OBSŁUGA ZASOBÓW INFORMACYJNO-ADRESOWYCH ZA POMOCĄ PROTOKOŁU LDAP – PRZEGLĄD DOSTĘPNYCH NARZĘDZI I PORÓWNANIE Z TECHNOLOGIĄ X.500

Maja Górecka **Tomasz Wolniewicz**

Maja.Gorecka@cc.uni.torun.pl *twoln@hpc.uni.torun.pl.*

Naukowa Akademicka Sieć Komputerowa NASK

Zakład Rozproszonych Systemów Informacyjnych

Referat odnosi się do najnowszych tendencji w sieci Internet dotyczących obsługi zasobów informacyjno-adresowych, zwanych katalogowymi bazami danych (***Directory Services***). Punktem odniesienia przeprowadzonej analizy zagadnienia jest standard X.500. Autorzy pracy od 1992 roku zajmują się tą tematyką i kierują rozwojem usługi X.500 na terenie Polski. Referat omawia zyskujący coraz większą popularność protokół LDAP (*Lightweight Directory Access Protocol*) na tle historii standardu X.500. Następnie prezentujemy konkretne narzędzia do obsługi baz katalogowych za pomocą protokołu LDAP. W zakończeniu oceniliśmy efekty przeprowadzonych testów polegających na uruchomieniu usługi katalogowej pracującej na oprogramowaniu LDAP.

Tematyka panujących obecnie tendencji w dziedzinie usług katalogowych była również przedmiotem naszego opracowania [13]. Lektura pozycji [3, 4] pozwala zapoznać się z poglądami osób intensywnie zaangażowanych w rozwój światowej usługi X.500.

Opracowanie podsumowuje działania zmierzające do przygotowania się do prac rozwojowych na nowych platformach.

1. Standard X.500

Pełną wersję międzynarodowych rekomendacji ITU-T dotyczących standardu X.500 można znaleźć w odpowiednich dokumentach ([1]). Jest to zestaw zaleceń (X.500-X.521) obejmujący m.in. definicję struktury bazy, opis modelu informacyjnego i funkcjonalnego, definicję protokołu komunikacji między współpracującymi systemami, specyfikację bazowych własności zasobów: typów obiektów oraz atrybutów. Standard X.509 precyzuje zasady komunikacji w ramach bezpiecznych systemów informacyjnych, określa metody uwierzytelniania użytkowników systemu. Tematykę X.500 przybliża w sposób przystępny, a jednocześnie wyczerpujący pozycja [2]. Prezentowane przez nas w ubiegłych latach referaty ([5]) były z jednej strony opisem cech i funkcjonalności X.500, z drugiej stanowiły podsumowanie prowadzonych przez nas prac rozwojowych w tym zakresie.

Pierwsza wersja standardu ukazała się w 1988 roku. Potrzeba tego typu specyfikacji wynikła z charakteru usługi X.400 (poczta elektroniczna), która stosowała skomplikowane łańcuchy do identyfikacji stron komunikujących się. Poczta elektroniczna oparta o protokół X.400 nie przyjęła się, natomiast funkcjonalność X.500 rozszerzono z zamiarem stosowania tej technologii do zarządzania rozproszonymi zasobami informacyjno-adresowymi, gromadzącymi adresy, telefony, opisy itp. osób, jednostek organizacyjnych, instytucji.

Tuż po ukazaniu się standardu X.500 zaczęły pojawiać się pierwsze jego implementacje. W środowisku akademicko-naukowym najpopularniejszy stał się pakiet `Quipu`, autorstwa Collina Robinsa, który szybko zdominował światowy rynek i stał się podstawą późniejszych komercyjnych implementacji sprzedawanych m.in. przez firmy Isode Ltd, NEXOR, czy ISOCOR.

Specyfikacja X.500 jest bardzo obszerna, zdefiniowana w ramach siedmiowarstwowego sieciowego modelu OSI. Podstawowym założeniem jest brak uzależnienia od wykonywanego programu, czy środowiska sieciowego. Standard określa globalną, rozproszoną bazę danych opartą na hierarchicznym modelu nazywania obiektów, które mogą być wyszukiwane w zasobach lub przeglądane. X.500 funkcjonuje na zasadzie sieci serwerów (DSA), każdy ma utrzymywać porcję globalnej bazy danych. Użytkownik zasobów X.500 nie jest świadomy ich rozproszenia, ma wrażenie, że korzysta z jednej dużej bazy.

Kluczowe komponenty specyfikacji X.500 w wersji X.500 to:

1. DSA (*Directory System Agent*) – podstawowy serwer usługi, zarządzający fragmentem globalnej bazy.
2. DUA (*Directory User Agent*) – interfejs użytkownika, proces kliencki zgłaszający się do serwera w celu wyszukania informacji.
3. DAP (*Directory Access Protocol*) – protokół stosowany przez DUA dla uzyskania dostępu do serwerów DSA.
4. DSP (*Directory System Protocol*) – protokół stosowany do komunikowania się serwerów DSA między sobą.

Zastosowania usługi katalogowej opartej na standardzie X.500 są różnorodne. Przykładem jest światowa baza X.500 środowiska akademicko-naukowego rozwinięta w trakcie projektu PARIDISE i obecnie koordynowana przez organizację DANTE. Istnieje również sporo zastosowań w instytucjach, gdzie standard X.500 i odpowiednie oprogramowanie służy do zarządzania bazami pracowniczymi, czy systemami ewidencji zasobów różnego typu. W takich przypadkach w minimalnym stopniu, lub wcale nie jest wykorzystywana funkcja rozproszenia zasobów, stosowany jest model scentralizowanej bazy.

2. LDAP

Protokół LDAP wyrósł na bazie doświadczeń w rozwijaniu usługi katalogowej X.500 w latach 1989-91. Dwóch autorów interfejsów użytkowych do zasobów X.500, Marshall Rose i Tim Howes, rozwinęło „odchudzony" protokół pośredniczący w komunikacji programu klienckiego z serwerem X.500. Idea polegała na konstruowaniu przez stronę kliencką prostych zleceń, które przekazywane są serwerowi LDAP pełniącemu rolę bramki pośredniczącej między DUA a DSA i konwertującej zlecenia protokołu LDAP do postaci zleceń X.500 (DAP). Sposób komunikacji został zdefiniowany w standardzie LDAP, rozwijanym w grupie roboczej IEFT OSI-DS. Rezultatem były dokumenty RFC 1487 i aktualizacja w RFC 1777 ([6, 7]).

Porównując protokół LDAP w stosunku do standardu X.500 następujące elementy LDAP uznawane były za „lżejsze", określone w sposób bardziej przystępny:

1. Prostszy protokół kodowania.
2. Nazwy i atrybuty stosują tekstowe kodowanie (w X.500 używany jest standard ASN.1)
3. LDAP jest posadowiony bezpośrednio na protokole TCP/IP, ominięto specyfikację całości protokołu OSI.
4. Prosty interfejs programowania (API); w efekcie prac nad LDAPem grupy programistów z University of Michigan opublikowano RFC 1823 ([8]), dokument definiujący zasady konstruowania API (interfejs X/OPEN XDS, preferowane API X.500 jest znacznie bardziej skomplikowane)
5. LDAP opiera się na X.500 w zakresie definicji usługi i rozproszonych operacji, jest specyfikacją protokołu dostępowego, nie kompletnej usługi katalogowej.

Celem, do którego zmierzali autorzy standardu LDAP było powstanie narzędzi wspomagających rozwój interfejsów użytkowych do zasobów X.500 i rozszerzenie zasięgu tych aplikacji. M.in.

użyto LDAPa do zaimplementowania programów współpracujących z usługą `gopher`, `finger`, czy interfejsy poczty elektronicznej, a gdy najpopularniejszą formą dostępu do zasobów informacyjnych stało się WWW w oparciu o LDAP powstała bramka X.500-WWW. Popularność protokołu LDAP rosła, bez wątpliwości dzięki niemu X.500 stało się jedną z istotnych usług sieci Internet.

Skalę popularności LDAP podsumowało ogłoszenie w 1996 roku przez firmę Netscape oraz czterdzieści innych firm integracji swoich produktów z protokołem LDAP. Konsekwencją stał się zataczający coraz szersze kręgi się pogląd, że LDAP jest synonimem „**`Internet Directory`**".

3. Cechy wspólne standardu X.500 i protokołu LDAP

Analizując rekomendacje X.500 oraz protokół LDAP nie trudno zauważyć, że specyfikacje te mają więcej elementów wspólnych niż różnic. Główne punkty styczności dotyczą modelu informacyjnego i standardowych usług. Podstawowa definicja obu produktów zawiera:

1. **Hierarchiczne nazewnictwo**. LDAP na wzór X.500 definiuje hierarchiczną strukturę samej bazy oraz nazw encji umieszczanych w bazie danych, cały model informacyjny LDAPa opiera się na specyfikacji X.500.
2. **Składniki nazw o określonych typach**. Nazwa wyróżniona na każdym poziomie drzewa informacji opisana jest typem atrybutu oraz jego wartością.
3. **Obiekty o określonych typach**. Obiekty reprezentowane są w zasobach X.500 i LDAP jako encje, posiadające typ, zwany klasą obiektów. Typ obiektu jest określany atrybutem „klasa obiektu" (*object class*). X.500 i LDAP stosują wspólną definicję podstawowych klas obiektów.
4. **Atrybuty o określonych typach**. Informacja na temat obiektu jest utrzymywana w postaci zbioru atrybutów, posiadających określone typy. X.500 i LDAP stosują wspólną definicję podstawowych atrybutów.
5. **Operacje bazy danych**. X.500 i LDAP mają wspólny podstawowy zakres operacji dostępu i zarządzania danymi w bazie (`read, compare, search, add, delete, modify`).

4. Rozwój standardu X.500 (1993)

Prace nad specyfikacjami standardu X.500 nie zakończyły się w 1988 roku. Definicję niektórych elementów celowo odłożono na późniejszy okres. Autorzy rekomendacji zdobywali spore doświadczenie obserwując jak rozwijają się produkty programowe implementujące X.500, śledząc problemy dotyczące współpracy pakietów różnych producentów. W efekcie, z opóźnieniem, bo w 1995 roku ukazał się standard tytułowany X.500'93, znacznie wzbogacający możliwości. Najistotniejsze własności nowego standardu to:

1. Technika replikacji oparta na protokole DISP (*Directory Information Shadowing Protocol*); replikacja umożliwia znaczną elastyczność i zwiększa efektywność usługi.
2. Sterowanie dostępem (*Access Control*); opracowano standard określania praw dostępu do wybranych danych.
3. Usprawnienie modelu informacyjnego; wprowadzono podtypy atrybutów, wydzielono atrybuty operacyjne, co pozwala rozróżnić dane użytkowe od informacji wspomagających usługę.
4. Wprowadzono pojęcie obszaru administracyjnego w celu usprawnienia zarządzania danymi; dane mogą być grupowane, w ramach wspólnych obszarów można stosować atrybuty zbiorowe.

Dalsze działania standaryzacyjne doprowadziły do rozbudowania w zakresie obsługi wielojęzyczności zasobów informacyjnych. Wersja '97 zawiera pojęcie kontekstu atrybutu. Jednym z zastosowań kontekstu jest rozróżnianie języka atrybutu. Użytkownik specyfikuje język dostępu i system, w

miarę możliwości, zapewnia mu odpowiednią interpretację wartości atrybutu. Przewidywane jest użycie kontekstu domyślnego, który stosowany jest w przypadku, kiedy niemożliwe jest dostarczenie wartości dla wyspecyfikowanego kontekstu.

5. Rozwój protokołu LDAP

Protokół LDAP również rozwijał się na bazie doświadczeń z pierwszą jego wersją. Od 1996 roku trwały, w ramach grupy roboczej IETF ASID, prace nad kolejną edycją, zwana LDAP version 3. Podstawowe elementy nowego protokołu to:

1. Dostęp do funkcjonalności X.500'93; celem jest umożliwienie oprogramowaniu klienckiemu LDAP korzystania z nowej usługi.
2. Komponenty w zakresie bezpieczeństwa systemu; uwierzytelnianie stron komunikujących się i poufność wymiany informacji dzięki zastosowaniu protokołu SSL (*Secure Socket Layer*).
3. Mechanizm rozszerzalności; taka organizacja bazowego protokołu, by możliwe było dodawanie nowych operacji bez zmian w podstawowych modułach.
4. Odsyłacze (*referrals*); wbudowanie technik przekierunkowania klienta LDAP do innego serwera w celu realizacji zlecenia.

LDAP v. 3 nie wymaga zasobów X.500 dla swojego istnienia. Może być stosowany na dwa sposoby:

- jako uproszczony sposób dostępu do bazy X.500,
- jako mechanizm tworzenia serwerów LDAP, nie będących oczywiście serwerami X.500, ale ze strony użytkowej traktowanych jako abstrakcja serwisu X.500.

Omówione cechy protokołu LDAP v. 3 pokazują, że znacznie wzrasta jego funkcjonalność, co przyczynia się do rosnącej popularności. Właśnie z implementacjami tej wersji protokołu świat Internetu wiąże największe oczekiwania. Niezbędne dla efektywności usługi są nowe elementy: dostępność technik bezpiecznej komunikacji oraz możliwość połączenia i współpracy serwerów LDAP za pomocą odsyłaczy.

Zakres rozbudowy protokołu LDAP w pierwszym etapie nie objął takich funkcji jak operacje rozproszone, czy replikacja. W efekcie pojawiające się implementacje stosują swoje własne mechanizmy, na ogół bardzo podobne do wykorzystywanych w produktach X.500. Takie rozwiązanie prowadzi do niekompatybilności serwisów bazujących na oprogramowaniu różnych firm. Obecnie kontynuowane są prace nad rozbudową specyfikacji LDAPa.

6. X.500 a LDAP

Historia standardu X.500 i protokołu LDAP pokazuje, że LDAP rozwinął się jako protokół dostępowy do X.500. Potrzeba takiej specyfikacji wynikała z kłopotów, jakie napotkali autorzy interfejsów użytkowych do zasobów X.500. Ich implementacja w oparciu o rodzimy protokół X.500 DAP została oceniona jako trudna, a produkty bazujące na DAPie wymagały zbyt wiele zasobów. Cały standard X.500, typowy przykład rekomendacji OSI, świat Internetu uznał za przeciążony, skomplikowany, intensywnie wykorzystujący zasoby komputerowe. Produktom opartym na X.500 zarzucano niedojrzałość i duży stopień trudności w trakcie instalacji i konfiguracji. Jednocześnie prace nad modyfikacją standardu postępowały wolno, istotną przeszkodą był długi czas ratyfikacji wszelkich dokumentów ukazujących się pod szyldem OSI. Technologia „*top-down*" stosowana w rekomendacjach OSI wychodziła pokonana w konkurencji ze specyfikacjami pojawiającymi się w Internecie, gdzie krok po kroku, metodą „*bottom-up*" konstruowano kolejne składniki systemów, by w efekcie uzyskać sprawny i wydajny system w czasie zdecydowanie krótszym.

Rozwój LDAPa z jednej strony zmierza w kierunku, który wskazuje na dążenie do odcięcia się od standardu X.500, a dokładnie od implementacji opartych na X.500 – dodefiniowywane są elementy, które obecnie są realizowane przez X.500 (zdalne operacje, replikacja). Z drugiej strony wszelkie działania realizowane są na wzór doświadczeń uzyskanych w fazie eksploatacji X.500 i nie przewiduje się definitywnego zerwania z produktami X.500.

W dziedzinie systemów informatycznych ważna jest zawsze dobra specyfikacja zagadnienia, nie ma jednak pożytku z modelu i projektu, jeśli nie powstanie odpowiednie oprogramowanie. „Odpowiednie" nie znaczy wyłącznie dobrze przygotowane i wiernie implementujące projekt. Musi być ono również łatwo dostępne, co, w środowisku akademicko-naukowym, oznacza na ogół bezpłatne. Tylko dzięki temu, że pakiet `Quipu` dostępny był za darmo możliwe było uruchomienie projektu X.500 w Polsce. Obecnie, ośrodki pragnące posiadać produkt implementujący standard X.500'93 muszą za takie oprogramowanie zapłacić. Ogranicza to bardzo zasięg usługi i wprowadza znaczne ograniczenia w jej rozwoju. Nadal dostępne bezpłatne oprogramowanie `Quipu` (X.500'88) nie jest rozwijane od 1992 roku i brakuje wersji na aktualne platformy systemowe. Pakiet LDAP zrealizowany przez programistów University of Michigan jest ogólnodostępny, niestety, nie jest zgodny z aktualną wersją standardu.

To jak rozwijać się będzie oprogramowanie będzie w znacznym stopniu decydować w jakim kierunku toczyć się będą losy usługi katalogowej.

7. Oprogramowanie X.500

W trakcie prac w dziedzinie serwisu X.500 mieliśmy do czynienia z oprogramowaniem `Quipu` w wersji ogólnodostępnej (pakiet `Isode-8.0`), następnie wykorzystywaliśmy produkt firmy Isode, `IC`. Obecnie Isode wymaga opłaty subskrypcji, która pozwala na otrzymywanie w ciągu roku dostępu do kolejnych edycji oprogramowania. Najnowsza, ogłoszona ostatnio wersja to `ICR4`. Ostatnią edycją, nad którą pracowaliśmy było `ICR3.2`. Nasze doświadczenia z eksploatacji pakietu są duże, tym bardziej, że wielokrotnie w pracach rozwojowych niezbędne było zrozumienie fragmentów kodu źródłowego. Oceniamy, że faza kompilacji, instalacji i konfiguracji nie powinna przynieść większych trudności osobom mającym związek ze środowiskiem Unix i z technikami adaptacji oprogramowania.

Począwszy od wersji R3 pakiet `IC` implementuje standard X.500'93. Wnosi to sporo istotnych zmian w samą usługę i sposoby zarządzania. W tym celu zostały znacznie rozbudowane moduły zarządzania systemem – wszystkie działania odbywają się poprzez interfejsy graficzne. Pakiet `IC` bardzo się rozrasta, zwiększają się też wymagania sprzętowe. W celu kompilacji oprogramowania potrzebna jest instalacja innych pakietów, przede wszystkim graficznych. Począwszy od wersji R4 zapowiadana jest możliwość uzyskania binariów na popularne platformy.

W maju 1997 roku wzięliśmy udział w międzynarodowych testach oprogramowania X.500'93, prowadzonych przez organizację DANTE, nadzorującą usługę X.500 w Europie (projekt NameFLOW-Paradise). W kilku instytucjach na świecie zostały wystartowane serwery pracujące na oprogramowaniu implementującym X.500'93 oferowanym przez różnych producentów. Serwery te kontaktowały się między sobą oraz ze światem zewnętrznym. W Toruniu uruchomiono dwa serwery: poziomu krajowego oraz serwer Uniwersytetu Mikołaja Kopernika w Toruniu. Doświadczenia zdobyte w trakcie eksperymentu można podsumować następująco:

1. Translacja zasobów w formacie `Quipu` do postaci wymaganej przez serwis X.500'93 nie sprawia większych kłopotów.
2. Uzyskana w wyniku konwersji baza najprawdopodobniej (sądząc po szybkości przeszukiwania zasobów) ma mało efektywnie ustawione prawa dostępu do encji.
3. Ustalanie praw dostępu wymaga dogłębnej znajomości problemu, nie jest łatwe.
4. Współpraca poprzez odsyłacze (*referrals*) i łańcuchowanie (*chaining*) funkcjonuje prawidłowo.

5. Realizacja mechanizmu replikacji jest uciążliwa, konieczne są wzajemne uzgodnienia stron oraz wymagane jest zatrzymanie serwera w trakcie rekonfiguracji.
6. System, w testowanej postaci, wykazywał małą efektywność, okres oczekiwania na wyniki zleceń był zdecydowanie zbyt długi (może to wynikać nie z cech oprogramowania, lecz postaci bazy, którę stosowaliśmy do testów).

Obecnie przewidujemy kontynuacje działań związanych z oprogramowaniem IC. Planowanie jest wykorzystanie pakietu w wersji ICR4 i modelu X.500'93 w usłudze X.500 prowadzonej na Uniwersytecie Mikołaja Kopernika w Toruniu. W szczególności interesować nas będą problemy ustalania praw dostępu i tworzenia domen administracyjnych.

Warto wspomnieć, że autorzy najnowszej wersji pakietu ICR4.0 twierdzą, że przeprowadzone testy efektywnościowe wskazują znaczne udoskonalenie oprogramowania. M.in. operacje odczytu i wyszukania są około trzy razy szybsze niż w poprzedniej wersji, bardziej wydajny jest również LDAP. Podawane są także porównania w stosunku do wyników publikowanych przez firmę Netscape dla Directory Server'a – około dwukrotnie większa wydajność.

8. Oprogramowanie implementujące protokół LDAP

Pakiet ldap-3.3

Najpopularniejszym oprogramowaniem implementującym LDAP jest udostępniany bezpłatnie pakiet LDAP, napisany przez grupę z University of Michigan. Ostatnia edycja to ldap-3.3. Jest on również częścią składową dystrybucji Isode (oprogramowanie X.500, obecna wersja to ICR4). Implementacja ta, mimo numeracji 3.3, opiera się na standardzie LDAP v. 2, ale posiada wbudowane elementy obsługi współpracy serwerów oraz realizacji replikacji pomiędzy serwerami. Oprogramowanie ldap-3.3 dostarcza serwer ldapd, biblioteki wspomagające oraz programy klienckie, służące do przeglądania i modyfikacji zasobów. Jest również możliwe uruchomienie samodzielnego serwera, zwanego slapd (*stand-alone* LDAP *daemon*), który zarządza własną bazą danych, wzorowaną na modelu X.500. Zasoby wykorzystywane przez slapd mogą mieć następującą postać:

1. LDBM – efektywna baza dyskowa, oparta na czterobajtowych unikalnych identyfikatorach, stosowanych do wskazywania konkretnych encji w zasobach; dopuszcza się stosowanie indeksów wygenerowanych dla wybranych atrybutów (w celu optymalizacji operacji przeszukiwania bazy).
2. SHELL – interfejs bazy danych do komend UNIXa czy skryptów powłoki, po odebraniu zapytania wykonywana jest odpowiednia komenda, lub skrypt.
3. PASSWD – baza oparta na pliku haseł w systemie UNIX.

W skład pakietu wchodzi również serwer replikacji – slurpd, uruchamiany na tej samej stacji co slapd i odpowiedzialny za propagowanie zmian do podporządkowanych (na zasadzie wzajemnych uzgodnień) serwerów.

Usługa katalogowa wykorzystująca pakiet ldap-3.3 może być zrealizowana na różne sposoby:

1. LDAP jako serwis lokalny. Oznacza to, że uruchamiany jest serwer slapd, który zarządza lokalną bazą danych, nie kontaktuje się z innymi serwerami. Jest to postać usługi zalecana w fazie testowej, czy eksperymentalnej, lub w przypadku, gdy celem jest oferowanie dostępu do lokalnych zasobów.
2. LDAP jako serwis lokalny z możliwością kontaktu z innymi serwerami. W tej konfiguracji uruchamiany jest zarówno serwer slapd jak i ldapd. Serwer ldapd daje dostęp do świata X.500. Możliwe jest również zrezygnowanie ze stosowania własnego serwera, w sytuacji, gdy jest znany odpowiedni serwer ldapd, który może zostać wskazany jako usługodawca w zakresie X.500.

3. LDAP jako interfejs dostępowy (*front-end*) do X.500. Jest to jedno z typowych zastosowań LDAPa, polegające na stosowaniu serwera `ldapd` jako pośrednika translującego zapytania klienta LDAP do postaci X.500.
4. Replikowana usługa `slapd`. Oznacza stosowanie serwera `slurpd` do propagowania zmian do jednego lub więcej serwerów `slapd` (technika *master-slave*). Ten typ usługi może być stosowany w połączeniu z dwiema pierwszymi konfiguracjami.

Zarządzanie bazą danych `slapd` może odbywać się poprzez interfejsy klienckie, jest to dobra metoda w przypadku małych modyfikacji zasobów. Istnieją również narzędzia przeznaczone do operowania bezpośrednio na bazie, *off-line*. Do reprezentacji encji (*entries*) w prostej postaci tekstowej stosowany jest format LDIF (LDAP *Data Interchange Format*), zdefiniowany w dokumencie Internet-Draft [9]. W pakiecie `ldap-3.3` istnieją programy translacji tego formatu do postaci DBM, czy tworzenia na ich podstawie plików zawierających indeksy atrybutów. Opracowano także narzędzia do konwersji plików EDB, stosowanych w serwisie X.500 opartym na `Quipu`, do plików LDIF. Baza danych `slapd` może być wystarczająca tylko w przypadku stosowania odseparowanych zasobów informacyjnych.

Jeżeli wymagana jest komunikacja z innymi serwerami `slapd` tworzone są tzw. *referral entries*, czyli encje będące odesłaniem do innego serwera. Muszą one zawierać atrybut *`ref`*, któremu jest przypisywany identyfikator URL odpowiedniego serwera.

Netscape Directory Server

Firma Netscape dostarcza wśród swoich produktów wiele typów serwerów, m.in. `Messaging Server`, `Collabra Server`, `Proxy Server`, `Certificate Server`, a również `Directory Server`. Integralną częścią serwera każdego typu jest serwer administracyjny – `Netscape SuiteSpot`, wspomagający proces zarządzania. Produkt ten jest tak zaprojektowany, że większość operacji odbywa się poprzez zestaw odpowiednich formularzy i programów wykonywanych w odpowiedzi na zlecenie. Niewielka ilość funkcji dostępna jest spoza przeglądarki. Obecnie firma Netscape umożliwia pozyskanie wersji `Directory Server 3.1`. Ponieważ ukazała się ona w ostatnich dniach nasze doświadczenia dotyczą edycji 3.0. Oprogramowanie jest oferowane na okres 60 dni, w formie wersji eksperymentalnej. Istnieją implementacje na większość popularnych platform systemowych, m.in. Solaris, Digital-Unix, HP-UX, AIX, IRIX, Windows NT.

Testowa instalacja pakietu `Netscape Directory Server 3.0`, posłużyła nam jako platforma oceny możliwości przejęcia przez ten system obsługi zasobów katalogowych, udostępnianych obecnie w oparciu o oprogramowanie firmy Isode `ICR3.2` (realizuje ono standard X.500). Podstawowym celem eksperymentu było stwierdzenie na ile proste jest przeniesienie istniejącej usługi X.500 oraz ocena kompatybilności serwisów obu typów.

Sama instalacja pakietu `Netscape Directory Server` jest stosunkowo prosta. Następnie należy za pomocą `SuiteSpot`'a przeprowadzić konfigurację. Wymaga ona znajomości zagadnienia obsługi zasobów katalogowych (dostarczana jest bogata dokumentacja). Serwer administracyjny może współpracować na podstawie protokołu LDAP z serwerami `ldapd` lub kontaktować się z lokalnie uruchamianym serwerem `ns-slapd`, który jest eksploatowany w sposób bardzo podobny do tego, z czym mamy do czynienia w pakiecie `ldap-3.3`. Serwer `ns-slapd` powinien zostać skonfigurowany odpowiednio do potrzeb środowiska. Przede wszystkim można rozbudować obowiązującą postać informacji umieszczanej w zasobach bazy danych, rozszerzyć klasy obiektów, czy typy atrybutów. Ta operacja realizowana jest w serwerze za pomocą zestawu formularzy. W ten sposób dodawane są definicje tzw. „polskich" klas obiektów i atrybutów (podobna była procedura postępowania w przypadku pakietu `Quipu`). Temat projektu realizacji usługi X.500 dla potrzeb środowiska Polski omawiają prace [10, 11, 12]. `Directory server` stosuje, podobnie jak `ldap-3.3`, LDAP *Data Interchange Format* (LDIF) w celu przedstawiania encji w zasobach katalogowych. Dotyczy to zarówno encji wprowadzanych do zasobów jak i formy ich prezentacji. Format LDIF pozwala również na przygotowanie danych do modyfikacji zasobów. Pliki w formacie LDIF mogą zostać przygotowane

w dowolny sposób, chodzi tu o utworzenie odpowiednich zbiorów tekstowych. Warto zauważyć fakt, że wszystkie dane katalogowe są zapamiętywane wewnętrznie przy użyciu kodowania UTF-8, co oznacza, że pliki LDIF stosują ten typ kodów. Usługa katalogowa uruchamiana w Polsce musi zakładać umieszczanie w zasobach danych polskojęzycznych. Do tego celu należy wykorzystać tzw. znaczniki językowe (*language tags*), które mogą wystąpić po typie konkretnego atrybutu w linii pliku LDIF określającego wskazaną atrybutem *dn* encję. Zabronione jest natomiast stosowanie znaczników językowych dla jednoznacznych nazw obiektów. Właściwa nazwa encji musi być przedstawiona, podobnie jak to miało miejsce w zasobach X.500, jako jedna konkretna nazwa, nie są możliwe wielowartościowe *dn*'y rozróżniane poprzez język (taka technika została wprowadzona w standardzie X.500'97). O konsekwencjach tak przyjętego modelu pisaliśmy w pracach [10, 11] i w efekcie została zaprojektowana odpowiednia postać systemu. Rozwiązanie zaprezentowane we wskazanych opracowaniach może zostać przeniesione na płaszczyznę `Netscape Directory Server`'a. Z punktu widzenia wewnętrznej organizacji zasobów wymaga ono rozbudowania tablic klas obiektów oraz atrybutów, następnie w fazie wprowadzania i modyfikacji zasobów należy pamiętać o umieszczaniu w opisie encji polskich atrybutów. Zgromadzenie informacji w rodzimym języku to nie wszystko. Należy dysponować interfejsami użytkownika, które przedstawią wyszukiwane w bazie informacje we właściwej postaci, czyli obsłużą polskie atrybuty. Sam serwer nie zawiera modułów przeglądania danych, które zadowoliłyby polskiego użytkownika, również przeglądarka Netscape, nie jest w stanie jako odpowiedź udostępnionej operacji „`Directory Search`" zaprezentować wyniki w odpowiedniej formie. Zaimplementowany przez nas program stanowiący bramkę pomiędzy X.500 a WWW („spolszczony" `Web500gw` F. Richtera z Politechniki w Chemnitz) wykorzystuje protokół LDAP jako warstwę pośrednią do zasobów X.500. Zasada działania tego programu jest zgodna z zaleceniami tworzenia aplikacji LDAPowskich, jest oparta o LDAP API. Wydaje się, że dostosowanie tego programu do współpracy z serwerem `ns-slapd` byłoby stosunkowo łatwe.

Jeżeli zakładać przeniesienie istniejącej usługi X.500 z oprogramowania `Quipu` na `Netscape Directory Server` konieczne jest przełożenie zasobów z postaci `Quipu` do formatu stosowanego przez ten serwer. Translacja taka jest bardzo prosta, należy ją dokonać dwustopniowo: najpierw konwertujemy drzewiasto zlokalizowane dane `Quipu` do postaci pliku LDIF. Ponieważ dane w X.500 stosują kody T.61 należy zastosować przekodowanie do UTF-8. Tak przygotowane zasoby umieszczone w pliku LDIF mogą już zostać przekazane odpowiednim modułom odpowiedzialnym za dodawanie encji. Narzędzia stosowane przy translacji zasobów nie są dostępne, administrator musi przygotować skrypty wykonujące potrzebne operacje. Można tu również wykorzystać oferowane w pakiecie `ldap-3.3` programy obsługi zasobów.

Serwis katalogowy oparty na pakiecie `Netscape Directory Server` musi nadal funkcjonować jako fragment globalnej usługi. Oznacza to możliwość komunikowania się z innymi serwerami oferującymi dane informacyjno-adresowe. W ramach serwera `ns-slapd` jest to realizowane za pomocą odsyłaczy (*refferals*). Po pierwsze stosowany jest odsyłacz określony w pliku konfiguracyjnym jako punkt kontaktowy, w przypadku, gdy zadano pytanie dotyczące encji nie rezydującej na serwerze, jest on przekazywany stronie klienckiej, która odpowiednio wykorzystuje informacje. Poza tym, gdy strona kliencka poszukuje określonej encji, lub pragnie ją modyfikować może zostać zwrócony odsyłacz, który został wprowadzony do bazy danych jako encja klasy obiektów *referral* (*smart refferal*).

Oprogramowanie `Netscape Directory Server` przewiduje również replikacje wskazanych części drzewa informacyjnego. Mechanizm ten funkcjonuje na podstawie wzajemnych uzgodnień i stosuje model podobny do X.500.

Wnioski z przeprowadzonych testów

Przeprowadzone prace testowe pokazały, że przeniesienie obecnie eksploatowanej bazy X.500 na platformę opartą na protokole LDAP nie powinno napotkać większych problemów. Jeśli założyć, że kierunek w jakim zmierzają obecnie aplikacje sieciowe będzie kontynuowany, czyli rozwijane będą systemy zintegrowane z protokołem LDAP świadczenie usługi katalogowej w tej postaci stanie się

niezbędne. Oczywiście można stosować serwer `ldapd` jako pośredniczący między klientem i serwerem X.500, ale z drugiej strony, jeśli fakty pokażą, że stosowanie LDAPa do zarządzania bazą danych jest efektywniejsze będzie trzeba pójść w tym kierunku. Zasadniczą przyczyną problemów, jakąkolwiek drogę wybierzemy, może być prawdopodobnie pozyskanie odpowiedniego oprogramowania. Tendencje panujące na rynku wskazują, że zabraknie firm, czy grup programistów oferujących swoje produkty za darmo. Ostatnia wersja pakietu `ldap-3.3` pochodzi z 1996, jeden z głównych programistów, Tim Howes, przeszedł do firmy Netscape, która dostarcza pakiet bezpłatnie na okres 60 dni, a w celu uzyskania licencji pełnej należy wnieść odpowiednie opłaty.

9. Podsumowanie

Wyniki doświadczeń zdobytych w trakcie przeprowadzonych prac będą wykorzystywane dla potrzeb polskiego projektu X.500. Nie można przeoczyć szansy jaka pojawia się obecnie, gdy większość produktów zmierza do integracji z usługą katalogową. Te okoliczności sprzyjają tworzeniu dobrych narzędzi, dzięki którym będzie znacznie łatwiejsze tworzenie interfejsów użytkownika. Godne uwagi są dostępne już pakiety `Netscape Directory SDK` i `Netscape LDAP Java SDK`. Pierwsze próby implementacji w oparciu te biblioteki pokazały, że są to narzędzia bardzo wygodne. Nie można również pominąć inicjatywy o nazwie `Java Naming and directory interface - JNDI (http://jaca.sun.com/products/jndi)`. Jest to specyfikacja rozwinięta przez *JavaSoft* w celu wbudowania w aplikacje Javy interfejsu dostępu do zasobów katalogowych.

Literatura

[1] Data Networks and Open System Communications: *Directory*, ITU-T Recommendations X.500-X.525

[2] D. Chadwick, *Understanding X.500. The Directory.* Chapman & Hall 1994 (`http://www.salford.ac.uk/its024/X500.htm`)

[3] D. Goodman, C. Robbins, *Understanding LDAP and X.500* (`http://www.eema.org./understanding_ldap.html`)

[4] S. Kille, *LDAP and X.500*, First published i Messaging Magazine, September 1996

[5] Raporty i prace na temat projektu X.500 w Polsce: `http://ocelot.uni.torun.pl/raporty_pl.html`

[6] W. Yeong, T. Howes, S. Kille. *X.500 Lightweight Directory Access Protocol*. RFC1487

[7] W. Yeong, T. Howes, S. Kille, *Lightweight Directory Access Protocol*, RFC1777

[8] T. Howes, M. Smith, *The LDAP Application Program Interface,* RFC1823

[9] *The LDAP Data Interchange Format (LDIF)* – Technical Specification, Filename: `draft-ietf-asid-ldif-02.txt`, 30.07.1997

[10] M. Górecka, T. Wolniewicz, *Dostosowanie bazy X.500 do specyfiki języka lokalnego*, materiały konferencyjne, Miedzeszyn'96

[11] M. Górecka, T. Wolniewicz, *Nazewnictwo obiektów w rozproszonej międzynarodowej bazie X.500*, maj 1997, materiały konferencyjne Miedzeszyn'97.

[12] M. Górecka, T. Wolniewicz, *Use of national languages in X.500 Directory*, listopad 1996, materiały konferencyjne Bled, Słowenia, konferencja robocza n.t. standardu Unicode.

[13] M. Górecka, T. Wolniewicz, *Najnowsze tendencje w dostępie do zasobów adresowo-informacyjnych — protokół LDAP a X.500*, kwiecień 1998, Poznań, materiały konferencyjne POLMAN'98.