

Instalace AD, single sign-on

Šimon Suchomel, David Leška

Prerekvizity

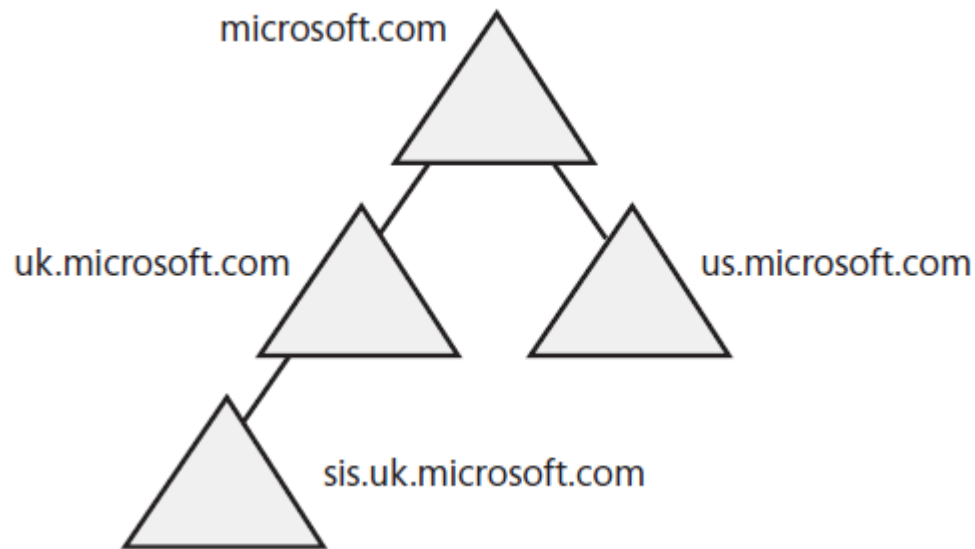
- Server 0 a 1 vyvolat instalaci aktualizací, volitelně i další stroje.

Motivace, pojmy

- Jeden zdroj identit a dalších informací (např. tiskárny, politiky = konfigurace).
- AD je postavena na otevřených protokolech LDAP, Kerberos, DNS. Možnost propojení s jinými systémy.
- Doména je jedna instance AD.
- Doménový řadič je stroj hostující databázi a služby AD.
- Doména má hierarchickou strukturu s definicí práv podobně jako třeba filesystem.

Logická struktura AD

- Tree (strom)
 - Je hierarchické spojení domén, vytvoření vztahem rodič-potomek
 - Domény ve stromě sdílí souvislý DNS namespace



Instalace AD – požadavky

- Windows Server
- Administrátorský přístup
- DNS (a NetBIOS) jméno domény – *login.local*
 - Možná instalace nového DNS serveru
- Statickou IP adresu
- Pokud v prostředí běží starší verze AD, musí být připravená na provoz nového řadiče s Windows Server 2012 za použití Adprep.exe

Úkoly – instalace DC

- Přejmenujeme server1 na DC1 (reboot!)
- Přidáme roli AD Domain Services na server1
- Power Shell nebo GUI Server Manager
- Vyberete roli **Active Directory Domain Services** Pozor je jich tam více s podobným názvem.
- **Restart** i když není vyžádán!

Instalace AD role

Add Roles and Features Wizard

DESTINATION SERVER
dc2.ad.local

Select server roles

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

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

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

< Previous Next > Install Cancel

Úkoly – instalace DC

- Tímto je pouze nainstalovaná role, je nutné provést konfiguraci – povýšení stroje na doménový řadič.
- **Pro jméno AD vybrat nekonfliktní s existujícími DNS doménami!**
- Post-deployment Configuration in Server Manager – konci ukáže odpovídající příkaz v PowerShellu.
 - Promote this server to a domain controller
 - Add a new forest
 - Funkční úroveň – probírané později
 - lesa: Windows Server 2016
 - domény: Windows Server 2016
 - Heslo pro obnovu AD (DSRM)
 - není heslo pro doménového správce = nepoužívá se v produkčním prostředí
 - nelze změnit, pokud není dostupná databáze AD! – napsat na bezpečné místo
 - pro cvičení použijte heslo Pa\$\$w0rd
 - Nová DNS zóna integrovaná do AD

Povýšení DC1 1

The screenshot shows the Server Manager interface. The top navigation bar includes 'Server Manager' and 'Dashboard'. A task pane is open, displaying two tasks with yellow warning icons:

- Post-deployment Configura...**
Configuration required for DHCP Server at DC2
[Complete DHCP configuration](#)
- Post-deployment Configuration**
Configuration required for Active Directory Domain Services at DC2
[Promote this server to a domain controller](#)

Red arrows point from the 'Manage' button in the top right and the 'Promote this server to a domain controller' link in the task pane.

The main dashboard area is titled 'WELCOME TO SERVER MANAGER' and contains a 'QUICK START' section with the following steps:

- 1 Configure this local server
- 2 Add roles and features
- 3 Add other servers to manage
- 4 Create a server group
- 5 Connect this server to cloud services

Below this is the 'ROLES AND SERVER GROUPS' section, showing a summary of roles and server groups. The roles listed are AD DS, DHCP, and File and Storage Services, each with a 'Manageability' status and a list of sub-items (Events, Services, Performance, BPA results). The server groups listed are Local Server and All Servers, each with a 'Manageability' status and a list of sub-items (Events, Services, Performance, BPA results).

Povýšení DC1 2

The screenshot shows the 'Active Directory Domain Services Configuration Wizard' window. The title bar includes the application name and standard window controls. The main area is titled 'Deployment Configuration'. On the right, it indicates the 'TARGET SERVER' as 'pv176-server-0'. A left-hand navigation pane lists several steps: 'Deployment Configuration' (highlighted in blue), 'Domain Controller Options', 'Additional Options', 'Paths', 'Review Options', 'Prerequisites Check', 'Installation', and 'Results'. The main content area is divided into two sections. The first section, 'Select the deployment operation', contains three radio button options: 'Add a domain controller to an existing domain', 'Add a new domain to an existing forest', and 'Add a new forest' (which is selected). The second section, 'Specify the domain information for this operation', contains a text box labeled 'Root domain name:' with the value 'ad.local' entered. At the bottom of the window, there are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'. A link for 'More about deployment configurations' is located at the bottom left of the main content area.

Active Directory Domain Services Configuration Wizard

Deployment Configuration

TARGET SERVER
pv176-server-0

Deployment Configuration

Domain Controller Options

Additional Options

Paths

Review Options

Prerequisites Check

Installation

Results

Select the deployment operation

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

Specify the domain information for this operation

Root domain name:

[More about deployment configurations](#)

< Previous Next > Install Cancel

Povýšení DC1 3

Active Directory Domain Services Configuration Wizard

Domain Controller Options

TARGET SERVER
pv176-server-0

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

Select functional level of the new forest and root domain

Forest functional level: Windows Server 2016

Domain functional level: Windows Server 2016

Specify domain controller capabilities

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

Type the Directory Services Restore Mode (DSRM) password

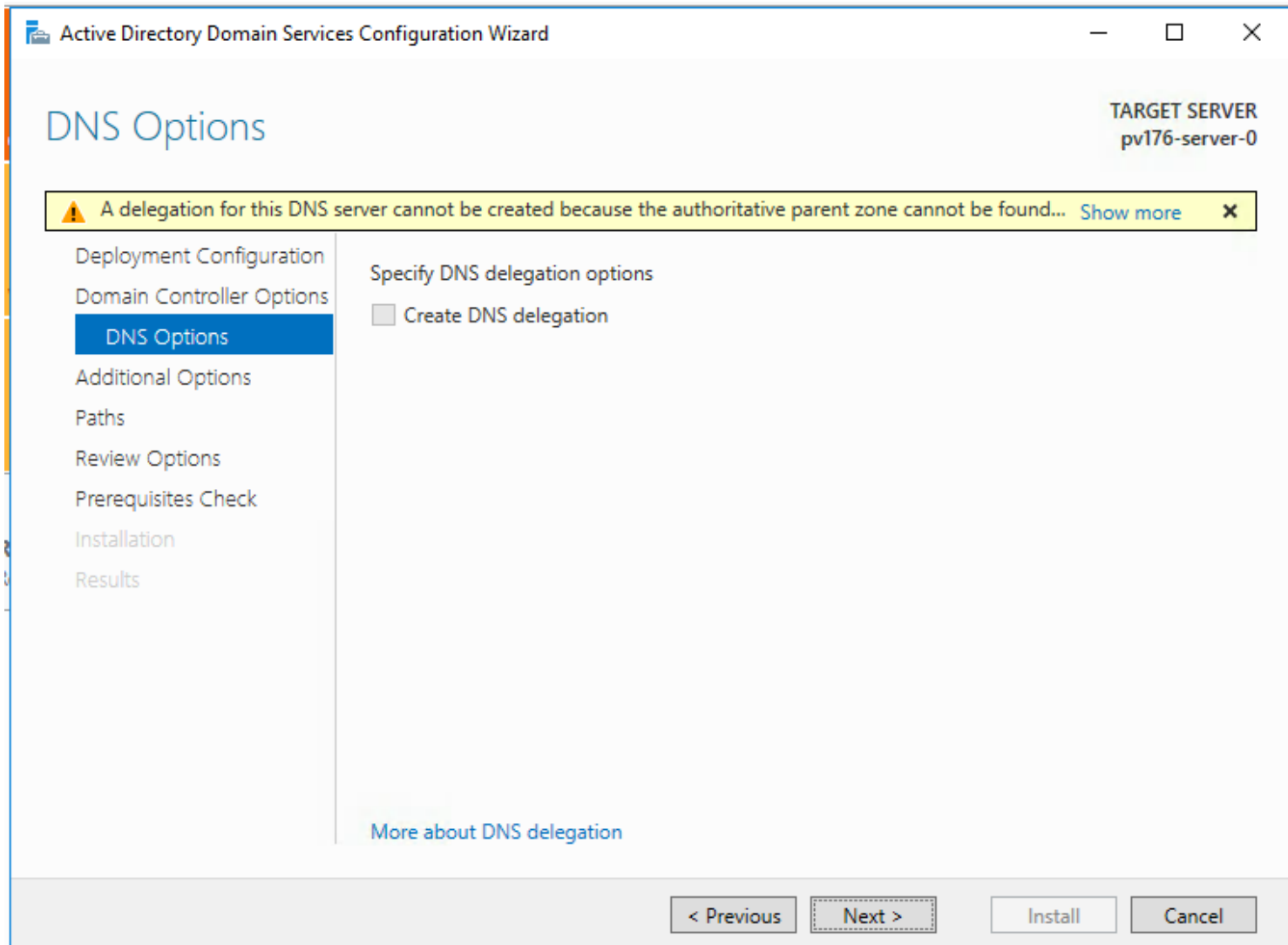
Password:

Confirm password:

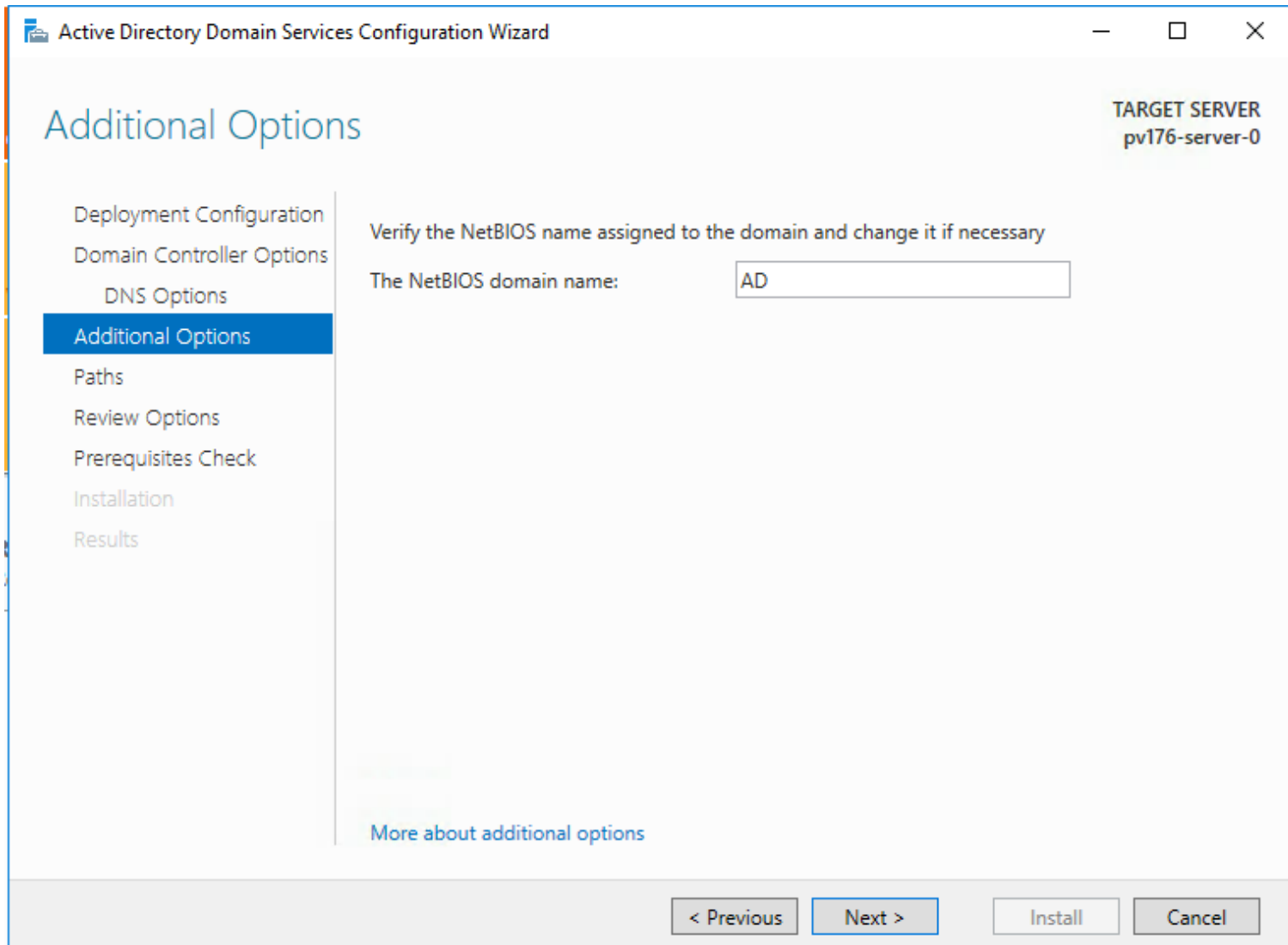
[More about domain controller options](#)

< Previous Next > Install Cancel

Povýšení DC1 4



Povýšení DC1 5



Povýšení DC1 6

Active Directory Domain Services Configuration Wizard

Paths

TARGET SERVER
pv176-server-0

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

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

Database folder: C:\windows\NTDS ...

Log files folder: C:\windows\NTDS ...

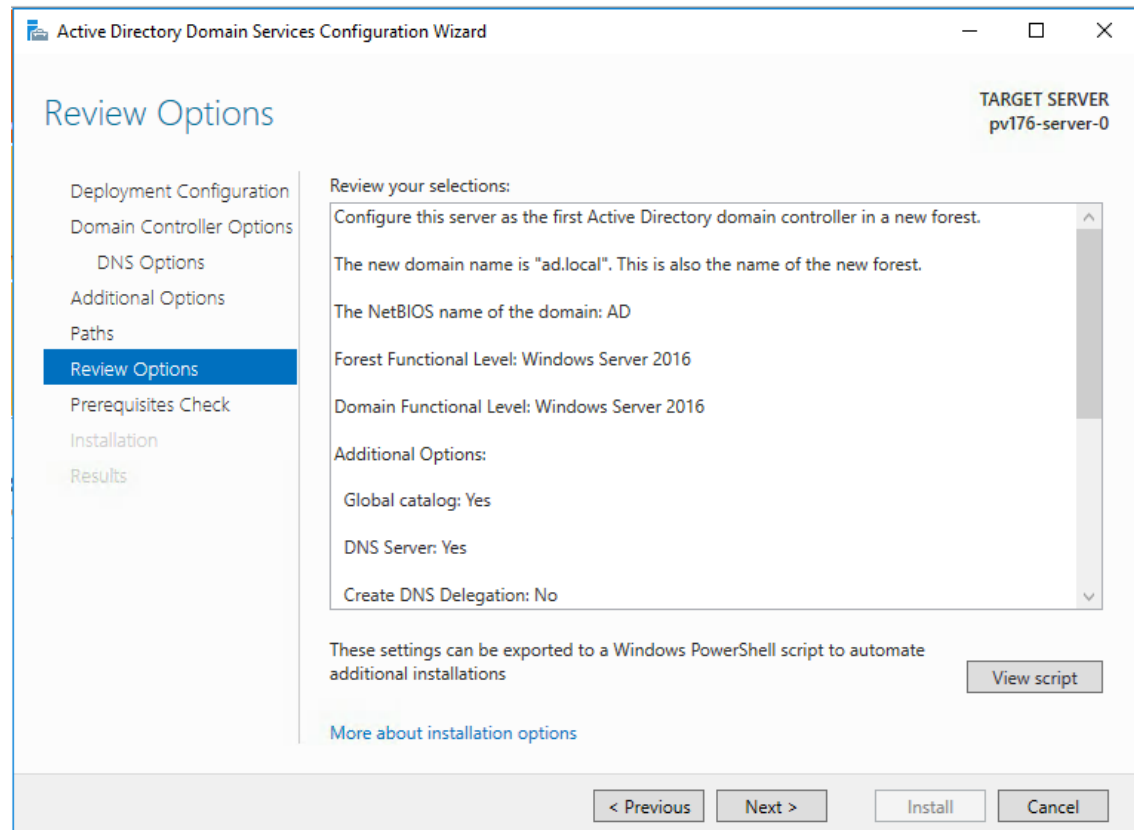
SYSVOL folder: C:\windows\SYSVOL ...

[More about Active Directory paths](#)

< Previous Next > Install Cancel

Povýšení DC1 7

- Všichni zmáčknou View Script a prohlédnou si kód v PowerShellu



Povýšení DC1 8

```
#  
# Windows PowerShell script for AD DS Deployment  
#
```

```
Import-Module ADDSDeployment  
Install-ADDSForest `  
-CreateDnsDelegation:$false `  
-DatabasePath "C:\windows\NTDS" `  
-DomainMode "WinThreshold" `  
-DomainName "ad.local" `  
-DomainNetbiosName "AD" `  
-ForestMode "WinThreshold" `  
-InstallDns:$true `  
-LogPath "C:\windows\NTDS" `  
-NoRebootOnCompletion:$false `  
-SysvolPath "C:\windows\SYSTEM32\sysvol" `  
-Force:$true
```

Povýšení DC1 9

Active Directory Domain Services Configuration Wizard

Prerequisites Check

TARGET SERVER
pv176-server-0

✓ All prerequisite checks passed successfully. Click 'Install' to begin installation. [Show more](#)

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

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

[Rerun prerequisites check](#)

View results

⚠ Windows Server 2016 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.

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

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

⚠ If you click Install, the server automatically reboots at the end of the promotion operation.

[More about prerequisites](#)

< Previous Next > Install Cancel

Povýšení DC1 10

- Následuje instalace a po ní automatický restart.
- Restart trvá delší dobu, použijte konzolový přístup, abyste věděli, že váš server nastartoval.
- Po přihlášení kontrola DNS serveru ve vlastnosti sítě, pokud je tam 127.0.0.1, dát tam adresu interního interface 10.x.x.x

složka NTDS

- C:\Windows\NTDS
- Ntds.dit
 - databázový soubor Active Directory
 - obsahuje všechny objekty AD na doménovém řadiči
- Edb*.log
 - logovací soubor databázových transakcí
- Edb.chk
 - soubor s checkpointy transakcí
 - ukazuje, které transakce z logu, byly zapsány do Active Directory

složka SYSVOL

- C:\Windows\NTDS
- obsahuje systémový svazek, který bude sdílen a replikován mezi všemi doménovými řadiči
- obsahuje veškeré skupinové politiky domény

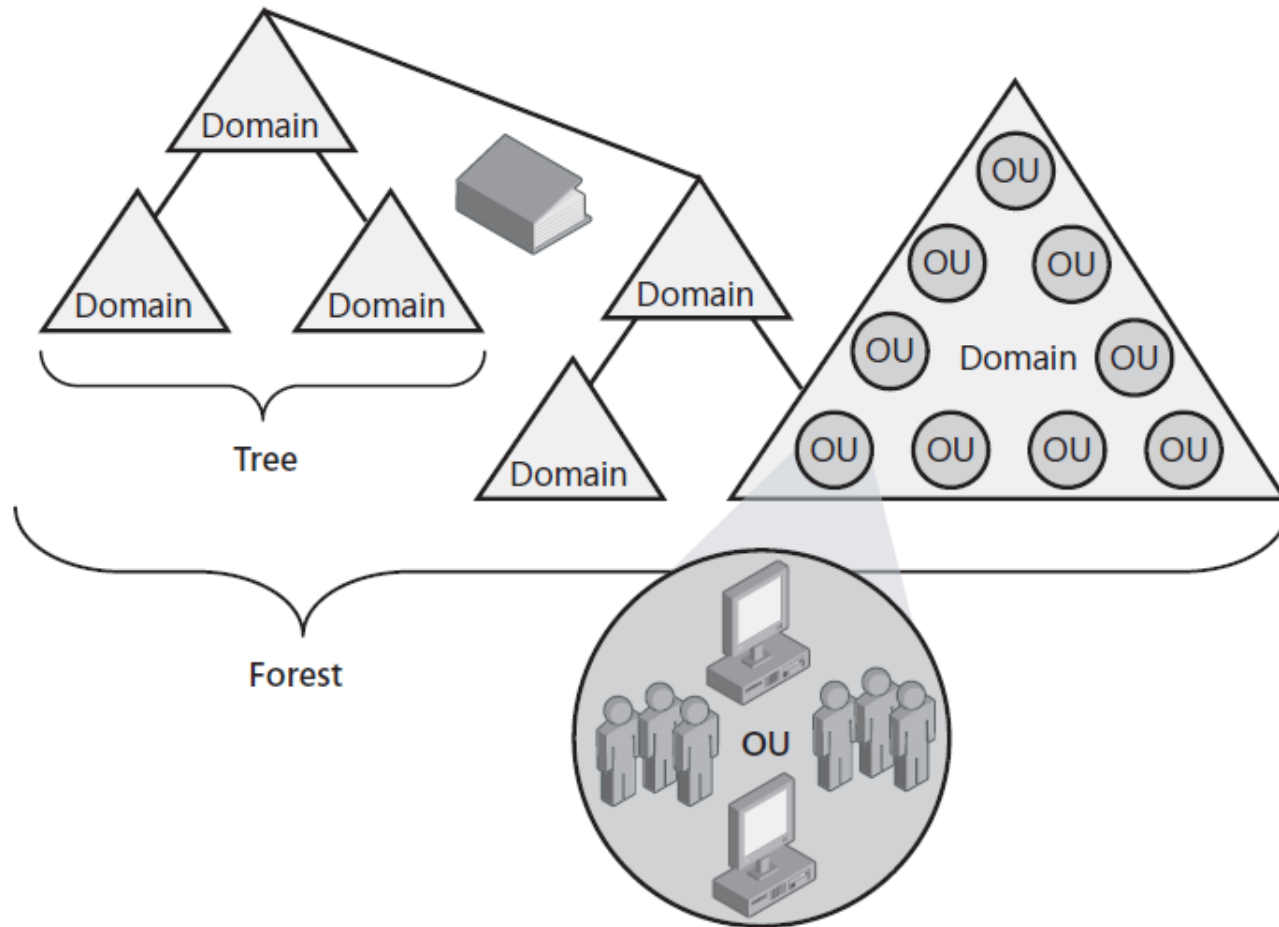
Kontrolní otázka

- Po přidělení nové IP adresy určitému počítači jste zjistili, že místní DNS server špatně překládá jméno tohoto počítače ze své lokální cache. Jak tento problém vyřešíte?
 - a) Na DNS serveru spustíte `dnscmd /clearcache`
 - b) Restartujete službu DNS klient na klientském počítači
 - c) Na klientském počítači spustíte `ipconfig /flushdns`
 - d) Restartujete všechny DNS klientské počítače

Globální katalog (GC)

- Doménový řadič s rozšířenou databází
 - Kromě všech atributů objektů z vlastní domény obsahují i omezenou množinu atributů všech objektů z celého lesa
 - Nutné pro přihlášení uživatelů
 - Umožňují rychlé vyhledávání v objektech lesa
- Real world practice: GC ze všech DC

Logická struktura AD – pokračování



Uživatelské účty

- Lokální
 - Uložený lokálně na počítači
 - Pro interaktivní přihlášení lze použít pouze na tom počítači
- Doménový
 - Uložený na doménovém řadiči
 - Lze se s ním přihlásit na všechny doménové počítače, pokud to práva umožňují
 - Doménové řadiče nemají lokální účty, ale ostatní počítače zařazené v doméně je mít mohou

Úkoly

- Přihlášení na DC
- Uvědomit si, že neexistují lokální účty
- Dostupnost domény z jiných počítačů – DNS překlad (+ping) jména domény

- mmc snap in – AD Users and Computers (dsa.msc)
- Delegate Control Wizard zjednodušení definice ACL v doméně
- AD Administrative Centrum, umí doménový odpadkový koš
- ADSI Editor, low level

- DNS snap in – prohlídka SRV záznamů, ukázka koexistence různých typů zón na jednom DNS serveru.

- Instalace 2. řadiče domény
 - Add a domain controller to an existing domain

Povýšení DC2 1

- Přejmenovat server na DC2, reboot.
- Nastavit ve vlastnostech sítě první server jako DNS server!!!!!!
- Otestovat, že se resolvuje jméno domény na IP adresu prvního řadiče: nslookup ad.local
- Přidat server do domény, reboot.

Povýšení DC2 2 přidání do domény

The screenshot displays the Windows Server Manager interface for a server named 'dc2'. The 'PROPERTIES' pane shows the current configuration: Computer name 'dc2', Workgroup 'WORKGROUP', and various system settings like Windows Firewall (Public: On) and Windows Defender (Real-Time Protection: On). A red arrow points from the 'WORKGROUP' text to the 'System Properties' dialog box.

The 'System Properties' dialog box is open, showing the 'Computer Name' tab. It displays the current 'Full computer name' as 'dc2' and 'Workgroup' as 'WORKGROUP'. A red arrow points from the 'Change...' button to the 'Computer Name/Domain Changes' dialog box.

The 'Computer Name/Domain Changes' dialog box is open, showing the 'Member of' section. The 'Domain' radio button is selected, and the text box contains 'ad.local'. The 'Workgroup' radio button is unselected, and its text box contains 'WORKGROUP'. The 'OK' and 'Cancel' buttons are visible at the bottom.

Povýšení DC2 3

- Po rebootu se přihlásit jako doménový administrátor **Administrator@ad.local**
- Nainstalovat ze server manager roli **Active Directory Domain Services** nesplést s jinými podobně pojmenovanými.
- Reboot bez ohledu na to, zda byl požadován.
- Jdeme povyšovat – pozor některé věci budou jinak, protože nebudeme vytvářet novou doménu, ale přidávat kontroler do stávající!

Povýšení DC2 4

The screenshot shows the Server Manager interface. The main dashboard area displays a 'WELCOME TO SERVER MANAGER' section with a 'QUICK START' list of five steps: 1. Configure this local server, 2. Add roles and features, 3. Add other servers to manage, 4. Create a server group, and 5. Connect this server to cloud services. Below this is the 'ROLES AND SERVER GROUPS' section, which shows a grid of server roles and groups. The roles listed are AD DS, DHCP, and File and Storage Services, each with a 'Manageability' icon and a count of 1. The server groups listed are Local Server and All Servers, each with a 'Manageability' icon and a count of 1. A task pane is open on the right side of the dashboard, showing two tasks: 'Post-deployment Configuration' for DHCP Server at DC2 and 'Post-deployment Configuration' for Active Directory Domain Services at DC2. The second task has a link to 'Promote this server to a domain controller', which is highlighted by a red arrow. Another red arrow points to the 'Manage' button in the top right corner of the Server Manager window.

Server Manager Dashboard

Server Manager Dashboard

Dashboard

- Local Server
- All Servers
- AD DS
- DHCP
- File and Storage Services

WELCOME TO SERVER MANAGER

1 Configure this local server

- 2 Add roles and features
- 3 Add other servers to manage
- 4 Create a server group
- 5 Connect this server to cloud services

QUICK START

WHAT'S NEW

LEARN MORE

ROLES AND SERVER GROUPS

Roles: 3 | Server groups: 1 | Servers total: 1

Role	Count
AD DS	1
DHCP	1
File and Storage Services	1
Local Server	1
All Servers	1

Post-deployment Configuration

Configuration required for DHCP Server at DC2

Complete DHCP configuration

Post-deployment Configuration

Configuration required for Active Directory Domain Services at DC2

Promote this server to a domain controller

Task Details

Hide

Povýšení DC2 5

Active Directory Domain Services Configuration Wizard

Deployment Configuration

TARGET SERVER
dc2.ad.local

Deployment Configuration

Domain Controller Options

Additional Options

Paths

Review Options

Prerequisites Check

Installation

Results

Select the deployment operation

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

Specify the domain information for this operation

Domain:

Supply the credentials to perform this operation

AD\Administrator (Current user)

[More about deployment configurations](#)

< Previous **Next >** Install Cancel

Povýšení DC2 6

Active Directory Domain Services Configuration Wizard

Domain Controller Options

TARGET SERVER
dc2.ad.local

Deployment Configuration

Domain Controller Options

DNS Options

Additional Options

Paths

Review Options

Prerequisites Check

Installation

Results

Specify domain controller capabilities and site information

Domain Name System (DNS) server

Global Catalog (GC)

Read only domain controller (RODC)

Site name: Default-First-Site-Name

Type the Directory Services Restore Mode (DSRM) password

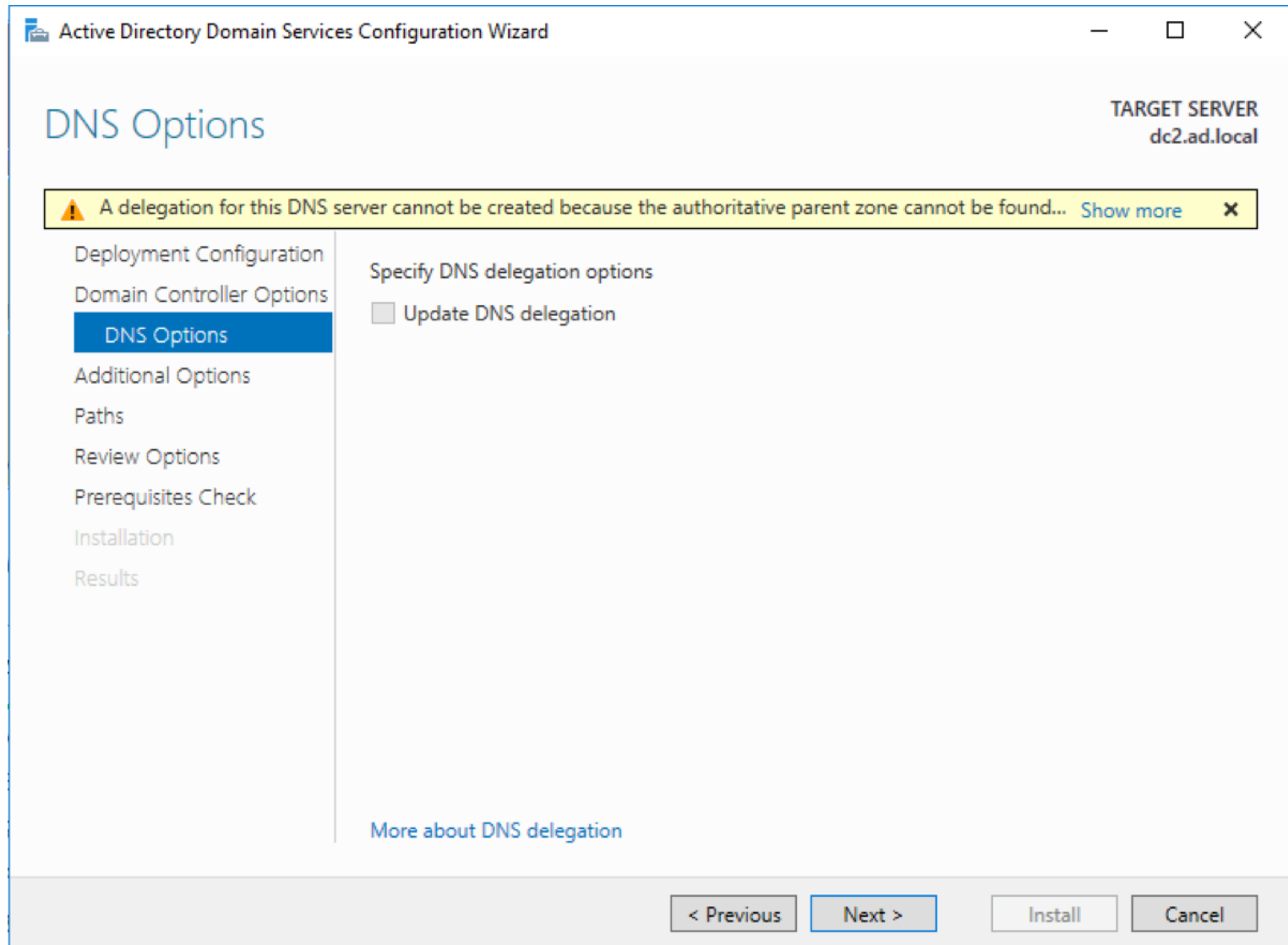
Password:

Confirm password:

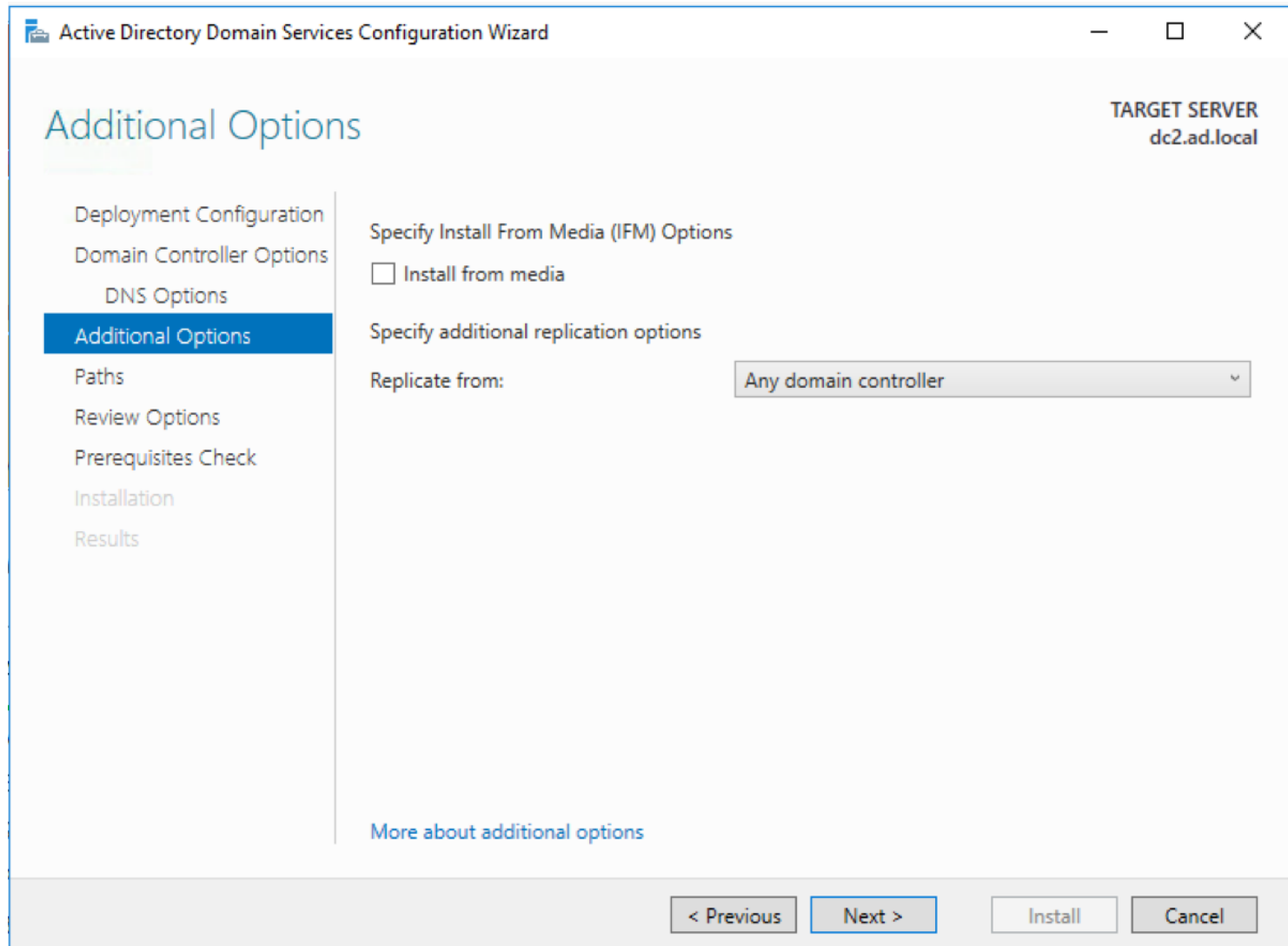
[More about domain controller options](#)

< Previous Next > Install Cancel

Povýšení DC2 7



Povýšení DC2 8



Povýšení DC2 9

Active Directory Domain Services Configuration Wizard

Paths

TARGET SERVER
dc2.ad.local

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

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

Database folder: C:\windows\NTDS ...

Log files folder: C:\windows\NTDS ...

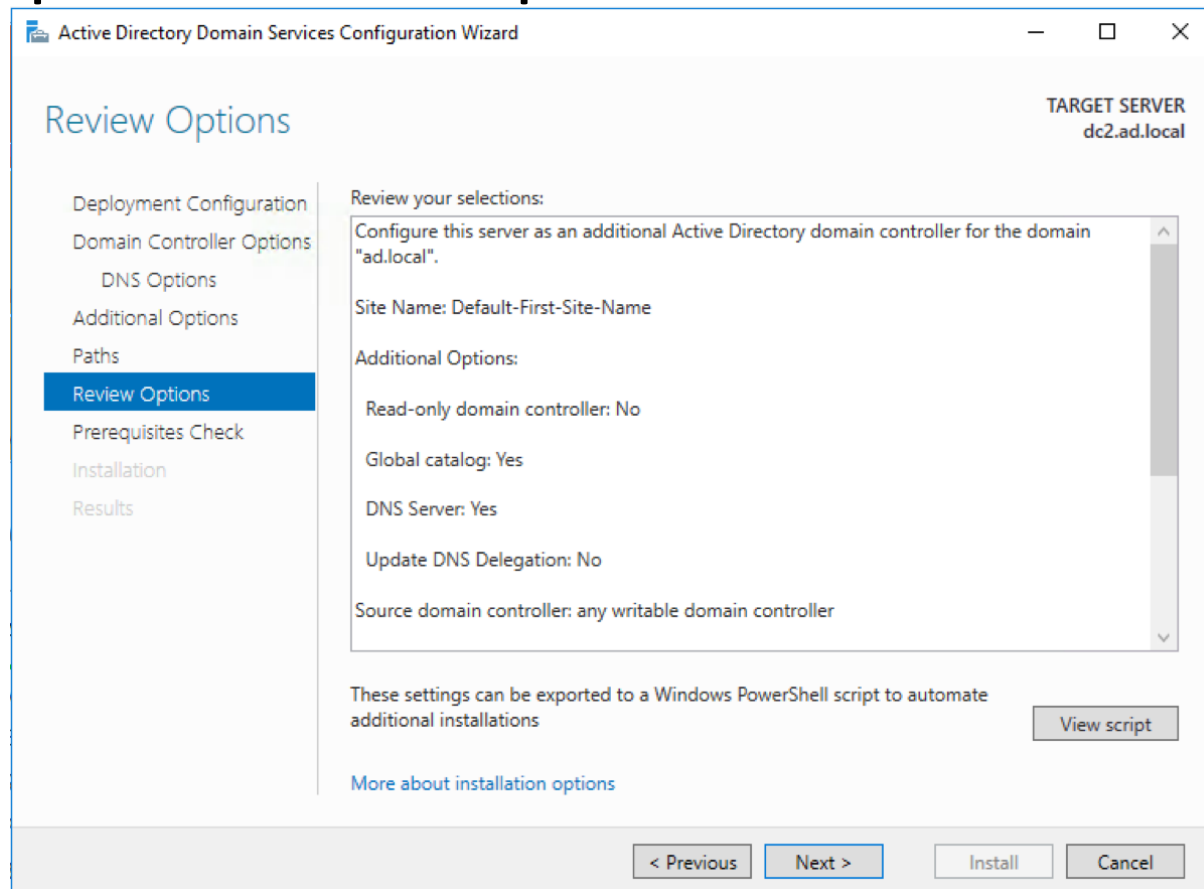
SYSVOL folder: C:\windows\SYSVOL ...

[More about Active Directory paths](#)

< Previous Next > Install Cancel

Povýšení DC2 10

- Klikněte na View Script a zkuste porovnat rozdíly oproti instalaci prvního kontroleru.



Povýšení DC2 11

```
#  
# Windows PowerShell script for AD DS Deployment  
#
```

```
Import-Module ADDSDeployment  
Install-ADDSDomainController `  
-NoGlobalCatalog:$false `  
-CreateDnsDelegation:$false `  
-CriticalReplicationOnly:$false `  
-DatabasePath "C:\windows\NTDS" `  
-DomainName "ad.local" `  
-InstallDns:$true `  
-LogPath "C:\windows\NTDS" `  
-NoRebootOnCompletion:$false `  
-SiteName "Default-First-Site-Name" `  
-SysvolPath "C:\windows\SYSTEM\sysvol" `  
-Force:$true
```

Povýšení DC2 12

Active Directory Domain Services Configuration Wizard

Prerequisites Check

TARGET SERVER
dc2.ad.local

✓ All prerequisite checks passed successfully. Click 'Install' to begin installation. [Show more](#) ✕

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

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

[Rerun prerequisites check](#)

View results

- ⚠ Windows Server 2016 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.

For more information about this setting, see Knowledge Base article 942564 (<http://go.microsoft.com/fwlink/?LinkId=104751>).
- ⚠ This computer has at least one physical network adapter that does not have static IP address(es) assigned to its IP Properties. If both IPv4 and IPv6 are enabled for a network adapter, both IPv4 and IPv6 static IP addresses should be assigned to both IPv4 and IPv6 Properties of the physical network adapter. Such static IP address(es) assignment should be done to all the physical network adapters for reliable Domain Name System
- ⚠ If you click Install, the server automatically reboots at the end of the promotion operation.

[More about prerequisites](#)

< Previous Next > Install Cancel

Povýšení DC2 13

The screenshot shows the 'Active Directory Domain Services Configuration Wizard' window. The title bar includes the application name and standard window controls. The main area is titled 'Results' and shows the 'TARGET SERVER' as 'dc2.ad.local'. A sidebar on the left lists various configuration steps, with 'Results' selected. The main content area shows the progress of configuring the DNS Server service. A warning box is displayed, detailing three issues: a security setting default on Windows Server 2016, missing static IP addresses on network adapters, and a missing delegation for the DNS server. At the bottom, there are navigation buttons for '< Previous', 'Next >', 'Close', and 'Cancel'.

Active Directory Domain Services Configuration Wizard

Results

TARGET SERVER
dc2.ad.local

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

Progress

Configuring the DNS Server service on this computer...

View detailed operation results

- Windows Server 2016 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.

For more information about this setting, see Knowledge Base article 942564 (<http://go.microsoft.com/fwlink/?LinkId=104751>).
- This computer has at least one physical network adapter that does not have static IP address(es) assigned to its IP Properties. If both IPv4 and IPv6 are enabled for a network adapter, both IPv4 and IPv6 static IP addresses should be assigned to both IPv4 and IPv6 Properties of the physical network adapter. Such static IP address(es) assignment should be done to all the physical network adapters for reliable Domain Name System (DNS) operation.
- A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this

If you close this wizard, the installation will continue and the target server will restart when the installation is complete.

More about results

< Previous Next > Close Cancel

Povýšení DC2 14

- Následuje instalace a po ní automatický restart.
- Dát na obou dvou řadičích jako první adresu DNS serveru interní IP adresu druhého řadiče 10.x.x.x. Jako druhou adresu DNS serveru zadejte jeho vlastní 10.x.x.x.

Rest of Domain Tasks 1

- DHCP servery je nutné autorizovat do domény, jinak nebudou přidělovat adresy.
- Pokud máte DHCP na obou dvou řadičích, musíte je autorizovat na obou zvlášť.
- Přidání třetího serveru a stanice do domény (DNS servery, pak přidat).

Rest of Domain Tasks 2

Server Manager

Server Manager Dashboard

Manage Tools View Help

WELCOME TO SERVER MANAGER

QUICK START

- 1 [Configure this local server](#)
- 2 [Add roles and features](#)
- 3 [Add other servers to manage](#)
- 4 [Create a server group](#)
- 5 [Connect this server to cloud services](#)

WHAT'S NEW

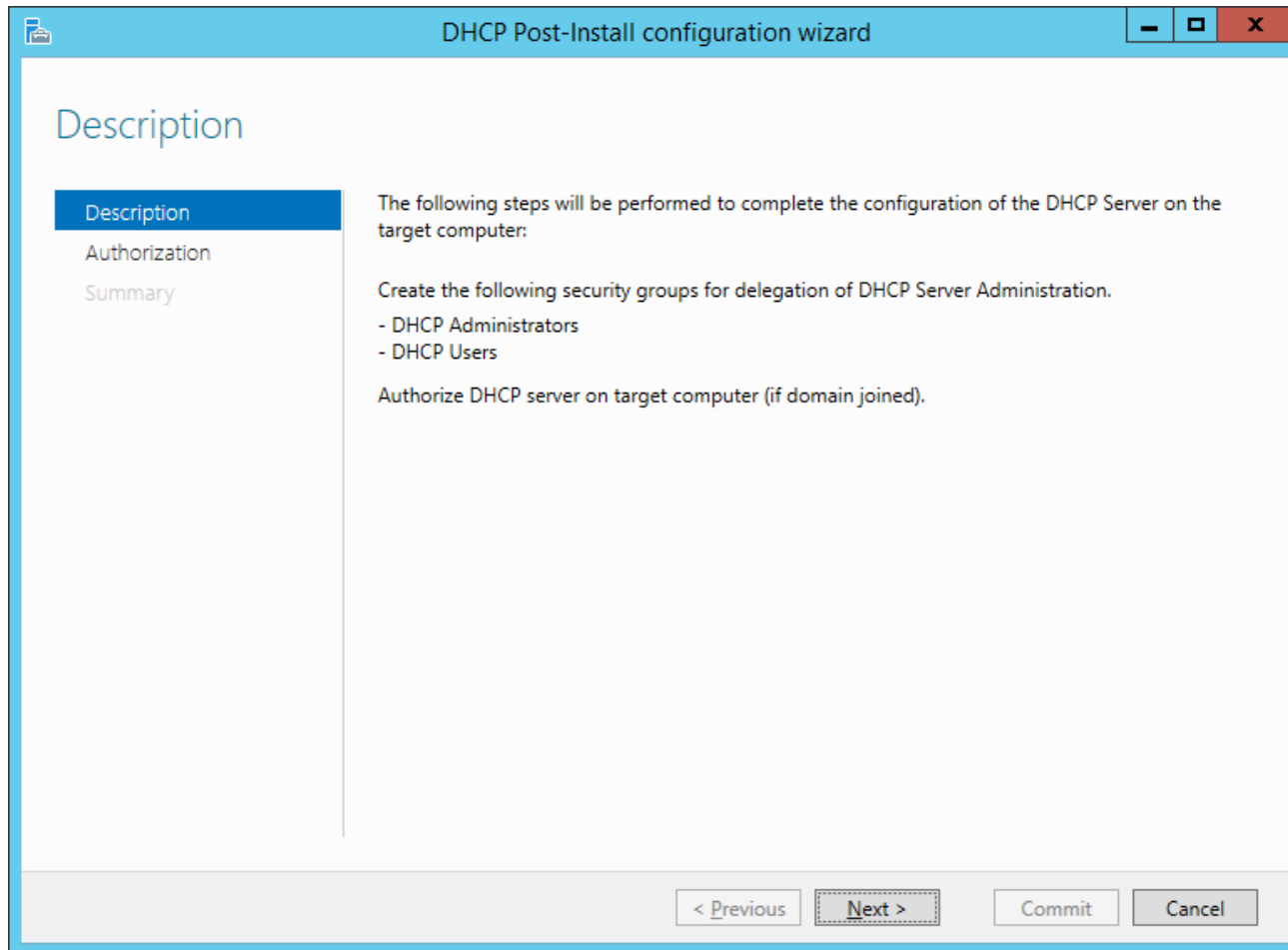
[LEARN MORE](#)

ROLES AND SERVER GROUPS
Roles: 4 | Server groups: 1 | Servers total: 1

Role	Count
AD DS	1
DHCP	1
DNS	1

Post-deployment Configuration
Configuration required for DHCP Server at PV176-10-1
[Complete DHCP configuration](#)
Task Details

Rest of Domain Tasks 3



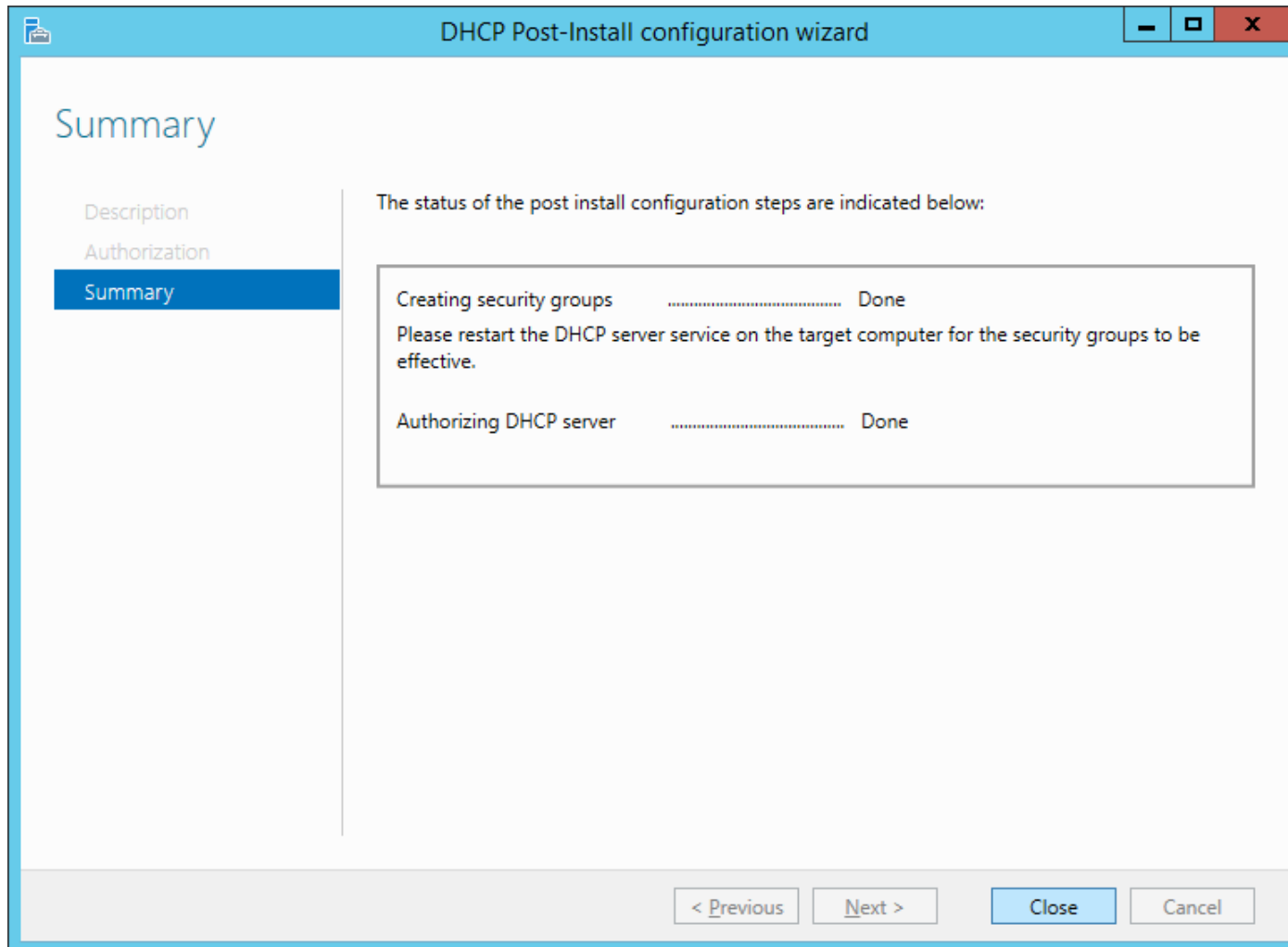
Rest of Domain Tasks 4

The screenshot shows a window titled "DHCP Post-Install configuration wizard" with a blue header bar. On the left, a sidebar contains three items: "Description", "Authorization" (highlighted in blue), and "Summary". The main area is titled "Authorization" and contains the following text: "Specify the credentials to be used to authorize this DHCP server in AD DS." Below this text are three radio button options:

- Use the following user's credentials
User Name:
- Use alternate credentials
UserName:
- Skip AD authorization

At the bottom of the window, there are four buttons: "< Previous", "Next >", "Commit", and "Cancel".

Rest of Domain Tasks 5



Single sign-on

- Uživatel se přihlašuje na jednom místě
- Toto jedno přihlášení mu zajistí přístup ke všem sdíleným zdrojům ve forestu
- V AD zajišťuje Kerberos
 - [https://en.wikipedia.org/wiki/Kerberos_\(protocol\)](https://en.wikipedia.org/wiki/Kerberos_(protocol))

Účty v AD

- Uživatelský účet
 - Nutný pro přihlášení člověka k doméně
 - Ustanovuje uživateli identitu, kterou operační systém následně používá pro autentizaci na síti a autorizaci prováděných činností
- Účet počítače
 - Ustanovuje identitu počítače, která se používá pro autentizaci, autorizaci a audit
 - Pod účtem počítače běží všechny systémové procesy
- Účet skupiny
 - Účet sdružující a zastupující jiné účty
 - Může obsahovat účty uživatelů, počítačů i dalších skupin
 - Každý účet (i účet skupiny) může být členem libovolného množství skupin
 - Zjednodušuje administraci a správu přístupu ke zdrojům

Skupiny – typ

- Bezpečnostní
 - využívají se k přidělování práv a oprávnění a
- Distribuční
 - Skupinové mailové adresy

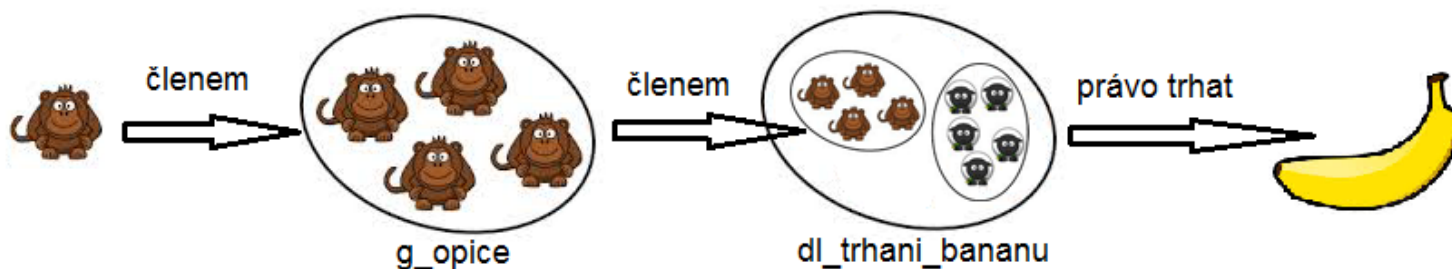
Bezpečnostní skupinu lze také použít pro skupinovou mailovou adresu – někteří správci distribuční adresy vůbec nepoužívají.

Účty skupin – scope

- Globální skupiny (G)
 - Členství: Členy mohou být pouze účty a skupiny ze stejné domény jako je daná skupina
 - Oprávnění: Globální skupině mohou být udělena oprávnění k libovolným objektům v celém lese
- Doménové lokální skupiny (DL)
 - Členství: Členy doménové lokální skupiny mohou být účty a skupiny z celého vlastního lesa
 - Oprávnění: Doménové lokální skupině mohou být udělena oprávnění pouze v rámci její domény
- Univerzální skupiny (U)
 - Členství: Členy mohou být účty a skupiny z libovolné domény v lese
 - Oprávnění: Univerzálním skupinám mohou být přiřazena oprávnění k libovolným objektům v celém lese
 - Univerzální skupiny jsou ukládány pouze na globálním katalogu

Jmenné konvence + AGDLP přístup

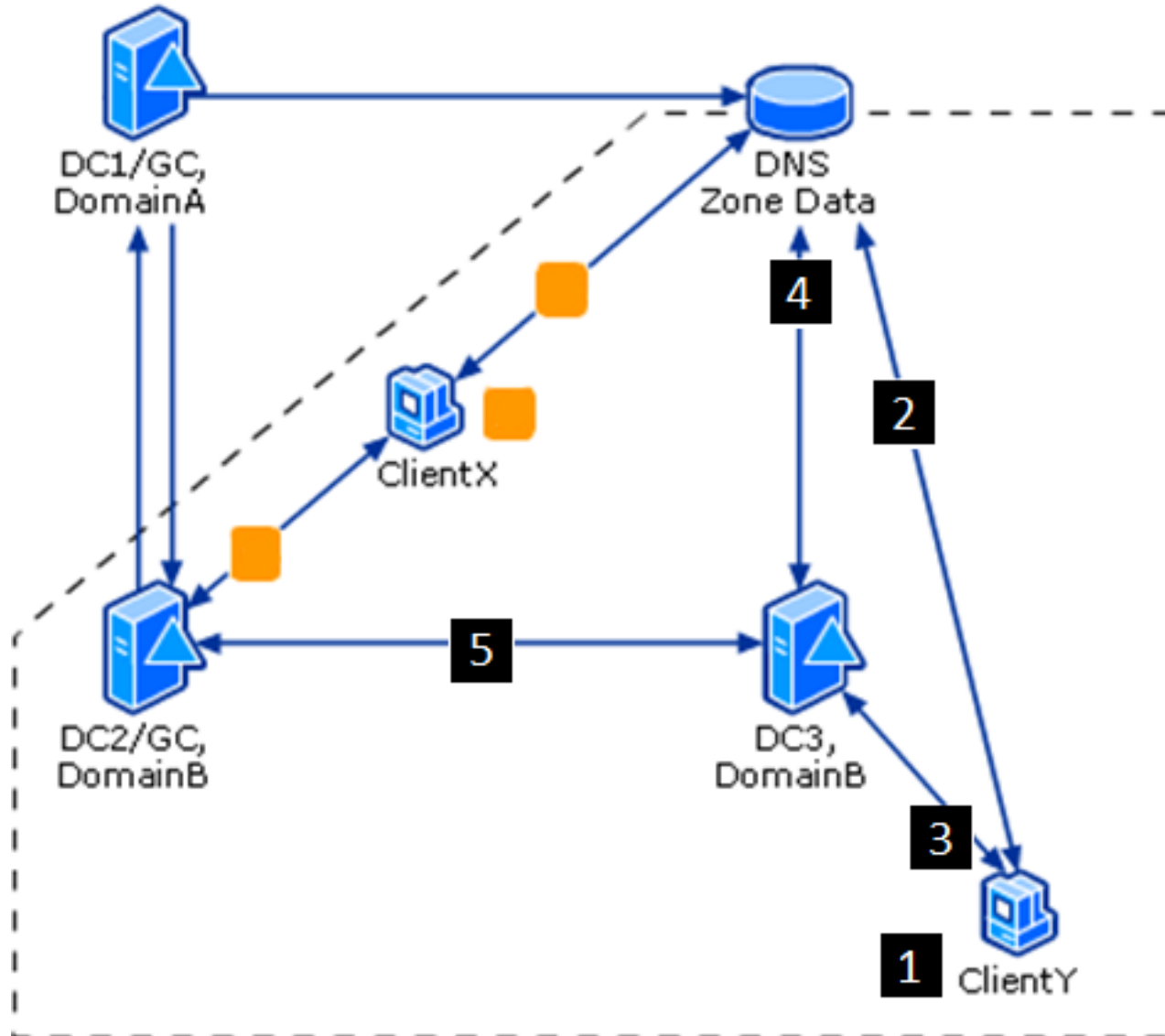
- Definovat konvence pro vytváření veškerých objektů
- Ulehčení vyhledávání, ulehčení skriptování, ulehčení správy
- **AGDLP** – **A**ccess **G**lobal **D**omain **L**ocal **P**ermissions
- př. globální skupina g_opice, doménová lokální skupina dl_trhání_banánů




Autentizace uživatele v AD

1. Uživatel zadává svůj login a heslo.
2. Stanice se ptá DNS, kde se nachází LDAP a Kerberos služba pro uživatelovu doménu. DNS poskytuje odpověď.
3. Stanice kontaktuje DC, jehož IP adresu dostala, a žádá o autentizaci uživatele.
4. DC ověřuje platnost loginu a hesla, jsou platné. DC ale není GC, takže kontaktuje DNS a žádá o SRV záznamy o GC. DNS poskytuje odpověď.
5. DC se ptá GC, zda je uživatel členem nějaké univerzální skupiny, která nedovoluje přihlášení na dané stanici. Pokud není, DC povoluje uživateli přihlášení na stanici.

Autentizace uživatele v AD



Identifikace objektu v LDAP

Name	Type
 Kocka Pes	User

- Distinguished Name
 - "CN=Kocka Pes,OU=Zvirata,DC=test,DC=local,,
- Common Name, Display Name
 - Kocka Pes
 - Z DN plyne, že CN je unikátní v rámci OU
- User logon name, sAMAccountName
 - unikátní v rámci domény

General	Address	Account	Profile	Telephones	Organization
User logon name:					
<input type="text" value="kockopes"/>		<input type="text" value="@test.local"/>			
User logon name (pre-Windows 2000):					
<input type="text" value="TEST\"/>		<input type="text" value="kockopes"/>			
<input type="button" value="Logon Hours..."/>		<input type="button" value="Log On To..."/>			

Identifikace objektu v LDAP

- SID
 - pokud uživatel změní doménu, změní se SID
 - udržuje se historie
 - SID existuje z historických kompatibilních důvodů
- GUID
- UPN sufix
 - nelze změnit
 - UPN tvoří přihlašovací jméno informující o tom jaký uživatel se chce přihlásit (User Principal Name)
 - 2 varianty:
 - kockopes@zoo.local
 - zoo.local\kockopes
 - ZOO\kockopes – NetBIOS varianta
- Access Token uživatele - whoami

objectClass	top; person; organizationalPerson; user
objectGUID	ac0cadf6-e5ef-4c28-b573-b179de8bd025
objectSid	S-1-5-21-1268746369-2550591081-4619241

Významné účty skupin

- Domain Users
 - Skupina všech uživatelských účtů v doméně
- Domain Computers
 - Skupina všech účtů počítačů v doméně
- Domain Controllers
 - Skupina všech účtů doménových řadičů v doméně

Významné účty skupin

- Domain Admins
 - Správci domény, mají nejvyšší možná práva v rámci své domény
- Enterprise Admins
 - Správci organizace, mají nejvyšší možná práva ve všech doménách celého lesa
 - Mohou vytvářet nové domény a navazovat nové vztahy důvěry mezi doménami
 - Tato skupina se nachází pouze ve forest-root doméně lesa
- Schema Admins
 - Členové této skupiny mohou provádět změny schématu Active Directory
 - Tato skupina se nachází pouze ve forest-root doméně lesa

Vytváření a správa účtů

- Malá organizace/výjimečné požadavky
 - Active Directory Users and Computers
 - Základní grafický nástroj pro správu účtů a organizačních jednotek
- Střední organizace/občasné hromadné změny
 - Skripty a nástroje příkazové řádky
 - **powerShell**
 - **import-module ActiveDirectory**
 - **get-help *-AD***
 - Idifde
 - Csvde
 - dsadd, dsmod, dsquery, dsget, dsmove, dsrm
 - Visual Basic Script
- Velká organizace/dynamicky se měnící prostředí
 - Propojení s existujícím personálním systémem
 - Proprietární řešení

PowerShell

- Preferujte ho
- Rozšíření ke standardním od Microsoftu: www.quest.com koupila firma Dell, přejmenovala na ActiveRoles Management Shell for Active Directory
- Popis AD commandletů na [stránkách Technetu](#)
- New- Get- Set-ADComputer
- New- Remove- Get- Set-ADUser
- Všechny atributy účtu: `Get-ADUser -Identity 25631 -Properties *`
- Vypíše všechny účty v organizační jednotce: `Get-ADUser -Filter * - SearchBase "OU=System,OU=MU,DC=UCN,DC=MUNI,DC=CZ,,`
- Hledání s filtrem: `Get-ADUser -Filter {GivenName -eq "David"} - Properties "sn"`

PowerShell

- Založení skupiny: `New-ADGroup -Name "RODC Admins" -SamAccountName RODCAdmins -GroupCategory Security -GroupScope Global -DisplayName "RODC Administrators" -Path "CN=Users,DC=Fabrikam,DC=Com" -Description "Members of this group are RODC Administrators"`
- Atributy skupiny: `Get-ADGroup 'TSUKBUsers'`
- Členové skupiny: `Get-ADGroupMember 'TSUKBUsers,`
- Přidání do skupiny: `Add-ADGroupMember -Identity SvcAccPSOGroup -Members SQL01,SQL02`

ds nástroje

- dsadd – přidání objektu
- dsmod – úprava objektu
- dsget – zobrazení vlastností objektu
- dsquery – nalezení objektů v adresáři
- dsmove – přesun objektu
- dsrm – odstranění objektu

- Př.:
dsadd user CN=Kockopes,OU=Zvirata,DC=zoo,DC=local -samid Kockopes
-pwd Pa\$\$w0rd

Idifde

- LDAP Data Interchange format directory exchange
- import/export účtů ve velkém množství
 - Import: Idifde -i -f INPUT.LDF
 - Export: Idifde -f OUTPUT.LDF
- Struktura souboru:

dn: CN=Kocko Pes,OU=Zvirata,OU=Student,DC=zoo,DC=local

changetype: add

cn: Kocko Pes

objectclass: user

givenname: Kocka

sn: Domaci

csvde

- Comma-separated values directory exchange
- import/export účtů ve velkém množství
 - Import: `csvde -i -f INPUT.CSV`
 - Export: `csvde -f OUTPUT.CSV`
- Struktura souboru:

`dn,UserPrincipalName,objectClass,givenName,sn`
`"CN=Kocko Pes,OU=Zvirata,OU=Student,`
`DC=zoo,DC=local",kockopes@zoo.local,user,Kocka,Domaci`

Úkoly

1. Vytvořit uživatelský účet nástrojem AD Users and Computers
2. Zakázat/povolit tento účet
3. Resetovat účtu heslo
4. Vytvořit skupinu v AD Users and Computers
5. Vložit do skupiny další účty i další skupiny
6. Zkontrolovat access token (whoami /all)
7. Vytvořit účet commandletem v PowerShellu (new-adUser)
8. Vytvořit účet příkazem dsadd a upravit ho přes dsmod
9. Vytvořit účty nástrojem Idifde