Administracja serwerami linuksowymi
Instrukcja do ćwiczenia:
Protokół LDAP

Krzysztof Boryczko Remigiusz Górecki

7 grudnia 2015

Data wykonania	
Skład Grupy	
Ocena	

Podczas wykonywania ćwiczenia odznaczaj wykonane podpunkty Przed przystąpieniem do wykonania ćwiczenia sprawdź obecność i stan sprzętu. Wszelkie nieprawidłowości należy natychmiast zgłosić prowadzącemu.

Wprowadzenie

System fizyczny posiada możliwość uruchomienia różnych maszyn wirtualnych. W tym ćwiczeniu będziemy wykorzystywać system *CentOS 7.0*. Prosze uruchomić maszynę wirtualną. Do systemu możemy podłączyć się z interfejsu graficznego jako użytkownik *student* hasłem *student*. Czynności administracyjne wymagają jednak uprawnień użytkownika *root*. Stąd po podłączeniu się do systemu i uruchomieniu konsoli należy wykonać polecenie: **su** −. Hasło dla użytkownika *root* to *root123*.

Konfiguracja serwera LDAP

Od wersji 2.4 `OpenLDAP` konfiguracja serwera `OpenLDAP` nie jest już w pliku konfiguracyjnym, a w bazie. Przez co praktycznie rzecz biorąc nie ma już potrzeby posługiwania się plikami, a można na bierząco modyfikować całą konfigurację.

☐1 Uruchom serwer `OpenLDAP`;

☐2 Sprawdź czy serwer nasłuchuje na protokole TCP (który to port?).

☐3 wykorzystując polecenie `ldapsearch` wyświetl zawartość całego drzewa konfiguracji (od *cn=config*) – nie można zrobić tego w kontekście użytkownika anonimowego, więc konieczne jest odpowiednie uwierzytelnienie, czyli opcje: *-Y EXTERNAL -H ldapi:///*.

☐4 W gałęzi konfiguacyjnej *dn: olcDatabase={0}config,cn=config* zmień nazwę głównego administratora – pole `olcRootDN` oraz ustaw mu hasło – `olcRootPW` w formacie *SSHA*.

☐5 Sprawź poprawność powyższych zmian wyświetlając zawartość drzewa konfiguracyjnego wykorzystując uwierzytelnienie typu *simple* z podaniem zdefiniowane nazwy i hasła administratora.

☐6 W gałęzi konfiguacyjnej bazy przechowywanych obiektów *dn: olcDatabase={2}bdb,cn=config* ustaw następujące parametry:

- nazwę obsługiwanej przez serwer domeny – pole `olcSuffix`,
- pełną nazwę administratora bazy (w swej domenie) – pole `olcRootDN`,
- hasło utworzonego administratora – pole `olcRootPW`

☐7 Przetestuj wprowadzone ustawienia wyświetlając wartość artybutu `namingContexts` używając opcji:

☐8 Wykorzystując polecenie `ldapsearch` zapytaj lokalną serwer *LDAP* o wartość atrybutu namingcontexts wydając polecenie ustaw opcje:

- suffix drzewa: pusty (' '),
- autentykacja typu: simple
- zakres poszukiwań: base
- filtr: objectClass=*

Zanotuj otrzymane wartości atrybutu namingcontexts.....

☐9 Wezwij prowadzącego celem sprawdzenia poprawności wykonania zadania.

Dodawanie rekordów do katalogu

☐1 Zdefiniuj w systemie grupę pracownicy oraz użytkowników zyzio i franio, dla których będzie to grupa dodatkowa. Określ również ich opis (atrybut gecos). Ustaw hasła obu użytkownikom.

☐2 Sprawdź czy zainstalowany jest pakiet migrationtools, jeśli nie – zainstaluj go.

☐3 Wykorzystaj skrypt `/usr/share/migrationtools/migrate_base.pl` do wygenerowania podstawowej struktury drzewa bazy danych *LDAP* – aby dostosować skrypt do zarządzanej domeny, należy zmienić wartość zmiennej DEFAULT_BASE zdefiniowanej w pliku: `/usr/share/migrationtools/migrate_common.ph`.

☐4 Za pomocą polecenia `ldapadd` Dodaj do katalogu rekordy opisujące strukturę bazy.
Uwaga. W wygenerowanym przez powyższy skrypt pliku znajdują się wpisy dotyczące węzłów drzewa „powyżej" części, którą będzie obsługiwała nasza baza usługi katalogowej. Rekordy te **nie** powinny być dodane do bazy. Możliwe są więc dwa rozwiązania:

- ☐a usunięcie z wygenerowanego pliku zbędnych wpisów (bezpieczniejsze rozwiązanie),
- ☐b użycie opcji `-c` podczas dodawania rekordów do bazy danych, co spowoduje zignorowanie błędów podczas dodawania rekordów.

☐5 Wykorzystaj skrypt `/usr/share/migrationtools/migrate_passwd.pl` do wygenerowania rekordów opisujących użytkowników aktualnie istniejących w sytemie (zdefiniowanych w `/etc/passwd`. Wygenerowane rekordy zapisz do pliku.

☐6 Wykorzystaj skrypt `/usr/share/migrationtools/migrate_group.pl` do wygenerowania rekordów opisujących zdefiniowane w systemie grupy (plik `/etc/group`. Wygenerowane rekordy zapisz do pliku.

☐7 Usuń z obydwu plików użytkowników i grupy związane z systemowymi. Tak aby w plikach pozostały tylko informacje związane z użytkownikami zyzio i franio

☐8 Za pomocą polecenia `ldapadd` dodaj do katalogu rekordy zawarte w przygotowanych plikach.

☐9 Za pomocą polecenia `ldapsearch` wyświetl informace o dodanych użytkownikach tak aby uzyskać tylko wartości atrybutów uid i gecos

☐10 Poleceniem `ldapsearch` wyświetl wszystkich użytkowników, których nazwy kończą się na io, a więc należących do klasy posixAccount oraz mających uid zakończony znakami io.

☐11 Wezwij prowadzącego celem sprawdzenia poprawności wykonania zadania.

Zmiana wartości rekordów

☐1 Sporządź plik w formacie LDIF, w którym będą informacje dotyczące zmiany wartości następujących atrybutów związanych z użytkownikiem franio

- ☐a Zmień katalog domowy użytkownika na `/tmp`,
- ☐b Dodaj użytkownikowi jego adres e-mail – atrybut mail opisany w klasie inetOrgPerson,
- ☐c Usuń użytkownika z grupy pracownicy

☐2 Za pomocą polecenia `ldapsearch` wyświetl informacje dotyczące użytkownika franio w celu sprawdzenia poprawności wprowadzonych zmian.

☐3 Wezwij prowadzącego celem sprawdzenia poprawności wykonania zadania.

Konfiguracja komputera klienckiego jako stacji wykorzystującej *LDAP* do autoryzacji użytkowników

☐1 Przed wykonaniem zmian konfiguracji komputera klienckiego wykonaj kopię pliku `/etc/nsswitch.conf` oraz `/etc/pam.d/system-auth-ac`

☐2 Odpytaj serwer *LDAP* o wartość atrybutu namingcontexts (w podobny sposób jak uprzednio).

☐3 Uruchom polecenie `authconfig-tui` (jeśli go nie ma – zainstaluj pakiet authconfig) i zdefiniuj za jego pomocą (w przypadku zgłaszań błędów przez tę aplikację doinstaluj brakujące pakiety):

- ☐a Nazwę węzła określającą obsługiwaną przestrzeń nazw, zgodną z wartością atrybutu namingcontexts uzyskaną w poprzednim punkcie,
- ☐b Adres serwera *LDAP* w postaci nazwy FQDN lub adresu IP,
- ☐c Nie ustawiaj szyfrowania sesji wykorzystującego mechanizm TLS.

☐4 Sprawdź wprowadzone zmiany w konfiguracji stacji klienckiej poprzez porównanie aktualnej zawartości pliku `/etc/nsswitch.conf` z poprzednią oraz zwróć uwagę na wartości odpowiednich parametrów zawartych w pliku `/etc/ldap.conf`.

☐5 Za pomocą polecenia `id` wyświetl podstawowe dane o użytkownikach franio i zyzio.

☐6 Za pomocą polecenia `su - login` przełącz się na użytkownika franio, a później analogicznie na użytkownika zyzio. Zaobserwuj zachowanie systemu związane z definicją ich katalogów domowych.

☐7 Będąc podłączony do systemu klienckiego jako zyzio (przy pomocy komendy `su`) uwtórz w katalogu `/tmp` dowolny plik.

☐8 Sprawdź prawa utworzonego pliku. Zwróć uwagę na właściciela pliku.

☐9 Zatrzymaj serwer *LDAP*.

☐10 Ponownie dokonaj sprawdzenia właściwości utworzonego pliku.

☐11 Wezwij prowadzącego celem sprawdzenia poprawności wykonania zadania.