Operační systémy Windows 7

Klíčové pojmy:

- Významné rysy systému
- Active Directory
- Hyper-V
- Failover Clustering
- Storage Spaces Direct
- Windows Admin Center
- Šifrování zařízení (BitLocker)
- Shielded Virtual Machines
- Microsoft Defender for Endpoint
- Active Directory Domain Services (AD DS)
- Active Directory Certificate Services (AD CS)
- DHCP Server
- DNS Server
- File and Storage Services
- Web Server (IIS)
- Remote Desktop Services (RDS)
- Print and Document Services
- Windows Deployment Services (WDS)
- Network Policy and Access Services (NPAS)
- Windows Server Update Services (WSUS)

Windows Server

Windows Server je řada serverových operačních systémů vyvinutých společností Microsoft. Je navržena pro podporu podnikových potřeb, jako je správa sítí, hostování webových serverů, databázových služeb, virtualizace a další kritické úlohy. Windows Server poskytuje spolehlivou a škálovatelnou platformu pro podniky všech velikostí.

7.1 Významné rysy systému

- **Active Directory**: Centrální služba pro správu uživatelských účtů, skupin, počítačů a dalších síťových zdrojů.
- **Hyper-V**: Integrovaná virtualizační technologie umožňující běh více operačních systémů na jednom fyzickém serveru.
- **PowerShell**: Pokročilý skriptovací a automatizační nástroj pro správu systému.
- **Failover Clustering**: Funkce pro zajištění vysoké dostupnosti aplikací a služeb prostřednictvím klastrů. Umožňuje seskupit dva nebo více serverů (tzv. uzly) do jednoho clusteru pro zajištění vysoké dostupnosti služeb a aplikací. Pokud jeden z uzlů selže, služby jsou automaticky přesunuty na jiný uzel v clusteru (tzv. failover), což minimalizuje výpadky služeb.
- **Storage Spaces Direct**: Řešení pro softwarově definované ukládání dat, umožňující vytváření vysoce dostupných a škálovatelných úložných řešení.

- **Windows Admin Center**: Webové uživatelské rozhraní pro správu serverů, clusterů, hyperkonvergované infrastruktury a Windows klientských počítačů.
- **Vylepšená Bezpečnost:** Funkce jako Shielded Virtual Machines**,** Microsoft Defender for Endpoint a Just Enough Administration pro zvýšení bezpečnosti systému.

Pozn.:

Storage Spaces Direct (S2D) je technologie společnosti Microsoft, která byla poprvé představena ve **Windows Server 2016** a dále vylepšena ve verzích **Windows Server 2019** a **Windows Server 2022**. S2D umožňuje vytvořit vysoce dostupné a škálovatelné úložné řešení pomocí místních disků připojených k běžným serverům (tzv. **hyperkonvergovaná infrastruktura**). Tato technologie umožňuje sdružovat **úložné kapacity jednotlivých serverů** do jednoho celku, který poskytuje služby **ukládání dat** pro virtuální stroje, databáze a další aplikace.

Rozdíl od Failover Clustering je ten, že Failover clustering se zaměřuje na vysokou dostupnost aplikací a služeb, zatímco Storage Spaces Direct se zaměřuje na vytváření vysoce dostupného a škálovatelného úložiště dat. S2D je však funkce, která běží **nad** Failover Clusteringem; využívá clusterovou infrastrukturu pro zajištění vysoké dostupnosti dat, takže Failover Clustering potřebuje ke své činnosti.

Pozn.:

Shielded Virtual Machines (Stíněné virtuální stroje) jsou bezpečnostní funkcí zavedenou společností Microsoft ve **Windows Server 2016** a vylepšenou v následujících verzích, jako je **Windows Server 2019** a **Windows Server 2022**. Tato technologie je navržena tak, aby chránila virtuální stroje (VM) před neoprávněným přístupem nebo manipulací, a to i v případě, že je kompromitován hostitelský server nebo administrátor infrastruktury. Vyžaduje TPM na hostitelských strojích a při použití Host Guardian Service (HGS), která ověří, zda je hostitel důvěryhodný. Data ve virtuálním stroji jsou následně zašifrována pomocí Bitlocker. Administrátoři hostitele nemohou přistupovat k obsahu VM přes Hyper-V Manager nebo PowerShell.

Pozn.:

Microsoft Defender for Endpoint je navržen pro podnikové prostředí, kde je vyžadována pokročilá ochrana, centralizovaná správa a schopnost rychle reagovat na sofistikované kybernetické hrozby. Oproti standardnímu **Windows Defender Antivirus** na Windows 11 nabízí řadu pokročilých funkcí, které zajišťují komplexní bezpečnostní řešení:

- Pokročilá detekce a reakce na hrozby (EDR)
- Centralizovaná správa a viditelnost napříč organizací
- Správa zranitelností a snížení plochy útoku
- Automatizovaná vyšetřování a náprava hrozeb
- Integrace s dalšími bezpečnostními nástroji Microsoftu
- Multiplatformní podpora pro ochranu různých zařízení

Pozn.:

Použití **Just Enough Administration** umožňuje bezpečně delegovat specifické administrativní úlohy na uživatele bez nutnosti poskytovat jim plná administrátorská oprávnění. Tím se zvyšuje bezpečnost a snižuje riziko neúmyslného nebo úmyslného zneužití oprávnění.

Při nasazování JEA je důležité pečlivě plánovat a testovat konfigurace, aby bylo zajištěno, že uživatelé mají přístup pouze k potřebným cmdletům a že jsou dodrženy bezpečnostní zásady organizace.

Obvyklý postup prací:

1. Vytvoření Role Capability File – v souboru specifikujeme cmdlety pro konkrétního uživatele
2. Vytvoření Session Configuration File
3. Registrace JEA Endpointu
4. Testování Konfigurace a ověření dostupných cmdletů

Charakteristické rysy řešení:

- **Nutnost Připojení k JEA Endpointu**: Aby byly role a omezení definované v JEA účinné, uživatelé musí spouštět své akce v kontextu JEA endpointu.
- **Automatizace a Usnadnění Pro Uživatele**: Administrátoři mohou vytvořit skripty, zkratky nebo upravit uživatelské prostředí tak, aby se připojení k JEA endpointu stalo pro uživatele transparentním nebo jednodušším.
- **Bezpečnostní Důvody**: Je důležité zajistit, aby uživatelé neměli alternativní cesty, jak získat přístup k serveru s vyššími oprávněními, než jaké jim byly přiděleny prostřednictvím JEA.

7.2 Role a funkce

Ve Windows Serveru jsou **role** a **funkce (features)** základními stavebními kameny, které určují, jaké služby a funkce bude server poskytovat. Role představují hlavní funkční oblasti, zatímco funkce jsou dodatečné komponenty, které podporují role nebo přidávají další funkčnosti.

Pozn:
Role neexistují v klientských operačních systémech jako je např. Windows 11. Jde o klíčový pojem vztahující se výhradně k OS Windows Server.

Obecný postup pro instalaci role:

1. Analýza Požadavků
    - Určete, jaké role a funkce jsou potřebné pro splnění požadavků organizace.
    - Zkontrolujte závislosti a kompatibilitu s existujícím prostředím.
2. Použití Server Manageru:
    - Spuštění Server Manageru:
        - Otevřete Server Manager, který je výchozím nástrojem pro správu serveru ve Windows Serveru.
    - Přidání Rolí a Funkcí:
        - Klikněte na Add roles and features.
    - Výběr Typu Instalace:
        - Role-based or feature-based installation: Pro instalaci rolí a funkcí na místním serveru nebo vzdáleném serveru.
        - Remote Desktop Services installation: Specifické pro instalaci RDS rolí.
    - Výběr Cílového Serveru:
        - Vyberte server, na který chcete role nebo funkce instalovat.
    - Výběr Rolí:
        - Zaškrtněte požadované role.

        - Pokud role závisí na jiných komponentách, objeví se dialog s výzvou k instalaci nezbytných funkcí.
    - Výběr Funkcí:
        - V dalším kroku vyberte požadované funkce.
    - Potvrzení a Instalace:
        - Zkontrolujte souhrn vybraných rolí a funkcí.
        - Klikněte na Install pro zahájení instalace.
3. Použití Windows Powershell:
    - Role a funkce lze instalovat pomocí PowerShellu, což je užitečné pro skriptování a automatizaci.
    - Příklad příkazu:

```
Install-WindowsFeature -Name Web-Server -IncludeManagementTools
```

    - Pro zobrazení dostupných rolí a funkcí:

```
Get-WindowsFeature
```

4. Restart Systému:
    - Některé role nebo funkce mohou vyžadovat restart systému po instalaci.
    - Server Manager nebo PowerShell vás na tuto skutečnost upozorní.

Příklady rolí, které závisí na jiných rolích:

Active Directory Domain Services (AD DS):

Závislosti:

- Vyžaduje funkci **DNS Server**, pokud chcete vytvořit doménu, protože AD DS silně spoléhá na DNS pro replikaci a služby.
- Během instalace AD DS je možné nainstalovat také DNS Server.

Remote Desktop Services (RDS):

Závislosti:

- Skládá se z více rolí, jako je **Remote Desktop Session Host**, **Remote Desktop Connection Broker**, **Remote Desktop Gateway** atd.
- Některé komponenty RDS mohou vyžadovat **Web Server (IIS)** a **Network Policy and Access Services**.

Web Server (IIS):

Závislosti:

- Pro hostování webových aplikací může vyžadovat funkce jako **.NET Framework 3.5** nebo **4.8**, **ASP.NET**, **WebSocket Protocol** apod.

Failover Clustering:

Závislosti:

- Pro použití některých funkcí, jako je **Storage Spaces Direct**, je nutné mít nainstalovanou roli **Failover Clustering**.
- Vyžaduje také specifické síťové konfigurace a úložné funkce.

7.3 Přehled rolí

1. Active Directory Certificate Services (AD CS)

- **Účel**: AD CS je role, která umožňuje vytvářet a spravovat certifikační autority (CA) pro vydávání **digitálních certifikátů**. Tyto certifikáty se používají k ověřování identity uživatelů, počítačů a služeb v síti a k zajištění **šifrování komunikace**.
- **Použití**: AD CS je zásadní pro **implementaci PKI** (Public Key Infrastructure) v podnikovém prostředí. Certifikáty jsou nezbytné pro zabezpečené připojení pomocí SSL/TLS, digitální podpisy, šifrování e-mailů (S/MIME) a autentizaci uživatelů či zařízení.
- **Důležitost**: Certifikační služby jsou důležité pro zajištění bezpečnosti ve firmách, kde je vyžadována autentizace a šifrování datových přenosů.

2. Windows Deployment Services (WDS)

- **Účel**: WDS slouží k **nasazení operačních systémů** v síťovém prostředí. Umožňuje administrátorům instalovat Windows na více počítačů současně pomocí síťových bootovacích služeb, aniž by bylo nutné používat instalační média na každém zařízení.
- **Použití**: WDS se používá pro **automatizaci instalací** operačních systémů, což výrazně zkracuje čas potřebný k instalaci Windows na nové stroje nebo při obnově stávajících zařízení.
- **Důležitost**: Je neocenitelný pro střední a velké podniky, kde je nutné nasadit operační systémy na velký počet počítačů najednou, například při upgradu hardwaru nebo při standardizaci prostředí.

3. Network Policy and Access Services (NPAS)

- **Účel**: NPAS poskytuje funkce pro správu **síťových připojení** a přístupu uživatelů k síti. Hlavní součástí je **Network Policy Server (NPS)**, který slouží jako server pro ověřování, autorizaci a účtování (AAA) a implementuje **RADIUS** (Remote Authentication Dial-In User Service).
- **Použití**: NPAS se používá pro správu **bezdrátových přístupových bodů**, VPN (Virtual Private Network) a zabezpečení přístupu k síti. NPS ověřuje uživatele a zařízení předtím, než jim umožní přístup do podnikové sítě.
- **Důležitost**: Je klíčový pro zajištění bezpečného přístupu k firemní síti a pro řízení síťových politik. Zajišťuje také sledování a auditování přístupů k síti.

4. Failover Clustering

- **Účel**: Failover clustering umožňuje vytvářet **clusterové servery**, které poskytují vysokou dostupnost a spolehlivost pro klíčové aplikace a služby. V případě výpadku jednoho serveru v clusteru převezme jiný server jeho roli a zajistí **nepřetržitý provoz**.
- **Použití**: Failover clustering se často používá pro kritické aplikace, jako jsou databáze (např. **Microsoft SQL Server**), virtuální stroje (v kombinaci s **Hyper-V**) nebo souborové servery, které vyžadují nepřetržitý provoz.
- **Důležitost**: Pro organizace, které závisí na nepřetržité dostupnosti služeb, je failover clustering nepostradatelnou technologií pro zajištění vysoké dostupnosti a zotavení po havárii.

5. Remote Access Services (RAS)

- **Účel**: Remote Access Services umožňuje vzdálený přístup k síti a zdrojům organizace pomocí technologií jako **VPN** nebo **DirectAccess**. VPN vytváří šifrované připojení mezi uživatelem a podnikovou sítí, zatímco DirectAccess poskytuje průběžné připojení k síťovým prostředkům bez nutnosti uživatelského zásahu.
- **Použití**: RAS je využíván pro vzdálený přístup k firemním datům a aplikacím, což je obzvlášť důležité pro zaměstnance pracující z domova nebo na cestách.
- **Důležitost**: S rostoucím trendem práce na dálku a zvýšenou mobilitou pracovníků jsou RAS a VPN zásadními technologiemi pro bezpečný přístup k firemním datům.

6. Windows Server Update Services (WSUS)

- **Účel**: WSUS umožňuje centrální správu **aktualizací softwaru** a záplat pro počítače ve firemní síti. Administrátoři mohou kontrolovat, testovat a schvalovat aktualizace, než jsou nasazeny na jednotlivé stroje.
- **Použití**: WSUS se používá pro distribuci aktualizací a oprav pro operační systémy Windows, serverové aplikace a další software. Je nezbytný pro zajištění toho, aby všechna zařízení ve firmě byla **aktuální a bezpečná**.
- **Důležitost**: Správa aktualizací je klíčová pro udržování bezpečnosti a stability systémů. WSUS umožňuje organizacím minimalizovat rizika spojená se zastaralým softwarem.

7. Print and Document Services

- **Účel**: Tato role umožňuje správu tiskových úloh a tiskových serverů ve firemním prostředí. Umožňuje centrální správu tiskových front, tiskáren a dokumentů.
- **Použití**: Umožňuje spravovat tiskové služby pro velké podniky, zajišťovat **monitorování a optimalizaci** tiskových úloh, a poskytuje lepší přístup k tiskárnám pro uživatele.
- **Důležitost**: Tato role je důležitá zejména v organizacích, kde tiskové služby hrají klíčovou roli, jako jsou školství, zdravotnictví nebo státní správa.

8. Distributed File System (DFS)

- **Účel**: DFS poskytuje organizacím možnost správy souborů uložených na více serverech v rámci jedné síťové struktury. DFS umožňuje **sjednocený přístup k souborům** a replikaci dat mezi servery.
- **Použití**: DFS umožňuje uživatelům přistupovat k souborům, které jsou fyzicky umístěny na různých serverech, prostřednictvím jedné společné adresářové struktury. Je také užitečný pro synchronizaci dat mezi lokalitami.
- **Důležitost**: DFS zajišťuje, že uživatelé mohou snadno a transparentně přistupovat k souborům, i když jsou tyto soubory rozloženy na více fyzických serverech nebo umístěních.

9. Dynamic Host Configuration Protocol (DHCP) Failover

- **Účel**: DHCP Failover zajišťuje vysokou dostupnost přidělování IP adres tím, že umožňuje **dva DHCP servery** pracovat v tandemu. V případě výpadku jednoho serveru pokračuje druhý server v přidělování IP adres.
- **Použití**: Tato technologie je nezbytná pro podniky, které chtějí zajistit **nepřetržitou dostupnost** sítě a zabránit výpadkům způsobeným selháním DHCP serveru.
- **Důležitost**: Je klíčový v prostředích, kde stabilita sítě závisí na neustálém přidělování IP adres a spravě síťových prostředků.

10. Storage Spaces Direct (S2D)

- **Účel**: S2D je technologie pro vytvoření **software-defined storage** (SDS), která umožňuje vytvářet vysoce dostupná úložná řešení bez nutnosti specializovaného hardwaru. Pomocí běžných serverů lze vytvořit robustní úložiště s podporou redundance.
- **Použití**: Storage Spaces Direct umožňuje vytvářet **virtuální disková pole** a poskytuje vysokou dostupnost a výkon. Používá se pro vytvoření úložiště pro aplikace jako SQL Server, Hyper-V nebo souborové servery.
- **Důležitost**: S2D je ideální pro organizace, které potřebují cenově dostupné a škálovatelné úložné řešení s vysokou dostupností a flexibilitou.

Odkazy:

Microsoft.com

Wikipedia

Cisco Linux Essentials

Root.cz

Chatgpt