

Serverové systémy Microsoft Windows

IW2/XMW2 2013/2014

Jan Fiedor

ifiedor@fit.vutbr.cz

Fakulta Informačních Technologií

Vysoké Učení Technické v Brně

Božetěchova 2, 612 66 Brno

Revize 5. 3. 2014

Active Directory

Úvod, Služby, Komponenty, Instalace

Active Directory

- Implementace adresářových služeb firmou MS
 - Centralizovaná správa a řízení sítí Microsoft
 - Rozšíření standardu X.500 a protokolu LDAP
- Obsahuje informace o
 - Uživatelích, skupinách, počítačích, ...
 - Službách, topologii sítě, ...
- Zajišťuje
 - Autentizaci identit (uživatelů, počítačů, ...)
 - Vyhledávání a řízení přístupu k prostředkům

Autentizace identit

- Identita
 - Entita, jenž může provádět akce v podnikové síti
 - Identifikována podle SID (*Security Identifier*)
- Autentizace
 - Ověření identity (řadičem domény)
 - Využívá se protokol Kerberos verze 5
 - Prokázání identity předložením tajemství (hesla, ...)

Řízení přístupu

- Probíhá na základě definovaných oprávnění
- Využití ACL (*Access Control List*) seznamů
 - Obsahují oprávnění pro přístup k danému prostředku pro jednotlivé identity (uživatelé, skupiny, ...)
- Podpora auditování
 - Monitorování přístupu k prostředkům

Služby Active Directory

- **Doménové služby Active Directory (AD DS)**
 - Active Directory Domain Services
- **Adresářové služby Active Directory (AD LDS)**
 - Active Directory Lightweight Directory Services
- **Certifikační služby Active Directory (AD CS)**
 - Active Directory Certificate Services
- **Služby oprávnění Active Directory (AD RMS)**
 - Active Directory Rights Management Services
- **Federační služby Active Directory (AD FS)**
 - Active Directory Federation Services

Doménové služby Active Directory

- Zajišťují
 - Uložení identit (uživatelských účtů, účtů počítačů, ...)
 - Autentizaci identit (přihlášení do domény)
 - Autorizaci identit (přístup k prostředkům)
- Umožňují
 - Správu objektů Active Directory (identit, ...)
 - Sdílení prostředků
 - Vyhledávání prostředků

Adresářové služby Active Directory

- Odlehčená verze Active Directory pro aplikace
 - Obsahuje (a replikuje) jen data týkající se aplikací
- Využívá protokol LDAP (bez modifikací)
 - Kompatibilní s řadou aplikací nevytvářených pro AD
- Podpora více datových úložišť
 - Každé úložiště vlastní schéma, SSL porty, protokoly, ...
- Autentizace identit
 - Možnost využití doménových služeb Active Directory
 - Nezávisle na AD (často v nechráněných sítích či DMZ)

Certifikační služby Active Directory

- Umožňují
 - Vytváření certifikačních autorit (CA)
 - Vydávání certifikátů (manuálně nebo automaticky)
 - Správu vydaných certifikátů (zneplatňování, ...)
- Použití certifikátů v Active Directory
 - Autentizace identit (uživatelů, počítačů, ...)
 - Ověřování důvěryhodnosti externích identit
 - Prokazování se externím prostředkům
 - ...

Služby oprávnění Active Directory

- Zajišťují ochranu dokumentů i po jejich otevření
 - Možnost znemožnit tištění dokumentů (např. emailů), kopírování nebo úpravu jejich obsahu, přeposílání, ...
- Vyžaduje
 - Windows 2000 Server SP3 nebo novější
 - Službu IIS (Internet Information Services)
 - Databázový server (např. MS SQL Server)
 - Klienta RMS (AD RMS client)
 - RMS aplikaci (Internet Explorer, Microsoft Office, ...)

Federační služby Active Directory

- Zajišťují centrální autentizaci identit (SSO, *Single Sign-On*) napříč federačním prostředím
 - Identity autentizované v jedné síti (prostředí) mohou přistupovat k prostředkům v jiné síti (prostředí)
- Federační prostředí
 - Skládá se z ověřených partnerů (Active Directory, ...)
 - Každý partner spravuje své vlastní identity
 - Každý partner důvěřuje identitám ostatních partnerů
 - Komunikace pomocí protokolů HTTP a HTTPS

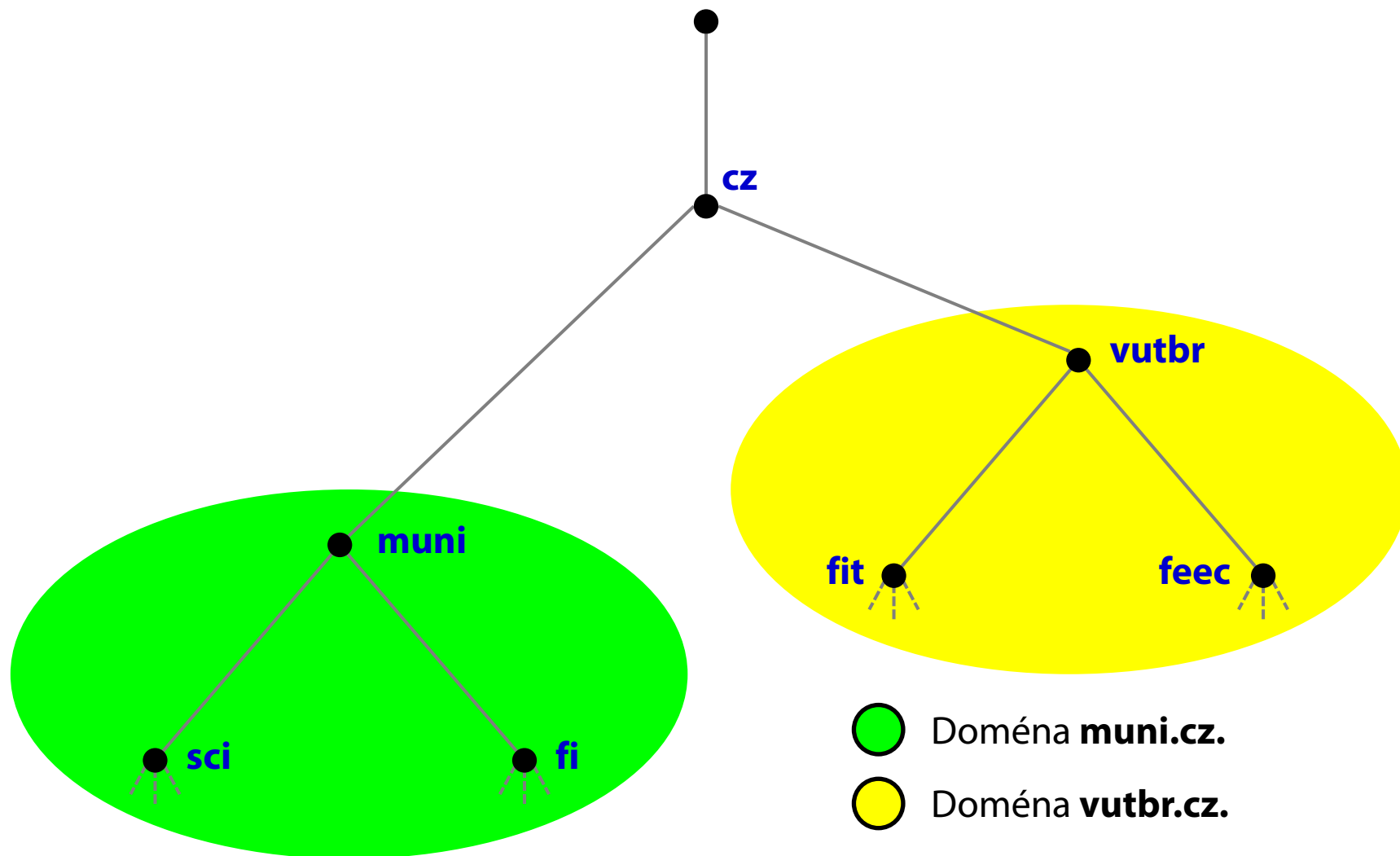
Komponenty Active Directory

- Logické komponenty
 - Určují fyzickou a logickou strukturu sítě a databáze Active Directory
- Programové komponenty
 - Ovlivňují vlastnosti a funkcionálnitu Active Directory

Logické komponenty

- Domény (*Domains*)
- Stromy (*Trees*)
- Lesy (*Forests*)
- Organizační jednotky (*Organizational Units*)
- Místa (*Sites*)

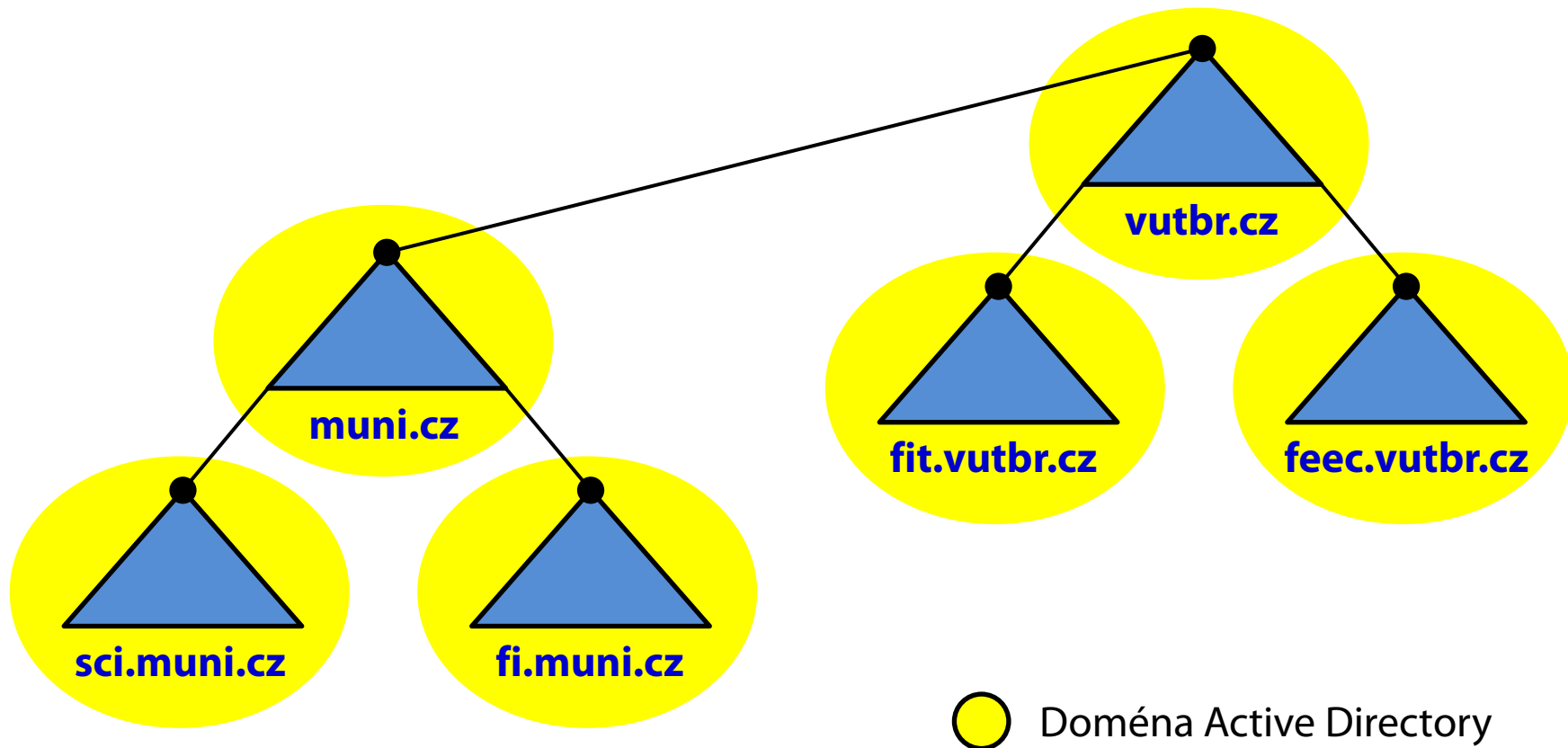
Ilustrace domén systému DNS



Doména (Domain)

- Základní (administrativní) jednotka AD
 - Ohraničuje rozsah platnosti identit a nastavení (zásad skupiny), jenž jsou platná pouze v rámci domény
 - Definuje hranici pro replikaci oddílu domény (*domain partition*), jenž je replikován pouze v rámci domény
- Konkrétní uzel stromu DNS doménových jmen
 - Nezahrnuje synovské domény (na rozdíl od DNS)
 - Jednoznačná identifikace doménovým jménem uzlu
 - Všechny počítače v doméně listové uzly tohoto uzlu
 - Sdílejí stejný DNS suffix (připojován k hostitelskému jménu)

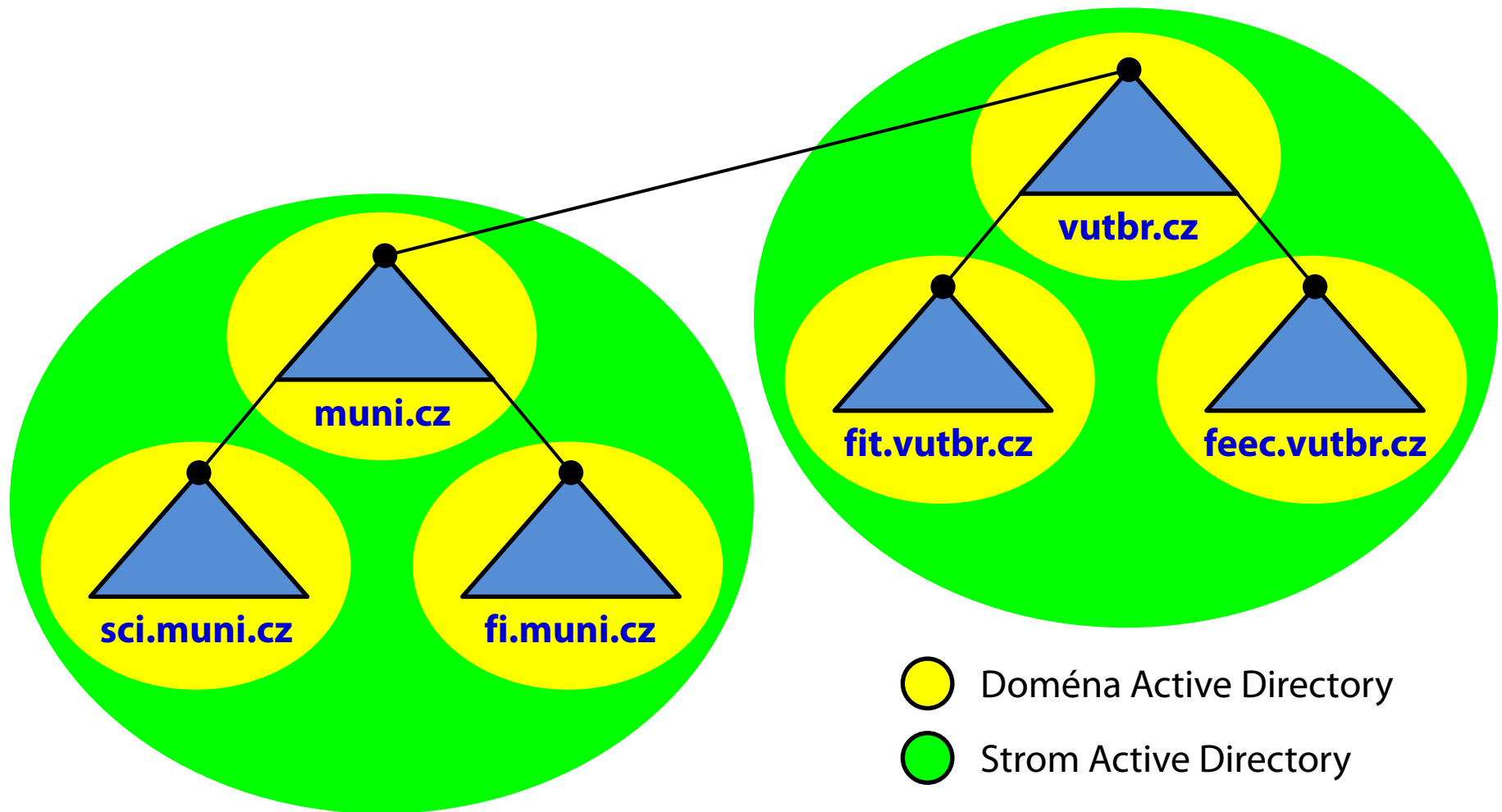
Ilustrace domén Active Directory



Strom (Tree)

- Kolekce domén (i jediné), jenž sdílí souvislou část prostoru DNS doménových jmen
 - Odpovídá doméně v systému DNS (reprezentuje celý strom domén, ne pouze jednu)
 - Domény stromu si navzájem důvěřují

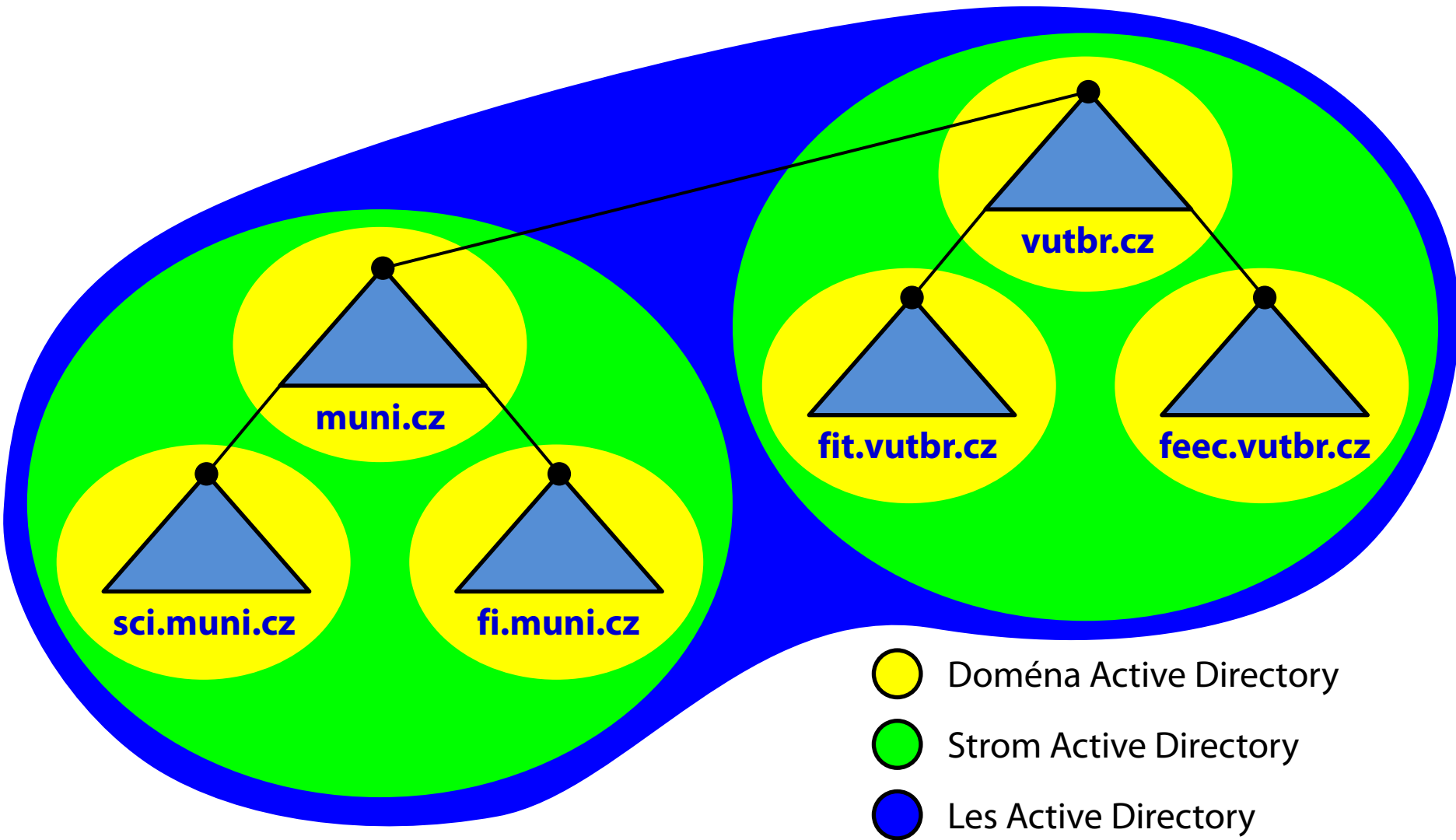
Ilustrace stromů Active Directory



Les (Forest)

- Kolekce jedné nebo více (stromů) domén
 - Domény nemusí pocházet ze souvislého prostoru
 - První (nejvyšší) doména je tzv. kořenová doména lesa (*forest root domain*) v kořenovém stromu (*root tree*)
- Všechny domény v lese
 - Sdílí konfiguraci sítě, schéma a globální katalog
 - Si navzájem důvěřují (jsou spojeny vztahy důvěry)
- Tvoří bezpečnostní hranici replikace
 - Žádná data nejsou nikdy replikována za hranici lesa

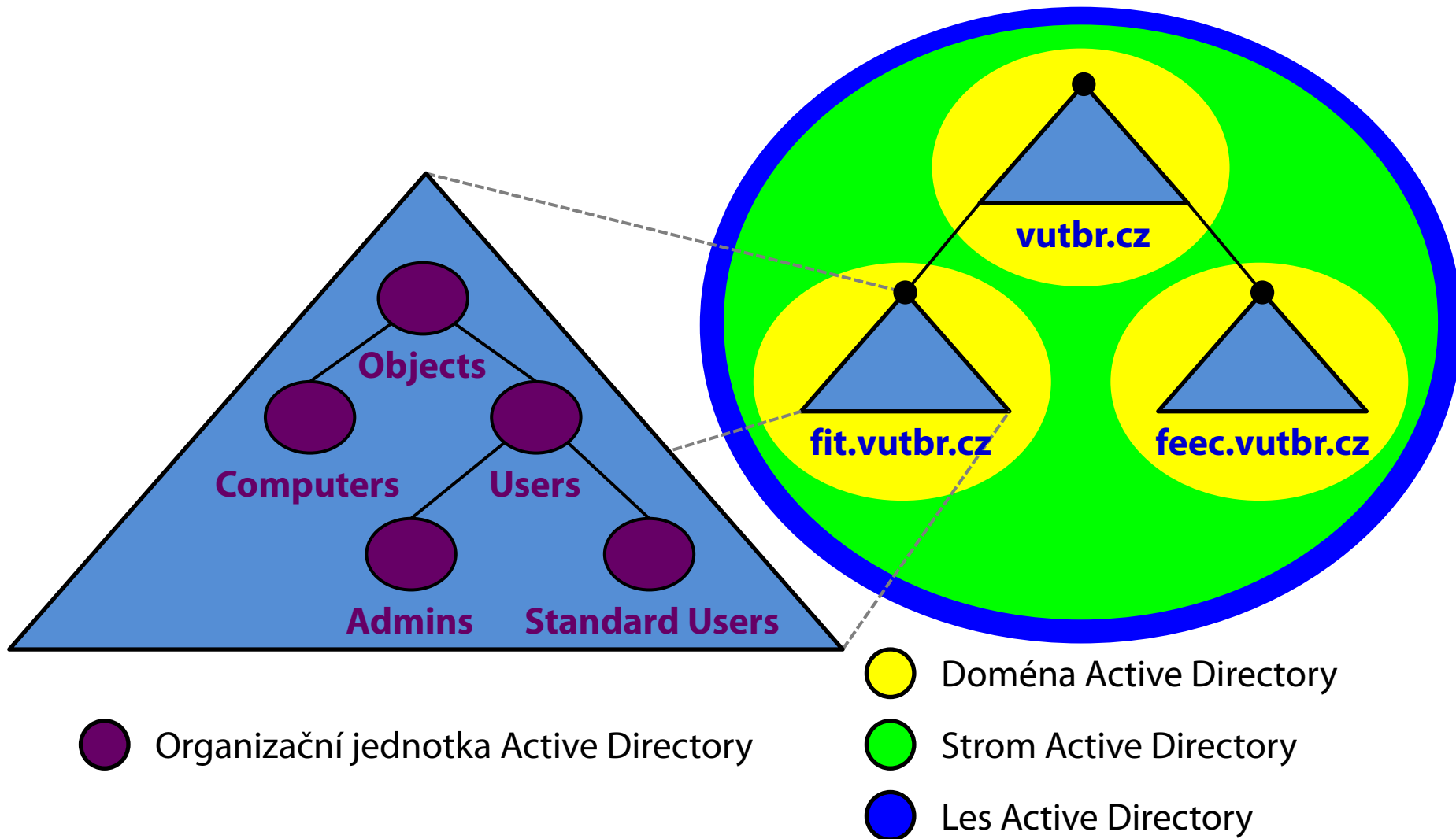
Ilustrace lesů Active Directory



Organizační jednotka (OU)

- Kontejner pro objekty Active Directory
 - Základní struktura pro seskupování objektů
- Tvoří vnitřní strukturu databáze Active Directory
 - Kontejnery mohou obsahovat vnořené kontejnery
 - Stromová hierarchie o maximální hloubce 12 úrovní
- Umožňuje
 - Samostatnou administraci obsažených objektů
 - Aplikaci zásad skupiny na obsažené objekty

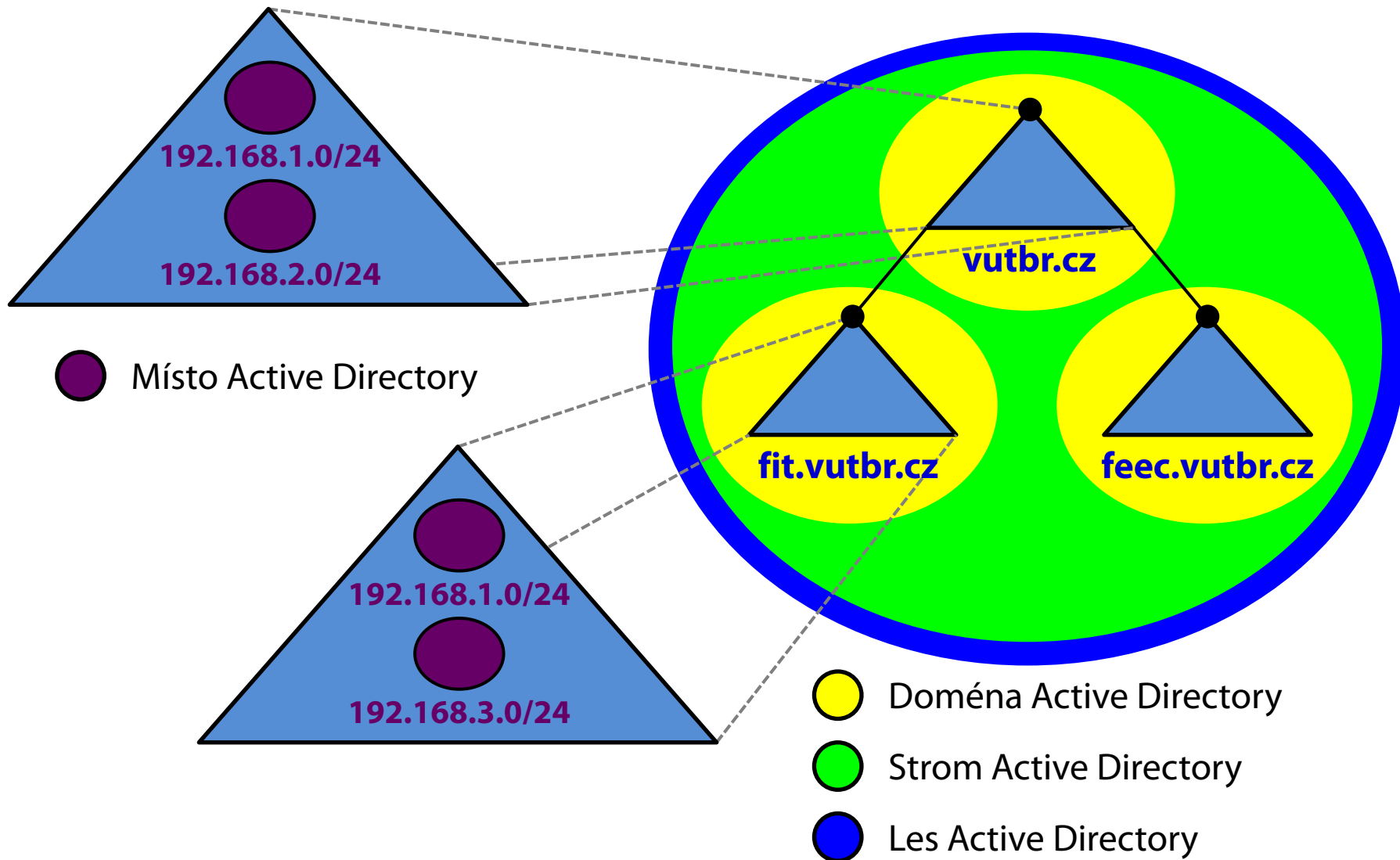
Ilustrace OU Active Directory



Místo (Site)

- Oblast vyznačující se dobrou konektivitou
 - Rozděluje (fyzicky) doménu Active Directory
- Definováno rozsahy jedné nebo více (pod)sítí
 - Většinou odpovídá jedné konkrétní fyzické (pod)síti
- Může obsahovat jednu i více domén
 - Neovlivňuje samostatnost jednotlivých domén
- Tvoří hranice pro
 - Místní replikaci databáze Active Directory
 - Lokalizaci a používání služeb

Ilustrace míst Active Directory



Programové komponenty

- Řadiče domény (DCs, *Domain Controllers*)
- Úložiště dat AD (*Active Directory Data Store*)
- Systémový oddíl (*System Volume*)
- Funkční úrovně (*Functional Levels*)

Řadiče domény (Domain Controllers)

- Servery s doménovými službami Active Directory
 - Spravují jednu konkrétní doménu Active directory
 - Obsahují kopii databáze Active Directory
- Obsahují centrum distribuce klíčů Kerberos (*KDC, Kerberos Key Distribution Center*)
 - Zajišťuje autentizaci identit, přístup ke službám, ...

Úložiště dat Active Directory

- Datové úložiště objektů Active Directory
 - Soubor **Ntds.dit** v adresáři **<system>\Ntds**
- Databáze objektů rozdělená do 4 částí
 - Schéma
 - Konfigurace
 - Globální katalog (*Global Catalog*)
 - Část obsahující všechny objekty domény neboli oddíl domény (*domain partition, domain naming context*)

Systemový oddíl (System Volume)

- Datové úložiště dat sdílených mezi řadiči domény
 - Obsahuje zásady skupiny, skripty, ...
- Kolekce adresářů v adresáři **<system>\SYSVOL**
- Synchronizace obsahu pomocí
 - Služby replikace souborů
(FRS, *File Replication Service*)
 - Replikace distribuovaného souborového systému
(DFSR, *Distributed File System Replication*)

Funkční úroveň (Functional Level)

- Ovlivňuje celkovou funkcionalitu (možnosti) lesa resp. domény Active Directory
 - Určuje nejnižší verzi systému Windows, jenž musí být přítomna na všech řadičích domény v lese či doméně
- Rozdělena do dvou kategorií podle rozsahu
 - Funkční úroveň domény (*Domain Functional Level*)
 - Funkční úroveň lesa (*Forest Functional Level*)

Přehled funkčních úrovní domény

Funkční úroveň	Popis
Windows 2000 native	Univerzální distribuční a bezpečnostní skupiny , vnořování skupin, konverze skupin (distribuční na bezpečnostní a naopak), SID historie
Windows Server 2003	Přejmenování domény pomocí nástroje netdom , aktualizace času posledního přihlášení identity (uživatele, počítače, ...), přesměrování kontejnerů Users a Computers , ukládání zásad pro autorizaci Správce autorizací (AzMan) v AD, omezená delegace, výběrová autentizace
Windows Server 2008	Replikace systémového oddílu pomocí replikace distribuovaného souborového systému (DFSR), podpora šifrování pomocí AES (128-bit a 256-bit) pro protokol Kerberos, podrobné informace o posledních přihlášeních (<i>last interactive logon</i>), fine-grained zásady hesel , osobní virtuální plochy (PVD, <i>Personal Virtual Desktops</i>)
Windows Server 2008 R2	Autorizace založená na metodě autentizace, automatická správa SPN (<i>Security Principal Name</i>) pro spravované účty služeb
Windows Server 2012	Podpora KDC pro nárokování (<i>claims</i>), složenou autentizaci (<i>compound authentication</i>) a <i>Kerberos armoring</i>

Přehled funkčních úrovní lesa

Funkční úroveň	Popis
Windows 2000 native	
Windows Server 2003	Vztahy důvěry mezi lesy (<i>forest trusts</i>), přejmenování domény, linked-value replikace příslušnosti do skupin, read-only řadiče domény (RODC), optimalizovaný generátor replikační topologie AD, deaktivace a redefinice atributů a tříd ve schématu AD
Windows Server 2008	
Windows Server 2008 R2	Active Directory koš (<i>Active Directory Recycle Bin</i>)
Windows Server 2012	

Instalace Active Directory

- Proces transformace serveru na řadič domény
 - 1) Instalace **Doménových služeb Active Directory**
 - 2) Povýšení serveru do role řadiče domény (DC)
- Při vytváření domény je správce počítače povýšen do role správce domény (člena skupiny **Domain Admins**)
- Oba kroky instalace lze provést pomocí
 - Nástroje **Správce serveru** (*Server Manager*)
 - Nástrojů pro **Windows PowerShell** (*cmdletů*)
 - 1) **Install-WindowsFeature -name AD-Domain-Services**
 - 2) Skript pro povýšení lze vygenerovat přes **Správce serveru**

Instalace AD DS přes Správce serveru

Průvodce přidáním rolí a funkcí

Vybrat role serveru

Než začnete
Typ instalace
Výběr serveru
Role serveru
Funkce
Služba AD DS
Potvrzení
Výsledky

Vyberte role, které chcete nainstalovat na vybraném serveru.

Role

- Aplikační server
- Faxový server
- Hyper-V
- Server DHCP
- Server DNS
- Služba Active Directory Domain Services**
- Služba AD CS (Active Directory Certificate Services)
- Služba AD FS (Active Directory Federation Services)
- Služba AD LDS (Active Directory Lightweight Directory Services)
- Služba AD RMS (Active Directory Rights Management Services)
- Služba pro nasazení systému Windows
- Služba pro správu souborů a úložiště (Nainstalováno)
- Služba Síťové zásady a přístup
- Služby aktivace multilicence
- Tiskové a dokumentové služby
- Vzdálená plocha
- Vzdálený přístup
- Webový server (IIS)
- Windows Server Update Services

Průvodce přidáním rolí a funkcí

Chcete přidat funkce, které jsou požadovány pro:
Služba Active Directory Domain Services?

Nelze nainstalovat funkci Služba Active Directory Domain Services, pokud nejsou nainstalovány také následující služby rolí nebo funkce.

- ▲ Nástroje pro vzdálenou správu serveru
 - ▲ Nástroje pro správu rolí
 - ▲ Nástroje služby AD DS a AD LDS
 - Modul služby Active Directory pro prostředí Windows IIS
 - ▲ Nástroje služby AD DS
 - [Nástroje] Centrum správy služby Active Directory
 - [Nástroje] Moduly snap-in a nástroje příkazového řádku
 - [Nástroje] Správa zásad skupiny

Zahrnout nástroje pro správu (pokud jsou k dispozici)

Přidat funkce **Storno**

< Předchozí **Další** > **Nainstalovat** **Storno**

Způsoby povýšení serveru

- Přidání řadiče domény do existující domény
 - Nástroj (*cmdlet*) **Install-AddsDomainController**
- Vytvoření nové domény v existujícím lese
 - Nástroj (*cmdlet*) **Install-AddsDomain**
 - Dva typy vytvářených domén
 - Synovská doména v existujícím stromu
 - Nová doména v novém stromu
- Vytvoření nového lesa
 - Nástroj (*cmdlet*) **Install-AddsForest**

Povýšení serveru přes Správce serveru

Průvodce konfigurací služby AD DS (Active Directory Domain Services)

Konfigurace nasazení

CÍLOVÝ SERVER
wsrv2012

Konfigurace nasazení

Možnosti řadiče domény
Další možnosti
Cesty
Kontrola možností
Kontrola předpokladů
Instalace
Výsledky

Vyberte operaci nasazení.

Přidat řadič domény do již existující domény
 Přidat novou doménu do existující doménové struktury
 Přidat novou doménovou strukturu

Zadejte informace o doméně pro tuto operaci.

Vyberte typ domény: Doména stromové struktury

Název doménové struktury: *

Název nové domény: *

Zadejte pověření k provedení této operace.

<Nebyla zadána žádná pověření.>

[Další informace konfigurace nasazení](#)

Informace potřebné pro povyšování

- Pojmenování domény
 - Unikátní DNS doménové jméno a NetBIOS jméno
 - Pokud není NetBIOS jméno specifikováno, použije se prvních 15 znaků nejnižší části doménového jména
- Funkční úroveň domény
 - Nižší funkční úroveň poskytuje zpětnou kompatibilitu
 - Vyšší funkční úroveň přináší vyšší zabezpečení a nové možnosti Active Directory
- Umístění databáze a systémového oddílu
 - Ve výchozím nastavení v adresáři systému

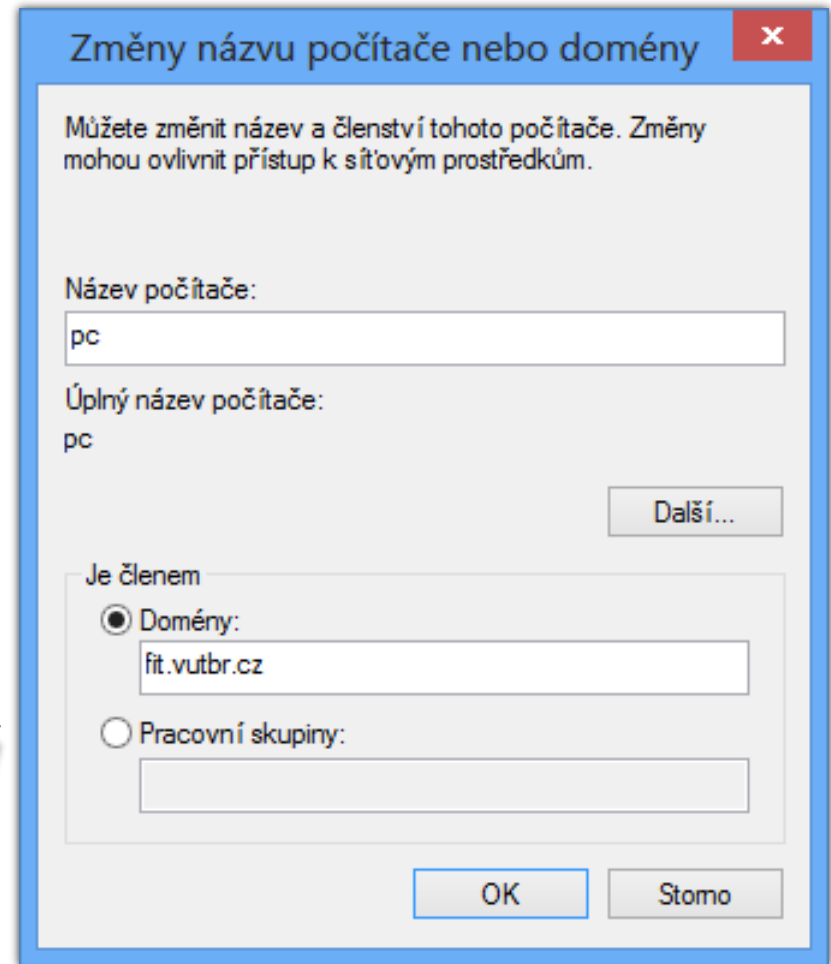
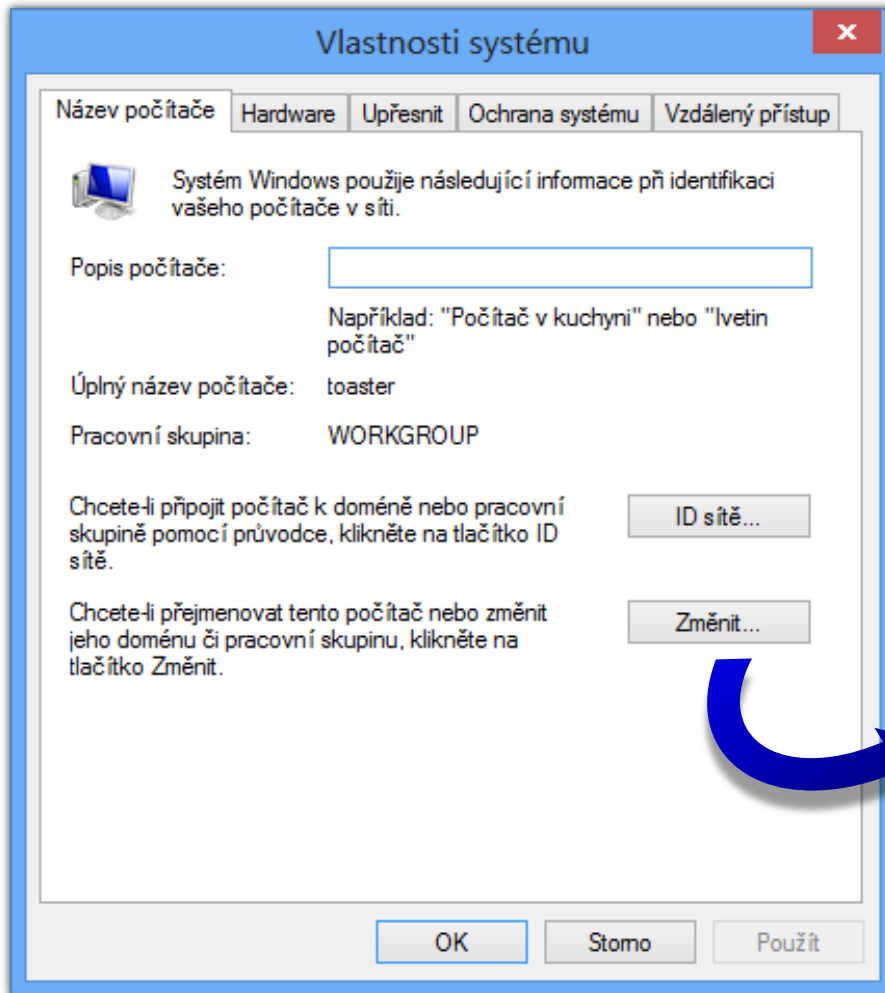
Požadavky pro povyšování

- Přítomnost DNS serveru
 - Lze vytvořit automaticky během povyšování
 - Obsahuje informace potřebné pro činnost AD
 - U zón integrovaných v AD jsou do nich potřebné záznamy zapsány automaticky, jinak se musí vložit manuálně
- Povyšovaný server musí mít
 - Statické IP adresy na svých síťových rozhraních
 - Nastavenou IP adresu DNS serveru
- Povýšení vyžaduje oprávnění lokálního správce
 - Účet správce musí mít neprázdné heslo

Připojení počítače do domény

- Vyžaduje
 - Dostupnost DNS serveru (počítač musí mít nastavenou IP adresu DNS serveru se záznamy Active Directory)
 - Oprávnění lokálního správce (člen [Administrators](#))
- Postup
 - Specifikace názvu domény (ve vlastnostech systému)
 - Zadání pověření (jména a hesla) uživatele z AD
 - Standardní uživatel může připojit maximálně 10 počítačů
 - Správce domény může připojit neomezeně počítačů
 - Restart počítače

Specifikace názvu domény



Přihlášení do domény

- Stanice nebo členský (*member*) server v doméně
 - Možnost přihlášení lokálně nebo do domény
- Řadič domény
 - Možné pouze přihlášení do domény
 - Standardní uživatel se nemůže přihlásit
- Lokální přihlášení
 - ***<login>@<hostname>*** resp. ***<hostname>\<login>***
- Přihlášení do domény
 - ***<login>@<dns-název>*** resp. ***<netbios-název>\<login>***