Microsoft Windows Server [Povinné]

Vývojové kanály Windows Server [Povinné]

Od vydání Windows Server 2016 došlo ke sjednocení způsobu vývoje mezi klientskými a serverovými systémy Windows.

Long-Term Servicing Channel (LTSC)

Kanál „Long-term servicing channel“ je zaměřena na situace, kde je kladen důraz na maximální stabilitu, dlouhou životnost a minimální změny systémů. Životní cyklus této větve se podobá starším verzím Windows – vychází jen jednou za 2-3 roky a obsahuje pouze již ověřené a dostatečně stabilní funkce. Kritické bezpečnostní záplaty jsou garantovány po dobu 10 let. Nejnovějšími verzemi jsou Windows Server 2016 vydaný na podzim 2016 a Windows Server 2019 vydaný na podzim 2018.

Dříve označován jako Long-Term Servicing Branch.

Semi-Annual Channel (SAC)

Systémy Windows Server vydané pod Semi-Annual Channel vychází přibližně každého půl roku a jsou podporovány pouze po dobu 18 měsíců. V tomto se podobají aktuálnímu vývoji u Windows 10. V současné době jako SAC vychází pouze systémy ve variantách bez grafického rozhraní - Core a Nano. Verze v SAC se označují rokem a měsícem. Poslední verze je Windows Server, version 1809.

Vyhází ze staršího Current Branch for Business.

Edice [Povinné]

Windows Server je dostupný ve dvou edicích - Standard a Datacenter, lišících se především licenčním modelem a některými pokročilými funkcemi (jako Software-defined networks).[1] [2]

Systém Windows Server můžete nainstalovat v režimu with Desktop Experience, s plnohodnotným grafickým rozhraním, nebo v režimu Core.

Core [Povinné]

Režim instalace Core znamená instalaci systému s převážně textovým rozhraním a pouze s několika základními grafickými nástroji. Uvedení tohoto režimu bylo motivováno bezpečností (plnohodnotné GUI není nainstalováno a tedy nelze zneužít případné chyby) a snížením hardwarových nároků. Lokální správa se prování především pomocí PowerShellu, nástrojem sconfig a dalšími nástroji pro příkazový řádek.

Od Windows Server 2016 se jedná o výchozí režim instalace.

Nano [Povinné]

Windows Server Nano[3] je zcela samostatná minimalistická verze vycházející z režimu Core s úplně odstraněnou možností lokálního přihlášení (lze spravovat pouze vzdáleně) a s výrazně omezenou nabídkou rolí. Tato edice klade velký důraz na výkonnost a minimalismus a je určena výhradně pro běh

[1] https://docs.microsoft.com/en-us/windows-server/get-started/2016-edition-comparison
[2] https://docs.microsoft.com/en-us/windows-server/get-started-19/editions-comparison-19
[3] https://docs.microsoft.com/en-us/windows-server/get-started/getting-started-with-nano-server

v tzv. kontejnerech[4] (technologie Windows Containers a Docker), kdy je obraz systému poskládán z jednotlivých komponent a požadované aplikace. Aktualizace systému probíhá vytvořením nového obrazu systému s novější verzí komponent.

Možnosti administrace Windows Server [Povinné]

Windows Server lze spravovat několika způsoby[5] – grafickými (MMC, Server Manager), textovými, (PowerShell, příkazový řádek) a nejnověji i webovými nástroji.

Server Manager [Povinné]

Server Manager je grafický nástroj poskytující přehledné informace o jednom nebo více[6] systémech Windows Server. Využívá se pro správu (přidávání a odebírání) rolí a funkcí na jednotlivé spravované servery nebo i do virtuálních disků (offline).

Server Manager nabízí va základní pohledy na správu – přehled serverů (Local Server a All Servers), pod nimiž můžeme spravovat role, nebo z pohledu jednotlivých rolí, kde naleznete pouze servery nesoucí danou roli.

Na samotnou správu rolí pak většinou využívá níže uvedené MMC.

MMC [Povinné]

Microsoft Management Console je framework pro pokročilou správu systémů Windows v grafickém režimu. Skládá se ze tří podoken – navigačního panelu se stromovou hierarchií vlevo, středního panelu obvykle zobrazujícím detaily vybraných uzlů a pravým panelem s možnými akcemi. Pokročilejší nastavení se odehrává v samostatných dialogových oknech. Do MMC lze přidat jednotlivé konfigurační komponenty, tzv. snap-iny (Computer Management, Group Policy Management, …). Snap-iny lze přidávat do mmc.exe, nebo je volat samostatně ve formě *.msc souborů (např. compmgmt.msc, devmgmt.msc, …)

PowerShell [Povinné]

PowerShell lze použít jak k lokální, tak i k vzdálené správě systémů Windows s využitím WS-Management a WMI.

Jednou z variant jsou commandlety přijímající název vzdáleného počítače jako parametr (typicky přepínač -ComputerName), např. Restart-Computer. Další možností je vzdálené spuštění příkazu nebo skriptu pomocí Invoke-Command. Poslední možností je vytvoření interaktivního sezené pomocí Enter-PSSession.

Remote Server Administration Tools [Povinné]

Remote Server Administration Tools (RSAT)[7] je sada nástrojů (MMC a powershell modulů) určených pro vzdálenou správu jednotlivých rolí a funkcí systému Windows Server (2008 a novější) z jiného systému Windows, a to i klientského (v edici Pro nebo vyšší). Správce se tak nemusí přihlašovat na

[4] https://docs.microsoft.com/en-us/windows-server/get-started/nano-in-semi-annual-channel
[5] https://docs.microsoft.com/cs-cz/windows-server/administration/manage-windows-server
[6] https://docs.microsoft.com/en-us/windows-server/administration/server-manager/add-servers-to-server-manager
[7] https://support.microsoft.com/en-us/help/2693643/remote-server-administration-tools-rsat-for-windows-operating-systems

server lokálně ani přes vzdálenou plochu. U serverových Windows je RSAT součástí systému a jednotlivé nástroje lze aktivovat přidáním funkcí (features). U klientských systémů do Windows 10 1803 bylo nutné stáhnout instalační msu balíček z webu Microsoftu[8] a následně aktivovat požadované nástroje průvodcem Turn Windows features on or off, od verze 1810 je RSAT zahrnut přímo ve Windows 10 jako Feature on demand.

Windows Admin Center [Povinné]

Windows Admin Center[9] (WAC, dříve známý pod názvem Project Honolulu) je nová variace na Server Manager a různé MMC konzole, dostupná přes webové rozhraní (webovým prohlížečem). Podporuje správu serverových systémů od Windows Server 2008 R2, klientských systémů Windows 10 a také napojení na Azure Services.

Oproti starším nástrojům je jeho cílem především správa mnoha zařízení z jednoho místa (včetně tzv. hybridních cloudových scénářů), multiplatformní přístup (prohlížeč), ale také vyšší bezpečnost (lze definovat přístupová práva na úrovni rolí).

Windows Admin Center lze nainstalovat ve dvou režimech – na klientské na Windows 10 (v. 1709) jako lokální webová aplikace (Desktop Mode) a v režimu síťové služby Windows Admin Center gateway (Gateway mode) na serverové systémy. Komunikace probíhá po HTTPS a od gateway k jednotlivým spravovaným serverům pomocí PowerShell Remoting, WinRM.

V současné době WAC nenahrazuje veškerou funkcionalitu/možnosti nastavení známé z MMC.

Role Remote Access Server [Povinné]

Jedná se o jednu z nejstarších a základních rolí Windows Server, dříve označovanou jako Routing and Remote Access Services. Skládá se ze tří základních služeb – Routing, kdy může server fungovat jako síťový router, resp. NAT, DirectAccess and VPN (RAS) zajišťující vzdálený přístup do sítě VPN, a Web Application Proxy umožňující zpřístupnit vybrané HTTP/HTTPS aplikace z vnitřní sítě do klientským zařízením ve vnější síti.

[8] https://www.microsoft.com/en-us/download/details.aspx?id=45520
[9] https://docs.microsoft.com/en-us/windows-server/manage/windows-admin-center/overview

Studentské úkoly

- Pro přístup na server **file** (a jiné) přes síťové rozhraní *Default switch* je nutné použít jeho plně kvalifikované doménové jméno **file.nepal.local**
- Přístupové údaje na server **file**: **nepal\hstudent** heslo: **aaa**
- Rozsah IP adres přidělených z *Default switch* se může od níže uvedeného rozsahu lišit.

Lab S00 – konfigurace virtuálních stanic

[Projít]

Připojte sítové adaptéry stanic k následujícím virtuálním přepínačům:

Adaptér (MAC suffix)	LAN1 (-01)	LAN2 (-02)	LAN3 (-03)	LAN4 (-04)
w10-base	Nepřipojeno	Private1	Nepřipojeno	Nepřipojeno
w2016-base	Nepřipojeno	Private4	Nepřipojeno	Nepřipojeno
w2019-core	Default Switch	Private1	Private4	Nepřipojeno

- v případech, kdy je potřeba přistupovat na externí síť z **w10-base** a **w2016-base**, připojte adaptér **LAN1** k přepínači *Default switch*.

Lab S01 – dokončení základní instalace Windows Server Core

[Povinné]

Cíl cvičení

Dokončit instalaci Windows Server 2019 Standard Core

Potřebné virtuální stroje

w2019-core (w2019-core OOBE)

Další prerekvizity

Virtuální disk s Windows Server 2019 Standard Core vzniklý aplikací bitové kopie skriptem Convert-WindowsImage.ps1

1. Spusťte VM **w2019-core OOBE** a počkejte na dokončení konfigurace HW a následný restart
   - trvá asi 3 minuty.
2. Budete vyzváni k nastavení hesla uživatele **administrator**
   a. Zvolte OK a potvrďte klávesou Enter
   b. Zadejte nové heslo **aaaAAA111** a pokračujte Tab
      - (musí splňovat standardní požadavky na komplexitu – 8 znaků a 3 ze 4 skupin: velká písmena, malá písmena a číslice a speciální znaky)
   c. Zopakujte nové heslo, potvrďte Enter, následně zvolte OK a opět potvrďte Enter
3. Přihlaste se novým heslem
4. Nyní přejmenujte server
   a. Spusťte nástroj **Server Configuration**
      - V příkazovém řádku zadejte příkaz **sconfig**
   b. Zvolte volbu **2** Enter
   c. Zadejte nové jméno **w2019-core** a potvrďte Enter
   d. Zobrazí se dialog, zda chceme server rovnou restartovat, zvolte Yes

Lab S02 – místní správa Windows Server Core

[Povinné]

Cíl cvičení

Seznámit se se základy místní správy Windows Server Core

Potřebné virtuální stroje

w2019-core (w2019-core OOBE)

Další prerekvizity

Dokončený úkol S01.

1. Přihlaste se k **w2019-core** jako uživatel **administrator** s heslem **aaaAAA111**
2. Zavřete okno příkazového řádku
3. Pokuste se znovu otevřít příkazový řádek
   a. Vyvolejte správce úloh (**Task Manager**) pomocí Ctrl + Alt + Del a výběru z nabídky
      - Alternativně lze použít i Ctrl + Shift + Esc
   b. Přepněte se do pokročilého zobrazení pomocí More details
   c. Z nabídky File vyberte Run new task
   d. Zadejte **cmd** a potvrďte
   e. Zavřete okno správce úloh
4. Spusťte nástroj **Server Configuration** v novém okně
   a. V příkazovém řádku zadejte příkaz **start sconfig**
5. Nastavte správnou časovou zónu
   a. V nástroji **Server Configuration** vyberte volbu **9**
   b. V okně Date and Time klikněte na Change time zone
   c. Vyberte **(UTC+01:00) … Prague** a potvrďte OK
   d. Zavřete okno Date and Time
6. Nastavte IP adresu síťového rozhraní s MAC 20-19-EE-00-00-02
   a. V nástroji **Server Configuration** vyberte volbu **8**
   b. V okně příkazového řádku použijte **ipconfig /all** pro identifikaci jednotlivých síťových adaptérů, najděte adaptér s požadovanou MAC adresou a poznačte si jeho popis (description).
   c. Vraťte se do okna **Server Configuration**
   d. Zadejte číslo (index) adaptéru s popisem poznačeným v bodě b.
   e. Zobrazí se informace o stávajícím nastavení
   f. Pokračujte volbou **1** pro nastavení IP adresy
   g. Pro statickou IP adresu zvolte **S**
   h. Zadejte
      - IP: **10.10.10.1**
      - Maska: **255.255.255.0**
      - Výchozí brána: nevyplňovat
   i. Volbou **4** vyskočte z nabídky nastavení síťového rozhraní (Network Adater Settings)

   Pozn: Alternativně lze použít **netsh**
7. Nastavte IP adresu síťového rozhraní s MAC 20-19-EE-00-00-03
   a. Opakujte postup z bodu 6
      - IP: **192.168.200.1**
      - Maska: **255.255.255.0**
      - Výchozí brána: nevyplňovat
8. Ověřte, zda má rozhraní s MAC 20-19-EE-00-00-01 přidělenou IP adresu z DHCP serveru a fungující konektivitu do internetu
   a. Pomocí výpisu z **ipconfig /all**
   b. Pomocí **ping file.nepal.local**
      - Alternativně zkuste nějakou veřejnou IP (např. Google public DNS 8.8.8.8 a 8.8.4.4, Cloudflare public DNS 1.1.1.1, …) nebo přímo doménové jméno

9. Ověřte, že je povolena vzdálená správa
    a. V **Server Configuration** zkontrolujte stav u položky 4) Configure Remote Management.
    b. Pokud zde není uvedena hodnota Enabled, zadejte volbu **4** a následně volbu **1** (Enable Remote Management). Potvrzovacím dialog zavřete tlačítkem OK.

Lab S03 – Příprava základní topologie sítě [Povinné]

Cíl cvičení

Vytvořit síť podle topologického schématu na obrázku Obrázek 1 a ověřit konektivitu pomocí **ping**.

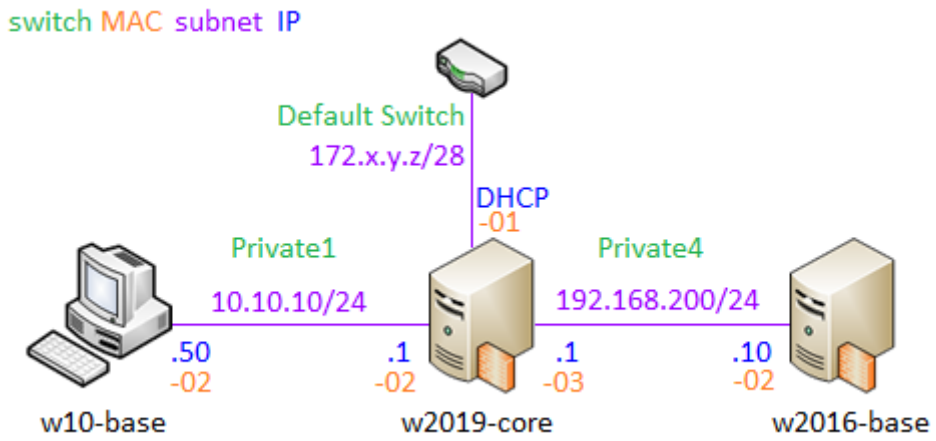
Potřebné virtuální stroje

w10-base
w2016-base
w2019-core (w2019-core OOBE)

Další prerekvizity

Dokončený úkol S02

1. Přihlaste se k **w10-base** jako uživatel **student** s heslem **aaa**
2. Na **w10-base** nastavte pomocí grafického rozhraní příslušnou *IPv4 adresu*, *masku podsítě* a *výchozí bránu* na základě schématu na obrázku 1
    a. Otevřete okno **Network Connections** (Settings – Network & Internet – Ethernet – Change adapter options), zvolte LAN2 a pak Properties
        ➢ Zvolené síťové rozhraní musí odpovídat *Private1*, standardně to je LAN2
    b. Vyberte Internet Protocol Version 4 (TCP/IPv4) a zvolte Properties
    c. Zvolte Use the following IP address a jako IP address zadejte **10.10.10.50**
    d. Klikněte do zadávacího pole u Subnet mask a zadejte **255.255.255.0**
    e. U Default gateway zadejte **10.10.10.1**
    f. Potvrďte OK



Obrázek 1. Schéma základní topologie sítě

3. Přihlaste se k **w2016-base** jako uživatel **administrator** s heslem **aaa**
4. Na **w2016-base** nastavte pomocí příkazové řádky příslušnou *IPv4 adresu*, *masku podsítě* a *výchozí bránu* na základě schématu na obrázku 1
    a. Spusťte následující příkaz **netsh interface ip set address name="LAN2" source=static addr=192.168.200.10 mask=255.255.255.0 gateway=192.168.200.1**

- Název **name** musí odpovídat síťovému rozhraní *Private4*, standardně to je LAN2

5. Nyní na firewallech všech tří stanic povolte ICMP Echo Request (ping) - na všech profilech v příchozím i odchozím směru.
   a. Spusťte **PowerShell**
      - w2019-core: v příkazové řádce zadejte příkaz **start powershell**
      - w10-base: spustit jako **administrátor**
   b. Zadejte příkaz: **Get-NetFirewallRule | where-object {$_.DisplayName -like "File*Echo Request*" -and $_.Enabled -eq "False"} | Enable-NetFirewallRule**

Lab S04 – příprava na vzdálenou správu Windows Server bez domény – na stanici, odkud budeme spravovat [Povinné]

Cíl cvičení

V naší infrastruktuře máme dva samostatné servery, které si navzájem nedůvěřují, a také nemáme zajištěn překlad jmen na IP adresy (nemáme DNS a Windows Server Core má ve výchozím nastavení deaktivovaný protokol NetBIOS).

Potřebné virtuální stroje

w2016-base

Další prerekvizity

Dokončený úkol S03.

1. Přihlaste se k **w2016-base** jako uživatel **administrator** s heslem **aaa**
2. Do souboru **C:\Windows\System32\drivers\etc\hosts** přidejte záznam odkazující na server **w2019-core** a soubor uložte:
   192.168.200.1 w2019-core
3. Přidejte server **w2019-core** mezi důvěryhodné servery vzdálené správy
   - bylo by to nutné i v případě místního serveru v doméně a samostatného vzdáleného serveru
   a. Spusťe **PoweShell** a zadejte příkaz:
   Set-Item wsman:\localhost\Client\TrustedHosts w2019-core -Concatenate -force
4. Uložte alternativní přístupové údaje k serveru **w2019-core**
   - v případě serverů v doméně není nutné
   a. V příkazovém řádku nebo v **PowerShellu** zadejte:
   cmdkey /add:2016-core /user:w2019-core\administrator /pass:aaaAAA111
   - pokud vypustíte parametr /pass:, jednotlivé nástroje by se měly na heslo doptat (ale některé se neptají, např. Server Manager)

Lab S05 – příprava na vzdálenou správu Windows Server pomocí UI – na spravované stanici [Povinné]

Cíl cvičení

Připravit Windows Server Core na příchozí připojení využívaná jednotlivými MMC snap-iny

Potřebné virtuální stroje

w2019-core

1. Přihlaste se k **w2019-core** jako uživatel **administrator** s heslem **aaaAAA111**
2. Spusťte **PowerShell**
3. Zadejte příkazy:
   # snap-in Event Viewer

Enable-NetFirewallRule -DisplayGroup "Remote Event Log Management"
snap-in Services
Enable-NetFirewallRule -DisplayGroup "Remote Service Management"
snap-in Shared Folders
Enable-NetFirewallRule -DisplayGroup "File and Printer Sharing"
snap-in Task Scheduler
Enable-NetFirewallRule -DisplayGroup "Performance Logs and Alerts"
snap-in Disk Management
Enable-NetFirewallRule -DisplayGroup "Remote Volume Management"
snap-in Windows Firewall with Advanced Security
Enable-NetFirewallRule -DisplayGroup "Windows Defender Firewall Remote Management"
u w2016: Enable-NetFirewallRule -DisplayGroup "Windows Firewall Remote Management"

Pozn: některé snap-iny vyžadují i další konfiguraci jako spuštění některých služeb apod.

Lab S06 – vzdálená správa Windows Server pomocí UI

[Povinné]

Cíl cvičení

Seznámit se se základy vzdálené správy Windows Server s využitím grafických nástrojů

Potřebné virtuální stroje

w2016-base
w2019-core (w2019-core OOBE)

Další prerekvizity

Dokončené úkoly S04 a S05.

1. Přihlaste se k **w2016-base** jako uživatel **administrator** s heslem **aaa**
2. Otevřete **Server Manager**
3. Z nabídky Manage vyberte Add Servers
4. Vyhledejte server **w2019-core** podle názvu
   a. Přepněte na panel DNS
   b. Do vyhledávacího pole zadejte **w2019-core** a dejte vyhledat
   c. Pomocí tlačítka > přidejte nalezený server do seznamu vybraných a potvrďte OK
      ➢ **Server Manager** se pokusí zkontaktovat server **w2019-core**
5. Přejděte na All Servers
   a. Ověřte, že server **w2019-core** byl přidán mezi spravované servery
6. Pokud se nepodařilo přihlášení stávajícím účtem nebo uloženými údaji (viz úkol S04 bod 4)
   a. Po chvíli ve sloupci Manageability naleznete informaci **"Online – access denied"**
   b. Z kontextové nabídky nad záznamem **w2019-core** vyberte Manage As …
   c. Zadejte přihlašovaní údaje:
      w2019-core\administrator s heslem **aaaAAA111**
      ➢ **Server Manager** se opět pokusí zkontaktovat server w2019-core, tentokrát se správnými přihlašovacími údaji
7. Z kontextové nabídky nad **w2019-core** vyberte Computer Management
   a. Dojde ke spuštění standardní MMC Computer Management připojené k serveru **w2019-core**. Obdobně lze připojit téměř jakoukoliv MMC

Lab S07 – instalace role RAS na vzdálený server [Povinné]

Cíl cvičení

Vzdáleně nainstalovat roli Remote Access Server na w2019-core

Potřebné virtuální stroje

w2016-base
w2019-core (w2019-core OOBE)

Další prerekvizity

Dokončený úkol S06.

1. Přihlaste se k w2016-base jako uživatel administrator s heslem aaa
2. Spusťte **Server Manager**
   a. Start → **Server Manager**
3. Nainstalujte roli **Routing and Remote Access**
   a. Vyberte Add Roles and Features z nabídky Manage
   b. Pokračujte Next >
   c. Vyberte Role-based or feature-based installation a pokračujte Next >
   d. Vyberte server **w2019-core** a pokračujte Next >
   e. V kroku *Server Roles* zaškrtněte **Remote Access** a pokračujte Next >
   f. V kroku *Features* pokračujte Next >
   g. V kroku *Remote Access* pokračujte Next >
   h. V kroku Role Services zaškrtněte službu **Routing** a v dialogu se závislostmi potvrďte Add Features, pokračujte Next >
      ➢ Pozn.: dojde k zatržení služby DirectAccess and VPN (RAS)
   i. V kroku *Confirmation* zaškrtněte Restart he destination server automatically if required
   j. Všimněte si možnosti exportu nastavení a možnosti specifikace instalačního zdroje
   k. Spusťte instalaci pomocí Install
      ➢ Instalace může zabrat několik minut, v jejím průběhu můžete začít následující úkol.
   l. V kroku *Results* nyní můžete vidět rekapitulaci rolí a funkcí, které se právě instalují. Okno průvodce můžete zavřít pomocí Close a instalace bude probíhat na pozadí.
4. Stav dokončení instalace naleznete v **Server Manager** při rozkliknutí Notification (vlaječka) jako položku Feature installation
5. Pokud máte lokálně přihlášeného uživatele na serveru **w2019-core**, nemusí dojít k automatickému restartu serveru **w2019-core**.
   a. V **Server Manager** zvolte All Servers
   b. Z kontextové nabídky serveru **w2019-core** zvolte Restart Server a dotaz potvrďte OK
   a. Vyčkejte na dokončení restartu
6. Přihlaste se lokálně na k **w2019-core** jako uživatel **administrator** s heslem **aaaAAA111**
7. Spusťte **PowerShell**
8. Zadejte příkaz a ověřte, že došlo k instalaci role **Remote Access**
9. **Get-WindowsFeature | where-object {$_.InstallState -eq "Installed"}**

Lab S08 – Instalace nástrojů vzdálené správy Remote Server Administration Tools [Povinné]

Cíl cvičení

Nainstalovat nástroje správy role RAS na server w2016-base

Potřebné virtuální stroje

w2016-base

Další prerekvizity

Dokončené úkoly S06.

1. Přihlaste se k **w2016-base** jako uživatel **administrator** s heslem **aaa**
2. Spusťte **Server Manager**
   a. Start → **Server Manager**
3. Nainstalujte nástroje **Remote Access**
   a. Vyberte Add Roles and Features z nabídky Manage
   b. Pokračujte Next >
   c. Vyberte Role-based or feature-based installation a pokračujte Next >
   d. Vyberte server **w2016-base** a pokračujte Next >
   e. V kroku Server Roles Pokračujte Next >
   f. V kroku Features rozklikněte Remote Server Administration Tools \ Role Administration Tools a zaškrtněte Remote Access Management Tools a v dialogu se závislostmi potvrďte Add Features, pokračujte Next >
   g. Spusťte instalaci pomocí Install
   h. Okno průvodce můžete zavřít pomocí Close, a vyčkejte na dokončení instalace

Lab S09 – Konfigurace serveru jako NAT [Povinné]

Cíl cvičení

Vzdáleně nakonfigurovat NAT v roli Remote Access Server na w2019-core

Potřebné virtuální stroje

w2016-base
w2019-core (w2019-core OOBE)

Další prerekvizity

Dokončené úkoly S08.

4. Přihlaste se k **w2016-base** jako uživatel **administrator** s heslem **aaa**
5. Ověřte, že server **w2016-base** nemůže přistoupit na internet
   a. Pomocí **ping 8.8.8.8**
6. Spusťte **Server Manager**
   a. Start → **Server Manager**
7. Zvolte Remote Access
8. Z kontextové nabídky nad **w2019-core** vyberte Remote Access Management
   a. V okně **Remote Access Management Console** zvolte v navigačním panelu položku DirectAccess and VPN
   b. V podokně akcí zvolte Open RRAS Management
   c. Otevře se MMC konzole Routing and Remote Access
      ➢ Alternativně je tato konzole součástí Computer Management MMC pod uzlem Services And Applications

9. V MMC **Routing and Remote Access** vyberte uzel w2019-core
10. Z kontextové nabídky vyberte Configure and Enable Routing and Remote Access
11. V průvodci zvolte Next >
12. Vyberte Network address translation (NAT) a pokračujte Next >
13. Pokud se zobrazí chyba o nenainstalovaném protokolu IP nebo se nezobrazí žádné rozhraní pod Use this public interface to connect to the Internet, zkuste povolit službu RRA:
    a. připojte se pomocí **Computer Management** MMC
    b. vyberte Services and Applications \ Services
    c. najděte službu Routing and Remote Access
    d. z kontextové nabídky zvolte Properties
    e. Změňte startup type na **Automatic** a potvrďte Apply
    f. Spusťte službu tlačítkem Start a potvrďte OK
    g. Zopakujte bod 12, pokud chyba nezmizí, server **w2019-core** restartujte
14. V průvodci zvolte Use this public interface to connect to the Internet a vyberte rozhraní připojené k *Default switch*, pokračujte Next >
15. V kroku *Network Selection* vyberte rozhraní s IP **10.10.10.1**, pro které chceme zpřístupnit překlad adres, pokračujte Next >
16. V kroku *Name and Address Translation Services* přepněte na I will set up name and address services later, pokračujte Next >
17. Ukončete průvodce Finish
18. Skončí-li průvodce chybou *Permission denied*, zavřete **Routing and Remote Access** MMC a **Remote Access Management Console**, vraťte se do **Server Manager**, nastavte Manage As … (viz úkol S06 bod 6) a zopakujte body 7 až 17
19. Nastavte NAT i pro rozhraní s IP **192.168.200.1**
    a. V **Routing and Remote Access** MMC rozbalte uzel w2019-core \ IPv4 \ NAT
    b. Z kontextové nabídky zvolte New Interface
    c. Vyberte rozhraní odpovídající IP **192.168.200.1** a pokračujte OK
        - Pod uzlem w2019-core \ IPv4 \ General najdete přehled rozhraní s jejich detaily
    d. Zvolte Private interface connected to private network a potvrďte OK

20. Ověřte, že server **w2016-base** nyní může přistoupit na internet
    a. Pomocí **ping 8.8.8.8**
    b. Pomocí **tracert 8.8.8.8**
21. Ověřte, že stanice **w10-base** může přistoupit na internet
    a. Pomocí **ping 8.8.8.8**
    b. Pomocí **tracert 8.8.8.8**