o365connect - AOSI plugin za sinkronizaciju Azure AD i LDAP imenika

Predradnje

Prije instalacije plugina potrebno je obaviti predradnje opisane u uputama za konfiguriranje usluge MS Office 365 za autentikaciju korisnika putem sustava AAI@EduHr.

Opis

Ovaj plugin služi sinkronizaciji podataka u LDAP imeniku s Azure AD-om, kako bi se posjednicima elektroničkog identiteta u sustavu AAI@EduHr omogućila autentikacija za uslugu Office 365 putem login servisa sustava AAI@EduHr. Plugin je pisan u Perlu, a podatke prenosi u Azure AD posredstvom Azure AD GRAPH API-a.

Način rada

Zbog raznih ograničenja i zahtjeva koji su postavljeni pred plugin, te heterogenog okruženja u kojem radi, plugin se sastoji od dvije glavne komponente:

- komponente koja sve promjene koje se na određenom setu atributa dogode u LDAP imeniku piše u .ldif datoteku;
- komponente koja asinkrono promjene zapisane u ldif datoteci proslijeđuje u Azure AD pozivom metoda GRAPH API-a;

Kako se promjene u Azure AD prenose asinkrono, korisnik nije kreiran u Azure AD istog trenutka kad je dodan u LDAP imenik, već tek nakon prvog sljedećeg pokretanja komponente koja promjene prenosi u Azure. Iz istog razloga administrator ne može znati jesu li sve promjene uspješno prenesene u Azure AD, pa je potrebno povremeno provjeravati log datoteku.

Promjene koje se prenose u Azure AD

- **dodavanje korisnika**: kreira se novi korisnik u Azure AD. Sukladno vrijednosti atributa hrEduPersonPrimaryAffiliation (primarna povezanost s ustanovom), te postavkama korisnik se automatski pridružuje određenoj grupi, te mu se dodjeljuje odgovarajuća licenca;
- **brisanje korisnika**: korisnik u Azure AD proglašava neaktivnim. Kako se kod kreiranja korisnika u Azure AD prenosi i hrEduPersonPersistentID, Azure AD vodi brigu o tome da je, iako je korisnik obrisan, nemoguće dodati korisnika s istom vrijednosti atributa hrEduPersonPersistentID;
- **promjena vrijednosti atributa**: za atribute određene konfiguracijom, promjene se prenose u Azure AD;

Komponente

Instalacijski paket sastoji se od 5 datoteka:

- **/usr/lib/aosi/Plugins/o365connect.pm** - komponenta s kodom plugina koja se uključuje u AOSI web servis i sve promjene u atributima određenim konfiguracijskom datotekom piše u ldif datoteku koja se nalazi na stazi **`/var/log/aosi/o365connect/o365connect_REALM.ldif`**
- **/usr/lib/aosi/Plugins/o365connectTransferToAzure.pl** - komponenta koja se pokreće iz crona svakih 10 minuta i sve promjene zapisane u datoteci **`/var/log/aosi/o365connect/o365connect_REALM.ldif`** proslijedi u Azure AD koristeći GRAPH API. Izlaz ove datoteke piše se u log na stazi **`/var/log/aosi/o365connect/o365connectTransferToAzure.log`**. Nakon što obradi ldif datoteku, ako je tako određeno konfiguracijom, kompresira ldif datoteku i preimenuje je u **o365connect_REALM.ldif.timestamp.gz**
- **/etc/aosi/plugins/o365connect.conf** - konfiguracijska datoteka. U njoj je moguće postaviti sljedeće parametre:
  `ofc_clientID` je CLIENT ID dobiven u postupku registracije plugina u Azure AD web sučelju. Postupak registracije opisan je u ovim uputama.
  `ofc_clientSecret` je KEY dobiven u postupku registracije plugina u Azure AD web sučelju. Postupak registracije opisan je u ovim uputama.
  `ofc_archive_processed_ldif` je parametar koji određuje hoće li ldif datoteka s promjenama, nakon što su promjene prenesene u Azure AD, biti izbrisana ili arhivirana. Default je 1 i on označava da će datoteka biti arhivirana.
- **/etc/aosi/plugins/o365connectAttributes.pm** - konfiguracijska datoteka u kojoj s popisom atributa koji se prenose u Azure AD. U nastavku su opisani parametri dostupni kroz tu datoteku:
  Parametar **attr_map** određuje koji se atributi prenose prilikom kreiranja novog korisnika iz LDAP-a u Azure AD, te u koje se atribute u Azure AD mapiraju pojedini atributi iz hrEduPerson sheme. Defaultna vrijednost je:

```
$attr_map={
            'cn'=>'displayname',
            'givenName'=>'GivenName',
            'sn'=>'Surname',
            'hrEduPersonUniqueID'=>'userprincipalname',
            'uid'=>'mailNickname',
            'hrEduPersonPersistentID'=>'immutableid',
            'hrEduPersonPrimaryAffiliation'=>'jobTitle'
        };
```

Parametar **upd_attr** je popis atributa za koje se promjene prenose iz LDAP-a u Azure AD. Defaultna vrijednost je:

```
$upd_attr=['cn','givenName','sn','hrEduPersonPrimaryAffiliation'];
```

Parametar **group_map** određuje u koju će grupu biti pridružen korisnik prilikom dodavanja u Azure AD, a na osnovi vrijednosti atributa hrEduPersonPrimaryAffiliation (primarna povezanost s ustanovom). Jedan korisnik može biti pridružen u više grupa odjednom. Npr. kad bi djelatnike htjeli prilikom dodavanja postaviti i u grupu SG_djelatnik i u grupu SG_zaposlenik, redak **`'djelatnik'=>['SG_djelatnik'],`** biste u datoteci zamijenili redkom **`'djelatnik'=>['SG_djelatnik', 'SG_zaposlenik'],`** Ako grupa ne postoji u Azure AD, bit će kreirana kod prvog korisnika koji treba biti pridružen toj grupi. Hrvatski dijakritici su namjerno izbačeni iz definicije, pa tako umjesto učenik piše uenik, a umjesto cjeloživotno cjeloivotno. Defaultna vrijednost je:

```
$group_map={
            'cjeloivotno obrazovanje'=>['SG_cjelozivotno_obrazovanje'],
            'djelatnik'=>['SG_djelatnik'],
            'gost'=>['SG_gost'],
            'korisnik usluge'=>['SG_korisnik_usluge'],
            'student'=>['SG_student'],
            'uenik'=>['SG_ucenik'],
            'vanjski suradnik'=>['SG_vanjski_suradnik'],
        };
```

Parametar **licence_map** određuje koja će licenca biti dodijeljena korisniku prilikom dodavanja u Azure AD, a na osnovi vrijednosti atributa hrEduPersonPrimaryAffiliation (primarna povezanost s ustanovom). Jednom korisniku može biti dodijeljeno više različitih licenci (ako to vrsta licence dozvoljava). Hrvatski dijakritici su namjerno izbačeni iz definicije, pa tako umjesto učenik piše uenik, a umjesto cjeloživotno cjeloivotno. Defaultna vrijednost je:

```
$licence_map={
            'cjeloivotno obrazovanje'=>[],
            'djelatnik'=>['STANDARDWOFFPACK_FACULTY'],
            'gost'=>[],
            'korisnik usluge'=>[],
            'student'=>['STANDARDWOFFPACK_STUDENT'],
            'uenik'=>[],
            'vanjski suradnik'=>[],
        };
```

- **o365connectLdapExport.pl** - izvršna datoteka koja služi inicijalnoj sinkronizaciji Azure AD s LDAP imenikom. Nju je potrebno pokrenuti kod prve instalacije plugina. Ona sve korisnike iz imenika upiše u datoteku **`/var/log/aosi/o365connect/o365connect_REALM.ldif`** kako bi ih komponenta koja proslijeđuje podatke u Azure AD proslijedila u prvom sljedećem pokretanju. Da biste izvršili ovu datoteku potrebno je imati root ovlasti.
  VAŽNO: ova se datoteka pokreće samo jednom kod prve instalacije plugina!

Log

Log datoteka koja opisuje prijenos podataka u Azure AD nalazi se na stazi:

```
/var/log/aosi/o365connect/o365connectTransferToAzure.log
```

Ako je u konfiguraciskoj datoteci **`o365connect.conf`** parametar **`ofc_archive_processed_ldif`** postavljen u **1**, ldif datoteka s promjenama se nakon obrade komprimira, preimenuje je u **o365connect_REALM.ldif.timestamp.gz** i ostaje na u direktoriju **`/var/log/aosi/o365connect/`**

Instalacija

Prije instalacije plugina potrebno je obaviti predradnje opisane u uputama za konfiguriranje usluge MS Office 365 za autentikaciju korisnika putem sustava AAI@EduHr.

Plugin se instalira naredbom:

```
# apt-get install libo365connect-aosi-aai
```

U postpuku instalacije potrebno je unijeti CLIENT ID i KEY koji služe autentikaciji plugina za pristup funkcijama GRAPH API-a.