

## Monitorování a výkon

[ Povinné ]

### Sledování výkonu (Performance Monitor)

[ Povinné ]

Nástroj **Sledování výkonu** slouží k vizuálnímu zobrazení hodnot vybraných čítačů v reálném čase. Systém Windows obsahuje velké množství vestavěných čítačů, které lze využít pro měření výkonu systému. Velkou část tvoří čítače hardwarových prostředků (procesor, paměť, disk, ...), ovšem jsou zde i čítače softwarové (databáze, TCP/IP stack, .NET platforma). Kromě vestavěných čítačů si programy mohou registrovat i své vlastní čítače, pokud to může být z hlediska jejich činnosti výhodné.

### Sady kolekcí dat (Data Collector Sets)

[ Povinné ]

**Sady kolekcí dat** (Data Collector Sets) jsou součástí nástroje **Sledování výkonu**. Sada kolekcí dat sdružuje čítače dat do opakovaně použitelných skupin. Od Windows 7 umožňují zaznamenávat tyto informace:

- Čítače výkonu a výstrahy
- Trasování událostí zobrazující detailní ladící informace
- Nastavení registrů zobrazující nastavení systému a aplikací

Získané hodnoty čítačů lze poté zobrazit v nástroji **Sledování výkonu**, souhrn zbylých dat je zobrazen ve vygenerované zprávě.

Ve Windows je obsaženo několik vestavěných kolekcí dat, které byly navrženy pro získávání relevantních informací k řešení častých problémů. Patří sem:

- **Výkon systému** (System Performance) – Základní sada čítačů (procesor, disk, paměť, síť) a trasování jádra. Vhodné pro řešení problému při náhlém zpomalení počítače.
- **Diagnostika systému** (System Diagnostics) – Obsahuje navíc sběr detailních informací o systému. Vhodné pro řešení problémů stability systému jako selhávání ovladačů, problematického hardwaru, pádů systému (modrá obrazovka) apod.

Monitorování systému a sběr dat nezanedbatelně zatěžuje samotný systém, proto je důležité volit relevantní data pro sběr a provádět monitorování jen po nezbytnou dobu. Lze definovat vlastní kolekce dat, buď na základě existujících šablon, nebo úplně od začátku.

Pro usnadnění porovnávání grafů hodnot čítačů lze spustit nástroj **Sledování výkonu** v samostatném režimu, k tomu slouží přepínače **/sys /comp**. V tomto režimu naleznete v menu položku **compare**, která umožňuje nastavit průhlednost okna a přichytit ho k jinému oknu nástroje **Sledování výkonu**.

### Správce úloh (Task Manager)

[ Povinné ]

Poskytuje základní informace o výkonu počítače a správě aplikací, procesů, služeb a sezení uživatelů. Obsahuje grafy využití procesoru a paměti a graf vytížení sítě a umožňuje sledovat další prostředky systému. Tyto informace jsou často dostačující k zjištění příčiny náhlého zpomalení systému nebo jiných potíží.

Hlavní důležitost **Správce úloh** ovšem spočívá ve správě procesů. Nástroj poskytuje informace o běžících procesech a umožňuje ovlivňovat jejich běh. Lze vynutit explicitní ukončení běhu programu nebo nastavit jeho prioritu (prioritu reálný čas se doporučuje používat pouze v odůvodněných případech, protože takto běžící proces získá prioritu, která může být vyšší než priorita procesů samotného operačního systému). U víceprocesorových systémů nebo vícejaderných procesorů je možné nastavit spřažení (*affinity*), čímž je možné explicitně specifikovat, na kterých procesorech (nebo jádrech) může daný proces běžet. Dále je zde možnost povolení či zakázání UAC virtualizace pro jednotlivé procesy. UAC virtualizace umožňuje simulovat u procesu běžícího s oprávněním standardního uživatele přístup k částem systému (registry, systémové soubory), ke kterým by normálně přístup neměl. Tyto přístupy jsou transparentně přesměrovány do jiné části systému, kde

má proces vyžadované oprávnění pro danou operaci (např. při zápisu do chráněné části registrů je tento zápis přesměrován do větve uživatele, kde má proces právo zápisu, aniž by to proces jakkoliv zjistil). U 64bitové verze Windows jsou navíc u procesů informace o typu architektury (zda je aplikace 32 nebo 64 bitová).

**Správce úloh** lze využít pro násilné ukončení procesů v případě, že přestaly reagovat nebo neúměrně vytěžují systém. Násilné ukončení by mělo být až posledním pokusem o vypnutí programu, protože nezaručuje korektní uložení nastavení a jiných dat. Dalším častým využitím **Správce úloh** je omezení chodu určitých náročnějších aplikací pouze na specifické procesory nebo jádra, aby měl systém dostatek času procesoru pro svou vlastní činnost a adekvátní rychlostí mohl reagovat na nastalé události v systému.

Ve Windows 8 byl správce úloh přepracován. Je přehlednější, umožňuje zobrazovat statistiky využívání prostředků Modern UI aplikacemi, a také umožňuje spravovat **Služby** a aplikace **Po spuštění**.

## Process Explorer

[ Povinné ]

Alternativní náhrada za **Správce úloh**, zdarma ke stažení na stránkách Microsoft TechNet<sup>1</sup>. Poskytuje rozšířené možnosti správy procesů. Zobrazuje procesy ve stromové hierarchii, která poskytuje informace o nadřazených procesech jednotlivých procesů. Kromě mnohem podrobnějšího seznamu procesů (**Správce úloh** nezobrazuje všechny běžící procesy) umožňuje tato hierarchie lepší lokalizaci procesů (např. procesy služeb jsou situovány pod uzlem procesu **services.exe**, protože tento proces zajišťuje spouštění veškerých služeb systému). Také lze jednoduše zjistit, který proces spustil které jiné procesy. Tyto informace jsou velice výhodné při klasifikaci neznámých procesů, které mohou být např. viry nebo lokalizaci procesů, které běží v pozadí bez našeho vědomí, a zjišťování, který proces tyto skryté procesy vlastně spustil (např. zda jsou spouštěny jako služba, jako program po spuštění nebo je třeba spouští jiný proces při svém startu).

U každého procesu lze získat nepoměrně více informací než u **Správce úloh**, kromě informací o prioritách, využití procesoru a paměti apod., lze například zjistit informace ohledně využívaných DLL knihoven, popisovačů (otevřených souborů, semaforů, mutexů a jiných využívaných zařízení), platformě .NET (Počet načtených tříd, alokace paměti, čas Garbage Collectoru) nebo vláken, které proces vytvořil.

**Process Explorer** může zcela nahradit **Správce úloh**, stačí zvolit **options -> Replace Task Manager**. Systém bude poté vyvolávat automaticky místo **Správce úloh** vždy **Process Explorer**. Protože od Windows 8 jsou veškeré programy vždy spouštěny s oprávněními standardního uživatele, je po zobrazení **Process Exploreru** pouze část informací o procesech (hlavně se to týká procesů služeb a jiných systémových procesů), pro přepnutí **Process Exploreru** do režimu pod právy administrátora (a zobrazení veškerých možných informací) stačí zvolit **File -> Show Details for All Processes**.

## Prohlížeč událostí (Event Viewer)

[ Povinné ]

V průběhu chodu systému dochází k velké řadě událostí, tyto události jsou zaznamenávány do protokolů událostí. **Prohlížeč událostí** umožňuje zobrazit obsah těchto protokolů uživateli v přehledné podobě. Tyto informace jsou velmi často užitečné při řešení problémů s operačním systémem, ovladači nebo běžícími aplikacemi. Zaznamenané události se dělí do 4 kategorií:

- **Kritické** (Critical)
- **Chyby** (Error)
- **Výstrahy** (Warning)
- **Informace** (Information)

Většina událostí je informačního rázu a mohou být bezpečně ignorovány. Je velice důležité umět mezi tímto obrovským množstvím zanedbatelných událostí najít ty důležité, které mohou popisovat chyby hardwaru nebo narušení bezpečnosti systému.

<sup>1</sup> Stažení na adrese <http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx>

Protokoly událostí rozděleny do dvou hlavních kategorií:

- **Protokoly systému Windows** (Windows Logs) – Shromažďují události, které nastaly činností běžících aplikací (kategorie Aplikace), události auditování spojené s bezpečností (kategorie Zabezpečení) nebo události samotného systému (kategorie Systém).
- **Protokoly aplikací a služeb** (Applications and Services Logs) – Obsahují detailní popis událostí velké řady služeb systému a vlastní protokoly různých aplikací. Poskytují řadu informací, které v předchozích verzích nebyly k dispozici.

Kromě detailnějších informací v protokolech událostí poskytuje **Prohlížeč událostí** také statistické informace o událostech.

Dále jsou zde možnosti filtrování. Události lze filtrovat podle velkého množství kritérií a pomocí těchto filtrů definovat vlastní pohledy na události a vytvářet tak vlastní protokoly událostí. K událostem lze přidružit akci, která se vykoná při výskytu události (*event trigger*), akcí může být spuštění programu, poslání e-mailu nebo zobrazení zprávy. Události lze také přeposílat na vzdálené počítače, což velice usnadňuje správu systému v rozsáhlých sítích s velkým počtem klientských stanic. Kromě standardních protokolů jsou navíc k dispozici protokoly pro ladění a analýzu (Trace and Debug Logs) poskytující detailní informace vhodné pro vývojáře.

## Zasílání událostí (Event Forwarding)

[ Povinné ]

Rozšíření možností protokolování představené ve Windows Vista. Umožňuje centralizovat kontrolu protokolů a tím podstatně usnadnit správu rozsáhlejších sítí počítačů.

Pokud nastalá událost splňuje specifikované pravidla je automaticky odeslána na vzdálený počítač. Přenos je realizován pomocí protokolu HTTP nebo HTTPS. I když protokol HTTP není šifrován (na rozdíl od HTTPS) jsou při zasílání událostí data vždy šifrována. Šifrování dat probíhá rozdílně podle charakteru sítě. V pracovních skupinách se typ šifrování vybírá na základě vzájemné domluvy mezi komunikujícími stranami, které se dohodnou na **poskytovateli zabezpečení**<sup>2</sup> (SSP, *Security Service Provider*). V doménovém prostředí se pro šifrování dat použije Microsoft Kerberos SSP. Použití protokolu HTTPS pouze přidá další úroveň ochrany šifrováním pomocí SSL certifikátu, tato další úroveň navíc však ve většině prostředí není potřeba.

K správné činnosti zasílání událostí je potřeba, aby na obou počítačích běžely dvě služby:

- **Vzdálená správa systému Windows** (Windows Remote Management)
- **Sběr událostí systému Windows** (Windows Event Collector)

Kromě těchto běžících služeb je ještě potřeba specifikovat výjimky v bráně firewall systému Windows, které povolují komunikaci mezi oběma počítači.

Zasílání událostí může fungovat ve dvou režimech. Liší se tím, kdo iniciuje sběr událostí, čili zdroj události kontaktuje sběratelskou protistranu (*source-initiated*) nebo sběratel žádá o poslání událostí (*collector-initiated*). V prvním případě tedy počítač, kde událost vznikla, kontaktuje sběratelův počítač a přepoše mu událost. Tento způsob je vhodný pro použití v prostředí s velkým množstvím zdrojových počítačů generujících události, výhodou je také to, že jej můžete konfigurovat pomocí Zásad skupiny (*group policy*). Druhý způsob je doporučován spíše do menších prostředí.

Na počítači, jenž bude sloužit jako sběratel událostí, musí být nainstalován operační systém Windows Vista a novější, ze serverových produktů Windows Server 2003 R2 a novější. Jako operační systém na zdrojových počítačích postačí alespoň Windows XP SP2 nebo Windows Server 2003 SP1.

## Plánovač úloh (Task Scheduler)

[ Povinné ]

**Plánovač úloh** umožňuje reagovat na velkou řadu událostí jako např. start nebo vypínání systému. Akce mohou být vyvolány, pokud je do protokolu událostí přidána definovaná událost. Vyvolání úlohy

<sup>2</sup> Více informací o poskytovatelích zabezpečení na <https://docs.microsoft.com/cs-cz/windows/win32/secauthn/ssp-packages-provided-by-microsoft>

může být závislé na celé sadě podmínek, stejně tak lze jako reakci definovat celou skupinu akcí. U akcí lze kromě spuštění programů nebo skriptů také poslat e-mail nebo zobrazit zprávu. Pokud některá z úloh selže, může být automaticky opětovně spuštěna (tedy restartována).

Hesla účtů, které využívají nastavené úlohy pro svůj chod, jsou uloženy pomocí **Správce pověření** (Credentials Manager) pro zajištění větší ochrany. U každé úlohy lze také nastavit automatické zaslání e-mailu, pokud dojde k selhání úlohy. Podrobné informace o předchozích běžích úlohy jsou k dispozici pod záložkou historie, tyto informace mohou být užitečné při řešení problémů týkajících se dané úlohy.

## Ochrana dat

[ Povinné ]

Ochrana dat je vždy nedílnou a důležitou částí správy počítače. Data mohou být ohrožena v mnoha ohledech. Mohou být ztracena vinou selhání hardwaru vlivem stárí nebo mechanického poškození, mohou být odcizena nepovolanou osobou nebo mohou být nevědomky modifikována samotným uživatelem. Systém Windows 10 poskytuje možnosti ochrany dat ve všech zmíněných situacích. Na rozdíl od svých předchůdců také poskytuje více zálohovacích nástrojů.

## Obnovení souborů Windows 7 (Windows 7 File Recovery)

[ Povinné ]

### Záloha bitové kopie systému (System Image Backup) od Windows 8.1

Důležitost zálohování dat je uživateli často opomíjena. Příčinou tohoto stavu je hlavně relativní spolehlivost pevných disků, které jsou většinou vyměněny, za novější a větší, dříve, než vlivem stárí selžou. U uživatelů budí tento stav dojem, že pevný disk je bezpečné úložiště dat, kde o data nemohou přijít. Selhání pevného disku ovšem nemusí být jen vlivem stárí, ale i vlivem okolí, jako např. přepětím v síti, které může způsobit poškození dat. Nemusí jít ani o samotné poškození, zálohování je také ochrana proti ztrátě dat odcizením.

Windows 10 poskytuje stejně jako jeho předchůdci sadu nástrojů pro zálohování a obnovu dat, tyto nástroje (často ve formě průvodců) lze nalézt v **Obnovení souborů Windows 7** v Ovládacích panelech (resp. jako odkaz Záloha bitové kopie v levém panelu v Historii souborů). Zatímco zálohování vyžaduje administrátorská oprávnění, obnovu může provést jakýkoliv uživatel, ovšem tento uživatel bude moci obnovit pouze ta data, ke kterým má dostatečná oprávnění a které jsou zahrnuty na místě aktuální zálohy.

**Nastavit zálohování** umožňuje provést okamžitou manuální zálohu vybraných souborů, nebo naplánovat automatické zálohování ve zvolenou dobu. Zatímco systém Windows Vista umožňoval zálohovat pouze vybrané kategorie souborů, což výrazně snižovalo využitelnost zálohování, od Windows 7 lze zálohovat jakékoliv soubory a adresáře. Také je podporováno zálohování souborů šifrovaných pomocí EFS. V záloze ovšem nejsou zahrnuty soubory systému (pokud se nevytváří se zálohou také bitová kopie systému), známých programů (soubory, jenž jsou v registrech definovány jako součást nainstalovaného programu), soubory uložené na oddílech se souborovým systémem FAT, dočasné soubory a obsah koše.

Kromě možnosti zálohy souborů umožňují Windows také vytvoření tzv. bitové kopie systému (*system image*). Tato záloha vytvoří kompletní obraz systému i dalších oddílů disku. V případě selhání počítače je možné pomocí instalačního média obnovit tento obraz a navrátit tak systém do funkčního stavu, ve kterém byl při vytváření obrazu. Po obnově tohoto obrazu je nutné provést novou validaci systému Windows.

## Obnovení systému (System Restore)

[ Povinné ]

Systém Windows 10, stejně jako předchozí verze, umožňuje vytvářet tzv. body obnovení (*restore points*). Při vytváření bodu obnovení se provede zálohování části systému, tato záloha probíhá většinou inkrementálně vzhledem k poslednímu bodu obnovení a je uložena na stejném oddílu jako zálohovaná data. Pokud dojde k situaci, že nelze systém spustit nebo je vážně narušena jeho stabilita, lze navrátit jeho stav na stav v době vybraného bodu obnovení. Body obnovení se mohou provádět automaticky

např. při instalaci nových ovladačů a aplikací, nebo manuálně uživatelem. Pokud dojde k poškození celého oddílu a ne jen systému, je velice pravděpodobné, že dojde i k poškození bodu obnovy. Pro tyto situace se doporučuje vytvářet bitové kopie systému zmíněné v předchozím textu.

## Refresh a Reset PC

[ Povinné ]

Jedná se o novinky představené ve Windows 8. Systém Windows si udržuje automaticky záložní bitovou kopii pro případ rychlé obnovy do normálního továrního nastavení (out-of-box). Tyto funkce ve Windows 10 naleznete v **Nastavení Windows – Aktualizace a zabezpečení - Obnovení** (Windows Settings – Update & Security – Recovery), od verze 1709 pak v **Centru zabezpečení v programu Windows Defender** (Windows Defender Security Center) nebo pomocí odkazu umístěného v **Ovládacích panelech – Obnovení** (Control Panel – Recovery).

### Refresh

Volba **Částečné obnovení počítače, které neovlivní soubory** (Refresh your PC without affecting your files). Obnoví systém do továrního nastavení při zachování uživatelských profilů a nainstalovaných Modern UI aplikací. Jiné aplikace a nastavení budou odstraněny.

### Reset

Volba **Všechno smazat a přeinstalovat Windows** (Remove everything and reinstall Windows). Kompletně obnoví systém do továrního nastavení. Vhodné pokud pomocí Refresh nedošlo k vyřešení potíží nebo pokud počítač dáváte někomu jinému.

## Historie souborů (File History)

[ Povinné ]

Jedná se v o nástupce **Stínových kopií** (Shadow Copies) známých z předchozích verzí Windows. **Historie souborů**, stejně jako **stínové kopie**, poskytují ochranu proti ztrátě dat při modifikacích souborů. Zaznamenávají předchozí verze jednotlivých souborů a umožňují návrat k těmto verzím. Na rozdíl od **stínových kopií** však nejsou data ukládána na stejném diskovém oddílu, ale na jiný oddíl, jiný disk nebo do sdílené složky.

Dalším rozdílem proti stínovým kopiím je, která data se budou ukládat – ukládají se všechny uživatelské knihovny, složka kontaktů, oblíbené, data synchronizovaná s MS OneDrive a Plocha.

Funkci historie souborů naleznete v ovládacích panelech i v Nastavení Windows – Aktualizace a zabezpečení, kde je nutné ji nejprve povolit a nakonfigurovat (na který disk se budou předchozí verze souborů ukládat, jak často bude ukládání probíhat a kolik verzí nebo diskového prostoru může být použito). Obnova předchozích verzí souborů se provádí opět v **ovládacích panelech** v nástroji Historie souborů.

## Stínové kopie (Shadow Copies)

[ Povinné ]

Poskytují ochranu proti ztrátě dat při modifikacích souborů. Zaznamenávají předchozí verze jednotlivých souborů a umožňují návrat k těmto verzím. **Stínové kopie** jsou úzce spjaty s body obnovy. Od Windows 7 je možné zapnout vytváření **stínových kopií** samostatně, bez souběžného vytváření bodů obnovy (tedy bez aktivace **Obnovení systému**), což přispívá k vyšší využitelnosti této technologie, hlavně v případě jiných než systémových oddílů, kde není potřeba vytvářet body obnovy. **Obnovení systému** naopak nelze zapnout jinak než zároveň s vytvářením **stínových kopií**.

**Stínové kopie** jsou vytvářeny automaticky, pokud byl soubor modifikován od doby posledního vytvořeného bodu obnovy. Správa předchozích verzí souborů se provádí ve **vlastnostech** daného souboru na záložce **předchozí verze**.



## OneDrive

[ Povinné ]

S OneDrivem můžete svoje soubory synchronizovat mezi počítačem a cloudem a dostat se tak k nim odkudkoliv – z počítače, mobilního zařízení nebo dokonce z webové stránky OneDrivu na adrese OneDrive.com. Když přidáte, změníte nebo odstraníte nějaký soubor nebo složku z vaší onedrivové složky, tento soubor nebo složka se přidá, změní nebo odstraní i na webových stránkách OneDrivu a naopak. S vašimi synchronizovanými soubory můžete pracovat přímo přes Průzkumníka souborů a dostanete se k nim i pokud jste zrovna offline. Všechny změny, které uděláte vy, nebo ostatní uživatelé se automaticky synchronizují pokaždé, když budete online. U jednotlivých souborů se v cloudu také vede historie verzí (vše za poslední měsíc nebo 25 předchozích verzí (může se změnit)). Smazaný soubor je možné obnovit po dobu 30 dnů z Koše dostupného přes webovou stránku OneDrive).

Jednotlivé složky v cloudovém úložišti, které se mají na počítač synchronizovat lze vybrat a snížit tím potřebné místo.

Klient OneDrive umožňuje zároveň používat až jeden osobní účet/Microsoft Account (složka OneDrive) a více účtů spravovaných organizací v rámci Office365 (složka OneDrive – NázevOrganizace).

Z pohledu zálohování je užitečná nejnovější možnost OneDrive ve Windows 10 a to zálohování Plochy, knihovny Dokumenty a knihovny Obrázky. Tato umístění pak budou synchronizována a chráněna stejně jako složka OneDrive. U osobního účtu pak lze nastavit i automatické ukládání fotografií a videí z externích zařízení (fotoaparáty, telefony,...)

## Další součásti systému Windows

[ Volitelné ]

### Hlášení a řešení problémů

[ Volitelné ]

V případě, že běžící program přestane pracovat nebo reagovat, umožňuje Windows zaslat informace o tomto problému Microsoftu a pokusit se zjistit, jak jej vyřešit. [Hlášení a řešení problémů](#) umožňuje procházet informace o nastalých problémech a měnit nastavení chování oznamování těchto problémů. [Hlášení a řešení problémů](#) je součástí [Zabezpečení a údržby](#), které lze najít v ovládacích panelech v sekci [Systém a zabezpečení](#), a je úzce spjata s nástrojem [Sledování spolehlivosti](#).

Nastavení oznamování problémů ([Zabezpečení a údržba](#), sekce [Údržba](#), [Nastavení u Vyhledat řešení hlášených problémů](#)) v předchozích verzích systému Windows zahrnovalo čtyři možnosti - automaticky vyhledávat řešení (s nebo bez rozšířených informací o problému), vyžadovat před vyhledáním potvrzení uživatele nebo nikdy nevyhledávat. Dále šlo specifikovat výjimky pro určité programy, jejichž problémy se nebudou oznamovat.

Ve Windows 10 je k dispozici pouze úroveň automatického oznamování, která je navíc ovlivněna úrovní zasílání diagnostických dat, a možnost hlášení problémů vypnout. Pokud je nastaveno automatické oznamování problému, nejsou informace odeslány vždy. V případě, že by informace mohly prozradit detaily o uživateli nebo počítači, bude systém vyžadovat potvrzení tohoto kroku uživatelem. Pokud by pro řešení zjištěného problému bylo třeba více informací, je tato skutečnost oznámena uživateli (pro potvrzení poskytnutí dalších informací **není třeba** mít administrátorské oprávnění). Někdy vyžaduje navržené řešení problému administrátorské oprávnění.

Pokud je oznamování problémů vypnuto, nedochází již k monitorování nastalých problémů, ani k ukládání informací o těchto problémech lokálně v systému. Pomocí seznamu problémů (sekce [Údržba](#), [Zobrazit historii spolehlivosti](#), [Zobrazit všechna hlášení problému](#)) lze procházet informace o nastalých problémech, aktualizovat jejich řešení nebo je odstranit ze seznamu.

## Centrum synchronizace (Sync Center)

[ Volitelné ]

Kromě zajištění ochrany dat je často velice důležité zajistit také dostupnost dat. Uživatel může mít uložena svá data na mnoha místech od pevného disku, přes výměnné disky a síťové disky až po mobilní telefony, mp3 přehrávače nebo flash disky. Sledovat všechna tato data může představovat podstatný

problém. **Centrum synchronizace** umožňuje jednoduše synchronizovat informace mezi počítačem a jiným zařízením. Aby tato synchronizace mohla probíhat je nejprve potřeba definovat partnerství mezi oběma zařízeními. Existují dva typy partnerství:

- **Jednosměrné** (*one-way*) – Data jsou synchronizována pouze v jednom směru
- **obousměrné** (*two-way*) – Data jsou synchronizována v obou směrech

U obousměrných partnerství může docházet ke konfliktům při synchronizaci. Tato situace nastane, pokud dojde ke změně dat na obou místech jejich uložení v době od poslední synchronizace. V takovém případě **Centrum synchronizace** oznámí tuto skutečnost uživateli a vyzve ho k výběru řešení situace (uživatel může vybrat kterou verzi ponechat nebo ponechat obě).

## Studentské úkoly

- Pro přístup na server **file** (a jiné) přes síťové rozhraní *Default switch* je nutné použít jeho plně kvalifikované doménové jméno **file.nepal.local**
- Přístupové údaje na server file: **nepal\hstudent** heslo: **aaa**
- Veškeré programy a skripty používané v následujících úkolech lze nalézt v adresáři **utils** v archivu s materiály ke cvičení.

## Lab S00 – konfigurace virtuálních stanic

[ Provést ]

Připojte síťové adaptéry stanic k následujícím virtuálním přepínačům:

Adaptér (MAC suffix)	LAN1 (-01)	LAN2 (-02)	LAN3 (-03)	LAN4 (-04)
<b>w10-domain</b>	Default switch	Private1	Nepřipojeno	Nepřipojeno
<b>w2016-dc</b>	Default switch	Private1	Nepřipojeno	Nepřipojeno

Stanici **w10-domain** nastavte pevnou velikost paměti na **2GB**.

## Lab S01 – Sady kolekcí dat a porovnávání grafů

[ Povinné ]

### Cíl cvičení

Vytvořit sadu kolekcí dat, jenž bude monitorovat vytížení CPU, a použít ji pro monitorování CPU během krátkého časového intervalu. Porovnat dva naměřené grafy vytížení CPU.

### Potřebné virtuální stroje

**w10-domain**

### Další prerekvizity

Vytvořený adresář **C:\Logs** a skript **simulate\_workload.vbs** (obsažen v **utils**).

1. Přihlaste se lokálně na **w10-domain** (uživatelské jméno **w10-domain\student**)
2. Spusťte **Sledování výkonu** (Performance Monitor) a rozbalte **Sady kolekcí dat** (Data Collector Sets)
3. Klikněte pravým tlačítkem na položku **Definované uživatelem** (User Defined) a vyberte **Nová položka -> Sada kolekcí dat** (New -> Data Collector Set)
4. Pojmenujte novou kolekci např. **Performance** a zvolte **Vytvořit ručně** (Create manually), pokračujte pomocí **Další** (Next)
5. Jako typ dat zvolte **Protokoly vytváření dat** (Create data logs) a zaškrtněte možnost **Čítač výkonu** (Performance counter), pokračujte pomocí **Další** (Next)
6. Přidejte do seznamu **Čítače výkonu** (Performance counters) čítač vytížení procesoru
  - Klikněte na tlačítko **Přidat ...** (Add ...)
  - Vyberte **Procesor -> % času procesoru** (Processor -> % Processor Time)
  - Jako **Instanci vybraného objektu** zvolte **\_Total**
  - Klikněte na **Přidat >>** (Add >>)
  - Potvrďte **OK**
7. Jako **Vzorkovací interval** (Sample interval) zvolte 2 sekundy, pokračujte pomocí **Další** (Next)
8. Nastavte **C:\Logs** jako adresář pro uložení sbíraných dat, pokračujte pomocí **Další** (Next)
9. Ponechte výchozí nastavení účtu, pod kterým sběr dat poběží, a zvolte možnost **Otevřít vlastnosti pro tuto sadu kolekcí** (Open properties for this data collector set), potvrďte pomocí **Dokončit** (Finish)



10. Ve vlastnostech (Properties) kolekce dat **Performance** přejděte na záložku **Podmínka ukončení** (Stop Condition)
  11. Zaškrtněte **Celková doba trvání** (Overall duration) a nastavte tuto dobu na 30 sekund, potvrďte pomocí **OK**
  12. Spusťte vytvořenou kolekci dat, např. klikněte pravým na **Performance** a zvolte **Začátek** (Start), vyčkejte, dokud sběr dat nebude dokončen
  13. Opětovně spusťte vytvořenou kolekci dat **Performance**, tentokrát zároveň se spuštěním skriptu **simulate\_workload.vbs**, a vyčkejte na dokončení sběru dat
  14. Spusťte 2x nástroj **Sledování výkonu** (Performance Monitor) v samostatném režimu (příkaz **perfmon /sys /comp**)
  15. V obou oknech otevřete první resp. druhý protokol s daty získanými dříve
    - Klikněte na **Zobrazit data protokolu** (View Log Data), druhá ikona vlevo nebo CTRL+L
    - V záložce **Zdroj** (Data source) vyberte Soubory protokolů (Log files) a klikněte na **Přidat ...** (Add ...)
    - Lokalizujte první resp. druhý protokol získaný dříve ve složce **C:\Logs**
    - Potvrďte **OK**
- Poznámka: pokud se po načtení log souboru se v okně nic nezobrazí, pak klikněte na přidat (+) a vyberte požadovaný čítač.
16. U druhého okna zvolte **Porovnat** -> **Nastavit Průhlednost** -> **Průhlednost 70%** (Compare -> Set Transparency -> 70% Transparency), poté zvolte **Porovnat** -> **Přichytit k porovnání** (Compare -> Snap to Compare)

## Lab S02 – Vytvoření vlastního zobrazení

[ Povinné ]

### Cíl cvičení

Vytvořit filtr pro zobrazení pouze událostí o spuštěných výstrahách (*alerts*) za poslední hodinu.

### Potřebné virtuální stroje w10-domain

1. Přihlaste se lokálně na **w10-domain** (uživatelské jméno **w10-domain\student**)
2. Otevřete **Prohlížeč událostí** (Event Viewer), vyberte kontejner **Vlastní zobrazení** (Custom Views)
3. Zvolte **Vytvořit vlastní pohled ...** (Create Custom View ...) v panelu akcí vpravo
4. V nabídce **Protokolováno** (Logged) zvolte **Poslední hodinu** (Last hour)
5. Jako **Úroveň událostí** (Event level) zaškrtněte pouze **Informace** (Information)
6. Zvolte **Podle zdroje** (By Source) a vyberte zdroj **Diagnosis-PLA**
7. U **Zahrnout nebo vyjmout ID událostí** (Includes/Excludes Event IDs) zadejte ID číslo **2031**
8. Vytvořte vlastní zobrazení potvrzením pomocí **OK**
9. Zadejte název zobrazení **LastHourPerformanceAlerts** a potvrďte pomocí **OK**

## Lab S03 – Nastavení výstrahy a reakcí na výstrahy

[ Povinné ]

### Cíl cvičení

Vytvořit výstrahu (*alert*), která při nedostatku místa na disku tento stav oznámí uživateli prostřednictvím e-mailu s informacemi o aktuálním stavu volného místa.

### Potřebné virtuální stroje w10-domain

### Další prerekvizity

Dokončený [Lab S02](#)

Soubor s šablonou **fsaTemplate.xml** (obsažena v **utils**).

Skript **send\_nefs\_mail.vbs** (obsažen v **utils**).

1. Přihlaste se lokálně na **w10-domain** (uživatelské jméno **w10-domain\student**)
2. Spusťte **Sledování výkonu** (Performance Monitor), rozbalte **Sady kolekcí dat** (Data Collector Sets)
3. Klikněte pravým tlačítkem na položku **Definované uživatelem** (User Defined) a vyberte **Nová položka** -> **Sada kolekcí dat** (New -> Data Collector Set)
4. Pojmenujte novou kolekci např. **FreeSpaceAlert** a zvolte **Vytvořit ze šablony** (Create from a template), pokračujte pomocí **Další** (Next)
5. Pro výběr šablony klikněte na **Procházet ...** (Browse ...) a lokalizujte **fsaTemplate.xml**
6. Po načtení šablony vyberte v seznamu **FreeSpaceAlert** a potvrďte pomocí **Dokončit** (Finish)
  - Tato šablona definuje výstrahu (*alert*) monitorující stav volného místa na disku C, pokud volné místo klesne pod 95% (normálně bude tato hranice samozřejmě nižší) zapíše tato výstraha informace o překročení hlídaného limitu do protokolu událostí, kontrola místa (hlídaného čítače) probíhá co 10 sekund
7. Spusťte **FreeSpaceAlert**, např. klikněte pravým na **FreeSpaceAlert** a zvolte **Začátek** (Start), vyčkejte alespoň 10 sekund, poté **FreeSpaceAlert** zastavte, např. pravým na **FreeSpaceAlert** a zvolte **Zastavit** (Stop)
8. Spusťte **Prohlížeč událostí** (Event Viewer) a lokalizujte záznam události překročení hlídaného prahu výstrahy (ID **2031**) některým z následujících postupů:
  - Využit **vlastní zobrazení LastHourPerformanceAlerts** vytvořené v **Lab S02**, jenž zobrazuje události týkající se překročení limitů u výstrah během poslední hodiny
  - Lokalizovat ručně daný záznam, **Protokoly aplikací a služeb** (Application and Services Logs) -> **Microsoft** -> **Windows** -> **Diagnosis-PLA** -> **Operational**
9. Klikněte pravým na nalezený záznam události a zvolte **Přidružit k této události úlohu ...** (Attach Task To This Event ...)
10. Ponechte vygenerovaný název a pokračujte pomocí **Další >** (Next >)
11. Zkontrolujte, zda akce reaguje na událost s ID **2031** a pokračujte pomocí **Další >** (Next >)
12. Jako akci vyberte **Spustit program** (Start a program) a pokračujte pomocí **Další >** (Next >)
13. V poli **Program či skript** (Program/script) lokalizujte skript **send\_nefs\_mail.vbs** a v poli **Přidat argumenty** (Add arguments) zadejte e-mailovou adresu (nejlépe vlastní, na kterou se rychle dostanete skrze webové rozhraní) a pokračujte
14. Potvrďte vytvoření akce stiskem **Dokončit** (Finish)
15. Ve **Sledování výkonu** (Performance Monitor) na cca 10-15 sekund spusťte **FreeSpaceAlert** (tak aby došlo k vygenerování výstrahy). Po chvíli ověřte doručení zprávy na zadanou e-mailovou adresu (Tip: zkontrolujte i složku s nevyžádanou poštou).
16. Otevřete **Plánovač úloh** (Task Scheduler) a lokalizujte úlohu, která byla vytvořena během tohoto úkolu (umístěna v kontejneru **Úlohy prohlížeče událostí** (Event Viewer Tasks)).
17. V případě potíží s odesláním e-mailu skriptem **send\_nefs\_mail.vbs**, smažte plánovanou úlohu a použijte program **msg** k zobrazení zprávy:
  - i. Zopakujte body 8 až 12
  - ii. V poli **Program či skript** (Program/script) zadejte **msg** a v poli **Přidat argumenty** (Add arguments) zadejte **"Dochází místo na disku"**
  - iii. Potvrďte vytvoření akce stiskem **Dokončit** (Finish)
  - iv. Ve **Sledování výkonu** (Performance Monitor) na cca 10-15 sekund spusťte **FreeSpaceAlert** (tak aby došlo k vygenerování výstrahy).

[ Povinné ]

## Lab S04 – Zasílání událostí

### Cíl cvičení

Zajistit, aby události vzniklé v předchozím úkolu (**Lab S03**) byly automaticky zasílány na počítač **w2016-dc**, kde mohou být centrálně monitorovány.

### Potřebné virtuální stroje

**w10-domain**  
**w2016-dc**

### Další prerekvizity

Dokončený úkol **Lab S03**.

Ve virtuálních strojích zakažte všechna síťová rozhraní mimo jejich vzájemného propojení (ověřte pomocí ping na celé doménové jméno druhé stanice).

1. Přihlaste se na **w10-domain** pod účtem správce domény (uživatel **testing\administrator**).
2. Z příkazové řádky spusťte **winrm quickconfig**
  - Na jednotlivé dotazy odpovězte kladně (y)
  - Alternativně bez dotazů: **winrm quickconfig -q**
3. Otevřete **Editor místních zásad skupiny** (Local Group Policy Editor) např. příkazem **gpedit.msc**
4. Vyberte **Konfigurace počítače** -> **Šablony pro správu** -> **Součásti systému Windows** -> **Předávání událostí** (Computer Configuration -> Administrative Templates -> Windows Components -> Event Forwarding).
5. Otevřete vlastnosti politiky **Nakonfigurovat cílového správce odběrů** (Configure target Subscriptions Manager). Povolte ji a nastavte adresu serveru:

**Server=http://w2016-dc.testing.local:5985/wsman/SubscriptionManager/WEC,Refresh=30**

- Pozn: lze samozřejmě nakonfigurovat i centrálně pomocí doménových zásad skupin
6. Z příkazové řádky spusťte **gpupdate /force**
  7. Přihlaste se na **w2016-dc** pod účtem správce domény (uživatel **testing\administrator**).
  8. Spusťte **příkazový řádek** se zvýšeným oprávněním.
  9. Pro povolení WinRM a sběru událostí spusťte následující příkazy:
    - a. **winrm quickconfig -q**
    - b. **wecutil qc**
      - jedná se o nástroj pro konfiguraci a ovládání sběru událostí (Windows Event Collector Utility)
      - qc = quick-config = základní konfigurace služby sběru událostí
      - Na jednotlivé dotazy odpovězte kladně (y)
      - Alternativně bez dotazů: **wecutil qc -q**
  10. Otevřete prohlížeč událostí, např. příkazem **eventvwr.msc**.
  11. Klikněte pravým tlačítkem myši na **Odběry** a vyberte **Vytvořit odběr...** (Subscription -> Create Subscription...). Pojmenujte nový odběr, např. **Free Space Alert**.
  12. Jako typ odběru vyberte **Spuštěno zdrojovým počítačem** (Source computer initiated).
  13. Dále přidejte účet počítače **w10-domain** mezi zdrojové počítače.
    - Použijte tlačítko **Vybrat skupinu počítačů** (Select Computer Groups...)
    - **Přidat doménové počítače...** (Add Domain Computers...), vyhledejte účet počítače a Potvrďte **OK**
  14. Ve vlastnostech odběru klikněte na **Vybrat události...** (Select Events...). Jako **Úroveň událostí** (Event level) zaškrtněte pouze **Informace** (Information)
  15. Zvolte **Podle protokolu** (By log) a vyberte uzel **Diagnosis-PLA** z Applications and Services Logs \ Microsoft \ Windows
  16. U **Zahrnout nebo vyjmout ID událostí** (Includes/Excludes Event IDs) zadejte ID číslo **2031** -> **OK** -> **OK**.

17. Pomocí tlačítka **Upřesnit** (Advanced...) přejděte do rozšířeného nastavení.
18. Přepněte optimalizaci doručení na **Minimalizovat zpoždění** (Minimize Latency) a potvrďte **OK**.
19. Zavřete okno vlastností odběru tlačítkem **OK**.  
Poznámka: Ačkoliv jsme nastavili filtr na cílovém systému, dochází k filtrování již na zdrojovém systému. V případě odběru iniciovaných zdrojovým počítačem a výběru událostí podle zdroje může v někdy docházet k zpožděním nebo problémům s filtrováním.
20. Pod uzlem **Odběry** (Subscriptions) prohlížeče událostí uvidíte nakonfigurovaný odběr.
  - Zkontrolujte stavovou ikonu a prohlédněte si možnosti kontextové nabídky i nabídky panelu **Akce** (Actions)Poznámka: pokud se po vytvoření odběru ukazuje u názvu žlutý trojúhelník s vykřičníkem a v detailech stavu je uvedena chyba 0x8033808F, zakažte všechny nepotřebné síťové adaptéry a případně zkuste vytvořit odběr znova
21. Prohlédněte si výpis příkazů
  - **wecutil es** (výpis odběrů)
  - **wecutil gs "<názevOdběru>"** (zobrazí informace o odběru, všimněte si parametru DeliveryMaxLatencyTime v ms)
  - **wecutil gr "<názevOdběru>"** (zobrazí aktuální stav odběru; naleznete zde i informaci kdy došlo k poslední komunikaci - hodnota LastHeartBeatTime)
22. Zopakujte kroky z předchozího úkolu pro vyvolání události s ID **2031**. Zkontrolujte příchod událostí v části **Windows Logs** -> **Forwarded Events** (u výše uvedené kombinace Refresh intervalu a nastavení latence by se měly události začít objevovat cca po minutě od dokončení konfigurace).

## Lab S05 – Historie souborů

[ Volitelné ]

### Cíl cvičení

Seznámit se s **Historií souborů**.

### Potřebné virtuální stroje

**w10-domain**

**w2016-dc**

1. Přihlaste se lokálně na **w2016-dc** (uživatelské jméno **testing\administrator**).
2. Na **w2016-dc** vytvořte a nasdílejte složku **C:\filehistory** (pro everyone).
3. Přihlaste se lokálně na **w10-domain** (uživatelské jméno **w10-domain\student**).
4. Ve složce dokumenty vytvořte textové soubory **student1.txt** a **student2.txt** (a případně další) s libovolným neprázdným obsahem.
5. Otevřete **Historii souborů** (File History).
  - Z ovládacích panelů – **Systém a zabezpečení** (System and Security).
  - Z **Nastavení** (PC Settings) – **Aktualizace a zabezpečení** (Update & Security) – **Zálohování** (Backup) – sekce **Zálohovat pomocí Historie souborů** (Back up using File History) – odkaz **Další možnosti** (More options) – odkaz **Zobrazit upřesňující nastavení** (See advanced settings).
6. Pokud není k dispozici žádná disková jednotka, objeví se žlutě podbarvené varování s možností zvolit **Vybrat umístění v síti** (Use network location). Pokud je k nějaká disková jednotka použitelná, zobrazí se v přehledu.
7. V levé nabídce zvolte **Vybrat jednotku** (Select drive).
8. Použijte odkaz **Přidat umístění v síti** (Add network location) a připojte sdílenou složku **filehistory** z **w2016-dc**. Následně se v okně **Vybrat jednotku** (Select drive) ujistěte, že je toto síťové umístění vybrané a pokračujte **OK**.
9. Ve výchozím nastavení Historie souborů zálohuje knihovny, plochu, kontakty a oblíbené položky. Pokud chcete některé z těchto umístění vynechat, použijte **Vyloučit složky** (Exclude folders) z levé nabídky.

10. Prozkoumejte možnosti pokročilých nastavení - [upřesnit nastavení](#) (Advanced settings) z levé nabídky.
11. Na hlavní obrazovce [Zapněte](#) (Turn on) [Historii souborů](#) (File History) a počkejte na dokončení úvodní kopie
12. Pozměňte obsah souboru student1.txt a soubor student2.txt smažte.
13. Vraťte se do [Historie souborů](#) (File history) a pomocí [Spustit](#) (Run now) vynuťte další zálohu.
14. Předchozí 2 kroky dle vlastního uvážení zopakujte.
15. Přepněte se na **w2016-dc** a prozkoumejte obsah složky **C:\filehistory**
16. Vraťte se na **w10-domain**, otevřete okno [Historie souborů](#) (File history) a z nabídky vlevo zvolte [Obnovit osobní soubory](#) (Restore personal files).
17. Najděte poslední existující verzi souboru student2.txt a obnovte jej.

## Lab S06 – Zálohování (Windows 7)

[ Volitelné ]

### Cíl cvičení

Seznámit se s možnostmi zálohování.

### Potřebné virtuální stroje

**w10-domain**

### Další prerekvizity

Připojený disk1.vhdx, naformátovaný jako NTFS a připojený jako B:

Textový soubory **student1.txt** a **student2.txt** (s libovolným neprázdným obsahem) ve složce dokumenty uživatele student.

1. Přihlaste se lokálně na **w10-domain** (uživatelské jméno **w10-domain\student**).
2. Spustíte [Zálohování a obnova \(Windows 7\)](#) (Backup and Restore (Windows 7)).
  - Z ovládacích panelů – [Systém a zabezpečení](#) (System and Security)
  - Z [Nastavení](#) (PC Settings) – [Aktualizace a zabezpečení](#) (Update & Security) – [Zálohování](#) (Backup) – sekce [Hledáte starší zálohu?](#) (Looking for an older backup?) – odkaz [Přejít k zálohování a obnovení \(Windows 7\)](#) (Go to Backup and Restore (Windows 7)).
3. V přehledu zálohování bude informace, že zatím není žádné zálohování nastaveno. Pokračujte odkazem [Nastavit zálohování](#) (Set up backup).
4. Vyberte Diskovou jednotku B: a pokračujte [Další](#) (Next).

Poznámka: V tomto kroku lze také zvolit uložení zálohy do sdílené složky. V tom případě pamatujte na omezení zachování pouze jedné kopie obsahující bitovou kopii (stará záloha se před zálohováním smaže).
5. V kroku [Co chcete zálohovat?](#) (What do you want to back up?) zvolte [Nechat rozhodnout mě](#) (Let me choose) a pokračujte [Další](#) (Next).
6. Zrušte zaškrtnutí vše políček a zaškrtněte pouze knihovnu dokumenty uživatele student.
7. Zrušte zaškrtnutí u [Zahrnout bitovou kopii systému z jednotek SYSTEM, \(C:\)](#) (Include a system image of drives: EFI System Partition, (C:)) a pokračujte [Další](#) (Next).
8. Zkontrolujte plán zálohování a prozkoumejte možnosti.

Poznámka: Bitová kopie se provede pouze při prvním běhu zálohování. Pro pravidelnou zálohu systému je potřeba vytvořit plánovanou úlohu spouštějící wbadmin.exe s odpovídajícími parametry.
9. Ukončete průvodce [Uložit nastavení a spustit zálohování](#) (Save settings and run backup).
10. Prozkoumejte změny na disku B:
  - Objeví se soubor MediaID.bin a složka W10-DOMAIN
  - Přímou v průzkumníku se při pokusu o přístup do složky se zálohou zobrazí dialog nástroje Zálohování.

- Pro prozkoumání obsahu zálohy použijte kontextovou nabídku a [Otevřít](#) (Open).
  - i. Prozkoumejte obsah složky Backup Set YYYY-MM-DD hhmmss
    - 1. Backup Files YYYY-MM-DD hhmmss\Backup files X.zip
    - 2. Catalogs
- 11. Vraťte se do okna nástroje zálohování a prozkoumejte možnost [Spravovat místo](#) (Manage space).
- 12. Pozměňte obsah souboru student1.txt a soubor student2.txt smažte.
- 13. Vraťte se do okna [Zálohování a obnova \(Windows 7\)](#) (Backup and Restore (Windows 7)) a pomocí [Zálohovat](#) (Back up now) vynuťte další zálohu.
- 14. Znova vytvořte soubor student2.txt, tentokrát s jiným obsahem.
- 15. Vynuťte další zálohu.
- 16. Smažte soubor student2.txt.
- 17. Vynuťte další zálohu.

## Lab S07 – Obnova dat ze zálohy (Windows 7)

[ Volitelné ]

### Cíl cvičení

Obnovení dat ze zálohy.

### Potřebné virtuální stroje w10-domain

### Další prerekvizity

Dokončený úkol S06

1. Přihlaste se lokálně na **w10-domain** (uživatelské jméno **w10-domain\student**).
2. Spusťte [Zálohování a obnova \(Windows 7\)](#) (Backup and Restore (Windows 7)).
3. V sekci [Obnovení](#) (Restore) klikněte na Obnovit moje soubory (Restore my files).
  - Všimněte si, že obnovení vlastních dat může provést i obyčejný uživatel.
  - [Obnovit soubory všech uživatelů](#) (Restore all user's files) může provést člen skupiny Backup operators nebo Administrators.
4. Zobrazí se dialog pro obnovu dat.
  - Dialogy obnovy vlastních dat a dat všech uživatelů se vyjma zpřístupněných dat neliší.
5. Prozkoumejte možnosti skrývajících se za tlačítka [Hledat...](#) (Search), [Vyhledat soubory](#) (Browse for files) a [Vyhledat složky](#) (Browse for folders).
  - Všimněte si existence souboru student2.txt, přestože při posledním běhu zálohy byl smazaný. Standardně je k dispozici obnova poslední existující verze.
6. My však budeme chtít obnovit jeho úplně první verzi. V dialogu obnovy dat klikněte na [Zvolit jiné datum](#) (Choose a different date) a vyberte nejstarší záznam odpovídající prvotní záloze. Potvrďte **OK**.
7. Nyní vyhledejte soubor student2.txt a vraťte se zpět do dialogu obnovy dat. Pokračujte [Další](#) (Next).
8. V kroku [Kam chcete uložit obnovené soubory?](#) (Where do you want to restore your files?) zvolte [Do následujícího umístění:](#) (In the following location) a vyberte cílovou složku, např. plochu. Můžete také nechat vytvořit původní hierarchii zaškrtnutím [Obnovit soubory do původních složek](#) (Restore the files to their original subfolders)
9. Obnovu dokončete tlačítkem [Obnovit](#) (Restore) a následně [Dokončit](#) (Finish).
10. Prozkoumejte obnovený soubor a ověřte jeho obsah.



**Lab S08 – Nastavení odesílaných informací o chybách programů** [ Volitelné ]**Cíl cvičení**

Seznámit se s různými úrovněmi nastavení **Hlášení a řešení problémů**.

**Potřebné virtuální stroje**

**w10-domain** (w10-domain)

**Další prerekvizity**

Program **Crash.exe** (obsažen v **utils**).

1. Přihlaste se lokálně na **w10-domain** (uživatelské jméno **w10-domain\student**)
2. Otevřete **Zabezpečení a údržbu** (Security and Maintenance) v **Ovládacích panelech** (Control Panel)
3. V sekci **Údržba** (Maintenance) u **Vyhledat řešení hlášených problémů** (check for solutions to problem reports) ověřte stav **Zapnuto** (On)
4. Spusťte program **Crash.exe**, který simuluje pád programu
5. Ověřte, že systém reaguje na pád programu a vyčkejte, než proběhne analýza problému
6. Otevřete nástroj **Sledování spolehlivosti** (Reliability Monitor)
  - Odkazem **Zobrazit historii spolehlivosti** (View reliability history) z okna zabezpečení a údržby
  - `perfmon /rel`
7. Zvolte **Zobrazit všechna hlášení problémů** (View all problem reports) a ověřte, že byly odeslány informace o pádu programu **Crash.exe**
8. **Zobrazte technické podrobnosti** o odesílaných informacích (View technical details) z kontextové nabídky a podívejte se, které soubory s informacemi jsou vyžadovány pro získání více informací o problému
  - Standardně tyto soubory obsahují informace o DLL knihovnách, jenž aplikace využívala, částečný nebo úplný výpis paměti aplikace a tzv. signaturu problému (informace o problému, operačním systému a platformě)
9. Spusťte Powershell se správcovskými oprávněními.
10. Příkazem **Get-WindowsErrorReporting** ověřte stav hlášení chyb
11. Příkazem **Disable-WindowsErrorReporting** vypněte hlášení chyb a příkazem opět ověřte stav pomocí **Get-WindowsErrorReporting**
12. V okně zabezpečení a údržby v sekci **Údržba** (Maintenance) u **Vyhledat řešení hlášených problémů** (check for solutions to problem reports) ověřte stav **Vypnuto** (Off)
  - Pokud nyní zkusíte **Vyhledat řešení** (Check for Solutions), systém vás upozorní, že je hlášení problémů vypnuté a umožní vám přejít do nastavení (jako bylo v předchozích verzích Windows). Zde však bude vše pouze pro čtení, mimo možnosti vyloučit konkrétní programy z hlášení problému. Takto nastavená výjimka bude po opětovném spuštění hlášení problémů ignorována.
13. Naposled spusťte program **Crash.exe** a ověřte, že nedojde k žádné analýze problému
14. Opět zobrazte historii problémů a ověřte, že informace o pádu programu **Crash.exe** nebyly odeslány