



KIV/SPOS 7.4.2015

L. Pešička

WINDOWS PLATFORMA

OBSAH PRVNÍ ČÁSTI

- role serveru
- core server
- server manager

TYPICKÁ KONFIGURACE FIRMY

○ **klientské stanice**

- Windows 7/8.1/10
- Windows XP – konec podpory 8.4.2014

○ **server**

- Linux: Samba pro sdílení souborů
(navíc i tiskové služby, doménový řadič)
- Windows Server 2012R2
 - Small Business Server => Essential

FUNKCIONALITA SERVERU

- typická role serveru:
 - sdílení souborů
 - správa uživatelů (ActiveDirectory)
 - Webový server (IIS)
 - DNS
 - DHCP
- dnes i integrace cloudových služeb
- licencování
 - licence na server
 - licence na pracovní stanice,
 - přístup pracovní stanice na server CAL
 - Exchange CAL, Outlook, ...

WINDOWS SERVERY – PŘEHLED

- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008
- Windows Server 2003

- Small Business Server 2011
- Windows Server 2012 R2 Essentials
(25uživ/50 zař.)

EDICE SERVERU 2012 (R2)

○ **Foundation**

- server s max. 1 CPU
- OEM licence, uživatelé nemusí mít CAL
- max. 15 účtů

○ **Essentials**

- odpovídá dřívějšímu Small Business Serveru
- max. 2 procesory, max. 25 uživatelských účtů
- OEM, krabice, multilicence

○ **Standard, Datacenter**

- rozdíl jen v licenčních právech
- Standard – 2 virtuální prostředí,
Datacenter – neomezena

zdroj: <http://www.zive.cz/clanky/windows-server-2012-dalsi-licence-uplne-jinak/sc-3-a-165747/default.aspx>

CENY MS WINDOWS SERVER 2012

Orientační přehled:

- **Foundation Edition** - pouze OEM
- **Essentials Edition** - 450 €
- **Standard Edition** - 940 €
- **Datacenter Edition** - 5145 €

Zdroj:

<http://www.bajty.info/2012/08/ms-windows-server-2012-edice.html>

LICENCOVÁNÍ

Licence Standard a Datacenter zahrnuje až **2 fyzické procesory** na jednom serveru.

Minimální počet licencí požadovaný pro každý server – podle počtu fyzických procesorů.

- **Foundation Edition** - server limit 15 uživatelů s 1 procesorem, není třeba CAL
- **Essentials Edition** - server limit 25 uživatelů, se 2 procesory, není třeba CAL
- **Standard Edition** - procesor + CAL
- **Datacenter Edition** - procesor + CAL

NOVINKY SERVER 2012 R2

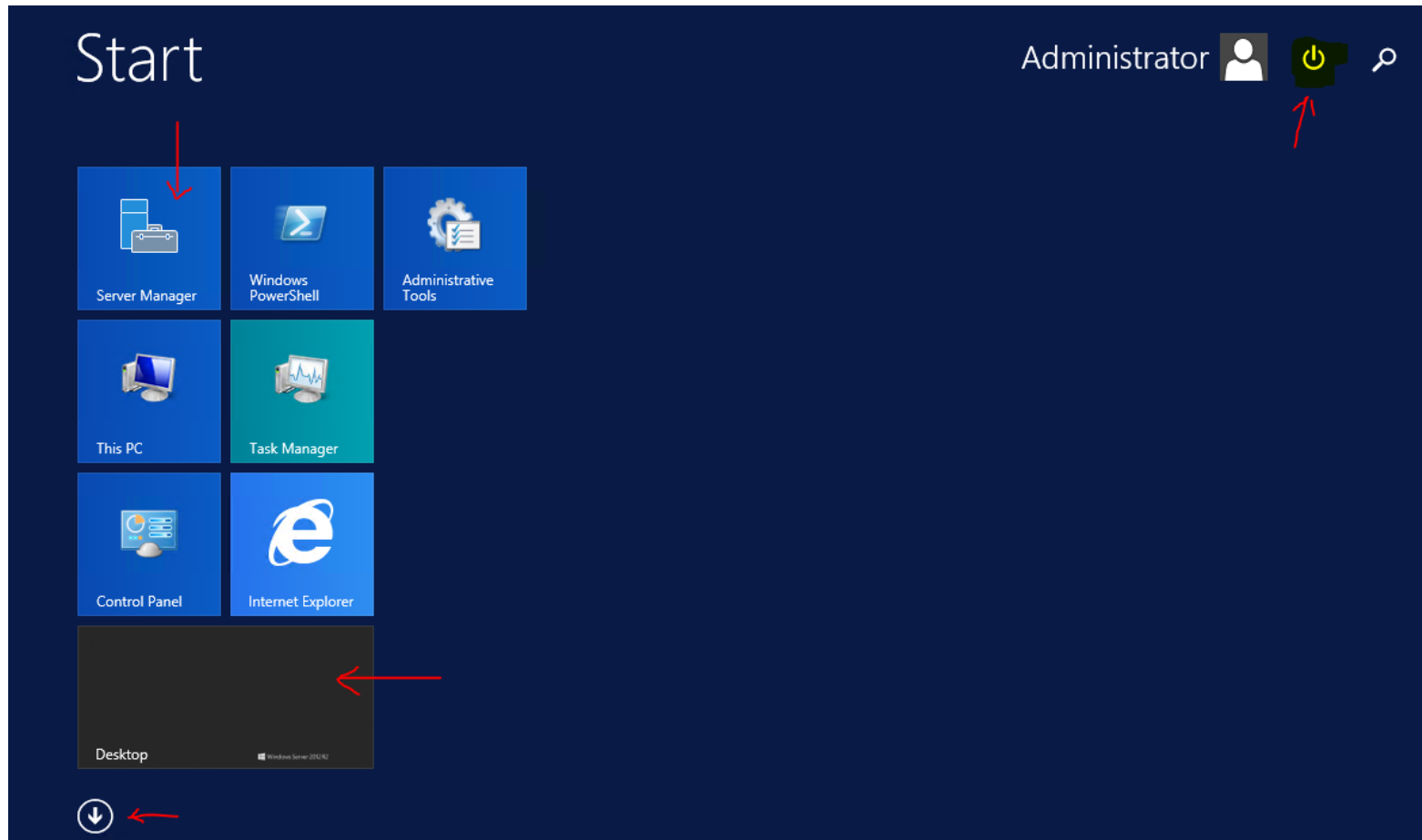
- automatická aktivace virtuálních serverů
 - pokud jsou opět Server 2012R2
- sdílený virtuální pevný disk
 - .vhdx disk zpřístupnit více strojům
- klonování virtuálních strojů za běhu
 - klon bez přerušení činnosti
- storage QoS
 - dříve už byla síťová propustnost (min, max)
 - propustnost vůči diskovému systému IOPS
- emulace rozhraní UEFI
 - použití SecureBootu

NOVINKY SERVER 2012 R2

- komprese živých migrací
 - bez přerušení činnosti šlo už dříve
 - nově komprimace při přenosu – cca polovina času
- dynamická změna velikosti virt. pevného disku
 - bez nutnosti vypnutí stroje
- storage tiering
 - mix pevných disků a SSD, automaticky rozpozná a vhodně využije

<http://www.daquas.cz/articles/621-windows-server-2012-r2-co-je-noveho>

WINDOWS SERVER 2012 R2



ROLE SERVERU

- povolujeme jednotlivé činnosti, které bude server umět
- snižuje riziko bezpečnostních chyb – nepoužívané funkce nejsou dostupné
- <http://technet.microsoft.com/en-us/library/hh831669.aspx>

přidání role

- nástroj Server Manager
- přes Windows PowerShell



Add Roles and Features Wizard



Select server roles

DESTINATION SERVER
afrodita

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

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

Roles

- ☐ Active Directory Certificate Services
- ☐ Active Directory Domain Services
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Application Server
- ☐ DHCP Server
- ☐ **DNS Server**
- ☐ Fax Server
- ▶ ☒ File and Storage Services (1 of 12 installed)
- ☐ Hyper-V
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Access
- ☐ Remote Desktop Services

Description

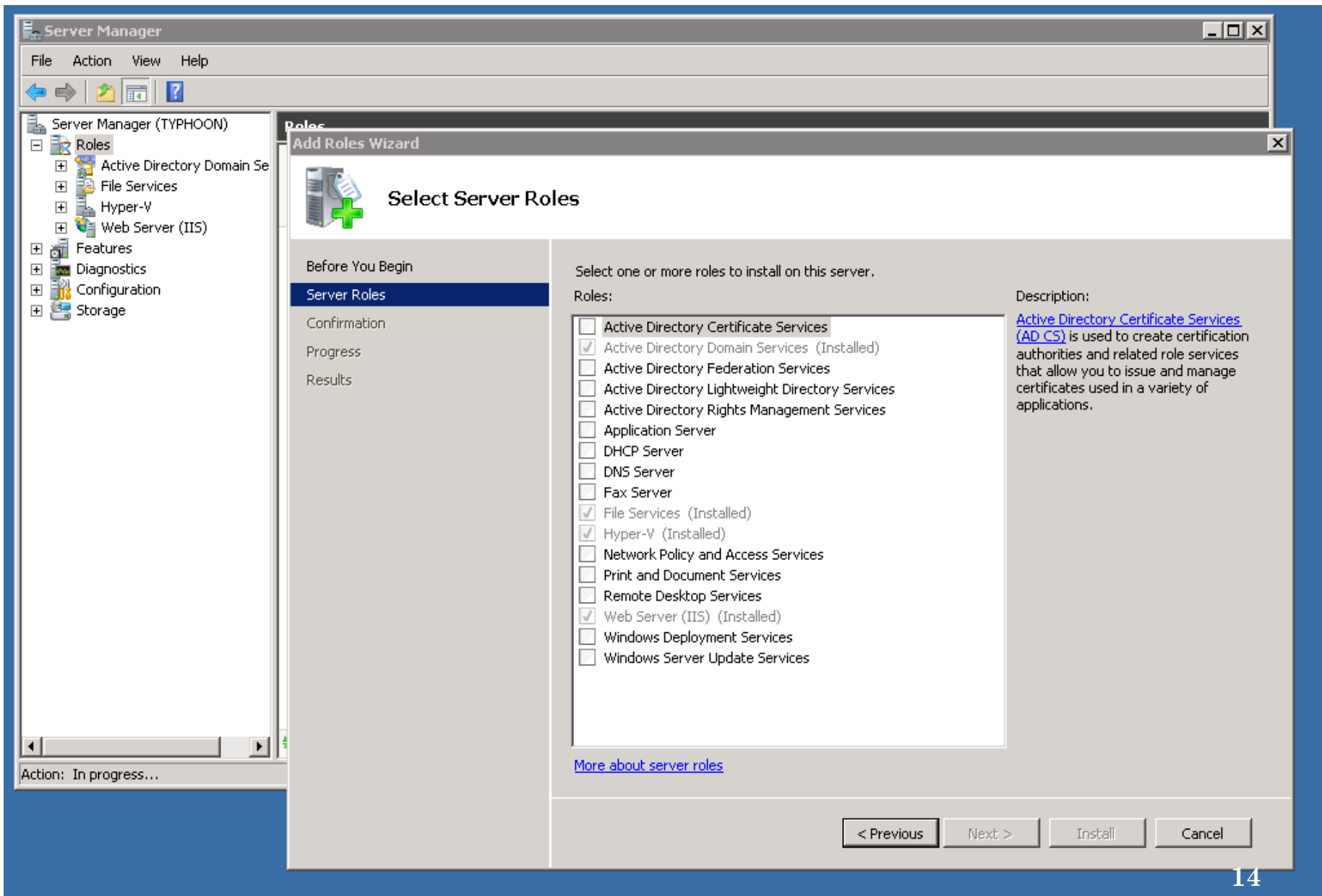
Domain Name System (DNS) Server provides name resolution for TCP/IP networks. DNS Server is easier to manage when it is installed on the same server as Active Directory Domain Services. If you select the Active Directory Domain Services role, you can install and configure DNS Server and Active Directory Domain Services to work together.

< Previous

Next >

Install

Cancel



VÝZNAM ROLÍ PRO BEZPEČNOST

- Bezpečnost řešena na mnoha vrstvách IS
- Analogie sportovní disciplíny skok do výšky
 - Každé bezpečnostní opatření o kus zvýší laťku
 - Snižuje pravděpodobnost, že ji někdo přeskočí
- **Instalovat** a **spouštět** pouze ty služby, které jsou opravdu potřeba
 - Core server
 - Instalace rolí a komponent serveru (viz cvičení – DNS, IIS)

ROLE SERVERU (WINDOWS SERVER 2012R2)

○ ActiveDirectory

- AD certificate services {certifikáty}
- **AD domain services** {ActiveDirectory}
- AD federation services {federace identit, SSO}
- AD lightweight directory services
{pro directory-based aplikace, nemusí být na DC}
- AD rights management services
{ochrana dokumentů před neoprávněným přístupem}

○ Aplikační server

○ DHCP server

○ DNS server

ROLE SERVERU - POKRAČOVÁNÍ

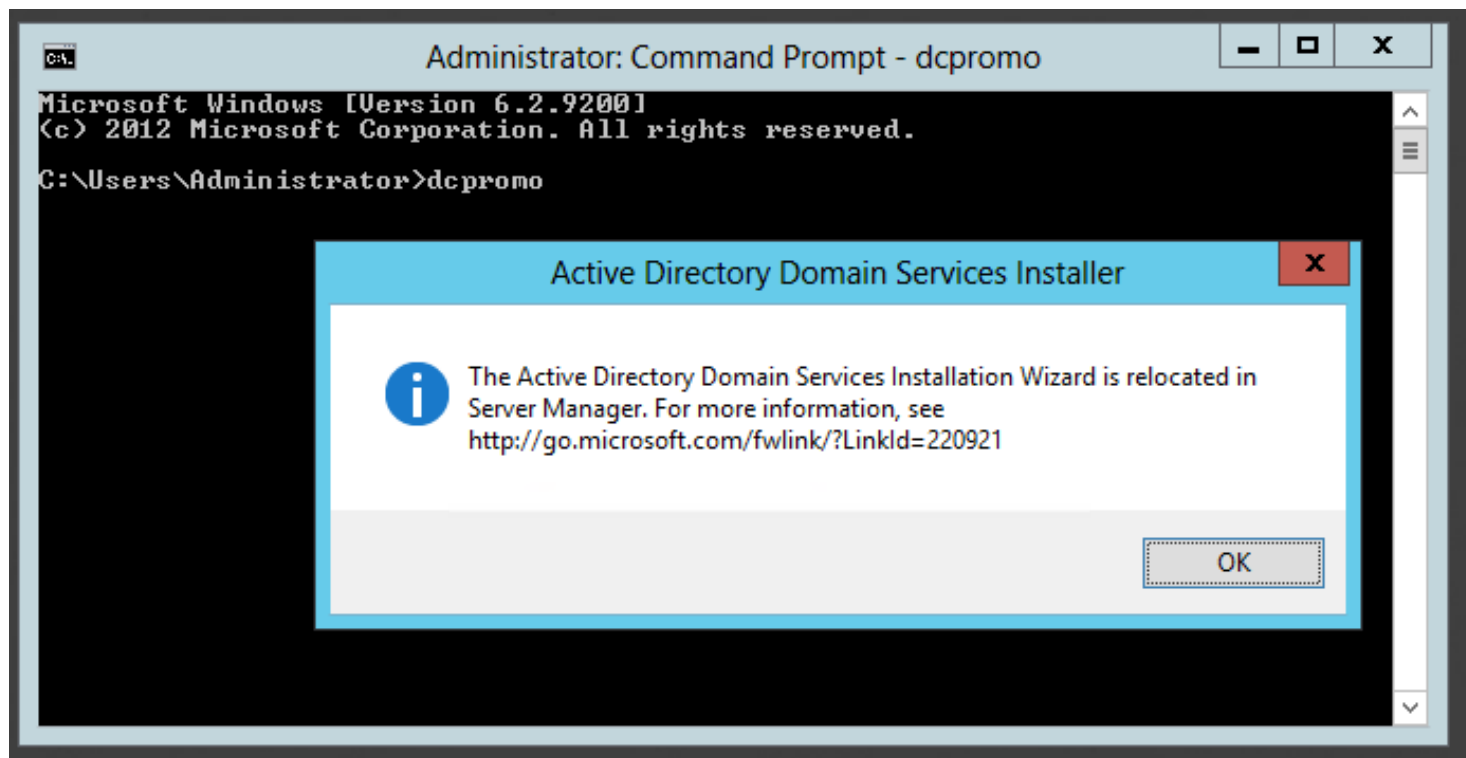
- Fax server
- File and Storage services
- Hyper-V {virtualizace}
- Network Policy and Access Server
- Print and Document Services
- Remote Access
- Remote desktop services {RD session host}
- Volume Activation services
- Web Server (IIS)
- Windows Deployment Services
- Windows Server Essential Experience
- Windows Server Update Services

ROLE – AD CERTIFICATE SERVICES

- vydávání certifikátů
- Enterprise CA
 - využívá Active Directory
 - automatické vydávání
- Stand-alone CA
 - manuální vydávání <https://server/certsrv>
 - lze instalovat na standalone server
- Root CA
 - podepisuje vlastní certifikát během instalace
 - vydává certifikáty Subordinate CA uzlům
- Subordinate CA
 - vydává certifikáty uživatelům, počítačům, službám

ROLE – AD DOMAIN SERVICES

- od serveru 2012 není příkaz **dcpromo**
- to, co běžně využijeme pro AD správu uživatelů



ROLE – AD FEDERATION SERVICES

- řešení přístupu k identitám
- SSO (single sign on)
- uživatelské účty a aplikace v rozdílných sítích nebo organizacích
- každá organizace spravuje vlastní identity
- akceptace identit z jiných organizací
- proces ověřování v jedné síti během přístupu k prostředkům v jiné síti (bez nutnosti opakovaného přihlášení uživatele)

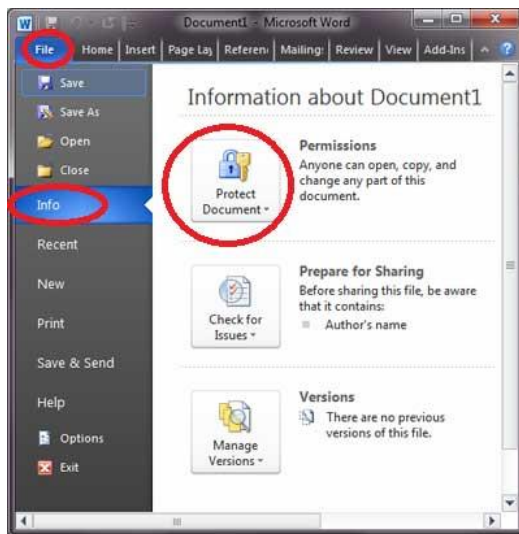
(zdroj: Technet)

ROLE – AD LIGHTWEIGHT DIRECTORY SERVICES

- adresářová služba
- využívá protokol LDAP
- lze na členských i samostatných serverech
- více instancí na 1 serveru, každá vlastní schéma
- podobné služby jako AD
- nevyžaduje nasazení domén ani řadičů domén
- dříve označení ADAM (AD Application Mode)

ROLE – AD RIGHTS MANAGEMENT SERVICES

- ochrana dokumentů
kdo může otevřít, měnit, tisknout dokument
- Použití např.
<http://www.ancsite.com/restrict-access-documents-information-rights-management-service>



Chráněný dokument můžete odeslat vně organizace, ale příjemci bude k ničemu

ROLE – APLIKAČNÍ SERVER

- pro běh podnikových aplikací
 - centrální správa a hostování aplikací
 - vývojář aplikace řekne, že bude danou roli potřebovat na server nainstalovat
-
- IIS, .NET FW, ASP.NET, COM+
 - služba řízení front zpráv
 - webové služby WCF (Windows Communication Foundation)

DALŠÍ ROLE

- DHCP server
- DNS server
- Fax server

ROLE - FILE AND STORAGE SERVICES

- File Server
- Data Deduplication
 - 1 kopie identických dat na svazku
- DFS Namespaces
 - Sdílení z více serverů do jednotného logického prostoru
- iSCSI Target Server
- Server for NFS
- Work folders
 - Podobné jako „onedrive“ pro pracovní data
 - Synchronizace na další mobilní zařízení uživatele (např. iPad)

ROLE – HYPER-V

- vytváření a správa virtuálních strojů a jejich zdrojů
- běh více systémů současně

Add Roles and Features Wizard

Create Virtual Switches

DESTINATION SERVER
andromeda

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Hyper-V
Virtual Switches
Migration
Default Stores
Confirmation
Results

Virtual machines require virtual switches to communicate with other computers. After you install this role, you can create virtual machines and attach them to a virtual switch.


One virtual switch will be created for each network adapter you select. We recommend that you create at least one virtual switch now to provide virtual machines with connectivity to a physical network. You can add, remove, and modify your virtual switches later by using the Virtual Switch Manager.

Network adapters:

Name	Description
<input type="checkbox"/> NIC2	Broadcom NetXtreme Gigabit Ethernet
<input type="checkbox"/> NIC1	Broadcom NetXtreme Gigabit Ethernet

We recommend that you reserve one network adapter for remote access to this server. To reserve a network adapter, do not select it for use with a virtual switch.

POKRAČOVÁNÍ HYPER-V

Add Roles and Features Wizard— □ ×

Virtual Machine Migration

DESTINATION SERVER
andromeda

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Hyper-V

Virtual Switches

Migration

Default Stores

Confirmation

Results

Hyper-V can be configured to **send and receive live migrations** of virtual machines on this server. Configuring Hyper-V now **enables any available network** on this server to be used for live migrations. If you want to **dedicate specific networks for live migration**, use Hyper-V settings after you install the role.


☐ Allow this server to send and receive live migrations of virtual machines

Authentication protocol —

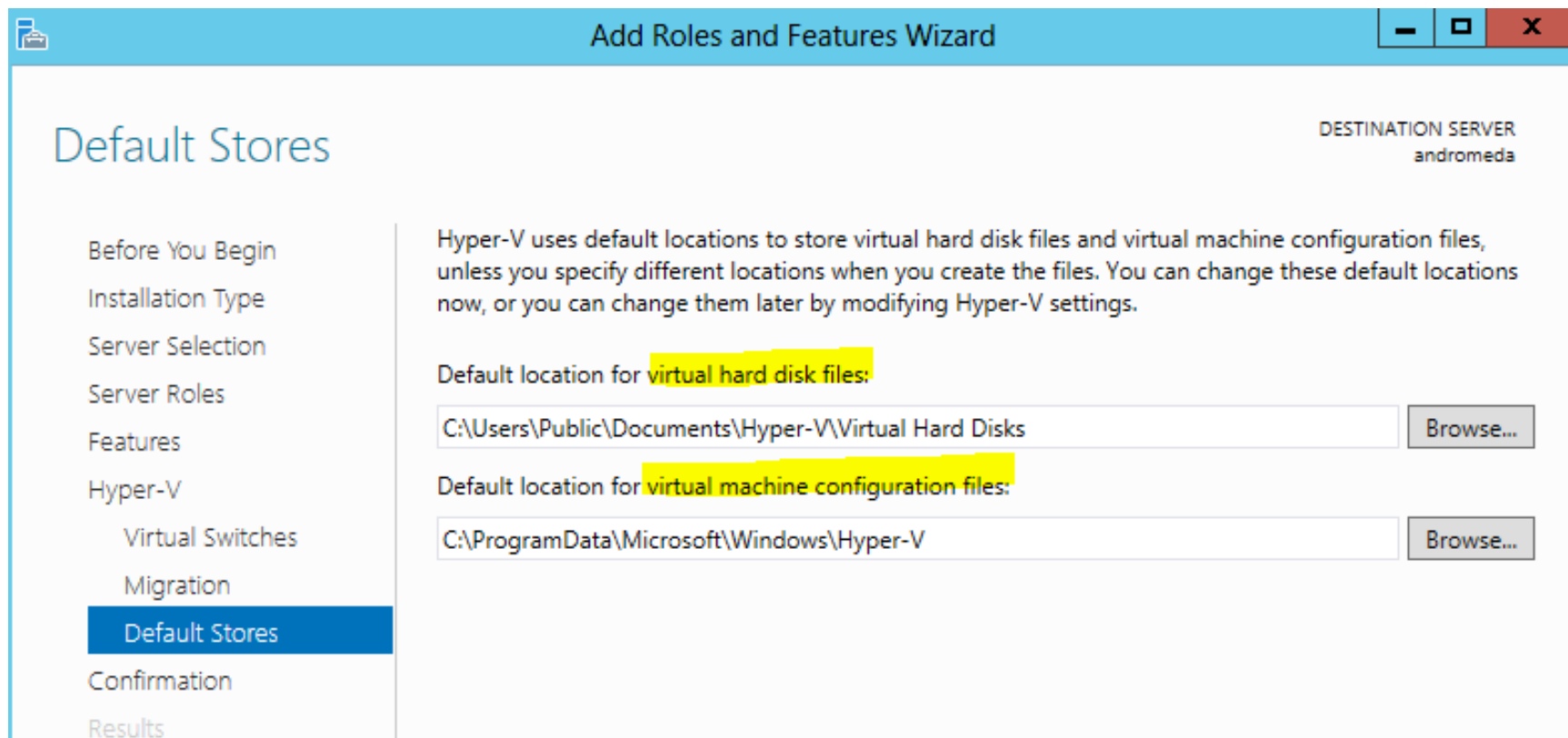
Select the protocol you want to use to authenticate live migrations.

☒ Use Credential Security Support Provider (CredSSP)
This protocol is less secure than Kerberos, but does not require you to set up constrained delegation. To perform a live migration, you must be logged on to the source server.

☐ Use Kerberos
This protocol is more secure but requires you to set up constrained delegation in your environment to perform tasks such as live migration when managing this server remotely.

 If this server will be part of a cluster, do not enable migration now. Instead, you will configure the server for live migration, including specifying networks, when you create the cluster.

POKRAČOVÁNÍ HYPER-V



The screenshot shows the 'Add Roles and Features Wizard' window. The title bar is blue with the text 'Add Roles and Features Wizard' and standard window controls. The main content area is white. On the left, there is a vertical navigation pane with the following items: 'Before You Begin', 'Installation Type', 'Server Selection', 'Server Roles', 'Features', 'Hyper-V', 'Virtual Switches', 'Migration', 'Default Stores' (highlighted in blue), 'Confirmation', and 'Results'. The main area is titled 'Default Stores' in blue text. In the top right corner of the main area, it says 'DESTINATION SERVER' and 'andromeda'. Below the title, there is a paragraph: 'Hyper-V uses default locations to store virtual hard disk files and virtual machine configuration files, unless you specify different locations when you create the files. You can change these default locations now, or you can change them later by modifying Hyper-V settings.' There are two sections for setting default locations. The first is 'Default location for virtual hard disk files:' with a text box containing 'C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks' and a 'Browse...' button. The second is 'Default location for virtual machine configuration files:' with a text box containing 'C:\ProgramData\Microsoft\Windows\Hyper-V' and a 'Browse...' button.

DESTINATION SERVER
andromeda

Default Stores

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Hyper-V
Virtual Switches
Migration
Default Stores
Confirmation
Results

Hyper-V uses default locations to store virtual hard disk files and virtual machine configuration files, unless you specify different locations when you create the files. You can change these default locations now, or you can change them later by modifying Hyper-V settings.

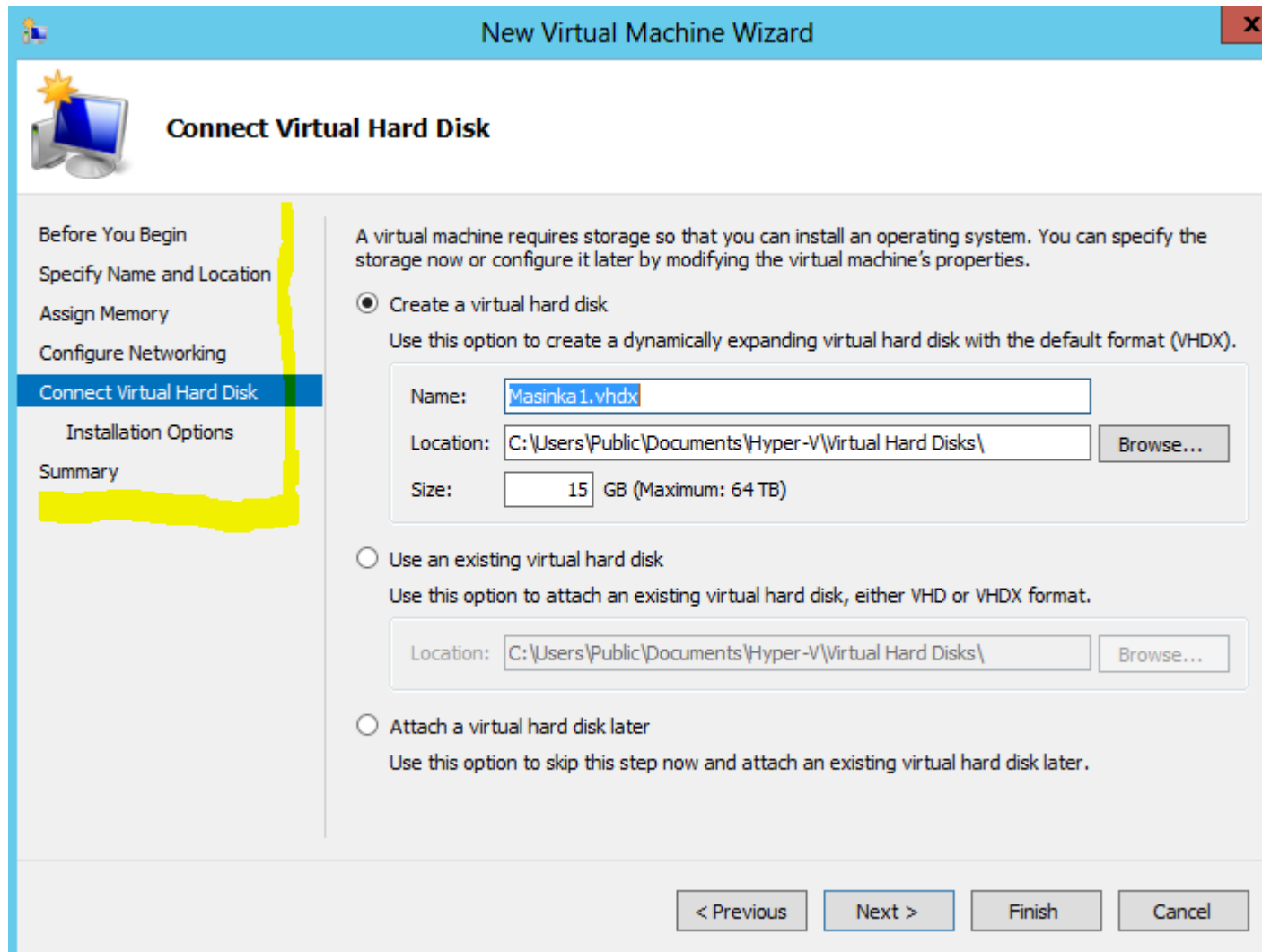
Default location for virtual hard disk files:

C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks

Default location for virtual machine configuration files:

C:\ProgramData\Microsoft\Windows\Hyper-V

KONFIGURACE HYPER-V



The screenshot shows the 'New Virtual Machine Wizard' window, specifically the 'Connect Virtual Hard Disk' step. The window has a blue title bar with the text 'New Virtual Machine Wizard' and a close button. On the left, there is a navigation pane with a yellow highlight around the 'Connect Virtual Hard Disk' step, which is currently selected. The main area of the window contains instructions and options for connecting a virtual hard disk.

Connect Virtual Hard Disk

Before You Begin
Specify Name and Location
Assign Memory
Configure Networking
Connect Virtual Hard Disk
Installation Options
Summary

A virtual machine requires storage so that you can install an operating system. You can specify the storage now or configure it later by modifying the virtual machine's properties.

☒ Create a virtual hard disk
Use this option to create a dynamically expanding virtual hard disk with the default format (VHDX).

Name:

Location:

Size: GB (Maximum: 64 TB)

☐ Use an existing virtual hard disk
Use this option to attach an existing virtual hard disk, either VHD or VHDX format.

Location:

☐ Attach a virtual hard disk later
Use this option to skip this step now and attach an existing virtual hard disk later.

< Previous Next > Finish Cancel

DOKONČENÍ HYPER-V

Podrobnější informace např.:

<http://technet.microsoft.com/en-us/library/hh831531.aspx>

ROLE — NETWORK POLICY AND ACCESS SERVICE

- VPN
- 802.11 protected wireless access
- viz nástroj
System Center ConfigurationManager
 - Health policy creation, enforcement, remediation

NAP – NETWORK ACCESS PROTECTION

- Klient pošle informaci o svém stavu
- Na jejím základě se rozhodne o **udělení přístupu**
- Pokud klientovi **chybí** např. některé bezpečnostní aktualizace, dostane **omezený přístup** a má možnost si je stáhnout a poté opět požádat o povolení k přístupu k síti
- Omezený přístup
- Plný přístup
- Klienti
 - Vista, Win7,...

NAP

- NAP klient
 - Reportuje svůj stav
- NAP enforcement point
 - Dostane report od klienta
 - Pošle jej NAP health policy serveru (RADIUS protokol)
 - Umí omezit přístup
 - 802.1x switche, VPN server
- NAP health policy server
 - Obsahuje politiky týkající se požadovaného stavu klienta
- Remediation server
 - Obsahuje updaty

Firemní síť

Síť s omezeným přístupem

Mohu získat aktualizaci?

Tady ji máš!

Požaduji
přístup.
Zde je můj stav.



Klient

Získáváš omezený
přístup do doby, než
splníš podmínky.

Požaduji opět přístup. Zde
je můj aktuální stav.

Remediation
Servers
(např. SCCM)



Network
Access
Device
(Switch, VPN)



Windows Server 2008
System Health
Servers



Politiky aktualizují IAS Server

Měl by tento klient být
omezen na základě
svého stavu?

Klient není v
pořádku. Zakaž
přístup.

Klient je v pořádku,
uděl přístup.

IAS Policy
Server
(RADIUS)



ROLE – PRINT AND DOCUMENT SERVICES

- tiskový server
 - monitorování tiskových front
 - notifikace při problémech
- přijímá scannované dokumenty ze síťových scannerů a přesměruje je na sdílení
- fax service

ROLE SERVERU – WINDOWS DEPLOYMENT SERVICES

- vzdáleně nainstalovat OS přes síť
- Windows PE obrazy (Preinstallation Environment)
- defaultní boot image **Boot.wim**
- instalační image **Install.wim**
 - v adresáři \sources na instalačním DVD
 - úprava Windows Automated Installation Kit (AIK)
 - nástroj Sysprep – generalizace OS

scénář použití:

uživatel zvolí na PC boot ze sítě (F12), nabootuje boot.wim, provede instalačním procesem (disková oblast a image co chce); uživ. data na serveru

další info: <http://technet.microsoft.com/en-us/library/hh831764.aspx>

ROLE – WINDOWS SERVER ESSENTIALS

Windows Server Essentials Dashboard

Windows Server 2012 R2

HOME USERS DEVICES STORAGE APPLICATIONS

Get Started Health Monitoring Health Report

SETUP

Complete these tasks to configure your server for the first time.

- Get updates for other Microsoft products
- Add user accounts
- Add server folders
- Set up Server Backup
- Set up Anywhere Access
- Customize Health Report Settings
- Set up Client Restore Service
- Connect computers

- Dashboard
- Client computer backup
- Není zde limit

SERVICES

Integrate your server with business productivity and collaboration solutions.

ADD-INS

Install valuable add-ins for your business.

QUICK STATUS

View a summary of the server configuration status.

HELP

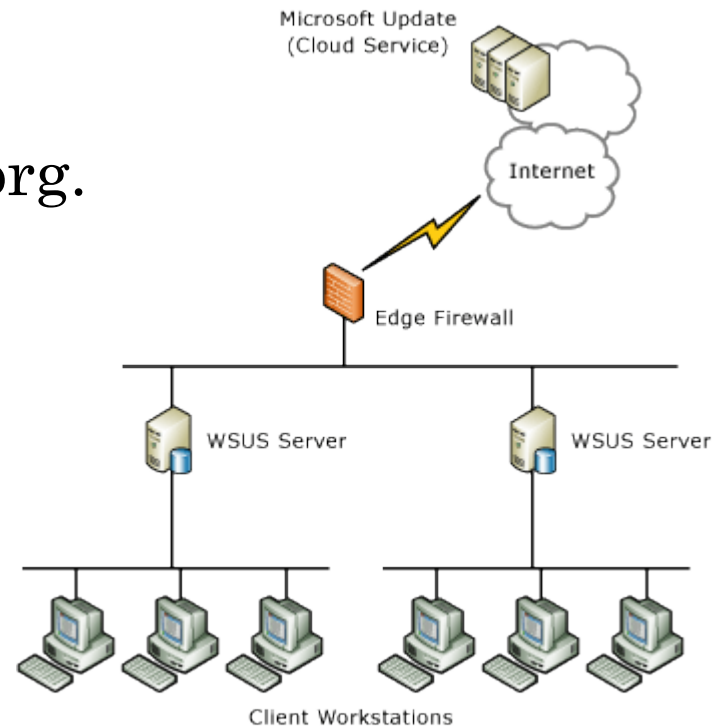
Get online help and other information for your

Zdroj:

<http://blogs.technet.com/b/matthewms/archive/2013/11/08/why-windows-server-2012-r2-the-windows-server-2012-r2-essentials-experience-step-by-step.aspx>

ROLE SERVERU – WINDOWS SERVER UPDATE SERVICES (WSUS)

- řízená distribuce updatů (Microsoft Update)
 - jen schválené updaty
 - v definovaný čas
- může být zdrojem updatů pro další WSUS servery v org.



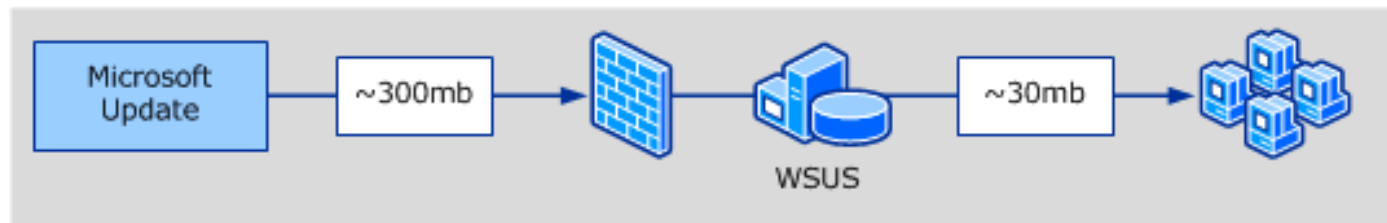
scénáře nasazení:

<http://technet.microsoft.com/en-us/library/hh852344.aspx>

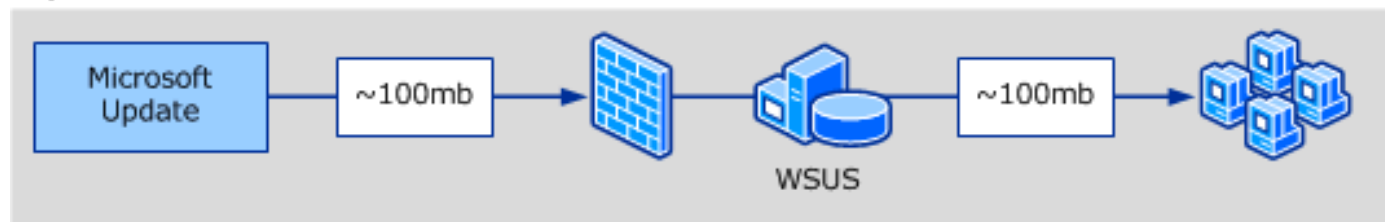
WSUS POKRAČOVÁNÍ

- express installation files: enabled x disabled

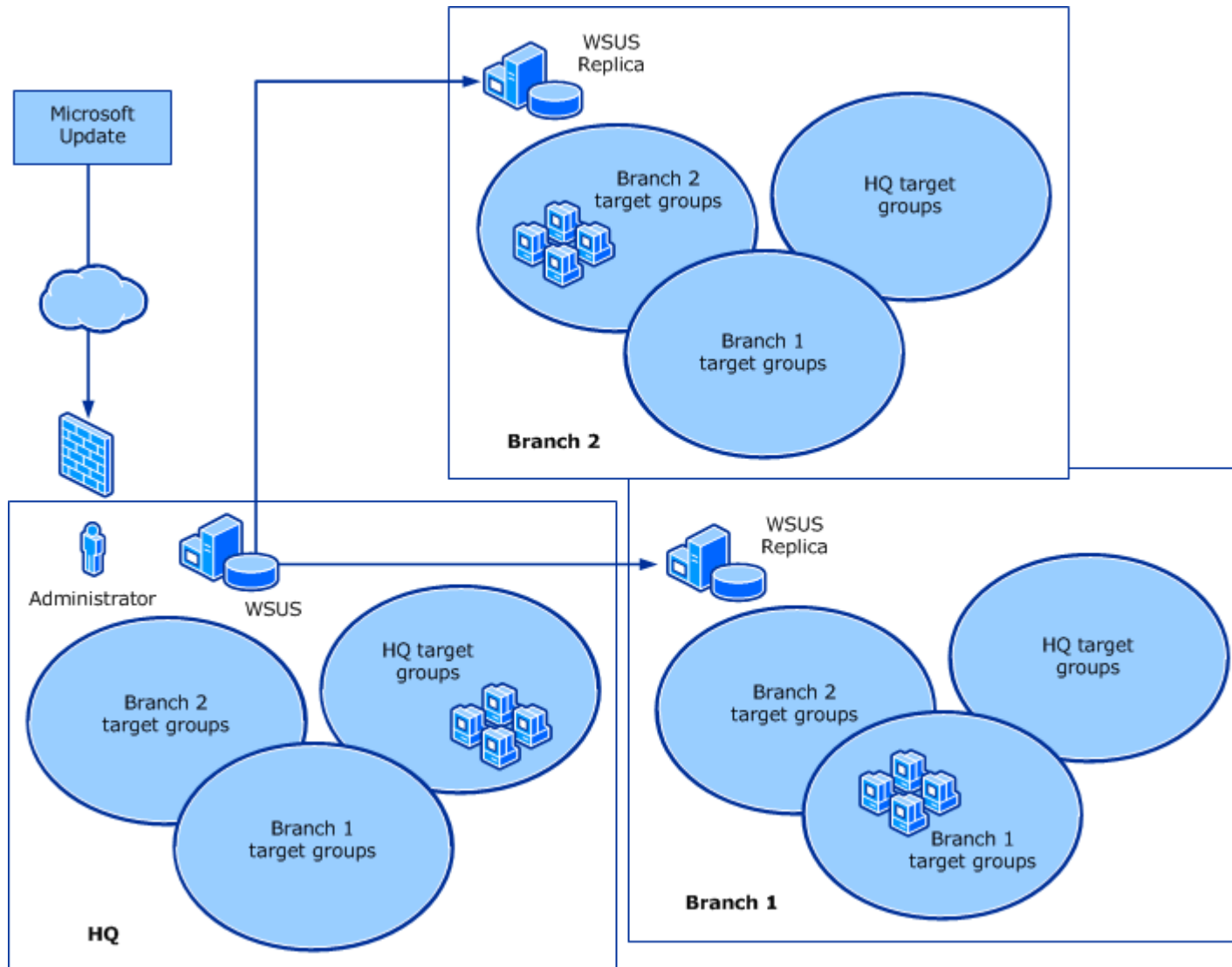
Express installation files enabled



Express installation files disabled



WSUS POKRAČOVÁNÍ



FEATURES – FAILOVER CLUSTERING

- skupina nezávislých strojů spolupracujících pro zvýšení dostupnosti a škálovatelnosti
- clusterové servery – nody – propojené
- nod selže - službu převezme jiný (failover)
- storage připojené k uzlům clusteru
- na všech edicích Windows 2012 serveru, včetně Server Core instalací

WINDOWS SERVER 2012 CORE

Minimální prostředí pro běh určitých rolí serveru

AD, DHCP, DNS, File & Print, IIS

Streaming Media Services

Windows Virtualizace

Chybí

- Windows Explorer, Internet Explorer, .NET FW

Nastavení

- Příkazová řádka
- MMC (Microsoft Management Console)

PROČ CORE SERVER?

Aktualizace MS pro serverové systémy Win2000/3
za posledních 8 let: **60%** chyb v GUI

Core

- Ne že by GUI neměl, ale minimalizováno
- Neznamená snížení požadavků na výkon HW (!)

SERVER 2008 CORE – INSTALACE ROLE IIS

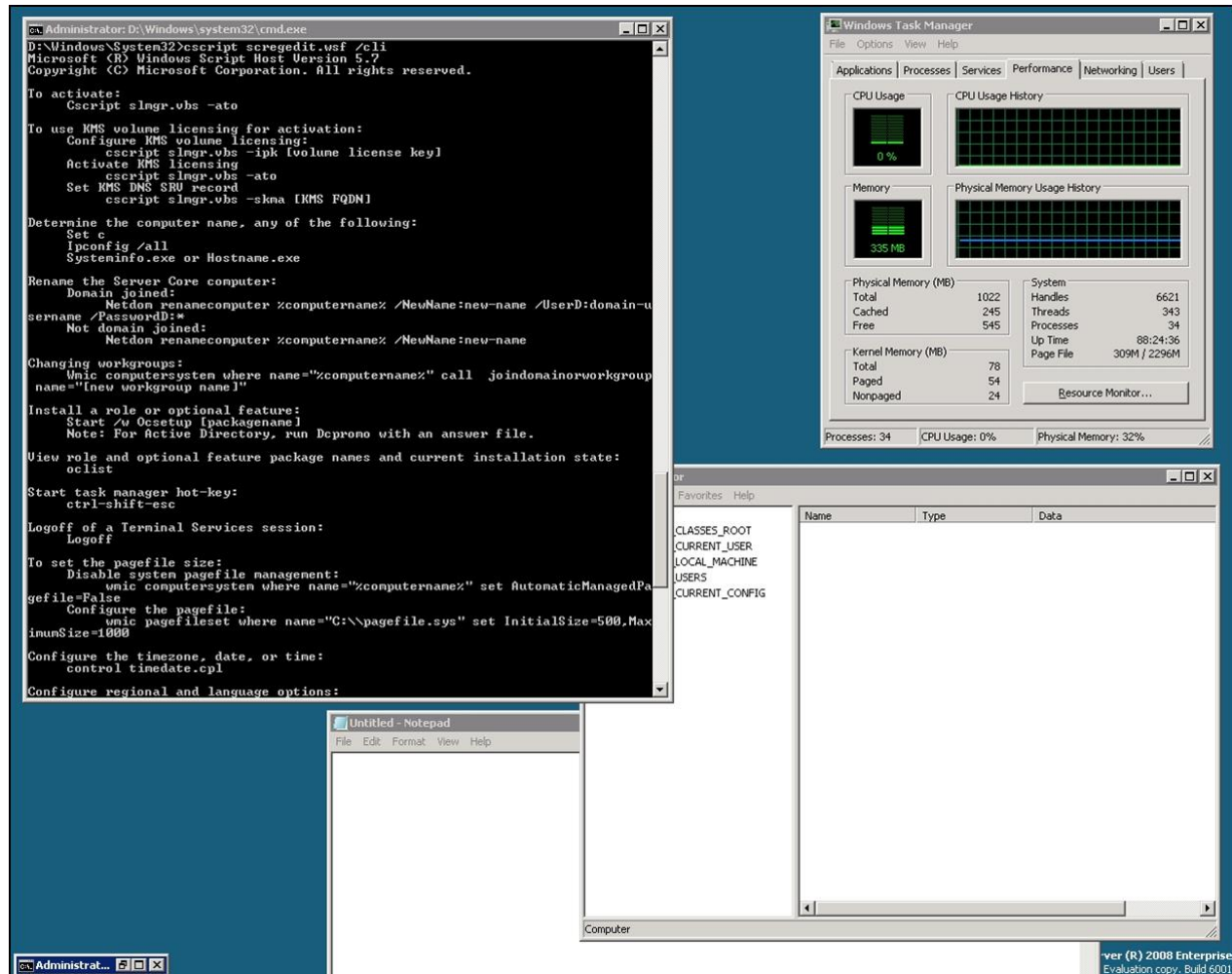
Defaultní:

*start /w pkgmgr /iu:IIS-WebServerRole;WAS-
WindowsActivationService;WAS-ProcessModel*

Full IIS instalace:

*start /w pkgmgr /iu:IIS-WebServerRole;IIS-WebServer;IIS-CommonHttpFeatures;IIS-StaticContent;IIS-
DefaultDocument;IIS-DirectoryBrowsing;IIS-HttpErrors;IIS-HttpRedirect;IIS-ApplicationDevelopment;IIS-ASP;IIS-
CGI;IIS-ISAPIExtensions;IIS-ISAPIFilter;IIS-ServerSideIncludes;IIS-HealthAndDiagnostics;IIS-HttpLogging;IIS-
LoggingLibraries;IIS-RequestMonitor;IIS-HttpTracing;IIS-CustomLogging;IIS-ODBCLogging;IIS-Security;IIS-
BasicAuthentication;IIS-WindowsAuthentication;IIS-DigestAuthentication;IIS-
ClientCertificateMappingAuthentication;IIS-IISCertificateMappingAuthentication;IIS-URLAuthorization;IIS-
RequestFiltering;IIS-IPSecurity;IIS-Performance;IIS-HttpCompressionStatic;IIS-HttpCompressionDynamic;IIS-
WebServerManagementTools;IIS-ManagementScriptingTools;IIS-IIS6ManagementCompatibility;IIS-Metabase;IIS-
WMICompatibility;IIS-LegacyScripts;IIS-FTPPublishingService;IIS-FTPService;WAS-WindowsActivationService;WAS-
ProcessModel*

SERVER CORE 2008 SCREENSHOT



SERVER CORE 2012

- zdroj: <http://www.mstvcz.cz/it/videos/542>
- základní konfigurace:

```
netsh interface ipv4 show interfaces
```

```
netsh interface ipv4 set address name=ethernet static  
192.168.201.20 255.255.255.0 192.168.201.1
```

```
netsh interface ipv4 add dnsserver name=ethernet  
192.168.201.10
```

```
netdom renamecomputer localhost /NewName:srcore  
shutdown /r /t 0
```

SERVER CORE 2012

vzdálená správa

`winrm quickconfig`

`netdom join localhost /domain:demo.int`

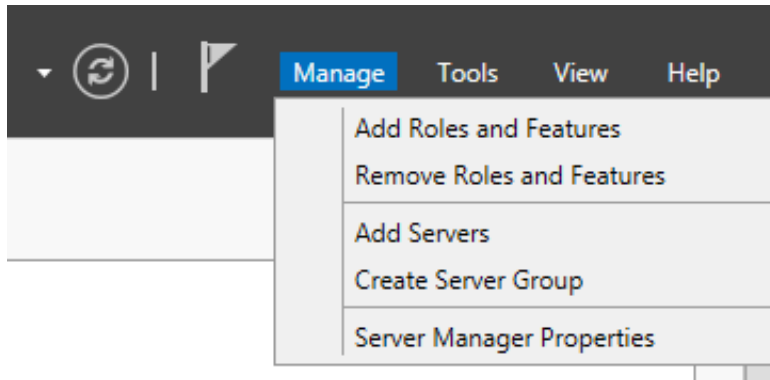
`/userd:demo\administrator /passwordd:*`

- lze spravovat z Windows Server manageru
- lze doinstalovat User Interface (Features – User Interface) a přejít z Core na plný grafický shell
- lze provést doinstalaci i z řádky:
`dism /online /enable-feature /all /featurename:Server-Gui-Shell`
- lze i odinstalovat UI -> zpátky na Core edici

SERVER MANAGER (SM)

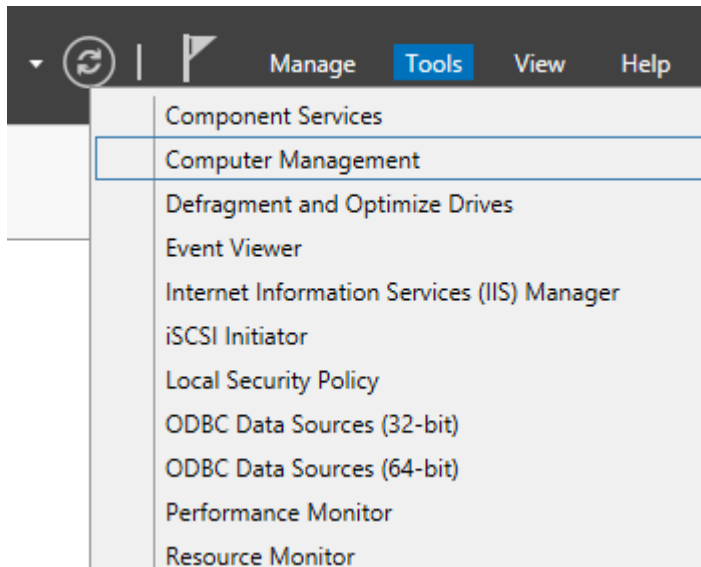
- základní nástroj pro management
- lze přidat i servery 2008 R2
- vzdálená instalace rolí jen pro Server 2012
- alerty performance counteru
- BPA – best practice analyzer

SERVER MANAGER – MANAGE, TOOLS



Manage

- přidání rolí
- přidání serverů do správy



Tools

nástroje pro správu:

- Computer Management
- IIS manager
- Performance monitor
- Windows Firewall ...







SERVER MANAGER

- dashboard
- local server
- all servers
- file and storage services
- iis

SM - DASHBOARD

ROLES AND SERVER GROUPS





Roles: 2 | Server groups: 1 | Servers total: 1

 File and Storage Services 1	 IIS 1	 Local Server 1
 Manageability	 Manageability	 Manageability
Events	Events	Events
Performance	Services	Services
BPA results	Performance	Performance
	BPA results	BPA results

SM – LOCAL SERVER

- properties (tasks – shut down)
- events
- services (start, stop, restart)
- bpa (best practices analyzer)
- performance (configure alerts)

SM – LOCAL SERVER - PERFORMANCE ALERT

Local Server : Configure Performance Alerts

Set Performance Alert Thresholds

After you change thresholds and click Save, updated data is displayed for this group or role.

CPU (% usage)

Memory (MB available)

Set Performance Graph Display Period

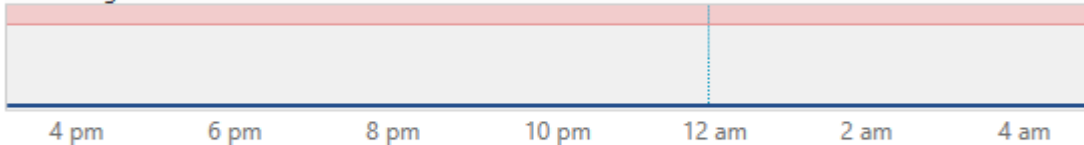
The performance graph area for this role or server group displays performance data for the number of days specified in the Graph display period setting. Lower values show a shorter graph.

Graph display period (days)

PERFORMANCE

All results | 1 total | Last 24 hours

CPU Usage 0.00 % - 0.14 %



Available Memory 60.39 GB - 60.63 GB

SM – ALL SERVERS

- správa více serverů z jednoho místa
- provedení akcí na více serverech

SM – FILE AND STORAGE SERVICES

- Servers, Volumes, Disks, Storage Pools
- Shares, iSCSI
- Storage Pool
 - fyzické disky do storage poolu
 - lze vytvářet volumes ze storage poolu

PŘÍSTUPOVÁ PRÁVA, FILESYSTEMY

○ NTFS

- Pozor na ADS (Multiple/Alternate Data Streams) – ukázka
 - Soubor:stream
 - notepad **soubor.txt:skryty.txt**
 - Velikost udaná příkaze dir je bez ADS streamů
 - Viry, backdoors
- Práva privilegovaného uživatele (administrator)
 - uživatel může odmítnout přístup uživateli s adm. právy
 - admin může převzít vlastnictví souboru (take ownership)

SOUBORY, PŘÍSTUPOVÁ PRÁVA

známe z Linuxu:

- základní unixová práva r,w,x pro u,g,o
`chmod 777 ahoj.txt`

u NTFS:

- ACL (Access Control List)
podrobný seznam přístupových práv
více uživatelů
více skupin

PŘÍSTUPOVÁ PRÁVA

- Převzetí vlastnictví
- Nastavení práv na soubor/adresář
- **Dědění práv** z nadřazeného adresáře
- Přerušení dědění práv
- Propagace práv na podřízené objekty

- Práva na adresář,soubor **x** práva na sdílení (share)
 - Např. nastavit práva na soubory a share: full everyone
 - Další filtr (další pomyslná laťka)

NASTAVENÍ PŘÍSTUPOVÝCH PRÁV

1. rem Skript na pridani problemoveho uzivatele
2. net user %1 tajneHeslo /add /fullname:%2
/passwordchg:no *(a další volby)*
3. mkdir D:\lidicky\%1
4. cacs D:\lidicky\%1 /e /g %1:f
5. mkdir D:\lidicky\%1\profile-TITANIC
6. net group CRAZY %1 /add

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

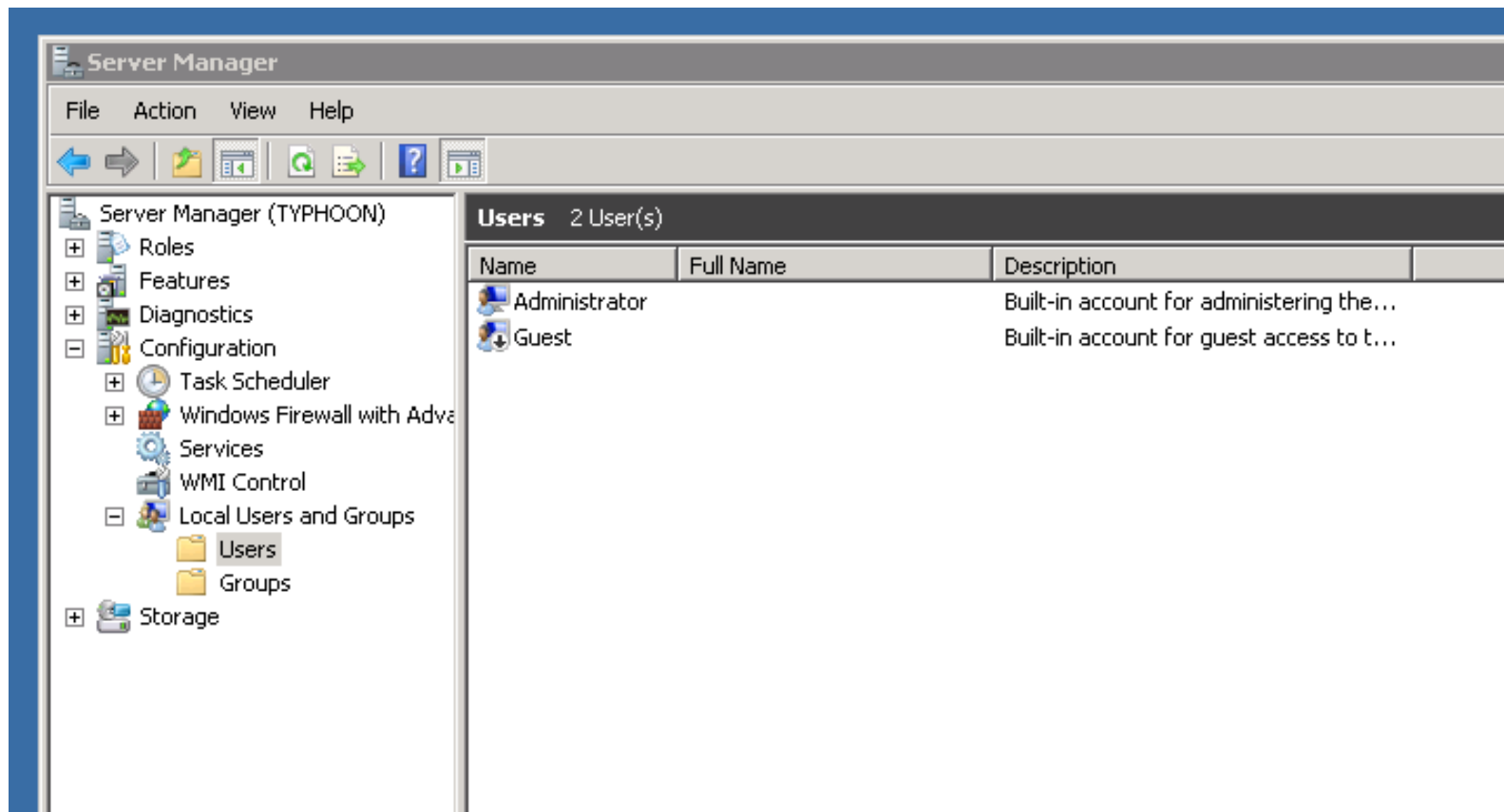
SPECIÁLNÍ ÚČTY A SKUPINY

- IUSR_VOPICKA .. IIS na serveru VOPICKA
- INTERACTIVE .. hlavně na PC
(např. skupina PowerUsers – přidat INTERACTIVE)
- Guest

Skupiny (WS, Server, AD)

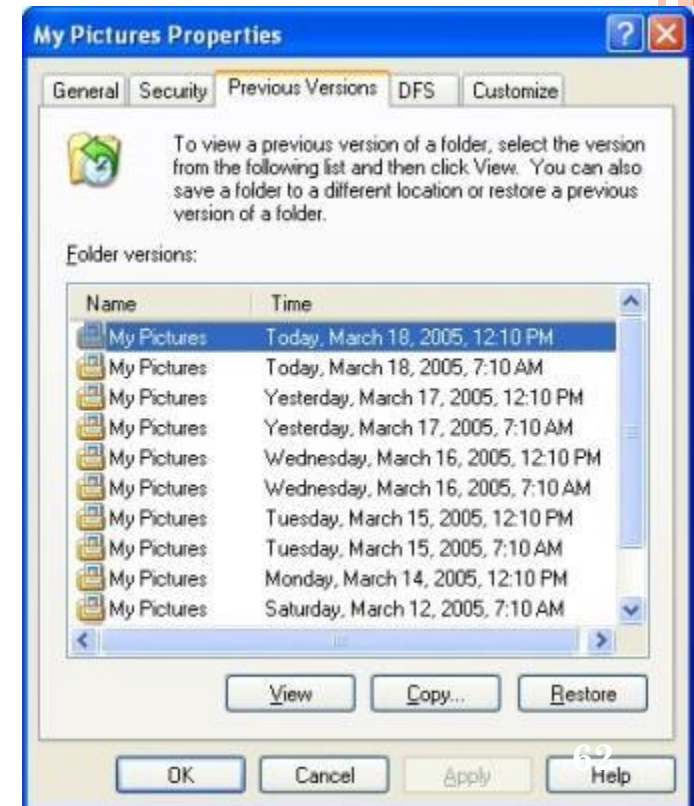
- Administrators
- Power users
- Backup Operators
- Print Operators

SERVER MANAGER – SPRÁVA UŽIVATELŮ



SHADOW COPIES (NTFS), PREVIOUS VERSIONS

- Předchozí verze souboru adresáře v **určitém časovém bodě** v minulosti
- Zálohování i včetně otevřených souborů
- ukázka na cvičení



ZÁLOHOVÁNÍ (LIŠÍ SE V RŮZNÝCH VERZÍCH)

- Accessories – System Tools – Backup
 - Backup
 - Restore
 - Automated System Recovery
- Zálohování – kromě souborů důležitá položka System State
 - Active Directory, Boot Files, COM+ Class Registry, Registry, SYSVOL

AUDITOVÁNÍ PŘÍSTUPU

Sdílení (share) a co s ním bylo prováděno

Properties – Security – Advanced – Auditing

Čtení, vytváření, rušení ..

Info do security logu

SDÍLENÍ

- \\server\sdileni
- \\server\sdileni\$
 - Skrytá sdílení, např. C\$, D\$, lze vlastní
 - Systémová např. NETLOGON
- net view \\server
- Adm tools-Computer Management-Shared Folders
 - Shares .. Sdílení včetně skrytých, export do txt
 - Sessions
 - Open Files .. možnost close

SDÍLENÍ

- Práva týkající se sdílení
- Práva k souborům, adresářům
- Použití v lokální síti (LAN)
- Přístup ke sdílení zvenku přes VPNku
 - Viz např. support.zcu.cz CiscoVPN
 - Externí PC dostane IP adresu z rozsahu dané LAN sítě

DFS

- Konsolidace sdílení

- \\server1\dok1
- \\server2\dok2

- DFS root - sdílení z různých serverů přístupné z 1 bodu
 - Dok1
 - Dok2
- Organizace mnoha SMB sdílení do distribuovaného FS

DFS KONFIGURACE

- Server – Role – File Services – DFS
 - \\ds19-win\public
 - C:\DFSRoots\public (lze změnit)

BEZPEČNOSTNÍ NÁSTROJE

- IIS Lockdown Tool
 - Zabezpečení IIS4,5 (historie)
- RootkitRevealer
 - Mark Russinovich
 - Registry a file system API vypisy
 - také jen pro starší servery
- **Microsoft Baseline Security Analyzer 2.2**
 - Stav updatů, doporučení jak řešit problémy
- **Hijackthis** (<http://www.hijackthis.cz/>)

DALŠÍ NÁSTROJE

Sysinternals - Mark Russinovich

- Monitorování procesů, přístupů k souborům a registrům
- Newsid
- Celá řada dalších utilit

Další

- Příkaz netstat
- netsh

*netsh interface ip set address name="MistniSit" static
192.168.1.32 255.255.255.0 192.168.1.1 gwmetric=0*

SPRÁVA UŽIVATELSKÝCH ÚČTŮ

Využití ActiveDirectory

KIV:

lokální počítač (lokální účet a heslo)

doména KIV (účet v doméně, doménové heslo)

ZCU.CZ (účet v doméně,
ověřenícentrálním Kerberem – SSO)

Použití: *student, host 1 PC, host laboratoř*

ACTIVE DIRECTORY

- Centrální adresář (LDAP) – zdroje, služby, uživatelé
 - Uživatelé
 - Skupiny
 - Počítače
 - Doménové řadiče
 - Trust s dalšími systémy
- Profil uživatele
 - Lokální
 - Roamingový (film na ploše, cache IE, složka dokumenty..)
 - Mandatory (např. školení, prezentace)

WINDOWS SERVER

○ Řadič domény

- Ve větších organizacích alespoň 2
- RO řadič domény (read-only) do malých poboček firmy, kde mohou být s bezpečností na štíru

○ Member server

- Server je členem domény, ale není jejím řadičem

○ Standalone server

- Stojí mimo, nemá s doménou nic společného
- Např. licenční servery,...

DEFINICE

Adresář

hierarchická struktura, v níž jsou obsaženy informace o objektech v síti

Adresářová služba (např. AD)

poskytuje metody pro ukládání dat v adresářích a zpřístupňuje tato data oprávněným uživatelům

CO LZE V AD UKLÁDAT?

Celá řada objektů a atributů

Lze měnit

Pouze v odůvodněných případech

Active Directory Schema

- Schema classes
 - Určuje **objekty**, které lze uložit v AD
- Schema attributes
 - Určuje jednotlivé **atributy**

Nástroj pro správu schematu není v defaultní nabídce admin nástrojů, je potřeba explicitně nastavit (viz dále)

LOGICKÁ STRUKTURA AD

- Les
- Strom
- Doména
- Organizační jednotka (OU)
- Objekty
 - atributy

FYZICKÁ STRUKTURA AD

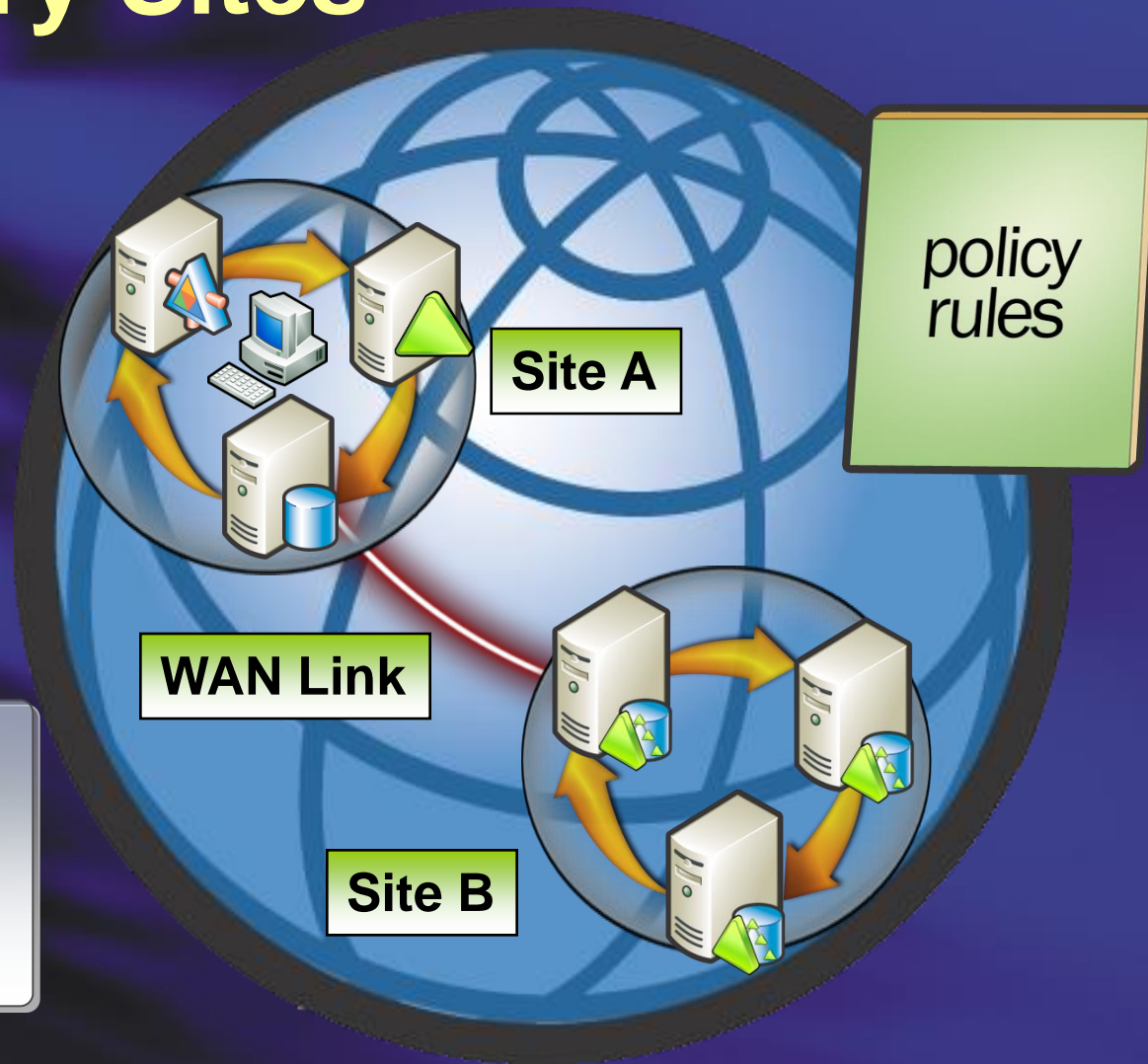
- Doménové řadiče (server)
- Site (sít, rozsah adres)
 - množina „well-connected“ TCP/IP subsítí
 - nalezení služeb (locate services)
 - optimalizace replikací (uvnitř situ více replik. spojení)
 - lze definovat politiky na úrovni situ

Význam pro replikace

Nástroj:

Active Directory Sites and Services

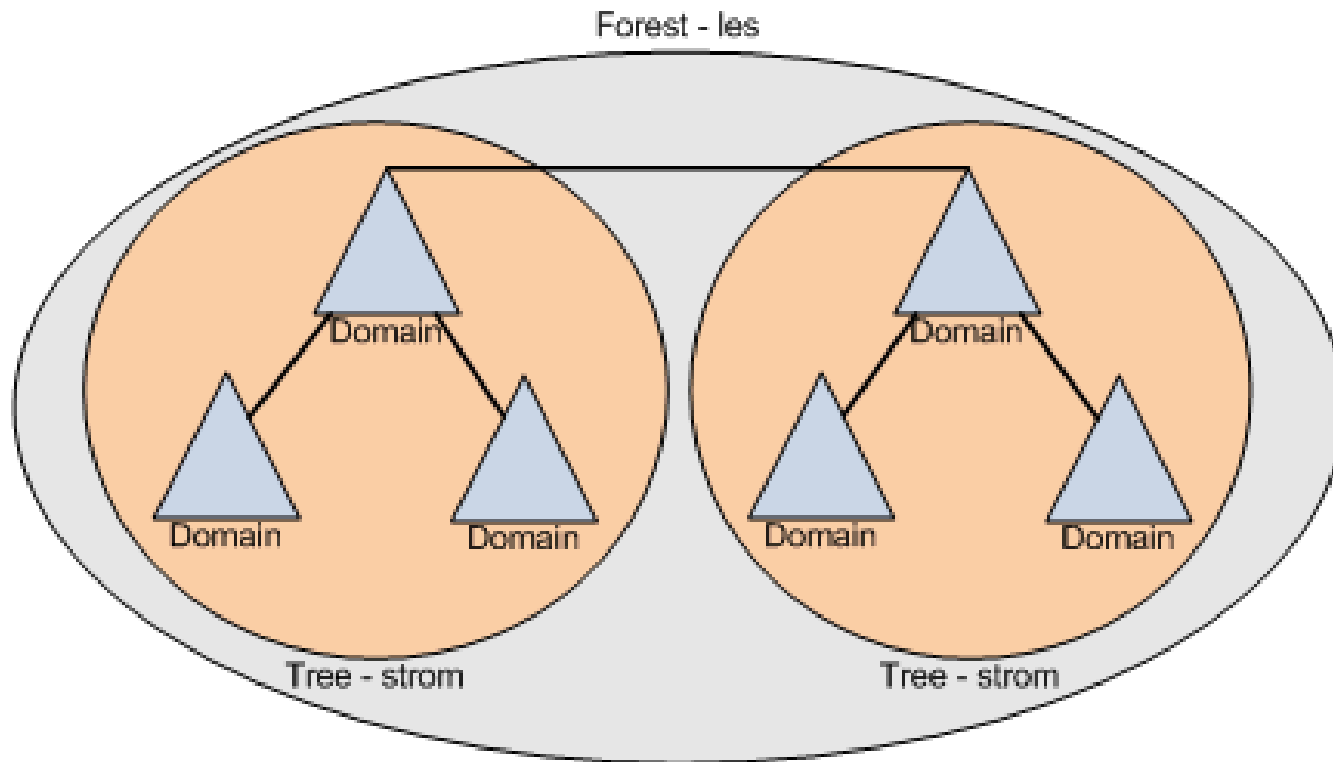
Active Directory Sites



Sites Used To:

- Locate Services
- Optimize Replication
- Define Policies

FOREST, TREE, DOMAIN

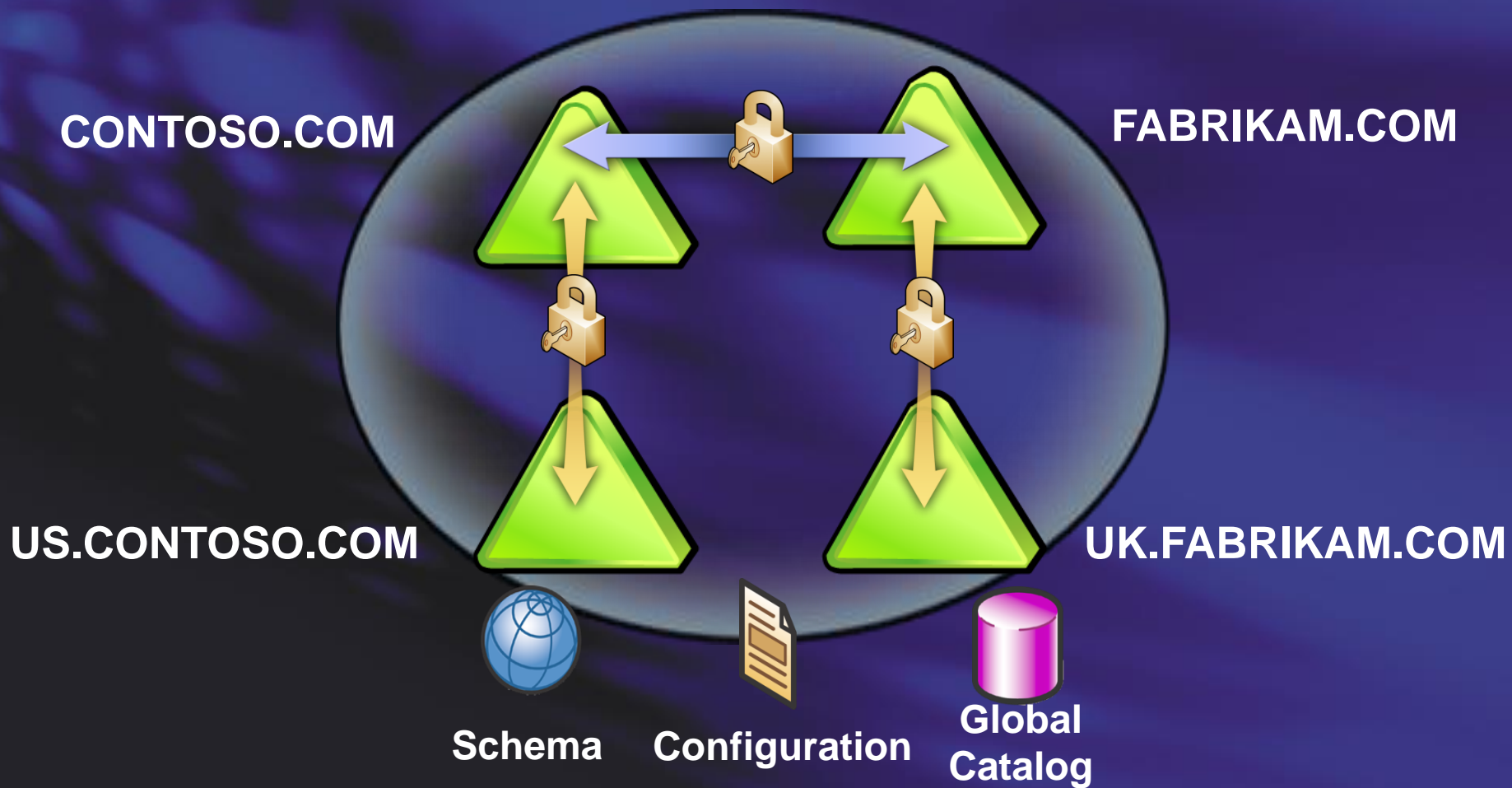


Zdroj materiálů k AD: samuraj.cz

LES - FOREST

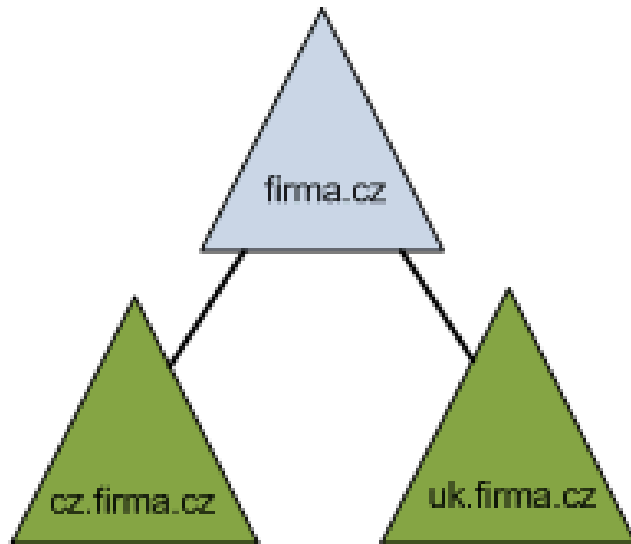
- 1 nebo více **nezávislých** stromů
- Všechny domény v lese sdílí
 - Stejné schéma
 - Globální katalog
 - Implicitní dvoucestná důvěra (trust)
 - Stromy v lese mají vlastní pojmenování

Active Directory Forests



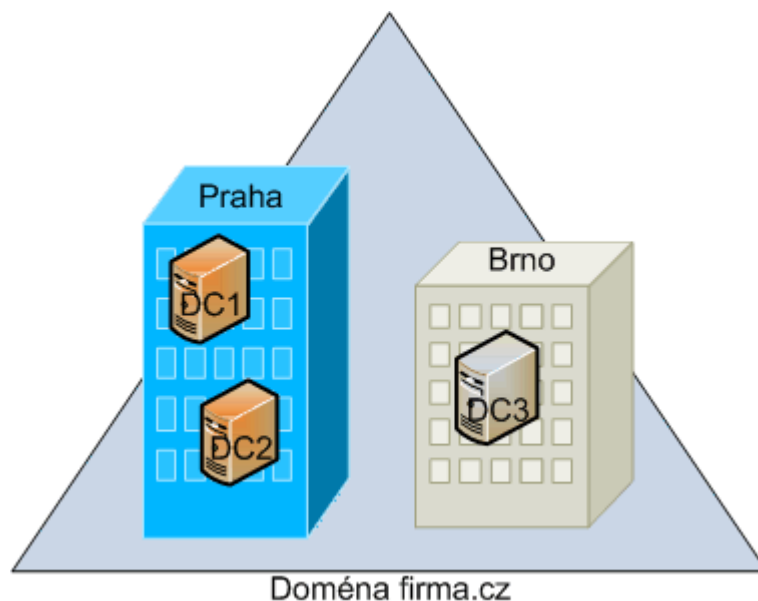
STROM - TREE

- K rodičovské doméně (parent, root domain) přidáme podřízenou doménu (child domain)
- Sdílejí souvislý jmenný prostor



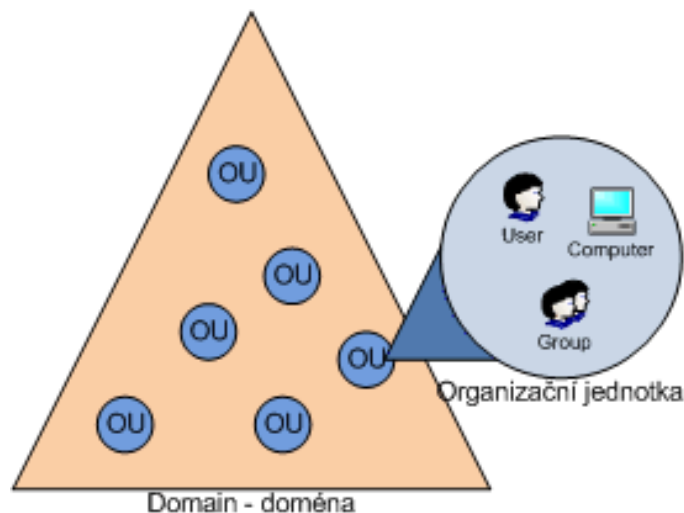
DOMÉNA - DOMAIN

- Základním prvkem AD
- Není omezena fyzicky – může být přes více poboček
- Tvoří bezpečnostní hranici
 - Řízení přístupu k doménovým objektům, ACL



ORGANIZAČNÍ JEDNOTKA - OU

- Kontejner uvnitř domény
- Slouží k logickému seskupování objektů
- Na OU lze delegovat administrační oprávnění
- Lze je libovolně zanořovat (cca kolem 15 úrovní)



DOMÉNOVÝ ŘADIČ

- Server, obsahuje repliku doménového adresáře
- V doméně jich může být více
- Na 1 řadiči – pouze 1 doména

Změna v AD – na 1 řadiči – automatická replikace
(periodicky plánovaná, okamžitá)

Multimaster – běžné replikace, všechny DC
rovnocenné

Singlemaster – 1 DC je hlavní
(operations masters roles)

JEDINEČNÉ ROLE

Jedinečné v rámci **lesa**

Schema master

Domain naming master

Jedinečné v rámci **domény**

Relative identifier master (RID)

Primary domain controller (PDC) emulator

Infrastructure master

Operations Master Roles

Forest Roles

Schema Master



Domain Master



Domain Roles

PDC Emulator



RID Master



Infrastructure



FOREST-WIDE ROLE

○ Schema master

- řídí updaty a modifikace **schématu**
- př.: přidání tříd, atributů (např. pro Exchange)
- po dokončení updatu je replikován ze schema masteru na ostatní DC
- není-li dostupný, nejde měnit schéma

○ Domain Naming master

- Přidávání a odebírání **domén** do lesa
- není-li, nelze přidávat a odebírat domény
- musí být globálním katalogem

DOMAIN-WIDE ROLE

Relative Identifier Master (RID)

- Přiděluje řadičům bloky čísel RID
- když začne zásoba čísel docházet, požádá řadič RID mastera o další
- Používají se pro vytvoření SID (security identifier) každého objektu v AD = **domain SID stejný + relative ID (RID) unikátní**
- řídí přesun objektů mezi doménami
- pokud není RID master, když DC dojdou čísla, nemůže vytvořit nový security principal (uživatele, skupinu, ...)

DOMAIN-WIDE ROLE

Infrastructure Master (IM)

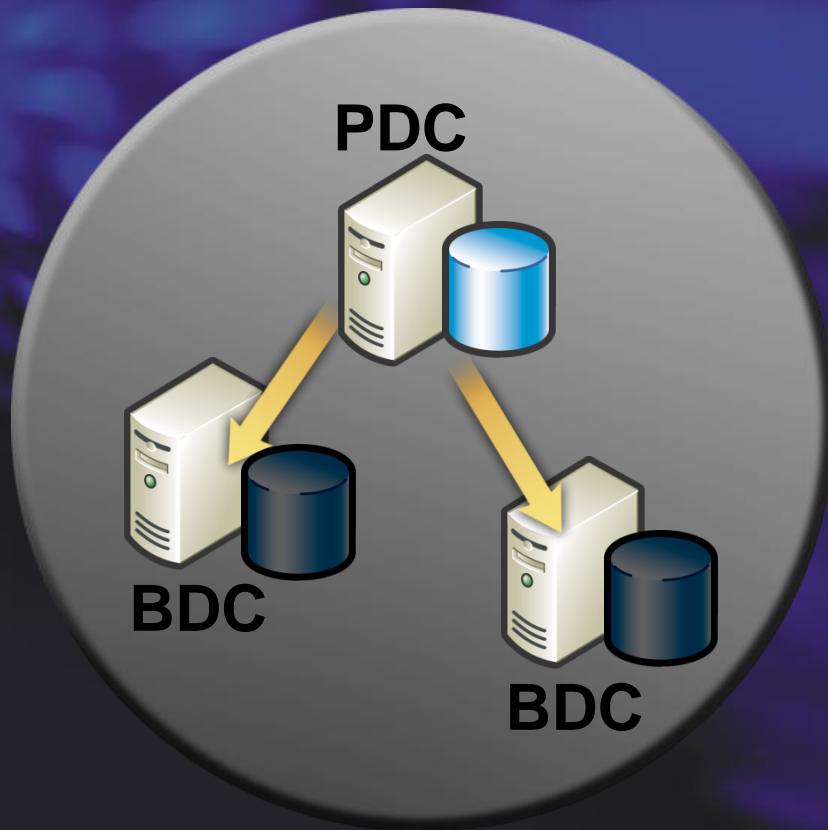
- Objekt v doméně referencuje objekt v jiné doméně s využitím GUID, SID a DN
 - př.: skupina v jedné doméně referencuje uživatele nebo skupinu v jiné doméně
- IM updatuje SID a DN v cross-domain referencích
 - např. přesun referencovaného objektu
- pokud máme více domén, IM by nemělo být na serveru, kde je GC (global catalog)
 - nevadí v jedno-doménovém lesu (nejsou externí reference)

DOMAIN-WIDE ROLE

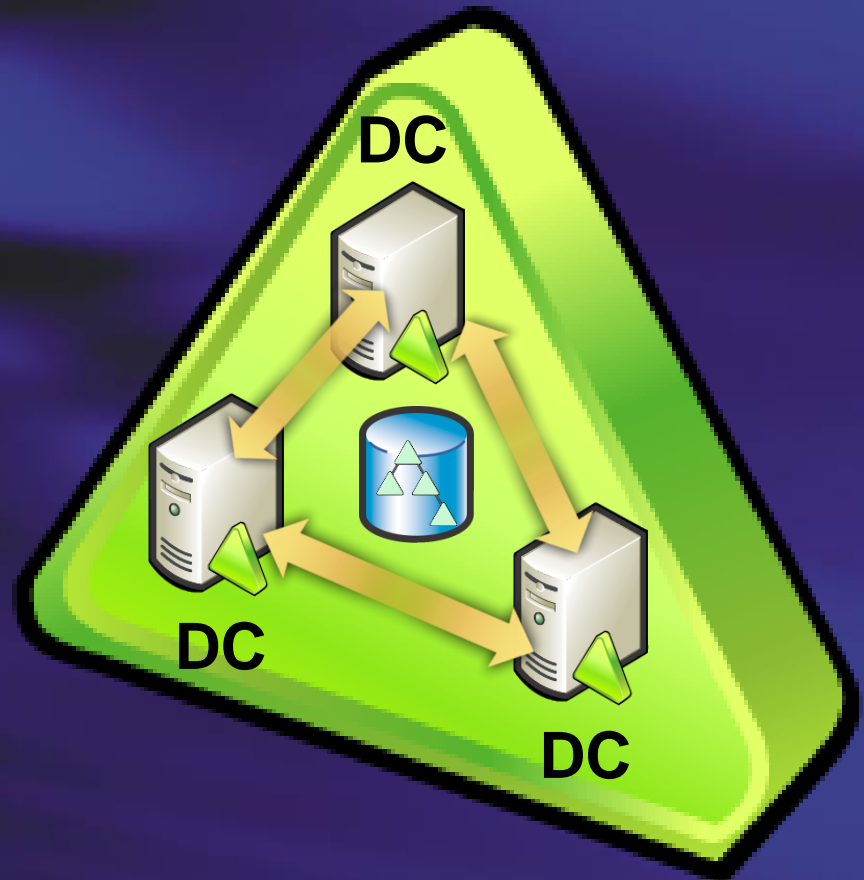
Primary Domain Controller (PDC) Emulator

- dříve: emulace Windows NT 4.0 PDC pro staré klienty
- synchronizace času v doméně
(=> vyžaduje autentikační protokol Kerberos)
- autoritativní pro doménu
- změny hesel jsou replikovány preferenčně na PDC
- account lockout (odemčení konta)
- vytváření, editace GPO (group policy objects)
- funguje jako Domain Master Browser

Domain Controllers



Windows NT 4.0



Windows Server 2003

DEFAULTNÍ ROLE

- První DC ve forestu má všechny role
 - 5 rolí
- První DC v nové doméně, pokud již forest je, má všechny doménové role
 - 3 role

UMÍSTĚNÍ ROLÍ - DOPORUČENÍ

- **schema master** a **domain naming master** na stejném DC, a také by měl být **globálním katalogem**
- RID master a PDC emulátor na stejný DC
- vícedoménový forest
infrastructure master nesmí být globálním katalogem (ale měl by na něj mít dobré spojení)

UMÍSTĚNÍ ROLÍ - DOPORUČENÍ

- jednodoménový forest
 - všech 5 rolí na jednom DC, který je také globálním katalogem
- vícedoménový forest
 - Infrastructure master role na DC, které není globálním katalogem

ZJIŠTĚNÍ ROLÍ (SERVER 2012)

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

GLOBALNÍ KATALOG GC

- Vybrané informace o objektech z celého stromu/lesa
- může najít objekty v libovolné doméně, aniž by potřeboval znát jméno domény
- Global Catalog Server
- Může jich být více, multimaster replikace
- Umístění do poboček
 - zvážit náklady na replikace
- AD Sites and Services – Server – NTDS settings
 - nastavení, zda je server GC

Pozn. Universal Group Membership Caching
(AD Sites and Services, site, ntds settings)

NÁSTROJE PRO SPRÁVU – PŘEVOD ROLÍ

- Active Directory **Schema** (není defaultně)
 - Pro změnu Schema Master
- Active Directory **Domains and Trusts**
 - Převod role Domain Naming Master
- Active Directory **Users and Computers**
 - RID, PDC, Infrastructure

nástroje najdete: Start – Administrative Tools

přidání schéma: `regsvr32 schmmgmt.dll`, `mmc /a,Add/Remove Snap-in`

Console Root\Active Directory Schema [herakles.kiv.zcu.cz]\Attributes

Console Root

Active Directory Schema [herakles.kiv.zcu.cz]

Classes

Attributes

Name	Syntax	Status	Description
accountExpires	Large Integer/Interval	Active	Account-Expires
accountNameHistory	Unicode String	Active	Account-Name-History
aCSAggregateTokenRa...	Large Integer/Interval	Active	ACS-Aggregate-Token-Ra...
aCSAllocableRSVPBand...	Large Integer		
aCSCacheTimeout	Integer		
aCSDirection	Integer		
aCSDSBMDDeadTime	Integer		
aCSDSBMPriority	Integer		
aCSDSBMRefresh	Integer		
aCSEnableACSService	Boolean		
aCSEnableRSVPAccount...	Boolean		
aCSEnableRSVPMessag...	Boolean		
aCSEventLogLevel	Integer		
aCSIdentityName	Unicode String		
aCSMaxAggregatePeak...	Large Integer		
aCSMaxDurationPerFlow	Integer		
aCSMaximumSDUSize	Large Integer		
aCSMaxNoOfAccountFiles	Integer		
aCSMaxNoOfLogFiles	Integer		
aCSMaxPeakBandwidth	Large Integer		
aCSMaxPeakBandwidth...	Large Integer		

accountExpires Properties

General

accountExpires

Description: Account-Expires

Common Name: Account-Expires

X.500 OID: 1.2.840.113556.1.4.159

Syntax and Range

Syntax: Large Integer/Interval

Minimum:

Maximum:

This attribute is single-valued.

☐ Allow this attribute to be shown in advanced view

☒ Attribute is active

☐ Index this attribute in the Active Directory

☐ Ambiguous Name Resolution (ANR)

☐ Replicate this attribute to the Global Catalog

☒ Attribute is copied when duplicating a user

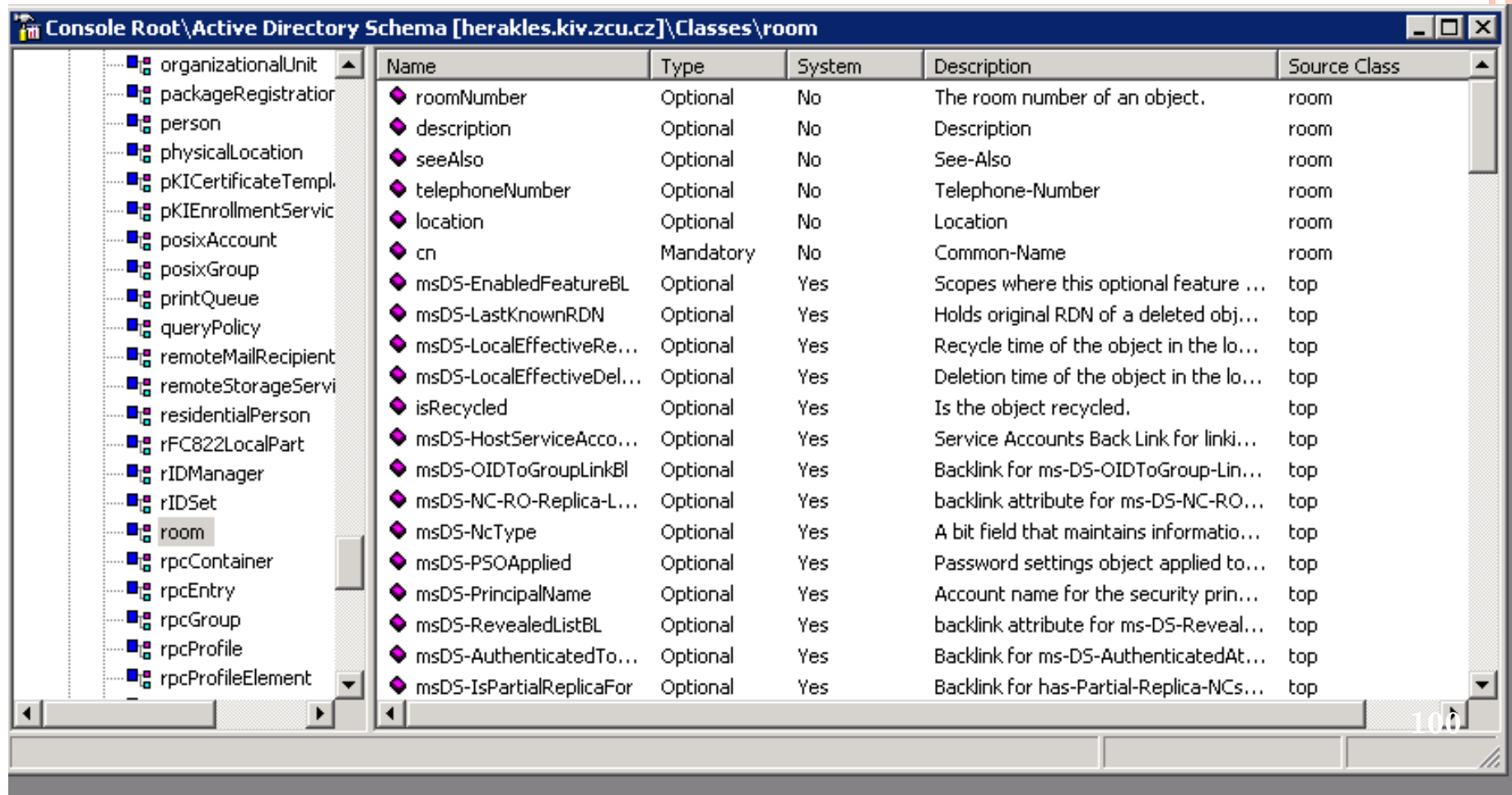
☐ Index this attribute for containerized searches in the Active Directory

OK

Cancel

Apply

AD schéma – třída room

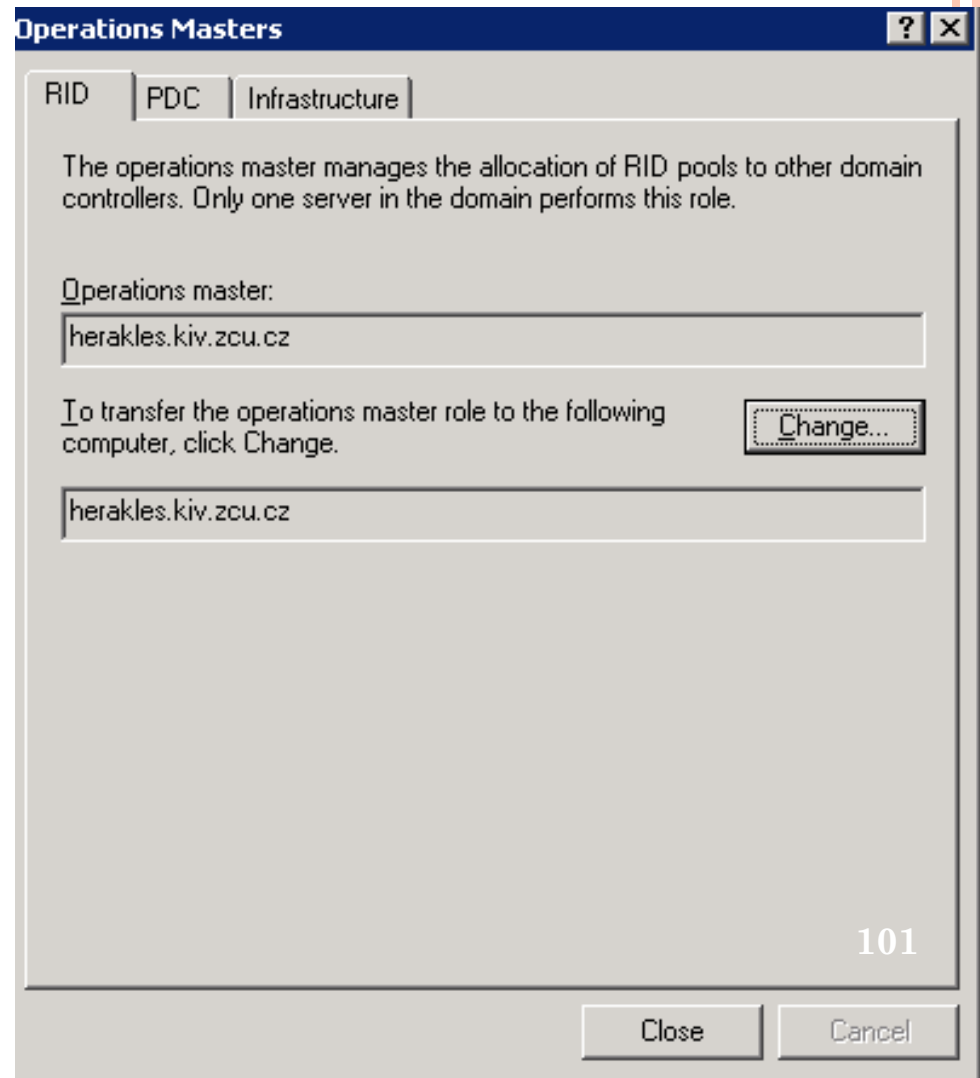


The screenshot shows the 'Active Directory Schema' console window. The left pane displays a tree of schema classes, with 'room' selected under 'Classes'. The right pane shows a table of attributes for the 'room' class.

Name	Type	System	Description	Source Class
roomNumber	Optional	No	The room number of an object.	room
description	Optional	No	Description	room
seeAlso	Optional	No	See-Also	room
telephoneNumber	Optional	No	Telephone-Number	room
location	Optional	No	Location	room
cn	Mandatory	No	Common-Name	room
msDS-EnabledFeatureBL	Optional	Yes	Scopes where this optional feature ...	top
msDS-LastKnownRDN	Optional	Yes	Holds original RDN of a deleted obj...	top
msDS-LocalEffectiveRe...	Optional	Yes	Recycle time of the object in the lo...	top
msDS-LocalEffectiveDel...	Optional	Yes	Deletion time of the object in the lo...	top
isRecycled	Optional	Yes	Is the object recycled.	top
msDS-HostServiceAcco...	Optional	Yes	Service Accounts Back Link for linki...	top
msDS-OIDToGroupLinkBl	Optional	Yes	Backlink for ms-DS-OIDToGroup-Lin...	top
msDS-NC-RO-Replica-L...	Optional	Yes	backlink attribute for ms-DS-NC-RO...	top
msDS-NcType	Optional	Yes	A bit field that maintains informatio...	top
msDS-PSOApplied	Optional	Yes	Password settings object applied to...	top
msDS-PrincipalName	Optional	Yes	Account name for the security prin...	top
msDS-RevealedListBL	Optional	Yes	backlink attribute for ms-DS-Reveal...	top
msDS-AuthenticatedTo...	Optional	Yes	Backlink for ms-DS-AuthenticatedAt...	top
msDS-IsPartialReplicaFor	Optional	Yes	Backlink for has-Partial-Replica-NCs...	top

AD USERS AND COMPUTERS

zvolíme doménu –
operation masters



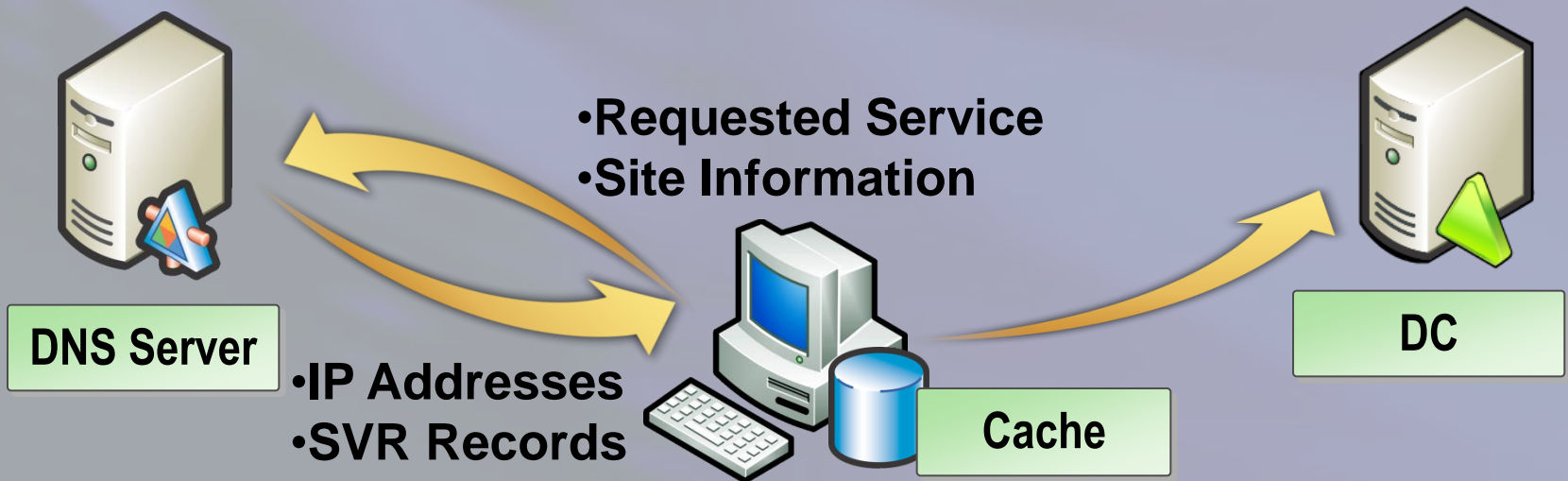
POUŽITÍ DNS PRO PŘÍSTUP KE SLUŽBÁM AD

- AD vyžaduje DNS pro svou funkci
- klient chce nějakou funkci (přihlášení do AD)
- pošle požadavek na DNS server
 - jakou službu hledá a site, kde je
- DNS server odpoví informací o lokaci doménových řadičů a SRV záznamy o službách dostupných na daných DC
- je vybrán nejvhodnější poskytovatel
- informace je kešována na klientu

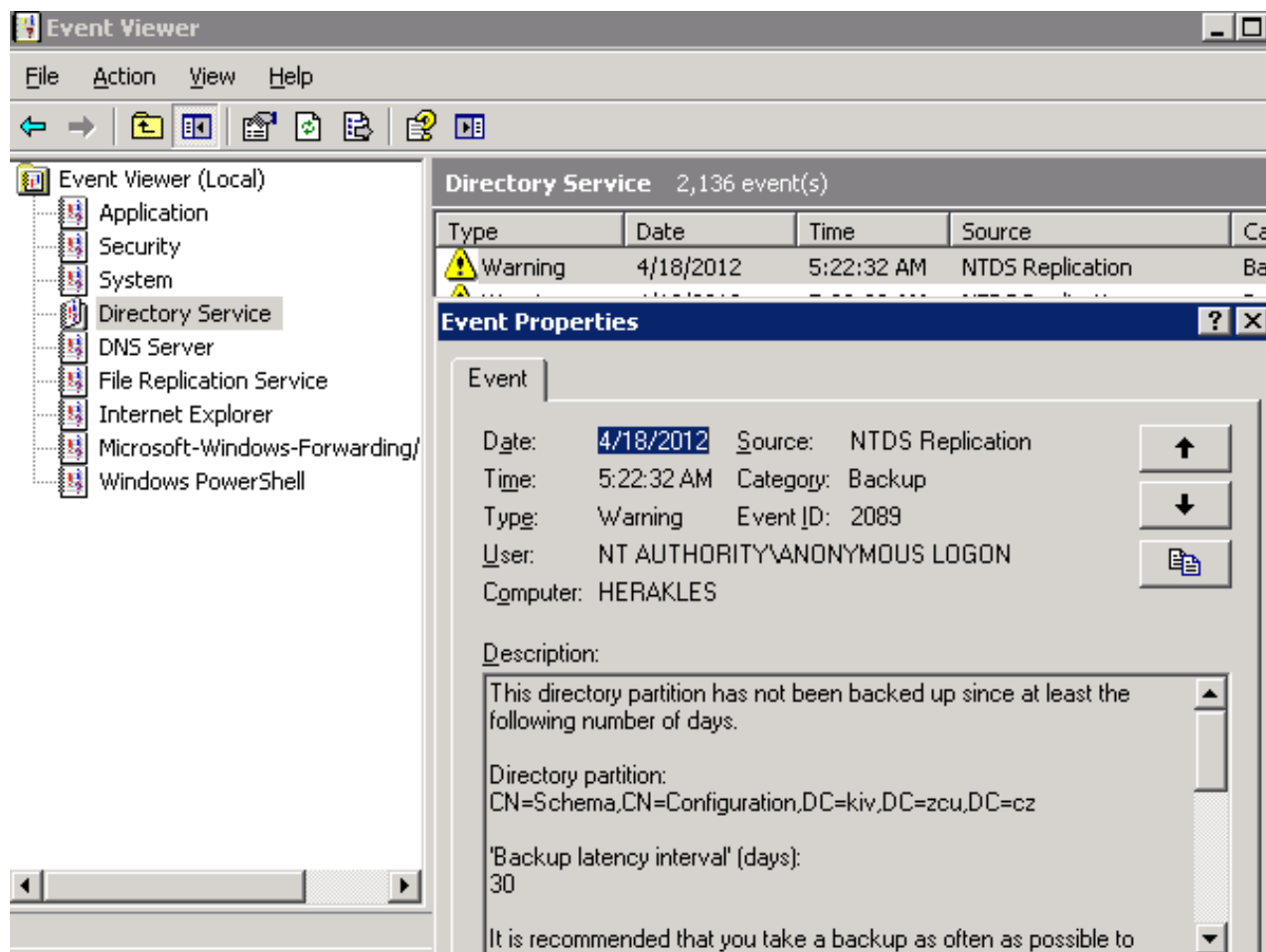
DNS

Domain Naming System locates network services and resources.

DNS Request Process



SLEDOVÁNÍ EVENTLOGU



následující
záznam
informuje o tom,
že je potřeba
adresářové
služby po
určitém počtu
dnů zálohovat

=>
backup
systemstate

INSTALACE AD

dcpromo – instalace/odinstalace AD (Win 2008R2)

- diagnostické nástroje
 - dcdiag
 - netdiag

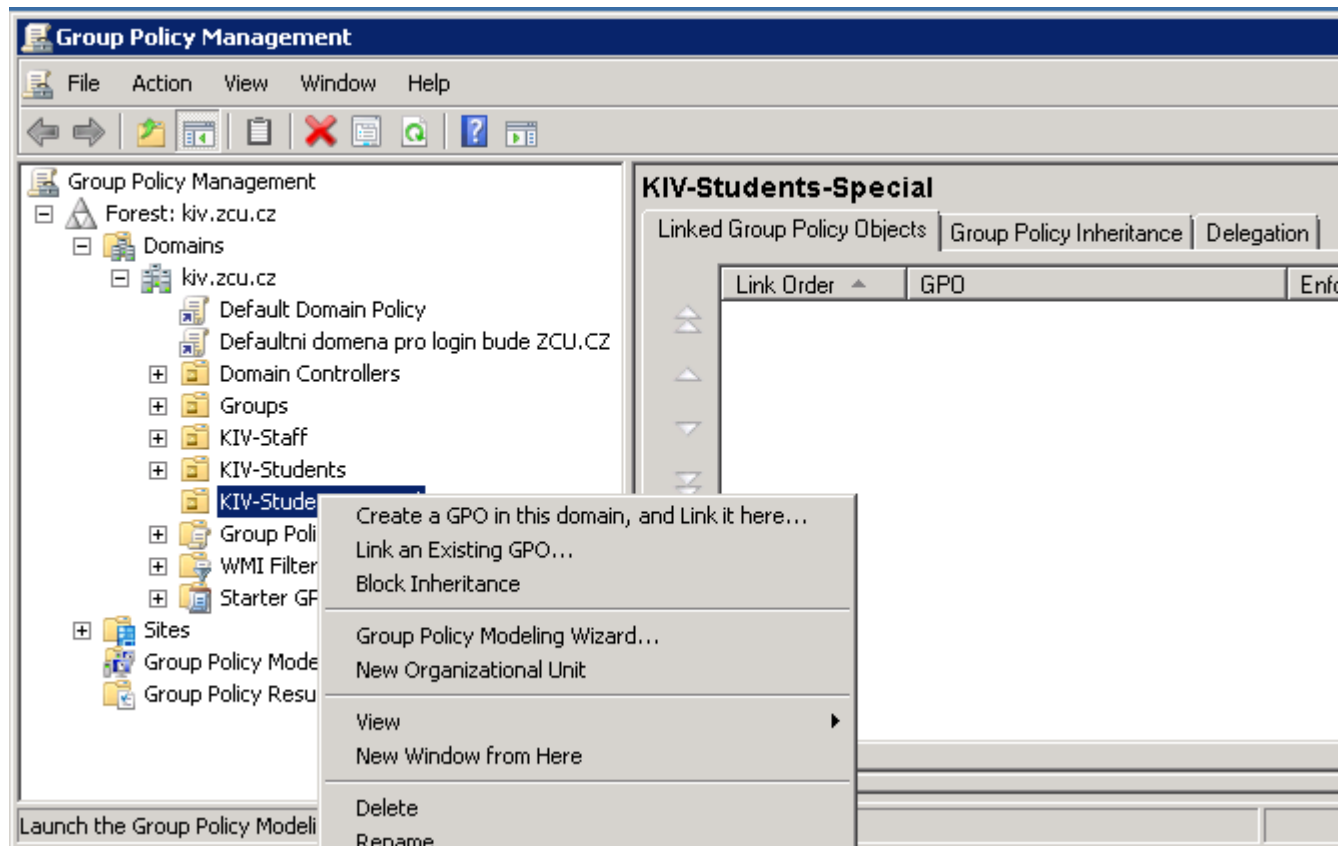
- reportovací nástroje

GROUP POLICY (SKUPINOVÉ POLITIKY)

- Aplikovány při startu PC, přihlášení uživatele
- Periodicky kontrolovány 60-120 minut
- **gpedit.msc**
 - Podrobné vysvětlení u každého nastavení
 - Šablony pro správu
 - Př: kolik předchozích hesel si má systém pamatovat
 - Př: zakázat přístup k ovládacím panelům

APLIKACE POLITIKY V DOMÉNĚ

- Group policy management (**gpmc.msc**)
- vybrat organizační jednotku
- pravá myš – Link Existing GPO



GROUP POLICY

- Instalace aplikací (msi balíčky)
- Zákaz ovládacích panelů
- Defaultní stránka v IE

politiky jsou aplikovány na organizační jednotky (OU) ve formě GPO (Group Policy Object)

SYSTEM CENTER

- Sada nástrojů pro správu sítě s AD
- Configuration Manager
- Operation Manager
- Data Protection Manager
- Virtual Machine Manager
- Essential

*Možnost vyzkoušení ve formě stáhnutí vhd souboru pro virtuál
(obecný trend i u dalších produktů)*

SYSTEM CENTER

- **Správa celého životního cyklu serveru**
 - **Deployment (nasazení)**
 - Splnění HW kritérií, způsob instalace OS, ovladače, konfigurace (sít, domény), updaty, uživatelské aplikace
 - **Správa**
 - Inventarizace hw a sw, Sledování využívání sw(!)
 - Centrální distribuce updatů a aplikací
 - Wake on LAN – instalace – vypnutí
 - **Monitorování**
 - Model zdraví
 - Např. minimální volná kapacita disku $\geq 2\text{GB}$

SYSTEM CENTER

○ Zálohování a Disaster

- **Jaká data** zálohovat
- V jakých **intervalech** zálohovat
- Kolik **verzí** záloh udržovat

- Plná záloha a pak přenos datových rozdílů
 - Na bitové úrovni, změněné bity, ne celé soubory

S využitím materiálu:

<http://www.zive.cz/Clanky/System-Center-pro-serverove-profiky/sc-3-a-145517/default.aspx>

HEALTH MODEL - POŠTA

- distribuovaná aplikace
- health modely DNS, Exchange, AD, HW, ...
- **pohled** na služby ze strany **uživatele**
 - funguje pošta? ano – ne
 - je mu jedno, zda je rozbitá síťová karta X nebo ventilátor Y

SCOM 2012 – System Center Operations Manager

<http://www.zive.cz/clanky/prvni-pohled-na-system-center-operations-manager-2012/sc-3-a-159484/default.aspx>

SCOM 2012

- všechny management servery rovnocenné (rozdělení zátěže, zvýšení dostupnosti)
- operační konzole
- web konzole (Silverlight)
- monitorování sítě (switche, routery)
- aplikační monitoring (ASP.NET aplikace)
- dohled nad Unix/Linux systémy

DEPLOYMENT (= NASAZENÍ) - PODROBNĚJI

- instalace OS
 - sysprep
 - Windows Image (WIM)
 - Windows PE 2.0
 - referenční PC
- instalace ovladačů
- konfigurace OS (sít, doména)
- updaty, service packy
- uživatelské aplikace
- obnovení nastavení, dokumenty, ...

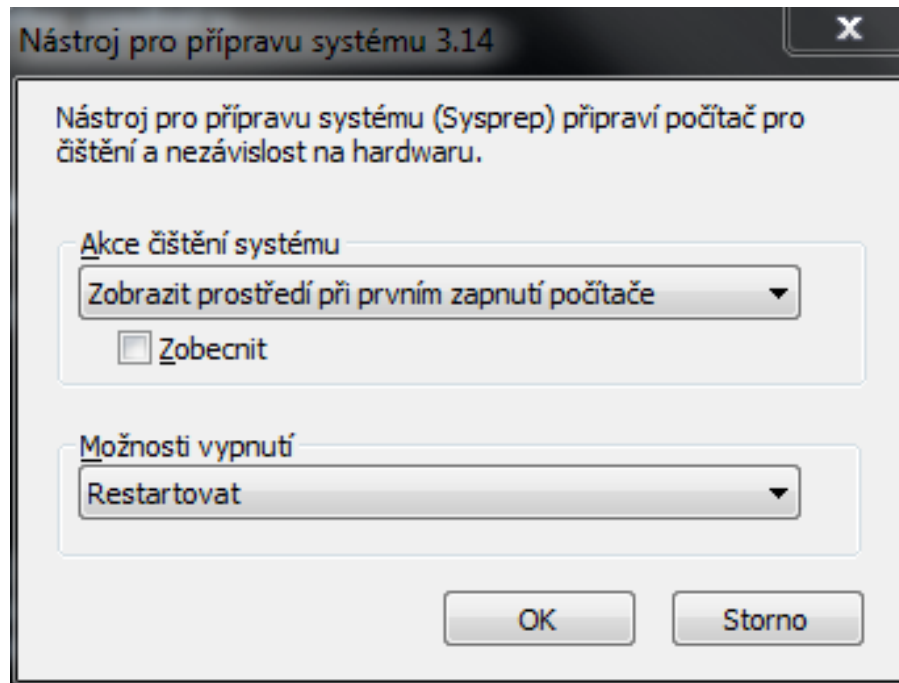
SYSPREP

Připravuje počítač pro klonování (čištění, nezávislost na HW)

- odstraní z image unikátní vlastnosti instalace
- SID (Security Identifier)
- název PC
- odebere z domény
- odinstaluje Plug and play ovladače
- může odstranit event logy
- odstraní body obnovy (restore point)
- odstraní účet místního administrátora
- po první startu bude spuštěn „minisetaup“
- vynuluje časový interval, kdy je možno používat systém bez aktivace

SYSPREP NA WINDOWS 7

C:\Windows\System32\sysprep>sysprep



odpovědní soubor: sysprep /unattend:soubor.xml

KOMPLETNÍ PRŮVODCE INSTALACÍ

<http://www.administratori.cz/instalacni-obraz-win7-pomoci-imagex/>

IMAGEX

- vytvoření diskového obrazu do souboru
- řádkový nástroj

`imagex.exe /capture c: z:\pc.wim “nazev” /verify`

- zachycení image nástrojem `imagex`
- vznikne soubor `.wim`

WINDOWS PE (PREINSTALLATION ENVIRONMENT)

- lze pouštět z CD nebo USB disku
- „Live CD“, cca 160MB
- přístup k NTFS disku

- oprava PC
- avast rescue disk, AVG rescue CD
- BartPE – úprava

- Windows Automated Installation Kit (AIK)
 - pro instalaci např. Windows 7

INSTALACE BĚŽNÉHO SW PRO UŽIVATELE

- <https://ninite.com/>
- vyberete si potřebný sw
 - webové prohlížeče
 - evernote, skype, vlc, PuTTY, WinSCP
 - eclipse, java, teamviewer, truecrypt, gimp
 - openoffice, acrobat reader, 7zip, dropbox
- stáhnete instalátor
- bezobslužná instalace vybraného sw

NINITE - SEZNAM SW

1. Click all the apps you want

You can learn more about a program by hovering over it.

2. Click Get Installer and run it

Ninite installs apps for you in the background. No clicking next. We say NO to toolbars or other junk.

3. Run it again later

Your installer will update apps to the latest versions. If something is up-to-date we'll skip it.

Web Browsers

- ☐ Chrome
- ☐ Opera Chromium
- ☐ Firefox

Other

- ☐ Evernote
- ☐ Google Earth
- ☐ Steam
- ☐ KeePass 2
- ☐ Everything
- ☐ NVDA

Messaging

- ☐ Skype
- ☐ Pidgin
- ☐ Digsby
- ☐ Google Talk
- ☐ Thunderbird
- ☐ Trillian
- ☐ AIM
- ☐ Yahoo!

Developer Tools

- ☐ Python
- ☐ FileZilla
- ☐ Notepad++
- ☐ JDK
- ☐ WinSCP
- ☐ PuTTY
- ☐ WinMerge
- ☐ Eclipse

Media

- ☐ iTunes
- ☐ Hulu
- ☐ VLC
- ☐ KMPlayer
- ☐ AIMP
- ☐ foobar2000
- ☐ Winamp
- ☐ Audacity
- ☐ K-Lite Codecs
- ☐ GOM
- ☐ Spotify
- ☐ CCCP
- ☐ MediaMonkey
- ☐ QuickTime

Runtimes

- ☐ Java
- ☐ .NET
- ☐ Silverlight
- ☐ Air
- ☐ Shockwave

Utilities

- ☐ TeamViewer
- ☐ ImgBurn
- ☐ Auslogics
- ☐ RealVNC
- ☐ TeraCopy
- ☐ CDBurnerXP
- ☐ TrueCrypt
- ☐ Revo
- ☐ Launchy
- ☐ WinDirStat
- ☐ Glary
- ☐ InfraRecorder
- ☐ Classic Start

Imaging

- ☐ Paint.NET
- ☐ Picasa
- ☐ GIMP
- ☐ IrfanView
- ☐ XnView
- ☐ Inkscape
- ☐ FastStone
- ☐ Greenshot

Documents

- ☐ OpenOffice
- ☐ Reader
- ☐ SumatraPDF
- ☐ Foxit Reader
- ☐ CutePDF
- ☐ LibreOffice
- ☐ PDFCreator

Compression

- ☐ 7-Zip
- ☐ PeaZip
- ☐ WinRAR

Security

- ☐ Essentials
- ☐ Avast
- ☐ AVG
- ☐ Malwarebytes
- ☐ Ad-Aware
- ☐ Spybot 2
- ☐ Avira
- ☐ Super

File Sharing

- ☐ qBittorrent
- ☐ eMule

Online Storage

- ☐ Dropbox
- ☐ Google Drive
- ☐ Mozy
- ☐ OneDrive
- ☐ SugarSync
- ☐ BitTorrent Sync

Get Installer

SMALL BUSINESS SERVER

- Komplexní funkcionality pro malé podniky
 - Sdílení souborů
 - Pošta
 - Lokální Intranet
 - Přístup k Internetu

SMALL BUSINESS SERVER 2003

Windows Server

SharePoint Services

Exchange Server (+ Outlook)

Update Services

Shared Fax Services

SQL Server

Internet Security Acceleration (ISA server)

FrontPage 2003 (vývoj webu)

SMALL BUSINESS SERVER 2008

○ Edice Standard

- Windows Server 2008
- Exchange Server 2007
- SharePoint Services 3.0
- Update Services 3.0
- Forefront Security for Exchange Server
- Integration

○ Edice Premium

- SQL Server 2008
- Aj.

SMALL BUSINESS SERVER 2011

- Edice Standard
 - 25 uživatelů
- Edice Essential
 - 75 uživatelů / zařízení
- <http://www.microsoft.com/cze/sbs/produkt/edice/porovnani-funkci.aspx>

SHAREPOINT

- Sdílení a správa informací a dokumentů na webu
- SharePoint Services
- SharePoint Portal Server

Čtenář
Přispěvatel
Webdesigner
Administrator



SCREENSHOT

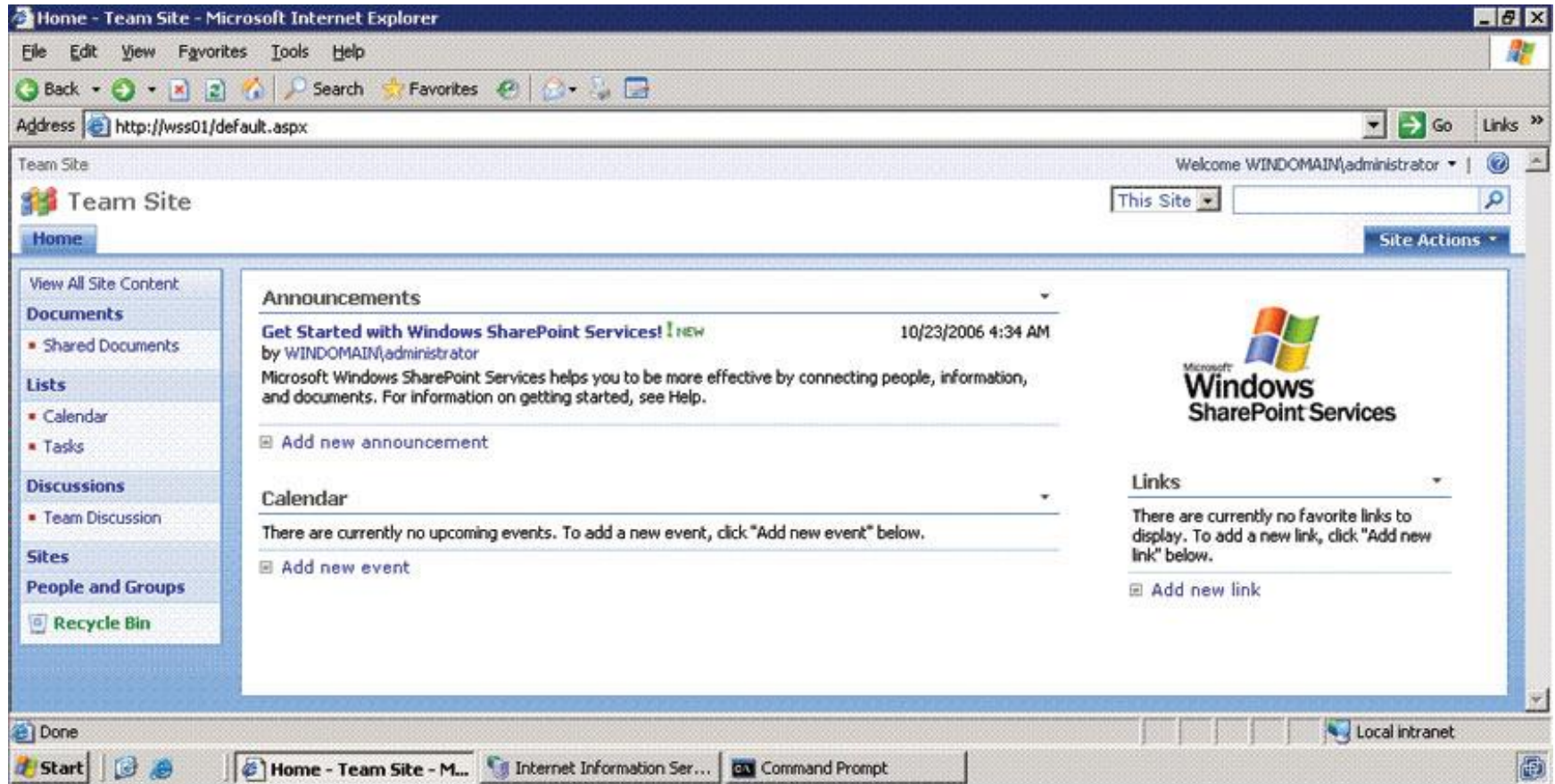


Figure 1: Default Team Site home page

EDICE SHAREPOINTU

- Sharepoint Foundation 2010
 - bezplatný
- Sharepoint Server 2010 standard CAL
- Sharepoint Server 2010 enterprise CAL
- Sharepoint Server 2013
 - online (předplatné) x lokální instalace

vyhledávání:

Search Server 2010 Express

Sharepoint Server 2010

FAST Search Server 2010 for Sharepoint

FUNKČNÍ KATEGORIE

○ list (seznam)

- tabulka pro ukládání strukturovaných informací na webu
- kontakty, kalendáře událostí, ...

○ library (knihovna)

- ukládání dokumentů
- vlastní obsah dokumentu + metadata (název, úprava, autor)

○ web parts

- portlety založené na ASP.NET

○ content types

- jednotné zpracování dokumentů

WORKFLOW

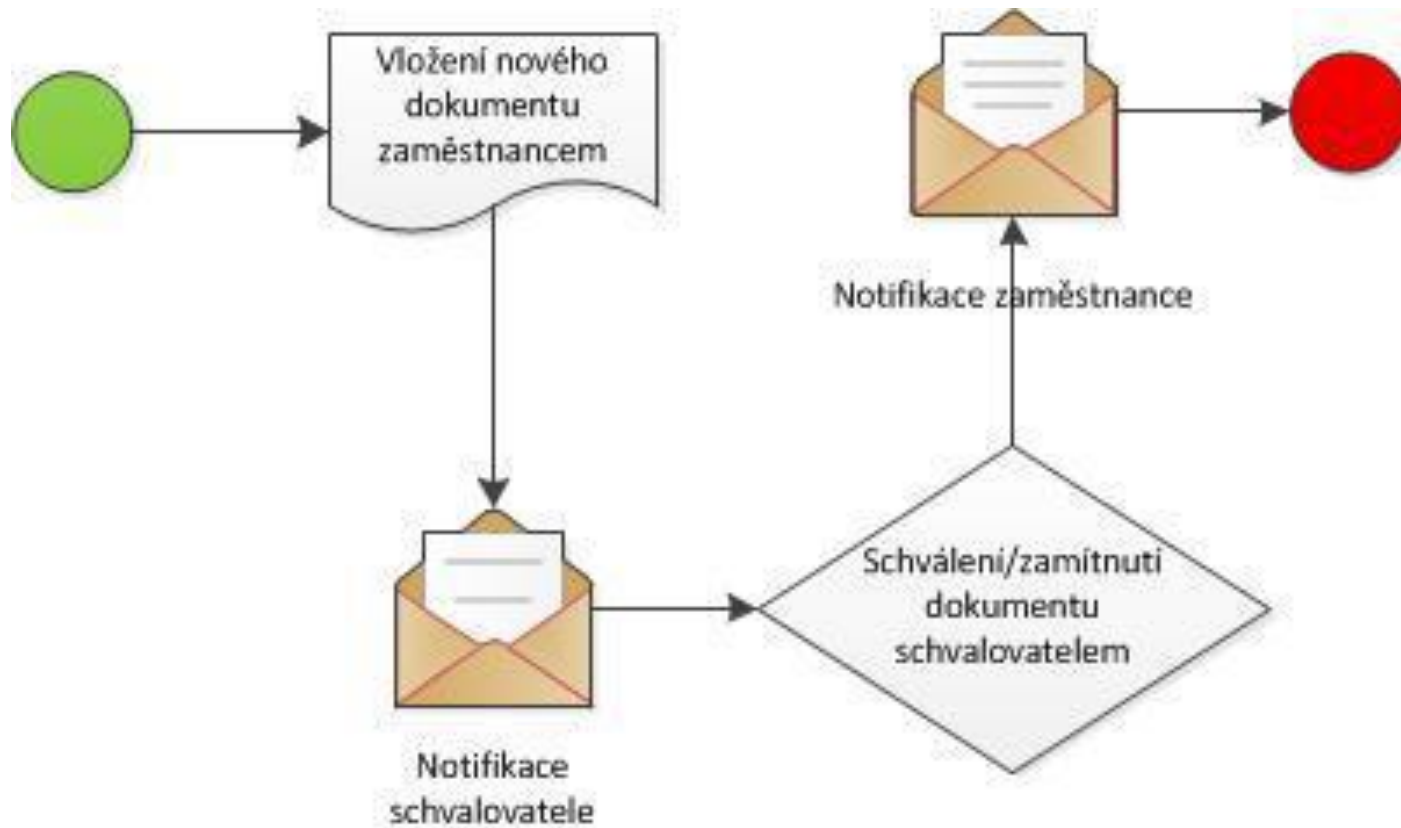
○ příklad workflow:

- schválení dokumentu nadřízeným
- přidání úkolu danému zaměstnanci

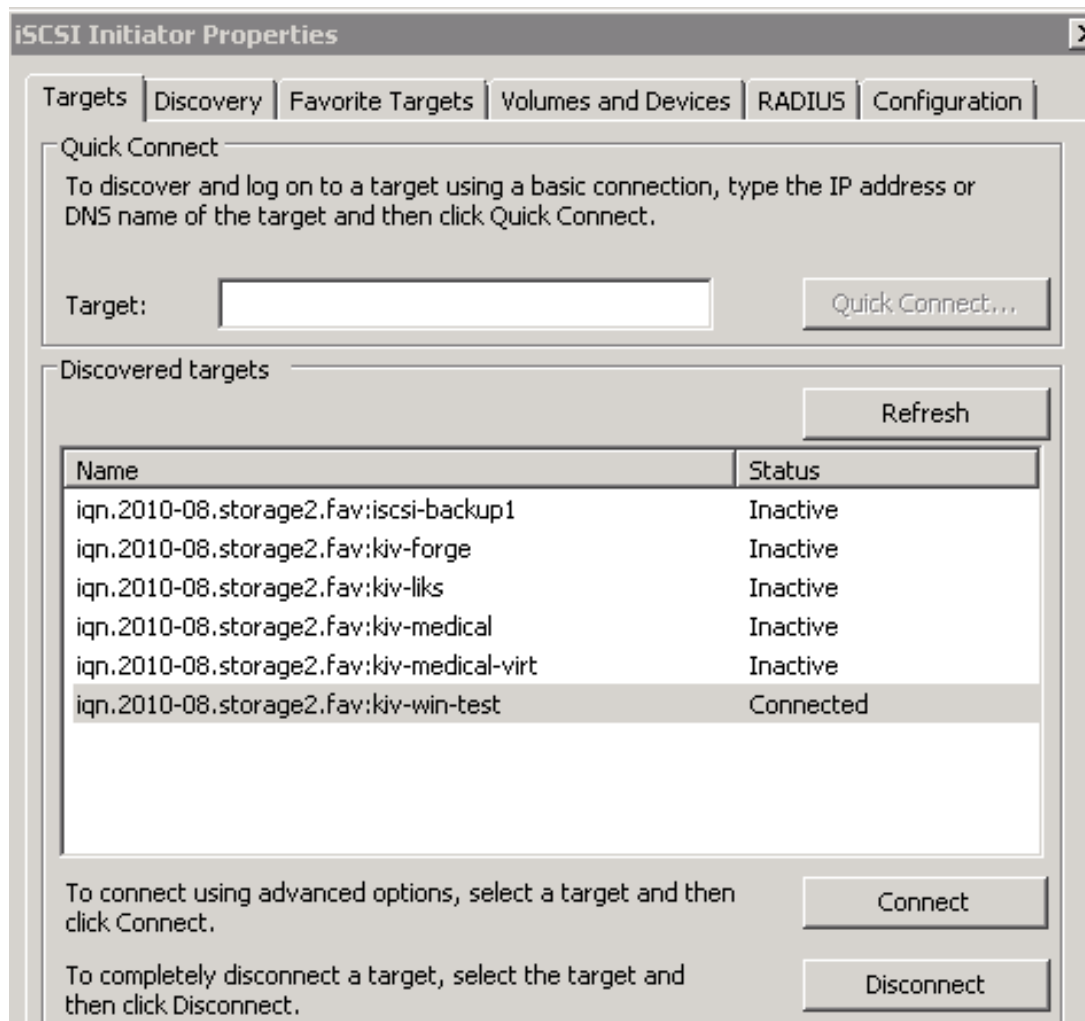
spuštění:

- manuálně
- při vzniku nebo změně položky
- programově

WORKFLOW



PŘIPOJENÍ DISKOVÉHO POLE ISCSI PROTOKOLEM (ISCSI INITIATOR)



Připojení Win
počítače k externímu
iSCSI diskovému poli
prostřednictvím
Ethernetu

Discover target portal
IP adresa, port 3260

zobrazí objevené
targets

možnost použít CHAP

VIRY, ŠKODLIVÝ KÓD

- Nechráněné počítače v síti
 - Chybějící bezpečnostní updaty
 - Slabá hesla (zapomenutá konta)
- Služební notebooky
 - Zavlečení z cizí sítě, domova
- Notebooky návštěvníků firmy
- VPN připojení
 - Přístup do vnitřní sítě
- Činnost uživatele
 - Spouštění neznámého sw, ...

UKÁZKA

- Dell OpenManage Server Administrator
 - Stav RAIDů, senzory
- Webcam
 - Vizuální stav, detektor pohybu, ...
- Active eXperts network monitor
 - Konfigurace testů, intervaly, ...

DELL OPEN MANAGE SERVER

Dell OpenManage Server Administrator

DELL

TYPHOON

Properties

Health | [Information](#) | [System Components \(FRU\)](#) | [Front Panel](#)

System

[-] Main System Ch

- Batteries
- BIOS
- Fans
- Firmware
- Intrusion
- Memory
- Network
- Ports
- Power Supplies
- Processors
- Remote Acces
- Slots
- Temperatures
- Voltages

[+] Software

[+] Storage

Health

Click the component to view its details.

Severity	Component
✓	Batteries
✓	Fans
✓	Hardware Log
✓	Intrusion
✓	Memory
✓	Power Supplies
✓	Processors
✓	Temperatures
✓	Voltages

UKÁZKY

Front Panel LCD Information

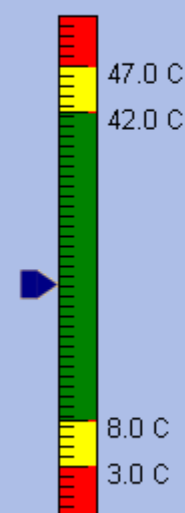
LCD Line 1

Custom

typhoon

Status	Probe Name	Reading	Warning Threshold		Failure Threshold	
			Minimum	Maximum	Minimum	Maximum
✓	System Board FAN 1 RPM	6300 RPM	[N/A]	[N/A]	3450 RPM	[N/A]
✓	System Board FAN 2 RPM	6375 RPM	[N/A]	[N/A]	3450 RPM	[N/A]
✓	System Board FAN 3 RPM	5775 RPM	[N/A]	[N/A]	3450 RPM	[N/A]
✓	System Board FAN 4 RPM	5850 RPM	[N/A]	[N/A]	3450 RPM	[N/A]

✓ System Board Ambient Temp



Status : OK
Reading : 23.0 C
Minimum Failure Threshold : 3.0 C
Maximum Failure Threshold : 47.0 C
Threshold Settings : ☒ Set to Default
 : ☐ Set to Values
Minimum Warning Threshold : 8.0 C
Maximum Warning Threshold : 42.0 C

UKÁZKY

Physical Disks

Status	Name	State	Failure Predicted	Tasks		Bus Protocol	Media
✓	Physical Disk 0:0:0	Online	No	Available Tasks	Execute	SATA	HDD
✓	Physical Disk 0:0:1	Online	No	Blink	Execute	SATA	HDD
✓	Physical Disk 0:0:2	Online	No	Available Tasks	Execute	SATA	HDD

WEBCAM ☺

EDIMAX
NETWORKING PEOPLE TOGETHER

✓ Camera ✓ Pan & Tilt ✓ Network ✓ Motion Detection ✓ System Info. ✓ Account ✓ SDHC

1 2 3 4 5
6 7 8 9 C

Pan/Tilt Speed: 2
Resolution: 1024 x 768
Video Quality: Highest
Video Type: MPEG4
Frame Rate: 15
Frequency: 50 Hz
Flip Mode: Rotate 180
Brightness - +
Volume - +
Multi-Camera Display Apply

The main video feed shows a room with a wooden door, a sink, and some equipment. A yellow warning sign is visible on the door.

VIRTUALIZACE: HYPER-V

- Windows Server 2008 (R2)
 - Nainstalovat roli Hyper-V
 - max 4 jádra, u WS 2012 Hyper-V až 64 procesorů
- Microsoft Hyper-V server
 - Standalone, nevyžaduje nainstalovaný Windows Server 2008
 - Ve skutečnosti je Win2008 server s rolí Hyper-V a ostatní role zakázané
- Od Windows Server 2008 R2 Live Migration
 - Cluster shared volume (CSV)

VIRTUALIZACE

- Windows 8 Professional
 - také obsahuje Hyper-V
 - stejné jádro jako Hyper-V serverové
 - SLAT – second level address translation
 - použití i pro bring your own device
pro připojení dáme zaměstnanci virtuál

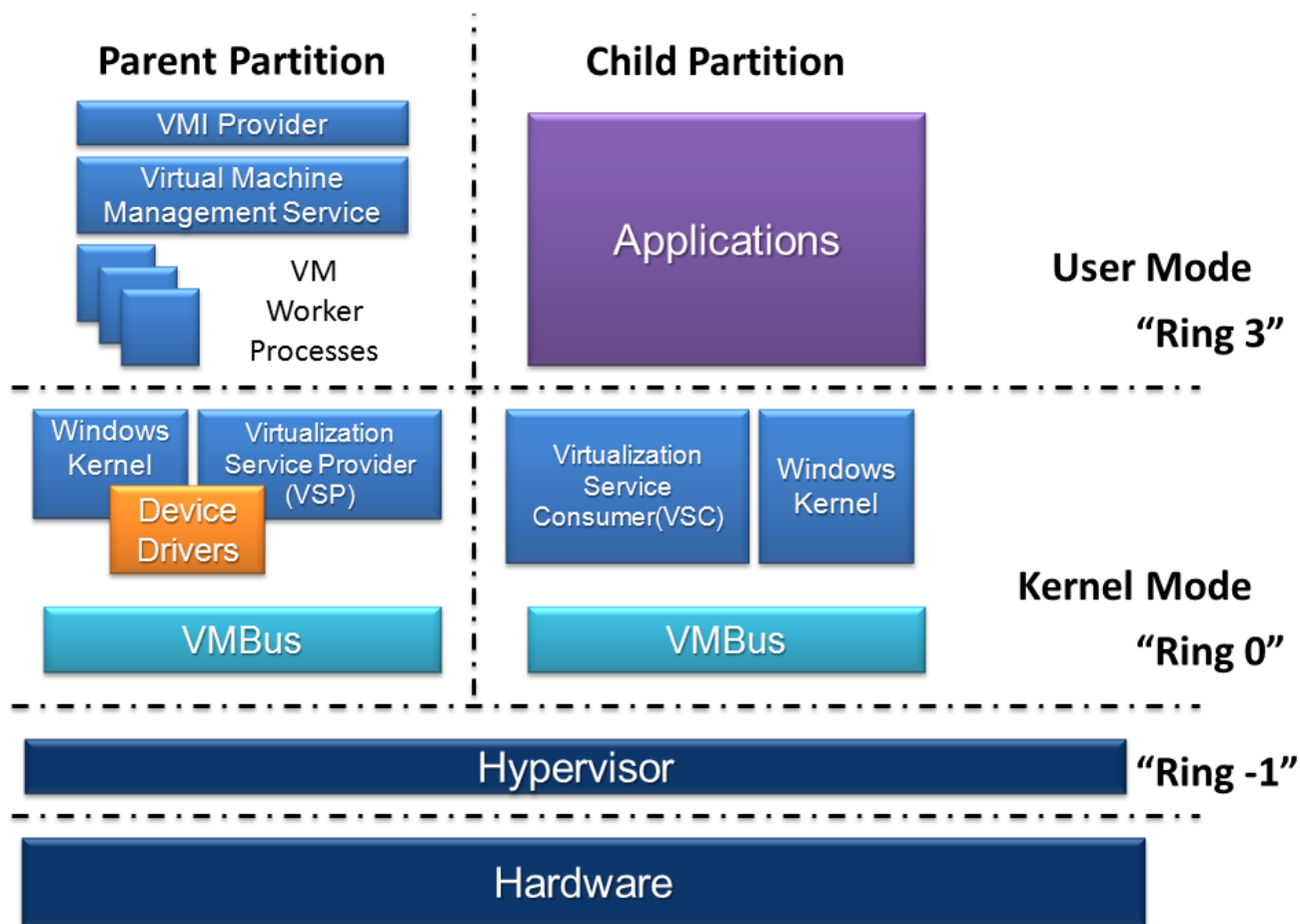
POROVNÁNÍ

Performance in General

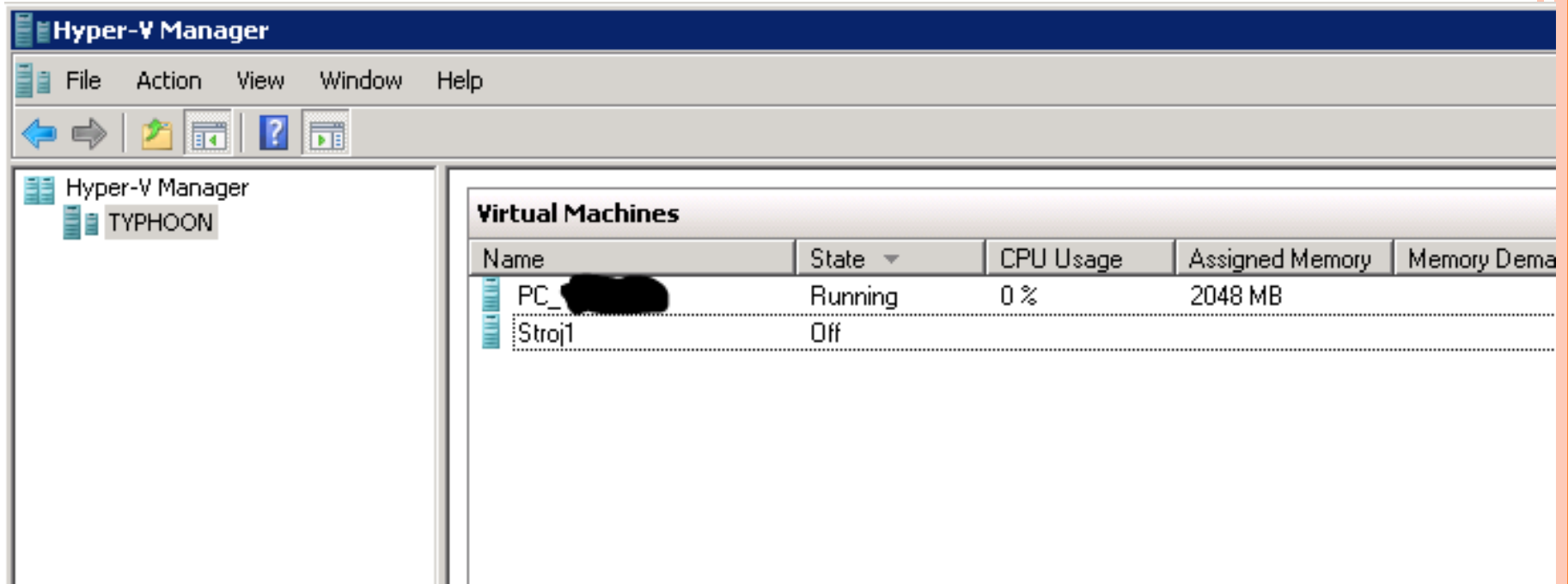
System	Resource	Windows Server 2008 R2 Hyper-V	Windows Server 2012 Hyper-V	Boost
Host	Logical processors	64	320	5×
	Physical Memory	1TB	4TB	4×
	# vCPU	512	2,048	4×
VM	# vCPU	4	64	16×
	Memory per VM	64GB	1TB	16×
	# Active VM	384	1,024	2.7×
Cluster	Max. nodes	16	64	4×
	Max. VMs	1,000	8,000	8×

zdroj: Technet 2013

HYPER-V (OBRÁZEK: WIKIPEDIA)

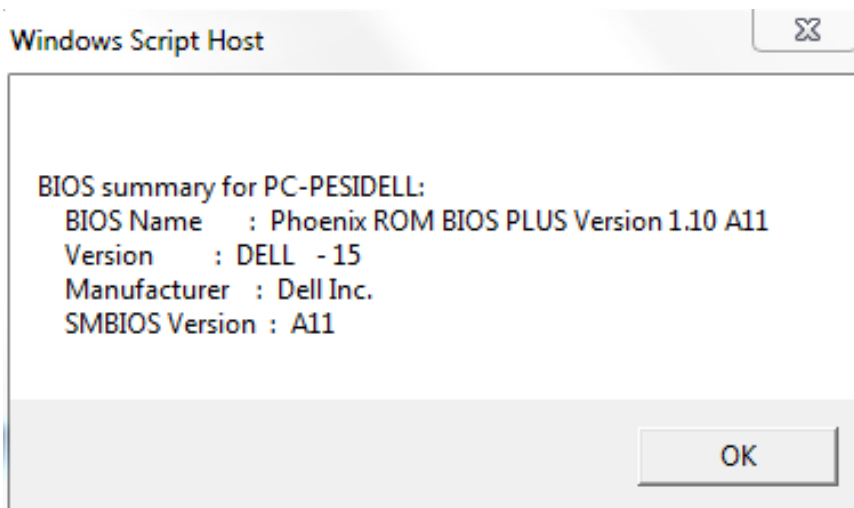


HYPER-V MANAGER



WMI

- Windows Management Instrumentation
- Nástroj pro zjištění informací o systému
 - Běží na baterii? Stav baterky
 - HW konfigurace
 - SW
- <http://www.robvanderwoude.com/wmiexamples.php>
 - zkusit bios.vbs



POWERSHELL

- Založený na OOP a .NET frameworku
- Shell se skriptovací jazykem
 - Exchange 2007 – vše přes příkazovou řádku a GUI rozhraní je postaveno nad ní
- verze 1.0
- verze 2.0
- verze 3.0 (Win 7, Win Server 2008, ...)
- verze 4.0 (Win8.1 int., Win2012ServerR2 ,...)
- připravuje se verze 5.0

Server manager – Feature – Power Shell

POWER SHELL

- také na Windows 7
- Start -> Příslušenství -> Windows Power Shell
Windows Power Shell (řádka)
Windows Power Shell ISE (editor)
- **cmdlet**
příkaz, který manipuluje s objekty v PowerShellu
sloveso-podstatné jméno
get získání hodnoty
set nastavení
format formátuje data
out směrování výstupu

PS

- v PS lze spouštět klasické příkazy
- lze i kombinovat s power shellem

ipconfig | select-string -pattern 147.228

- politka spouštění skriptů
Get-ExecutionPolicy
Set-ExecutionPolicy -ExecutionPolicy unrestricted
get-help about_execution_policies

default – spouštění příkazů, ne skriptů

unrestricted – nepodepsané skripty lze spustit

POWERSHELL

write-host “Ahoj, svete”

man příkaz (Linux)

- **Get-Help** příkaz
- Příkazy .. Cmdlety
- př.: man ls

Roura (|)

- Linux .. proud bytů
- PS .. objektová roura, plně typované objekty

CMDLETS

Sloveso-podstatné jméno

Get-Location	pwd
--------------	-----

Set-Location	cd
--------------	----

Copy-Item	cp
-----------	----

Get-Help	man
----------	-----

Remove-Item	rm, rmdir
-------------	-----------

Rename-Item	mv
-------------	----

Move-Item	mv
-----------	----

Get-Childitem	ls
---------------	----

CMDLETY A ALIASY

Write-Output	echo
Get-Content	cat
Select-String	grep
Get-Process	ps
Stop-Process	kill

Vypište běžící procesy
Pustte notepad
Ukončete přes kill proces notepad

PŘÍKLADY

Get-Date

Get-Date -displayhint time (date,time,datetime)

(Get-Date).AddMinutes(100)

New-TimeSpan \$(Get-Date) \$(Get-Date -month 12 -day 31 -
year 2009)

\$A="Ahoj,svete"

\$A

\$B=5

\$C=7

\$D=\$B+\$C

\$D

GET-COMMAND

- Základní informace o cmdletech
 - get-help je podrobně, např. get-help get-command
- Get-command ipconfig
- Get-command ipconfig | fl
- Get-command dir // a stejně tak ls
- *ipconfig* je **aplikace**
- *dir* je **alias** na *get-childitem*
- *Get-Childitem* je **cmdlet**

NÁPOVĚDA

- Get-process -?
- **Help** get-process
- Help get-process **-full**
 - Výpis nápovědy včetně parametrů
- Get-help about*
- Get-Alias

FUNKCE

- Function cas {Get-Date}
 - Definice funkce
- cas
 - Vyvolani funkce
- Get-Command cas
 - Informace o funkci

FUNKCE S PARAMETRY

```
Function secti($x, $y) {  
    $vysledek = $x + $y  
    Write-Host "Vysledek je $vysledek"  
}
```

Secti 10 15

Vysledek je 25

Get-Command secti | fl

```
Function secti {$args[0] + $args[1]}
```

DATOVÉ TYPY

typ	popis
[int]	32-bit signed integer
[long]	64-bit signed integer
[string]	Fixed-length string of Unicode characters
[char]	A Unicode 16-bit character
[byte]	An 8-bit unsigned character
[bool]	Boolean True/False value
[decimal]	An 128-bit decimal value
[single]	Single-precision 32-bit floating point number
[double]	Double-precision 64-bit floating point number
[xml]	Xml object
[array]	An array of values
[hashtable]	Hashtable object

FUNKCE S DATOVÝM TYPEM

```
Function Vek {  
    Param( [int] $x)  
  
    Write-Host "Je ti $x let"  
}
```

Vek 20

Vek A .. Chyba

Defaultní hodnota: Param ([int] \$x=18)

Data z roury: \$input

INFO O PROCESECH

Get-Process

Get-Process dns

Get-Process dns,winlogon

Get-Process w*

Get-Process w* | Select-Object
name,fileversion,company

PRÁCE SE SLUŽBAMI

Get-Service DNS

Get-Service –displayname “DNS Server”

Stop-Service dns

Start-Service dns

Restart-Service jedna,dve

suspend-service dns

resume-service dns

SLUŽBY

- Pozastavení x zastavení služby

Set-Service clipsrv -startuptype "manual"
(automatic,disabled)

DALŠÍ - WMI

Get-WmiObject win32_bios

SMBIOSBIOSVersion : VirtualBox

Manufacturer : innotek GmbH

Name : Default System BIOS

SerialNumber : 0

Version : VBOX - 1

Get-WmiObject win32_bios | get-member
get-help Get-WmiObject -examples | more

WMI

- `Get-WmiObject win32_process | more`
- `get-wmiobject win32_service -computename 127.0.0.1`
- `get-wmiobject -query "select * from win32_service where name='WinRM' " -computename server01, server02`

PRÁCE S LOGY

```
get-eventlog -list
```

```
get-eventlog system
```

```
Get-EventLog system -newest 3
```

```
Get-EventLog system -newest 3 | Format-List
```

```
Get-EventLog "Windows PowerShell" | Where-Object  
{$_.EventID -eq 403}
```

SPUŠTĚNÍ PROGRAMU

notepad

Invoke-Item c:\windows\system32\calc.exe

Invoke-Item c:\scripts*.txt

Measure-Command {calc.exe}

\$A="ahoj"

\$B="Cau"

Compare-Object \$A \$B

InputObject

SideIndicator

Cau

=>

ahoj

<=

POWERSHELL

Copy-Item c:\scripts c:\test -recurse

New-Item c:\scripts\new_file.txt -type file

New-Item c:\scripts\Windows PowerShell -type directory

\$(Get-Item hkcu:\software).subkeycount

Test-Path

HKCU:\Software\Microsoft\Windows\CurrentVersion

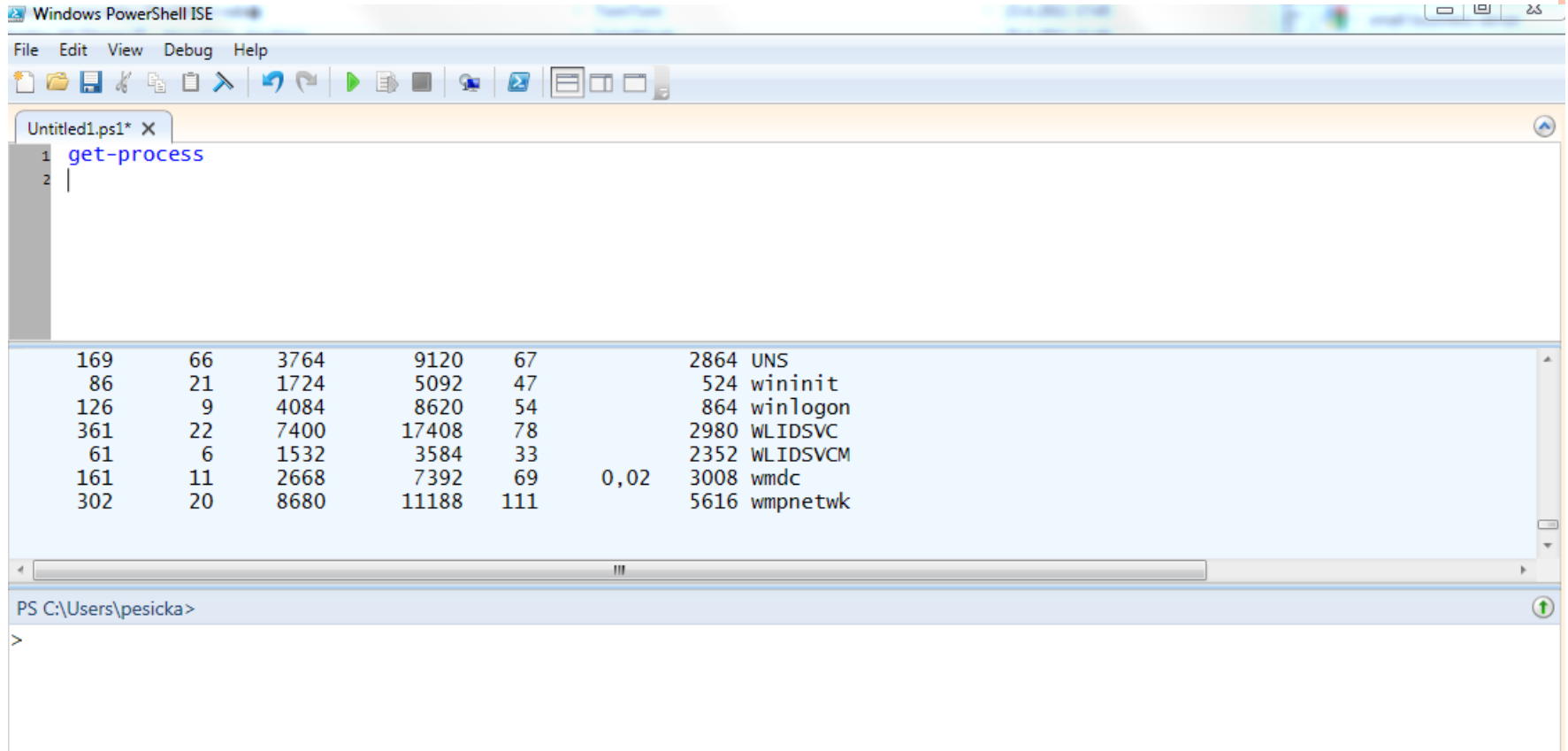
powershell.exe -file c:\my scripts\test.ps1

UKÁZKA SPUŠTĚNÍ SKRIPTU

```
C:\Users\pesicka>
C:\Users\pesicka>
C:\Users\pesicka>
C:\Users\pesicka>powershell.exe -file "c:\!!spos2011\skript01.ps1"
Name                : Phoenix ROM BIOS PLUS Version 1.10 A08
Version             : DELL - 15
Manufacturer        : Dell Inc.
SMBIOSBIOS Version  : A08

C:\Users\pesicka>
```

WINDOWS POWERSHELL ISE



The screenshot shows the Windows PowerShell ISE interface. The menu bar includes File, Edit, View, Debug, and Help. The toolbar contains icons for file operations and execution. The editor window, titled 'Untitled1.ps1', contains the command 'get-process' on line 1. The console window at the bottom displays the output of the command, which is a table of running processes. The table has columns for PID, PPID, Working Set, Private Bytes, Session ID, Name, and CPU. The processes listed are UNS, wininit, winlogon, WLIDSVC, WLIDSVC, WLIDSVC, wmdc, and wmpnetwk. The CPU column shows values for each process, with '0,02' for wmdc.

```
1 get-process
2
```

PID	PPID	Working Set	Private Bytes	Session ID	Name	CPU
169	66	3764	9120	67	2864 UNS	
86	21	1724	5092	47	524 wininit	
126	9	4084	8620	54	864 winlogon	
361	22	7400	17408	78	2980 WLIDSVC	
61	6	1532	3584	33	2352 WLIDSVC	
161	11	2668	7392	69	3008 wmdc	0,02
302	20	8680	11188	111	5616 wmpnetwk	

PS C:\Users\pesicka>

POUŽITÉ MATERIÁLY

Zpracováno s využitím materiálů dostupných na Internetu (wikipedia, samuraj.cz aj.)

<http://www.powershellpro.com/powershell-tutorial-introduction/powershell-functions-filters/>