Migrační postup Active Directory

pro

Verze:	1.21
Datum:	7.2.2017

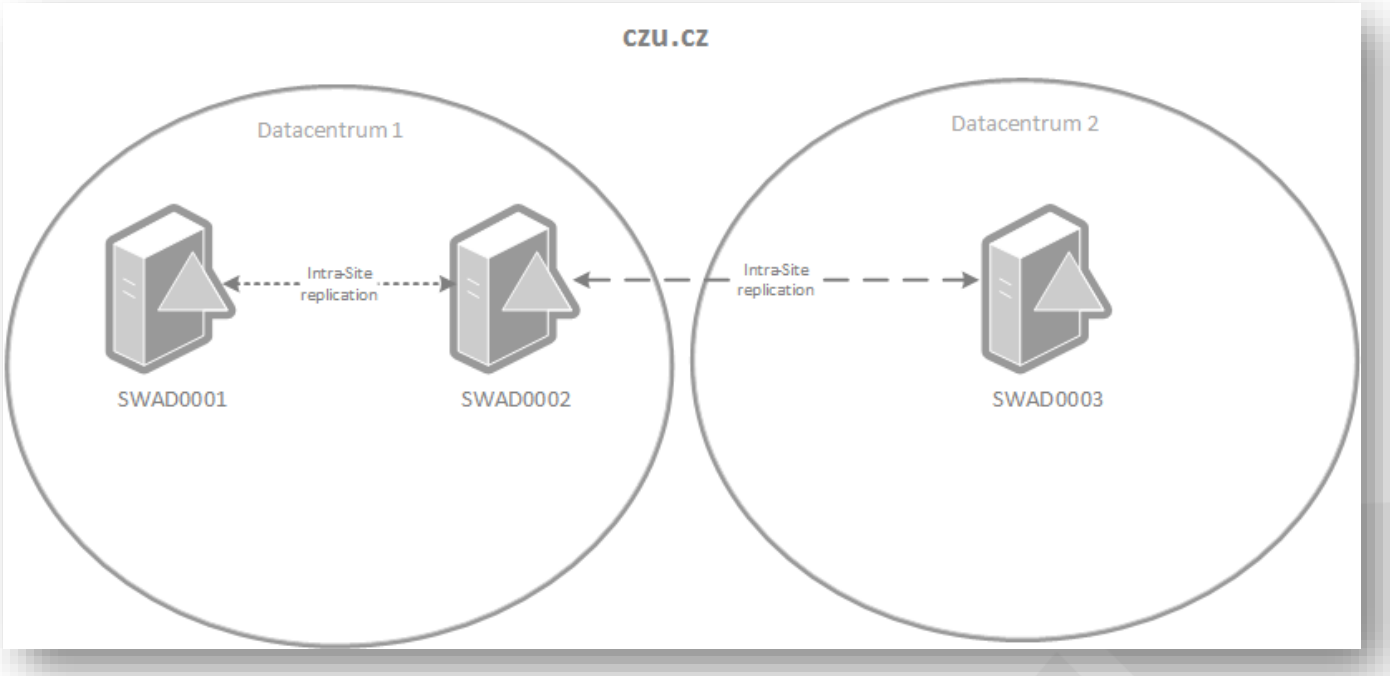
Obsah

Seznam tabulek

Seznam obrázků

1 Cílový stav služby Active Directory

Dvě samostatná datová centra, kdy v primárním datovém centru budou umístěny dva doménové řadiče a v druhém datovém centru třetí doménový řadič.



Obrázek 1 - Cílový stav služby Active Directory

2 Navrhované migrační kroky

Stručný postup migračních kroků je následující:

1. Příprava a kontrola prostředí
2. Dokumentace stávajícího stavu
3. Instalace cílových serverů AD
4. Vytvoření domény czu.cz
5. Migrace domény z adds.oikt.czu.cz do czu.cz
6. Migrace dat a aplikací závislých na Novell eDirectory
7. Migrace identit z eDirectory
8. Odstranění Novell eDirectory

3 Příprava a kontrola prostředí (AD)

Před vlastním zahájením instalace nového prostředí je třeba provést kontrolu celého stávajícího prostředí se zaměřením na Active Directory.

Správné fungování replikací a služeb DNS ve zdrojové doméně je klíčové pro úspěšnou implementaci nových doménových řadičů a především pak pro pozdější migraci.

3.1 Kontrola současných DC

Prvním krokem je ověření, že současné DNS servery fungují správně pomocí nástroje dcdiag.exe.
První příkaz zkontroluje korektní funkcionalita DNS služby. Druhý pak zkontroluje celkové zdraví doménového řadiče.
Následuje ověření DNS servisních záznamů služby AD pomocí nástroje dnslint

Ověření replikace služby Active Directory pomocí nástroje repadmin.

Následuje ověření, zda služba DHCP funguje a odpovídá klientům na jejich požadavky. Později bude provedena rekonfigurace DHCP a nahrazení stávajícího nastavení DNS serverů.

3.2 Příprava prostředí před migrací

3.2.1 Aplikace

Účelem tohoto kroku je zaznamenat všechny důležité aplikace, které bude nutné migrovat do nového prostředí.

Po definování těchto aplikací je potřeba zdokumentovat jejich závislost na stávající Active Directory „adds.oikt.czu.cz“ a připravit migrační postup pro přesun do nové domény czu.cz.

4 Vytvoření domény czu.cz

V rámci tohoto kroku bude provedena instalace a konfigurace domény czu.cz. Do této struktury budou namigrovány objekty jak ze současné Active Directory, tak z Novell eDirectory.

4.1 Instalace cílových serverů AD

Nové servery je potřeba připravit na migraci dle následujících kroků:

- Nainstalovat operační systém
- Přiřadit jméno serveru
- Přiřadit pevné IP adresy serveru
- Aktualizovat server dostupnými aktualizacemi z Microsoft Update

Detailní postup:

1. Instalace 1. doménového řadiče s Windows Server 2016
2. Instalace 2. doménového řadiče s Windows Server 2016
3. Instalace 3. doménového řadiče s Windows Server 2016
4. Instalace 4. doménového řadiče s Windows Server 2012 R2

4.2 Instalace role AD

Server je potřeba povýšit na doménový řadič prostřednictvím průvodce přidáním role Active Directory

V průvodci je potřeba provést následující:

- Vytvořit nový forest a novou doménu (u prvního DC)
- Přidat další server do existující domény (u ostatních DC)
- Nastavit server jako DNS, GC
- Umístění do adekvátní SITE (Suchdol)
- Nastavení a dokumentace DSRM hesla

4.3 Konfigurace NTP

Konfigurace nového PDC Emulator pro synchronizaci času s externím NTP zdrojem času.

4.4 Rekonfigurace DNS

4.4.1 DNS

Více informací pro nastavení vypnutí EDNS lze provést dle KB článku společnosti Microsoft.[1]

4.5 Recycle Bin

Nástrojem Active Directory Administration Center lze zapnout funkcionalitu doménového koše.

4.6 Konfigurace GPO a dalších nastavení v rámci domény

4.6.1 Kontrola DNS záznamů a změna nastavení

1. Proveďte kontrolu aktuálnosti NS záznamů
2. Proveďte kontrolu aktuálnosti delegací např. _msdcs.czu.cz
3. Proveďte kontrolu SRV záznamů

4.6.2 Příprava centrálního úložiště nových GPO šablon

Proveďte zkopírování souborové struktury PolicyDefinitions z jednoho ze serverů Windows Server 2012 R2 do příslušné složky v SYSVOL.

4.6.3 Konfigurace zálohování nových doménových řadičů

Pro zajištění kontinuity je nutné nastavit zálohování alespoň jednoho z nových doménových řadičů.

Nastavení zálohy „Bare metal“ pro “Bare Metal Recovery“ na dvou nových doménových řadičích pomocí HP Data Protector.

4.7 Modifikace schématu

Podle tabulky z kapitoly věnující se logickému designu, bude provedena modifikace schématu.

1. Vytvoření vstupního souboru nutného pro modifikaci schématu schemamodify.ldf, který obsahuje následující parametry
2. Kontrola, zda účet pod kterým děláme rozšíření je členem skupiny „Schema Admins“.
3. Provedení importu/modifikace schématu
4. Vynucení replikace mezi všemi doménovými řadiči
5. Prověření viditelnosti atributů u objektů “**Users**” v Active Directory a to pomocí:

[1] Více informací: http://support.microsoft.com/kb/832223

- ADSI Editor
  nebo
- Atribut Editor

4.8 Skrytí atributů

Skrytí atributů: czu-mobile pomocí metody searchFlags.

Nastavení výjimky (viditelnost atributů):

Poznámka: Hromadné modifikace/nastavení vyjímek je nutné pak řešit automatizovaně pomocí skriptu apod.

5 Politiky hesel

5.1 Default domain policy

Politika hesel bude nastavena dle specifikací uvedených v tabulce níže:

Security parametr	Hodnota
Password History	24 hesel
Minimum Password Length	8 znaků
Minimum Password Age	2 dny
Maximum Password Age	180 dní
Password complexity	Vyžadováno

Tabulka 1– Default Password policy

6 Migrace z domény z adds.oikt.czu.cz do czu.cz

Cílem této kapitoly je popsat seznam kroků migrace z původního prostředí do nové AD infrastruktury. K migraci se použije nástroj Microsoft ADMT v poslední dostupné verzi, který bude doplněn o KPCS skripty, které budou využity k maximalizování automatizace.

Při migraci Active Directory je nutné řešit i veškeré navázané systémy na původní (zdrojovou) doménu. Pokud existují služby, servery nebo programový kód, který využívá původní identity k zajištění přístupu k jednotlivým prostředkům, je nutné před migrací provést řadu testů. V rámci těchto testů musí vzniknout harmonogram a popis migrace pro každou z těchto služeb. Při migraci identit se změní primární identifikátor těchto objektů - SID. Při migraci pomocí ADMT je možné tento identifikátor přenést do jiného atributu, který zajistí udržení historie těchto identifikátorů. Bohužel v různých aplikacích nebo službách se využívají i jiné identifikátory, které se ve většině případů při migraci identit změní. Z tohoto důvodu je důležité otestovat veškeré systémy a jejich připravenost na migraci.

Metoda: ADMT se SID History

Tato metoda je nejběžnější migrační procedurou při konsolidaci Active Directory. V tomto případě se k migraci využívá nástroj pro tyto účely vytvořený společností Microsoft. Tento nástroj se nazývá ADMT – Active Directory Migration Tool. Tento nástroj je určen pro migraci uživatelských účtů, počítačových účtů, skupin, uživatelských profilů a zabezpečení na souborových systémech. Díky těmto možnostem je nejvhodnějším nástrojem pro komplexnější migrace. Po dokončení migrací identit je možné nahradit ACL listy a tímto zrušit veškerou závislost na původním prostředí.

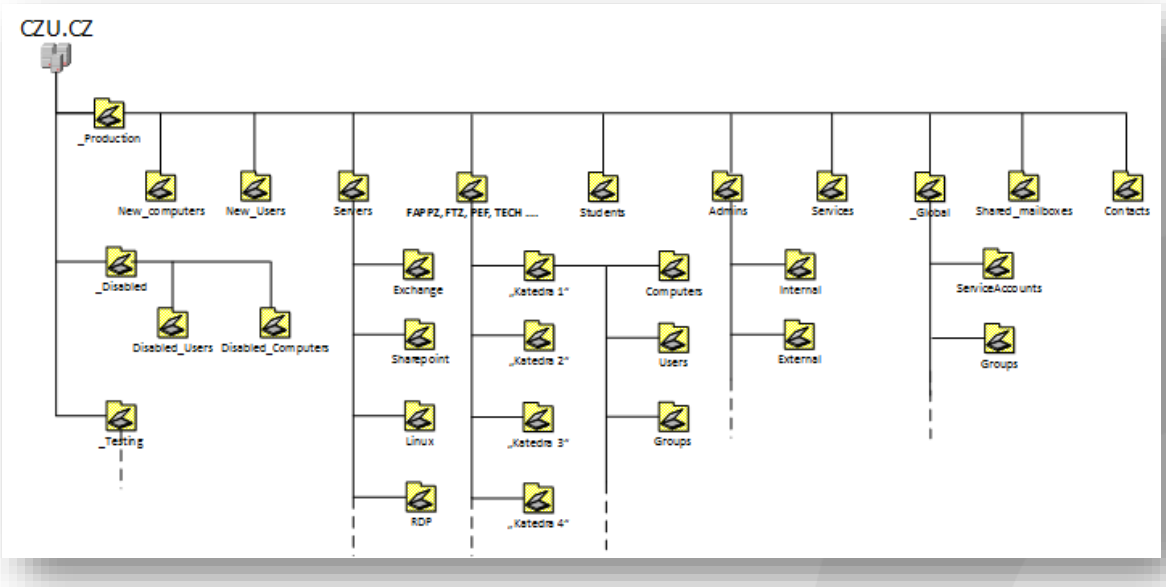
6.1 Předpoklady

V této kapitole jsou popsány technické předpoklady pro zahájení migrace.

Dále se předpokládá, že během migrace (po úspěšné testovací fázi) se nové AD objekty budou vytvářet už jen v nové doméně, a modifikace objektů ve zdrojové doméně se omezí na nutné minimum.

6.1.1 OU struktura

OU struktura je již vytvořena dle dokumentu „CZU_AD_Design.doc“.



Obrázek 2 – OU struktura

6.1.2 Zdrojové DC

Na zdrojovém DC (ve zdrojové doméně / forestu), je nutné nainstalovat „Password Export Server“ a to na **MENEGROTH** v původní doméně s operačním systémem Windows 2008 R2.[2]

[2] Více informací: http://www.microsoft.com/en-us/download/details.aspx?id=34595

6.1.3 DNS

DNS překlady na zdrojové domény jsou potřeba pro tvorbu doménových trustů a pro koexistenci obou prostředí po dobu migrace. Členové zdrojové domény musí být schopni nalézt členy z domén cílových, a opačně. Platí i pro krátké názvy stanic.

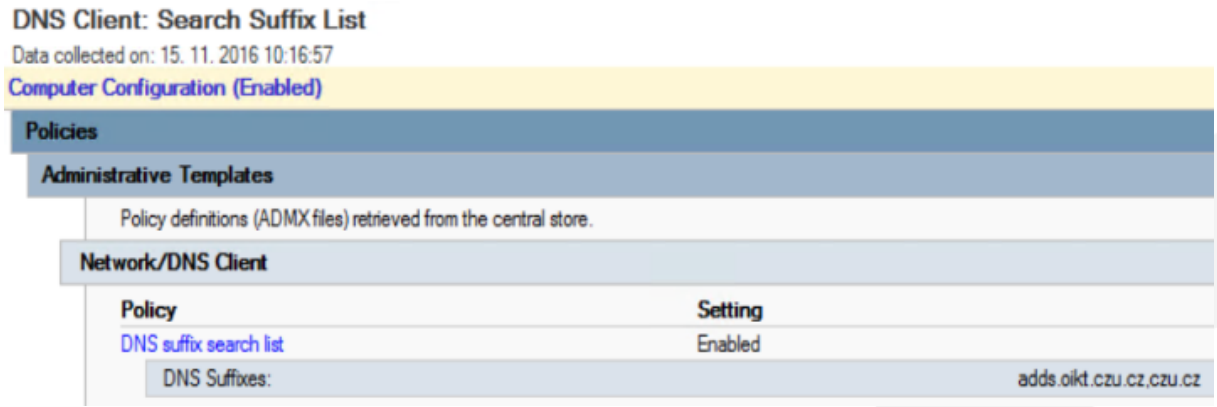
Vytvoření dopředné DNS zóny na řadičích „czu.cz“:

Nastavení DNS server forwarding (obecný) na řadičích „czu.cz“:

Vytvoření podmíněné přesměrování DNS zón na řadičích „czu.cz“:

Vytvoření podmíněné přesměrování DNS zón na řadičích „adds.oikt.czu.cz“:

Po dobu migrace se ještě umožní překlad krátkých jmen. To se zajistí přes GPO, která definuje DNS „**suffix search list**“.



6.1.4 Lokální Administrátor

Před migrací serverů anebo stanic existuje znalost credentials k lokálnímu účtu s administrátorským oprávněním.

6.1.5 Powershell policy

Veškeré migrační skripty doporučujeme spouštět na doménovém řadiči. Před spouštěním skriptů je nutné splnit následující:

1. PowerShell v3 a vyšší
2. Dále je nutno nastavit PowerShell exekuční politiku příkazem „*Set-ExecutionPolicy -ExecutionPolicy unrestricted*“.

6.1.6 Powershell remoting

Ověření, zda je možné alespoň po dobu migrace pouštět a volat Powershell skripty anebo ovládat přes „server manager“ vzdáleně. WinRM používá port TCP/5985.

6.1.7 Active Directory Recycle Bin (Koš)

Tímto příkazem lze otestovat, že koš je povolen a dají se provádět obnovy ve zdrojové doméně:

```
Get-ADobject -filter 'isdeleted -eq $true -and name -ne "Deleted Objects" -and (sAMAccountName -like "deleted_object*")' -includeDeletedObjects -property * | Restore-ADObject
```

6.1.8 Kontrola uživatelských GPO

Ve zdrojové doméně administrátor provede prověření všech GPO aplikovaných na uživatele. Ze všech GPO vybere pouze kritická nastavení GPO mající bezprostřední vliv na práci uživatelů a bez kterých není možné objekty migrovat. Tato nastavení GPO vyexportujte.

Tento požadavek k migraci bude obsahovat:

- HTML report politiky pomocí GPMC
- Zálohu politiky pomocí GPMC
- Pokud jsou zde skripty, certifikáty nebo se používají vlastní specifické adm šablony, tak je nutné přidat tyto soubory jako přílohu

6.1.9 Dešifrování všech souborů šifrovaných pomocí EFS

Před zakázáním samotného EFS prostřednictvím GPO je nutné provést dešifrování všech souborů na všech discích na všech stanicích.

Toho lze docílit např. použitím VBScriptu, který lze spustit na všech počítačích, např. jako součást logon skriptu.

Následně lze provést od-publikování šablony "**Basic EFS**" v rámci certifikační autority.

6.1.10 Windows XP a ADMT

V případě migrace stanic s operačním systémem Windows XP je třeba pro úspěch migrace zajistit následující kroky:

- Instalace SP2, nebo lépe SP3 (v případě, že není instalován)

- Instalace Patch: http://www.microsoft.com/en-us/download/details.aspx?id=7707
  Souvisí s chybou: http://blogs.technet.com/b/askds/archive/2009/10/19/admt-rodc-s-and-error-800704f1.aspx

Poznámka: Každá instalace následně vyžaduje restart počítače. Pozor na instalaci správné jazykové verze.

Podpora Windows XP a starších byla již ukončena a nelze garantovat úspěšnou migraci.

6.2 Příprava

Zde je popsáno, co je třeba nastavit na doménové úrovni.

6.2.1 Vztahy důvěry (Trusty)

Provádí: Lokální správce s právy pro úpravu konfigurace vztahu důvěry

V politice pro doménové řadiče je potřeba povolit „**Anonymous SID/Name translation**“

Nastavení neselektivního obousměrného Forest trust se zdrojovou doménou

- adds.oikt.czu.cz

6.2.1.1 Postup tvorby vztahů důvěry mezi zdrojovou a cílovou Active Directory doménou

Pro správné sestavení vztahů důvěry je předpokladem řádně nastavená DNS infrastruktura. Z hlediska migrace uživatelských účtů bude na straně vztahu důvěry vypnuta SID karanténa a SID filtrování.

V „adds.oikt.czu.cz“ Active Directory je potřeba nastavit vztahy důvěry pro cílovou doménu czu.cz.

V „czu.cz“ Active Directory připravte vztah důvěry pro „adds.oikt.czu.cz“ doménu:

Následuje vypnutí SID karantény na „adds.oikt.czu.cz“

Povolte SID History na „adds.oikt.czu.cz“

6.2.2 Migrační účty

Jeden účet v cílové doméně, který má FULL control práva nad objekty (users, computers, groups, contacts, profiles etc..) určené k migraci.[3]

Ideálně uživatelský účet z cílové domény s oprávněními doménového administrátora v doméně zdrojové (dále jen migrační účet).

Migrační účet musí mít práva lokálního administrátora na migračním serveru (DC).

6.2.2.1 Delegace oprávnění pro migrační uživatelský účet

Zařazení migračního účtu do doménové lokální skupiny.

6.2.3 ADMT migrační server

Jedná se o Windows 2012 R2 server (s podporou 128-bit encryption), na kterém běží Active Directory Migration tool (ADMT).

Migrační účet musí mít práva lokálního administrátora na migračním serveru.

Pro instalaci ADMT je třeba provést instalaci SQL Server (edice Express).

Z důvodů skriptovaných migrací, a BUGu v ADMT, se tento ADMT členský server, po dobu migrace, povýší na DC.

6.2.3.1 Konfigurace domén pro SID history

U instalace ADMT se může zvolit, aby automaticky nakonfiguroval domény k migraci SID history.[4]

6.2.3.2 Migrační logy

ADMT si detailně loguje každý krok migrace mezi doménami, včetně chyb, které ADMT nezobrazí. Je doporučeno prozkoumat LOG po každé migraci, či dokonce po každém kroku, takže objevíme případné chyby včas a máme čas na jejich řešení.

[3] Více informací: http://technet.microsoft.com/en-us/library/cc974398(WS.10).aspx

[4] Více informací: http://technet.microsoft.com/en-us/library/cc974410(v=ws.10).aspx

6.2.4 ADMT PES služba

ADMT používá Password Export Server (PES) k migraci hesel. PES se může nainstalovat na jakýkoli RW DC ve zdrojové doméně, který podporuje 128-bit šifrování.[5]

Před instalací této služby je potřeba ještě vytvořit šifrovací klíč na počítači v cílové doméně, kde je nainstalován ADMT.

Následuje spuštění instalačního průvodce, kterému je poskytnut výše vytvořený klíč. Následně proběhne restart serveru. Tato služba je ve výchozím stavu nastavena na StartUp Type Manual. Tzn. že před migracemi je potřeba tuto službu zapnout.

Důvod, proč nechat službu běžet pod účtem z cílové domény je bezpečnostní. Kdyby byl zvolen LOCAL SYSTEM, bylo by potřeba do skupiny „ADDS\Pre–Windows 2000 Compatible Access“ přidat skupiny Everyone a „Anonymous Logon“. [6]

Pokud se během instalace nedaří naimportovat PES klíč, i když je zadáno správné heslo, bude to pravděpodobně UAC. Je potřeba MSI pak spustit přes Elevated příkazovou řádku.[7]

6.2.5 AD objekty

Pro snažší dohledávaní skupin nebo při řešení případných po-migračních problémů:

- Původní jména všech účtů a skupin budou zálohovány do „extensionAttribute15“
- Původní DN všech účtů a skupin budou zálohovány do „PreferedOU“

Celá migrace bude probíhat na základě definovaných dávek. V rámci přípravy dávek se provede export, a zákazník bude označovat párované jména a počítače k migraci.

6.2.5.1 Hesla

Po dobu migrace se upraví politika hesel v obou doménách tak, aby nebyli uživatelé nuceni si hesla změnit. Tímto se zajistí unifikovaná hesla v novém i starém prostředí a usnadní případný rollback pro uživatele, u kterého by se vyskytly (po)migrační problémy.

[5] Více informací: https://connect.microsoft.com/site1164/program8540
[6] Více informací: https://technet.microsoft.com/en-us/library/cc974435%28v=ws.10%29.aspx?f=255&MSPPError=-2147217396
[7] Více informací: http://support.microsoft.com/en-us/kb/2004090

6.2.6 Vytvoření GPO pro podporu migrace

6.2.6.1 Konfigurace klientských stanic před fází migrace

Ve zdrojové doméně je třeba upravit konfiguraci migrovaného počítače. Toto bude provedeno hromadně pomocí objektu zásad skupiny (Group Policy).

Požadavky: (je zajištěno pomocí GPO)

- Konfigurace služby vzdálené registry
- Konfigurace sdílení souborů a tiskáren
- Konfigurace administrátorského sdílení Admin$
- Konfigurace brány firewall systému Windows
- Konfigurace síťových rozhraní
- Konfigurace DNS suffix search list
- Vypnutí Offline files

6.3 Fáze testovací

Před tím, než lze přistoupit k migraci produkčních dávek uživatelů, je potřeba ověřit migrační kroky na testovacích uživatelích. Kroky přípravy migrace jsou popsány v následující kapitole.

1. Definujte 5 testovacích uživatelů
2. Ověřte migraci skrze ADMT
3. Zkonzultujte výsledky s ČZU, a v případě chyb změňte migrační postup k novému pokusu
4. Otestujte GPO a login skripty v cílové doméně

6.4 Fáze migrační

Konflikty se mohou objevit během migrace a mohou zastavit ADMT migraci. Minimalizovat zdržení budeme kontrolou jmenných konfliktů ještě před spuštěním migrační dávky.

Požadavky:

- Soubor se zdrojovými jmény a cílovými jmény pro automatizované přejmenování počítačových stanic (definice migrační dávky)
- Před-migrační konfigurace počítačových stanic (GPO)

Migrace se bude pouštět na ADMT serveru pomocí skriptů. Migrační dávka se definuje tzv. IncludeFilem, který obsahuje seznam uživatelů a počítačů.

Je nutné vytvořit checklist, který bude po každé migrační dávce aktualizován, aby existovala evidence postupu migrací a jednotlivých migračních dávek.

6.4.1 Manuální před-migrace uživatelů a skupin

Před započetím ostrých migrací budou všechny účty a skupiny před-migrovány do cílové domény.

Tomuto kroku ještě předchází poslání seznamu pravděpodobně zastaralých účtů, který ČZU reviduje a rozhodne, zda-li budou součástí migrace. Pokud ne, objekty se přesunou do jiné OU, kde se disablují.

Doménové skupiny se migrují zvlášť a migrace skupin proveďte ještě před migrací uživatelských účtů a účtů počítačů. Migraci skupin pak probíhá naráz v jedné migrační dávce.

6.4.1.1 Postup migrace pro doménové skupiny

1) V rámci ADMT server je potřeba spustit „Group Account Migration Wizard“
2) Následuje výběr všech skupin ze zdrojové domény, které budou migrovány
3) Následuje migrace vybraných skupin do specifického kontejneru v cílové doméně

6.4.2 Servery

Aplikační servery budou migrovány dle vlastního migračního procesu, který není součástí této dokumentace.

6.4.3 Počítače

Migrace počítačů se skládá z několika navazujících kroků, přičemž platí, že počítače se migrují po dávkách společně s uživateli. Platí, že nejprve se migrují identity uživatelů a následně se migrují účty počítačů pomocí ADMT agenta.

Obecně se dá předpokládat, že na cca 5% počítačů migrace nebude úspěšná. Zde potom bude potřeba zasáhnout manuálně. Proto je doporučeno migrovat počítače v dávkách do 40 počítačů.

6.4.4 Uživatelé

Migrace uživatelů se skládá z několika navazujících kroků. Přičemž platí, že uživatelé se migrují po dávkách do 40 –ti uživatelů.

6.4.5 Postup testovací migrace obecně

1. Pomocí custom PowerShell skriptu (Automatizace ADMT) proveďte migraci testovacích doménových účtu ze zdrojového forestu do cílového Forestu
2. Konfigurujte GPO
    i. Nastavte GPO v cílovém forest dle požadavků
3. Přesuňte migrované účty počítačů ve zdrojové doméně/forestu do specifické organizační jednotky v Rootu strukty Active Directory
4. Proveďte jednou až dvakrát restart u těchto migrovaných účtů počítačů, tak aby se projevila aplikovaná GPO
5. Test aplikací
    i. Pro nově vytvořené testovací objekty ČZU otestuje přístup k jimi definovaným aplikacím.
    ii. Odsouhlasení funkční migrace
6. Podpis akceptačního protokolu a povolení pilotní migrace.

6.4.6 Postup migrace obecně

1. Pomocí custom PowerShell skriptu (Automatizace ADMT) je provedena migrace pilotních doménových účtu ze zdrojového forestu do cílového Forestu
2. Následuje přesunutí migrovaných účtů počítačů ve zdrojové doméně/forestu do specifické organizační jednotky v Rootu strukty Active Directory
3. Poté je nutné provést jednou až dvakrát restart u těchto migrovaných účtů počítačů, aby se projevila aplikovaná GPO
4. Pilotní migrace objektů
   Zde je stejný postup jako při testovací migraci, avšak s produkčními uživateli.

i. Test aplikací
ii. Migrace stanice do nového forest
iii. Odsouhlasení funkční migrace

6.5 Fáze finalizační

Finalizační fázi je možné zahájit až v okamžiku, kdy jsou všechna data i aplikace z domény adds.oikt.czu.cz přenesena do nového prostředí.

Jakmile budou všechny objekty zmigrovány, je potřeba změnit zpět některá nastavení, která byla potřebná pouze po dobu migrace.

1. Spuštění ADMT a "Security translation wizard" na všech serverech
2. Revize vytvořené lokální administrátory
3. Revize PowerShell politiku
4. Revize registry nastavení
5. Zrušení trustů, migrační GPO, DNS Conditional forwarding
6. Kontrola závislosti na zdrojové doméně (pokud stav migrace aplikačních serverů dovolí)
   i. Vypněte zdrojové DC po dobu 14 dnů
   ii. Nejsou-li hlášeny problémy, zrušte doménové trusty
   iii. Vyčistěte SID history na objektech v nové doméně

6.5.1 UPN suffixy

Nastavte UPN suffixy globálně na doménu „czu.cz":

- adds.oikt.czu.cz

Nastavte UPN suffixy globálně na doménu „adds.oikt.czu.cz":

- czu.cz

6.6 Rollback

Existence Rollback plánu napomáhá zkrátit výpadek v případě, kdy uživatel nemůže po migraci po delší dobu pracovat, například z důvodů:

- Nemůže se přihlásit
- Nemůže využívat prostředky
- Problém v lokálním profilu na pracovní stanici

Protože objekty ve zdrojové doméně zůstávají v podobě, jaké byli před migraci, můžeme obnovit předchozí stav:

- Povolením uživatelských objektů ve zdrojové doméně
- Instruovat uživatele odhlásit se z cílové domény
- Instruovat uživatele přihlásit se účtem zdrojové domény
- Ověřit, že uživatel může přistupovat k prostředkům
- Ověřit, že logon skripty a uživatelské profily fungují, jak se očekává
- Přepojte počítače do původní domény

7 Migrace z eDirectory do czu.cz

7.1 Předpoklady

- Uživatele s právy Domain Admins v cílové doméně Active Directory
- Práva NDS supervisor ve zdrojové Novell eDirectory/SUSE serveru
- Zmigrovaná data souborových serverů
- Zmigrované aplikace
- Uživatelé se budou ke stanicím přihlašovat doménovými účty (doména CZU.CZ)
- Stávající Novell Open Server/eDirectory musí splňovat požadavky na instalaci Novell Domain Services for Windows

7.1.1 Omezení platné pro migraci dat/souborů

- Data/soubory je sice možné migrovat postupně, ale je nutné provést migraci po určitých závislých celcích.
- Není možné přistupovat k souborům v rámci Novellu pomocí účtu z Active Directory a to ani s použitím Novell Domain Services for Windows. Naopak ano.
  OES2: http://www.novell.com/documentation/oes2/acc_dsfw_lx/data/bax16ko.html
  OES11: http://www.novell.com/documentation/oes11/acc_dsfw_lx/data/bax16ko.html
  OES2015: http://www.novell.com/documentation/oes2015/acc_dsfw_lx/data/bax16ko.html

7.2 Příprava

7.2.1 Párování uživatelských účtů

- Vytvoření seznamu všech aktivních uživatelských účtů z Novell eDirectory
- Vytvoření seznamu všech aktivních uživatelských účtů z domény czu.cz
- Provedení spárování účtů, vyřešení duplicity a nesrovnalosti

7.2.2 Vytvoření trustu mezi Windows Active Directory a Novell Domain Services for Windows

- Instalace dalšího Novell Open Serveru.
- Instalace Novell Domain Services for Windows
- Konfigurace Novell Domain Services for Windows a vytvořte “AD” domény **Novell.local**
- Vytvoření dvousměrného forest trust mezi doménou **Novell.local** a **czu.cz**

7.2.3 Vytvoření AD skupin pro mapování práv

- Vytvoření skupiny dle modelu AGDLP. Vytvoření Globální doménové skupiny, kde členové budou uživatelské účty a dále Lokální doménové skupiny, kde členové těchto skupin budou dříve vytvořené Globální doménové skupiny.
- Do globálních skupin je potřeba přidat uživatelské účty z Novell eDirectory (místo z AD), členství je možné díky existenci Forest trustu.

7.2.4 Přenesení práv na nově vytvořenou strukturu dat na FS

- Vytvoření odpovídající struktury adresářů (bude popsáno v designu souborových služeb)
- V této struktuře adresářů je potřeba nastavit práva a to přiřazením práv pro dříve vytvořené Doménové lokální skupiny

7.2.5 Kopie dat do nové struktury

- Rozdělení dat na logické celky tak, jak jsou mapovány jednotlivým skupinám uživatelů. Např. home adresáře uživatelů jedné fakulty, pracovní adresář v rámci katedry atd.
- Pozastavení sdílení pro uživatele po dobu migrace
- Za pomocí mapování (Novell Client) lze provést kopírování dat/souborů do nově vytvořené struktury adresářů na Windows File serveru
- Již překopírovaná původní data je potřeba nastavit do režimu read-only na straně Novell File services a zrušit jejich sdílení, aby nemohlo dojít ke změně dat na dvou místech a zároveň. V případě potřeby bude možnost se k těmto datům vrátit.
- Změna logon skriptů dotčeným uživatelům tak, aby se nově připojovali k datům/sdílení na Windows File serveru. Tím bude zajištěno, že pomocí účtu z Novell eDirectory se uživatelé dostanou ke svým datům

7.2.6 Migrace GroupWise

- Proveďte migraci poštovních služeb Novell GroupWise (popsáno v samostatném dokumentu)

7.3 Fáze testovací

1. Vytvoření 10 testovacích účů v eDirectory, přidělení oprávnění na sdílená data (účty je možné využít i pro testování dalších návazných aplikací)
2. Vytvoření identických testovacích účtů v doméně czu.cz a zařazení do Globálních skupin
3. Naplnění sdílení testovacími daty, vytvoření e-mailové schránky a přidělení přístup do aplikací
4. Přihlášení do účtů na testovací stanici, aby došlo k vytvoření lokálního profilu a aplikovaly se všechny změny dané instalací Novell Client

5. Vynucení odhlášení testovacích uživatelů pomocí GPO a deinstalaci Novell Client
6. Odebrání eDirectory účty z Global groups a zaměňte je za účty z AD
7. Otestování přihlášení pouze AD účtem
8. Ověření správného fungování systému

7.4 Fáze migrační

Migrace bude prováděna v dávkách automaticky pomocí skriptů a GPO.

1. Vynucení odhlášení testovacích uživatelů pomocí GPO a deinstalace Novell Client
2. Odebrání eDirectory účty z Global groups a záměna za účty z AD
3. Otestování přihlášení pouze AD účtem
4. Ověření správného fungování systému

7.5 Fáze finalizační

7.5.1 Odstranění Novell eDirectory

Po úspěšné migraci všech identit z Novell eDirectory a po úspěšné migraci všech aplikací závislých na Novell eDirectory. Po úspěšné migraci souborových služeb z Novellu, již toto prostředí není zapotřebí a je možné provést decomissioning celého prostředí.

- Odstraňte Trust
- Proveďte decommissioning Novell eDirecotery