



EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání



jihořmoravský kraj

OPERAČNÍ SYSTÉMY

Ověřování uživatelů pomocí AD

Metodický list

Autor: Ing. Marek Kocan, Metodik: Ing. Roman Koláčný

Recenzent: Mgr. Jiří Činčura

Rok vydání: 2023

Ověřování uživatelů pomocí AD podléhá licenci CC BY-SA 4.0 International License (Offline use:
<http://creati-vecommons.org/licenses/by-nc-sa/4.0/>).



Obsah

Cíle.....	2
Dovednosti	2
Pracovní prostředí	2
1 Adresářové služby – teoretický základ.....	3
1.1 Microsoft Active Directory	3
2 Active Directory prakticky.....	5
2.1 Pracovní prostředí	5
2.2 Úvodní část	5
2.3 Role Active Directory Domain Services – základní kroky	5
2.4 Povýšení serveru na Domain Controller	11
2.5 Základní struktura AD a její naplnění.....	13
3 Napojení klientské stanice.....	16
Shrnutí a závěr	17
Seznam použitých zdrojů.....	18

Cíle

Studenti se seznámí s teoretickými základy v oblasti adresářových služeb. Dále si osvojí základní dovednosti související s nastavením Active Directory. S ohledem na dotaci sice nelze předpokládat úplné zvládnutí této problematiky, cílem je ale poskytnout studentovi dostatečný podklad pro orientaci v dané oblasti.

Student bude schopen vlastními slovy vysvětlit co jsou to adresářové služby, uvést příklady existujících řešení a vysvětlit základní principy zprovoznění Active Directory. V dlouhodobém horizontu bude student schopen samostatně využít nové znalosti a dovednosti v reálném prostředí pro správu operačních systémů.

Současně je nicméně vhodné předřadit tomuto modulu výuku adresářových služeb v teoretické rovině, mj. i s ohledem na možnost pracovat s různorodými adresářovými službami a principy řízení přístupu (včetně odlišností ve Windows a linuxových systémech).

Dovednosti

Student bude schopen provést základní instalaci a nastavení Active Directory v prostředí operačního systému Windows Server. V dlouhodobém horizontu bude student schopen aplikovat získané dovednosti pro efektivní správu operačních systémů.

Pracovní prostředí

Výuku lze realizovat v prostředí:

- Cylab JCEKB, operační systém Windows (Server i desktopová edice – pro propojení s AD)

Pro práci postačí standardní nástroje na počítači v použitých systémech dle tohoto scénáře.

1 Adresářové služby – teoretický základ

Dle české Wikipedie je adresářová služba aplikace shromažďující a poskytující informace o pojmenovaných objektech, ke kterým bývá intenzivně přistupováno, ale mění se jen zřídka. Informace jsou uloženy ve formě atributů hierarchicky pojmenovaných záznamů, které jsou pro lepší integraci systémů standardizovány. Adresářová služba je často ústřední bezpečnostní komponenta a udržuje odpovídající záznamy pro řízení přístupu – tedy jakým způsobem může někdo zacházet s nějakým objektem. V adresářové službě mohou být udržovány informace například o uživateli (telefon, e-mail, pracovní zařazení), tiskárnách či počítačích, ke kterým přistupují ostatní systémy skrze síť.

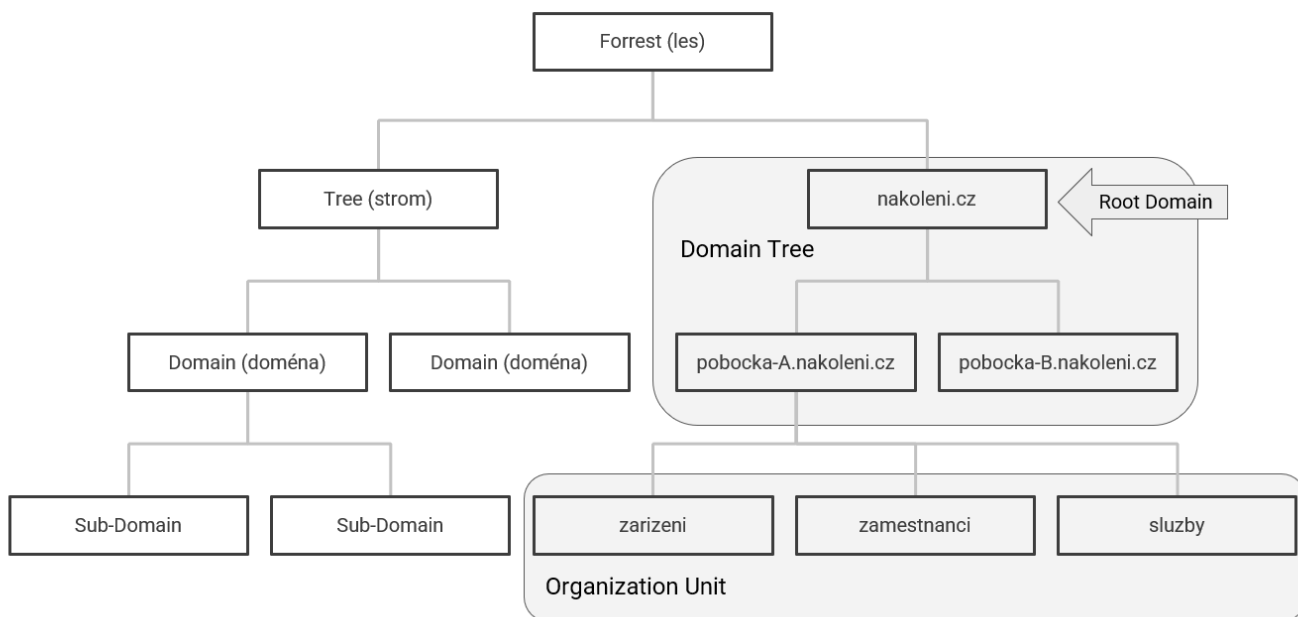
Zjednodušeně řečeno tak lze adresářovou službu chápat jako rozhraní k databázi, která obsahuje informace o jednotlivých systémech a uživateli i jejich oprávněních k přístupu do dalších systémů a prvků podnikové informační architektury. Mezi možnosti patří například zajištění tzv. SSO (Single-SignOn), tedy mechanismu jednotného přihlášení.

Přestože typickým, všeobecně známým zástupcem pro adresářovou službu je Active Directory společnosti Microsoft, nejde o jedinou implementaci. Za základ lze považovat protokol LDAP (Lightweight Directory Access Protocol), který má opět řadu konkrétních implementací. Rozdílem mezi LDAP a AD je, že LDAP je standardní protokol využívaný pro adresářovou službu, zatímco AD je ve skutečnosti proprietární řešení, konkrétní implementací. Na druhou stranu platí, že LDAP není jediným protokolem tohoto typu. Za pozornost určitě stojí bezpečnostní autentizační protokol Kerberos, jehož smyslem je především zajištění ověřování identit v nezabezpečené síti.

1.1 Microsoft Active Directory

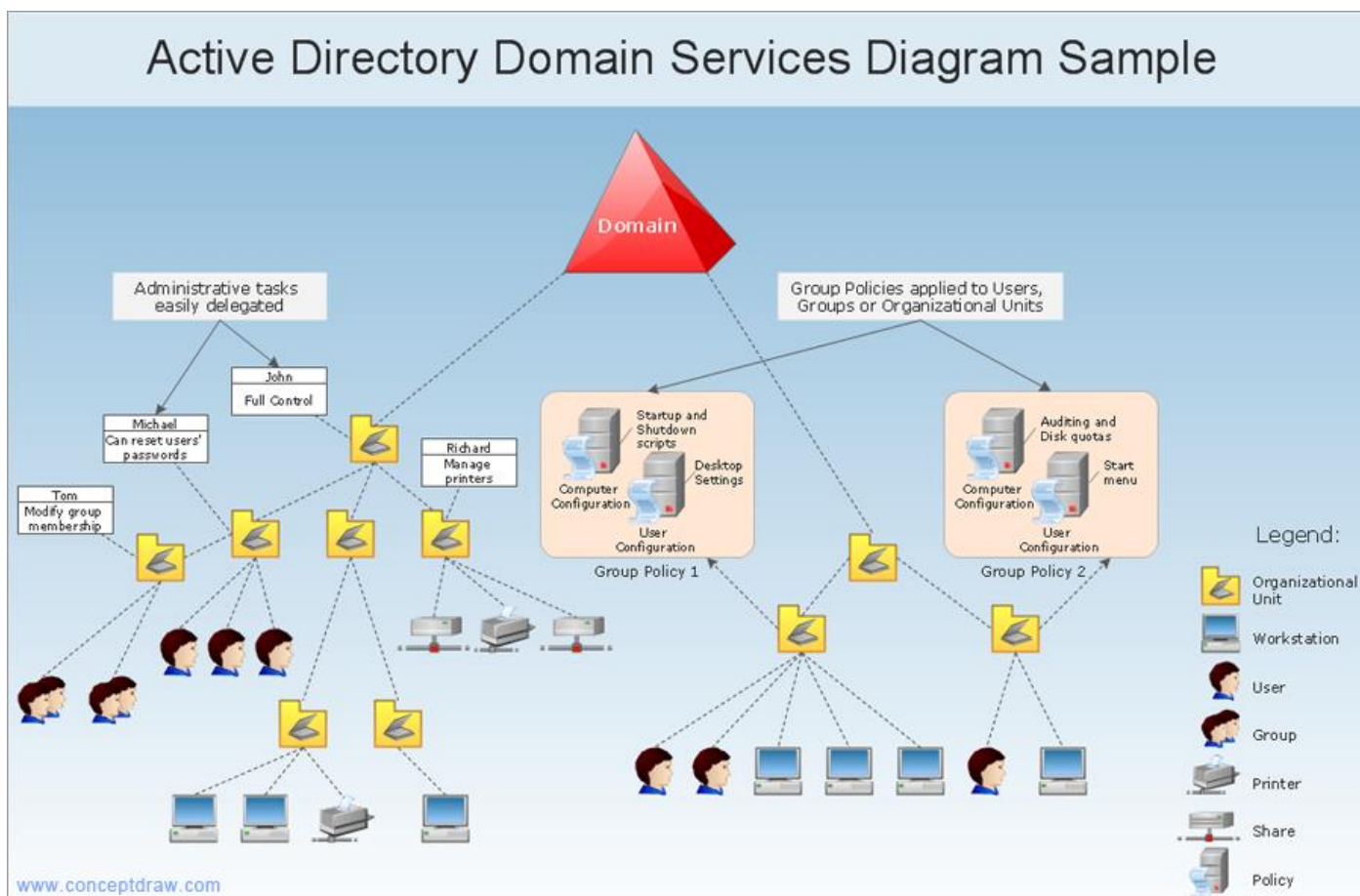
Microsoft AD je dnes bezesporu jednou z nejznámějších adresářových služeb – nicméně jak již bylo uvedeno, nikoli jedinou (alternativou v linuxovém světě je například FreeIPA nebo OpenLDAP). Pro realizaci svých základních činností využívá stromovou strukturu objektů, která obsahuje informace o strukturách jak z logického, tak i fyzického pohledu. Logické struktury jsou například organizační jednotky, domény, stromy domén a lesy domén (celá teorie je nad rámec tohoto scénáře, vyučující by si měl v případě potřeby rozšířit své znalosti dalším studiem). Organizační jednotky jsou tak vlastně kontejnery pro umístění informací o uživatelských účtech, prostředích a zdrojích a dalších organizačních jednotkách (samotná struktura tak i v tomto případě může být hierarchická). Fyzické struktury pak vychází z fyzicko-logických pohledů na podnikovou informační architekturu a pracují tak mj. se sítěmi a podsítěmi. Obsah databáze je ve skutečnosti adresářem.

Rozčlenění je patrné z následujícího obrázku:



Na výše uvedeném obrázku je patrný hlavní les, stromy domén i jednotlivé domény včetně členění do organizačních jednotek.

Členění v rámci jedné domény pak může vypadat například dle následujícího obrázku:



Služba nemusí být provozována jen na jednom vybraném stroji, může být členěna do hierarchicky provázaných částí / replikována v rámci prakticky jakéhokoli jiného doménového řadiče.

2 Active Directory prakticky

2.1 Pracovní prostředí

Výuku lze realizovat v prostředí Cylab JCEKB, operační systém Windows (Server i desktopová edice – pro propojení s AD). Pro práci postačí standardní nástroje.

2.2 Úvodní část

Vyučující seznámí studenty s teoretickými základy a následně je nasměruje k přihlášení do prostředí použitého Windows serveru.

Kontrolní bod

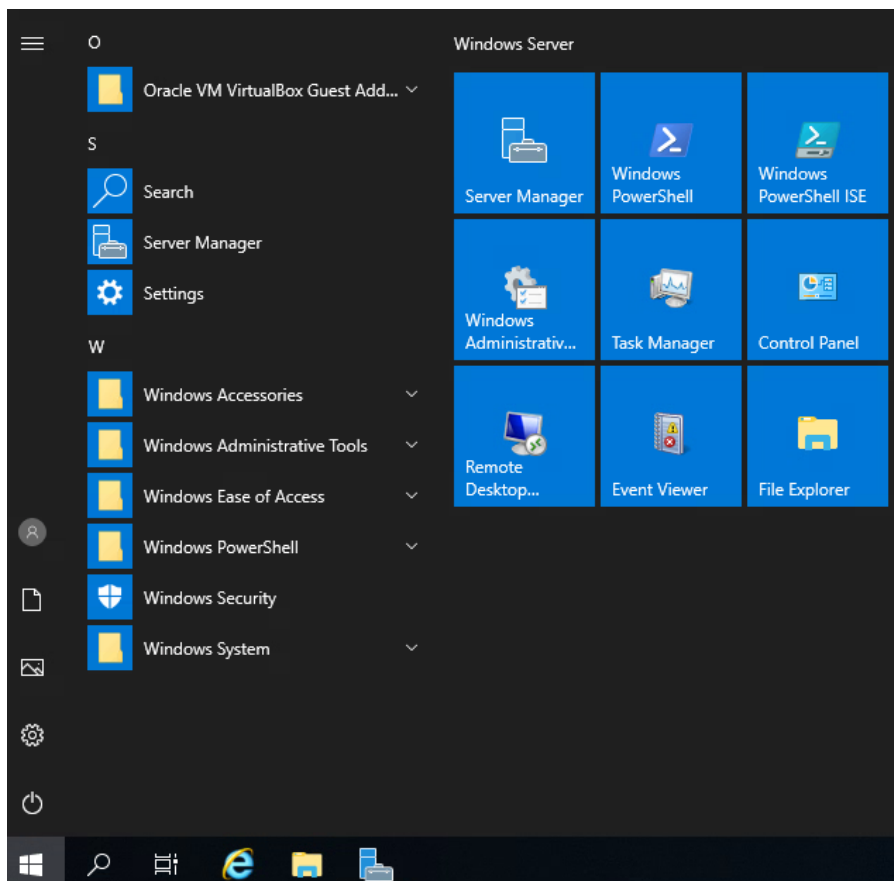
Studenti diskutují s vyučujícím základní pojmy z oblasti LDAP/AD (dle volby vyučujícího) a samostatně se přihlásí do prostředí serveru dle pokynů vyučujícího.

Předpokladem používání Active Directory je zprovoznění této služby nejméně na jednom serveru. Nestačí samotná instalace adresářové služby, ale je nezbytné provedení i důsledně přesné konfigurace – obojí je popsáno v nejméně možné míře v následujících částech scénáře. *Vyučující musí mít na paměti, že jde pouze o základní nastavení omezené časovou dotací. Dle svého uvážení může předvést i další konfigurační možnosti či rozvést celé prostředí do větší šíře – vždy ale s ohledem na dosavadní míru pochopení ze strany studentů.*

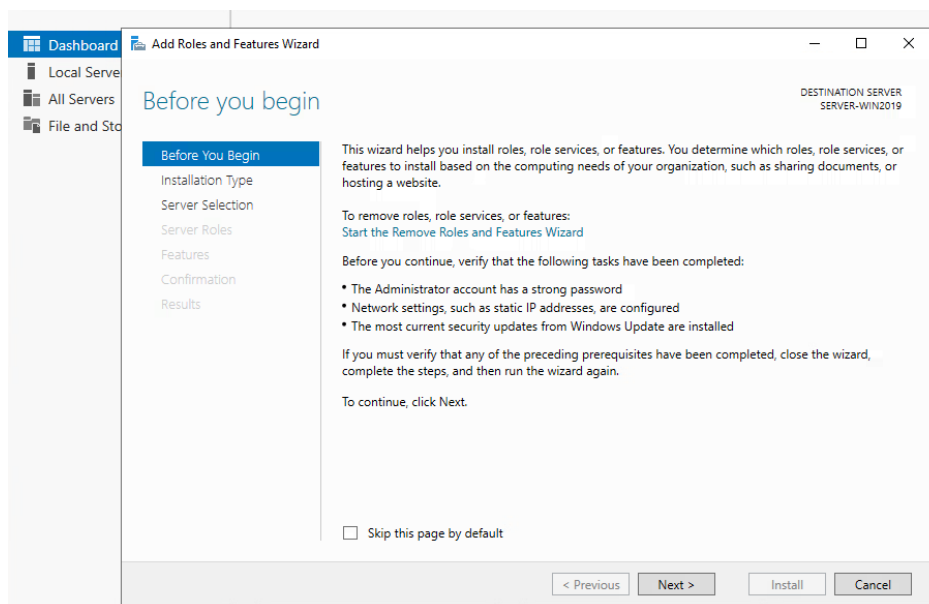
2.3 Role Active Directory Domain Services – základní kroky

Prvním krokem je instalace příslušné role *Active Directory Domain Services* do prostředí operačního systému. Existuje více způsobů, jak tohoto cíle dosáhnout, nejjednodušší pro předvedení je nicméně využít administrátorského nástroje Server Manager.

Pro spuštění správce lze využít nabídku Start (uživatelské rozhraní správce ale již může být zobrazeno automaticky po přihlášení), například dle následujícího obrázku.

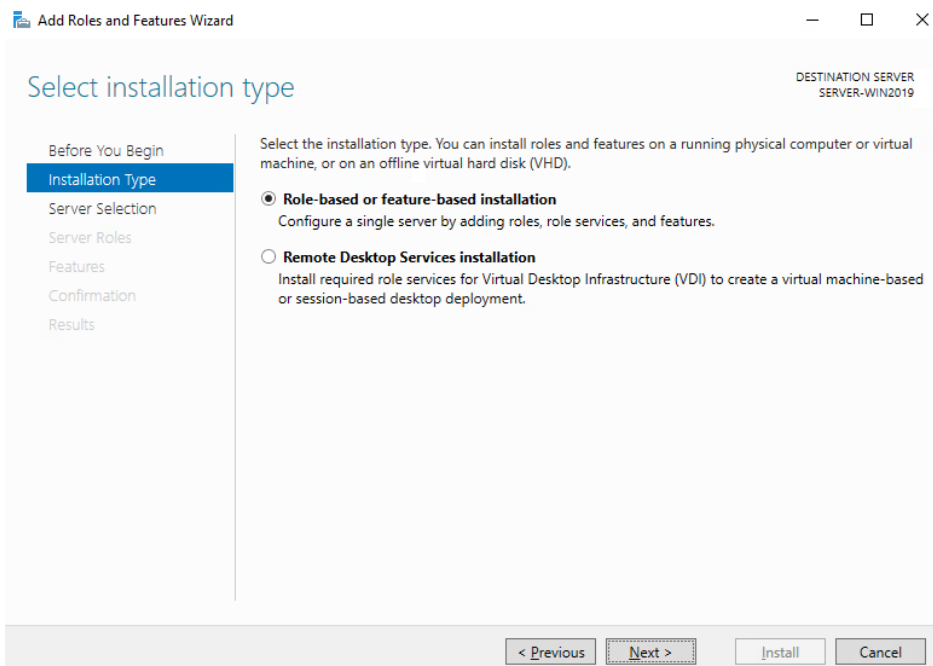


Samotné přidání role *Active Directory Domain Services* vyučující zahájí výběrem volby *Add Roles and Features* z nabídky *Manage*. Tato volba vyvolá průvodce, který usnadní přidání požadované role. *Vyučující projde postupem dle následující obrázkové sekvence.*



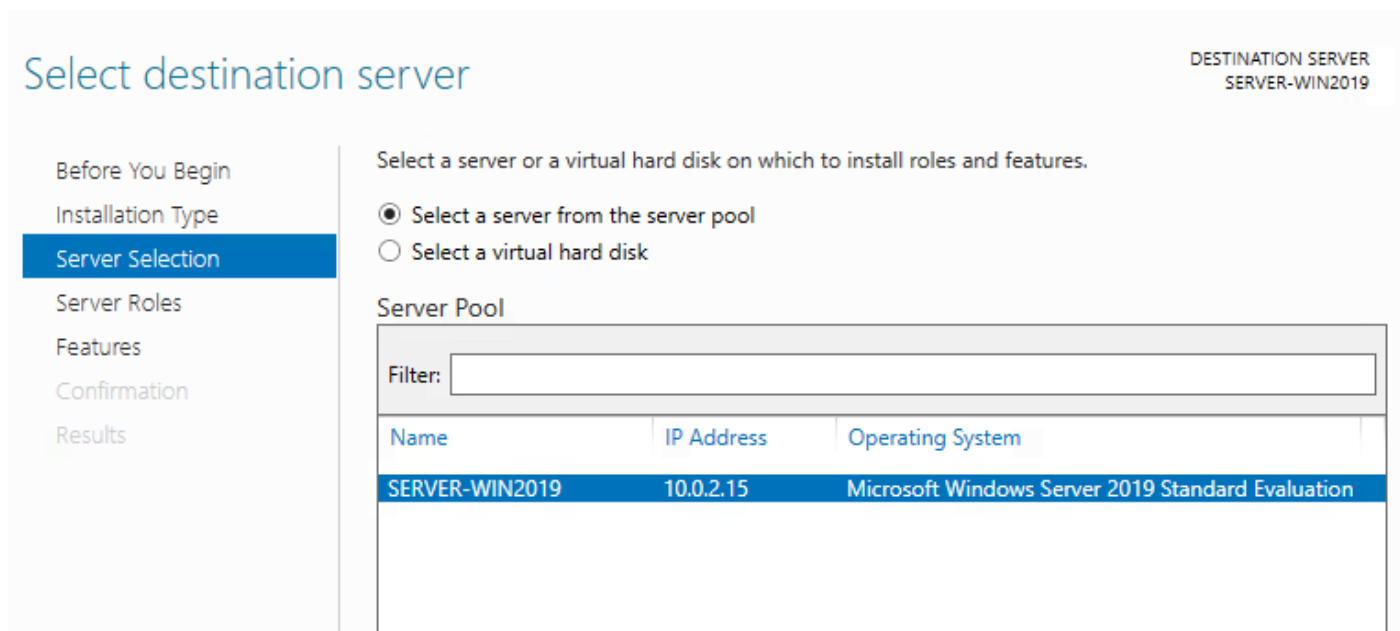
Vyučující v rámci tohoto kroku upozorní na požadované prerekvizity a pravidla (silné heslo, správná konfigurace síťového prostředí včetně použití statické IP adresy a uplatněných aktualizací). Dle svého uvážení vyučující diskutuje důležitost jednotlivých doporučení.

K pokračování je nutné stisknout tlačítko *Next>*.



Vyučující v rámci tohoto kroku dle svého uvážení a znalostí vysvětlí rozdíly mezi jednotlivými možnostmi a doporučí instalaci založenou na rolích.

K pokračování je nutné stisknout tlačítko *Next>*.



Nejprve je nutné zvolit (pokud tomu tak již není) volbu *Select a server from the server pool*. Díky této možnosti lze vybrat konkrétní server, na který bude požadovaná role přidávána – v případě tohoto scénáře je zobrazený v dostupných serverech systém s názvem SERVER-WIN2019 (může být v okamžiku výuky odlišný), který je tím správným pro pokračování. *Vyučující předvede vybrání správných voleb.*

K pokračování je nutné stisknout tlačítko *Next>*.

Kontrolní bod

Studenti projdou jednotlivé kroky od spuštění Server Manageru až po výběr serveru pro instalaci role Active Directory Domain Services.

Dalším krokem je výběr samotné role *Active Directory Domain Services* pro její přidání, viz následující obrázek.

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

Select one or more roles to install on the selected server.

Roles	Description
<input type="checkbox"/> Active Directory Certificate Services	Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.
<input checked="" type="checkbox"/> Active Directory Domain Services	
<input type="checkbox"/> Active Directory Federation Services	
<input type="checkbox"/> Active Directory Lightweight Directory Services	
<input type="checkbox"/> Active Directory Rights Management Services	
<input type="checkbox"/> Device Health Attestation	
<input type="checkbox"/> DHCP Server	
<input type="checkbox"/> DNS Server	
<input type="checkbox"/> Fax Server	
▸ <input checked="" type="checkbox"/> File and Storage Services (1 of 12 installed)	
<input type="checkbox"/> Host Guardian Service	
<input type="checkbox"/> Hyper-V	

V průběhu procesu dojde ke zobrazení informací o tom, že požadovaná role vyžaduje další prerekvizity v podobě služeb a funkcí rolí – k jejich přidání do instalačního procesu dojde po stisku tlačítka Add Features.

Add features that are required for Active Directory Domain Services?

You cannot install Active Directory Domain Services unless the following role services or features are also installed.

- [Tools] Group Policy Management
- ▲ Remote Server Administration Tools
 - ▲ Role Administration Tools
 - ▲ AD DS and AD LDS Tools
 - Active Directory module for Windows PowerShell
 - ▲ AD DS Tools
 - [Tools] Active Directory Administrative Center
 - [Tools] AD DS Snap-Ins and Command-Line Tools

Include management tools (if applicable)

Vyučující dle svých znalostí vysvětlí jednotlivé prerekvizity a vysvětlí význam volby Include management tools.

K pokračování je nutné stisknout tlačítko Next>

Select features

DESTINATION SERVER
SERVER-WIN2019

Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results

Select one or more features to install on the selected server.

Features	Description
<input type="checkbox"/> .NET Framework 3.5 Features	<p>.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.</p>
<input checked="" type="checkbox"/> .NET Framework 4.7 Features (2 of 7 installed)	
<input type="checkbox"/> Background Intelligent Transfer Service (BITS)	
<input type="checkbox"/> BitLocker Drive Encryption	
<input type="checkbox"/> BitLocker Network Unlock	
<input type="checkbox"/> BranchCache	
<input type="checkbox"/> Client for NFS	
<input type="checkbox"/> Containers	
<input type="checkbox"/> Data Center Bridging	
<input type="checkbox"/> Direct Play	
<input type="checkbox"/> Enhanced Storage	
<input type="checkbox"/> Failover Clustering	
<input checked="" type="checkbox"/> Group Policy Management	
<input type="checkbox"/> Host Guardian Hyper-V Support	
<input type="checkbox"/> I/O Quality of Service	
<input type="checkbox"/> IIS Hostable Web Core	
<input type="checkbox"/> Internet Printing Client	
<input type="checkbox"/> IP Address Management (IPAM) Server	
<input type="checkbox"/> iSNS Server service	

< Previous Next > Install Cancel

K pokračování je nutné stisknout tlačítko *Next*>. Dojde ke zobrazení informace o DS/DNS, *vyučující dle svých zkušeností vysvětlí, že k jejímu přidání dojde později*. Viz následující obrázek.

Add Roles and Features Wizard

Active Directory Domain Services


DESTINATION SERVER
SERVER-WIN2019

Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results

Active Directory Domain Services (AD DS) stores information about users, computers, and other devices on the network. AD DS helps administrators securely manage this information and facilitates resource sharing and collaboration between users.

Things to note:

- To help ensure that users can still log on to the network in the case of a server outage, install a minimum of two domain controllers for a domain.
- AD DS requires a DNS server to be installed on the network. If you do not have a DNS server installed, you will be prompted to install the DNS Server role on this machine.

 Azure Active Directory, a separate online service, can provide simplified identity and access management, security reporting, single sign-on to cloud and on-premises web apps.
[Learn more about Azure Active Directory](#)
[Configure Office 365 with Azure Active Directory Connect](#)

< Previous Next > Install Cancel

K pokračování je nutné stisknout tlačítko *Next*>, k samotnému přidání role dojde po stisku tlačítka *Install*. Průběh a dokončení instalace je patrný z následujícího obrázku.

Confirm installation selections

DESTINATION SERVER
SERVER-WIN2019

Before You Begin

Installation Type

Server Selection

Server Roles

Features

AD DS

Confirmation

Results

To install the following roles, role services, or features on selected server, click Install.

 Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

- Active Directory Domain Services
- Group Policy Management
- Remote Server Administration Tools
 - Role Administration Tools
 - AD DS and AD LDS Tools
 - Active Directory module for Windows PowerShell
 - AD DS Tools
 - Active Directory Administrative Center
 - AD DS Snap-Ins and Command-Line Tools

[Export configuration settings](#)
[Specify an alternate source path](#)

< Previous

Next >

Install

Cancel

Installation progress

DESTINATION SERVER
SERVER-WIN2019

Before You Begin

Installation Type

Server Selection

Server Roles


Features

AD DS

Confirmation

Results

View installation progress

 Feature installation

Installation started on SERVER-WIN2019

- Active Directory Domain Services
- Group Policy Management
- Remote Server Administration Tools
 - Role Administration Tools
 - AD DS and AD LDS Tools
 - Active Directory module for Windows PowerShell

Installation progress

DESTINATION SERVER
SERVER-WIN2019

Before You Begin

Installation Type

Server Selection

Server Roles


Features

AD DS

Confirmation

Results

View installation progress

 Feature installation

A restart is pending on SERVER-WIN2019. You must restart the destination server to finish the installation.

- Active Directory Domain Services
- Group Policy Management
- Remote Server Administration Tools
 - Role Administration Tools
 - AD DS and AD LDS Tools
 - Active Directory module for Windows PowerShell

Základní část zprovoznění AD na serveru bude dokončena po stisku tlačítka *Close*.

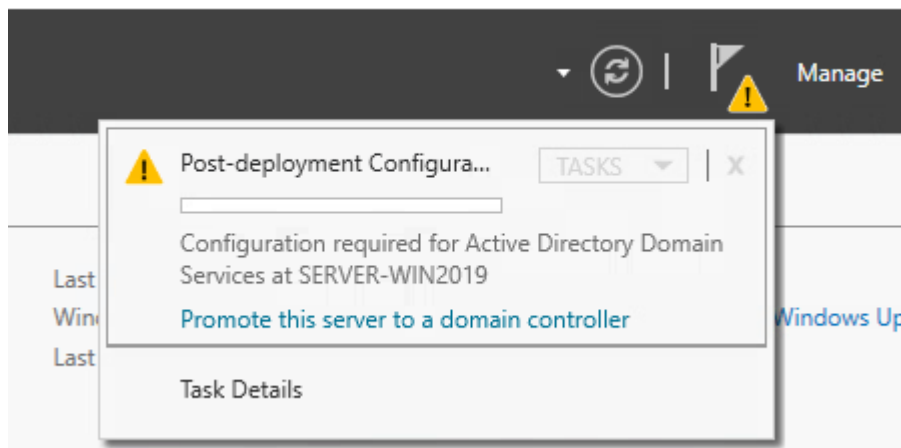
Kontrolní bod

Studenti projdou jednotlivé kroky vlastního přidání role Active Directory Domain Services (navázáno na předchozí kontrolní bod).

2.4 Povýšení serveru na Domain Controller

Samotné přidání role není z pohledu AD dostačující – v dalším kroku (po restartu) je nutné povýšit server na tzv. domain controller. Vyučující projde postupem dle následující obrázkové sekvence.

V rámci Server Manageru stačí klepnout na žlutý vykřičník a provést následnou konfiguraci, která bude zahájena po klepnutí na odkaz *Promote this server to a domain controller*.



Deployment Configuration

TARGET SERVER
SERVER-WIN2019

- Deployment Configuration
- Domain Controller Options
- Additional Options
- Paths
- Review Options
- Prerequisites Check
- Installation
- Results

Select the deployment operation

- Add a domain controller to an existing domain
- Add a new domain to an existing forest
- Add a new forest

Specify the domain information for this operation

Domain:

Supply the credentials to perform this operation

<No credentials provided>

Vyučující vysvětlí jednotlivé volby (přidání doménového řadiče do existující domény, přidání nové domény do existujícího forestu a přidání nového forestu) – vzhledem k tomu, že scénář využívá zcela novou doménu, je logické využití poslední – třetí – volby.

Do položky *Root domain name* vloží vyučující novou doménu, například *nakoleni.cz*.

Deployment Configuration

Deployment Configuration

Domain Controller Options

Additional Options

Paths

Review Options

Prerequisites Check

Installation

Select the deployment operation

- Add a domain controller to an existing domain
- Add a new domain to an existing forest
- Add a new forest

Specify the domain information for this operation

Root domain name:

nakoleni.cz

K pokračování je nutné stisknout tlačítko *Next*>.

Další krok umožňuje změnu chování včetně výběru použitého operačního systému (funkční úrovně). V rámci scénáře je vhodné ponechat nastavení dle následujícího obrázku.

Deployment Configuration

Domain Controller Options

DNS Options

Additional Options

Paths

Review Options

Prerequisites Check

Installation

Results

Select functional level of the new forest and root domain

Forest functional level: Windows Server 2016

Domain functional level: Windows Server 2016

Specify domain controller capabilities

- Domain Name System (DNS) server
- Global Catalog (GC)
- Read only domain controller (RODC)

Type the Directory Services Restore Mode (DSRM) password

Password:

Confirm password: *

Vyučující upozorní na heslo DSRM, které může být v zásadě shodné s heslem administrátora. Toto heslo umožňuje odebrat instanci služby AD offline.

✔ All prerequisite checks passed successfully. Click 'Install' to begin installation. Show more ✕

- Deployment Configuration
- Domain Controller Options
 - DNS Options
- Additional Options
- Paths
- Review Options
- Prerequisites Check
- Installation
- Results

Prerequisites need to be validated before Active Directory Domain Services is installed on this computer

[Rerun prerequisites check](#)

⬆ View results

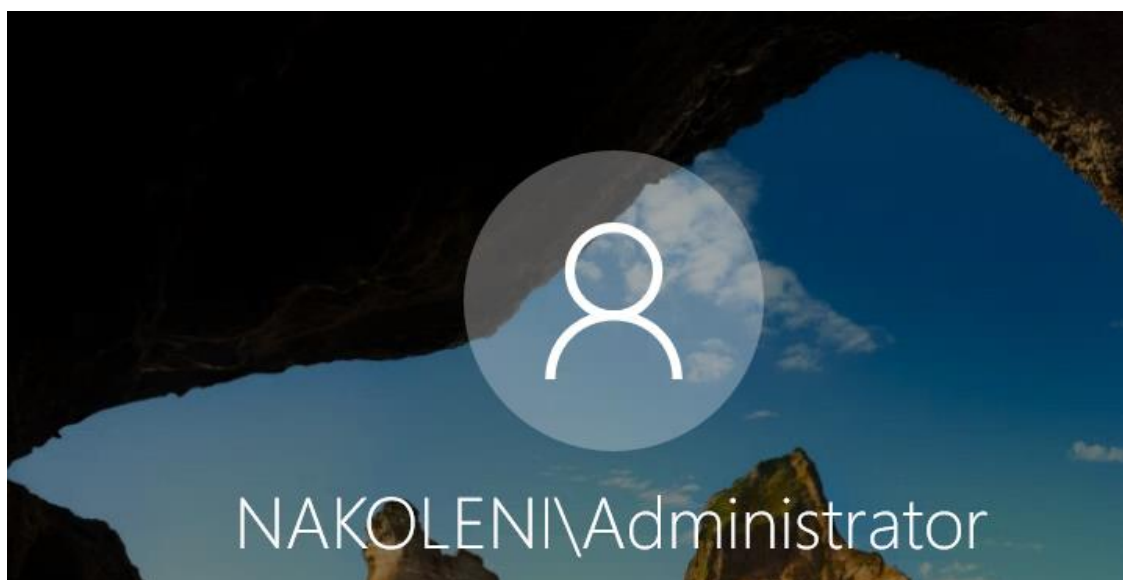
⚠ Windows Server 2019 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.

For more information about this setting, see Knowledge Base article 942564 (<http://go.microsoft.com/fwlink/?LinkId=104751>).

⚠ This computer has at least one physical network adapter that does not have static IP address(es) assigned to its IP Properties. If both IPv4 and IPv6 are enabled for a network adapter, both IPv4 and IPv6 static IP addresses should be assigned to both IPv4 and IPv6 Properties of the physical network adapter. Such static IP address(es) assignment

K pokračování je nutné stisknout tlačítko *Next>* a projít procesem instalace, viz jednotlivé následující obrázky. *Vyučující komentuje postup dle svého uvážení.*

Po restartování operačního systému by měla přihlašovací obrazovka již zohledňovat doménový název zadaný v předchozí části.



Kontrolní bod

Studenti projdou jednotlivé kroky nastavení doménového řadiče a následných kroků dle ukázky vyučujícího. Ověří si i podobu přihlašovací obrazovky i po restartu počítače.

2.5 Základní struktura AD a její naplnění

V následující části dojde k vytvoření uživatelů, viz následující obrázková sekvence. *Vyučující předvede nejméně vytvoření doménového administrátora včetně jeho přidání mezi doménové administrátory a vytvoření běžného uživatele. Dále upozorní na to, že předvedený nástroj není jediný pro tyto kroky (např. Active Directory Administrative Center).*

Active Directory Users and Computers

File Action View Help

Active Directory Users and Computers

Active Directory Users and Computers

Name	Type	Description
Administrator	User	Built-in account for ad...
Allowed RO...	Security	...
Cert Publish...	Security	...
Cloneable D...	Security	...
Denied ROD...	Security	...
DnsAdmins	Security	...
DnsUpdateP...	Security	...
Domain Ad...	Security	...
Domain Co...	Security	...
Domain Con...	Security	...
Domain Gue...	Security	...
Domain Users	Security	...
Enterprise A...	Security	...

New Object - User

Create in: nakoleni.cz/Users

First name: Karel Initials:

Last name: Jiman

Full name: Karel Jiman

User logon name: kareljiman @nakoleni.cz

New Object - User

Create in: nakoleni.cz/Users

Password: ●●●●●●

Confirm password: ●●●●●●

User must change password at next logon

User cannot change password

Password never expires

Account is disabled

Active Directory Users and Computers

Active Directory Users and Computers

Name	Type	Description
Administrator	User	Built-in account for ad...
Allowed RO...	Security	...
Cert Publish...	Security	...
Cloneable D...	Security	...
Denied ROD...	Security	...
DnsAdmins	Security	...
DnsUpdateP...	Security	...
Domain Ad...	Security	...
Domain Co...	Security	...
Domain Con...	Security	...
Domain Gue...	Security	...
Domain Users	Security	...
Enterprise A...	Security	...

Copy...

Add to a group...

Disable Account

Reset Password...

Move...

Open Home Page

Send Mail

All Tasks >

Cut

Delete

Select Groups

Select this object type:

From this location:

Enter the object names to select (examples):

Name	Description	In Folder
Domain Admins	Designated administrators of th...	nakoleni.cz/Users
Domain Computers	All workstations and servers joi...	nakoleni.cz/Users
Domain Controllers	All domain controllers in the do...	nakoleni.cz/Users
Domain Guests	All domain guests	nakoleni.cz/Users
Domain Users	All domain users	nakoleni.cz/Users

Select Groups

Select this object type:

From this location:

Enter the object names to select (examples):

Alternativně:

Create User:

TASKS SECTION

Account

Organization

Member Of

Password Settings

Profile

Policy

Silo

Account

First name:

Middle initials:

Last name:

Full name: *

User UPN logon: @

User SamAccountName I...: *

Password:

Confirm password:

Create in: CN=Users,DC=nakoleni,DC=cz [Change...](#)

Protect from accidental deletion

Log on hours... Log on to...

Account expires: Never End of

Password options:

User must change password at next log on

Other password options

Microsoft Passport or smart card is required for interactive log...

Password never expires

User cannot change password

Encryption options:

Other options:

Kontrolní bod

Studenti si dle ukázky vyučujícího vytvoří základní strukturu AD včetně založení doménového administrátora a běžného uživatele. Studenti důsledně dbají pokynů vyučujícího.

3 Napojení klientské stanice

Tuto část scénáře může vyučující realizovat dle svého rozhodnutí – měla by být provedena včetně vyzkoušení ze strany studentů, nicméně v případě časové nedostatečnosti se lze spokojit se základním předvedením ze strany vyučujícího či s předvedením v jiné části výuky (například i vůči jinému AD nebo dokonce LDAP dle volby vyučujícího).

Pro tuto část scénáře je nutné využít desktopový operační systém, který má síťovou viditelnost na výše popsany server.

Vyučující předvede napojení tohoto klientského počítače do domény, a to pomocí následujících kroků:

- 1. Nastavení DNS serverů na adresu AD serveru (vlastnosti připojení)*
- 2. Napojení počítače do domény (např. z Informace o počítači->Upřesnit nastavení systému)*
- 3. Restartování počítače*
- 4. Přihlášení doménovým uživatelem*

Kontrolní bod

Studenti si napojí svoji instanci desktopového operačního systému na dříve konfigurovanou doménu (AD).

Shrnutí a závěr

Studenti se seznámili s principem adresářových služeb, vyzkoušeli si zprovoznění Microsoft Active Directory a dle časové dotace také základní správu a napojení klientského počítače. Dle svého uvážení může vyučující připravit pro studenty praktický úkol nebo v případě větší časové dotace rozebrat další funkcionalitu, jako je nastavení služby včetně implementace bezpečnostních politik.

Seznam použitých zdrojů

Learn. *Active Directory Domain Services*. Dostupné z: <https://learn.microsoft.com/cs-cz/training/paths/active-directory-domain-services/>

Nápověda Windows. Dostupné z operačního systému.

Wikipedia. *Active Directory*. Dostupné z: https://cs.wikipedia.org/wiki/Active_Directory

ConceptDraw. *ActiveDirectoryHierarchicalStructure*. Dostupné z: <https://www.conceptdraw.com/samples/resource/images/solutions/network-diagram/network-diagram-ActiveDirectoryHierarchicalStructure.png>