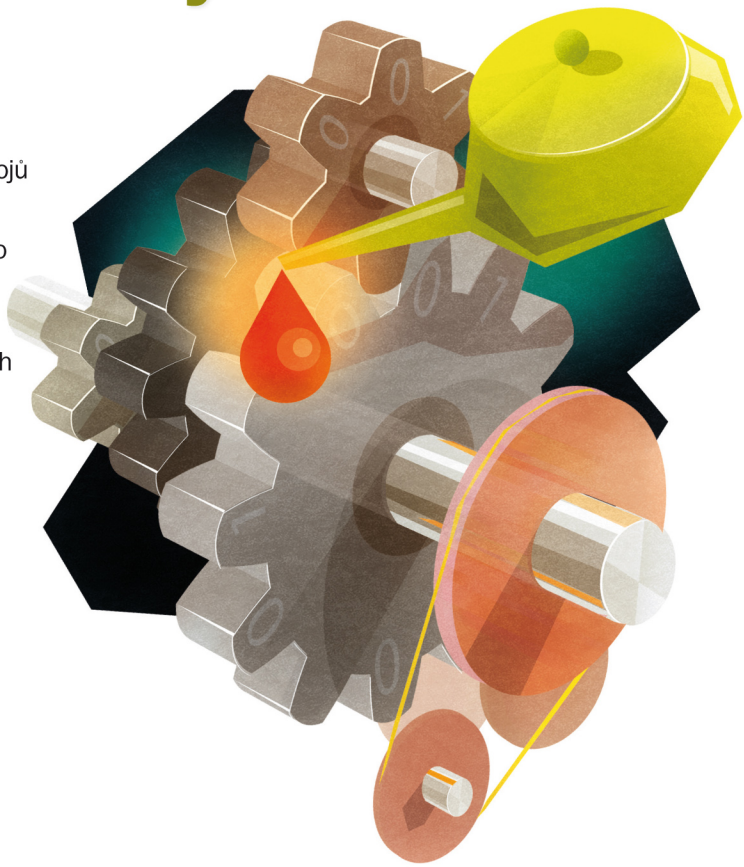
Matúš Selecký

Windows Sysinternals

Vyladťe si systém

- Více než 100 profesionálních nástrojů
- Seznamy parametrů a příklady praktického využití všech utilit
- Dokonalá správa a diagnostika místních i vzdálených systémů
- Výkladový slovník použitých pojmů



computer press

Matúš Selecký

Windows Sysinternals
Vyladťe si systém

Computer Press
Brno
2013

Windows Sysinternals
Vyladťe si systém

Matúš Selecký

Překlad: Martin Herodek
Obálka: Martin Sodomka
Odpovědný redaktor: Libor Pácl
Technický redaktor: Jiří Matoušek

Objednávky knih:
http://knihy.cpress.cz
www.albatrosmedia.cz
eshop@albatrosmedia.cz
bezplatná linka 800 555 513
ISBN 978-80-251-3823-6

Vydalo nakladatelství Computer Press v Brně roku 2013 ve společnosti Albatros Media a. s.
se sídlem Na Pankráci 30, Praha 4. Číslo publikace 16 918.

1. vydání

ALBATROS MEDIA a.s.

Obsah

Úvod

O autorovi

Matúš Selecký působí v oblasti ICT pět let, z toho v oblasti bezpečnosti tři roky. Je absolventem několika kurzů z dílen společností Microsoft, Cisco, EC Council a CompTIA zaměřených na diagnostiku, správu a zabezpečení síťové infrastruktury. Je členem mezinárodní profesní organizace IEEE, konkrétně spolku IEEE Computer Society. V současnosti působí na pozici síťového administrátora v nadnárodní společnosti, která poskytuje služby v oblasti IT outsourcingu. Hlavní náplní jeho práce je zajišťování bezpečnosti počítačových sítí čtvrté největší společnosti na světě.

Předmluva autora

Kniha *Windows Sysinternals – Vyladťe si systém* se snaží zaplnit mezeru na českém a slovenském knižním trhu. Nástroje Sysinternals jsou velmi často využívány v profesní praxi profesionály v oblasti vývoje softwarových řešení, administrátory a systémovými analytiky. Utility najdou široké uplatnění i v domácím prostředí u pokročilých uživatelů, kteří si chtějí sami efektivně diagnostikovat a spravovat svůj operační systém.

Kniha je určena všem, kteří denně pracují s operačním systémem Windows na úrovni diagnostiky a správy, a zájemcům o sadu nástrojů Sysinternals. Prostřednictvím této knihy, která by měla sloužit jako referenční manuál k jednotlivým nástrojům, je možné získat přehled nejen o nástrojích v balíku Sysinternals, jejich nabízené funkcionalitě a možnostech použití, ale i o utilitách integrovaných v operačním systému Windows.

Autor se dále v knize snažil podat i obecnější pohled na správu a diagnostiku operačního systému Windows. Dozvíte se několik tipů, jak zefektivnit práci, jak postupovat při diagnostice nebo zvyšování zabezpečení operačního systému Windows. Součástí knihy je i stručný výkladový slovník, který by měl objasnit některé technické pojmy používané v této oblasti.

O této knize

Hlavním cílem této knihy je nabídnout přehled nástrojů balíku Sysinternals a integrovaných utilit operačního systému Windows. V knize najdete popsaných přes sto nástrojů vhodných ke správě, diagnostice a ladění lokálních a vzdálených operačních systémů Windows. Popisované nástroje pojímají širokou oblast od diagnostiky přístupu disku k údajům přes analýzu

běhu procesů a služeb až po diagnostiku síťové komunikace a zabezpečení prostřednictvím firewallu integrovaného v operačním systému Windows.

Vzhledem k obšírnosti jednotlivých oblastí a nástrojů není možné na takto malém rozsahu, jaký má tato kniha, vyčerpávajícím způsobem prezentovat a popsat všechny možnosti použití, které jednotlivé nástroje nabízejí.

Většina popisovaných nástrojů obsahuje návod, který v některých případech více, v jiných bohužel méně detailněji popisuje jednotlivé nabízené funkce. Každý nástroj nabízí určitou funkcionalitu, která najde uplatnění v různých situacích. Na tomto místě je tedy důležité vědět, že takový nástroj existuje a nabízí danou funkcionalitu.

Kniha je rozdělena do šesti kapitol. Součástí knihy jsou i přílohy, které obsahují krátký výkladový slovník technických pojmů, tabulky odkazů, kódů a klávesových zkratek či rejstřík zařazený na konci knihy.

Každá z kapitol obsahuje na začátku seznam utilit, které budou v rámci této kapitoly prezentovány. Představení samotných nástrojů začíná stručným úvodním štítkem, který obsahuje základní informace o kategorii utility, typu (s grafickým rozhraním, respektive pro příkazový řádek), velikosti, URL odkaz, případně QR kód, který po oskenování vede přímo na stránku utility na portálu *Sysinternals.com*.

Některé nástroje (například Process Explorer, Process Monitor atd.) nabízejí funkce, které by umožňovaly jejich zařazení do více kategorií, respektive nabízejí možnosti v oblastech správy a diagnostiky disku, procesů, síťového připojení atd. Pro ucelený přehled byl zvolen komplexní a jednotný přístup, který prezentuje všechny (anebo aspoň většinu) funkce na jednom místě, namísto toho, aby část funkcí byla prezentována v jedné kapitole a zbytek ve druhé.

Co se v knize dozvíte

V knize *Windows Sysinternals – Vyladťe si systém* se v jednotlivých kapitolách postupně dozvíte velké množství zajímavých a užitečných informací, z nichž zmiňme například:

- Co jsou alternativní datové proudy, jak je lze vytvořit, detekovat a odstranit.
- Způsoby vytváření a detekce tvrdých a měkkých odkazů.
- Jak diagnostikovat problémy se síťovým připojením a konektivitu.
- Jak kontrolovat vzdáleně otevřené soubory.
- Jak sledovat aktuálně otevřené síťové připojení.
- Jak monitorovat procesy a vytížení procesoru v prostředí příkazového řádku.
- Jak zjišťovat detailnější informace o vlastnících domén.
- Jaké jsou možnosti zrychlení spouštění operačního systému Windows.
- Na kterých clusterech pevného disku je uložen konkrétní soubor.
- Způsoby, jak získat výpis paměti (dump) aplikace, která překročí stanovené hodnoty spotřeby systémových prostředků.
- Kde najít význam chybových kódů.

- Jaké typy rootkitů existují.
- Identifikování procesu, který drží konkrétní soubor.
- A mnoho dalších informací a zajímavostí.

Popis nástrojů

Popis jednotlivých nástrojů prezentovaných v této knize je většinou rozdělen do čtyř částí:

- **Použití** – prezentuje formát zápisu parametrů do příkazového řádku (jen u nástrojů určených pro příkazový řádek).
- **Seznam podporovaných parametrů** – podrobnější popis všech podporovaných parametrů (jen u nástrojů určených pro příkazový řádek).
- **Příklady použití** – prezentuje některé základní situace použití daného nástroje i s ukázkou výstupních informací získaných po zadání uvedeného příkazu.
- **Využití** – popisuje možnosti využití, případně cílovou skupinu uživatelů, která by mohla používat tento nástroj v největší míře.

Porozumění zápisu příkazů

V textu jsou u nástrojů pro příkazový řádek prezentovány příkazy pro jejich použití. Zápis je v kompletní podobě, jak ho uvádí návod k použití daného nástroje. V návodu se ale nachází několik formátů a typů závorek. Ke správnému pochopení zápisu je potřeba znát význam jednotlivých forem zápisu.

Znak	Význam
|	Odděluje varianty příkazů a parametrů. Může být použita pravá ,nebo levá varianta. Například parametr **-u**, nebo parametr **-v**. Ve většině případů není možné použít oba parametry zároveň.
`[ ]`	Hranaté závorky ohraničují volby, které spolu souvisejí. V některých případech se jedná jen o jednu volbu, například `[-q]`, v jiných případech může jít o více voleb, které se vztahují k jednomu nastavení `[-l <levels> | -n | -v]`.
`{ }`	Tento typ závorek prezentuje povinné volby, které musejí být přítomny v příkazu. V těchto závorkách bývá uvedena jedna z nutných voleb, například `{yes|no}`, případně název zařízení: `{diskname}`. Z nabízených voleb může být zvoleno jen jedno nastavení.
`< >`	Ostré závorky reprezentují požadavek na zadání například názvu procesu, adresáře apod., například: `[-p <processname>|<pid>]`. Tyto znaky bývají navázány na ostatní parametry. Podobně jako v případě složených závorek není možné zvolit více variant z nabízených možností.

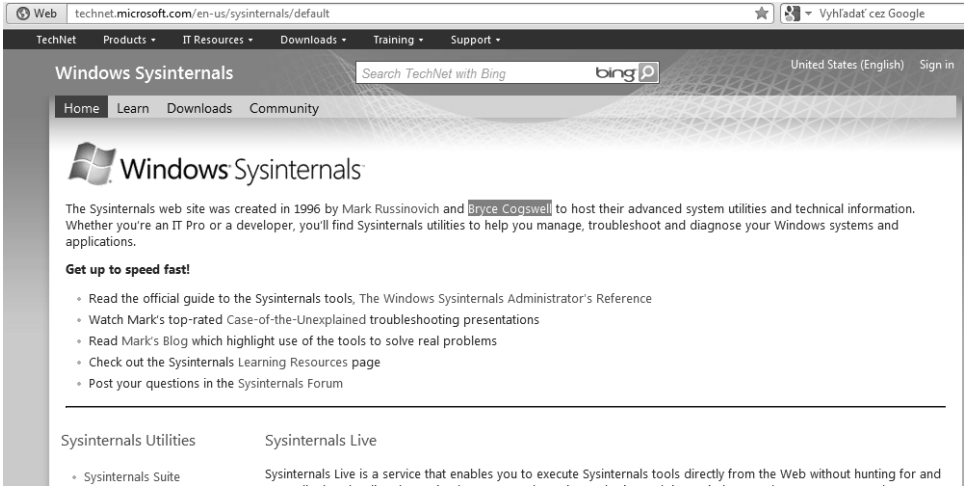
Co je Sysinternals

Sysinternals je balík systémových nástrojů určených ke správě, diagnostice, monitorování a ladění operačních systémů Windows. Nástroje byly vytvořeny Markem Russinovichem ve spolupráci s kolegou Brycem Cogswellem.

V roku 1996 byly vytvořeny webové stránky NT Internals, které spravovala společnost Winternals Software LP. V polovině roku 1996 společnost Microsoft Corporation získala akvizicí

firmu Winternals Software LP a tím získala i projekt NT Internals, který se časem přejmenoval na Windows Sysinternals.

V současnosti jsou stránky Windows Sysinternals umístěny na portálu TechNet, který je vlastnictvím společnosti Microsoft (*http://technet.microsoft.com/en-us/sysinternals/default*).



Obrázek Ú.1 Web Sysinternals

Na stránkách můžete vidět, že se jedná o živý projekt, protože na domovskou stránku jsou přibližně jednou za měsíc přidávány novinky k jednotlivým utilitám, které byly vylepšeny, případně rozšířeny.

FAQ o Sysinternals

Na zmíněném portálu je jednou z kategorií i položka FAQ, což jsou v překladu často kladené otázky (Frequently Asked Questions) vztahující se k balíku a utilitám Sysinternals.

V následující části najdete jejich volný překlad:

Q: Kolik kopií utilit Sysinternals mohu volně stahovat a používat na počítači vlastněném mou společností?
A: Neexistuje žádný limit na počty stažení nebo instalací limitující používání softwaru z balíku Systinternals na vašem počítači nebo zařízeních, které podporujete.

Q: Mohu distribuovat nástroje balíku Sysinternals jako součást svého softwaru, na svých webových stránkách nebo blogu, případně časopisu?
A: Ne, autoři utilit neposkytují distribuční licence ani v případech, kdy jsou výsledné produkty distribuovány zdarma. Doporučujeme zájemcům, aby si utility Sysinternals stahovali z našeho download centra, kde si mohou být jisti, že získají poslední verzi utility.
Dodatek autora: Navíc si na originálních stránkách můžete být jisti, že nestahujete škodlivý software, který se může tvářit jako požadovaná utilita.

Q: Mohu měnit licencování nebo znovu používat a upravovat zdrojový kód utilit Sysinternals?

A: Ne, v současnosti už naše společnost nenabízí možnost stahování zdrojových kódů utilit Sysinternals pro možnost jejich úpravy nebo relicencování.

Q: Budou utility Sysinternals i nadále dostupné zadarmo?

A: Ano, společnost Microsoft neplánuje odstranit nebo zpoplatnit tyto nástroje.

Q: Je k nástrojům Sysinternals dostupná i technická podpora?

A: Ne, všechny nástroje jsou nabízeny tak, jak jsou, bez oficiální podpory ze strany Microsoftu. Autoři utilit udržují stránku a provozují komunitu, která poskytuje podporu prostřednictvím diskuzního fóra, které je dostupné na adrese *http://forum.sysinternals.com/*.

V následujícím textu je uvedeno několik (autorem této knihy vytvořených) doplňujících otázek a odpovědí (tyto otázky nejsou součástí oficiálního FAQ na stránkách Sysinternals).

Q: Na jakých operačních systémech je možné používat utility Sysinternals?

A: Podporované operační systémy jsou různé a závisejí na konkrétní utilitě. Některé utility je možné spustit jen na serverových systémech.

Q: Jak jsou nástroje Sysinternals licencovány?

A: Při spuštění většiny nástrojů z balíku Sysinternals je pro možnost dalšího používání potřeba potvrdit, respektive vyjádřit souhlas s koncovými licenčními podmínkami. Tyto podmínky se označují akronymem EULA – End User License Agreements. Laicky řečeno tyto licenční podmínky určují, co uživatel může a co nemůže.

V současnosti na stránkách Sysinternals není dostupný překlad těchto licenčních podmínek do jiných jazyků. Ke každé utilitě je přibalen textový soubor, který obsahuje originální znění těchto licenčních podmínek v anglickém jazyce (některé klauzule obsahují překlad do kanadské francouzštiny).

Volný překlad EULA

V následujícím textu je prezentován volný překlad nejdůležitějších částí originální verze EULA.

Upozornění: Následující překlad je volným překladem autora. Tyto volně přeložené smluvní podmínky nejsou oficiálně uznány společností Microsoft a nemají žádnou právní sílu ani záruku. Účelem tohoto překladu je umožnit čtenářům vytvořit si základní představu o podmínkách EULA v anglické verzi. Pro ty čtenáře, jejichž angličtina je na pokročilé úrovni, autor doporučuje studovat původní anglickou verzi.

SYSINTERNALS SOFTWARE – LICENČNÍ PODMÍNKY

Tyto licenční podmínky jsou dohodou mezi Sysinternals (plně vlastněným společností Microsoft Corporation) a vámi. Prosíme o pozorné čtení. Tyto podmínky jsou aplikovány na software, který byl stažen z portálu *Sysinternals.com*.

Tyto podmínky jsou aplikované na jakýkoliv Sysinternals:

- update,
- doplněk,
- internetovou službu a
- službu podpory.

Při souhlasu s těmito licenčními podmínkami máte práva uvedená níže.

POUŽÍVÁNÍM SOFTWARU SOUHLASÍTE S TĚMITO PODMÍNKAMI. POKUD S TĚMITO PODMÍNKAMI NESOUHLASÍTE, NEPOUŽÍVEJTE TENTO SOFTWARE.

1. INSTALAČNÍ A UŽIVATELSKÁ PRÁVA. Můžete nainstalovat a používat libovolný počet kopií tohoto softwaru na svých zařízeních.

2. ÚČEL LICENCE. Software je licencovaný a neprodejný. Tyto licenční podmínky vám dávají jen některá oprávnění používat software. Sysinternals si vyhrazuje všechna ostatní práva. Pokud vám aplikovatelné zákony nedávají větší práva než tyto podmínky, můžete software používat jen v mezích určených těmito podmínkami. V rámci tohoto musíte souhlasit se všemi technickými limity, které vám umožňují používat software daným způsobem.

Na základě těchto licenčních podmínek nemůžete:

- obcházet jakákoliv technická omezení v binárních verzích používaného softwaru;
- podrobovat aplikace procesům reverzního inženýrství, dekompilovat nebo disasemblovat binární verzi softwaru;
- publikovat software umožňující ostatním kopírovat dotknutý software;
- pronajímat nebo půjčovat software;
- přenášet software nebo tyto podmínky do softwaru třetích stran; anebo
- používat software pro komerční hostingové služby.

3. DOKUMENTACE. Jakákoliv osoba, která má platný přístup k vašemu počítači nebo interní síti, může kopírovat a používat dokumentaci pro vaše interní, příslušné účely.

5. SLUŽBY PODPORY. Vzhledem k tomu, že software je poskytován „tak, jak je", není k němu poskytována služba technické podpory.

7. APLIKOVATELNÉ PRÁVO

a) Spojené státy. Pokud jste získali software ve Spojených státech, na výklad se vztahuje právo státu Washington a jeho záruky a nároky spojené s porušením, bez ohledu na konflikt právních principů.

b) Mimo Spojené státy. Pokud jste získali software v jakékoliv jiné zemi, na výklad se aplikuje právo dané země.

8. PRÁVNÍ EFEKT

Tato smlouva opisuje určitá zákonná práva. Můžete mít i další práva podle právních předpisů své země. Můžete mít též další práva ve vztahu ke straně, od které jste software získali. Tato

smlouva nemění vaše práva v rámci právního pořádku vaší země, pokud právní pořádek vaší země nepovoluje, aby tak tato smlouva učinila.

9. ZÁRUKY. Software je licencován v takovém stavu, jak je distribuován. Používáním na sebe přebíráte riziko, které plyne z jeho používání. Sysinternals neposkytuje žádné garance, záruky nebo jiné podmínky. Ve vaší zemi mohou existovat další záruky, které plynou ze spotřebitelského práva, které tyto licenční podmínky nemohou změnit. O rozšířeném rozsahu práv ve vašem lokálním právu Sysinternals vylučuje zahrnuté záruky prodejnosti a vhodnosti pro určitý účel.

10. OMEZENÍ A VYLOUČENÍ NÁPRAVY A NÁHRADY ŠKODY. Od Sysinternal a jeho dodavatelů můžete získat náhradu přímé škody do výšky 5,00 (slovem pět) amerických dolarů. Nemůžete získat náhradu žádné jiné škody ani úhradu následků, ušlého zisku ani jiných nepřímých a náhodných škod.

Omezení se vztahují na:

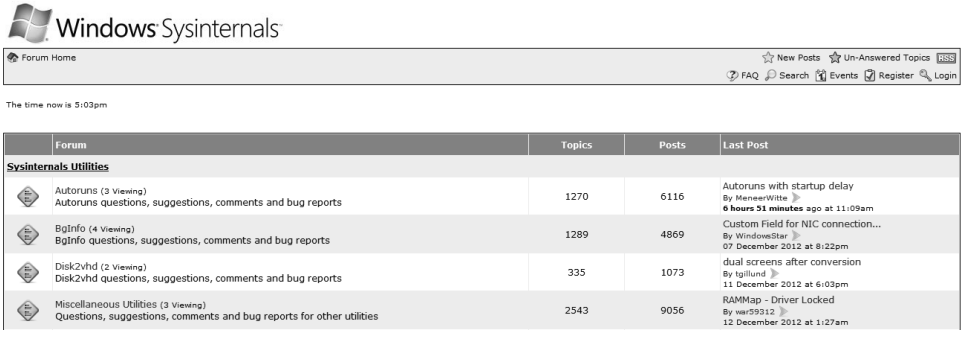
- cokoliv, co se vztahuje k softwaru, službám anebo obsahu (včetně kódu) na internetových stránkách třetích stran nebo aplikace třetích stran, a
- stížnosti za porušení smlouvy, porušení záruky, garance nebo podmínky, objektivní zodpovědnost, nedbalost anebo jiné občanskoprávní delikty v rozsahu povoleném rozhodným právem.

Omezení se aplikují i na situaci, kdy Sysinternals ví, nebo by měl vědět o možnosti vzniku škody. Výše uvedené podmínky anebo omezení nemusejí být aplikovatelné, protože vaše země nemusí povolovat výjimky a omezení náhodných, následných anebo jiných škod.

Sysinternals Forum

Na webových stránkách projektu je v sekci **Forum dostupné diskuzní fórum** (*http://forum.sysinternals.com/*).

Prostřednictvím tohoto fóra mohou uživatelé oznamovat nalezené chyby, diskutovat o používání, problémech a všem, co souvisí s nástroji Sysinternals. Samotní autoři občas procházejí příspěvky a opravují reportované chyby, případně doplňují požadované vlastnosti a funkce.



Obrázek Ú.2 Fórum Sysinternals

V diskuzním fóru lze nalézt některé užitečné informace, například o nefunkčnosti utility na některých operačních systémech, chybný popis v nápovědě nástroje a tak podobně.

Balík Sysinternals

Nástroje balíku Sysinternals je možné stáhnout jednotlivě, případně i v jednom archívu, který obsahuje kompletní sadu nástrojů. Balík, který má přibližně 13 MB, je dostupný na odkazu *http://technet.microsoft.com/cs-cz/bb842062*.

Tento balík bývá průběžně aktualizován, aby obsahoval poslední verze opravených a vylepšených utilit. Po stažení archívu ZIP jej stačí rozbalit na požadované umístění a začít nástroje používat.

Tip: Téměř každá utilita před svým spuštěním zobrazuje licenční podmínky, tzv. EULA, s nimiž je potřeba souhlasit, aby bylo možné požadovaný nástroj dále používat.

V případě, že se daná utilita používá například při automatizaci, případně je v systémové správě implementována do skriptů, není žádoucí, aby se zobrazovaly dialogy, které budou blokovat další běh skriptu.

Akceptování licenčních podmínek EULA je možné v prostředí příkazového řádku zabezpečit použitím parametru `-accepteula`.

Pro jednodušší používání je možné celý balík v archívu ZIP rozbalit do umístění:

```
%Systémový_disk%\Windows\System32\
```

Z této cesty bude následně možné spouštět všechny utility z příkazového řádku jen prostřednictvím zadání názvu utility. Alternativní možností je přidání vlastního adresáře do systémové proměnné `Path`. Aktuálně nastavené položky v seznamu proměnných systémového prostředí je možné ověřit zadáním následujícího příkazu do příkazového řádku:

```
echo %path%
```

```
C:\Program Files (x86)\PC Connectivity Solution\;
C:\Program Files\Common Files\Microsoft Shared\Windows Live;
C:\Program Files (x86)\Common Files\Microsoft Shared\Windows Live;
C:\Windows\system32;
C:\Windows;
C:\Windows\System32\Wbem;
```

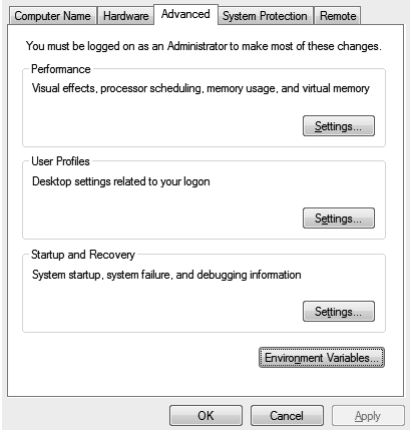
Tip: Seznam jednotlivých proměnných prostředí (systémových i lokálních) je uveden na konci knihy v přílohách.

Systémové proměnné

Systémové proměnné se využívají například v oblasti skriptování, v prostředí příkazového řádku, případně u některých aplikací, které využívají například klientské databázové moduly, případně jiné moduly pro správnou funkčnost aplikací.

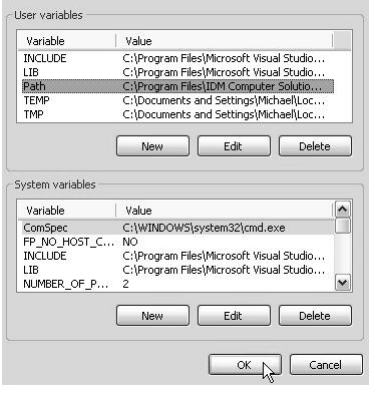
Proměnnou lze vložit tímto postupem:

1. Vyvolejte dialog rychlého spuštění, do kterého zadejte a potvrďte příkaz:
   `control.exe sysdm.cpl,System,3`
2. Po potvrzení příkazu se zobrazí okno s nastaveními (viz obrázek 1.3).



Obrázek Ú.3 Systémová nastavení

3. V dolní části okna je tlačítko **Proměnné prostředí (Environment Variables)**.
4. Po klepnutí na toto tlačítko se zobrazí další okno (obrázek 1.4), které obsahuje možnosti pro konfiguraci systémových a uživatelských proměnných.



Obrázek Ú.4 Konfigurace proměnných

5. Systémové proměnné se nastavují obecně pro celý operační systém (a všechny uživatele), přičemž uživatelské proměnné se nastavují jen pro konkrétního uživatele (nemají dopad na ostatní uživatele).
6. V tomto okně je potřeba zvolit volbu přidání nové proměnné, kde je potřeba nadefinovat název a cestu ke spustitelnému souboru, skriptu, knihovně a tak podobně.
7. Do cesty je tedy potřeba vložit úplnou absolutní cestu, například ve formátu *F:\tools\Junction*.
8. Po zadání je potřeba všechna nastavení a okna zavřít potvrzovacím tlačítkem **OK.**

Sysinternals Live

Sysinternals Live je nová služba, která na webových stránkách projektu zpřístupňuje všechny utility balíku Sysinternals ve spustitelné formě. Není tedy nutné stahovat archívy ZIP a následně je rozbalovat, abyste mohli utility spouštět.

Tato nová služba je dostupná na webových stránkách *http://live.sysinternals.com/*.

V případě, že uživatel zná přesný název utility, kterou si chce spustit, může za uvedenou adresu napsat název utility a potvrdit adresu v prohlížeči. Obecný formát adresy je:

http://live.sysinternals.com/<nazev_utility>

Například:

http://live.sysinternals.com/AccessEnum.exe

Další informace o Sysinternals

Na webových stránkách Sysinternals lze v sekci **Sysinternals Learning Resources** najít odkazy na další zdroje obsahující informace o některých nástrojích Sysinternals, možnostech a postupech jejich použití (*http://technet.microsoft.com/en-us/sysinternals/bb469930.aspx*).

V uvedené sekci jsou dostupné odkazy na:

- články,
- videa,
- webcasty,
- blogy a diskuze o jednotlivých nástrojích balíku Sysinternals.

Na stránkách portálu Microsoft je možné najít i placený e-learningový kurz zaměřený na pokročilou diagnostiku operačních systémů Windows s nástroji Sysinternals (Course 5371: Advanced Troubleshooting with Windows Sysinternals Tools).

Využití nástrojů Sysinternals

Nástroje Sysinternals jsou vhodné k diagnostice operačního systému při různých problémech. Proces diagnostiky, identifikace problému a určení možného řešení se v angličtině nazývá troubleshooting. V této části bude představen základní obecný postup troubleshootingu, který by měl pomoci uživatelům (administrátorům, analytikům a jiným) při diagnostice a řešení problémů v operačním systému Windows.

Dalším doporučením, které bude v následujícím textu představeno, je takzvaný hardening. Jedná se o proces vypínání, případně odstraňování provozovaného systému. Tento proces postupného odstraňování nepoužívaných služeb, komponent a funkcionalit zvyšuje celkové zabezpečení systému tím, že odstraňuje body, které by mohly být cílem potenciálního útoku a v případě napadnutí a zneužití potenciální slabiny se tak stát místem průniku do systému. Hardening je možné realizovat na všechny prvky přítomné ve firemní infrastruktuře (servery, směrovače atd.).

U aplikací procesů troubleshootingu a hardeningu najdou uplatnění nástroje balíku Sysinternals a nástroje systému Windows prezentované v následujících kapitolách této knihy.

Troubleshooting

Proces diagnostiky (troubleshootingu) lze ve všeobecnosti popsat následujícími kroky:

- **Definování problému** – proces identifikování problému může být problematický, protože oznamovací reporty zadávají i uživatelé s netechnickým zázemím. Proto je potřeba, aby technik na základě získaného reportu nejprve ověřil problém a následně na základě znalostí vytvořil kvalifikovanou definici problému.
- **Získání informací** – na identifikování problému navazuje proces sbírání potřebných informací. Samotný proces získávání informací je potřeba systematicky naplánovat, určit cílové prvky, o kterých se budou informace sbírat (ovladače, software, hardware a tak podobně), a identifikovat nástroje, které umožní potřebné informace získat. V případě, že není možné získat potřebné informace vlastními silami a oprávněními, je potřeba eskalovat požadavek na potřebné informace na patřičná místa (jiné oddělení, zodpovědnou osobu).
- **Analýza informací a vyloučení příčin vzniku problému** – po získání všech potřebných informací je nezbytná jejich správná interpretace, s jejíž pomocí lze vyloučit příčiny vzniku problému.
- **Formulování hypotézy vzniku problému** – po identifikování, co způsobilo vznik problému, je potřeba zformulovat hypotézu, která předpokládá akci, jež vyřeší problém.
- **Testování hypotézy** – na základě zformulované hypotézy je potřeba otestovat její validnost. Otestováním hypotézy se ověří, že předpokládaná akce skutečně napraví vzniklý problém.
- **Vyřešení problému** – poslední fáze celého procesu troubleshootingu představuje implementaci řešení, které zabezpečí trvalé, případně dočasné řešení. Ideální případ představuje

situaci, kdy je implementované řešení trvalé, nevytváří další problémy a plně odpovídá firemním a bezpečnostním politikám (nevytváří bezpečnostní slabiny v systému).

Hardening

Následující body uvádějí hlavní oblasti, na které je potřeba myslet, a operace, které je potřeba vykonat, ke zvýšení zabezpečení systému. Proces hardeningu obnáší:

- Instalaci posledních záplat (patchů) používaného operačního systému. Záplaty obvykle obsahují opravy bezpečnostních chyb a zranitelností systémových služeb a procesů.
- Instalaci posledních záplat (patchů) používaných aplikací.
- Používání silného hesla, které by bylo odolné vůči slovníkovým útokům.
- Implementaci bezpečnostních doporučení výrobců používaného softwaru a hardwaru.
- Používání antivirového/spyware/adware softwaru s implementovanou poslední aktualizací databáze. Uvedené nástroje chrání stanice a servery (e-mail, FTP) proti škodlivému kódu.
- Zablokování nepoužívaných služeb.
- Zablokování nebo vymazání účtu hosta a jiných uživatelských účtů v operačním systému, které se nepoužívají.
- Přidělování přístupových práv k prostředkům jen těm uživatelům, kteří to nezbytně potřebují ke své práci.
- Implementaci bezpečnostní politiky. Prostřednictvím bezpečnostních politik je možné blokovat, omezovat a kontrolovat uživatelský přístup k systémovým službám a prostředkům.
- Používání varovných bannerů. Tyto bannery jsou důležité pro případné právní vyvozování důsledků v případě řešení sporů soudní cestou.
- Implementování auditu a logovací politiky pro zaznamenávání uživatelské aktivity.
- Fyzické zabezpečení kritických prvků síťové infrastruktury.
- Vytvoření zálohovacího plánu, kterým je potřeba chránit citlivá data pro případ ztráty.
- Otestování vytvořeného hardeningu.
- Zdokumentování celého procesu hardeningu.

KAPITOLA 1

Souborové a diskové nástroje

V této kapitole:
- Contig, Disk Usage (DU)
- DiskView, NTFSInfo
- FindLinks, Junction
- Streams, Sync
- Disk2vhd, PageDefrag
- MoveFile a PendMoves
- DiskMon, DiskExt
- EFSDump, VolumeID
- LDMDump, CacheSet
- Chkdsk, BCDboot
- BCDedit

V první kapitole budou prezentovány nástroje zaměřené na diagnostiku a správu diskového prostoru a souborů uložených na disku. Systémoví administrátoři často potřebují v rámci správy diskového prostoru sledovat intenzitu využívání diskového prostoru, jeho fragmentaci, přístup k jednotlivým souborům, identifikovat chybné sektory, a předcházet tak znehodnocení ukládaných dat.

Ze zajímavostí, které budou v této kapitole probírány, lze zmínit například problematiku alternativních datových proudů či způsoby odstraňování škodlivého softwaru z disku. V závěru kapitoly najdete několik stran věnovaných možnostem a způsobům obnovení chybných sektorů, případně oblasti bootovacího sektoru.

Tato kapitola obsahuje popis následujících nástrojů:

SYSINTERNALS:

- Streams
- Contig
- Disk2vhd
- DiskView
- FindLinks
- Junction
- PendMoves
- CacheSet
- DiskExt
- DiskMon
- EFSDump
- LDMDump

- MoveFile
- NTFSInfo
- PageDefrag
- VolumeID
- Sync
- Disk Usage

WINDOWS UTILITY:

- Chkdsk
- BCDboot
- BCDedit

Contig

Název:	Contig	
Velikost:	103 kB	
Kategorie:	File and disk tools	
Typ utility:	CMD	
URL:	*http://technet.microsoft.com/en-us/sysinternals/bb897428*	

Popis

Contig je nástroj umožňující defragmentování specifického souboru nebo souborů, které jsou často používány. Fragmentace způsobuje, že soubory nejsou na disku zapsány za sebou, ale každý fragment se nachází na jiném místě disku. Následně musí čtecí hlava disku při čtení přeskakovat mezi různými umístěními fragmentů souborů, což zpomaluje celkový proces předávání a zpracování informací. Fragmentace vzniká standardní prací s diskem, kdy se často vytvářejí, kopírují a odstraňují data, což vytváří různě velké mezery v prostoru mezi jednotlivými informacemi zapsanými na disku, do kterých jsou zapisovány různě velké nové soubory.

Operace defragmentace umožňuje optimalizaci spouštění souborů, ke kterým se často přistupuje.

Použití

```
contig [-a] [-s] [-q] [-v] [existing file]
contig [-f] [-q] [-v] [drive:]
contig [-v] [-l] -n [new file] [new file length]
```

Seznam podporovaných parametrů

`-a`	Analýza fragmentace.
`-f`	Analýza volného místa.

`-l`	Nastavení validní délky dat pro rychlé vytvoření souboru (vyžaduje administrátorská práva).
`-q`	Tichý režim.
`-s`	Rekurzivní průchod podadresáři.
`-v`	Podrobný režim – rozšířený výpis výstupních informací.

Nástrojem Contig lze také defragmentovat následující NTFS metadata:

`$Mft`	Záznamy Master File Table.
`$LogFile`	Soubory transakčních protokolů.
`$Volume`	Informace o diskové jednotce (název, identifikátor, verze).
`$AttrDef`	Definice atributů.
`$Bitmap`	Údržba statusu všech nealokovaných clusterů.
`$Boot`	Udržování záznamů lokace Master Boot Record.
`$BadClus`	Záznam o označených chybných clusterech.
`$Secure`	Informace o zabezpečení a kontrole přístupu.
`$UpCase`	Tabulka velkých písmen používaných pro sběr.
`$Extend`	Adresář obsahující další podadresáře (**`$ObjId`**, **`$Quota`**, **`$Reparse`**, **`$UsnJrnl`**) s detailnějšími informacemi.
`$Extend\$ObjId`	Údržba informací o unikátním ID pro každý soubor.
`$Extend\$Quota`	Informace o diskové kvótě.
`$Extend\$Reparse`	Informace o bodu propojení. Tato oblast udržuje informace o namapovaných potomcích a relativních cestách k těmto potomkům. Tento typ informací se využívá například u Microsoft Remote Storage Server (RSS), kdy administrátor může ukládat na vzdálené úložiště málo používané soubory.
`$Extend\$UsnJrnl USN`	Žurnál. Funkce se aplikuje při zapnutí funkce chránění souborů nebo adresářů, které jsou sdílené, případně při zapnutí ochrany na serverových úložištích.
`$Extend\$RmMetadata`	Transakční data. Tato data jsou používána k zachování integrity dat na disku se souborovým systémem NTFS.

Příklady použití

1. Spuštění analýzy volného místa

```
contig -f

Summary:
  Free cluster space          : 78016135168 bytes
  Free space fragments        : 106 frags
  Largest free space block    : 68969963520 bytes
```

2. Analýza diskové jednotky F:\

```
contig F:\*

Summary:
  Number of files processed   : 19
  Number of files defragmented: 0
  All files were either already defragmented or unable to be defragmented.
```

3. Skenování záznamů v Master File Table

```
contig -v -s $mft

-----------------------
Processing F:\$Mft:
Scanning file...
F:\$Mft is already in 1 fragment.
-----------------------
Processing F:\$Mft::$BITMAP:
Scanning file...
Scanning disk...
File is 2 physical clusters in length.
File is in 2 fragments.

Found a free disk block at 2608323 of length 3 for entire file.
Moving 2 clusters at file offset cluster 0 to disk cluster 2608323
File size: 4104 bytes
Fragments before: 2
Fragments after : 1
-----------------------
Summary:
  Number of files processed   : 2
  Number of files defragmented: 1
  Average fragmentation before: 1.5 frags/file
  Average fragmentation after : 1 frags/file
```

Využití

Nástroj najde uplatnění u systémových administrátorů a analytiků, kteří řeší problémy se zpomalením počítače způsobeným diskovou jednotkou. Po identifikování zdrojů fragmentace pomocí nástroje Contig je možné snáze určit postup nápravy. Například pokud je rozsáhlý software (případně v domácím prostředí to může být i hra) fragmentovaný po celém disku, jeho odinstalování a instalace na jiný oddíl mohou pomoci ke zvýšení výkonu celé aplikace.

Disk Usage (DU)

Název:	Disk Usage	
Velikost:	115 kB	
Kategorie:	File and disk tools	
Typ utility:	CMD	
URL:	*http://technet.microsoft.com/en-us/sysinternals/bb896651*	

Popis

Nástroj Disk Usage, zkráceně DU, nabízí možnost analyzování využití diskového prostoru. Výstup nástroje popisuje využití diskového prostoru definovaných souborů nebo adresářů.

Použití

```
du [-c] [-l <levels> | -n | -v] [-u] [-q] <directory>
```

Seznam podporovaných parametrů

`-c`	Výpis výstupu ve formátu CSV.
`-l`	Určení hloubky podadresářů. Předvolená hodnota je nastavena na všechny úrovně.
`-n`	Neaplikovat rekurzivní procházení.
`-q`	Tichý režim (nezobrazení banneru).
`-u`	Počítání každé instance pevného odkazu na soubor.
`-v`	Zobrazení velikosti (v kilobajtech).

Příklad použití

Zobrazení detailů o velikosti aktuálního adresáře:

```
du .\

Files:        97
Directories:  0
Size:         29 391 238 bytes
Size on disk: 29 581 312 bytes
```

Využití

Informace, které lze získat na výstupu z utility Disk Usage, jsou totožné s informacemi dostupnými na kartě vlastností adresáře nebo souboru. Kartu vlastností lze vyvolat klepnutím pravým tlačítkem myši na soubor a volbou položky **Vlastnosti (Properties)**, případně označením souboru nebo adresáře a následným stisknutím klávesové zkratky Alt+Enter. Nástroj DU najde

uplatnění například v oblasti automatizované správy, kde je potřeba tyto informace získávat v textové podobě.

DiskView

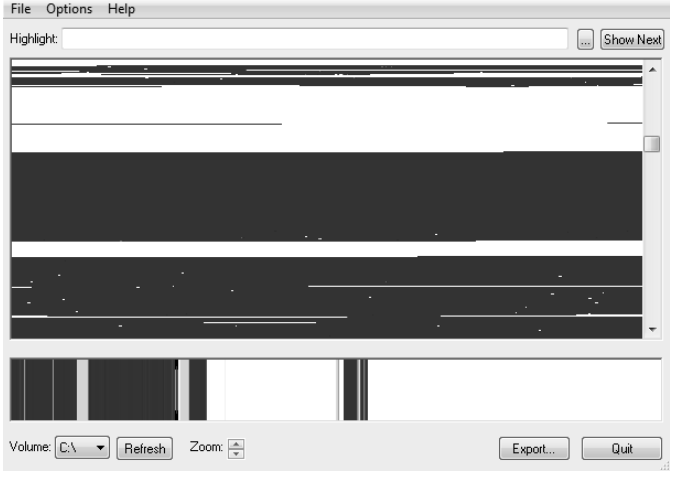
Název:	DiskView	
Velikost:	288 kB	
Kategorie:	File and disk tools	
Typ utility:	GUI	
URL:	*http://technet.microsoft.com/sk-sk/sysinternals/bb896650*	

Popis

Hlavní funkcí nástroje je výpis základních informací o obsazení disku. Nástroj dokáže identifikovat soubory, které obsazují zvolené clustery na testované diskové jednotce.

Použití

Používání nástroje je poměrně intuitivní. Po jeho spuštění je potřeba vybrat diskovou jednotku a spustit proces skenovacího procesu. Následně se v horní části barevně zobrazí rozložení souborů na disku.



Obrázek 1.1 DiskView

Po klepnutí do okna se v horní části v adresním řádku zobrazí cesta k souboru, který je v označené lokaci uložen. Volba **Show Next** umožňuje stopovat všechny fragmenty daného souboru.

Nástroj DiskView umožňuje vypisovat i základní statistiky o počtu souborů, fragmentů a obsazenosti disku. Statistiky jsou dostupné po klepnutí na nabídku **File**.

```
Files:        261112
Fragments:    200359
% Free Space: 67.62 %
```

Využití

Zpomalení počítače může být způsobeno i častou instalací a odinstalací softwaru, která po určité době způsobí nepravidelnosti v rozmístění volného místa na disku, čímž dojde při dalším ukládání dat k jejich fragmentaci. V důsledku fragmentace musí hlava disku vyhledávat potřebná data na různých místech, což prodlužuje čas předání výsledku.

Při těchto problémech je vhodné provést defragmentaci disku. Nástroj DiskView umožňuje sledovat, která data v které části disku jsou defragmentována. Utilita se uplatní u systémových administrátorů ve firmách či u forenzních analytiků, kteří vyhledávají fragmentované soubory na disku (například forenzní analýza při vyšetřování trestné činnosti), ale také u pokročilých uživatelů na domácích počítačích.

NTFSInfo

Název:	NTFSInfo	
Velikost:	28 kB	
Kategorie:	File and disk tools	
Typ utility:	CMD	
URL:	*http://technet.microsoft.com/en-en/sysinternals/bb897424*	

Popis

NTFSInfo je nástroj zobrazující podrobné informace o diskových jednotkách používajících souborový systém NTFS. Tento souborový systém vyvinula společnost Microsoft a v současnosti je nejběžnějším souborovým systémem na domácích stanicích, na kterých běží operační systém Windows.

Příklad použití

Nástroj nepodporuje žádné doplňující parametry. K jeho použití je potřeba jen definovat testovanou diskovou jednotku. Výstup informuje o celkovém počtu clusterů, sektorů a jejich obsazenosti.

```
ntfsinfo C:

Volume Size
```

```
-----------
Volume size             : 145919 MB
Total sectors           : 298844159
Total clusters          : 37355519
Free clusters           : 24758808
Free space              : 96714 MB (66% of drive)

Allocation Size
---------------
Bytes per sector        : 512
Bytes per cluster       : 4096
Bytes per MFT record    : 1024
Clusters per MFT record: 0

MFT Information
---------------
MFT size                : 237 MB (0% of drive)
MFT start cluster       : 786432
MFT zone clusters       : 11313600 - 11332480
MFT zone size           : 73 MB (0% of drive)
MFT mirror start        : 2

Meta-Data files
---------------
```

Využití

Nástroj se uplatní u všech uživatelů, kteří potřebují získat informace o aktuální struktuře diskové jednotky připojené ke sledované stanici. Mezi vypisovanými informacemi lze najít například údaje o velikosti a počtu clusterů, sektorů, případně detaily o MFT (Master File Table).

FindLinks

Název:	FindLinks	
Velikost:	57 kB	
Kategorie:	File and disk tools	
Typ utility:	CMD	
URL:	*http://technet.microsoft.com/sk-sk/sysinternals/hh290814*	

Popis

Souborový systém NTFS umožňuje vytváření několika druhů odkazů (tvrdé, měkké a propojení). Nástroj FindLinks umožňuje vyhledávat a vypisovat takzvané tvrdé odkazy k souborům.

Funkce tvrdých odkazů umožňuje odkazovat více cestami k jednomu souboru. Funkce je podporována jen pro soubory, ne pro adresáře. Tvrdé odkazy je možné používat jen v rámci jedné stanice, jedné diskové jednotky a jednoho souborového systému.

Alternativou k tvrdým odkazům jsou takzvané měkké odkazy, které je možné používat pro adresáře, síťové stanice nebo jiné diskové jednotky v rámci lokální stanice.

Postup vytvoření tvrdého odkazu:

```
echo Pokusny text. > test.txt
mklink hard_link.txt test.txt /H

Hardlink created for hard_link.txt <<===>> test.txt
```

Po vytvoření tohoto propojení tvrdým odkazem oba soubory existují samostatně. Ve skutečnosti je to ale jeden soubor. V případě editace jednoho souboru a uložení změn se tyto změny projeví i ve druhém z propojených souborů. Po odstranění jednoho ze souborů zůstává druhý zachován beze změny.

Použití

```
findlinks <file>
```

Při použití utility je potřeba při spouštění vložit jako parametr cestu k souboru, který má být otestován na přítomnost tvrdých odkazů.

Příklad použití

```
findlinks .\test.txt


D:\Tools\FindLinks\test.txt
      Index:  0x000005FD
      Links:  1
Linking file:
D:\Tools\hard.txt
```

Z výpisu je možné vidět, že k testovanému souboru existuje jedno propojení. Ve výpisu je uvedena i adresa druhého propojeného souboru.

Výhodou funkce tvrdých odkazů je možnost vytvořit proceduru zálohování souborů, která se realizuje okamžitě po uložení editovaného souboru. Tento způsob zálohování je použitelný jen v případech ochrany před poškozením souboru, ne při nesprávné editaci. Pokud je do souboru zavedena nesprávná informace, bude uložena i v druhém souboru.

Funkce měkkých odkazů je vhodná například pro urychlení přístupu k hluboko vnořeným souborům a adresářům bez nutnosti procházení celou adresářovou strukturou.

Předvolené nastavení symbolických odkazů lze ověřit pomocí příkazu:

```
fsutil behavior query SymLinkEvaluation
```

```
Local to local symbolic links are enabled.
Local to remote symbolic links are enabled.
Remote to local symbolic links are disabled.
Remote to remote symbolic links are disabled.
```

Nastavení symbolických odkazů můžete měnit pomocí příkazu:

```
fsutil behavior set SymLinkEvaluation
```

Použití utility Fsutil

```
fsutil behavior set <option> <value>
```

Seznam a hodnoty podporovaných parametrů

Parametr	Hodnoty
`AllowExtChar`	`1 | 0`
`BugcheckOnCorrupt`	`1 | 0`
`Disable8dot3`	`[0 through 3] | [<Volume Path> 1 | 0]`
`DisableCompression`	`1 | 0`
`DisableEncryption`	`1 | 0`
`DisableLastAccess`	`1 | 0`
`EncryptPagingFile`	`1 | 0`
`MftZone`	`Od 1 do 4`
`MemoryUsage`	`Od 1 do 2`
`QuotaNotify`	Od `1` do `4294967295` sekund.
`SymlinkEvaluation`	`[L2L:{0|1}] | [L2R:{0|1}] | [R2R:{0|1}] | [R2L:{0|1}]` `L` – lokální symbolické odkazy. `R` – vzdálené (Remote) symbolické odkazy.
`DisableDeleteNotify`	`1 | 0`

Některé z výše uvedených parametrů ke své aplikaci vyžadují restart operačního systému.

Využití

Nástroj najde uplatnění u systémových analytiků, kteří podrobně zkoumají propojení souborů v operačním systému. Další skupinou uživatelů mohou být systémoví administrátoři, případně pokročilejší uživatelé, kteří chtějí vytvořit automatizovanou proceduru zálohování konkrétních souborů nebo zkrátit přístup k hluboko vnořeným adresářům a souborům.

Junction

Název:	Junction	
Velikost:	78 kB	
Kategorie:	File and disk tools	
Typ utility:	CMD	
URL:	*http://technet.microsoft.com/sk-sk/sysinternals/bb896768*	

Popis

Operační systémy Windows verze 2000 a vyšší podporují symbolické odkazy adresářů. Tato funkce symbolických odkazů je známa jako NTFS Junction.

Symbolické adresy jsou, pokud adresář *D:\SYMLINK* odkazuje na *C:\WINNT\SYSTEM32* jako cíl. Potom přístup k adresáři na cestě *D:\SYMLINK\DRIVERS* bude vést k adresáři *C:\WINNT\SYSTEM32\DRIVERS*.

K vytváření takovýchto symbolických odkazů lze použít právě utility Junction.

Použití

```
junction [-s] [-q] <file or directory>
junction <junction directory> <junction target>
junction -d <junction directory>
```

Seznam podporovaných parametrů

`-q`	Tichý režim. Potlačení chybových zpráv.
`-s`	Rekurzivní procházení adresářů.
`-d`	Odstranění propojení.

Příklad použití

Vytvoření odkazu vyžaduje definování adresáře, ve kterém je uložen nástroj Junction, do systémových proměnných. Po nastavení cesty k nástroji Junction do systémových proměnných můžete tento nástroj začít používat.

Výpis z vytvoření odkazu z adresáře na disku F na adresář na disku C lze realizovat zadáním tohoto příkazu:

```
junction .\TEST "c:\xampp"

Created: F:\Junction\TEST
Targetted at: c:\xampp
```

Po potvrzení vytvoření propojení je možné prostřednictvím adresáře *F:\Junction\TEST* přistupovat k adresáři na cestě *C:\xampp*.

Vytvořené propojení odstraníte pomocí příkazu:

```
junction –d .\TEST
```

Využití

Nástroj najde uplatnění například v oblasti automatizace, případně při správě a propojování adresářů vzdálených systémů. V domácím prostředí je pro běžné uživatele vhodné vytvořit propojení pomocí klasických grafických funkcí systému Windows pro vytvoření odkazu.

Streams

Název:	Streams	
Velikost:	41 kB	
Kategorie:	File and disk tools	
Typ utility:	CMD	
URL:	*http://technet.microsoft.com/en-us/sysinternals/bb897440.aspx*	

Popis

Streams je nástroj umožňující vyhledávání a výpis takzvaných alternativních datových proudů, v angličtině označovaných zkratkou ADS (Alternative Data Stream). Přítomnost ADS může představovat potenciální nebezpečí v podobě operací, které umožňují skrývání souborů, aplikací, skriptů na disku počítače.

Takto ukryté soubory a skripty nejsou viditelné běžným Průzkumníkem, a proto je není možné odhalit jednoduchým procházením adresářů.

Závažnější problém může představovat spouštění škodlivých skriptů a aplikací prostřednictvím datových proudů. Tímto způsobem se ukrývají a maskují v systému různé rootkity, keyloggery a jiný škodlivý kód, který má za úlohu získávat citlivé informace (například přihlašovací údaje).

Použití

```
streams [-s] [-d] <file or directory>
```

Seznam podporovaných parametrů

`-s`	Rekurzivní procházení adresářů.
`-d`	Odstranění datového proudu.

Příklad použití

Před použitím samotného nástroje Streams bude pro demonstrační účely prezentován postup vytvoření datového proudu ADS.

Vytvoření ADS umožňuje i samotný operační systém Windows prostřednictvím dialogu rychlého spuštění.

1. Klávesovou zkratkou **Win+R** vyvolejte dialogové okno **Spustit**.
2. Do tohoto dialogu napište příkaz ke spuštění Poznámkového bloku s doplněním o název datového proudu. To, že se má vytvořit alternativní datový proud, oznámíte pomocí dvojtečky, kterou vložíte mezi název spouštěné aplikace a zvolený název datového proudu (viz následující příkaz).
   ```
   notepad c:\test.txt:teststream
   ```
3. Po spuštění Poznámkového bloku bude uživatel dotázán na uložení souboru. Pro účely této prezentace je potřeba potvrzení a uložení souboru. Následně vložte libovolný text do vytvořeného textového souboru. Například:
   ```
   Toto je testovací ADS.
   ```
4. Za povšimnutí rozhodně stojí záhlaví okna, kde můžete vidět popis:
   ```
   test.txt:teststream
   ```
5. Po vložení textového obsahu tento soubor uložte (postačí klávesová zkratka Ctrl+S).
6. Následující operace ukáže zvláštnost, že nově vytvořený textový soubor je sice uložen na umístění *C:\test.txt*, je ale prázdný, má velkost 0 bajtů, a po opětovném otevření uvidíte, že neobsahuje žádná data.
7. Text, který jste vložili v bodě 2, je v takzvaném alternativním datovém proudu navázaném na soubor *test.txt*, a ne přímo v souboru *test.txt*.
8. Vytvořený datový proud není běžně viditelný a dostupný. Právě nástroj Streams z balíku Sysinternals umožňuje odhalování a odstraňování takovýchto skrytých datových proudů.
9. Jak můžete vidět z následujícího výpisu, ani standardní příkaz `dir` neodhalí skryté datové proudy.
   ```
   dir
   ```

```
 Volume in drive C has no label.
 Volume Serial Number is 227F-D92F
 Directory of C:\
14. 07. 2009  04:20    <DIR>          PerfLogs
13. 10. 2012  14:24    <DIR>          Powershell
24. 11. 2012  16:28    <DIR>          Program Files
01. 12. 2012  13:29    <DIR>          Program Files (x86)
27. 04. 2007  10:17            87 424 streams.exe
08. 12. 2011  10:58    <DIR>          SWSetup
29. 12. 2012  15:24                 0 test.txt
27. 10. 2012  13:10    <DIR>          Users
26. 10. 2012  09:24    <DIR>          Windows
```

```
11. 07. 2012  21:00    <DIR>          xampp
               2 File(s)         87 424 bytes
               8 Dir(s)  103 150 510 080 bytes free
```

Použití nástroje Streams

1. Následující výpis prezentuje spuštění nástroje v příkazovém řádku s uvedením konkrétní cesty, v níž se mají vyhledávat alternativní datové proudy. Výpis obsahuje zadaný parametr `–s`, který aplikuje rekurzivní procházení adresářové struktury. Při použití nástroje ale není tento parametr povinný.

```
streams -s c:\

Error opening c:\hiberfil.sys:
Access blocked. File is in use.
Error opening c:\pagefile.sys:
Access blocked. File is in use.
c:\test.txt:
   :teststream.txt:$DATA 16
c:\Documents and Settings\All Users\Temp:
   :56E2E879:$DATA 134
c:\Documents and Settings\All Users\Application Data\Temp:
   :56E2E879:$DATA 134
c:\Documents and Settings\All Users\Application Data\Application Data\Temp:
   :56E2E879:$DATA 134
c:\Documents and Settings\All Users\Application Data\Application Data\
   Application Data\Temp:
   :56E2E879:$DATA 134
```

   Na prezentovaném výpisu můžete vidět i velikost datových proudů. Číslo uvedené za řetězcem `$Data` prezentuje počet znaků v navázaném datovém proudu.

2. Nežádoucí datový proud odstraníte pomocí parametru `–d`. Viz následující výpis.

```
streams -d c:\test.txt

c:\test.txt:
   Deleted :teststream.txt:$DATA
```

Využití

Nástroj najde uplatnění u testerů a vývojářů softwarových aplikací, případně u bezpečnostních analytiků, kteří vyhledávají škodlivý kód na disku, případně vyhledávají skryté soubory a datové proudy v systému.

Sync

Název:	Sync	
Velikost:	40 kB	
Kategorie:	File and disk tools	
Typ utility:	CMD	
URL:	*http://technet.microsoft.com/en-en/sysinternals/bb897438*	

Popis

Nástroj s názvem Sync se snaží na operačních systémech Windows nabídnout funkcionalitu unixového nástroje Sync. Utilita umožňuje uložení obsahu paměti cache souborového systému na disk. Nástroj vyžaduje pro svou činnost práva administrátora. Nástroj je vhodný k diagnostice pádů operačního systému.

Použití

```
sync [-r | drive letters]
```

Seznam podporovaných parametrů

`-r`	Uložení vyměnitelného média.
`-e`	Odpojení vyměnitelného média.

Příklad použití

Uložení obsahu paměti cache všech aktuálně připojených pevných disků.

sync

```
Flushing: C D F
```

Využití

Nástroj Sync budou nejčastěji využívat technici, kteří analyzují pády aplikací a operačního systému Windows. V takovýchto situacích mohou být užitečné informace, které jsou v paměti cache souborového systému v okamžiku před pádem aplikace nebo systému.

Disk2vhd

Název:	Disk2vhd	
Velikost:	811 kB	
Kategorie:	File and disk tools	
Typ utility:	GUI	
URL:	*http://technet.microsoft.com/en-en/sysinternals/ee656415*	

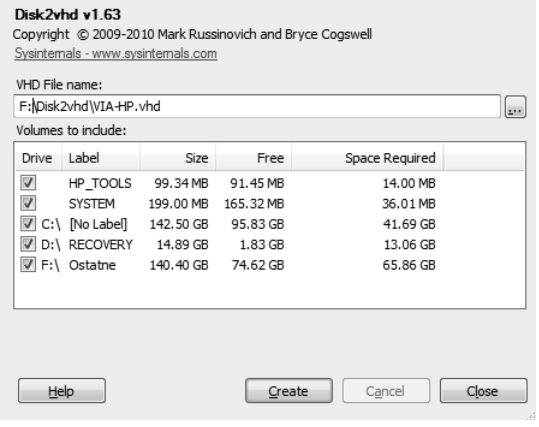
Popis

Utilita Disk2vhd umožňuje vytvoření virtuálního diskového souboru z fyzického systému. Tento soubor může být následně použit s technologií Hyper-V. Utilita podporuje operační systémy od Windows XP SP2 a vyšší. Podporovány jsou i 64bitové systémy.

Jednou z užitečných vlastností této utility je i schopnost vytvářet takzvané snapshoty (obrazy) disku, které mohou sloužit pro zálohovací účely.

Použití

Po spuštění nástroje se zobrazí jednoduché grafické okno (viz obrázek 1.2), kde je potřeba zvolit požadovaný disk a spustit tvorbu obrazu VHD.



Obrázek 1.2 Disk2vhd

Nástroj nabízí i jednoduché použití v prostředí příkazového řádku, které se dá využít například při automatizované správě operačního systému pomocí plánování úloh (task scheduling).

Použití v prostředí příkazového řádku:

```
disk2vhd <[drive: [drive:]...]|[*]> <VHD file>
```

Příklad použití

Příklad použití v prostředí příkazového řádku, kde se podle disku C vytvoří záloha ve formátu VHD, která bude uložena na disk C do adresáře *vhd*.

```
disk2vhd c: c:\vhd\vhdfile.vhd
```

Poznámka: Vytváření obrazů systémových disků (disků, kde je nainstalován operační systém) může být limitováno licenčními podmínkami. Před vytvářením kopie systémového disku je potřeba prostudovat licenční podmínky nainstalovaného operačního systému.

Využití

Jak už bylo zmíněno výše, nástroj je možné využít k zálohování. Uplatnění tedy najde u systémových administrátorů, kteří si chtějí vytvořit zálohu operačního systému a ten následně v případě potřeby implementovat.

PageDefrag

Název:	PageDefrag	
Velikost:	70 kB	
Kategorie:	File and disk tools	
Typ utility:	GUI	
URL:	*http://technet.microsoft.com/en-us/sysinternals/bb897426*	

Popis

PageDefrag umožňuje zobrazovat fragmentaci registrových záznamů a defragmentovat je. Výhodou tohoto nástroje je schopnost defragmentovat i soubory, které jsou nepřístupné běžným defragmentačním nástrojům. Jedná se například o stránkovací soubor *pagefile.sys* či podregistry.

Použití utility vyžaduje uživatelské oprávnění systémového administrátora. Nástroj je určen pro starší operační systémy (Windows XP). Na novějších operačních systémech (Windows 7) není spuštění možné ani v režimu kompatibility.

Použití

Nástroj má grafické rozhraní, umožňuje ale použití i z prostředí příkazového řádku. Nástroj se dá používat i při automatizované správě operačních systémů.

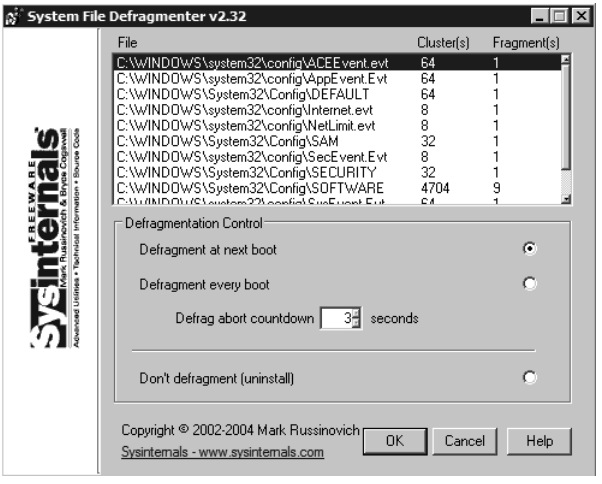
```
pagedefrag [-e | -o | -n] [-t <seconds>]
```

Seznam podporovaných parametrů

`-e`	Defragmentovat při každém spuštění.
`-o`	Defragmentovat jen jednou.
`-n`	Nedefragmentovat.
`-t`	Nastavení odpočítávání. Čas se nastavuje v sekundách.

Příklad použití

Nástroj PageDefrag komunikuje s uživatelem prostřednictvím grafického rozhraní, které je poměrně intuitivní (obrázek 1.3).



Obrázek 1.3 PageDefrag

V nastaveních utility můžete zvolit, kdy má dojít k defragmentaci potřebných systémových souborů. Na výběr je volba jednorázového defragmentování při následujícím startu systému, nebo opakované defragmentování při každém startu operačního systému.

Vzhledem k typu a počtu defragmentovaných souborů je defragmentace výrazně kratší než běžně při defragmentování celých diskových jednotek. První defragmentace těchto souborů ale může trvat delší dobu.

Správné použití tohoto nástroje vyžaduje dostatek volného diskového prostoru.

Využití

Nástroj neslouží jako náhrada klasických defragmentačních nástrojů, ale jako doplněk k těmto nástrojům, které nedokážou defragmentovat systémové soubory. Využití najde v situacích, kdy jsou poškozeny diskové oblasti, ve kterých se nacházejí uložené systémové soubory nebo registrové klíče. Hlavní cílovou skupinu uživatelů představují systémoví administrátoři.

MoveFile a PendMoves

Název:	MoveFile	
Velikost:	135 kB	
Kategorie:	File and disk tools	
Typ utility:	CMD	
URL:	*http://technet.microsoft.com/sk-sk/sysinternals/hh290814*	

Popis

Nástroje MoveFile a PendMoves jsou distribuovány ze společného odkazu v jednom archívu ZIP. Utility nabízejí funkcionalitu nahrazování souborů, která se využívá při aktualizacích. Během aktualizování operačního systému bývá zapotřebí nahradit určité soubory, které se mohou v tom čase používat (například ovladače zařízení, moduly a pluginy). Proto je potřeba jejich výměnu naplánovat na následující restart systému. Před jejich dalším použitím dojde k jejich aktualizaci – výměně za aktualizované soubory.

Obdobná situace s držením souboru může nastat při detekci malwaru nebo jiného škodlivého softwaru na stanici. Prostřednictvím těchto nástrojů lze naplánovat odstranění nežádoucích souborů, které se nedají ze systému odebrat běžným způsobem. Tímto způsobem je možné odstranit některé typy škodlivého softwaru. Sofistikovanější malware ale může mít vypracovanou ochranu proti takovýmto opatřením.

Použití nástrojů

Nástroj MoveFile vyžaduje definování cesty k cílovému souboru a cestu k destinaci, kam má být daný soubor přesunut.

```
movefile [source] [dest]
```

Utilita PendMoves nepodporuje žádné rozšiřující parametry.

```
pendmoves
```

Seznam podporovaných parametrů

Následující seznam podporovaných parametrů se týká nástroje MoveFile.

`[source]`	Cesta ke zdrojovému souboru, který má být přesunut nebo odstraněn.
`[dest]`	Cesta k cílovému místu, kam má být zdrojový soubor přesunut. V případě, že se jako cíl zadají uvozovky **""**, bude soubor odstraněn.

Příklad použití

K odstranění souborů je potřeba nejprve použít nástroj MoveFile, který naplánuje přesun, respektive odstranění požadovaných souborů. Následně je možné pomocí nástroje PendMoves vypisovat seznam souborů, jejichž odstranění je naplánováno na následující restart systému.

V následující ukázce bude prezentován postup, kde se prostřednictvím nástroje MoveFile naplánuje odstranění textového souboru.

```
movefile c:\test.txt ""

Move successfully scheduled.
```

Následně se s pomocí nástroje PendMoves vypíše naplánovaná úloha odstranění tohoto souboru po restartu operačního systému.

```
pendmoves

Source: c:\test.txt
Target: DELETE
Time of last update to pending moves key: 30. 12. 2012 18:42
```

Využití

Nástroj najde uplatnění u systémových administrátorů, ale i v domácí praxi u uživatelů, kteří potřebují odstranit soubory, ale nemohou to provést prostřednictvím klasického procesu odstraňování přes Průzkumníka (místní nabídka, případně klávesa **Delete**).

Pokud daný soubor neobsahuje škodlivý kód a není detekován ani antivirovým softwarem, který by toto plánované odstranění zabezpečil, je možné, že je daný soubor držen některým z aktuálně běžících procesů. Proto naplánované odstranění při dalším restartu může tento problém vyřešit. Situace s problémovým odstraňováním může nastat například při nekorektní odinstalaci softwaru.

DiskMon

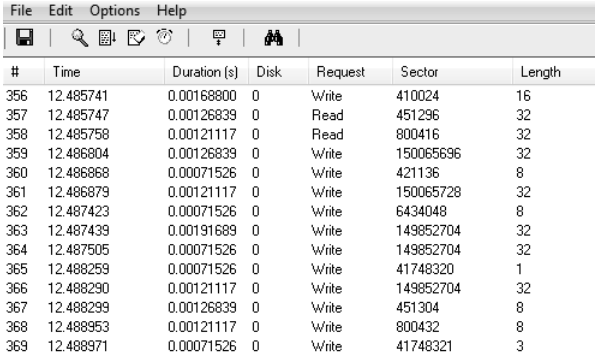
Název:	DiskMon	
Velikost:	80 kB	
Kategorie:	File and disk tools	
Typ utility:	GUI	
URL:	*http://technet.microsoft.com/en-us/sysinternals/bb896646*	

Popis

DiskMon je aplikace umožňující zaznamenávat a zobrazovat diskovou aktivitu operačního systému.

Použití

Po spuštění utility se automaticky spustí záznam údajů o diskové aktivitě. Mezi zaznamenávanými informacemi lze najít například: sektor, typ operace (čtení/zápis), čas spotřebovaný k vykonání operace a jiné údaje.


File Edit Options Help

#	Time	Duration (s)	Disk	Request	Sector	Length
356	12.485741	0.00168800	0	Write	410024	16
357	12.485747	0.00126839	0	Read	451296	32
358	12.485758	0.00121117	0	Read	800416	32
359	12.486804	0.00126839	0	Write	150065696	32
360	12.486868	0.00071526	0	Write	421136	8
361	12.486879	0.00121117	0	Write	150065728	32
362	12.487423	0.00071526	0	Write	6434048	8
363	12.487439	0.00191689	0	Write	149852704	32
364	12.487505	0.00071526	0	Write	149852704	32
365	12.488259	0.00071526	0	Write	41748320	1
366	12.488290	0.00121117	0	Write	149852704	32
367	12.488299	0.00126839	0	Write	451304	8
368	12.488953	0.00121117	0	Write	800432	8
369	12.488971	0.00071526	0	Write	41748321	3

Obrázek 1.4 DiskMon

Utilita podporuje jediný parametr v prostředí příkazového řádku, který umožňuje její spuštění v odlehčeném módu v oznamovací části hlavního panelu.

Spuštění v odlehčeném módu:

```
diskmon /l
```

Využití

Nástroj najde uplatnění u softwarových vývojářů, případně u systémových či forenzních analytiků, kteří potřebují detailně sledovat diskovou aktivitu. Sledováním diskové aktivity je možné diagnostikovat běh nežádoucích procesů na pozadí.

DiskExt

Název:	DiskExt	
Velikost:	40 kB	
Kategorie:	File and disk tools	
Typ utility:	CMD	
URL:	*http://technet.microsoft.com/en-us/sysinternals/bb896648*	

Popis

DiskExt je dalším z nástrojů, který ve svém výstupu poskytuje informace o diskových jednotkách připojených k dané stanici.