Przechowywanie drzewa struktury organizacyjnej w LDAP

autor: Sławomir Cichy

wersja: 0.0.1

data modyfikacji: 29.10.2013

Wstęp

Celem dokumentu jest zaprezentowanie i zasugerowanie sposobu przechowywania danych o strukturze organizacyjnej firmy w bazach LDAP (przykłady implementacji: Active Directory, OpenLDAP, Oracle Directory itp.).

Metodologia została opracowana i zaimplementowana w jednej z wiodących firm polskiego rynku internetowego i przez wiele lat sprawdza się jako optymalne rozwiązanie.

Zasady

Poniżej przedstawione zostaną zasady, o które zostanie oparte przechowywanie danych.

Przechowywanie danych

Jednostki organizacyjne reprezentowane będą jako obiekty klasy *group* (objectClass=group).

Struktura organizacyjna firmy to drzewo jednostek organizacyjnych w określonej hierarchii. LDAP do baza danych przechowująca dane hierarchicznie i naturalnym by się wydawało, że informacje o organizacji przechowywać należy w sposób hierarchiczny.

Niestety taka metoda przechowywania danych ma bardzo poważną wadę: w sposób drastyczny komplikuje operacje związane z modyfikacją drzewa. Komplikuje również budowanie filtrów wykorzystywanych do wyszukiwania odpowiednich powiązań pomiędzy jednostkami organizacyjnymi oraz pracownikami. Dlatego też proponujemy rozwiązanie w oparciu o model płaski a samą hierarchię zrealizujemy na podstawie atrybutów wartości odpowiednich:

- member – atrybut, którego wartość wskazuje na DN (jednoznaczny identyfikator obiektu wskazujący na położenie w drzewie, tzw. *Distinguished Name*) obiektu członka grupy reprezentującej daną jednostkę organizacyjną.
- memberOf – atrybut, którego wartość wskazuje na DN obiektu, którego członkiem jest dana jednostka organizacyjna.

Nazewnictwo grup

Dodatkowo ważnym elementem związanym z przechowywaniem jest stosowania odpowiedniego nazewnictwa grup, wykorzystanie odpowiednio skonstruowanych akronimów. Zaleca się następujące zasady:

- Nazwa grupy (atrybut CN, tzw. *Common Name*), powinna być jej akronimem, skrótem zawierającym jako prefix skrót grupy nadrzędnej. Najlepiej zobrazuje to przykład trzech jednostek organizacyjnych w następującej hierarchii:
  - Pion Technologii Informatycznej: CN=**PTI**
    - Dział Obsługi Infrastruktury: CN=**PTI**DOI
    - Dział Wytwarzania Oprogramowania: CN=**PTI**DWO

  Celem takiego działania jest prostota utworzenia drzewa zależności poprzez posortowanie grup (rosnąco) po atrybucie CN.
- Każda jednostka organizacyjna powinna zostać podzielona na dwie jednostki abstrakcyjne – pierwszą grupą będzie jednostka, której członkiem jest lider jednostki organizacyjnej, drugą grupą będzie jednostka z szeregowymi pracownikami. Taki podział powinien istnieć zawsze, niezależnie od tego czy jednostka organizacyjna posiada lidera czy nie (w skrajnym wypadku grupa lidera będzie pusta). Nazwę (CN) jednostki abstrakcyjnej tworzymy poprzez dodanie odpowiedniego sufiksu odseparowanego znakiem specjalnym. **UWAGA!** Obiekty użytkowników (pracowników) są przypisywane tylko i wyłącznie do grup abstrakcyjnych. Wykorzystując wcześniejszy przykład otrzymujemy następującą hierarchię:
  - Pion Technologii Informatycznej (CN=**PTI**)
    - Pion Technologii Informatycznej – lider (CN=**PTI-Manager**)
    - Pion Technologii Informatycznej – pracownicy (CN=**PTI-Workers**)
    - Dział Obsługi Infrastruktury (CN=**PTI**DOI)
      - Dział Obsługi Infrastruktury – lider (CN=**PTI**DOI-**Manager**)
      - Dział Obsługi Infrastruktury – pracownicy (CN=**PTI**DOI-**Workers**)
    - Dział Wytwarzania Oprogramowania (CN=**PTI**DWO)
      - Dział Wytwarzania Oprogramowania (CN=**PTI**DWO-**Manager**)
      - Dział Wytwarzania Oprogramowania (CN=**PTI**DWO-**Workers**)

Przykład drzewa – suche dane

Wykorzystajmy wcześniej zaprezentowany przykład uzupełniając go odpowiednimi danymi:

1. Grupy reprezentujące strukturę będą przechowywanie w gałęzi **ou=Struktura,dc=example,dc=com**
2. Użytkownicy (dane reprezentujące pracowników) będą przechowywani w gałęzi **ou=Pracownicy,dc=example,dc=com**
3. Jan Kowalski (jkowalski) jest szefem Pionu Technologii Informatycznej
4. Anna Asystentka (aasystentka) jest asystentką Jana Kowalskiego w Pionie Technologii Informatycznej

5. Witek Szarak (wszarak), Mirek Dzielny (mdzielny) są pracownikami Działu Obsługi Infrastruktury. Dział nie posiada bezpośredniego lidera, jego rolę pełni szef Pionu Technologii Informatycznej
6. Zdzisława Wielka (zwielka) jest liderem Dział Wytwarzania Oprogramowania. Pracownikami Działu Wytwarzania Oprogramowania są: Michał Mały (mmaly) oraz Michał Duży (mduzy)

Oto entry (obiekty wraz z atrybutami) przechowywane w AD:

- Pion Technologii Informatycznej (CN=**PTI**)

```
dn: cn=PTI,ou=Struktura,dc=example,dc=com
description: Pion Technologii Informatycznej
cn: PTI
member: cn=PTI-Manager,ou=Struktura,dc=example,dc=com
member: cn=PTI-Workers,ou=Struktura,dc=example,dc=com
member: cn=PTIDOI,ou=Struktura,dc=example,dc=com
member: cn=PTIDWO,ou=Struktura,dc=example,dc=com
```

  - Pion Technologii Informatycznej – lider (CN=**PTI-Manager**)

```
dn: cn=PTI-Manager,ou=Struktura,dc=example,dc=com
description: Pion Technologii Informatycznej - lider
cn: PTI-Manager
memberOf: cn=PTI,ou=Struktura,dc=example,dc=com
member: cn=jkowalski,ou=Pracownicy,dc=example,dc=com
```

  - Pion Technologii Informatycznej – pracownicy (CN=**PTI-Workers**)

```
dn: cn=PTI-Workers,ou=Struktura,dc=example,dc=com
description: Pion Technologii Informatycznej - pracownicy
cn: PTI-Workers
memberOf: cn=PTI,ou=Struktura,dc=example,dc=com
member: cn=aasystentka,ou=Pracownicy,dc=example,dc=com
```

  - Dział Obsługi Infrastruktury (CN=**PTI**DOI)

```
dn: cn=PTIDOI,ou=Struktura,dc=example,dc=com
description: Dział Obsługi Infrastruktury
cn: PTIDOI
memberOf: cn=PTI,ou=Struktura,dc=example,dc=com
member: cn=PTIDOI-Manager,ou=Struktura,dc=example,dc=com
member: cn=PTIDOI-Workers,ou=Struktura,dc=example,dc=com
```

    - Dział Obsługi Infrastruktury – lider (CN=**PTI**DOI-**Manager**)

```
dn: cn=PTIDOI-Manager,ou=Struktura,dc=example,dc=com
description: Dział Obsługi Infrastruktury - lider
cn: PTIDOI-Manager
memberOf: cn=PTIDOI,ou=Struktura,dc=example,dc=com
```

    - Dział Obsługi Infrastruktury – pracownicy (CN=**PTI**DOI-**Workers**)

```
dn: cn=PTIDOI-Workers,ou=Struktura,dc=example,dc=com
description: Dział Obsługi Infrastruktury - pracownicy
cn: PTIDOI- Workers
memberOf: cn=PTIDOI,ou=Struktura,dc=example,dc=com
member: cn=wszarak,ou=Pracownicy,dc=example,dc=com
member: cn=mdzielny,ou=Pracownicy,dc=example,dc=com
```

  - Dział Wytwarzania Oprogramowania (CN=**PTI**DWO)

```
dn: cn=PTIDWO,ou=Struktura,dc=example,dc=com
description: Dział Wytwarzania Oprogramowania
cn: PTIDWO
memberOf: cn=PTI,ou=Struktura,dc=example,dc=com
member: cn=PTIDWO-Manager,ou=Struktura,dc=example,dc=com
member: cn=PTIDWO-Workers,ou=Struktura,dc=example,dc=com
```

    - Dział Wytwarzania Oprogramowania (CN=**PTI**DWO-**Manager**)

```
dn: cn=PTIDWO-Manager,ou=Struktura,dc=example,dc=com
description: Dział Wytwarzania Oprogramowania - lider
cn: PTIDWO-Manager
memberOf: cn=PTIDWO,ou=Struktura,dc=example,dc=com
member: cn=zwielka,ou=Pracownicy,dc=example,dc=com
```

- Dział Wytwarzania Oprogramowania (CN=**PTI**DWO**-Workers**)

```
dn: cn=PTIDWO-Workers,ou=Struktura,dc=example,dc=com
description: Dział Wytwarzania Oprogramowania - pracownicy
cn: PTIDWO-Workers
memberOf: cn=PTIDWO,ou=Struktura,dc=example,dc=com
member: cn=mmaly,ou=Pracownicy,dc=example,dc=com
member: cn=mduzy,ou=Pracownicy,dc=example,dc=com
```

Korzyści

Poniżej zostaną opisane korzyści związane z prowadzeniem proponowanej organizacji danych opisującej strukturę organizacyjną.

Prosta transformacja danych

Za pomocą prostych mechanizmów można przenieść daną strukturę np. do relacyjnych baz danych. Utworzenie drzewa zależności poprzez posortowanie grup (rosnąco) po atrybucie CN.

Bardzo prosto jest wyciągnąć informację o pracownikach czy liderach doklejając odpowiednie sufiksy do nazw podstawowych.

Bardzo łatwo jest wyciągnąć informację o przełożonym danego pracownika wykonując proste operacje na nazwie grupy abstrakcyjnej, do której należy (usunięcie z nazwy sufiksu -Workers i doklejenie sufiksu -Manager, oraz wyszukanie członków grupy o tak powstałej nazwie).

Bez większego wysiłku jesteśmy w stanie stworzyć metodę eskalacji problemu od jednego przełożonego do drugiego.

Nadawanie uprawnień

Daną strukturę w bardzo prosty sposób można wykorzystać do zarządzania uprawnieniami. Uniezależniamy się od uprawnień nadawanych konkretnym pracownikom na rzecz uprawnień związanych z pełnieniem danej roli w strukturze organizacyjnej firmy.

Korespondencja do grup

Implementacja prostych mechanizmów dziedziczenia użytkowników pomiędzy grupami nadrzędnymi i podrzędnymi sprawia, że wysyłanie korespondencji do określonych jednostek organizacyjnych jest stosunkowo proste do realizacji.

Uproszczenie operacji modyfikacji struktury

Nie trzeba modyfikować DN'a użytkownika aby przenieść go z jednej grupy do drugiej.