Protokół LDAP jako technika zarządzania zasobami sprzętowo-programowymi akademicko-naukowej sieci komputerowej w Polsce

Maja Górecka-Wolniewicz, Tomasz Wolniewicz

Uniwersytet Mikołaja Kopernika, Toruń

Streszczenie

Artykuł jest propozycją działań związanych z rozbudową i popularyzacją usług katalogowych opartych na protokole LDAP. Przedstawiono aktualny stan bazy informacyjno-adresowej w polskim środowisku akademicko-naukowym. Omówiono możliwe zastosowania zasobów LDAP jako wsparcia dla różnorodnych usług sieciowych. Wskazano priorytetowe działania i zaproponowano harmonogram prac.

1 Wprowadzenie

Protokół LDAP (*Lightweight Directory Access Protocol*) zyskuje coraz większą popularność jako mechanizm obsługi zasobów o charakterze katalogowym. Umożliwia łatwy i uniwersalny dostęp do baz danych z informacjami o środowisku sieciowym: użytkownikach, usługach, urządzeniach, prawach dostępu itp. Jest obecnie częścią wielu systemów operacyjnych, a także składnikiem licznych aplikacji sieciowych (m.in. serwerów i interfejsów użytkowych poczty elektronicznej, przeglądarek WWW itp.). Zasady działania LDAP-a opierają się w znacznym stopniu na standardzie X.500, którego pierwsza wersja została opublikowana w 1988 roku. Standard X.500 jest osadzony w 7-warstwowej strukturze OSI, natomiast LDAP jest zdefiniowany w oparciu o protokół TCP/IP.

Od 1992 roku usługa katalogowa bazująca na standardzie X.500 jest dostępna w polskiej sieci akademicko-naukowej. Dzięki projektowi, którego celem była popularyzacja usług katalogowych i zaoferowanie zasobów informacyjno-adresowych na temat środowiska akademickiego, uczestniczące w nim zdobyły duże doświadczenie. LDAP odegrał istotną rolę we wdrażaniu usługi katalogowej. Pełnił funkcję protokołu dostępowego, przyczynił się do powstania łatwych i wszechstronnych interfejsów użytkownika, np. programów oferujących zasoby X.500 za pośrednictwem przeglądarki WWW. W oparciu o dotychczasowe prace można szybko rozpocząć działania propagujące zastosowanie usługi katalogowej opartej na protokole LDAP. W ramach realizowanego przez kilka lat projektu utworzono strukturę wiążącą kilka ważnych środowisk akademickich w kraju, która może teraz stanowić podstawę prac w ramach nowego przedsięwzięcia. Ogromną zaletą wszystkich usług katalogowych jest ich uniwersalność, elastyczność i łatwa skalowalność. Obecnie coraz częściej LDAP obsługuje nie tylko zasoby stanowiące swego rodzaju książkę adresowo-informacyjną użytkowników sieci, jest również stosowany do gromadzenia i zarządzania danymi, które dotyczą zasobów sprzętowo-programowych. Tego typu zastosowania należy uwzględnić w nowym projekcie.

2 LDAP jako wsparcie usług katalogowych

2.1 Korzenie LDAP-a

Zadaniem protokołu LDAP jest obsługa zasobów typu katalogowego (*directories*), czyli specyficznej bazy danych zoptymalizowanej do potrzeb odczytu, zawierającej informacje często wykorzystywane przez różne zastosowania sieciowe. Jego historia jest ściśle związana z międzynarodowym standardem ISO/ITU o nazwie X.500 ([1], [10]). Na początku lat osiemdziesiątych pojawiła się idea stworzenia specjalnego typu bazy danych, przeznaczonej do przechowywania informacji często używanych przez aplikacje sieciowe. Motywem działań w tym kierunku była potrzeba dwóch usług: odwzorowania nazw na adresy sieciowe i odwrotnie oraz poczta elektroniczna. W tych czasach dominowały sieci X.25, a poczta elektroniczna opierała się na skomplikowanych adresach standardu X.400. Pierwsza wersja X.500 została opublikowana w 1988 roku. Standard ten bazuje na warstwach protokołu OSI i jest bardzo rozbudowany. Głównie to spowodowało, że nie zyskał wielu zwolenników, tym bardziej, że okres jego adaptacji przypadł na lata rozwoju usług internetowych, stosujących dużo prostsze podejście do kwestii sieciowych. LDAP powstał jako typowy protokół dostępowy, przeznaczony do operowania na zasobach danych o strukturze zgodnej ze standardem X.500. Jest dużo prostszy i bardziej naturalny niż X.500. Korzysta z modelu informacyjnego oraz schematu nazewnictwa standardu X.500. Zbiór typów atrybutów i przypisanych im wartości tworzy tzw. wpis (*entry*). Wpisy umieszczane w zasobach są uporządkowane hierarchicznie. Każdy wpis ma unikatową nazwę na określonym poziomie drzewa informacyjnego, tzw. względną nazwę wyróżnioną (*relative distinguished name, RDN*). Lokalizacja wpisu determinuje jego nazwę wyróżnioną w globalnej strukturze danych (*distinguished name, DN*) – powstaje ona przez połączenie względnych nazw wyróżnionych wszystkich wpisów leżących na drodze od korzenia drzewa danych do bieżącego wpisu. Ważną rolę odgrywa schemat zasobów, gdyż on właśnie decyduje, jakie dane można umieścić w zasobach. Początkowo serwery LDAP pełniły funkcję pośrednika między klientem a bazą X.500. Interfejs programisty dostarczany w implementacjach LDAP zdefiniowany w [8] jest prosty, w przeciwieństwie do środowiska programowego X.500, dzięki czemu łatwo można przygotowywać aplikacje użytkowe. Dlatego właśnie LDAP przyczynił się do popularyzacji X.500. Sukces LDAP-a spowodował, że postanowiono rozbudować ten protokół, by oprócz komunikacji klient-serwer obsługiwał wymianę informacji między serwerami. W 1997 roku pojawiła się definicja wersji 3 LDAP-a ([6], [13]).

2.2 Rozwój LDAP-a

Nadal trwają prace standaryzacyjne, których celem jest rozbudowa protokołu LDAP. Już w obecnej formie LDAP oferuje pełnowartościową usługę katalogową. Główne kierunki prowadzonych prac to przygotowanie reguł przechowywania w bazie meta-informacji dotyczącej odsyłaczy do innych serwerów (*knowledge references*), kwestie uwierzytelniania użytkowników i podpisywania cyfrowego danych, rozbudowa interfejsu programisty, dostosowanie protokołu do pracy w oparciu o bezpołączeniową warstwę transportową (UDP) oraz do przechowywania dynamicznych danych, wymagających częstego odświeżania. Duży nacisk kładzie się na zdefiniowanie zasad kontroli dostępu do zasobów, z czym wiąże się zastosowanie atrybutów przeznaczonych dla danych tego typu. Bardzo ważne jest stworzenie mechanizmów replikacji zasobów katalogowych między serwerami LDAP, by sprostać wymogom nowoczesnych systemów rozproszonych, w których dostępność zasobów jest

sprawą kluczową. Standard X.500 już od 1993 roku definiuje zasady replikacji. Niektóre implementacje LDAP-a rozwiązują ten problem wprowadzając własną, nieprzenośną technikę lub korzystają z reguł replikacji stosowanych przez bazę danych (np. relacyjną) pracującą w tle. Dwie grupy robocze przy Internet Engineering Task Force zajmują się aktualizacją i modyfikacją protokołu. Grupa LDAP Directory Update (LDUP) określa zasady replikacji, a jej celem jest stworzenie uniwersalnego protokołu replikacji oraz odpowiednie rozbudowanie modelu informacyjnego zasobów, by zagwarantować przenośność w ramach replikacji. Grupa LDAP Extensions jest odpowiedzialna za opracowanie rozszerzeń standardu, określenie technik kontroli dostępu i rozbudowę interfejsów programisty.
Aktualne prace nad LDAP wskazują, że dąży się do dostosowania tego protokołu do bardzo rozbudowanych potrzeb. Początkowo usługi katalogowe były stosowane do przechowywania informacji o charakterze statycznym, rzadko modyfikowanej, przeznaczonej przede wszystkim do odczytu. Obecnie coraz częściej LDAP jest wymieniany jako wsparcie dla różnych aplikacji sieciowych, dlatego jest dostosowywany model informacyjny, powstają pomocnicze protokoły, by zwiększyć możliwości i zagwarantować uniwersalność.

2.3 LDAP a X.500

Obecnie LDAP i X.500 są kompatybilnymi protokołami do obsługi zasobów typu katalogowego. Na ogół dostęp do bazy X.500 jest realizowany nadal za pomocą LDAP-a. Oba podejścia wydają się bardzo podobne, ale nie można zapomnieć o kilku istotnych różnicach.
Po pierwsze LDAP ma wbudowane dodatkowe własności z zakresu bezpieczeństwa, używa protokołu SASL ([12]) i może pracować w oparciu o bezpieczną warstwę transportową TLS lub SSL ([2]). Poza tym LDAP ma mechanizmy, które pozwalają zaliczyć go do protokołów obsługujących wiele różnych usług katalogowych oraz tzw. meta-katalogi. Tę możliwość wprowadza stosowanie adresów będących URL-ami do przeszukiwania LDAP-owskich baz danych ([9]). Ogromną zaletą są definicje własnego interfejsu programisty oraz uniwersalnego formatu danych (LDAP Data Interchange Format, LDIF, [3]) – takich własności brakuje w standardzie X.500.
Nie można jednak pominąć niedostatków protokołu LDAP. W standardzie X.500 jest bardzo dobrze określona komunikacja między serwerami, kwestie łańcuchowania zleceń, przekazywania odesłań. W LDAP-ie te zagadnienia są na etapie opracowywania. X.500 zawiera specjalne protokoły: Directory Information Shadowing Protocol (DISP), definiujący zasady realizacji replikacji typu „single-master" oraz Directory Operational Binding Protocol (DOP) do negocjacji porozumień między serwerami (np. porozumienia replikacji). W X.500 istnieje od wielu lat definicja schematu kontroli dostępu, twórcy LDAP-a dopiero opracowują te elementy.
LDAP, w przeciwieństwie do standardu X.500, który z założenia realizuje 7-warstwowy model OSI, pracuje w oparciu o warstwę TCP/IP i to przede wszystkim decyduje o jego sukcesie. Może być w sposób naturalny integrowany z różnymi, popularnymi aplikacjami wyższego poziomu, a jego implementacja jest dużo prostsza.

3 Usługa katalogowa w Polsce

W polskim środowisku akademicko-naukowym usługa katalogowa, działająca w oparciu o standard X.500, jest obecna od 1992 roku, kiedy został uruchomiony na Uniwersytecie Mikołaja Kopernika w Toruniu serwer poziomu krajowego. Wkrótce wystartował serwer obsługujący UMK, a parę miesięcy później serwery regionalne w Warszawie, Poznaniu,

Wrocławiu i Krakowie. Przedsięwzięciu „X.500 w polskim środowisku akademicko-naukowym" patronowała Naukowa Akademicka Sieć Komputerowa, Komitet Badań Naukowych kilkakrotnie dofinansowywał prace związane z aktualizacją bazy informacyjno-adresowej. W kolejnych latach zostały uruchomione serwery X.500 w Łodzi (LODMAN), Gdańsku (TASK) oraz w Akademii Ekonomicznej we Wrocławiu, Politechnice Szczecińskiej, Politechnice w Zielonej Górze, Akademii Techniczno-Rolniczej w Bydgoszczy. Zasoby X.500 mają przede wszystkim charakter bazy informacyjno-adresowej. Odzwierciedlają strukturę organizacyjną uczelni, zawierają adresy, telefony instytucji oraz dane dotyczące pracowników, takie jak: e-mail, telefon, adres służbowy, stanowisko, specjalizacja, zainteresowania. Zakończenie dofinansowania przez Komitet Badań Naukowych sprawiło, że znacznie pogorszyła się aktualność danych. Po wprowadzeniu w życie ustawy o ochronie danych osobowych pojawiły się również problemy natury formalnej – konieczne stało się dysponowanie zgodą właścicieli danych na ich publikowanie. Kilka uczelni zrezygnowało z tego powodu z prowadzenia serwisu. Obecnie w środowisku akademickim pracuje siedem serwerów X.500.

Działania związane z wdrożeniem usługi katalogowej w polskim środowisku naukowo-akademickim nie ograniczały się do kwestii instalacyjno-administracyjnych. Były prowadzone prace o charakterze badawczo-rozwojowym, dotyczące przede wszystkim efektywności usługi katalogowej oraz problematyki związanej z dostosowaniem systemu do specyfiki języka lokalnego ([5]). W oparciu o ogólnodostępne oprogramowanie web500gw przygotowano polski interfejs użytkownika, program, za pomocą którego można korzystać z zasobów X.500 lub LDAP. Powstał również interfejs administracyjny, dający prosty sposób aktualizacji zasobów i umożliwiający przekazanie zarządzania danymi do jednostek, których informacje dotyczą.

Polska w 1992 roku dołączyła do projektu Paradise, kierowanego przez University College London, którego celem było utworzenie światowej usługi katalogowej. W 1994 roku patronat nad tymi pracami przejęła organizacja sieciowa Dante, od tego czasu projekt nosi nazwę NameFlow-Paradise. Obecnie działania uczestników tego projektu skupiają się na przeniesieniu usługi katalogowej na serwery LDAP.

4 Oprogramowanie

Wszechstronna specyfikacja i standardy nie wystarczają do wdrożenia przydatnej usługi. Do sukcesu jest potrzebne dobre oprogramowanie implementujące standard. W Polsce do spadku zainteresowania usługą katalogową opartą na X.500 w dużej mierze przyczynił się brak ogólnodostępnego oprogramowania implementującego nowe wersje standardu. Dodatkowo, pojawiły się problemy z instalacją bezpłatnego oprogramowania starszej wersji (pakietu Isode) na nowych systemach operacyjnych. LDAP od początku miał swoją bezpłatną implementację, tworzoną przez programistów University of Michigan. Obecnie działa projekt OpenLDAP, który udostępnia coraz nowsze wersje implementacji protokołu LDAP, starając się nadążać za ciągle zmieniającą się specyfikacją. Istnieje kilka komercyjnych pakietów LDAP. Najpopularniejszy jest produkt Sun-Netscape Alliance, iPlanet Directory Server. Inne znane implementacje to Oracle Internet Directory firmy Oracle oraz Innosoft Distributed Directory Server. Obecnie większość systemów operacyjnych ma domyślnie zainstalowane pakiety umożliwiające korzystanie z usługi LDAP (interfejs użytkownika). Jest tak w Solarisie 2.8, HP-UX oraz w systemach firm Silicon Graphics, Compaq Computer Corp. Novell od lat implementuje w swoim systemie własną usługę katalogową NDS, która wspo-

maga zarządzanie zasobami sprzętowymi i programowymi. Najnowsza jej wersja o nazwie eDirectory współpracuje z LDAP-em. Microsoft w systemach serii 2000 dodał usługę katalogową Active Directory, korzystającą z modelu informacyjnego X.500/LDAP i kompatybilną z protokołem LDAP.

5 Zastosowania LDAP-a

Usługi katalogowe stają się kluczowym elementem większości aplikacji sieciowych, pełnią rolę typowego oprogramowania pośredniczącego (*middleware*). Pozwalają szybko wyszukiwać potrzebne informacje o zasobach sieciowych oraz umożliwiają poświadczanie tożsamości użytkowników. W zasobach zarządzanych za pomocą protokołu LDAP można umieszczać różnorodne informacje: dane osobowe, adresy pocztowe, e-mail, telefony, adresy grup dyskusyjnych, wskazania serwerów WWW, zdjęcia, dźwięk, a także informacje o strukturze domenowej, komponentach sprzętowych. Ogromne możliwości daje przechowywanie w zasobach katalogowych uprawnień do usług sieciowych, urządzeń itp. Mówi się o trzech kategoriach zastosowania LDAP-a ([7]):

- do lokalizacji użytkowników oraz zasobów sieciowych,
- do zarządzania zasobami sieciowymi i ustalania praw dostępu użytkowników,
- do uwierzytelniania i zabezpieczenia użytkowników.

LDAP jest obecnie zintegrowany z wieloma programami. Firma Netscape od wielu lat korzysta z tego protokołu w swoich przeglądarkach do obsługi książki adresowej. Jest elementem programu PGP, gdzie wspomaga wyszukiwanie kluczy publicznych PGP. Program *sendmail* używa LDAP-a do realizacji rutingu poczty. Takie rozwiązanie jest szczególnie przydatne w przypadku, gdy jeden serwer obsługuje bardzo dużą jednostkę i ważne staje się przesyłanie komunikatów e-mail do konkretnych stacji (czyli adresy e-mail jednej domeny są kierowane do różnych serwerów). W bazie LDAP używanej do realizacji intranetowego rutingu można również umieszczać informację o preferowanych przez użytkownika metodach odbioru poczty, limitach dyskowych ([11]). System obliczeń rozproszonych Globus (http://www.globus.org) korzysta z LDAP-a do obsługi sieciowego środowiska superkomputerowego i optymalnej realizacji obliczeń rozproszonych. LDAP służy tu do przechowywania informacji na temat zasobów sprzętowo-programowych i wspomaga procedury wybierania miejsca obliczeń. Tego typu zastosowanie protokołu LDAP jest nowatorskie i narzuca dodatkowe wymagania związane z dynamiką zasobów. Model zasobów LDAP jest też idealnym miejscem gromadzenia certyfikatów kluczy publicznych wydawanych przez urzędy certyfikacyjne zorganizowane w infrastrukturę kluczy publicznych, a także list odwołanych certyfikatów. Certyfikat to klucz publiczny oraz dane identyfikujące jego właściciela poświadczone przez specjalny, zaufany urząd. Sposób określania nazwy właściciela certyfikatu jest spójny ze specyfikacją X.500/LDAP. Certyfikaty oraz listy odwołanych certyfikatów przechowywane w bazie LDAP, wspomagają korzystanie z aplikacji sieciowych stosujących protokoły SSL oraz TLS oraz z reguł pełnego bezpieczeństwa ([2], [4]).

LDAP znalazł również zastosowanie w oprogramowaniu Samba, w którym serwer LDAP pełni funkcję scentralizowanego magazynu danych uwierzytelniających. Tego typu zastosowania są ostatnio bardzo popularne. Apache, program implementujący serwer WWW, może korzystać ze specjalnego modułu (mod_auth_ldap, auth_ldap, mod_LDAPauth – istnieje kilka takich rozwiązań), który daje możliwość współpracy z serwerem LDAP w celu pobierania danych uwierzytelniających. Projekt Shibboleth, zainicjowany przez Internet2 Middleware Initiative ma za zadanie opracowanie metod uwierzytelniania użytkowników oraz auto-

ryzacji dostepu do zasobów, gdy są one współdzielone przez wiele instytucji. Cele te są realizowane w oparciu o możliwości protokołu LDAP i infrastruktury kluczy publicznych. Projekt użycia protokołu LDAP jako wspierającego usługę rozproszonego przeszukiwania katalogów bibliotecznych przedstawiono w [14].

6 Realizacja projektu

6.1 Cele projektu

Główne cele proponowanego projektu to:

1. Uruchomienie w ramach projektu PIONIER bazy informacyjno-adresowej pracującej na serwerach LDAP i połączonej z projektem Dante-Nameflow.
2. Umożliwienie wykorzystywania usług katalogowych do celów uwierzytelniania i autoryzacji w innych usługach (WWW, portale, biblioteki cyfrowe).
3. Integracja usług katalogowych z infrastrukturą kluczy publicznych (PKI).
4. Przygotowanie propozycji korzystania z bazy LDAP do przechowywania informacji o usługach i zasobach POL34.
5. Przygotowanie propozycji korzystania z bazy LDAP do zbierania statystyk o zasobach centrów MAN i KDMO.
6. Rozpoznanie zasadności włączenia protokołu LDAP do zarządzania siecią i QoS.

6.2 Proponowane kierunki prac

Pierwszym zadaniem projektu powinno być odnowienie kontaktów roboczych ze wszystkimi zespołami biorącymi udział w projekcie X.500 (TASK Gdańsk, Politechnika Wrocławska, Akademia Ekonomiczna Wrocław, ACK Cyfronet Kraków, Politechnika Łódzka, UAM Poznań, PCSS Poznań, Politechnika w Zielonej Górze, ICM Warszawa, ATR Bydgoszcz oraz Politechnika Szczecińska). Wszystkie te środowiska są dobrze przygotowane do działań związanych z protokołem LDAP. Oprogramowanie X.500 od 1995 roku w istotny sposób ograniczało możliwości działań w kierunku rozwoju usługi katalogowej w Polsce i dostosowania jej do nowoczesnych tendencji, gdyż przestały być dostępnie wersji, w których są implementowane własności standardu X.500'93. Projekt OpenLDAP oferujący nieodpłatnie pakiet, który implementuje LDAP-a ciągle rozwija się i wydaje się, że w ciągu najbliższych lat będzie zagwarantowany bezpłatny dostęp do oprogramowania. W oparciu o istniejące zasoby bazy X.500 można stosunkowo szybko przestawić usługę katalogową, tak by była oparta na LDAP-ie. Od lat szeroko stosowany interfejs dostępowy X.500 korzysta wyłącznie z LDAP-a (serwer LDAP pośredniczy w obsłudze zleceń kierowanych do systemu X.500), będzie więc mógł być nadal stosowany. Przejście na usługę katalogową obsługiwaną przez LDAP-a musi wiązać się z pełną aktualizacją zasobów (w wielu środowiskach X.500 dane są aktualizowane na bieżąco, ale niektóre regiony od pewnego czasu nie modyfikują zasobów) i ich reorganizacją, jeśli będą tego wymagać cele projektu. Na tym etapie każda jednostka prowadząca serwer LDAP musi legitymować się zgodą na gromadzenie i zarządzanie danymi osobowymi (zgodnie z ustawą o ochronie danych osobowych). Oznacza to konieczność uzyskania ekspertyzy na temat prawnych aspektów prowadzenia zasobów o charakterze prywatnym.

Kolejnym zadaniem projektu powinny być prace nad opracowaniem nowego schematu zasobów LDAP. Schemat ten (klasy obiektów, atrybuty) musi uwzględniać potrzeby innych

projektów programu PIONIER oraz przewidywane zastosowania LDAP-a. Ważne są następujące zagadnienia:

- zastosowanie w opisach osób i jednostek organizacyjnych atrybutów związanych z infrastrukturą kluczy publicznych oraz kluczy PGP;
- wprowadzenie odrębnej hierarchii drzewiastej do reprezentacji obiektów w sieci komputerowej: serwerów, urządzeń typu drukarka, routerów;
- konieczność stosowania atrybutów pozwalających na umieszczanie praw dostępu;
- zasady rozszerzenia schematu zasobów, tak by LDAP-owskie zasoby danych mogły być używane do specyficznych zastosowań (np. katalog wirtualny).

Projekt musi dopuszczać możliwość wykorzystania LDAP-a do nietypowych celów, w tej sytuacji mogą być stosowane odrębne schematy danych i trzeba uwzględnić potrzebę dynamicznej lokalizacji schematów bazy oraz ich dystrybucji.

Utrzymywanie i udostępnianie polskich zasobów katalogowych LDAP wymaga dokładnego sprawdzenia możliwości serwerów oraz programów użytkowych w zakresie obsługi kodowania polskich liter. Problematyka ta została szczegółowo przedstawiona w pracy [5]. OpenLDAP oraz większość nowoczesnych implementacji LDAP-a korzystają ze standardu Unicode do zapamiętywania danych. Należy zagwarantować prawidłową obsługę strony kodowej przy wprowadzaniu danych (najczęściej dane wejściowe są przygotowane w Latin2) oraz właściwą prezentację danych przez interfejsy użytkownika (np. przeglądarki). Dodatkowy problem stanowi tworzenie posortowanych wykazów oraz przeszukiwanie za pomocą wzorców zawierających polskie znaki diakrytyczne.

Odrębnym zagadnieniem jest ustalenie zasięgu polskich zasobów LDAP. Jeśli mają one stanowić fragment międzynarodowej usługi katalogowej (na wzór X.500 i projektu Paradise), to trzeba uwzględnić konieczność przechowywania angielskich odpowiedników nazw (np. instytucji, jednostek itp.). Zgodnie ze standardem LDAP służą do tego atrybuty wielowartościowe, w których można stosować podtypy atrybutu w celu specyfikacji języka. Należy jednak szczegółowo sprawdzić, jak te własności są realizowane w różnego rodzaju interfejsach użytkowych.

Jak już wcześniej podkreślono, elementem mającym istotne znaczenie dla właściwego przebiegu projektu jest oprogramowanie. Należy zapewnić, by wszystkie cele projektu mogły zostać zrealizowane przy użyciu nieodpłatnego oprogramowania OpenLDAP. Z drugiej strony trzeba liczyć się z tym, że niektórzy partnerzy będą stosować oprogramowanie komercyjne. Jednym z pierwszych zadań musi być szczegółowe rozpoznanie dostępnych na rynku implementacji LDAP, ocena jego możliwości i na tej podstawie określenie listy preferowanego oprogramowania.

Szczegółowe zadania powinny objąć:

1. Rozbudowę polskiego interfejsu (użytkownika i administratora danych) do bazy LDAP.
2. Przygotowanie pilotowych instalacji usług sieciowych korzystających z LDAP (sendmail, PAM, PGP, Apache) i opracowanie zaleceń dla polskiego środowiska akademickiego.
3. Opracowanie schematu polskiej bazy LDAP wspierającej m.in.:
   a) typową informację adresową,
   b) routing poczty elektronicznej,
   c) kontrolę dostępu do zasobów WWW,
   d) przechowywanie informacji o kluczach PGP,
   e) przechowywanie certyfikatów X.509.

4. Stworzenie narzędzi automatyzujących zarządzanie zasobami LDAP, w tym zmasowane ładowanie, synchronizacja zasobów LDAP z innymi bazami danych (np. relacyjnymi).
5. Nadawanie użytkownikom uprawnień dostępu do zasobów sprzętowych i programowych oraz utrzymywanie list dostępu dla aplikacji, urządzeń itp.
6. Opracowanie mechanizmów dostępu do zasobów sieciowych w oparciu o nadane uprawnienia.
7. Opracowanie mechanizmów obsługi kluczy publicznych oraz list odwołanych certyfikatów zgromadzonych w zasobach LDAP (związane z zarządzaniem PKI) w zakresie umieszczania danych w bazie oraz ich pobierania i automatycznego ładowania do aplikacji.
8. Zbudowanie wszechstronnych interfejsów do wyszukiwania różnego typu danych zgromadzonych w zasobach LDAP (metody poruszania się po różnych fragmentach drzewa danych, określania punktu startowego przeszukiwania, korzystanie z serwerów indeksujących itp.).
9. Opracowanie narzędzi korzystających z bazy LDAP zintegrowanej z systemem Globus w celu pobierania statystyk i monitorowania stanu systemu.
10. Zastosowanie LDAP-a do wspomagania obsługi bibliotek cyfrowych oraz innych usług, np. portali internetowych, wyszukiwarek.
11. Analiza efektywności usługi katalogowej, ocena wyników pod kątem wprowadzenia replikacji zasobów i zastosowanie replikacji w uzasadnionych przypadkach (obecnie brakuje ostatecznej standaryzacji zagadnień replikacji, ale jest zapowiadane zakończenie prac nad tym zagadnieniem; zapewne wkrótce potem ukaże się oprogramowanie implementujące tę własność).

W czasie projektu powinna zostać przeanalizowana zasadność uruchomienia prac w następujących tematach:
1. Rejestrowanie wykorzystania zasobów, m.in. dla potrzeb rozliczeniowych, wykorzystanie protokołu SNMP i stosowanej w nim drzewiastej struktury zasobów sieciowych, opracowanie reguł dystrybucji informacji o wykorzystaniu zasobów.
2. Zastosowanie LDAP-a w systemach dostępu do licencji oprogramowania.

7 Przewidywane efekty

Uruchomienie centralnej bazy użytkowników systemów komputerowych na uczelni pozwoli na scentralizowaną obsługę kontroli dostępu do zasobów WWW i do kont na systemach komputerowych oraz umożliwi wprowadzanie poprawek do informacji w bazie adresowej (użytkownik miałby tylko jedno hasło dostępu do wszystkich usług). W pewnych przypadkach można rozszerzyć wspomniane zastosowania np. o obsługę konta w bibliotekach uczelni. Należy również podjąć pilotowe prace nad użyciem takiej bazy dla celów billingu.
Opracowanie jednorodnego schematu bazy przechowującej dane o zasobach komputerowych centrów KDMO i MAN pozwoli na publikowanie danych zawsze aktualnych (obecnie KBN zbiera takie dane drogą listową i umieszcza je na swoim serwerze raz do roku). System taki pozwoliłby również na publikowanie bieżącej statystyki o zajętości zasobów w centrach obliczeniowych.
Opracowanie schematu przechowywania informacji o bibliotecznych serwerach protokołu Z39.50 pozwoli na automatyczną konfigurację polskiego katalogu wirtualnego ([14]).

Podziękowania

Autorzy dziękują Jerzemu Żenkiewiczowi z Uniwersyteckiego Centrum Technologii Sieciowych oraz Sebastianowi Szuberowi z Poznańskiego Centrum Superkomputerowo-Sieciowego za konsultacje w trakcie przygotowywania założeń projektu.

Bibliografia

1. Chadwick D., „Understanding X.500: The Directory", International Thomson Computer Press, 1999. Dostępna bezpłatnie pod adresem http://www.salford.ac.uk/its024/X500.htm.
2. Dierks T., Allen C., „The TLS Protocol Version 1.0", RFC 2246, January 1999.
3. Good G., „LDAP Data Interchange Format: Technical Specification", Internet Draft, 1998.
4. Górecka-Wolniewicz M., Żenkiewicz J., „Infrastruktura kluczy publicznych w polskim środowisku akademicko-naukowym", materiały konferencyjne PIONIER2001.
5. Górecka M., Wolniewicz T., „Dostosowanie bazy X.500 do specyfiki języka lokalnego", maj 1996, materiały konferencyjne Miedzeszyn'96.
6. Howes T. i in., „Understanding and Deploying LDAP Directory Services", MacMillan Network Architecture and Development Series, 1999.
7. Howes T., „LDAP: Use as Directed", Data Communications, February 1999 (http://www.networkmagazine.com/article/DCM20000502S0039).
8. Howes T., Smith M., „The LDAP Application Program Interface", RFC 1823, August 1995.
9. Howes T., Smith M., „The LDAP URL Format", RFC 2255, November 1997.
10. ITU/ISO Recommendation X.500 – Information technology – Open Systems Interconnection – The directory: Overview of concepts, models, and services, November 1993.
11. Lachman H., „LDAP Schema for Intranet Mail Routing", Internet Draft, October 1999.
12. Myers J., „Simple Authentication and Security Layer (SASL)", RFC 2222, October 1997.
13. Wahl M., Howes T., Kille S., „Lightweight Directory Access Protocol (v3)", RFC 2251, December 1997.
14. Wolniewicz T., „Wirtualny katalog biblioteczny", materiały konferencyjne PIONIER2001.