam wyraźnych błędów np. w trakcie uruchamiania, nie jesteśmy pewni, czy wykonane do tej pory czynności dały pozytywny efekt.

Jak w każdym serwerze warto oczywiście przeglądać logi, w naszym przypadku znajdują się one w katalogu *$CATALINA_HOME/log*.

Możliwe jest monitorowanie bieżącej pracy serwera tomcat nie tylko za pomocą analizy logów, ale tu również mamy do wyboru co najmniej kilka możliwości. Ponieważ forma tego artykułu sprowadza się do najprostszych rozwiązań, wykorzystana zostanie aplikacja Lambda Probe, którą należy pobrać ze strony *http://www.lambdaprobe.org/d/download.htm*.

Wybierzmy więc binarną wersję programu dostępną w formie archiwum zip. W chwili pisania tego artykułu najnowsza dostępna wersja jest oznaczona numerem 1.7.b. Pobrany plik należy rozpakować, otrzymując aplikację w formacie war. Ten format umożliwia w bardzo prosty sposób wdrożenie aplikacji internetowej. Aby to zrobić, przechodzimy do konsoli administracyjnej tomcata, w sekcji *WAR file to deploy* wskazujemy plik *war* aplikacji *probe* i klikamy *deploy*. Jeśli proces ten zostanie zrealizowany poprawnie, o czym może świadczyć komunikat *ok* w górnej części panelu administracyjnego, na liście wdrożonych aplikacji pojawi się wpis *probe* ze statusem *running* ustawionym na *true*. Aby uruchomić aplikację probe, należy po prostu wybrać link z listy aplikacji oraz zalogować się analogicznie jak do konsoli administracyjnej tomcata. Jeśli autoryzacja przebiegnie poprawnie, powinniśmy zobaczyć okno aplikacji podobne do tego z Rysunku 3.

Aplikacja probe umożliwia obserwację wielu parametrów serwera, my skupimy się na połączeniu do bazy danych. Przetestujmy więc, czy działa ono poprawnie. Dokładnie chcemy wiedzieć, czy możliwe jest wykonywanie zapytań do bazy danych h2 z poziomu tomcata. Tu z pomocą przychodzi nam właśnie aplikacja probe. Wybieramy w niej zakładkę data source, a następnie klikamy na jeden z linków wskazujących na resource, który w naszej aplikacji ma nazwę *jdbc/h2* (sami ją nadaliśmy w pliku *context.xml*). Teraz możemy wybrać opcję test connection, w wyniku której powinniśmy otrzymać następujące informacje:

```
Database InfoProperty Name Property Value
Database Product Name  H2
Database Product Version  1.2.133 (2010-04-10)
JDBC Driver Name H2 JDBC Driver
JDBC Driver Version 1.2.133 (2010-04-10)
```

Jak więc widać, testowe połączenie z tomcata do bazy danych zakończyło się sukcesem. Baza zwróciła nam informację o swojej wersji, to samo zrobił driver jdbc.

Idąc krok dalej, warto też zadać zapytanie bezpośrednio do bazy, wpisując polecenie sql:

```
select *
from t_kontakt
```

W jego wyniku powinniśmy otrzymać dane, które wprowadziliśmy do bazy (Listing 1).

Podsumowanie

Kształt tego artykułu nie umożliwia nawet pobieżnego opisania najważniejszych funkcji serwera tomcat. Nie zostało poruszone między innymi zagadnienie logów, load balancing, konfiguracji pamięci czy monitorowania serwera za pomocą jmx. Mam jednak nadzieję, że stanowi on zachętę do rozpoczęcia pracy z serwerem tomcat.

W Sieci

- *http://tomcat.apache.org/* - strona domowa tomcata;
- *http://www.coreservlets.com/Apache-Tomcat-Tutorial* – tutorial tomcata;
- *http://wiki.apache.org/tomcat/FAQ* – repozytorium faq na temat tomcata;
- *http://www.jguru.com/faq/home.jsp?topic=Tomcat* – repozytorium faq na temat tomcata;
- *http://java.sun.com/products/jsp/tomcat/faq.html* – repozytorium faq na temat tomcata.

SŁAWOMIR WOJCIECHOWSKI

Autor pracuje w firmie telekomunikacyjnej, gdzie zajmuje się zagadnieniami związanymi z przetwarzaniem oraz analizą danych. Do jego obowiązków należy analiza potrzeb oraz projektowanie systemów bazodanowych a także interfejsów danych. Patrząc od strony technologii najszersze doświadczenia posiada pracując z bazą danych SQL server oraz oczywiście Javą. Kontakt z autorem: s.wojciechowski@gmail.com

HOSTING NEXT LEVEL

NOWOŚĆ!

Jako nowy klient możesz zaoszczędzić 30 zł przy pierwszej płatności za którykolwiek z reklamowanych produktów: wystarczy przy zamówieniu podać kod: **013604**
(Kod ważny jest do 01 maja 2010 r.)

Windows Server 2008 R2
Microsoft

DEDYKOWANY SERWER HETZNER EQ 4

- Intel®Core™ i7-920 Quad-core z technologią HT
- 8 GB DDR3 RAM
- 2 x 750 GB SATA-II HDD (Software-RAID 1)
- System operacyjny Linux
- Windows Server Web Edition (69 zł miesięcznie)
- Nieograniczony transfer*
- System ratunkowy
- Instalator obrazów
- 100 GB na kopie zapasowe
- Usługa zdalnego restartu
- Umowa na czas nieokreślony
- Opłata instalacyjna 599 zł

199,-zł miesięcznie

DEDYKOWANY SERWER HETZNER EQ 8

- Intel®Core™ i7-920 Quad-core z technologią HT
- 24 GB DDR3 RAM
- 2 x 1500 GB SATA-II HDD (Software-RAID 1)
- System operacyjny Linux
- Windows Server Web Edition (69 zł miesięcznie)
- Nieograniczony transfer*
- System ratunkowy
- Instalator obrazów
- 100 GB na kopie zapasowe
- Usługa zdalnego restartu
- Umowa na czas nieokreślony
- Opłata instalacyjna 599 zł

329,-zł miesięcznie

DEDYKOWANY SERWER HETZNER EQ 9

- Intel®Core™ i7-975 Quad-core z technologią HT
- 12 GB DDR3 RAM
- 3 x 1500 GB SATA-II HDD (Software-RAID 5)
- System operacyjny Linux
- Windows Server Web Edition (69 zł miesięcznie)
- Nieograniczony transfer*
- System ratunkowy
- Instalator obrazów
- 100 GB na kopie zapasowe
- Usługa zdalnego restartu
- Umowa na czas nieokreślony
- Opłata instalacyjna 599 zł

399,-zł miesięcznie

* Nie pobieramy opłat za przesyłane dane. Po przekroczeniu 2000 GB miesięcznie przepustowość zostanie ograniczona do 10 MBit/s. Istnieje możliwość pozostawienia przepustowości na 100 MBit/s za opłatą 59 zł za każdy dodatkowy TB.

HETZNER ONLINE

Hosting Next Level: Hetzner Online oferuje najbardziej zaawansowane rozwiązania hostingowe na rynku. Platformy serwerów dedykowanych zapewniają znakomitą szybkość transmisji danych i wydajność dzięki własnej infrastrukturze sieciowej w centrach danych znajdujących się w Niemczech. Dzięki atrakcyjnym cenom i kompetentnej obsłudze technicznej jesteśmy w stanie zaoferować znacznie więcej, niż oczekują klienci.

www.hetzner.info
info@hetzner.com

Pentaho – open source dla biznesu

Rozwiązania dla biznesu służące do analizy danych stanowią zaawansowane i wyspecjalizowane oprogramowanie, tym niemniej nawet w tym segmencie znajdziemy wartościowe aplikacje dostępne na licencji open source. Doskonałym przykładem jest platforma Pentaho Business Intelligence.

Zaletę tego systemu stanowi olbrzymi zakres dostępnych funkcji, począwszy od umożliwiających pobieranie informacji z praktycznie dowolnych źródeł (lista wspieranych baz danych zawiera kilkanaście pozycji), po wykonywanie analiz, także z użyciem zaawansowanych algorytmów eksploracji danych (data mining) oraz generowanie raportów. To jednak nie wszystko. Razem z systemem oferowane są także między innymi narzędzia ETL. Wszystkie moduły udostępnione są na licencji wolnego oprogramowania. Jednocześnie oferowana jest również wersja komercyjna [1]. Producent zastrzega, że oprogramowanie na licencji open source przeznaczone jest przede wszystkim dla celów edukacyjnych, w celu rozwijania własnych aplikacji opartych na systemie Pentaho oraz na potrzeby testów. W przypadku większych wdrożeń zalecane jest natomiast skorzystanie z komercyjnego wsparcia. Nic nie stoi jednak na przeszkodzie, by wypróbować Pentaho na własną rękę, zwłaszcza że wraz z samym oprogramowaniem udostępniona została dokumentacja, bogata i przyjazna dla użytkownika. Ułatwia ona proces instalacji i konfiguracji systemu.

Pentaho Community [2] stanowi rozbudowany pakiet, na który składa się serwer obsługiwany za pośrednictwem przeglądarki internetowej, a także zestaw aplikacji klienckich, uruchamianych na lokalnych komputerach. Klienty systemu są programami wieloplatformowymi. Aplikacja serwerowa uruchamiana jest natomiast za pośrednictwem Apache Tomcat. Możliwe jest zarówno skorzystanie z już istniejącej architektury, jak i zainstalowanie całego pakietu w sposób zautomatyzowany, razem z oprogramowaniem serwera. My skorzystamy z drugiej spośród wymienionych metod.

Instalacja Pentaho

Pomimo rozbudowanej struktury systemu Pentaho jego instalacja nie jest bardzo skomplikowana. Przede wszystkim powinniśmy zadbać o serwer, na którym umieścimy opisywane oprogramowanie. Szczególnie istotne są kwestie sprzętowe. Wprawdzie Pentaho nie nakłada żadnych konkretnych ograniczeń, ale w przypadku instalacji wykorzystywanych przez dużą liczbę użytkowników sugerowane jest wyposażenie serwera w co najmniej 2 GB pamięci RAM. Poza tym przydatne okażą się bogate zasoby dyskowe oraz dwurdzeniowy procesor. Od strony programowej konieczne jest zainstalowanie pakietu Sun Java Runtime Environment w wersji 1.5. Starsze wydania wirtualnej maszyny Java na pewno nie pozwolą na uruchomienie Pentaho, z kolei JRE 1.6 nie jest jeszcze oficjalnie wspierane. Korzystając z najnowszej wersji środowiska Java Runtime Environment nie powinniśmy się jednak obawiać wystąpienia poważnych błędów.

Jaka dystrybucja najlepiej współpracuje z Pentaho? Producent zamieścił na liście oficjalnie wspieranych systemów operacyjnych SuSE Linux Enterprise Desktop/Server oraz Red Hat Enterprise Linux 5. Nie oznacza to jednak, że pozostałe dystrybucje nie mogą pełnić roli serwera. Bardzo dobrze sprawdza się między innymi Ubuntu w wersji co najmniej 9.04. Dystrybucja ta pozwala na szybkie i bezproblemowe zainstalowanie najnowszego wydania Pentaho.

Sama instalacja sprowadza się praktycznie do pobrania odpowiedniego pakietu i jego rozpakowania. Bardzo łatwo możemy jednak utknąć na witrynie Pentaho, szukając właściwego archiwum na liście wersji, funkcji oraz modułów. Najlepiej jest przejść od razu do portalu Sourceforge, odnaleźć stronę projektu i z sekcji *Files* [3] pobrać najnowsze wydanie pakietu opisanego jako Business Intelligence Server (`biserver-ce-x.x.x.stable.tar.gz`). Ma on objętość blisko 150 MB i zawiera serwer Pentaho wraz z towarzyszącym mu oprogramowaniem. Dodatkowo dostępny jest pakiet służący do ręcznej instalacji (`biserver-manual-ce-x.x.x.stable.tar.gz`). W wielu przypadkach najlepszym rozwiązaniem będzie jednak ściągnięcie archiwum działającego natychmiast po rozpakowaniu.

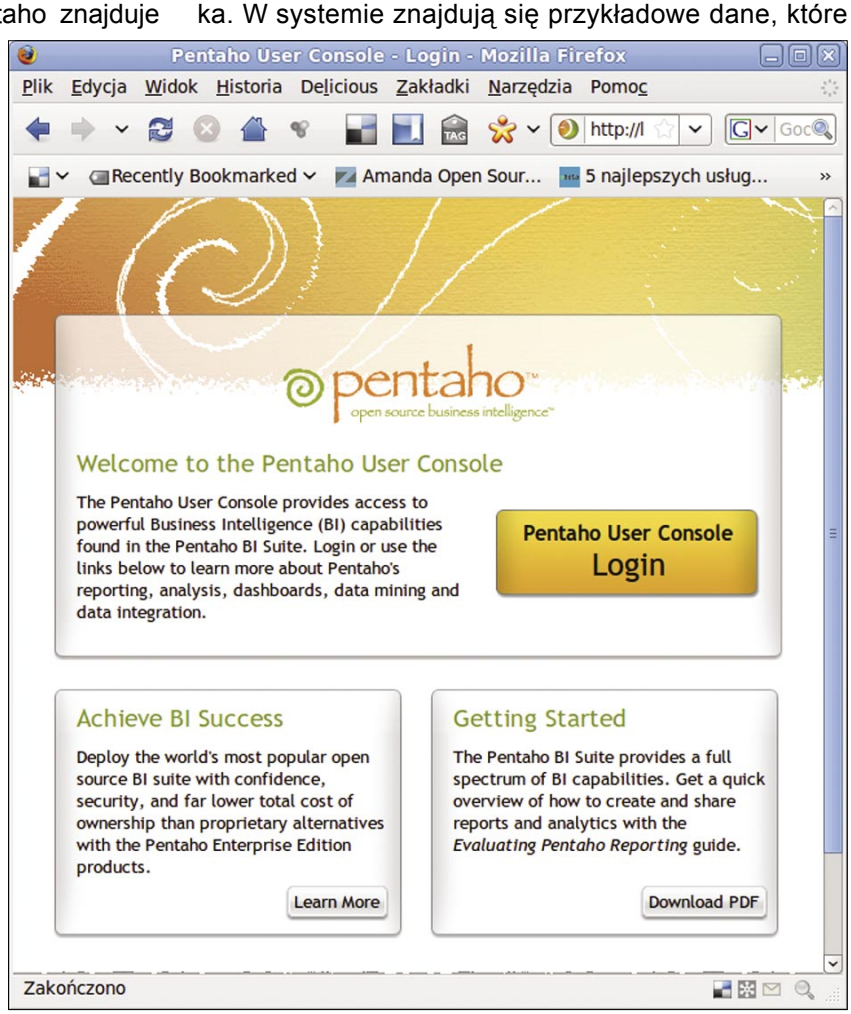
Wewnątrz pakietu zawierającego Pentaho znajduje się katalog `biserver-ce`. Po przejściu do niego powinniśmy wydać polecenie uruchamiające serwer. Komenda `./start-pentaho.sh` może wyświetlić komunikat błędu, jeśli zawczasu nie zadbaliśmy o instalację Java Runtime Environment. Jeśli JRE znajduje się na dysku, a mimo to serwer nie uruchamia się, to utwórzmy w bieżącym katalogu dowiązanie symboliczne o nazwie `jre`. Powinno ono wskazywać lokalizację, w której znajduje się środowisko Java Runtime Environment (na przykład `/usr/lib/jvm/java-6-sun-1.6.x.x/jre`). Alternatywne rozwiązanie stanowi ręczna edycja pliku `start-pentaho.sh` i wprowadzenie tam właściwej ścieżki dostępu, a także skorzystanie ze skryptu `set-pentaho-java.sh`.

Jeśli na ekranie pojawiają się komunikaty zawierające między innymi linijki zbliżone do następujących:

```
[Server@1d58aae]: Server socket opened
                  successfully in 172 ms.
[Server@1d58aae]: Database [index=0,
                  id=0, db=file:./
                  hsqldb/sampledata,
                  alias=sampledata]
                  opened sucessfully in
                  2443 ms.
```

to możemy przypuszczać, że serwery Tomcat oraz baz danych zostały uruchomione poprawnie. Najlepszym sposobem upewnienia się jest uruchomienie przeglądarki internetowej i wpisanie adresu *http://localhost:8080/*. Jeśli chcemy trafić na stronę uruchomionego przez nas oprogramowania Pentaho z komputera innego niż serwer, to oczywiście powinniśmy zastąpić w odpowiedni sposób ciąg znaków `localhost`. Poprawnie działający pakiet wyświetla ekran widoczny na Rysunku 1. Na jego pojawienie się trzeba trochę poczekać, zwłaszcza jeśli proces uruchamiania serwera nie został jeszcze zakończony. W większości przypadków czas oczekiwania nie powinien być jednak dłuższy niż kilka bądź kilkanaście sekund.

Teraz możemy już zalogować się do Pentaho. Kliknijmy na przycisk *Pentaho User Console Login*. Pojawi się niewielkie okienko z polami, w których należy wprowadzić login oraz hasło. Możemy też skorzystać z rozwijanej listy *Sample User*. Zawiera ona nazwy przykładowych kont. Po wskazaniu jednego z nich pola loginu oraz hasła zostaną wypełnione automatycznie. Naciśnięcie przycisku *Login* spowoduje wówczas przeniesienie się do pulpitu danego użytkownika. W systemie znajdują się przykładowe dane, które



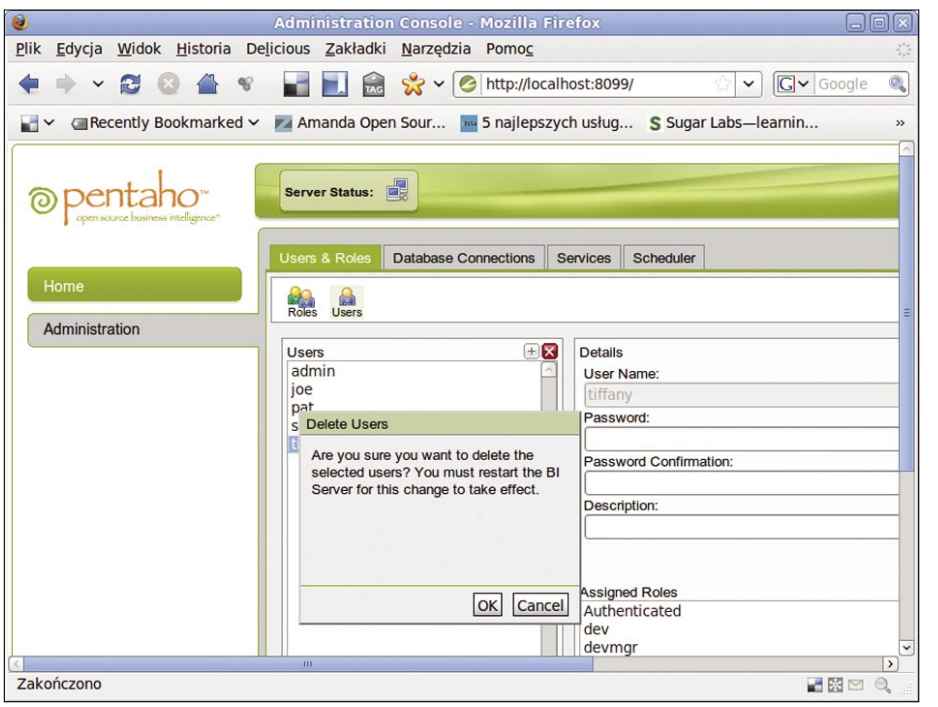
Rysunek 1. *Ekran powitalny Pentaho*

możemy wykorzystać w celu zapoznania się z możliwościami pakietu. Niezależnie od tego konieczne jest jednak wykonanie podstawowych czynności konfiguracyjnych. W tym celu należy uruchomić moduł *Pentaho Administration Console*. Znajduje się on w podkatalogu `administration-console`. Przejdźmy do niego, a następnie wydajmy polecenie `./start-pac.sh`. Powinniśmy ujrzeć kilka komunikatów zakończonych linijką `INFO: Console is now started. It can be accessed using http://localhost:8099 or http://127.0.1.1:8099` lub o podobnej treści. Oznacza ona, że proces uruchamiania konsoli administracyjnej dobiegł do szczęśliwego końca.

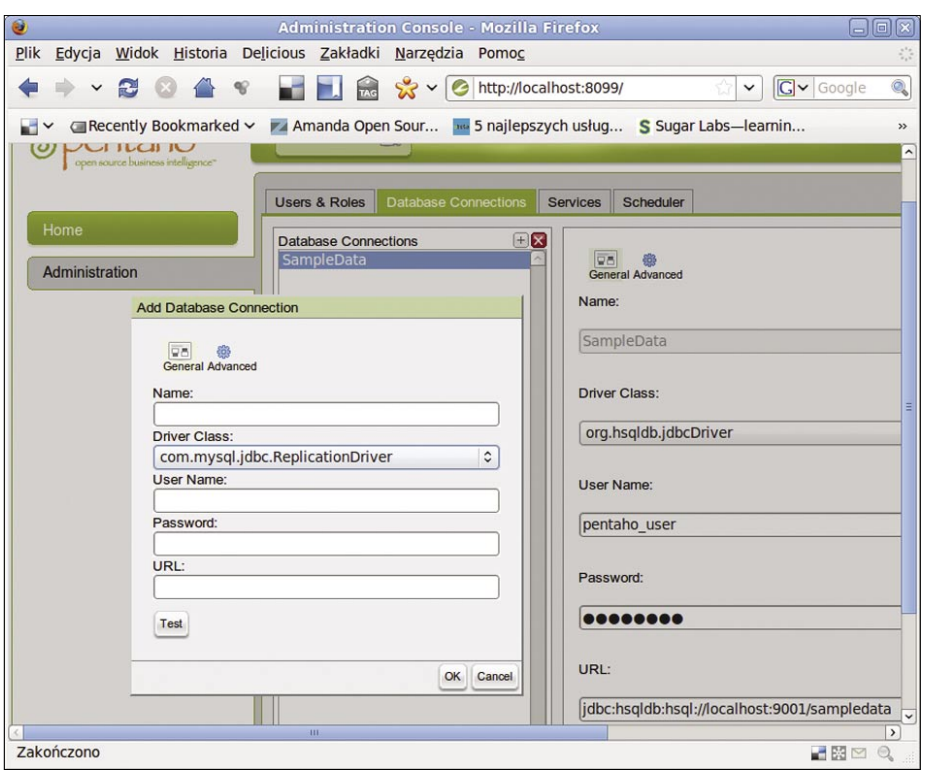
Administracja serwerem

Moduł *Pentaho Administration Console* uruchamiamy, wpisując w przeglądarce *http://localhost:8099*. Ujrzymy wtedy okienko domagające się podania danych dostępowych. Login administratora to `admin`, a domyślne hasło brzmi `password`. Po wpisaniu tych danych i odczekaniu kilku sekund ujrzymy konsolę administratora. Musimy wykonać w niej kilka podstawowych czynności. Powinniśmy rozpocząć od przejścia na kartę *Administration* (za pomocą przycisku widocznego z lewej strony okna przeglądarki). Na ekranie pojawią się kolejne cztery zakładki, z których domyślnie aktywna to *Users & Roles*. Pozwala ona na usunięcie przykładowych kont użytkowników. Dzięki temu zablokujemy niepowołanym osobom dostęp do usługi. Aby usunąć użytkownika, należy zaznaczyć go na liście *Users*, a następnie kliknąć ikonę czerwonego krzyżyka (*Delete Users*). Oczywiście możemy też tworzyć nowe konta. Pozwala na to ikona plusa. Natomiast znajdująca się po prawej stronie okna przeglądarki ramka *Details* służy do zmiany hasła, opisu oraz przypisanych ról. Po dokonaniu wszystkich niezbędnych poprawek należy zrestartować serwer Pentaho.

Druga z zakładek znajdujących się na karcie *Administration* to *Database Connections*. Pozwala ona na uzyskanie dostępu do źródeł danych. Standardowo Pentaho oferuje domyślną bazę przechowującą testowe informacje. Jest ona widoczna pod nazwą *SampleData*. Po prawej stronie zakładki, w osobnej ramce, wprowadzone są dane serwera baz danych oraz samej bazy, tam także określamy sterownik



Rysunek 2. *Konsola administracyjna serwera – zarządzanie użytkownikami*



Rysunek 3. *Ustanawianie połączenia z serwerem baz danych w konsoli administracyjnej*

JDBC. Dodatkowo, po naciśnięciu przycisku *Advanced*, możemy ustalić szczegółowe opcje połączenia. Dodanie nowego źródła danych sprowadza się do naciśnięcia przycisku z plusem. W osobnym okienku wprowadzamy wówczas adres serwera, nazwę użytkownika oraz hasło. Trzeba także wpisać nazwę sterownika JDBC. Konsola administracyjna znacznie nam to ułatwi – wystarczy wybrać odpowiednią pozycję z rozwijanej listy. Przykładowo, skorzystanie z bazy danych MySQL wymaga wskazania `com.mysql.jdbc.ReplicationDriver`.

Pozostałe dwie zakładki, do których otrzymujemy dostęp z poziomu karty *Administration*, pozwalają na wykonywanie dodatkowych czynności związanych z utrzymaniem serwera, przede wszystkim z jego optymalizacją. Dodatkowo możliwe jest zaplanowanie wybranych zadań (*Schedules*). Po dokonaniu poważnych zmian konfiguracyjnych, zwłaszcza po dodaniu źródeł danych oraz kont użytkowników, warto zrestartować serwer. Niezależnie od tego z poziomu konsoli administracyjnej możemy na bieżąco śledzić stan Pentaho. O aktywności serwera mówi nam ikona *Server Status* widoczna w pobliżu górnej krawędzi okna przeglądarki. Jej prawidłowy status to *BI Server is available*.

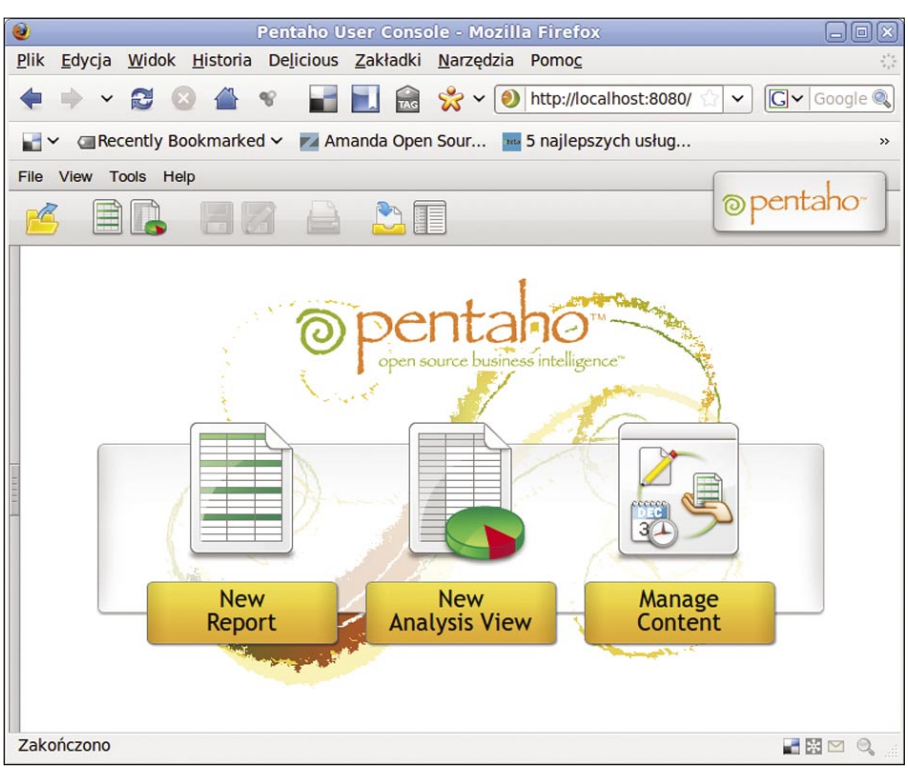
Pentaho w przeglądarce

Po zachowaniu zmian konfiguracyjnych możemy wypróbować konsolę użytkownika, do której trafiliśmy już wcześniej, wpisując adres *http://localhost:8080/*. Pentaho User Console nie pozwala już na zarządzanie serwerem, ale służy za to do prowadzenia analiz danych biznesowych. Po zalogowaniu się trafimy na pulpit, w którego górnym krańcu znajduje się system menu oraz pasek ikon, natomiast w części centralnej – trzy duże przyciski dające dostęp do najważniejszych funkcji. Wszystkie te moduły są dostępne, mimo że nie zainstalowaliśmy jeszcze dodatkowych klientów usługi, które pozwolą nam na wykorzystanie wszystkich możliwości Pentaho.

Pierwszy z przycisków to *New Report*. Otwiera on bardzo przyjaznego kreatora raportów. Przygotowanie czytelnego wyciągu z danych wymaga przejścia przez cztery etapy pracy. Każdy z nich jest dostępny za pośrednictwem linków wyświetlanych w górnej części okna. Zaczynamy od wskazania źródła danych (*Select Data Source*). Po kliknięciu *Add* mamy możliwość wybrania innej bazy niż domyślna, przetestowania połączenia, a także przygotowania zapytania SQL. Kliknięcie ikony plusa (na zakładce *Database*) otworzy dodatkowe okienko *Database Connection*. Działa ono w sposób bardzo przyjazny, wymagający tylko określenia rodzaju serwera (obsługiwane są między innymi MySQL, PosgreSQL, IBM DB2, MS SQL Server oraz Oracle), a także danych pozwalających na zalogowanie, w tym nazw bazy i użytkownika.

W pierwszym etapie przygotowywania raportu określamy także wygląd raportu (*Apply a Template*). Następnie przechodzimy do drugiego kroku (*Make Selections*). W tej chwili powinniśmy wskazać te pola baz danych, których zawartość zamierzamy pobrać. Trzeci etap tworzenia raportu (*Customize Selections*) pozwala natomiast na określenie sposobu wyświetlania informacji. Pracę kończymy, podejmując decyzje dotyczące formatowania całego raportu (wymiary papieru, nagłówki, stopki). Po określeniu tych ustawień możemy wygenerować gotowy dokument. W tym celu na rozwijanej liście *Preview As*, znajdującej się w dolnej części okna, wybieramy interesujący nas format wyjściowy, a następnie klikamy *Go*. Po chwili powinniśmy zobaczyć raport. Wspierane formaty to HTML, PDF, XLS oraz CSV.

Podgląd raportu wyświetlany jest w osobnej zakładce wewnątrz tej karty przeglądarki, w której uruchomiliśmy konsolę użytkownika. Na wygenerowanie dokumentu trzeba zaczekać kilka lub kilkanaście sekund. Gotowe raporty wyglądają bardzo dobrze.

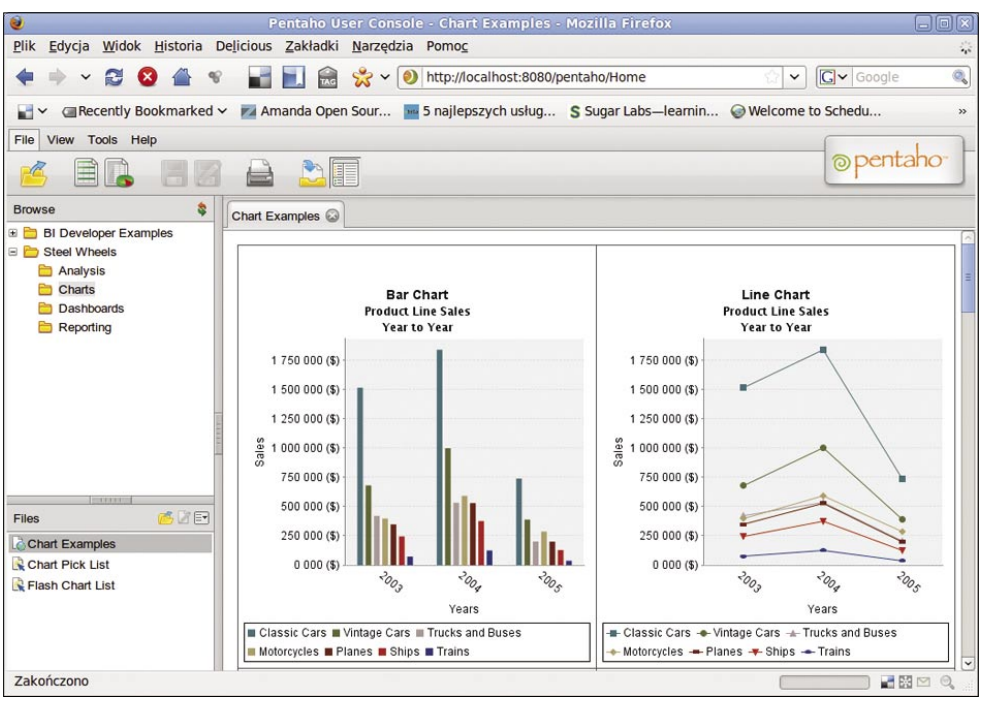


Rysunek 4. *Widok konsoli użytkownika po zalogowaniu się do systemu*

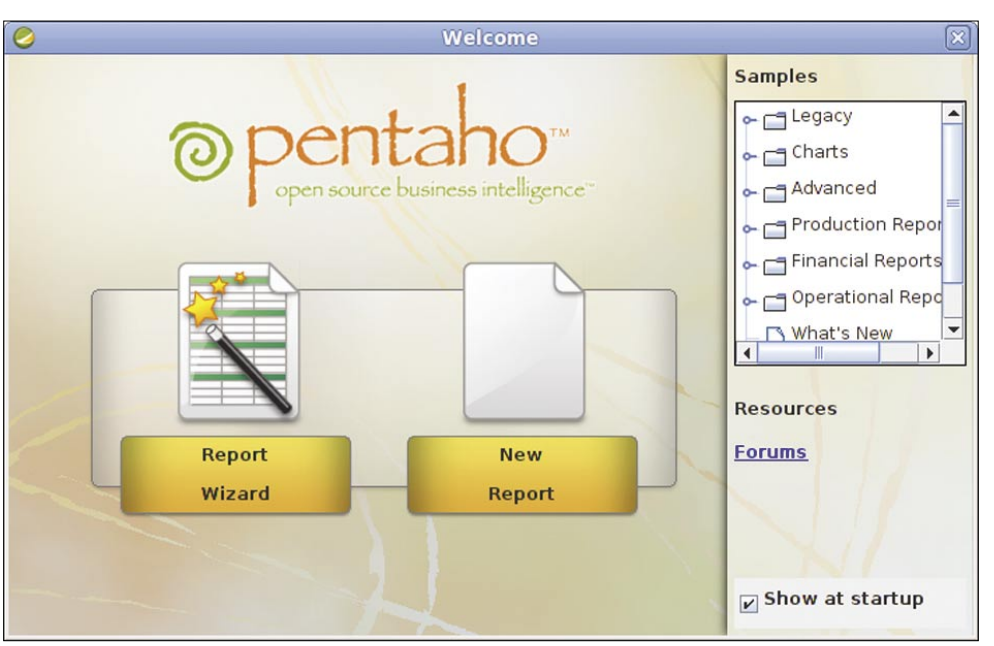
Choć szablony dostarczane razem z oprogramowaniem prezentują się korzystnie, to i tak z pewnością będziemy chcieli dostosować ich wygląd do wymagań firmowych. Zajmiemy się tym za moment. Po pobraniu i zapisaniu plików można natomiast zamknąć wszystkie zakładki otworzone wewnątrz konsoli użytkownika. Powrócimy wtedy do ekranu początkowego, z trzema przyciskami. Drugi z nich to *New Analysis View*. Pozwala on na badanie struktury analizowanych danych. Z kolei *Manage Content* umożliwia zarządzanie informacjami zgromadzonymi w systemie, w tym ich edycję oraz współdzielenie. Kilka przydatnych funkcji znajdziemy również za pośrednictwem paska ikon oraz menu widocznych w górnej części ekranu. Przycisk *Open* da dostęp do przykładowych raportów oraz analiz, a w przyszłości umożliwi nam korzystanie z własnych szablonów. Poza tym na pasku znajdują się cały czas ikony dające dostęp do generatora raportów oraz modułu analiz. Dodatkowo możliwe jest uaktywnienie przeglądarki plików (*Toggle Browser*), która ułatwi nam otwieranie plików znajdujących się w systemie. Ikona *Workspace* pozwala natomiast na szybkie przejrzenie listy zaplanowanych, oczekujących oraz zakończonych zadań skierowanych do serwera.

Podobny zestaw poleceń znajdziemy także w systemie menu. Ponadto umieszczone są tam komendy pozwalające na wylogowanie się z panelu użytkownika (*File* > *Log Out*), odświeżenie serwera (*Tools* > *Refresh*), a także na zmianę wersji językowej (*Tools* > *Languages*).

Do tej pory korzystaliśmy jedynie z gotowych szablonów raportów, a także z przykładowych analiz. Pentaho pozwala nam jednak na o wiele bardziej efektywną analizę danych – i to nie już dostarczonych przez producenta oprogramowania, ale naszych własnych. W tym celu wykorzystamy dodatkowe narzędzia instalowane niezależnie od serwera. Zanim jednak uruchomimy pierwszą z aplikacji, będziemy jeszcze musieli pobrać ze stron Sourceforge odpowiednie pakiety. Dodatkowe narzędzia klienckie nie są bowiem rozpowszechniane razem z serwerem. Pobierzmy zwłaszcza pakiety Report Designer, Data Integration oraz Design Studio. Należy je rozpakować. Producent zaleca umieszczenie wszystkich narzędzi w podkatalogu `design-tools`, utworzonym uprzednio w folderze, który zawiera również oprogramowanie serwera (`administration-console` oraz `biserver-ce`).



Rysunek 5. *Analiza danych w konsoli użytkownika Pentaho*



Rysunek 6. *Okienko powitalne programu Report Designer*

Edytor raportów

Co znajdziemy w ściągniętych przez nas pakietach? W ramach projektu Pentaho dostępny jest między innymi rozbudowany edytor raportów – Report Designer. Pozwala on na przygotowanie raportów oraz umożliwia modyfikację istniejących szablonów. Program oferuje bardzo bogaty zestaw funkcji, przewyższając pod tym względem podobne narzędzie tego typu, w tym prezentowaną już na łamach Linux+ 2/2010 aplikację DataVision (*http://datavision.sourceforge.net/*). Report Designer został napisany w języku Java. Aplikację uruchamiamy, przechodząc do katalogu `report-designer` i wydając komendę `./report-designer.sh`. Powinniśmy zobaczyć logo programu, a po kilku sekundach główne okno. Pracę rozpoczynamy od utworzenia nowego raportu. Możemy również zdecydować się na uruchomienie czarodzieja (*Report Wizard*). Jeśli chcemy edytować istniejące szablony, to powinniśmy wybrać drugie z rozwiązań. Wskazanie opcji tworzenia raportu od podstaw spowoduje natomiast otwarcie pustego szablonu. Składa się on z kilku podstawowych elementów – nagłówków i stopek stron oraz raportu, a także właściwej zawartości. Szablon wyświetlany jest w centralnej części okna, z kolei po lewej stronie znajduje się kolumna z elementami, które można osadzić wewnątrz raportu. Przeciągamy je za pomocą myszy. Po prawej stronie, w dolnej części okna, na dwóch osobnych zakładkach, wyświetlane są atrybuty elementu zaznaczonego w danym momencie, a także informacje dotyczące jego wyglądu.

Osobną kwestię stanowi dostęp do danych. Nowe źródła informacji dodajemy za pośrednictwem podmenu *Data* > *Add Data Source*. Wybranie opcji JDBC otworzy okno *JDBC Data Source*. Należy kliknąć w nim ikonę ze znakiem plusa, opisaną jako *Add connection*. W kolejnym okienku będziemy wówczas mogli określić rodzaj serwera baz danych oraz dane dostępowe.

Gotowe szablony można zapisywać, a także generować ich podglądy. Wszystkie niezbędne funkcje znajdują się w menu *File*. Szablony mogą zostać zapisane w kilku formatach, dla każdego z nich dostępny jest osobny podgląd. Report Designer oczywiście potrafi także wydrukować gotowe pliki. Dodatkowo możliwe jest również opublikowanie gotowego raportu na serwerze Pentaho (*File* > *Publish*). To bardzo ważna funkcja, gdyż Report Designer oferuje zdecydowanie większy pakiet funkcji niż opisane wcześniej oprogramowanie klienckie obsługiwane przez przeglądarkę.

Ważny atut programu stanowi jego czytelny i intuicyjny interfejs. Report Designer nie ustanawia w tej dziedzinie żadnych nowych standardów. Naśladuje natomiast dość wiernie inne narzędzia tego typu oraz aplikacje służące do tworzenia wszelkiego rodzaju interfejsów. Dzięki temu użytkownik nie musi poświęcać wiele czasu na rozpoznanie funkcji Report Designera, przystępując niemal od razu do efektywnej pracy.

Wraz z serwerem Pentaho dostępnych jest jeszcze kilka innych programów klienckich z nim współpracujących. Wszystkie one są warte uwagi, jednak szczególnie przydatne i bogate w funkcje jest narzędzie Pentaho Data Integration, wcześniej znane jako Kettle. Stanowi ono aplikację ETL, czyli służącą do wspomagania migracji i transformacji danych w obrębie hurtowni danych. Ważną zaletą Pentaho Data Integration jest, tak jak w przypadku innych modułów platformy Pentaho, wsparcie dla wielu źródeł informacji (systemów zarządzania bazami danych). Dopuszcza się także wykorzystywanie danych zapisanych w plikach tekstowych oraz arkuszach kalkulacyjnych. Bardzo duże znaczenie ma możliwość użycia Pentaho Data Integration poza środowiskiem Pentaho, dla innych zastosowań związanych z konwersją danych i obsługą hurtowni danych. Jest to zatem narzędzie wszechstronne i warte uwagi, nawet jeśli nie planujemy wdrożenia pozostałych komponentów opisywanej platformy.

Pentaho Business Intelligence to bardzo rozbudowany projekt, a my poznaliśmy jedynie jego najbardziej podstawowe moduły oraz funkcje. Niektóre klienty oraz narzędzia wchodzące w skład pakietu posiadają tak bogaty zestaw funkcji, że mogłyby one z powodzeniem sprawdzić się jako samodzielne aplikacje biznesowe. Świetny przykład stanowi Pentaho Data Integration (Kettle), będące doskonałym środowiskiem ETL. Inną wartościową funkcją jest wsparcie dla algorytmów przetwarzania danych stosowanych w aplikacji Weka. Rozszerza to zakres zastosowań Pentaho o możliwość wykorzystania zaawansowanych technik data mining. Nie należy też zapominać o wszechstronnej obsłudze systemów zarządzania bazami danych, a także o wchodzącym w skład systemu serwerze OLAP – projekcie Mondrian (*http://mondrian.pentaho.org/*). Tak bogaty zestaw możliwości sprawia, że Pentaho to dobry wybór dla użytkownika poszukującego systemu BI na licencji otwartego oprogramowania.

W Sieci

- *http://www.pentaho.com/* – Pentaho Business Intelligence;
- *http://community.pentaho.com/* – Pentaho Community – open source;
- *http://sourceforge.net/projects/pentaho/files/* – Pentaho – pakiety do pobrania;

PAWEŁ WOLNIEWICZ

Autor korzysta z Linuksa od kilkunastu lat, zajmuje się wdrażaniem oprogramowanie open source. Adres kontaktowy: pawelw@innodevel.net.

Zimbra Collaboration Suite – Praca grupowa w OpenSource

Część 2 z 3 – Migracja, konfiguracja urządzeń

W ostatnim numerze Linux+ można było przeczytać, czym jest Zimbra, czym różnią się wersje ZCS, na jakich urządzeniach można korzystać z systemu, jak wygląda wersja Offline. Dzisiaj chciałbym opisać, jak migrować do Zimbry, na co wtedy zwrócić uwagę i jakie narzędzia mogą być pomocne w trakcie tego procesu. Opiszę także, jak konfigurować urządzenia przenośne oraz jak optymalnie skonfigurować Zimbrę w firmie.

Zimbra z Exchange

Ten typ migracji wydaje się najbardziej oczywisty, jako że oba produkty są bardzo zbliżone pod względem funkcjonalności. Najczęściej przeprowadzaną migracją jest Microsoft Exchange + Outlook na Zimbra Collaboration Suite + Zimbra Desktop.

Mimo że migracja wydaje się z pozoru trudna, w rzeczywistości jest stosunkowo prosta. VMware, będący producentem ZCS, zapewnia nam narzędzie zwane „ZCS Exchange Migration Wizard", które można pobrać z zakładki „Pobieranie" w panelu administracyjnym, lub poprosić o to swojego dostawcę usług (w przypadku usługi hostowanej).

Migracja nie sprawia wiele trudności, ponieważ sprowadza się do przebrnięcia przez prosty kreator (Rysunek 1). Kolejne kroki do przejścia:

- wybrać docelową domenę (można migrować tylko jedną domenę naraz);
- wybrać użytkowników do migracji lub określić gałąź Active Direktory do migrowania;
- określić, do jakiej klasy usług (COS) mają przynależeć nowi użytkownicy
- określić hasło startowe dla importowanych użytkowników (nie trzeba go określać, można zrobić to później lub użyć zewnętrznego mechanizmu uwierzytelniania LDAP);
- zdecydować, czy importujemy *kosz*, wiadomości-śmieci;
- określić, ile skrzynek równolegle ma być importowanych.

Migracja ze „zwykłych" kont pocztowych – IMAP/POP3

Standardowo zalecana jest migracja z IMAP poprzez linuxowe oprogramowanie imapsync – faktycznie, ten sposób wydaje się być najłatwiejszy, wystarczy wykonać polecenie:

```
imapsync --buffersize 8192000 --nosyncacls --subscribe
                  --syncinternaldates \
   --host1 imap.host.com --user1 user@host.com --
                  password1 imappasswd --sep1 "/" --
                  prefix1 "" \
   --host2 zimbra.host.com --user2 user@host.com --
                  password2 zimbrapasswd
```

Jednak jako administrator mogę zalecić użytkownikom bardziej intuicyjną migrację: wystarczy podpiąć do naszej Zimbry poprzez panel Web zewnętrzne konto IMAP poprzez *Właściwości->Konta->Dodaj konto zewnętrzne* (Rysunek 2) i metodą *przeciągnij i upuść* przeprowadzić migrację (dotyczy to, w przeciwieństwie do powyższego skryptu, zarówno IMAP, jak i POP3).

Import z PST + Outlook Express

Wydawać by się mogło, że problemem będzie poczta

często archiwizowana na lokalnych dyskach, czyli pliki PST oraz dane Outlook Express. Na szczęście znowu przychodzi nam z pomocą prosty kreator ZCS PST Import Wizard (Rysunek 3).

Użycie samego narzędzia jest niezwykle proste (podajemy dane serwera Zimbry, wskazujemy plik PST wraz z katalogami do importu, i gotowe). Przy tej opcji warto jednak zwrócić uwagę na limity dotyczące największego przesłanego pliku po stronie serwera. Można je zmienić po stronie serwera komendami (pamiętajmy jednak, że 0 nie oznacza nieskończoności, lecz po prostu 0!):

```
zmprov mcf zimbraMtaMaxMessageSize 51200000
zmprov mcf zimbraFileUploadMaxSize 51200000
```

Migracja z Outlook Express sprowadza się do importu danych do pełnego Outlooka, a następnie przeprowadzenie powyższej procedury.

Konfiguracja urządzeń przenośnych – iPhone

Urządzeniem, które podczas moich testów najlepiej współpracuje z Zimbrą, jest iPhone (Rysunek 4). Można synchronizować pocztę, kalendarze, jak również kontakty, dzięki czemu dodanie kontaktu do naszego telefonu będzie skutkowało automatycznym dodaniem kontaktu na serwerze. Poza tym obsługa trybu *push* działa doskonale. Element, który wymaga podkreślenia, stanowi fakt, że dodane zdarzenie do kalendarza na serwerze powoduje dodanie owego wydarzenia w ciągu kilku sekund do naszego telefonu! Oczywiście synchronizacja przebiega dwustronnie, a jej konfiguracja jest banalnie prosta:

Wybieramy *Ustawienia->Poczta*, kontakty, *inne->Dodaj konto->Microsoft Exchange*
Ustawienia:
E-mail: login@domena
Domena: <puste>
Użytkownik: login@domena
Hasło: Twoje hasło
Wybieramy: *dalej*
Zaakceptuj certyfikat (jednorazowo)
Serwer: nazwa naszego serwera
Wybieramy: *dalej*

W następnym oknie wybierz elementy, które chcesz, żeby były synchronizowane, i na tym kończy się konfiguracja urządzenia.

Konfiguracja urządzeń z systemem Windows Mobile

Sama synchronizacja z urządzeniami (Rysunek 5) przebiega bezproblemowo poprzez ActiveSync i raczej nie wymaga komentarza. Problemem są certyfikaty dla połączeń szyfrowanych: Windows Mobile nie pozwala ściągnąć certyfikatów z ActiveSynca, trzeba umieścić je na urządzeniu ręcznie.

Certyfikat główny, jak i certyfikaty urzędów certyfikujących można pobrać poprzez narzędzie SSLChainServer[1] wykonując polecenie:

```
sslchainserver host.com
```

Polecenie to generuje, poza plikami certyfikatów, pliki xml przydatne przy tworzeniu plików instalacyjnych CAB, które można wygenerować za pomocą polecenia:

```
makecab host.com.wm5.xml wm5.cab
makecab host.com.wm6.xml wm6.cab
```

Dzięki czemu uzyskujemy certyfikaty na urządzenia Windows Mobile 5 i 6. Oczywiście, zawsze możemy przegrać same pliki certyfikatów i importować je ręcznie, co jest jednak mniej eleganckim rozwiązaniem.

Nokia Connecting with Zimbra, czyli ZCS na Symbianie

Dla urządzeń fińskiego giganta sytuacja jest podobna jak dla telefonów sterowanych przez Windows Mobile – wszystko działa prawidłowo, poza certyfikatami (dla starszych wersji oprogramowania konieczne jest zainstalowanie aplikacji Mail For Exchange dostęp-

Rysunek 1. *Do migracji z Exchange służy prosty kreator*

nej na stronie nokia.com). W przypadku Symbiana połączenie SSL jest możliwe, ale przy każdej synchronizacji telefon będzie nas pytał o to, czy zaakceptować certyfikat.

Tym razem musimy użyć uprawnień administratora na serwerze ZCS i logując się przez ssh jako root, wykonać polecenia:

```
cd /opt/zimbra/ssl/zimbra/ca
openssl x509 -in ca.pem -out ca.der -
                    outform DER
cp /opt/zimbra/ssl/zimbra/ca/ca.der /opt/
                    zimbra/jetty/webapps/
                    zimbra/downloads
cd /opt/zimbra/httpd/htdocs
vi /opt/zimbra/httpd/conf/mime.types
```

Na końcu tego pliku dodajemy linię:

```
application/x-x509-ca-cert   der
```

Rysunek 3. *ZCS PST Import Wizard*

Niestety, konieczny jest tutaj restart serwera poprzez polecenie `zmcontrol stop/start`.

Na swoim urządzeniu mobilnym wchodzimy na stronę:

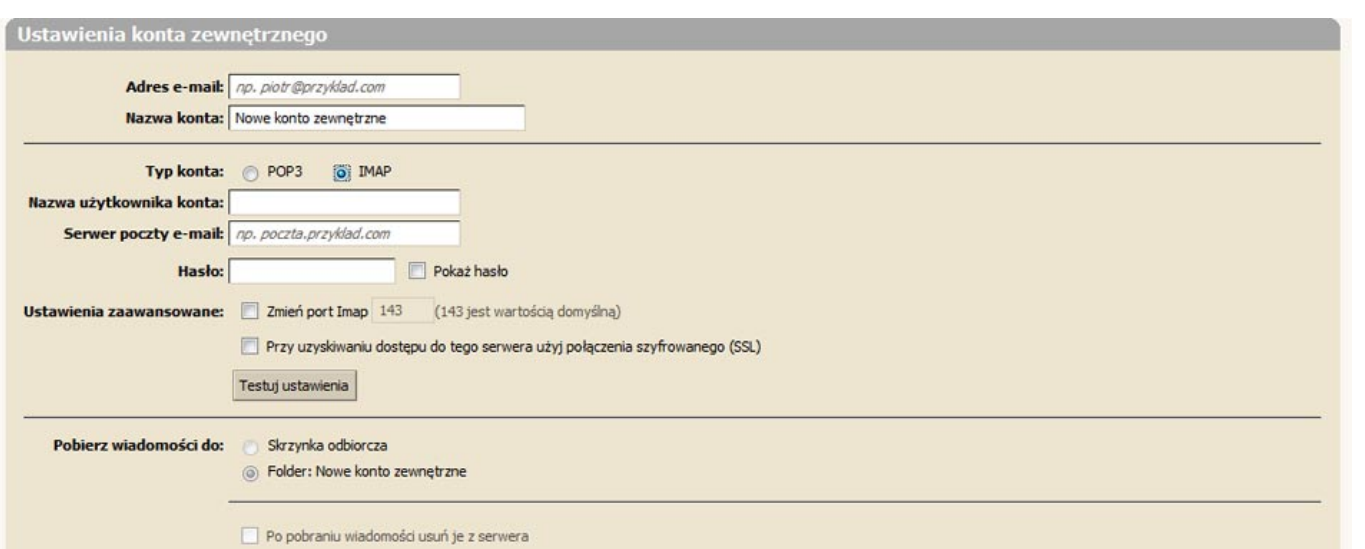
https://serwer.com:7071/zimbra/downloads/ca.der

Telefon powinien wykryć, że ściągany plik jest certyfikatem głównym i zaproponować jego zainstalowanie. Po tym kroku połączenia szyfrowane powinny działać bez zarzutu.

Warto zwrócić uwagę na fakt, że w wersji 6.0.6 Zimbra Collaboration Suite wprowadzono wiele poprawek dotyczących urządzeń mobilnych, w tym obsługę nowszych telefonów Nokia. Zatem w przypadku problemów zalecany jest upgrade do przynajmniej tej wersji.

Konta, współdzielone elementy, listy dystrybucyjne - czyli Zimbra w firmie

Powyżej opisałem, jak przejść z innych popularnych systemów pocztowych na Zimbrę oraz jak skonfigurować urządzenia przenośne. Jednak często pojawia się bardzo proste pytanie: „Jak skonfigurować Zimbrę u mnie w firmie”? Wbrew pozorom nie jest to pytanie proste. Pewne rzeczy w ZCS można zrobić na wiele sposobów, a co za tym idzie czasem może być trudno wybrać ten najszybszy i najprostszy. Spróbuję



Rysunek 2. *Migracja z IMAP/POP3 metodą przeciągnij i upuść za pomocą konta zewnętrznego*

przedstawić poniżej przykładową konfigurację systemu w średniej firmie.

W firmie mamy *n* pracowników, tworzących działy, a każdy pracownik ma swoje konto ZCS. My chcemy utworzyć wspólny kontakt dla wszystkich pracowników biurowych *biuro@naszafirma.com*. Sposobów jest wiele, ale wiążą się one z różnymi sposobami obsługi takiego wirtualnego konta.

Po pierwsze, możemy utworzyć listę dystrybucyjną *biuro@naszafirma.com,* umieścić w niej wszystkich pracowników biurowych. Przy tej opcji problem stanowi fakt, że listy dystrybucyjne w ZCS działają na zasadzie aliasu z wieloma adresami. Oznacza to, że kopia maila wysłanego na taką listę trafia do wszystkich odbiorców z osobna. Czasem jest to zamierzone działanie, jednak w większości wypadków jest to problematyczne, ponieważ nie mamy kontroli nad odpowiedziami na taką wiadomość. Innym problemem są odpowiedzi, które wysyłane są z różnych adresów e-mail (adresu konkretnego pracownika). Osoba pisząca do naszej firmy na adres *biuro@* może mieć problemy z ogarnięciem maili od 3 różnych pracowników, z 3 różnych adresów. Poza tym, pracownik firmy odpowiadając na taką wiadomość, powinien w kopii umieścić adres *biuro@,* tak żeby inni wiedzieli, że na tę wiadomość już odpowiedziano, unikając w ten sposób wielokrotnego odpisywania na jedno zapytanie.

Drugim sposobem, zdecydowanie bardziej zalecanym, jest utworzenie dodatkowego konta *biuro@naszafirma.com* i udostępnienie folderów *odebrane* i *wysłane* wszystkim pracownikom biurowym. Dzięki takiemu rozwiązaniu można odpowiedzieć na wiadomość w imieniu (*on behalf of*) *biuro@naszafirma.com* sprawiając, że nasz klient, szukając korespondencji z naszą firmą, będzie wyszukiwał zawsze jednego adresu e-mail.

Rysunek 4. *iPhone najlepiej wspieranym przez ZCS urządzeniem*

Rysunek 5. *Windows Mobile sprawia problemy z certyfikatami*

Rysunek 6. *Symbian jest kolejną platformą obsługiwaną przez ZCS*

Warto również udostępniać kalendarze, dając innym wgląd czy też możliwość edycji naszych wydarzeń. W takiej konfiguracji ogranicza nas tylko wyobraźnia: możemy wyobrazić sobie system planowania produkcji na zasadzie kalendarzy Zimbra. Linie produkcyjne są w rzeczywistości zwykłymi kontami z udostępnionymi kalendarzami, kierownicy umieszczają plany produkcyjne w takim kalendarzu (mają prawa do edycji), a pracownicy rozpoczynając zmianę sprawdzając, jaki jest plan (tylko do odczytu).

Podsumowanie

Powyższy artykuł to tylko fragment dużych działów, jakimi są migracja, konfiguracja urządzeń przenośnych czy też zastosowanie Zimbry. Pełne opisanie tych zagadnień jest niemożliwe.

W ostatniej części opiszę konfigurację i zarządzanie ZCS od strony administratora (Hierarchical Storage Management, prosty clustering, analiza wydajności i logów). Zapraszam !

1 *http://www.microsoft.com/downloads/en/NoResults.aspx?displaylang=en-US&freetext=sslchainserver*

PIOTR KUPISIEWICZ

Open-Source to jego hobby, znany z projektów EKG i EKG2. Właściciel firmy DELTEK.

Kontakt: piotr@deltek.pl

http://deltek.pl/

Okiem w chmurach

Nie jesteśmy dużą firmą, ale oferując projekt typu Open Source, pracujemy z takimi potentatami jak IBM, Telefonica czy SFR. Google ma ogromny rynek, ale jest też inny rynek użytkowników o konkretnych potrzebach – tajności informacji, prywatności i dostępności danych na platformie typu Cloud. Rynek ten chce kontrolować kod i opracowywać własne aplikacje, ten rynek szuka rozwiązań typu eyeOS. Jordi Collell – eyeOS Chief Communications Officer oraz eyeOS Community Global Leader

Przez wiele lat byliśmy świadkami nowych trendów i zmian w sposobie użytkowania komputerów, trudno jednak nazwać większość z tych zmian rewolucyjnymi, a raczej należało by skłonić się do określenia ich mianem ewolucji. Wszystko wskazuje jednak na to, iż nadchodzące lata przyniosą dużo radykalnych zmian. Zmiany te nie powinny jednak dziwić nikogo, kto z wyprzedzeniem obserwuje rozwój Internetu, gdyż to właśnie w nim powinniśmy doszukiwać się nadchodzącej przyszłości.

Nagły rozwój Chmur Obliczeniowych (ang. *Cloud computing*), które wbrew pozorom nie są niczym nowym, rozpoczął się w roku 2007 za sprawą firm takich jak Google, Apple czy Microsoft. Tempo dodatkowo mocno zostało podkręcone przez firmę Asus, która wprowadziła na rynek ukierunkowane na pracę w Internecie; bardzo małe o niskich parametrach sprzętowych laptopy EeePC. Nie ulega wątpliwości, iż wraz ze wzrostem popularności Chmur Obliczeniowych stopniowo tracić będą na popularności oraz przydatności systemy operacyjne, jakie w tej chwili znamy i używamy. Prekursorzy rozwiązań Cloud od niedawna zapowiadają nowe rozwiązania; Google opracowuje na bazie Linuksa swojego ChromeOS, Microsoft zapowiedział, iż Windows 7 będzie ostatnim systemem Windows, jakiego znamy w formie, w której występował od swoich początków. Nasze ulubione systemy spod znaku pingwina wcale nie są na tym polu w tyle. Trudno jednak oprzeć się wrażeniu, że wymienione wyżej systemy operacyjne nie są do końca niczym nowym, a raczej dobrze znanymi rozwiązaniami dostosowanymi do nowych potrzeb i zmian. Są jednak rozwiązania, które starają się iść o krok dalej, zrywając z koncepcją systemu rezydującego na maszynie, przenosząc go w całości do przeglądarki internetowej, mowa tutaj o tak zwanych internetowych systemach operacyjnych. Jednym z najpopularniejszych systemów tej klasy jest otwarto-źródłowy; rozwijany na licencji AGPL eyeOS, któremu to właśnie poświęcona będzie dalsza część tego artykułu.

Garść historii

EyeOS jest stosunkowo młodym projektem. Jego pierwsza wersja ujrzała światło dzienne w 2005 roku, była to jednak bardziej koncepcja oraz próba stworzenia czegoś nowego, niż w pełni funkcjonalny i gotowy do użytkowania produkt. Projekt dzięki swojej unikalności bardzo szybko zaskarbił sobie uwagę deweloperów i użytkowników z całego świata, czego konsekwencją było powstanie szybko rozwijającej się społeczności pracującej nad eyeOS. W roku 2007 miało miejsce wydanie pierwszej stabilnej wersji, a kilka miesięcy później doszło do otwarcia kodu projektu. EyeOS od niedawna może pochwalić się również wsparciem ze strony takiego giganta jak IBM czy też wydaniem w marcu tego roku nowej innowacyjnej wersji 2.0. Warto wspomnieć również, że przez te kilka lat ist-

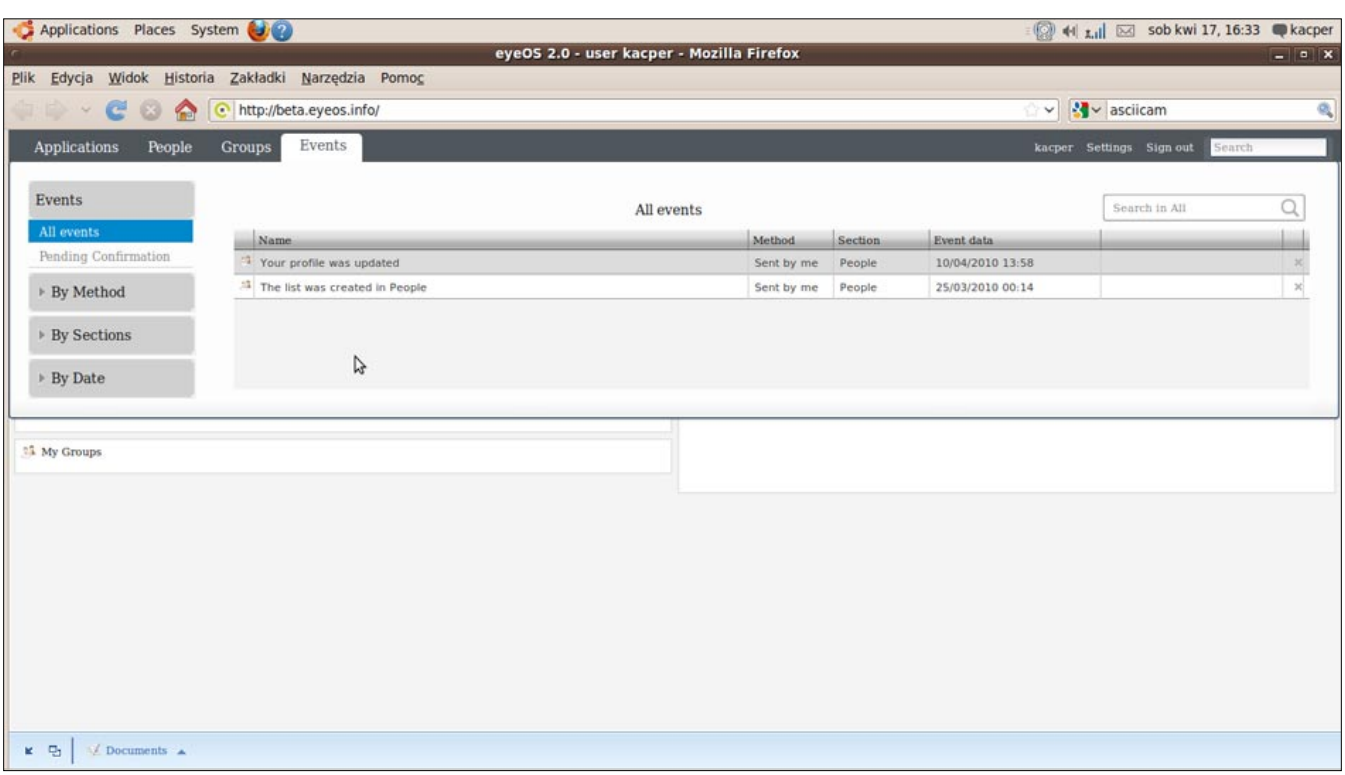
nienia eyeOS był wielokrotnie zdobywcą różnych nagród i wyróżnień.

EyeOS 2.0 – szybciej, wydajniej, prościej?

Podczas prac nad nową wersją eyeOS w celu poprawy wydajności systemu przeanalizowano i wprowadzono w życie wiele nowych koncepcji. Pierwsze, co od razu powinno rzucić się nam w oczy po zalogowaniu do nowego eyeOS, to z pewnością pulpit. Poprzednie wersje eyeOS oferowały znane wszystkim ze standardowych systemów operacyjnych podejście do pulpitu opierającego się o panele i ikony. W nowej wersji systemu pulpit został całkowicie przeprojektowany i dzięki temu stał się on bardziej funkcjonalny i intuicyjny. Wyświetla on teraz najistotniejsze informacje na temat aktualnej sesji, ponadto w szybki i wygodny sposób umożliwia dostęp do najczęściej używanych aplikacji czy funkcji systemu. Wszystkie te zmiany sprawiają, że podczas pierwszego kontaktu z nowym eyeOS mamy wrażenie, iż jest to raczej narzędzie wspomagające pracę grupową czy system zarządzania dokumentami(ang. *Document Management System*), niż wirtualny system operacyjny. Jednak zwolennicy standardowego podejścia do kwestii zarządzania pulpitem nie powinni zbyt długo narzekać, gdyż w kolejnych wydaniach planowane jest zaoferowanie użytkownikom możliwości wyboru modelu pulpitu, który preferują.

Praca w Chmurze

Dogłębnej przebudowie uległy również takie istotne elementy systemu, jak menadżer plików, klient poczty czy procesor tekstu. Aplikacje te poza zmianami interfejsu wzbogaciły się w dodatkowe opcje i funkcjonalności, które zostały przede wszystkim ukierunkowane na pracę grupową. W każdej chwili z poziomu aplikacji mamy dostęp do Social Bar-u, dzięki któremu możemy błyskawicznie i intuicyjnie udostępniać pliki, dodawać do nich tagi oraz uzyskać szczegółowe informacje na ich temat. Użytkowników, którzy często pracują z dokumentami, ucieszyć powinna nowa wersja eyeDoc, która została wyposażony na przykład w dwa tryby pracy; podstawowy – oferujący tylko niezbędne i kluczowe funkcje, oraz zaawansowany. W tym drugim trybie otrzymujemy dostęp do takich przydatnych, moim zdaniem, funkcji jak transformacja zaznaczonego tekstu w duże litery i na odwrót. Ponadto pracując grupowo nad dokumentem, żaden użytkownik nie powinien mieć problemu z odnalezieniem zmodyfikowanych przez innych użytkowników linii tekstu, gdyż są one na bieżąco odpowiednio wyróżniane. Ponadto eyeDoc został wyposażony w przydatną funkcję przeglądania historii zmian, dzięki której możemy śledzić postęp naszej pracy. Niestety wielu dotychczasowych użytkowników, zwłaszcza domowych, może czuć się lekko rozczarowana nową wersją eyeOS, gdyż wyraźnie została ona zaprojektowana z myślą o wykorzystaniu w firmach i instytucjach. Zawiera ona także dużo mniej domyślnych aplikacji niż starsze wersje. Deweloperzy po prostu postanowili skupić się na istotnych elementach systemu, pozostawiając stworzenie dodatkowych aplikacji społeczności. W repozytorium aplikacji eyeOS Apps[1]



Rysunek 1. *Centrum zarządzania wydarzeniami*

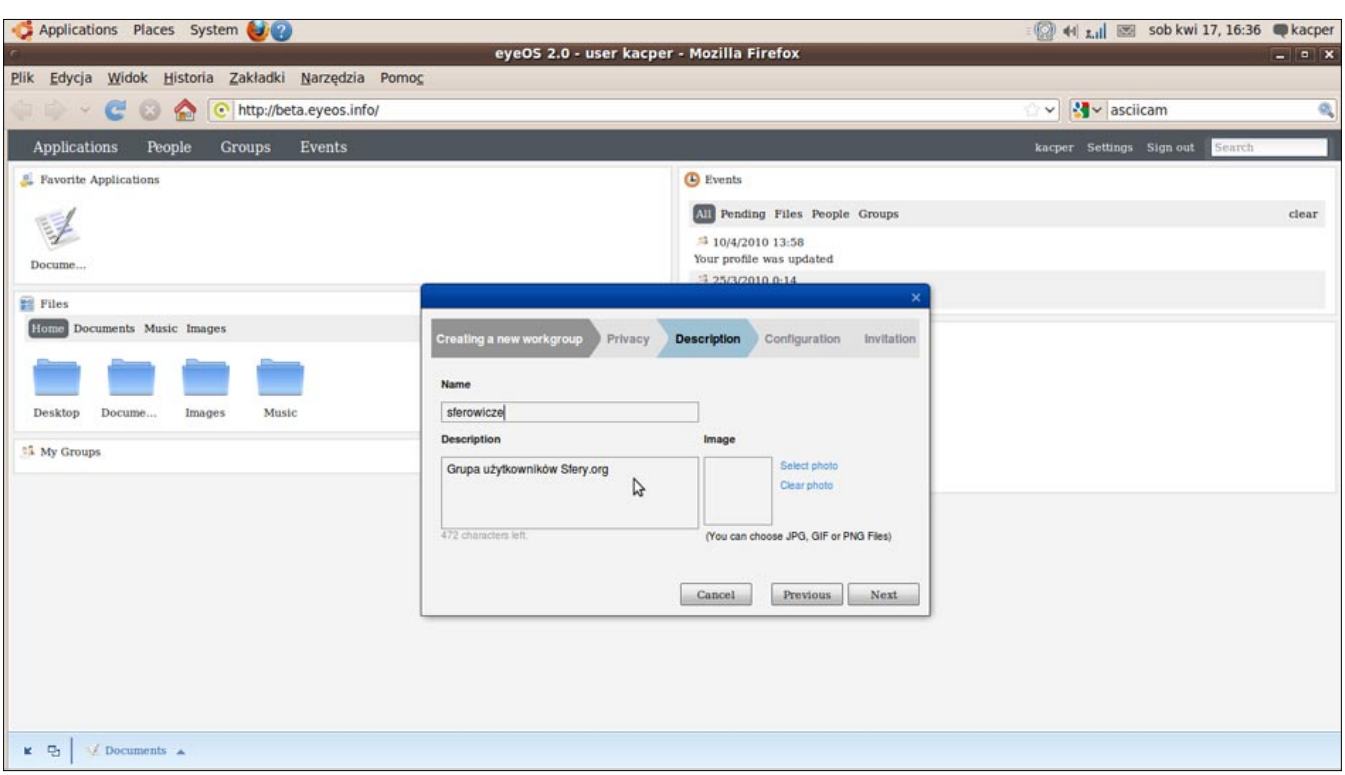
znaleźć możemy bogaty katalog dodatkowego oprogramowania. Jednak takie oprogramowanie może zostać zainstalowane tylko przez administratora, powinniśmy o tym pamiętać, korzystając z jednej z publicznie dostępnych instalacji tego systemu. Niestety podczas dłuższej pracy z nowym eyeOS szybko zauważymy, że nie wszystko działa jeszcze jak powinno. Kluczowe aplikacje, takie jak eyeDoc, posiadają kilka irytujących błędów, braków czy nie działających jeszcze funkcji. Wiele osób zapewne zada pytanie; dlaczego w takim razie doszło do publikacji wersji uchodzącej za stabilną, a która najwyraźniej taka nie jest? Sytuacja jest tutaj bardzo podobna, jak w przypadku wydania pierwszej stabilnej wersji środowiska graficznego KDE z serii 4. Główne komponenty eyeOS są już na tyle dopracowane, że programiści zdecydowali się wydać wersję stabilną, by zachęcić niezależnych deweloperów do prac nad nowymi aplikacjami czy też przepisaniem programów kompatybilnych ze starszymi wersjami, by działały również z nową wersją eyeOS.

A pod maską silnik rwie!

Nikogo nie powinno zdziwić, że nowy eyeOS to nie tylko zmiany od strony wizualno-użytkowej. Podczas projektowania tego wydania wydarzyło się bardzo wiele pod samą „maską" systemu. I tak mamy tutaj: kompletnie nowe jądro oraz część bibliotek czy usług. Wszystko zostało mocno zoptymalizowane, by radzić sobie jeszcze lepiej z większymi obciążeniami. Mocnym usprawnieniom został poddany również sposób komunikacji klienta z serwerem, tak że nowy eyeOS wykonuje teraz, zdaniem jego deweloperów, o 95% mniej wywołań w porównaniu z wcześniejszymi wersjami. Zrezygnowano również z wykorzystania XML na rzecz JSON, co dodatkowo uczyniło cały proces komunikacji wydajniejszym. Programiści zapewniają, że dzięki tym zmianom udało się osiągnąć dużo większą integralność środowiska oraz znacznie lepszą wydajność działania całego systemu. Jednak, jak pisałem wcześniej, na razie bywa z tym różnie, a całość potrafi czasem mimo wszystko strasznie zwolnić. Dużo pracy włożono również w usprawnienie i ułatwienie pisania nowych aplikacji. Cały interfejs użytkownika został oparty o zorientowany obiektowo JavaScript-owy framework QooxDoo, natomiast dzięki wykorzystaniu biblioteki GenericDao zyskujemy możliwość odczytu i zapisu bazy danych bez konieczności znajomości języka SQL. Ponadto osoby, które w przyszłości chciałyby zająć się tworzeniem aplikacji dla eyeOS, powinny zainteresować się EyeDesigner, który udostępnia programiście kompletne środowisko projektowe.

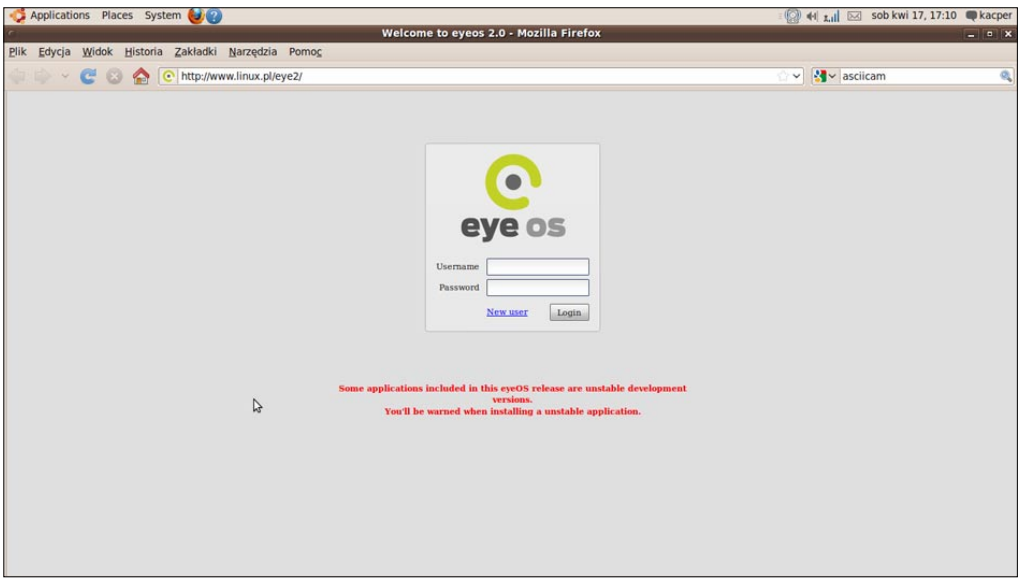
Dla kogo eyeOS?

Jak pisałem wyżej, nowy eyeOS to przede wszystkim spójne środowisko pracy grupowej oraz zarządzania osobistymi informacjami (ang. *Personal Information Management*). Dlatego też aktualny kształt i droga, jaką obrali twórcy w nowym wydaniu, skłania mnie do wniosku, iż eyeOS oddał przynajmniej na razie część rynku Chmur Obliczeniowych skierowanych do domowych użytkowników Google i jego nadchodzącemu ChromeOS. Skupiając się przy tym na niszy rozwią-



Rysunek 2. *Kreator grup roboczych*

zań Cloud dla firm oraz użytkowników szukających tego typu rozwiązań oferujących większą prywatność, spójność środowiska pracy oraz otwartość kodu czy też możliwość hostowania tego systemu na własnym serwerze, na przykład w naszej firmie. Dodatkowo dzięki możliwości zdobycia komercyjnego wsparcia technicznego czy też fakt współpracy eyeOS z takim gigantem jak IBM wpływa korzystnie na ewentualne rozważania na temat wykorzystania go w komercyjnych zastosowaniach.



Rysunek 3. *Ekran logowania eyeOS*

Oczywiście wymienione wyżej cechy najnowszego eyeOS nie sprawiają jednoznacznie, iż stał się on nieprzydatny na przykład dla studentów, którzy chcieliby mieć wszystkie notatki i materiały w Chmurze. Użytkowników domowych zachęcałbym jednak do założenia konta na jednej z wielu dostępnych instalacji publicznej niż próby instalacji tego systemu na koncie hostingowym[2][3][4][5]. Za postępowaniem takim przemawiają znacznie większe wymagania stawiane serwerowi, na którym mamy zamiar zainstalować eyeOS, który ponadto do osiągnięcia pełnej funkcjonalności wymaga na przykład instalacji po stronie serwera OpenOffice z serii 2 w celu obsługi popularnych formatów dokumentów. Więcej na temat wymagań systemowych znajdziemy tutaj[6], natomiast z przewodnikiem instalacji tutaj[7]. Starsze wersje mimo dużo niższych wymagań stawianych serwerowi często wymagały instalacji dodatkowego oprogramowania po stronie stacji klienckiej, co skutecznie uniemożliwiało uzyskanie pełnej funkcjonalności podczas korzystania z rozwiązań typu Splashtop[8]. Niestety na dzień dzisiejszy z powodu różnych niedociągnięć odradzałbym używania wersji 2.0 do normalnej codziennej pracy, i zalecał poczekać na wydanie odpowiednich poprawek lub używanie przynajmniej na razie starszej wersji.

Podsumowanie

Wyraźnie widać, że deweloperzy podczas prac nad wersją 1.x zdobyli dość doświadczenia, by wyznaczyć dla tego projektu konkretne zastosowanie, a także kierunek dalszego rozwoju. Duża część osób traktowała dotychczas eyeOS jako mało przydatny „system w systemie", nie widząc w nim przyszłości czy konkretnego zastosowania. Nowa wersja udowadnia że przeglądarkowe systemy posiadają potencjał, który tylko czeka, by go wykorzystać, jednak, jak widać, wymaga to zmiany podejścia i odcięcia się od utartych konwencji czy rozwiązań. Wykorzystanie rozwiązań takich jak omawiany tutaj eyeOS w naszych przedsiębiorstwach może wyraźnie zredukować koszty związane z zakupem odpowiednich licencji, czyniąc ponadto środowisko pracy odpornym na awarie wynikające z problemów po stronie klienta. Zyskujemy również dostęp do naszych danych wszędzie tam, gdzie tego sobie życzymy.

Mimo wielu pozytywnych zmian jednym z większych braków, jakie można zarzucić eyeOS, jest wsparcie dla pracy w trybie offline. Udało mi się jednak dowiedzieć, iż prace już trwają ,a wsparcia dla trybu offline powinniśmy spodziewać się w nadchodzących wydaniach.

Na skróty

- *http://eyeos-apps.org/*
- *http://classic.eyeos.info/* – eyeOS 1.x
- *http://beta.eyeos.info/* – eyeOS 2.x
- *http://eye.linux.pl/* – eyeOS 1.x na serwerze Linux.pl
- *http://linux.pl/eye2/* – eyeOS 2.x na serwerze Linux.pl
- *http://eyeos.org/index.php?p=downloads*
- *http://www.eyeos.org/installation_manual.pdf*
- *http://en.wikipedia.org/wiki/Splashtop/*

KACPER PLUTA

Na co dzień student Wyższej Szkoły Informatyki w Łodzi oraz wiceprezeses stowarzyszenia Pleszew XXI. Pasjonat Wolnego Oprogramowania, dobrej muzyki i książek.

Od niedawna stara się blogować na http://copyme.jogger.pl

Oprogramowanie Open Source wspomagające zarządzanie serwerami

W niniejszym artykule chciałbym przedstawić narzędzia Open Source, które mogą być przydatne osobom zajmującym się administracją serwerów. Są to narzędzia darmowe i oferujące szerokie możliwości.

Jak ciężka jest praca administratora serwera, nie trzeba chyba wyjaśniać. Jeszcze więcej pracy pojawia się w sytuacji, gdy pod opieką mamy kilka lub nawet kilkanaście/kilkadziesiąt serwerów. W takim przypadku warto wspomóc swoją pracę narzędziami, które nie tylko przyspieszą naszą pracę, ale również wpłyną na szybszą reakcję na pojawiające się problemy.

Panel administracyjny, analiza logów, monitoring serwerów

Bardzo często w momencie zakupu serwera dedykowanego lub VPS stajemy przed wyborem kilku komercyjnych paneli administracyjnych. Jeżeli do zarządzania dostajemy nowy serwer, warto rozważyć zastosowanie paneli Open Source, które oferują równie ciekawe funkcje co ich komercyjne odpowiedniki.

Webmin

Wartym rozważenia panelem administracyjnym jest pakiet Webmin. Jest to bardzo proste oprogramowanie napisane w perlu i uruchamiane na zarządzanym serwerze. Zdalne zarządzanie oraz konfiguracje przeprowadzane są za pomocą przeglądarki internetowej, np. Opera, Firefox i wiele innych. Aktualną dostępną wersją oprogramowania Webmin jest wersja 1.510. Pobrać ją można ze strony domowej projektu. Instalacja pakietu również nie stanowi problemu. W przypadku systemów Ubuntu/Debian wystarczy wykonać następującą sekwencję poleceń:

```
trustcom:~# wget -c http://prdownloads.sourceforge.net/
                    webadmin/webmin_1.510-2_all.deb
```

A następnie:

```
trustcom:~# dpkg --install webmin_1.510-2_all.deb
```

W przypadku otrzymania komunikatu o błędzie zależności należy wykonać polecenie uzupełniające brakujące pakiety. W tym celu wpisujemy:

```
trustcom:~# apt-get install -f
```

Otrzymamy informację o tym, jakie pakiety zostaną zainstalowane. Zatwierdzamy zmiany i powinniśmy otrzymać pod koniec komunikat o treści:

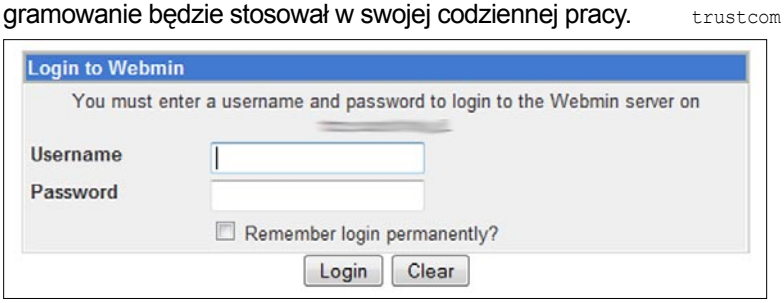
```
** initializing cache. This may take a while **
Setting up webmin (1.510-2) ...
Webmin install complete. You can now login to https://
                    localhost:10000/
as root with your root password, or as any user who can
                    use sudo
to run commands as root.
trustcom:~#
```

W tym momencie jest to dla nas informacja, że pakiet Webmin został pomyślnie zainstalowany. Aby zalogować

się do panelu, należy odwiedzić adres strony podany wyżej i zalogować się jako root lub użytkownik posiadający uprawnienia roota. Po wpisaniu adresu w przeglądarce Firefox możemy otrzymać komunikat o błędnym certyfikacie. Można oczywiście dodać wyjątek i wtedy pojawi się okno logowania. Bardziej zaawansowani użytkownicy mogą zaktualizować certyfikaty SSL. Pakiet Webmin działa standardowo na porcie 10000. Okno logowania wygląda tak jak na Rysunku 1.

Po zalogowaniu się do panelu mamy dostęp do całej gamy funkcji umożliwiających zarządzanie takimi usługami jak (w zależności od zainstalowanych pakietów na zarządzanym serwerze): Apache, Bind, MySQL, Fetchmail, Postfix, Sendmail, Zadania Cron i wiele, wiele innych. Oczywiście oprócz tego Webmin daje nam możliwość zarządzania typowymi pracami administratora, np. zarządzanie logami systemowymi, wykonywanie kopii zapasowych itp. (Rysunek 2).

Zaletą pakietu Webmin jest niewątpliwie jego szybkie działanie, co nie jest bez znaczenia na słabszych maszynach. Na pewno jest to pakiet warty rozważenia. Oczywiście podobnych rozwiązań jest znacznie więcej i tak naprawdę tylko od administratora serwera zależy, które oprogramowanie będzie stosował w swojej codziennej pracy.



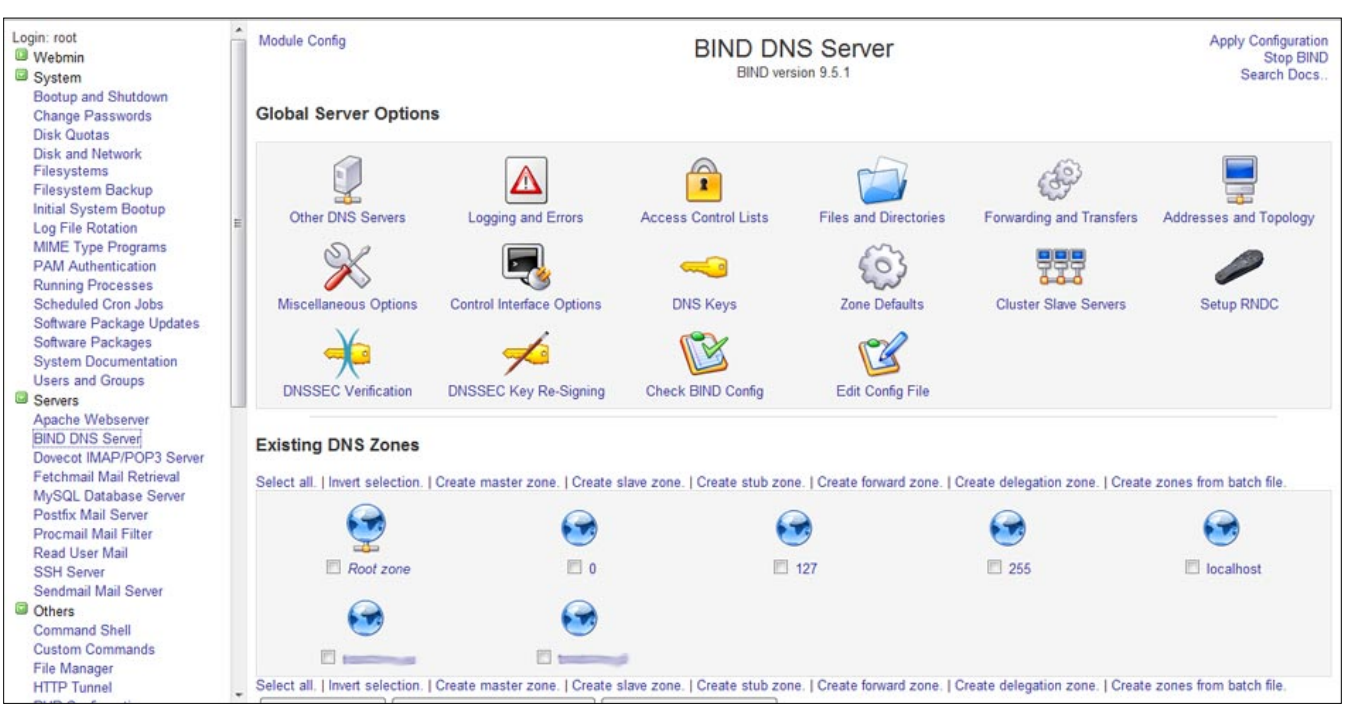
Rysunek 1. *Okno logowania do panelu Webmin*

Logwatch

O tym, jak ważne jest przeglądanie logów systemowych, nie trzeba chyba przekonywać żadnego szanującego się administratora. Pojawia się tylko pytanie, czy pamiętamy o tym, żeby systematycznie przeglądać zawartość logów? Najczęstszym przypadkiem jest przeglądanie logów w momencie pojawienia się problemów np. z pocztą elektroniczną lub np. po włamaniu na serwer. Bardzo często jest to przysłowiowa musztarda po obiedzie. Tym bardziej że pierwsze symptomy problemów pojawiają się wcześniej niż nastąpi faktyczna awaria. Zatem regularne przeglądanie logów uchroni nas przed poważniejszymi problemami. Warto w takim przypadku rozważyć zastosowanie oprogramowania logwatch. Jakie możliwości oferuje nam ten pakiet? Otóż okazuje się, że jest to bardzo skuteczne narzędzie przy codziennej administracji. W zależności od konfiguracji możemy na naszą skrzynkę pocztową otrzymywać zbiorcze zestawienie logów działających usług. Szczególnie jest to przydatne, kiedy pod opieką mamy kilka serwerów i przeglądanie pojedynczych logów sprawiłoby problem. Instalacja pakietu jest bardzo prosta. W przypadku systemów Ubuntu/Debian wystarczy wydać polecenie:

```
trustcom:~# apt-get install logwatch
```

I tym samym mamy już zainstalowany pakiet logwatch. Teraz pozostaje tylko odpowiednia konfiguracja. Logwatch jest tak elastycznym oprogramowaniem, że bez problemów można go dopasować do własnych potrzeb. W zależności od dystrybucji położenie pliku konfiguracyjnego może być różne. W przypadku dystrybucji Debian Lenny 5.0 jest to:



Rysunek 2. *Panel administracyjny Webmin*

```
/usr/share/logwatch/default.conf/logwatch.conf
```

Jeśli chodzi o plik konfiguracyjny, warto zwrócić uwagę na kilka istotnych szczegółów. Po pierwsze, jeśli chcemy otrzymywać informacje na maila, warto podać poprawny adres mailowy. Może to być adres systemowy, np. Root, jak również *jan@kowalski.pl*. Parametr odpowiadający za wysyłanie e-maili to: `MailTo`. Kolejnym elementem jest archiwum. Warto się zastanowić nad tym, czy logwatch ma „magazynować" zbiór logów. Parametr odpowiadający za tę funkcję to: `Archives = Yes` (lub `No`, jeśli nie chcemy tworzenia archiwum). Kolejnym ważnym parametrem jest rodzaj MTA zainstalowanego na serwerze. W domyślnej konfiguracji obsługiwanym programem jest sendmail. W przypadku Postfiksa należy zmienić parametr: mailer na:

```
mailer: „/usr/sbin/postfix".
```

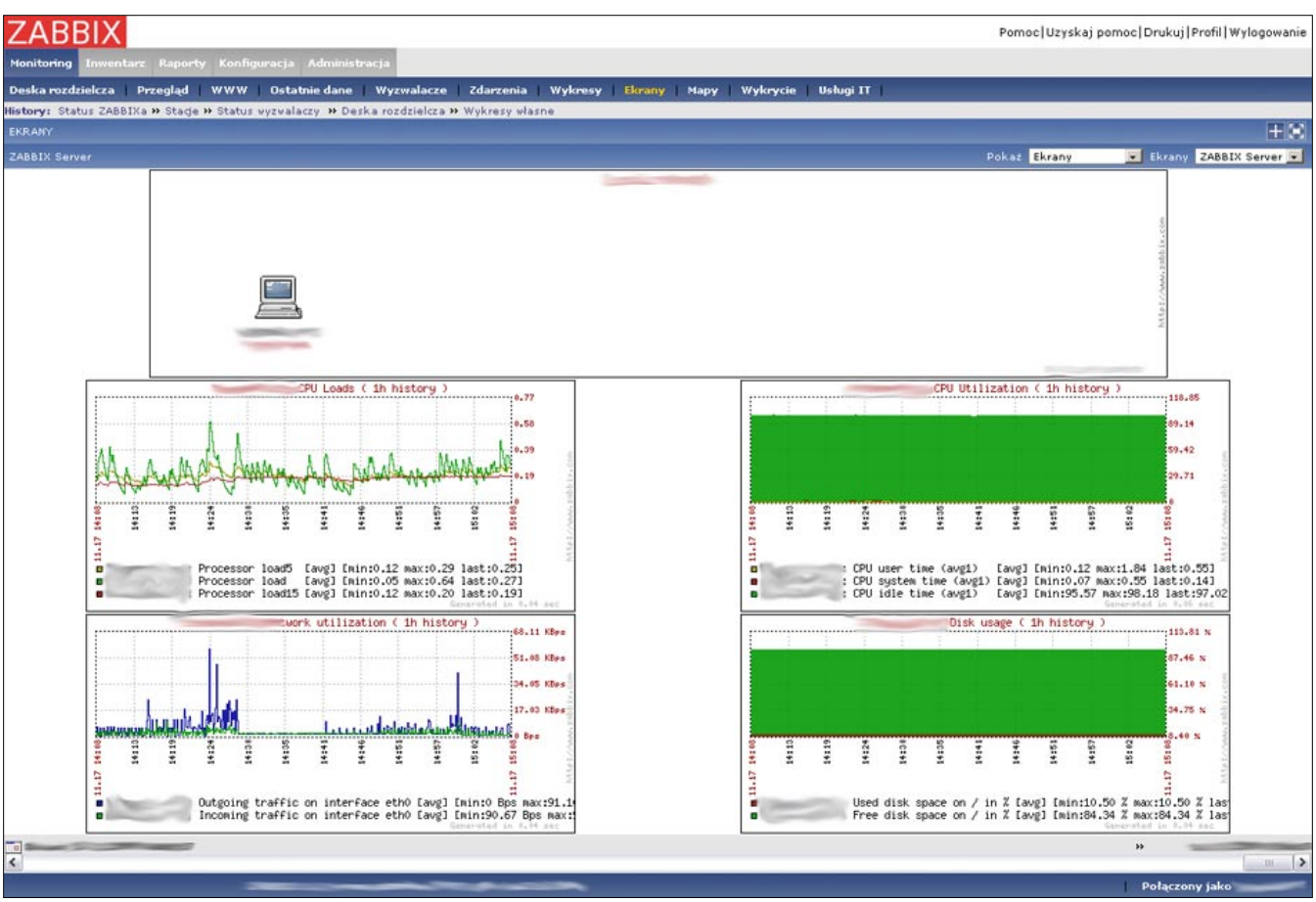
Kolejnym istotnym elementem jest okres czasu raportowania. Logowatch obsługuje 3 możliwości (All, Yesterday, Today). Parametr odpowiedzialny za to:

```
Range = Today.
```

Warto pamiętać również o ustawieniu zadań Cron. W przypadku domyślnych ustawień, raport jest generowany około godziny 1 w nocy. Oczywiście nic nie stoi na przeszkodzie, żeby zmienić te ustawienia w tabeli Cron. Przykładowy raport otrzymany z programu logwatch (Listing 1).

Oczywiście w zależności od skonfigurowanych parametrów raport może być mniej lub bardziej szczegółowy. Bar-

Rysunek 3. *Okno logowania monitora Zabbix*



Rysunek 4. *Panel administracyjny Zabbix'a*

Listing 1.

```
################## Logwatch 7.3.6+cvs20080702-debian (07/02/08) ####################
        Processing Initiated: Thu Apr 20 02:39:09 2010
        Date Range Processed: today
                              ( 2010-Apr-20 )
                              Period is day.
        Detail Level of Output: 5
        Type of Output/Format: mail / text
        Logfiles for Host: localhost
  ##################################################################
-------------------- httpd Begin ------------------------

 0.30 MB transferred in 57 responses  (1xx 0, 2xx 46, 3xx 4, 4xx 7, 5xx 0)
     1 Archives (0.00 MB),
    56 Content pages (0.30 MB),
```

dziej zaawansowane opcje są opisane w dokumentacji pakietu dostępnej na stronie domowej projektu.

Zabbix

Nie można mówić o właściwym i poprawnym zarządzaniu serwerami bez ich stałego monitorowania. W jakim celu serwery są monitorowane? Przede wszystkim w celu uniknięcia poważniejszych awarii oraz szybkiego reagowania na pojawiające się problemy (np. znaczne obciążenie procesora, pamięci RAM itp.). Zastosowanie pakietu Zabbix jest na pewno ciekawą alternatywą dla bardzo drogich monitorów sieci. Uwaga: do poprawnego działania wymagane są działające takie usługi jak: apache, php, mysql. Instalacja w przypadku dystrybucji Debian Lenny 5.0 wygląda następująco.:

```
trustcom:~# apt-get install zabbix-server-mysql zabbix-
                    frontend-php zabbix-agent
```

W trakcie instalacji będziemy pytani o ustawienia zabbix'a, np. nazwa i hasło użytkownika bazy danych, dane serwera itp. Warto też sprawdzić w /etc/services, na którym porcie działa Zabbix z tego względu, że czasami (w zależności od dystrybucji) może się okazać, że domyślnym portem jest port 10000, na którym działa również wyżej opisany Webmin.

W Sieci

- *http://www.webmin.com* – Strona domowa projektu Webmin (en);
- *http://www.isp-control.net* – Rozbudowany panel IspCP (alternatywa dla cPanel, DA);
- *http://www.logwatch.org/* – Strona domowa projektu logwatch;
- *http://www.zabbix.com/* – Strona domowa projektu Zabbix;
- *http://www.nagios.org/* – Strona domowa projektu Nagios – alternatywa dla Zabbix.

Teraz wystarczy w przeglądarce wpisać:

```
http://localhost/zabbix
```

i pojawi się okno logowania (Rysunek 3).

Warto też pomyśleć nad tym, aby przeznaczyć jeden komputer na monitorowanie serwerów, ze względu na to, że Zabbix oferuje nam możliwość pracy jako główny serwer oraz jako agent. Jest to doskonałe rozwiązanie, jeśli zależy nam na ciągłym obserwowaniu tego, co się dzieje z serwerami będącymi pod naszą opieką.

Zabbix oferuje nam możliwość monitorowania wielu funkcji, np. obciążenie procesora, ruch, wykorzystanie pamięci i wiele innych. Poniżej przykładowy ekran (Rysunek 4).

Konkurentem dla pakietu Zabbix jest Nagios. Jest to już bardziej zaawansowane narzędzie i niestety dużo trudniejsze w konfiguracji. Nie mniej jednak przy bardziej rozbudowanym środowisku warto wziąć go pod uwagę.

Podsumowanie

Niestety, nie ma fizycznej możliwości omówienia wszystkich niezbędnych narzędzi przydatnych w codziennej pracy administratora. Mam nadzieję, że powyższe narzędzia poprowadzą Was w dobrym kierunku. Warto je stosować w codziennej pracy ze względu na to, że bardzo ułatwiają standardowe zadania. Szczególnie jest to ważne, jeśli pod „naszymi skrzydłami" znajduje się kilkanaście serwerów i ew. awaria może spowodować duże szkody i utrudnić życie nie tylko użytkownikom, ale przede wszystkim administratorom.

PRZEMYSŁAW SZOSTAK

Pasjonat Linuksa od przeszło 11 lat. Właściciel firmy TRUSTCOM Systemy Informatyczne zajmującej się m.in. administracją serwerów.

Kontakt z autorem: przemyslaw.szostak@trustcom.pl

Software Developer's

new ideas & solutions for professional programmers

NR 6 CZERWIEC 2010 (186)

Już do pobrania ze strony SDJ
Pobierz

REWOLUCJA ON

BIBLIOTEKA MIESIĄCA

BIBLIOTEKA DOZER
PROSTE MAPOWANIE OBIEKTÓW

PARADYGMAT CLP
PRZYKŁADY PROBLEMÓW OPTYMALIZACYJNYCH ORAZ LOGICZNYCH

ANDROID NDK
CZYLI PROGRAMOWANIE NATYWNE W SYSTEMIE ANDROID

STARY, DOBRY ZNAJOMY: ORACLE FORMS

BRAKUJĄCY 1%
ZARZĄDZANIE ZAANGAŻOWANIEM PROGRAMISTÓW

TECHNOLOGIE PROGRESS OPENEDGE
CZĘŚĆ 7. REPLIKACJA I OBSŁUGA KLASTRÓW SYSTEMOWYCH W ŚRODOWISKU OPENEDGE

Zostań administratorem sieci komputerowej

Część ósma (8/9): Bezpieczeństwo sieci bezprzewodowych

W poprzedniej części cyklu przedstawione zostały podstawowe informacje niezbędne do budowy sieci bezprzewodowych standardu IEEE 802.11. W trakcie lektury zapoznałeś się również z przykładowymi konfiguracjami wykorzystującymi różne tryby pracy punktu dostępowego APPro 2405. W artykule przedstawione zostały jedynie podstawowe zagadnienia związane z bezpieczeństwem sieci bezprzewodowych; jest to jednak na tyle ważny temat, iż poświęcony jest mu cały niniejszy artykuł. Zapraszam do lektury!

We wstępie do siódmej części kursu przedstawione zostały liczne zalety bezprzewodowych sieci komputerowych standardu IEEE 802.11 – łatwość konfiguracji i podłączania nowych klientów, ograniczenie ilości uciążliwej pracy przy montażu okablowania oraz swoboda, jaką uzyskują użytkownicy. Są to cechy, które sprawiły, iż bezprzewodowe sieci komputerowe pojawiają się w coraz większych ilościach nie tylko w domach, lecz również w firmach i urzędach.

Należy mieć jednak świadomość, iż nieprawidłowa konfiguracja urządzeń bezprzewodowych może przyczynić się do narażenia całej sieci komputerowej (w tym części przewodowej). Zwróć uwagę, że każda z zalet sieci bezprzewodowej jest również bardzo atrakcyjna z punktu widzenia włamywacza. Nawet w przypadku, gdy nasza sieć nie jest wykorzystywana do przesyłania szczególnie poufnych danych, powinniśmy koniecznie zastosować chociaż podstawowe techniki zwiększania bezpieczeństwa, takie jak szyfrowanie danych przy użyciu odpowiedniego standardu.

W przypadku sieci przewodowych, w celu uzyskania dostępu do jej zasobów na takich samych uprawnieniach, jak pozostałe komputery, włamywacz musiał mieć fizyczny dostęp do gniazda sieciowego. W większości przypadków wiązałoby się to z koniecznością dostępu do pomieszczeń przeznaczonych wyłącznie dla uprawnionego personelu. W sieciach bezprzewodowych sytuacja ulega komplikacji – podjęcie próby połączenia możliwe jest w obrębie całego jej zasięgu. Wskutek użycia odpowiedniego sprzętu przez włamywacza (interfejsu sieciowego i anteny, a czasami również wzmacniacza) obszar ten może zostać znacznie zwiększony. Widać więc, iż granice naszej sieci są bardziej rozmyte niż mogłoby się nam wydawać.

Opisane powyżej zagrożenia nie wyczerpują problemów z bezpieczeństwem sieci bezprzewodowych. Nie zniechęcaj się jednak – większość z nich można wyeliminować lub znacząco ograniczyć poprzez poprawną konfigurację sieci oraz stosowanie odpowiednich praktyk, z których kilka zostanie omówionych w tym artykule. Rozpoczniemy od krótkiej charakterystyki sieci bezprzewodowych pod względem bezpieczeństwa w porównaniu do przewodowych sieci Ethernet. Następnie przedstawione zostaną podstawowe zasady poprawnej konfiguracji sieci bezprzewodowych, zapewniające poufność przesyłanych danych oraz bezpieczeństwo jej klientów. Poznasz również dystrybucję BackTrack Linux, przygotowaną specjalnie do analizy bezpieczeństwa sieci. W dalszej części omówione zostaną również najczęściej stosowane metody zabezpieczania sieci bezprzewodowych, wraz z analizą ich rzeczywistej skuteczności. Na koniec zajmiemy się wykorzystaniem znanego już Czytelnikowi programu OpenVPN w celu zabezpieczania szczególnie poufnych danych przesyłanych przy pomocy sieci bezprzewodowych.

Sieci bezprzewodowe Wi-Fi – charakterystyka pod względem bezpieczeństwa

Zastosowanie dowolnej technologii sieciowej lub oprogramowania serwerowego powinno być poprzedzone staranną analizą potencjalnych problemów z bezpieczeństwem. Podobnie jest w przypadku sieci bezprzewodowych – trudno mówić o świadomym zastosowaniu porad zawartych w tym artykule bez zrozumienia zagadnień przedstawionych w tym paragrafie.

Należy pamiętać, iż rozwiązania przedstawione w tym artykule dotyczą jedynie problemów powstających przy zastosowaniu sieci bezprzewodowych. Zagadnienia związane z bezpieczeństwem kablowych sieci Ethernet omówione zostały w poprzednich częściach kursu.

Określanie zasięgu sieci bezprzewodowej

Jednym z czynników o największym znaczeniu dla bezpieczeństwa sieci bezprzewodowej jest jej zasięg. Wydaje się to oczywiste, ponieważ brak możliwości nawiązania połączenia lub przechwytywania ramek z określonego miejsca uniemożliwia potencjalnemu włamywaczowi działanie.

W poprzedniej części kursu przedstawione zostały urządzenia wykorzystywane do budowy sieci bezprzewodowych: punkty dostępowe, interfejsy sieciowe oraz anteny. Okazuje się, iż obszar, w którym możliwe jest nawiązanie połączenia z siecią bezprzewodową może być różny w zależności od sprzętu używanego przez klienta. Użycie dobrej jakości interfejsów wraz z odpowiednią anteną umożliwia nawiązanie łączności na znacznie większym obszarze. Właściwość pozwalająca na polepszenie łączności poprzez poprawienie warunków pracy jednej z anten, nazywana jest wzajemnością.

Paradoksalnie, sieć bezprzewodowa powinna charakteryzować się jak najmniejszym zasięgiem, o ile pozwala on na podłączenie wszystkich klientów. Jak jednak w praktyce mierzyć poziom sygnału w różnych miejscach oraz w jaki sposób należy rozmieszczać punkty dostępowe? Problem ten zostanie szerzej omówiony w dalszej części artykułu.

Ataki DoS na sieci bezprzewodowe

Specyfika medium transmisyjnego, jakim są fale bezprzewodowe, zwiększa również podatność naszej sieci na ataki typu DoS (*Denial of Service* – odmowa usługi) na poziomie warstwy fizycznej. W zależności od stopnia wykorzystania pasma na danym obszarze, możliwe są również awarie transmisji nie spowodowane świadomym działaniem osób trzecich. Uruchomienie urządzenia na tym samym kanale (więcej informacji na temat kanałów transmisyjnych w sieciach IEEE 802.11 zawartych zostało w poprzedniej części cyklu) może zakłócić transmisję w dokładnie taki sam sposób, jak celowe działanie włamywacza.

Sieci bezprzewodowe standardu IEEE 802.11 działają w nielicencjonowanym paśmie ISM 2.4/5 GHz. Z jednej strony pozwala to na tworzenie nowych sieci bez potrzeby uzyskania zgody odpowiednich urzędów, z drugiej – znacznie ogranicza niezawodność łączności. Jedynym ograniczeniem, jakie narzucone jest urządzeniom działającym w tym paśmie jest maksymalna moc, wynosząca 100 mW EIRP (*Equivalent Isotropic Radiated Power* – równoważną mocy wyemitowanej przez idealną antenę dookólną). Ograniczenie to ma służyć poprawieniu jakości transmisji oraz zwiększeniu maksymalnej liczby urządzeń korzystających z łączności bezprzewodowej na danym obszarze.

Sieć bezprzewodowa a lokalna sieć Ethernet

Sieci bezprzewodowe standardu IEEE 802.11 bardzo często stosowane są jako rozszerzenie przewodowych sieci Ethernet. Poprzez odpowiednią konfigurację punktów dostępowych (opisaną w poprzedniej części kursu) umożliwia się bezpośredni dostęp klientów bezprzewodowych do zasobów sieci przewodowej. W większości przypadków jest to jednak niepożądane i naraża całą sieć na nieuprawniony dostęp.

Rozwiązaniem tego problemu jest zastosowanie firewalla oddzielającego klientów sieci bezprzewodowej od pozostałych segmentów i filtrowanie ruchu sieciowego. Urządzenia bezprzewodowe powinny znajdować się w obrębie jednej podsieci – znacząco zwiększa to bezpieczeństwo i ułatwia konfigurację routerów. Zwróć uwagę, iż sieć bezprzewodowa jest w takiej sytuacji traktowana jako sieć niezaufana (publiczna), a pochodzące z niej pakiety traktowane są na podobnych zasadach, jak w przypadku internetu i innych sieci rozległych.

Podstawowe zasady budowy bezpiecznych sieci bezprzewodowych

Po zidentyfikowaniu zagrożeń dla sieci bezprzewodowych Wi-Fi, przedstawione zostaną podstawowe zasady ich bezpiecznej budowy. Dotyczyć one będą zarówno zagadnień związanych z doborem sprzętu, jak i wykorzystania rozwiązań programowych oraz standardów szyfrowania. Szczególna uwaga zostanie poświęcona bezpiecznemu podłączaniu sieci bezprzewodowych do kablowej sieci lokalnej.

Zasięg sieci powinien być ograniczony do wymaganego obszaru

Zastosowanie odpowiednich anten oraz przemyślane rozmieszczenie punktów dostępowych, wykorzystujące przeszkody, pozwoli na uzyskanie pożądanego pokrycia obszaru sygnałem, zmniejszając jednocześnie ryzyko wykrycia przez osoby niepowołane.

W przypadku pomieszczeń zamkniętych, punkty dostępowe należy umieszczać zawsze w centrum pomieszczeń – pozwala to na pokrycie znacznej części pomieszczeń zasięgiem, nawet w przypadku zastosowania anten dookólnych o niewielkim zysku. Trudniej podać podobne porady dla połączeń punkt-punkt oraz punkt-wielopunkt na dużych odległościach. Zawsze warto jednak umieszczać anteny kierunkowe w położeniu utrudniającym osobom niepowołanym uzyskanie wysokiego poziomu sygnału.

Po każdej zmianie położenia anten lub punktów dostępowych, należy sprawdzić poziom sygnału na danym obszarze. Opisywany w dalszej części artykułu program Kismet (dostępny w dystrybucji BackTrack) doskonale sprawdzi się w tym celu.

Zawsze stosuj odpowiednie algorytmy szyfrujące

Dane przesyłane przy użyciu sieci bezprzewodowej mogą zostać przechwycone przez każdą osobę znajdującą się w jej zasięgu. Od zastosowanych algorytmów szyfrujących zależy, w jakim stopniu przechwycone informacje będą użyteczne dla potencjalnego włamywacza.

W sieciach bezprzewodowych standardu IEEE 802.11 zastosowane mogą zostać trzy standardy szyfrujące: WEP (*Wired Equivalent Privacy*), WPA (*Wireless Protected Access*) oraz WPA2. Każdy z nich posiada wiele wersji, często specyficznych dla danego producenta sprzętu, co może niekiedy powodować problemy z kompatybilnością (jest to szczególnie częste w przypadku standardu WEP).

WEP jest martwy!

Różne systemy szyfrowania przesyłanych danych charakteryzują się odmiennym poziomem bezpieczeństwa. Jest to fakt powszechnie znany, często jednak nie uświadamiamy sobie, iż niektóre z zabezpieczeń mogą jedynie sprowokować potencjalnego włamywacza. Doskonałym przykładem takiej sytuacji jest system WEP, który został złamany wiele lat temu, niestety jest on jednak ciągle spotykany.

Zapamiętaj – stosowanie standardu WEP, niezależnie od długości klucza i charakterystycznych dla producenta sprzętu rozszerzeń, nie uchroni Twojej sieci przed włamywaczami. Jak przekonamy się w jednym z następnych paragrafów, złamanie tego zabezpieczenia nie wymaga żadnej wiedzy technicznej, ani specjalnego sprzętu. Dodatkowo ryzykujemy, że niedoświadczeni script kiddies potraktują naszą sieć jako plac zabaw do testowania narzędzi służących do łamania szyfrowania WEP.

Sieć bezprzewodowa – sieć niezaufana

Umożliwienie bezpośredniego dostępu do wnętrza sieci kablowej klientom łączącym się przy użyciu punktów dostępowych jest bardzo ryzykowne. W przypadku uzyskania nieuprawnionego dostępu do sieci bezprzewodowej, włamywacz uzyskuje bowiem pełen dostęp do zasobów sieci.

Odpowiednim rozwiązaniem jest w takiej sytuacji zastosowanie routera z firewallem filtrującym ruch sieciowy. Informacje na temat budowy takiego rozwiązania znajdziesz w poprzednich częściach cyklu: trzeciej (podstawy routingu), czwartej (wykorzystanie komputera z systemem Linux jako routera), piątej (podstawy zabezpieczania sieci komputerowych) oraz szóstej (konfiguracja firewalla przy zastosowaniu iptables).

Sieć bezprzewodowa – sieć zawodna

W trakcie budowy i rozbudowy sieci bezprzewodowych, szczególną uwagę powinniśmy poświęcić funkcjom komputerów do niej podłączonych. Awaria bezprzewodowej części sieci nie powinna bowiem uniemożliwiać dostępu do ważnych zasobów sieciowych. W przypadku standardowych klientów, nieudostępniających żadnych usług krytycznych dla działania sieci, umieszczenie ich w bezprzewodowym segmencie sieci jest zazwyczaj dobrym rozwiązaniem. Problem pojawić się może w przypadku serwerów znajdujących się w jej obrębie – w takim przypadku należy zastanowić się, czy nie istnieje możliwość podłączenia serwera przy użyciu mniej wygodnego, ale bardziej niezawodnego połączenia przewodowego.

Alternatywnym rozwiązaniem jest zastosowanie łącz redundantnych, zapewniających awaryjne kanały łączności. Ich rolę mogą pełnić zarówno standardowe połączenia kablowe Ethernet, jak i bardziej nietypowe rozwiązania. W celu wykorzystania redundancji w sieci, konieczny jest zakup odpowiedniego sprzętu oraz zmiana konfiguracji routerów.

Stosuj wielopoziomowe systemy zabezpieczeń

W poprzednich częściach cyklu zostało wielokrotnie napisane, iż kluczem do bezpieczeństwa sieci jest nie tylko jakość, lecz również ilość poziomów zabezpieczeń. Stwierdzenie to pozostaje prawdziwe dla sieci bezprzewodowych standardu IEEE 802.11.

Zastanówmy się, jak powinna wyglądać dobrze zabezpieczona sieć bezprzewodowa. Na najniższym poziomie stosowane jest szyfrowanie przesyłanych danych przy użyciu standardu WPA/WPA2 – stanowi ono pierwszą linię obrony, uniemożliwiającą osobom nieuprawnionym połączenie z siecią oraz zmniejszającą zagrożenia, wynikające z podsłuchiwania transmisji. Dodatkowe zabezpieczenie stanowi wykorzystanie oprogramowania OpenVPN w celu tunelowania danych przesyłanych pomiędzy komputerami. Uwierzytelnianie odbywa się przy użyciu certyfikatów podpisanych przez lokalną jednostkę certyfikującą CA (*Certification Authority*). Zastosowanie aż tak mocnych za-

bezpieczeń może być dyskusyjne, doskonale sprawdzi się jednak w przypadku sieci służących do przesyłania szczególnie wrażliwych danych.

Szyfrowanie w sieciach bezprzewodowych

Znajomość klucza potrzebna jest nie tylko do szyfrowania przesyłanych danych – już na etapie nawiązywania połączenia (tzw. asocjacja) konieczne jest jego wprowadzenie. W zależności od stosowanego standardu szyfrowania, zarówno nawiązywanie połączenia, jak i szyfrowanie i odszyfrowywanie przesyłanych danych mogą odbywać się w różny sposób.

W paragrafie tym zajmiemy się krótkim omówieniem standardów szyfrowania wykorzystywanych w sieciach Wi-Fi: WEP, WPA oraz WPA2.

WEP – (nie)bezpieczne szyfrowanie?

W poprzednim paragrafie napisane zostało, iż wykorzystanie w sieci standardu szyfrowania WEP nie przyczyni się do zwiększenia bezpieczeństwa jej użytkowników. Nazwa WEP – *Wired Equivalent Privacy* – lepiej opisuje intencję twórców, niż faktyczny poziom bezpieczeństwa.

Standardowo WEP obsługuje klucze o długości wynoszącej 40 i 104 bity. Do klucza dołączany jest 24-bitowy wektor inicjalizujący (IV – *Initialization Vector*). Bardzo często spotkać można niepoprawne twierdzenia, jakoby WEP używał 64-bitowych i 128-bitowych kluczy.

Po wykryciu licznych problemów z bezpieczeństwem standardu WEP, producenci sprzętu sieciowego zaczęli wprowadzać rozwiązania, mające przedłużyć czas jego życia. Niestety, działania te przyniosły niewielki skutek, dodatkowo powodując problemy z kompatybilnością pomiędzy urządzeniami różnych producentów.

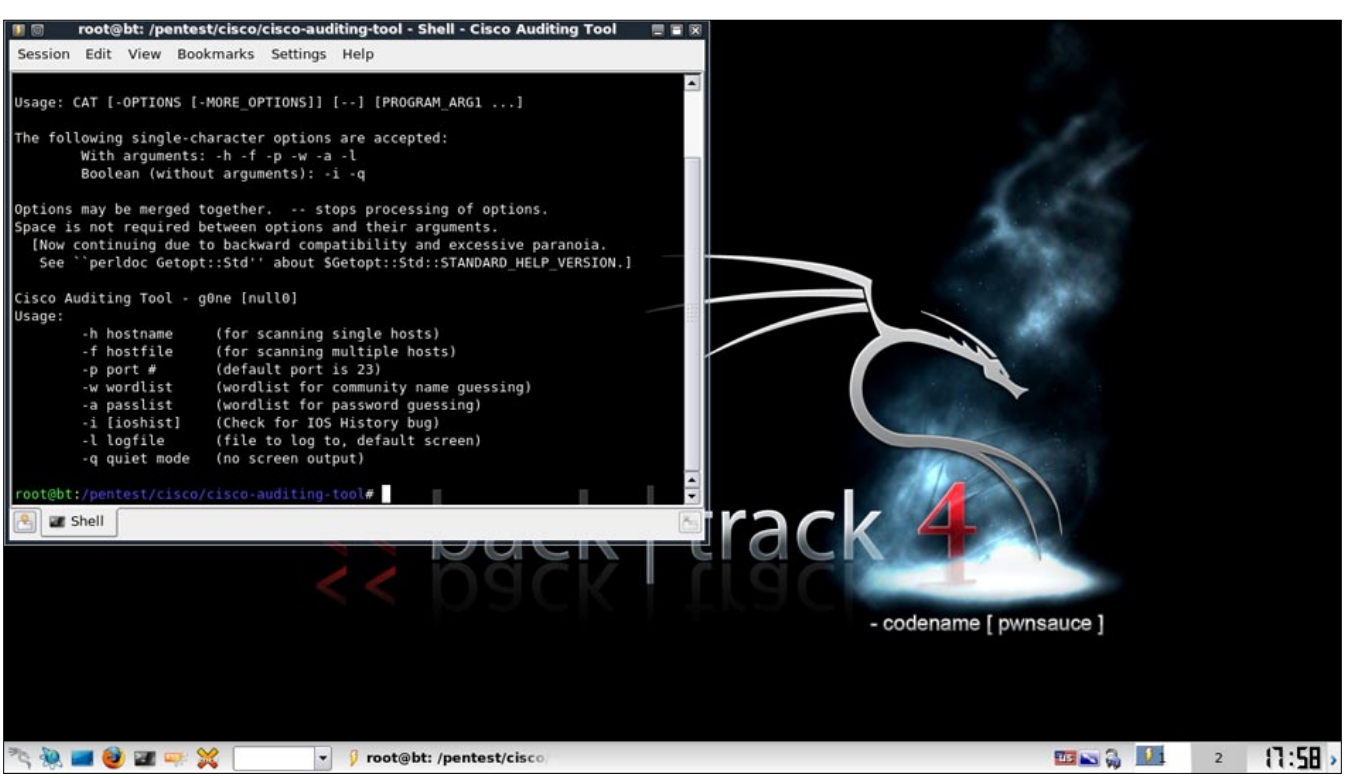
W internecie znaleźć można wiele instrukcji opisujących krok po kroku, w jaki sposób złamać zabezpieczenia sieci wykorzystującej szyfrowanie WEP. W artykule tym, ze względu na przekonanie autora, iż nie nie należy prezentować gotowych rozwiązań pozwalających na penetrację sieci, temat ten nie będzie omawiany.

WPA i WPA2 – pełne bezpieczeństwo?

Problemy z bezpieczeństwem standardu WEP spowodowały, iż konieczne stało się opracowanie nowego standardu szyfrowania. Ze względu na dużą ilość sprzętu obsługującego WEP obecnego na rynku, jednym z podstawowych założeń twórców WPA była możliwość dodania obsługi tego standardu poprzez aktualizacje oprogramowania punktów dostępowych oraz interfejsów sieciowych.

WPA częściowo rozwiązuje problemy z bezpieczeństwem standardu WEP poprzez cykliczną zmianę kluczy – umożliwia to zwiększenie bezpieczeństwa bez zmiany istniejących mechanizmów kryptograficznych. Pomimo znacznie większego poziomu bezpieczeństwa, szyfrowanie WPA może być podatne na ataki słownikowe oraz kryptoanalizę.

WPA2 jest najdoskonalszym dostępnym standardem szyfrowania dla bezprzewodowych sieci Wi-Fi. Używa



Rysunek 1. *Dystrybucja BackTrack Linux 4 w akcji*

szyfrowania opartego o algorytm CCMP/AES, uznawany za w pełni bezpieczny. Jego zastosowanie z odpowiednio mocnym kluczem gwarantuje pełne bezpieczeństwo sieci bezprzewodowej.

Zarówno WPA, jak i WPA2 obsługuje przydzielanie kluczy wielu użytkownikom przy użyciu serwerów RADIUS (*Remote Authentication Dial In User Service*). Dostępnych jest wiele implementacji, przeznaczonych zarówno dla systemów Linux, jak i Microsoft Windows, pozwalających na budowanie tego typu rozwiązań.

BackTrack – charakterystyka dystrybucji

Analiza bezpieczeństwa sieci, zarówno przewodowych, jak i bezprzewodowych, wymaga zastosowania specjalistycznych narzędzi. W przypadku sieci standardu IEEE 802.11 zadanie jest dodatkowo utrudnione, ponieważ przeprowadzenie dużej części zadań wymaga instalacji zmodyfikowanych sterowników, umożliwiających wykorzystanie karty w trybie monitora. Interfejs działający w tym trybie umożliwia przechwytywanie pakietów należących do wszystkich sieci działających na danym obszarze. Instalacja sterowników oraz odpowiedniego oprogramowania może być jednak dość czasochłonna.

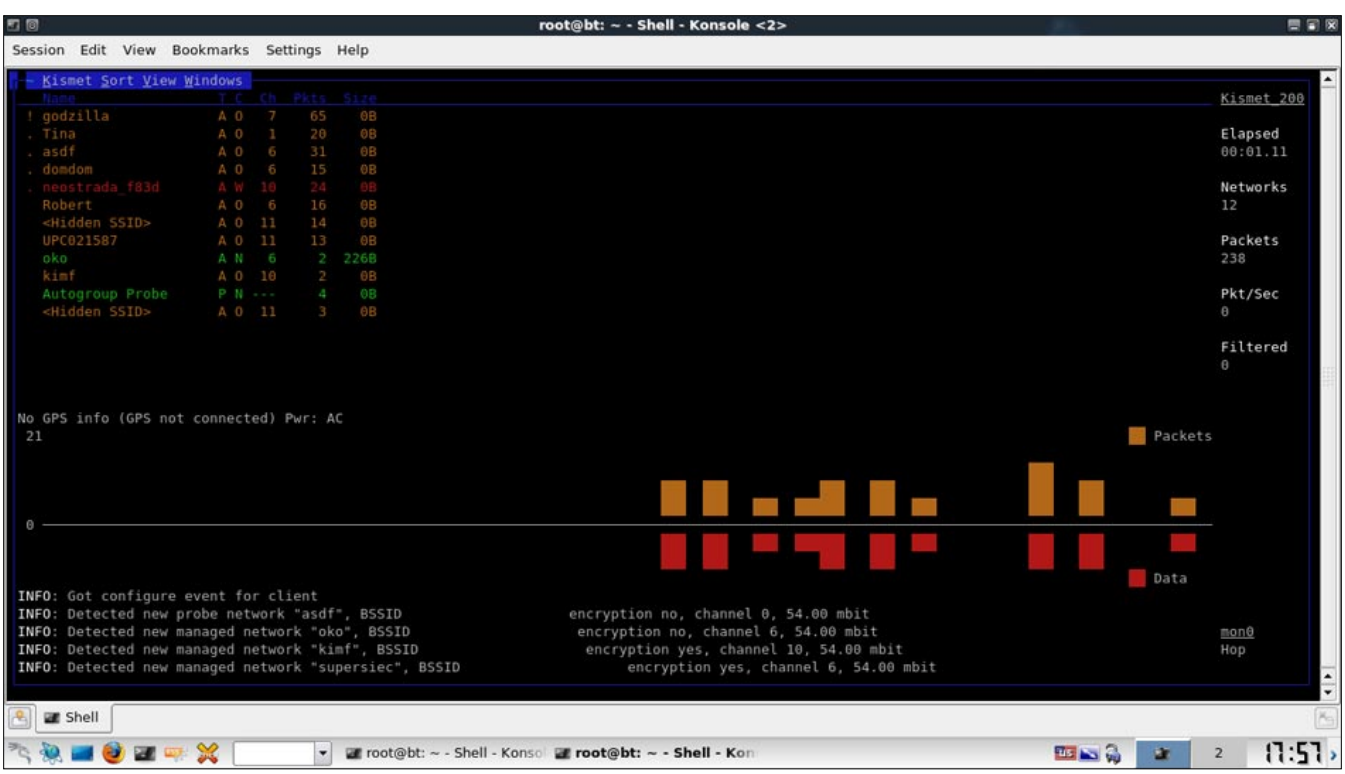
Dystrybucja BackTrack (Rysunek 1) wychodzi na przeciw potrzebom osób odpowiedzialnych za bezpieczeństwo sieci. Zawiera ona wszystkie narzędzia i sterowniki niezbędne do kompleksowej analizy bezpieczeństwa, przeprowadzania testów penetracyjnych oraz diagnozowania problemów i pomiaru wydajności jej pracy. Najnowsza wersja BackTrack Linux dostępna jest na stronie internetowej *http://www.backtrack-linux.org/* (w chwili pisania artykułu jest to wersja BackTrack 4 Final, wydana 11.01.2010).

BackTrack uruchamiany jest z płyty bootowalnej, może być jednak zainstalowany na twardym dysku lub pamięci USB. Większość popularnych interfejsów bezprzewodowych obsługiwana jest bez potrzeby instalacji dodatkowych sterowników lub przeprowadzania czasochłonnej konfiguracji.

Badanie zasięgu sieci przy pomocy programu Kismet

Badanie zasięgu sieci oraz poziomu sygnału jest jedną z podstawowych czynności, które należy przeprowadzić po każdej zmianie punktu dostępowego lub jego położenia. Odpowiednie oprogramowanie pozwala na znaczne uproszczenie tego procesu. Przykładem doskonałego narzędzia, które można wykorzystać w tym celu jest Kismet (*http://www.kismetwireless.net/*), dostępny w dystrybucji BackTrack.

Kismet wymaga do działania urządzenia działającego w trybie monitora. Większość popularnych interfejsów bezprzewodowych, w tym zintegrowanych, może działać w tym trybie bez potrzeby instalacji dodatkowych sterowników w dystrybucji BackTrack. Przełączenie karty w tryb monitora odbywa się przy pomocy polecenia `airmon-ng start interfejs`. Dostępne interfejsy bezprzewodowe możemy wyświetlić przy użyciu



Rysunek 2. *Sieci wykryte przy użyciu programu Kismet*

programu iwconfig. Po zakończeniu działania programu airmon-ng w systemie powinien znajdować się dodatkowy interfejs mon0.

Po przełączeniu karty w tryb monitora, możesz już uruchomić program Kismet. Jego konfiguracja sprowadza się do odpowiedzi na kilka pytań w trybie interakcyjnym, m. in. podać należy nazwę interfejsu monitora. Gdy proces konfiguracji zostanie zakończony, otwórz drugie okno emulatora terminala i ponownie uruchom program Kismet. Na ekranie powinna pojawić się lista sieci, wraz z podstawowymi informacjami na ich temat (Rysunek 2). Wybranie nazwy sieci powoduje wyświetlenie dokładniejszych danych: poziomu sygnału i szumu, liczby odebranych pakietów itd.

Więcej informacji na temat zastosowania programu Kismet znajdziesz w dokumentacji.

Inne sposoby zabezpieczania sieci bezprzewodowych

Wykorzystanie standardów szyfrowania jest podstawową metodą zabezpieczania sieci bezprzewodowych. Większość dostępnych na rynku punktów dostępowych, w tym opisywany w poprzedniej części kursu APPro 2405, udostępnia ponadto dodatkowe funkcje, takie jak filtrowanie adresów MAC, wyłączenie rozgłaszania identyfikatora SSID oraz blokowanie dostępu do sieci bezprzewodowej w określonych godzinach. Zajmiemy się teraz analizą przydatności i skuteczności tych funkcji.

Filtrowanie adresów MAC

Interfejsy bezprzewodowe, podobnie jak standardowe interfejsy Ethernet, posiadają 48-bitowe adresy MAC, służące do identyfikacji hostów na poziomie warstwy łącza danych modelu ISO/OSI. Mogą być one również wykorzystane do identyfikacji hostów uprawnionych do połączenia z siecią. Połączenia nawiązywane przy użyciu interfejsów o adresach MAC nie znajdujących się na odpowiedniej liście są w przypadku wykorzystania takiego rozwiązania odrzucane.

Dla urządzenia APPro 2405 uaktywnienie funkcji kontroli adresów MAC odbywa się przy użyciu strony *Wireless/Access Control* interfejsu przeglądarkowego. Adresy MAC dodajemy do listy *Access Control List* – każdy wpis może zostać włączony lub wyłączony. Domyślną politykę ustawiamy przy użyciu funkcji *Access Control Mode*. W praktyce, najczęściej blokuje się wszystkich klientów, oprócz znajdujących się na liście (uzyskujemy to poprzez wybranie z listy rozwijalnej *Allow*). W przypadku, gdy korzystamy już z funkcji menedżera ruchu (*Traffic Manager*), możemy zaimportować istniejącą listę adresów MAC poprzez zaznaczenie pola *Use TFM MACs*. Aktywacja filtrowania adresów MAC ma miejsce po zaznaczeniu pola *Access Control*.

Skuteczność metody filtrowania adresów jest jednak niewielka – zmiana adresu MAC interfejsu nie sprawia większego problemu zarówno w systemie Linux, jak i w systemach z rodziny Microsoft Windows. Również zdobycie adresów MAC klientów przyłączonych do sieci bezprzewodowej nie jest trudna – użycie narzędzia airodump-ng umożliwia zdobycie wielu adresów w bardzo krótkim czasie.

Ukrywanie identyfikatora SSID

W poprzedniej części cyklu omówione zostały identyfikatory ESSID i BSSID, używane do identyfikacji sieci bezprzewodowych. Są one rozgłaszane przez bezprzewodowe punkty dostępowe, co pozwala na tworzenie list sieci działających na danym obszarze wraz z ich parametrami, a następnie jej prezentację użytkownikowi komputera-klienta. Istnieje możliwość wyłączenia rozgłaszania tych identyfikatorów, przez co sieć stanie się trudniejsza do wykrycia przez potencjalnych włamywaczy oraz ciekawskich.

W przypadku punktu dostępowego APPro 2405, wyłączenie rozgłaszania odbywa się przy użyciu opcji *AP Cloaking* ze strony *Wireless/Security* interfejsu przeglądarkowego. Ten sam efekt można uzyskać poprzez wyłączenie funkcji *Broadcast SSID* na stronie *Wireless/Advanced Settings*.

Ukrycie identyfikatora SSID nie zabezpieczy Twojej sieci przed włamywaczami – podobnie jak w przypadku filtrowania adresów MAC. Poprzez zastosowanie np. programu airodump-ng lub Kismet, możemy zdobyć pełną listę sieci działających na danym obszarze. Wykorzystanie tej funkcji może również powodować niedogodność dla użytkowników, tak więc powinna być używana z ostrożnością.

Blokowanie dostępu do sieci bezprzewodowej w określonych godzinach

W przypadku większości sieci bezprzewodowych, szczególnie tych działających w przedsiębiorstwach oraz innych instytucjach, z łatwością można wskazać godziny, w których żaden z uprawnionych użytkowników nie będzie korzystał z tego typu podłączenia do zasobów sieciowych. Dobrym rozwiązaniem, zarówno z punktu widzenia oszczędności energii, jak i bezpieczeństwa, byłoby wyłączenie punktów dostępowych lub samych nadajników.

Część dostępnych na rynku urządzeń umożliwia ustawienie godzin pracy bezpośrednio z interfejsu przeglądarkowego. Opisywany w kursie punkt dostępowy APPro 2405 nie posiada niestety takiej funkcji. Przy pomocy połączenia poprzez telnet lub SSH możemy jednak przesłać odpowiedni skrypt do punktu dostępowego, a następnie dokonać konfiguracji programu cron, służącego do okresowego wywoływania programów.

W niektórych przypadkach dobrym rozwiązaniem jest zastosowanie standardowego wyłącznika czasowego, wpinanego pomiędzy zasilacz punktu dostępowego, a gniazdo sieciowe. Ogranicza to ilość zużywanej energii elektrycznej oraz zwiększa niezawodność sprzętu (krótsze cykle włączenie-wyłączenie).

OpenVPN w sieci bezprzewodowej

W części kursu poświęconej budowie firewalli oraz wirtualnych sieci prywatnych VPN, omówiona została instalacja, konfiguracja oraz wykorzystanie programu OpenVPN. Napisane zostało wtedy, iż do programu tego wrócimy przy okazji omawiania zagadnień związanych z zabezpieczaniem sieci bezprzewodowych. OpenVPN doskonale nadaje się bowiem jako dodatkowa warstwa zabezpieczeń w transmisji bezprzewodowej, zarówno typu punkt-punkt, jak i pomiędzy wieloma klientami.

W przypadku połączeń punkt-punkt o niewielkiej dynamice, dobrym rozwiązaniem jest zastosowanie kluczy statycznych o odpowiedniej długości. Jeżeli jednak wirtualna sieć prywatna ma służyć wymianie danych pomiędzy wieloma komputerami, to w celu uwierzytelniania i szyfrowania warto zastosować infrastrukturę klucza publicznego PKI. Obie te konfiguracje zostały dokładnie omówione w szóstej części kursu.

W przypadku sieci publicznych, w których istnieje konieczność zapewnienia bezpiecznego kanału transmisji danych przy jednoczesnym braku szyfrowania (WEP/WPA/WPA2) zastosowanie OpenVPN lub innego oprogramowania do tworzenia wirtualnych sieci prywatnych jest niemal koniecznością. Przykładem może być sieć akademicka, z którą połączyć się mogą wszyscy użytkownicy znajdujący się w jej obrębie (np. w celu dostępu do internetu), jednak tylko uprawnieni użytkownicy (tzn. posiadający oprogramowanie OpenVPN oraz odpowiednie certyfikaty) powinni mieć dostęp do usług udostępnianych przez serwery sieci wewnętrznej.

Podsumowanie

W artykule zostały omówione podstawowe zagadnienia związane z zabezpieczaniem sieci bezprzewodowych standardu IEEE 802.11 przed podsłuchiwaniem i nieuprawnionym dostępem. Mam nadzieję, iż zrozumiałeś, jak dużą wagę należy przykładać do bezpieczeństwa w tego typu sieciach.

Omówione metody: stosowanie szyfrowania, odpowiednie rozmieszczenie sprzętu, umożliwiające kształtowanie pokrycia obszaru zasięgiem, wykorzystanie mechanizmów szyfrowania i uwierzytelniania na poziomie warstwy aplikacji, umożliwiają uzyskanie najwyższego stopnia bezpieczeństwa w sytuacji, gdy wykorzystywane są jednocześnie. Spadek wydajności transmisji oraz drobne niedogodności wynikające z konieczności instalacji oprogramowania OpenVPN na komputerach klienckich, jest z pewnością usprawiedliwiony przez znaczne zwiększenie bezpieczeństwa.

Podobnie jak w przypadku każdego artykułu z tej serii, należy stwierdzić, iż zdobyte wiadomości zainteresowany Czytelnik może poszerzyć poprzez zapoznanie się z informacjami znajdującymi się na stronach wymienionych w ramce *W Sieci* oraz innych stronach internetowych. Szczególnie dużą uwagę polecam zwrócić na zagadnienia związane z bezpieczeństwem fizycznym oraz niezawodnością sprzętu sieciowego. Pomimo iż zagadnienia te nie zostały omówione w tym kursie z racji jego ograniczonej objętości, mają one ogromne znaczenie dla każdego projektanta i administratora sieci bezprzewodowych.

W następnej, ostatniej części cyklu zajmiemy się rozszerzeniem sieci o funkcje udostępniane przez technologie VoIP. Wykorzystamy w tym celu dostępny na wolnej licencji program Asterisk. Dowiesz się między innymi, w jaki sposób można udostępnić użytkownikom sieci możliwość taniego wykonywania połączeń międzynarodowych, zarówno przy użyciu standardowych telefonów analogowych, jak i softphonów (specjalnych aplikacji obsługujących protokół SIP) oraz telefonów VoIP. Do usłyszenia!

RAFAŁ KUŁAGA

Autor interesuje się bezpieczeństwem systemów informatycznych, programowaniem, elektroniką, muzyką rockową, architekturą mikroprocesorów oraz zastosowaniem Linuksa w systemach wbudowanych.

Kontakt z autorem: rl.kulaga@gmail.com

W Sieci

- Strona główna dystrybucji BackTrack Linux - *http://www.backtrack-linux.org/*
- Strona główna programu Kismet - *http://www.kismetwireless.net/*
- Strona główna pakietu aircrack-ng - *http://www.aircrack-ng.org/*
- Forum poświęcone tematyce sieci komputerowych, w tym bezprzewodowych - *http://www.trzepak.pl/*

25–26 maja 2010
Warszawa

WSTĘP BEZPŁATNY

Nowoczesne technologie sieciowe i rozwiązania teleinformatyczne

www.gigacon.org/network

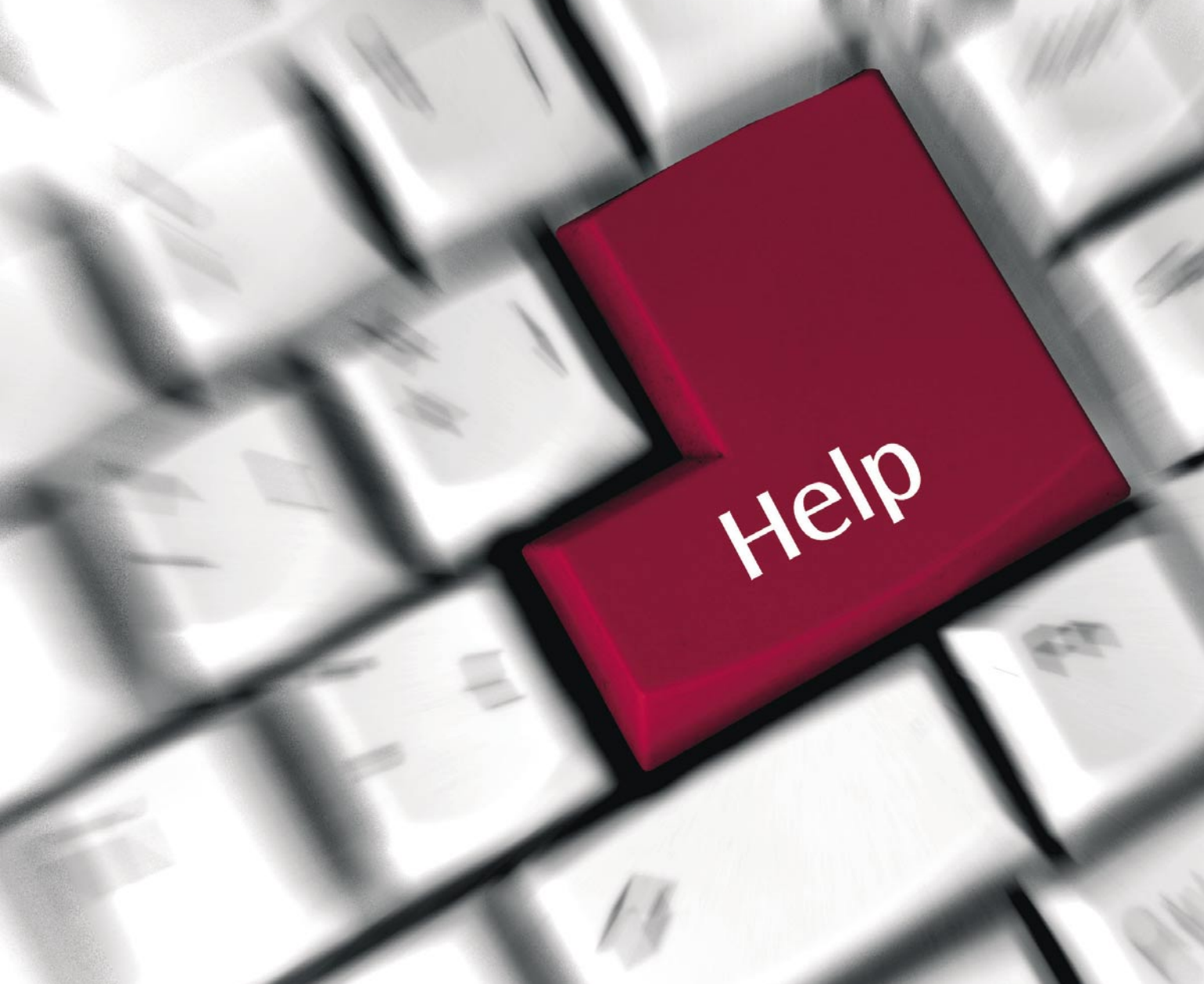
Serdecznie zapraszamy do udziału w kolejnej – XI już edycji konferencji poświęconej tematyce nowoczesnych rozwiązań i technologii sieciowych oraz ich obecności na polskim rynku teleinformatycznym. Celem konferencji jest określenie przekroju zastosowań nowych technologii, produktów i usług oraz upowszechnienie związanej z nimi wiedzy technicznej.

Tematyka sesji:

- Infrastruktura sieciowa
- Komunikacja bezprzewodowa
- Bezpieczeństwo sieci
- Wydajne rozwiązania dla Internetu
- Transmisja głosu i danych
- Konwergencja sieci
- Call/ Contact Center
- Zarządzanie i optymalizacja sieci

NETWORK GigaCon™

Kontakt z organizatorem:
Kamila Tarłowska
tel. 022 427 36 47
fax. 022 244 24 59
kamila.tarlowska@software.com.pl



27 kwietnia 2010 | Warszawa

IT Service & Support GigaCon – konferencja poświęcona najnowszym koncepcjom i systemom przeznaczonym do obsługi obszaru wsparcia serwisowego.

Proponowana tematyka:

- Zarządzanie incydentami,
- Zarządzanie problemami,
- Zarządzanie zmianą,
- Zarządzanie konfiguracją,
- Zarządzanie poziomem serwisu,
- Ewidencja i kontrola zasobów

IT Service & Support

WSTĘP **BEZPŁATNY**

Koordynator projektu
Ilona Kacprzak
ilona.kacprzak@software.com.pl
tel.: 22 427-37-16

http://gigacon.org/service

Systemy bankowe, ISOF

HEUTHES istnieje na rynku od 1989 r. Obok systemów informatycznych dla banków, oferuje nowoczesne oprogramowanie do obsługi firm. System ISOF jest udostępniany klientom w trybie SaaS lub licencji. Pracuje na platformie Linux i zawiera m.in. takie moduły jak CRM, DMS, Magazyn, Sprzedaż, Logistyka oraz Rachunkowość.
http://www.isof.pl

TTS Company Sp. z o.o.

Sprzedaż i dystrybucja oprogramowania komputerowego. Import programów na zamówienie. Ponad 200 producentów w standardowej ofercie. Chcesz kupić oprogramowanie i nie możesz znaleźć polskiego dostawcy? Skontaktuj się z nami – sprowadzimy nawet pojedyncze licencje.
www.OprogramowanieKomputerowe.pl

BetaSoft Sp. z o.o.

Jednym z naszych autorskich rozwiązań jest system eDokumenty realizujący wymagania DMS i CRM. Pracuje on na platformach Linux oraz Windows i należy do najnowocześniejszych aplikacji webowych działających w technologii AJAX. System jest zintegrowany z OpenOffice, MS Office i programami ERP.
www.betasoft.pl,
www.edokumenty.eu

Wyższa Szkoła Informatyki

Informatyka, Ekonomia, Fizjoterapia (NOWOŚĆ, Pedagogika, Wychowanie Fizyczne, Artystyczna Grafika Komputerowa, Architektura Wnętrz (NOWOŚĆ) Studia na odległość e-learning (Informatyka II stopnia) Kompleks sportowy w Łodzi (hala, basen, siłownia, sauna). Wydziały zamiejscowe: Włocawek, Bydgoszcz, Opatówek.
http://www.wsinf.edu.pl

OFERTA SKIEROWANA DO FIRM

Wyślij do nas: logo firmy, dane kontaktowe i informacje o firmie.

Reklama przez **12** kolejnych **numerów** tylko za **600 PLN** + VAT.

Skontaktuj się z nami:

linux@software.com.pl tel. 22 427 36 52

ZAJAWKA

Następny numer Linux+ ukaże się 30 maja. Temat numeru to:

E - commerce

W numerze tym planujemy zamieścić między innymi takie artykuły jak:

- Druga część z cyklu: Programowanie w Qt 4.6 pod Ubuntu
- GRUB szyty na miarę
- Prowadzenie projektów WWW dla małych i średnich przedsiębiorstw
- Aplikacja SaaS w małych i średnich przedsiębiorstwach
- Współtwórca polskiej wikipedii – wywiad dla Linux+
- Kontrola jakości projektu metodą client i server side control

Numer dostępny on-line na 30 maja

Redakcja zastrzega sobie możliwość zmiany zawartości pisma.