System centralnej autentykacji użytkowników - wdrożenie i administrowanie na klastrze komputerowym WCSS.

Bartłomiej Balcerek, Wrocławskie Centrum Sieciowo-Superkomputerowe

Dokument przedstawia procedurę wdrożenia oraz sposoby zarządzania systemem autentykacji użytkowników opartym o centralną bazę LDAP, jak i cele i założenia tego projektu.

1. Założenia i cele wdrożenia

W skład klastra komputerowego UKŁAD Wrocławskiego Centrum Sieciowo-Superkomputerowego wchodzą 32 komputery: 1 serwer dostępowy, plików i usług, 22 węzły liczące (typu PC i Intel Itanium), wszystkie w postaci typu "rack", zamontowane w szafie, oraz 9 węzłów liczących PC, wolnostojących, wyposażonych w karty wspomagające grafikę 3D, monitory 19" i konsole. Węzły te, prócz funkcji obliczeniowych, stanowią laboratorium multimedialne i mogą być wykorzystane do prowadzenia zajęć, warsztatów lub prezentacji. Powszechnie znajdują też zastosowanie jako terminale dostępowe użytkowników do wszystkich zasobów działu Komputerów Dużej Mocy (KDM). Założeniem obowiązującym od chwili powstania klastra jest, by dostęp do każdej z maszyn UKŁADu byl identyczny, tj. aby każdy użytkownik miał konto o takiej samej nazwie, haśle dostępu i innych parametrach na każdym z komputerów klastra. Założenie to pierwotnie realizowane było poprzez standardowy system autentykacji użytkowników w systemach uniksowych, oparty na danych o kontach przechowywanych w plikach tekstowych: nazw użytkowników (/etc/passwd), haseł (/etc/shadow) oraz grup (/etc/group). Dotychczasowe rozwiązanie zastosowane w klastrze UKŁAD polegało na replikowaniu takiej bazy danych, utrzymywanej i zarządzanej na serwerze dostępowym, na wszystkie węzły klastra z zadaną częstotliwością (przyjęte zostało 30 minut). Rozwiązanie to posiadało istotne wady, m.in.:

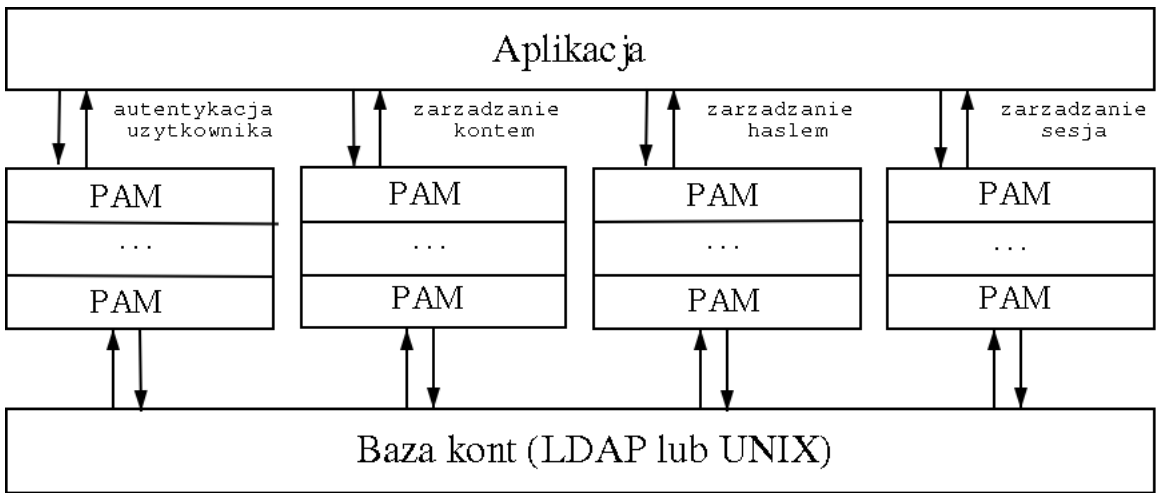
- Użytkownik, po uaktualnieniu swoich danych w bazie serwera (np. dotyczących domyślnej powłoki lub hasła) nie mógł natychmiast korzystać z efektów tych zmian na węzłach, a dopiero, maksymalnie po okresie do kolejnej synchronizacji.
- Silne obciążenie którejś z maszyn liczących wydłużało zakończenie całego procesu uaktualniania danych.

- Generowany okresowo ruch w sieci UKŁADu zakłócał wyniki pomiarów parametrów komunikacji używanych na klastrze programów dokonujących obliczeń równoległych.
- Proces synchronizacji generował obciążenie na serwerze, jak i węzłach obliczeniowych.

Głównym celem wdrożenia nowego rozwiązania miało być wyeliminowanie powższych niedogodności. W lipcu 2003 zaproponowane zostalo wdrożenie systemu autentykacji użytkowników opartego na jednej, centralnej bazie danych, pozbawionego wymienionych wad i spełniającego założenie o zunifikowanym dostępie.

2. System PAM-LDAP

Za podstawę rozwiązania obrany został projekt: "Using OpenLDAP For Authentcation" [3] opracowany z myślą o dystrybucji Linux Mandrake. Wybrany system autentykacji opiera się na wykorzystaniu, jednej w skali klastra, bazy danych o kontach. Do informacji przechowywanych w bazie LDAP aplikacje odwołują się poprzez biblioteki NSS (Name Serwer Switch) i moduły PAM (Pluggable Authentication Modules), które to moduły stanowią warstwę pośredniczącą w autentykacji. Na rysunku poniżej przedstawiono ogólny schemat interakcji modulów PAM z aplikacjami oraz bazami danych o kontach (rys. 1).



Moduł PAM można rozpatrywać w aspekcie biblioteki funkcji, z których korzysta aplikacja dokonująca autentykacji oraz dalszych etapów logowania (wymienionych na rysunku) poprzedzających udzielenie dostępu użytkownikowi do zasobów systemu. Komunikacja pomiędzy aplikacją a modułem PAM odbywa się poprzez standardowe API, a więc istnieje dowolność w rozwoju i tworzeniu samych modułów PAM, w tym w wyborze źródeł danych z informacjami o kontach użytkowników. Aplikacja odwołuje się do modułów PAM zgodnie z ich konfiguracją zawartą w odpowiednich plikach. Skonfigurować można zestaw modułów, kolejność ich przetwarzania, oraz znaczenie dla całej procedury logowania. Standardowo, zdecydowana większość systemów uniksowych wykorzystuje moduły PAM sprzężone z bazami danych w postaci plików tekstowych. W nowo wdrożonym systemie stosuje się hierarchiczną bazę danych w standardzie LDAP (Lightweight Directory Access Protocol) i darmowej implementacji OpenLDAP. Wykorzystano moduły firmy PADL Software [1].

Część powszechnie wykorzystywanych przez użytkowników aplikacji wymaga informacji dotyczących kont do celów innych niż autentykacja. Takie programy odwołują się do funkcji systemowych, najczęściej w poszukiwaniu powiązań pomiędzy numerami porządkowymi użytkowników czy grup a ich nazwami (np. polecenie "ps u"). Ustalenie źródeł takich danych odbywa się poprzez konfigurowanie mechanizmu NSS. Na UKŁADzie zainstalowane zostały biblioteki LIBNSS-LDAP, skonfigurowane do przekazywania danych pobieranych z bazy LDAP.

3. Procedura wdrożenia

1. Przygotowanie i instalacja pakietów w formacie dystrybucji Linux Debian. Użyto systemu OpenLDAP w wersji 2.1.22-1 i modułów PAM-LDAP w wersji 164-1, bibliotek LIBNSS-LDAP, wersji 211-1 oraz pakietu skryptów Migrationtools 44-6. Aplikacje OpenLDAP, PAM-LDAP i LIBNSS-LDAP zostały skompilowane i z wynikowych plików binarnych utworzone zostały pakiety instalacyjne w formacie .deb. Pakiet źródeł OpenLDAP posłużył do przygotowania dwóch rodzajów pakietów binarnych. Pakiet o nazwie "openldap", zawierający biblioteki, programy-demony udostępniające usługi bazodanowe oraz programy klienckie bazy danych, zainstalowany został na serwerze klastra. Pakiet "libldap2", o nazwie wybranej dla zachowania kompatybilności z nazewnictwem przyjętym w systemie pakietów Debiana, przeznaczony został do instalacji na węzłach klastra. Zawiera on oprogramowanie klienckie bazy danych oraz wykorzystywane przez nie biblioteki funkcji. Na etapie konsolidacji binarnej części pakietu "opanldap" - pliku demona "slapd" istotna była kolejność dołączania bibliotek funkcji - pierwszą biblioteką udostępniającą funkcję systemową "crypt()" musiała być biblioteka "libcrypt". Standardowo dołączana jako pierwsza biblioteka "libssl" dostarczała funkcję "crypt()" niekompatybilną z aktualnym sposobem kodowania haseł w pliku /etc/shadow. Pakiety PAM-LDAP i LIBNSS-LDAP zostały zainstalowane na każdej z maszyn klastra.
2. Konfigurowanie serwera OpenLDAP. Cały system bazy danych zainstalowany został na zewnątrz wyodrębnionego dla użytkowników środowiska ("CHROOT"). Głównym celem było tu odseparowanie części systemu plików dostępnej dla użytkowników od plików bazy danych, które to mają krytyczne znaczenie dla bezpieczeństwa całego systemu. Demon bazy danych - "slapd" pobiera ustawienia z pliku /etc/ldap/slapd.conf. Zgodnie z zawartą tam konfiguracją demon obsługuje jedną bazę danych, w domenie "kdm.net". Jako format składowania danych (backend) wybrany został prosty schemat "ldbm". Pliki bazy danych przechowywane są w katalogu /var/lib/ldap. W pliku slapd.conf zawarta jest także konfiguracja szyfrowanych tunelów TLS, która będzie opisana w punkcie 6. Czynności opisane w dalszych punktach wykonywane były wewnątrz przestrzeni wydzielonej dla użytkowników ("CHROOT").
3. Migrowanie danych. Przeniesienie danych o kontach do nowej bazy danych. Wykorzystane zostały skrypty języka PERL z pakietu Migrationtools. Katalogiem zawierającym skrypty jest /usr/share/migrationtools. Konfiguracje dla skryptów ustala się w pliku /usr/share/migrationtools/migrate_common.ph. Wykorzystane były 3 skrypty migrujące dane. Przy użyciu skryptu "migrate_base.pl" tworzy się główne katalogi w bazie danych, skrypty "migrate_group.pl" i "migrate_passwd.pl" przenoszą do tych katalogów odpowiednie dane. Bezpośrednim efektem działania skryptów są pliki typu "ldif", czyli wejściowe dla narzędzi operujących na bazie LDAP. Poniżej umieszczono przykład użycia jednego ze skryptów.

Przykład 1. Przenoszenie danych o nazwach kont i hasłach:

```
CHROOT uklad: export ETC_SHADOW=/etc/shadow

CHROOT uklad: migrate_passwd.pl /etc/passwd passwd.ldif

CHROOT uklad: ldapadd -x -D "cn=root,dc=mylan,dc=net" -W -f passwd.ldif
```

4. Konfigurowanie klientów bazy. Moduły PAM podczas komunikacji z centralną bazą danych korzystają z konfiguracji zawartej w plikach /etc/ldap.conf. Na serwerze klastra, klient bazy LDAP uruchomiony z prawami superużytkownika systemu operacyjnego automatycznie uzyskuje prawa administratora bazy, pobierając odpowiednie hasło z pliku /etc/ldap.secret. Takie rozwiązanie gwarantuje możliwość modyfikowania bazy LDAP przez moduły PAM i służy wygodzie ręcznego operowania na bazie LDAP przez administratorów. Ze względów bezpieczeństwa przyjęto, że hasła nie będą przechowywane na maszynach klienckich. Klienci PAM-LDAP skonfigurowani są tak, aby przy połączeniu dokonywać autentykacji serwera, co opisane zostało w punkcie 6.
5. Ustalenie konfiguracji serwisu NSS. Zainstalowane biblioteki LIBNSS-LDAP zapewniają mapowanie nazw użytkowników i grup na numery UID i GID. Konfiguracja mechanizmu NSS zawarta jest w plikach /etc/nsswitch.conf, biblioteki LIBNSS-LDAP korzystają z konfiguracji zapisanej w plikach /etc/ldap.conf.
6. Konfigurowanie modułów PAM i zapasowej bazy haseł. Jak wspomniano w punkcie 2, skonfigurowanie modułów PAM obejmuje ustalenie zestawu modułów, kolejności ich przetwarzania oraz znaczenia poszczególnych modułów w procedurze logowania. Wszystkie te ustawienia przechowywane są w plikach odpowiadających nazwom aplikacji, w katalogu /etc/pam.d. Konfiguracja została wybrana tak, żeby przy zachowaniu możliwie wysokiego poziomu bezpieczeństwa zapewnić możliwość logowania się także przy braku połączenia z centralną bazą LDAP. Główne założenia co do konfiguracji można sformułować następująco:
   - Podstawowym źródłem danych do autentykacji wszystkich aplikacji zainstalowanych na węzłach i przystosowanych do współpracy z modułami PAM jest centralna baza LDAP.
   - W wypadku niedostępności centralnej bazy danych, pobierane są informacje z lokalnych, standardowych baz w plikach tekstowych.
   - Dąży się do zachowywana pełnej zgodności danych pomiędzy centralną bazą a bazami lokalnymi.
   - Baza danych może być modyfikowana tylko z poziomu serwera zarządzającego.

   Moduły PAM dokonują na bazach kont zarówno operacji odczytu, jak i zapisu. Modułami modyfikującymi te dane są moduły typu "passwd". Zgodnie z wymienionymi założeniami wszystkie typy modułów (auth, account, session, passwd) skonfigurowane są do korzystania z dwóch źródeł danych, podstawowego i zapasowego. W przypadku, gdy moduł PAM-LDAP nie może przeprowadzić logowania, np. gdy połączenie z bazą jest niedostępne, lub podane hasło jest nieprawidłowe, kontrola przekazywana jest do standardowych modułów PAM-UNIX. Z przyczyn technicznych niemożliwe było zaprogramowanie, w prosty sposób, rozróżniania przez system

przypadków podania błędnego hasła i niedostępności bazy LDAP, dlatego ważne, głównie ze względów bezpieczeństwa, jest zachowywanie zgodności pomiędzy wszystkimi bazami danych. Tekstowa baza na serwerze zarządzającym, modyfikowana jednocześnie z bazą LDAP, rozprowadzana jest po węzłach klastra jeden raz dziennie.

7. Skonfigurowanie tunelów szyfrowanych dla połączeń z serwerem bazy danych. Dla zapewnienia większej poufności danych przesyłanych pomiędzy serwerem a klientami LDAP, zdecydowano się na wprowadzenie szyfrowania treści połączeń. Wykorzystany został protokół TLS (Transport Layer Security), zaprojektowany w oparciu o metody kryptografii asymetrycznej. Zestawienie tunelu szyfrowanego zaczyna się od pobrania przez system kliencki certyfikatu serwera, zawierającego jego klucz publiczny. Zaszyfrowane z wykorzystaniem klucza publicznego, wysyłane do serwera dane, są podstawą do szyfrowania metodą symetryczną w dalszej w części transmisji. Podczas uruchomienia demon LDAP sprawdza autentyczność certyfikatu serwera, odwołując się do certyfikatu CA (Certificate Authority), którym jest tutaj Polskie Centrum Certyfikacji EuroPKI. Klucz prywatny serwera znajduje się w pliku /etc/ssl/private/uklad.key, jego certyfikat w /etc/ssl/certs/uklad.cert a certifikat CA w /etc/ssl/certs/ca.cert. Wymienione dane, ze względu na duże znaczenie dla bezpieczeństwa mieszczą się na zewnątrz przestrzeni dostę?nej dla użytkowników. Komputery klienckie skonfigurowane są do dokonywania autentykacji serwera przy nawiązywaniu połączenia, w oparciu o posiadany certyfikat (klucz publiczny) CA przechowywany w /etc/ssl/certs/ca.cert, wewnątrz przestrzeni "CHROOT".

4. Administrowanie systemem

4.1. Narzędzia

W celu ułatwienia i zautomatyzowania zarządzania bazami kont utworzono narzędzia skryptowe. Ponieważ najbardziej popularne, dostępne w sieci Internet, darmowe narzędzia przetestowane w warunkach klastra UKŁAD, nie spełniły wszystkich oczekiwań, zdecydowano się na stworzenie nowych narzędzi od podstaw. Skrypty umiejscowione są w katalogu /root/bin, na zewnątrz środowiska "CHROOT", na serwerze klastra.

1. Narzędzie synchronizujące bazę LDAP ze standardową bazą haseł: **sync_pwdbs.sh**. Skrypt porównuje listy użytkowników przechowywane w obu bazach i w razie stwierdzenia różnic pomiędzy nimi, dokonuje modyfikacji bazy LDAP, tak żeby uzyskać zgodność obu baz, z dokładnością do listy użytkowników. Działanie obejmuje skasowanie, jak i dodawanie nowych rekordów do bazy LDAP. W przypadku ustalenia zgodności danych w bazach, program kończy działanie nie wypisując żadnych komunikatów.
2. Narzędzie synchronizujące dane o grupach użytkowników: **sync_group.sh**. Skrypt działa analogicznie do opisanego powyżej, operując na listach grup przechowywanych w obu bazach. Rekordy w bazie LDAP mogą być usunięte, dodane, lub zmodyfikowane.
3. Skrypt odświeżający wybrane rekordy z danymi o użytkownikach w bazie LDAP: **update_pwdbs.sh**. Dla podanej, jako parametr, nazwy użytkownika aktualizowane są dane w bazie LDAP, na podstawie plików /etc/passwd i /etc/shadow.

4. Skrypt odświeżający wybrane rekordy z danymi o grupach użytkowników: **update_group.sh**. Narzędzie działa analogicznie do opisanego powyżej, dokonując aktualizacji na podstawie pliku /etc/group.
5. Skrypt budujący bazę LDAP na podstawie zawartości plików /etc/passwd i /etc/shadow - **rebuild_pwdbs.sh**. Istniejąca baza LDAP jest usuwana.
6. Skrypt działający analogicznie do powyższego, w oparciu o plik /etc/group - **rebuild_group.sh.**

4.2. Procedury administrowania

Najczęstszym zadaniem wymagającym modyfikacji danych w bazach kont są operacje dodawania lub usuwania użytkownika. Jak już wspomniano, na klastrze UKŁAD zrezygnowano z używania powszechnie dostępnych, gotowych narzędzi służących do tego celu. Żaden testowany program zarządzający kontami nie potrafił w pełni i poprawnie obsłużyć zadania jednoczesnego dodania konta do obu baz, bądź jego usunięcia. Zdecydowano się na następującą procedurę wprowadzania i usuwania użytkowników systemu:

- wykonanie operacji na standardowej bazie tekstowej narzędziem systemowym (**adduser**, **deluser**). W przypadku programu adduser należy pamiętać o podaniu opcji zabraniającej ustawiania hasła: `--disabled-password`
- wykonanie skryptów **sync_pwdbs.sh** i **sync_group.sh**
- wykonanie programu **passwd**, zmieniającego hasła w rekordach obu baz.

W celu pełnej automatyzacji czynności zakładania i usuwania kont na klastrze UKŁAD, które obejmują też założenie lub zlikwidowanie przestrzeni /scratch na dyskach węzłów i rozprowadzenie tekstowych baz danych kont po węzłach, utworzone zostały skrypty **ADDUSER** i **DELUSER**, dostępne poza katalogiem "CHROOT", w ścieżce /root/bin.

Rzadziej wykonywaną na klastrze UKŁAD operacją jest zmiana danych istniejących kont. Po wprowadzeniu zmian w plikach tekstowych należy wykonać, odpowiednio: skrypt **update_pwdbs.sh** lub **update_group.sh** z właściwymi parametrami.

5. Propozycje rozwoju

W okresie przed wprowadzeniem w dziale KDM systemu zdalnej autoryzacji, opartego o certyfikaty X.509, jako wyłącznego, system autoryzacji PAM-LDAP może zostać rozszerzony na inne KDM-y: Groma, Letycję i Alphę. Baza LDAP może zostać w przyszłości zintegrowana z bazą zawierającą certyfikaty X.509 klientów PCC EuroPKI.

6. Wykorzystane materiały

1. PADL Software: http://www.padl.com
2. OpenLDAP: http://www.openldap.org
3. Using OpenLDAP For Authentication: http://mandrakesecure.net/en/docs/ldap-auth2.pl
4. A Linux PAM page: http://www.kernel.org/pub/linux/libs/pam/