Instalace AD, single sign-on

Šimon Suchomel, David Leška

Prerekvizity

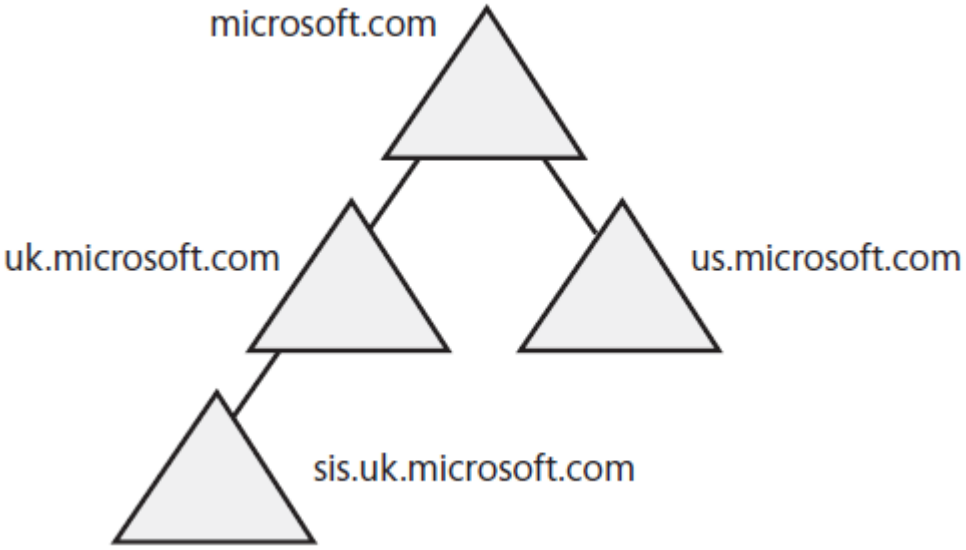
- Server 0 a 1 vyvolat instalaci aktualizací, volitelně i další stroje.

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

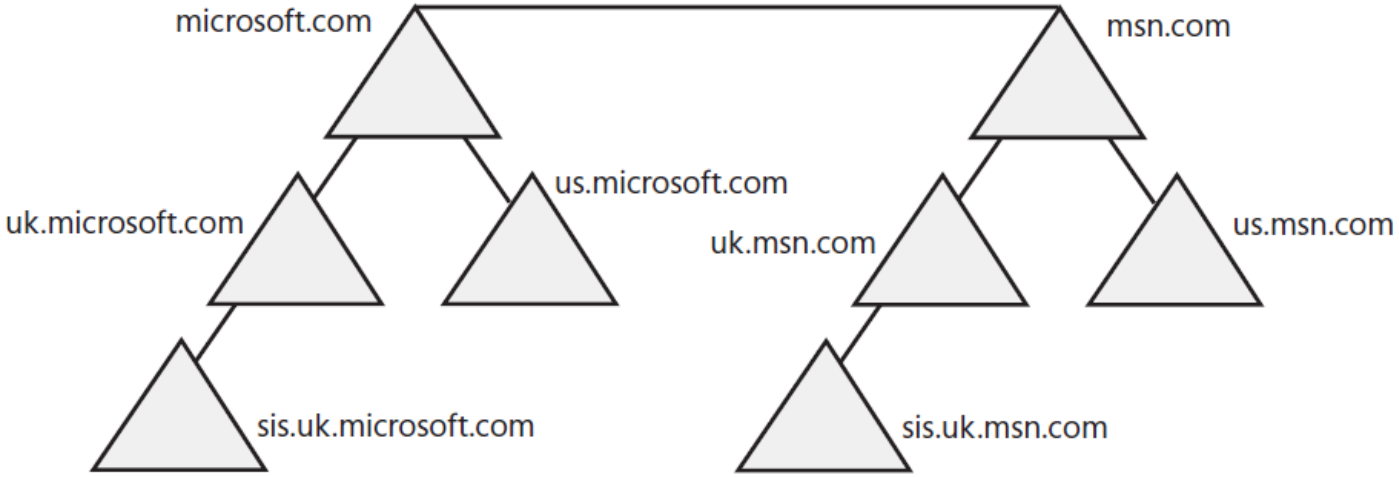
- Tree (strom)
  - Je hierarchické spojení domén, vytvoření vztahem rodič-potomek
  - Domény ve stromě sdílí souvislý DNS namespace



Obrázek převzatý z MS 70-270 Training kit

Logická struktura AD – pokračování

- Forest (les)
  - Kolekce jednoho nebo více trees
  - První doména v lese je tzv. *forest root domain*



Obrázek převzatý z MS 70-270 Training kit

Instalace AD – požadavky

- Windows Server
- Administrátorský přístup

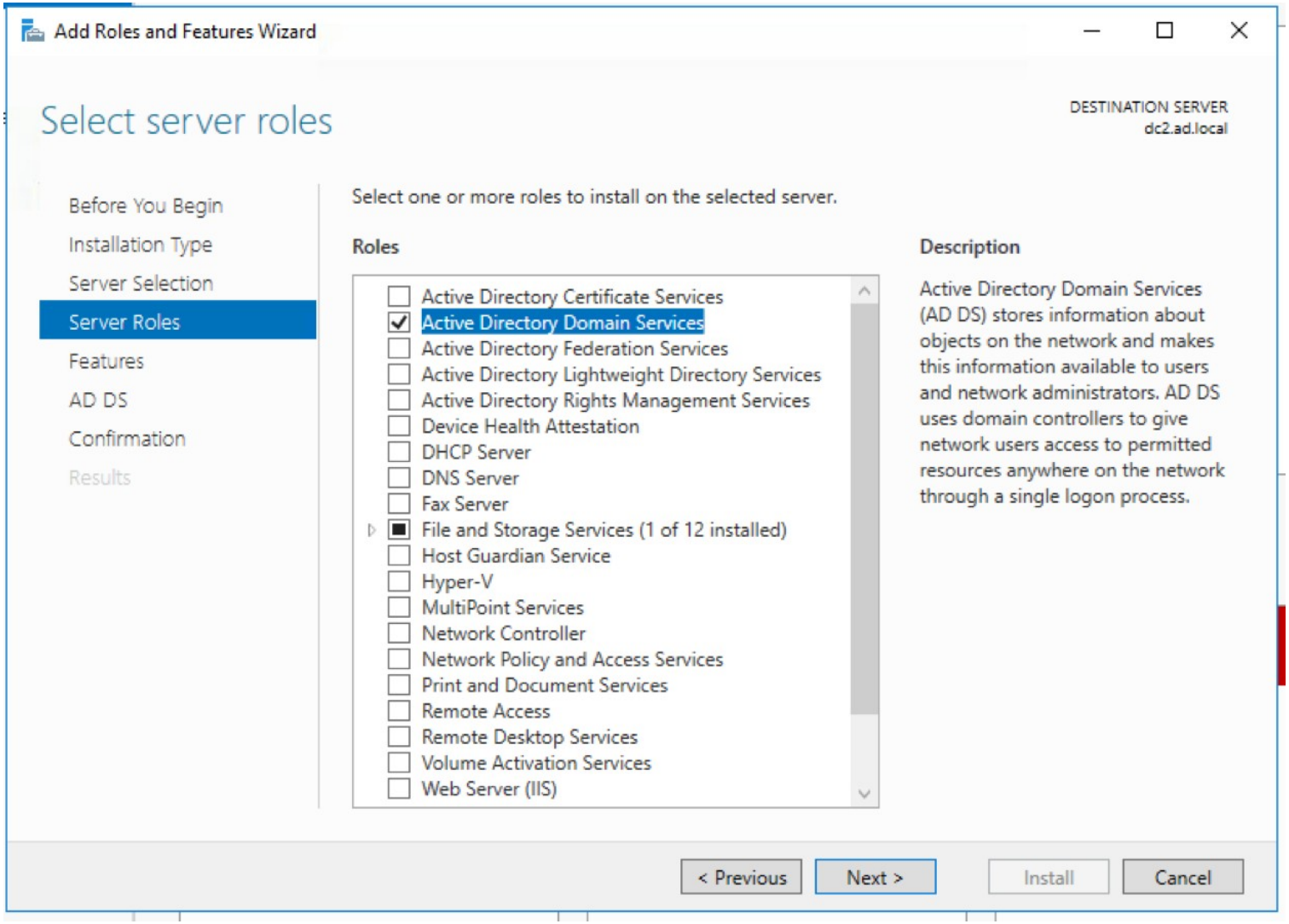
- DNS (a NetBIOS) jméno domény – *login*.local
  - Možná instalace nového DNS serveru
- Statickou IP adresu

- 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!

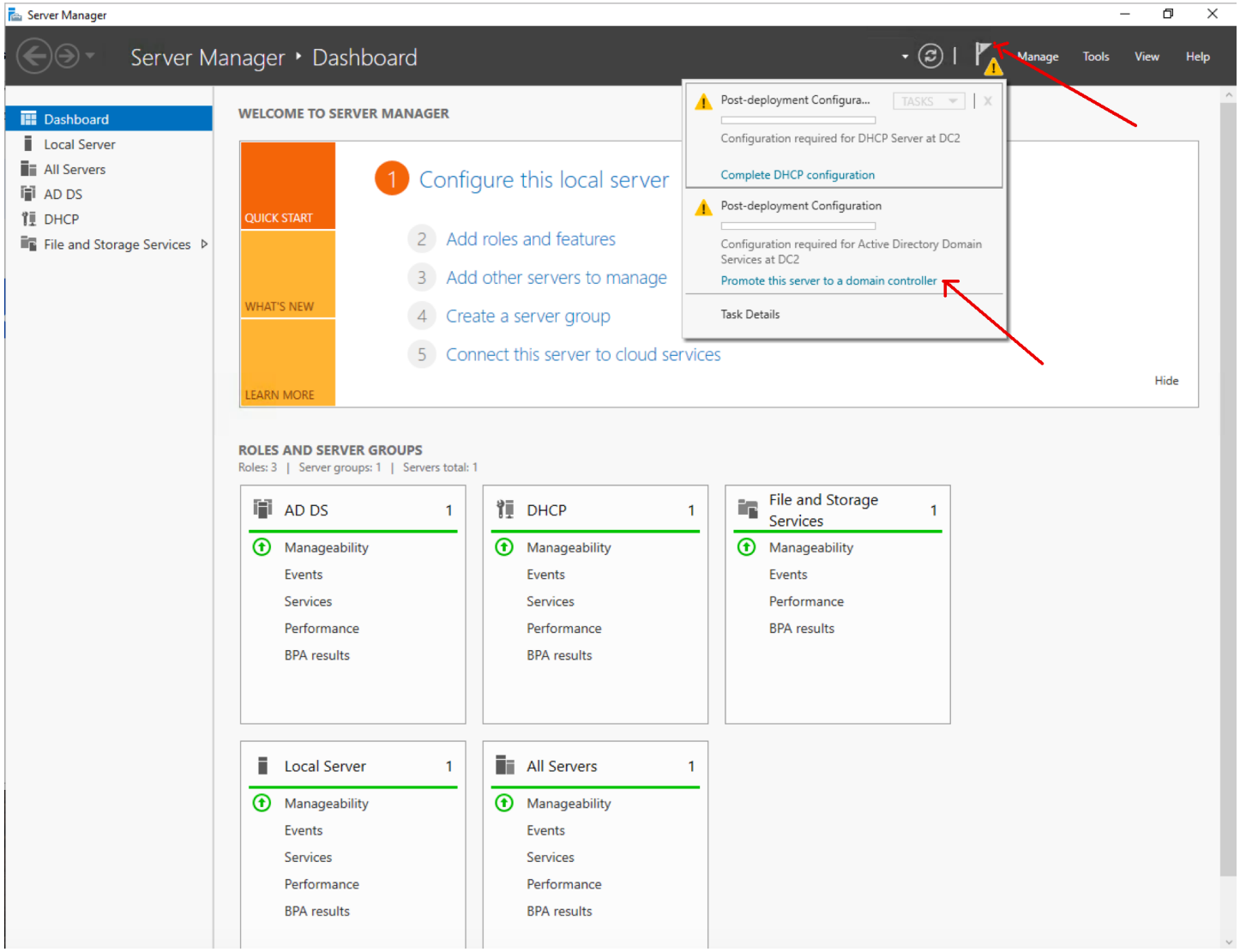
Instalace AD role



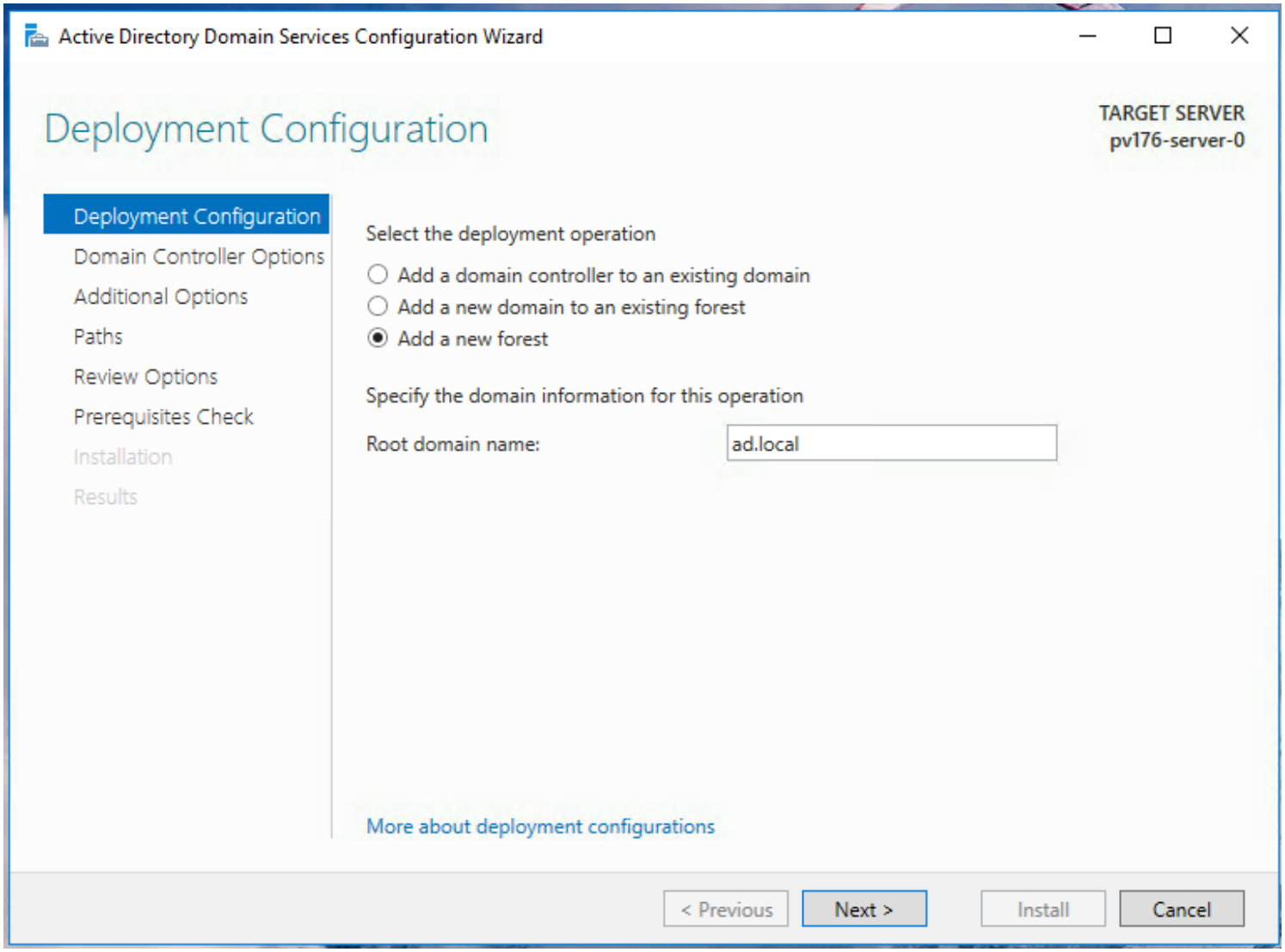
Úkoly – instalace DC

- 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

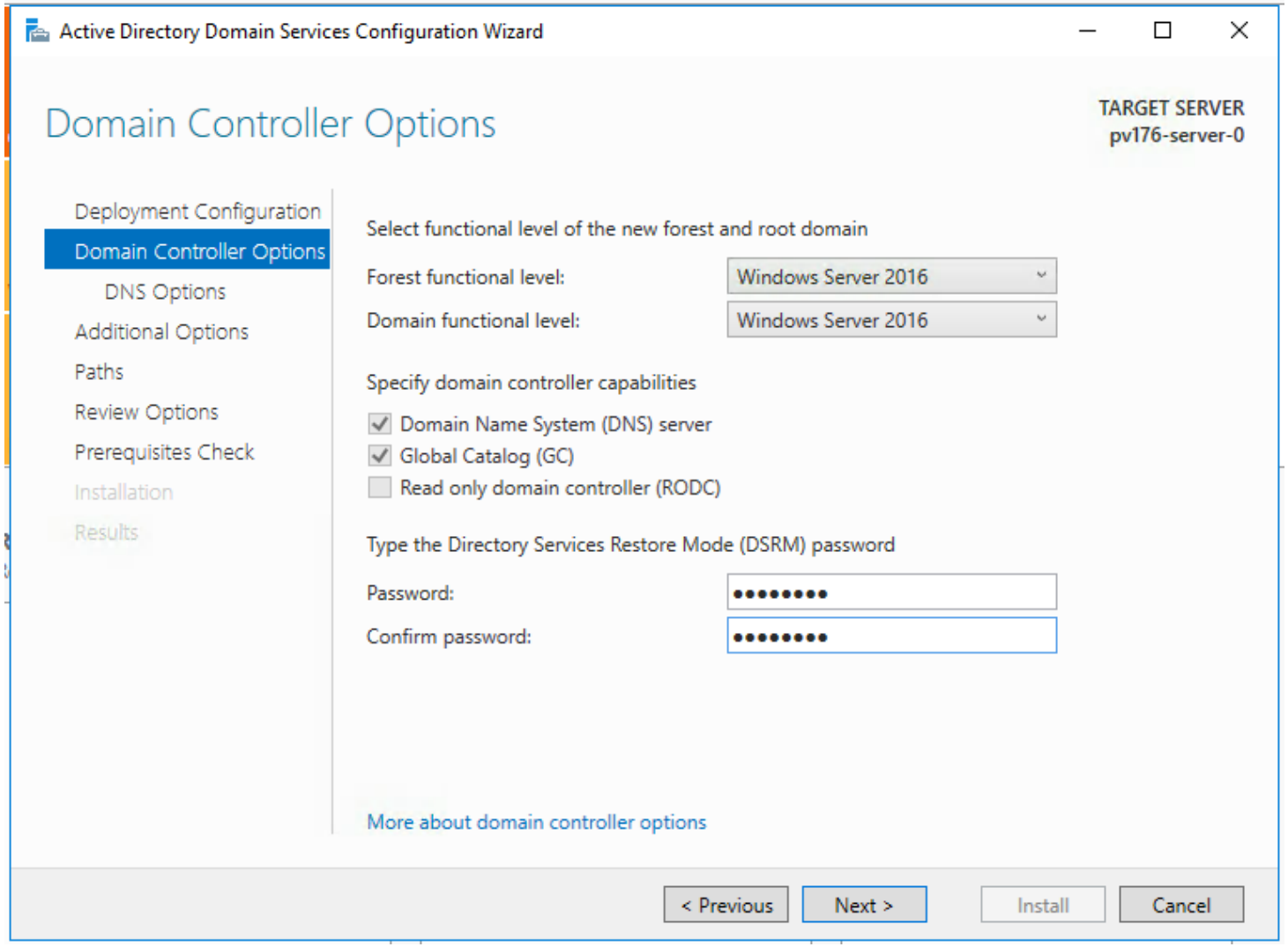
Povýšení DC1 1



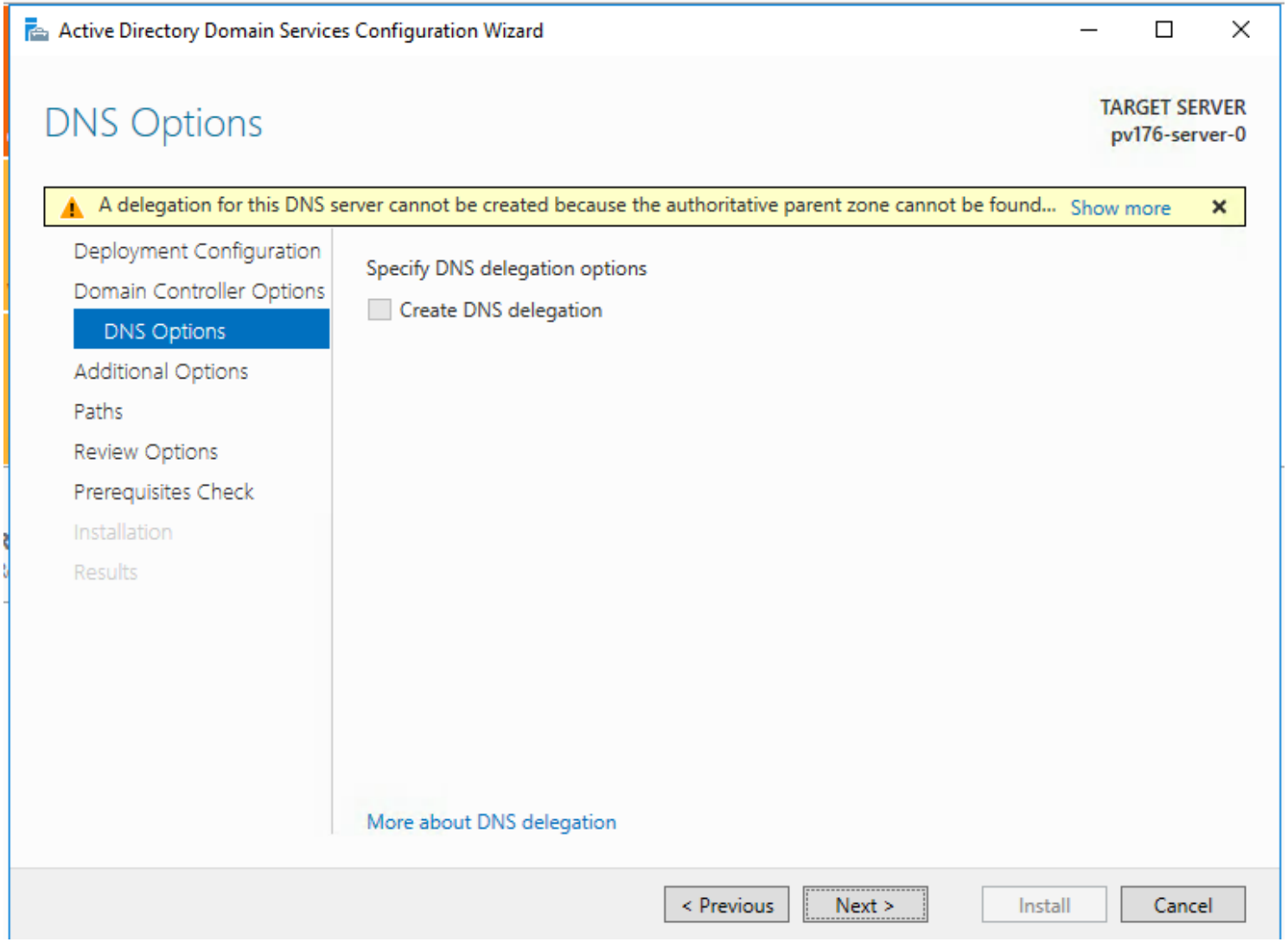
Povýšení DC1 2



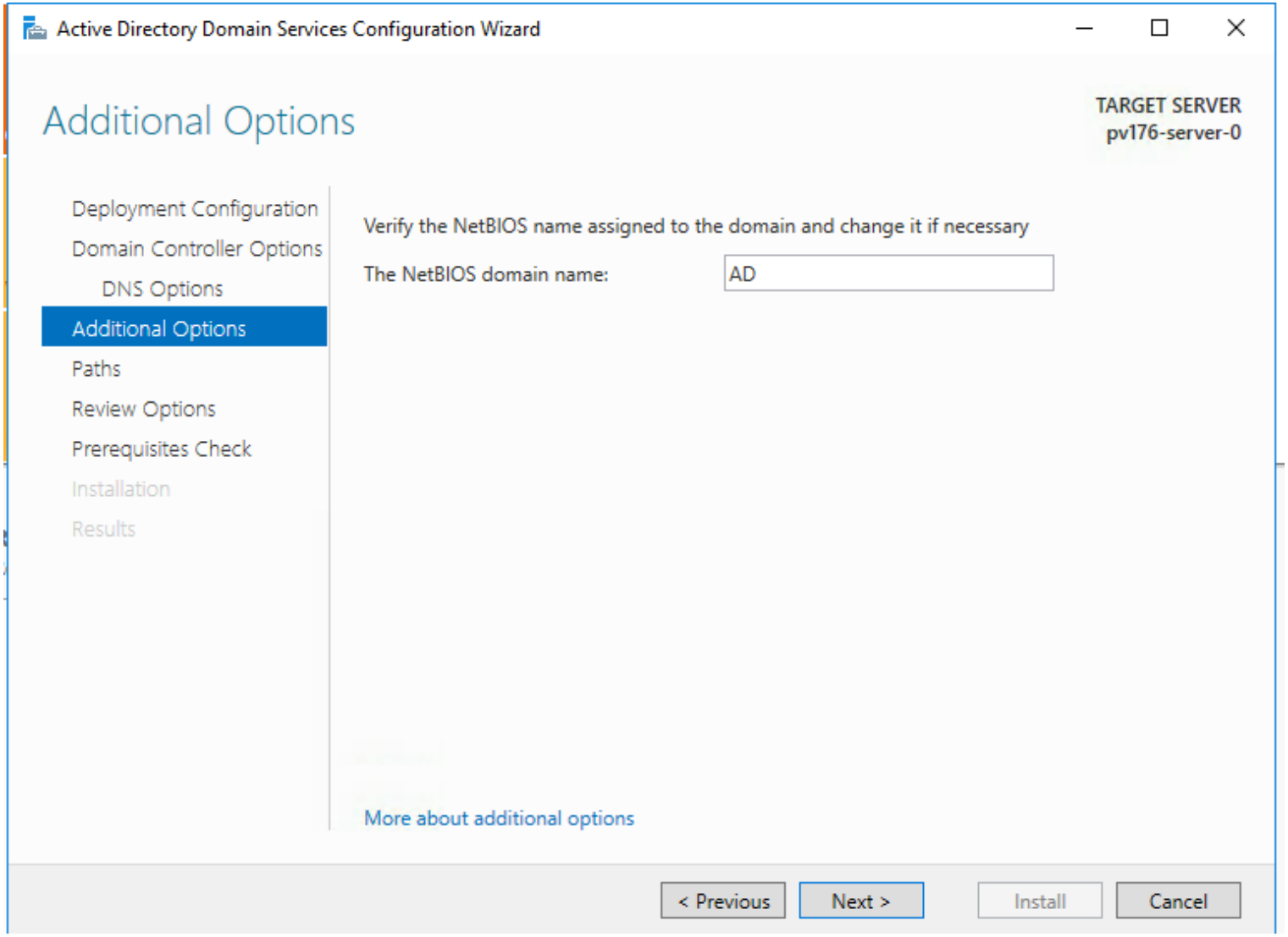
Povýšení DC1 3



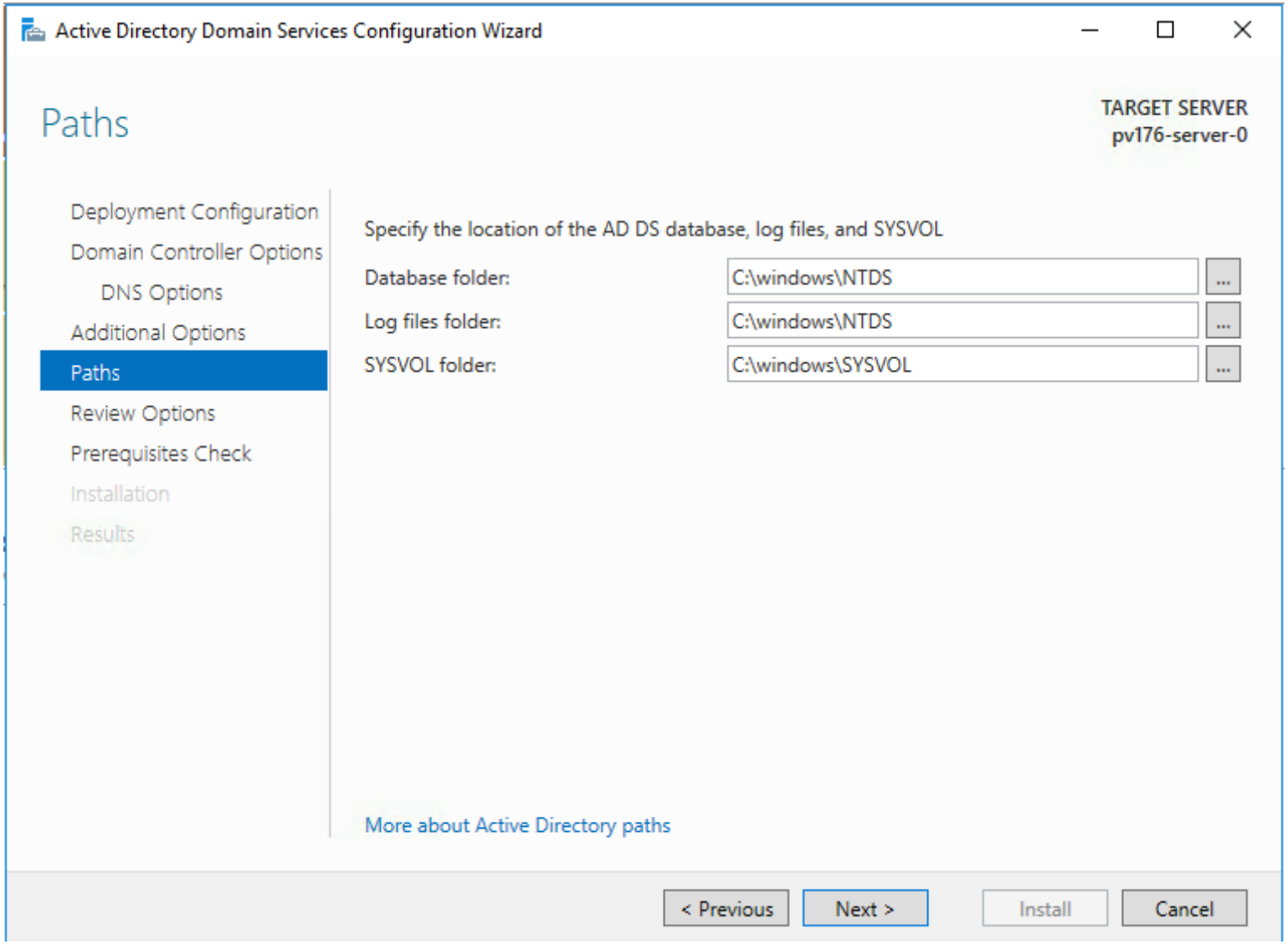
Povýšení DC1 4



Povýšení DC1 5

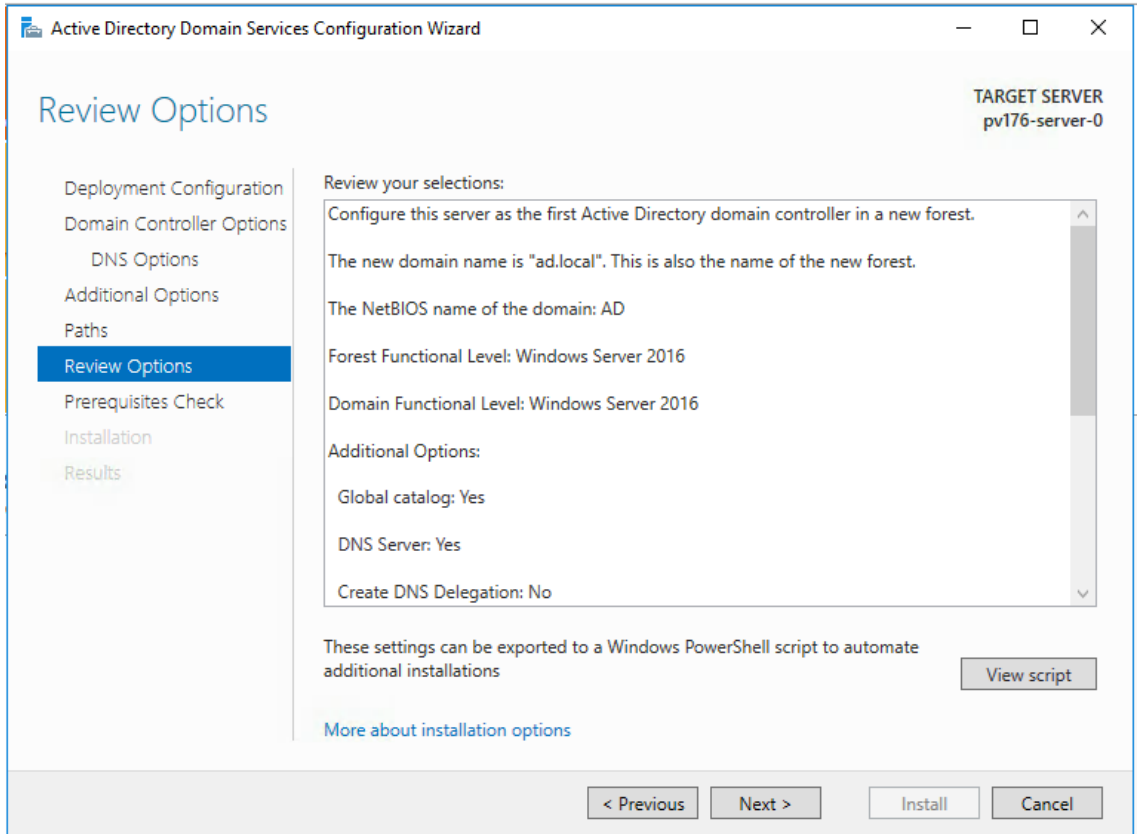


Povýšení DC1 6



Povýšení DC1 7

- Všichni zmáčknou View Script a prohlédnou si kód v PowerShellu

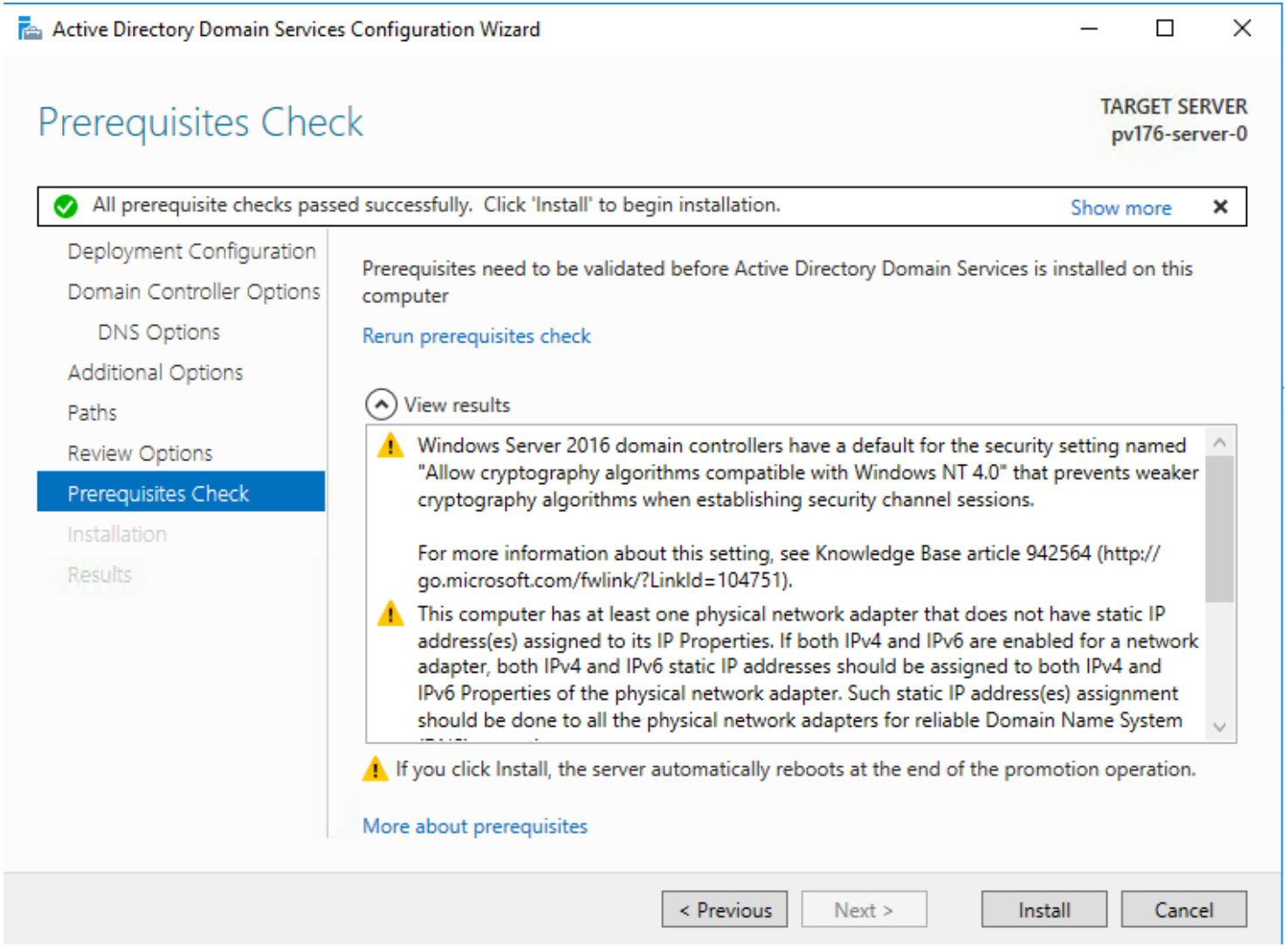


Povýšení DC1 8

```
#
# 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:$false `
-SysvolPath "C:\windows\SYSVOL" `
-Force:$true
```

Povýšeni DC1 9



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

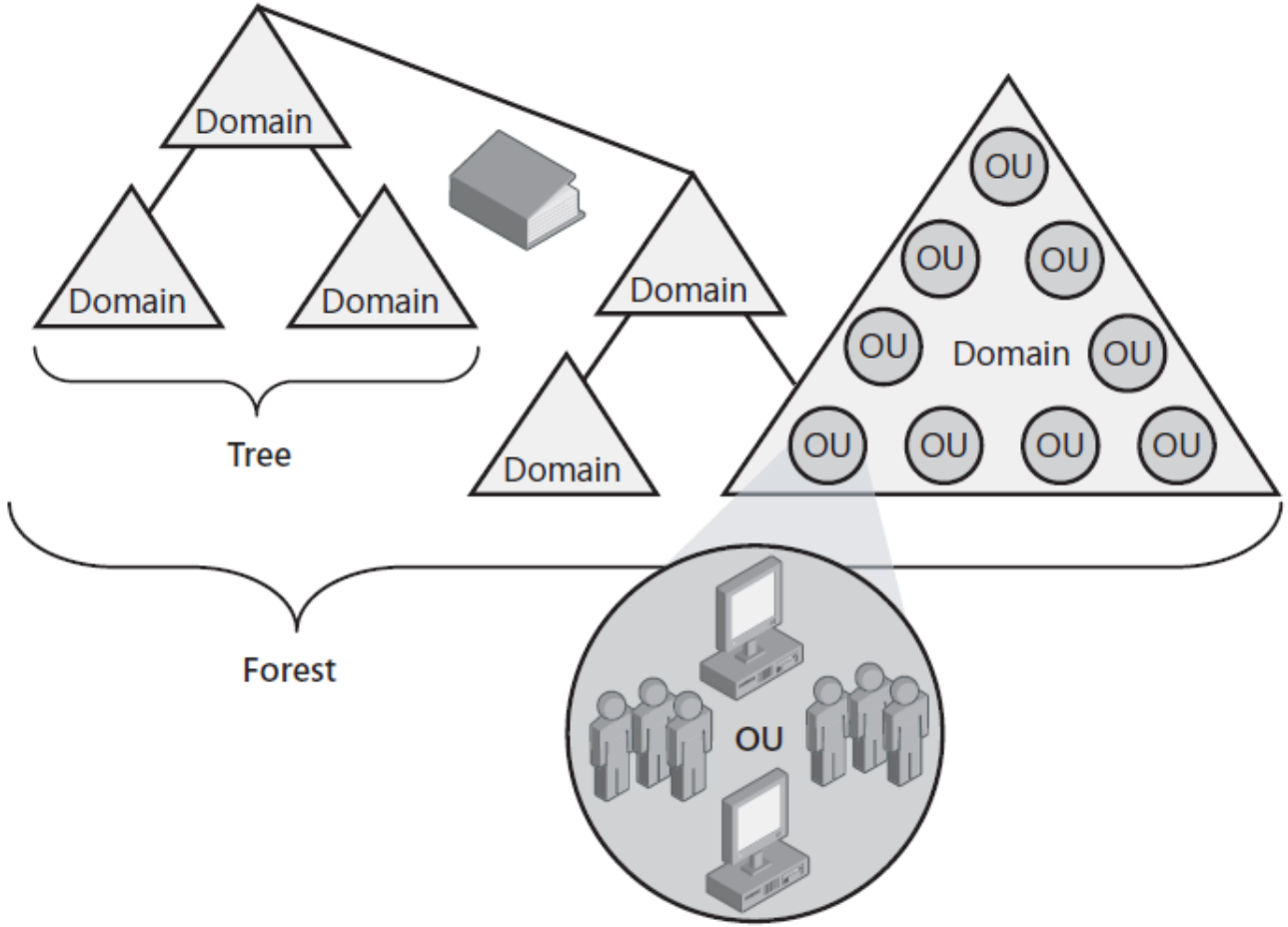
Kontrolní otázka

- 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



Obrázek převzatý z MS 70-270 Training kit

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

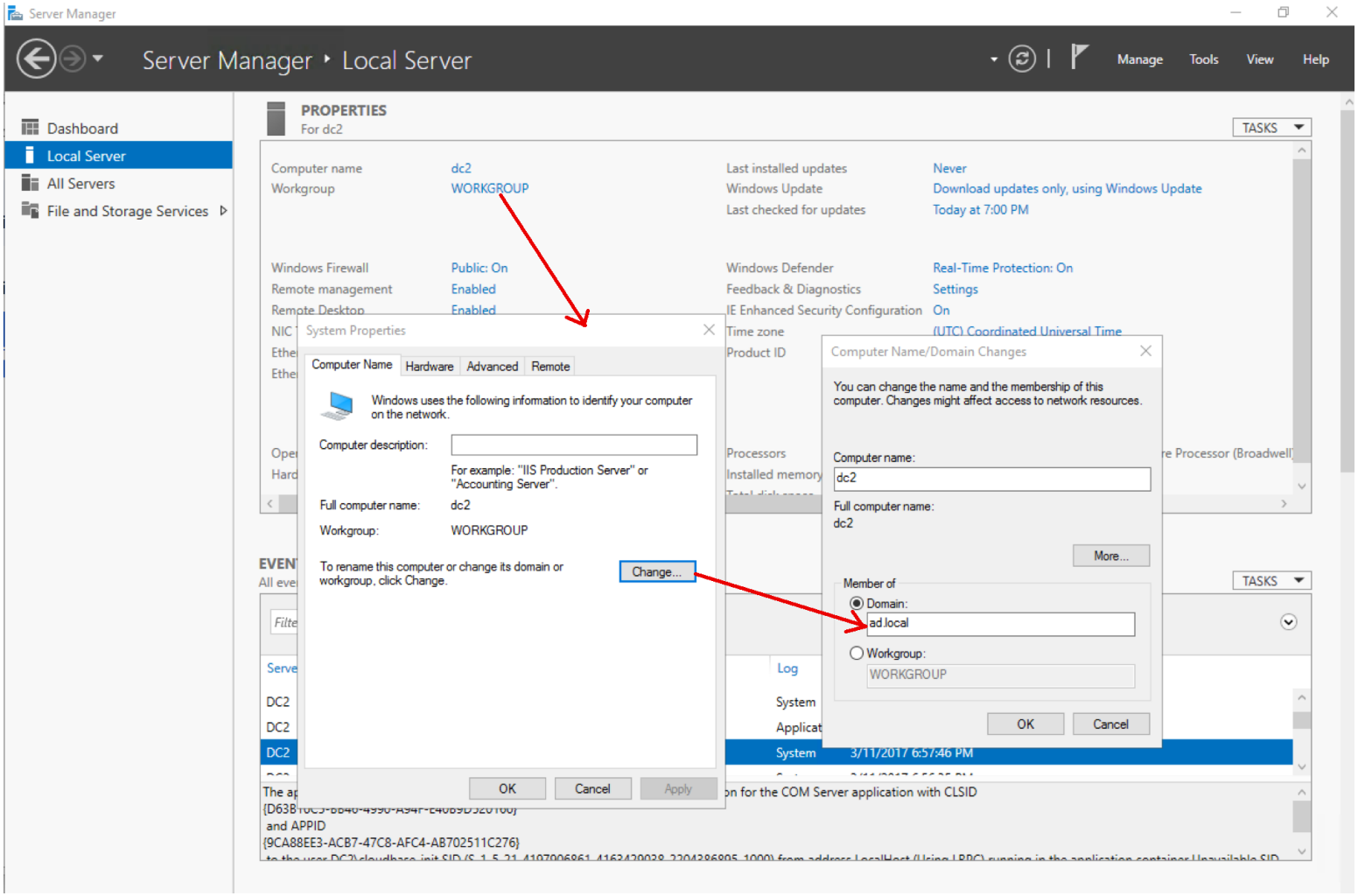
- DNS snap in – prohlídka SRV záznamů, ukázka koexistence různých typů zón na jednom DNS serveru.

- 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.

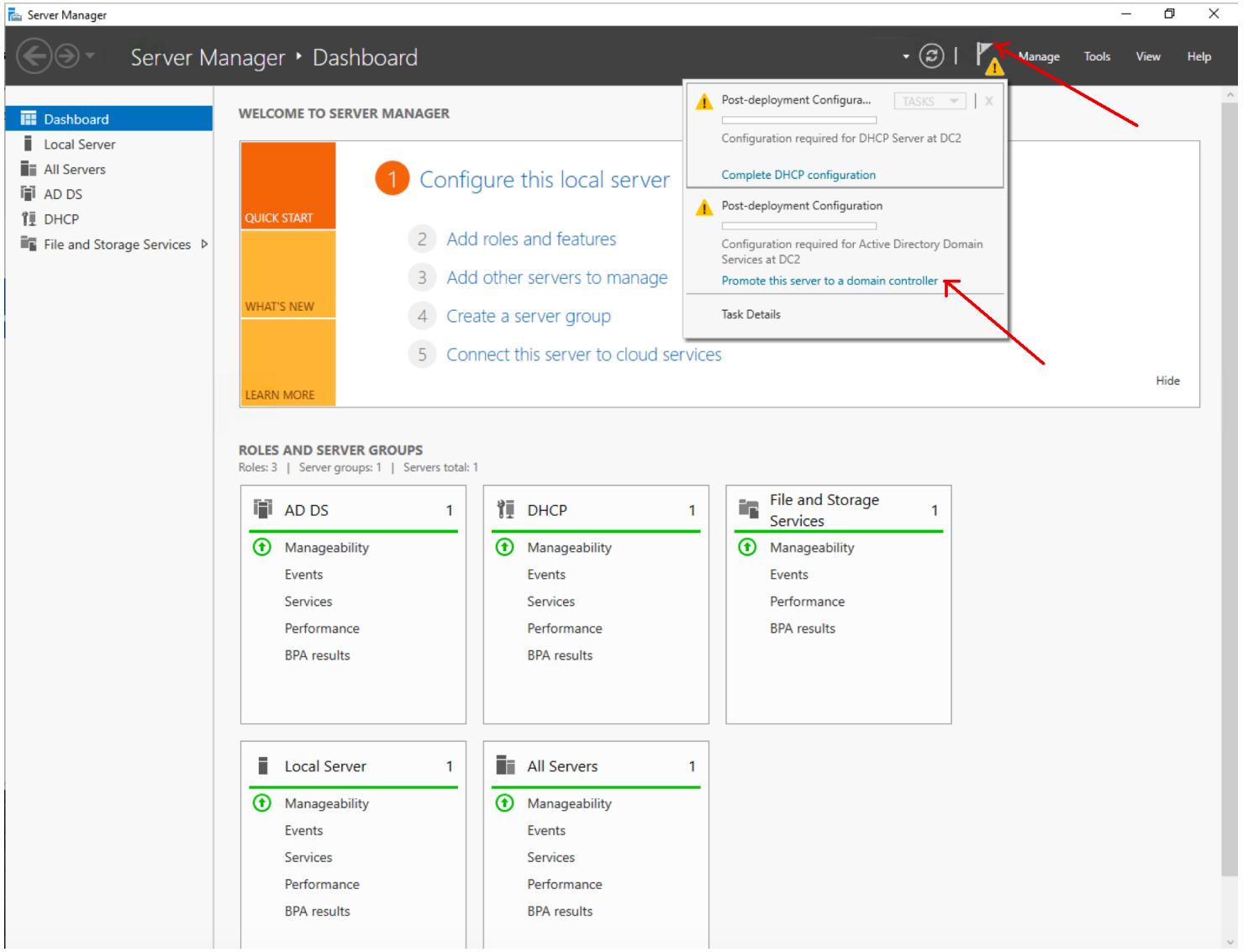
Povýšení DC2 2
přidání do domény



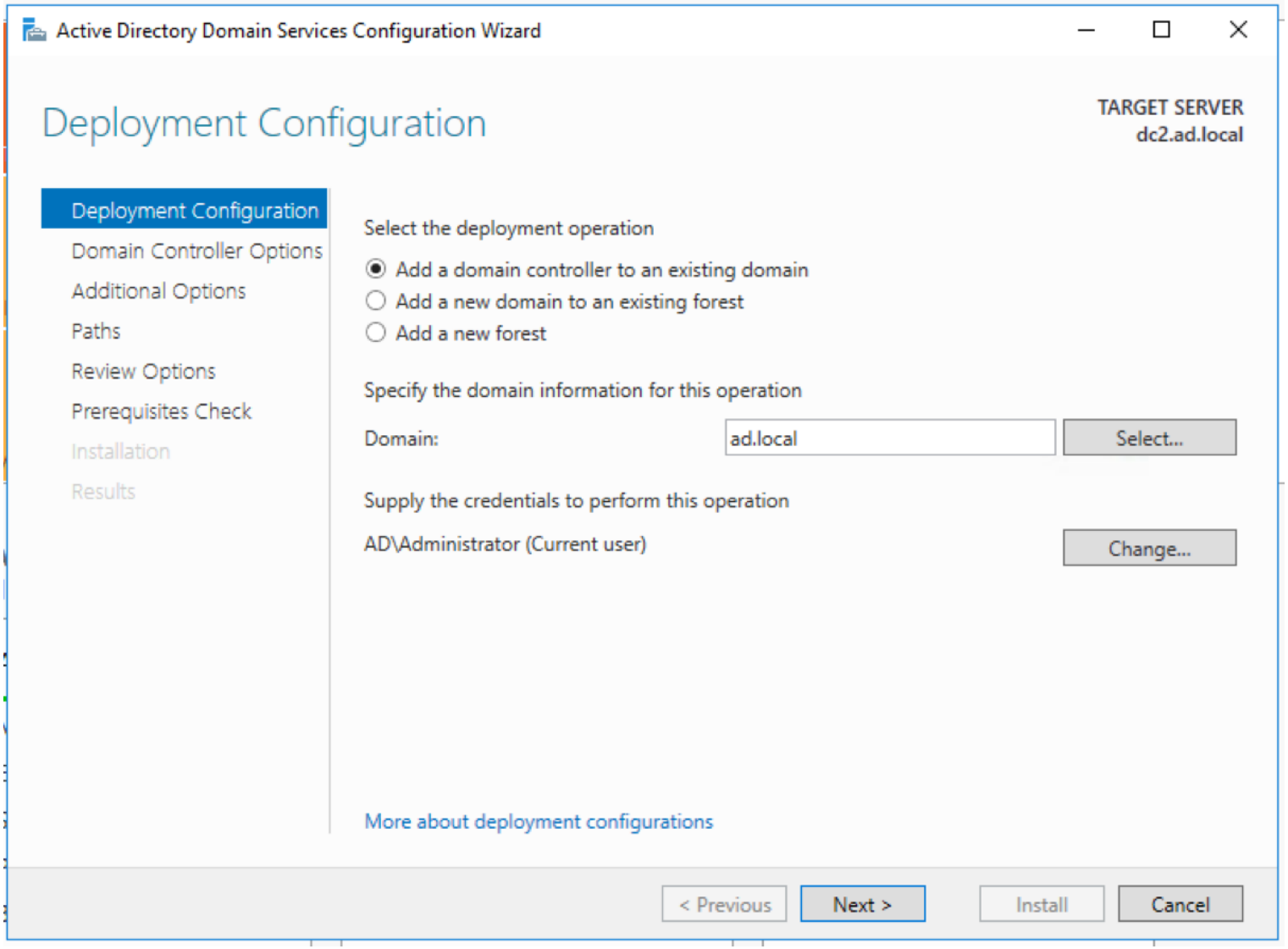
Povýšení DC2 3

- 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!

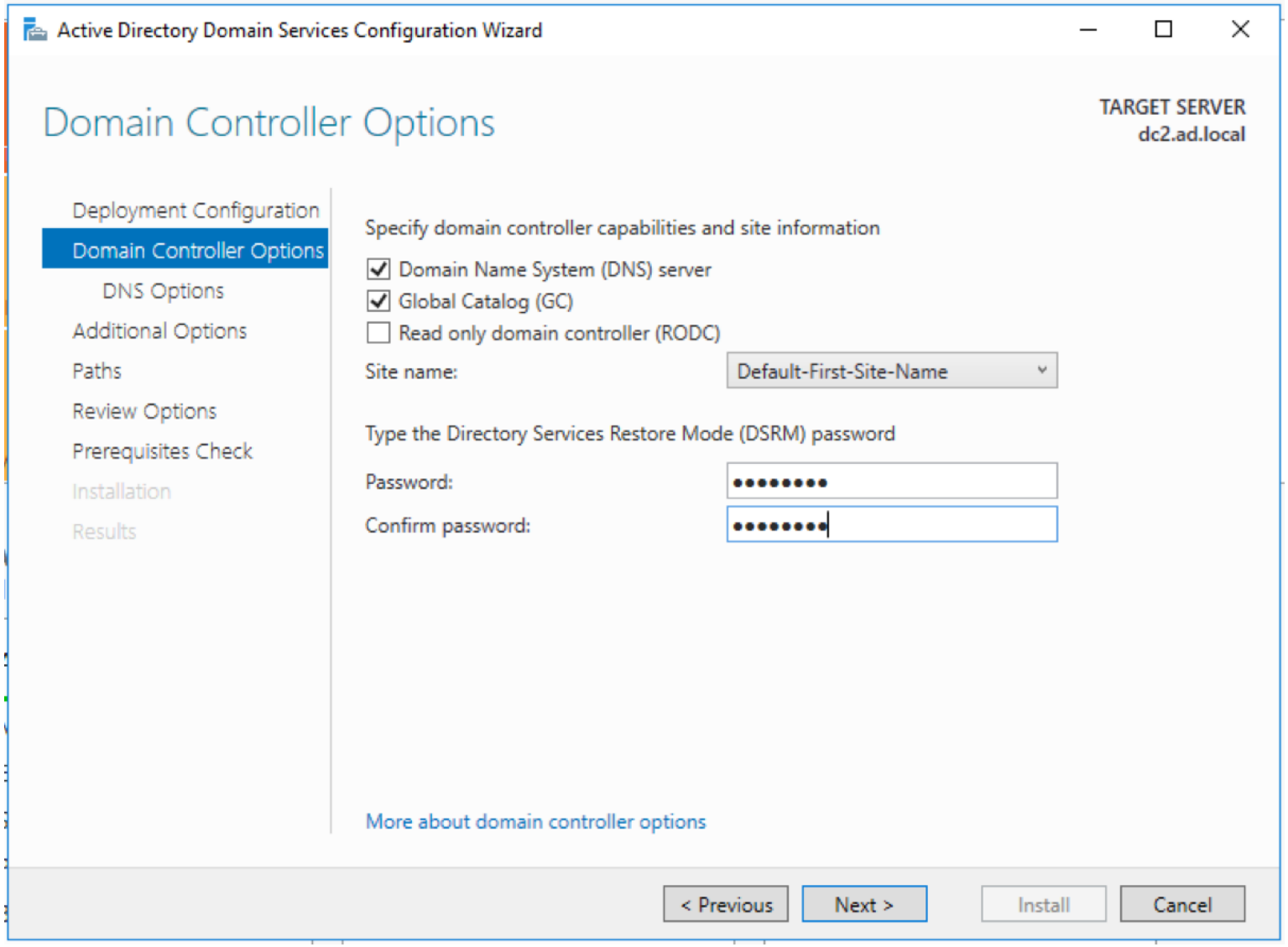
Povýšení DC2 4



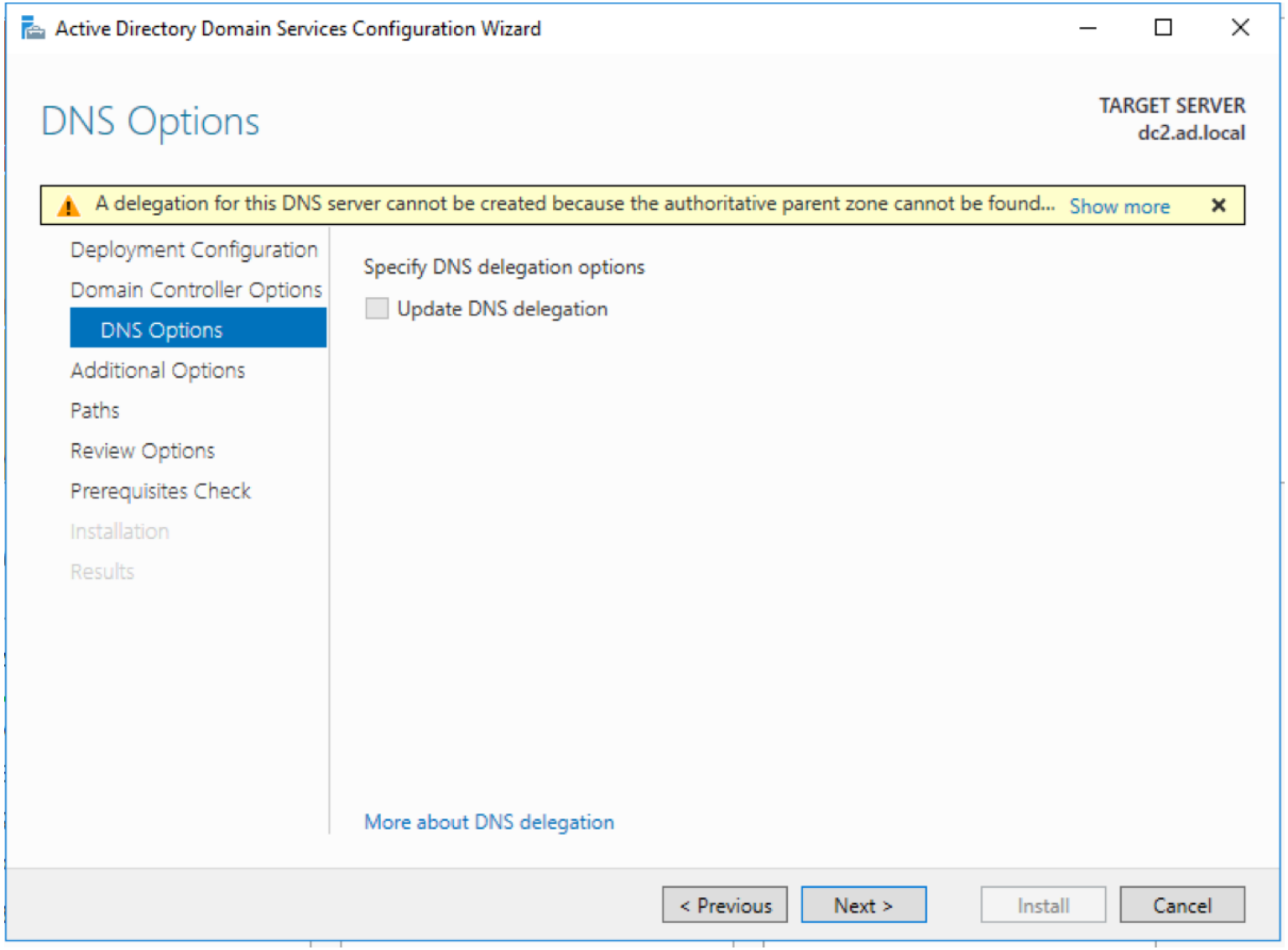
Povýšení DC2 5



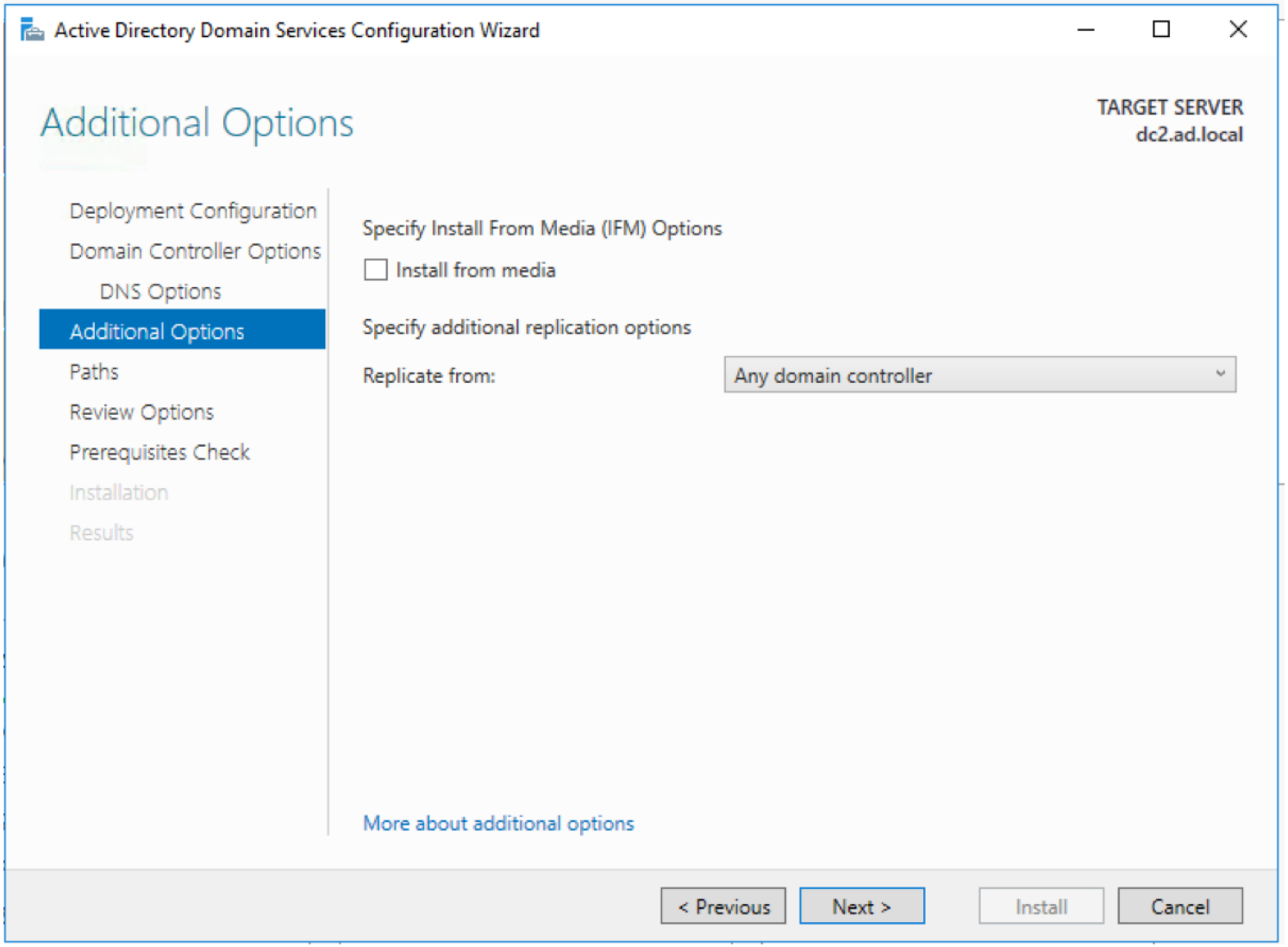
Povýšení DC2 6



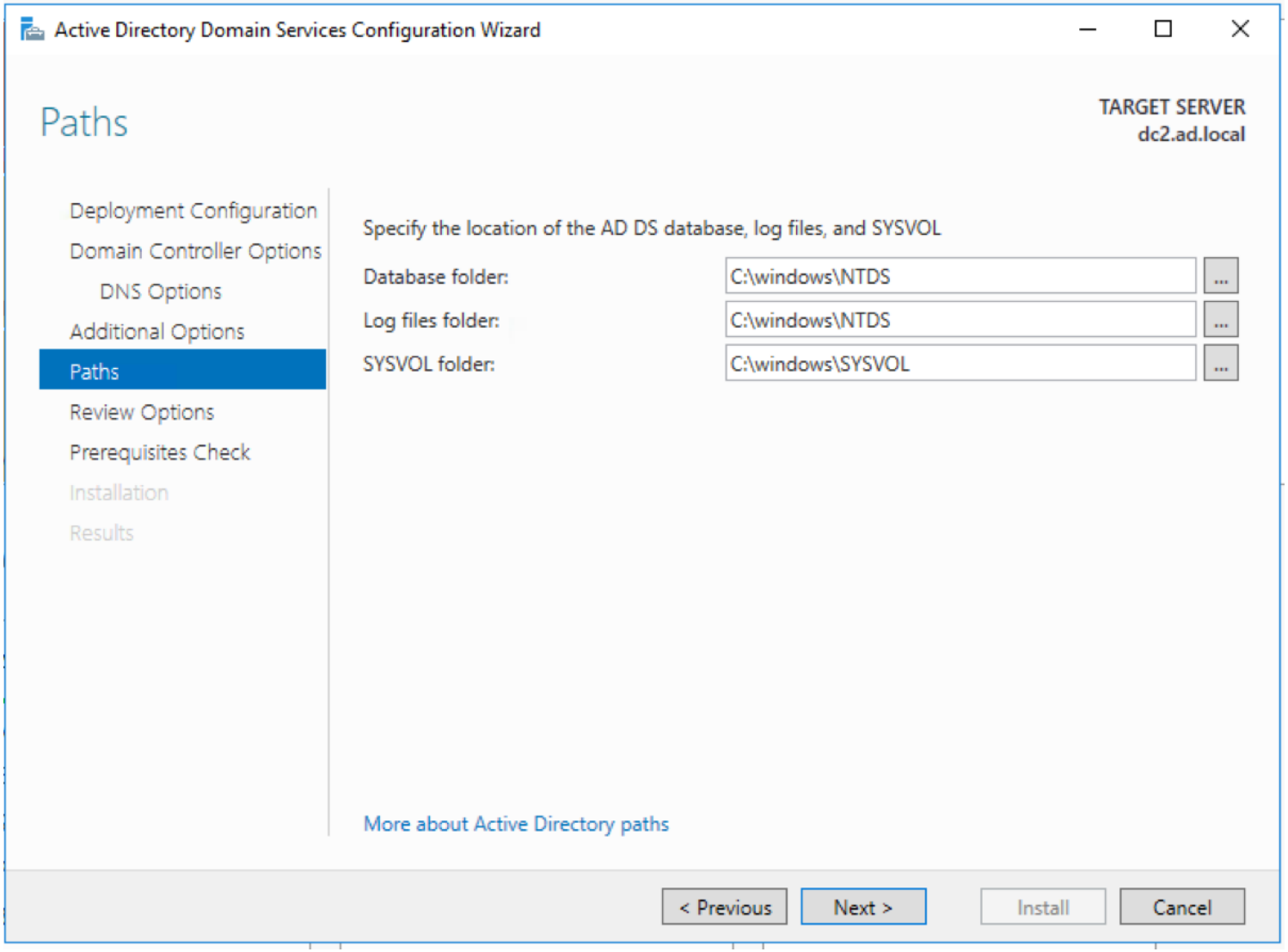
Povýšení DC2 7



Povýšení DC2 8

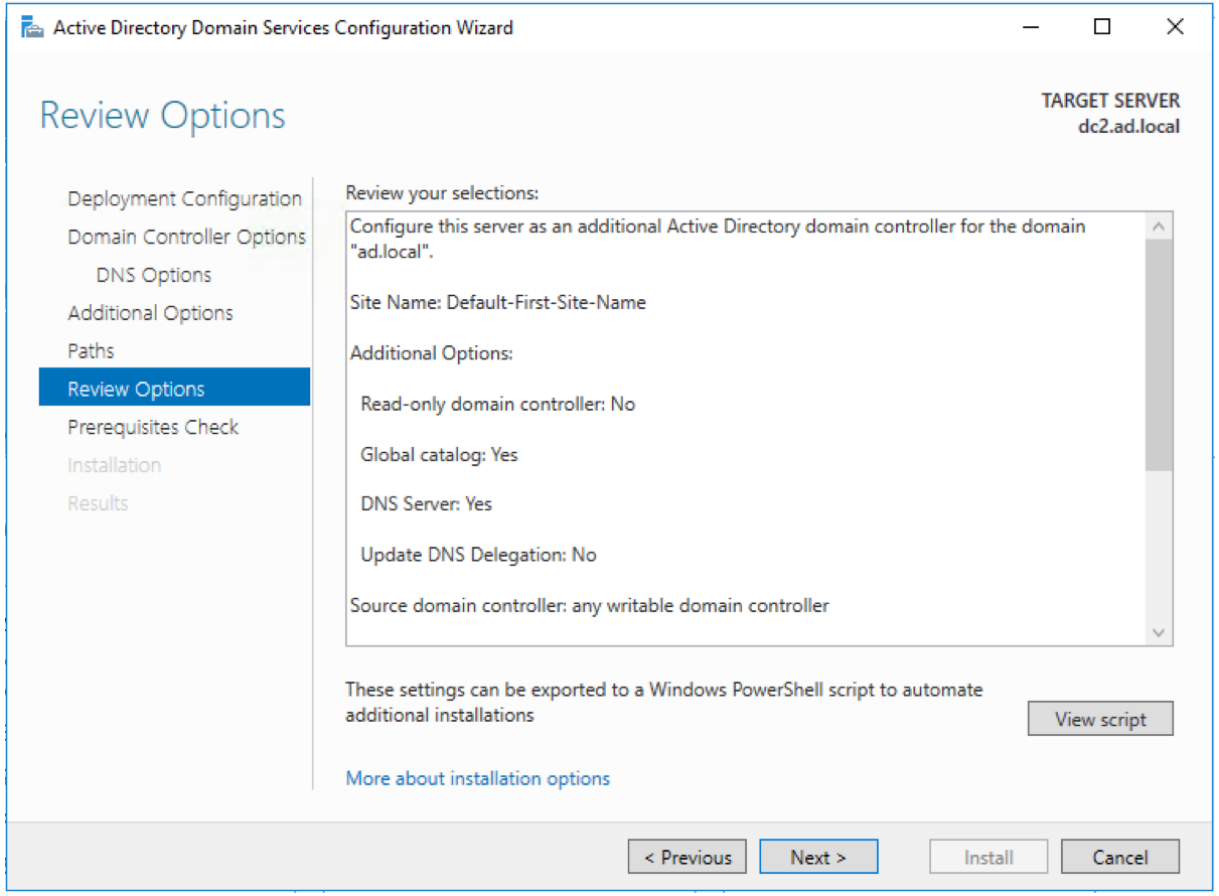


Povýšení DC2 9



Povýšení DC2 10

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

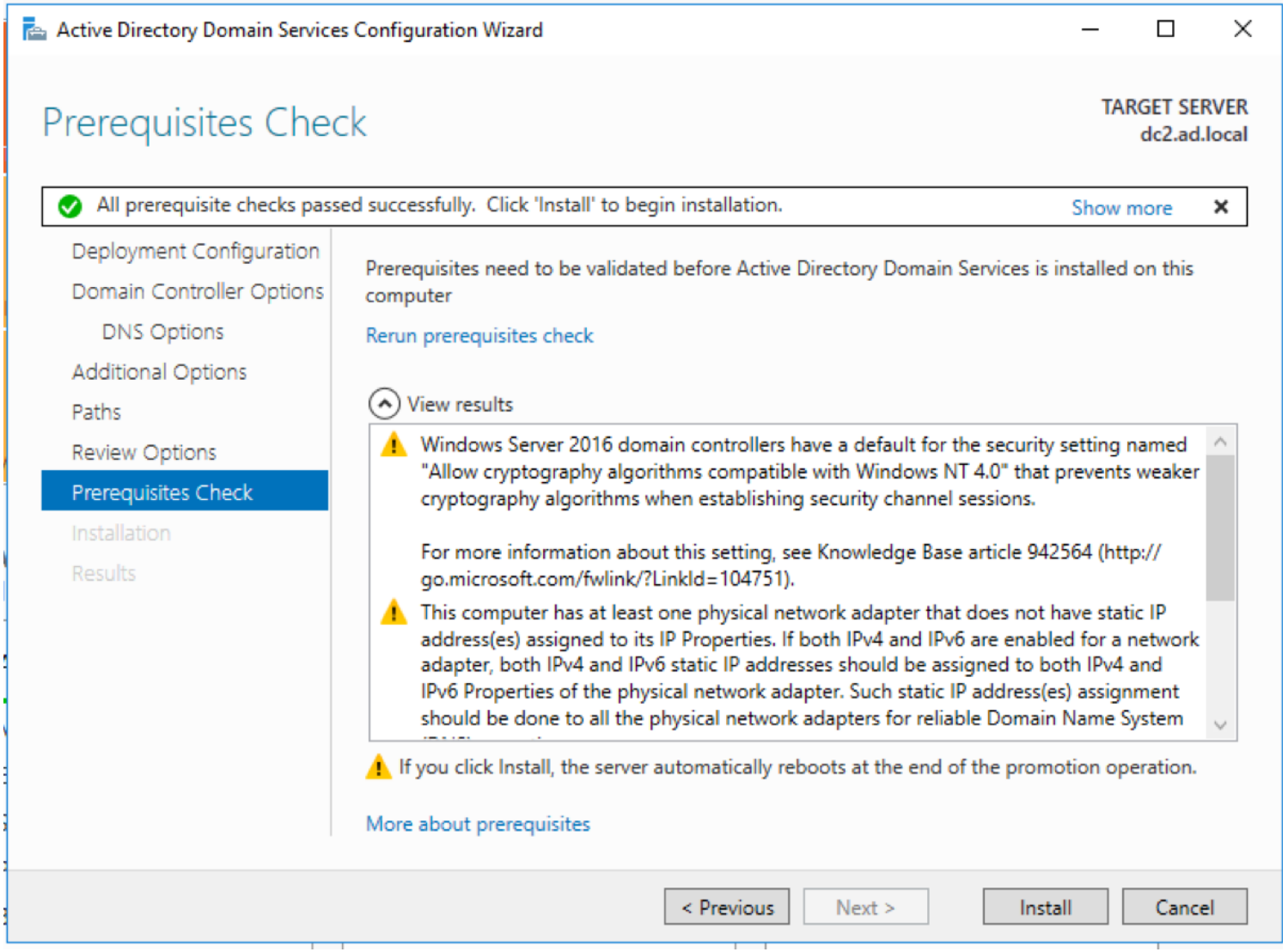


Povýšení DC2 11

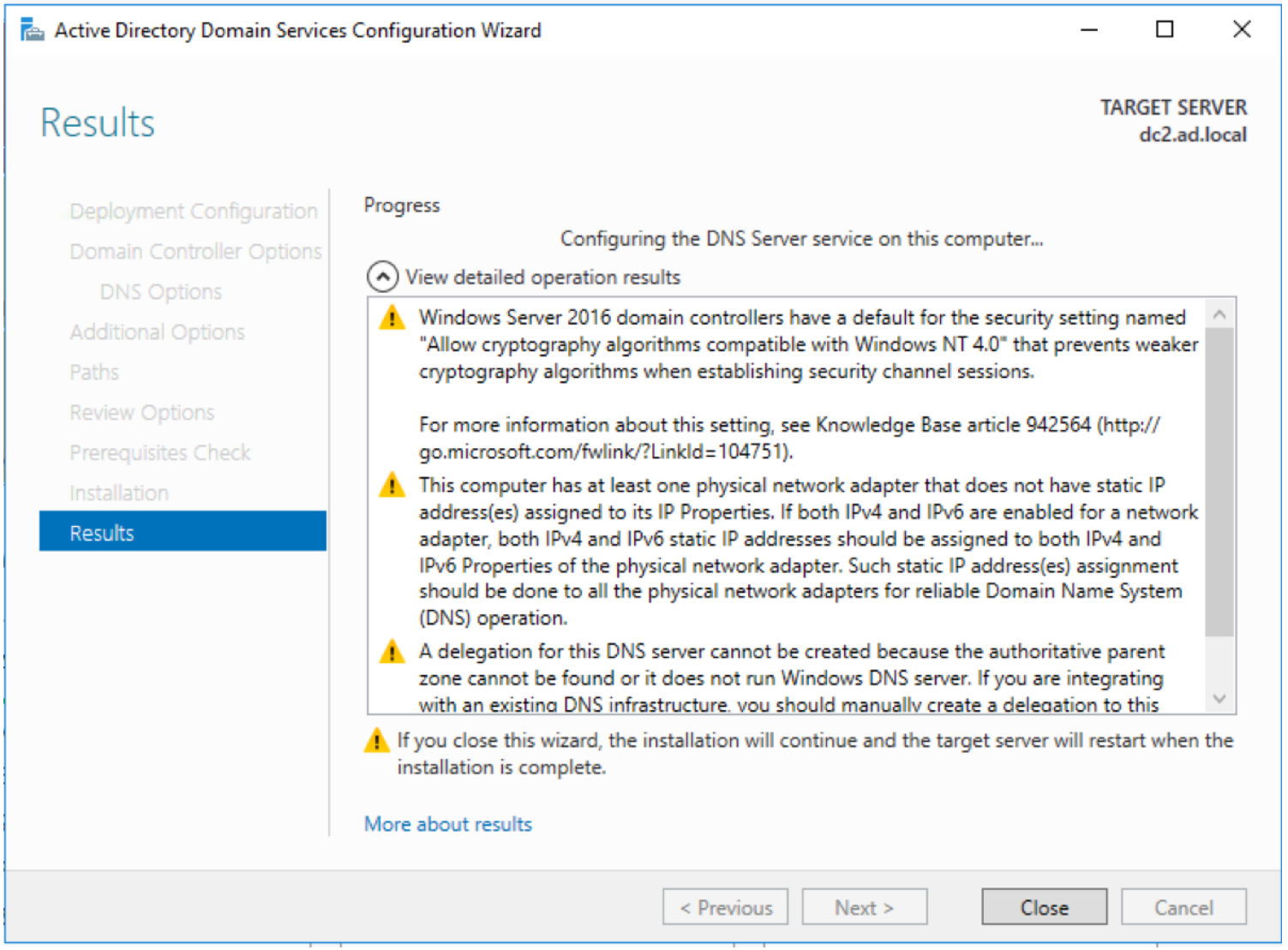
```
#
# Windows PowerShell script for AD DS Deployment
#

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:$false `
-SiteName "Default-First-Site-Name" `
-SysvolPath "C:\windows\SYSVOL" `
-Force:$true
```

Povýšení DC2 12



Povýšení DC2 13



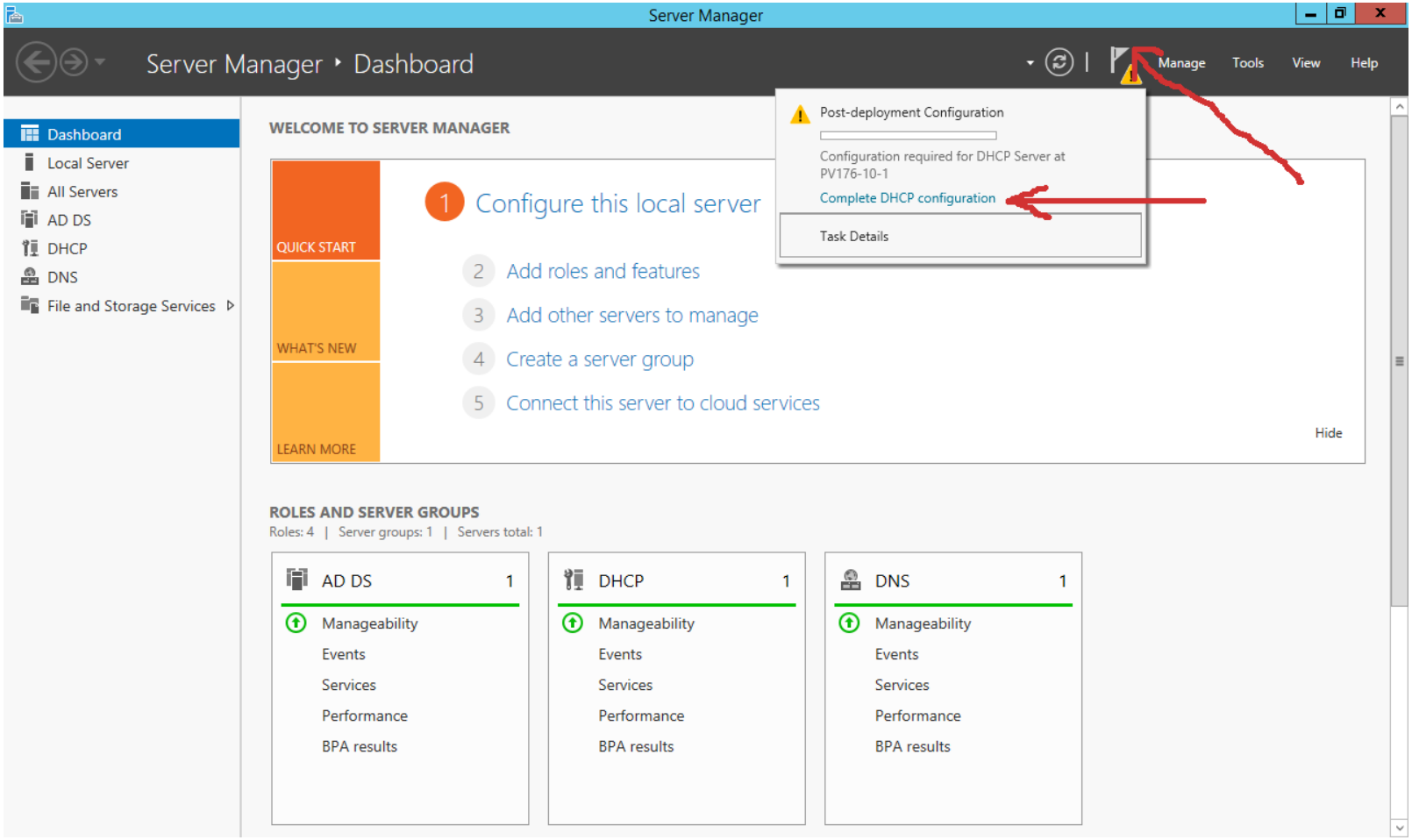
Povýšení DC2 14

- 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.

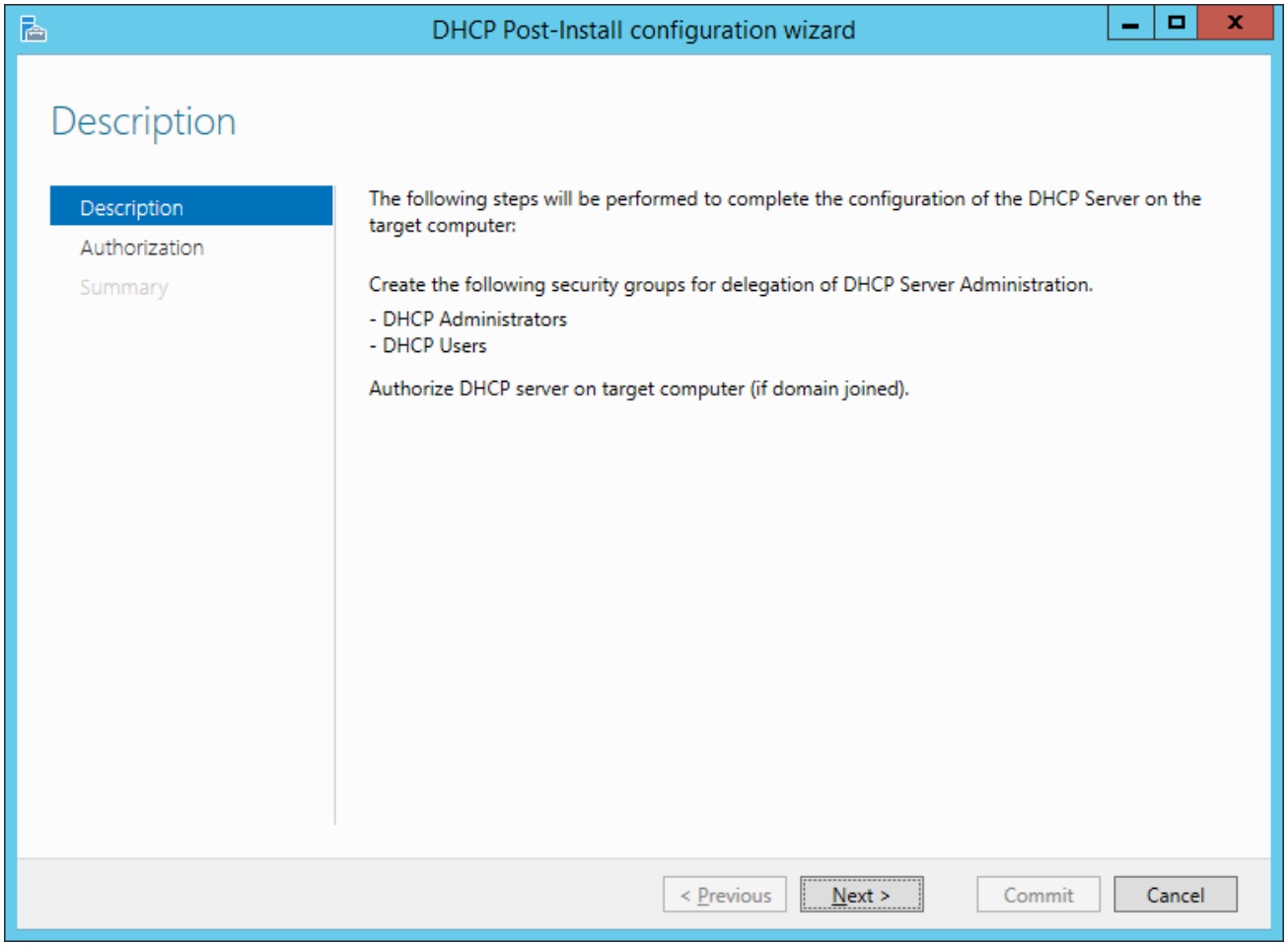
Rest of Domain Tasks 1

- 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).

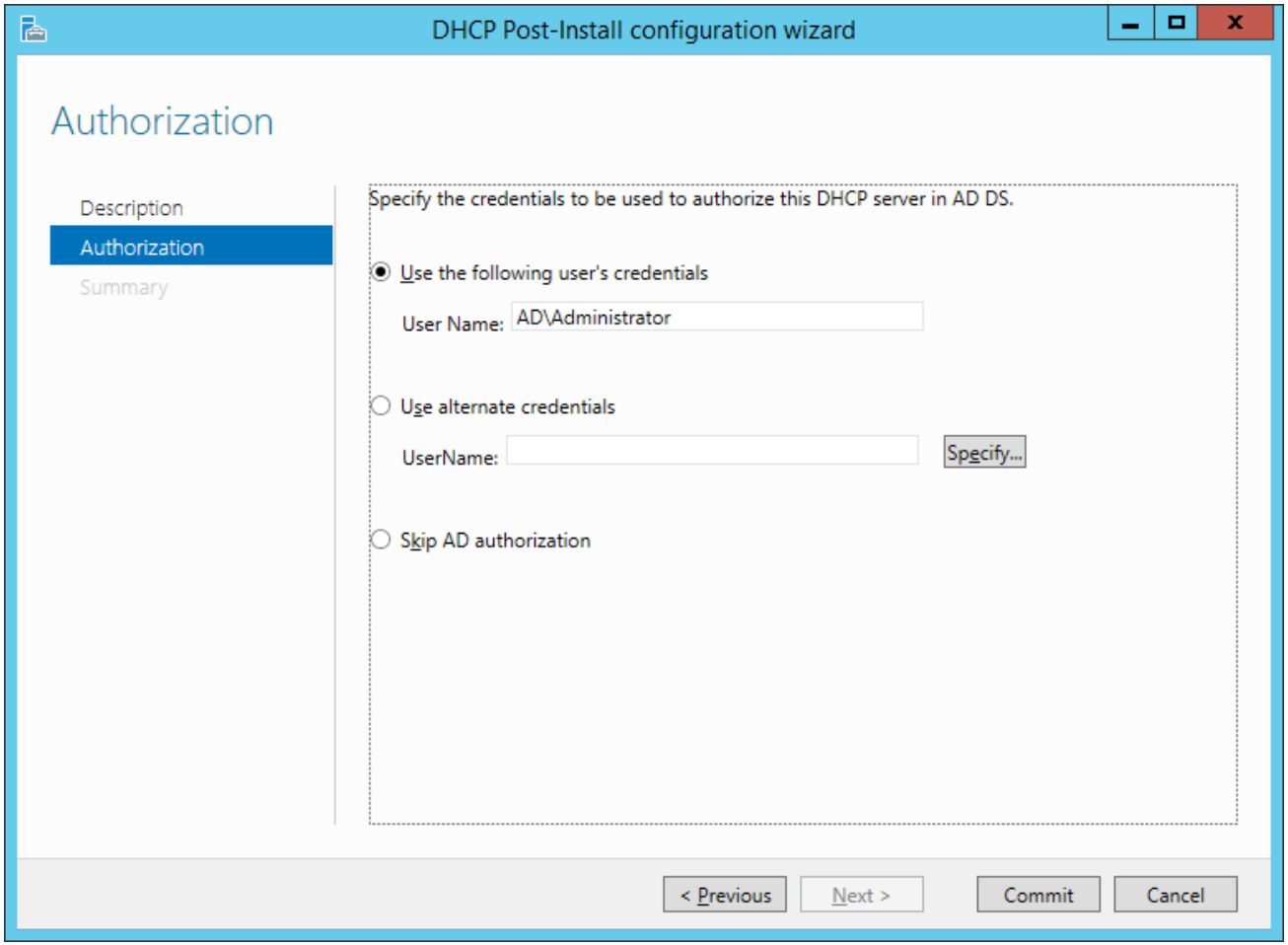
Rest of Domain Tasks 2



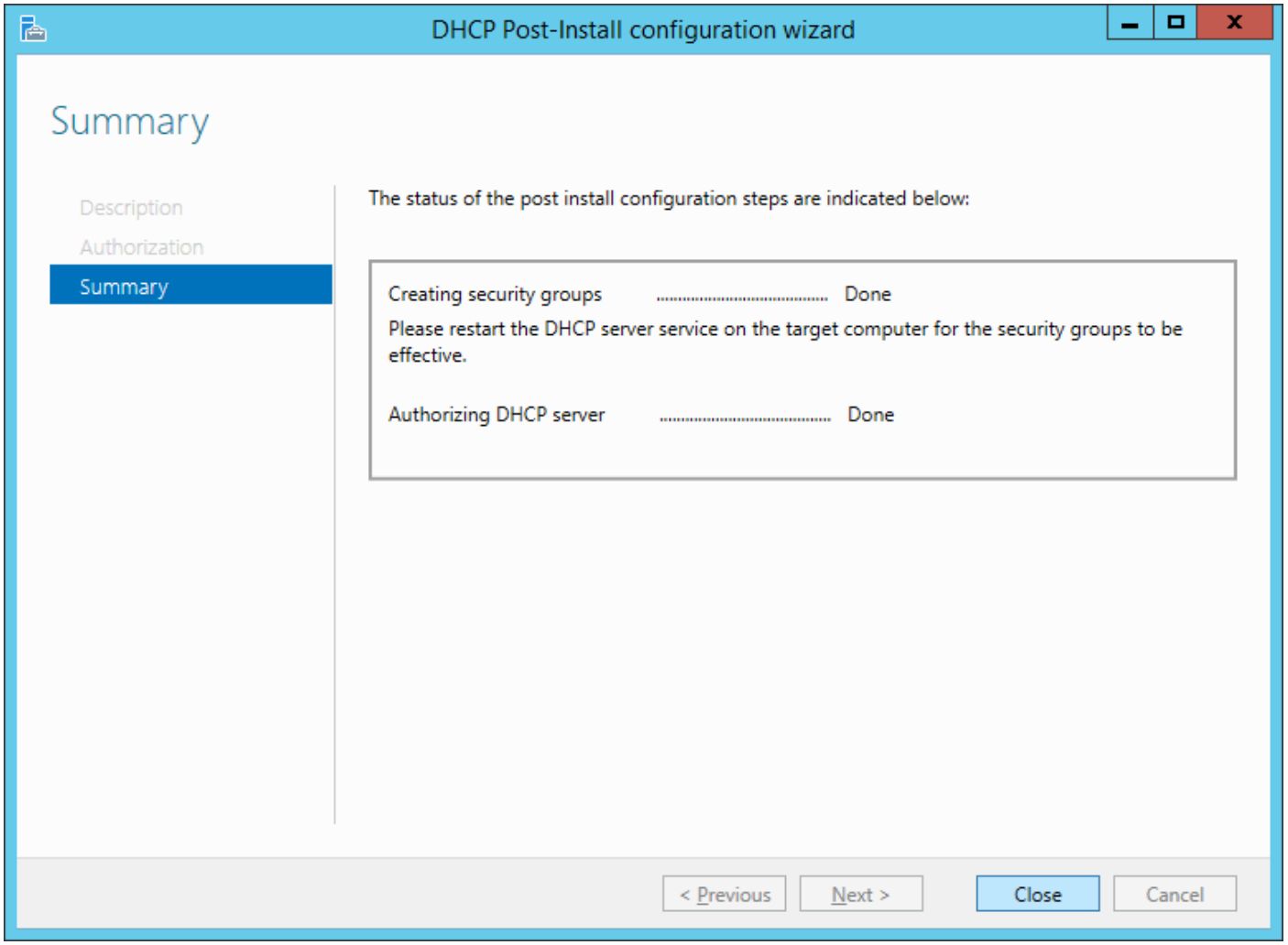
Rest of Domain Tasks 3



Rest of Domain Tasks 4



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)

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

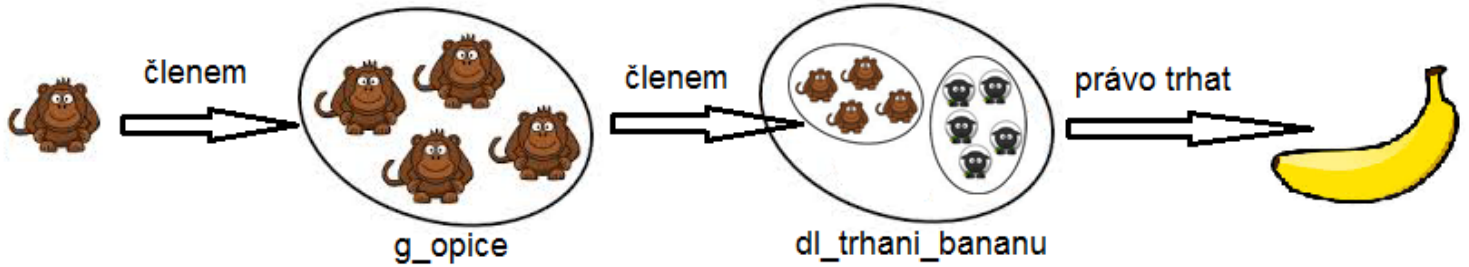
Bezpečnostní skupinu lze také použít pro skupinovou mailovou adresu – někteří správci distribuční adresy vůbec nepoužívají.

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

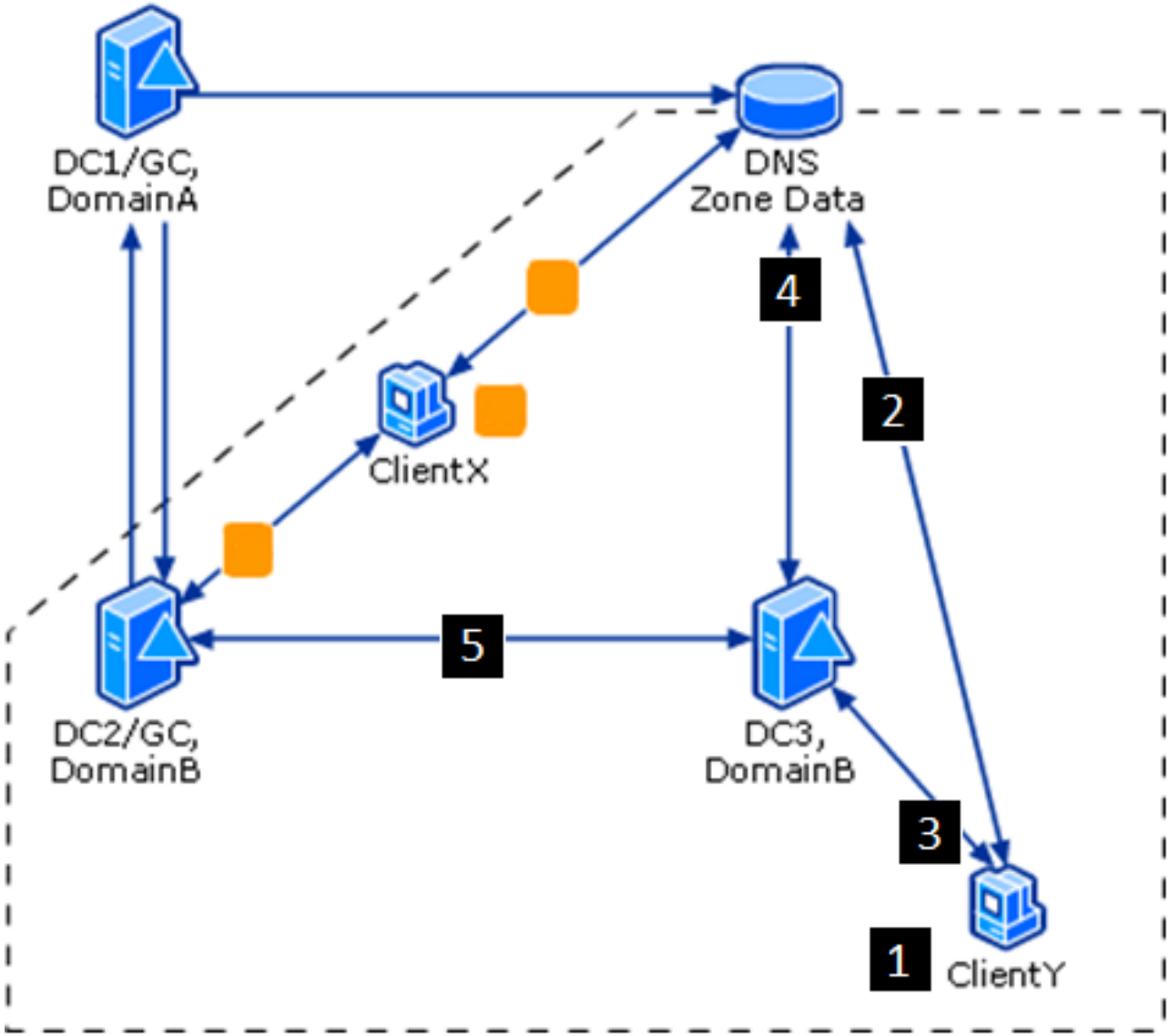
- Definovat konvence pro vytváření veškerých objektů
- Ulehčení vyhledávání, ulehčení skriptování, ulehčení správy
- AGDLP – Access Global Domain Local Permissions
- př. globální skupina g_opice, doménová lokální skupina dl_trhání_banánů



Autentizace uživatele v AD

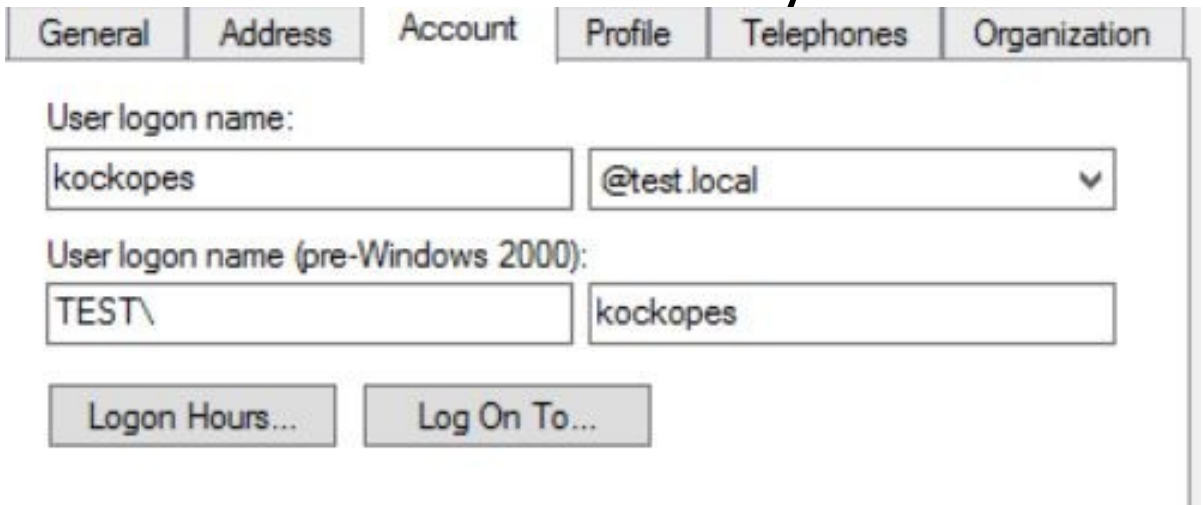
1. Uživatel zadává svůj login a heslo.
2. Stanice se ptá DNS, kde se nachází LDAP a Kerberos služba pro uživatelovu doménu. DNS poskytuje odpověď.
3. Stanice kontaktuje DC, jehož IP adresu dostala, a žádá o autentizaci uživatele.
4. DC ověřuje platnost loginu a hesla, jsou platné. DC ale není GC, takže 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



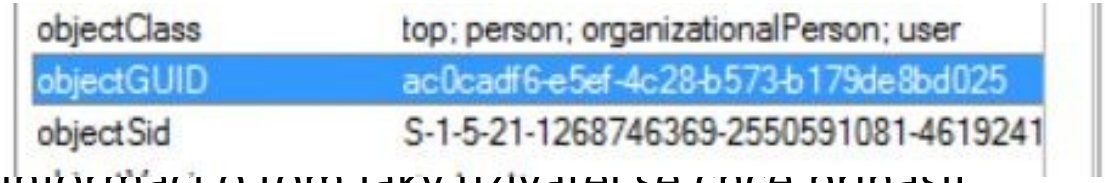
Identifikace objektu v LDAP

- 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



Identifikace objektu v LDAP

- SID
  - pokud uživatel změní doménu, změní se SID
  - udržuje se historie
  - SID existuje z historických kompatibilních důvodů
- GUID
  - nelze změnit
- UPN sufix
  - UPN tvoří přihlašovací informaci 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



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***
    - ldifde
    - 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

ldifde

- LDAP Data Interchange format directory exchange
- import/export účtů ve velkém množství
  - Import: ldifde –i –f INPUT.LDF
  - Export: ldifde –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 ldifde