AUTOCONT

Univerzita Palackého v Olomouci

IMPLEMENTAČNÍ PROJEKT

Integrace na AD pro PdF

Verze 1.1

vímejak

ZÁKLADNÍ INFORMACE O DOKUMENTU

Připravil

[redacted]

Pozměňovací návrhy

Datum	Verze	Popis	Autor
25.6.2018	Verze 1.0	Základní verze	[redacted]
24.8.2018	Verze 1.1	Zapracování připomínek UPOL PdF	

OBSAH

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
PdF	Pedagogická 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 PdF 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 PdF.

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 PdF, 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 PdF, 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 PdF 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 může být proveden vícekrát, pokud je více kontejnerů skupin, např. dvě spuštění init synchronizace pro tyto kontejnery: pdf/groups a pdf/departments (načtení proběhne i z podřízených OU). 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 PdF odlišit od stávajících skupin v IDM (které jsou použity pro AD UPOL, LDAP UPOL). Stávajícím skupinám v AD PdF bude nutné upravit název o prexif „PDF_" (např. skupina employess_3900 bude změněna na PDF_employess_3900). Úpravu názvů zajistí zadavatel (před init synchronizací do IDM). Skupiny s tímto prefixem nyní v IDM UPOL nejsou. Výstupní AD synchronizace pro UPOL a pro AD PdF bude upravena tak, aby AD skupiny s prefixem PDF_ byly použity pouze pro AD PdF a bez tohoto prefixu pro AD UPOL.

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 PdF. 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 (organization unit pdf/students nebo pdf/employees).

3.3. SYNCHRONIZACE SKUPIN UŽIVATELŮ

Do AD budou předávány změny skupin typu AD Security a AD Distribution s názvem začínajícím prefixem „PDF_“, 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 PdF z AC Identita budou umístěny v jednom, k tomu určeném kontejneru (pdf/groups). Kontejner bude určen pomocí parametru synchronizace. Nově vytvořenou skupinu může administrátor AD ručně v AD přesunout do jiné organization unit. IDM toto umístění pro stávající skupiny nebude měnit (pouze bude aktualizovat vlastnosti uvedené v mapovací tabulce).

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 PdF. V případě, že uživatel bude mít přiřazenou aplikační roli aplikace AD PdF, tak bude přenášen do adresářové struktury AD. Uživatel může mít přiřazeno více aplikačních rolí.

Všichni noví uživatelé budou synchronizováni do definovaného kontejneru, podle toho, zda jde o studenta nebo zaměstnance (kontejner pdf/students nebo pdf/employees). Nově vytvořeného uživatele může administrátor AD ručně v AD přesunout do jiné organization unit. IDM toto umístění pro stávající uživatele nebude měnit (pouze bude aktualizovat vlastnosti uvedené v mapovací tabulce).

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. Od tohoto data běží 150 dnů ochranná lhůta. 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

Změny (až na výjimky – změna hesla uživatele v IDM, změna loginu) budou propsány do adresářové struktury v offline režimu, tedy v intervalech nastavených v konfiguraci příslušné synchronizace.

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		„user“
sAMAccountName	Uživatel – login	Generuje se v IDM
Cn	Osoba - Příjmení + " " + Osoba - Jméno + " (" + Uživatel - login + ")"	priklad v AD: Klement Milan (klement)
displayName	Osoba – Titul Před + „ “ + Osoba – Jméno + „ “ + Osoba – Příjmení + „ “ + Osoba – Titul Za	
uidNumber	Osoba – GenerUID	Generuje se v IDM
userAccountControl	512 – aktivní uživatel	+ přenáší se informace, jestli se má změnit heslo pří prvním přihlášení nebo že heslo nikdy nevyprší.
userPassword	Heslo	Generuje se v IDM a předává do adresářových služeb. V IDM není uloženo.
accountExpires		Datum vypršení účtu + 150 dní
givenName	Osoba – Detail - Jméno	
mail	Uživatel – E-mail	
name	Osoba - Příjmení + " " + Osoba - Jméno + " (" + Uživatel - login + ")"	priklad v AD: Klement Milan (klement)
sn	Osoba – Příjmení	Příjmení s malými písmeny
Surname	Osoba - Příjmení	Příjmení s malými písmeny
userPrincipalName	Uživatel - login + “@” + jméno domény”	Jméno domény je uvedeno v konektoru, tj. „pdfad.upol.cz“

Atribut v AD	Mapování v IDM	Poznámka
title	Osoba – Detail - Titul před jménem	
department	Uživatel – Organizační jednotka - Zkratka	Jde o číslo nákladového střediska, např. 3912 pro OJ „správa budov Holice“
mobile	Osoba – Detail – Kontakty – Telefon do zaměstnání	V IDM je v poli telefon do zaměstnání více kontaktů, např. „585633051,739329978“. Budou z něj odebrány čísla začínající „5“.
mobilePhone	Osoba – Detail – Kontakty – Telefon do zaměstnání	V IDM je v poli telefon do zaměstnání více kontaktů, např. „585633051,739329978“. Budou z něj odebrány čísla začínající „5“.
officePhone	Osoba – Detail – Kontakty – Telefon do zaměstnání	V IDM je v poli telefon do zaměstnání více kontaktů, např. „585633051,739329978“. Budou ponechány čísla začínající „5“.
telephoneNumber	Osoba – Detail – Kontakty – Telefon do zaměstnání	V IDM je v poli telefon do zaměstnání více kontaktů, např. „585633051,739329978“. Budou ponechány čísla začínající „5“.

Pozn.: Hodnoty pro Osoba – Jméno a Osoba – Příjmení požadujeme **včetně diakritiky**

4.1.2. SKUPINA V AD

Atribut AD	Mapování v IDM	Pozn.
Cn	Skupina – detail - Jméno skupiny	
Description	Skupina – detail - Popis skupiny	
Mail	Skupina – detail – E-mail	
Info	Skupina – detail - Info	

Atribut AD	Mapování v IDM	Pozn.
GroupType	Skupina uživatelů – Detail - Rozsah skupiny	**mapování:** Pro AD Distribution: Doménově lokální (domain local) = 4 Globální (global) = 2 Univerzální (univerzal) = 8 AD security : Doménově lokální = -2147483644 Globální = -2147483646 Univerzální = -2147483640
SID	Generuje se v AD	Záznam v mapovací tabulce
Member	Skupiny uživatelů – Uživatelé	Multivalue proměnná. Seznam uživatelů, kteří jsou v IDM přiřazení do této skupiny.