Univerzita Palackého v Olomouci

AUTOCONT

IMPLEMENTAČNÍ PROJEKT

Integrace na AD pro PrF

Verze 1.2

vímejak

ZÁKLADNÍ INFORMACE O DOKUMENTU

Připravil

[redacted]

Pozměňovací návrhy

Datum	Verze	Popis	Autor
9.5.2018	Verze 1.0	Základní verze	[redacted]
1.6.2018	Verze 1.1	Zodpovězení komentářů UPOL	
19.7.2018	Verze 1.2	Zodpovězení komentářů UPOL, příjmutí revizí, finální verze	

OBSAH

1. Úvod 5
1.1. Princip integrace na AD 5
2. Způsob komunikace 6
3. Průběh synchronizace 7
3.1. Iniciační naplnění databáze AC IDENTITA 7
3.2. Průběžná synchronizace AC IDENTITA s AD 7
3.3. Synchronizace skupin uživatelů 8
3.4. Synchronizace uživatelů 8
3.5. Frekvence synchronizací 9
4. Mapování atributů AD na atributy AC IDENTITA 10
4.1. Interní AD 10
4.1.1. Uživatel v AD 10
4.1.2. Skupina v AD 11

SEZNAM ZKRATEK

Zkratka	Význam
AC	AutoCont
AD	Active Directory
DB	Database
UPOL	Univerzita Palackého v Olomouci
LDAP	Lightweight Directory Access Protocol
SAP	Personální systém pro zaměstnance
STAG	Personální systém pro studenty
INIS	Personální systém pro externisty
PrF	Přírodovědecká fakulta

1. ÚVOD

1.1. PRINCIP INTEGRACE NA AD

AD jako systém umožňující autentizaci uživatelů je klíčovou součástí organizace. Po implementaci systému IDM bude AD PrF cílovým systémem systému AC Identita, společně s AD, LDAP a OpenLDAP UPOL. Do AD budou zapisovány veškeré změny identit v zavislosti na přidělené aplikační roli aplikace AD PrF.

Zdrojovými systémy pro interní identity je personální systém SAP, STAG, INIS. V systému SAP je zavedena systemizace, která umožní evidovat a předávat do systému AC Identita kompletní hierarchickou organizační strukturu, včetně hierarchické struktury pracovních pozic a zařazení osob na jednotlivá funkční místa a do organizačních jednotek.

Do systému AD nebude organizační struktura předávána.

Vzhledem k tomu, že v současné době jsou interní uživatelé založeni a aktualizováni v AD PrF, je nutné promapovat stávající uživatele doplněním mapování do IDM. Mapování bude jednorázově naimportováno do databáze IDM, zadavatel dodá excel obsahující login uživatele a objectSid v hexadecimal formátu.

2. ZPŮSOB KOMUNIKACE

Komunikace mezi systémy IDM a AD probíhá prostřednictvím protokolu LDAP resp. LDAPS.

3. PRŮBĚH SYNCHRONIZACE

3.1. INICIAČNÍ NAPLNĚNÍ DATABÁZE AC IDENTITA

Vzhledem k tomu, že v současné době jsou interní uživatelé založeni a aktualizováni v AD PrF, je nutné doplnit mapování pro stávající IDM uživatele. Mapování bude jednorázově naimportováno do databáze IDM, **zadavatel dodá excel obsahující login uživatele a objectSid v hexadecimal formátu**. Login uživatele v AD PrF odpovídá loginu uživatele v IDM (a tedy loginu v AD UPOL, LDAP UPOL).

Při iniciační synchronizaci se systémem AD budou do AC Identita nahrány skupiny umístěné v definovaném kontejneru AD (parametr synchronizace) a členství uživatelů v těchto skupinách. Import bude proveden pro tento kontejner: [redacted]. Při iniciační AD synchronizaci mohou nastat tyto stavy:

1. Pokud bude v AD existovat skupina se stejným názvem jako je v AC Identita, tak se v IDM změní její typ a rozsah dle AD.
2. V případě, že v AC Identita nebude existovat skupina, která se nachází v AD tak se tato skupina založí (včetně odpovídajícího typu a rozsahu). Dále se porovná seznam členů skupiny v AD s uživateli v AC Identita a pokud je uživatel v AC Identita založen, tak se přiřadí do této nově vzniklé skupiny.

Z tohoto důvodu je nutné skupiny AD PrF odlišit od stávajících skupin v IDM (které jsou použity pro AD UPOL, LDAP UPOL). [redacted]

3.2. PRŮBĚŽNÁ SYNCHRONIZACE AC IDENTITA S AD

Synchronizace do AD podporuje kompletní i změnovou synchronizaci. Kompletní synchronizace načte veškeré přenášené entity pro definovanou doménu a organizaci, porovná stav objektů v AC Identita vůči AD a propíše případné změny. Jednoznačným určením, zda uživatele propisovat do AD bude pomocí aplikační role aplikace AD PrF. Změnová synchronizace pracuje na základě realizovaných změnových požadavků v AC Identita. Pokud v AC Identita dojde ke změně (ať už vstupní synchronizací, např. z HR nebo ruční změnou v UI AC Identita), zapíše se do databáze AC Identita změnový požadavek. Změnová synchronizace do AD si projde všechny změnové požadavky od posledního zpracovaného požadavku. Pokud se požadavek týká synchronizovaných entit do AD, synchronizace porovná stav v AC Identita vůči AD a propíše případné změny.

V reálném provozu se pro automatický propis změn do AD používá změnová synchronizace, spouštěná po definovaných intervalech, např. 2x denně (0:00, 12:00). Kompletní synchronizace se využívá především při náběhu synchronizace (jde zpravidla o ruční spuštění). Automatické spuštění kompletní synchronizace bývá nastaveno např. jednou týdně v mimopracovní dobu. Do AD nebude propisována struktura organizačních jednotek univerzity. Nový účet bude vytvořen do kontejneru (organization

unit) v AD podle toho, zda jde o studenta nebo zaměstnance [redacted]

3.3. SYNCHRONIZACE SKUPIN UŽIVATELŮ

Do AD budou předávány změny skupin typu AD Security a AD Distribution [redacted], které odpovídají příslušné doméně v AC Identita. Dále bude pro typ skupin AD Security, AD Distribution přenášen i její rozsah. Rozlišují se tři typy rozsahu a to: doménově lokální, globální a univerzální.

Skupina uživatelů může být vložena do jiné skupiny stejného typu i druhého typu. Lze také kombinovat různé typy rozsahů skupin a to dle následujících pravidel:

Pod doménově lokální skupinou lze vytvořit: doménově lokální, globální a univerzální. Pod globální lze vytvořit: globální. Pod univerzální lze vytvořit: univerzální a globální.

Nově vytvořené skupiny do AD PrF z AC Identita budou umístěny v jednom, k tomu určeném kontejneru [redacted]. Kontejner bude určen pomocí parametru synchronizace. Nově vytvořenou skupinu může administrátor AD ručně v AD přesunout do jiné organization unit.

AC Identita neumožňuje mazání skupin, pouze jejich deaktivaci. Pokud bude skupina v IDM deaktivována, tak se změna stavu do AD nepromítá (skupina nemá stav).

Mapování atributů pro interní AD je uvedeno v kapitole Mapování atributů AD na atributy AC IDENTITA.

3.4. SYNCHRONIZACE UŽIVATELŮ

Veškeré změny identit, zařazených do příslušné domény AD, které budou zaznamenány v AC Identita, budou v rámci synchronizace přeneseny do AD.

Jednoznačným určením, zda uživatele propisovat do AD bude pomocí aplikační role aplikace AD PrF. V případě, že uživatel bude mít přiřazenou aplikační roli aplikace AD PrF, tak bude přenášen do adresářové struktury AD. Uživatel může mít přiřazeno více aplikačních rolí.

Všichni stávající i noví uživatelé budou synchronizováni do definovaného kontejneru, podle toho, zda jde o studenta nebo zaměstnance [redacted]. Pokud bude student i zaměstnanec, bude synchronizován do kontejneru pro zaměstnance. Při změně student -> zaměstnanec a naopak dojde k přesunu uživatele v AD.

Při deaktivaci uživatele v AC Identita (ať už při deaktivaci z personalistiky nebo ručně) je v AC Identita uložen atribut aktivní do, kde se automaticky nastaví datum, kdy uživatel přešel do stavu Disabled. Při deaktivaci účtu v IDM bude uživatel odstraněn ze skupin v AD. [redacted] Ochrannou lhůtu je možné nastavit v konfiguraci AC Identita. Po uplynutí této doby dojde k automatickému smazání uživatele z AC Identita a následně i z AD.

Pokud bude v IDM neaktivní uživatel zaktivněn a nebude existovat v AD, pak bude znovu vytvořen.

3.5. FREKVENCE SYNCHRONIZACÍ

[redacted]

V rámci jedné synchronizace budou synchronizovány jak skupiny, tak i změny identit – uživatelů.

4. MAPOVÁNÍ ATRIBUTŮ AD NA ATRIBUTY AC IDENTITA

4.1. INTERNÍ AD

4.1.1. UŽIVATEL V AD

Atribut v AD	Mapování v IDM	Poznámka
objectClass		
sAMAccountName		
Cn		
displayName		
uidNumber		
userAccountControl		
userPassword		
accountExpires		
givenName		
mail		
name		
sn		
Surname		
userPrincipalName		

Atribut v AD	Mapování v IDM	Poznámka
title	[redacted]	
department		
mobile		
mobilePhone		
officePhone		
telephoneNumber		

4.1.2. SKUPINA V AD

Atribut AD	Mapování v IDM	Pozn.
Cn	[redacted]	
Description		
Mail		
Info		

Atribut AD	Mapování v IDM	Pozn.
GroupType	[redacted]	
SID		
Member		