# Active Directory – část 1

[ Povinné ]

**Active Directory**, nyní přesněji doménové služby **Active Directory** (AD DS, *Active Directory Domain Services*), je implementace adresářových služeb firmou Microsoft. Slouží jako úložiště informací o uživatelích, počítačích a službách, zajišťuje autentizaci uživatelů a počítačů a umožňuje také vyhledávání a přístup ke zdrojům. Tato funkcionalita se často označuje jako tzv. řešení identity a přístupu (IDA, *Identity and Access*).

## Řešení identity a přístupu

[ Povinné ]

Jak již bylo řečeno dříve, **Active Directory** poskytuje řešení identity a přístupu neboli **IDA**. Hlavním úkolem **IDA** je zajistit bezpečnost podnikových zdrojů (souborů, aplikací, databází apod.). Řešení **IDA** musí zajistit následující:

- **Uložení informací o uživatelích, skupinách, počítačích a jiných identitách**. Identita je pouze jakási abstraktní reprezentace entity, jenž provádí určité akce v podnikové síti. Nejběžnějším případem identity je samozřejmě uživatel, ale i další entity jako skupiny, počítače nebo služby mohou provádět různé akce v podnikové síti a musí být tedy reprezentovány odpovídajícími identitami. Kromě řady dalších informací, jenž se u každé identity uchovávají, musí být každá identita jednoznačně identifikována. K této identifikaci slouží **SID** (*Security identifier*), jednoznačný řetězec proměnlivé délky, který je unikátní v rámci celé sítě (lesa) Active Directory.
- **Autentizaci identit**. Server nikdy nesmí poskytnout identitě přístup ke zdroji, dokud neověří, že identita obsažená v požadavku pro přístup je validní. Ověření validity je zajištěno pomocí tajemství (*secret*), které zná pouze daná identita a **IDA**. Identita se musí prokázat tímto tajemstvím a to je porovnáno s informací uloženou v úložišti identit. Tento proces se označuje jako *autentizace*.
- **Řízení přístupu**. Ne všechny *autentizované* identity mají mít přístup k určitému zdroji, navíc je často potřeba rozlišovat více úrovní přístupu k jednomu zdroji. Tuto funkcionalitu zajišťuje řízení přístupu. Řízení přístupu je realizováno formou seznamů pro řízení přístupu (ACL, *Access Control List*). Tyto seznamy pro každý zdroj přesně definují oprávnění určující úroveň přístupu pro jednotlivé identity. Oprávnění mohou být různá, záleží na typu zdroje, např. pro soubor to budou oprávnění pro čtení, zápis apod., pro tiskárnu oprávnění pro tisk, správu tiskové fronty atd., pokud nejsou oprávnění pro nějakou identitu definována, znamená to, že daná identita nemá k danému zdroji žádný přístup.
- **Auditování**. Asi vždy existuje riziko, že některá identita získá přístup ke zdroji, ke kterému přístup mít nemá, případně získá vyšší úroveň oprávnění, než jí náleží. Pro tyto případy je důležité, aby existovaly mechanismy umožňující provádět auditování přístupů k jednotlivým zdrojům.

Řešení **IDA** ve Windows Server je složeno z pěti komponent, kde každá komponenta má specifickou funkcionalitu. Patří zde:

- **Doménové služby Active Directory** (AD DS, *Active Directory Domain Services*). AD DS zajišťuje uložení identit, jejich správu, autentizaci a autorizaci. Také poskytuje možnosti vyhledávání zdrojů a jejich sdílení.
- **Adresářové služby Active Directory** (AD LDS, *Active Directory Lightweight Directory Services*). AD LDS lze pokládat za odlehčenou verzi **Active Directory**, jenž poskytuje podporu aplikacím využívajícím adresářové služby. Je založena na stejném kódu jako AD DS, jen obsahuje, a také replikuje, pouze data týkající se aplikací. AD LDS využívá pro komunikaci standardizovaný protokol LDAP (*Lightweight Directory Access Protocol*) používaný většinou aplikací využívajících adresářové služby. AD LDS také podporuje více datových úložišť s vlastními schématy, SSL porty a protokoly událostí. I přesto, že AD LDS není nijak závislé na AD DS, může

využívat AD DS pro *autentizaci* identit. Ovšem i AD LDS lze využít pro *autentizaci*, čehož se často využívá hlavně v nechráněných sítích, kde by nasazení AD DS představovalo velké bezpečnostní riziko.

- **Certifikační služby Active Directory** (AD CS, *Active Directory Certificate Services*). AD CS slouží k vytváření certifikačních autorit (CA, *Certificate Authority*) vydávajících digitální certifikáty, které vážou identitu k odpovídajícímu soukromému (*private*) klíči. Certifikáty mají široké využití, lze je použít pro *autentizaci* uživatelů a počítačů, poskytují možnosti *autentizace* přes *web*, podporují čipové (*smart)* karty, využívající se u virtuálních privátních sítí (VPN, *Virtual Private Network*), protokolu IPSec nebo EFS (*Encrypting File System*) a mnoho dalších. AD CS poskytuje jednoduchou správu a vydávání certifikátu, jak manuální, tak automatické. Slouží také k vytváření vztahů důvěry (*trust*), jenž umožňují důvěřovat externím identitám a naopak prokazovat se externím zdrojům.
- **Služby oprávnění Active Directory** (AD RMS, *Active Directory Rights Management Services*). AD RMS zajišťuje ochranu dokumentů. Zatímco ACL umožňují zabezpečit dokumenty z hlediska neoprávněného přístupu, nemohou ovlivnit, co se děje s dokumentem a jeho obsahem po tom, co je úspěšně otevřen.
- **Federační služby Active Directory** (AD FS, *Active Directory Federation Services*). AD FS poskytuje SSO (*Single Sign-On*) řešení, tedy identity autentizované v jedné síti mohou přistupovat ke zdrojům v jiné síti. AD FS tedy umožňuje rozšířit **IDA** mezi ověřené partnery a navíc napříč více platforem, lze tedy využít i jiná prostředí než systém Windows. Ve federačním prostředí si každý partner spravuje své vlastní identity, může ale také bezpečně přijímat identity od jiných partnerů.

## Komponenty

[ Povinné ]

Komponenty lze rozdělit do dvou kategorií. První kategorii tvoří programové komponenty, které zajišťují samotnou funkcionalitu **Active Directory**. Druhá kategorie pak obsahuje logické komponenty, jenž určují logickou strukturu sítě.

Programové komponenty ovlivňují vlastnosti a funkcionalitu **Active Directory**. Mezi programové komponenty lze zařadit:

- **Řadiče domény** (DC, *Domain Controller*). Řadiče domény jsou servery plnící roli AD DS, také na nich běží centrum distribuce klíčů Kerberos (KDC, *Kerberos Key Distribution Center*), které zajišťuje *autentizaci* a další důležité služby **Active Directory**.
- **Úložiště dat Active Directory**. Datové úložiště identit a jiných informací z domény hostované na řadičích domény. Fyzicky je uloženo ve formě souboru **Ntds.dit** v adresáři ***<systém>*\Ntds**, kde *<systém>* je kořenový adresář systému Windows. Je rozděleno na několik částí zahrnující schéma, konfiguraci, globální katalog a část obsahující všechny objekty domény, označovaná jako tzv. *domain naming context*.
- **Systémový oddíl** (SYSVOL, *System Volume*). Datové úložiště, kde se ukládají zásady skupiny, skripty a další data sdílená mezi všemi řadiči domény. Na rozdíl od úložiště dat je systémový oddíl tvořen kolekcí adresářů s kořenovým adresářem v ***<systém>*\SYSVOL**, kde *<systém>* je kořenový adresář systému Windows. Replikaci dat v tomto adresáři zajišťuje služba replikace souborů (FRS, *File Replication Service*), jenž neustále monitoruje obsah systémového oddílu a při jakékoliv změně ihned iniciuje replikaci. Od Windows Server 2008 se místo FRS spíše využívá novější replikace distribuovaného souborového systému (DFSR, *Distributed File System Replication*), která je výrazně efektivnější a netrpí některými problémy FRS.
- **Funkční úroveň** (*Functional Level*). Ovlivňuje celkovou funkcionalitu domény nebo lesa **Active Directory**. Čím vyšší úroveň je nastavena, tím širší jsou možnosti **Active Directory**, ovšem za cenu zpětné kompatibility. Existuje několik funkčních úrovní domény, resp. lesa, **Active Directory**: *Windows 2000 native* (od Windows Server 2012 již nepodporováno), *Windows Server 2003* (od Windows Server 2012 označeno za zastaralé, od Windows Server 2016

nepodporováno), *Windows Server 2008* (od Windows Server 2019 nepodporováno)*, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2* a *Windows Server 2016*. Každá funkční úroveň také určuje nejnižší verzi systému Windows, jenž musí běžet na všech řadičích domény v dané doméně, resp. lese. Windows Server 2019 novou funkční úroveň nepřináší.

Logické komponenty, určující strukturu sítě, vycházejí ze systému **DNS**. Instalace **Active Directory** přímo vyžaduje přítomnost **DNS** serveru, ten je také často přítomen na stejném serveru jako **Active Directory**. Mezi logické komponenty patří:

- **Doména**. Doména je základní administrativní jednotka **Active Directory** ohraničující rozsah platnosti identit a nastavení (zásad). Reprezentuje také replikační hranici, kdy všechny řadiče domény replikují oddíl domény (*domain partition*), jenž je součástí datového úložiště. Oddíl domény obsahuje informace o identitách, zásadách a dalších objektech, je tedy zároveň také úložištěm identit. Protože toto úložiště identit je replikováno mezi všechny řadiče domény, může každou identitu *autentizovat* kterýkoliv řadič domény. Jakýkoliv řadič domény může také modifikovat objekty v datovém úložišti, tyto změny budou automaticky replikovány mezi ostatní řadiče domény. Mezi doménami lze také vytvářet vztahy důvěry (*trust*). Pro definici struktury sítě kopírují domény hierarchii systému **DNS**. Každá doména je jednoznačně identifikována doménovým jménem, všechny počítače v dané doméně pak sdílejí **DNS** *suffix* tohoto jména. Lze říci, že zatímco z hlediska **DNS** patří do určité **DNS** domény počítače sdílející stejný **DNS** *suffix*, z hlediska **Active Directory** patří do stejně pojmenované **Active Directory** domény počítače sdílející stejné datové úložiště (které je vždy sdílené pouze řadiči domény příslušné domény).
- **Les** (*Forest*). Les je kolekce jedné nebo více domén, kde první přidaná doména v každém lese se označuje jako tzv. kořenová doména lesa (*forest root domain*). Všechny domény v daném lese sdílí stejnou konfiguraci sítě, schéma, globální katalog a jsou spojeny důvěrou protokolu Kerberos. Les také reprezentuje bezpečnostní hranici, kdy data nikdy nejsou replikována přes hranice lesa.
- **Strom** (*Tree*). Strom je kolekce domén sdílející souvislou část prostoru jmen **DNS**. Přesněji pokud les obsahuje nějaké dvě domény takové, že jedna doména je subdoménou té druhé, tvoří tyto domény strom.
- **Organizační jednotky** (OUs, *Organizational Units*). **Active Directory** je hierarchická databáze jak z pohledu struktury sítě (domény, lesy, stromy), tak z pohledu vnitřní struktury. Objekty v úložišti dat mohou být umísťovány do kontejnerů, ty zanořovány do dalších kontejnerů (ale pouze do hloubky 12 úrovní) a obecně takto vytvářet celou hierarchii objektů. Organizační jednotka je speciální typ kontejneru, který navíc poskytuje možnosti samostatné administrace objektů v tomto kontejneru a jeho subkontejnerech. K organizačním jednotkám mohou být připojovány objekty zásad skupiny obsahující nastavení, které se má aplikovat na veškeré objekty v této organizační jednotce. Zároveň je organizační jednotka nejnižší strukturou pro seskupování objektů v rámci **Active Directory**.
- **Místa** (*Sites*). V kontextu **Active Directory** je místo (site) část podnik vyznačující se dobrou konektivitou. Místa tvoří hranice pro replikaci a používání služeb. Řadiče domény ve stejném místě se replikují velice rychle (v rámci sekund), zatímco replikace mezi dvěma řadiči domény z různých míst je problematická (výpadky apod.) a značně pomalá (slabá linka atd.). Stejně tak při využívání služeb budou klienti preferovat nejbližší servery (v daném místě), které jsou schopny reagovat na požadavky klientů rychle. Místa spíše rozdělují strukturu sítě po fyzické stránce, než po logické, jak to dělaly dříve zmíněné komponenty.

## Instalace

[ Povinné ]

Instalace, nebo přesněji povýšení serveru do role **AD DS** se provádí pomocí průvodce přidáním role nebo pomocí Windows PowerShellu. (Příkaz **dcpromo** známý z předchozích verzí Windows Serveru již

použít nelze.) Před samotnou instalací je ovšem dobré si promyslet několik věcí potřebných pro instalaci nebo budou zásadně ovlivňovat strukturu a funkcionalitu **Active Directory**:

- **Název domény**. Každá doména musí mít přiřazeno unikátní **DNS** doménové jméno a **NetBIOS** jméno (pokud není specifikováno, je použito prvních 15 znaků z nejnižší části **DNS** doménového jména).
- **Funkční úroveň**. Pokud musí být v doméně podporovány řadiče domény s předchozími verzemi systému Windows, musí být na úrovni domény i lesa nastaveny funkční úrovně, jenž tyto starší verze podporují. Naopak vyšší funkční úrovně poskytují širší možnosti **Active Directory** a také vyšší bezpečnost. Je tedy dobré volit nejvyšší možnou úroveň, při které jsou podporo-vány všechny potřebné verze systému Windows.
- **Nastavení DNS**. Přítomnost **DNS** serveru je přímo vyžadována pro instalaci **Active Directory**. Systém **DNS** zde neplní jen úlohu překladu doménových jmen na IP adresy, ale také umožňuje lokalizaci služeb a poskytuje další potřebné informace pro činnost **Active Directory**. Většinou se nasazuje **DNS** server, jenž je součástí serverových systému Windows. Vytvářené zóny se navíc často integrují do **Active Directory**, což je velice doporučováno, jelikož jsou v tomto případě do dané zóny automaticky zapsány veškeré potřebné informace pro činnost **Active Directory** (jinak se musí tyto informace doplnit manuálně). Samozřejmě lze využít také **DNS** servery třetích stran.
- **Nastavení IP adres**. Instalace **Active Directory** vyžaduje, aby měl daný server přidělené statické IP adresy a také IP adresu **DNS** serveru (často vlastní, jelikož je zároveň **DNS** serverem).
- **Účet administrátora**. Instalace **Active Directory** vyžaduje přítomnost lokálního účtu administrátora, který má neprázdné heslo.
- **Umístění dat**. Při instalaci je potřeba specifikovat umístění souboru **Ntds.dit**, jenž reprezentuje datové úložiště **Active Directory**, a také kořenový adresář systémového oddílu. Výchozí nastavení využívá adresáře ***<systém>*\Ntds** resp. ***<systém>*\SYSVOL**, kde *<systém>* je kořenový adresář systému Windows. Lze ovšem zvolit i jiné umístění, např. na odlišných discích, což může urychlit manipulaci s daty a tedy i práci **Active Directory**.

## Základní objekty [ Povinné ]

Jak již bylo řečeno dříve, **Active Directory** je adresářová služba obsahující informace o uživatelích, počítačích a dalších entitách. Tyto entity jsou reprezentovány objekty příslušného typu a informace o těchto entitách jsou uloženy ve formě atributů daného objektu. Ze všech typů entit lze vyzdvihnout hlavně tři, se kterými se pracuje nejčastěji. Patří zde uživatelé, skupiny a počítače.

V **Active Directory**, jakožto řešení **IDA**, je uživatel asi hlavní komponenta identity, proto je důležité vyznat se jak v uživatelských účtech, tak v úkonech, které se jich týkají. Efektivní práce s uživatelskými účty má výrazný vliv na celkovou produktivitu. **Active Directory** běžně obsahuje i tisíce uživatelských účtů, pracovat s každým účtem zvlášť je nemyslitelné. Je tedy potřeba celou správu účtů maximálně automatizovat. Hromadné vytváření účtů lze automatizovat:

- Použitím **šablon účtů** (*account templates*)
- Nástrojem **dsadd**
- Importem pomocí **csvde** nebo **ldifde**
- Příkazy **Windows PowerShell**
- **VBSkriptem** (*VBScript*)

Správu účtů, tedy provádění změn, lze pak automatizovat:

- Pomocí **ADUC** (*Active Directory Users and Computers*)
- Nástroji **dsget** a **dsmod**
- Příkazy **Windows PowerShell**
- **VBSkriptem** (*VBScript*)

Dalším důležitým typem objektů jsou skupiny. Hlavním úkolem skupin je umožnit jednoduchou správu kolekcí objektů, nejčastěji uživatelů nebo počítačů. Další využití nějaké skupiny je závislé na jejím typu. Existují celkem dva typy skupin:

- **Distribuční** (*Distribution*). Distribuční skupiny jsou určeny primárně pro *e-mailové* aplikace. Zpráva zaslaná na distribuční skupinu je zaslána všem členům této skupiny. Jelikož nemají **SID** (*Security Identifier*), nelze jim nastavovat oprávnění pro přístup ke zdrojům.
- **Bezpečnostní** (*Security*). Bezpečnostní skupiny mají **SID**, lze jim tedy přidělovat oprávnění pro přístup ke zdrojům (přesněji mohou být použity jako záznamy oprávnění (*permission entries*) v ACL). Bezpečnostní skupiny mohou být použity také jako distribuční skupiny, což se ovšem nedoporučuje. **SID** všech bezpečnostních skupin, kterých je uživatel členem, se totiž přidávají do jeho *security access tokenu*. Náhrada distribučních skupin bezpečnostními tedy znamená zbytečný nárůst **SID** v *security access tokenu* daného uživatele.

Kromě typu skupiny je důležitý také její rozsah (*group scope*). Rozsah skupiny ovlivňuje, co může daná skupina obsahovat, k čemu může patřit a kde může být použita. Každý rozsah skupiny je charakterizován vlastnostmi ze tří kategorií:

- **Replikace** (*Replication*). Kde je skupina definována a kam je replikována?
- **Členství** (*Membership*). Jaké typy bezpečnostních objektů[1] (*security principals*) může skupina obsahovat? Může skupina obsahovat bezpečnostní objekty z důvěryhodných domén?
- **Dostupnost** (*Availability*). Kde může být skupina použita? Může být skupina přidána do jiné skupiny? Může být skupina přidána do ACL?

Existují celkem čtyři rozsahy skupin:

- **Lokální** (*Local*). Lokální skupiny jsou definovány a také k dispozici pouze na konkrétním počítači. Jsou uloženy v **SAM** (*Security Accounts Manager*) databázi daného počítače. Lokální skupiny jsou jedinou možností jak spravovat přístup ke zdrojům v pracovních skupinách. V případě domén ovšem nemají příliš využití.
  - **Replikace**. Lokální skupiny jsou definovány v lokální **SAM** databázi, nedochází k replikaci.
  - **Členství**. Lokální skupina může obsahovat:
    - Bezpečnostní objekty z domény (uživatele, počítače, globální nebo doménově lokální skupiny).
    - Uživatele, počítače a globální skupiny z jakékoliv domény v daném lese.
    - Uživatele, počítače a globální skupiny z jakékoliv důvěryhodné domény.
    - Univerzální skupiny definované v jakékoliv doméně daného lesa.
  - **Dostupnost**. Lokální skupiny mohou být použity pouze na daném počítači a pouze tam je lze přidat do ACL. Lokální skupina nemůže být přidána do žádné jiné skupiny.
- **Doménově lokální** (*Domain local*). Doménově lokální skupiny se primárně používají ke správě oprávnění pro přístup ke zdrojům.
  - **Replikace**. Doménově lokální skupiny jsou definovány na úrovni domény (v tzv. *domain naming context*). Tyto skupiny, spolu s informacemi o jejich členství (atribut *member*), jsou replikovány na všechny řadiče domény v dané doméně.
  - **Členství**. Doménově lokální skupina může obsahovat:
    - Bezpečnostní objekty z domény (uživatele, počítače, globální nebo doménově lokální skupiny).
    - Uživatele, počítače a globální skupiny z jakékoliv domény v daném lese.

[1] Bezpečnostní objekt (*security principal*) je jakýkoliv objekt obsahující **SID**, tedy objekt, jemuž je možné přidělovat oprávnění pro přístup ke zdrojům

    - Uživatele, počítače a globální skupiny z jakékoliv důvěryhodné domény.
    - Univerzální skupiny definované v jakékoliv doméně daného lesa.
  - **Dostupnost**. Doménově lokální skupiny lze přidat do ACL jakéhokoliv zdroje v doméně. Navíc mohou být doménově lokální skupiny členy jiných doménově lokálních a lokálních skupin.

  Je vidět, že z hlediska členství není žádný rozdíl mezi lokálními a doménově lokálními skupinami. Ovšem replikace a dostupnost doménově lokálních skupin umožňuje jejich využití v rámci celé domény, proto se doménově lokální skupiny preferují před lokálními skupinami.
- **Globální** (*Global*). Globální skupiny se primárně používají pro definici kolekce doménových objektů, jenž plní stejnou roli v podniku.
  - **Replikace**. Globální skupiny jsou definovány na úrovni domény (v tzv. *domain naming context*). Tyto skupiny, spolu s informacemi o jejich členství (atribut *member*), jsou replikovány na všechny řadiče domény v dané doméně.
  - **Členství**. Globální skupina může obsahovat pouze uživatele, počítače a jiné globální skupiny z dané domény.
  - **Dostupnost**. Globální skupiny mohou být použity všemi příslušníky dané domény (*domain members*), dalšími doménami v daném lese a také všemi důvěryhodnými externími doménami. Globální skupiny mohou být členy doménově lokálních a univerzálních skupin v dané doméně či v daném lese. Také mohou být členy doménově lokálních skupin z důvěryhodných domén. Globální skupiny lze přidat do ACL v dané doméně, v daném lese nebo v důvěryhodné doméně.

  Je vidět, že globální skupiny mají nejvíce omezené členství, ale největší dostupnost v rámci domény, lesa a důvěryhodných domén, proto je lze s výhodou využít pro definici rolí.
- **Univerzální** (*Universal*). Univerzální skupiny mají využití hlavně v lesích obsahujících více domén (*multidomain forests*). Umožňují definovat role, nebo spravovat zdroje, které jsou rozprostřeny přes více domén.
  - **Replikace**. Univerzální skupiny jsou definovány v jedné konkrétní doméně, jsou ovšem replikovány v rámci globálních katalogů. Objekty uložené v globálním katalogu jsou přístupné v celém lese.
  - **Členství**. Univerzální skupina může obsahovat uživatele, globální skupiny a jiné univerzální skupiny z kterékoliv domény z daného lesa.
  - **Dostupnost**. Univerzální skupiny mohou být členy jiných univerzálních skupin nebo doménově lokálních skupin kdekoliv v daném lese. Univerzální skupiny mohou být také použity ke správě zdrojů kdekoliv v daném lese.

Posledním důležitým typem objektů jsou počítače. Často se zapomíná, že i počítače jsou bezpečnostní objekty (*security principals*) a tedy mohou náležet do skupin, mít definována oprávnění pro přístup ke zdrojům a mohou na ně být aplikovány zásady skupiny. I počítače, stejně jako uživatelé, se musí přihlašovat do domény, jejich přihlašovací jméno a heslo mění systém Windows automaticky co 30 dní.

# Společné úkoly

- Pro přístup na server **file** (a jiné) přes síťové rozhraní *Default switch* je nutné použít jeho plně kvalifikované doménové jméno **file.nepal.local**
- Přístupové údaje na server **file**: **nepal\hstudent** heslo: **aaa**
- Rozsah IP adres přidělených z *Default switch* se může od níže uvedeného rozsahu lišit.

## Lab LS00 – konfigurace virtuálních stanic

[ Projít ]

Připojte sítové adaptéry stanic k následujícím virtuálním přepínačům:

| Adaptér (MAC suffix) | LAN1 (-01) | LAN2 (-02) | LAN3 (-03) | LAN4 (-04) |
|---|---|---|---|---|
| **w10-base** | Nepřipojeno | Private1 | Nepřipojeno | Nepřipojeno |
| **w10-domain** | Nepřipojeno | Private1 | Nepřipojeno | Nepřipojeno |
| **w2016-base** | Nepřipojeno | Private2 | Nepřipojeno | Nepřipojeno |
| **D+R+C w2016-dc** | Nepřipojeno | Private1 | Nepřipojeno | Nepřipojeno |
| **D+R+C w2016-repl** | Nepřipojeno | Private1 | Nepřipojeno | Nepřipojeno |

- v případech, kdy je potřeba přistupovat na externí síť, připojte adaptér **LAN1** k přepínači *Default switch*.
- Servery D+R+C w2016-dc a D+R+C w2016-repl je nutné spouštět společně
- Tip: stanice **D+R+C w2016-dc** a **D+R+C w2016-repl** spusťte na začátku cvičení.

## Lab LS01 – Instalace Active Directory

[ Provést ]

**Cíl cvičení**

Povýšit server do role řadiče domény (prvního pro danou doménu)

**Potřebné virtuální stroje**

**w2016-base**

1. Na **w2016-base** nastavte statickou IPv4 adresu **192.168.64.5**
   a. Otevřete **Network and Sharing Center**, zvolte LAN2 a pak properties
      - Zvolené síťové rozhraní musí odpovídat *Private1*, standardně to je LAN2
   b. Vyberte Internet Protocol Version 4 (TCP/IPv4) a zvolte properties
   c. Zvolte Use the following IP address a jako IP address zadejte **192.168.64.5**
   d. Klikněte do zadávacího pole u Subnet mask, maska podsítě bude doplněna automaticky
   e. Potvrďte OK
2. Spusťte **Server Manager**
   a. Start → **Server Manager**
3. Nainstalujte roli **Active Directory Domain Services**
   a. Vyberte Add Roles and Features z nabídky Manage
   b. Pokračujte Next >
   c. Vyberte Role-based or feature-based installation a pokračujte Next >
   d. Vyberte aktuální server a pokračujte Next >

e. V seznamu rolí vyberte Active Directory Domain Services, potvrďte přidání potřebných funkcí Add Features a pokračujte třikrát Next >
f. Potvrďte instalaci Install
g. Po dokončení instalace najdete v notifikacích Server Manageru odkaz na Promote this server to a domain controller

4. V konfiguračním průvodci (Active Directory Domain Services Configuration Wizard)
   a. Zvolte Add a new forest
   b. Do pole root domain name zadejte **testing.local** a pokračujte Next >
   c. Nastavte funkční úroveň lesa i domény **Windows Server 2016**
   d. Ověřte zaškrtnutí instalace DNS serveru a globálního katalogu
   e. Zadejte (a potvrďte) heslo (**aaa**) pro Directory Services Restore Mode a pokračujte Next >
   f. Nyní jsme upozorněni na nemožnost delegace v nadřazené **DNS** zóně. Jelikož v tuto chvíli žádná neexistuje, můžeme to ignorovat. Next >
   g. Zadejte **NetBIOS** název domény (max. 15 znaků[2]) – ponechte **TESTING**. Next >
   h. Zadejte cesty k databázím Location for Database, Log Files, and SYSVOL (ponechte výchozí). Next >
   i. Zkontrolujte zadané údaje a zobrazte si odpovídající **skript pro PowerShell** (View Script). Pokračujte Next >
   j. Prohlédněte si výsledky kontroly prerekvizit.
      - **NEPOKRAČUJTE!!!** Dále se bude využívat už jen **w2016-dc**.

## Lab LS02 – ADUC (Active Directory Users and Computers) [ Na cvičeních ]

## Lab LS03 – Připojení klienta do domény [ Provést ]

**Cíl cvičení**

Připojit počítač do domény a ověřit připojení přihlášením do domény

**Potřebné virtuální stroje**

**w2016-dc** (D+R+C w2016-dc)
**w2016-repl** (D+R+C w2016-repl)
**w10-base**

1. Připojte **w10-base** do domény **testing.local**
   a. Otevřete System Properties
      - Alternativně: System z kontextové nabídky **Win+X** (resp. v levém dolním rohu taskbaru)
      - Alternativně: Properties z kontextové nabídky nad Computer (v průzkumníku)
   b. Na záložce Computer Name zvolte Change…
   c. V části Member of vyberte Domain a jako název domény zvolte **testing.local**
   d. Potvrďte OK
   e. Při výzvě o zadání účtu použijte účet **administrator@testing.local** s heslem **aaa**
   f. Potvrďte OK
   g. Po připojení do domény proveďte restart

[2] 15 bytů v kódování UTF-8

2. Na **w2016-dc** ověřte vytvoření účtu počítače
   a. Otevřete **Active Directory Users and Computers**
      1. Start → Administrative Tools → **Active Directory Users and Computers**
   b. Vyberte kontejner Computers
   c. Ověřte existenci účtu pro počítač **w10-base**
3. Na **w10-base** se přihlaste jako uživatel **homer** do domény **testing.local**
   a. Použijte uživatelské jméno **testing\homer** nebo **homer@testing.local**, heslo **aaa**

# Studentské úkoly

## Lab S01 – Delegace práv

[ Povinné ]

**Cíl cvičení**

Umožnit uživateli vytvářet a modifikovat uživatelské účty v dané organizační jednotce

**Potřebné virtuální stroje**

**w2016-dc** (D+R+C w2016-dc)
**w10-domain**

**Další prerekvizity**

Účet uživatele **homer** v doméně **testing.local**, organizační jednotka **brno** pod **testing.local**, nainstalovaný **RSAT** pro Windows 10 64-bit en[3]

1. Na **w10-domain** se přihlaste jako uživatel **homer** do domény **testing.local**
2. Ověřte nainstalovaní nástrojů pro správu doménových služeb **Active Directory**
   a. Control Panel → Programs → Programs and Features
   b. V levém panelu vyberte Turn Windows features on or off
   c. Zadejte přihlašovací údaje uživatele s právy lokálního správce **.\student** s heslem **aaa**
   d. Remote Server Administration Tools → Role Administration Tools → AD DS and AD LDS Tools → AD DS Tools, ověřte zaškrtnutí AD DS Snap-ins and Command-line Tools
   e. Potvrďte OK
      - Ve starších verzích se po instalaci **RSAT** musely tyto nástroje povolit
3. Ověřte, že nemůžete přidávat ani modifikovat účty v organizační jednotce **brno**
   a. Otevřete **Active Directory Users and Computers**
      1. Start → Windows Administrative Tools → Active Directory Users and Computers
   b. Zkuste přidat nový uživatelský účet nebo změnit stávající
      - Možnosti přidávání účtů budou úplně chybět, modifikace nebude proveditelná díky nedostačujícím oprávněním
4. Na **w2016-dc** delegujte práva na vytváření a modifikaci účtů pro organizační jednotkou **brno** na uživatele **homer**
   a. Otevřete **Active Directory Users and Computers**
      1. Start → Windows Administrative Tools → Active Directory Users and Computers
   b. Klikněte pravým na organizační jednotku **brno** a vyberte Delegate Control…
   c. Pokračujte Next >
   d. V části Users or Groups zvolte Add…
   e. V Enter the object names to select zadejte **homer** a zvolte Check Names pro ověření validity účtu
   f. Potvrďte OK a pokračujte Next >
   g. V další části Tasks to Delegate ponechte Delegate the following common tasks, vyberte Create, delete and manage user accounts a pokračujte Next >
   h. Proveďte delegaci práv pomocí Finish

[3] https://www.microsoft.com/en-us/download/details.aspx?id=45520

5. Na **w10-domain** ověřte, že již můžete přidávat i modifikovat účty v organizační jednotce **brno**
   a. Otevřete **Active Directory Users and Computers**
      1. Start → Administrative Tools → Active Directory Users and Computers
   b. Klikněte pravým na organizační jednotku **brno** a zvolte New → User
   c. Vytvořte nového uživatele a ověřte, že lze po vytvoření modifikovat

## Lab S02 – Správa Active Directory pomocí příkazové řádky [ Volitelné ]

**Cíl cvičení**

Seznámit se se základními nástroji příkazové řádky pro vytváření, modifikaci a mazání objektů **Active Directory**

**Potřebné virtuální stroje**

**w2016-dc** (D+R+C w2016-dc)

**Další prerekvizity**

Organizační jednotka **brno** pod **testing.local**

1. Na **w2016-dc** se přihlaste jako uživatel **administrator** do domény **testing.local**
2. přidejte pomocí **dsadd** nového uživatele **lisa** do organizační jednotky **brno**, křestní jméno nastavte na **Lisa** a heslo zvolte **aaa**
   a. Spusťte příkaz **dsadd user CN=lisa,OU=brno,DC=testing,DC=local -fn Lisa -pwd aaa**
   b. Ověřte v **Active Directory Users and Computers**, že uživatel byl přidán
3. Vytvořte pomocí **dsadd** organizační jednotku **vut** pod organizační jednotkou **brno**
   a. Spusťte příkaz **dsadd ou OU=vut,OU=brno,DC=testing,DC=local**
4. Ověřte v **Active Directory Users and Computers**, že organizační jednotka byla vytvořena
   a. Přesuňte pomocí **dsmove** uživatele **lisa** do organizační jednotky **vut**
   b. Spusťte příkaz **dsmove CN=lisa,OU=brno,DC=testing,DC=local -newparent OU=vut,OU=brno,DC=testing,DC=local**
5. Ověřte přesunutí vypsáním všech uživatelů v organizační jednotce **vut** pomocí **dsquery**
   a. Spusťte příkaz **dsquery user OU=vut,OU=brno,DC=testing,DC=local**
6. Změňte uživateli **lisa** příjmení pomocí **dsmod**
   a. Spusťte příkaz **dsmod user CN=lisa,OU=vut,OU=brno,DC=testing,DC=local -ln Simpson**
7. Ověřte změnu příjmení vypsáním aktuálního příjmení uživatele **lisa** pomocí **dsget**
   a. Spusťte příkaz **dsget user CN=lisa,OU=vut,OU=brno,DC=testing,DC=local -ln**
8. Smažte organizační jednotku **vut** i s celým jejím obsahem pomocí **dsrm**
   a. Spusťte příkaz **dsrm OU=vut,OU=brno,DC=testing,DC=local -subtree**
   b. Potvrďte smazání
   c. Ověřte v **Active Directory Users and Computers**, že organizační jednotka byla smazána