Univerzita Hradec Králové

Fakulta informatiky a managementu

Katedra informačních technologií

Analýza možností měření a optimalizace výkonu Windows server

Bakalářská práce

Autor: Libor, Filip
Studijní obor: Aplikovaná informatika

Vedoucí práce: Mgr. Josef Horálek, Ph.D.

Hradec Králové Duben 2017

Prohlášení:

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a s použitím uvedené literatury.

vlastnoruční podpis

V Hradci Králové dne 26.4.2017 Libor Filip

Poděkování:

Děkuji vedoucímu bakalářské práce Mgr. Josefu Horálkovi, Ph.D. za metodické vedení práce a odborné rady ke zpracování a tématu této práce.

Anotace

Bakalářská práce se zaměřuje na provedení analýzy možností měření výkonu a zatížení Windows Serveru a jeho vybraných služeb pomocí interních a externích nástrojů při praktickém používání. Úvodní představení systému a architektury je důležitým pohledem na terminologii a systémové prostředky, které je nutné monitorovat. Samotné představení nástrojů již je zaměřeno praktičtěji na možnosti měření výkonnostních údajů na reálných serverech v prostředí vzdělávací instituce.

Annotation

Title: Analysis of the possibility of measuring and optimizing the performance of Windows server

Bachelor thesis is focused on analyzing the possibility of measuring performance and load Windows Server and selected services using internal and external tools in practical use. The operating performance system architecture is an important insight into the terminology and system resources that should be monitored. The performance itself is focused tools already practically on the possibility of performance measurement data on real servers in an educational institution.

Obsah

Seznam obrázků

Seznam tabulek

Úvod

Možnosti monitorování a optimalizace ve Windows Serveru jsou důležitou a poměrně náročnou činností při každodenní práci systémového administrátora. Při výběru témata práce mě jako systémového administrátora zajímala možnost jak nejlépe představit zkušenosti s nastavením a monitorováním systému Windows Server, ale také další zkušenosti získat a dále je uplatnit v reálné praxi, tedy zdokumentovat vybraná měření z produkčního univerzitního prostředí.

Přestože pod pojmem monitorování si lze představit spíše dlouhodobou činnost určenou k prevenci a zajištění optimálního běhu systému, velmi těžko se lze obejít bez znalostí diagnostických nástrojů známých spíše ke krátkodobému monitorování a řešení problémů, těmi jsou hlavně nástroje Sysinternals, kterým by mohla být věnována samostatná práce.

Vyhodnocením zjištěných hodnot z monitorování chceme nejčastěji určit možné kroky k optimalizaci, ať již aplikace, systému nebo hardware. Optimalizací však nemusí být nutně myšlen maximální výkon, ale požadovaný výsledkem bývá spíše optimální výkon s ohledem na minimalizaci nákladů a uhlíkové stopy. Souvisejícím cílem stále zůstává úspora systémových prostředků a tím snížení nákladů na hardware a energie, pokud by se jednalo o mobilní zařízení tak maximalizace běhu na baterii.

Druhá kapitola představuje základní informace o rozdělení serverů, rozdíly v porovnání s desktopovými systémy a typické role serveru.

Třetí kapitola je věnována struktuře operačního systému, na tu lze pohlížet dle instalační volby grafického prostředí, výběru edice a dále dostupnosti rolí.

Čtvrtá část uvede podrobněji do architektury, tedy oblasti představující techničtěji operační systém a jeho komponenty. Bez těchto znalostí může být obtížné vyhodnocovat získané údaje a případné změny nastavení mohou situaci zhoršit.

Pátá a šestá kapitola jsou úvodem k praktičtějšímu pohledu na systém a popisují monitorování systému procesů.

Závěr práce je věnován souhrnu doporučení pro optimální nasazení systému na základě popisovaných vlastností systému. Optimální možnosti jsou shrnuty do následujících variant:

- Optimalizace kódu aplikace
- Optimalizace pomocí snížení zátěže systému v podobě ukončení či přesunu ostatních aplikací.
- Optimalizace pomocí silnějšího hardware.
- Konsolidace.
- Automatické optimalizace.

Konkrétní řešení je vždy silně závislé na konkrétním prostředí, ve kterém je systém nasazen. Optimální varianta či jejich kombinace mohou být ovlivněny různými atributy, které jsou zmiňovány v praktické i teoretické části.

1 Serverové OS

Tato kapitola byla zpracována s využitím zdrojů [1-5] a praktických poznatků.

Rozdělení operačních systémů na serverové a desktopové systémy vychází z poměrně známého termínu Klient/Server, který byl nejvíce známý v osmdesátých letech minulého století a rozděloval aplikace na serverovou a klientskou část. Přesto je termín pro mnoho uživatelů matoucí, kdy laické rozdělení předpokládá, že server je specializovaný počítač poskytující nějaké služby, například sdílení aplikací či dat v síti. Desktopem je pak osobní počítač určený využívat služby ze serveru nebo sloužit pro samostatnou zábavu či práci. Současné výkonné počítače mohou často plnit obě role a jejich využití je pak určeno především operačním systémem a aplikacemi, které mohou nabízet služby a plnit tak roli serveru.

Specializovaný serverový hardware je stále využíván u serverů velkých firem určených pro větší počet uživatelů, takové servery bývají fyzicky uzpůsobené pro umístění do skříní (Racku) ve specializovaných klimatizovaných místnostech (serverovnách), kde je zajištěna optimální teplota a záložní UPS zdroje pro případ výpadku elektrické energie. Velké serverovny či celé budovy s tisíci servery bývají často označovány jako datová centra. V porovnání s desktopy jsou specializované servery uzpůsobovány pro nepřetržitý provoz bez vypínání (24x7), s optimalizací chlazení, mají redundantní prvky a větší množství hardwarových zdrojů, kterými jsou velmi často větší množství procesorů, operační paměti RAM, disků a síťových karet.

Samotný desktopový operační systém je v mnoha ohledech cílen na jednoduché ovládání, to je zajištěno prostřednictvím propracovaného grafického prostředí. Účelem je poskytnutí prostředí pro zábavu a práci. Samozřejmostí je možnost hraní her, prohlížení filmů, procházení internetových stránek, tvorba dokumentů, programů nebo lze provádět jinou tvůrčí činnost. O oblíbenosti a použitelnosti desktopového operačního systému tak rozhodují především dostupné programy. Systém není určen pro současnou práci více uživatelů a systém se tak označuje jako jednouživatelský. S tím je často zmiňován termín víceúlohový systém, tedy schopnost běhu více úloh (programů) najednou, označovaný jako multitasking. Skutečný pravý multitasking vyžaduje více procesorů, s ohledem na výkon současných procesorů je možné multitasking provozovat i na jednom procesoru, kdy je výkon procesoru inteligentně rozdělován mezi systém a aplikace.

Serverový systém obvykle nabízí možnost volby grafického prostředí. Honba za maximálním výkonem a úsporou systémových prostředků nahrává v kombinaci se skriptováním využívání prostředí příkazového řádku. S využitím vhodných příkazů a skriptů lze konfiguraci uzpůsobit často mnohem rychleji než přes grafické prostředí. Navíc je zde nezanedbatelný zisk více dostupných systémových prostředků, systém je menší a spolehlivější. Rychlost, efektivita a spolehlivost jsou tak nejvíce zmiňované vlastnosti serverových systémů.

Použitelnost a oblíbenost serverového systému je kromě technických vlastností určován především službami. Ve Windows Serveru jsou základní služby serveru konfigurovány pomocí rolí. Přesněji jsou role popsány v další kapitole, pokud zůstaneme u obecnějšího popisu, tak role vlastně vytváří obecně známé typy serverů:

- **Webový** – uložení a poskytování webového obsahu (statických či dynamických stránek) dostupných nejčastěji pomocí webových prohlížečů.
- **Souborový** – poskytnutí přístupu k síťovému úložišti / prostoru pro uložení složek a souborů.
- **Tiskový** – poskytuje přístup k jedné nebo více síťovým tiskárnám. Časté řešení pro řešení bezpečnosti a ekonomického provozu, kdy provoz větších tiskáren bývá levnější než několika malých. Navíc může být služba rozšířena o skenování a fax.
- **Aplikační** – poskytuje podpůrné prostředky pro provoz specializovaných aplikací, například databázového systému. V případě Windows serveru jsou velmi často předpokládány aplikace založené na technologiích APS.NET a .NET Framework s napojením na nějaký databázový systém. Různé typy aplikací pak mohou vytvářet samostatné typy serverů, například FTP či DNS.
- **Virtualizační** – poměrné nový a ne vždy uváděný typ serveru. Poskytuje možnosti vytváření a správy samostatných instancí operačních systémů nazývaných jako virtuální stroje na fyzickém serveru. Důvodem používání bývá často také bezpečnost, kdy systém je rozdělen na více rolí a ty musí být odděleny. V minulosti bylo nutné tento problém řešit koupí několika fyzických serverů. Nově je fyzický server rozdělen na několik virtuálních, které se tváří jako skutečné fyzické stroje. Přínosem je usnadnění správy a optimalizování dostupných systémových prostředků na fyzickém hardware. Nový Windows Server 2016

podporuje odlehčenou virtualizaci v podobě komponenty Docker, kdy dochází k izolaci aplikací a souvisejících dat do samostatných kontejnerů, bez nutnosti nového samostatného operačního systému.

Z technických vlastností má desktopový systém více omezení.

Tabulka 1 Porovnání desktopového a serverového systému Windows (převzato z [3,4,5] (upraveno))

	Windows 10 Home	Windows 10 Ent	Windows Server 2012	Windows Server 2016 (změny)
Soketů / Logických CPU	Až 2 / 32	Až 2 /32	Až 64 soketů / 320 logických	512 soketů
Maximální velikost RAM pro X64	128GB	2TB	4TB	24TB
Cluster	Ne	Ne	64 Nodů	
Hyper-V	Ne	Ano	Ano	
Přístup přes vzdálenou plochu	Ne	Ano (1 současně)	Ano (2 současně, nebo více přes RDS)	

Klientský Windows 10 má omezené sdílení na 20 připojení. Ve smlouvě o užívání je řečeno: „*Přístup k softwaru, který je nainstalován v licencovaném zařízení, můžete umožnit až 20 dalším zařízením za účelem používání následujících funkcí softwaru na licencovaném zařízení: souborová služba, tiskové služby, Internetová informační služba, sdílení připojení k internetu a telefonní služby na licencovaném zařízení*“.

Z pohledu podpory hardware rozdíly téměř mizí, přesto server podporuje silnější hardware v počtu procesorů a paměti. Specifikace o počtu procesorů nemluví, přesto při testu Windows 10 na virtuálním čtyř paticovém serveru byla podpora jen dvě patice.

Desktopový systém je tak omezen o některé serverové funkce. Například v případě Hyper-V nejsou dostupné funkce živé migrace, Remote FX, SR-IOV networking, sdílené VHDX a Hyper-V Replica.

V serverovém systému naopak nejsou dostupné některé věci známé z desktopu, například multimediální přehrávač, podpora Windows Store či uzpůsobení vzhledu prostředí. Dodatečně však i toto lze nainstalovat, jde o volitelnou část s názvem Desktop Experience feature. Této možnosti se využívá například při vzdáleném přístupu, kdy má vzdálená plocha sloužit jako pracovní stanice.

Hardware musí podporovat virtualizaci (kombinace základní desky a procesoru vyžaduje aktivovanou podporu s označením Virtualization Technology) a k dispozici musí být dostatek operační paměti.

Operační paměť je na desktopu nastavena prioritně na služby, v serverovém systému je to více na aplikace.

Při nákupu fyzického serveru je doporučeno kupovat certifikovaný hardware a software, v případě potíží může být jiný hardware označen jako nekompatibilní a nárok na podporu ze strany firmy Microsoft může být odepřen. Výběr certifikovaného hardware se nemusí týkat jen celých serverů, ale i částí. Například dodatečně přidaná síťová karta může způsobovat problémy. Testované a následně certifikované produkty jsou k nalezení na stránce windowsservercatalog.com.

Příklad využívaného serverového hardware a SW (IBM x3650 M4):

Rackový Server s 2x CPU Intel Xeon E5-2680 2.70 Ghz (8 Cores / 16 Threads), 128GB ECC RAM, 2x 278GB HDD 15000RPM (RAID1) + karta FC pro připojení k diskovému poli, 4x Intel(r) I350 Gigabit Network Adapter, 2x redundantní zdroj. SW Windows Server 2012 R2 Standard a Windows Server 2016 Standard jako virtuální. Výkon CPU je cca 51 dle SPECint_base2006.

Příklad využívaného desktopového systému a SW (DELL Optiplex 790):

PC v provedení Tower s 1x CPU Intel Core i7-2600 3.40 GHz (4 Cores / 8 Threads), 8GB RAM, 1x 1TB HDD 7200RPM, 1x Gigabit Network Adapter. SW Windows 10 Education (X64). Výkon CPU je cca 44 dle SPECint_base2006.

2 Edice a role ve Windows Server 2012 R2

Tato kapitola byla zpracována s využitím zdrojů [3-8], část poznatků je všeobecně známá již z praktického používání předchozích verzí Windows Server.

Volba edice a rolí by měla být známá již při plánování scénáře použití, kdy s nákupem hardware je často kupován i samotný systém. Údaje ve scénáři mají jasně určovat technické nároky a způsob používání, tyto parametry poměrně přesně vymezují, jaká edice z níže uvedených edicí bude vyžadována.

- **Foundation** – určeno pro malé zákazníky s omezením do 15 uživatelů. Funkčnost je dále omezena na jeden procesor a není potřeba kupovat klientské licence (CAL). Toto řešení je dostupné pouze jako OEM, tedy jako součást nákupu některých serverových řešení. Nepodporuje virtualizaci, WSUS, Remote Desktop Services a Remote Access.
- **Essentials** – tato verze je dodávána s předkonfigurovaným připojením do Cloudu a je zde omezení na 25 uživatelů bez nutnosti klientských licencí. Podporuje dva procesory a možnost virtualizace jedné instance.
- **Standard** – tato edice je plnohodnotným serverem bez omezení uživatelů. Počet licencí se kupuje dle počtu procesorů a virtualizovaných systémů. Jedna licence umožnuje provozovat dvě virtualizované instance Windows Serveru s licencováním na dva fyzické procesory. K tomu je nutné dokoupit klientské licence dle počtu uživatelů.
- **Datacenter** – tato edice je vhodná do vysoce virtualizovaného prostředí s vyšším počtem virtuálních serverů. Na rozdíl od licence standard lze na fyzickém serveru licenčně provozovat neomezený počet virtuálních systémů.

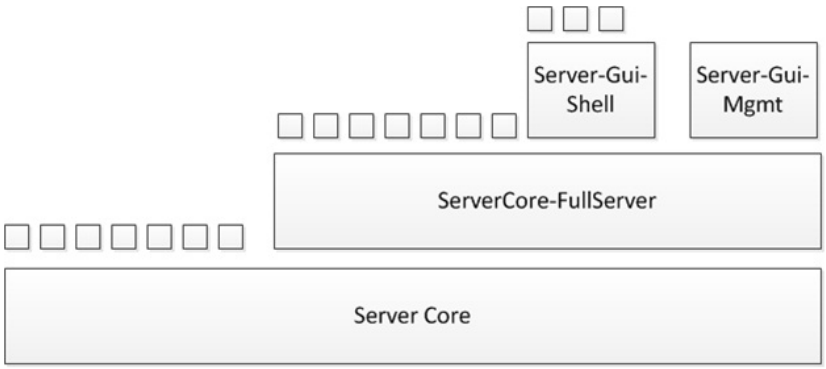
S příchodem Windows 2016 zaniká edice Foundation. Nově jsou navíc v edici Datacenter některé funkcionality pro podniková prostředí. Nové je také licencování na počet jader, původní licencování je na sokety. Toto může při plánování nákupu znevýhodnit procesory s vyšším počtem jader.

2.1 Server Core nebo Server with a GUI?

Při instalaci systému je u každé edice volba možnosti instalace grafického rozhraní. Důvodem je minimalizace tzv. systémového otisku (footprint), kdy minimalizace

znamená úsporu systémových prostředků, lepší zabezpečení, ale složitější správa. Novinkou od systému Windows Server 2012 R2 je možnost přepínání i po instalaci systémů (pomocí PowerShell). V průběhu začátku instalace jsou dostupné dvě možnosti:

- **Server Core** – volba bez grafického rozhraní šetří systémové prostředky, poskytuje vyšší výkon a zabezpečení. Administrace je prováděna v konzoli pomoci příkazového řádku nebo vzdáleně přes PowerShell a další známé nástroje. Některé role a aplikace však nelze nainstalovat. V případě potřeby lze grafické prostředí dodatečně instalovat, čímž však bude edice povýšena na standardní Server with a GUI. Edice může být vyžadována při požadavku na vyšší service-level agreement (SLA), kdy díky absenci grafiky bývá požadavek na menší počet restartů při aktualizacích systému.
- **Server with a GUI** – volba s grafickým prostředím je zmiňována především z důvodu zpětné kompatibility s rolemi a aplikacemi, které na edice Server Core nefungují.



Obr. 1 Instalační volby (Převzato z [6])

Ve Windows 2016 je ještě další nová možnost instalace v podobě **Nano Server**, který je podobný volbě Server Core, ale je ještě více optimalizovaný na výkon a má menší velikost a systémové požadavky. Podporuje pouze 64bitové aplikace, ale podpora rolí a možnosti konfigurace jsou také menší.

2.2 Role

Každý server poskytuje jednu nebo více služeb, požadavky na jejich volbu by měla být známa již před koupí serveru. Součástí systému je několik základních rolí, kdy po výběru každé z nich bude do systému přidána jedna nebo více služeb a příslušné administrativní

nástroje. Pokud role umožnuje při instalaci měnit nastavení, bude spuštěn průvodce, jinak bude nastaveno výchozí nastavení s možnostmi úprav později.

Active Directory Certificate Services – umožnuje budovat certifikační infrastrukturu veřejných klíčů (PKI), která umožnuje pokročilé možnosti kryptografie s využíváním veřejných klíčů, certifikátů a tím možnosti digitálního podpisu.

Active Directory Domain Services – Active Directory je implementace adresářových služeb LDAP určena k tvorbě infrastruktury sloužící k pokročilé správě uživatelů, skupin, počítačích a dalších objektech. Zjednodušeně umožnuje široké možnosti nastavení zabezpečení a některých dalších nastavení (Group Policy) pro různé počítače a uživatele.

Active Directory Federation Services – poskytuje podporu k použití jednotného přihlašování (SSO), tedy bezpečného sídlení digitální identity. Nejčastěji je využíváno k ověřování na webu.

Active Directory Lightweight Directory Services – poskytuje zjednodušené úložiště adresářové služby pro specifické aplikace nevyžadující infrastrukturu Active Directory Domain Services.

Active Directory Rights Management Services – služba k vytváření identity uživatelů a následné ochraně informací před neautorizovaným použitím pomocí poskytování licencí.

Application Server (Aplikační server) – poskytuje různé další role a služby k podpoře distribuovaných transakcí. Role je velmi často vyžadována pro aplikace ASP.NET a Windows Communication Foundation (WCF).

DHCP Server – poskytuje automatické přidělování konfigurace TCP/IP pro klientské počítače a zařízení.

DNS Server – zajišťuje překlad doménových jmen na IP adresy. Obvykle funguje společně se službami Active Directory.

Fax Server – pokročilé služby faxu pro příjem a odesílání ze serveru nebo jiných počítačů v síti.

File and Storage Services (Souborová služba a služba úložiště) – základní souborová služba, která je vždy nainstalována a doplňkové služby k pokročilým funkcím (BranchCache, Deduplication, DFS, iSCSI) a správě souborových úložišť.

Hyper-V – role zastupující instalaci technologie Hyper-V, která poskytuje virtualizaci počítačů na podporovaném fyzickém hostiteli. Na jednom fyzickém počítači lze provozovat další virtuální počítače s podporou různých operačních systémů. Tato možnost je velmi populární a to jak pro ostré či testovací prostředí. Mezi nejčastěji zmiňované funkčnosti patří možnost snadného zálohování, přenositelnosti a vynikající kontrola nad rozdělením systémových prostředků.

Network Policy and Access Services (Služba Síťové zásady a přístup) – role ke zvýšení zabezpečení sítě pomocí serveru NPS (Network Policy Server), autority pro registraci stavu (HRA) a protokolu HCAP (Host Credential Authorization Protocol).

Print and Document Services (Tiskové a dokumentové služby) – role k centralizaci tisku a skenování. Možnost nasměrování dokumentů do síťového úložiště, Sharepoint nebo na e-mail.

Remote Access (Vzdálený přístup) – role umožňující vzdálený přístup do firemní sítě z internetu s technologiemi VPN, DirectAccess a proxy.

Remote Desktop Services (Vzdálená plocha) – služba pro poskytování terminálových služeb. Server se pomocí vzdálené plochy stává terminálem pro více uživatelů. Tohoto je často využíváno. Tedy server je zároveň aplikační a klient poté může vzdáleně využívat terminál k používání serverové aplikace a prostředků na serveru.

Volume Activation Services (Služby aktivace multilicence) – služby a nástroje ke správě aktivací multilicenčního software v doméně (aktivace pomocí licenčních klíčů KMS).

Web Server (IIS) – služba a nástroje webového serveru ve verzi 8.5 poskytuje především podporu pro provoz aplikací naprogramovaných v ASP.NET. Plnohodnotný webový server však podporuje i další programovací jazyky, druhým nejčastějším bývá PHP.

Windows Deployment Services (Služba pro nasazení systému) – role poskytující vzdálenou instalaci systému prostřednictvím počítačové sítě. Po instalaci role lze na

server nahrát instalační obraz obsahující instalaci Windows, instalované programy a data. Tento obraz pak lze distribuovat na klientské počítače.

Windows Server Essential Experience – role instaluje některé pokročilé funkce vzdáleného webového přístupu, zálohování a práci se soubory, kdy se zjednodušuje přístup k uloženým datům z Internetu.

Windows Server Update Services – role poskytující kontrolu nad aktualizační službou Windows Update v počítačích patřící do domény.

Každá role může být složena z více služeb. Kromě rolí a jejich služeb ještě existují funkce (features) poskytující další funkcionalitu, například pro zálohování jde o funkci Windows Server Backup.

Tabulka 2 Dostupnost rolí v Server Core (převzato z [7,8]).

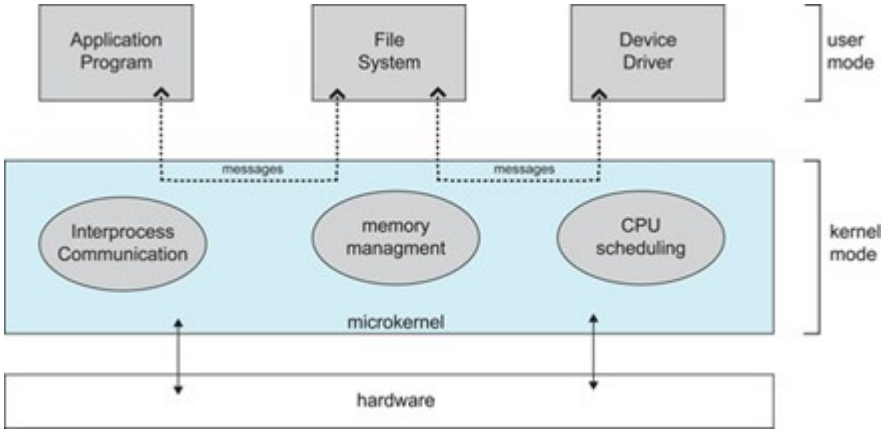
Dostupné:	Nedostupné:
Active Directory Certificate Services	Active Directory Federation Services
Active Directory Domain Services	Application Server
Active Directory Lightweight Directory Services	Fax Server
Active Directory Rights Management Services	Network Policy and Access Services
DHCP Server	Remote Desktop Services
DNS Server	Volume Activation Services
File and Storage Services	Windows Deployment Services
Hyper-V	
Print and Document Services	
Routing and Remote Access: including the following sub-roles: • Remote Desktop Services Connection Broker • Licensing • Virtualization	

Dostupné:	Nedostupné:
Web Server (IIS)	
Windows Server Update Services	

3 Architektura systému Windows Server 2012

Tato kapitola byla zpracována s využitím zdrojů [12-18], převážně [15]. V létě 2017 je očekáváno vydání nejnovější edice knihy Windows Internals, která by měla podrobně mapovat architekturu Windows 10 a Windows 2016.

Stabilita, rychlost a další základní vlastnosti jsou velkou měrou závislé na typu jádra operačního systému. Prvním typem bývá **mikrojádro** (mikrokernel), kdy součástí jádra je zcela naprosté minimum nezbytných funkcí k zajištění obsluhy přerušení, plánování vláken, obsluhy výjimek a posílání zpráv mezi procesy. Další systémové komponenty běží v uživatelském režimu jako aplikace. Výhodou je vysoká stabilita a menší nároky na zkušenosti vývojáře. Minimum kritického kódu v jádře omezuje možnosti selhání. Možnosti selhání se soustředí do komponent v uživatelském režimu, kde pádem komponenty obvykle není narušen chod celého systému. Nevýhodou je však časté přepínání mezi uživatelským režimem a režimem jádra, kdy dochází k častým změnám virtuálního adresového prostoru a velkému vytížení procesoru [12,13,14].

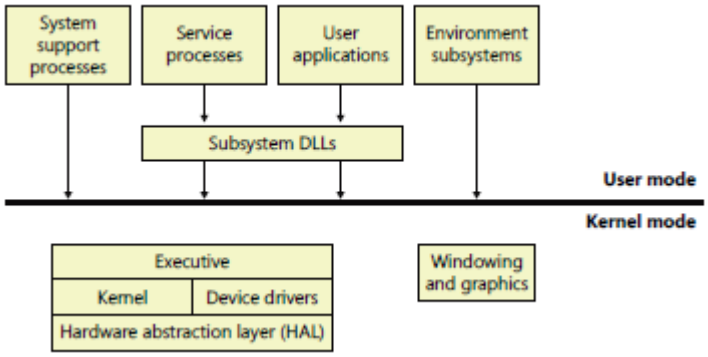


Obr. 2 Architektura Mikrokernel (Převzato z [12])

Druhým typem je **monolitická architektura**, která je obvykle rychlejší. Uvnitř jádra bývá umístěna většina základních komponent nutných k chodu celého systému. Obvykle je v režimu jádra sdílen jeden virtuální adresový prostor, což znamená rychlou komunikaci, ale možné nebezpečí v poškození datových struktur, tedy možný problém nižší stability a bezpečnosti [13,14]. V systému Windows jsou implementovány některé mechanismy, které mají stabilitu a bezpečnost zajistit, příkladem je PatchGuard či Kernel Mode mechanism Signing.

Architektura systému Windows Server je řazena mezi monolitickou architekturu.

3.1 Uživatelský režim a režim jádra



Obr. 3 Zjednodušená architektura systému Windows (převzato z [15])

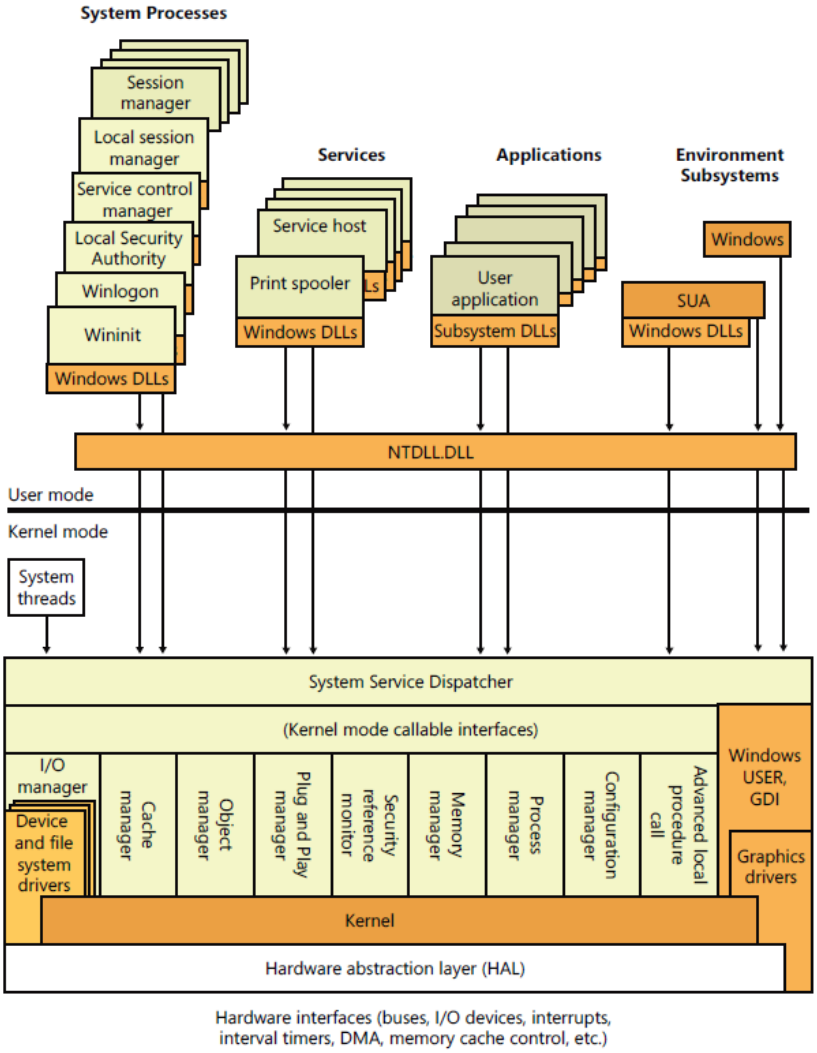
Procesy v uživatelském režimu jsou rozděleny na čtyři typy:

- **Systémové podpůrné procesy** (System support processes) k zajištění přihlášení a vytváření relací.
- **Servisní procesy** neboli služby. Běží skrytě na pozadí systému a obvykle je vyžadován i jejich běh bez přihlášení uživatele. Kromě některých Windows služeb, jako je plánovač úloh může jít i o některé serverové aplikace, například SQL server.
- **Uživatelské aplikace** jsou aplikace spouštěné různými podsystémy nejčastěji Windows 32-bit or 64-bit, POSIX, ve vývoji je Windows Subsystem for Linux (WSL).
- **Knihovny DLL** musí být vždy využity službami k překladu známých systémových požadavků na skryté nedokumentované systémové volání.

Procesy v privilegovaném režimu jádra zahrnují:

- **Exekutiva** – obsahuje několik dále zmíněných správců spolupracující s jádrem, zajišťuje základní služby systému provádějící správu objektů, paměti procesů, vstupu / výstupu, konfigurace a bezpečnosti.
- **Jádro** – jednoduché mechanismy k zajištění plánování vláken na procesoru, obsluha hardwarových přerušení, odložené volání procedur, částečná obsluha systémových volání, synchronizační mechanismy.
- **Ovladače zařízení (*.sys)** – softwarový kód dodávaný výrobci hardware, zajišťující komunikaci s konkrétním hardwarem.

- **Vrstva HAL (hal*.dll)** – nejnižší úroveň jádra určená k „odstínění“ operačního systému od různých verzí hardware (především základní desky a procesoru). Umožnuje snadnou přenositelnost, tedy možnost přenesení disku (nebo jeho klonování) na nový hardware (podporující architekturu X64)
- **The windowing and graphics system** – správce oken řídící jejich umístění, ovládání a vzhled.



Obr. 4 Architektura Windows (převzato z [15])

- **Hardware Abstraction Layer (HAL)** – nejnižší abstraktní vrstva nad fyzickým hardwarem s účelem zajistit komunikaci součástí OS na různém hardware bez nutnosti úprav systému a jeho částí. V systému Windows je většina funkcí vrstvy uložena v knihovně **hal.dll**.

- **Kernel** – jádrem je myšlena sada funkcí zajišťující základní funkce systému. Nejznámější je plánování vláken. Hlavní část jádra je zastoupena souborem ntoskrnl.exe.
- **Správce konfigurací (configuration manager)** – odpovědný za zavedení a správu systémových registrů.
- **Správce procesů (Process manager)** – zajišťuje kompletní správu procesů a vláken. Kromě vytváření, běhu a ukončování pracuje také s nastavením priority a násilné ukončování běhu.
- **Správce paměti (Memory manager)** – slouží ke správě fyzické a virtuální paměti, zajišťuje příděl a uvolnění bloků paměti, mapuje mezi fyzickou a virtuální pamětí a obsluhuje výpadky stránek. Přidává mnoho bezpečnostním prvků (např. ASLR).
- **Security reference monitor (SRM)** – zajišťuje bezpečnost vynucováním některých bezpečnostních politik, chrání systémové zdroje a provádí audit.
- **The Plug and Play (PnP) manager** – zajišťuje detekci a načtení zařízení při startu systému, nebo přidání či odebrání zařízení při běhu systému.
- **Správce objektů (Object manager)** – určen k obsluze, správě, sdílení a zajištění bezpečnosti objektů v exekutivě. Objektů je více než 20, příkladem jsou soubory, klíče registru, procesy, vlákna, události a další.
- **Cache manager** – uchovává v paměti odkazy na některá data na disku a tím urychluje některé souborové operace.
- **I/O manager** (správce zařízení) – poskytuje správu komunikace mezi vstupními a výstupními zařízeními.
- **Správce relací / Session manager (Smss.exe)** – prvním procesem pro vykonávání kódu v uživatelském režimu. Vytváří a spravuje relace, které jsou jakýmsi odděleným prostorem pro přihlášené uživatele. Načítá subsystém Windows (Win32k.sys), inicializuje registry, systémové proměnné a známé knihovny DLL (KnownDLLs), spouští přihlašovací proces Winlogon.
- **Winlogon (winlogon.exe)** – poskytuje uživateli zabezpečené přihlášení pomocí grafického uživatelského rozhraní. Po zadání jména a hesla jsou informace zaslány k ověření procesu Local Security Authority Process **(**Lsass.exe), který zároveň ověřuje, jaké má uživatel oprávnění a poté vytváří tzv. autentizační token

a spouští prostředí uživatele (**userinit.exe**). Po inicializaci prostředí zůstává winlogon spuštěný a čeká na požadavky na odhlášení nebo vypnutí, kdy poté zajišťuje odhlášení uživatele.

- **Client Server Runtime Process (Csrss.exe)** – část subsystému Windows inicializující DLL: Basesrv.dll, Winsrv.dll, and Csrsrv.dll.
- **Správce řízení služeb** (Service Control Manager / SCM – services.exe) – zavádí a inicializuje automaticky spouštěné ovladače zařízení a služby Windows.

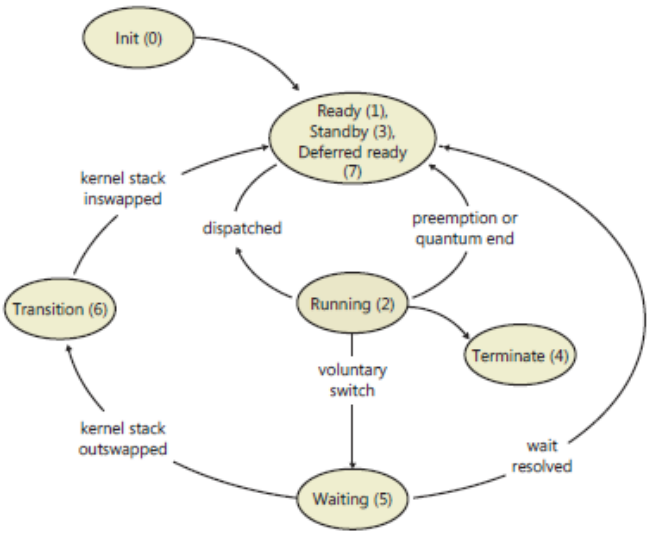
3.2 Procesy a vlákna

- **Proces** (*.exe) – proces je instance spuštěného programu plánovaná plánovačem, tvořená minimálně jedním hlavním vláknem, využívající vlastní paměťový prostor a ostatní systémové zdroje.
- **Vlákno (thread)** – objekt pracující podle kódu programu. Plánování činnosti zajišťuje proces od kterého má obvykle zděděné i některá další nastavení, například prioritu. Od procesu se liší tím, že je jeho součástí a sdílí prostředky (adresní prostor paměti, prostředky jádra atd.) s ostatními vlákny procesu. Vlákno je někdy nazýváno podprocesem.
- **Aplikace** – bývá obvykle synonymem pro proces, přesněji se může aplikace skládat z jednoho nebo více procesů. Síťové aplikace navíc mohou k práci s daty využívat databázi, která může být na jiném počítači nebo v prostředí internetu (cloudu).
- **Odkaz / popisovač zdroje (handles)** – jde o identifikátor zdrojů, například otevřený soubor.
- **Plánovač (scheduler)** – rozhoduje o řazení vláken do plánovacích front a o jejich vykonávání (přidělení na procesor). K rozhodování může využívat různé algoritmy. V prostředí Windows to bývá preemptivní prioritní plánování.
- **Multithreading** – schopnost programu pracovat s více vlákny. Vícevláknová architektura ve spojitosti s více procesory představuje obvykle skvělé řešení k vysoce výkonným aplikacím, přílišný počet vláken však může znamenat vysokou režii na paměť a přepínání mezi vlákny. Detailní informace o procesech a vláknech poskytuje nástroj Process Explorer, kde ve vlastnostech procesu je k

nalezení karta Threads poskytující informace o využívaných vláknech, například identifikační číslo (TID), priorita, stav a další charakteristiky.

- **Priorita** – priorita určuje důležitost procesu. Její změnou lze ovlivnit přidělování procesorového času. Nejvyšší prioritu mají systémové procesy. Z této priority je dopočítávána dynamická priorita vlákna. Dostupné volby:
    - **Nízká** – nenáročné procesy spuštěné na pozadí.
    - **Nižší než normální** – určeno pro procesy, které chceme oproti ostatním mírně znevýhodnit, určit je jako méně důležité.
    - **Normální** – obvyklá hodnota pro většinu aplikací.
    - **Vyšší než normální** – určeno pro programy, kterým chceme zvýšit důležitost.
    - **Vysoká** – kritické systémové procesy.
    - **Reálný čas** – nejvyšší možná hodnota, která by se neměla používat, protože může ohrozit stabilitu systému.
- **Odložená volání procedur (DPC)** – přerušení spouštěná s nižší prioritou, než mají standardní přerušení.
- **Přepínání kontextů** – přepnutí vzniká při přidělení času procesoru jinému procesu nebo vláknu, případně pokud dojde k přechodu mezi režimem jádra a uživatelským režimem. Ideální je, aby jedno vlákno vykonávalo činnost bez přepínání, ale jen pokud musí čekat na nějaká data. Existuje-li jiné čekající vlákno s vyšší prioritou dochází k přepnutí kontextu. Velké množství přepínání znamená větší zátěž na režii procesoru. S vyšším využíváním moderních vícevláknových aplikací je zvýšené přepínání samozřejmostí.
- **Process Control Block (PCB)** – tabulka obsahující popis procesu (vlastník, priorita, stav).
- **Zásobník (stack)** – obsahuje vykonávané instrukce, nejčastěji v podobě nazev_modulu!funkce+adresa.

3.2.1 Stav procesu a změna plánování



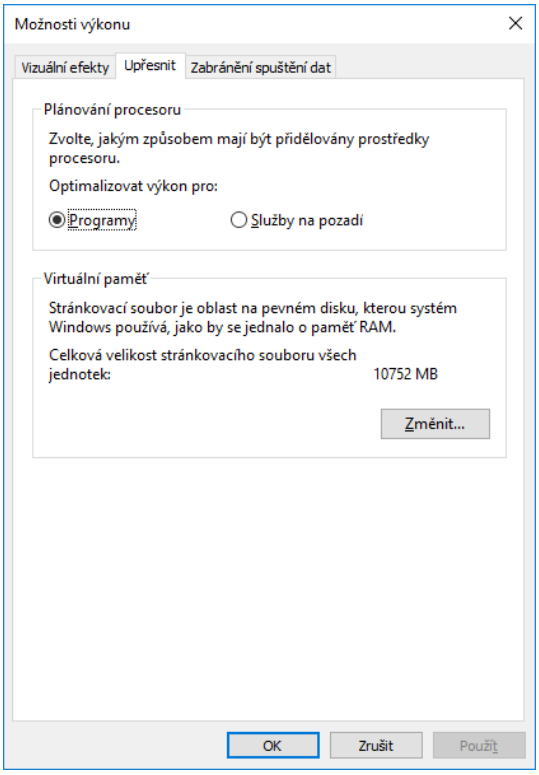
Obr. 5 Stav vlákna (zpracováno dle [15])

Stav vlákna může být:

- Nový (init) – probíhá inicializace / vytváření struktur, například s využitím funkce CreateThread.
- Připraven (Ready) – čeká se na přidělení procesoru.
- Probíhající (Running) – má přidělený procesor a vlákno na něm provádí instrukce programu.
- Náhradní (Standby) – čeká se na nějakou událost, například dokončení I/O operace.
- Dokončen (Terminated) – dokončené zpracování instrukcí, ale vlákno nebylo odstraněno.
- Čekající (Waiting) – čeká se na nějakou událost, například dokončení I/O operace.
- Přechod (Transition) – stav, kdy zásobník jádra pro dané vlákno není načten v paměti.
- Odložená příprava (Deffered ready) – speciální verze režimu připraveno, kdy je vlákno vybráno na procesor, ale ještě není naplánováno na provádění.

Rozdíl mezi serverovým operačním systémem je také v přidělení délky času procesoru (hodnota kvanta), která ovlivňuje, zda priorita plánování procesoru má být nastavena na Programy nebo služby na pozadí.

Nastavení je možné provést ve **Vlastnostech systému** > na kartě **Upřesnit** kliknout na tlačítko **Nastavení** v Části **Výkon** a poté v nově otevřeném okně **Možnosti Výkonu** nastavit na kartě **Upřesnit** > **Plánování procesoru**:



Obr. 6 Změna plánování procesoru (zdroj: vlastní zpracování)

- **Programs (38)** – volba určená pro běžné aktivní aplikace. Nejčastěji je tato volba zmiňována, když je server využíván podobně jako desktopový operační systém, nejznámější je RDS role. Časové kvantum je kratší, což vyhovuje více běžným aplikacím.
- **Backgroud services (24)** – nejčastější výchozí volba pro serverové aplikace, které zpravidla běží na pozadí systému. Časové kvantum je delší, což vyhovuje více aplikacím na pozadí.

V registru je hodnota Win32PrioritySeparation uložena v klíči: ***HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\PriorityControl***

4 Monitorování systému

Zpracováno dle zdrojů [10, 11, 12, 13, 14, 15, 16, 17]:

Jedna z mnoha oficiálních příruček [16] ke sledování výkonu serveru jasně říká, že monitorování je trvalou strastí všech správců systému. Od systému je očekávána dobrá výkonost a dostupnost. Pokud tomu tak není, je nutné zjistit příčinu problému. A zjišťování příčin je dovednost, která je z části vědou a z části umění.

Do oblasti vědy lze zařadit znalosti monitorování. Je nutné určit, co **lze monitorovat**. Jak již naznačila předchozí kapitola o architektuře, monitorovat lze celý systém nebo jeho části. Oblastí umění již lze nazvat základní princip monitorování, a tím je zdůvodnění a výběr vhodného nástroje s následnou volbou požadovaných výkonnostních dat. Právě touto problematikou se bude zabývat tato kapitola.

Větší prostor je věnován programům Sysinternals, které jsou určeny pro pokročilé uživatele s detailním zaměřením, nejen na jednotlivé procesy, ale i vlákna a jejich činnost.

Již před výběrem nástrojů by měl být znám důvod monitorování:

- **Dostupnost** je základním ukazatelem, zda je server, služba či aplikace funkční. Vděčným příkladem je nějaký druh obchodního systému, kdy s nedostupným systémem nelze přijímat a vyřizovat objednávky a dochází k finančním ztrátám. Pokud je funkční jen z části, je například pomalý, může ve velkých firmách dojít ke snížení množství objednávek a opět dochází ke ztrátám. Monitorování dostupnosti by mělo být testováno ještě před nasazením systému do produkčního prostředí. Komplexní monitorování dostupnosti aplikace může být celkem složité, kromě samotné dostupnosti aplikace, může být testována dostupnost hardware, sítě, internetu, jednotlivých částí aplikace, například databázového serveru, vše navíc s měřením odezvy aplikace. Někdy se lze setkat s číselným vyjádřením, kdy poskytovatel a odběratel systému vytvoří dokument s označením Service Level Agreement (SLA) definující určité výkonnostní metriky. Na základě toho se vyhodnocuje dostupnost systému v procentech. Základní charakteristikou však bývá zajistit dostupnost a funkčnost na maximální možnou dobu, v případě požadavku na vysoce dostupný systém s 99,9% dostupností nesmí výpadek systému trvat déle než 44 minut v měsíci (doba na řešení aktualizací a případných

výpadků). Součástí SLA může být i problematika zabezpečení, zálohování a jiné zdánlivě nesouvisející témata.

- **Zjištění kapacity systému** je požadavek u téměř jakéhokoliv většího systému. Při překročení kapacity se může systém stát nedostupným. Z pohledu administrace je zde nutné zaměřit se na využívání systémových prostředků, kdy získávaná data mohou být již konkrétněji zaměřena nejen na operační systém, ale již na jednotlivé ukazatele výkonosti určité služby, aplikace či procesu. Nejběžnějším příkladem je sledování databázového serveru s analýzou využívaných systémových prostředků. V případě databázového serveru jsou navíc sledovány nejnáročnější dotazy, kdy by následně měla být provedena analýza jejich optimalizace a tím kapacitu navýšit. Ke zjištění maximální kapacity jsou využívány údaje v průběhu ostrého provozu nebo vhodněji v kombinaci se zátěžovým testováním, před nasazením aplikace. Pokud se požadavky liší, mají různé požadavky na systémové zdroje, výsledek tedy může být nepřesný. Zjištění kapacity může být použito pro plánování trendů. Předpovědi budoucí kapacity může ovlivnit i nepřesnost v odhadu dat, kdy se zvyšováním obvykle dochází k zpomalení systému a snížení kapacity. Přesto je zjištění aktuální kapacity důležité při vzniklém požadavku na vyšší výkon, příkladem řešení může být navýšení systémových prostředků. Způsobů, jak to provést je více. V případě virtualizace jednoduše přidělíme více prostředků, nebo přesuneme prostředky na silnější server. Dále může být řešeno nákupem silnějšího hardware (může jít jen o část hardware, který vylepší stávající), případně zapojením nového počítače do clusteru. Pokud lze systém snadno rozšířit, můžeme mluvit o dobré škálovatelnosti.
- **Zajištění optimální rychlosti a času odezvy** je základním z cílů optimalizace výkonu. Bez průběžného monitorování výkonnostních dat je velmi obtížné, zda v systému není **úzké místo**, což je část systému dosahující svojí kapacity, tedy problematická část hardware limitující rychlost a pravděpodobně i kapacitu systému. Zjištění obvykle provádíme sledováním celkových využívaných HW prostředků, jak je později probráno, může jít o vytížení **procesoru**, **paměti**, **pevného disku** nebo **sítě**.

- **Řešení havárie** bývá nejméně příjemným důvodem zjišťování údajů o systému. Přesto nástroje pro monitoring v mnoha příkladech mohou odhalit problémové místo, nebo naopak můžou zjistit jinou závadu, kterou je chybné nastavení či oprávnění.

S výběrem vhodného nástroje souvisí **způsob monitorování**, související s požadavkem typu získávaných a monitorovaných dat:

- **Průběžné proaktivní monitorování** - nutné k zjištění zda je systém dostupný a v jakém je stavu. Velmi často získáme s předstihem údaje naznačující budoucí problémy. Příkladem problémů může být málo místa na disku nebo nadměrné vytížení procesoru. Toto monitorování obvykle zahrnuje obecné údaje o systému, ale také historické záznamy hodnot. Zpětně se lze podívat na různé způsoby vizualizace dat, nejčastěji v podobě grafů a vyhodnocovat určité trendy. Délka období je obvykle závislá na účelu sledování. Někdy je v rámci proaktivního monitorování řešen i způsob nápravy, například restart služby, přesun virtuálního stroje na jiný hardware nebo poslání varování prostřednictvím SMS či emailu. Složitější proaktivní monitorování mohou zajišťovat mnoho pokročilých funkcionalit, jako je audit systému či nějaké jednoduché pravidelné reporty, báze znalostí a pokročilá diagnostika. Používání těchto pokročilejších podnikových systémů však může být finančně a časově náročné.
- **Sledování v reálném čase** – nejčastěji je využíváno až v případě potíží, kdy přicházejí varovné informace z proaktivního monitorování nebo v horším případě jsou hlášeny potíže od uživatelů o nedostupnosti služby. Získávání údajů o systému v reálném čase dává přehled o aktuálním stavu systému a možnost zjistit problémy nebo údaje uchovat pro další použití. Údaje lze samozřejmě současně ukládat a tvořit z nich historická data právě pro účely proaktivního monitorování. Omezením některých nástrojů může být pohled jen na celkový stav systému, mohou chybět podrobnosti o procesech, nebo nemusí vyhovovat druh výstupních informací.
- **Zátěžové testování** – s využitím nástrojů pro generování zátěže můžeme simulovat různou zátěž systému a získat tak přibližnější představu o maximálních možnostech a chování systému při různém vytížení. Tento typ testování se používá pro odhalení úzkých míst software nebo hardware. Také může být

užitečné při tvorbě scénářů používání, plánování přidělování systémových prostředků nebo nákupu hardware.

Při výběru monitorování a parametrů by měly být zohledněny dvě možné situace:

- Nadměrné monitorování může znamenat přílišné zatížení systému na úkor výkonu aplikací, náročnější úschovu dat a jejich vyhodnocení.
- Nedostatečné monitorování a chybějící údaje mohou vést k chybnému závěru příčiny problémů.

Názornější představení nejpoužívanějších nástrojů k monitorování představují následující kapitoly.

4.1 Interní nástroje pro monitorování systému

Možnosti nástrojů pro monitorování instalovaných jako součást systému je opravdu veliká. Dále budou v této kapitole především popsány nástroje používané v grafickém prostředí, stále více je však doporučeno, nebo někdy i nutnost použití příkazového řádku s využitím skriptovacího jazyka PowerShell a technologie WMI, dosud bylo jejich hlavní použití v oblasti skriptování a automatizace správy více serverů.

4.1.1 Správce úloh

Nástroj **Správce úloh (Task Manager)** je součástí systému. Jeho hlavní funkcionalitou je poskytnout rychlý základní pohled na stav systému, přesněji základní výkonové ukazatele, a dále na jednotlivé programy s možností případné problémové procesy ukončit. Výkonnostní číselné údaje jsou obvykle získávány z tzv. čítačů výkonu, které jsou v systému okamžitě dostupné. Vývojáři aplikací mohou přidávat další, specifičtěji zaměřené na monitorování konkrétní aplikace.

Ke spuštění je nejčastěji využívána známá trojkombinace kláves Ctrl+Alt+Del. Na výchozí zobrazené kartě **Procesy (Processes)** lze okamžitě vidět spuštěné programy a s využitím pravého tlačítka myši poskytuje i další důležité funkce pro optimalizaci chodu systému:

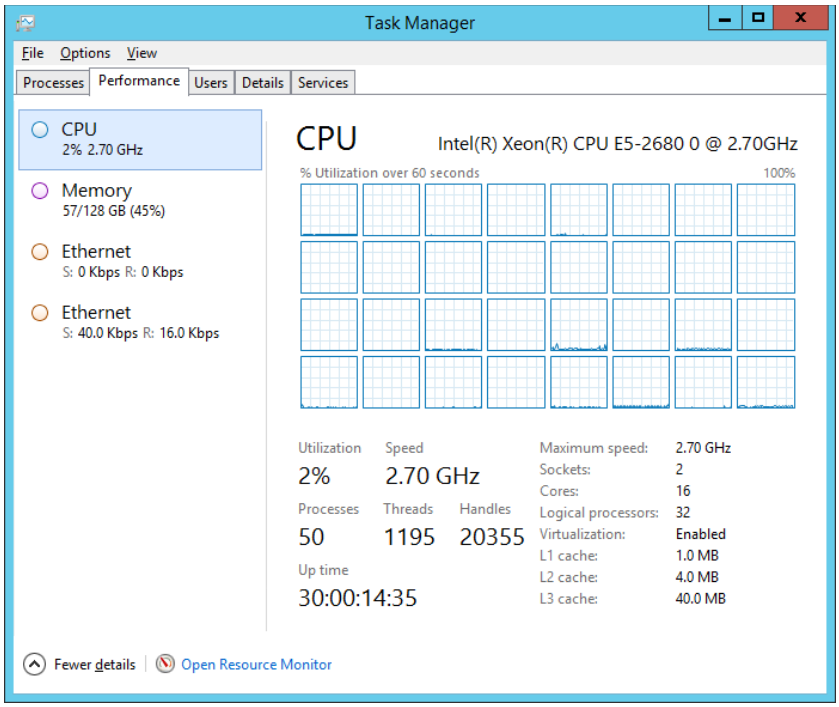
- **Ukončit úlohu** – je využíváno pro ukončení problémových procesů. Důležitá je jistá opatrnost, aplikace označená jako zaneprázdněná může být nedostupná jen dočasně, kdy provádí nějakou náročnější činnost.

- **Nastavit prioritu** – již zmíněná priorita ovlivňující plánovač, vyšší priorita znamená přednostní přidělení prostředků procesoru. Na výběr je celkem šest úrovní.
- **Nastavit spřažení (afinitu) procesoru** – poskytuje možnost přiřazení jader procesoru. Ve výchozím nastavení jsou využívány všechny jádra procesoru, v případě potíží s aplikací nebo požadavkem na méně prostředků může být řešením určit méně jader.

Výše uvedené je však doporučeno měnit s nejvyšší opatrností ve speciálních situacích, jinak může ve vyváženém plánování přidělování systému dojít k problémům s optimálním přidělováním prostředkům.

Při zaneprázdněném systému může být vhodné omezit rychlost obnovy dat v menu **View > Update speed** z volby **Normal** na **Low**, kdy dojde ke změně frekvence z 1s na 4s. Data lze obnovit i ručně stiskem klávesy F5.

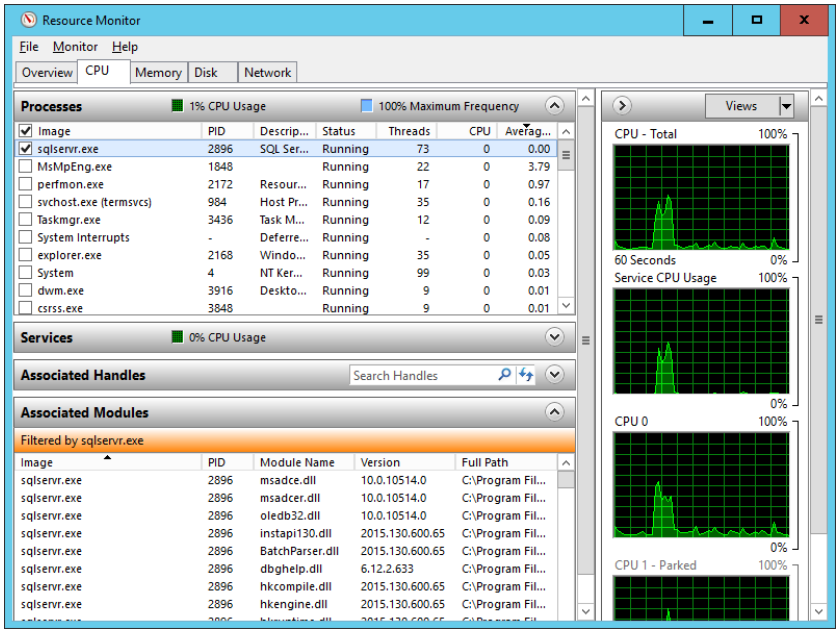
Pro získání základních souhrnných monitorovacích charakteristik je důležitější karta **Performance**.



Obr. 7 Task Manager (zdroj: vlastní zpracování)

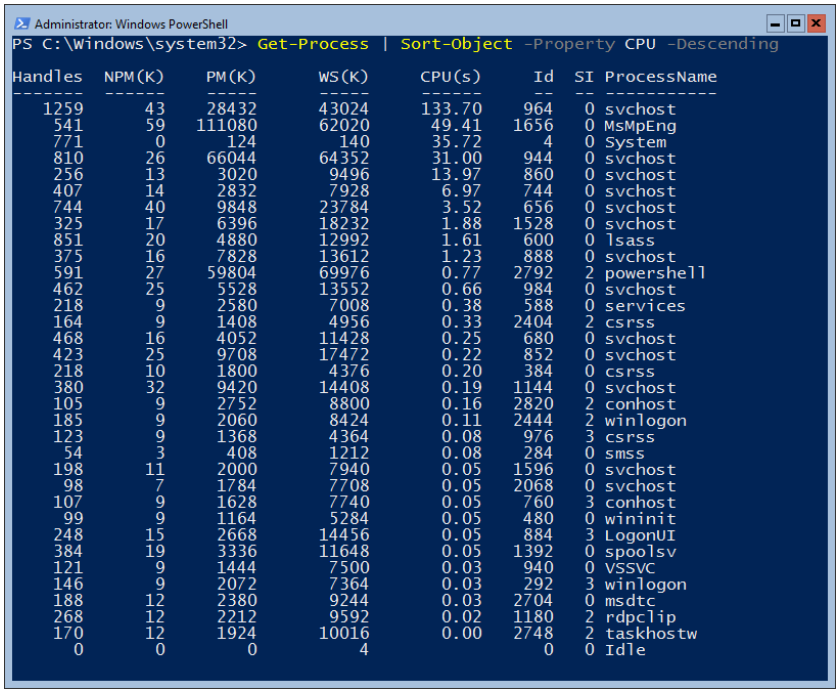
V levé části můžete určit, jaké charakteristiky vás zajímají, tedy zda chcete grafy a hodnoty týkající se CPU, paměti, disku nebo sítě. Kromě sledování paměti bývají hodnoty srozumitelné pro každého pokročilejšího uživatele. V případě paměti je již výhodou znalost architektury paměti. Kliknutím myši na graf pomocí pravého tlačítka lze získat některé další funkce, například zobrazení času v režimu jádra.

Nepřehlédnutelný a důležitý je odkaz **Open Resource Monitor** ke spuštění nástroje Sledování prostředků (Resource monitor). Tento nástroj jde více do hloubky a umožní získat detailní informace o využívaných prostředcích na úrovni jednotlivých procesů.



Obr. 8 Resource Monitor (zdroj: vlastní zpracování)

Jednotlivé karty nástroje odlišují oblasti sledování. V horní části lze označit konkrétní jeden nebo více procesů a v dolní části poté budou zobrazeny informace pro výběr.

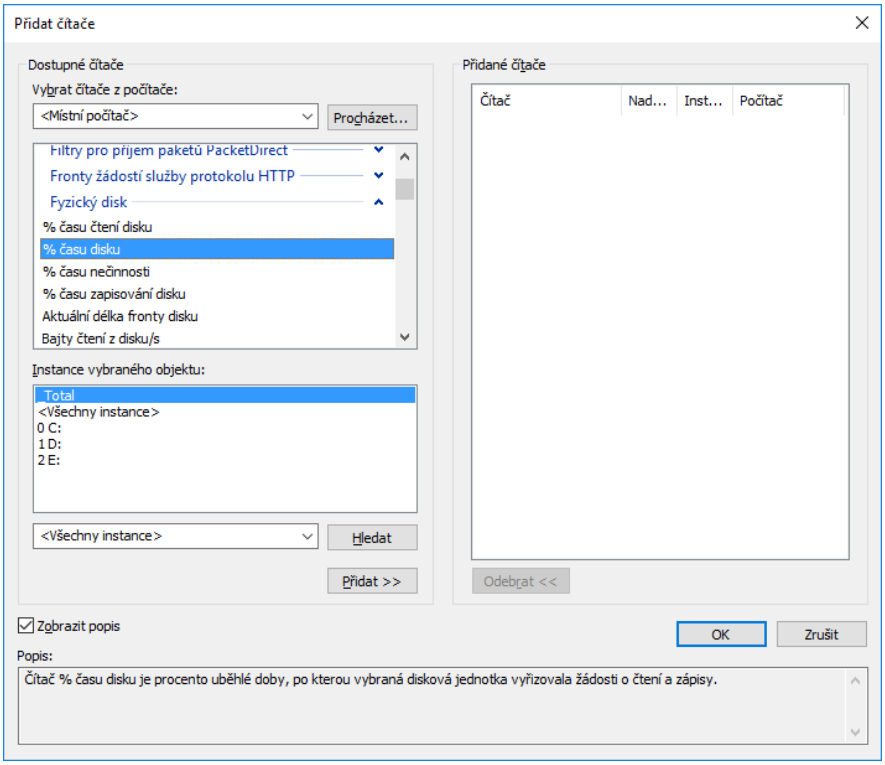


Obr. 9 Powershell : Get-Process na edici Core (zdroj: vlastní zpracování)

Znalost skriptovacího jazyka PowerShell se stává téměř nezbytností při správě Core a Nano edice. Hlavní výhodou textového režimu je menší náročnost na systémové prostředky a možnost využití ve skriptech.

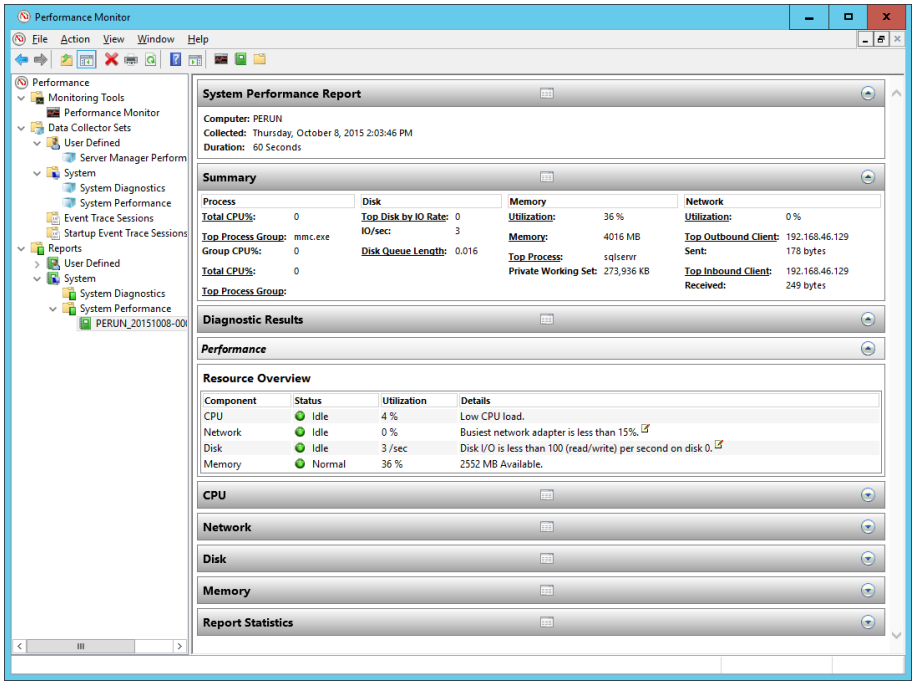
4.1.2 Performance monitor a čítače výkonu

Performance monitor poskytuje nástroje monitorování a analýzy výsledků nasbíraných dat. Již po spuštění se na úvodní obrazovce objeví některé základní výsledky z čítačů výkonu. Základním prvkem je zobrazení a práce s čítači výkonu, tedy již zmíněných číselných hodnot, které jsou na požádání zjištěny a vypovídají o stavu a aktivitě určitých částí systému nebo aplikace. Výběr čítačů v části Nástroje pro sledování nabízí stovky možností řazené dle kategorií. Při výběru je vhodné zobrazit popis ve spodní části a získat tak podrobnější informaci o účelu čítače.



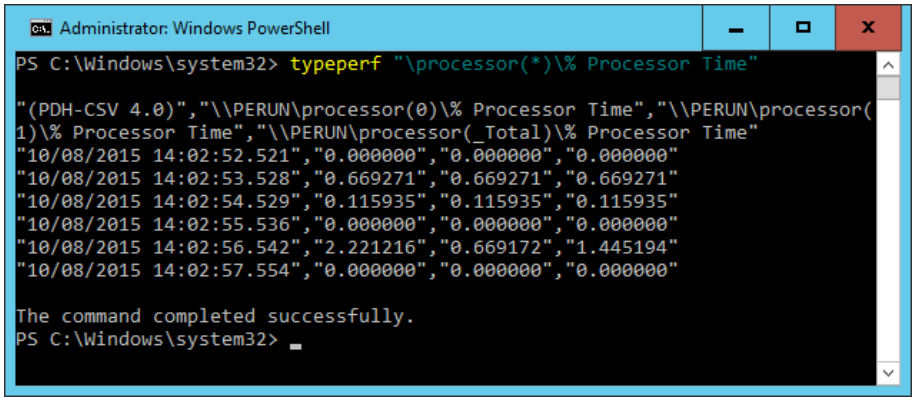
Obr. 10 Sledování výkonu a výběr čítače (zdroj: vlastní zpracování)

Z vybraných čítačů lze vytvořit kolekci dat pro snazší orientaci a pozdější použití. Velmi zajímavou možností je využití předvybrané kolekce k provedení systémové diagnostiky (**perfmon /report**). Výsledkem minutového testu je i automatická analýza hodnot, kdy číselné údaje jsou vygenerovány do přehledného reportu obsahující výkonnostní a konfigurační údaje, kde se nachází stručné textové popisy i s případným varováním či doporučením provedení určitých změn v systému.



Obr. 11 Performance monitor (zdroj: vlastní zpracování)

Alternativou pro příkazový řádek může být příkaz **typeperf**. Seznam dostupných čítačů získáte pomocí přepínače -q (**typeperf -q**). V prostředí **PowerShell** může být využit příkaz **Get-Counter '\Processor(_Total)\% Processor Time'**.



Obr. 12 Příkazový řádek : typeperf (zdroj: vlastní zpracování)

Tabulka vybraných čítačů výkonu se věnuje nejčastějšímu problému, kterým je správné vybrání čítače a jeho interpretace. Drtivá většina používaných systémů Windows pro servery je v angličtině, proto jsou čítače uváděny doplňkově také v angličtině. Příklad grafu a podrobnější popis některých hodnot je v sedmé kapitole.

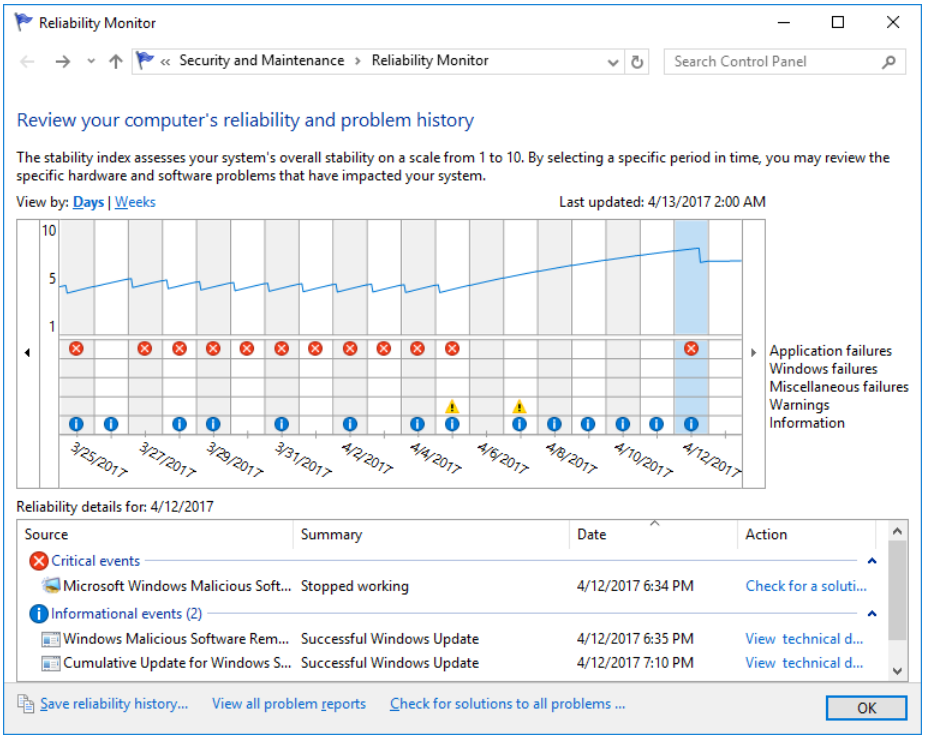
Tabulka 3 Vybrané hlavní čítače výkonu (převzato z [11,16] (upraveno)).

Objekt	Čítač	Popis
System(*)	System Up Time (Doba provozu sytému)	Uplynulá doba v sekundách od posledního spuštění / restartu.
	Processor Queue Length (Délka fronty procesoru)	Počet vláken umístěných ve frontě procesoru.
	Context Switches/sec (Přepnutí kontextu/s)	Rychlost přepínání kontextů zmíněná v kapitole o architektuře.
Processor(*)	% Processor Time (% čas procesoru)	Procentuální čas vykonávání instrukcí aplikací nebo operačního systému. Určuje celkové zatížení procesoru. Je součtem dvou níže uvedených čítačů. Dlouhodobé 100% zatížení může znamenat problém s aplikací nebo nedostatečný hardware.
	% User Time (% uživatelský čas)	Procentuální čas věnovaný aplikacím v uživatelském režimu. Vyšší hodnoty mohou být v pořádku na aplikačním serveru, ale mohou taky značit problém s nějakou aplikací.
	% Privileged Time (% privilegovaný čas)	Procentuální čas instrukcí v privilegovaném režimu jádra. Vyšší hodnoty bývají ve spojení činností operačního systému a ovladačů, například práce se soubory či grafikou.
Memory	Page Faults/sec (Chyby stránkování/s)	Chyby stránkování vznikají v důsledku chybného požadavku na stránku paměti (z důvodu jejího přesunutí na jiné umístění či disk).
	Available MBytes	Celkové množství volné paměti, které lze dále přidělit. Při nedostatku dochází k nadměrnému stránkování a vyšší zátěži na pevných discích. Velikost volné paměti by neměla klesnout pod 5% z celkové velikosti fyzické paměti.

Objekt	Čítač	Popis
	Pages/sec (Stránky/s)	Počet stránek čtených z disku nebo zapisovaných na disk, které mají vyřešit hardwarové chyby stránkování.
	Pool Paged Bytes (Bajty stránkovaného fondu)	Oblast paměti jádra pro nepoužívané objekty, které lze zapsat na disk.
	Pool Nonpaged Bytes (Bajty nestránkovaného fondu)	Oblast paměti jádra pro nepoužívané objekty, které není možné zapsat na disk.
	Free System Page Table Entries (Volné položky stránkovací tabulky systému)	Stránkovací tabulka je využívána k ukládání mapování mezi virtuálními a fyzickými adresami v paměti. Číslo udává počet položek nepoužívaných systémem. Nemělo by klesnout pod **5000**. Problém představuje především na 32 bitových systémech.
LogicalDisk(*) **(Logický disk)**	% Free Space % Volného místa	Procentuální množství dostupného místa na vybraném fyzickém disku. Doporučení je více než 15%, případně dle uvážení. Při nedostatku může dojít k nefunkčnosti aplikace, případně nemožnosti zápisu důležitých dat.
Physical disk	(Current Disk Queue Length) Aktuální délka fronty disku	Ukazuje počet nevyřízených požadavků. Kritickou hodnotu je vhodné zjistit testováním nebo porovnáním s historickými údaji.
Process(*)	Více než 20 čítačů.	Měření výkonnostních dat pro konkrétní instanci (Instance) procesu.
Network	Bytes Total/Sec	Měření rychlosti přenosu dat na síťové kartě. Vysoké zatížení vlivem počtu požadavků a objemů dat bývá řešeno spojením více síťových karet (NIC Teaming) nebo rychlejší kartou (např. z 1Gb na 10Gb).

4.1.3 Sledování spolehlivosti

Nástroj Sledování spolehlivosti (Reliability Monitor) vytváří na základě automatické analýzy logů index a graf stability systému. Nejrychlejší spuštění představuje příkazový řádek a zadání příkazu **perfmon /rel**. Po spuštění můžete v přehledu rychle zjistit výskyt prvních potíží systému a po označení dne je možné zjistit další podrobnosti zobrazené pod grafem. Příkladem kritických zobrazených událostí může být selhání aplikace, neočekávaný restart systému, hardwarové chyby a jiné podrobnosti.



Obr. 13 Reliability Monitor (zdroj: vlastní zpracování)

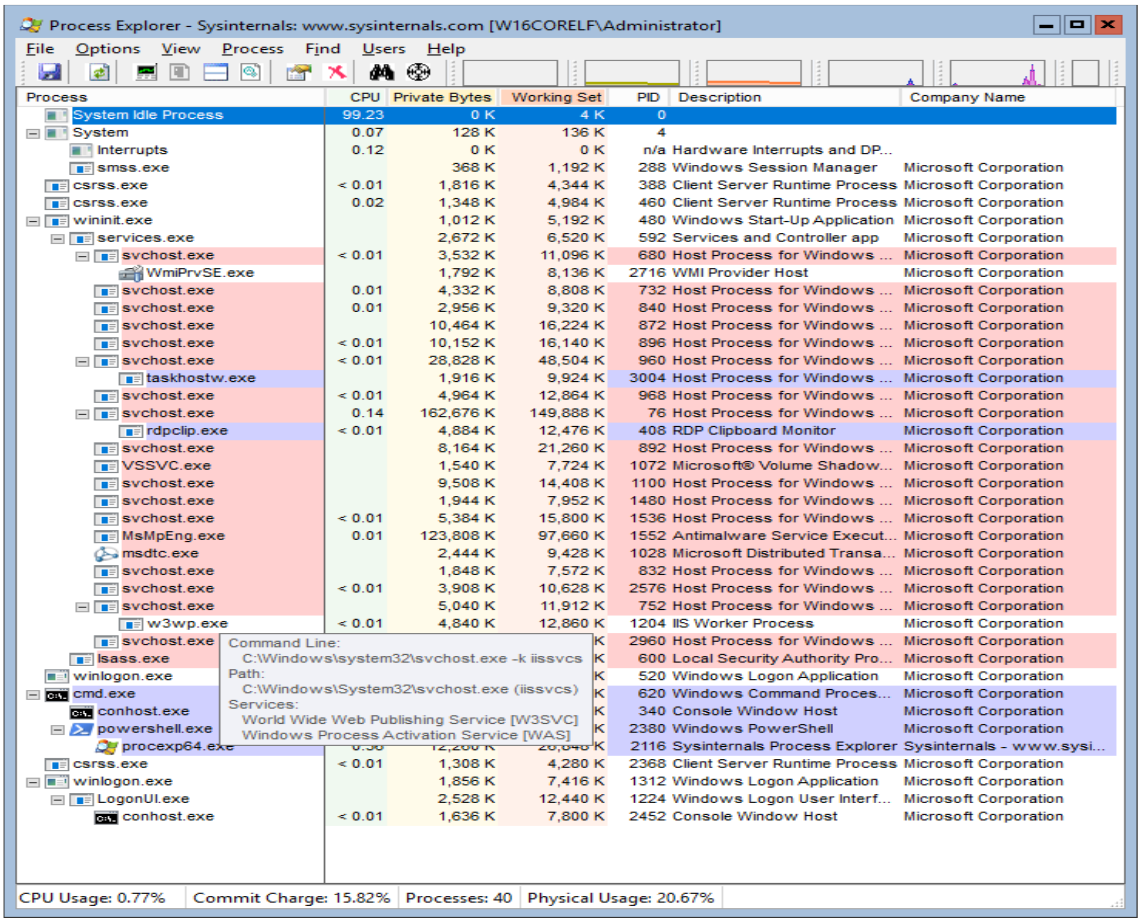
4.2 Externí nástroje Sysinternals

Stránky Sysinternals.com vznikly v roce 1996 a od té doby zpřístupňují mnoho systémových nástrojů usnadňujících práci administrátorům a vývojářům. Nástroje jsou prezentovány jako pomocníci při správě, řešení problémů a diagnostikování operačního systému a aplikací. V roce 2006 byla firma koupena společností Microsoft a zakladatel Mark Russinovich v současnosti pracuje pod společností Microsoft na rozvoji cloudových technologií, navíc publikuje a přednáší na odborných konferencích. Nástroje, kterým se budeme dále věnovat, jsou ty nejznámější a nejpoužívanější. Jejich vývoj dále

zajišťuje přímo společnost Microsoft, ale nejsou součástí systému. K jejich používání je nutné stažení ze stránek Sysinternals.

4.2.1 Process Explorer

Process Explorer bývá označován jako pokročilejší náhrada Správce úloh. V konfiguraci lze najít i volbu **Replace Task Manager**, kdy program bude nastaven jako nový správce úloh. Po spuštění poskytuje nejen základní známé funkce, ale dokáže zobrazovat detailnější informace nejen o procesech, ale také o souvisejících vláknech a knihovnách DLL. Samozřejmostí jsou základní výkonnostní charakteristiky, ale také pokročilejší grafy a další číselné údaje. Velmi často je zmiňován jako pomocný nástroj při hledání nebezpečného Malware. Pro zobrazení všech důležitých informací je doporučeno spuštění jako správce.



Obr. 14 Process Explorer : Windows 2016 Core + IIS (zdroj: vlastní zpracování)

Na úvodní obrazovce zabírá její největší část seznam procesů, kde jsou ke každému procesu uváděny tyto údaje:

- **Process** – jméno procesu. Po najetí myši jsou zobrazeny parametry spouštění, umístění souboru a služeb.
- **CPU** – procentuální využití procesoru.
- **Private bytes** – počet alokovaných a využívaných bytů (heap + stack memory).
- **Working Set** – velikost přiřazené paměti od správce paměti.
- **Proces ID** – identifikační číslo.
- **Description and company** – popis souboru a jeho výrobce (pokud je uvedeno).

Další sloupce lze přidat v konfiguraci programu (**View > Select Columns**). Pokud je vyžadováno seřazení dle hodnot (určitého sloupce), například vytížení CPU, stačí kliknout na záhlaví.

Výchozí řazení je zobrazení jako **strom procesů**, kdy existují rodičovské procesy, které mohou spustit další podprocesy označované jako jejich potomci.

Barva na pozadí každého řádku odlišuje druhy procesů, toto rozlišení je možné zobrazit a změnit v menu **Option** a volbě **Configure Colors.** Celkem je ve výchozím nastavení rozlišováno 7 druhů:

- **Služby (růžová)** – systémové procesy. Velmi často může jít o více služeb pod jedním procesem.
- **Vlastní procesy (levandulová)** – procesy běžící pod stejným účtem jako Process Explorer.
- **Nové procesy (světle zelená)** – při spuštění nového procesu je krátce podbarven.
- **Smazané objekty (červená)** – při ukončení je ještě krátce zobrazen s červeným podbarvením
- **Packed Images (fialová)** – procesy využívající komprimaci nebo šifrování. Velmi často se může za těmito procesy skrývat škodlivý kód.
- **Suspended proces (šedá)** – procesy označené jako pozastavené.
- **Immersive proces (světle modrá)** – označuje procesy aplikací z Windows Store.

Podbarvení u nových či smazaných procesů je pouze 1s. Nastavení delšího času je možné v menu **Options** a volbě **Difference Highlight Duration**. V případě, kdy je proces rozlišen více druhy, může být zobrazen dle priority: Suspended, Immersive, Protected, Packed, Jobs, Services, Vlastní procesy.

Zjednodušený strom systémových procesů (již zmíněné v architektuře systému):

- **System Idle Process** není plnohodnotným procesem. Běží v režimu jádra a zastupuje nečinné procesy systému. Obsahuje jedno vlákno ntoskrnl.exe. Běží vždy v jednom jádru, kde slouží k určení nečinného času procesoru (počet vláken je závislý na počtu jader).
- **System** zastupuje většinu vláken v režimu jádra. Je nadřazeným procesem pro:
  - Hardware Interrupts and DPCs (Interrupts)
  - Windows Session Manager (smss.exe)
- Client Server Runtime Process (csrss.exe) – Windows Subsystem
- Windows Start-Up Application(wininit.exe)
  - Services and Controller app (services.exe) – Správce řízení služeb
    - Host Process for Windows Services (svchost.exe) + jiné dceřiné procesy služeb
  - Local Security Authority Process (lsass.exe) – ověřování zabezpečení
- Windows Logon Application (winlogon.exe) – Přihlašovací proces
  - Windows Logon User Interface Host (LogonUI.exe)
  - Desktop Window Manager (dwm.exe)

Po kliknutí myši pravým tlačítkem na vybraný řádek je zobrazeno místní menu nabízející různé akce:

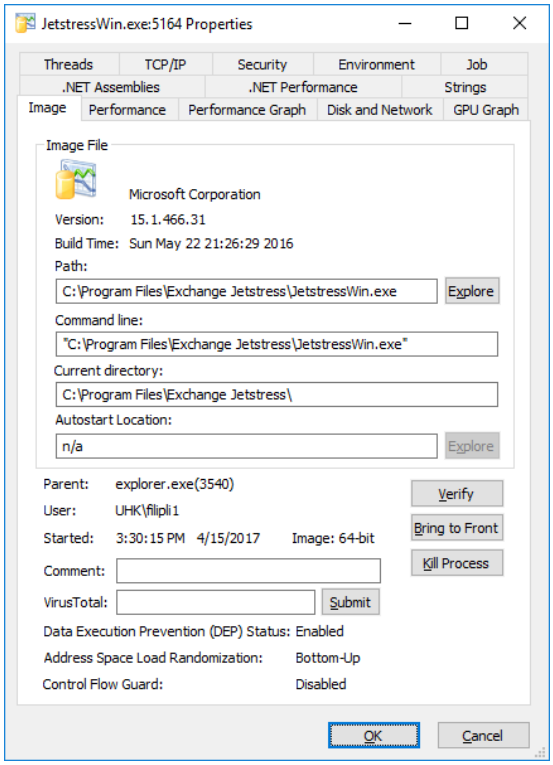
- **Windows menu** dostupné pro aplikace s GUI nabízí standardní položky oken, kdy můžete okno přenést na popředí, minimalizovat, maximalizovat nebo zavřít.
- **Set Affinity** je možnost určit na jakých jádrech procesoru mají být vlákna spouštěna. V případě potíží s celkovou stabilitou systému může být užitečné problémovému procesu odebrat jádra a uvolnit tak prostředky pro samotný systém či diagnostické nástroje. Možné jsou i další scénáře. Obecně je

doporučována jistá opatrnost. Změnou afinity může dojít k nevyváženosti běhu systému a tím celkový výkon zhoršit.

- **Set Priority** umožní změnu priority ovlivňující plánovač procesů.
- **Kill Process** je volbou k násilnému ukončení procesu. V menu Option >> Confirm Kill lze zakázat potvrzovací výzvu k ukončení.
- **Restart** provede ukončení a start procesu se stejnými parametry.
- **Suspend** umožní dočasné uspání a tím odlehčí prostředky pro ostatní procesy a operační systém. U uspaných procesů se objeví volba **Resume**.
- **Dump** zachytí obraz paměti pro pokročilejší analýzu.
- **Chechk VirusTotal** je poměrně nová vlastnost k ověření důvěryhodnosti pomocí služby VirusTotal.com.
- Dále mohou být dostupné volby pro ladění (Debug k použití s Visual Studio nebo Launch Depends pro použití nástroje Dependency Walker).

Po najetí kurzoru nad určitý proces je zobrazen popisek s dalšími informacemi. Dvojklikem na vybraný proces je zobrazeno okno s dalším množstvím informací, některé ze záložek jsou dále popsány. K zobrazení seznamu knihoven DLL nebo Ukazatelů ve spodní části programu slouží v panelu nástrojů ikony DLLs nebo Handles.

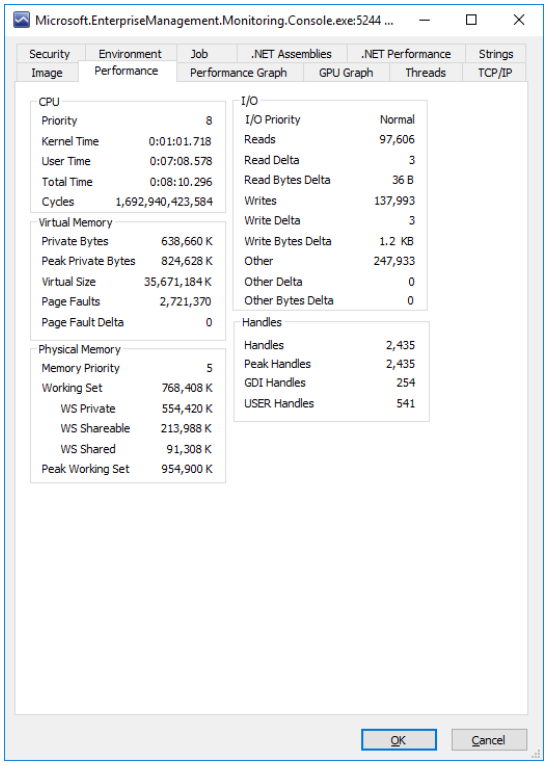
Image



Obr. 15 Process Explorer Image Tab (zdroj: vlastní zpracování)

Záložka obsahuje základní identifikační údaje o názvu, výrobci, verzi, umístění na disku (Path), parametrech spouštění (Command line) a odkud je spouštěn (Autorun location). Spodní část zobrazí informace o nadřazeném procesu, kontextu spouštěného uživatele, kdy byl spuštěn a zda se jedná o 32 bitový či 64bitový proces. V pravé části jsou tlačítka určená k přenesení procesu na popředí obrazovky nebo jeho ukončení. DEP, ASLR a CFG jsou různé technologie zabezpečení.

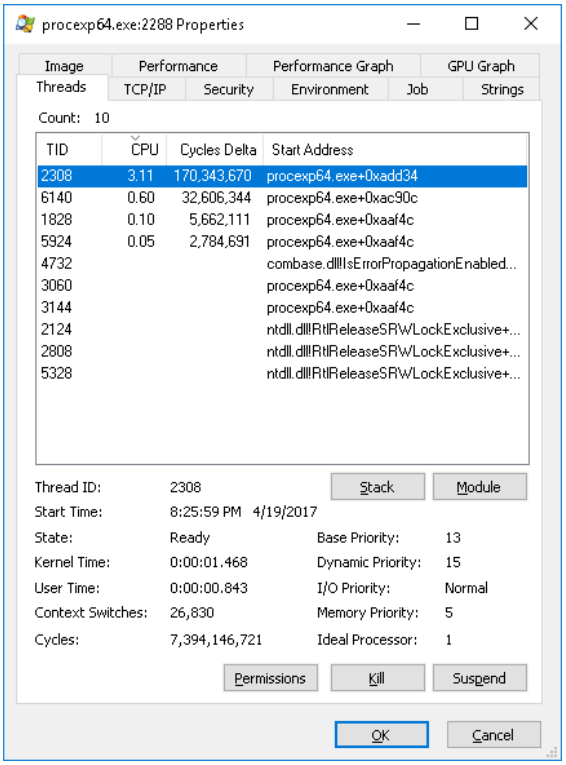
Performance Tab



Obr. 16 Process Explorer Performance Tab (zdroj: vlastní zpracování)

Detailní pohled na aktuálně využívané prostředky (metriky) procesu poskytuje záložka Performance. Většina údajů bude jistě známá z předchozího textu, pro zjednodušený náhled na krátkodobý historický vývoj procesu s pomocí grafu je určena záložka Performance Graph.

Threads Tab



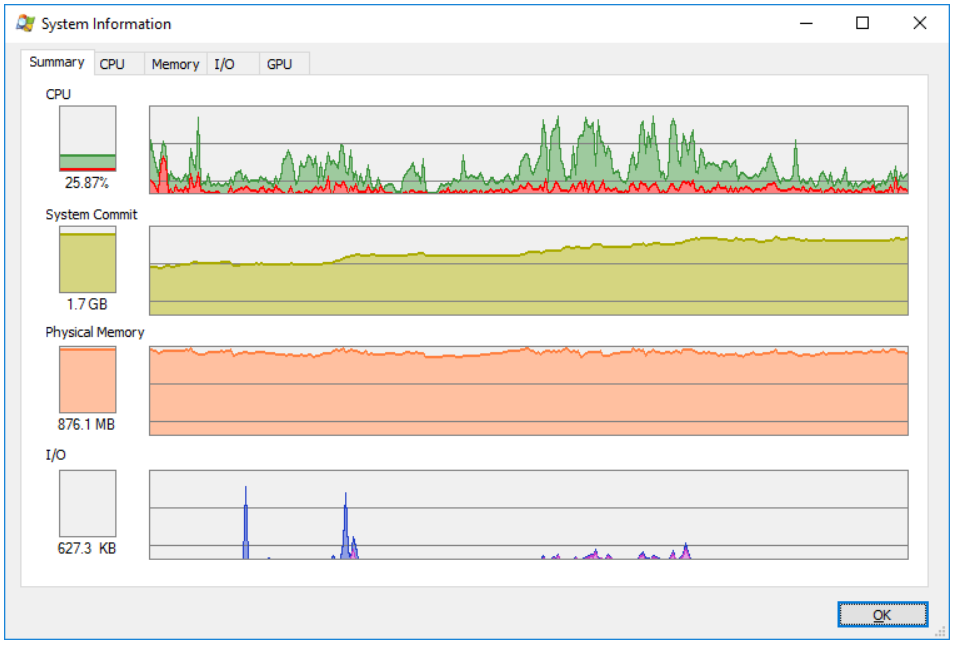
Obr. 17 Process Explorer Threads Tab (zdroj: vlastní zpracování)

Nejnižší systémový pohled na jednotlivá vlákna poskytuje záložka Threads. Po označení konkrétního vlákna lze získat přístup k výkonnostním datům, informacím o modulech, zásobníku, či vlákno ukončit nebo uspat.

Pro překlad symbolů na funkční jména je nutná správná konfigurace **Configure Symbols** v nabídce **Configure Symbols**.

Systémové informace

Okno s grafy a číselnými souhrnnými údaji o jednotlivých částech systému poskytuje okno Systémové informace vyvolané kliknutím na grafy v panelu nástrojů nebo z nabídky **View** > **System Information** (Ctrl + I). Nejvíce informací poskytuje karta Memory.



Obr. 18 Process Explorer: System Information (zdroj: vlastní zpracování)

Další okna jsou již z pohledu monitorování výkonu serveru méně důležitá.

4.2.2 Process Monitor

Trasování (logování) aktivity jednotlivých procesů a vláken dokáže Process Monitor. Aplikace tedy není určena primárně k měření výkonu, ale nejčastěji ji využívají vývojáři k analýze, co jednotlivé procesy dělají, respektive pokusy o změny, skutečné změny, a na základě uváděných informací může být uveden i důvod, který vede k selhávání běhu aplikace.

Samotné používání aplikace představuje důslednou minimalizaci času spuštění a následné využití pokročilého filtrování. Jinak by bylo nutné probrat tisíce událostí přibývajících s každou vteřinou. Sledovat stovky událostí za vteřinu v reálném čase je jinak téměř nemožné, nepřehledné, navíc velmi náročné na systémové zdroje. Uchovávání každé minuty může znamenat desítky MB dat.

Řešením je minimalizace sledovaného času, tedy zachycení konkrétního časového úseku a jeho uložení do souboru. V následné analýze již vhodným filtrem omezit, jaké informace nás zajímají. Příkladem může být problém se spuštěním aplikací, kde v Process Monitoru zjistíme chybu NAME NOT FOUND, což nás nasměruje k chybějícímu klíči nebo problému s oprávněním.

Populární je také porovnávání funkčního a nefunkčního systému, například na funkčním systému zjistíme volání určitého klíče registru se specifickým nastavením, na nefunkčním systému je však nastavení jiné nebo zcela chybí.

Operace se rozdělují na 5 tříd (první tři jsou spouštěny automaticky):

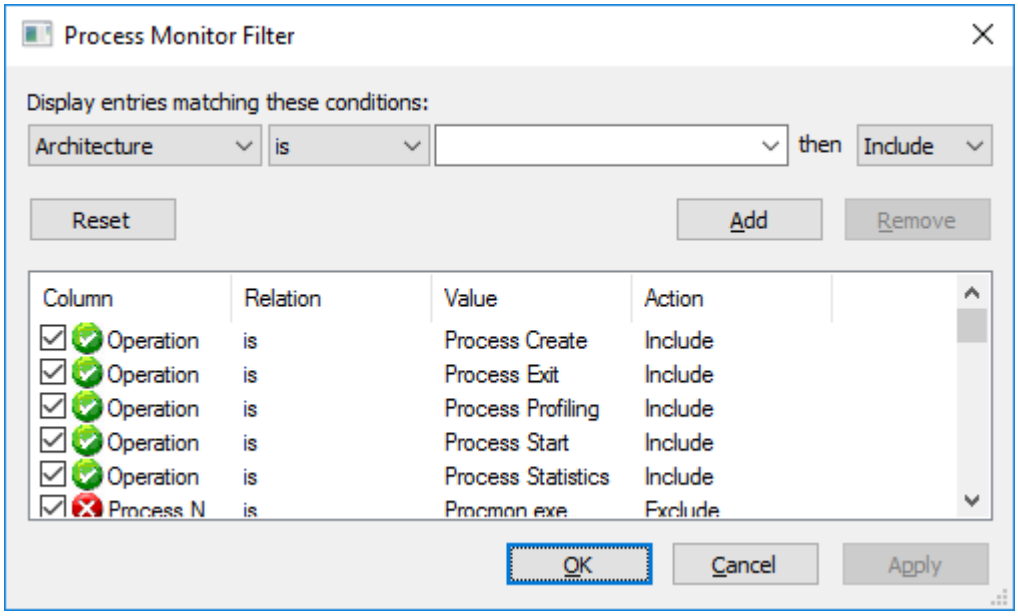
- **File System** – sledování činností se soubory a adresáři na lokálních nebo vzdálených úložištích. Odhaluje například chybějící, či poškozené soubory, nebo problémy s oprávněním.
- **Registry** – sledování činností v registru, tedy samotné dotazy na záznamy v registru, výsledky dotazů, tvorbu nových či mazání. Podobně jako v případě systému souborů i zde můžeme zjišťovat problémy s poškozenými nebo chybějícími daty.
- **Process** – události vláken a procesů, sleduje vytváření a ukončování procesů a vláken, nebo nahrávání knihoven dll.
- **Profiling** – při zapnutí poskytuje u procesů informace o času v režimu jádra, času v režimu uživatele a počet context switches, Private Bytes a Working Set.
- **Network** – sledování síťové komunikace, záznamy o zdrojových a cílových parametrech.

Skrytí nebo zobrazení operací patřící konkrétní třídě lze omezit kliknutím na ikonu v panelu nástrojů. Dle typu vybraných tříd jsou v hlavním okně zobrazovány řádky obsahující jednotlivé události. Po kliknutí na řádek se zobrazí okno se všemi podrobnostmi o záznamu. Níže je uveden popis sloupců, které jsou ve výchozím nastavení zobrazeny, celkem jich je dostupných 28.

- **Time** – čas vzniku události. Zároveň jde o sloupec, dle kterého se data řadí.
- **Process Name** – jméno procesu a vděčný údaj k uplatnění filtru.
- **PID** – identifikační číslo procesu.
- **Operation** – druh prováděné operace, kterých je několik desítek. Čisté události týkající se vzniku, zániku a dalších operací procesu jsou Create, Exit, Profilling, Start, Statistics.
- **Path** – cesta k souboru.
- **Result** – kód výsledku, kterých je opět pár desítek. Z těch nejznámějších lze zmínit SUCCESS, ACCESS DENIED, NO SUCH FILE.

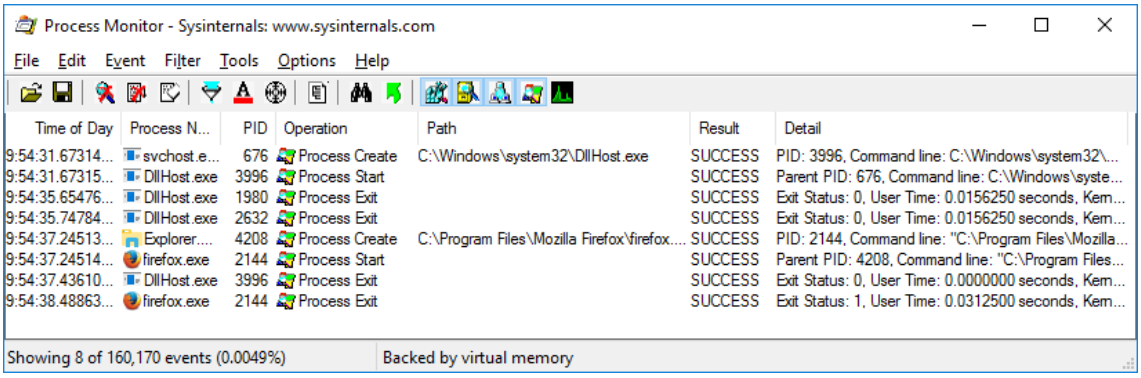
- **Detail** – detailní informace vztahující se k události.

Po spuštění programu je zobrazen filtr, který umožní nastavit množství parametrů, které mají omezit množství zobrazovaných informací. Na obrázku níže je filtr omezen na operace s procesy, pro praktické použití to však moc není.



Obr. 19 Process Monitor Filter (zdroj: vlastní zpracování)

Na obrázku s výsledkem po aplikaci filtru lze vidět pouze 8 událostí ze 160 000, vhodnější je nechat filtr po spuštění s výchozími údaji a filtr nastavovat dodatečně pomocí myši a klikáním na vybrané události a s využitím místní nabídky filtr přizpůsobit.



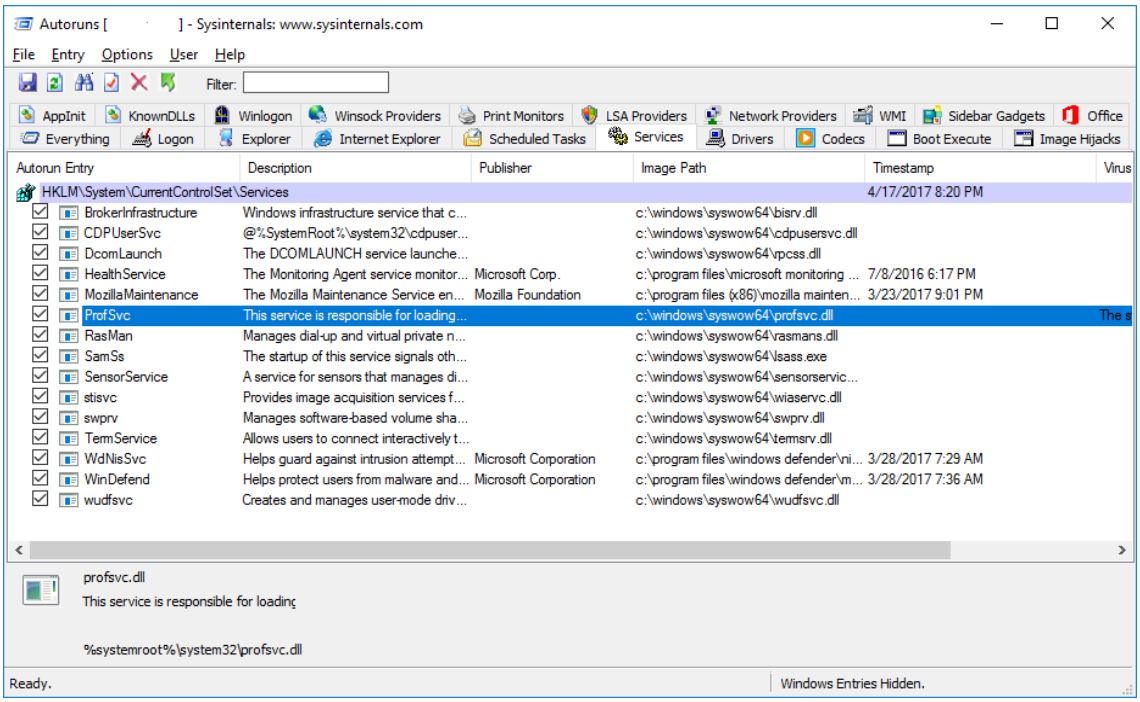
Obr. 20 Process Monitor s filtrem (zdroj: vlastní zpracování)

4.2.3 Autoruns

Nástroj Autoruns je neocenitelným pomocníkem při rychlé analýze a odstraňování nechtěných procesů spouštěných při startu systému. Po spuštění programu se prohlédne více než 200 umístění v souborovém systému a registru (Autostart Extensilibity Points), ze kterých mohou být procesy spouštěny. Než jsou jednotlivé položky zobrazeny v hlavním okně, jsou ověřeny, zda obsahují digitální podpis a volitelně je provedena analýza pomocí služby VirusTotal.

Podezřelé položky jsou odlišeny barevně.

S odstraňováním položek je nutná zvýšená obezřetnost, kdy nevhodným výběrem může dojít k nefunkčnosti aplikace či systému.



Obr. 21 Autoruns (zdroj: vlastní zpracování)

5 Enterprise nástroje

Zpracováno dle zdrojů [20, 21, + Vlastní zpracování]:

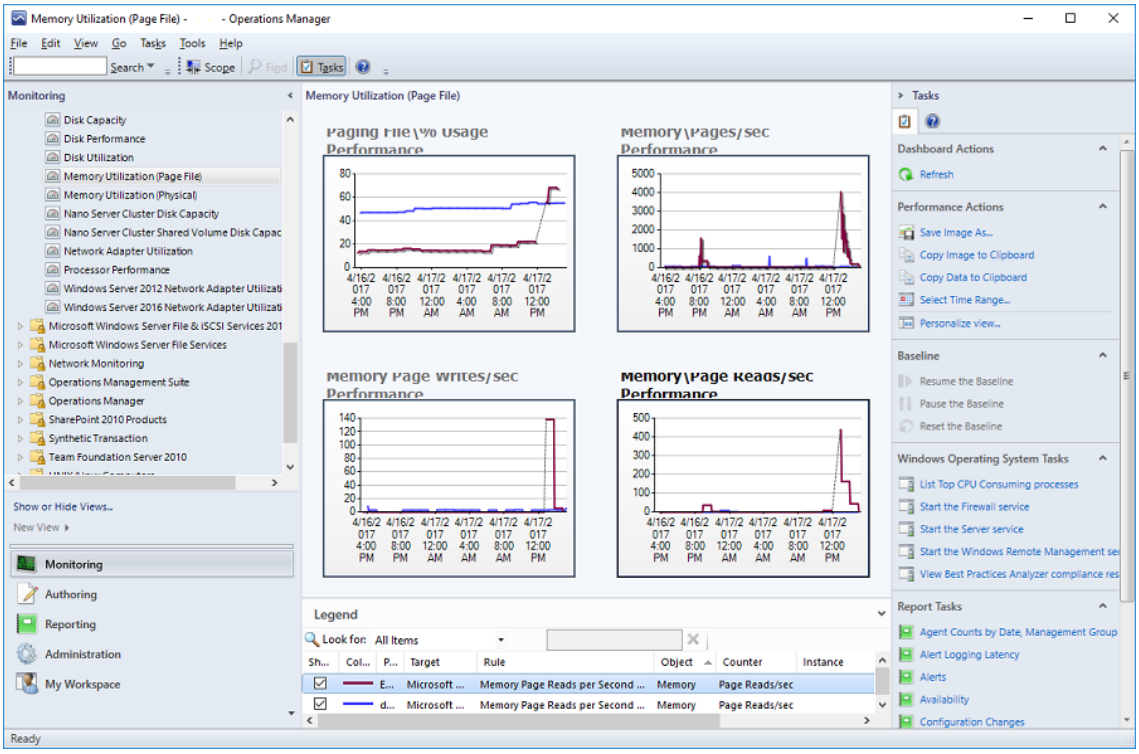
Velké společnosti mají i tisíce serverů, každá vteřina výpadku je zde nežádoucí. Správa rozsáhlých serveroven s požadavkem zajištění vysoké dostupnosti již vyžaduje automatizované sledování a upozorňování na problémy s výkonem či jiné incidenty. To je obvykle řešeno specializovanými dohledovými aplikacemi, které využívají externí monitorovací agenty instalované do sledovaných systémů. Ty v určitých intervalech monitorují systém a vysílají diagnostické informace na monitorovací server. V případě problémů je odeslána zpráva na zadaný email či telefon. Za určitých podmínek mohou tyto agenti zjednat automatickou nápravu problému, například restartem problémové služby.

5.1 System Center Operation Manager

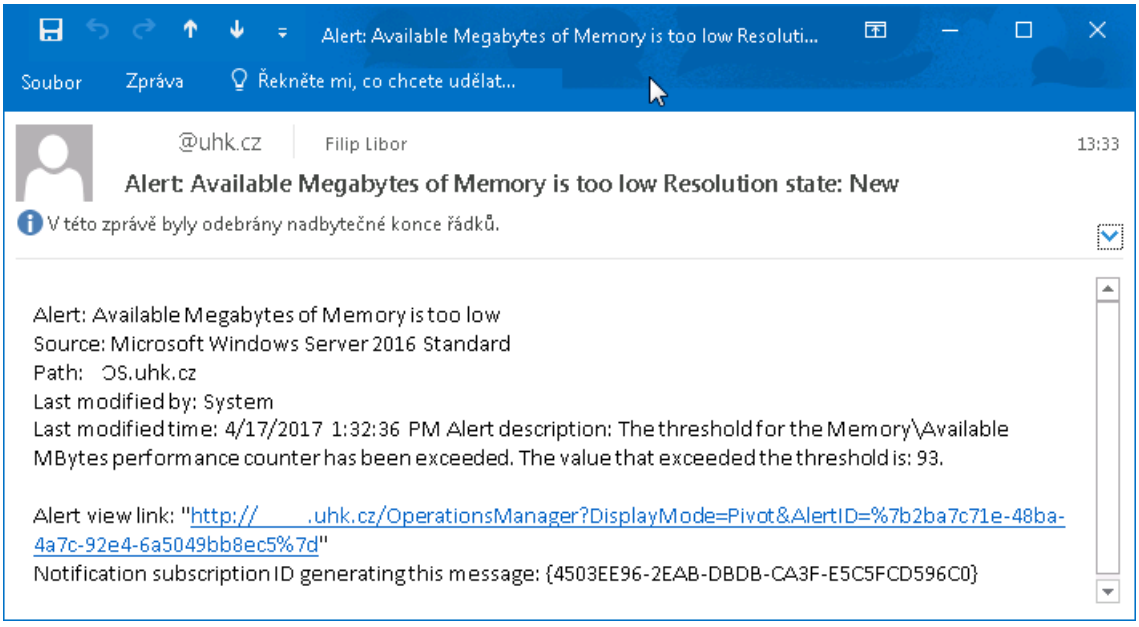
Jedním z dostupných systémů k monitorování dostupnosti a výkonu systému Windows je aplikace System Center Operation Manager. Systém má zjednodušit a zefektivnit správu většího množství serverů. Mezi nejčastěji zmiňované přednosti patří:

- Vyvíjen, používán a podporován přímo firmou Microsoft – vývojový tým může těžit přímo ze znalostí vývojového týmu systému Windows Server.
- Poskytuje různé možnosti způsoby monitorování. Bez instalace agenta do systému lze monitorovat například jen dostupnost systému. S instalací dodatečného software do systému (agenta) již hlídá výkonnostní charakteristiky, ale monitoruje i logy a další důležité části systému.
- Údaje jsou uchovávány po specifikovaný čas, tedy možno i několik let.
- Dle konfigurace, kdy je překročen určitý limit (threshold), zasílá v případě potíží varovnou zprávu na email nebo SMS. S napojením na bázi znalostí může doporučit i řešení problému.
- Instalací tzv. management packů je možnost rozšířit funkcionalitu systému o možnost sledování dalších systémů (například Linux), aplikací (SQL Server, IIS, Exchange) a infrastruktury (sítových prvků, hardware serverových systémů). Součástí bývají testy na optimální nastavení a běh systému dle tzv. Best practices,

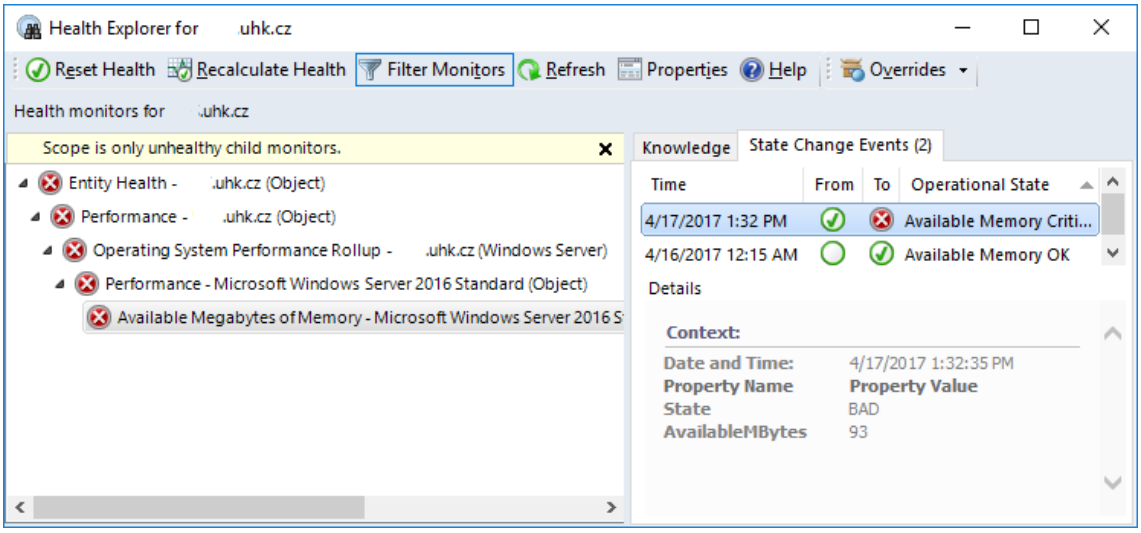
což jsou doporučené postupy k optimálnímu a bezpečnému provozu ke konkrétnímu typu systému či aplikace.



Obr. 22 System Center Operation Manager (zdroj: vlastní zpracování)



Obr. 23 SCOM : Příklad varování na email - Nedostatek RAM (zdroj: vlastní zpracování)



Obr. 24 SCOM : Health Explorer (zdroj: vlastní zpracování)

Plánování serveru k monitorování vysoké dostupnosti pomocí Systém Center má svá specifika (inspirace z praxe):

- Skutečné fyzické umístění dohledového serveru je vhodné a někdy i vyžadované zajistit mimo monitorovanou infrastrukturu (monitorován zvenčí) – pokud selhává připojení infrastruktury do internetu, monitorování z vnitřní sítě nemusí odhalit problémy a požadované parametry pro internetové uživatele. Někdy je využíváno více serverů nebo je požadavek kontroly řešen ze vzdáleného serveru (agenta).
- Pro dohledový server by měla být zajišťována také vysoká dostupnost, včetně infrastruktury.
- Při nesprávné konfiguraci týkající se odesílání varování, nebo nedostupnosti poštovního serveru či cílové schránky nebude varování o problémech doručeno.
- Implementace dohledu a následné řešení množství hlášení mohou být poměrně náročné.

6 Měření systémových prostředků

Zpracováno dle zdrojů [16, 20]:

Prvním měřením systémových prostředků bývá zjištění standardních hodnot, které jsou nejčastěji zjišťovány po instalaci systému, kdy ještě systém není zpřístupněn dalším uživatelům. V produkčním prostředí mohou být hodnoty upřesněny v době, kdy není systém využíván, například mimo pracovní dobu (v noci). Měření by nemělo být prováděno hned po spuštění, neboť prostředky mohou být mírně zvýšené z důvodu spouštění některých systémových úloh. Naše tabulka se zaměřila na porovnání používaných operačních systémů. Naměřené údaje v tabulce byly měřeny cca 30 minut po spuštění.

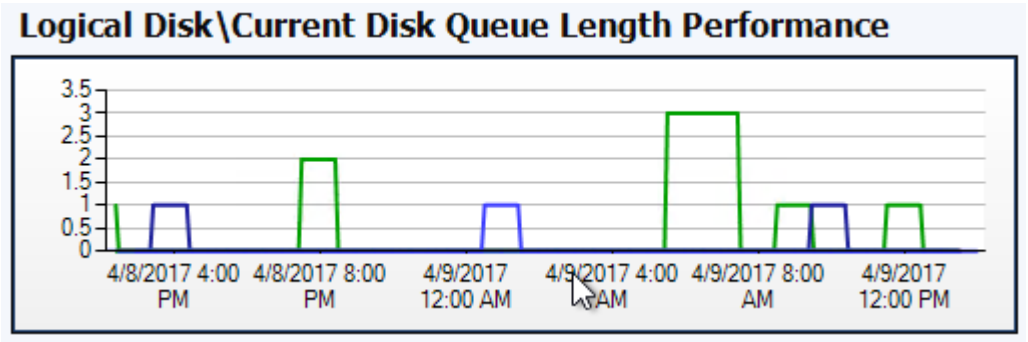
Tabulka 4 Systémové prostředky po instalaci (zdroj: vlastní zpracování)

	Srv 2012R2	Srv2016	Srv2016 Core	Win10 EDU (1607)
VHD File	8.97GB	9.78GB	6.7GB	8.78GB
Files	114 353	114 517	60 963	101 410
Folders	24 050	21 967	41 269	20 141
Pagefile.sys	1.37GB	1.37GB	1.37GB	1.37GB + 0.25GB*
Handles	9 690	14 095	8274	18 360
Threads	369	467	331	575
Processes	27	36	29	43
System Commit	606MB	612MB	416MB	821MB
Physical Memory	797MB	701MB	437MB	960MB

*Windows 10 má navíc soubor swapfile.sys (256 MB)

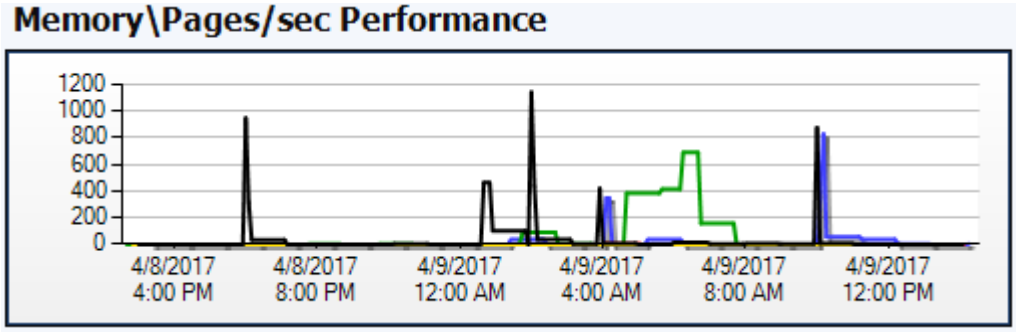
Na základě zjištěných hodnot, rezervy pro systémová data (aktualizace, logy, dočasná data) a požadavků na instalované role a aplikace můžeme určit skutečné přiřazené prostředky (velikost RAM a místa na disku). Ve velkých podnikových prostředích se někdy ještě využívají kalkulátory pro odhad systémových zdrojů na základě počtu uživatelů a dalších parametrů. Kontrolní nebo průběžné monitorování má následně zajistit, že přiřazených prostředků je dostatek.

V případě Univerzity Hradec Králové je jedním ze sledovacích systémů určený k proaktivnímu sledování výkonu již zmíněný nástroj Microsoft Operation Manager, proto je v této kapitole věnován prostor pro výchozí aktivované čítače a jejich grafy. Zmíněné toleranční hodnoty vycházejí z historických či praktických doporučení společnosti Microsoft, každý systém je přesto vhodné posuzovat individuálně a hraniční hodnotu výstrahy lze upravovat pro všechny nebo konkrétní systémy.



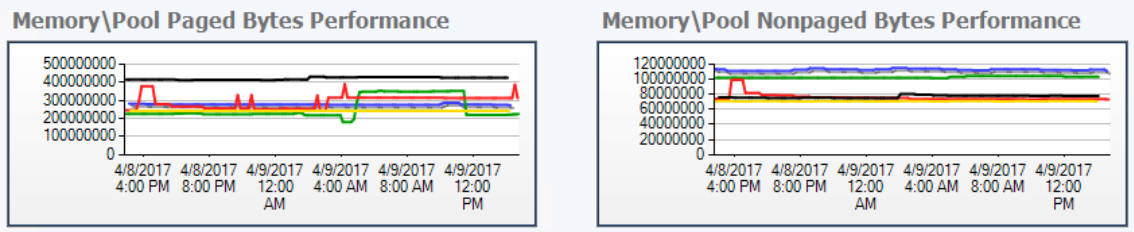
Obr. 25 MOM Graf: LogicalDisk\Current Disk Queue Length (zdroj: vlastní zpracování)

Aktuální délka fronty disku pro logický disk ukazuje počet nevyřízených požadavků. Výchozí prahová hodnota k tvorbě varování je **32**, při překročení je zaslána varovná zpráva „Aktuální délka fronty logického disku je příliš vysoká“. Důvodem může být vysoký počet požadavků od procesů nebo síťových požadavků na čtení z disku. Dalším krokem by bylo zjistit, jaké procesy disk využívají, zda jde o zápis nebo čtení a tím přibližněji určit bližší původ problému. Druhým důvodem mohou být chyby na disku, nebo nějaký problém s úložištěm, či konfigurací disků. Řešením může být kontrola disku, zlepšit výkon úložiště, omezit počet operací nebo rozložení operací na více disků. Instalace SQL serveru například může být rozdělena na systémový disk, disk pro data, disk pro soubory TEMPDB a disk pro záložní soubory.



Obr. 26 MOM Graf: Pages/sec (zdroj: vlastní zpracování)

Počet paměťových stránek za sekundu sleduje již ukazatele pro čtení či zápis paměťových stránek řešící hardwarové chyby stránkování. Chybová zpráva „Hodnota čítače Stránky paměti/s je příliš vysoká“ je zasílána při překročené hodnoty **250**. Nejčastěji se problém vyskytuje při nedostatku paměti RAM, pro další posouzení řešení je vhodné zajistit monitorování volné paměti a využívání stránkového souboru.

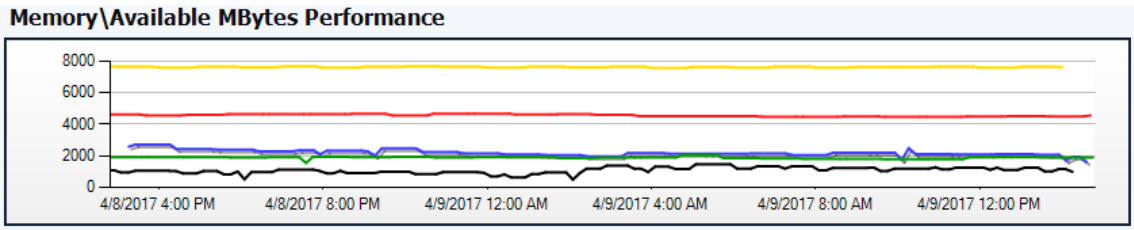


Obr. 27 MOM Graf: Memory\Pool Paged Bytes a Nonpaged (zdroj: vlastní zpracování)

Počet bajtů v nestránkovaném fondu paměti je oblast ve fyzické paměti určená pro objekty, které nelze zapsat na disk, ale je požadavek na jejich alokaci.

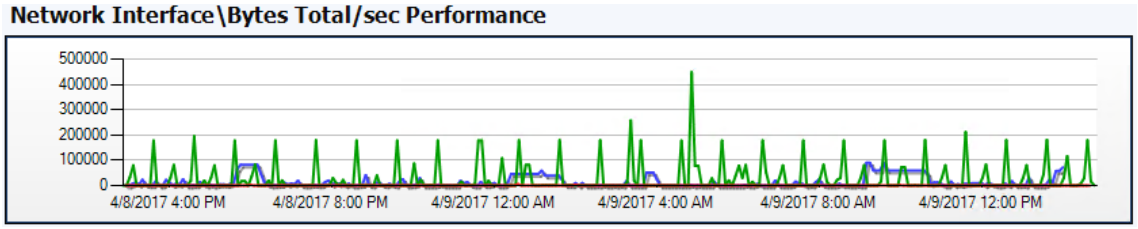
Počet bajtů ve stránkovaném fondu paměti je oblast ve fyzické paměti určená pro objekty, které lze zapsat na disk, pokud nejsou používány.

Pro oba čítače je udávaná kritická hodnota **2 000 000.**



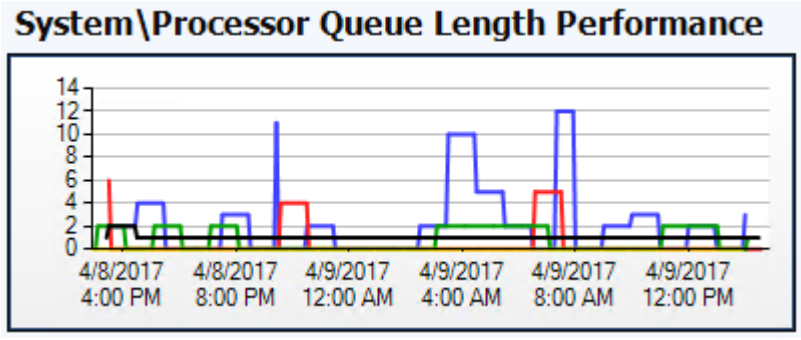
Obr. 28 MOM Graf: Memory\Available Mbytes (zdroj: vlastní zpracování)

Počet dostupných megabajtů paměti sleduje ukazatel volné paměti. Pokud ukazatel klesne pod **100**, je odeslána zpráva „Dostupná paměť v megabajtech je příliš nízká“. Kritický nedostatek paměti může způsobit nízký výkon operačního systému či konkrétní aplikace. Důvodem může být velký počet aplikací, nebo konkrétní aplikace zabírá příliš paměti v důsledku nějaké chyby. Samozřejmě může být i v malé velikosti paměti RAM.



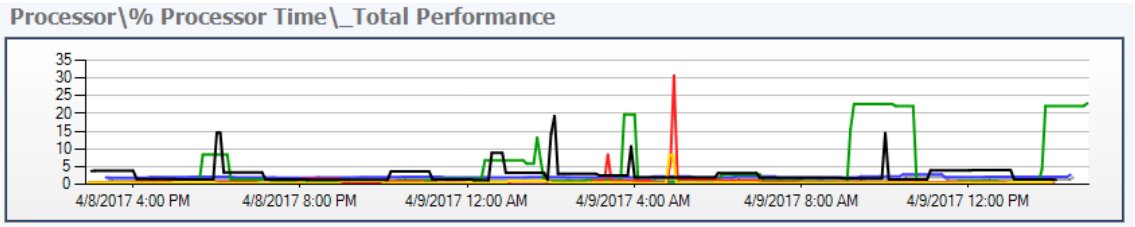
Obr. 29 MOM Graf : Network (zdroj: vlastní zpracování)

Celkový počet bajtů síťového adaptéru za vteřinu sleduje údaje o síťovém adaptéru a čítače výkonu celkového počtu přijatých a odeslaných bajtů za vteřinu. Udávaná kritická hodnota je 25% celkové propustnosti, která je závislá na síťovém adaptéru a síťovém připojení. Při případném řešení provozu je nutné dále určit, zda jde o data přijímaná či odesílaná. Optimalizace síťového provozu je ve velké míře závislá na architektuře sítě a používaných síťových prvcích, adaptérech a jejich ovladačích. V prostředí Windows serveru a virtualizace je navíc doporučeno věnovat se tématům týkajících se technologií jako je VMQ, SR-IOV, Receive Side Scaling, TCP Chimney Offload, NetDMA, NIC Teaming a případně dalším. Zapomínané řešení úspory šířky pásma je využívání komprese obsahu, to však může přinést vyšší nároky na procesor.



Obr. 30 MOM Graf : Processor Queue (zdroj: vlastní zpracování)

Délka fronty systémového procesoru obsahuje počet vláken umístěných ve frontě procesoru čekající na spuštění. Fronta je společná i pro počítače s více procesory. Problém dlouhé fronty vzniká, když procesy vyžadují více času než je k dispozici. Jako kritická hranice je uváděno 10 vláken na jedno jádro. Pokud nelze snížit dlouhodobě zátěž procesoru, měla by se zvážit jeho výměna. Problémy někdy může způsobovat i chybný ovladač nebo hardware. Chybu hardware může naznačovat procentuální hodnota času přerušení, kdy více než 10% je považováno za podezřelé.



Obr. 31 MOM Processor Time (zdroj: vlastní zpracování)

Celkové procento využití procesoru sleduje čítač monitorující celkové využívání procesoru v procentech, Za kritickou hranici je považováno **95%**.

Při vyhodnocování výsledků je nutné zohlednit určité specifické trendy, tvořící výkonnostní anomálie, nebo dobu, kdy se tvoří špičky. Také některé úkony údržby mohou tvořit v měření anomálie. Volba delšího časového období, například v akademickém prostředí odhalí větší zatížení studijních systémů v průběhu zápisů a zkouškového, v tuto dobu může být nutné přidělení větších systémových prostředků, zatímco v průběhu školního roku vyžadují větší prostředky spíše e-learningové aplikace. O prázdninách mohou být některé systémy i vypnuty nebo jim využívání systémových prostředků může být omezeno.

7 Shrnutí výsledků a doporučení

Práce se zabývá principy a údaji týkající se monitorování operačního systému Windows 2012, a v některých částech byla již rozšířena o zkušenosti autora s verzí 2016, ke které zatím bohužel chybí dokumentace vypovídající o případných změnách v architektuře.

Kapitola o edicích a rolích zmiňuje možnosti, které server nabízí a informace o edicích poukazují na edice Core a Nano, které mohou přispět k optimalizaci výkonu.

Architektura byla nedílnou součástí s ohledem na nutnou znalost termínů a konkrétních systémových procesů, které se dále objevují v částech věnované monitorování.

Praktičtější pohled na systém a získávání konkrétních výkonnostních dat je v kapitole monitorování rozdělen na interních a externí nástroje. Každé mají svá specifika a mohou být vhodná pro jiné situace, nebo se mohou doplňovat. Jejich používání je však už závislé na praxi, okolnostech a znalostech jak nástrojů, tak částí systému a výkonnostních dat.

Podnikový nástroj Operation manager může budit zdání o snadnosti správy, ukázkou jsou pěkné grafy a naznačení, že značně ulehčí práci. Jeho nastavení a úvodní seznamování, je však více než na pár dnů. Případná optimalizace a zjištění problémů do hloubky může být nakonec stejně závislá na sledování dat v reálném čase s využitím klasických nástrojů. Oba způsoby se tak vhodně doplňují.

Dle výsledků sledování operačního systému a běžících aplikací vznikalo několik možných řešení optimalizací:

- **Optimalizace kódu aplikace** – toto bývá často mimo možnosti administrátora a v případě hotových aplikací není možné. Někdy však existuje novější optimalizovanější verze. Příkladem může být zkušenost s hledáním řešení pomalé odezvy webové aplikace, využívající Microsoft SQL Server 2008R2, kdy přechodem na Microsoft SQL Server 2014 byl problém s odezvou vyřešen.
- **Optimalizace pomocí minimalizace využívání prostředků od ostatních aplikací** – jde o případ, kdy je na serveru příliš mnoho procesů nebo rolí, které je možné přesunout na jiný server či spouštět v jiný čas. Příkladem může být zálohování, antivirová kontrola či aktualizace na čas mimo špičku, nejčastěji je toto naplánováno na noční hodiny a prováděno automatizovaně. V případě zmíněného přesunu na jiný server, jde o možný přesun jedné z rolí na jiný server.

Velmi často se zvažuje rozdělení databázového serveru a aplikačního serveru na samostatné servery. Předpokladem je vhodný hardware cílového serveru a dobré síťové připojení, aby nedošlo naopak ke zpomalení.

- **Optimalizace pomocí silnějšího hardware** – v případě virtualizace může být velmi snadné přidělení dodatečných systémových prostředků, například dalšího virtuálního procesoru nebo paměti RAM. Na možnost rozšíření fyzického serveru musí být brán zřetel již při nákupu systému, i zde lze v mnoha případech dokoupit paměť RAM nebo vyměnit procesor. Při požadavcích na řešení problémů s náročnými aplikacemi na diskové operace je velmi často doporučované používat SSD disky nebo přikoupení více disků do diskového pole. Při dokupování HW do existujícího řešení je nutné zvážit životnost starého serveru, kdy často vhodnější je investice do nového serveru (příležitost zohlednit aktuální a budoucí požadovanou kapacitu, možnou škálovatelnost a konkrétní požadavky dle způsobu využívání).
- **Konsolidace** – optimalizace může být i s ohledem na cenu a zjednodušení správy, kdy se více serverů může naopak sloučit. V minulosti byla konsolidace hodně diskutovaným tématem, kdy se fyzické servery staly virtuálními a tím se mohlo z několika desítek serverů stát jeden či jen několik fyzických strojů. Svůj díl obvykle sehrál i nákup nového výkonnějšího hardware.
- **Automatizované optimalizace –** správu prostředků i celých virtuálních serverů lze do jisté míry automatizovat. Tento trend je zřejmý především ve větších datacentrech. Prvním krokem může být využití dynamické paměti, kdy správu paměti řídí Hypervizor, zde můžou být určité obavy ze ztráty výkonu, ale přesto je toto řešení zmiňováno nově i ve spojení SQL serverem, který bývá na paměť velmi náročný. V případě zajištění optimálního umístění virtuálního serveru na nejvhodnějšího fyzického hostitele v privátním cloudu může sloužit System Center Virtual Machine Manager nebo konkurenční virtualizační platforma Vmware vSphere [22].

Delší období odhaluje určité trendy v průběhu roku. V akademickém prostředí může být například větší zatížení studijních systémů v průběhu zápisů a tím i nutnost přidělení větších systémových prostředků, zatímco v průběhu školního roku vyžadují větší prostředky spíše e-learningové aplikace.

8 Závěr

Práce v úvodu připomněla architekturu klient / server, možné role serveru a vlastnosti desktopového systému Windows 10, který především v domácím prostředí může plnohodnotný Windows server nahradit. Problémy s výkonem nebo funkčností se mohou dotknout obou systémů, kdy k odhalení příčin je k dispozici mnoho různých nástrojů. Jejich použití je snadnější, pokud známe architekturu systému, jednotlivé procesy a různá výkonnostní data, které jsou probírány ve třetí kapitole.

Ještě před použitím nástrojů je téměř nutné určit důvod a provádění měření. Jen optimální běh není příliš vhodný a určitý cíl. Proto se úvod čtvrté kapitoly zaměřuje na potřeby zjištění dostupnosti, kapacity systému a maximalizace rychlosti. Doplněny jsou způsoby monitorování v podobě proaktivního, sledování v reálném čase či zátěžového. V úvodu čtvrté kapitoly jsou některé důvody, proč nejčastěji monitorujeme

Zbývající část čtvrté kapitoly již je více zaměřena na praktickou část obsahující popis nástrojů a souvisejících výkonnostních dat, které jsou užitečné pro správce systémů, kteří chtějí najít nejvhodnější způsob monitorování a rozhodnout jak vyřešit problém s optimalizací výkonu.

Konkrétní doporučení je však velmi obtížné. Každý systém je silně individuální, obsahuje různé aplikace a je využíván od různých uživatelů s výsledkem různé zátěže, která se může často měnit. Proto i výběr představených nástrojů se může měnit. Ale věřím, že mnoho z údajů uvedených v práci se bude hodit. S ohledem na rozsáhlost tématu nejsou některá specifika probírána příliš do hloubky, i když by to bylo vhodné. V dalším prohloubení znalostí může pomoci uváděná literatura.

Jako blízké a důležité téma by mohla být dále v práci zmíněna problematika monitorování a vyhodnocování logů, které zachycují některé mimořádné situace, například chyby aplikace nebo hardware. Částečně to řeší nástroje Operation manager a Sledování spolehlivosti.

Samostatná témata jsou specifická monitorování aplikací, kdy například monitorování a optimalizace SQL Serveru je téma na samostatnou velmi obsáhlou práci.

Na úplný závěr bych připomenul zjednodušený souhrn doporučení pro optimální nasazení systému, těmito variantami jsou:

- Optimalizace kódu aplikace – ne vždy je to možné a může to být finančně nákladné. U průběžně vyvíjené aplikace může být řešení novější, aktualizované a optimalizované verze. V případě webové aplikace může pomoci aktualizace podpůrné části, například novější SQL Server 2014/2016 přináší v porovnání se staršími verzemi výrazné zlepšení výkonu.
- Optimalizace pomocí snížení zátěže systému v podobě ukončení či přesunu ostatních aplikací – obvykle nejjednodušší varianta, kdy server může být zatěžován více aplikacemi, což je nežádoucí. Aplikace provádějící zálohování nebo jinou činnost údržby je doporučeno přeplánovat na noční hodiny. Aplikace složené z více rolí, je vhodné rozdělit na více serverů. Opět toto vždy není možné a mohou se vyskytnout omezení, například nutnost více licencí a provozování více serverů.
- Optimalizace pomocí silnějšího hardware – v této variantě rozhodují především finance. Pokud je server virtualizován, mohou být k přidělení další prostředky bez dalších nákladů. V mnoha případech může být finančně přijatelný částečný upgrade, kdy nejčastější volbou ke zrychlení je výměna CPU, více disků nebo SSD disky.
- Konsolidace – nejčastější volba při nákupu nového hardware, kdy pomocí virtualizace lze z více fyzických serverů přenést do virtualizované infrastruktury, případně lze umístit na nový server více virtuálních počítačů. Výhodou toho to řešení bývá snadnější správa a úspora licencí.
- Automatické optimalizace – určeno do velkých prostředí s využitím skriptování a dohledových systémů. Výhodou bývá úspora času a zajištění vysoké míry poměrně kvalitní automatizace systémových zdrojů. Nevýhodou můžou být vyšší nároky na finance a čas při nasazení.

Problematika monitorování a optimalizace je velice komplexní a dynamicky se vyvíjející. Byly představeny jak interní tak externí nástroje pro měření a optimalizaci výkonu operačních systémů rodiny Windows a za jejich použití byl prakticky částečně optimalizován jejich výkon a využity uváděné varianty. Autor si je však vědom komplexnosti tématu a dané problematice do hlubší úrovně by se chtěl dále věnovat.

Seznam použité literatury

[1] Performance Tuning Guidelines for Windows Server 2012 R2. Hardware Dev Center [online]. 2012 [cit. 2015-08-18]. Dostupné z: https://msdn.microsoft.com/en-us/library/windows/hardware/dn529133.aspx

[2] CARPENTER, Tom. *Microsoft Windows server administration essentials*. Indianapolis, Ind.: Wiley, c2011. ISBN 978-1-118-01686-2.

[3] Introduction to Hyper-V on Windows 10 [online]. [cit. 2015-10-18]. Dostupné z:https://msdn.microsoft.com/en-us/virtualization/hyperv_on_windows/about/hyperv_on_windows

[4] Using Windows 10 Client Hyper-V [online]. [cit. 2015-10-18]. Dostupné z: https://www.microsoft.com/en-us/download/details.aspx?id=48128

[5] Memory Limits for Windows and Windows Server Releases. Windows Dev Center [online]. [cit. 2015-10-18]. Dostupné z: https://msdn.microsoft.com/en-us/library/windows/desktop/aa366778.aspx

[6] ZACKER, Craig. *Exam ref 70-410: installing and configuring Windows server 2012*. ISBN 9780735673168.

[7] Windows Server Installation Options [online]. [cit. 2015-10-18]. Dostupné z: https://technet.microsoft.com/en-us/library/hh831786.aspx

[8] Instalace Nano Serveru[online]. [cit. 2017-04-01]. Dostupné z: https://technet.microsoft.com/cs-cz/windows-server-docs/get-started/getting-started-with-nano-server

[9] Server Roles and Technologies in Windows Server 2012 R2 and Windows Server 2012. Microsoft Technet [online]. [cit. 2015-10-13]. Dostupné z: https://technet.microsoft.com/en-us/library/hh831669.aspx

[10] Stanek W. Windows Server 2016: Installing & Configuring. Stanek & Associates; 2016. ISBN 1535074094.

[11] STANEK, William R. *Microsoft Windows Server 2012: kapesní rádce administrátora*. Přeložil Jiří HUF. Brno: Computer Press, 2015. ISBN 9788025138175.

[12] SILBERSCHATZ, Abraham., Peter B. GALVIN a Greg. GAGNE. *Operating system concepts*. Ninth edition. ISBN 9781118063330.

[13] Operační systémy I. Horalek.org [online]. [cit. 2015-11-10]. Dostupné z: http://www.horalek.org/os/

[14] DRÁB, Martin. Jádro systému Windows: kompletní průvodce programátora. Vyd. 1. Brno: Computer Press, 2011, 472 s. Programování (Computer Press). ISBN 978-80-251-2731-5.

[15] RUSSINOVICH, Mark E, David A SOLOMON a Alex IONESCU. Windows internals. 6th ed. Redmond, Wash.: Microsoft Press, c2012, 2 v. ISBN 97807356658732.

[16] FRIEDMAN, Mark. *Sledování a optimalizace výkonu Microsoft Windows Serveru 2003*. Přeložil Karel VORÁČEK. Brno: Computer Press, 2006. ISBN 9788025112632.

[17] User mode and kernel mode [online]. [cit. 2017-02-18]. Dostupné z: https://msdn.microsoft.com/windows/hardware/drivers/gettingstarted/user-mode-and-kernel-mode

[18] MALINA, Patrik. Procesy a jejich "běh" ve Windows. *Wug.cz* [online]. 2010 [cit. 2017-01-05]. Dostupné z: http://www.wug.cz/zaznamy/32-Procesy-a-jejich-beh-ve-Windows

[19] RUSSINOVICH, Mark E a Aaron MARGOSIS. Troubleshooting with the Windows Sysinternals Tools, 2nd Edition. Redmond, WA: Microsoft Press, 2016, 688 p. ISBN 9780735684447.

[20] System Center Core Technical documentation Library of management packs for Operations Manager and Service Manager. [online]. [cit. 2017-04-01]. Dostupné z: http://systemcentercore.com/

[21] MEYLER, Kerrie., Cameron FULLER, John. JOYNER a Andy. DOMINEY. *System Center Operations Manager 2007 unleashed*. Indianapolis, Ind.: Sams, c2008. ISBN 9780672329555.

[22] Running SQL Server with Hyper-V Dynamic Memory [online]. [cit. 2017-04-01]. Dostupné z: https://msdn.microsoft.com/en-us/library/hh372970.aspx

Oskenované zadání práce

Univerzita Hradec Králové
Fakulta informatiky a managementu
Akademický rok: 2014/2015

Studijní program: Aplikovaná informatika
Forma: Kombinovaná
Obor/komb.: Aplikovaná informatika (ai3-k)

Podklad pro zadání BAKALÁŘSKÉ práce studenta

PŘEDKLÁDÁ:	ADRESA	OSOBNÍ ČÍSLO
Filip Libor	Na Obci 365, Předměřice nad Labem	I1300223

TÉMA ČESKY:

Analýza možností měření a optimalizace výkonu Windows server

TÉMA ANGLICKY:

Analysis of performance monitoring and tuning of Windows Server

VEDOUCÍ PRÁCE:

Mgr. Josef Horálek, Ph.D. - KIT

ZÁSADY PRO VYPRACOVÁNÍ:

Cílem práce je provést analýzu možností a interních a externích nástrojů pro měření výkonu a zatížení serveru a jeho vybraných služeb a provést návrh optimálních metod pro tato měření. Autor práce představí možnosti a nástroje pro měření výkonu a zátěže služeb na Windows serveru a provede praktická měření s využitím vybraných nástrojů pro prostředí vzdělávací instituce.

SEZNAM DOPORUČENÉ LITERATURY:

Russinovich, M. E., & Margosis, Aaron. Troubleshooting with the Windows Sysinternals tools. Redmond, WA: Microsoft Press, 2016, 688 pages. ISBN 978-073-5684-447.

RUSSINOVICH, Mark E., David A. SOLOMON a Alex. IONESCU. Windows internals. 6th ed. Redmond, Wash.: Microsoft Press, c2012. ISBN 978-0735648739.

RUSSEL, Charlie. Exam Ref 70-411: administering Windows Server 2012 r2. Boston, MA: Springer-Verlag New York Inc, 2013, pages cm. ISBN 978-073-5684-799.

THOMAS, Orin. Training guide: configuring advanced windows server 2012 r2 services. Boston, MA: Springer-Verlag New York Inc, 2013, pages cm. ISBN 978-073-5684-713.

Podpis studenta: ..... **Datum:** .....

Podpis vedoucího práce: ..... **Datum:** .....