Magazyn użytkowników otwartego oprogramowania

dragonia magazine

Numer 36 specjalny – 2010

Piotr Krzysztof Smoleń
Wszechstronny Intranet
Na Bazie Open Source Software

Drodzy Czytelnicy

Oddajemy w Wasze ręce kolejny numer specjalny. Ten nie dość, że jest poświęcony jednemu tematowi, to jeszcze jest popełniony przez jednego autora – Piotra Smolenia, którego miło nam gościć na naszych łamach.

Bieżący numer to studium przypadku, czyli historia wdrożenia otwartoźródłowego oprogramowania w dużym szpitalu wojewódzkim, w części serwerowej. Innymi słowy jak zapanować nad użyszkodnikami, sprzętem i oprogramowaniem nie mając na to góry pieniędzy, by w efekcie zmienić „młyn" w sympatyczną pracę.

Przeczytamy także o niezmiernie ważnym elemencie każdego wdrożenia, tzw. części miękkiej – jak przekonać lub zmusić użytkowników do korzystania z „nowego" lub „po nowemu". A także ile za komfort zmuszenia ich trzeba zapłacić.

Aplikacje, których nazwy przewiną się w treści, są w większości powszechnie znane. Z tymi mniej znanymi warto się zapoznać. Jak przekonamy się, spięcie wielu aplikacji w jedną spójną całość jest nie tylko możliwe, ale znakomicie ułatwia pracę tak użytkownikom (jedno hasło), jak i administratorom.

Zapraszam do zatopienia się w pasjonującej opowieści jak w chaosie pojawiła się wizja normalności oraz jak i z jakim trudem tę normalność wprowadzano.

Miłej lektury!

Tomasz Łuczak
zastępca redaktora naczelnego

Wszystkie publikowane materiały są objęte prawem autorskim na zasadach licencji Creative Commons CC-BY. Nie ponosimy odpowiedzialności za treść ogłoszeń. Nazwy firm, nazwy handlowe i znaki towarowe zostały użyte w publikacji jedynie w celach informacyjnych i są własnością poszczególnych podmiotów.

Spis treści

Geneza . . . 4
Topologia sieci . . . 11
CUPS (1) . . . 13
Samba (2) . . . 15
Serwer DHCP (3) . . . 17
Serwer Proxy (4) . . . 18
Serwer NTP (5) . . . 20
System SNORT IDS (6) . . . 20
Serwer poczty (7 i 11) . . . 21
LDAP (8) . . . 22
Firewall (9) . . . 25
VPN (10) . . . 25
Ewidencja i zarządzanie zasobami informatycznymi GLPI (12) . . . 25
Serwer www (13) . . . 28
Serwery baz danych MySQL i PostgreSQL (14) . . . 29
Automatyczna inwentaryzacja sprzętu komputerowego i oprogramowania OCS Inventory (15) . . . 29
Serwer monitorujący dostępność usług i hostów Zabbix (16) . . . 30
Serwer backupowy Bacula (17) . . . 33
Repozytorium dokumentów OWL (18) . . . 34
System zarządzania treścią Joomla (19) . . . 37
Logowanie połączeń sieciowych ARGUS (20) . . . 37
UltraVNC (21) . . . 38
Co dalej? . . . 38
Czy jest zatem tak dobrze? . . . 39
Czas podsumować . . . 39
O autorze . . . 40

Piotr Krakowiak – redaktor naczelny, założyciel, koordynacja, skład,
Tomasz Łuczak – zastępca redaktora naczelnego, skład,
Krzysztof Biskup – opieka nad www,
Paulina Budzoń – korekta,
Rafał Domeracki – sekretarz redakcji, opieka nad hostingiem,
Karol Kozioł – koordynator redaktorów i artykułów,
Krzysztof Ołowski – korekta,
Piotr Szewczuk – opieka nad hostingiem,
Kamil Galos, Keyto, Łukasz Wojno, Andrzej Warzyński.
Współpracujący: Piotr Smoleń

www: http://www.dragonia.pl
forum: http://forum.dragonia.pl
e-mail: redakcja@dragonia.pl

Skład za pomocą systemu LaTeX fontami TeX Gyre i Latin Modern
Pierwowzór layoutu Dragonia Magazine przygotował m4c

Opracowanie niniejsze dedykuję dyrektorom dużych firm, a zwłaszcza instytucji budżetowych, właśnie takich, jak publiczne szpitale, szkoły i urzędy.
Specjalne dedykacje kieruję do osób stojących na czele organów założycielskich, takich jak Urzędy Marszałkowskie, zwłaszcza w Polsce południowo-wschodniej.

Piotr Krzysztof Smoleń

Geneza

Na początku sprzęt komputerowy i wszelkie rozwiązania informatyczne w dużych jednostkach pojawiały się, niestety, spontanicznie. Z potrzeby chwili, doraźnie bez większego planu. Zwłaszcza w dużych firmach z budżetówki. Szpitale nie są i nie były pod tym względem wyjątkiem. Może nie wszystkie, ale przyznam się, że nie znam takich, które byłyby wyjątkiem od tej reguły.

Zazwyczaj scenariusz wyglądał tak, że pojawiał się jakiś komputer w księgowości z programem dosowym napisanym w DB lub Clipperze pracującym na jednym stanowisku. Systematycznie pojawiały się równie spontanicznie i bezmyślnie instalowane komputery w najbliższej okolicy księgowości. Po jakimś czasie ktoś odkrywał prawa autorskie, konieczność zakupienia systemu operacyjnego, mimo że przecież „nam jest niepotrzebny". Dowiadywał się, że Worda nie można ot tak sobie instalować na dowolnym komputerze. Szybko w takich sytuacjach pojawiała się konieczność połączenia komputerów w sieć. Podówczas wiedza, jak to zrobić, była wiedzą tajemną, niespotykaną, niezrozumiałą, zarezerwowaną dla wybrańców a sprzęt i materiały niezbędne do realizacji pomysłu kosztowały majątek. Wyrywano więc gdzieś na chwilkę fachowców i na zasadzie umów zleceń realizowali z doskoku wizję sieci w jednostce. Zazwyczaj byle jak, bo liczyła się cena, byle szybko. Sieć taka oczywiście rozrastała się w sposób niekontrolowany i chaotyczny. Na zasadzie „co fachowiec, to pomysł na realizację". Bardzo szybko okazywało się ponadto, że drożej wychodzi wzywanie do każdego problemu Wiedzącego niż zatrudnienie we własnej jednostce takiej osoby. Zatrudniano więc, jak to w budżetówce, za niewielkie pieniądze i bez weryfikacji kwalifikacji, bo i w sumie kto je miał zweryfikować? Efekt domina narastał, z tym że w przeciwieństwie do typowego domina, to miało kostki całkowicie się różniące od siebie. Topologia sieci przyprawiająca o zawrót głowy, kable walające się pod kółkami foteli i szpilkami pracownic. Urządzenia sieciowe każde od innego producenta, komputery wszelkiej maści przy czym znalezienie dwóch o identycznej konfiguracji graniczyło z cudem. Wszelkie możliwe systemy operacyjne (MS DOS 5.X, MS DOS 6.X, DR DOS, Free DOS, Windows 3.10, Windows 3.11 FW, Windows 95, OS/2, OS/2 Warp, OS/2 Warp Connect, Linux w Bóg wie ilu odmianach, Solaris, AIX, SCO UNIX i inne jeszcze bardziej egzotyczne). Prawdziwy horror był jednak przy drukarkach, każda innego typu, milion sterowników pod różne systemy i do różnych zastosowań i prawdziwa męczarnia z materiałami eksploatacyjnymi, kiedy trzeba było zrobić zestawienie roczne na taśmy, kasetki i kartridże. I na koniec oczywiście wszystkomogący użytkownicy z prawami administratorów albo z powodu systemu, na którym pracowali, całkowicie pozbawionego jakichkolwiek funkcji ochronnych, czy to z powodu programów napisanych w taki sposób przez domorosłych programistów, że działać poprawnie mogły tylko z prawami admina. Istna wieża Babel pełna sprzeczności i … sprzeczek wynikających ze sprzeczności. Chaosem da się zarządzać, ale tylko do pewnego poziomu, powyżej którego 100% mocy przerobowych trzeba zużyć na walkę z przeciwnościami sprzętu i oprogramowania, a nie na obsługę aplikacji i, co najważniejsze, na nadzór i rozwój.

Nadszedł zatem i u nas w jednostce czas, kiedy należało powiedzieć dość i mimo, że z założenia wiadomo było, że na początku będzie boleć, koniecznym stało się podjąć męskie decyzje i zdecydowane działania. Nie będę ukrywał, że pomógł tutaj trochę przypadek. Mianowicie odszedł z naszego zespołu kolega. Ot życiowa sprawa zakochał się i przeniósł do innego miasta. To był akurat nasz lider, pracujący w jednostce od samego początku, znający na wylot wszelkie jej potrzeby oraz bolączki i skupiający wszelką tajemną wiedzę w swojej głowie. W ten sposób w ciągu 3 dni od ogłoszenia decyzji o odejściu rzeczywiście zostaliśmy bez naszego guru i bez sporej części wiedzy. Jest powiedzenie „rzucić na głęboką wodę" – my trafiliśmy od razu nad Rów Mariański. Jednocześnie powstał też vacat i z góry było wiadomo, że ta jedna brakująca osoba, czyli 25% składu, robi wielką różnicę. Rozpoczął się zatem proces rekrutacji. Na jedną z rozmów kwalifikacyjnych przyszedł gość z przyklejonym uśmiechem do twarzy i bijącym wokół spokojem. Zadałem mu dosłownie 2 pytania i wiedziałem, że to jest ta osoba. Była to także jedyna osoba, o której z założenia pomyślałem, że nie ma sensu sprawdzać czy mówi prawdę, że potrafi i to na pewno lepiej ode mnie. Okazało się, że ten wybór był strzałem w setkę na tarczy z dziesiątką na środku, o czym przekonałem się w ciągu 3 dni od momentu rozpoczęcia pracy przez Grześka.

Rozpoczęło się niewinnie. Pierwszą potrzebą było odpalenie serwera z udostępnianiem katalogów użytkownikom na odpowiednich prawach. Jak to przy każdym zadaniu dokonana została analiza potrzeb i środków. Nasz biznes plan okazała się bezlitosny. Potrzebujemy wszystkiego a nie mamy dosłownie nic. Okazało się jednak, że to wystarczy. Tutaj genialnym okazało się zderzenie podejścia Grześka i jego znajomości Linuksa z naszym przywiązaniem do okienek i znajomością bardzo specyficznej sytuacji w szpitalu. Chodzi mi tutaj o podejście użytkowników, a zwłaszcza personelu medycznego do zagadnienia, co komu wolno, co kto musi a co powinien. Jak mawia szwagier, było u nas jak u ludzi normalnie, a nie jak być powinno.

Brak jakichkolwiek funduszy na zakup komercyjnych rozwiązań pchnął nas w jedyną możliwą drogę. Linux i wolne oprogramowanie. Rozpatrując pierwszą potrzebę oczywiście szybko okazało się, że najlepszym wyjściem będzie Samba. Maszyny na tą usługę oczywiście nie mieliśmy i nie było szans na zakup. Przeszperane zostały więc przepastne szafki, szuflady i piwnice, ale nie te firmowe, tylko nasze własne. Wyniki tych prac archeologicznych były zaskakują-

ce. Skompletowana została dwuprocesorowa maszyna na genialnej płycie TYAN z dyskiem SCSI 9GB. Od tego się zaczęło, a maszyna do chwili obecnej pracuje w szpitalu, ale służy już do zdecydowanie mniej odpowiedzialnej funkcji. Choć przyznać należy, że wbrew naszym obawom, nasz serwerowy składak okazał się stabilny jak skała i dosłownie niezniszczalny.

Dyskutując o schemacie uprawnień rozgorzała gorąca dyskusja, w wyniku której jasne szybko się stało, że to dopiero początek… Niewinny początek czegoś, co przerodziło się a w zasadzie wyewoluowało w tak potężne rozwiązanie, jakim jest teraz twór nazwany przez nas WINBOSS, czyli *Wszechstronny Intranet Na Bazie Open Source Software*. Przy okazji skrót od pełnej nazwy zawiera trochę mylnych ścieżek, niuansów i smaczków językowych, co tym bardziej nam przekornym i niepokornym pasuje.

W trakcie dyskusji, nie piszę tej, gdyż można powiedzieć, że trwa ona nieprzerwanie od kilku lat, wyszło na jaw, jak ogromnego problemu dotknęliśmy. Zostały określone ogólnie zagadnienia, z jakimi należy się zmierzyć:

1. Struktura organizacyjna szpitala jest niezmiernie skomplikowana i płynna. Do tego stopnia, że formalne dokumenty statutowe i rejestrowe nie nadążają za rzeczywistymi zmianami. Kto zatem ma dbać o jej odzwierciedlenie w pracującym na rzeczywistych danych systemie? Kto ma dbać o nadawanie i odbieranie uprawnień?
2. Rotacja personelu to także powszechne zjawisko. W firmie, gdzie pracuje ok. 1600 osób, właściwie codziennie ktoś zwalnia się, odchodzi na emeryturę, rozpoczyna pracę, awansuje, spada w drabince czy zmienia komórkę organizacyjną, gdzie pracuje. Jak zapanować nad tym problemem?
3. Co to są uprawnienia? Do czego i komu nadawać? Tu się rozsypał ogroooomny worek. Roztrząsając na części pierwsze okazało się, że jest to niezmiernie skomplikowane zagadnienie. Do jakich systemów prawa, jakie prawa, kiedy, czy z każdego komputera, czy codziennie, czy może różne prawa w różnych godzinach? Na co w ogóle nakładać prawa, na co musimy z powodu prawa a na co możemy i na co powinniśmy?
4. Właśnie… różne systemy, różne dostępy, różne konta i hasła. A może by tak to ujednolicić?
5. Jeden człowiek – jedno hasło. Jak przekonać lekarza, że hasło pielęgniarki, to hasło pielęgniarki, a nie jego?
6. Jak jest ze świadomością pracowników o prawach i obowiązkach wynikających z użytkowania systemów IT?
7. Jaki jest poziom wiedzy i umiejętności? Czy są tacy, co nie wiedzą jak się włącza komputer a już od wielu lat powinni na nim wykonywać swoje obowiązki? Są! Więc niestety szkolenia, jakie? Kiedy? W jakim zakresie? Dla kogo? Jak „przekonać", że są konieczne?
8. Gdzie przeprowadzać te szkolenia? Przydałaby się salka szkoleniowa, ale przecież nie ma kasy nawet na uszkodzony dysk u księgowej…
9. Jak nasza struktura sieci? Czy mamy wystarczającą ilość punktów dostępowych? Czy topologia jest właściwa? Czy szkielet jest wydolny? Czy przerwanie jednego kabelka nie wyłoży całego szpitala? Czy da się zarządzać tym wszystkim?
10. Serwery: co mamy a co mieć powinniśmy. Jak zabezpieczyć się przed skutkami awarii, które na pewno prędzej czy później się przydarzą? Jak wykonywać pewne kopie bezpieczeństwa, kiedy, gdzie je przechowywać?
11. Jak wygląda nasza serwerownia a jak wyglądać powinna? Co może się tam zepsuć?
12. Sprzęt… dlaczego mamy wszelkie cuda świata a nie jeden typ komputerów i monitorów, jeden typ drukarek itd.
13. Dostęp do Internetu, co mamy a jak to powinno wyglądać i czy możemy czuć się bezpiecznie?
14. Problemy z wirusami… jak się bronić i jak usuwać skutki ich działania?
15. Co gdzie jest? Jak zapanować nad tym jaki sprzęt gdzie jest, gdzie być powinien, kto jest za niego odpowiedzialny i jak to wygląda w księgowości?
16. Komunikacja pomiędzy pracownikami wzajemna i ze światem zewnętrznym. Co i jak?
17. Jak pokazać światu, że jesteśmy i jak to modyfikować tak, żeby nie tracić ogromnej ilości czasu na wprowadzenie najdrobniejszej zmiany?
18. Wielki Brat… Żeby administrować trzeba wiedzieć, żeby wiedzieć trzeba monitorować… Co nam wolno, co powinniśmy, czego nie możemy. Jak wytłumaczyć innym, że trzeba i jak przeżyć czas, kiedy nagle okaże się, że od dzisiaj pan doktor czegoś nie może… a jak może, to my wiemy, co robi. Jakie informacje zapisywać i czy w ogóle?
19. Ok, jeżeli nawet wymyśliliśmy co chcemy i jak to zrobimy, ale jeżeli nie będziemy mieli poparcia w paragrafach czy w dyrekcji, to nas przecież zjedzą za „robienie problemów"! Musimy więc powalczyć o takie poparcie.
20. Czy wszyscy zawsze wiedzą co i kiedy powinni zrobić na styku swoich obowiązków i naszej infrastruktury IT? Potrzebne są procedury, zatwierdzone przez dyrekcję i ogólnie znane i dostępne dla każdego.
21. Czy ja tego przypadkiem kiedyś nie robiłem? Gdzie są do cholery moje notatki, przecież były ołówkiem zapisane na takiej charakterystycznie przedartej karteczce z plamą kawy na środku! Potrzebna nam baza wiedzy!
22. I milion innych bardziej szczegółowych pytań…

Uświadomienie sobie aktualnego stanu faktycznego było bardzo bolesne i spowodowało nastrój ogólnej apatii. Właściwie powinniśmy wtedy wziąć łopatkę i zakopać się z żałości. Z drugiej strony gorzej już mogło być tylko wtedy, gdyby nic nie działało. Na dobrą sprawę perspektywy były tylko różowe.

Postanowiliśmy wykonać pierwszy krok testowy będący jednocześnie poligonem doświadczalnym dla reszty prac. Cała przychodnia specjalistyczna wyposażona była w identyczny sprzęt. W każdym gabinecie stał dumny HP Brio z Celeronem 400, 32MB RAM, 4GB HDD, kartą sieciową, Windows 98SE i drukarką igłową OKI Microline 3390. W sumie około 60 jednostek. Serwer linuksowy z Sambą już czekał… Dlaczego przychodnia? Z dwóch powodów: po pierwsze jednolitość sprzętu gwarantowała minimalizację problemów konfiguracyjnych. Z drugiej strony właśnie ta komórka organizacyjna przysparzała nam najwięcej problemów spowodowanych instalacją dowolnego oprogramowania przez użytkowników, ich grzebactwem w konfiguracji (świadomej bądź też nie) i działalnością wirusów. Dobrze, ale przecież to jest Windows 98… zero mechanizmów ochronnych, przecież każdy, kto odpali system będzie mógł zrobić z nim wszystko… Teoretycznie tak, praktycznie jednak dało się tak ograniczyć możliwości ingerencji, że 95% użytkowników nie wiedziała jak to zrobić a pozostałym się nie chciało, gdyż nie było to już takie proste. W ruch poszedł Policy Editor i Google. Śmiem twierdzić, że udało nam się uzyskać jeden z najlepiej zabezpieczonych Win 98, jakie widzieliście. Żadne sztuczki typowe z bootowaniem z innego nośnika, F8 podczas startu, anulowanie logowania itp. nie działały. Pracować mogły wyłącznie takie programy, jakie przewidzieliśmy itd. Czy był w 100% bezpieczny? Na pewno nie, choćby z założenia samego systemu. Na pewno dałoby się to lepiej zrobić, na pewno mając dłuższą chwilę samotności przy jednostce jednak dobralibyście się do niej. Właśnie jednak ta chwila była już na tyle duża, że mało komu się chciało a my mieliśmy czas na zauważenie anomalii.

Po opracowaniu takiej konfiguracji trzeba było jeszcze tylko powielić ją na 60 stacji. W tym miejscu użyliśmy jedynego w całej naszej twórczości komercyjnego oprogramowania. Symantec Ghosta zna i kocha każdy, kto go używał. A ponieważ mamy licencję, więc użyliśmy go, choć na 100% w sieci znaleźlibyśmy darmowe narzędzia do tego samego. Zatem Ghost i darmowe już DOS TCP/IP zapewniło nam narzędzie do sklonowania każdej jednostki, byle by tylko podpiąć do sieci i uruchomić system z dyskietki. Potem nastąpił jeden falstart, gdy okazało się, że nasza konfiguracja systemu jednak ma istotne wady, ponowne klonowanie i po zarwaniu piątkowego popołudnia i całej soboty plan został zrealizowany. Ujemne skutki tej akcji są obserwowane do dzisiaj… Mianowicie gabinety lekarskie, które poszły na pierwszy ogień, są nadal na nas obrażone, że jako pierwszym zabraliśmy im dostęp do Internetu… Cała reszta była już tylko miodem na nasze serca. Już po 2 tygodniach okazało się, że ilość zgłoszeń awarii spadła dosłownie 10-krotnie! Zamiast reinstalowanych nawet 2-3 jednostek dziennie mieliśmy takie przypadki 1, góra 2, w miesiącu i to już z naturalnych powodów: ot dysk wyzionął ducha czy spalił się zasilacz razem z całą resztą, co biorąc pod uwagę wiekowość jednostek dziwnym nie było.

W tym samym czasie przekonaliśmy się o wielkości innych narzędzi. Zainstalowany na tych jednostkach system antywirusowy zrobił swoje, mimo że nie była to wypasiona komercyjna wersja jakiegoś znanego producenta, ale jeden z bodaj 3 dostępnych wtedy i rozsądnych w działaniu programów darmowych w komercyjnym zastosowaniu. Dodatkowo zainstalowany VNC, dzięki któremu nie ruszając 4 liter z własnego fotela mogliśmy przeprowadzić wszelkie czynności, byleby tylko sieć działała, oszczędził nam masę czasu i par butów. Nie jest to wcale przesada, jeden tylko przykład, z własnego pokoju na oddział ginekologii i z powrotem mam ponad 1 km idąc po korytarzach! Ponadto pracujący w tle agent OCS Inventory wysyłał na bieżąco informację o zainstalowanym sprzęcie i oprogramowaniu. Życie stało się piękne a apetyt wzrósł i pomysłów przybyło. W ten oto sposób zrębek naszego systemu powstał i rozpoczął funkcjonowanie. Teraz nadszedł czas na weryfikację pomysłów, poprawki i realizację dalszych etapów. A i jeszcze jedno: mam nieodparte wrażenie, że jakby kolejki pacjentów pod gabinetami zmalały…

Kilka tygodni pracy tak skonfigurowanych jednostek przekonało nas o jednym, niestety najgorszym przypuszczeniu. To nie brak pieniędzy był największym problemem w realizacji naszego planu. To brak świadomości i kompletna niewiedza większości pracowników co do samych już obowiązków wobec regulaminu! A gdzie tu jeszcze zrozumienie np. zapisów ustawy o ochronie danych osobowych… Wpajanie tej świadomości i mozolne budowanie pozycji stróżów prawa trwa nieustannie do dzisiaj. Przypuszczamy także, że nigdy się nie zakończy. Właściwie codziennie słyszymy, że jesteśmy formalistami, że utrudniamy pracę, że w innych jednostkach gdzie medycy pracują nie ma takich „durnot", że co to za hasła, że ja muszę mieć prawa administratora itd. Niektóre próby tłumaczenia poszczególnym osobom kończyły się wręcz karczemnymi awanturami i obrazami na całe życie. Tutaj także należy wtrącić o jednej rzeczy. Zrozumienie przełożonych co do pewnych zasad, których *nie wolno nigdy łamać!* Dla przykładu podam sytuację, kiedy zadzwonił do nas pewien nobliwy lekarz z problemem zapomnianego hasła. Został poinformowany, że niestety odczytać hasła się nie da, ale możemy go zmienić na siłę na nowe. Lekarz zażądał takiej zmiany. Poinformowaliśmy go, że nie ma sprawy zapraszamy do nas do pokoju z jakimś dokumentem tożsamości (nie sposób przecież znać z imienia, nazwiska, twarzy czy głosu w telefonie ponad 1500 pracowników!) i pan doktor sam sobie wpi-

sze nowe hasło. Niestety pan doktor zareagował nerwowo, mimo że podpisał wcześniej stosowny regulamin odbierając konto domenowe i odmówił w mało sympatycznych słowach przybycia do naszego działu. Zadzwonił za to do ówczesnego dyrektora ze skargą, dyrektor zadzwonił do mnie i wydał polecenie (wbrew podpisanemu wcześniej przez siebie regulaminowi), aby zmienić panu docentowi hasło i nie robić szopek, jak to nazwał, z jego wizytą w naszym dziale. Usiłowałem dyrektora przekonać, że nie jest to dobre, bo podważa sens zarządzeń, że po czymś takim będziemy lekceważeni przez innych pracowników itd. Skończyło się to irytacją dyrektora i wydania polecenia uniesionym głosem. Efekty potem niestety ciągnęły się dość długo.

Osoby pracujące w dziale IT, które w dodatku chcą coś konkretnego zrobić, a nie przetrwać od pierwszego do pierwszego, muszą posiadać pewne cechy osobowości. Albo muszą być cierpliwe jak kamień i odporne na wszystko łącznie z promieniowaniem kosmicznym, albo nie posiadając cierpliwości na odpowiednim poziomie muszą być przerażająco pewne siebie i elokwentne do granic możliwości. Inaczej mówiąc: jak nie potrafisz spokojnie wysłuchać przytyków pod swoim adresem, musisz przegadać swojego adwersarza w sposób nie budzący wątpliwości kto tu ma rację i kto postawił na swoim. Oba typy i tak muszą być w 100% asertywne. Ogólnie w dziale potrzebne są jednak dwa typy wzajemnie się uzupełniające, zwłaszcza w kontaktach formalnych z przełożonymi i zwłaszcza wtedy, kiedy wywalczyć trzeba kilka złotych na inwestycje.

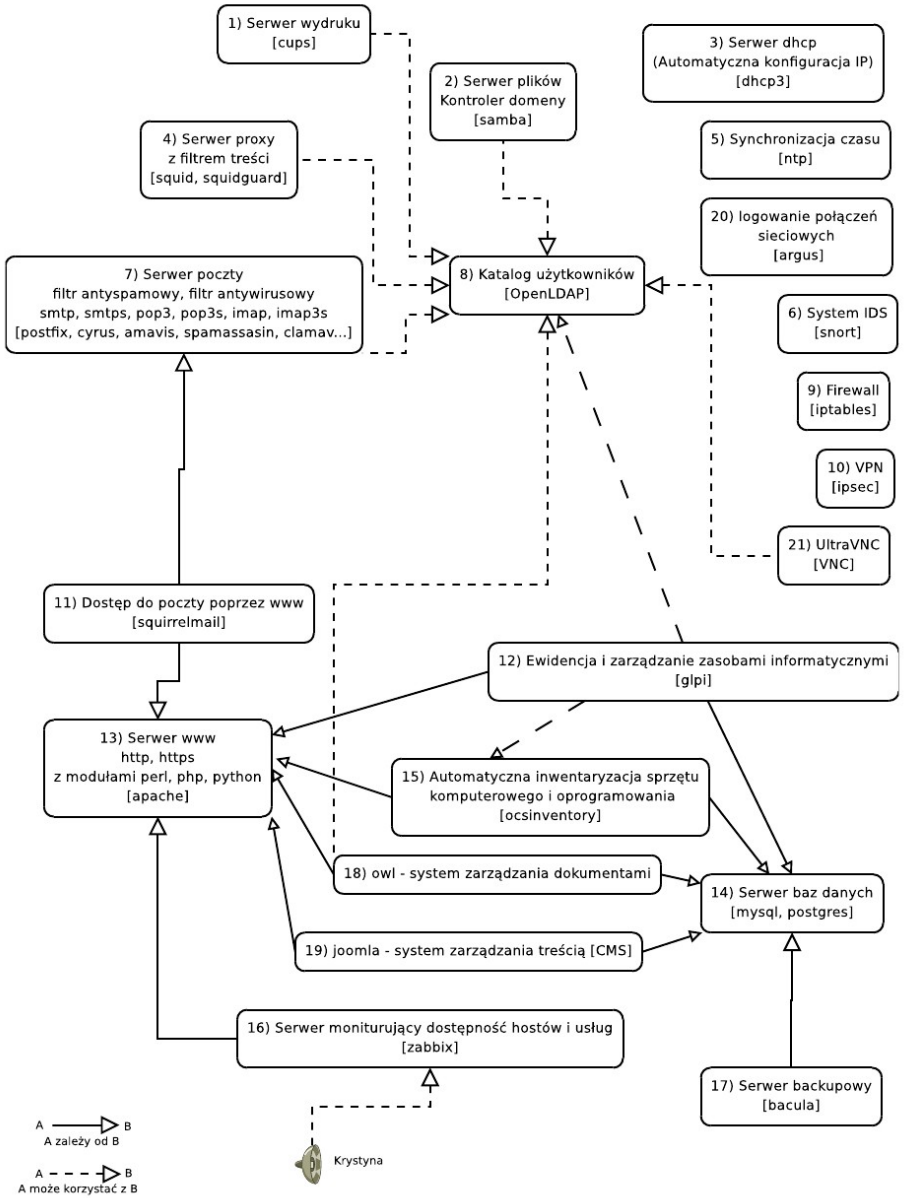
Poligon doświadczalny przeprowadzony na przychodni uzmysłowił nam kilka spraw. Po pierwsze jak nieprawdopodobnie ważnym jest, aby sprzęt w tak dużych jednostkach był jednolity. Raz opracowane procedury instalacji i reinstalacji potrafią skrócić wielokrotnie czas potrzebny na przywrócenie stanowiska do pracy po jakiejś awarii. W chwili obecnej, kiedy 99% jednostek w szpitalu to identyczne maszyny DELL z Windows XP Pro, wiemy, że instalacja jednego komputera wraz z niezbędnym oprogramowaniem zajmuje średnio 2 dni robocze. I to pod warunkiem, że właściwie jest się non stop nie dalej niż 2-3 metry od konsoli tak, aby wcisnąć odpowiednie klawisze w odpowiednim momencie. Jednak jeżeli mamy identyczne jednostki i raz opracujemy poprawną konfigurację, to za pomocą dostarczanych przez Microsoft narzędzi możemy bez problemu spreparować paczkę instalacyjną wykonującą wszystkie czynności za nas i jedyne, co będziemy musieli zrobić, to wpisać nazwę maszyny i podłączyć ją do domeny, a cała czynność łącznie z klonowaniem dysku zajmie 20 minut. Później się okazało, że jedna osoba dzięki temu w ciągu dnia pracy bez problemu może przygotować w ten sposób 20 jednostek! Przy czym jako przygotowanie rozumiem instalację oprogramowania, oklejenie etykietami z numerami ewidencyjnymi zarówno z księgowości, jak i systemu GLPI (o tym w dalszej części), wpisaniem odpowiednich informacji w system GLPI, rozpakowaniem i oklejeniem monitora oraz ustawieniem wszelkich restrykcji w BIOS maszyny tak, aby uniemożliwić dostęp z innych bootowalnych nośników itd…

Wtedy też, po rozmowie z dyrektorem, udało nam się uzyskać zarządzenie, w którym wprowadzenie jakiegokolwiek sprzętu informatycznego do pracy na terenie szpitala musi być poprzedzone uzyskaniem przez zainteresowane osoby akceptacji naszego działu, co do poprawności i adekwatności konfiguracji rzeczonego sprzętu. Dzięki temu mamy kontrolę nad tym co i w jakim stanie jest pozyskiwane dla szpitala, nawet w procesie darowizn. W zdecydowany sposób zapobiega to wprowadzaniu egzotycznych jednostek, które potem musiałyby być specjalnie, czytaj długo, obsługiwane.

Kolejnym wnioskiem, jaki się nasuwa tutaj, jest żelazna dyscyplina w procesie zamawiania sprzętu. Piszę żelazna, choć sam wiem, że jest to praktycznie niemożliwe, ale dążyć do ideału trzeba. Jeżeli w procesie przetargowym mamy zamiar kupić 150 jednostek, to:

- w specyfikacji określmy parametry na wyrost: raz, że realizacja zamówienia potrwa, dwa, że sama instalacja i rozdysponowanie takich jednostek też potrwa, a trzy, że na pewno w ciągu następnych 10 lat nie dostaniemy środków na nowsze jednostki, dotyczy to komputerów, monitorów i drukarek, przy których zawsze okazuje się, że nie doszacowaliśmy wymaganej wydajności,
- nie eksperymentujmy z wyborem, jeżeli mamy sprawdzone jakieś modele, to w nie celujmy, dotyczy to zwłaszcza drukarek,
- jeżeli już dostarczono nam zamówiony sprzęt i pojawia się konieczność uzupełnienia stanu pojedynczymi jednostkami, to żeby nie wiem jak bolało, kupujemy identyczne, jak w postępowaniu, aż do zaprzestania ich produkcji, nawet jeżeli są już nowsze, lepsze i tańsze modele, a jeżeli już wymieniać na nowe to *wyłącznie globalnie, po całości!*

Powróćmy jednak do globalnych zagadnień. Czas eksperymentów zakończył się, błędy zostały zauważone, wnioski wyciągnięte, struktura i funkcje zweryfikowane. Teraz trzeba było te wiadomości wdrożyć w życie. Proces zmian dopasowywania systemu do potrzeb trwa jednak wciąż i na pewno nigdy się nie zakończy. Na podstawie przemyśleń powstał taki oto schemat naszego rozwiązania:



Centralnym, w dosłownym słowa znaczeniu, elementem systemu jest katalog użytkowników OpenLDAP na rysunku przedstawiony jako fragment o numerze 8. Przy czym słowo katalog należy raczej rozumieć jako usługa, czyli serwer, ale serwer w rozumieniu właśnie usługi, a nie maszyny. Katalog ten przechowuje informacje o użytkownikach, takie jak dane administracyjne i przynależność do grup, co pociąga za sobą posiadanie lub nie stosownych praw do zasobów sieciowych. Ideą naszą jest to, aby każdy fragment systemu, zarówno obecnie używany, jak i instalowany w przyszłości, integrował się z ową usługą. Czyli jeden człowiek, jeden login, jedno hasło i różne uprawnienia w zależności od potrzeb.

Użytkownik włączając komputer zostanie zapytany o swoje konto i hasło. Po jego podaniu komputer, na jakim przebiega proces logowania, połączy się z serwerem Samba, jako kontrolerem domeny (element nr 2 rysunku), ten zapyta usługę LDAP o użytkownika i po pozytywnym zweryfikowaniu po pierwsze zadecyduje czy nie należy zmienić hasła (zgodnie z Ustawą o ochronie danych osobowych), a po drugie po otrzymaniu informacji o przynależności do odpowiednich grup, udostępni odpowiednie zasoby sieciowe w postaci zamapowanych dysków sieciowych i drukarek. Użytkownik otrzyma dostęp do systemu z uprawnieniami, jakie zostały mu przydzielone.

W tle, bez wiedzy użytkownika, a czasami nawet mimo jego sprzeciwu, dzieją się już inne potrzebne z punktu widzenia administratora działania. Jednym z podstawowych jest uruchomienie odpowiedniego klienta systemu OCS Inventory (15) działającego w tle jako niewidoczny proces systemowy, którego celem jest zebranie możliwie maksymalnej ilości informacji o konfiguracji sprzętowej i programowej stacji roboczej i przekazanie ich do centralnego rejestru mającego swoją reprezentację na serwerze bazodanowym (14). Informacje pobierane automatycznie za pomocą agentów mogą być i są uzupełniane o wszelkie informacje dodatkowe, takie jak nr gniazd sieciowych, lokalizacja w budynkach, numer telefonu najbliższego danemu gniazdu, osoby odpowiedzialne, numery inwentarzowe itd. Z tego centralnego rejestru system GLPI (12), za pośrednictwem interfejsu przeglądarki internetowej, umożliwia raportowanie, rejestrowanie i zarządzanie wszelkim sprzętem informatycznym, oprogramowaniem oraz innymi elementami, takimi jak baza wiedzy czy grafik rezerwacji sali szkoleniowej. Kolejną ważną dla służb informatycznych usługą uruchamianą na stacjach klienckich jest serwer UltraVNC (21), czyli znowu rozwiązanie klasy Open Source pozwalające na przejęcie kontroli nad konsolą (ekran, klawiatura i mysz) użytkownika i wykonanie za niego pewnych czynności czy pomoc w codziennych pracach. Co ważne, do używania dobrodziejstw VNC mają prawo ci użytkownicy, którzy należą do grupy administratorów po podaniu swojego konta i hasła domenowego! Oczywiście

na stacji rozpoczyna działanie również program antywirusowy. W naszym przypadku jest to Comodo, ale może być każdy inny.

Dodatkowo, podczas startu systemu, na stacji roboczej sprawdzane są aktualne wersje oprogramowania i porównywane z tymi, jakie być powinny. W wypadku stwierdzenia obecności niepożądanego oprogramowania może być uruchomiona procedura jego deinstalacji, albo przeciwnie, jeżeli brakuje czegoś lub jest w niewłaściwej wersji system OCS rozpocznie jego instalację dbając o to ,aby np. poranne włączanie wszystkich komputerów nie spowodowało zapchania sieci przy próbie zainstalowania np. najnowszych poprawek systemu XP. System po prostu na poszczególnych komputerach procedurę instalacyjną (oczywiście parametryzowaną) uruchomi w ściśle określonych odstępach czasu, zapobiegając przeciążeniu sieci.

Kolejnym, bardzo przydatnym, elementem systemu jest usługa CUPS (1). Jest to usługa zapewniająca możliwość drukowania przy użyciu wszelkich dobrodziejstw, jakie niesie ze sobą sieć informatyczna. Usługa ta zapewnia obsługę sieciowych kolejek drukarskich w połączeniu z uprawnieniami. Możliwe zatem staje się podłączenie każdej drukarki poprzez kolejkę obsługiwaną przez CUPS i nadanie stosownych praw do niej użytkownikom domenowym zarejestrowanym w LDAP i obsługiwanym przez Sambę. System CUPS dostarcza własne sterowniki do zdecydowanej większości popularnych drukarek dając przy tym możliwość uzyskania dodatkowych funkcji, takich jak zliczanie wydrukowanych stron, tytuły drukowanych dokumentów czy umożliwia przechwytywanie zadań drukarskich w celach kontroli. Funkcje te nie są standardowymi funkcjami systemu CUPS, uzyskaliśmy je dzięki własnej aplikacji współpracującej jednak z systemem. Drukarki, dla których nie znajdziemy sterowników w systemie, oczywiście również będą obsługiwane za pośrednictwem kolejek, ale niestety nie będziemy mieli tu dodatkowych możliwości, o których wspomniałem w poprzednim zdaniu.

Dostęp do Internetu jest realizowany za pośrednictwem serwera proxy (4) komunikującego się z bazą LDAP. Oczywiście każdy użytkownik chcący połączyć się ze światem musi wpisać swój login i hasło, na podstawie którego otrzyma stosowne uprawnienia. I tak dzięki połączeniu kilku usług możemy zadecydować jaki użytkownik, w jakich godzinach, na jakim komputerze oraz w jaki sposób może łączyć się ze światem. Dla przykładu na wszystkich komputerach działających w poradniach przychodni specjalistycznej nie ma możliwości korzystania z zasobów Internetu (poza kilkoma stronami typu Narodowy Fundusz Zdrowia czy Ministerstwo Zdrowia). Na innych komputerach, w godzinach popołudniowych i nocnych, użytkownicy mogą trochę więcej, ale w godzinach typowej pracy, czyli 7:30-15:05, restrykcje są największe. Oczywiście dostęp do stron internetowych potrzebnych w pracy jest możliwy bez konieczności logowania się, a jeżeli użytkownik będzie próbował wejść na stronę, która powinna być dostępna, ale została zablokowana, może, klikając odpowiedni odnośnik, zgłosić potrzebę odblokowania tejże strony. Stosowna informacja o takiej prośbie dotrze do administratorów systemu. Dodatkowo serwer proxy umożliwia zestawianie połączeń potrzebnych do pracy niektórych programów pracujących wewnątrz sieci szpitalnej z odpowiednimi hostami poprzez Internet. Typową funkcjonalnością serwera proxy jest także filtrowanie ruchu sieciowego. Dostępne są tzw. białe i czarne listy adresów (domen), z którymi można lub nie można nawiązywać połączenia. Dostępny jest także zestaw słów i fraz których obecność w przekazywanych czy odbieranych informacjach świadczy o tym, że połączenie nastąpiło z serwerem zawierającym np. treści pornograficzne.

Jak każda jednostka, tak i nasz szpital, posiada oczywiście własny serwer www (13) i pocztowy (7). Na serwerze www działa system zarządzania treścią Joomla (19). Dzięki niemu modyfikowanie zawartości stron jest możliwe za pomocą dość łatwego i intuicyjnego w obsłudze interfejsu przeglądarkowego. Dzięki niemu np. niektórzy użytkownicy, po uprzednim zalogowaniu, mogą umieszczać na stronach www informacje o np. przetargach publicznych czy zarządzeniach i rozporządzeniach wewnętrznych. Zatem funkcje do niedawna zarezerwowane dla administratorów czy programistów wręcz zostały przekazane użytkownikom bezpośrednio odpowiedzialnym za merytoryczną stronę spraw związanych np. z zamówieniami publicznymi.

Dostęp do poczty elektronicznej jest realizowany przez SquirrelMail w postaci strony www dostępnej z poziomu strony internetowej szpitala. W ten sposób uniknięto konieczności konfigurowania programów pocztowych typu Outlook oraz niebezpieczeństw związanych z błędami, jakie posiadają programy obsługujące pocztę elektroniczną. Dzięki napisaniu odpowiednich skryptów, założenie konta domenowego oznacza jednoczesne założenie konta poczty elektronicznej z możliwością przydzielenia dodatkowych aliasów (przekierowań nazw) dla zainteresowanych. Dzięki temu wiadomo, że np. konto alojz16 może oznaczać zarówno adres `alojz16@szpital.lublin.pl`, jak też `Aneta.Alojziewicz@szpital.lublin.pl`. Nadmienić tutaj należy, że w sieci wewnętrznej nie ma możliwości skonfigurowania programów pocztowych do połączeń z innymi serwerami pocztowymi, np. WP czy ONET. Zostało to świadomie zablokowane.

Serwer DHCP (3) jest odpowiedzialny za dynamiczne przydzielanie wewnętrznych adresów IP wszystkim urządzeniom korzystającym z sieci według odpowiednich schematów. Dzięki temu wiadomo później, iż adresy 10.0.11.XXX to pula drukarek sieciowych, a 10.0.0.XXX to serwery. Oczywiście dodatkowo

powiązanie adresów IP z adresami sprzętowymi (MAC address) daje dodatkowe możliwości śledzenia ruchu sieciowego. System IDS (6) jest właśnie tym fragmentem, który odpowiedzialny jest za monitorowanie ruchu sieciowego w kierunku nietypowych zachowań sugerujących włamania, wadliwą pracę urządzeń czy obecność wirusów komputerowych w sieci. Za jego pomocą jesteśmy w stanie wykryć większość nieprawidłowości i złośliwego działania nawet jeżeli brak jest jeszcze w programach antywirusowych funkcji wykrywających dany typ szkodnika.

Usługa NTP (5) odpowiedzialna jest za synchronizację czasu we wszystkich kluczowych miejscach systemu.

Przed niepowołanym dostępem z zewnątrz do wewnętrznej sieci chroni odpowiednio skonfigurowany firewall (9).

Dzięki usłudze VPN (10) jest możliwość realizacji tzw. bezpiecznych połączeń prywatnych poprzez sieć publiczną. Usługa ta oraz grupy VLAN obsługiwane przez sieciowe urządzenia, umożliwia zestawianie nietypowych połączeń potrzebnych do pracy niektórych aplikacji oraz do separacji ruchu sieciowego dla podmiotów dzierżawiących pomieszczenia wewnątrz szpitala. Niezmiernie ważna jest tutaj pełna unifikacja sprzętu sieciowego. Zachowanie jednego producenta urządzeń sieciowych zapewniło taką możliwość.

Jako element o numerze 18 widnieje elektroniczne repozytorium dokumentów OWL. Jest to przetłumaczony przez nas na język polski system działający jako wewnętrzny serwis www umożliwiający obieg dokumentów w postaci elektronicznej. System ten powiązany jest ściśle z usługą LDAP oraz rozszerzony o własny system uprawnień. Dzięki temu można w nim odzwierciedlić formalną i nieformalną strukturę organizacyjną jednostki, zdefiniować typy dokumentów i specyficzne dla danego typu cechy, na podstawie których następnie będą zarządzane dokumenty. Dzięki temu systemowi możliwa jest do realizacji obsługa sekretariatów i kancelarii oraz zadaniowych grup np. ds. wdrożenia norm jakości ISO z całą proceduralno-formalną otoczką. Przyznać jednak w tym miejscu należy, że o ile system jest skonfigurowany i gotowy do użycia, to jego wdrażanie zostało zawieszone z powodów konieczności opracowania precyzyjnych procedur postępowania. Pomóc ma w tym rozpoczęty proces uzyskania certyfikatu ISO.

Każdy system ma swoje słabe strony, ot chociażby w postaci możliwych uszkodzeń sprzętu, na którym działa lub awarii oprogramowania. Przed skutkami takich awarii zabezpiecza serwer kopii zapasowych Bacula (17). Usługa ta zapewnia wykonywanie kopii zapasowych kluczowych elementów systemu. Za jego pomocą archiwizowana jest zawartość dysków wszystkich serwerów i wskazanych stacji roboczych oraz poszczególnych elementów, jak np. konkretnej bazy danych jednej z wielu obecnych na wskazanym serwerze. Praca tego systemu jest w pełni zautomatyzowana i jedyna akcja ze strony administratora, jaka jest potrzebna do przeprowadzenia, to przeniesienie plików z kopiami bezpieczeństwa na zewnętrzne nośniki, ale co, kiedy i w jaki sposób kopiować automatycznie decyduje opisywany system.

Oczywiście staramy się, aby system był jak najbardziej niezawodny. Staramy się przewidywać nieprzewidywalne oraz najszybciej, jak to możliwe, reagować na zaistniałe sytuacje. Aby zareagować, należy najpierw posiąść wiedzę o tym, że coś nietypowego wydarzyło się. Odpowiedzialny za to jest system Zabbix (16). Stale monitorując działanie wskazanych elementów systemu za pomocą odpowiednich agentów lub używając protokół SNMP czy też reagując na wyniki działania innych programów i skryptów informuje natychmiast o niepokojących objawach. Używając odpowiednich agentów dedykowanych do konkretnych systemów może dodatkowo podjąć stosowną akcję np. restartu usługi, której wadliwe działanie zostało wykryte. Do współpracy z Zabbiksem zaprosiliśmy Krystynę, czyli syntetyzer mowy informujący nas bezpośrednio o zaistniałej sytuacji. Często występuje sytuacja, kiedy Krystyna powie o np. braku zasilania w szafie krosowej zanim zadzwoni pierwszy telefon z informacją, że „coś jest nie tak". Dlaczego Krystyna, to wie każdy, kto widział przynajmniej raz pewną reklamę w TV. Oczywiście sposób przekazywania informacji nie jest ograniczony wyłącznie do syntetyzera mowy. Równie dobrze może to być email czy sms. W chwili obecnej oprócz wymienionej już Krystyny informacyjną rolę pełni duży 42-calowy monitor wiszący na ścianie naszego działu, na którym prezentowane są informacje o aktualnym stanie poszczególnych elementów systemu oraz komunikaty generowane automatycznie przez poszczególnych agentów zainstalowanych w odległych miejscach.

Monitorowanie bieżącej pracy to jedno zagadnienie. Innym niezmiernie ważnym jest logowanie (zapisywanie) informacji o aktywności systemu. Przy czym aktywność należy rozumieć tutaj bardzo szeroko. I tak w rożnych częściach systemu są logowane różne informacje o aktywności i zdarzeniach. Argus (20) jest odpowiedzialny za logowanie informacji o połączeniach sieciowych. Informacje o ruchu z Internetem (kto, kiedy i jakie strony odwiedzał lub próbował odwiedzić) są przechowywane na serwerze proxy (4). Informacje o wydrukach są przechowywane oczywiście przez CUPS (1). Natomiast o aktywności użytkowników (kto, kiedy i gdzie się zalogował oraz co zrobił na plikach) w systemie Samba (2). Oczywiście na serwerze poczty (7) są logowane wszelkie informacje o przesyłkach email oraz informacje systemów współpracujących z serwerem pocztowym (np. antywirus) a na serwerze www (13) analogiczne informacje odnośnie połączeń z tymże serwerem. Zabbix (16) przechowuje informacje

o zdarzeniach w systemie itd. Właściwie każdy system przechowuje informacje odnośnie usług, jakie wykonuje i wszelkich zdarzeń z nimi związanych, przy czym ilość i zakres przechowywanych informacji zależy wyłącznie od inwencji administratorów oraz pojemności dysków twardych, na których te informacje są przechowywane. Należy rozsądnie podejść do tematu, aby proces monitorowania nie pochłaniał większych zasobów systemu niż zużywają je normalne procesy produkcyjne.

Teraz kilka liczb

Opisywany system obsługuje duży szpital, w którym jest około 650 łóżek. Sieć komputerowa oparta jest o miedziane łącza kategorii 5 rozmieszczone w 12 punktach dystrybucyjnych (szafach krosowych) połączonych światłowodami. Komunikację ze światem zapewnia również światłowodowe łącze o przepustowości do 8 Mb/s. Wewnątrz jednostki pracuje około 400 komputerów o ujednoliconej konfiguracji sprzętowej i programowej. 75% tej liczby stanowią jednostki Dell OptiPlex z dwurdzeniowym procesorem AMD, 1GB RAM, 80GB HDD, monitor LCD 19". 99% wszystkich jednostek pracuje pod kontrolą MS Windows XP Pro. Tak jest teraz, ale początki były trudne. Właściwie w naszej jednostce można było znaleźć wszystko. Myślę, że niektórym producentom łezka w oku by się zakręciła na widok swoich produktów sprzed prawie 20 lat! Było tam wszystko, od jednostek jeszcze klasy Pentium, do najnowszych wielordzeniowych. Spotkać można było praktycznie wszystkie systemy operacyjne: MS DOS, DR DOS, Free DOS, MS Windows 3.1x, MS Windows 9x, MS Windows 2000, MS Windows ME, MS Windows NT Server, MS Windows NT Workstation, MS Windows XP, MS Serwer 2003, Linux, SUN Solaris itd. Trzon stanowiły jednak systemy Microsoft Windows 98 i XP Professional.

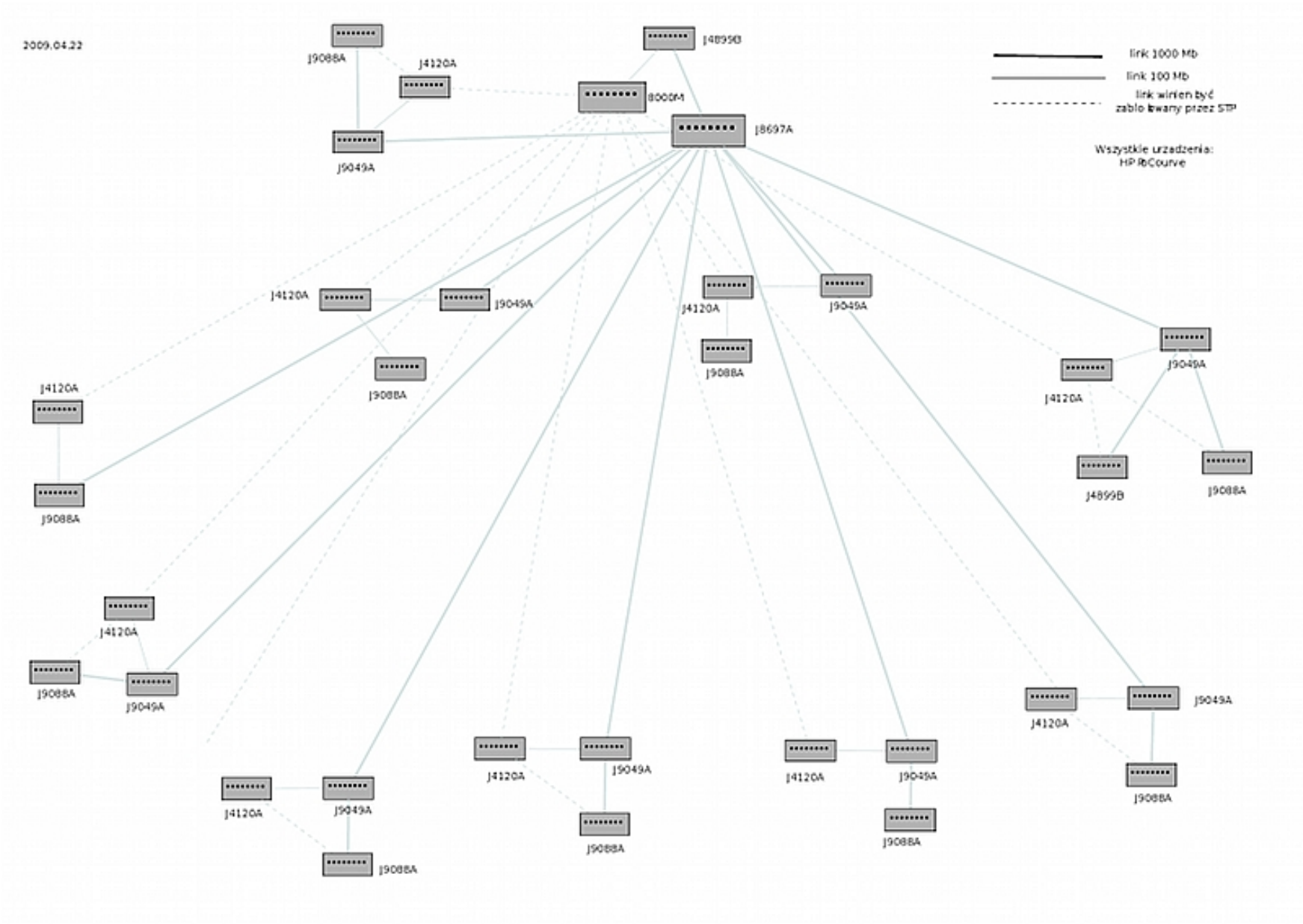
Obecnie w skład systemu wchodzi kilkanaście serwerów. Trzon stanowią tutaj jednostki Dell PowerEdge 2950 z dwoma czterordzeniowymi procesorami Intel XEON każda (4 jednostki) oraz jeden egzemplarz Dell PowerEdge 2970 z dwoma sześciordzeniowymi potworami AMD Opteron. Całość uzupełnia kilka pomniejszych jednostek będących pozostałościami z kryzysowych czasów miniony. Są nimi dwuprocesorowe HP NetServer E60 (3 szt.) i HP NetServer LH3r (2 szt.), Compaq Proliant 8000 ze swoimi 8 procesorami Intel XEON (tyle że pierwszej generacji) oraz kilka innych jednostek często składanych z rzeczy, które akurat z szuflady wypadły. Tak zwany szary system produkcyjny (kadry, płace, księgowość, magazyn, zbyt itd.) pracują, zarówno serwer jak i aplikacje, na poczciwym słoneczku SUN Enterprise E450 z dwoma procesorami SPARC pod kontrolą Solarisa i z użyciem bazy danych INFORMIX. Do niedawna na tym samym serwerze działał również podstawowy system biały, czyli obsługujący część leczniczą jednostki. W kącie dodatkowo czekają na ewentualną reimplantację dwie inne maszyny SUN stanowiące źródło części zapasowych. Tak się akurat składało, że taniej było kupić identyczną maszynę poleasingową z 8 dyskami niż jeden nowy dysk do serwera…

Brzmi to przerażająco i bardzo drogo. System swój wcale nie wirtualny byt rozpoczął jednak na maszynach, których nikt z racji miernej wydajności, nie chciałby widzieć u siebie na biurku, a tym bardziej w domu. Zdecydowana większość z nich pozyskana była jako przesunięcia „starych" sprzętów. Inne to jednostki zakupione w firmie oferującej sprzęt poleasingowy, czyli np. 8-o procesorowy serwer COMPAQ za 700 zł brutto! Śmiało mogę powiedzieć, że sprzęt potrzebny do obsługi opisywanego systemu można kupić już za … 3-4 tysiące złotych! Wartość oprogramowania to ZERO złotych! Parafrazując pewną reklamę za sprzęt zapłacisz kartą Maestro, ale możliwości jakie daje system są bezcenne. Jestem pewien, że wdrożenie komercyjnego systemu o podobnych możliwościach pochłonęłoby sześciocyfrowe kwoty niebezpiecznie zbliżające się do siedmiu cyfr.

Topologia sieci

Poniższy rysunek przedstawia topologię naszej sieci i daje również wyobrażenie o rozmiarach i skomplikowaniu całości. Dodać należy, że na schemacie poniższym nie umieszczono tzw. „małpek", czyli durnowatych urządzeń sieciowych typu 4-portowy hub czy print server, co w niektórych miejscach, z powodu braku kabli w ścianach, zmuszeni byliśmy uskutecznić. Sokołem być nie trzeba, aby zauważyć, że w schemacie owym nie ma ani jednego symbolu sugerującego sieć bezprzewodową. Tak właśnie jest w istocie. Przyczyna takiego stanu rzeczy jest prosta. Przy obecnym kształcie Ustawy o ochronie danych osobowych uważam, że administratorskim seppuku byłoby uruchomienie łączności bezprzewodowej w jednostce. Świadomie więc, póki życie w nas się tli, bez walki tego nie zainstalujemy.

Monstrum owo powstało na bazie sieci zorganizowanej w topologii gwiazdy z dodatkowym ringiem jako alternatywną drogą połączeniową. Tak było przynajmniej w założeniach. Potrzeby spowodowały konieczność uruchomienia przynajmniej szkieletu sieci w technologii gigabitowej. W efekcie tego, zostały zakupione urządzenia pracujące z taką prędkością. Przy okazji, wszystkie koncentratory zostały zastąpione przełącznikami z powodu zbyt dużych domen kolizyjnych i zbyt dużego ruchu rozgłoszeniowego generowanego w takich przypadkach. Szkoda nam jednak było „stare" urządzenia odsyłać do lamusa, więc topologia w tym momencie to mniej więcej podwójna gwiazda z poprzeczkami.


2009.04.22
J9088A
J4120A
J4899B
8000M
J8697A
J9049A
link 1000 Mb
link 100 Mb
link winien być zablokowany przez STP
Wszystkie urządzenia: HP ProCurve
J4120A
J9049A
J9088A
J4120A
J9049A
J9088A
J4120A
J9088A
J9049A
J4120A
J4899B
J9088A
J4120A
J9088A
J9049A
J4120A
J9049A
J9088A
J4120A
J9049A
J9088A
J4120A
J9049A
J9088A
J4120A
J9049A
J9088A

Czyli stare urządzenia pracujące z prędkością 100 Mbit/s stanowią alternatywę połączeń dla łączy gigabitowych, w razie jakiejś poważnej awarii.

Dodatkowo, w newralgicznych miejscach, dają one „drogę na skróty" zmniejszając liczbę hopów sieciowych czy zwiększając, ale jednocześnie omijając najbardziej obciążone gałęzie sieci. Per saldo wychodzi i tak na lepsze. Niektóre połączenia standardowo są nieaktywne i czekają na gorsze czasy, czyli ewentualne awarie. Sytuacja taka może mieć miejsce dzięki specyficznym funkcjom i protokołom urządzeń sieciowym Hewlett Packard serii Pro Curve. Nie jestem pewien czy inne urządzenia pozwoliłyby na taką realizację struktury sieci. Domyślacie się pewnie, że każde pudełko na schemacie to przełącznik sieciowy o pojemności od 16 do 48 portów. Przedstawione na schemacie urządzenia, tak jak napisałem, są wszystkie produktami firmy Hewlett Packard. Jeżeli będzie potrzeba rozbudowy, kolejne będą także tego samego producenta albo…wszystkie zostaną wymienione na modele konkurencji. Nie zanosi się jednak na zbyt dużą ilość pieniążków do wydania, więc spodziewać się należy dozgonnej miłości do HP. Jasno trzeba jednak powiedzieć, że miłość owa jest uczuciem pragmatycznym. Zastaliśmy bowiem pierwotną konfigurację w oparciu o produkty HP i tak już zostało. Ciężko już teraz powiedzieć czy kochamy, bo musimy czy dlatego, że najlepsze. Oczywiście w rzeczywistości jest jeszcze jakaś ilość tzw. małpek, czyli urządzeń sieciowych durnowatych zazwyczaj, bo niezarządzalnych, które zmuszeni byliśmy dorywczo instalować w kryzysowych sytuacjach. Ot, jakieś małe koncentratorki, 8-portowe przełączniki czy serwery wydruków. W takiej oto druciano-światłowodowej rzeczywistości funkcjonuje nasz system.

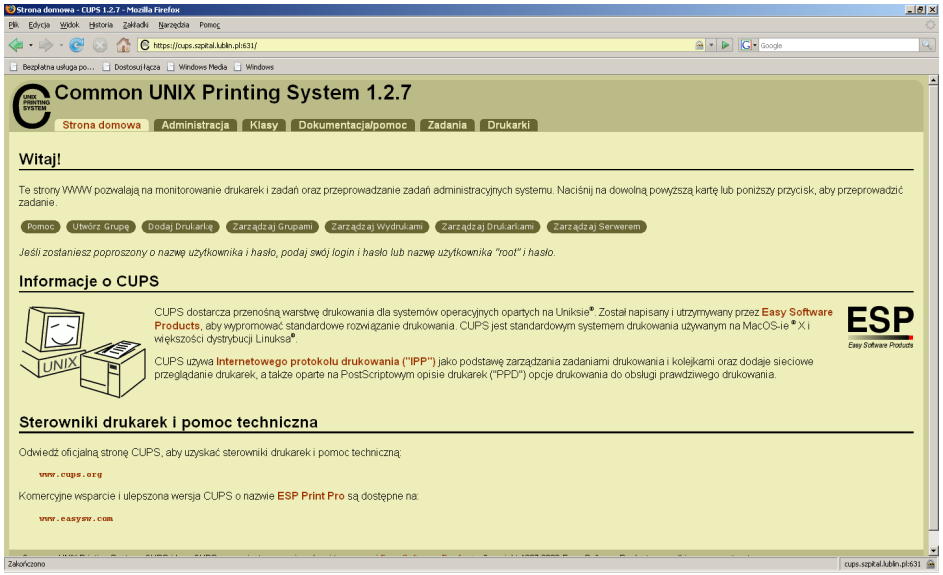
Czas już rozłożyć go na czynniki pierwsze i dokładniej opisać poszczególne elementy systemu.

CUPS (1)

Jednym z podstawowych efektów pracy z systemem informatycznym jest taki czy inny wydruk. Wciąż jesteśmy zobowiązani do podpisywania zestawień i przekazywania ich potem zazwyczaj przełożonym czy petentom. Proces drukowania jest więc ważnym elementem, jaki musi być zapewniony w każdym przedsiębiorstwie i każdej instytucji. Opanowanie jednak tego procesu w sieci, zwłaszcza bardzo dużej, nie jest prostym ani trywialnym zadaniem. Zwłaszcza, jeżeli chcemy mieć jakiekolwiek informacje o tym, co gdzie, kiedy i przez kogo jest drukowane. Z problemem tym świetnie sobie radzi Novell NetWare, ale ma on jedną ważną wadę, decydującą o odrzuceniu jego kandydatury w naszym rozwiązaniu. Jest systemem komercyjnym, a więc płatnym. I to w dodatku sumy jakie wchodziłyby w grę przy sieci zawierającej ok. 400 komputerów i 1200 użytkowników przerażałyby większość dyrektorów. Inną rzeczą jest, że od dawna systemy klasy UNIX nie miały najlepszej renomy, jeżeli chodzi właśnie o obsługę zagadnienia druku w sieci. Pogląd ten panuje poniekąd do tej pory. Czy nadal słusznie, to już inna sprawa.

Mamy więc następujące zadanie. W naszej jednostce jest masa drukarek, wszelkiej możliwej maści czy to pod względem producentów, technologii wydruku, czy to ze względu na interfejs, dzięki któremu można podłączyć je do komputera. Chcemy, aby każda z tych drukarek była dostępna do użycia dla uprawnionych osób, aby wydruki były kolejkowane na serwerze i chcemy oczywiście wiedzieć kto, kiedy, gdzie i co wydrukował.

Z pomocą przychodzi nam tutaj system CUPS obsługujący właśnie sieciowe drukowanie, a po niewielkich modyfikacjach umożliwiający także gromadzenie informacji, na podstawie których możemy zapanować nad wydrukami i zdecydowanie ograniczyć ilość zużywanych materiałów eksploatacyjnych. System także ma niezaprzeczalną zaletę, jaką jest fakt, że jest to system klasy Open Source, więc nie wydamy na niego ani grosza!

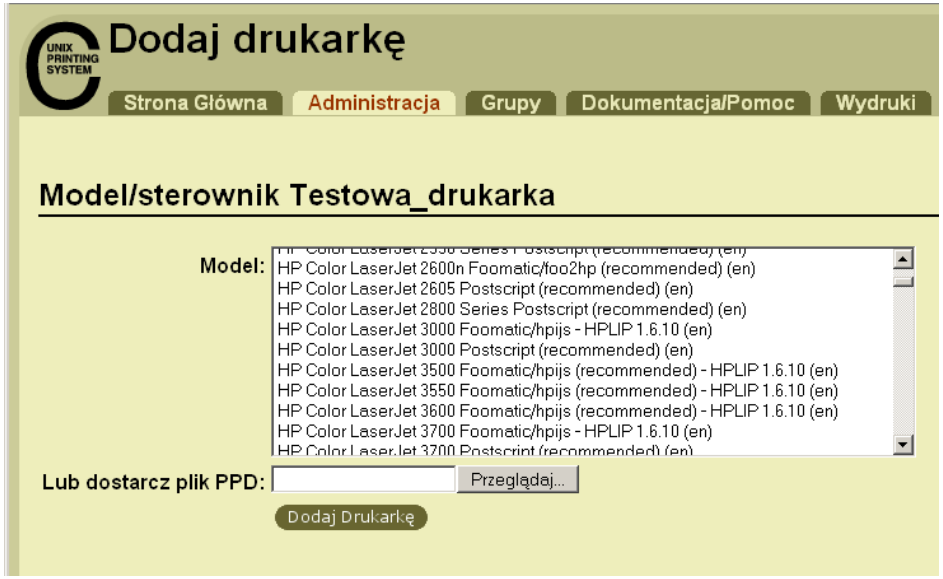


Rysunek 1. Rysunek przedstawia ekran powitalny interfejsu webowego obsługi systemu CUPS. Zauważyliście Państwo coś jeszcze ciekawego? Tak, tak jest po polsku!

Jak to działa? Zasada działania jest dosyć prosta. Mamy serwer obsługujący tę usługę. Na serwerze definiujemy, za pomocą interfejsu webowego, drukarki, jakie będą używane w naszej sieci. Następnie na stacjach roboczych instalujemy

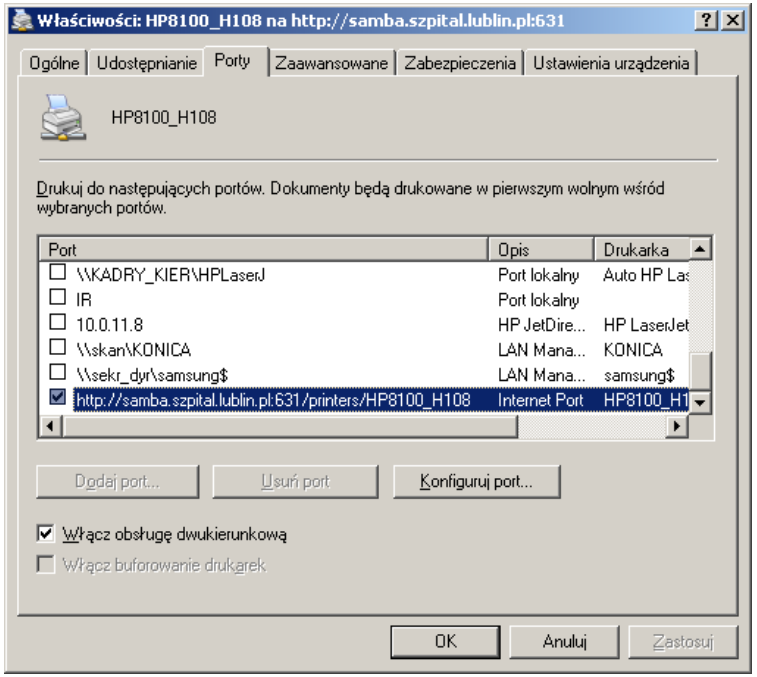
drukarki i podłączamy je do odpowiedniej kolejki zdefiniowanej na serwerze. Jeżeli to konieczne, nadajemy odpowiednie uprawnienia komu wolno drukować i już! System CUPS posiada całe mnóstwo sterowników – właściwie do większości drukarek, jakie można znaleźć na rynku. Sterowniki te są na bieżąco uaktualniane i udostępniane, także nie ma zazwyczaj problemów z odnalezieniem odpowiedniego, a jeżeli nawet nam się trafi taki egzemplarz, to zawsze możemy skorzystać ze sterownika ogólnego. Funkcjonalność użytkową otrzymamy pełną w tym wypadku, natomiast nie będziemy mieli dostępu do danych typu ile stron zostało wydrukowane.

Rysunek 2. Kolejny rysunek obrazujący możliwości konfiguracyjne systemu



Rysunek 3. Widać bogactwo sterowników

Rysunek 4. Widok strony do obsługi już zdefiniowanych i działających drukarek



Rysunek 5. A tak to wygląda ze strony systemu operacyjnego stacji roboczej

Ciut inaczej wygląda sprawa dla drukarek, które interfejsu sieciowego nie posiadają. Co wcale nie znaczy, że jesteśmy w tym momencie bezradni. Instalujemy drukarkę lokalnie, korzystając z konta administratora, najlepiej domeny. Następnie do tej drukarki nadajemy wszelkie prawa specjalnemu wirtualnemu użytkownikowi domenowemu i udostępniamy tą drukarkę w sieci. Teraz definiujemy kolejkę drukarki w CUPSYS i wskazujemy odpowiedni URL dostępu do drukarki wraz parametrami określającymi naszego specjalnego wirtualnego użytkownika, który ma dostęp do tejże drukarki. Od tej pory drukarka jest dostępna przez mechanizm serwera wydruku. Instalujemy ją ponownie na komputerze użytkownika, ale odwołujemy się do kolejki sieciowej, a nie do rzeczywistego portu sprzętowego lokalnej maszyny. Oczywiście, że w takim wypadku wszystkie wydruki przechodzą przez sieć dwukrotnie, ale korzyści, jakie uzyskujemy dzięki takiemu rozwiązaniu, są zdecydowanie większe niż wada, jaką jest niewątpliwie dwukrotne przesłanie przez sieć w sumie lokalnego wydruku.

Bez znaczenia, jakim mechanizmem podłączamy drukarkę, pamiętać musimy o nadaniu stosownych praw dla grup użytkowników (a samych użytkowników w ostateczności) do stosownej kolejki w systemie CUPSYS reprezentującej drukarkę. W ten sposób drukowanie sieciowe mamy opanowane, a Wielki Brat zyskuje możliwości śledzenia działań związanych z drukowaniem.

Analizując tę usługę, oczywistym staje się dążenie do unifikacji sprzętu drukującego w jednostce. Im mniej modeli drukarek, tym mniej potencjalnych problemów konfiguracyjnych. W procesach analizy przed zakupem kolejnych urządzeń zadbać należy, aby pozyskane jednostki były obsługiwane przez CUPSYS w sposób natywny. Zdecydowanie polecamy wcześniejsze przeprowadzenie dłuższych testów. Dlaczego? Ano dlatego, że mamy przykład, iż mimo zapewnień producenta o spełnianiu pewnych warunków, mamy drukarki Lexmark E250dn, których interfejsy sieciowe mają „jakieś problemy" i nie współpracują idealnie z resztą systemu. Systematyczna konieczność twardego resetowania drukarki sugeruje, że to jednak ona, a nie inne elementy, jest przyczyną problemu. Taki detal byliśmy jednak w stanie zaobserwować dopiero po kilku tygodniach pracy z tym modelem.

Drugi wniosek jaki się nasuwa jest taki, że zdecydowanie lepszym pomysłem jest zakupienie mniejszej ilości, ale większych, wydajniejszych i o większych możliwościach drukarek umieszczanych w strategicznych miejscach firmy, niż kupowanie większej ilości prostszych modeli instalowanych na biurkach użytkowników. Już sama konieczność podniesienia się z krzesła i przejścia 5 czy 10 metrów skutecznie ogranicza ilość wydruków przepisów kucharskich z sieci…

Samba (2)

Jest to usługa polegająca na udostępnianiu plików według ustalonego porządku poprzez mapowanie stosownych katalogów w postaci dysków sieciowych, oczywiście z punktu widzenia systemów operacyjnych Microsoft, udostępniających poszczególne udziały jako dyski logiczne widoczne pod nazwami w postaci kolejnych literek alfabetu.

Udostępnianie przestrzeni dyskowej serwera to nie jedyny obowiązek tejże usługi. Kolejnym jest przechowywanie na dyskach serwera pewnych informacji o użytkowniku, jego ustawieniach oraz dokumentów, które zazwyczaj są przechowywane na lokalnych dyskach twardych stacji klienckich. Dzięki takiemu podejściu użytkownik dostosowując do swoich potrzeb pulpit nie musi ponawiać tej czynności na każdym komputerze na którym przyjdzie mu pracować. Nie musi się także martwić o zawartość typowych katalogów, jak i organizacji czy zawartości pulpitu. W momencie dokonywania jakichkolwiek zmian, stosowne informacje o tym fakcie są zapisywane w profilu użytkownika na dysku serwera usługi. W momencie, kiedy użytkownik wyłącza komputer lub wylogowuje się, system synchronizuje informacje ze stacji roboczej z informacjami przecho-

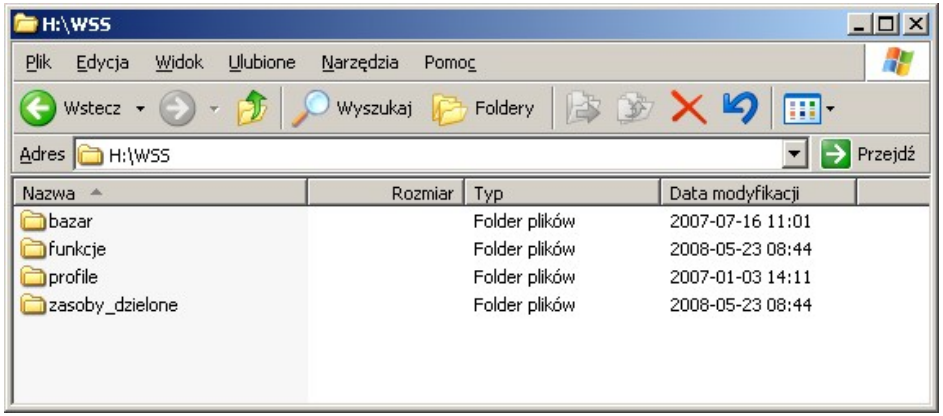
wywanymi na serwerze. Odwrotna sytuacja jest w momencie logowania. System operacyjny stacji roboczej pobiera stosowne dane z serwera i stosuje je na końcówce, na której aktualnie zalogował się użytkownik. Dzięki takiemu podejściu każdy pracownik na dowolnym komputerze ma dostęp do swoich ustawień i plików zarówno z danymi i dokumentami, jak także tych, które zawierają konfigurację programów ot chociażby pocztowych. Oczywiście pod warunkiem, że świadomie lub nie, ale zapisze jakieś informacje w innym miejscu lokalnego dysku twardego. Dodatkową korzyścią tego jest fakt, iż zawartość dysków serwera usługi jest systematycznie archiwizowana i nawet całkowite uszkodzenie czy zniszczenie stacji roboczej nie powoduje utraty danych. Jest także jeden mały, w początkowym okresie użytkowania, minus takiego rozwiązania. Mianowicie użytkownicy przyzwyczajeni do zapisywania wszystkiego na pulpicie nie mogą się odzwyczaić od tego nawyku, przez co np. posiadanie na pulpicie katalogu zawierającego 1,5 GB danych spowoduje konieczność synchronizacji tych danych zarówno podczas logowania, jak i wylogowywania się. Po jakimś czasie, wraz ze wzrostem świadomości użytkowników, problem ten odchodzi do lamusa.

Jest także inna, trzeba to jasno powiedzieć, wada. Otóż w firmach, gdzie pracuje duża liczba użytkowników i dodatkowo użytkownicy ci często korzystają z różnych komputerów, obserwuje się zjawisko zapychania dysków lokalnych. Dlaczego? Właśnie dlatego, że wystarczy, aby na danej maszynie raz ktoś się zalogował. Podczas tego procesu system synchronizuje profil użytkownika lokalnie z serwerem. Jeżeli nasi użytkownicy w swojej beztrosce będą mieli profile o objętości 1-2 GB, to wystarczy, że zaloguje się na maszynie choć raz 20 użytkowników i typowy (80 GB) dysk stacji roboczej zaczyna ledwo zipać. Wniosek z tego taki, że pojemność dysków stacji roboczych powinna być tym większa, im większa jest, nawet potencjalna, ilość użytkowników. Jasno też trzeba powiedzieć, że opisana sytuacja przestaje być problemem w dobie obecnych typowych maszyn, gdzie dyski 500 GB czy 1 TB już nikogo nie dziwią. Nasze zostały zakupione już ponad rok temu (niestety w informatyce rok to JUŻ cała era), kiedy typowa pojemność to było właśnie około 80 GB.

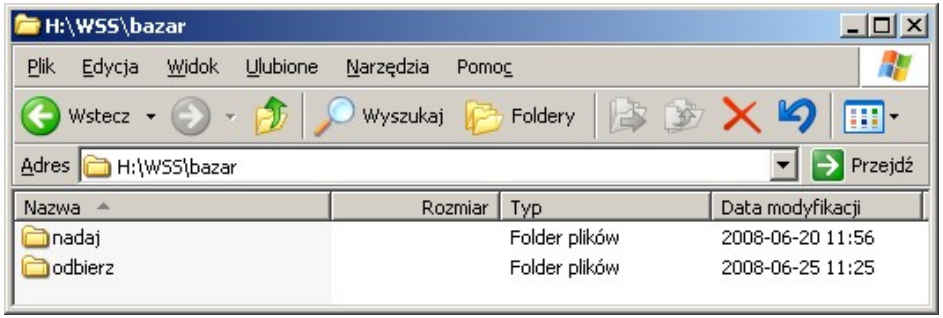
Stosowne informacje o uprawnieniach czy to specyficznych dla danego użytkownika, czy wynikających z przynależności do określonej grupy roboczej, czy też z faktu okupowania danej roli, są pobierane z serwera usługi LDAP. Samba w momencie logowania pobiera odpowiednie informacje z LDAP i na tej podstawie uruchamia odpowiednie skrypty oraz mapuje sieciowe dyski. I tak użytkownik należący do grup *Gastrologia* i *Endoskopia* zauważy pojawienie się dysku H (w naszym przypadku oczywiście) i w jednym z podkatalogów będzie miał dostęp do dalszych oznaczonych jako *Endoskopia* oraz *Gastrologia*. Oprócz specyficznych dla danego użytkownika zasobów, system zmapuje wszystkie typowe.

W naszym przypadku do typowych będą należały:

- Dysk publiczny – objętość plików przechowywane na tym dysku ograniczona jest pojemnością dysku serwera, niemniej jednak system jest tak skonfigurowany, że zawsze jest dostępne co najmniej 20% powierzchni użytkowej. W wypadku, kiedy informacje przekraczają magiczną objętość 80% powierzchni dysku, system automatycznie kasuje pliki poczynając od najstarszych do momentu aż zostanie przywrócony gwarantowany 20% zapas,
- Katalog domowy użytkownika,
- Katalog *Kosz* – czyli odpowiednik kosza na pulpicie Windows, ale odnoszący się oczywiście do zasobów sieciowych. Czyli wszystko, co skasujemy z dysku sieciowego, najpierw ląduje w koszu z zachowaniem pełnej struktury kasowanych katalogów. W momencie usunięcia z tego katalogu pliki są rzeczywiście i trwale kasowane. Oczywiście, jeżeli w systemie zaczyna brakować miejsca, wtedy kasowane są pliki właśnie z tego katalogu poczynając od najstarszych. System automatycznie może kasować pliki z kosza starsze niż np. 30 dni,
- Katalogi grupowe – czyli katalogi przyporządkowane jako domowe dla poszczególnych grup roboczych, do których należy logujący się użytkownik,
- Katalogi funkcyjne – czyli katalogi przyporządkowane jako domowe dla poszczególnych funkcji, jakie sprawuje logujący się użytkownik,
- Katalog *Bazar* – czyli plikowy odpowiednik skrzynki odbiorczej i nadawczej. Rozwiązanie to zostało opracowane w trakcie prac i jest z powodzeniem używane przez pracowników. Zasada działania jest następująca: wewnątrz katalogu *Bazar* znajdują się dwa kolejne *Nadaj* i *Odbierz*. Odbierz to po prostu plikowa skrzynka odbiorcza, tam znajdziemy wszystkie pliki, jakie ktoś danemu użytkownikowi przesłał. Oczywiście zawartość tego katalogu jest unikalna dla każdego użytkownika zarejestrowanego w systemie. Katalog *Nadaj* to odpowiednik skrzynki nadawczej. W jego wnętrzu znajdują się podkatalogi reprezentujące wszystkie grupy robocze zarejestrowane w systemie. We wnętrzu każdego z podkatalogów znajdują się kolejne subfoldery reprezentujące konkretnych użytkowników systemu. Przy czym nazwy tych folderów zawierają zarówno imię i nazwisko, jak także nick sieciowy osoby, dzięki czemu w oczywisty sposób możemy odszukać i zidentyfikować osobę. Zawartości tych katalogów reprezentujących konkretne osoby nie są już dostępne (to są właśnie katalogi *Odbierz* dla tych osób). Ale można do nich skopiować plik lub pliki metodą *drag & drop*. Oczywiście struktura wszystkich tych katalogów, wraz z uprawnieniami, jest tworzona automatycznie po aktualizacji grup i użytkowników w systemie poprzez uruchomienie odpowiedniego skryptu na serwerze.

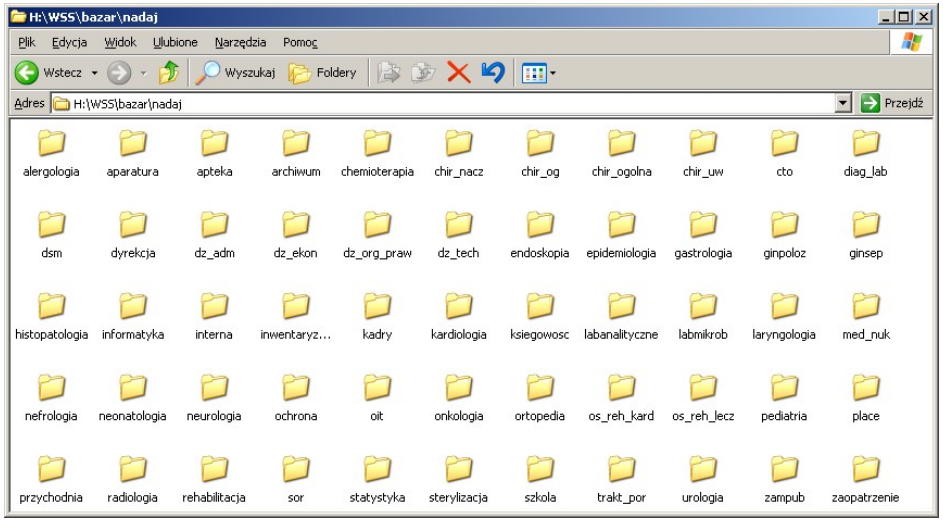


Rysunek 6. Widok zawartości dysku sieciowego. Na poziomie wyższym dostępny jest katalog *Kosz*. Na tym poziomie widnieje katalog *Funkcje*, w którym dostępne są kolejne, w zależności od uprawnień np. *Kierownik kadr*. Katalog *Profile* z przechowywanymi ustawieniami i plikami synchronizowanymi ze stacją roboczą. Katalog *Zasoby dzielone*, w którym znajdują się katalogi grup roboczych do których należy użytkownik. Oraz szeroko opisywany katalog *Bazar*.



Rysunek 7. Kolejny rysunek pokazujący zawartość katalogu *Bazar*.

I jeszcze na koniec dodatkowa informacja. Dla systemów MS Windows 9X w katalogu z profilem przechowywana jest zawartość katalogów i plików: Cookies, Dane aplikacji, Historia, Otoczenie sieciowe, Pulpit, Recent oraz fragment rejestru tyczący się gałęzi NTUSER. Natomiast w wypadku systemów MS Windows NT i MS Windows XP dotyczy to: Cookies, LocalSettings, My Documents, LOG, PrintHood, SendTo, Dane aplikacji, Menu Start, NetHood, ntuser.ini, Pulpit, Szablony, Moje dokumenty, Osobiste, Recent, Ulubione oraz, oczywiście, odpowiedni fragment rejestru.



Rysunek 8. Kolejny bardziej szczegółowy widok zawartości katalogu *Nadaj* w katalogu *Bazar*.

Rysunek 9. Na rysunku powyżej widoczne są już katalogi reprezentujące konkretnych użytkowników.

Serwer DHCP (3)

Przeznaczenie usługi DHCP jest oczywiste. Zamiast nadawać każdemu podłączonemu do sieci urządzeniu adresy IP ręcznie, konfigurujemy tą usługę, aby przydzielała adresy automatycznie wraz z pozostałymi informacjami niezbędnymi do komunikowania się poprzez sieć, takimi jak maska sieci, adres bramy, adresy serwerów nazw DNS i serwer nazw WINS. Usługa ta działa praktycznie bez konieczności większej konfiguracji. Niemniej jednak takie podejście do tematu powoduje pozostawienie pewnego chaosu w sieci oraz umożliwia uzyskanie adresu i podłączenie do sieci każdemu urządzeniu, które potrafi z takiej usługi skorzystać.

Wewnętrzną pulę adresów IP podzieliliśmy zatem na podgrupy. I tak, wszystkie serwery mieszczą się w puli 10.0.0.X, urządzenia sieciowe w 10.0.10.X, drukarki z interfejsami sieciowymi 10.0.11.X, komputery w przychodni specjalistycznej 10.0.43.X itd. Dodatkowo, ustawiony bardzo długi czas dzierżawy adresu oraz wpis w pliku konfiguracyjnym powoduje, że urządzenia zawsze dostają ten sam adres i jest jednoznaczność pomiędzy adresem IP a MAC adresem sprzętowym. Poza tym wskazywanie, jakie urządzenie ma otrzymywać jaki konkretny adres, gwarantuje nam możliwość jednoznacznej identyfikacji urządzenia. Jak wielkie to ma znaczenie dla obsługi systemu i diagnozowania problemów, wie każdy administrator. Takie podejście daje nam też natychmiastową możliwość detekcji nieautoryzowanych urządzeń w sieci, co w połączeniu ze znajomością fizycznej topologii sieci, czyli który port przełącznika sieciowego jest podłączony do którego gniazda w konkretnym pomieszczeniu, umożliwia nam złapanie za rękę na gorącym uczynku intruza.

Dodawanie kolejnych urządzeń podczas typowej pracy polega na dopisaniu kolejnego fragmentu do pliku konfiguracyjnego usługi i restartowanie jej, tak aby dokonane zmiany zaczęły obowiązywać. Każde urządzenie sieciowe jest reprezentowane przez przedstawiony poniżej fragment pliku konfiguracyjnego.

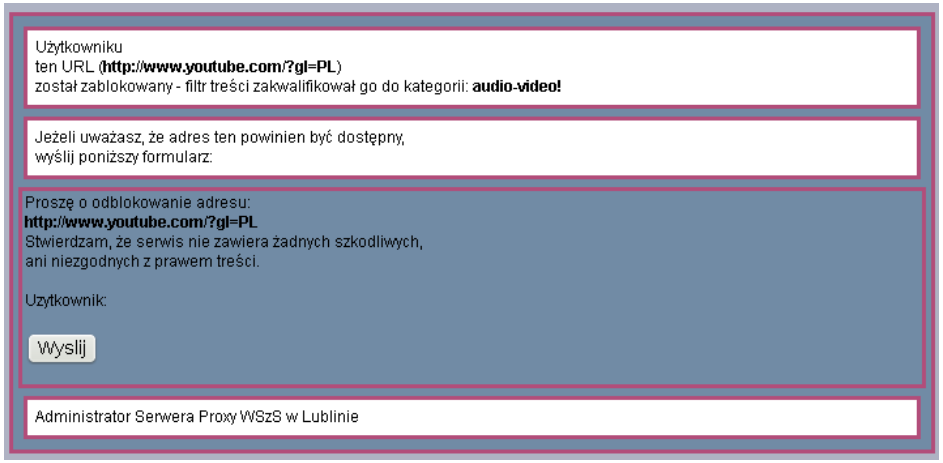
```
host zampub-107 {
     hardware ethernet 00:45:cc:34:b3:cf;
     fixed-address 10.0.11.157;
}
```

Serwer Proxy (4)

Usługa serwera proxy jest warstwą pośredniczącą pomiędzy wewnętrzną siecią a całym Internetem, za pomocą protokołów http, https i ftp, ze wszystkimi jego zaletami i wadami. I jako warstwa pośrednicząca wprowadza wiele dodatkowych możliwości, istotnych zwłaszcza z punktu widzenia administratorów, choć skutki jego działania są widoczne dla wszystkich i mam na myśli tutaj skutki pozytywne. Po pierwsze dostęp do zawartości światowej sieci uzyskuje się po podaniu odpowiedniego loginu i hasła. Na jego podstawie jest identyfikowany użytkownik i przydzielane są mu stosowne prawa. Sam login nie jest jedynym wyznacznikiem tego, co komu wolno. Decyzje o udostępnieniu są podejmowane między innymi także na podstawie adresów IP czy MAC adresów, godziny zgłoszenia żądania dostępu. Oczywiście same informacje o użytkowniku, grupach, do których należy i uprawnieniach, jakie danym grupom przysługują, są przechowywane w bazie LDAP jako głównej składnicy informacji o użytkownikach i prawach. Ponadto usługa ta zawiera specyficzne dla siebie pliki konfiguracyjne zawierające informacje o dostępnych i blokowanych adresach i domenach, czyli tzw. czarne i białe listy.

Za jego pomocą możliwa jest zatem taka konfiguracja, gdzie:

- niektóre domeny (np. www.nfz.gov.pl, www.zus.gov.pl itd.) czy strona domowa szpitala są dostępne bez konieczności podawania loginu i hasła, czyli dozwolone w ten sposób jest wszystko służące do normalnej pracy,
- niektóre domeny (adresy) są permanentnie zablokowane,
- niektóre domeny (adresy) są odblokowane dla wybranych grup i użytkowników,
- niektóre domeny (adresy) są odblokowane dla wybranych grup i użytkowników po zgłoszeniu,
- cały ruch z Internetem jest blokowany na określonych stacjach w określonych godzinach,
- blokowane są domeny (adresy) zawierające określone słowa i wyrażenia (np. związane z pornografią),
- … i wszelkie możliwe kombinacje związane z adresami, czasem, dniem tygodnia, komputerem, grupą itd.



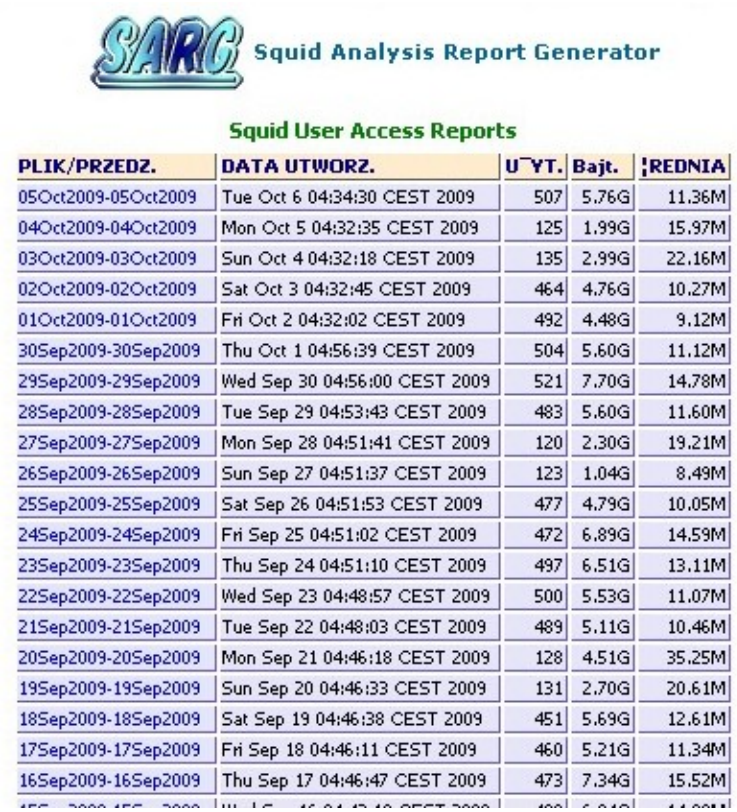
Rysunek 10. Tak wygląda komunikat o zablokowaniu z jednoczesną możliwością zgłoszenia do odblokowania.

Oczywiście wszystkie listy dostępu czy odmowy są w pełni edytowalne. Istnieje także możliwość ich synchronizowania z listami udostępnianymi w Internecie przez zaufane organizacje, publikujące np. listę adresów z pornografią, nosicieli wirusów itp. Oczywiście może się tak zdarzyć, że jakaś strona zostanie niewłaściwie zakwalifikowana do zabronionej grupy. Weźmy np. słowo „sekstans" znane każdemu miłośnikowi żagli, które ze względu na cząsteczkę „seks" może

zostać zakwalifikowane do grupy stron dla „dorosłych” (o bezpośrednim znaczeniu słowa sex w języku angielskim mówić nie muszę). W takich przypadkach użytkownik dostaje stosowny komunikat o powodzie zablokowania dostępu wraz z komunikatem i odpowiedni formularz, którym może zgłosić wniosek o odblokowanie danej strony. Taki wniosek automatycznie trafia do administratorów, którzy podejmują stosowną decyzję. Oczywiście taki wniosek nie jest anonimowy, więc z pewnością nikt nie będzie nas zasypywał prośbami odblokowania „wesołych” stron.

Kolejną bardzo istotną sprawą, zwłaszcza z punktu widzenia administratorów i przełożonych, jest możliwość zbierania wszelkich danych do statystyk odnośnie kto, co, kiedy, gdzie, na jakim komputerze… Niektórzy nazwą to Wielkim Bratem i cenzurą, inni administracją, nadzorem i utrzymaniem. W końcu od pracowników oczekujemy pracy a nie spędzania czasu przy kawie klikając kolejne zdjęcia na „pudelku”. W połączeniu z serwerem www i kilkoma ogólnie dostępnymi skryptami uzyskamy przejrzysty interfejs, dzięki któremu będziemy mogli sprawdzić kiedy i jakie osoby korzystały z Internetu i jakie zasoby oraz jak często odwiedzają.

Rysunek 11.



PLIK/PRZEDZ.	DATA UTWORZ.	U¯YT.	Bajt.	¦REDNIA
05Oct2009-05Oct2009	Tue Oct 6 04:34:30 CEST 2009	507	5.76G	11.36M
04Oct2009-04Oct2009	Mon Oct 5 04:32:35 CEST 2009	125	1.99G	15.97M
03Oct2009-03Oct2009	Sun Oct 4 04:32:18 CEST 2009	135	2.99G	22.16M
02Oct2009-02Oct2009	Sat Oct 3 04:32:45 CEST 2009	464	4.76G	10.27M
01Oct2009-01Oct2009	Fri Oct 2 04:32:02 CEST 2009	492	4.48G	9.12M
30Sep2009-30Sep2009	Thu Oct 1 04:56:39 CEST 2009	504	5.60G	11.12M
29Sep2009-29Sep2009	Wed Sep 30 04:56:00 CEST 2009	521	7.70G	14.78M
28Sep2009-28Sep2009	Tue Sep 29 04:53:43 CEST 2009	483	5.60G	11.60M
27Sep2009-27Sep2009	Mon Sep 28 04:51:41 CEST 2009	120	2.30G	19.21M
26Sep2009-26Sep2009	Sun Sep 27 04:51:37 CEST 2009	123	1.04G	8.49M
25Sep2009-25Sep2009	Sat Sep 26 04:51:53 CEST 2009	477	4.79G	10.05M
24Sep2009-24Sep2009	Fri Sep 25 04:51:02 CEST 2009	472	6.89G	14.59M
23Sep2009-23Sep2009	Thu Sep 24 04:51:10 CEST 2009	497	6.51G	13.11M
22Sep2009-22Sep2009	Wed Sep 23 04:48:57 CEST 2009	500	5.53G	11.07M
21Sep2009-21Sep2009	Tue Sep 22 04:48:03 CEST 2009	489	5.11G	10.46M
20Sep2009-20Sep2009	Mon Sep 21 04:46:18 CEST 2009	128	4.51G	35.25M
19Sep2009-19Sep2009	Sun Sep 20 04:46:33 CEST 2009	131	2.70G	20.61M
18Sep2009-18Sep2009	Sat Sep 19 04:46:38 CEST 2009	451	5.69G	12.61M
17Sep2009-17Sep2009	Fri Sep 18 04:46:11 CEST 2009	460	5.21G	11.34M
16Sep2009-16Sep2009	Thu Sep 17 04:46:47 CEST 2009	473	7.34G	15.52M

Rysunek 12.

Kolejną dość ważną, acz tracącą ostatnimi czasy na znaczeniu, jest funkcja cachowania ruchu internetowego. Jeżeli zatem ktoś będzie chciał się dostać na jakąś stronę, która ostatnio była już odwiedzana, to zamiast pobierać jeszcze raz te same dane, przez zazwyczaj 10-100 razy wolniejsze łącze internetowe niż nasza sieć, dane zostaną „podrzucone” przez serwer oszczędzając czas i pasmo naszego łącza.

SARG Squid Analysis Report Generator

Squid User Access Reports

Przedział czasowy: 17Sep2009-17Sep2009
Użytkownik: _
Sortowanie: BYTES, reverse
Użytk. Raport

ODWIEDZONE SERWISY	POŁĄCZENIA	Bajt.	%Bajt.	Wyj-CACHE-Wyj	CZAS UŻYTKOWANIA	MILISEK	%CZAS
poznan5-6.radio.pionier.net.pl:8000	16	304.89M	95.01%	0.00%	100.00%	07:02:49	25.36M	97.45%
cnt.akademiaparp.gov.pl	930	10.15M	3.16%	1.97%	98.03%	00:00:54	54.06K	0.21%
images.tuba.fm	192	1.41M	0.44%	7.72%	92.28%	00:00:17	17.85K	0.07%
player.zloteprzeboje.tuba.fm	786	789.84K	0.25%	0.04%	99.96%	00:01:29	89.90K	0.35%
www.akademiaparp.gov.pl	311	606.43K	0.19%	13.97%	86.03%	00:00:23	23.12K	0.09%
www.ebgz.pl:443	17	528.32K	0.16%	0.00%	100.00%	00:01:02	62.89K	0.24%
static.nasza-klasa.pl	858	445.62K	0.14%	87.58%	12.42%	00:00:16	16.04K	0.06%
www.mbank.com.pl:443	9	444.82K	0.14%	0.00%	100.00%	00:04:02	242.49K	0.93%
poczta.wp.pl	147	324.89K	0.10%	37.78%	62.22%	00:00:20	20.71K	0.08%
nasza-klasa.pl	393	281.30K	0.09%	1.29%	98.71%	00:00:45	45.57K	0.18%
www.tuba.fm	64	258.99K	0.08%	0.42%	99.58%	00:00:09	9.83K	0.04%
www.mbank.pl	73	82.81K	0.03%	30.90%	69.10%	00:00:09	9.06K	0.03%
rek.www.wp.pl	15	81.02K	0.03%	48.97%	51.03%	00:00:00	991	0.00%
info.mbank.com.pl	15	76.73K	0.02%	5.76%	94.24%	00:00:00	692	0.00%
www.umcs.lublin.pl	27	53.88K	0.02%	16.12%	83.88%	00:00:01	1.48K	0.01%
banery.mbank.eu	5	51.44K	0.02%	0.00%	100.00%	00:00:00	833	0.00%
ad.afilo.pl	4	49.03K	0.02%	1.55%	98.45%	00:00:00	622	0.00%
adv.wp.pl	15	39.61K	0.01%	0.00%	100.00%	00:00:00	387	0.00%

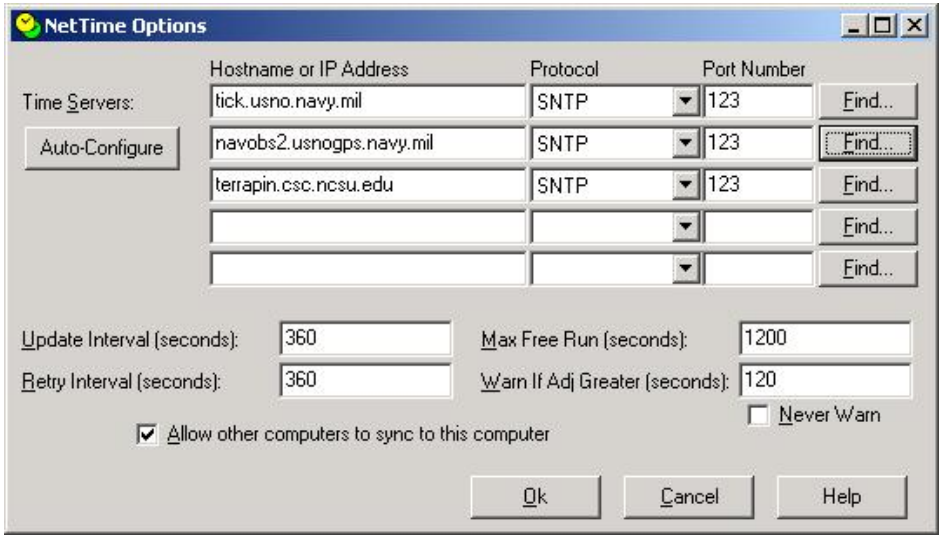
Rysunek 13. To krótki przykład możliwych do uzyskania raportów o działalności użytkowników.

Serwer NTP (5)

Usługa serwera NTP jest jedną z najprostszych w działaniu, acz jedną z najważniejszych. Jej zadaniem jest synchronizacja czasu wszystkich urządzeń współpracujących ze sobą w naszej sieci. Po pierwsze, serwer NTP sam synchronizuje się w odpowiedni sposób z serwerami światowymi, uwzględniając w tej procedurze także czas, w jakim sygnał synchronizujący dociera z odległego czasami o wiele setek czy tysięcy kilometrów serwera nadrzędnego. Po drugie, sam stanowi wzorzec czasu wewnątrz naszej sieci korporacyjnej.

Aby cała usługa działała poprawnie, na wszystkich serwerach i stacjach roboczych muszą być zainstalowani klienci, którzy będą pobierali wzorce czasu z naszego serwera a następnie synchronizowali lokalne zegary maszyn. W sieci dostępnych jest cała masa rozwiązań tego typu na licencjach otwartych. Ważna jest tylko ich pewna istotna cecha. Klient tej usługi musi się tak instalować, aby o ich obecności nie wiedzieli użytkownicy a tym bardziej nie mieli możliwości zablokowania ich pracy, czyli: żadnych ikonek w pasku zadań i widocznych procesów w menadżerze.

Dzięki tej usłudze uzyskujemy spójność czasową wszystkich pracujących urządzeń, a co za tym idzie 100% pewności chronologii działań, kolejności powstawania plików, wydruków itd. Dzięki temu także istnieje logiczny porządek w kopiach zapasowych i ukrócamy ewentualne możliwości „przypadkowej" zmiany daty w kluczowych dokumentach typu historia choroby. Oczywiście blokada zmiany czasu lub daty przez użytkowników, niezbędna do pracy tej usługi, następuje na podstawie odpowiedniego wpisu w rejestr, który jako taki może być dystrybuowany razem z innymi informacjami w profilu. Istnieje zatem możliwość odblokowania tej funkcji dla wybranych użytkowników i/lub komputerów. W naszym przypadku korzystamy z klienta NetTime w wersji 2b7.



Rysunek 14. Tak wygląda okienko konfiguracyjne klienta czasu NetTime

System SNORT IDS (6)

Cytując za serwisem http://pl.docs.pld-linux.org : *Snort to bardzo silny sieciowy system wykrywania ataków (ang. Network Intrusion Detection System, NIDS), który daje szeroki zakres mechanizmów detekcji, mogących w czasie rzeczywistym dokonywać analizy ruchu i rejestrowania pakietów w sieciach opartych na protokołach IP/TCP/UDP/ICMP. Potrafi przeprowadzać analizę strumieni pakietów, wyszukiwać i dopasowywać podejrzane treści a także wykrywać wiele ataków i anomalii, takich jak przepełnienia bufora, skanowanie portów typu stealth, ataki na usługi WWW, SMB, próby wykrywania systemu operacyjnego i wiele innych.*

System ten można nazwać pasywnym snifferem sieci. Sniffer zazwyczaj kojarzy się z oprogramowaniem używanym przez hakerów do włamań. Tak jak w wypadku większości narzędzi, o jego zaszufladkowaniu decydować będzie jednak zastosowanie, a nie potencjalne możliwości (jak w starym kawale o bacy jako potencjalnym gwałcicielu). Pasywny dlatego, że system ten obserwuje ruch sieciowy nie podejmując żadnych działań uwarunkowanych od dynamicznej sytuacji panującej w danym momencie w sieci.

Jego zadaniem jest obserwowanie ruchu sieciowego i jego analiza w celu wykrycia wszelkiego rodzaju anomalii związanych czy to z błędną konfiguracją urządzeń sieciowych i stacji roboczych, czy też prób włamań, działalności wirusów czy innych szkodników itd. W przeciwieństwie do większości snifferów system ten jest tak przemyślany i skonfigurowany, że o ile owszem za jego pomocą można by było przechwycić i odczytać cały ruch sieciowy, to jego zadaniem jest detekcja anomalii i informowanie o nich administratorów. Zawiera zatem wiele reguł, które charakteryzują znane już niepokojące sytuacje. Analizując ruch sieciowy, zarówno pod kątem adresów nadawców i odbiorców, portów, protokołów, natężenia w czasie itd., jest w stanie po pierwsze: wykryć zdecydowaną większość znanych problemów, a po drugie: z bardzo dużym prawdopodobieństwem zareagować na nieznane dotychczas, ale niepokojące objawy.

Dzięki niemu jesteśmy w stanie wykryć i zabezpieczyć się przed typowymi atakami na wewnętrzną sieć, które mogą być realizowane za pomocą całej masy dostępnego w sieci złośliwego oprogramowania, gdzie wystarczy wpisać adres instytucji, której chce się zaszkodzić, aby skutecznie utrudnić czy wręcz zablokować jej pracę. Takie automaty są niestety dostępne na stronach www, gdzie nawet totalny laik może wpisać adres jakiegoś serwera i zapoczątkować katastrofę. Jesteśmy także w stanie zapobiegać połączeniom z i do stref sieci doskonale znanych z destrukcyjnej i szpiegowskiej działalności. Jesteśmy w stanie wykryć obecność nowego jeszcze nieznanego odpowiednim programom wirusa, zanim jeszcze pojawi się na niego antidotum.

Ponieważ system ten analizuje ruch sieciowy, musi być więc „karmiony" odpowiednimi informacjami, czyli ruchem sieciowym. W dobie inteligentnych przełączników sieciowych niezmiernie istotne jest zatem umiejscowienie tego systemu w naszej sieci. Z jednej strony należy zadbać o to, aby istotny ruch sieciowy był w zasięgu systemu, a z drugiej strony, aby nie zapchać go np. potężnymi transmisjami multimedialnego ruchu radiologii cyfrowej. Serwer, na którym działa ten system, musi zatem być wyposażony w kilka kart sieciowych wpiętych w odpowiednie miejsca systemu. Zazwyczaj są to miejsca styku naszej sieci z sieciami zewnętrznymi, spinające segmenty sieci czy zawierające krytyczne urządzenia, takie jak serwery. Potrzebna jest tutaj jednak spora wiedza i doświadczenie administratora, aby z jednej strony uzyskać oczekiwany efekt, a z drugiej nie powielać potężnego ruchu szkieletowego i nie zapisywać bez potrzeby nieistotnych informacji.

System ten oczywiście jest źródłem wielu statystyk i cennych informacji. Jest tym ważniejszy im większa i bardziej zaawansowana jest nasza infrastruktura sieciowa. Można śmiało powiedzieć, że konieczność jego posiadania i analizowania wyników jego pracy rośnie wykładniczo wraz z liniowym wzrostem naszej sieci.

Powiedzieć tutaj wyraźnie trzeba, że ten fragment naszej sporej całości wymaga systematycznego doglądania, dopieszczania i uwagi administratora posiadającego niezbędną wiedzę i spore doświadczenie.

Serwer poczty (7 i 11)

O usłudze tej rozpisywać się nie ma sensu. Wszyscy doskonale wiedzą do czego służy. Nadmienić jednak należy o specyficznych cechach:

- dostęp za pośrednictwem protokołów smtp, smtps, pop3, pop3s, imap i imap3s,
- szyfrowana transmisja pomiędzy klientem a serwerem,
- filtr antyspamowy,
- filtr antywirusowy,
- synchronizacja kont z LDAP (8),
- dostęp do poczty za pośrednictwem www (SquirrelMail).

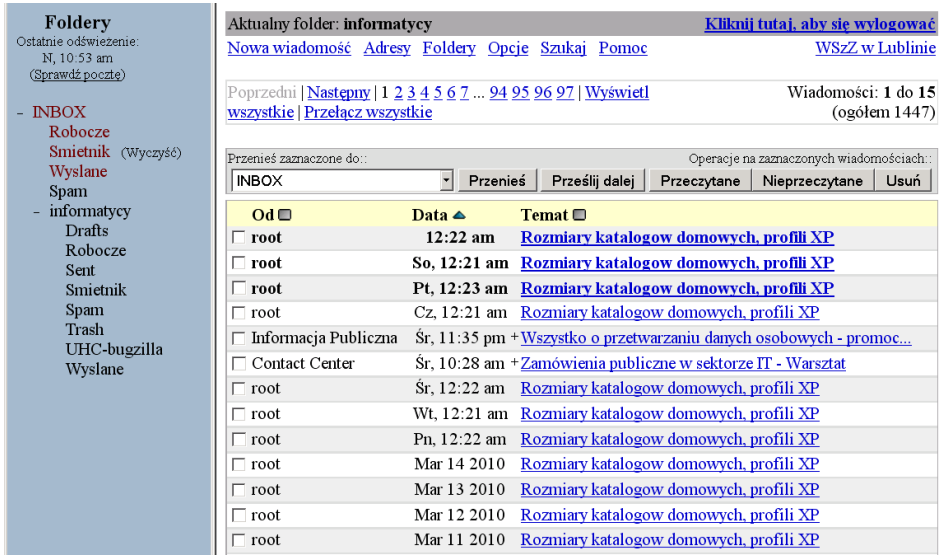
Oczywiście zastosowanie filtrów antyspamowych i antywirusowych nie blokuje ewentualnej możliwości dostępu do zakwalifikowanej jako „potencjalnie niebezpieczna" korespondencji. Użytkownik może uzyskać do niej dostęp w odpowiednim folderze. Niemniej jednak, jeżeli w ciągu 30 dni nie podejmie żadnej akcji, wiadomości tak zakwalifikowane zostaną skasowane z serwera.

W całkowicie świadomy sposób zrezygnowaliśmy wewnątrz naszej sieci z klientów pocztowych typu Outlook czy Outlook Express jako potencjalnych nośników problemów czy to z bezpieczeństwem, czy to z przenoszeniem danych pomiędzy maszynami dla użytkowników używających różnych komputerów w różnych miejscach szpitala. Jedynym więc legalnym klientem pocztowym jest ten dostępny poprzez przeglądarkę, zarówno z wewnątrz, jak i zewnątrz sieci lokalnej.

Nadmienić tutaj należy, że jedyną polecaną przeglądarką w sieci jest popularna Mozilla Firefox, choć zdarzają się oczywiście strony i portale, które niestety bez Internet Explorera działać poprawnie nie chcą. Czy to z powodów obecności formantów ActiveX, czy też innych specyficznych cech.

Również całkowicie świadomie do wnętrza sieci nie przepuszczamy innych protokołów niż http, https i ftp. Czyli nie ma możliwości skonfigurowania klienta pocztowego dla prywatnych kont. Dostęp do nich istnieje za pośrednictwem stron macierzystych serwisów, na których są założone, jednak używanie innych niż służbowe kont traktujemy jako spore faux pas i w miarę możliwości „naciskamy" na używanie wyłącznie poczty służbowej, zwłaszcza w służbowej komunikacji i wymianie danych i dokumentów.

Rysunek 15. Ekran powitalny SquirrerMaila dostępnego ze strony www naszego serwera. Oczywiście https i odpowiedni certyfikat.



Rysunek 16. Kolejny obrazek bliżej prezentujący interfejs klienta pocztowego wraz z możliwościami, jakie niesie ze sobą IMAP.

LDAP (8)

Jak już zostało wspomniane wcześniej, LDAP jest usługą przechowującą w bezpieczny sposób między innymi następujące informacje:

- konta,
- informacje osobowe o właścicielu konta wraz z wszelkimi parametrami potrzebnymi do pracy,
- grupy robocze,
- przynależność poszczególnych osób do grup.

Typowa struktura organizacyjna właściwie każdego przedsiębiorstwa zawiera trzy podstawowe elementy: komórki organizacyjne, role oraz pracowników. Właściwie w każdej firmie, która zatrudnia już przynajmniej kilka osób, struktura ta jest hierarchiczna i najlepiej jest ją przedstawić w postaci drzewa, gdzie poszczególne gałęzie drzewa będą przedstawiały kolejno piony, wydziały, działy, sekcje itd. W każdym takim elemencie reprezentującym kolejną komórkę będą znajdowały się role, czyli inaczej mówiąc stanowiska pracy, np. kierownik działu, główny księgowy itd.

Poniżej zaprezentowano typowy przykład takiej struktury:

— Szpital specjalistyczny
- Dyrekcja
- Dyrektor naczelny
- v-ce dyrektor ds. lecznictwa
- v-ce dyrektor ds.administracyjno gospodarczych
- v-ce dyrektor ds. ekonomicznych
- Sekretarka
- Administracja
  - Dział finansowo-księgowy
    - Główny księgowy
    - Zastępca głównego księgowego
  - Dział służb pracowniczych
    - Kierownik działu służb pracowniczych
  - Dział płac
    - Kierownik działu płac
  - Księgowość inwentarzowa
- Oddziały lecznicze
  - Oddział kardiologiczny
    - Ordynator oddziału
    - Zastępca ordynatora oddziału
    - Pielęgniarka oddziałowa
    - Sekretarka medyczna

- Oddział nefrologiczny
  - Ordynator oddziału
  - Zastępca ordynatora oddziału
  - Pielęgniarka oddziałowa
  - Sekretarka medyczna
- Oddział ginekologiczny
  - Ordynator oddziału
  - Zastępca ordynatora oddziału
  - Sekretarka medyczna
  - Pododdział ginekologii septycznej
    - Lekarz koordynujący
    - Pielęgniarka oddziałowa
  - Pododdział ginekologii operacyjnej
    - Lekarz koordynujący
    - Pielęgniarka oddziałowa

itd. …

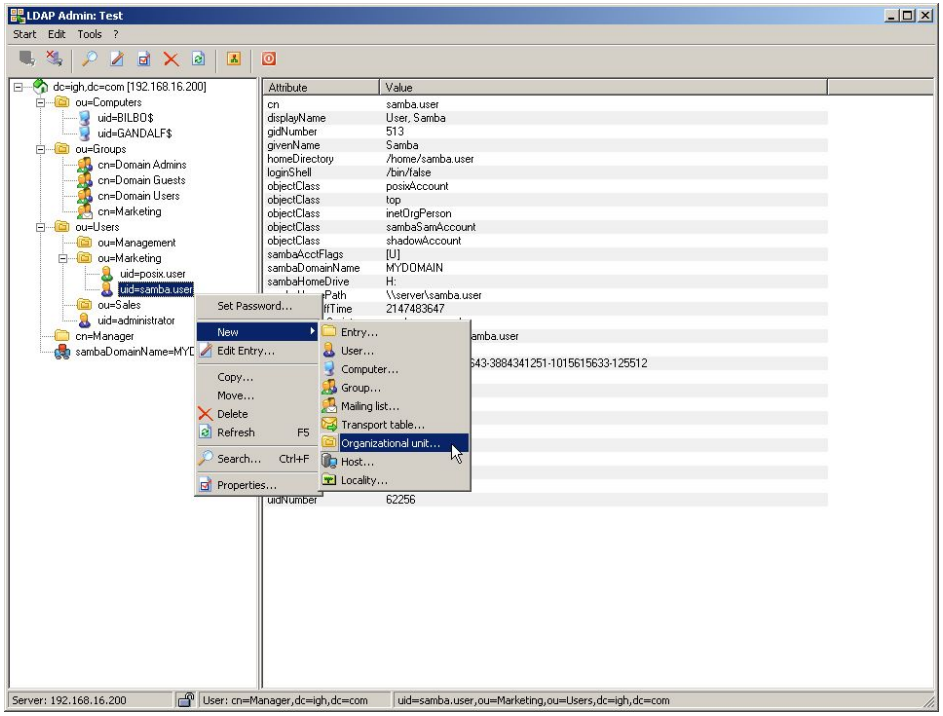
Oczywiście jest to drobna część takiej struktury i przedstawiona w uproszczony sposób z pominięciem specyficznych dla jednostki grup i ról. W przykładzie tym nie ma zaznaczonych poszczególnych pracowników. Jednak nie ma takiej potrzeby, gdyż jako pracowników „typowych" należy rozumieć osoby należące do grupy, np. „Dział finansowo-księgowy".

Usługa Samba, połączona z naszą usługą LDAP, nie potrafi obsługiwać hierarchicznej struktury oraz ról, mimo iż LDAP ma takie możliwości. Obiekty w niej reprezentowane są w postaci „jednowymiarowej", czyli mamy wykaz grup oraz wykaz użytkowników. Nic nie stoi jednak na przeszkodzie, aby, mimo takiego ograniczenia, drzewiastą strukturę jednak obsłużyć. W naszym przypadku realizowane jest to w ten sposób, że każdemu elementowi odpowiadającemu komórce organizacyjnej z powyższego przykładu przyporządkowywana jest stosowna grupa. Oczywiście nie mamy tutaj możliwości przenoszenia uprawnień w dół struktury w sposób automatyczny (choć nic nie stoi na przeszkodzie, aby funkcjonalność taką osiągnąć tworząc dodatkowy skrypt na serwerze), czyli dziedziczenia. Funkcjonalność taką uzyskujemy nadając prawa i przyporządkowując użytkowników, dla każdej grupy oddzielnie. Jest to pewna uciążliwość, niemniej jednak nie taka straszna biorąc pod uwagę, że strukturę taką zazwyczaj definiuje się tylko raz w procesie wdrożenia a później tylko modyfikuje przy zatrudnianiu nowych pracowników czy zwalnianiu obecnie pracujących.

Podobnie sprawa się ma z rolami organizacyjnymi. Mimo iż LDAP nie obsługuje takich obiektów, to jako reprezentację roli przyjmujemy po prostu jednoosobową grupę z jej uprawnieniami. Dzięki takiemu podejściu osiągnięto funkcjonalność podobną do NDS. Jeżeli od jakiegoś dnia osoba Zdzisław Bejzik nie pracuje na stanowisku ordynatora oddziału, to wystarczy, iż usuniemy go z jednoosobowej grupy reprezentującej ordynatora oddziału np. kardiologii a w jego miejsce wpiszemy Romana Koparę. Jeden straci wszelkie uprawnienia po kilku kliknięciach myszką, a drugi je zyska kosztem pierwszego.

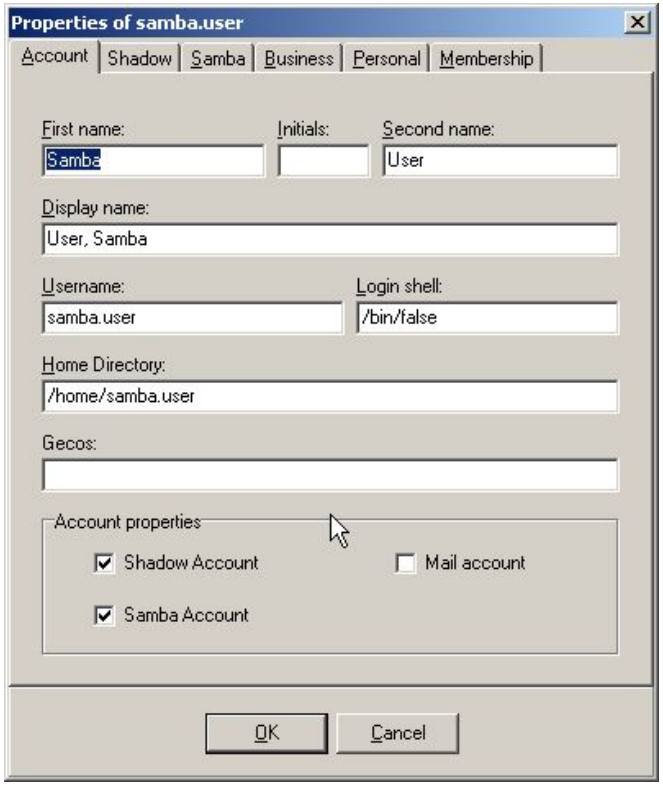
Tak jak zostało powiedziane, LDAP to specjalna usługa działająca (w naszym przypadku) na serwerze opartym o system Linux. Dostęp do zasobów tejże usługi z użytecznością administratora jest oczywiście możliwy z poziomu serwera, na którym usługa działa. Niemniej jednak istnieje spora liczba programów umożliwiających prace administracyjne np. na stacjach roboczych wyposażonych w MS Windows. My korzystamy z LDAP Admin, jednego z wielu reprezentantów wolnych (czyli darmowych!) programów. Poniżej przedstawiam kilka obrazów przedstawiających tenże program w akcji.

Rysunek 17. Ogólny widok okna LDAP Admin. Po lewej stronie widać drzewo kategorii dostępnych w usłudze LDAP. Po prawej cechy wskazanego obiektu.



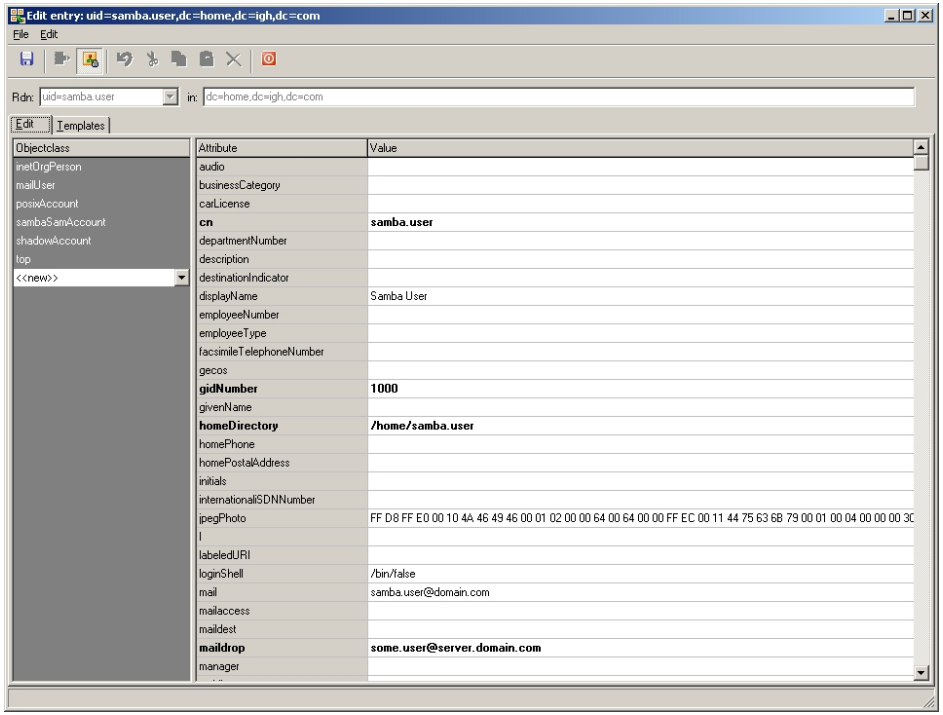
Rysunek 18. Powyższy rysunek pokazuje okno programu z rozwiniętą listą użytkowników w lewej części i właściwościami wskazanego obiektu po prawej. Widać w przedstawionej liście trzy typy obiektów występujących w kategorii „people". O ile nie dziwią na

pewno nikogo ikony reprezentujące użytkowników (te z zielonym kolorem reprezentują konta typu „shadow" wskazujące na konta w innych systemach, np. poczty email), o tyle dziwić mogą ikony wskazujące na komputery. Nie ma tu żadnej pomyłki. Współpraca z systemem Samba wymaga, aby komputery podłączone do domeny miały założone konta tak, jak użytkownicy, ale ze specyficznymi właściwościami.



Rysunek 19. Rysunek pokazuje okno z właściwościami obiektu typu użytkownik. Na zakładce „Membership" mamy możliwość zarządzania przynależnością do grup.

Katalog LDAP posiada predefiniowane typy obiektów oraz pewne właściwości, które mogą być wypełniane dla obiektów konkretnego typu (np. nazwisko i imię dla użytkowników). Nic nie stoi jednak na przeszkodzie, aby predefiniować nowe typy obiektów oraz nowe cechy dla danego typu obiektu. I tak bez problemu dla obiektu typu użytkownik (people) można zdefiniować kilka dodatkowych pól zawierających np. numer praw wykonywania zawodu lekarza, identyfikator osoby w systemie kadrowo-płacowym (odnośnik do innej bazy danych) czy identyfikator w systemie medycznym. Dzięki takim definicjom możemy w łatwy sposób połączyć różne systemy. Dodatkowo mając odrobinę wprawy w pisaniu skryptów możemy zautomatyzować uzupełnianie danych poprzez pobieranie ich z innej bazy po wskazaniu identyfikatora lub odwrotnie przesyłając dane z katalogu LDAP do innego systemu.



Rysunek 20. I kolejny ekran pokazujący możliwe do przechowywania dane.

Dzięki danym przechowywanym w katalogu LDAP, usługa serwera plików Samba przydziela odpowiednim użytkownikom właściwe prawa na podstawie np. przynależności do konkretnej grupy roboczej. I tak logujący się pracownik oddziału gastrologii pracujący jednocześnie w ośrodku endoskopii uzyska dostęp do katalogów „Gastrologia" i „Endoskopia" na odpowiednio zmapowanym dysku sieciowym.

Obsługa typowych działań w katalogu LDAP w powiązaniu z uprawnieniami nadawanych w Sambie jest zautomatyzowana i zazwyczaj wymaga uruchomienia konkretnego skryptu, dzięki któremu nawet początkujący administrator może dokonać stosownych operacji bez znajomości magicznych poleceń wydawanych w linii komend znakowej konsoli Linuksa.

Firewall (9)

Na straży dostępu, pomiędzy światowym Internetem a siecią wewnętrzną, stoi nasz firewall. Jest to typowy i bodaj najpopularniejszy przedstawiciel programów w tej klasie, czyli IPTABLES. Jego zadaniem jest odpowiednie filtrowanie pakietów ruchu przychodzącego i wychodzącego. Na podstawie zapisanych reguł decyduje jakie kombinacje protokołu, portu, usługi, adresu itd. są dozwolone. Ukrywa możliwość wykrycia obecności hostów i szeroko pojętego skanowania sieci. Zapobiega również przed nieautoryzowanym wyciekiem informacji na zewnątrz, jeżeli mimo dołożonych starań jakiemuś szkodnikowi udałoby się zagnieździć wewnątrz naszej sieci. Odpowiedzialny jest także za usługę NAT tłumaczącą adresy z nierutowalnej puli adresów wewnętrznych.

VPN (10)

Zapewne w większości dużych firm, a na pewno w każdej współpracującej z wieloma podmiotami zarówno komercyjnymi, jak i instytucjonalnymi, istnieje konieczność zestawienia nietypowych połączeń pomiędzy konkretnymi punktami naszej sieci a siedzibami tychże firm. Połączenia takie są zestawiane pomiędzy znanymi urządzeniami i zazwyczaj wymagają zdecydowanie innych uprawnień niż typowy ruch wychodzący. Wiąże się to z udostępnieniem pewnych standardowo zablokowanych protokołów i portów, z zabezpieczeniem przed podsłuchem z powodu przesyłania np. danych medycznych i np. z koniecznością umożliwienia traktowania naszego małego kawałka sieci jak fragmentu własnej sieci innego podmiotu często w lokalizacjach na innym kontynencie.

Połączenia takie są zazwyczaj zestawiane w celach serwisowych. Typowym przykładem są tutaj instalacje zaawansowanych systemów diagnostycznych np. tomografii komputerowej, rezonansu magnetycznego, radiologii cyfrowej, pracowni chemodynamicznej, systemów laboratoryjnych itd. Dzięki temu umożliwiamy zdalny dostęp służbom serwisowym opiekującym się daną aparaturą bezpośrednio z siedziby własnej firmy. Zmiana na nowszą wersję oprogramowania czy typowe prace diagnostyczne nie wymagają dzięki temu obecności osobistej pracowników serwisu, co zdecydowanie poprawia dostępność i jakość usług oraz oczywiście obniża koszty utrzymania takich systemów.

Obsługą takich łączy zajmują się OpenVPN i IP Sec. Tłumaczenie w jaki sposób są zestawiane poszczególne połączenia nie jest tutaj celowe z kilku powodów. Pierwszym i najważniejszym jest bezpieczeństwo tychże łączy a innym jest specyficzne traktowanie każdego z nich z osobna.

Ewidencja i zarządzanie zasobami informatycznymi GLPI (12)

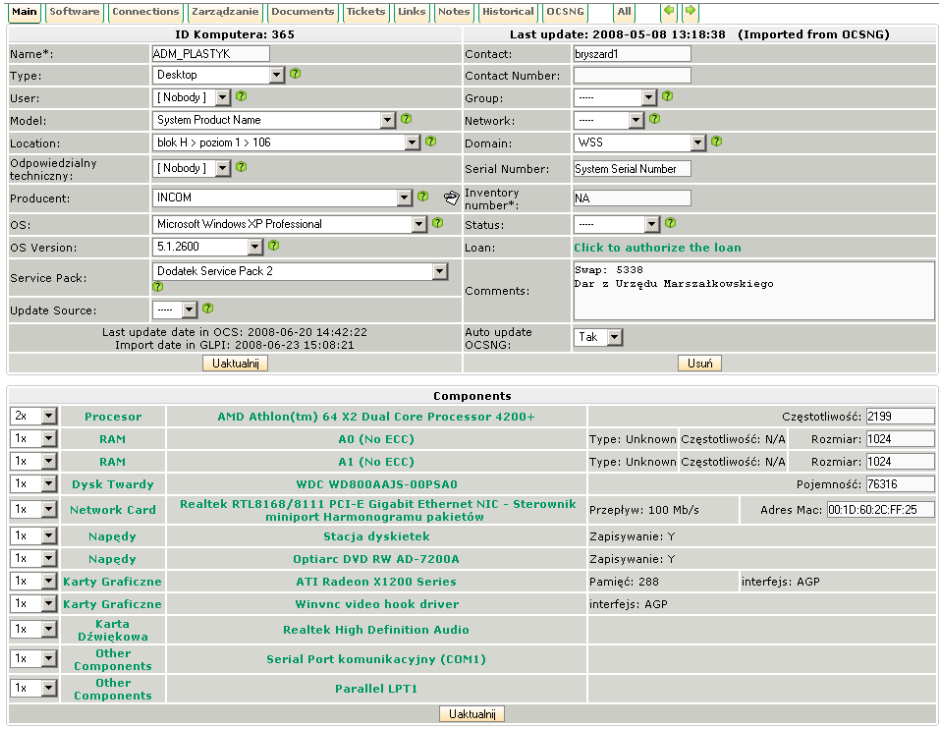
Ten fragment naszego systemu to po prostu potęga! Chyba najbardziej doceniana przez administratorów część naszej infrastruktury informatycznej. Ogromna, wręcz przepastna baza informacji na temat wszystkiego, co z komputerami ma jakikolwiek związek. Oczywiście każdy program, aby był użyteczny, najpierw musi być tymi informacjami napełniony. Z pomocą przychodzi nam tutaj OCS Inventory (15), dzięki któremu dane odnośnie konfiguracji sprzętowej i programowej działających w sieci komputerów są pobierane i zapisywane w sposób w pełni automatyczny. Oczywiście informacje o konfiguracji to dopiero początek, ale bardzo ważny i obszerny.

Żaden najmądrzejszy program nie wie w jakim pomieszczeniu, którego bloku jest umieszczony sprzęt, pod jakie gniazdo sieciowe jest podłączony, kto jest imiennie za niego odpowiedzialny itd. Ilość i rodzaj zapamiętywanych w programie danych jest przeogromna, ale przy tym są one ułożone w sposób logiczny, czytelny i prosty w obsłudze.

Najlepiej będzie skrócony opis funkcjonalności tej części systemu przeprowadzić na konkretnym przykładzie. Wyobraźmy sobie, że dostarczono nowy zestaw komputerowy i należy go zainstalować a następnie zewidencjonować. Sam proces instalacji oprogramowania na takim komputerze już jest warty sporej uwagi. Proszę sobie wyobrazić ile czasu trzeba by było poświęcić na zainstalowanie 10 komputerów, kiedy systemy operacyjne leżą w paczkach podobnie, jak cała reszta niezbędnego oprogramowania, a potem czeka nas jeszcze żmudne ustawianie sieci i konfigurowanie niektórych usług… Odpowiadam: proces takiej instalacji wraz z pobraniem najświeższych aktualizacji ze strony producenta może trwać dobrych kilkadziesiąt godzin skutecznie absorbując jedną osobą, która przy odrobinie wprawy w ciągu jednego dnia pracując jednocześnie na kilku komputerach, będzie w stanie przygotować 3 takie jednostki. A co zrobić jak są ich setki?! Proszę zauważyć, że 90% albo więcej komputerów ma dokładnie tą samą konfigurację programową. Różnią się na początku właściwie tylko numerem licencji systemu operacyjnego i pakietu biurowego (jeżeli jest komercyjny, bo przecież możemy korzystać z darmowego Open Office), nazwą i opisem sieciowym oraz, z punktu widzenia sieci, adresem IP i adresem sprzętowym MAC. Widać, że właściwie różne są tylko małe detale… A gdyby tak przygotować jakąś „matrycę" a potem tylko zmieniać te szczegóły? Ależ oczywiście, że można! Z pomocą przychodzą nam tutaj dwa narzędzia. Pierwszy to popularnie zwany SysPrep, czyli narzędzie Microsoft służące właśnie do przygotowywania ta-

kiej instalacji, w której raz definiujemy wszystkie wspólne parametry, a program instalacyjny zapyta nas potem wyłącznie o detale charakterystyczne dla danej jednostki, czyli właśnie np. numery licencji. Cała reszta zostanie automatycznie skonfigurowana. To jest zadanie pierwszego z narzędzi. Teraz potrzebny nam jest jeszcze sposób na zapis tak przygotowanej wersji instalacyjnej na docelowy dysk, do tego celu służy inne narzędzie tworzące obrazy dysków. Świat informatyczny pełen jest programów służących temu celowi. Jednym z najpopularniejszych jest oczywiście Norton Ghost, będący sztandarowym przedstawicielem. Jest to program komercyjny i płatny. Uważam, że zdecydowanie warty swojej niewielkiej ceny. Nic nie stoi jednak na przeszkodzie, aby wykorzystać jakikolwiek inny darmowy. Tak przygotowana procedura instalacyjna skraca czas przygotowania jednostek kilkunastokrotnie!! Jedna osoba przy minimalnej wprawie jest w stanie w ciągu dnia „wyprodukować" w ten sposób kilkadziesiąt jednostek! Instalacja więc 400 komputerów to zadanie dla dwóch osób na tydzień czasu. W typowy sposób trwało by to pewnie ponad 3 miesiące. W tym momencie każdemu czytającemu powinna się nasunąć jedyne właściwe w tej sytuacji spostrzeżenie. Takie postępowanie ma sens, jeżeli instalowane jednostki będą możliwie identyczne pod względem sprzętowym i programowym! Inaczej mówiąc zastanówmy się najpierw dwa razy jaki sprzęt i oprogramowanie jest nam potrzebne, a następnie trzymajmy się tych ustaleń możliwe najdłużej jak się da, czyli do momentu, kiedy producenci przestaną produkować wybrane przez nas modele! Dlatego planować z głową i na zapas. Jeżeli wybierzemy Dell Opti Plex 740 z Windows XP Professional PL, monitor LCD Dell 19" i drukarkę Hewlett Packard LaserJet 2015nw jako typowe, to niech się wali i pali, niech ten zestaw będzie droższy od innych za pół roku, ale kupujmy już tylko takie dokąd tylko będzie można!

Koniec dygresji instalacyjnej. Mamy skonfigurowany zestaw, podłączamy go do gniazda w docelowym pokoju, gdzie ma pracować i powracamy do GLPI. Mamy więc zainstalowany komputer podłączony do sieci w odpowiednim miejscu firmy. Dokonaliśmy stosownego wpisu w konfiguracji DHCP. Przy pierwszym uruchomieniu komputera zaczyna już działać agent OCS Inventory i przekazuje dane o konfiguracji do stosownej bazy. GLPI pobiera dane z owej bazy i zasila swoje czeluści stosownymi informacjami. Mamy już dostępny w systemie odpowiedni komputer. Teraz nadszedł czas na wypełnienie bazy dodatkowymi informacjami. I tak pojawiają się kolejno: numer inwentarzowy, wskazanie pomieszczenia (można definiować strukturę hierarchiczną), w którym zainstalowano jednostkę, numer telefonu, osoba odpowiedzialna, numer gniazda sieciowego (także hierarchiczna struktura, oczywiście połączona z konfiguracją naszych urządzeń sieciowych z dokładnością do portu konkretnego urządzenia!) itd.

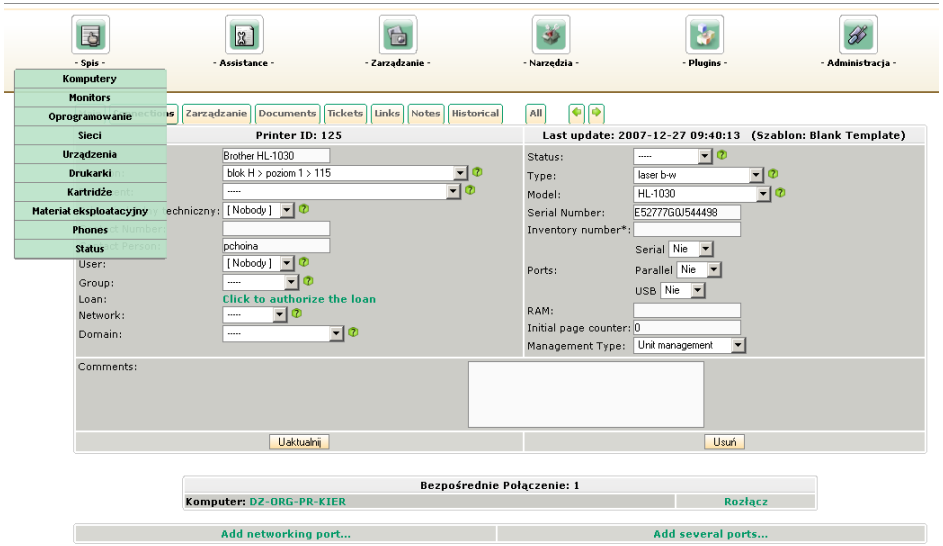


Rysunek 21. Powyższy rysunek pokazuje kartę jednego komputera wypełnioną automatycznie danymi o konfiguracji sprzętowej i programowej oraz z dodatkowymi informacjami dotyczącymi np. lokalizacji i pochodzenia danej jednostki. Proszę zwrócić uwagę na ilość zakładek w górnej części ekranu! Tam kryje się dodatkowy ogrom możliwości.

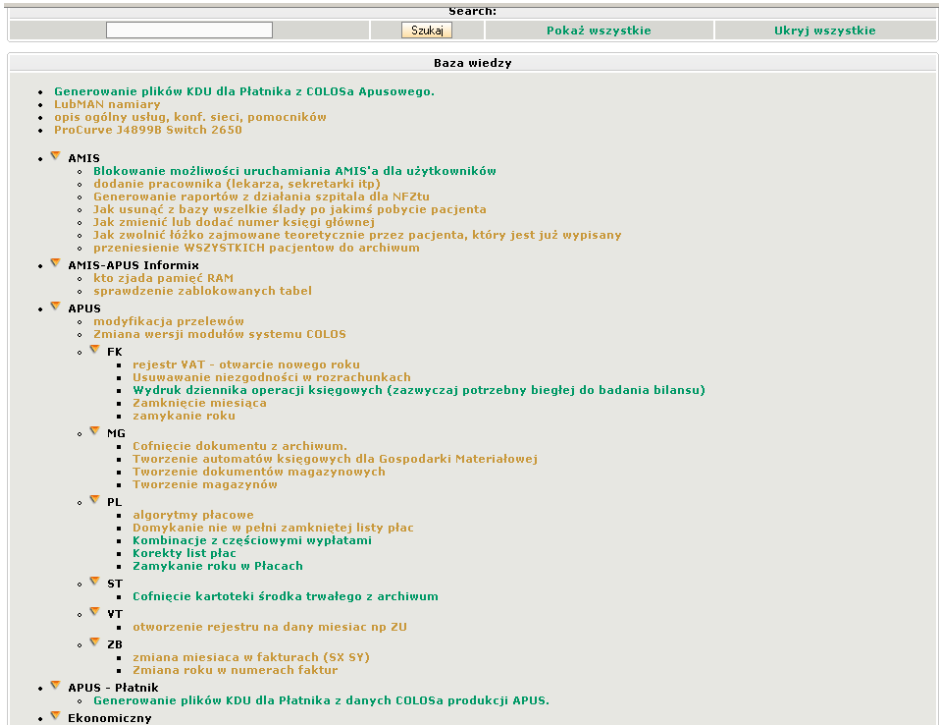
Teraz trzeba sobie uświadomić, że inne urządzenia współpracujące w całej infrastrukturze informatycznej mają również swoją reprezentację w tej bazie! Oczywiście z uwzględnieniem informacji przeznaczonych dla danego typu urządzenia, nikt przecież nie będzie oczekiwał od drukarki numeru licencji systemu operacyjnego. Tak więc drukarki, monitory, skanery, UPSy, koncentratory i przełączniki sieciowe również są opisane w tej bazie. Trzeba oczywiście logicznie połączyć te urządzenia ze sobą. Opisując zestaw komputerowy możemy dołączyć do niego już istniejącą w systemie drukarkę i wskazać, że w tym przypadku jest ona połączona z komputerem za pośrednictwem interfejsu USB 2.0. Następnie wskazujemy, że interfejs sieciowy nr 1 komputera jest połączony z gniazdem sieciowym nr 1H23.2. W definicji tegoż gniazda znajdziemy dalej, że jest ono połączone z gniazdem 46 panelu nr 2, III szafy krosowniczej na poddaszu bloku C. Gniazdo tego panelu skrosowane jest do portu 18 przełącznika HP ProCurve

o numerze… itd. itd. W ten sposób w odpowiednio logicznie poukładaną i połączoną strukturę wpisane jest każde urządzenie. Oczywiście system pozwala prześledzić od dowolnego miejsca każdy element.

GLPI ponadto pozwala na zapisywanie przy każdym urządzeniu dodatkowych informacji w postaci plików i linków. Zapamiętuje zdarzenia, jakie miały miejsce dla tego elementu, takie jak instalację kolejnej poprawki systemu czy jakiegoś oprogramowania, dodanie dodatkowego dysku twardego czy wymiana pamięci RAM. Oczywiście historia tych zdarzeń jest dostępna na żądanie. Każde urządzenie, zwłaszcza tak skomplikowane jak sprzęt komputerowy, może się kiedyś zepsuć. Czasami jest to rzeczywiste uszkodzenie jakiegoś podzespołu, a czasami tylko brak odpowiedniej wiedzy użytkownika go obsługującego. Jaka by jednak nie była przyczyna tegoż zdarzenia, może ono zostać odnotowane w systemie w celach dalszej analizy i rozliczeń.

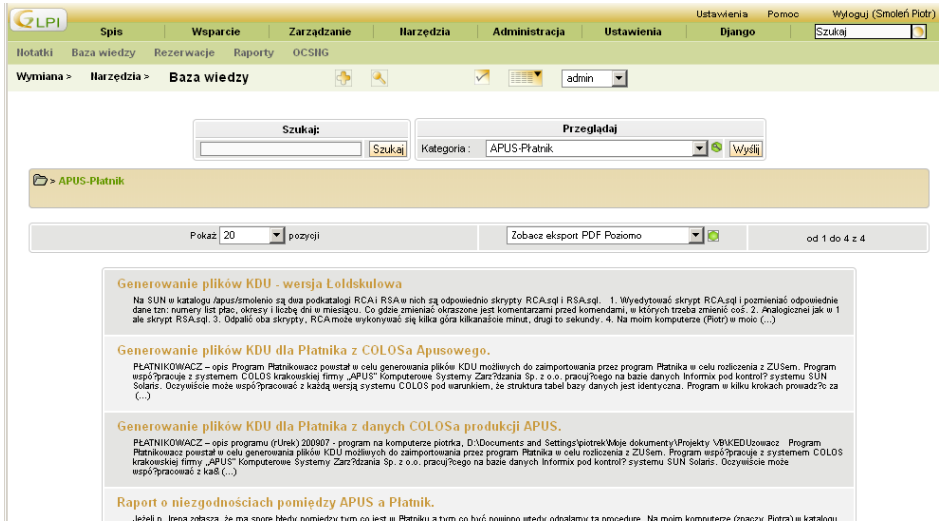


Rysunek 22. Na powyższym rysunku widnieje karta drukarki z wybraną zakładką „Connections” pokazującą (w dolnej części) do jakiego komputera jest ona podłączona. Oczywiście nazwa tego komputera jest linkiem, który pokieruje nas dalej. Proszę zwrócić uwagę, na rozwinięte menu kontekstowe. Tak to nie pomyłka! W systemie można zarządzać także materiałami eksploatacyjnymi wszelkich urządzeń. Kwestia tylko chęci, gdyż oczywiście system będzie tak użyteczny, jak wpisane do niego informacje.



Rysunek 23.

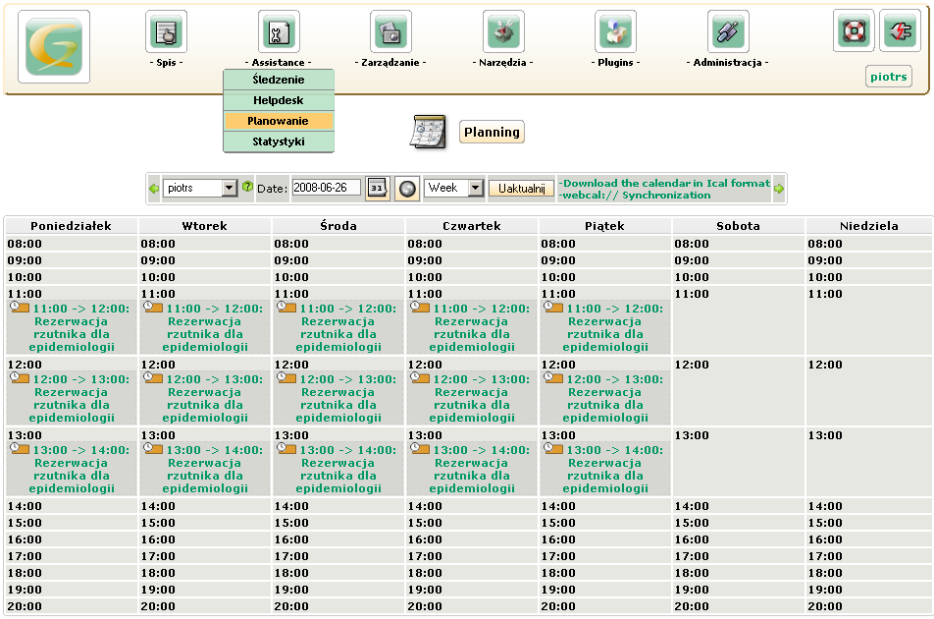
Oczywiście GLPI to nie tylko informacje o sprzęcie i sieci informatycznej czy telefonicznej. To także baza dokumentów, kontaktów i informacji o firmach, które mają (choć nie koniecznie) związek z infrastrukturą teleinformatyczną firmy. GLPI to także możliwość przechowywania informacji, czyli tzw. baza wiedzy. Są takie czynności, które wykonuje się bardzo rzadko, ale są niezmiernie istotne. Ot dla przykładu z powodu awarii zasilania został zapisany niepełny dokument w bazie powiedzmy systemu księgowego (systemy nietransakcyjne nadal funkcjonują). Każdy administrator dobrze wie, że wiedza „jak to odkręcić” jest bardzo ważna. Każdy ją gdzieś odnotowuje, a przynajmniej powinien. W typowych sytuacjach takie zdarzenie natychmiast generuje kontakt z firmą, która jest autorem naszego systemu. Odpowiedni fachowiec nie jest akurat dostępny pod telefonem, księgowa się denerwuje a nam rośnie w tej firmie „wskaźnik uciążliwego klienta” i co najgorsze tracimy czas. Odpowiedzią na ten problem jest właśnie baza wiedzy, która jak i większość innych elementów może być hierarchiczna.



Rysunek 24. Tak wygląda baza wiedzy systemu GLPI. W zhierarchizowany przez nas sposób przechowywane są wszelkie informacje o nietypowych czy typowych akcjach na jakieś zdarzenia. Baza żyje, rozrasta się. Nieobecność jakiegoś pracownika działu IT nie powoduje paraliżu firmy. Wyobraźmy sobie taką bazę wypełnioną np. informacją o tym, jak postępować z codziennymi dokumentami i jak przeprowadzać archiwizację i odtwarzanie systemu… Toż to tylko dopisać z przodu „Procedury dla systemu zarządzania jakością ISO" i szybko prosić o certyfikację!

GLPI to także możliwość zarządzania czasem. Bez problemu możemy zaplanować sobie czas, co, gdzie i kiedy należy zrobić. Istnieje także możliwość rezerwacji np. godzin zajęcia sali szkoleniowej czy rzutnika multimedialnego.

Teraz proszę sobie wyobrazić, że przedstawiona w tym opracowaniu funkcjonalność to tylko fragment możliwości, że te wszystkie informacje mogą być podstawą dla wszelkiego typu raportów. Tak wiem, ciężko to sobie wyobrazić. Ilość i jakość (w pozytywnym znaczeniu) danych skutecznie nam utrudnia takie wyobrażanie. Ponieważ wszystkie te informacje są przechowywane w bazie danych, podobnie jak większość informacji z systemów produkcyjnych i rozliczeniowych, nic nie stoi na przeszkodzie, aby szczegółowe dane o urządzeniach czy zdarzeniach były automatycznie przenoszone czy choćby powiązane z bazą danych ot chociażby środków trwałych. W szpitalu, w którym mam przyjemność pracować, panie z księgowości inwentarzowej GLPI używają jak własnej „efki" i wręcz potrafią zwracać uwagę na jakieś braki czy dopominać się dopisania „czegoś", żeby „coś" było możliwe do uzyskania automatycznie.



Rysunek 25. Tak wygląda panel planowania, wykorzystywany przez nas do rezerwowania np. sali szkoleniowej czy rzutnika multimedialnego.

Oczywiście system GLPI współpracuje z innymi elementami całego naszego Intranetu, oczywiście korzysta z kont użytkowników przechowywanych w bazie LDAP i oczywiście jest systemem Open Source, i darmowym!!

Serwer www (13)

Ciśnie się na usta tutaj słynny cytat z encyklopedycznej definicji konia. Do czego służy serwer www chyba już dzisiaj nie trzeba nikomu tłumaczyć, a na pewno nikomu kto pracuje w dziale IT. W naszym przypadku mamy także typowego i chyba najpopularniejszego przedstawiciela z tego gatunku, czyli Apache.

Jak pewnie czytelnicy zauważyli już z samego schematu systemu, a także wyczytali (i wyczytają w dalszej części), większość elementów naszej układanki ma swój interfejs wykorzystujący strony www. Obecność zatem usługi www stała się koniecznością, nawet gdyby pominąć ustawowe obowiązki prezentowania w Internecie takiego tworu, jakim jest szpital. To, co warto w tym miejscu powiedzieć, to że o ile wolność oprogramowania użytego w naszym rozwiązaniu cieszy, o tyle wprowadza także trochę chaosu, gdyż ciężko znaleźć dwa identyczne środowiska potrzebne do pracy każdej części naszej układanki z osobna. Mamy zatem

nasz serwer www z zainstalowanymi modułami wszelkiej maści. Mam tutaj na myśli obsługę języków skryptowych takich jak Perl, PHP czy Python.

Serwery baz danych MySQL i PostgreSQL (14)

Serwery baz danych w systemie WINBOSS stanowią pomocniczy element całości. Służą one do przechowywania danych dla innych części. Same w sobie nie odgrywają żadnych autonomicznych funkcji. Niemniej jednak stanowią bardzo istotną część, bez której elementy takie jak GLPI (12), OCS Inventory (15), OWL (18), Joomla (19) i Bacula (17) po prostu by nie działały.

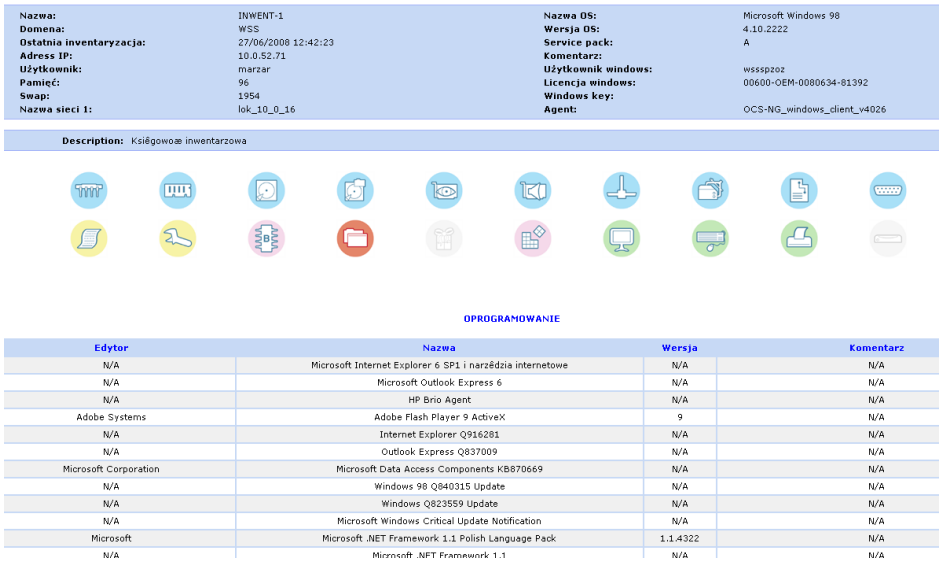
Na serwerach tych ponadto kreowane są bazy służące do realizacji zadań jednorazowych typu wykonanie skomplikowanych zestawień, niemożliwych do uzyskania w prosty sposób i w rozsądnym czasie za pomocy arkuszy kalkulacyjnych.

Obecnie trwają ponadto prace nad zapisywaniem do bazy wszelkich informacji, które w tej wersji systemu są przechowywane w plikach logów serwerów, na których działają poszczególne usługi. Takie podejście uprości i wzbogaci możliwości raportowania. Ponadto planowane jest dołączenie dynamiczne danych o tychże zdarzeniach do procesu logowania się na stacjach przez poszczególnych użytkowników. Będzie możliwe wtedy prewencyjne generowanie ostrzeżeń i komunikatów. Każdy użytkownik dwa razy się zastanowi nad tym, czy szukać czegoś niepotrzebnego do pracy w Internecie, jeżeli podczas logowania otrzyma komunikat o treści *Czy wiesz, że w ciągu ostatniego miesiąca wydrukowałeś 2376 stron i spędziłeś w Internecie średnio 3,5 godziny dziennie, a Twój program do obsługi pacjentów był aktywny średnio 1,2 godziny dziennie!?*

Automatyczna inwentaryzacja sprzętu komputerowego i oprogramowania OCS Inventory (15)

Usługa ta jest odpowiedzialna za automatyczne zbieranie informacji o konfiguracji sprzętowej i programowej każdego komputera, który pracuje wewnątrz naszej sieci. Działanie usługi, z punktu widzenia użytkownika, jest całkowicie niewidoczne. Od użytkowników nie jest wymagana jakakolwiek praca w częściach oprogramowania stanowiących tę usługę. Zainstalowane raz oprogramowanie nie wymaga jakiegokolwiek nakładu pracy ze strony stacji roboczych. Odpowiednio dociekliwy użytkownik może co najwyżej zauważyć w liście zainstalowanego oprogramowania klienta naszego systemu, oczywiście pod warunkiem, że będzie miał stosowne do tego uprawnienia.

Poprawnie działająca usługa w sposób w pełni automatyczny pobiera wszelkie informacje o konfiguracji sprzętowej stacji roboczej, na której został uruchomiony agent i przekazuje do serwera, który z kolei zapisuje odpowiednie informacje do bazy danych (14). Baza ta stanowi podstawę do prezentacji wyników pracy za pomocą interfejsu webowego na serwerze www (13). Informacje oczywiście przekazywane są automatycznie i także automatycznie co pewien czas są odświeżane, tak że system przechowuje te najbardziej aktualne. Oczywiście, jeżeli zajdzie taka potrzeba, można wymusić aktualizację danych na konkretną chwilę.



Nazwa:	INWENT-1	**Nazwa OS:**	Microsoft Windows 98
Domena:	WSS	**Wersja OS:**	4.10.2222
Ostatnia inwentaryzacja:	27/06/2008 12:42:23	**Service pack:**	A
Adress IP:	10.0.52.71	**Komentarz:**	
Użytkownik:	marzar	**Użytkownik windows:**	wssspzoz
Pamięć:	96	**Licencja windows:**	00600-OEM-0080634-81392
Swap:	1954	**Windows key:**	
Nazwa sieci 1:	lok_10_0_16	**Agent:**	OCS-NG_windows_client_v4026

Description: Księgowoæ inwentarzowa

OPROGRAMOWANIE

Edytor	Nazwa	Wersja	Komentarz
N/A	Microsoft Internet Explorer 6 SP1 i narzędzia internetowe	N/A	N/A
N/A	Microsoft Outlook Express 6	N/A	N/A
N/A	HP Brio Agent	N/A	N/A
Adobe Systems	Adobe Flash Player 9 ActiveX	9	N/A
N/A	Internet Explorer Q916281	N/A	N/A
N/A	Outlook Express Q837009	N/A	N/A
Microsoft Corporation	Microsoft Data Access Components KB870669	N/A	N/A
N/A	Windows 98 Q840315 Update	N/A	N/A
N/A	Windows Q823559 Update	N/A	N/A
N/A	Microsoft Windows Critical Update Notification	N/A	N/A
Microsoft	Microsoft .NET Framework 1.1 Polish Language Pack	1.1.4322	N/A
N/A	Microsoft .NET Framework 1.1	N/A	N/A

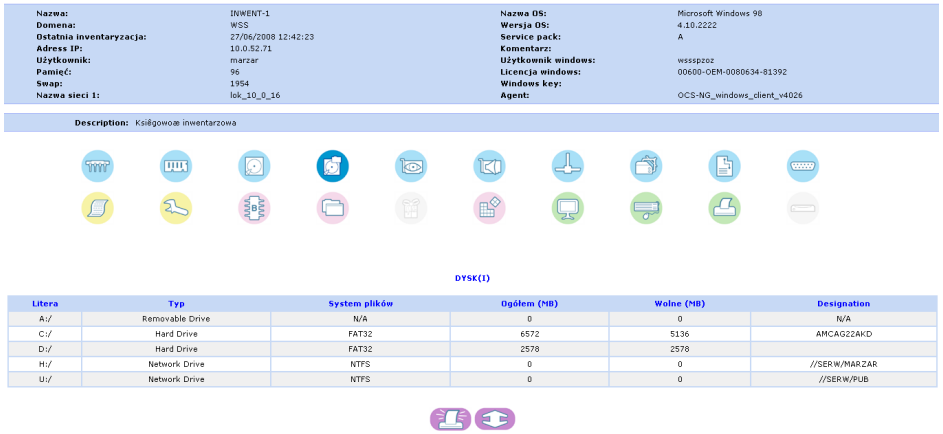
Rysunek 26. Powyższy rysunek przedstawia ekran z przeglądarki internetowej pokazujący fragment z informacjami na temat zainstalowanego oprogramowania.

System kolekcjonuje dane o wszelkich podzespołach zainstalowanych w komputerze czy to jako autonomiczne urządzenia, czy to jako części wchodzące w skład większego elementu, tak jak chipset na płycie głównej. Ponadto rozpoznaje wszelkie peryferia podłączone do komputera. Dane dotyczą nie tylko samego typu urządzenia, ale i jego wersji, numeru seryjnego, wersji BIOS i innych specyficznych dla danego typu urządzenia, jak np. to czy pamięć jest z korekcją błędów czy też nie (ECC). Podobnie sprawa ma się z oprogramowaniem zain-

stalowanym na stacji. Oprócz nazwy programu, producenta i wersji mamy także informację o kluczu instalacyjnym. Oczywiście jako oprogramowanie nie mam tutaj na myśli wyłącznie całych pakietów, ale ich składników czy wręcz bibliotek i każdej z osobna aktualizacji zarówno systemu, jak też jakiegoś pakietu!

Informacje kolekcjonowane i przechowywane w tym systemie mogą posłużyć do generowania raportów. Jednak informacje te są podstawą do pracy dla systemu Ewidencji i zarządzania zasobami informatycznymi GLPI (12). Wzbogacone o dodatkowe dane odnośnie infrastruktury sieciowej,położenia wewnątrz pomieszczeń, numerów telefonów itd. stanowią środowisko dalszej pracy. O tym jednak traktuje wcześniejszy fragment opracowania.

Informacje przechowywane w obu częściach systemu są, w powiązaniu z numerem inwentarzowym, doskonałym uzupełnieniem informacji dla księgowości inwentarzowej. W naszej jednostce panie pracujące w tym dziale na bieżąco korzystają z dobrodziejstw OCS Inventory i GLPI. Ba, przyzwyczajone do zakresu informacji zaczęły traktować te systemy jako integralne części systemu FK.



Rysunek 27. Powyższy rysunek pokazuje fragment informacji o sprzęcie – w tym wypadku dyskach twardych wraz z ich podziałem na partycje i rodzajem systemu plików użytych do każdej partycji z osobna.

Informacje o konfiguracji programowej stanowią podstawę do jednej z bardziej przydatnych w dużych sieciach funkcji. Mianowicie na tej podstawie jest możliwe sprawdzanie konfiguracji programowej i podejmowanie stosownych działań polegających na instalowaniu lub odinstalowaniu stosownego oprogramowania. Przy czym proces instalacji może przebiegać całkowicie automatycznie (np. dla kolejnej poprawki systemu Windows) i jest przeprowadzony w odpowiedni sposób zapobiegający przeciążeniu systemu (jako całej infrastruktury) i sieci. Mianowicie instalacje na kolejnych stacjach będą uruchamiane z zachowaniem odstępów czasowych (np. 5-minutowych) eliminując nagłą 100% utylizację sieci. Ponadto instalacja takich składników może przebiegać całkowicie niewidocznie dla użytkownika pracującego akurat na stacji. Po jej zakończeniu użytkownik, jeżeli będzie to konieczne, zostanie poinformowany o konieczności restartu systemu. Jeżeli nie chce posłuchać i na to znajdzie się sposób bez konieczności wycieczek dla administratorów.

Serwer monitorujący dostępność usług i hostów Zabbix (16)

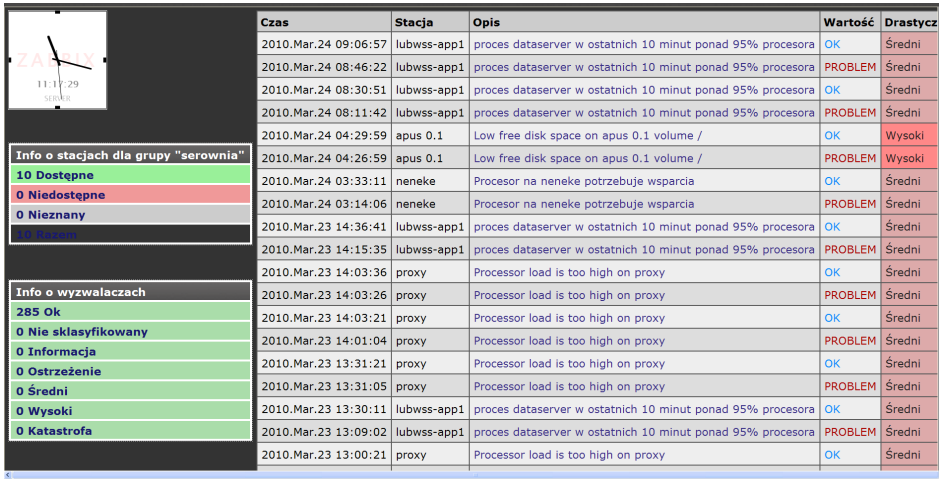
Można śmiało powiedzieć, że to jest bardzo silna strona naszej układanki. Uruchomienie takiej usługi polecam wszędzie, gdzie pracuje więcej niż kilka komputerów, i gdzie cała infrastruktura IT nie mieści się w jednym pomieszczeniu zwanym pokojem informatyka.

Wiedza to potęga. Informacje na temat tego, co się dzieje są bezcenne. Odpowiednio szybkie informowanie o zdarzeniach jest podstawą zapobiegania problemów czy ich sprawnego rozwiązywania. Śmiało tutaj można porównać działanie tego kawałka systemu do działania służb wywiadowczych dbających o bezpieczeństwo państwa. Potrzebna jest centrala koordynująca i siatka wywiadowców oraz rzecznik prasowy informujący w przejrzysty sposób o wszelkich nietypowych wydarzeniach, jakie ostatnio miały miejsce. Potrzebne jest także archiwum, w którym będą przechowywane wszelkie informacje, tak aby była możliwa ich późniejsza analiza.

Centralę usługi stanowi tutaj odpowiednio skonfigurowany serwer. Siatka wywiadowców reprezentowana jest przez odpowiednie programy klienckie zainstalowane na maszynach, których praca jest monitorowana. Oprogramowanie takie jest oczywiście zainstalowane jako usługa działająca w tle w sposób całkowicie niewidoczny dla użytkownika. Klient sam w sobie ma możliwości zbierania typowych danych. Ma także, co bardzo ważne, mechanizm pozyskiwania informacji nie przewidzianych w jego standardzie. Załóżmy, że chcemy mieć informacje, jaki w danym momencie program jest aktywny na stacji roboczej. Czy jest to nasz program produkcyjny służący pracy czy może jednak nie…może to jest np. przeglądarka internetowa. Ponieważ klient Zabbiksa zdecydowanie lubi wyniki w postaci cyferek, więc piszemy skrypt czy jakiś programik w dowolnym języku pracujący wsadowo. W wyniku działania takiego skryptu czy programu powinniśmy otrzymać liczbę, np. „0” będzie oznaczało, że nasz system produkcyjny jest oknem nieaktywnym na stacji, a „1”, że jak najbardziej aktywnym. Albo

inny przykład. Na stacjach roboczych chcemy sprawdzać ile miejsca na dysku zajmują katalogi z profilami użytkowników. Piszemy nawet prostą baczówkę zwracającą ilość zajmowanego miejsca przez zadany katalog. W programie klienckim Zabbiksa definiujemy, że, aby uzyskać taki parametr, musi uruchomić tą baczówkę systematycznie co, powiedzmy, 2 godziny. Klient oczywiście z cierpliwością kamienia będzie wykonywał zlecone zadanie i przekazywał w odpowiedni sposób do serwera. Serwer taką informację zapisze w bazie danych i ewentualnie podejmie jakąś akcję np. wyśle email czy sms do administratora z odpowiednim komunikatem.

Oczywiście sam serwer potrafi za pomocą odpowiednich reguł sprawdzać dostępność niektórych elementów, dla których z założenia nie istnieje możliwość instalacji odpowiedniego agenta. Ot chociażby urządzenia sieciowe czy drukarki. Serwer w takim przypadku wysyła odpowiednie pakiety i czeka na odpowiedź, na której podstawie (lub jej braku) podejmie decyzję czy wszystko jest jak należy, czy może jednak czas larum podnieść.



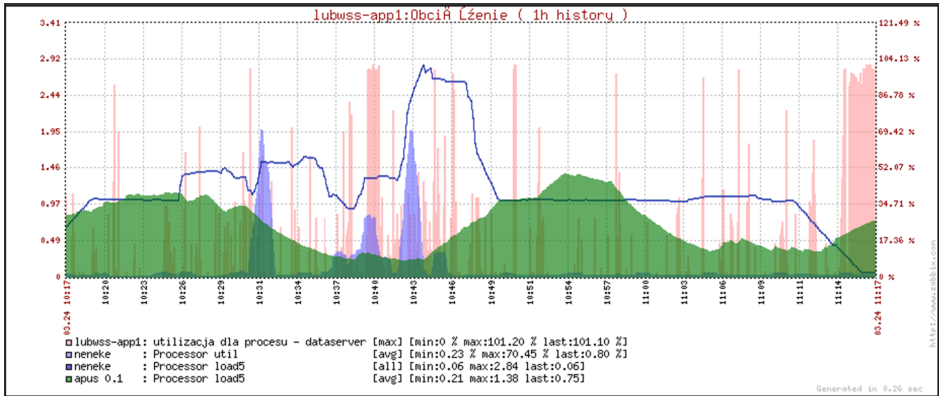
Info o stacjach dla grupy "serownia"
10 Dostępne
0 Niedostępne
0 Nieznany
10 Razem

Info o wyzwalaczach
285 Ok
0 Nie sklasyfikowany
0 Informacja
0 Ostrzeżenie
0 Średni
0 Wysoki
0 Katastrofa

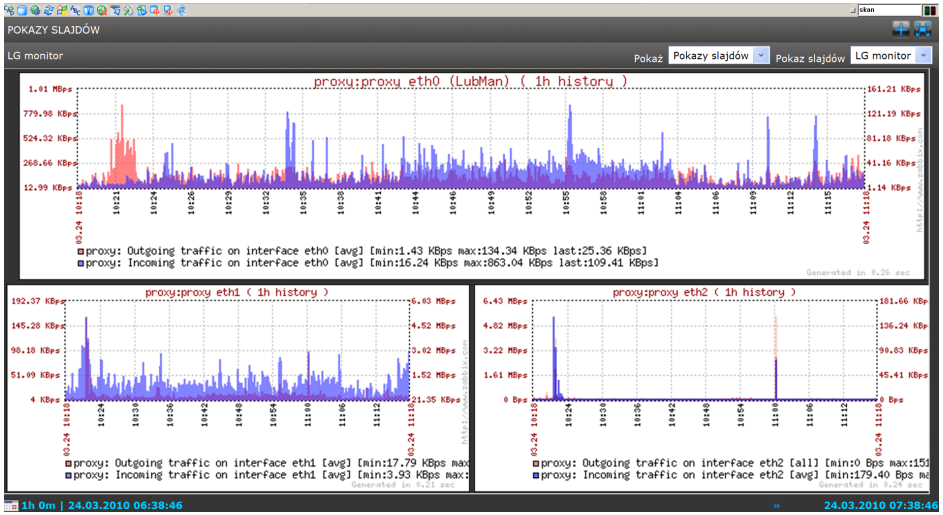
Czas	Stacja	Opis	Wartość	Drastycz
2010.Mar.24 09:06:57	lubwss-app1	proces dataserver w ostatnich 10 minut ponad 95% procesora	OK	Średni
2010.Mar.24 08:46:22	lubwss-app1	proces dataserver w ostatnich 10 minut ponad 95% procesora	PROBLEM	Średni
2010.Mar.24 08:30:51	lubwss-app1	proces dataserver w ostatnich 10 minut ponad 95% procesora	OK	Średni
2010.Mar.24 08:11:42	lubwss-app1	proces dataserver w ostatnich 10 minut ponad 95% procesora	PROBLEM	Średni
2010.Mar.24 04:29:59	apus 0.1	Low free disk space on apus 0.1 volume /	OK	Wysoki
2010.Mar.24 04:26:59	apus 0.1	Low free disk space on apus 0.1 volume /	PROBLEM	Wysoki
2010.Mar.24 03:33:11	neneke	Procesor na neneke potrzebuje wsparcia	OK	Średni
2010.Mar.24 03:14:06	neneke	Procesor na neneke potrzebuje wsparcia	PROBLEM	Średni
2010.Mar.23 14:36:41	lubwss-app1	proces dataserver w ostatnich 10 minut ponad 95% procesora	OK	Średni
2010.Mar.23 14:15:35	lubwss-app1	proces dataserver w ostatnich 10 minut ponad 95% procesora	PROBLEM	Średni
2010.Mar.23 14:03:36	proxy	Processor load is too high on proxy	OK	Średni
2010.Mar.23 14:03:26	proxy	Processor load is too high on proxy	PROBLEM	Średni
2010.Mar.23 14:03:21	proxy	Processor load is too high on proxy	OK	Średni
2010.Mar.23 14:01:04	proxy	Processor load is too high on proxy	PROBLEM	Średni
2010.Mar.23 13:31:21	proxy	Processor load is too high on proxy	OK	Średni
2010.Mar.23 13:31:05	proxy	Processor load is too high on proxy	PROBLEM	Średni
2010.Mar.23 13:30:11	lubwss-app1	proces dataserver w ostatnich 10 minut ponad 95% procesora	OK	Średni
2010.Mar.23 13:09:02	lubwss-app1	proces dataserver w ostatnich 10 minut ponad 95% procesora	PROBLEM	Średni
2010.Mar.23 13:00:21	proxy	Processor load is too high on proxy	OK	Średni

Rysunek 28. Zbiorczy slajd pokazujący najświeższe informacje o stanie systemu. Widoczne są zarówno zgłoszenia niepokojących zdarzeń, jak również odwołania alarmów. Po lewej stronie widoczne jest zbiorcze zestawienie informacji o zgłoszeniach. Aaaa…„serwerownia” to za długie słowo, więc skróciliśmy…

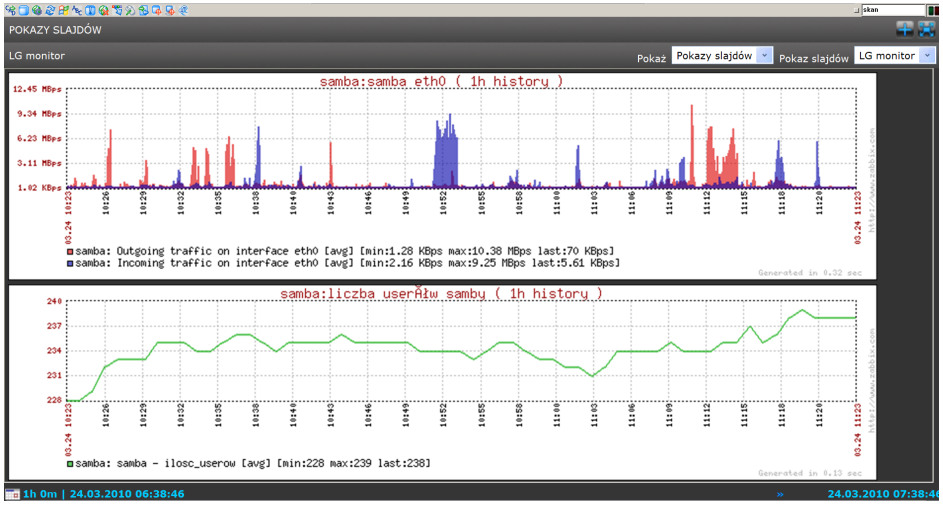
W naszym przypadku stosujemy trzy rodzaje powiadomień o stanie systemu. Po pierwsze: informacje są przekazywane jako wiadomości email na konto grupy informatyków. Po drugie: na jednej z linuksowych stacji roboczych w naszym pokoju jest zainstalowany syntetyzer mowy i w przypadku ważnych informacji wiadomość jest po prostu odczytywana na głos przez automat. To jest właśnie enigmatyczna Krystyna ze schematu naszego systemu. Dlaczego Krystyna? A pamiętacie reklamę z gazownią? Właśnie… stąd ta nazwa, choć obecnie głos raczej przypomina szpiega ukradkiem na ucho przekazującego informacje zaufanej osobie. Trzecim i najbardziej czytelnym i jednocześnie widowiskowym sposobem jest graficzna prezentacja na wielkim 42” monitorze wiszącym w centralnym miejscu naszego działu. Na jego ekranie w postaci odpowiednich tabel i wykresów prezentowane mamy dane o kluczowych parametrach.



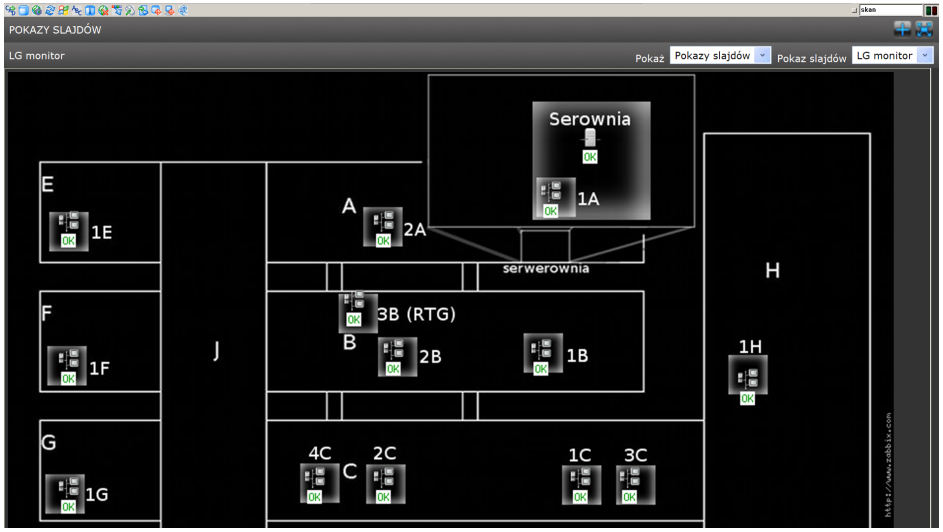
Rysunek 29. A tutaj widoczne są wykresy przedstawiające na przestrzeni czasu wykorzystanie wybranych serwerów czy wręcz procesów



Rysunek 30. Tutaj dla odmiany graficzna prezentacja obciążenia wybranych interfejsów sieciowych



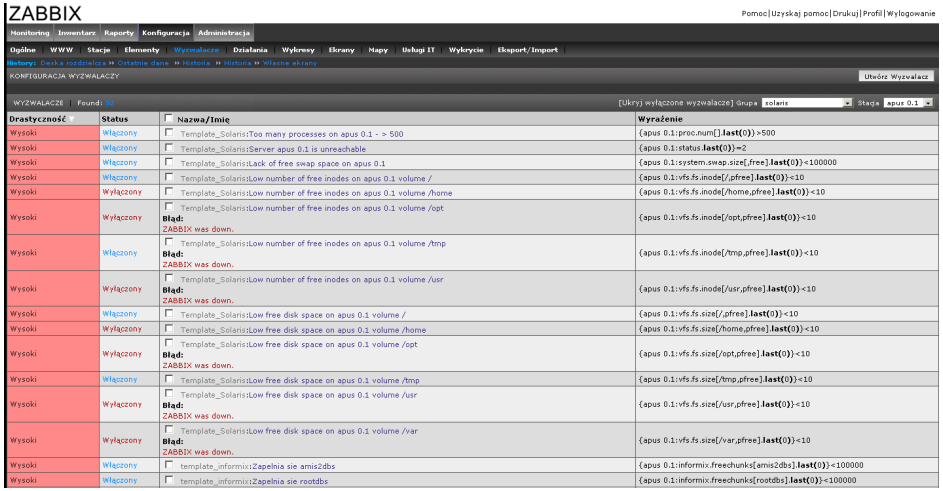
Rysunek 31. Ten slajd pokazuje ruch na interfejsie sieciowym serwera Samby oraz ilość zalogowanych użytkowników. Ta ilość nie jest jeszcze przerażająca. Bywa prawie dwukrotnie wyższa.



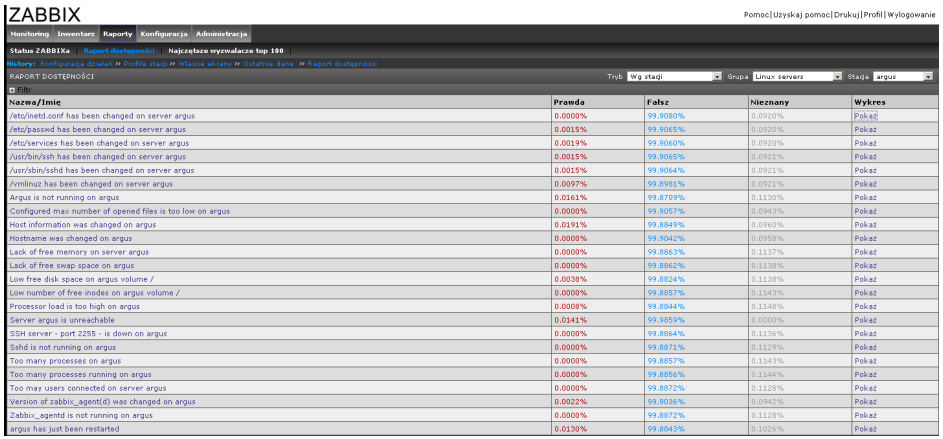
Rysunek 32. Tutaj poglądowy obrazek ze stanem całego systemu. Żeby uzmysłowić sobie skalę, proszę sobie wyobrazić, że ten obrazek w rzeczywistości to jakieś 300 metrów długości i ponad 100 szerokości. Osi Z nie widać, ale też posiada zacne około 40 metrów. Z naszego pokoju w bloku H na ginekologię w bloku E i z powrotem jest około 1 km idąc cały czas korytarzami! Zielone napisy *OK* mówią, że wszystko w danym punkcie jest w porządku. W przypadku pojawienia się jakiegoś alarmu w oczy kłuć będzie czerwień i stosowny napis.

Znając rozmiary naszej placówki rozumiecie zapewne jak bardzo istotne jest takie monitorowanie stanu. Bez takiego rozwiązania po prostu nogi bolą.

Powyższe rysunki przedstawiają graficzne informacje przedstawiane w postaci zapętlonej sekwencji slajdów na naszym wielkim monitorze. Oczywiście pokazują wybrane przez nas do takiej prezentacji parametry. Nic nie stoi jednak na przeszkodzie, aby korzystając z webowego interfejsu Zabbiksa, dobrać się do przepastnej ilości wszelkich danych.



Rysunek 33.



Rysunek 34. Powyżej dwa rysunki przedstawiają ogólne bogactwo konfiguracji Zabbiksa

Oczywiście Zabbix to nie tylko monitorowanie. To także możliwość automatycznego warunkowego podjęcia jakiejś akcji. Może to być np. restart jakiejś usługi przed uprzednim przywróceniem „na wszelki wypadek" właściwych plików konfigurujących daną usługę.

Całość składa się na nieprawdopodobnie użyteczne narzędzie, dzięki któremu 4 ludzi jest w stanie obsłużyć i administrować taką Hydrę.

Serwer backupowy Bacula (17)

Najbardziej niezawodny sprzęt i najlepsi administratorzy nie gwarantują nigdy, że nie wystąpi żadna awaria czy złośliwe działanie sfrustrowanego wykolejeńca. Nikt nam nie zagwarantuje, że piorun nie uderzy w nasz budynek a jak uderzy, że instalacja odgromowa zadziała. Podstawowym działaniem każdego szanującego się administratora jest przewidywanie scenariusza, kiedy wszystkie zabezpieczenia zawodzą i trzeba startować od zera. Trzeba zabawić się wtedy w czarnowidza i metodą Kubusia fatalisty przewidywać nieprzewidywalne. Ostatnią deską ratunku jest przywrócenie do życia systemu z kopii zapasowych na nowym sprzęcie, gdyż poprzedni się spalił lub został skradziony.

Żeby było to w ogóle możliwe, trzeba wykonywać kopie zapasowe. O konieczności takiej nikogo nie muszę przekonywać. Dyrektorzy, którzy nie rozumieją nakładów, jakie trzeba ponieść na takie zadanie, przekonają się o swoim błędzie wcześniej czy później. W takich sytuacjach ważne jest, aby dział IT jednak, mimo grymasu dyrekcji, systematycznie sporządzał odpowiednie notatki służbowe. Wróćmy jednak z dygresji do tematu. Aby kopie zapasowe miały jakąkolwiek wartość, musi być spełnionych kilka warunków:

1. kopie muszą być wykonywane;
2. kopie muszą być wykonywane na tyle często, aby dane na nich zawarte miały jakąś wartość i aby z powodu awarii systemu utracić maksymalnie tylko kilka ostatnich sprzed awarii godzin. Czasami, np. w przypadku systemów medycznych, wymagane są to nie godziny a minuty;
3. kopie muszą być weryfikowane, czyli co jakiś czas systematycznie należy wykonać próbną procedurę przywracania systemu z kopii wraz z oceną jakości przywróconego systemu. Dyrekcja MUSI tutaj zrozumieć, że czasami ten „nieużywany" komputer za 15 tys. zł to jest nasza polisa i gwarancja być albo nie być w wypadku awarii;
4. kopie muszą być składowane w innym pomieszczeniu niż zabezpieczane systemy. Jak najdalej od niego;
5. muszą istnieć jasne, czytelne dla laika i pisemne (!) procedury przywracania z kopii poszczególnych części systemu. Procedury te, podobnie jak kopie, muszą być przechowywane w odpowiednio odległych i zabezpieczonych miejscach;
6. nośniki służące do przechowywania kopii zapasowych nie są wieczne i muszą być systematycznie wymieniane – w bankach stosuje się zasadę jednokrotnego użycia taśm do streamerów i nie ma, że kosztuje;
7. oprócz kopii musi istnieć także archiwum, dzięki któremu będziemy w stanie dotrzeć do poprzedniej wersji jakiegoś dokumentu sprzed 3 miesięcy;
8. należy także pamiętać, że kopia bezpieczeństwa może także ulec uszkodze-

niu, podobnie jak urządzenie do jego wykonywania i odpowiednio się na tą intencję przygotować.

Raz opracowana i przetestowana procedura jest następnie żmudnie do znudzenia powtarzana dzień po dniu. Tak się nieszczęśliwie składa, że najlepszy czas na wykonywanie kopii zapasowej jest także najlepszym czasem na spanie i/lub weekendowe wyluzowanie się. Naturalne zatem jest, że można by go zlecić jakiejś bezdusznej i cierpliwej maszynie robiącej to za nas automatycznie w czasie naszego snu. Tutaj z pomocą przychodzi nam system Bacula. I znowu mamy do czynienia z odpowiednio skonfigurowanym serwerem i agentami zainstalowanymi na wybranych serwerach.

Sam system posiada szereg programów klienckich możliwych do zainstalowania w strategicznych miejscach systemu. Agenci tacy radzą sobie z nietypowymi zadaniami, takimi jak bieżące archiwizowanie działającego systemu wraz z zablokowanymi systemowymi plikami, nietypowymi systemami plików czy działającymi bazami danych. Możemy zatem wybiórczo i w różnych momentach skopiować zawartość całych dysków, wybranych katalogów czy plików lub baz danych. Oczywiście tak skopiowane dane są w odpowiedni sposób skatalogowane i zapisane. Oczywiście zapisane na odpowiednim urządzeniu znajdującym się w przeciwległym skrzydle szpitala.

W naszym przypadku zabezpieczenia są na kilku poziomach. Po pierwsze miejsce standardowych dysków twardych w serwerach przejęły macierze dyskowe odpowiednio wysokiego poziomu z nadmiarowymi dyskami. Po drugie wykonywane przez Baculę kopie są składowane na innej macierzy w odległym od serwerowni pomieszczeniu. Po trzecie oprócz tego niektóre elementy systemu (np. serwer SUN z bazą Informix) na bieżąco zapisują stosowne logi na tasiemce streamera. Po czwarte pliki z danymi z baculowej macierzy dyskowej przenoszone są na dyski DVD tworząc kopię kopii i jednocześnie archiwum. I po piąte w tej chwili trwają prace nad pełną wirtualizacją serwerów.

Dzięki temu wszystkiemu przeżyliśmy już kilka poważnych awarii. I jeszcze nigdy po takiej awarii nie trzeba było wykonywać ponownie więcej pracy niż z ostatniego dnia. Mamy nadzieję, że będzie nawet lepiej i nigdy nie trzeba będzie ponownie „wklepywać" danych nawet tych sprzed 5 minut.

Reasumując, dzięki Baculi możemy w jednym miejscu zarządzać kopiami zapasowymi z kilkunastu serwerów i maaasy stacji klienckich (jeżeli będzie taka potrzeba), a sam proces wykonywania kopii jest w ponad 90% zautomatyzowany. Wiadomo, próbnej reinstalacji systemu automat nie wykona za nas, musimy przynajmniej włożyć odpowiednio spreparowaną płytkę CD do napędu i pozwolić na jej zabootowanie.

Właściwie jedyną wadę, jaką ma takie rozwiązanie, czemu oczywiście zaprzeczają zwolennicy uniksów, jest tekstowy interfejs, dzięki któremu jesteśmy w stanie odzyskać odpowiednie pliki.

I na koniec praktyczna uwaga. Systemy zapisu kopii zapasowych systemami, ale jednak nie ma to jak tekstowy plik eksportu bazy danych…

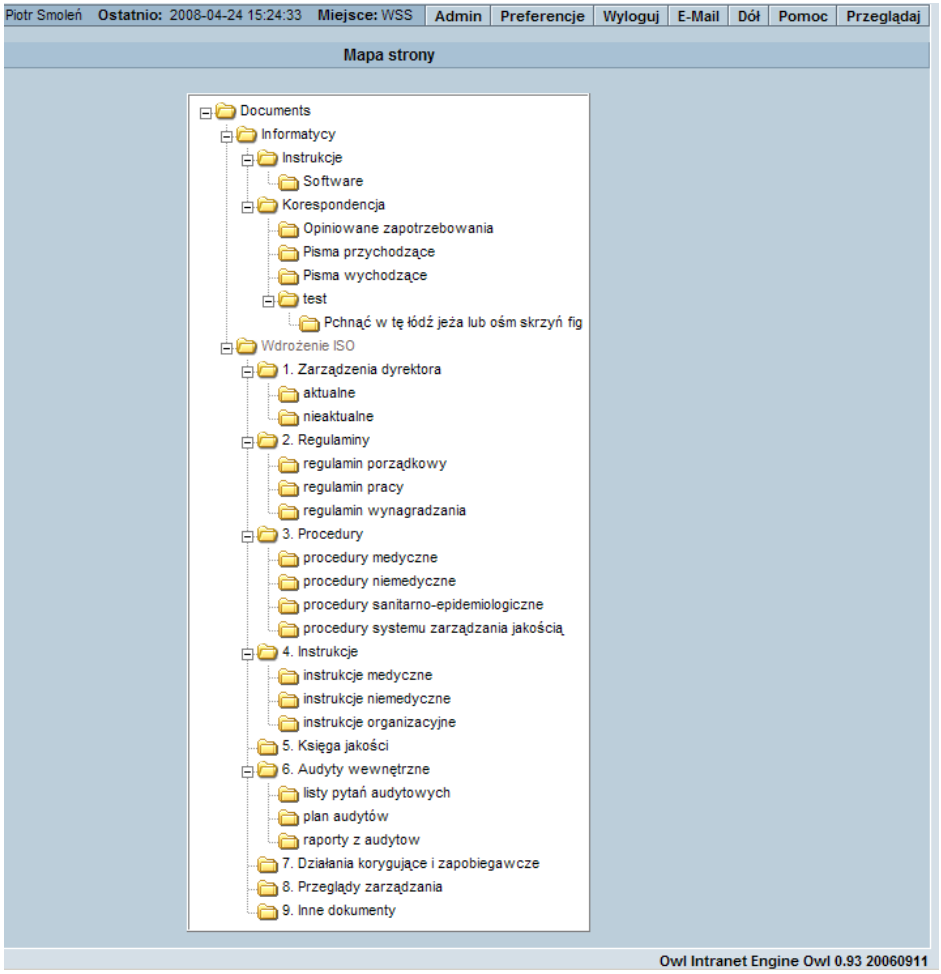
Repozytorium dokumentów OWL (18)

Kolejny przykład systemu, którego obecność użytkownicy widzą i doświadczają własnymi zmysłami, nie tak jak w przypadku innych fragmentów WINBOSS'a, które są cichymi strażnikami informatycznego ładu, niewidocznymi dla użytkowników. OWL jest programem, w którym pracuje się na co dzień. Efekty jego pracy są widoczne i mierzalne.

OWL to repozytorium dokumentów. Dzięki jego pomocy możemy zapanować nad informacjami przekazywanymi w postaci pism, listów elektronicznych, linków do witryn internetowych czy czegokolwiek innego co można zapisać w postaci elektronicznej, ot chociażby nagranej notatki głosowej w postaci pliku mp3. Jest to system, do którego dostęp mamy za pośrednictwem przeglądarki internetowej, czyli bez potrzeby instalowania żadnego oprogramowania klienckiego.

Praca systemu opiera się na 3 podstawowych elementach: użytkownikach, katalogach i dokumentach. Dzięki współpracy z katalogiem LDAP użytkownicy całego systemu i OWL to jedność. Chcąc korzystać z usług repozytorium po prostu używamy tego samego konta i hasła, którego używamy do włączenia komputera czy dostępu do Internetu. Oczywiście nie każdy użytkownik domeny jest aktywnym użytkownikiem OWL, dlatego też system ten rządzi się własnymi prawami, jeżeli chodzi o uprawnienia dostępu do katalogów jak i przynależność do grup. Katalogi to z kolei nic innego jak uporządkowana hierarchicznie struktura służąca do przechowywania dokumentów, analogiczna do systemu plików na dysku twardym, ale wzbogacona o wiele dodatkowych atrybutów i możliwości. Natomiast dokumenty to, jak już wspomniałem wcześniej, wszystko to, co można zapisać w postaci elektronicznego pliku, czyli zeskanowane pisma, pliki pakietów biurowych, projekty programów typu CAD, linki, listy i wszystko inne. Te 3 podstawowe elementy współpracują ze sobą w systemie umożliwiając zapanowanie nad nieprzebraną biurokracją.

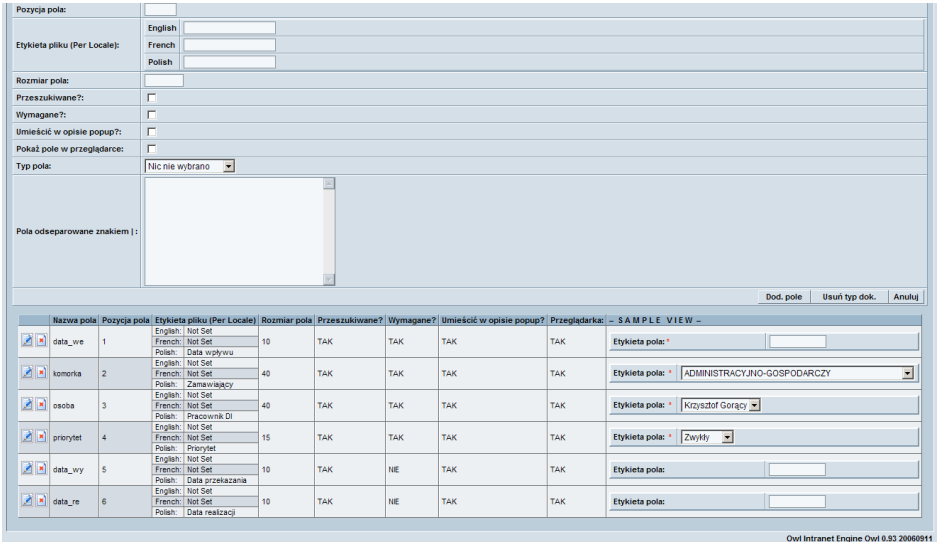
Rozpoczynając pracę z OWL należy zdefiniować wszystkich niezbędnych użytkowników i grupy, do których będą oni należeć. Następnie definiujemy strukturę katalogów.



Rysunek 35. Rysunek obok pokazuje rozwinięte drzewo przykładowej struktury katalogów. Zarówno sam układ, jak nawet ikonki, pokazują pełną analogię do systemu zapisu plików na dyskach. Właściwie to jest jakby dysk tylko z tą różnicą, że nie będziemy go widzieli jako kolejnej literki po kliknięciu *Mój komputer*.

Mając zdefiniowanych użytkowników i strukturę katalogów musimy w następnej kolejności przyporządkować katalogi do użytkowników i grup, nadając im tym samym odpowiednie uprawnienia początkowe. Oczywiście te uprawnienia można później modyfikować w trakcie pracy dostosowując całość do własnych nawet bardzo specyficznych oczekiwań.

Jedyne, czego teraz nam potrzeba do pracy, to właściwie już same dokumenty. Pracę właściwie można by było już rozpocząć w tym momencie zapisując jakiś dokument do odpowiedniego katalogu. Od tej pory dokument rozpoczął by już swoje wirtualne życie, w którym może być przeglądany, modyfikowany (z zachowaniem wszystkich poprzednich wersji zmian!), przekazywany, komentowany, wysyłany, opatrzony dodatkowymi informacjami. Tak będzie się działo w przypadku większości dokumentów, których struktury i zawartości nie jesteśmy w stanie przewidzieć. Choć już nawet w tym miejscu każdy dokument powinien posiadać jakieś atrybuty.



Rysunek 36. Powyższy rysunek pokazuje panel administratora z definicją atrybutów schematu pism „zapotrzebowanie". Jak widać na rysunku definiujemy nie tylko nazwy atrybutów, ale także ich rodzaj, podobnie jak definiuje się zmienne w językach programowania. Do dyspozycji w tym momencie mamy także listy wyboru (combo box) z wyborem wstępnie zdefiniowanych wartości parametru. Przy okazji widać możliwość pracy w jednym systemie użytkowników posługujących się różnymi językami.

Załóżmy, iż otrzymaliśmy właśnie faksem pismo od Urzędu Marszałkowskiego, z jakąś sygnaturą, odwołujące się do innej sprawy o innej sygnaturze. Pismo jest podpisane przez konkretną osobę i adresowane do innej konkretnej osoby. Ponadto pismo nosi datę przedwczorajszą, ale przecież przyszło do nas dopiero dzisiaj i my również nadamy mu jakiś numer dziennika korespondencji przychodzącej. To wszystko, co opisałem powyżej, to przykład atrybutów praktycznie każdego pisma. Pewne typowe dokumenty, którymi posługujemy się w naszym szpitalu i do których istnieją gotowe formularze, mogą być opatrzone zupełnie

innymi atrybutami bądź są rozszerzone o kolejne w stosunku do tych opisywanych powyżej. Oczywiście atrybuty te są istotne z punktu widzenia obsługi danego pisma/tematu i mają służyć ułatwieniu czy wręcz umożliwieniu poruszania się wśród nich, odszukiwania, raportowania i podejmowania decyzji. OWL umożliwia tworzenie schematów typowych dokumentów, definiowania dla nich zestawów atrybutów, co następnie przekłada się na łatwość odszukiwania i segregowania korespondencji.

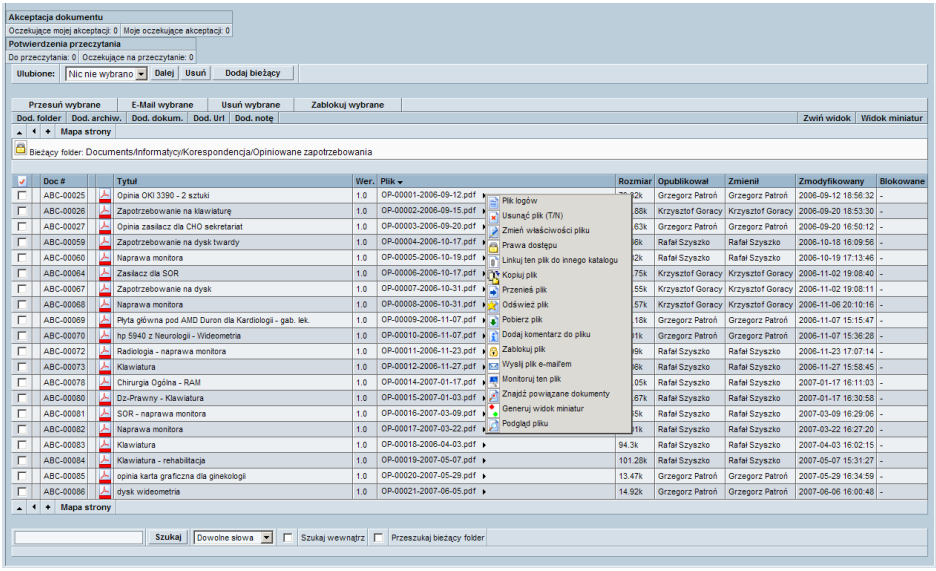
W ten sposób definiujemy wszystkie rodzaje dokumentów i przyporządkowujemy do nich stosowne atrybuty stosownego rodzaju. Teraz system będzie mógł pokazać, co potrafi przy wyszukiwaniu i sortowaniu.

Dodając do systemu kolejny dokument wskazujemy jego typ a następnie wypełniamy stosowne parametry. Przykład poniżej pokazuje zawartość jednego z katalogów zawierającego np. zapotrzebowania.

System umożliwia wymuszenie akceptacji publikacji dokumentu dzięki czemu osoby na szeregowych stanowiskach będą mogły opublikować wiadomość dopiero po jej zaakceptowaniu przez wskazaną osobę. Unikamy dzięki temu pojawianiu się w naszym Intranecie nieprzemyślanych do końca treści.

Odpowiednie katalogowanie plików to podstawowa funkcja systemu OWL, jednak nie jedyna. Znajdziemy tutaj obsługę „niusów", czyli szybkich i ważnych informacji. Znajdziemy tutaj także pewną dodatkową funkcję dopisaną przez nas a zapewniającą pewną podstawową funkcjonalność spotykaną w systemach elektronicznego obiegu dokumentów. Mianowicie chodzi tu o funkcję wymuszenia potwierdzenia przeczytania. Wygląda to tak, iż osoba umieszczająca jakiś dokument w katalogu może wskazać osoby lub grupy osób, od których wymaga się potwierdzenia przeczytania tegoż dokumentu i w dodatku oczekujemy tego potwierdzenia do określonej daty, czyli typowy deadline. Wszelkie potwierdzenia oczywiście następują za pomocą konta i hasła domenowego. Osoba będąca autorem takiej publikacji na bieżąco ma wgląd w informacje kto i kiedy dokument przeczytał. W ten sposób można np. przekazywać wszelkie zarządzenia dyrekcji, których znajomość i przestrzeganie jest obowiązkowe, a które są adresowane do kierowników wszystkich komórek organizacyjnych odpowiedzialnych za ich wdrożenie we własnej jednostce. W ten sposób przyspieszamy obieg dokumentów i oszczędzamy zarówno papier jak i materiały eksploatacyjne dla drukarek i kserokopiarek.

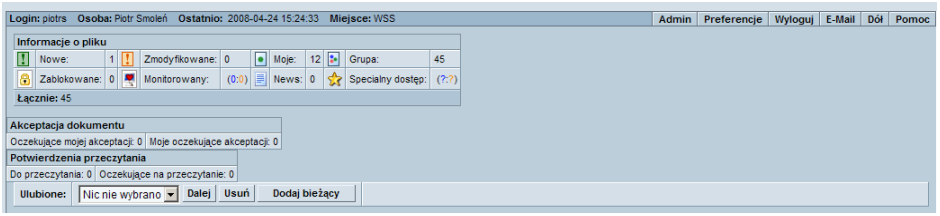
Ilość informacji możliwych do obsługi w systemie jest olbrzymia. Wraz ze wzrostem tej ilości coraz ciężej by było poruszać się w gąszczu dokumentów, coraz ciężej byłoby rozpoznać nowość od nieaktualnego już starocia czy odpowiedzieć sobie na pytanie *czy ja to już czytałem i czy to jest nowa wersja*. Z pomocą tutaj przychodzi pasek stanu, który oferuje funkcjonalność typową dla forów dyskusyjnych, ale oczywiście dostosowaną do specyfiki tegoż repozytorium.



Rysunek 37. Na rysunku widać rozszerzoną listę dokumentów zdefiniowanego typu „Opiniowane zapotrzebowania". Jak widać pola definiowane przez użytkownika mogą być widoczne jako kolumny w zestawieniu. Ponadto rozwinięte menu kontekstowe pokazuje mnogość akcji, jakie mogą być wykonane na wybranym dokumencie lub ich grupie. Proponuję zwrócić uwagę na niepozorną opcję na dole rysunku „Szukaj wewnątrz". Jej użycie pozwala na wyszukiwanie zadanej frazy nie tylko w nazwie i parametrach dokumentu, ale także w jego zawartości. Niestety lista typów dokumentów, dla których ta opcja działa jest ograniczona.

Tak jak zostało już powiedziane, OWL jest systemem pracującym, z punktu widzenia użytkownika, jak każda typowa strona internetowa. System powiadomień o wszelkich zdarzeniach realizowany jest drogą poczty elektronicznej. Użytkownicy systemu są na bieżąco w ten sposób informowani o wszystkim, co się dzieje. Nic nie stoi na przeszkodzie, aby dzięki drobnym pracom takie powiadamianie było również za pomocą SMS.

Dokładne omówienie pełnej funkcjonalności systemu zdecydowanie wykracza poza zakres tego opracowania i wymagało by napisania co najmniej kilkudziesięciostronicowej rozprawy. Dla przykładu nie poruszyłem tutaj większości funkcji administracyjnych służących do importowania i zasilania wstępnego, jak też tworzenia kopii bezpieczeństwa i ewentualnego ich później wykorzystania.



Rysunek 38. Na rysunku powyżej widzimy pasek stanu z informacjami co też pojawiło się nowego od naszej ostatniej wizyty i wymaga naszej uwagi. Dzięki temu nie musimy dokopywać się do katalogów, w których być może jest coś ważnego dla nas.

Jak wszystkie elementy naszej układanki, również OWL jest oprogramowaniem klasy Open Source. Został przez nas przetłumaczony na język polski i poszerzony o dodatkową funkcjonalność pozwalającą realizować podstawy obiegu dokumentów. Trzeba jednak nadmienić, iż najlepszym momentem na wdrażanie tego rozwiązania jest albo moment, kiedy mamy już certyfikację ISO 9001 albo prace nad certyfikacją są rozpoczęte. Przeanalizowane, przemyślane i poprawnie opisane procedury postępowania, zwłaszcza procedury kancelaryjne, są absolutną podstawą działania tego systemu.

System zarządzania treścią Joomla (19)

Jak zostało wspomniane już wcześniej, instytucje takie jak szpital mają obowiązek posiadania swojej strony internetowej. Mają także obowiązek umieszczania na takiej stronie niektórych informacji związanych z Biuletynem Informacji Publicznej (BIP) czy zamówieniami publicznymi. Z natury rzeczy informacjami prezentowanymi w BIPie zajmują się zdecydowanie inne działy niż informatyki, a przynajmniej powinny. Podobnie dla zamówień publicznych w każdej takiej instytucji jest oddzielny, specjalnie do tego celu powołany dział. W obu przypadkach (i wielu innych także) produkowane są wszelkiego rodzaju ogłoszenia, zarządzenia, komunikaty, dekrety itp., przy których magistrat rzymski z kreskówki *12 prac Asteriksa* to po prostu przedszkole. Wcześniej oczywiście konieczność wpisywania i publikowania wszelkich dokumentów i informacji na naszej tronie www spadała na nasz dział. W pewnym momencie należało powiedzieć dość. Po przejrzeniu dostępnego oprogramowania wybór padł na Joomlę. Może są i lepsze, i bardziej rozbudowane systemy, nam jednak ten w zupełności wystarcza. Mamy więc system wraz z prawami dostępu, dzięki którym wyznaczeni i przeszkoleni użytkownicy z właściwych działów aktualizują na bieżąco zawartość strony www naszej jednostki. Nasza praca w tym zakresie sprowadza się do nadawania lub odbierania praw użytkownikom oraz do jednorazowej konfiguracji, aby dział „Ogłoszenia wewnętrzne" był dostępny wyłącznie tylko wewnątrz naszej jednostki.

System kont dostępu w Joomli jest oddzielony od LDAP. Przy czym szczerze mówiąc już nie pamiętamy, czy jest tak dlatego, że Joomla została uruchomiona przed naszym Winbossem, czy dlatego, że nie miała natywnego połączenia z tą bazą. Oficjalna wersja jest taka, że ze względów bezpieczeństwa celowym było rozdzielenie użytkowników domenowych od użytkowników Joomli, zwłaszcza jeżeli mają oni mieć dostęp z zewnątrz.

W ten oto sposób rozwiązany został problem dynamicznej zmiany zawartości naszego serwisu www przez osoby bezpośrednio odpowiedzialne za informacje danego typu bez konieczności angażowania „programistów".

Wybaczcie proszę, że nie prezentuję tutaj obrazków naszej strony internetowej, ale nie byłyby one w żaden sposób reprezentatywne i raczej pewnie ukrywałyby niż uwypuklały możliwości samej Joomli, która u nas wykorzystywana jest w podstawowym zakresie.

Logowanie połączeń sieciowych ARGUS (20)

Argus to fragment systemu odpowiedzialny za logowanie informacji o ruchu sieciowym. Jego zadaniem jest śledzenie ruchu w określonych miejscach systemu i zapisywanie zagregowanych informacji w plikach logów, z możliwością ich późniejszego użycia. Analiza takiego ruchu ma sens, kiedy usługa ta ma dostęp do wybranych punktów sieci i jest „karmiona" odpowiednim ruchem. Z tego powodu istotne jest, aby miejsca podłączenia do sieci były przemyślane. Z jednej strony, w dobie inteligentnych przełączników, możemy niechcący pominąć jakiś istotny fragment ruchu sieciowego, a z drugiej zapchać system gigantyczną ilością niepotrzebnych informacji, choć przyznać należy, że ARGUS właśnie tak został zaprojektowany, aby zapchać go było nie sposób. Miejsce styku Argusa z siecią musi być zatem mocno przemyślane. Podobnie muszą być dobrze przeanalizowane potrzeby co i jak szczegółowo rejestrować. Argus potrafi przechwycić i zapisać cały ruch sieciowy z pełną zawartością treści. W takim jednak przypadku stalibyśmy się jednak największym odbiorcą dysków twardych na świecie, na których zapisywane byłyby informacje o całym ruchu sieciowym. Podejście całkowicie nieuzasadnione i nieekonomiczne. Dodatkowo w tym wypadku trzeba ostrożnie poruszać się w przestrzeni prawnej tak, aby nie naruszyć

prywatności korespondencji. Doświadczenie administratora, wraz z podstawową wiedzą z zakresu prawa, jest tutaj absolutnie niezbędne.

W naszym przypadku Argus wyposażony jest w kilka interfejsów sieciowych podłączonych w strategicznych miejscach sieci (np. na styku z Internetem, na styku ze specjalistycznymi systemami medycznymi typu radiologia cyfrowa czy przy serwerach). Analizując ruch sieciowy zapisywane są informacje o nadawcy i odbiorcy (w rozumieniu logiki sieci) konkretnych pakietów, czasie zaistnienia zdarzenia i ilości bajtów przesyłanych informacji. Nie jest natomiast zapisywana zawartość transmisji, mimo że oczywiście sam system na to pozwala. Z założenia jedynym zadaniem Argusa jest kolekcjonowanie takich informacji wraz z przygotowaniem podstawowych statystyk typu ilość przesłanych bajtów w jednostce czasu.

Zapytacie na pewno po co zapisywać te informacje? Jest kilka powodów: po pierwsze dajemy sobie szansę na znalezienie przyczyny ewentualnych kłopotów, po drugie chcemy mieć możliwość śledzenia niektórych działań, kiedy zakładając nawet, że nie zapobiegniemy niektórym wydarzeniom, to przynajmniej będziemy w stanie odnaleźć winowajcę w rozumieniu zarówno osoby, jak i sprzętu i po trzecie mamy obowiązek takiego monitorowania ze względu na ewentualną konieczność współpracy z przedstawicielami prawa.

UltraVNC (21)

Zdecydowanie więcej niż połowa zgłoszeń o problemach to nie rzeczywiste problemy techniczne, tylko kłopoty wynikające z braku umiejętności użytkowników w posługiwaniu się programami lub niechęć do czytania komunikatów. Nie wiem dlaczego, ale każdy komunikat, jaki pojawi się na ekranie, zawsze wywołuje panikę i w słuchawce telefonu słyszę, że „komputer mi się zawiesił". Oczywiście w takich przypadkach na jakąkolwiek próbę wytłumaczenia, że wystarczy wcisnąć ten JEDYNY przycisk zatytułowany OK, użytkownicy reagują oburzeniem i kwitują, że nie są informatykami. W typowej sytuacji nie ma innego wyjścia, jak założyć beret na głowę i przespacerować się do „problemu". Kłopot w tym, że spora ilość stacji roboczych i odległości liczone co najmniej w setkach metrów, czynią takie podejście całkowicie nieefektywne czasowo i finansowo. Często w takich przypadkach zdarzało się, że zanim dotarliśmy na miejsce problem „sam się naprawił".

Z pomocą w takich przypadkach przychodzi nam instalowany na WSZYSTKICH stacjach klient VNC, czyli programik, dzięki któremu możemy widzieć na swoim monitorze obraz z monitora odległej stacji oraz przejąć kontrolę nad jej klawiaturą i myszką. Możliwe jest także przesyłanie informacji, jak w programach do czatu czy też mamy dostęp do systemu plików maszyny, do której się podłączyliśmy. Dodatkowo UltraVNC ma tą zaletę, że możemy podłączyć go do LDAP i prawo do podłączania się zdalnego do stacji uzyskają automatycznie wszyscy użytkownicy z grupy administratorów domeny. Nie ma więc konieczności pamiętania miliona haseł do każdej stacji z osobna.

Niestety jest jednak mały problem z VNC. Polega on na tym, że większość programów antywirusowych traktuje go jak typowego trojana i czasami są problemy z przekonaniem, że jednak się mylą.

Co dalej?

WINBOSS nie jest systemem zamkniętym. Wręcz przeciwnie: ciężko zdefiniować jego granice działania, zarówno czasowe, jak i tematyczne. Na pewno będzie się rozwijał w miarę doskonalenia poszczególnych elementów. Coraz większa jego skuteczność umożliwi skierowanie wolnych mocy przerobowych na rozwiązywanie coraz nowszych problemów, które dotychczas były pomijane, czy to ze względu na mniejszy kaliber, czy wręcz przeciwnie ze względu na monstrualne skomplikowanie. Jest już na chwilę obecną kilka tematów, które zapewne będą dopominać się realizacji.

1. Uruchomienie wewnętrznego komunikatora umożliwiającego użytkownikom wymianę informacji online na zasadzie czatu czy też pozostawianie krótkich wiadomości do późniejszego odczytania. Po głowie chodzi nam Jabber.
2. System elektronicznego obiegu dokumentów. Ale nie jakieś tam repozytorium, tylko work flow z prawdziwego zdarzenia! Takie z możliwością implementacji skomplikowanych i warunkowych procesów biznesowych. I tutaj także oprogramowanie Open Source daje spore możliwości. Temat jest jednak wielce skomplikowany i uzależniony od całej masy decyzji na poziomie dyrektorskim w naszej jednostce. Osobiście uważam, że temat powinien zacząć żyć własnym życiem w końcowym etapie wdrażania polityki jakości w naszej jednostce, wtedy kiedy wszystkie procedury będą wielokrotnie zweryfikowane i przetarte w boju. Poza tym takie rozwiązania wymagają więcej niż żelaznej dyscypliny wszystkich bez wyjątku pracowników. Samo rozwiązanie jednak istnieje i czeka na swój czas: mam tutaj na myśli projekt BONITA.
3. Dokończenie procesu wirtualizacji serwerów. Wszyscy administratorzy doskonale wiedzą, co oznacza praca jakiegoś systemu na maszynie, która jest jedyna w swoim rodzaju czy to ze względów specyfikacji technicznej czy programowej. Awaria czegoś takiego, to koszmar dla każdego z nas. A jeżeli jeszcze dodatkowo z jakichś tam powodów maszyna taka nie jest serwerem z krwi i kości i posiada np. tylko jeden zasilacz, to pozostawienie takie-

go stanu rzeczy jest jak pozostawienie bomby zegarowej, która przyspiesza wraz z upływem czasu. Proces wirtualizacji serwerów jest u nas rozpoczęty i w niektórych przypadkach doprowadzony do końca. Zadowoleni jednak będziemy, kiedy wszystkie usługi produkcyjne i zarządzające infrastrukturą zostaną przeniesione na serwery wirtualne pracujące na maszynach z założenia przeznaczonych do pracy 24 godziny na dobę (czasami nawet 25) i 365 dni w roku (a czasami nawet 366).

4. Teraz pozwolę sobie na swoje osobiste marzenie. Komputery, które pracują u nas w jednostce łącznie stanowią całkiem pokaźną moc obliczeniową. Moc, która na pewno będzie się zwiększać i która na pewno jest porównywana do najsilniejszego klastra obliczeniowego w Polsce… Wiecie już, co mi chodzi po głowie. Taka moc jest nie do pogardzenia. Za takie możliwości np. firmy farmaceutyczne płacą ogromne pieniądze w procesie projektowania leków. Dlaczego nie dać sobie szansy na częściowy chociażby zwrot kosztów zakupu sprzętu wynajmując go w godzinach bezczynności dla innych? Poza tym medycyna, jak mało która dziedzina, prosi się o system ekspercki. Olbrzymie ilości danych powiązanych ze sobą w mało przewidywalny sposób czekają na eksplorację.

Pomysłów na dalsze doskonalenie naszego rozwiązania na pewno nie zabraknie. Na szczęście nasza czwórka nie należy do pokornych, którzy godzą się z tym, co jest, ale szuka rozwiązań, które pozwolą coś zrobić lepiej, szybciej, taniej i bardziej widowiskowo.

Czy jest zatem tak dobrze?

Nie, nie jest wcale tak idealnie, jak wydawać by się mogło po przeczytaniu tych kilkudziesięciu stron. Nie mam na myśli tutaj jednak jakichś ukrytych problemów technicznych czy konfiguracyjnych. Oczywiście takie wyzwania na pewno są, ale nie stanowią zazwyczaj większego problemu w dłuższym okresie czasu. Największy problem stanowią tutaj ludzie, nie wyłączając także samych pracowników działu informatyki. Największe wyzwanie stanowi tutaj zmuszenie siebie i innych do systematycznego przestrzegania raz ustalonych zasad. Czasami małe zaniedbanie pociąga za sobą skutki ciągnące się potem tygodniami.

W przestrzeganiu procedur upatruję zarówno największe niebezpieczeństwo dla powodzenia takiego projektu, jak i największe potencjalne możliwości. Nawet najlepsza grupa fachowców nic nie zwojuje, jeżeli nie będzie potrafiła wdrożyć w życie nawet najbardziej genialnych swoich pomysłów. Niezbędne zatem jawi się pozyskanie przychylności dyrekcji i zdobycie jej zaufania, tak aby pozwoliła robić to, na czym się znamy najlepiej, bez odgórnego ingerowania w założenia. Oczywiście, że prace takowe muszą być konsultowane w swoich najważniejszych założeniach z kierownictwem placówki. Jednak bądźmy szczerzy: ilu z nas ma przełożonych, którzy choćby w połowie orientują się w temacie, jak każdy pracownik działu z osobna? Dlatego zaufania i pozostawienie wolnej ręki jest tak ważne.

Tutaj mam także kilka zdań do ludzi kierujących działami IT (a właściwie do wszystkich kierujących jakimiś grupami osób): pamiętajcie, że nie musicie być wcale najlepszymi programistami czy administratorami, żeby być bardzo dobrymi kierownikami! Musicie być jednak świadomi swoich zalet a zwłaszcza wad! Pozwólcie zatem swoim kolegom z działu robić to, co potrafią najlepiej i zadbajcie o to, żeby nikt im w tym nie przeszkadzał i żeby mieli minimum tego, co mieć powinni, aby czuć się w miarę komfortowo. Za swoimi ludźmi musicie stać murem, nawet jeżeli nie zgadzacie się z nimi w 100%. Jeżeli nawet zawinili, to zwróćcie im uwagę, ale za zamkniętymi drzwiami i nie pozwólcie, aby ktoś inny za was kierował waszym działem. Słuchajcie co do was mówią, bo jak przestaną mówić, to znaczy, że czas na was szukać nowego miejsca pracy. Pamiętajcie, że niekoniecznie jesteście najlepsi. Pamiętajcie, że czasami najlepsze, co możecie zrobić, to nie wtrącać się, odciążyć od prostych i przyziemnych obowiązków, i pozwolić robić innym to, co potrafią najlepiej. Pamiętajcie, że korona z głowy wam nie spadnie, gdy w wolnych od „papierkowych obowiązków" chwilach złapiecie za śrubokręt i wymienicie uszkodzony zasilacz. Może wtedy właśnie zauważycie, że w dziale nie ma śrubokręta…

Czas podsumować

WINBOSS nie jest systemem produkcyjnym. Za jego pomocą nie wyprodukujecie nawet jednej wykałaczki, nie wyleczycie nawet jednego chorego i nie zaksięgujecie ani jednej faktury. Ale bez takiego rozwiązania nawet 100 milionów € wydanych na najlepszy sprzęt i oprogramowanie produkcyjne zamieni się w stertę nieprzydatnego i awaryjnego żelastwa produkującego jedynie chaos. WINBOSS pozwala zapanować nad sprzętem i oprogramowaniem w dużej i bardzo dużej firmie położonej w wielu miastach, nawet w różnych krajach. Pozwala na wprowadzenie reguł i egzekwowanie ich przestrzegania. Pozwala na minimalizację nakładów pracy, ujednolicenie informatycznych narzędzi i sposobów postępowania. Daje możliwość, minimalnej liczbie osób, zapanowania nad ogromnym majątkiem. Porządkuje zbiory danych i schematy postępowań. Kataloguje wiedzę i daje szansę na analizę przyczyn i skutków, nawet jeżeli nie uda nam się zabezpieczyć przed wszystkimi czarnymi scenariuszami. Umożliwia trzymanie w ryzach, na rozsądnym poziomie, kosztów utrzymania potężnej infrastruktury

IT niezbędnej do pracy w *Statutowych celach*. Minimalizuje koszty eksploatacyjne i daje potężne możliwości kontrolowania, weryfikacji i rozliczania pracy poszczególnych osób i jednostek. I najważniejsze: WINBOSS gwarantuje sprawne podniesienie się z kolan nawet po najbardziej koszmarnych awariach. A każdy dyrektor powinien wiedzieć, że zdecydowanie więcej niż połowa firm, w których nastąpiły poważne awarie systemów, nie dało radę podźwignąć się i upadło po tym fakcie w ciągu 2 lat.

Każdy dobry menadżer zna także regułę Pareto, która mówi, że 80% pracy w firmie wykonuje 20% pracowników. My nie wykonujemy co prawda tych 80% pracy, ale umożliwiamy, aby 19% innych ją wykonało. Patrząc na ilość pracowników działu IT w naszym szpitalu możemy bez cienia zarozumiałości stwierdzić, że sprawna możliwość pracy całości zależy od 0,25% wszystkich zatrudnionych.

Ile to kosztuje?

Bardzo mało, a porównując do rozwiązań komercyjnych, właściwie nic. Jeżeli mamy zatrudnionego odpowiedniego fachowca, to koszt takiego rozwiązania jest wyłącznie kosztem maszyn, które należy przeznaczyć na serwery. Śmiało możemy uruchomić system na komputerach, na które wydamy 5-7 tysięcy złotych brutto! W dużych firmach na 80% znajdą się jakieś maszyny mogące spełnić to zadanie w początkowej fazie. Docelowo profesjonalne serwery wraz z wyposażeniem dla sporego przedsiębiorstwa, zatrudniającego powyżej 1000 osób i posiadającego około 500 komputerów, będą kosztować 100-200 tys. zł, w zależności od naszej koncepcji całości. Myślę, że powyższe środki bez problemu można wygospodarować w tak dużych jednostkach. Polecam także wszelkiego rodzaju dofinansowania z funduszy unijnych, które tylko czekają, aby z nich skorzystać. Może się okazać, że płacąc kilkanaście tysięcy złotych specjalistycznej firmie za sporządzenie stosownego wniosku aplikacyjnego, pozyskamy takie fundusze nawet w 85%! A jeżeli nie mamy odpowiedniego fachowca? Zapraszam wtedy do nas. Za kwotę nie większą niż 50 tys. złotych zainstalujemy na powierzonym sprzęcie, w jednostce o podobnej wielkości, wszystkie wymienione elementy w czasie 1-2 miesięcy. Czy to dużo? Odpowiedzcie sobie sami. Z moich wyliczeń wynika, że jest to 4-6 pensji przeciętnego lekarza z dyżurami w publicznym szpitalu w mieście z Polski „B". W celu lepszego zrozumienia skali proponuję porównanie tych kwot z ewentualnymi wydatkami choćby tylko na licencje komercyjnego sieciowego systemu operacyjnego obsługującego 800 użytkowników…

O autorze

Jestem absolwentem docenianego i lubianego w regionie Technikum Łączności przy Zespole Szkół Elektronicznych w Lublinie. W latach 90-tych ukończyłem Wydział Fizyki Doświadczalnej Uniwersytetu Marii Curie-Skłodowskiej w Lublinie, gdzie uzyskałem także tytuł magistra po obronie pracy z zakresu plazmy niskoenergetycznej o temacie *Wpływ poświaty jonów ujemnych na powierzchnię elektrody*. Wraz z dr Heleną Murlak-Stachurą (UMCS) jestem współautorem kilku publikacji naukowych w tematyce swojej pracy magisterskiej, której wyniki były prezentowane na kilku zjazdach i sympozjach naukowych.
Jeszcze podczas studiów dziennych rozpocząłem pracę w firmach branży IT, gdzie pnąc się od najniższego szczebla instalatorów i techników zyskiwałem wiedzę i doświadczenie. W czasie współpracy z firmami komercyjnymi branży IT uzyskałem certyfikaty z instalacji okablowania strukturalnego Mod-Tap, instalacji central telefonicznych Lucent Technologies, administracji Novell NetWare, Hewlett Packard Network Star i inne.

W 2000 roku trafiłem do Wojewódzkiego Szpitala Specjalistycznego im. Stefana Kardynała Wyszyńskiego SP ZOZ w Lublinie, gdzie pracuję do dnia dzisiejszego. Jestem jednym z obecnie czterech, a w przeszłości sześciu, osób opracowujących i wdrażających rozwiązania informatyczne dla szpitala. Razem korzystamy z dość dużej autonomii obecnego Działu Informatyki. Z racji powszechnie znanej sytuacji placówek służby zdrowia i nie mając innego wyjścia, zagłębiłem się w nurt otwartego oprogramowania, co, jak się szybko okazało, było bardzo dobrym wyborem.

Z racji własnych ambicji i planów na przyszłość ukończyłem kolejne dwa kierunki podyplomowe *Nadzór, kontrola i audyt wewnętrzny w gospodarce i administracji* oraz *Zarządzanie zakładami opieki zdrowotnej i administracja zdrowiem publicznym* na Wyższej Szkole Ekonomii i Innowacji w Lublinie. W tym roku prawdopodobnie rozpocznę naukę na kierunku MBA na tutejszej politechnice. 14 października 2009 roku byłem prelegentem na konferencji *Informatyka w służbie zdrowia* zorganizowanej w hotelu Marriott przez wydawnictwo Computerworld.

W wolnych chwilach oddaję się pasji akwarystycznej aktywnie udzielając się także w Polskim Klubie Miłośników Dyskowców (`http://pkmd.pl`).

Piotr Krzysztof Smoleń
`winboss@szpital.lublin.pl`

Książki wydawnictwa HELION

Zarządzanie projektami IT. Przewodnik po metodykach.

Adam Kloszajda

Krzysztof Ołowski

Temat zarządzania projektami IT jest znany od dawna, jako niełatwe pole do działania. Wszystkim wydaje się, że się na informatyce znają, informatycy wiedzą najlepiej, co użytkownikom najlepiej będzie używać, dyrekcja zastanawia się na co idą tak olbrzymie pieniądze i czemu często rzeczy wyglądające na proste w wykonaniu wydłużają się niemiłosiernie.

Jeżeli szukasz złotego pomysłu na rozwiązanie wszystkich problemów dotyczących prowadzenia projektów informatycznych, to …nie sięgaj po tą książkę. Jeśli jednak chcesz poznać główne koncepcje metodyk prowadzenia projektów informatycznych, to zdecydowanie polecam tę książkę. W sposób przystępny dobrze rozdziela metody zarządcze (Prince2, PMBoK), wytwórcze (RUP, MSF), adaptacyjne (eXtreme Programming, Scrum) i organizacyjne (CMMI, Six Sigma, ITIL, COBIT). Jeśli jesteś członkiem zespołu informatyków, prowadzisz taki zespół lub go rozliczasz z prac, warto choćby przejrzeć charakterystyki powyższych metod i wybrać najbardziej pasującą do Twojej firmy.

Jako osobie pracującej w zespole informatyków i mającej wpływ na część działań zespołu, szczególnie mi przypadł do gustu rozdział o metodach adaptacyjnych, dobrym rozdzieleniu zadań osób zlecających, pilnujących wykonania i faktycznie wykonujących tą pracę. Rozdział o Programowaniu Ekstremalnym zawiera zbiór bardzo dobrych praktyk dla informatyków (tak programistów, jak i administratorów), rozdział o SCRUM pokazuje, w jaki sposób można poradzić sobie z niedotrzymaniem terminów wykonania prac.

Książka na pewno przyda się również członkom zarządów firm, w których dział informatyczny wykonuje więcej prac niż instalowanie drukarek i skręcanie komputerów. Pomoże zrozumieć wiele, niekoniecznie oczywistych, niuansów, które pomogą we wzajemnym zrozumieniu z informatykami. Z kolei informatykom może pomóc w spojrzeniu „z drugiej strony monitora" na ich pracę i zrozumienie, że, niestety, czasem potrzebne są kompromisy pomiędzy zadaniami wykonanymi w sposób idealny od strony sztuki informatycznej a sposobem akceptowalnym przez przełożonych.

Ciekawym elementem tej książki są wywiady z osobami od wielu lat zajmującymi się prowadzeniem projektów informatycznych. Nie do pominięcia jest również fakt, że książka jest napisana przez Polaka i traktuje o ściśle polskich realiach, co z pewnością ułatwi wdrożenie części pomysłów na rodzimym gruncie.