



KIV/SPOS

Poznámky k cvičením na platformě Windows

aktuální verze: 7.4.2015

OBSAH

- vytvoření virtuálního stroje
- konfigurace RAIDu
- shadow copy
- dodatky
- sdílení
- firewall
- DNS server



VYTVOŘENÍ VIRTUÁLNÍHO STROJE



POUŽITÝ SW

○ Oracle VM VirtualBox

- zdarma ke stažení (Windows, Linux, Mac OS X,...)

○ Windows Server 2012 R2 with Update

- pro studenty dostupný v rámci DreamSpark Premium

soubor **.vdi** obsahuje vlastní obraz virtuálního stroje
- velikost v řádu GB, např. cca 10GB

kromě něj ještě musíme nakonfigurovat virtuální stroj



KDE JSOU VIRTUÁLNÍ OBRAZY ULOŽENY?

V UC326 po přihlášení do Windows

d:\spos2015

master - vzorový, nechat být

u1 - na Vaše experimenty

Pokud se Vám něco pokazí, vytvořit si podadresář

d:\spos2015*vas_login*

a zkopírovat si sem soubor z adresáře master
(trvá několik minut)



KONFIGURACE NOVÉHO VIRTUÁLU

1. Pustíme Oracle VM VirtualBox
2. Počítač – Nový – next
 - název: *SPOS_login*
 - OS: *Microsoft Windows*
 - verze: *Windows 2012 64bit*
3. velikost paměti: *8GB*
4. *2 CPU*
5. pevný disk
 - bootovací pevný disk
 - použít existující pevný disk => vybrat
d:\spos2015\u1\disk1.vdi



PROVOZ VIRTUÁLNÍHO STROJE

○ spuštění

- zařízení – Instalovat přídatky pro hosta
- menu **Počítač – Vložit Ctrl+Alt+Dell** (!!!)
- zadat heslo (tady je nenajdete!)

○ ověřit konektivitu

- Firefox – oblíbená web. stránka
- jak mě vidí vnější svět? Firefox – <http://mojeip.cz>
- jakou IP adresu mám?
příkazový řádek - `ipconfig /all {10.0.2.15}`

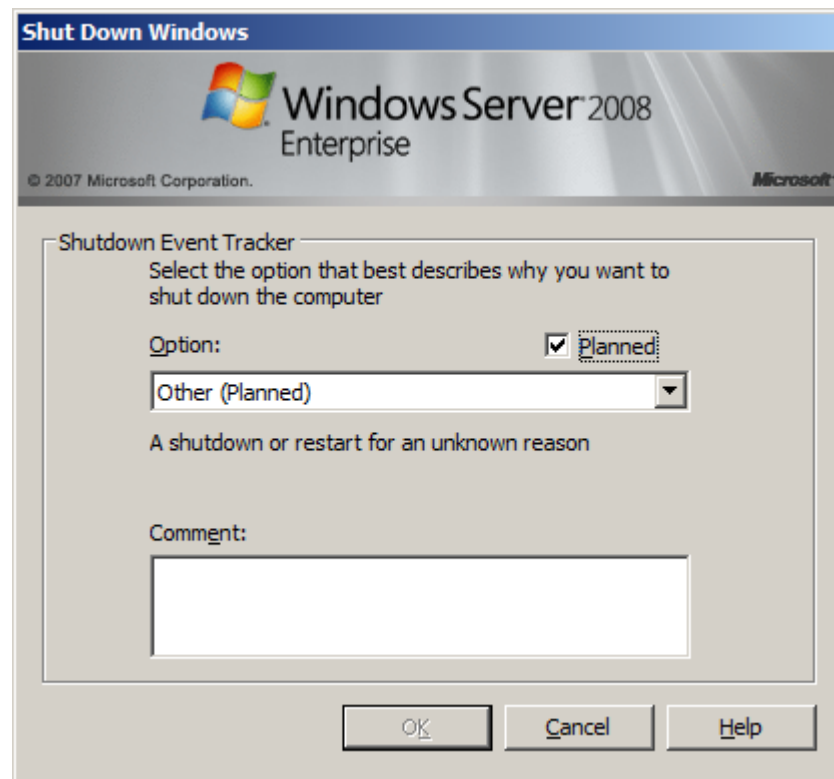


VYPNUTÍ VIRTUÁLNÍHO STROJE (SERVER2008)

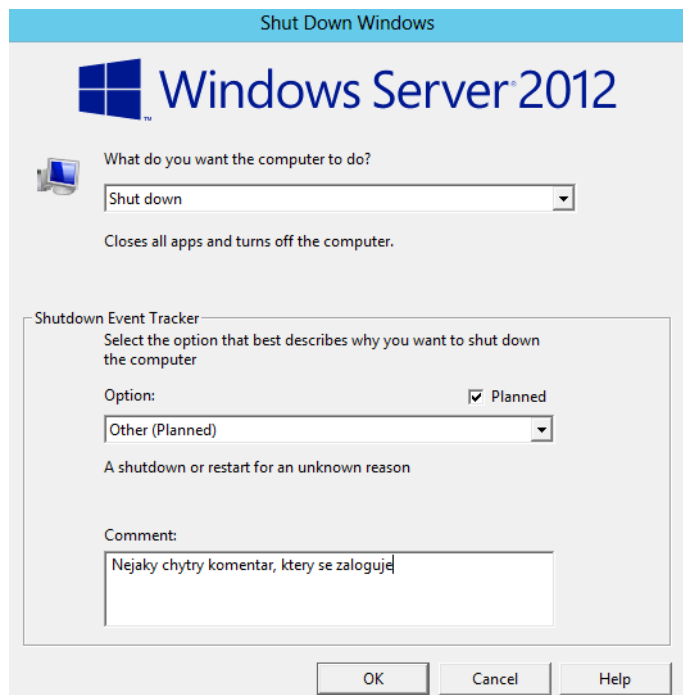
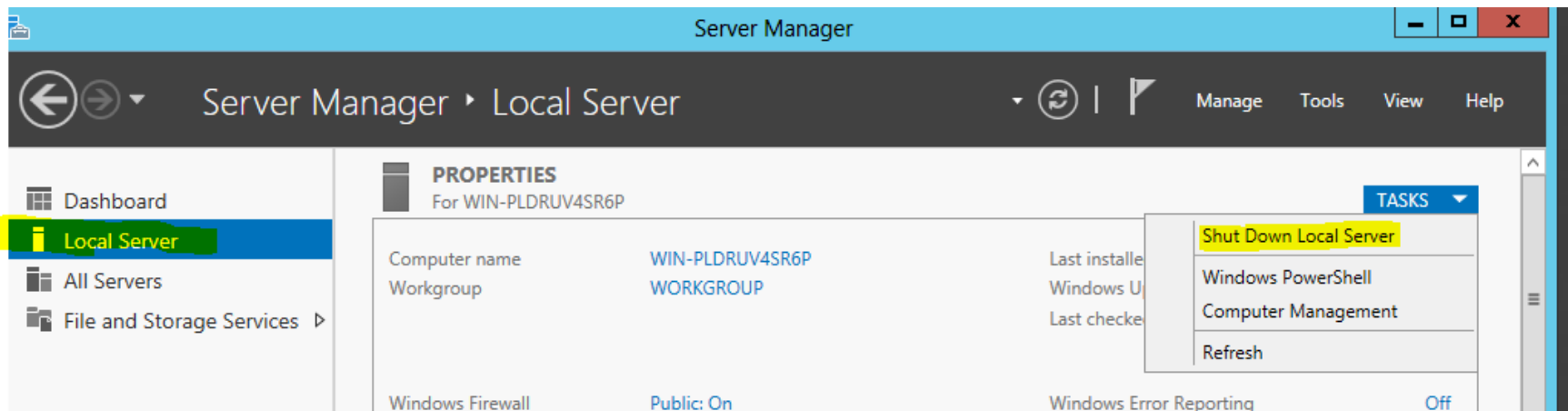
○ Start – Shutdown

Windows Server 2008
požaduje vždy zadat
důvod restartu –
kvůli logování

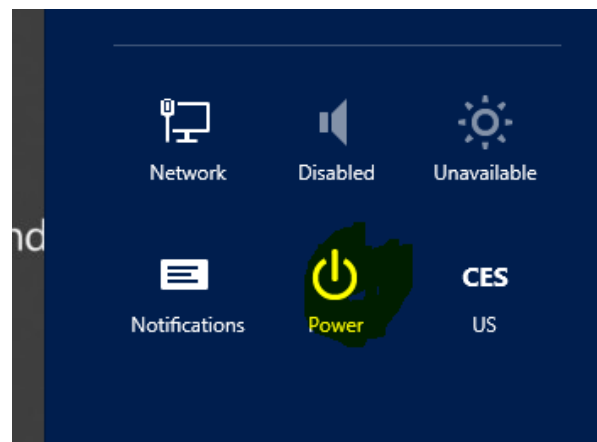
- HW údržba
- HW instalace
- OS rekonfigurace
- Aplikace údržba
- Aplikace instalace
- Security Issue
- Other



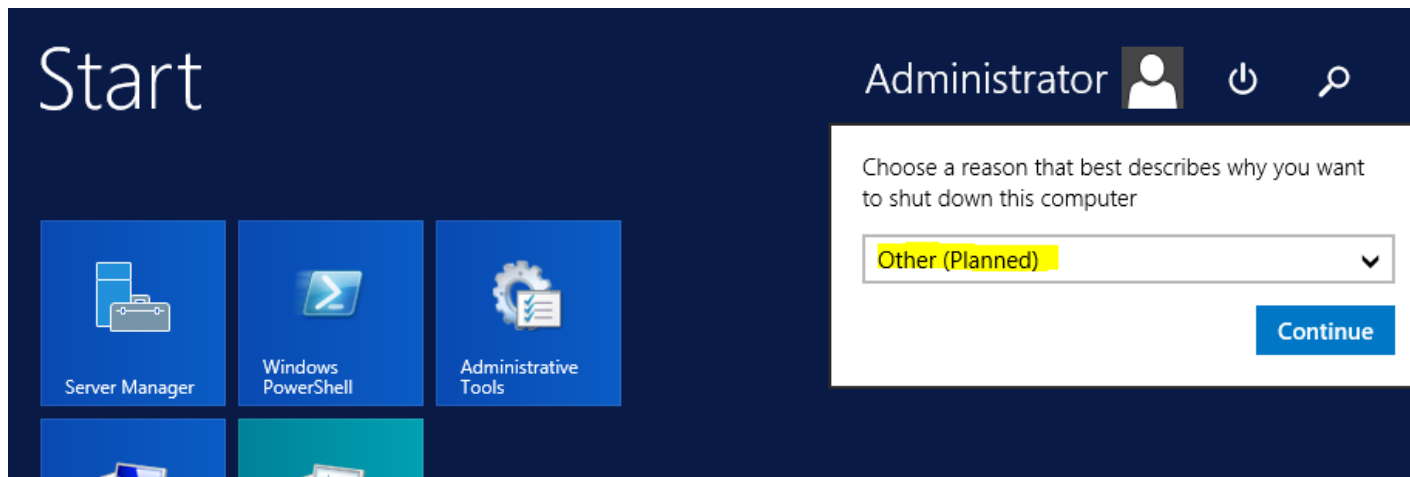
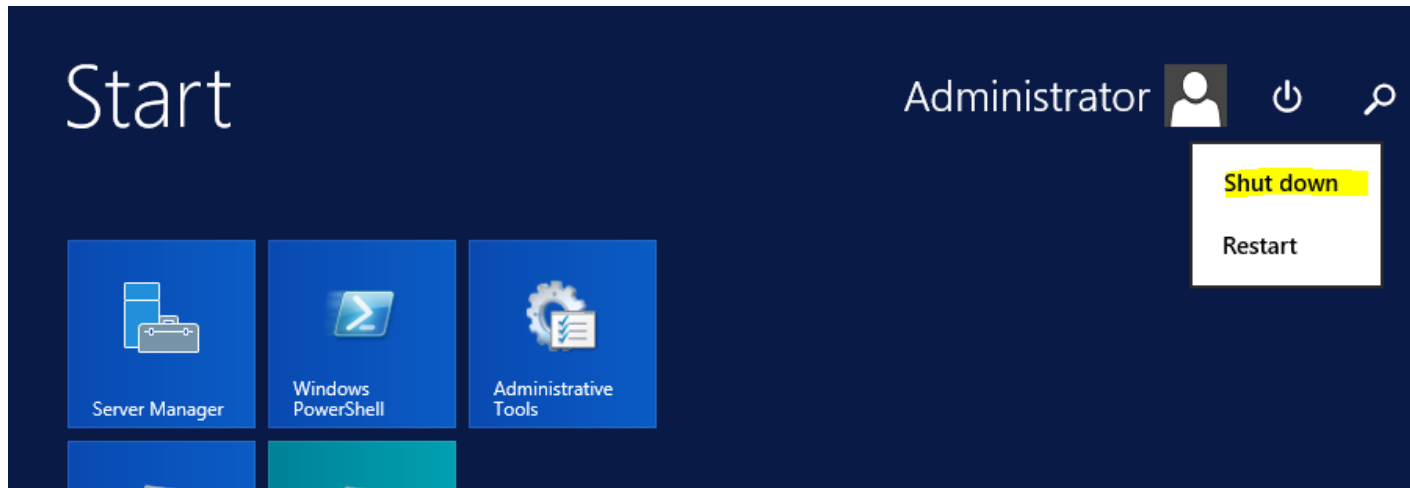
VYPNUTÍ VIRTUÁLNÍHO STROJE (2012)



Windows Server 2012 požaduje zadat důvod restartu – kvůli logování, při vypnutí viz dole ne



VYPNUTÍ VIRTUÁLNÍHO STROJE 2012R2



ZMĚNA KONFIGURACE VIRTUÁLNÍHO STROJE – SÍŤ

- U vypnutého virtuálního stroje můžeme měnit jeho nastavení
- Síť – karta 1
 - povolit síťovou kartu
 - Připojena k:
 - NAT
 - Síťový most
 - název: Intel (skutečná síťová karta PC)
 - pokročilé
 - typ síťové karty: Intel Pro/1000 MT Desktop
 - MAC adresa: ponechat

síťová karta PC u kterého sedíte

síťová karta kterou uvidí Váš virtuál

NASTAVENÍ SÍTĚ

- Zkuste změnit síťovou kartu (z NAT => síťový most)
- je třeba nastavit síťovou adresu (nedostane přes DHCP)
- na monitoru máte číslo PC, např. 7
 - IP adresa: 147.228.67.**70+7**
 - subnet mask: 255.255.255.0
 - default gateway: 147.228.67.1
 - DNS server: 147.228.52.11
 - Windows se zeptají na profil sítě: *private network*
- Firefox, <http://mojeip.cz>



ZMĚNA JMÉNA POČÍTAČE

Server Manager – Local Server –
Computer Name – Change



Stejným způsobem lze server přidat do domény.



SERVER MANAGER -> LOCAL

- jméno serveru
- doména, ve které je
- **nastavení updatů (automaticky, vypnout)**
- firewall
- remote desktop
- **ethernet - změna IP adresy atd.**
- IE enhanced security conf (nainstalovat Firefox)
- časová zóna

Task – Computer Manager (!), ShutDown



VYTVOŘENÍ RAID



PŘÍPRAVA FYZICKÝCH DISKŮ

Před spuštěním virtuálního stroje:

- Virt.stroj – nastavení – úložiště
 - (přidat SATA řadič)
 - přidat nový disk

disk2.vdi 100MB

d:\spos2015\u1\diskA.vdi

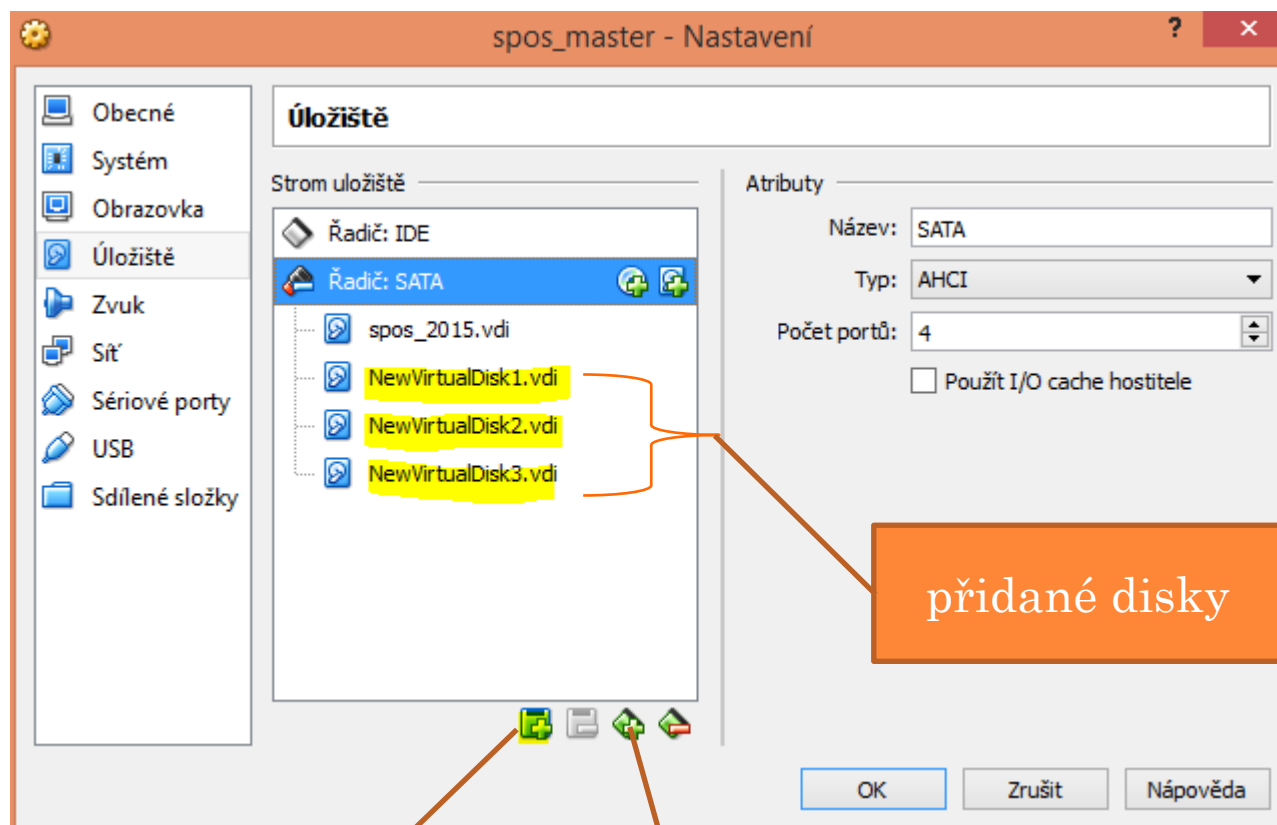
disk3.vdi 100MB

d:\spos2015\u1\diskB.vdi

disk4.vdi 100MB

d:\spos2015\u1\diskC.vdi





přidá disk

přidá řadič



KONFIGURACE DISKŮ

Server Manager – Local Server - Tasks-Computer
Management – Storage - Disk Management
(z příkazové řádky: `diskmgmt.msc`)

- disk online / offline
- basic disk / convert to dynamic disk
- convert to GPT disk (x MBR)
- properties – policies (enable write caching)

http://en.wikipedia.org/wiki/Logical_Disk_Manager

http://en.wikipedia.org/wiki/GUID_Partition_Table

<http://www.dynamic-disk.com/difference-between-basic-and-dynamic-disk.html>



VYTVOŘENÍ RAID 5

- disk1 – pravá myš – new RAID 5 volume
- přidáme disk2, disk3

výsledek:

- disky se změny na dynamické
- probíhá resynchronizace
- vytvořen RAID 5 (odlišení barvou)



EXPERIMENTY

- zkontrolovat výslednou kapacitu disku (3x100MB na RAID 5, tedy 200MB)
- disk2 offline – RAID stále funguje
(Win2008: EventLog: System, FT Orphaning, id 26)
(Win2012: EventLog: System id 142 volmgr)
- reaktivace disku
- shodíme 2 disky (zkuste pak hned vrátit)
- delete volume

Filtr logu na id 142
nebo source volmgr



VYTVOŘENÍ RAID 1 (MIRROR)

- disk1 – pravá myš – new MIRRORED volume
- přidáme disk2
- zkontrolovat kapacitu? (2x100MB, výsledná 100MB)
- jeden disk offline
- vrátit (foreign) – import foreign disk
- REMOVE MIRROR
 - bude unallocated
- BREAK MIRROR
 - E:, F: budou obsahovat stejná data



VYTVOŘENÍ STRIPPED VOLUME (RAID 0)

- Disk1 a lze přidat Disk2, i Disk3, kapacita 300MB
- kterýkoliv dáme offline - failed
- (online - vzpamatuje se)



SPANNED VOLUME

- vytvoříme z Disk1, disk2
- **extend** volume
 - přidáme disk3
- **shrink** volume
 - dialog, o kolik dovolí disk zmenšit (!)



SHADOW COPY

- Nechť je dán E: RAID 5, a soubor pokus.txt
- pravá myš na souboru – restore to previous versions

jak povolit?

- disk E:, vlastnosti, shadow copies
- enable, je tam možnosti změnit plány (7:00 a 12:00)
 - Create Now
 - změní obsah pokus.txt
 - pokus.txt, vlastnost, previous versions
 - *open* - vidíme předchozí verzi
 - *restore* - obnovíme do předchozí verze



DODATKY, FIREWALL



ZOBRAZOVÁNÍ SOUBORŮ V EXPLORERU



- přípony souborů, skrývání souborů aj.
- častý problém *index.html.txt*, *index.aspx.txt*

pustit explorer.exe

- View – ribbon Options – tab View
 - odznačit hide extensions, hide protected OS files
 - oznacit show hidden files and folders

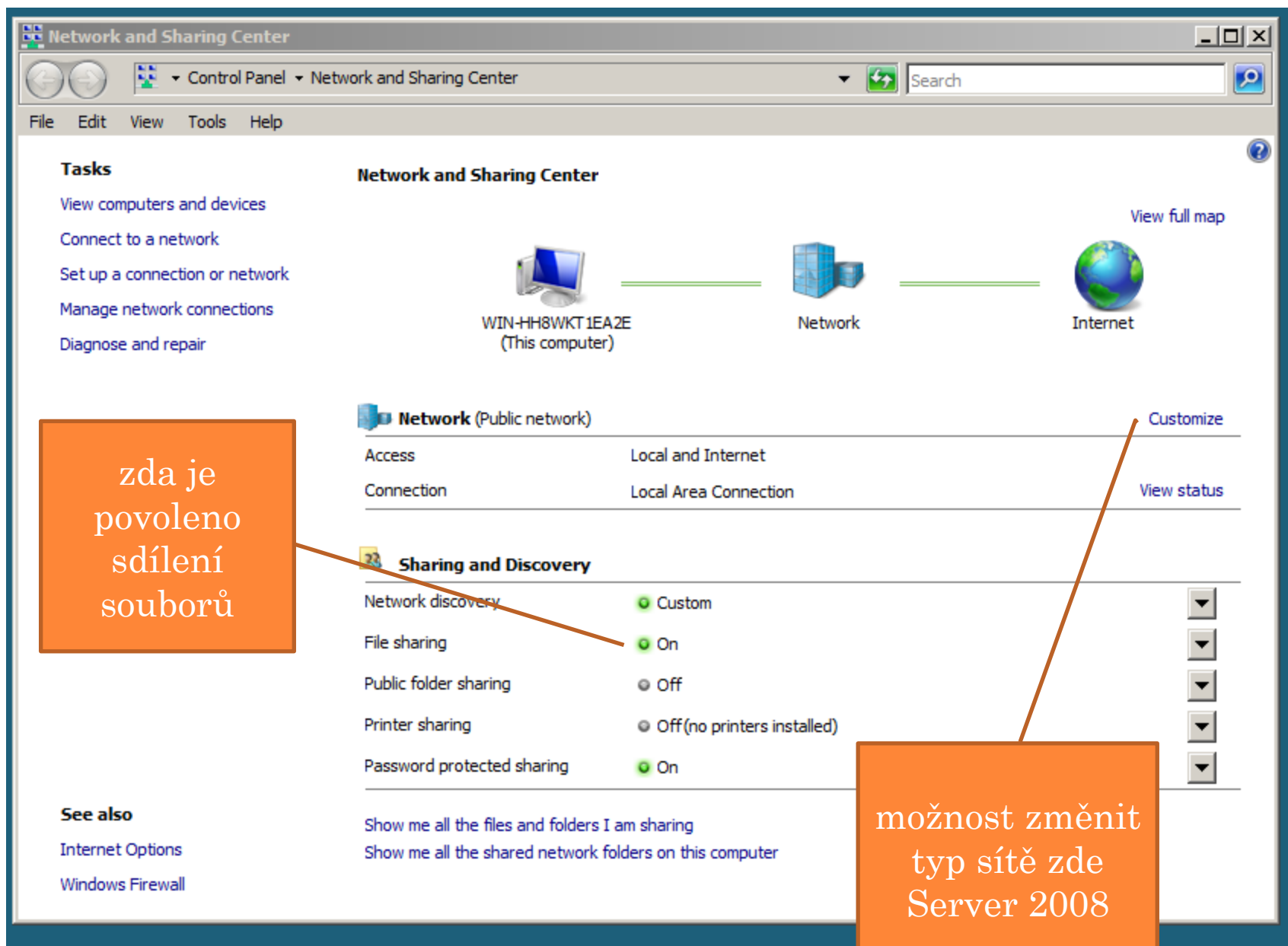
skrývání přípon souborů –
častý problém, který se přehlédne



SÍŤ

- Control panel (Win+X) – network and sharing center
- možnost změnit typ sítě (server 2008)
 - **public** network, **private** network (viz další slide)
 - další možnost **domain** network (když jsme v doméně)
 - souvisí s nastavením firewallu

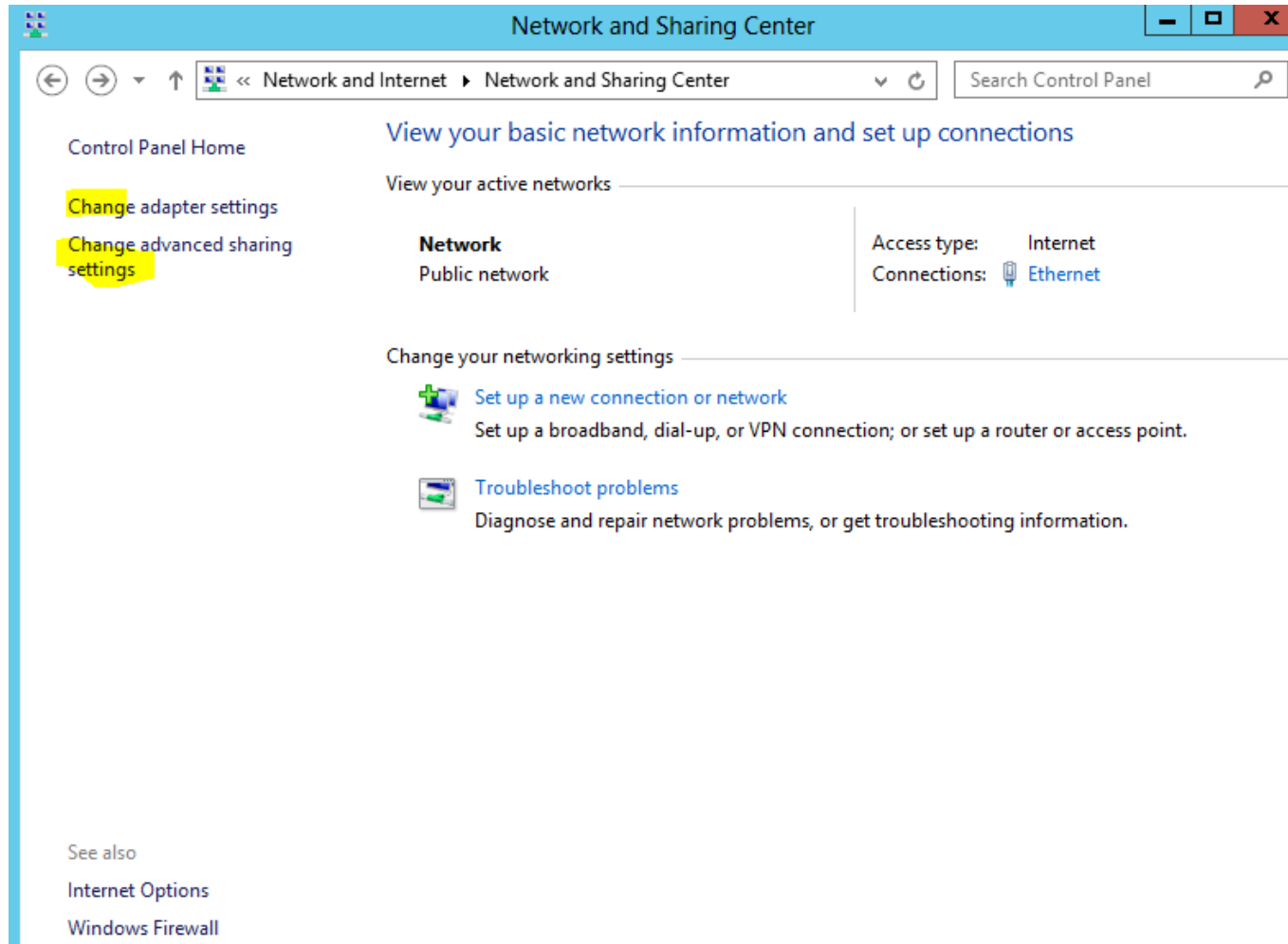




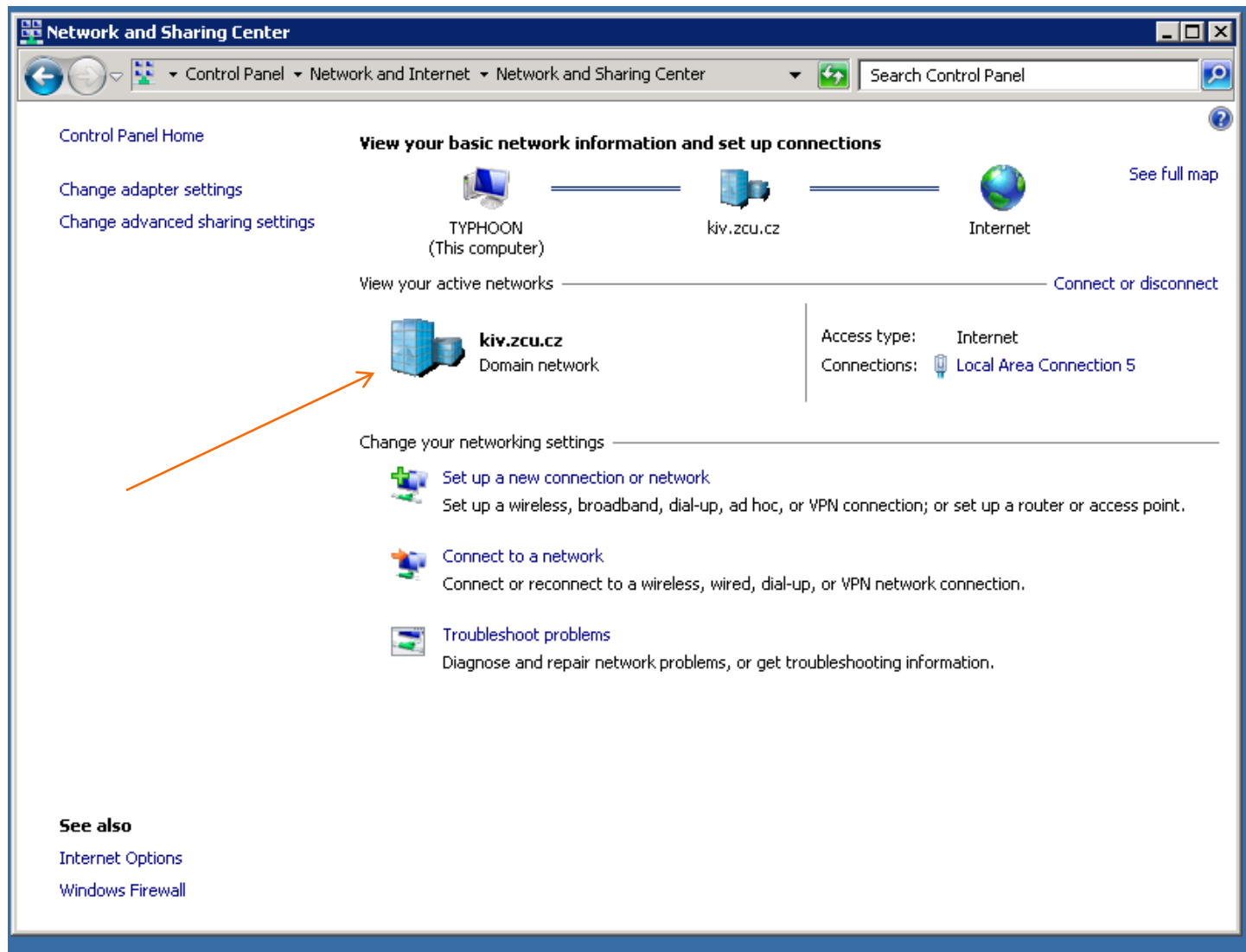
zda je
povoleno
sdílení
souborů

možnost změnit
typ sítě zde
Server 2008

NETWORK SHARING CENTER, SERVER 2012



UKÁZKA DOMAIN NETWORK (2008)



ZMĚNA TYPU SÍTĚ

- Gpedit.msc
Computer Configuration / Windows Settings /
Security Settings / Network List Manager
Policies.



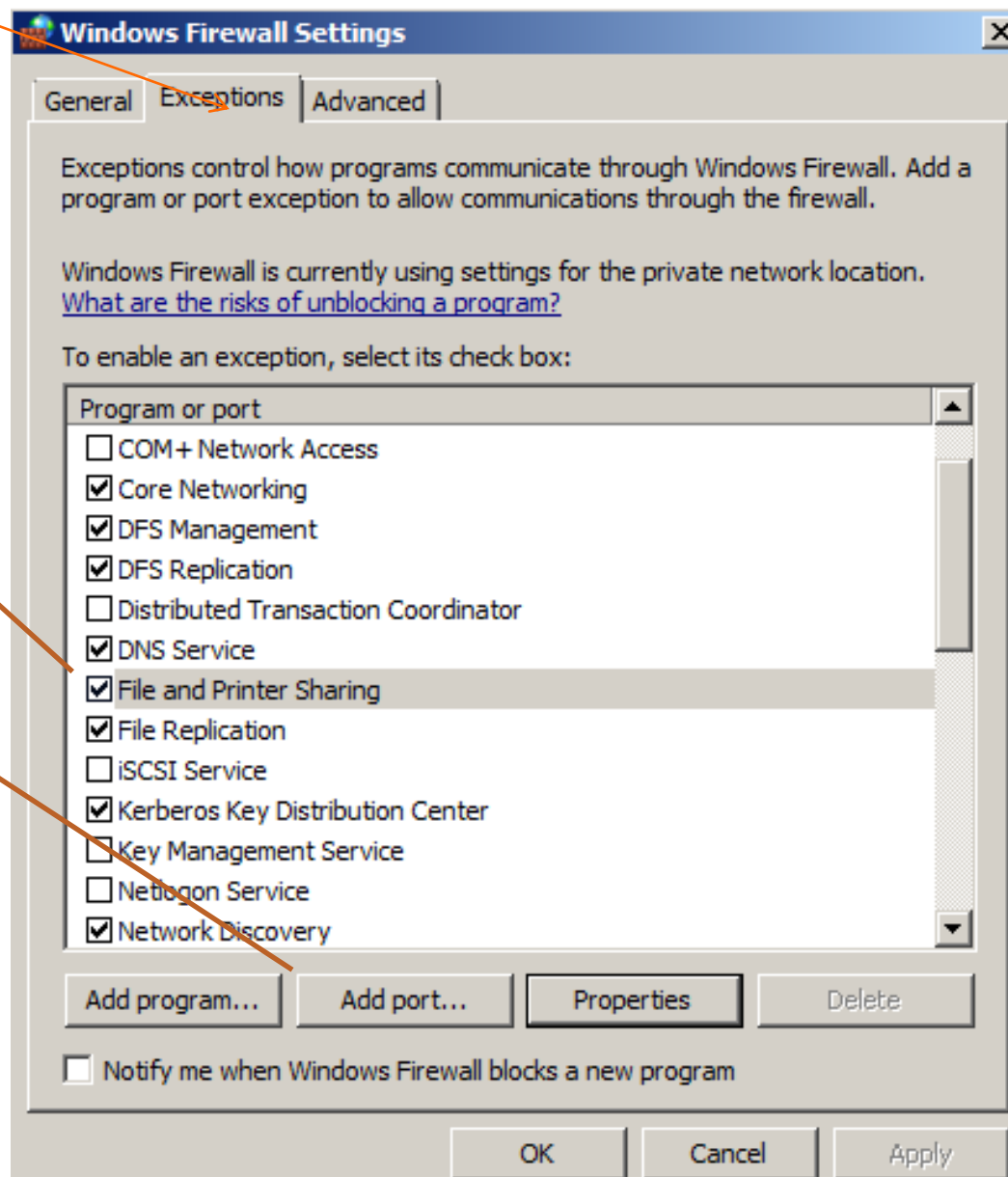
FIREWALL

- windows firewall
- windows firewall with advanced security
- windows firewall:
 - povolit port (TCP, UDP)
 - povolit program
 - omezit rozsah např. jen na určitý segment

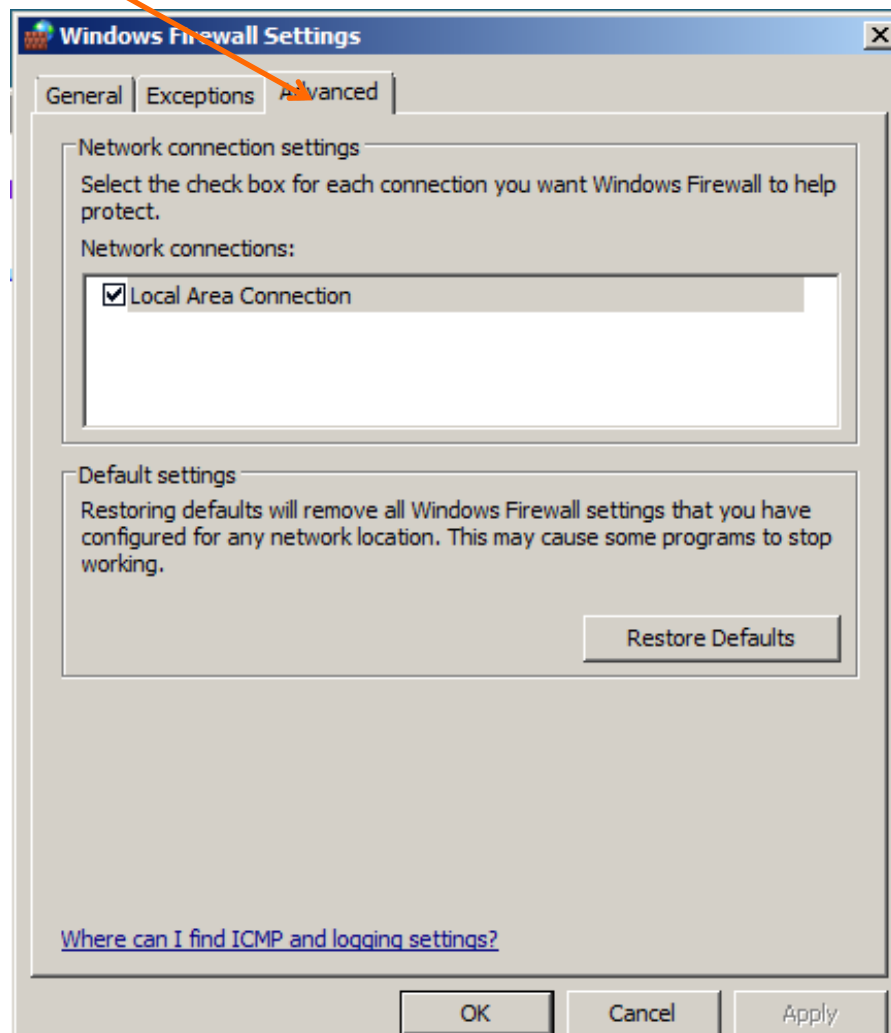
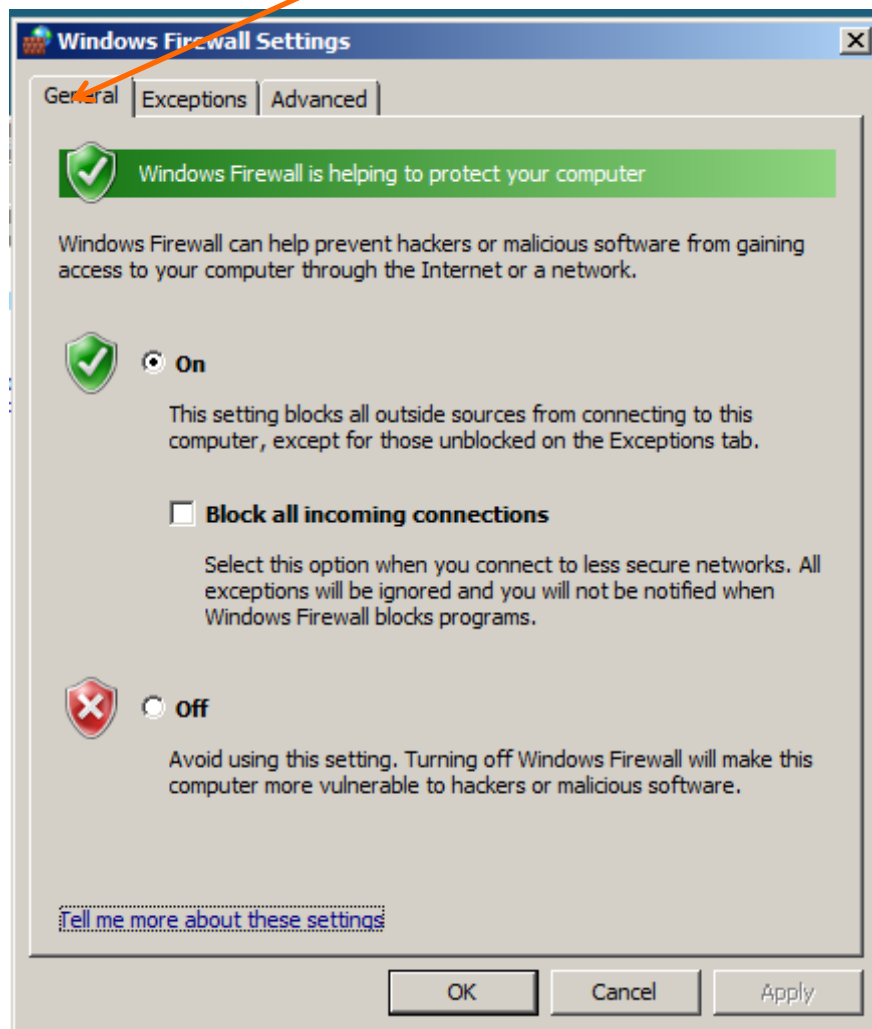


povolené
sdílení souborů

přidat program,
port



VYPNUTÍ-ZAPNUTÍ FW, POUŽITÁ ROZHRAŇÍ



FIREWALL – SERVER 2012

Windows Firewall

Control Panel > System and Security > Windows Firewall

Search Control Panel

Control Panel Home

Allow an app or feature through Windows Firewall 1

Change notification settings

Turn Windows Firewall on or off

Restore defaults

Advanced settings 2

Troubleshoot my network

Help protect your PC with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Private networks Not connected

Guest or public networks Connected

Networks in public places such as airports or coffee shops

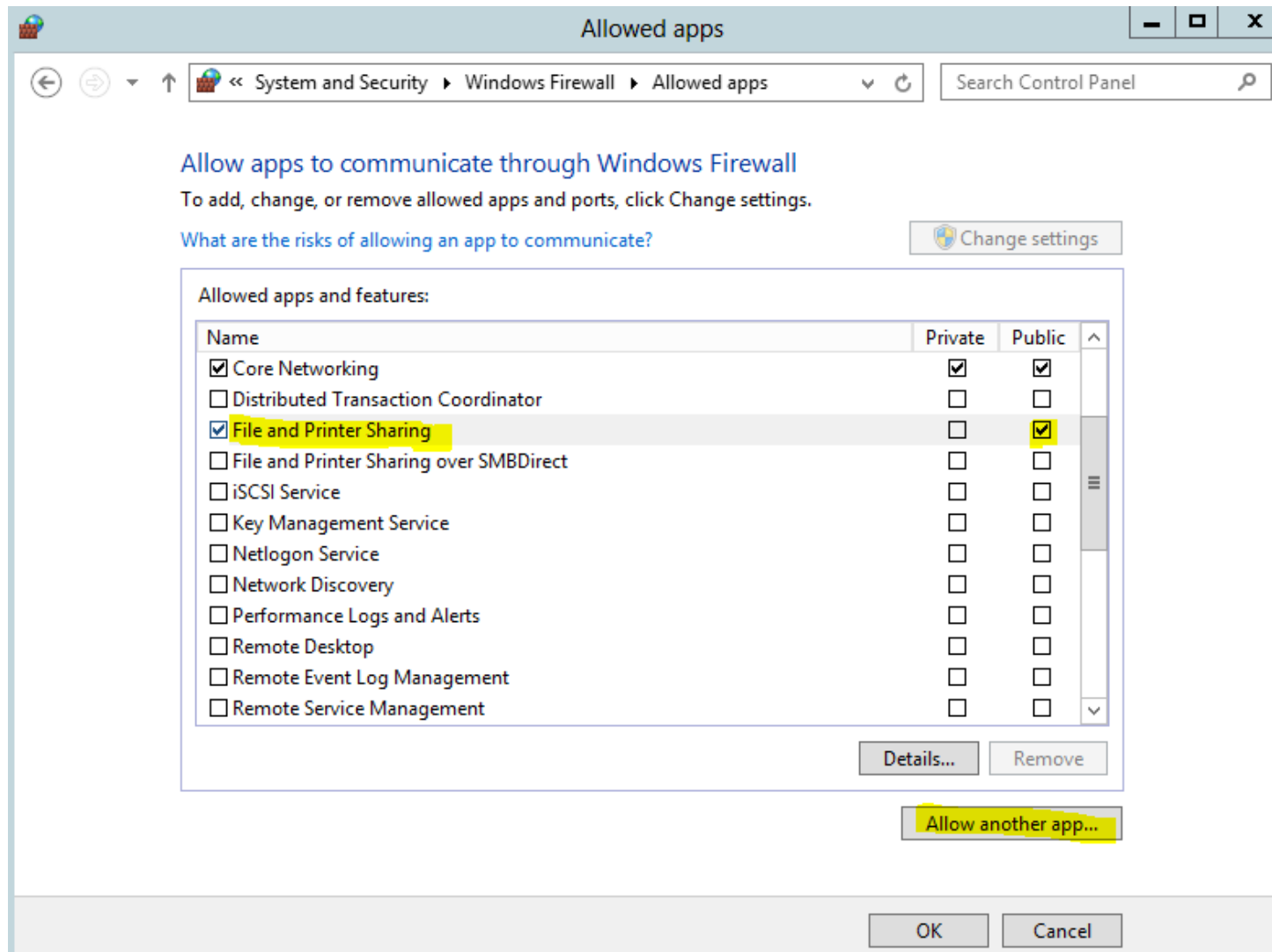
Windows Firewall state:	On
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active public networks:	Network
Notification state:	Do not notify me when Windows Firewall blocks a new app

See also

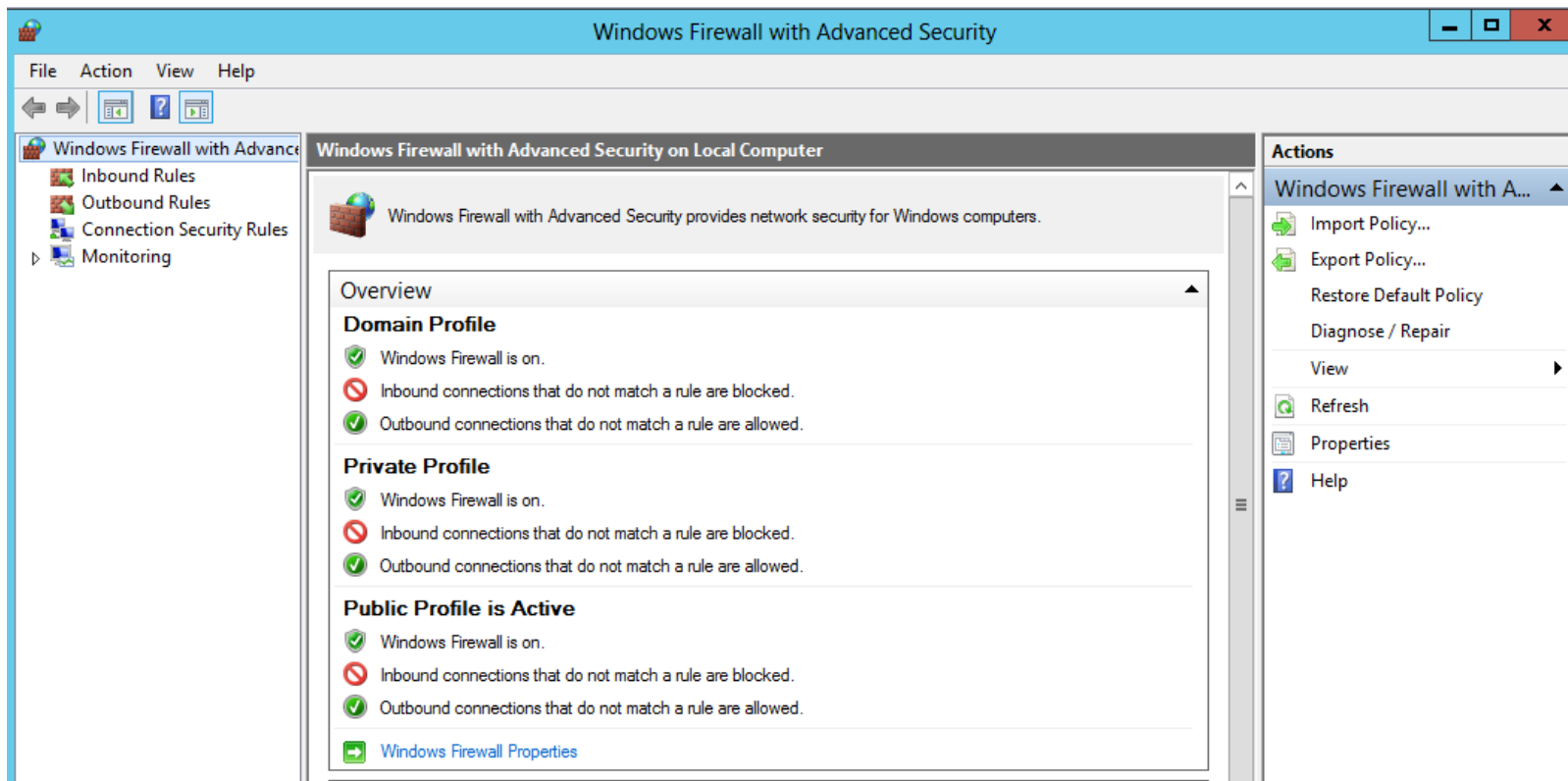
Action Center

Network and Sharing Center

FIREWALL – SERVER 2012



FIREWALL – SERVER 2012 - ADVANCED



WINDOWS FIREWALL WITH ADVANCED SECURITY

- **domain, private, public** profile
- poznáme, který profil je *aktivní* (*.. is ACTIVE*)
- poznáme, jestli je v daném profilu firewall *spuštěný*
- jak se chová k příchozím / odchozím spojením, která *nejsou* v pravidlech



PŘÍKLAD – SOUHRNNÁ INFORMACE

Public Profile is **Active**

Windows firewall is **on**

Inbound connections that do not match a rule are
blocked

Outbound connections that do not match a rule are
allowed



PŘÍKLAD – INBOUND PRAVIDLO

- **File and Printer Sharing** (group)
 - (Echo Request ICMPv4-in, ICMPv6-in, NB-Datagram-In, NB-Name-In, NB-Session-In, SMB-In, Spooler Service- RPC, Spooler Service-RPC-EPMAP)
- Domain, Private, Public
- Enabled: yes .. říká jen že pravidlo je aktivní!!
- Action: allow

pozor, snadno se splete, *enabled yes* neznamená že je *action allow*, pravidlo může být i opačného významu

VYZKOUŠEJTE

- Nastavit filter, aby se zobrazila pravidla jen pro
Group: File and Printer Sharing
Profile: Public
- Vytvořit nové vstupní pravidlo, které povolí port 8005 pro TCP ve všech profilech
 - název: moje 8005 TCP
- Jak zařídím aby byl port povolen pro TCP i UDP?
- Jak vyfiltruji zobrazení, aby bylo vidět pouze
námi vytvořená pravidla?
(Rules without a group)



ZOBRAZENÍ LOGU

- Adv. Firewall – Monitoring

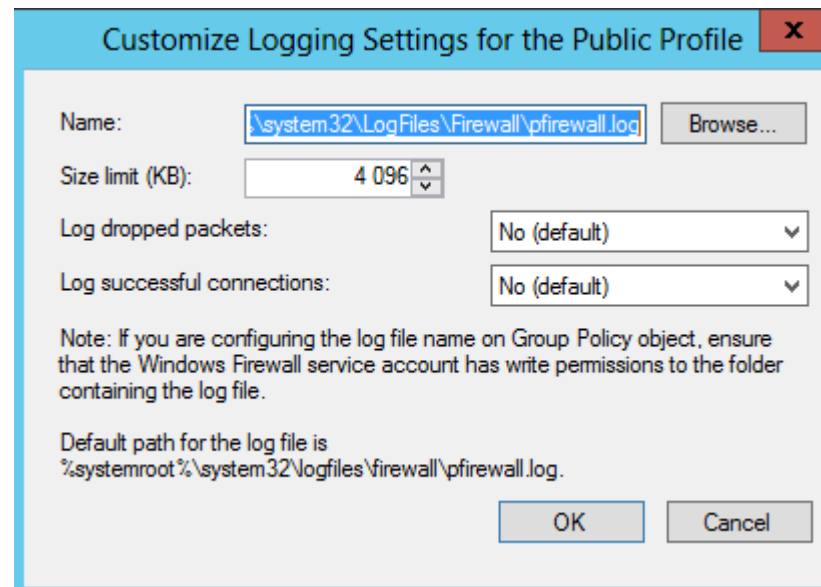
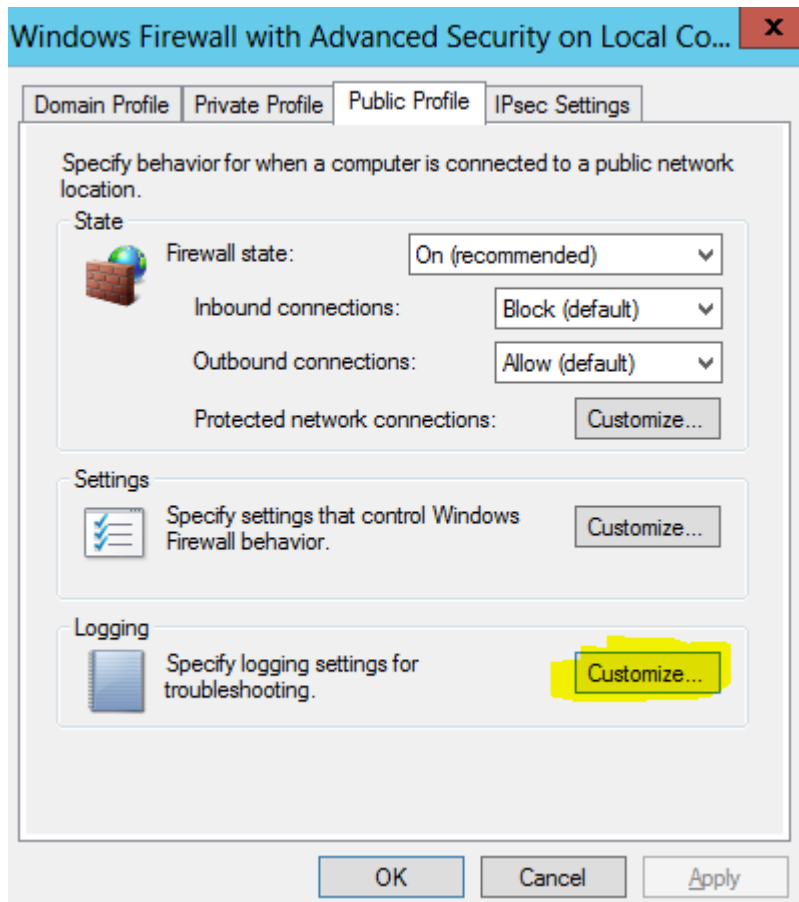
- je zde cesta k log souboru:

*%systemroot%\system32\LogFiles\Firewall
\pfirewall.log*

- log dropped packets (není defaultně)
- log successful connection (není defaultně)
- lze nastavit pro každý profil
(WfwithAS – properties – Logging)



NASTAVENÍ LOGOVÁNÍ (WINDOWS FIREWALL – PRAVÁ MYŠ – PROPERTIES)



IMPORT, EXPORT NASTAVENÍ

- Import Policy, Export Policy
 - zaloha.wfw
 - binární soubor
- Inbound (Outbound) Rules -> Export List
 - vyfiltrovaný seznam na obrazovce
 - seznam.txt



SDÍLENÍ

- vytvořit E:\sdileni
- nastavit **advanced sharing** pro *everyone read*
- namapovat jako disk Z:
- ověřit, že nejde zapsat do adresáře
- zobrazit seznam sdílení daného serveru
(Computer Management – Shared Folders - Shares)



VYTVOŘENÍ LOKÁLNÍHO UŽIVATELE (ZATÍM BEZ ACTIVE DIRECTORY)



- Control Panel – User Accounts
- Server Manager – Local Server – Tasks – Computer Management – Local Users and Groups
- Manage another account – Create new account
 - jméno účtu (např. **ufon**)
 - typ účtu (standarní, admin)
- Nastavení hesla vytvořenému účtu
- Zkuste vytvořit / zrušit účet



ÚLOHA

- vytvořte si lokální účet
(user: *ufon* , heslo: *vzducholod..11*)
- vytvořte sdílení
adresář: *c:\data*
název sdílení: *share1*
práva: *ufon (r,w)*
- nasdílejte si adresář vašeho kolegy
- příkazová řádka:
net user
net user ufon



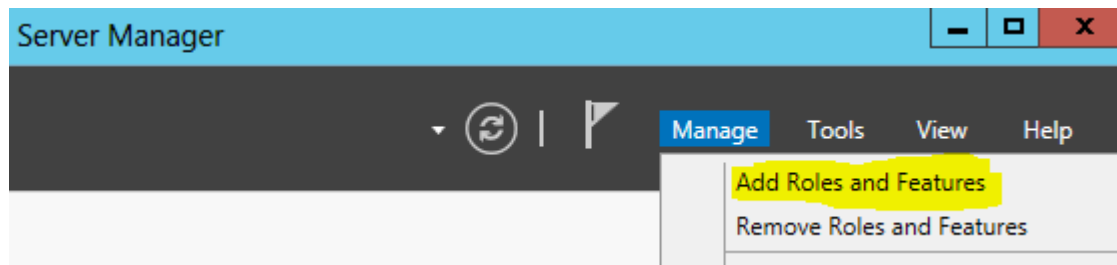
VYTVOŘENÍ UŽIVATELE Z PŘÍKAZOVÉ ŘÁDKY

- `net user ufon vzducholod.11 /add`
 - Přidá uživatele ufon
 - Nastaví heslo na vzducholod.11

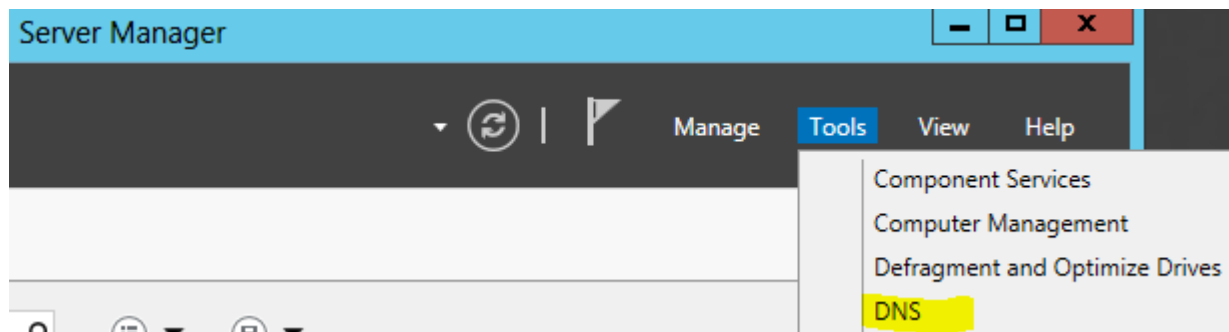


DNS

- Server Manager – Local Server
- Manage - Add Role – DNS Server



- puštění nástroje pro správu DNS:



KONFIGURACE DNS (!)

- Forward Lookup Zones - New Zone –
Primary zone - ***pesi.local***
- Zone file: pesi.local.dns
(bude v c:\windows\system32\dns)
- občas je třeba *update server data files*
(pravá myš na ikoně serveru)



PŘÍKLAD KONFIGURACE (ČÁST)

výsledný soubor:

@	A	147.228.64.148
@	MX	10 pesi.local.
konference	A	147.228.63.9
www	CNAME	pesi.local.
www2	CNAME	pesi.local.



PŘÍKLAD KONFIGURACE

klikneme na *pesi.local*

new host - (name nechat prazdne) - 147.228.64.148

new alias (CNAME) - www - Browse a
(same as parent..)

new alias (CNAME) - www2 - Browse a
(same as parent..)

new MX - host (same as parent) - fully qualified
name: pesi.local., priority:10



OVĚŘENÍ FUNKCIONALITY

- start – run – cmd

- nslookup

- help
- server **127.0.0.1**
- pesi.local
- www.pesi.local
- www2.pesi.local
- set type=ANY
 - pesi.local

IP adresa DNS serveru,
kterého se budete ptát



NASTAVENÍ POUŽÍVÁNÍ NAŠEHO DNS SERVERU (!!)

- jedna z nejčastějších chyb !!
- musíme nastavit DNS server, na který chceme, aby byly dotazy směrovány
- zkuste ping pesi.local, proč nejde?
- jako DNS server se nevyužívá náš vytvořený
- v konfiguraci sítě nastavíme jako používaný DNS server tento náš
- ověříme, že ping pesi.local zafunguje



DNS SERVER - DALŠÍ

- server – pravá myš – properties – root hints
.. seznam kořenových serverů
- dále např. seznam IP adres, na kterých poslouchá
- zkuste nslookupem otestovat, jak funguje DNS
vašeho kolegy
- **nslookup -debug**
- **dnscmd localhost /info**



SERVER MANAGER

○ Add Role

- DNS server, DHCP server, Web server
- File and Storage Services
- Active Directory Domain Services

○ Add Role Services

- u konkrétní role
- např. u WebServeru: ASP.NET, FTP server

○ Add Features

- .NET Framework, Message Queues, ...





Add Roles and Features Wizard



Select role services

DESTINATION SERVER
WIN-PLDRUV4SR6P

Before You Begin


Installation Type

Server Selection

Server Roles

Features

Web Server Role (IIS)

 Role Services

Confirmation

Results

Select the role services to install for Web Server (IIS)

Role services

<input checked="" type="checkbox"/>	Web Server
<input checked="" type="checkbox"/>	Common HTTP Features
<input checked="" type="checkbox"/>	Default Document
<input checked="" type="checkbox"/>	Directory Browsing
<input checked="" type="checkbox"/>	HTTP Errors
<input checked="" type="checkbox"/>	Static Content
<input type="checkbox"/>	HTTP Redirection
<input type="checkbox"/>	WebDAV Publishing
<input checked="" type="checkbox"/>	Health and Diagnostics
<input checked="" type="checkbox"/>	HTTP Logging
<input type="checkbox"/>	Custom Logging
<input type="checkbox"/>	Logging Tools
<input type="checkbox"/>	ODBC Logging
<input type="checkbox"/>	Request Monitor

Description

Web Server provides support for HTML Web sites and optional support for ASP.NET, ASP, and Web server extensions. You can use the Web Server to host an internal or external Web site or to provide an environment for developers to create Web-based applications.

IIS 8 (INTERNET INFORMATION SERVER)

- přidat roli WebServer (IIS)
 - Server Manager – Roles – Add – **Web Server (IIS)**
- přidat role service
 - WebServer: **Application Development – ASP.NET 4.5**
- ověření funkcionality:
 - <http://localhost>
- přibude Administrative Tools – IIS Manager





Server Manager



Windows
PowerShell



Administrative
Tools



Mozilla Firefox



DNS



Computer



Task Manager



Internet
Information...



Control Panel



Internet Explorer

Desktop

Windows Server 2012



NASTAVENÍ DNS – VÍCE WEBŮ

@	A	147.228.64.146
www	CNAME	pesi.local.
www2	CNAME	pesi.local.

○ budeme mít tři různé weby:

- <http://www.pesi.local>
- <http://www2.pesi.local>
- <http://pesi.local>

po spuštění IIS manageru nabídne instalaci Microsoft Web Platform !



MICROSOFT WEB PLATFORM



Spotlight, **Products**, Applications (WordPress, Joomla, ...)



IIS – VÍCE WEBŮ

- Start - Administrative tools - IIS Manager – Sites
- Add web site
 - Site name: www.pesi.local
 - Fyzická cesta: C:\inetpub\wwwroot\www.pesi.local
 - Host name: www.pesi.local
- Add web site
 - Site name: www2.pesi.local
 - Fyzická cesta: C:\inetpub\wwwroot\www2.pesi.local
 - Host name: www2.pesi.local

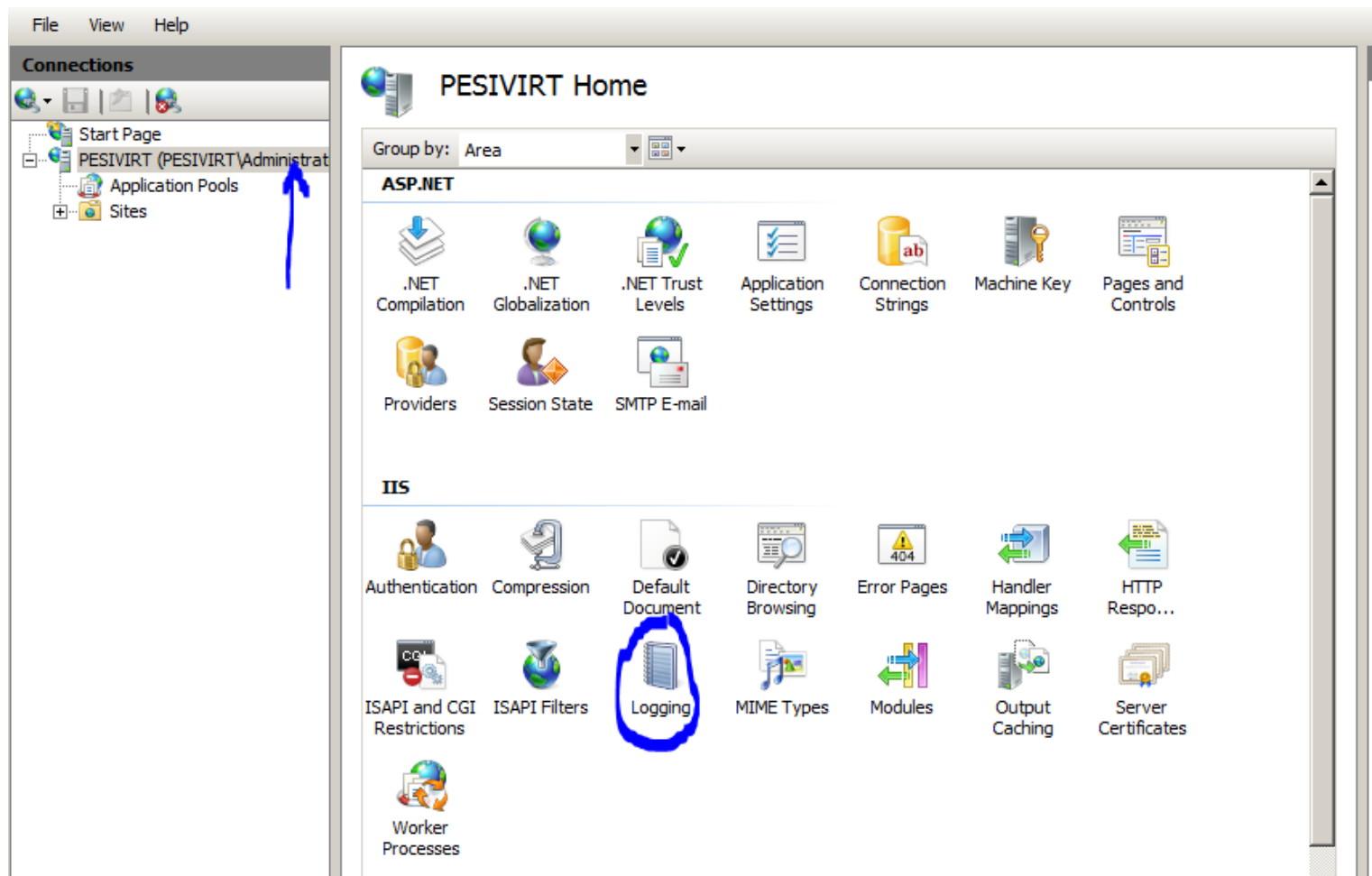


IIS: LOGOVÁNÍ

- IIS manager - jméno serveru (WIN-HH...) – sekce IIS - Logging
 - one log per site
 - format w3c - zkuste si select fields
 - adresář kam loguje:
%SystemDrive%\inetpub\logs\LogFiles
(tedy: c:\inetpub\logs\LogFiles)
- HTTP návratové kódy:
 - 200 - OK
 - 304 - Not Modified
 - 404 - Not Found



NASTAVENÍ LOGOVÁNÍ



ZÁZNAM V LOGU

- <http://www.pesi.local/URCITETOTAMNENI>
- zkontrolujeme záznam v logu:

Version: 1.0

#Date: 2011-03-23 09:57:12

#Fields: date time s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip
cs(User-Agent) sc-status sc-substatus sc-win32-status time-taken

2011-03-23 09:57:12 147.228.64.146 **GET /URCITETOTAMNENI** - 80 -
147.228.64.146

Mozilla/5.0+(Windows;+U;+Windows+NT+6.0;+cs;+rv:1.9.2.15)+Gecko/20110303
+Firefox/3.6.15+(.NET+CLR+3.5.30729) **404** 0 2 20



ASP.NET – PŘÍKLAD 1

vytvoříme soubor **pokus1.aspx**

(viz <http://home.zcu.cz/~pesicka/spos/>)

ověříme: <http://www.pesi.local/pokus1.aspx>

```
<%@ LANGUAGE = "VBScript" %>
<% on error resume next %>
<html>
<head><title>Ahojte všichni</title></head>
<% DIM i as Integer %>
<% For i = 1 To 3%>
    <body bgcolor="eaddfd">
        <font SIZE="<% = i %>">
            <font face="verdana, arial, helvetica">
                <p> Ahojte všichni<br>
            </font>
        </font>
    <% Next %>
</p>
</font>
</body></html>
```

Ahojte všichni

Ahojte všichni

Ahojte všichni



ASP.NET MOŽNOST ZMĚNY NASTAVENÍ (NENÍ POTŘEBA)

- IIS Manager – Application Pools
- www.pesi.local .. pravá myš - basic settings

The screenshot shows the Internet Information Services (IIS) Manager console. The left pane displays the 'Connections' tree with 'Start Page', 'WIN-PLDRUV4SR6P (WIN-PLD...', 'Application Pools', and 'Sites'. The right pane shows the 'Application Pools' page with a table of application pools. The 'www.pesi.local' pool is selected. An 'Edit Application Pool' dialog box is open, showing the configuration for 'www.pesi.local'.

Name	Status	.NET Fram...	Managed Pipel...	Identity	Applications
.NET v2.0	Started	v2.0	Integrated	ApplicationPoolId...	0
.NET v2.0 Classic	Started	v2.0			
Classic .NET AppPool	Started	v2.0			
DefaultAppPool	Started	v4.0			
www.pesi.local	Started	v2.0			
www2.pesi.local	Started	v4.0			

Edit Application Pool

Name:

.NET Framework version:

Managed pipeline mode:

☒ Start application pool immediately

OK Cancel

ASP.NET – PŘÍKLAD 2

pokus2.aspx:

```
<%@ LANGUAGE = "VBScript" %>
```

```
<% on error resume next %>
```

```
<html>
```

```
<head> <title>Ahojte všichni</title> </head>
```

```
<body bgcolor="eadfdf">
```

```
<form runat="server">
```

```
<asp:Label id="Label1"
```

```
runat="server"
```

```
forecolor="Blue">Ahoj</asp:Label>
```

```
<asp:Calendar id="Calendar1" runat="server" />
```

```
</form> </body> </html>
```

Ahoj

<	duben 2015							>
po	út	st	čt	pá	so	ne		
30	31	1	2	3	4	5		
6	7	8	9	10	11	12		
13	14	15	16	17	18	19		
20	21	22	23	24	25	26		
27	28	29	30	1	2	3		
4	5	6	7	8	9	10		

podívejte se do
zdrojového kódu
stránky v prohlížeči:
VIEWSTATE
posílá stav při
každém požadavku,
aby fungovalo na
bezstavovém
serveru



ASP.NET – PŘÍKLAD 3

pokus3.aspx

```
<%@ Page Language="C#" %>
<script runat="server">
void ZmenitText(object sender, System.EventArgs e)
{   Label1.Text = "Změněný text"; }
</script>
<html>
<head> <title>Demonstrace událostí</title> </head>
<body>
<form runat="server">
<asp:Label id="Label1" runat="server"
    forecolor="Blue">Ahoj</asp:Label>
<br />
<asp:Button id="Button1" runat="server" text="Změnit text"
onclick="ZmenitText" />
</form> </body> </html>
```

Ahoj

Změnit text

Změněný text

Změnit text



ODKAZ NA KONFIGURACI IIS

- <http://technet.microsoft.com/cs-cz/library/cc731196%28WS.10%29.aspx>



Z PŘÍKAZOVÉ ŘÁDKY

- `cd c:\windows\system32\inetsrv`
- příkaz **appcmd.exe**
- `.\appcmd list site`
- `appcmd stop site /site.name: "www2.pesi.local"`
- `appcmd start site /site.name: "www2.pesi.local"`

- `appcmd add site`
 `/name: pokus`
 `/id:4 /physicalPath: c:\nekde`
 `/bindings:http/*:85: nekde.pesi.local`



ZÁLOHA KONFIGURACE

záloha

- appcmd add backup
- appcmd add backup IISBackup .. pojmenovaná
 - zálohuje do: *%windir%\System32\Inetsrv\Backup*

obnova zálohy

- appcmd.exe restore backup "IISBackup"

výpis konfigurace

- appcmd.exe list config



NASTAVENÍ HTTPS

když zkusíte <https://www.pesi.local> .. nejde

potřebné kroky:

1. získat certifikát
2. vytvořit SSL binding



HTTPS – ZÍSKÁNÍ CERTIFIKÁTU

- IIS manager – jméno PC (WIN-HH..) – IIS - ikona Server certificates – create self signed certificate

friendly name: pokus

vytvoří se..

pravá myš - view



Server Certificates

Use this feature to request and manage certificates that the Web server can use with Web sites configured for SSL.

Name	Issued To	Issued By	Expiration Date	Certificate H
pokus	PesiVirt.pesipokus.czf	PesiVirt.pesipokus.czf	23.3.2012 1:00:00	05F32731C6

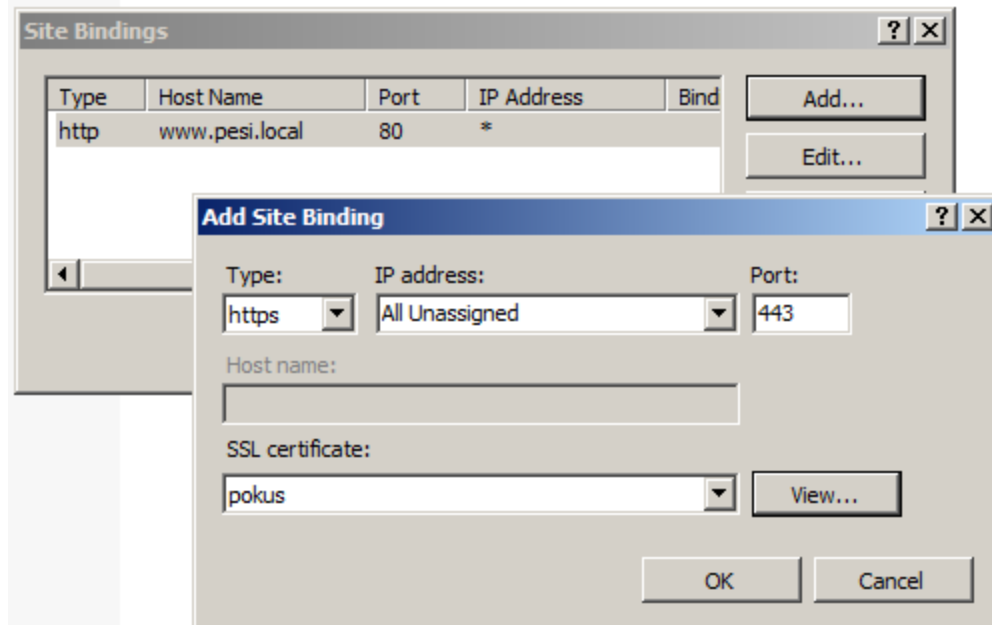
expirace



HTTPS – VYTVOŘENÍ BINDING

- IIS manager - site – www.pesi.local – pravá myš
 - bindings - add
 - https
 - all unassigned
 - port 443
 - SSL certificate: pokus

○ <https://www.pesi.local>



VISUAL STUDIO 2013 (2010)

- Visual C#, Web, ASP.NET WebApplication
- přepneme na Design
 - text
 - textbox
 - button1 (Jedna)
 - button2 (Dva)
- při stisku tlačítka nastaví
TextBox1.Text = "Zmackl jsi tlacitko JEDNA";
- vyzkoušet - Start without debugging
- Build - Publish WebApplicationXY
 - do nejakeho adresare,
 - pres sdileni pak nakopirujeme do rootu naseho
www2.pesi.local



DFS

- jednotný kořen sdílení
- Server Roles –
File and iSCSI services – DFS namespaces
- nástroj DFS Management
- New Namespace
Namespace server: jméno serveru
Shared folder: korenDFS
Local path: c:\DFSRoot\korenDFS



DFS

Edit Settings

Namespace server:

WIN-PLDRUV4SR6P

Shared folder:

korenDFS

Local path of shared folder:

C:\DFSRoots\korenDFS

Browse...

Shared folder permissions:

☐ All users have read-only permissions

☐ All users have read and write permissions

☐ Administrators have full access; other users have read-only permissions

☒ Administrators have full access; other users have read and write permissions

☐ Use custom permissions:

Customize...

Select the type of namespace to create.

☒ Domain-based namespace

A domain-based namespace is stored on a single server or multiple servers. You can increase the availability of a domain-based namespace by creating a stand-alone namespace. When created in Windows Server 2008 mode, a domain-based namespace provides increased scalability and access-based enumeration.

☒ Enable Windows Server 2008 mode

Preview of domain-based namespace:

\\pesi.local\korenDFS

☐ Stand-alone namespace

A stand-alone namespace is stored on a single server. The availability of a stand-alone namespace by default is limited to the server on which it is created.

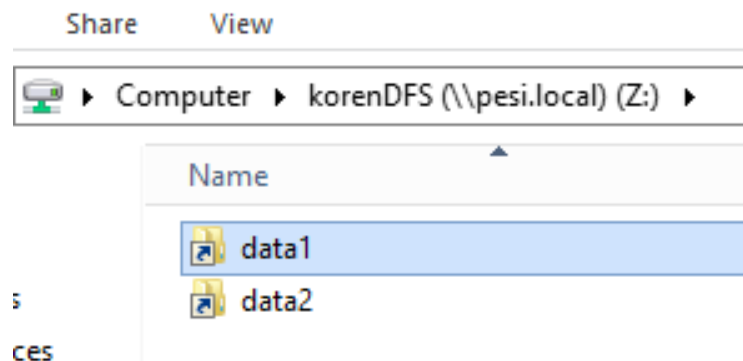
Preview of stand-alone namespace:

\\WIN-PLDRUV4SR6P\korenDFS



DFS – PŘIDAT SDÍLENÍ

- pravá myš na namespacu – Add Folder
- data1
 - add folder target - přidáme sdílení sdileni
- data2
 - add folder target - přidáme sdílení sdileni2
- namapovat síťovou jednotku
Z: *pesi.local*\korenDFS (používám už AD)



WINDOWS SERVER BACKUP

- SM – Manage - Add Roles and Features
- Features – Windows Server Backup

nástroj – Windows Server Backup

- plánované backupy
- jednorázový backup
- bare metal recovery, system state, c:, ...
- na disk dedikovaný pro backup
- na svazek
- na sdílení



ACTIVE DIRECTORY (2008)

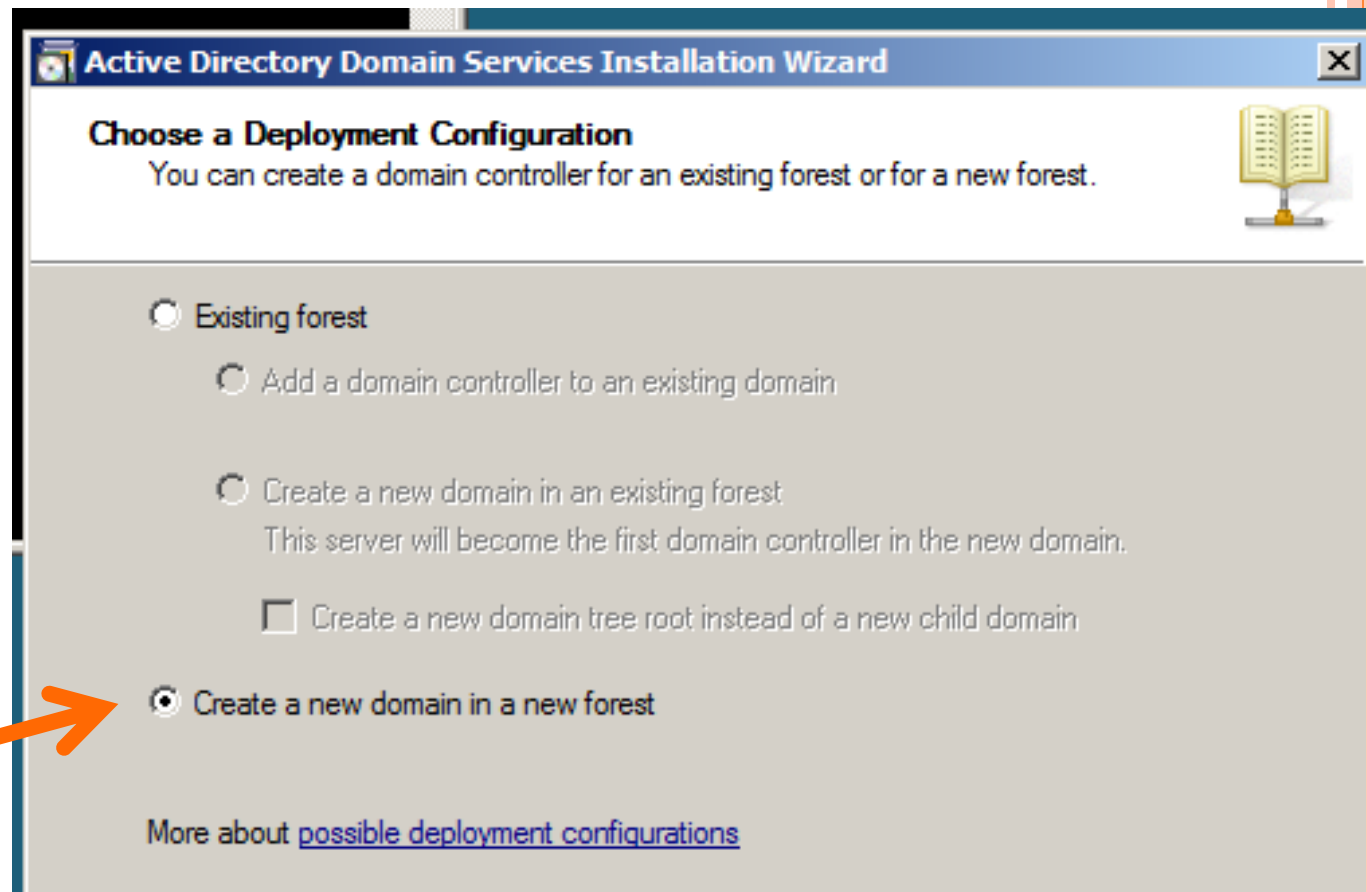
před instalací zrušíme
DNS

instalace Active Directory:
příkaz **dcpromo**

nový řadič
v doméně

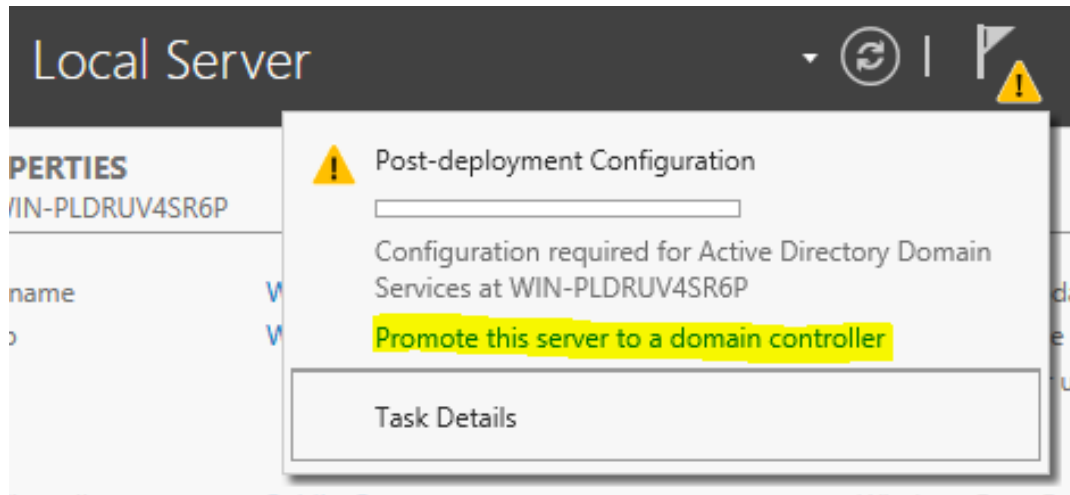
nová
doména v
existujícím
lese domén

nová
doména v
novém lese
domén



ACTIVE DIRECTORY – SERVER 2012

- Přidat roli **Active Directory Domain Services**
- vlajka → AD Domain Services Configuration Wizard



AD - KONFIGURACE

- Add a new forest
Root domain name: pesi.local
- Forest functional level: WS2012, 2008R2, 2008,...
- Domain func. level: WS2012, 2008R2, 2008,...
- DNS, Global Catalog
- DS Restore mode password: ... stejne ...
- NetBIOS domain name: PESI



AD - KONFIGURACE

Specify the location of the AD DS database, log files, and SYSVOL

Database folder:	<input type="text" value="C:\Windows\NTDS"/>	<input type="button" value="..."/>
Log files folder:	<input type="text" value="C:\Windows\NTDS"/>	<input type="button" value="..."/>
SYSVOL folder:	<input type="text" value="C:\Windows\SYSVOL"/>	<input type="button" value="..."/>

View Script – Powershellový script pro vytvoření AD



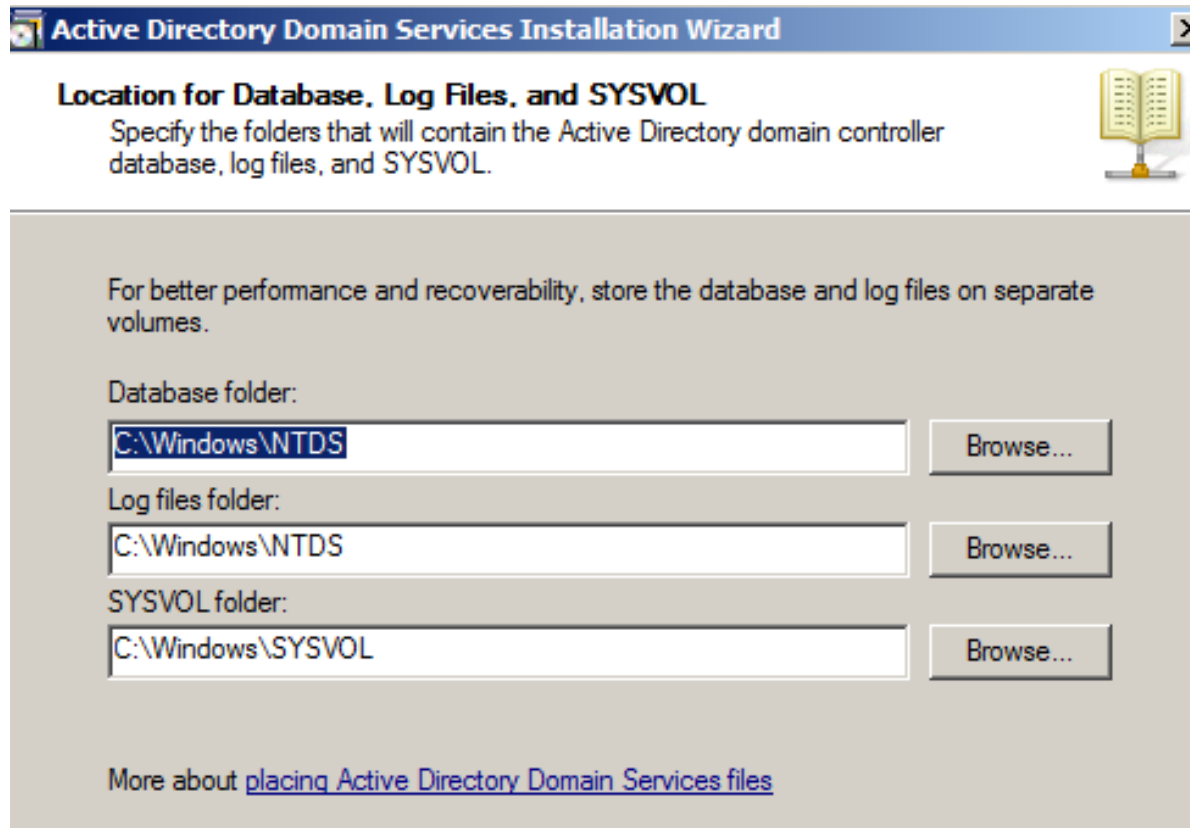
AD - INSTALACE

- plně kvalifikované jméno (FQDN) domény
pesi.local
- domain NetBIOS jméno: **PESI**
- forest functional level:
 - windows server 2003
 - windows server 2008, 2008R2
 - windows server 2012
- domain functional level:
 - windows server 2003
 - windows server 2008, ...

doménový řadič: DNS server, Global catalog



AD – INSTALACE – UMÍSTĚNÍ SOUBORŮ



The screenshot shows the 'Active Directory Domain Services Installation Wizard' window. The title bar is blue with the text 'Active Directory Domain Services Installation Wizard' and a close button. Below the title bar, the section is titled 'Location for Database, Log Files, and SYSVOL' with a small icon of an open book. The text below the title says 'Specify the folders that will contain the Active Directory domain controller database, log files, and SYSVOL.' The main area has a light gray background and contains the following text: 'For better performance and recoverability, store the database and log files on separate volumes.' Below this, there are three rows of input fields and buttons. The first row is for the 'Database folder:' with the text 'C:\Windows\NTDS' and a 'Browse...' button. The second row is for the 'Log files folder:' with the text 'C:\Windows\NTDS' and a 'Browse...' button. The third row is for the 'SYSVOL folder:' with the text 'C:\Windows\SYSVOL' and a 'Browse...' button. At the bottom, there is a link that says 'More about [placing Active Directory Domain Services files](#)'.

Active Directory Domain Services Installation Wizard

Location for Database, Log Files, and SYSVOL

Specify the folders that will contain the Active Directory domain controller database, log files, and SYSVOL.

For better performance and recoverability, store the database and log files on separate volumes.

Database folder:
C:\Windows\NTDS Browse...

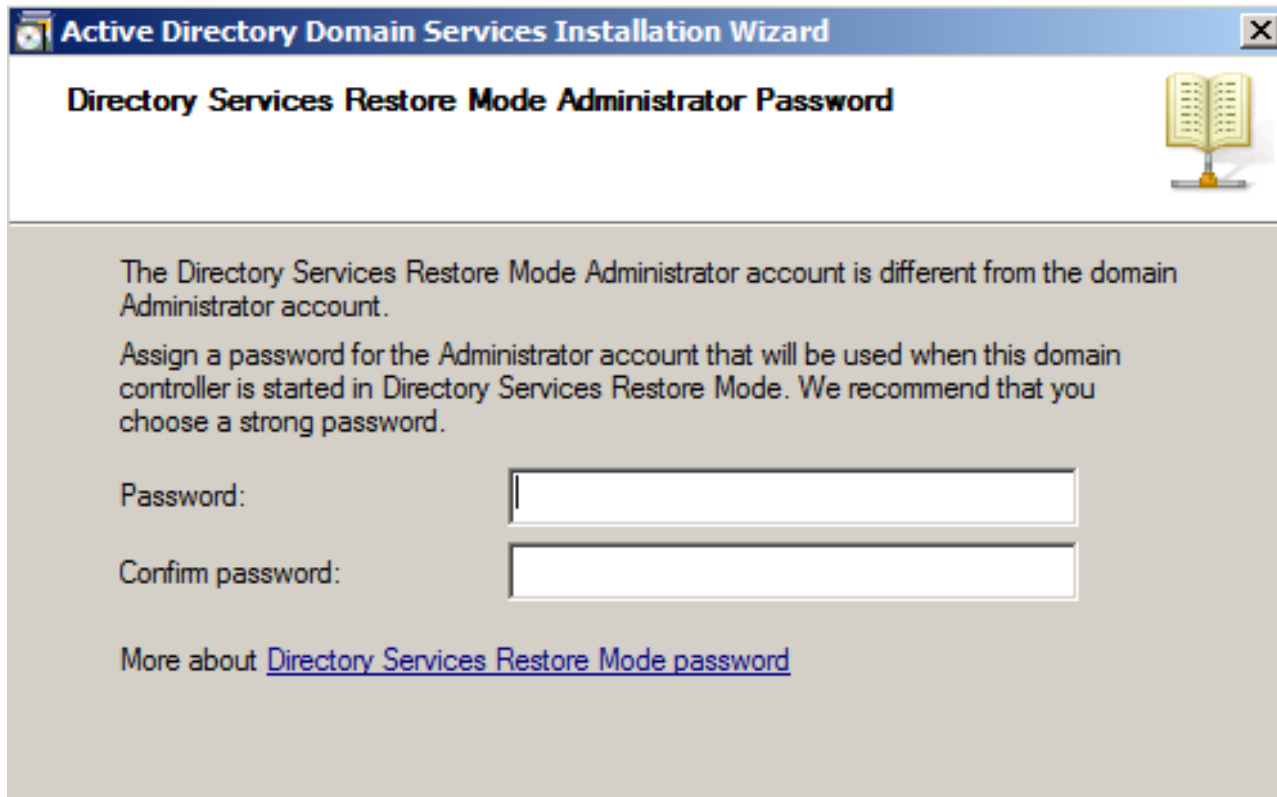
Log files folder:
C:\Windows\NTDS Browse...

SYSVOL folder:
C:\Windows\SYSVOL Browse...

More about [placing Active Directory Domain Services files](#)



AD – RESTORE MODE ADMINISTRATOR PASSWORD



The screenshot shows a Windows XP-style window titled "Active Directory Domain Services Installation Wizard". The main heading inside the window is "Directory Services Restore Mode Administrator Password". To the right of the heading is an icon of an open book. The main text area contains the following instructions:

The Directory Services Restore Mode Administrator account is different from the domain Administrator account.

Assign a password for the Administrator account that will be used when this domain controller is started in Directory Services Restore Mode. We recommend that you choose a strong password.

Below the text are two input fields:

Password:

Confirm password:

At the bottom, there is a link: [More about Directory Services Restore Mode password](#)

velmi důležité – poznamenat na bezpečné místo pro
pozdější použití



AD – KONFIGURACE

- Active Directory Users and Computers
 - vytváření uživatelů, ...
- Active Directory Sites and Services
 - zda je server global catalog
Sites – Default First Site Name – Servers – PESIVIRT –
NTDS Settings – Properties - GlobalCatalog
- Active Directory Domains and Trusts



AD – VYTVOŘENÍ UŽIVATELE

vytvoření uživatele:

- ručně
- skriptem

```
net user %1 tajneHeslo /add /fullname:%2
```

```
net group LAMA /add
```

```
net group LAMA %1 /add
```



SKRIPT NA PŘIDÁNÍ UŽIVATELE

rem Skript na pridani problemoveho uzivatele

net user %1 tajneHeslo /add /fullname:%2

 /passwordchg:no

mkdir D:\lidicky\%1

caccls D:\lidicky\%1 /e /g %1:f

mkdir D:\lidicky\%1\profile-TITANIC

net group LAMA %1 /add

/e .. Editace ACL místo nahrazení, /g f .. práva full



DALŠÍ VOLBY

další volby viz např..

<http://www.ss64.com/nt/netuseroptions.html>

- **vytvoření organizační jednotky**

nově - ochrana proti nechtěnému smazání

jak přesto smažu? menu View - Advanced Features – zrušit ochranu proti smazání

- **přidání uživatele do skupiny**

net user ufon2 – vypíše, v jakých je skupinách

net group lama – vypíše členy skupiny lama



ZJIŠTĚNÍ ROLÍ SERVERU (VIZ PŘEDNÁŠKY)

dsquery server - seznam DC serverů

dsquery server -hasfsmo schema - vypíše, kdo má roli Schema Master

dsquery server -hasfsmo name - vypíše, kdo má roli Domain Naming Master

dsquery server -hasfsmo infr - vypíše, kdo má roli Infrastructure Master

dsquery server -hasfsmo pdc - vypíše, kdo má roli PDC Emulator

dsquery server -hasfsmo rid - vypíše, kdo má roli RID Master

dsquery server -isgc - vypíše DC, které mají GC

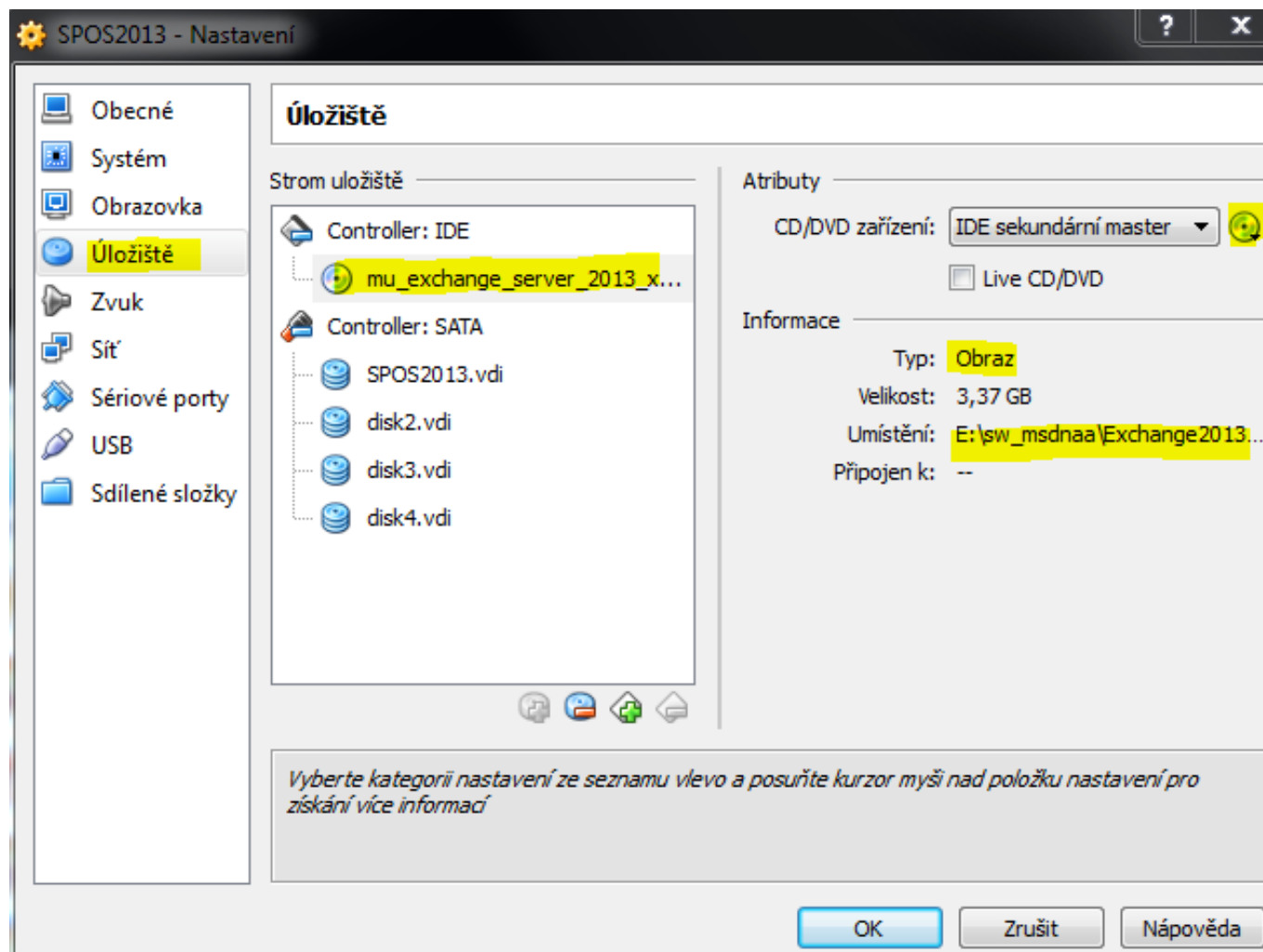


MSBA

- Microsoft Baseline Security Analyzer 2.2
- stáhnout, zkusit



PŘIPOJENÍ DVD IMAGE PRO INSTALACI SW



EXCHANGE 2013 SETUP

- setup.exe
- dotaz, zda má zkontrolovat updaty
- rozbalování souborů
- úvodní obrazovka setupu
- souhlas s licencí
- výběr
 - recommended setting (YES)
 - don't use recommended setting
- výběr rolí



VÝBĚR ROLÍ (EXCHANGE 2013)

- mailbox role
- client access role
- Win Server role and features required

MICROSOFT EXCHANGE SERVER 2013 SETUP

Server Role Selection

Select the Exchange server roles you want to install on this computer:



Mailbox role



Client Access role



Management tools



Automatically install Windows Server roles and features that are required to install Exchange Server



KONTROLA DISKOVÉHO PROSTORU

MICROSOFT EXCHANGE SERVER 2013 SETUP

Installation Space and Location

Disk space required: 7869,3 MB

Disk space available: 11966,8 MB

Specify the path for the Exchange Server installation:

C:\Program Files\Microsoft\Exchange Server\V15

browse



DALŠÍ KROKY

- Jméno organizace: PesiOrg
- Malware protection:
disable malware scanning NO
- kontrola připravenosti
 - vadí nedokončené updaty
 - stahuje Unified Comm. Managed API 4.0 Runtime



Readiness Checks

The computer will be checked to verify that Exchange is ready to be installed.

Prerequisite Analysis

100%

Warning:

Installing Exchange Server on a domain controller will elevate the permissions for Exchange Trusted Subsystem to domain administrators.

For more information, visit: [http://technet.microsoft.com/library\(EXCHG.150\)/ms.exch.setupreadiness.WarningInstallExchangeRolesOnDomainController.aspx](http://technet.microsoft.com/library(EXCHG.150)/ms.exch.setupreadiness.WarningInstallExchangeRolesOnDomainController.aspx)

Warning:

Setup will prepare the organization for Exchange 2013 by using 'Setup /PrepareAD'. No Exchange 2010 server roles have been detected in this topology. After this operation, you will not be able to install any Exchange 2010 servers.

For more information, visit: [http://technet.microsoft.com/library\(EXCHG.150\)/ms.exch.setupreadiness.NoE14ServerWarning.aspx](http://technet.microsoft.com/library(EXCHG.150)/ms.exch.setupreadiness.NoE14ServerWarning.aspx)

Warning:

This computer requires the Microsoft Office 2010 Filter Packs - Version 2.0. Please install the software from <http://go.microsoft.com/fwlink/?LinkID=191548>.

For more information, visit: [http://technet.microsoft.com/library\(EXCHG.150\)/ms.exch.setupreadiness.MSFilterPackV2NotInstalled.aspx](http://technet.microsoft.com/library(EXCHG.150)/ms.exch.setupreadiness.MSFilterPackV2NotInstalled.aspx)

Warning:

This computer requires the Microsoft Office 2010 Filter Packs - Version 2.0 - Service Pack 1. Please install the software from



DÁLE...15 KROKŮ (AUTOMATICKY)

- 1 Organization Preparation
- 3 Copy Exchange files
- 4 Language Files
- 6 Languages
- 7 Management tools
- 8 Mailbox role: Transport Service
- 9 Mailbox role: Client Access Service
- 13 Client Access Role: CA Front End Service
- 14 Finalizing Setup



EXCHANGE SERVER 2007

- připojit přes **sdílení** (např. při vypnutém virtualu)
- pro produkci 64bitová aplikace, stejně tak Exchange Server 2010
- jen pro vyzkoušení **32bitová** verze Exchange 2007
- spuštění
- extrakce souborů
- z rozbaleného adresáře spustíme **setup.exe**
- vidíme, jaké komponenty je potřeba doinstalovat
- spuštění vlastní instalace



EXCHANGE SERVER 2007



Microsoft Exchange Server enables users to send and receive e-mail, schedule meetings, receive faxes, and receive voice mail.

Microsoft
Exchange Server 2007

Plan

[Read about Microsoft Exchange Server 2007 SP3](#)

Install

Step 1: Install .NET Framework 2.0 - Installed

Step 2: Install Microsoft Management Console (MMC) - Installed

Step 3: Install Microsoft Windows PowerShell™ - Installed

Step 4: Install Microsoft Windows Installer 4.5 - Installed

Step 5: Install Microsoft Exchange Server 2007 SP3

Step 6: Get Critical Updates for Microsoft Exchange

Enhance

[Read about Microsoft Exchange Hosted Services](#)

[Read about Microsoft Forefront™ Security for Exchange Server](#)

[Install Forefront Security for Exchange Server](#)

Close





Exchange Server 2007 SP3 Setup

- ☒ Introduction
- ☒ License Agreement
- ☒ Error Reporting
- ☒ Installation Type
- ☐ Readiness Checks
- ☐ Progress
- ☐ Completion

Installation Type

Select the Exchange Server installation type:



Typical Exchange Server Installation

The following will be installed on this computer:

- Hub Transport server role
- Client Access server role
- Mailbox server role
- Exchange Management Tools



Custom Exchange Server Installation

This option lets you select which of the following server roles you want to install on this computer:

- Hub Transport
- Client Access
- Mailbox (with or without clustering)
- Unified Messaging
- Edge Transport
- Exchange Management Console

Specify the path for the Exchange Server installation:

C:\Program Files\Microsoft\Exchange Server

Browse...

Help

< Back

Next >

Cancel

TYPICKÁ INSTALACE

- typická
- **hub transport** role
- **client access server** role
- **mailbox server** role
- exchange management tools



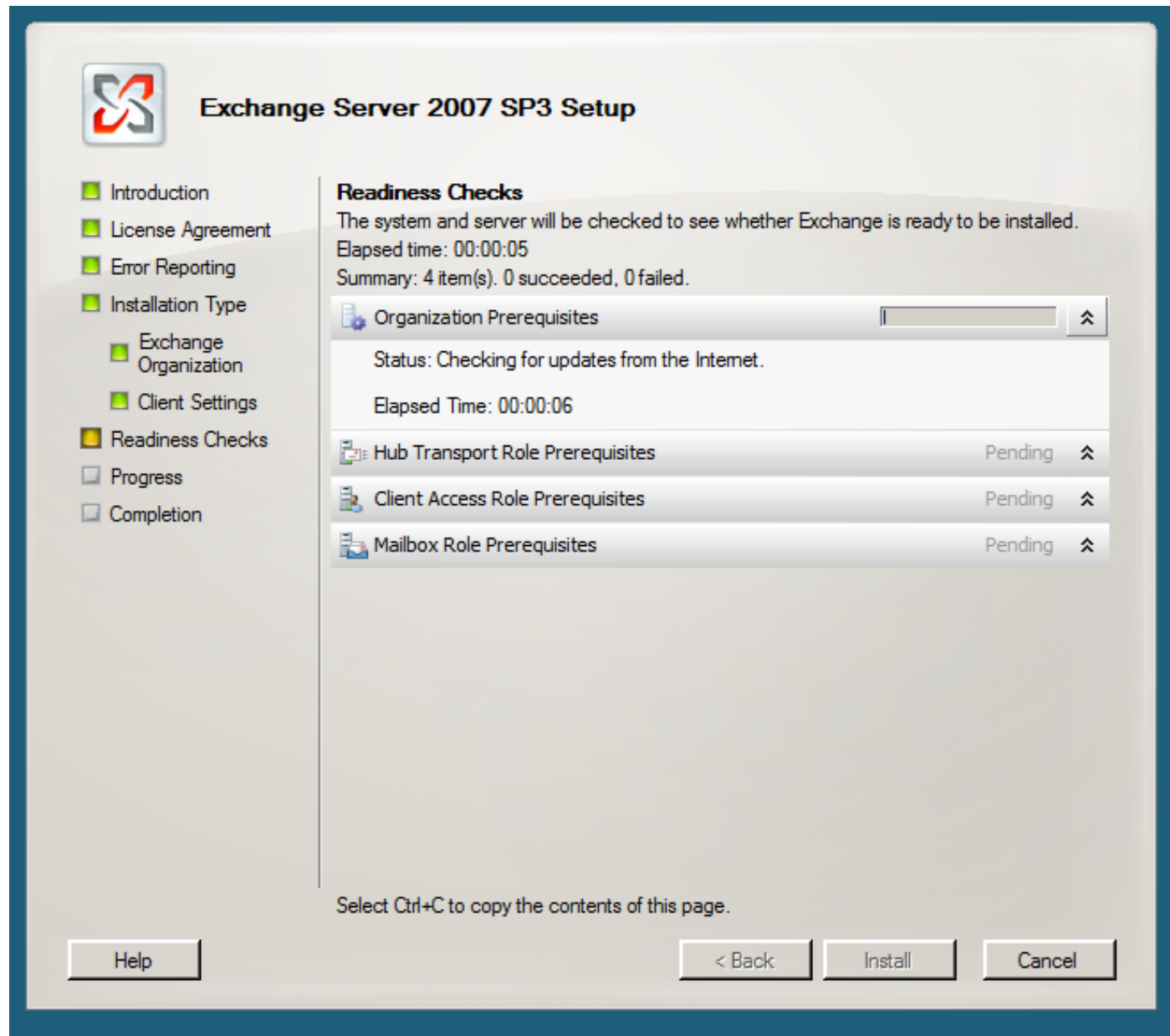
FirstOrganization: PesiOrg

Mate Outlooku 2003? NE

pokud ano, vytvoří public folder databazi pro
pripojeni k Exchange 2007



postup instalace.. kontrola splnění předpokladů



V PŘÍPADĚ PROBLÉMŮ DOINSTALOVAT KOMPONENTY...

- server manager – IIS – add role services
- management tools, security, performance
.. zaškrtnout celé podstromy
- opět instalace.. čekání..



KONFIGURACE

- Start – All Programs –>

Microsoft Exchange Server 2007 – Exchange
Management Console



PŘÍSTUP PŘES WEB

- <https://localhost/owa>

- nejlépe Internet Explorer
- dejte pozor, aby nebylo https bindování na jiný síť z předchozích experimentů s IIS, a na jaký certifikát
- administrator, klasické heslo

- pošta, kalendář, kontakty

- vyzkoušejte

- poslat e-mail sám sobě
- přidat událost do kalendáře



PŘIDÁNÍ UŽIVATELE KARKULKA

○ **AD Users and Computers**

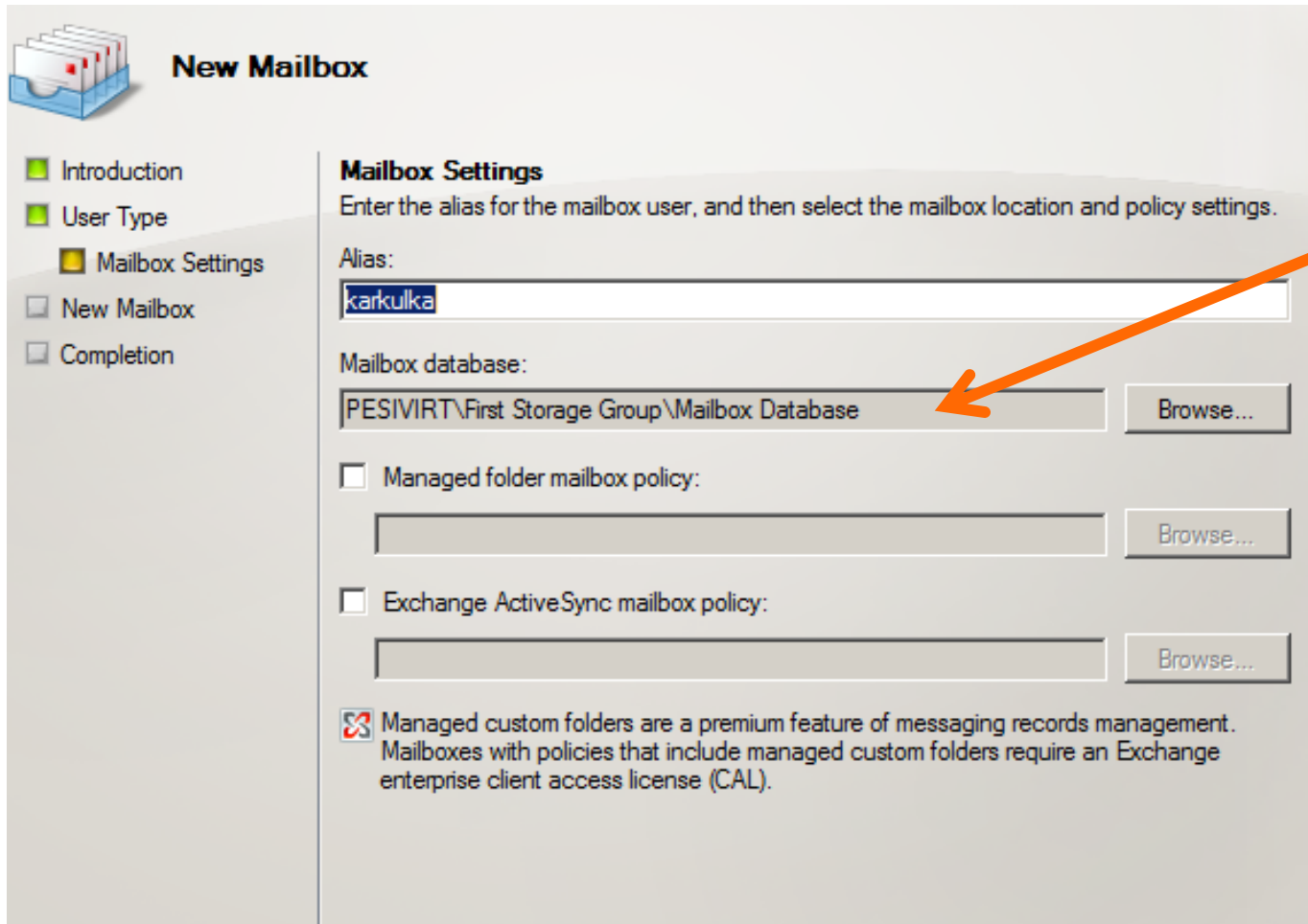
- Cervená Karkulka, karkulka
- karkulka@pesi.local
- heslo: cepec.2012
- v záložce general přidáme: karkulka@pesi.local

○ **exchange management console**

- recipient configuration
- mailbox - new mailbox - user mailbox
- (vsimnete si typu: user, room, equipment, linked)
- přidat existujícího uživatele



JE TŘEBA ZVOLIT I MAILBOX DATABASE



New Mailbox

Introduction
User Type
Mailbox Settings
New Mailbox
Completion


Mailbox Settings
Enter the alias for the mailbox user, and then select the mailbox location and policy settings.

Alias:
karkulka

Mailbox database:
PESIVIRT\First Storage Group\Mailbox Database **←** Browse...

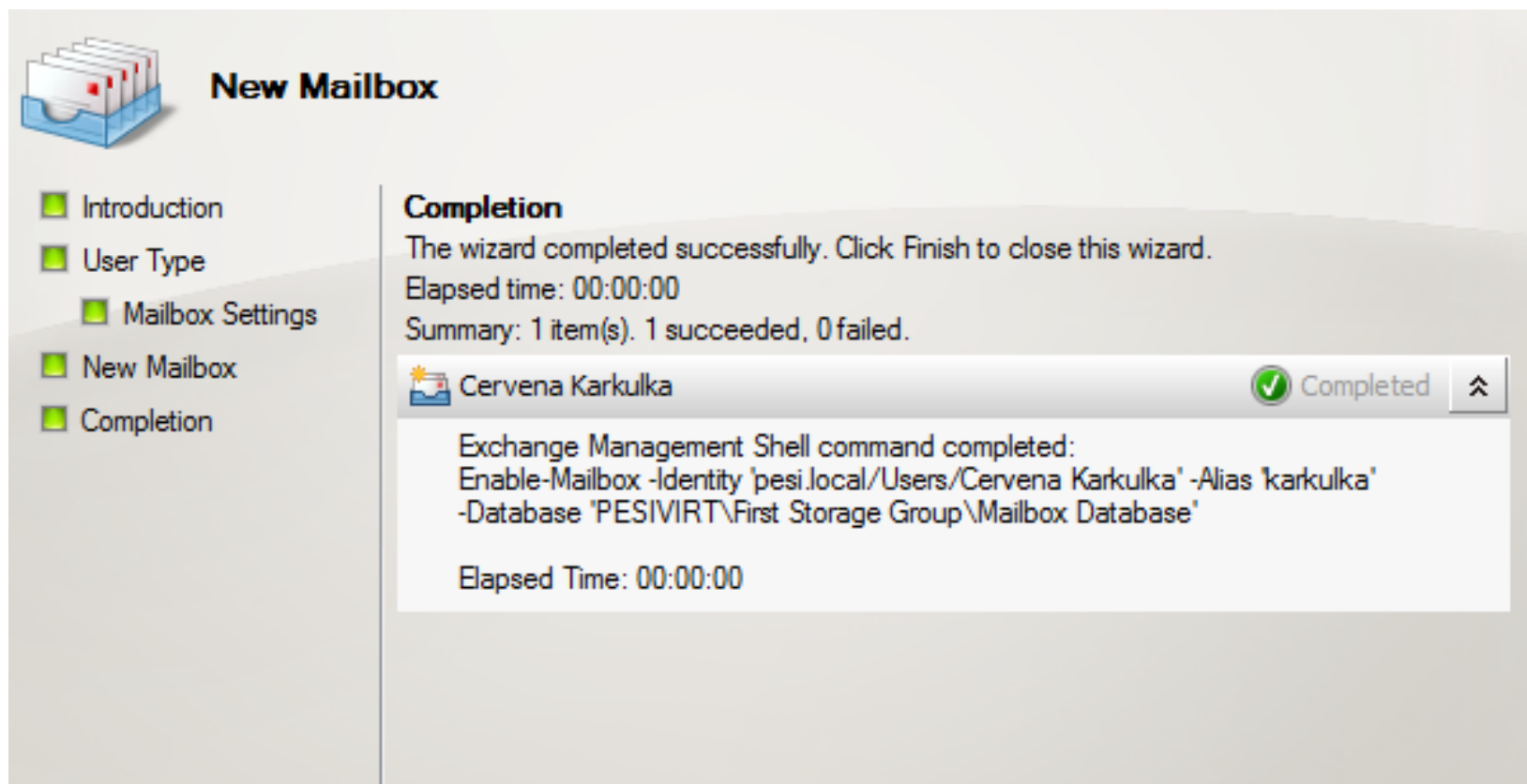
☐ Managed folder mailbox policy:
Browse...

☐ Exchange ActiveSync mailbox policy:
Browse...

 Managed custom folders are a premium feature of messaging records management. Mailboxes with policies that include managed custom folders require an Exchange enterprise client access license (CAL).



ZOBRAZÍ PŘÍKAZ, KTERÝ PROVÁDÍ



POKUS

- přihlásit se jako administrator do OWA
- poslat e-mail karkulce
- přihlásit se jako karkulka a zkontrolovat mail
- vytvořit distribuční skupinu pohádkové postavy, jejíž součástí bude karkulka
- využít distribuční skupinu pro posílání e-mailu



SLUŽBA IMAP4

- server manager – configuration – services
- Microsoft Exchange IMAP4
 - zastavená / spuštěná
 - typ spuštění (manual, ...)
- Microsoft Exchange POP3
 - analogicky
 - preferovanější je IMAP4
- spuštění z řádky:
`net start MSExchangeIMAP4`



TEST PROGRAMEM PUTTY

- stáhnout putty
- telnet localhost **143**
 - * OK The Microsoft Exchange IMAP4 service is ready.
- telnet localhost **25**
 - 220 Pesivirt.pesi.local Microsoft ESMTP MAIL Service ready at Wed, 13 Apr 2011 09:30:42 +0200



POŠTOVNÍ KLIENT THUNDERBIRD (IMAP4)

Založení poštovního účtu

Vaše jméno: Cervena Karkulka Vaše jméno tak, jak se bude zobrazovat ostatním.
E-mail: karkulka@pesi.local
Heslo: ●●●●●●●●
☒ Zapamatovat si heslo [Začít znovu](#)

Testováním obvyklých jmen serverů bylo nalezeno následující nastavení

Uživatelské jméno karkulka [Upravit](#)

	Příchozí	pesi.local	IMAP	143	STARTTLS
	Odchozí	pesi.local	SMTP	587	STARTTLS

[Ruční nastavení...](#) [Zrušit](#) [Vytvořit účet](#)

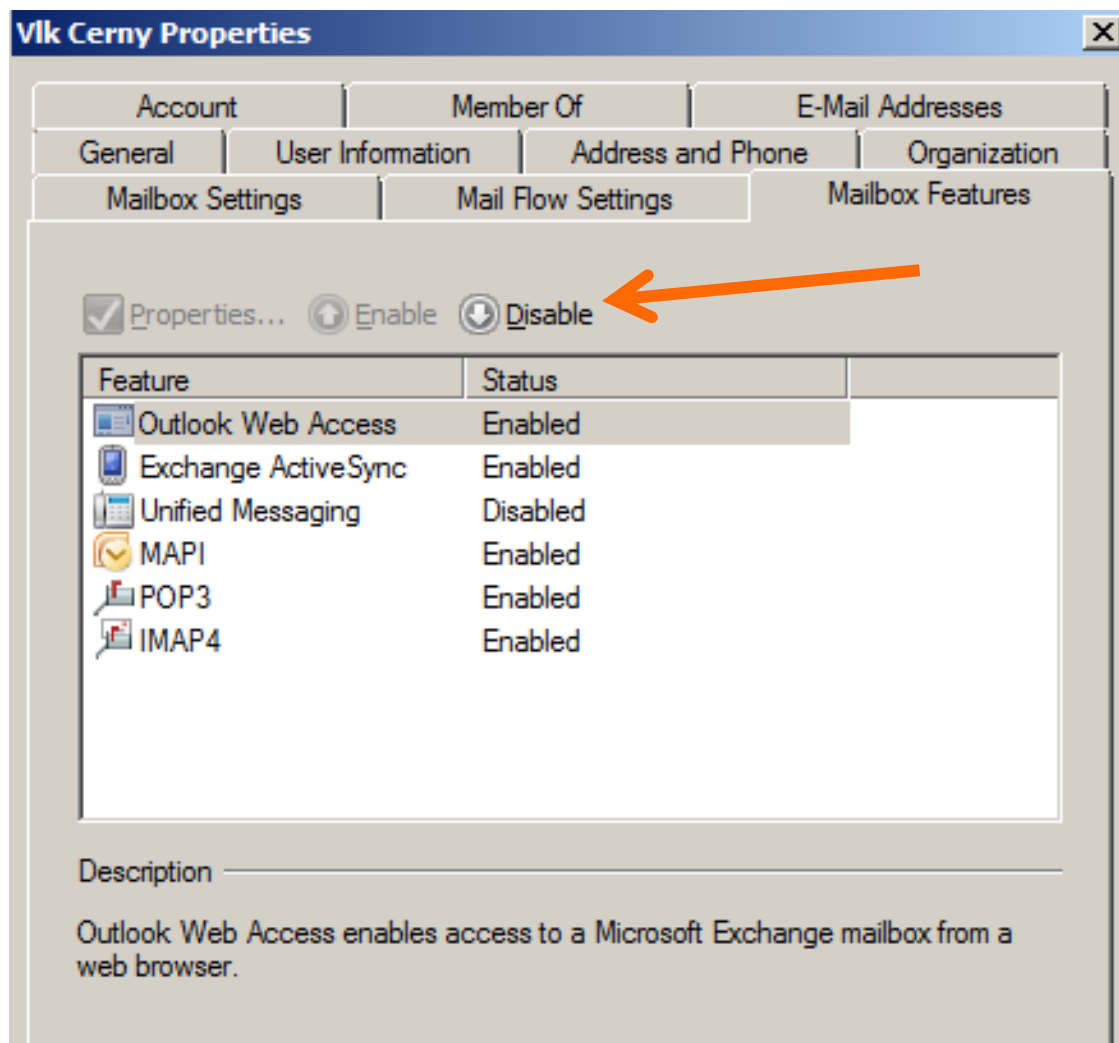
VYTVOŘENÍ UŽIVATELE PŘÍMO Z EXCHANGE MANAGEMENT CONSOLE

- abychom nemuseli vytvářet zvlášť účet a mailbox
- **Exchange management console**
 - recipient configuration – mailbox – pravá myš – new mailbox
 - user mailbox – new user
 - vlk@pesi.local, cepec.2012, Vlk Cerny

```
New-Mailbox -Name 'Vlk Cerny' -Alias 'vlk' -  
OrganizationalUnit 'pesi.local/Users' -UserPrincipalName  
'vlk@pesi.local' -SamAccountName 'vlk' -FirstName 'Vlk' -  
Initials '' -LastName 'Cerny' -Password  
'System.Security.SecureString' -ResetPasswordOnNextLogon  
$false -Database 'PESIVIRT\First Storage Group\Mailbox  
Database'
```



VLASTNOSTI KONTA



můžeme pro daného uživatele (vlk) zakázat např. OWA

- přes web

MAPI

- velký Outlook

zakažte
uživateli vlk
přístup přes
OWA

ZAKÁZANÝ PŘÍSTUP PŘES OWA



Aplikace Microsoft Outlook Web Access je nyní pro uživatele PESI\vlk zakázána.
Klepnutím sem pokračujte v práci.

Request

Url: `https://localhost:443/owa/auth/error.aspx`

User host address: `::1`

User: `Vlk Cerny`

EX Address: `/o=PesiOrg/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=vlk`

SMTP Address: `vlk@pesi.local`

OWA version: `8.3.83.4`

Mailbox server: `PesiVirt.pesi.local`



NASTAVIT, ABY KAŽDÝ MAIL PRO UŽIVATELE VLK BYL FORWARDOVÁN I KARKULCE

The screenshot shows the 'Vlk Cerny Properties' dialog box with the 'Delivery Options' tab selected. The 'Mailbox Settings' sub-tab is active, showing a tree view with 'Delivery Options' selected. The 'Forwarding address' field is set to 'Cervena Karkulka', and the 'Forward to:' checkbox is checked. The 'Deliver message to both forwarding address and mailbox' checkbox is also checked. The 'Description' field contains the text: 'Delivery options control delegated permissions and forwarding.'

Vlk Cerny Properties

Account | Member Of | E-Mail Addresses

General | User Information | Address and Phone | Organization

Mailbox Settings | Mail Flow Settings | Mailbox Features

☒ Properties...

- Delivery Options
- Message Size Restrictions
- Message Delivery Restrictions

Description

Delivery options control delegated permissions and forwarding.

Delivery Options

Send on behalf

Grant this permission to:

+ Add... X

Forwarding address

☒ Forward to:

Cervena Karkulka

☒ Deliver message to both forwarding address and mailbox

VYTVOŘIT POŠTOVNÍ SCHRÁNKY MÍSTNOSTI, ZAŘÍZENÍ

- recipients – new mailbox – **room mailbox**
 - ul402, cepec.2012
 - ul402@pesi.local
- recipients – new mailbox – **equipment mailbox**
 - datak, cepec.2012

odstraníme přesměrování
vlk svolá schůzku, kam pozve karkulku, administradora,
ul402 a datak na určitý čas



SMTP KONEKTOR

- Organization Configuration – Hub transport
 - new send connectors
 - name: muj send connector
 - typ: internet
 - address space: SMTP, zcu.cz, include all subdom., 1
 - use DNS MX record to route mail automatically
 - source server: PESIVIRT

zapneme logovani

C:\Program Files\Microsoft\Exchange
Server\TransportRoles\Logs\ProtocolLog\SmtpSend



UKÁZKA Z LOGU

```
nt,remote-endpoint,event,data,context
.57.19:25,*,,attempting to connect
64.146:15434,147.228.57.19:25,+,
64.146:15434,147.228.57.19:25,<,220 fred.zcu.cz ESMTP Postfix (Debian/GNU),
64.146:15434,147.228.57.19:25,>,EHLO spos.pokus,
64.146:15434,147.228.57.19:25,<,250-fred.zcu.cz,
64.146:15434,147.228.57.19:25,<,250-PIPELINING,
64.146:15434,147.228.57.19:25,<,250-SIZE 25000000,
64.146:15434,147.228.57.19:25,<,250-VRFY,
64.146:15434,147.228.57.19:25,<,250-ETRN,
64.146:15434,147.228.57.19:25,<,250-STARTTLS,
64.146:15434,147.228.57.19:25,<,250-AUTH GSSAPI LOGIN PLAIN,
64.146:15434,147.228.57.19:25,<,250-AUTH=GSSAPI LOGIN PLAIN,
64.146:15434,147.228.57.19:25,<,250-ENHANCEDSTATUSCODES,
64.146:15434,147.228.57.19:25,<,250-8BITMIME,
64.146:15434,147.228.57.19:25,<,250 DSN,
64.146:15434,147.228.57.19:25,>,STARTTLS,
64.146:15434,147.228.57.19:25,<,220 2.0.0 Ready to start TLS,
64.146:15434,147.228.57.19:25,*,,Received certificate
64.146:15434,147.228.57.19:25,*,BB7E93DFA487BDC9C2D48A8EBFCDC198C9EBCA63,Certificate thumbprint
64.146:15434,147.228.57.19:25,>,EHLO spos.pokus,
64.146:15434,147.228.57.19:25,<,250-fred.zcu.cz,
64.146:15434,147.228.57.19:25,<,250-PIPELINING,
64.146:15434,147.228.57.19:25,<,250-SIZE 25000000,
64.146:15434,147.228.57.19:25,<,250-VRFY,
64.146:15434,147.228.57.19:25,<,250-ETRN,
64.146:15434,147.228.57.19:25,<,250-AUTH GSSAPI LOGIN PLAIN,
64.146:15434,147.228.57.19:25,<,250-AUTH=GSSAPI LOGIN PLAIN,
64.146:15434,147.228.57.19:25,<,250-ENHANCEDSTATUSCODES,
64.146:15434,147.228.57.19:25,<,250-8BITMIME,
64.146:15434,147.228.57.19:25,<,250 DSN,
64.146:15434,147.228.57.19:25,*,24,sending message
64.146:15434,147.228.57.19:25,>,MAIL FROM:<karkulka@pesi.local> SIZE=1067 BODY=7BIT,
64.146:15434,147.228.57.19:25,>,RCPT TO:<pesicka@kiv.zcu.cz>,
64.146:15434,147.228.57.19:25,<,250 2.1.0 ok,
64.146:15434,147.228.57.19:25,<,450 4.1.8 <karkulka@pesi.local>: Sender address rejected: Domain not found
64.146:15434,147.228.57.19:25,>,QUIT,
64.146:15434,147.228.57.19:25,<,221 2.0.0 Bye,
64.146:15434,147.228.57.19:25,-,,Local
.57.19:25,*,,attempting to connect
```

