ZÁPADOČESKÁ UNIVERZITA V PLZNI
FAKULTA ELEKTROTECHNICKÁ

KATEDRA ELEKTROENERGETIKY A EKOLOGIE

DIPLOMOVÁ PRÁCE

Vzdálená správa Windows v lokální počítačové síti

Bc. Lukáš Hofman **2015**

ZÁPADOČESKÁ UNIVERZITA V PLZNI
Fakulta elektrotechnická
Akademický rok: **2014/2015**

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Lukáš HOFMAN**
Osobní číslo:	**E13N0005K**
Studijní program:	**N2644 Aplikovaná elektrotechnika**
Studijní obor:	**Aplikovaná elektrotechnika**
Název tématu:	**Vzdálená správa Windows v lokální počítačové síti**
Zadávající katedra:	**Katedra elektroenergetiky a ekologie**

Zásady pro vypracování:

1. Popište možnosti vzdálené správy a ovládání Windows v lokální počítačové síti.
2. Uveďte prostředky, které vzdálenou správu usnadňují a automatizují.
3. Vytvořte nástroj pro zobrazení přehledu a informací o zapnutých/vypnutých PC s možností jejich ovládání.
4. Vytvořte nástroj pro zobrazení informací a správu jednotlivých vzdálených PC v oblastech: běžící procesy, služby, nainstalovaný software.

Rozsah grafických prací:	**podle doporučení vedoucího**
Rozsah pracovní zprávy:	**30 - 40 stran**
Forma zpracování diplomové práce:	**tištěná/elektronická**

Seznam odborné literatury:

Student si vhodnou literaturu vyhledá v dostupných pramenech podle doporučení vedoucího práce.

Vedoucí diplomové práce:	**Ing. Jiří Basl, Ph.D.** Katedra aplikované elektroniky a telekomunikací
Datum zadání diplomové práce:	**15. října 2014**
Termín odevzdání diplomové práce:	**11. května 2015**

Doc. Ing. Jiří Hammerbauer, Ph.D.
děkan

L.S.

Doc. Ing. Karel Noháč, Ph.D.
vedoucí katedry

V Plzni dne 15. října 2014

Abstrakt

Tato diplomová práce se zabývá možnostmi vzdálené správy a ovládání operačního systému Windows v lokální počítačové síti. Jsou zde popsány prostředky, které vzdálenou správu usnadňují a automatizují (příkazový řádek, dávkové soubory, skripty). Využívají se nástroje, které jsou součástí Windows nebo se dají zdarma doinstalovat. V praktické části byly vytvořeny v aplikaci Excel pomocí jazyka VBA dva nástroje. První slouží pro zobrazení přehledu a informací o zapnutých/vypnutých počítačích s možností jejich ovládání. Druhý je určen pro zobrazení informací a správu jednotlivých vzdálených počítačů v oblastech: běžící procesy, služby, nainstalovaný software. Při jejich realizaci bylo využito rozhraní WMI, funkce API a také objekty COM.

Klíčová slova

Microsoft Windows, vzdálená správa, příkazový řádek, VBScript, WMI, API, proces, služba, ovladač, registr, Wake on LAN, MAC, Active Directory, Excel, VBA.

Abstract

This thesis deals with remote management and control of Windows operating system in a local area network. Possibilities for making administration and automation easy are described (command line, batch files and scripts). There are used the tools those are included in Windows or can be installed for free. In the practical part there were created two programs in Microsoft Excel using language VBA. The first one is used to display overview and related information about switched on/off computers with the possibility to control them. The second one shows information and manages individual remote computers in the areas of running processes, services and installed software. Both programs were implemented by the help of WMI interface, API functions and COM objects.

Key words

Microsoft Windows, remote administration, command line, VBScript, WMI, API, process, service, driver, registry, Wake on LAN, MAC, Active Directory, Excel, VBA.

Prohlášení

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně, s použitím odborné literatury a pramenů uvedených v seznamu, který je součástí této diplomové práce.

Dále prohlašuji, že veškerý software, použitý při řešení této diplomové práce, je legální.

.....

podpis

V Plzni dne 13.4.2015 Bc. Lukáš Hofman

Obsah

Seznam zkratek

AD ..... Active Directory

API..... Application Programming Interface

COM ..... Component Object Model

CPU ..... Central Processing Unit

DHCP ..... Dynamic Host Configuration Protocol

ICMP ..... Internet Control Message Protocol

LDAP..... Lightweight Directory Access Protocol

MAC ..... Media Access Control

RPC..... Remote Procedure Call

UAC..... User Account Control

VBA..... Visual Basic for Applications

VBScript ..... Visual Basic Scripting Edition

WMI ..... Windows Management Instrumentation

WQL ..... WMI Query Language

WOL ..... Wake on LAN

XML ..... Extensible Markup Language

<*text*>..... popisný text v ostrých závorkách zastupuje nějaký konkrétní název, např. zkratka <*PC*> nahrazuje jméno určitého počítače; obsahuje-li konkrétní název mezery, je nutné jej uzavřít do uvozovek

Úvod

V dnešní době jsou počítačové sítě nezbytnou součástí většiny organizací. Při správě několika málo počítačů fyzicky dostupných na jednom místě je možné řešit administraci přímo na jednotlivých stanicích. Ovšem v případě většího počtu počítačů, které mohou být umístěny v různých budovách či lokalitách, je nezbytné využít prostředky pro jejich vzdálenou správu a ovládání. Vhodné je též používat takové nástroje, které potřebné činnosti usnadňují a automatizují. Nejpoužívanějším operačním systémem je Microsoft Windows, který sám o sobě poskytuje pro tyto účely dostatek možností.

Cílem této práce je ukázat možnostmi vzdálené správy a ovládání operačního systému Windows v lokální počítačové síti. Dále popsat prostředky, které vzdálenou správu usnadňují a automatizují. Využijí se nástroje, které jsou přímo součástí Windows, případně se dají zdarma doinstalovat.

Úkolem praktické části je vytvořit dva nástroje. První pro zobrazení přehledu a informací o zapnutých/vypnutých počítačích s možností jejich ovládání. Seznam počítačů bude možné načítat z Active Directory. Počítače půjde vzdáleně zapínat, vypínat, restartovat a provádět s nimi další uživatelsky volitelné operace. Druhý nástroj bude sloužit pro zobrazení informací a správu jednotlivých vzdálených počítačů v oblastech: běžící procesy, služby, nainstalovaný software. Nástroje budou vytvořeny v aplikaci Microsoft Excel za pomoci jazyka VBA. Využijí se bohaté možnosti formátování, filtrování a seřazování, které Excel nabízí. Pro realizaci bude použito rozhraní WMI, funkce API a také objekty COM.

I. TEORETICKÁ ČÁST

1 Vzdálená správa z příkazového řádku

Příkazový řádek (Command Prompt) hraje důležitou roli při správě a konfiguraci Windows. Spuštění patřičného příkazu je často jednodušší a rychlejší než provedení téhož pomocí grafického uživatelského rozhraní. S výhodou lze využít řetězení příkazů pomocí roury (pipe) nebo přesměrovat výstup do souboru.

Mnoho příkazů umožňuje spravovat také vzdálené počítače. K tomuto účelu se často používá přepínač /S <*PC*>, nicméně není to pravidlem. Většinou je možné zadat též přístupové údaje (uživatelské jméno a heslo) pro případ, že aktuální uživatel nedisponuje potřebným oprávněním.

Při práci se soubory se často nastavuje výchozí pracovní složka příkazem *cd*. Příkazový řádek však nepodporuje síťové (UNC) cesty jako aktuální adresáře. Jde to vyřešit použitím příkazu *pushd*, který provádí namapování složky jako síťové jednotky, tj. obdobně jako příkaz `net use * \\<PC>\<sdílená složka>`. Toto namapování ruší příkaz *popd*.

Pro automatizaci činností slouží dávkové soubory (*.bat, *.cmd) obsahující posloupnost příkazů pro příkazový řádek. Lze v nich používat i jednoduché programové konstrukce jako je *if* nebo *for*. Dávkový soubor je možné spustit s parametry, ke kterým se poté přistupuje pomocí speciálních proměnných (%1 až %9 nebo %*).

Následující kapitoly popisují nejčastější oblasti vzdálené správy Windows.

1.1 Správa procesů

Procesy mají v systému Windows výsadní postavení, jelikož odpovídají spuštěným aplikacím a službám. Jejich přehled je důležitý nejen pro celkové zobrazení stavu systému, ale také pro případné objevení problémů a nadměrného vytížení procesů. [1]

V seznamu procesů se vyskytují také systémové procesy, které jsou nezbytné pro vlastní funkčnost operačního systému. Např. procesy „smss.exe“ a „csrss.exe“ zajišťují základní běh Windows, proces „services.exe“ ovládá služby a proces „winlogon.exe“ zprostředkovává přihlašování uživatelů. Při ukončení systémového procesu může dojít k nestabilitě nebo pádu systému.

Každý proces má přidělen jedinečný identifikátor *PID*. Ten se často využívá pro jednoznačné určení procesu při jeho ukončování.

- Příkazy tasklist a taskkill

Základním nástrojem pro výpis informací o procesech z prostředí příkazového řádku je příkaz *tasklist* a pro jejich ukončování slouží *taskkill*. Oba využívají pro svou činnost rozhraní WMI. Některé přepínače mají shodné, např. přepínač /S <*PC*> pro určení vzdáleného počítače nebo /FI "<*filtr*>" pro zadání filtrů.

Zadáním příkazu *tasklist* bez dalších přepínačů se vypíší názvy všech procesů a další základní údaje (PID, název relace, číslo relace, paměť). Přidáním přepínače /V se výpis rozšíří o další sloupce (stav, uživatelské jméno, čas CPU, titulek okna), avšak pro vzdálený počítač nejsou některé dostupné (stav, titulek okna).

Důležitým prvkem je možnost omezit výběr procesů pomocí filtrů. Následující příklad vypíše případné procesy „msiexec.exe“ související s probíhající instalací/odinstalací balíčku MSI, nikoliv však stejnojmenný proces spuštěné instalační služby „msiserver“, která běží ještě 10 minut po dokončení instalace:

```
tasklist /FI "IMAGENAME eq msiexec.exe" /FI "SERVICES ne msiserver"
```

Další ukázka použití filtru zobrazí procesy, které alokují v paměti více jak 100 MB:

```
tasklist /FI "MEMUSAGE gt 102400"
```

Příkaz *taskkill* slouží k ukončení určitého procesu. Proces lze zadat pomocí jeho PID přepínačem /PID <*PID*> nebo podle názvu přepínačem /IM <*název procesu*>. Využít se dají i filtry obdobně jako u příkazu *tasklist*. Přidáním přepínače /T je možné zajistit také ukončení všech podprocesů (potomků) daného procesu. Ukončení vzdálených procesů je vždy provedeno násilně (jako by byl použit přepínač /F), případná neuložená data procesu jsou ztracena.

- Nástroj WMIC

Procesy lze ovládat také pomocí WMI prostřednictvím konzolového nástroje *wmic*. K definování příslušné WMI třídy je možné využít alias *process* případně uvést plné jméno třídy zadáním výrazu *path Win32_Process*. Ke vzdálenému přístupu slouží přepínač /node.

Pro výpis procesů se všemi dostupnými vlastnostmi třídy Win32_Process lze použít příkaz `wmic process get /value`. Výběr zobrazovaných vlastností je samozřejmě možné omezit uvedením jejich jmen, např. příkaz `wmic process get` **`ExecutablePath`** vypíše pouze cesty souborů procesů.

Využít lze také filtrování pomocí standardních WQL dotazů. Následující dvě varianty příkazů vypíší řetězec příkazové řádky procesů „msiexec.exe“ souvisejících s probíhající instalací/odinstalací balíčku MSI, nikoliv však stejnojmenný proces spuštěné instalační služby „msiserver“:

```
wmic process where (Name = "msiexec.exe" and not CommandLine like
 "%\\msiexec.exe /V") get CommandLine

wmic process where (Name = "msiexec.exe" and CommandLine !=
 "C:\\Windows\\system32\\msiexec.exe /V") get CommandLine
```

K ukončení procesu se používá klíčové slovo *call Terminate* nebo jen *delete*. Ukončovaný proces se nejčastěji identifikuje podle PID nebo názvu. Příkaz k ukončení procesu může být např. `wmic process where ProcessId=<PID> call Terminate` nebo `wmic process where Name="<název procesu>" delete`.

- Příkazy qprocess a tskill

Další možností pro zobrazení a ukončení procesů jsou příkazy *qprocess* a *tskill*. Pro práci se vzdáleným počítačem slouží přepínač /SERVER:<*PC*>, nicméně musí být na něm povolené *vzdálené volání procedur* (RPC). V serverových verzích Windows je toto standardně povoleno, ale na běžných stanicích je nutné provést příslušné nastavení v registru. K nastavení vzdáleného počítače lze použít následující příkaz:

```
reg add "\\<PC>\HKLM\SYSTEM\CurrentControlSet\Control\Terminal
 Server" /v AllowRemoteRPC /t REG_DWORD /d 1 /f
```

Vzdálené volání procedur využívají i jiné příkazy, např. příkaz *msg* pro odeslání zprávy na vzdálený počítač nebo *quser* pro vypsání přihlášených uživatelů.

Příkaz *qprocess* (nebo ekvivalent *query process*) zobrazuje základní informace o procesech (název procesu, PID, číslo a název relace, uživatelské jméno). Pro výpis všech procesů na vzdáleném počítači lze použít příkaz `qprocess /SERVER:<PC> *`.

K ukončení procesu se používá příkaz *tskill*. Ukončovaný proces lze zadat pomocí PID nebo názvu (v názvu se neuvádí přípona souboru procesu). Příkaz k ukončení vzdáleného procesu je `tskill /SERVER:<PC> <PID|název procesu> /A`. Ukončení procesů (vzdálené i lokální) je vždy provedeno násilně, případná neuložená data procesu jsou ztracena.

1.2 Správa služeb

Služby jsou speciální programy běžící na pozadí Windows. Poskytují nejrůznější funkce nutné pro běh operačního systému nebo některých aplikací. Většinou se spouští při startu systému, případně automaticky dle potřeby nebo ručním zásahem uživatele. Činnost služeb je řízena systémovým procesem „services.exe“, který je využíván jako prostředník pro jejich ovládání. Obdobou služeb jsou také ovladače, zaváděné do jádra (kernelu) Windows.

- Příkaz sc

Všestranným pomocníkem pro správu služeb z příkazové řádky je příkaz *sc*. Umožňuje komplexní ovládání a konfiguraci služeb i ovladačů. K vykonání akce na vzdáleném počítači je určen přepínač \\<*PC*>.

Pro výpis aktuálně spuštěných služeb stačí zadat příkaz `sc query` a pro vypsání spuštěných ovladačů příkaz `sc query type= driver`. Všechny služby resp. ovladače lze zobrazit přidáním přepínače state= all. Mezera za znakem „=“ je nutná.

K ovládání běhu služeb slouží přepínače start, stop, pause a continue. Příkaz *sc* však neumožňuje zastavit službu, na níž jsou závislé další spuštěné služby. Rovněž nelze službu restartovat (zastavit a následně opět spustit), ale to jde vyřešit např. následujícím dávkovým souborem:

```
@echo off
set /P PC=Zadejte PC: || exit /b
set /P SERVICE=Zadejte službu: || exit /b

sc \\%PC% stop "%SERVICE%"

:A
sc \\%PC% query "%SERVICE%" | find "STOP_PENDING" > NUL  && goto A

sc \\%PC% start "%SERVICE%"
```

- Nástroj WMIC

Služby lze spravovat také přes WMI pomocí příkazu *wmic*. K definování příslušné WMI třídy je možné využít alias *service* případně uvést plné jméno třídy zadáním výrazu *path Win32_Service*. Obdobně pro práci s ovladači lze využít alias *sysdriver* nebo zadat výraz *path Win32_SystemDriver*. Pro přístup k vzdáleným počítačům slouží přepínač /node.

Pro výpis seznamu všech služeb se základními údaji (Name, ProcessId, StartMode, State, Status) lze použít příkaz `wmic service list brief`. Výstup je možné ovlivnit zadáním podmínky a určením vypisovaných vlastností. Následující příklad vypíše jména automaticky spouštěných, ale aktuálně zastavených služeb:

```
wmic service where (StartMode="Auto" and Started=FALSE) get Name,
 DisplayName
```

Ke konfiguraci a ovládání služeb se používají standardní metody WMI třídy *Win32_Service*. Následující ukázka příkazů nastaví na vzdáleném počítači automatický typ spouštění služby RemoteRegistry (Vzdálený registr) a poté provede spuštění této služby:

```
wmic /node:<PC> service where Name="RemoteRegistry" call
 ChangeStartMode "Automatic"

wmic /node:<PC> service where Name="RemoteRegistry" call
 StartService
```

- Příkaz tasklist

Příkaz *tasklist* je určen k zobrazení běžících procesů. Pomocí přepínače /SVC však lze zobrazit také spuštěné služby související s některými procesy. Příkaz pro vypsání procesů služeb vzdáleného počítače vypadá takto:

```
tasklist /S <PC> /SVC | findstr /V /C:"Není k dispozici" /C:"N/A"
```

1.3 Ovládání plánovače úloh

Plánovač úloh zajišťuje provádění určitých akcí (nejčastěji spuštění programu) na základě časového plánu nebo nějaké aktivační události. Aktivační událostí může být spuštění počítače nebo přihlášení či nečinnost uživatele. Spouštění naplánovaných úloh obstarává služba Schedule (Plánovač úloh).

- Příkaz schtasks

Pro plnohodnotnou správu naplánovaných úloh slouží příkaz *schtasks*. Umožňuje úlohy vyhledat, vytvořit, odstranit, upravit, spustit nebo zastavit. Pro správu naplánovaných úloh na vzdáleném počítači slouží přepínač /S <*PC*>. Následující příkaz naplánuje na vzdáleném počítači spuštění defragmentace všech disků pravidelně každý pátek v 22:00.

```
schtasks /create /S <PC> /TN Defragmentace /SC WEEKLY /D FRI
 /ST 22:00 /RU SYSTEM /TR "defrag /C" /F
```

- Příkaz at

Příkaz *at* lze využít zejména pro jednoduché naplánování jednorázových akcí. Např. příkaz `at \\<PC> 23:00 shutdown /r` naplánuje na vzdáleném počítači jeho restart v 23:00. Úlohy jsou spouštěny skrytě v kontextu uživatele „NT AUTHORITY\SYSTEM“.

1.4 Práce s registrem

Registr ve Windows slouží jako jakási databáze k ukládání údajů a nastavení systému, aplikací a uživatelů. Prvky registru se dělí na klíče, podklíče a jednotlivé hodnoty.

Základní kořenové klíče registru jsou:

- HKEY_CLASSES_ROOT (HKCR): asociace programů k příponám souborů
- HKEY_CURRENT_USER (HKCU): nastavení aktuálně přihlášeného uživatele
- HKEY_LOCAL_MACHINE (HKLM): nastavení a konfigurace počítače
- HKEY_USERS (HKU): obsahuje podregistry aktuálně připojených uživatelů
- HKEY_CURRENT_CONFIG (HKCC): aktuálně používaný hardwarový profil

Při přístupu ke vzdálenému počítači je možné pracovat pouze s klíči HKLM a HKU. Ostatní kořenové klíče lze využít pouze lokálně a jsou to v podstatě pouze zástupci na určité podklíče v HKLM nebo HKU.

- Příkaz reg

Pro práci s registrem z prostředí příkazového řádku se používá příkaz *reg*. Použití příkazu je následující: reg <*operace*> <*klíč registru*> <*přepínače*>.

K vykonání operace (čtení, vytváření, mazání klíčů a hodnot) na vzdáleném počítači se na začátek klíče přidává řetězec „\\<*PC*>\“. Operace jako je import/export částí registru či načtení/uvolnění (load/unload) podregistrů však nelze vzdáleně provádět. Pro práci s registrem musí být na vzdáleném počítači spuštěna služba RemoteRegistry (Vzdálený registr). Automatické spouštění této služby je nutné nastavit, případně službu před připojením k vzdálenému registru operativně spustit.

Např. pro vypsání *položek po spuštění*, uložených v registru aktuálně přihlášeného uživatele, lze na lokálním počítači použít následující příkaz:

```
reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Run
```

Jak již bylo uvedeno, na vzdáleném počítači je možné pracovat pouze s klíči HKLM a HKU. K provedení výše uvedeného příkazu pro vzdálený počítač je nutné použít klíč „\\<*PC*>\HKU\<*SID*>\Software\Microsoft\Windows\CurrentVersion\Run“, kde *SID* je identifikátor zabezpečení uživatele přihlášeného na vzdáleném počítači. Následující dávkový soubor zjistí přihlášeného uživatele a jeho SID (s využitím příkazu *wmic*), spustí službu RemoteRegistry a nakonec vypíše zmíněné *položky po spuštění* z registru:

```
@echo off
set /P PC=Zadejte PC: || exit /b

for /F "skip=1" %%A in ('wmic /node:%PC% ComputerSystem get
 UserName') do  (set USER=%%A) & goto K
:K

if "%USER%"=="" echo Není přihlášen žádný uživatel & pause & exit /b

for /F "tokens=1,2 delims=\" %%A in ("%USER%") do (
  for /F "skip=1" %%X in ('"wmic /node:%PC% path Win32_UserAccount
 where (Domain="%%A" and Name="%%B") get SID"') do  (set SID=%%X) &
 goto K
)
:K

sc \\%PC% start RemoteRegistry >NUL 2>&1

reg query
 \\%PC%\HKU\%SID%\Software\Microsoft\Windows\CurrentVersion\Run

echo %CMDCMDLINE% | find "%~0" >NUL  && pause
```

2 Nástroje PsTools

Vhodným doplňkem pro vzdálenou správu počítačů z příkazové řádky je sada konzolových nástrojů s názvem *PsTools* [2]. Jsou součástí zdarma dostupných utilit označovaných jako „Windows Sysinternals“. Jejich autorem je hlavně Mark Russinovich z původní firmy Winternals, kterou v roce 2006 koupil Microsoft. Od té doby je nutné při prvním spuštění těchto programů potvrdit tlačítkem licenční ujednání (EULA), což může být dost omezující zejména u řádkových utilit předurčených pro bezobslužný běh. Naštěstí to jde většinou obejít přidáním přepínače `-EulaAccepted`, případně lze předem provést zápis do registru např. příkazem `reg add HKCU\Software\SysInternals\<utilita> /v EulaAccepted /t REG_DWORD /d 1 /f`.

Všechny nástroje PsTools umožňují vykonání operace na vzdáleném počítači pomocí přepínače `\\<PC>`. U některých je také možné uvést více počítačů oddělených čárkou nebo předat soubor se seznamem počítačů přepínačem `@<soubor>`. Kompletní syntaxi utilit lze vypsat pomocí přepínače `-?`.

Tab. 2.1: Nástroje PsTools

Nástroj	**Popis**
PsExec	spustí program (příkaz)
PsFile	vypíše seznam vzdáleně otevřených souborů
PsGetSid	zobrazí SID (Security Identifier) počítače nebo uživatele
PsInfo	vypíše informace o systému
PsKill	ukončí spuštěný proces
PsList	vypíše informace o spuštěných procesech
PsLoggedOn	vypíše přihlášené uživatele a uživatele využívající sdílené zdroje
PsLogList	vypíše záznamy z protokolu událostí (event log)
PsPasswd	změní heslo uživatelského účtu
PsPing	testuje výkon sítě
PsService	spravuje a ovládá služby
PsShutdown	vypne, uspí nebo restartuje počítač
PsSuspend	pozastaví/obnoví běh procesu

- Nástroj PsExec

Největší využití najde především nástroj *PsExec*. Tato utilita umožňuje spouštět programy na vzdáleném počítači nebo vzdáleně ovládat vlastní příkazový řádek. Zjednodušená syntaxe je následující:

PsExec [\\PC[,PC2][,...] | @soubor] [další přepínače] program [parametry]

PsExec jde použít hlavně ke spuštění konzolových programů (příkazů) včetně získání jejich výstupu (např. `cmd /C PsExec \\<PC> -e` **`ipconfig /all`** `& pause`). Dále lze vzdáleně spustit příkazový řádek (`PsExec \\<PC> -e` **`cmd`**) a pracovat v něm obdobně jako lokálně. Také se může využít např. k vzdálené instalaci/odinstalaci software, který podporuje přepínače pro bezobslužný průběh.

Vyžaduje-li spouštěný program přístup k síťovým zdrojům (např. ke sdílené složce na serveru), je nutné při spuštění utility PsExec specifikovat oprávněné uživatelské jméno (přepínač `-u` <*doména\uživatel*>) a heslo uvést buď jako parametr (přepínač `-p` <*heslo*>) nebo ho zadat až při výzvě po spuštění. Heslo je v novějších verzích PsExec přenášeno šifrovaně.

Spuštění programu na vzdáleném počítači funguje tak, že se nejprve ze souboru „PsExec.exe“ extrahuje soubor „PSEXESVC.exe“, který se zkopíruje do sdílení „Admin$“ cílového počítače. Následně se soubor zaregistruje jako služba „PSEXESVC“ a spustí se pomocí Windows Service Control Manager API. Spuštěná služba vytvoří komunikační kanál, kterým se PsExec připojí a odešle službě příkazy k vykonání. Po dokončení činnosti je služba včetně souboru odstraněna. [3]

PsExec standardně čeká na ukončení spuštěného programu a následně vypíše jeho návratový kód. Pokud je použit přepínač `-d`, na dokončení programu se nečeká, ale zobrazí se identifikátor spuštěného procesu (PID), který je též uložen do proměnné %ERRORLEVEL%.

Nástroj PsExec je použitelný i k jinému účelu. Pomocí příkazu `PsExec -i -d -s` <*`program s parametry`*> se na lokálním počítači interaktivně spustí určitý program pod systémovým účtem (uživatelem „NT AUTHORITY\SYSTEM“), který disponuje vysokým oprávněním. Takto je možné např. spustit konzolu „Služby“ (program `mmc services.msc`) a ovládat jinak neovladatelné služby „Klient zásad skupiny“ či „Plánovač úloh“ nebo spustit Editor registru (program `regedit`) a prohlédnout si obsah běžně nedostupných klíčů „HKLM\SAM\SAM“ a „HKLM\SECURITY“.

3 Windows Management Instrumentation

Rozhraní WMI je univerzálním prostředkem pro pokročilou správu Windows. Jedná se o výbornou platformou především pro získávání podrobných systémových informací, ale využít jde také pro vykonání nejrůznějších akcí prostřednictvím metod dostupných u řady tříd WMI. Umožňuje též sledování a zpracování událostí (např. při spuštění či ukončení procesu nebo služby).

Velkou výhodou WMI je snadný a přirozený přístup ke vzdáleným počítačům. Pro přístup je nutné administrátorské oprávnění (členství uživatele ve skupině „Administrators“ na cílovém počítači) nebo zajistit předání potřebných přístupových údajů. Také musí být případně povoleno WMI (resp. DCOM a RPC) v používaném firewallu.

Rozhraní WMI využívá bezpečnostní mechanismy operačního systému a vytváří nad ním další bezpečnostní vrstvu. Pomocí konzoly „wmimgmt.msc“ lze upravit zabezpečení přístupu k jednotlivým jmenným prostorům WMI.

WMI je tvořeno jmennými prostory (namespace), které jsou uspořádány ve formě stromové struktury. Kořenový prostor se nazývá „root“. Výchozí a nejčastěji využívaný namespace je „root\CIMV2“. Jmenné prostory obsahují jednotlivé WMI třídy.

Třídy WMI reprezentují určitou oblast systému. Může se jednat např. o procesy (třída Win32_Process), služby a ovladače (třída Win32_Service), operační systém (třída Win32_OperatingSystem), registr (speciální třída StdRegProv ve jmenném prostoru „root\default“) nebo hardware (např. třídy Win32_ComputerSystem a Win32_BIOS).

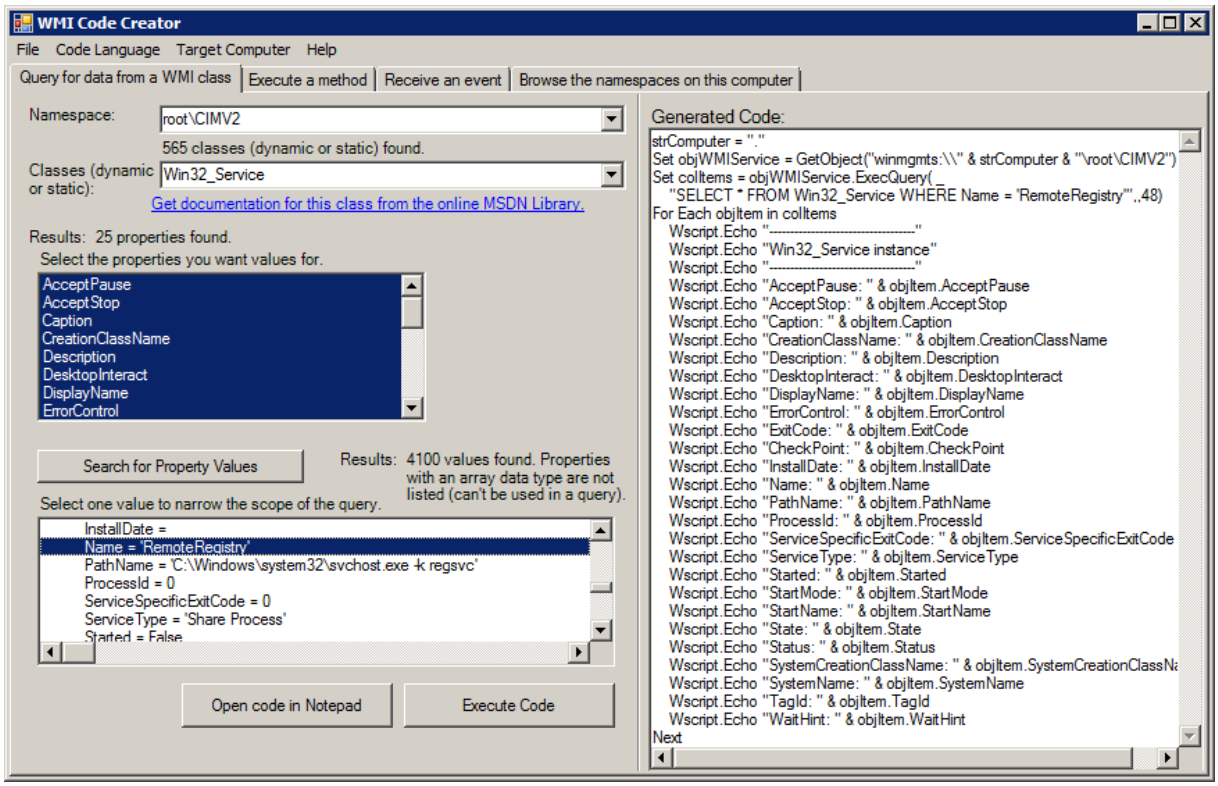
Existují také speciální WMI třídy: asociační třídy (association class) definují vztahy mezi jinými objekty (např. třídy Win32_SessionProcess a Win32_DependentService) a událostní třídy (event class) umožňují čekat na výskyt určité události (např. třída Win32_ProcessStopTrace).

Pro práci s WMI se používá dotazovací jazyk WQL (WMI Query Language), který vychází z jazyka SQL. Obdobně jako SQL obsahuje sadu klíčových slov a operátorů. Následuje ukázka WQL dotazu, který vrátí běžící procesy „msiexec.exe“, které nebyly spuštěny s přepínačem /V.

```
SELECT * FROM Win32_Process WHERE Name="msiexec.exe" AND NOT
 CommandLine LIKE "%\\msiexec.exe /V"
```

3.1 Použití WMI

K rozhraní WMI lze přistupovat z různých skriptovacích a programovacích jazyků (např. VBScript a Visual Basic). Využívá se princip vytváření objektových proměnných, které poté slouží k dalším operacím. Pro usnadnění tvorby skriptů nebo zdrojových kódů existuje řada nástrojů, např. *WMI Code Creator* od Microsoftu.



Obr. 3.1: WMI Code Creator

Následující ukázka skriptu v jazyce VBScript nastaví na vzdáleném počítači automatické spouštění služby RemoteRegistry (Vzdálený registr), spustí tuto službu a nakonec vypíše všechny spuštěné služby. Pro vykonání na lokálním počítači stačí místo jména počítače zadat tečku. Skript je vhodné spustit interpretem *cscript*.

```
PC = "<PC>"
Set objWMIService = GetObject("winmgmts:\\" & PC & "\root\CIMV2")

Set colItems = objWMIService.ExecQuery("SELECT * FROM Win32_Service
 WHERE Name='RemoteRegistry'")
For Each objItem in colItems
  WScript.Echo "ReturnValue: " & objItem.ChangeStartMode("Automatic")
  WScript.Echo "ReturnValue: " & objItem.StartService
Next
```

```
Set colItems = objWMIService.ExecQuery("SELECT * FROM Win32_Service
 WHERE State='Running'")
For Each objItem in colItems
  WScript.Echo objItem.Name & ";" & objItem.DisplayName
Next
```

3.2 Nástroj WMIC

WMI Console (WMIC) je nástroj příkazového řádku pro práci s rozhraním WMI. Na rozdíl od skriptovacích nebo programovacích jazyků zcela izoluje uživatele od objektové podstaty WMI. Ovládání probíhá prostřednictvím příkazu *wmic* (jedná se o program „C:\Windows\System32\wbem\WMIC.exe“).

Pro práci se vzdálenými počítači se používá přepínač /node:<*PC1*>,<*PC2*>… Předat lze také soubor se seznamem počítačů pomocí /node:@<*soubor se seznamem*>. Vhodné je přidat přepínač /failfast:1, který zabrání časovým prodlevám v případě nedostupnosti počítačů.

Jméno WMI třídy, s níž se bude pracovat, se zadává za přepínač *path* (např. `wmic` **`path`** `Win32_Service`). Pro mnohé třídy lze využívat zkrácené názvy (aliasy). Kupříkladu pro třídu Win32_Service existuje alias *Service* a pro Win32_OperatingSystem je alias *OS*. Seznam všech aliasů se vypíše příkazem `wmic alias get friendlyname,target`.

Následující ukázka dávkového souboru provádí totéž co ukázka v předchozí kapitole.

```
set wmicService=wmic /node:<PC> Service where

%wmicService% Name="RemoteRegistry" call ChangeStartMode "Automatic"
%wmicService% Name="RemoteRegistry" call StartService
%wmicService% State="Running" get Name,DisplayName
```

Nástroj WMIC umožňuje také formátování výstupu pomocí transformačních šablon (přepínač /format:<*název šablony*>). Následující dávkový soubor vytvoří v aktuální složce soubor „OS.csv“ s podrobnými informacemi o operačních systémech vzdálených počítačů, jejichž seznam je uveden v souboru „PC.txt“. Výstupní soubor lze poté otevřít v Excelu.

```
(
  echo sep=,
  wmic /node:@PC.txt /failfast:1 OS get /format:csv
) > OS.csv
```

4 Vzdálené zapnutí a vypnutí počítače

Úkony, související se správou počítačů (údržba a aktualizace systému, instalace aplikací), je zpravidla nutné provádět mimo běžnou pracovní dobu uživatelů, kdy ale počítače bývají vypnuté. Většinou je nereálné jednotlivé počítače obcházet a zapínat, navíc některé nemusí být ani fyzicky dostupné (nepřístupné prostory, vzdálená lokalita). V této situaci přicházejí na řadu prostředky pro vzdálené zapnutí a vypnutí počítače.

4.1 Probuzení počítače po síti (Wake on LAN)

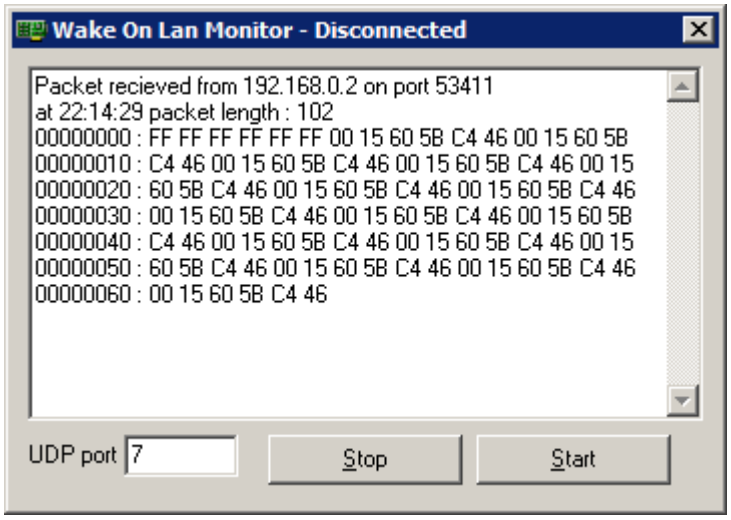
Technologie *Wake on LAN* (dále jen WOL) umožňuje probuzení (zapnutí) počítače po síti pomocí speciálního síťového paketu. Funkčnost WOL se většinou musí povolit v nastavení BIOSu, nejčastěji v sekci pro řízení spotřeby (Power Management). Síťová karta je poté napájena i při vypnutém počítači, což se pozná podle svítící diody na kartě i na portu switche. Pokud karta zachytí pro ni určený paket (podle MAC adresy), zajistí prostřednictvím základní desky zapnutí počítače.

K probuzení počítače po síti je nutné znát jeho MAC (Media Access Control) adresu, často též nazývanou fyzická adresa. Je to celosvětově jedinečný identifikátor síťového zařízení. MAC adresa je složena ze 48 bitů a nejčastěji se zapisuje jako šestice dvojciferných hexadecimálních čísel oddělených pomlčkou nebo dvojtečkou. Lze ji zjistit u zapnutého počítače vzdáleně např. příkazem `getmac /S <PC>` nebo `nbtstat -a <PC> | find " MAC "`. Další možný způsob je provedení příkazu `ping -n 1 <IP adresa>` a následný dotaz do ARP tabulky (slouží pro překlad IP adres na fyzické adresy) pomocí `arp -a <IP adresa>`, nicméně takový postup je funkční pouze v rámci lokální podsítě.

WOL funguje tak, že z nějakého počítače odešleme speciální paket tzv. *Magic Packet*. Jedná se o standardní paket zaslaný na cílovou adresu, která může být adresou cílové stanice nebo multicastovou (tzn. i broadcast) adresou. Paket obsahuje synchronizační data, což je 6 bytů o hexadecimální hodnotě FF, následovaný 16x zopakovanou MAC adresou cílové stanice (bez oddělovače). Paket se odesílá jako UDP (User Datagram Protocol) a nejčastěji se používá port 7 (Echo) nebo 9 (Discard). [4]

Programů umožňujících WOL existuje celá řada. Např. na [5] je k dispozici zdarma příslušná konzolová utilita (pro použití v příkazovém řádku), objekt COM (využití ve skriptech a programovacích jazycích) a také běžná GUI aplikace. Dále je zde ke stažení

program *Wake On Lan Monitor*, pomocí kterého lze otestovat přijmutí probouzejícího síťového paketu na zapnutém cílovém počítači (obr. 4.1).



Obr. 4.1: Program „Wake On Lan Monitor" po přijmutí probouzejícího paketu

Za zmínku stojí též program *WakeMeOnLan* od NirSoft [6]. Umožňuje oskenovat zadaný rozsah IP adres a načíst MAC adresy zapnutých počítačů, které si následně uloží pro budoucí použití. Když jsou potom počítače vypnuté, lze je probouzet jednotlivě i hromadně.

4.2 Vzdálené vypnutí, restart, odhlášení uživatele

Při vzdálené správě počítačů je často zapotřebí provést jejich vypnutí nebo restart. Občas je také nutné odhlásit přihlášeného uživatele, např. protože by to bránilo automatickému restartu počítače při plánované instalaci aktualizací operačního systému.

Nejjednodušší způsob jak vzdáleně vypnout nebo restartovat počítač je použít program *shutdown.exe*. Jedná se primárně o řádkový příkaz, ale lze vyvolat i grafické uživatelské rozhraní pomocí příkazu `shutdown /i`. Pro vypnutí počítače slouží přepínač /s a pro restart přepínač /r. K provedení akce na vzdáleném počítači stačí přidat přepínač /m \\<*PC*>. Standardně se akce vykoná až po 30 sekundách, avšak toto zdržení lze zcela eliminovat nastavením časového limitu na nulu pomocí přepínače /t 0. Také je možné přidat přepínač /f, který vynutí ukončení spuštěných aplikací bez předchozího upozornění.

Občas je potřeba provést např. restart serveru v nočních hodinách. K tomuto účelu se hodí příkaz *at*, který slouží pro jednoduché naplánování zejména jednorázových akcí pomocí Plánovače úloh. Např. příkaz `at \\<PC> 0:00 shutdown /r` naplánuje na vzdáleném počítači jeho restart o půlnoci téhož dne.

Pro lokální odhlášení uživatele slouží příkaz `shutdown /l`, nejde jej však použít v kombinaci s přepínačem /m k vykonání akce na vzdáleném počítači. Nicméně pro vzdálené odhlášení uživatele lze využít rozhraní WMI prostřednictvím příkazu *wmic*:

```
wmic /node:<PC> OS where Primary=TRUE call Win32ShutDown 0
```

Ve skriptech je možné pro vypnutí, restart nebo odhlášení uživatele použít WMI. Metoda *Win32Shutdown* třídy *Win32_OperatingSystem* přijímá číselný parametr „Flags“, který určuje požadovanou operaci (8=vypnutí, 2=restart, 0=odhlášení uživatele). Pro vynucení operace je možné k hodnotě parametru přičíst číslo 4 (Force flag), čili např. vynucené vypnutí bude mít hodnotu 12. Vynucené vypnutí nebo restart je nezbytné použít např. v případě, že je na počítači přihlášen nějaký uživatel. Následuje ukázka kódu v jazyce VBScript:

```
Set objWMIService = GetObject("winmgmts:\\<PC>\root\CIMV2")
objWMIService.Get("Win32_OperatingSystem=@").Win32Shutdown <Flags>
```

Pro vypnutí nebo restart počítače může posloužit také PowerShell a jeho cmdlety *Stop-Computer* a *Restart-Computer*. Tyto cmdlety využívají též rozhraní WMI. Příkaz pro vzdálené vypnutí počítače může vypadat takto:

```
powershell Stop-Computer <PC>
```

II. PRAKTICKÁ ČÁST

Úvod k praktické části

Úkolem praktické části této práce bylo vytvořit:

1) nástroj pro zobrazení přehledu a informací o zapnutých/vypnutých PC s možností jejich ovládání
2) nástroj pro zobrazení informací a správu jednotlivých vzdálených PC v oblastech: běžící procesy, služby, nainstalovaný software

Nástroje (dále jen programy) jsem vytvořil v aplikaci Microsoft Excel 2010 za pomoci jazyka VBA (Visual Basic for Applications). Jedná se tedy o dokumenty (sešity) aplikace Excel s podporou maker ve formátu *Office Open XML* (soubory *.xlsm). Využil jsem bohaté možnosti formátování, filtrování a seřazování, které Excel nabízí. Při programování jsem používal rozhraní WMI, volání funkcí API a také objekty COM.

První program jsem nazval *OnlinePC* a druhý *AdminPC*. Oba jsou k dispozici na přiloženém CD. K programům jsem vytvořil také uživatelské nápovědy.

Pro funkčnost programů, konkrétně rutin pro ošetření chyb, nesmí být v Excelu nastavena ve VBA volba „Break on All Errors“. Ovšem toto nastavení je nepravděpodobné, protože výchozí volbou je „Break on Unhandled Errors“. Příslušný přepínač je umístěn v editoru „Visual Basic“ na záložce General dialogu Options z menu Tools. [7]

Standardní uživatelské rozhraní Excelu jsem přizpůsobil potřebám programů. Vytvořil jsem vlastní kartu pro pás karet a původní karty Excelu jsem skryl, nicméně v případě potřeby lze všechny karty opět zobrazit použitím skriptu „Upravit pás karet.vbs“ a nastavením atributu „startFromScratch“ na hodnotu „false“. Standardní řádek vzorců je také skrytý. Dále se v programech používá vlastní kontextové menu. Někdy se však mohou hodit volby „Filtr“ a „Seřadit“ ze standardního kontextového menu Excelu. Tyto volby je možné zobrazit přidržením klávesy Ctrl při vyvolání kontextového menu. Standardní kurzor myši Excelu (bílý kříž) měním v programech na běžný symbol šipky. Při tomto nastavení však kurzor myši při pohybu v okně kódu editoru VBA nepříjemně bliká. Změnu kurzoru lze případně zakázat úpravou konstanty „Cursor“ v modulu „Module1“ editoru VBA. Programy se ve výchozím nastavení otevírají v režimu na celou obrazovku (nezobrazuje se pás karet ani stavový řádek).

K vytváření hlavního a kontextového menu využívám vlastní třídu s názvem „Menu“, která používá kolekci *CommandBars*. Hlavní menu se zobrazí po kliknutí na tlačítko „Menu“ v levém horním rohu okna sešitu nebo stisknutím klávesy F10. Pro zobrazování menu

v levém horním rohu okna (nikoliv na pozici myši) jsem musel napsat poměrně složitý kód, který respektuje řadu okolností (velikost a pozici okna, zoom, zobrazení pásu karet, režim zobrazení na celou obrazovku, verzi operačního systému a nastavený motiv).

Většině voleb a funkcí programů jsem přiřadil klávesové zkratky. Jejich přehled je uveden v nápovědách k programům. Všechny klávesové zkratky daného programu jsou zapsané v proceduře *KlavesoveZkratky*, umístěné v modulu „ThisWorkbook“ editoru VBA. Tam je uveden také návod na jejich nastavení. V případě potřeby je možné zkratky upravit a nastavení programu uložit. K nastavení klávesové zkratky v Excelu se používá metoda *Application.OnKey*.

Pro všechny položky hlavního a kontextového menu jsou také nadefinovány přístupové klávesy, které jsou zvýrazněny podtržením daného písmena v názvu položky. Po stisknutí příslušné klávesy se odpovídající položka vykoná. V kódu se tyto přístupové klávesy nastavují přidáním znaku „&“ před dané písmeno v názvu položky.

Při realizaci programů v uživatelském rozhraní Excelu jsem narazil na několik problémů, které se mi ale podařilo úspěšně vyřešit. Jedna potíž však zůstala. Pokud by se uzamknul list (volba „Zamknout list“ na kartě Revize) pro zamezení úprav buněk, nefungovalo by poté seřazování sloupců, ani když se v nastavení uzamčení povolí akce „Seřadit“ a „Použít automatický filtr“. V knize [8] se o tom píše: „V tříděné oblasti uzamknutého listu (včetně nadpisu) nesmí být žádné uzamčené buňky. Stačí, aby byla jedna buňka v seřazované oblasti a už žádné seřazování neproběhne. Excel místo toho zobrazí varovné hlášení o tom, že aby bylo možné seřadit data, musí být všechny buňky odemčeny.“ Uzamknutí listů jsem tedy nepoužil. Do buněk lze normálně psát, avšak potvrzení změn jsem alespoň zamezil pomocí funkce „Ověření dat“ (zobrazí se zpráva „Úprava buněk je zakázána“).

Funkčnost programů jsem testoval v Excelu 2010 32-bit na systémech Windows 7 32-bit a Windows 8 64-bit. Program AdminPC bude funkční i v 64-bitové verzi Excelu, program OnlinePC však nikoliv. Bylo by nutné přinejmenším upravit deklarace všech funkcí API (přidat klíčové slovo „PtrSafe“ a každý pointer a handle změnit na datový typ LongPtr), což jsem nerealizoval. Při psaní kódu jsem využíval nové funkce Excelu, tudíž programy nebudou funkční ve starých verzích 2003 a nižších.

5 OnlinePC

Program OnlinePC slouží pro zobrazení přehledu a informací o zapnutých/vypnutých počítačích s možností jejich ovládání. Umožňuje jednotlivě či hromadně zapínat, vypínat a restartovat počítače nebo odhlašovat uživatele.

Program načítá seznam počítačů dle údajů v souboru se zdrojem počítačů. Výchozím zdrojem počítačů je soubor „ZdrojPC.txt“ (**příloha A**), který je bohatě komentován a obsahuje příklady použití. Vytvořit lze libovolné další soubory s příponou ONL (*.onl) a tuto příponu asociovat s programem „OnlinePC.exe“ pomocí dávkového souboru „Asociace přípony ONL.bat“. Poté je možné takovýto soubor otevřít v programu OnlinePC prostým poklikáním. Soubory se zdrojem počítačů jsou určeny pro zadání:

- změn výchozího nastavení programu
- cest načítaných počítačů z Active Directory
- jmen nebo IP adres počítačů či jiných síťových zařízení

Pro načtení počítačů z Active Directory (dále jen AD) se zadává rozlišovací jméno (Distinguished Name) kontejneru s počítači (např. OU=Computers,DC=firma,DC=cz) nebo přímo ke konkrétnímu počítači (např. CN=PC1,OU=Computers,DC=firma,DC=cz). Přednastaven je prohledávací LDAP filtr pro vyhledání nezakázaných a nainstalovaných počítačů, ovšem lze zadat libovolné další vlastní filtry. Výsledný LDAP filtr je následující: (&(objectCategory=computer)(!userAccountControl:1.2.840.113556.1.4.803:=2)(operatingSystem=*)<*vlastní filtry*>) . Standardně jsou prohledávány i případné podkontejnery (subtree), což lze eventuálně zrušit (nastavit onelevel). K načtení údajů z AD je využita komponenta ADO (ActiveX Data Objects). Načítány jsou tyto atributy:

- name (jméno počítače)
- distinguishedName (rozlišovací jméno objektu počítače)
- description (popis)
- location (umístění)
- operatingSystem (operační systém)
- operatingSystemServicePack (verze opravného balíku)
- whenCreated (datum a čas vytvoření objektu počítače)

Do souboru se zdrojem počítačů lze také zadat přímo jména nebo IP adresy počítačů či jiných síťových zařízení. Přidat je možné také jejich popis a umístění.

Program využívá pro svou činnost mnoho funkcí API a také rozhraní WMI.

Tab. 5.1: Některé funkce API použité v programu

Funkce API	**Knihovna**	**Popis**
WSAStartup	wsock32.dll	inicializace síťového rozhraní socket verze 1.1
gethostbyname	wsock32.dll	zjištění IP adresy
gethostbyaddr	wsock32.dll	zjištění jména počítače
IcmpCreateFile IcmpSendEcho IcmpCloseHandle	icmp.dll	ICMP ping
SendARP	iphlpapi.dll	zjištění MAC adresy
WTSOpenServer WTSEnumerateSessions WTSQuerySessionInformation WTSCloseServer	wtsapi32.dll	zjištění přihlášených uživatelů

V titulku okna programu je uveden počet lokálně přihlášených uživatelů (pouze je-li zobrazení uživatelů zapnuto), počet spuštěných počítačů a celkový počet načtených počítačů vzájemně oddělené lomítkem. Dále se v hranatých závorkách zobrazuje případné jméno souboru se zdrojem počítačů.

5.1 Soubory programu

Program OnlinePC se skládá z následujících souborů:

- OnlinePC.xlsm

Hlavní soubor programu. Jedná se o dokument (sešit) aplikace Excel s podporou maker. Spouští se pomocí „OnlinePC.exe“.

- OnlinePC.exe

Spustitelný soubor, kterým se otevírá „OnlinePC.xlsm“ v oddělené instanci Excelu. Zdrojový kód (Visual Basic 6.0) je umístěn ve složce „Zdrojový kód“. Umožňuje spuštění s parametrem: <*soubor se zdrojem počítačů*>. Po spuštění zkontroluje požadovanou verzi Excelu (2010 32-bit), následně jej spustí a provede patřičná nastavení. Poté v něm otevře soubor „OnlinePC.xlsm“.

- Asociace přípony ONL.bat

Dávkový soubor pro asociaci souborů se zdrojem počítačů (*.onl) s programem „OnlinePC.exe“.

- ZdrojPC.txt (**příloha A**)

Výchozí zdroj počítačů. Soubory se zdrojem počítačů jsou určeny pro zadání načítaných počítačů a pro případnou změnu výchozího nastavení programu. Podrobnosti jsou popsány v úvodní části k programu.

- KontextoveMenu.txt (**příloha B**)

Určeno pro zadání vlastních položek kontextového menu.

- Upravit pás karet.vbs

Tento skript v jazyce VBScript upravuje *pás karet* - kartu „OnlinePC“. Skript nejprve rozbalí ze souboru „OnlinePC.xlsm“ (ZIP archiv formátu Office Open XML) konfigurační XML soubor „customUI\customUI.xml“ a otevře jej v textovém editoru. Následně je možné obsah souboru (kód RibbonX) upravit a při ukončení editoru provedené změny uložit. Pokud byl soubor „customUI.xml“ změněn, dojde k jeho zpětnému zabalení do „OnlinePC.xlsm“. K rozbalení/zabalení souboru se používají běžné systémové prostředky (COM objekt *Shell.Application* a jeho metody), není zapotřebí žádný dodatečný komprimační program.

- Tools

Složka se soubory, které jsou volány z ukázkového vlastního kontextového menu.

- WakeOnLan

Složka s pomocnými soubory pro zapnutí počítačů. Obsahuje níže uvedené soubory.

- WakeOnLan\MAC.csv

Soubor pro uchování načtených MAC adres počítačů.

- WakeOnLan\Masky.txt

Určeno pro zadání IP adres a masek podsítí, které slouží pro zapnutí počítačů v jiné podsíti.

- WakeOnLan\Načíst MAC ze serveru DHCP.bat (**příloha C**)

Dávkový soubor pro načtení MAC adres počítačů ze serveru DHCP. Lze jej spustit přímo (bez spuštěného programu) nebo volbou „Načíst MAC ze serveru DHCP“ z hlavního menu programu. Pro svou činnost potřebuje funkci „Nástroje pro server DHCP“ z balíku „Nástroje pro vzdálenou správu serveru“ (Remote Server Administration Tools). Po spuštění zkontroluje, zda jsou potřebné nástroje k dispozici a případně uživatele vyzve k jejich

instalaci. Pro získání MAC adres ze zjištěných oborů (scope) se používá příkaz `netsh dhcp server \\<server DHCP> scope <adresa oboru> show clients 1`.

- WakeOnLan\WOL.bat

  Pomocný dávkový soubor pro zapnutí počítače.

- WakeOnLan\WolCmd.exe

  Řádková utilita pro zapnutí (probuzení) počítače. Dostupné z [5]. Voláno z dávkového souboru „WOL.bat“.

- Zdrojový kód

  Složka se zdrojovým kódem (Visual Basic 6.0) programu „OnlinePC.exe“.

- Nápověda.xlsx

  Soubor s nápovědou k programu. Jedná se o dokument (sešit) aplikace Excel. Lze jej otevřít přímo nebo vyvolat z hlavního menu programu, z pásu karet nebo klávesou F1.

  Pás karet je pro tento soubor záměrně skrytý. Pro jeho zobrazení je možné ve složce s programem spustit příkaz `"Upravit pás karet.vbs" Nápověda.xlsx` a v zobrazeném textovém editoru změnit na řádce „<ribbon startFromScratch="*true*" />“ hodnotu na „*false*“.

5.2 Sloupce

Program OnlinePC zobrazuje následující sloupce:

- Stav

Zobrazuje stav počítače prostřednictvím barevného symbolu (zelená=zapnuto, červená=vypnuto, žlutá=nedostupné). Stav se zjišťuje s využitím ICMP ping pomocí funkce API *IcmpSendEcho*. Základ kódu jsem převzal z [9]. V převzatém kódu jsem zjistil skrytou chybu v definici datového typu pro ICMP_ECHO_REPLY.DataSize, kterou jsem tedy opravil (změnil jsem Long na Integer). Funkce IcmpSendEcho vrací hodnotu *Reply.Status*. Je-li tato výstupní hodnota SUCCESS (0), je zobrazen zelený symbol. Pro hodnoty REQUEST_TIMED_OUT (11010) a DESTINATION_HOST_UNREACH (11003) je symbol červený. V jiných případech se zobrazí žlutý symbol a v komentáři je uveden popis stavu resp. výsledek odpovědi na ping.

Došlo-li ke změně stavu během posledních 5 minut, je pozadí zvýrazněno černě pomocí podmíněného formátování.

- PC

Sloupec uvádí jméno počítače případně jiného síťového zařízení. Pokud byl počítač načten z AD, je v komentáři uvedeno jeho rozlišovací jméno (atribut *distinguishedName*).

- Popis

Zobrazuje popis počítače načtený z AD (atribut *description*) nebo ze souboru se zdrojem počítačů.

Pokud byl údaj načten z AD, je možno jej ve sloupci upravit a potvrdit klávesou Enter. Tímto se zobrazí dotaz, zda se má upravit záznam v AD. V případě potvrzení se využije rozhraní ADSI (Active Directory Service Interfaces) a metodou *Put* se upraví příslušný atribut objektu počítače. Pro uložení prázdné (vymazané) hodnoty je použita metoda *PutEx* s parametrem ADS_PROPERTY_CLEAR. Nakonec se zápis potvrdí metodou *SetInfo*.

- Umístění

Zobrazuje umístění počítače načtené z AD (atribut *location*) nebo ze souboru se zdrojem počítačů. Pro možnost úpravy hodnoty platí totéž, co bylo popsáno výše u sloupce „Popis“.

- Operační systém

Udává název operačního systém a verzi opravného balíku (SP) načtené z AD (atributy *operatingSystem* a *operatingSystemServicePack*). Pokud není počítač načten z AD, je u zapnutého počítače odvozen typ systém (zda se jedná o Windows či nikoliv) od hodnoty TTL - viz sloupec „TTL“. Systém Windows používá jako výchozí TTL hodnotu 128, kdežto jiné operační systémy či síťová zařízení používají zpravidla hodnoty 64, 192 nebo 255.

- Vytvořeno

Zobrazuje datum a čas vytvoření objektu počítače v AD (atribut *whenCreated*).

- IP adresa

Zobrazuje IP adresu počítače. Adresa se zjišťuje ze jména počítače pomocí funkce API *gethostbyname*. Její platné přidělení počítači se poté ověřuje zpětným získáním jména pomocí funkce API *gethostbyaddr*. Je-li zjištěn rozpor, je IP adresa označena světlou barvou a ve sloupci „Stav“ se zobrazí žlutý symbol s komentářem „Zjištěná IP adresa je již přidělena pro <*jméno počítače*>“.

- Odezva

Doba odezvy na ping v milisekundách (výstupní hodnota *Reply.RoundTripTime* funkce IcmpSendEcho). Odezva větší než 5 ms je zvýrazněna červeně pomocí podmíněného formátování.

- TTL

Udává hodnotu „Time To Live“ (výstupní hodnota *Reply.Options.TTL* funkce IcmpSendEcho). Je to číslo, které omezuje počet průchodů paketů skrz směrovače resp. určuje maximální dobu existence paketu. Výchozí hodnota TTL (zpravidla 64, 128, 192 nebo 255) je snížena o jedničku při každém průchodu směrovačem. Systém Windows používá jako výchozí hodnotu 128.

- Hop

Počet průchodů směrovači. Vypočteno jako rozdíl odhadnutého výchozího TTL a hodnoty TTL v přijaté odpovědi na ping. Počítač ve stejné podsíti má hodnotu hop nula. Nenulová hodnota je zvýrazněna červeně pomocí podmíněného formátování.

- MAC adresa

Zobrazuje MAC (Media Access Control) adresu síťového rozhraní počítače. Pro počítač v lokální podsíti se MAC adresa zjišťuje s využitím protokolu ARP pomocí funkce API *SendARP*. Pro počítač se systémem Windows v jiné podsíti je využit protokol NetBIOS prostřednictvím skrytě spuštěného příkazu `nbtstat -A <IP adresa>`. Ve výchozím nastavení programu (ZjistovatMAC=2) jsou zjišťovány pouze dosud nezjištěné MAC adresy. Případné vypnuté zjišťování (ZjistovatMAC=0) je zvýrazněno šedou barvou pozadí. Adresy lze také načíst z DHCP serveru pomocí volby „Načíst MAC ze serveru DHCP“ z hlavního menu. Jednotlivé adresy je též možné ve sloupci ručně přidávat nebo upravovat. MAC adresy se ukládají do souboru „WakeOnLan\MAC.csv“ pro budoucí použití (zapínání počítačů).

- Uživatel

Zobrazuje jméno a případně odlišnou doménu lokálně přihlášeného uživatele. Není-li přihlášen žádný lokální uživatel, je pole prázdné. Pokud se uživatele nepodařilo zjistit (např. z důvodu nedostatečného oprávnění), zobrazí se text „(Nezjištěno)“. Ve výchozím nastavení programu (ZjistovatUzivatele=2) jsou uživatelé zjišťováni na běžných stanicích pomocí vlastnosti *UserName* WMI třídy *Win32_ComputerSystem* a na serverových systémech s využitím funkcí API *WTSEnumerateSessions* a *WTSQuerySessionInformation* (umístěny v modulu „Sessions“ editoru VBA). Při použití WMI (zvýrazněno šedou barvou pozadí) je zjištěn pouze lokálně přihlášený uživatel. Jsou-li použity funkce API, objeví se v komentáři také případná jména vzdáleně přihlášených uživatelů včetně jména počítače, z něhož jsou připojeni. Pokud je uživatel aktuálně odpojen, zobrazí se text „odpojen“.

Pro funkčnost zmíněných funkcí API však musí být na cílovém počítači povoleno *vzdálené volání procedur* (RPC). V serverových verzích Windows je toto standardně povoleno, ale na běžných stanicích je nutné provést příslušné nastavení v registru. K nastavení vzdáleného počítače lze použít následující příkaz:

```
reg add "\\<PC>\HKLM\SYSTEM\CurrentControlSet\Control\Terminal
 Server" /v AllowRemoteRPC /t REG_DWORD /d 1 /f
```

Pokud je v programu nastaveno zjišťování uživatelů pomocí funkcí API (ZjistovatUzivatele=1) a cílový počítač nemá povoleno vzdálené RPC, zobrazí se ve sloupci text „(Zakázané RPC)“.

Zjišťování a zobrazení uživatelů lze zapnout/vypnout volbou „Zobrazit uživatele“ v hlavním menu.

- Posl. obnovení

  Zobrazuje čas posledního obnovení údajů.

- Posl. změna stavu

  Zobrazuje čas poslední změny, ke které došlo ve sloupci „Stav“. Změna vzniklá během posledních 5 minut je zvýrazněna oranžovou barvou pozadí a změna během poslední hodiny žlutou barvou. Intenzita barvy pozadí je dána blízkostí času změny.

- Čas operace

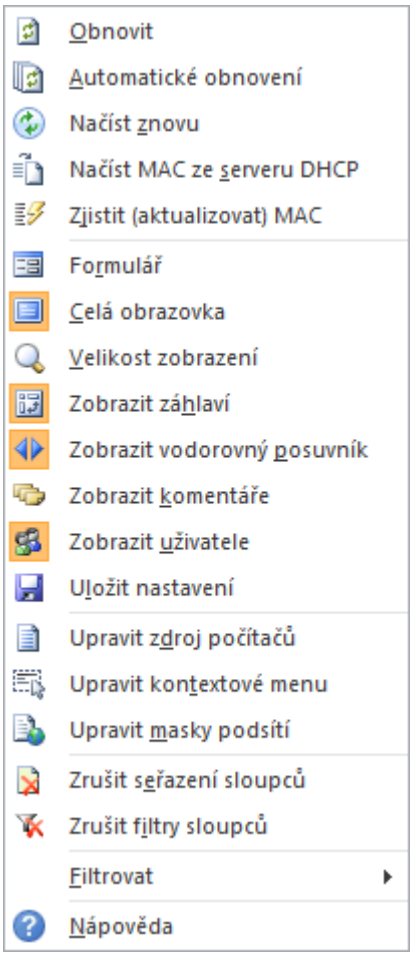
  Zobrazuje čas naposledy provedené operace. Zvýrazňování je stejné jako u sloupce „Posl. změna stavu“.

- Provedená operace

  Název provedené operace (Zapnout, Vypnout, Restartovat, Odhlásit uživatele). V komentáři je uvedena případná chyba nebo upozornění. Při chybě je název operace zvýrazněn červeně.

5.3 Hlavní menu

Hlavní menu obsahuje důležité volby pro ovládání programu. Menu se zobrazí po kliknutí na tlačítko „Menu“ v levém horním rohu okna sešitu nebo stisknutím klávesy F10.



Obr. 5.1: Hlavní menu programu OnlinePC

Popis položek hlavního menu:

- Obnovit

Slouží pro ruční obnovení (znovunačtení) údajů. Probíhající obnovení lze přerušit přidržením klávesy „Escape“. Během obnovení nefungují klávesové zkratky, nicméně funkce programu lze případně vyvolat pomocí hlavního nebo kontextového menu či pásu karet.

- Automatické obnovení

Tato volba zapíná/vypíná automatické obnovování údajů. Zapnutí je indikováno červenou barvou hlavičky sloupců a znakem „~“ v titulku okna. Funkce provádí postupné obnovování jednotlivých počítačů (standardně obnoví každé dvě sekundy jeden). K zajištění spouštění obnovovací procedury se využívá metoda Excelu *Application.OnTime*.

- Načíst znovu

  Znovu načte zdroj počítačů. Využitelné např. po úpravě souboru se zdrojem počítačů.

- Načíst MAC ze serveru DHCP

  Načte MAC adresy počítačů ze serveru DHCP s využitím dávkového souboru „WakeOnLan\Načíst MAC ze serveru DHCP.bat“.

- Zjistit (aktualizovat) MAC

  Zjistí či aktualizuje MAC adresy všech nebo vybraných počítačů i v případě, že není nastaveno: ZjistovatMAC=1 (zjišťování MAC adres - vždy).

- Formulář

  Využívá se nástroj Excelu nazvaný *Formulář*, který zobrazuje jednotlivé položky (řádky) seznamu v přehledném okně ve formě formuláře. Položky seznamu lze postupně procházet a případně i filtrovat nastavením kritérií tlačítkem „Kritéria“.

  Formulář jde vyvolat prostřednictvím `ActiveSheet.ShowDataForm`, ovšem v tomto případě se datum zobrazuje v americkém formátu <*měsíc*>/<*den*>/<*rok*>. Řešením je otevřít formulář pomocí `Application.CommandBars.ExecuteMso` **`"DataFormExcel"`** případně `Application.CommandBars.FindControl(ID:=`**`860`**`).Execute`.

  V Excelu bohužel neexistuje možnost, jak při otevření formuláře rovnou zobrazit konkrétní položku seznamu, vždy se zobrazí první položka. Tento problém jsem vyřešil tak, že se po otevření formuláře odešle patřičný počet virtuálních stisků klávesy „Page Down“ (posun po 10 záznamech) a klávesy „šipka dolů“ (posun po 1 záznamu). Odeslání stisků kláves zajišťuje dočasný pomocný skript „%TEMP%\Formular.vbs“, který je vytvářen a spouštěn následujícím řádkem kódu (proměnná s názvem „Pozice“ udává číslo záznamu, který má být zobrazen):

```
Shell "cmd /V:ON /C set F=%TEMP%\Formular.vbs & echo With
 CreateObject(""WScript.Shell""): .SendKeys ""{PGDN " & Pozice \ 10
 & "}"": .SendKeys ""{DOWN " & Pozice Mod 10 & "}"": End With>!F! &
 wscript !F! & del !F!", vbHide
```

- Celá obrazovka

  Pomocí této volby lze zapnout/vypnout zobrazení na celou obrazovku. Ve výchozím nastavení se program spouští na celé obrazovce (nezobrazuje se pás karet ani stavový řádek), nicméně celoobrazovkové zobrazení je možné vypnout a nastavení programu uložit.

Při zobrazení na celou obrazovku se skryje pás karet pomocí příkazu `Application.ExecuteExcel4Macro "Show.ToolBar(""Ribbon"", False)"` a stavový řádek pomocí `Application.DisplayStatusBar = False`.

- Velikost zobrazení

  Otevře standardní dialogové okno „Lupa“ pro nastavení úrovně zvětšení dokumentu.

- Zobrazit záhlaví

  Zapne/vypne zobrazení záhlaví řádků a sloupců.

- Zobrazit vodorovný posuvník

  Zapne/vypne zobrazení vodorovného posuvníku.

- Zobrazit komentáře

  Umožňuje zapnout/vypnout zobrazení všech komentářů. Jedná se o standardní funkci Excelu, která je běžně dostupná přes volbu „Zobrazení všech komentářů“ na kartě „Revize“.

- Zobrazit uživatele

  Tato volba zapne/vypne zjišťování a zobrazení přihlášených uživatelů (viz sloupec „Uživatel“).

- Uložit nastavení

  Uloží provedené změny a nastavení programu do souboru „OnlinePC.xlsm“. V podstatě se jedná o standardní uložení souboru v Excelu, ovšem před uložením se nejprve odstraní aktuálně načtené údaje a po uložení souboru se opět obnoví. Možnosti přizpůsobení a nastavení programu jsou uvedeny v nápovědě.

- Upravit zdroj počítačů

  Otevře soubor se zdrojem počítačů v textovém editoru.

- Upravit kontextové menu

  Otevře soubor „KontextoveMenu.txt“ v textovém editoru.

- Upravit masky podsítí

  Otevře soubor „WakeOnLan\Masky.txt“ v textovém editoru.

- Zrušit seřazení sloupců

  Zruší uživatelské seřazení sloupců a obnoví výchozí seřazení podle pořadí načtení.

- Zrušit filtry sloupců

  Vymaže všechny nastavené filtry.

- Filtrovat

  Rozbalovací nabídka obsahuje následující předvolené filtry:

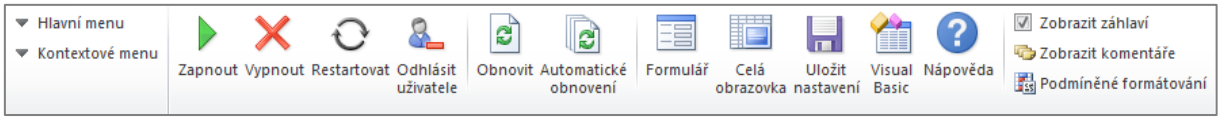
  - Zapnuté počítače
  - Vypnuté nebo nedostupné počítače
  - Přihlášení uživatelé
  - Zapnuté počítače bez přihlášených uživatelů

- Nápověda

  Zobrazí nápovědu k programu (otevře soubor „Nápověda.xlsx“).

5.4 Pás karet

Karta „OnlinePC“ na pásu karet obsahuje některé položky hlavního menu programu a navíc další volby: *Visual Basic* (editor VBA), *Podmíněné formátování*. Umožňuje vyvolat hlavní menu a také kontextové menu vybraného záznamu. Ovšem při zobrazení programu na celou obrazovku (volba „Celá obrazovka“) není pás karet dostupný.



Obr. 5.2: Pás karet - karta OnlinePC

Konfigurační soubor „customUI.xml“ (kód RibbonX) pásu karet je možné upravit pomocí skriptu „Upravit pás karet.vbs“. Obsah konfiguračního souboru je v **příloze D**. Standardní karty Excelu jsou záměrně skryty, ale lze je případně ve zmíněném konfiguračním souboru povolit nastavením atributu „startFromScratch“ na hodnotu „false“.

Pro pás karet jsou nadefinovány procedury zpětného volání, umístěné v modulu „Module1“ editoru VBA:

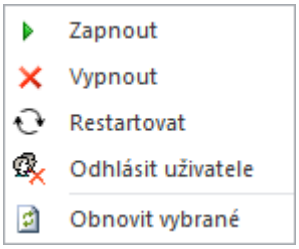
```
Sub RibbonOnLoad(Ribbon As IRibbonUI)
  'přepnutí na kartu programu (nutné při zakázání startFromScratch)
  Ribbon.ActivateTab "MyCustomTab"
End Sub

Sub RibbonAction(Control As IRibbonControl)
  'spuštění procedury dle stisknutého tlačítka
  Application.Run Control.ID
End Sub
```

5.5 Kontextové menu

Kontextové menu programu OnlinePC obsahuje standardní položky a případně také vlastní položky uložené v souboru „KontextoveMenu.txt“.

Je-li vybráno více počítačů, zobrazí se po zvolení položky z menu dotaz, zda se má operace provést pro všechny vybrané počítače. Výběr více počítačů se provádí standardním způsobem pomocí myši v kombinaci s klávesami Ctrl nebo Shift. Postačí vybrat jen jedinou buňku v řádku. Pro výběr všech zobrazených počítačů lze použít zkratku Ctrl+A. Zrušení výběru konkrétního počítače se provede kliknutím za současného držení kláves Ctrl a Alt.

5.5.1 Standardní položky



Obr. 5.3: Standardní položky kontextové menu

- Zapnout

Pro zapnutí počítačů se používá technologie *Wake on LAN* (viz kapitola **4.1**). Musí být známa MAC adresa cílového počítače a pro počítač v jiné podsíti je zapotřebí zjistit také jeho IP adresu a masku. Potřebné soubory a nástroje jsou umístěny ve složce „WakeOnLan“. Zapnutí zajišťuje pomocný dávkový soubor „WOL.bat“, který se spouští s parametry: <*MAC*> [<*IP*> <*MASKA*>]. Pro zapínání počítačů v jiných podsítích je nutné zadat masky podsítí do souboru „Masky.txt“ např. volbou „Upravit masky podsítí“ v hlavním menu.

- Vypnout / Restartovat / Odhlásit uživatele

Pro vypnutí, restart nebo odhlášení uživatele se používá rozhraní WMI. Metoda *Win32Shutdown* třídy *Win32_OperatingSystem* přijímá číselný parametr „Flags“, který určuje požadovanou operaci (8=vypnutí, 2=restart, 0=odhlášení uživatele). Pokud je před vypnutím nebo restartem počítače přihlášen nějaký uživatel, zobrazí se dotaz, zda se má pokračovat. V případě kladné odpovědi je použito vynucení operace (přidán Force flag).

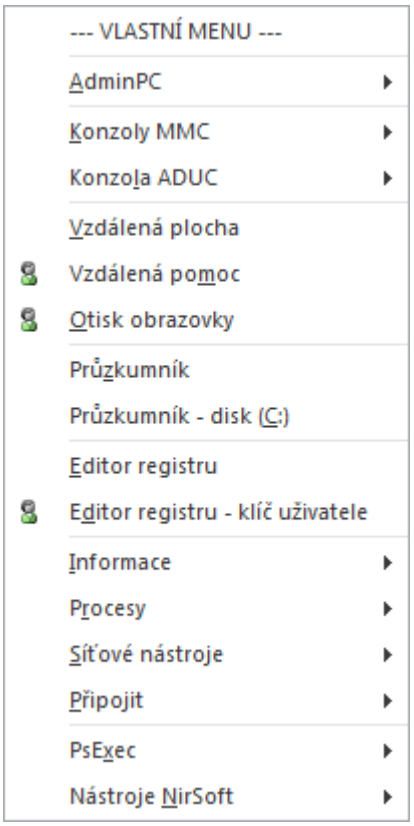
- Obnovit vybrané

Obnoví pouze vybrané počítače.

5.5.2 Vlastní položky

Do kontextového menu lze přidat libovolné vlastní položky. Pro zadání vlastních položek slouží soubor „KontextoveMenu.txt“, který je možné otevřít např. volbou „Upravit kontextové menu“ v hlavním menu. Při úpravě souboru za běhu programu se uložené změny po vyvolání kontextového menu ihned promítnou. Do souboru se zadává název položky menu, příkaz a případně také styl okna či klávesová zkratka. V parametrech příkazu lze uvést zástupný výraz pro počítač (%PC% případně !PC!) a uživatele (%USER%). Položky související s přihlášeným uživatelem mají v menu ikonu se symbolem uživatele.

Soubor „KontextoveMenu.txt“ (**příloha B**) již obsahuje několik ukázkových položek kontextového menu (obr. 5.4). Používá nástroje, které jsou umístěny ve složce „Tools“ nebo jsou standardní součástí Windows. Umožňuje např. vyvolat příslušnou funkci programu AdminPC (viz kapitola **6 AdminPC**). Dále lze kupříkladu zobrazit vlastnosti objektu počítače nebo uživatele v konzole ADUC (Active Directory Users and Computers). Využívá také utilitu PsExec ze sady PsTools (viz kapitola **2 Nástroje PsTools**) a několik nástrojů od NirSoft [6].



Obr. 5.4: Ukázka vlastních položek kontextového menu

6 AdminPC

Program AdminPC slouží pro zobrazení informací a správu jednotlivých vzdálených počítačů v oblastech: běžící procesy, služby, nainstalovaný software. Využívá rozhraní WMI, tudíž na vzdáleném počítači není potřeba instalovat žádného pomocného klienta (službu) ani provádět speciální nastavení, kromě případného povolení WMI (resp. DCOM a RPC) v používaném firewallu. Pro přístup na vzdálený počítač je nutné administrátorské oprávnění (členství uživatele ve skupině „Administrators“ na cílovém počítači), v opačném případě program nabídne možnost zadat potřebné přístupové údaje (uživatelské jméno a heslo).

6.1 Soubory programu

Program se skládá z následujících souborů:

- AdminPC.xlsm

Hlavní soubor programu. Jedná se o dokument (sešit) aplikace Excel s podporou maker. Obsahuje listy Procesy, Služby a Software. Po jeho otevření a povolení spuštění maker dojde k načtení informací na výchozím listu (standardně Procesy) pro lokální počítač.

- AdminPC.bat

Dávkový soubor pro otevření programu na zvoleném listu a připojení k zadanému počítači. Umožňuje spuštění s parametry: {<*LIST*>|zadat} [<*PC*>|localhost] , kde *LIST* je default|Procesy|Služby|Software nebo 0|1|2|3 (např. příkaz `AdminPC.bat Software PC1` otevře program na listu Software a připojí se k počítači PC1). Při jeho spuštění bez parametrů se zobrazí výzva k zadání jména počítače a zvolení funkce (listu).

Tento dávkový soubor nejprve kontroluje dostupnost vzdáleného počítače příkazem `ping -n 1 -w 1 <PC>`. Poté vytvoří dočasný soubor „%TEMP%\AdminPC.par“ s parametry (list, počítač, složka programu). Dále otevře soubor „AdminPC.xlsm“ v Excelu pomocí skriptu „AdminPC.vbs“. Spuštěný program načte dočasný soubor s parametry a zobrazí požadované údaje (zvolený list pro zadaný počítač).

- AdminPC.vbs

Pomocný skript v jazyce VBScript pro otevření souboru v Excelu. Skript je volán z „AdminPC.bat“.

- AdminPC_Spustit jako správce.bat

Dávkový soubor pro spuštění programu se zvýšeným oprávněním. Nutné použít pro práci s lokálním počítačem ve Windows Vista a výše, protože obsahují bezpečnostní nástroj *Řízení uživatelských účtů* (UAC), jinak se program spustí s oprávněním běžného uživatele, což způsobí omezenou funkčnost programu. Pro práci se vzdáleným počítačem toto omezení neplatí. Ke spuštění se zvýšeným oprávněním se používá utilita *nircmd.exe* (popsáno níže). Obsah dávkového souboru vypadá následovně:

```
@"%~dp0\Tools\nircmd.exe" elevate excel "%~dp0\AdminPC.xlsm"
```

- Upravit pás karet.vbs

Tento skript v jazyce VBScript upravuje *pás karet* - kartu „AdminPC“. Podrobný popis je uveden u stejného souboru programu OnlinePC.

- Tools\OpenInRegedit.vbs

Pomocný skript v jazyce VBScript pro otevření zadaného klíče registru v programu *Editor registru* (regedit.exe). Spouští se při volbě „Otevřít záznam v Editoru registru“ z kontextového menu na listu Služby a Software. Umožňuje spuštění s parametry: {<*PC*>|localhost|""} [<*klíč registru*>].

V případě lokálního počítače pouze upraví hodnotu „LastKey“ v klíči „HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Applets\Regedit“ a spustí novou instanci Editoru registru příkazem `regedit /m`.

Pro práci s registrem na vzdáleném počítači je nutné, aby na něm byla spuštěna služba RemoteRegistry (Vzdálený registr). V současných verzích Windows je tato služba standardně zastavena (nastaven ruční typ spouštění). Při otevírání klíče registru vzdáleného počítače skript kontroluje, zda je potřebná služba spuštěna. Pokud neběží, provede její spuštění. Je-li služba zakázána, zobrazí se dotaz, zda se má dočasně povolit. Poté se do Editoru registru odešlou virtuální stisky kláves (pomocí funkce SendKeys objektu WScript.Shell), které vyvolají z menu „Soubor“ volbu „Připojit síťový registr“ a zadají jméno počítače. Tímto dojde k připojení registru tohoto vzdáleného počítače. Nakonec se zobrazí požadovaný klíč spuštěním příkazu `nircmd regedit <klíč registru>`.

- Tools\nircmd.exe

Pomocný program pro „OpenInRegedit.vbs“ a „AdminPC_Spustit jako správce.bat“. Jedná se o řádkovou utilitu od NirSoft [6], která je dostupná zdarma na adrese

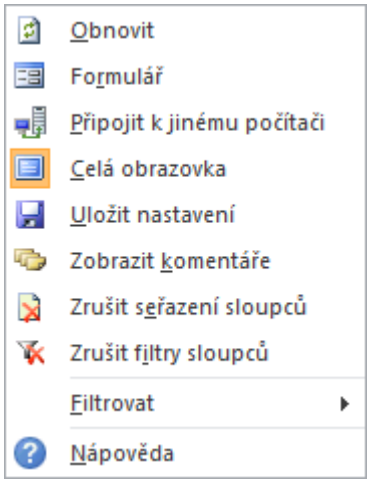
http://www.nirsoft.net/utils/nircmd.html. Poskytuje velké množství různorodých funkcí při velmi malé velikosti souboru 43 kB. Ve skriptu „Tools\OpenInRegedit.vbs“ je využita v případě přístupu k vzdálenému počítači pro úpravu titulku okna Editoru registru (příkaz `nircmd win settext foreground <titulek>`) a pro otevření klíče registru (příkaz `nircmd regedit <klíč registru>`). V dávkovém souboru „AdminPC_Spustit jako správce.bat“ se používá k otevření souboru „AdminPC.xlsm“ v Excelu se zvýšeným oprávněním (příkaz `nircmd elevate excel "%~dp0\AdminPC.xlsm"`).

- Nápověda.xlsx

Soubor s nápovědou k programu. Jedná se o dokument (sešit) aplikace Excel. Lze jej otevřít přímo nebo vyvolat z hlavního menu programu, z pásu karet nebo klávesou F1.

6.2 Hlavní menu

Hlavní menu obsahuje důležité volby pro ovládání programu. Většina položek menu je společná pro všechny listy (Procesy, Služby, Software), pouze jeho spodní část se mění v závislosti na vybraném listu. Menu se zobrazí po kliknutí na tlačítko „Menu“ v levém horním rohu okna sešitu nebo stisknutím klávesy F10.



Obr. 6.1: Hlavní menu programu AdminPC

Popis položek hlavního menu:

- Obnovit

Slouží pro ruční obnovení (znovunačtení) údajů na aktuálním listu. Při přepnutí na jiný list probíhá obnovení automaticky.

- Formulář

Využívá se nástroj Excelu nazvaný *Formulář*, který zobrazuje jednotlivé položky (řádky) seznamu v přehledném okně ve formě formuláře. Položky seznamu lze postupně procházet a případně i filtrovat nastavením kritérií tlačítkem „Kritéria“. Dále platí totéž, co je uvedeno pro stejnou volbu programu OnlinePC.

- Připojit k jinému počítači

Tato volba umožňuje zadat jméno počítače, se kterým se má pracovat. Pokud se nevyplní žádné jméno, bude se pracovat s lokálním počítačem. Před připojením k vzdálenému počítači se neprovádí kontrola jeho dostupnosti (ping), rovnou se vytváří objekt pro práci s WMI pomocí `Set WMI = GetObject("winmgmts:\\<PC>\root\.....")`. Je-li připojení úspěšné, načtou se příslušné údaje. V opačném případě se zobrazí zpráva „Počítač

není dostupný“. Pokud vznikne chyba „přístup byl odepřen“ (tj. uživatel, pod nímž program běží, nemá pro přístup k vzdálenému počítači náležité oprávnění), nabídne se možnost zadat potřebné přístupové údaje (uživatelské jméno a heslo) a použije se alternativní způsob připojení pomocí `Set WMI = CreateObject("WbemScripting.SWbemLocator"). ConnectServer(<PC>, "root\……", <uživatelské jméno>, <heslo>)`. Bylo-li připojení úspěšné, zobrazí se dotaz, zda se mají zapamatovat přístupové údaje pro aktuální sezení (tj. po dobu běhu programu).

- Celá obrazovka

Pomocí této volby lze zapnout/vypnout zobrazení na celou obrazovku. Ve výchozím nastavení se program spouští na celé obrazovce (nezobrazuje se pás karet ani stavový řádek), nicméně celoobrazovkové zobrazení je možné vypnout a nastavení programu uložit. Režim na celou obrazovku se aktivuje pomocí `Application.DisplayFullScreen = True` a je platný pro všechny otevřené soubory (dokumenty) v dané instanci Excelu. Při přepnutí na jiný dokument se proto prostřednictvím události *Workbook_Deactivate* zobrazení na celou obrazovku vypne a při opětovném aktivování okna programu se pomocí události *Workbook_Activate* znovu zapne. Je-li v Excelu otevřen jen jeden soubor, tak se bohužel celoobrazovkový režim po minimalizaci okna a jeho následném obnovení deaktivuje. Toto nežádoucí chování jsem odstranil vytvořením vlastní procedury, která vhodně nastavuje stav zobrazení okna sešitu (`ActiveWindow.WindowState = ……`), aby při obnovení okna z minimalizace zareagovala událost *Workbook_WindowResize*, která obnoví zobrazení na celou obrazovku.

- Uložit nastavení

Uloží provedené změny a nastavení programu do souboru „AdminPC.xlsm“. V podstatě se jedná o standardní uložení souboru v Excelu, ovšem před uložením se nejprve odstraní ze všech listů aktuálně načtené údaje a po uložení souboru se opět obnoví. Možnosti přizpůsobení a nastavení programu jsou uvedeny v nápovědě.

- Zobrazit komentáře

Umožňuje zapnout/vypnout zobrazení všech komentářů. Jedná se o standardní funkci Excelu, která je běžně dostupná přes volbu „Zobrazení všech komentářů“ na kartě „Revize“. Nastavení je trvalé a platné i pro ostatní dokumenty Excelu.

- Zrušit seřazení sloupců

  Zruší uživatelské seřazení sloupců a obnoví výchozí seřazení aktuálního listu (list Procesy seřadí podle sloupce „Čas spuštění“, list Služby podle sloupce Služba/Ovladač a list Software dle sloupce Software).

- Zrušit filtry sloupců

  Vymaže všechny nastavené filtry na aktuálním listu.

- Filtrovat

  Rozbalovací nabídka, která obsahuje předvolené filtry pro aktuální list.

- *Specifické položky pro vybraný list*

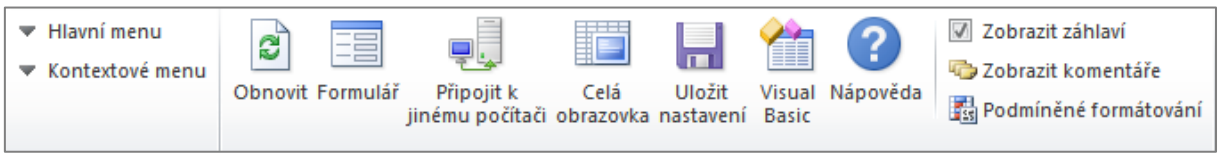
  Na listu Procesy jsou položky „Automatické obnovení“ a „Spustit příkaz“, na listu Služby potom „Otevřít konzolu Služby“ a „Zobrazit ovladače“.

- Nápověda

  Zobrazí nápovědu k aktuálnímu listu (otevře soubor „Nápověda.xlsx“ a zobrazí příslušný list).

6.3 Pás karet

Karta „AdminPC“ na pásu karet obsahuje některé položky hlavního menu programu a navíc další volby: *Visual Basic* (editor VBA), *Zobrazit záhlaví* (zapnutí/vypnutí záhlaví řádků a sloupců aktuálního listu), *Podmíněné formátování*. Umožňuje vyvolat hlavní menu a také kontextové menu vybraného záznamu. Ovšem při zobrazení programu na celou obrazovku (volba „Celá obrazovka“) není pás karet dostupný.



Obr. 6.2: Pás karet - karta AdminPC

Konfigurační soubor „customUI.xml“ (kód RibbonX) pásu karet je možné upravit pomocí skriptu „Upravit pás karet.vbs“. Dále platí totéž, co je uvedeno pro pás karet programu OnlinePC.

6.4 List Procesy

Zobrazuje běžící procesy a poskytuje o nich důležité údaje. Umožňuje provádět operace: ukončení procesu, ukončení stromu procesu, nastavení priority. Nabízí též možnost spustit příkaz (proces), sledovat jeho běh a po ukončení procesu zobrazit návratový kód a případně také výstup. Dále lze zapnout automatické obnovování údajů. V titulku okna se zobrazuje počet spuštěných procesů a aktuální využití procesoru (CPU).

K práci s procesy se používá WMI třída *Win32_Process* z jmenného prostoru „root\CIMV2“.

Tab. 6.1: Vlastnosti a metody třídy Win32_Process použité v programu

Vlastnost	**Popis**
Name	jméno procesu
ExecutablePath	cesta k spustitelnému souboru procesu
ProcessId	identifikátor procesu, který jednoznačně identifikuje proces
ParentProcessId	identifikátor rodičovského procesu
Priority	označuje plánovací prioritu procesu v operačním systému
SessionId	číslo označující vlastníka procesu
CommandLine	příkazový řádek použitý ke spuštění procesu
KernelModeTime, UserModeTime	spotřebovaný strojový čas ve stovkách nanosekund; celkový strojový čas využitý procesem se získá sečtením hodnot těchto dvou vlastností
PrivatePageCount	velikost paměti používané procesem, kterou nelze sdílet s jinými procesy (soukromá pracovní sada)
ReadTransferCount	objem přečtených dat z disku
WriteTransferCount	objem zapsaných dat na disk
CreationDate	datum a čas spuštění procesu
Metoda	
GetOwner	načte uživatelské jméno a název domény, pod nimiž je proces spuštěn
SetPriority	nastaví prioritu procesu
Terminate	ukončí proces
Create	vytvoří nový proces

6.4.1 Sloupce

Sloupce na listu Procesy jsou následující:

- Proces

Zobrazuje jméno procesu (vlastnost *Name*), což je spustitelný soubor, většinou *.exe. V komentáři je uvedena plná cesta k souboru procesu (vlastnost *ExecutablePath*). Sloupec obsahuje také speciální proces s názvem *Nečinné procesy systému* (System Idle Process),

který vyjadřuje procento doby nečinnosti procesoru a dále proces *System*, zastupující jádro operačního systému.

Proces *WmiPrvSE.exe*, běžící pod uživatelem „NT AUTHORITY\NETWORK SERVICE“, je používán tímto programem v souvislosti s využíváním rozhraní WMI, proto se u něj vždy zobrazuje určité procento využití CPU. Je označen světlou barvou. Po 1,5 minutě nevyužívání se tento proces automaticky ukončuje a při opětovném využití WMI (např. obnovení údajů) se znovu spouští.

Při obnovení údajů jsou nově spuštěné procesy zvýrazněny zelenou barvou pozadí a ukončené procesy červenou barvou pozadí. Procesy služeb jsou označeny oranžovým vzorkem pozadí. Zda se jedná o službu se určuje (až na výjimky) dle rodičovského procesu, kterým je u služeb proces *services.exe*. Dále jsou zvýrazněny modrou barvou procesy, jejichž jméno je uvedené v souboru „Procesy\ZvýraznitProces.txt“, který je možné upravovat dle potřeby.

Je-li nastaveno výchozí seřazování sloupců, dojde po spuštění programu k aktivování poslední řádky seznamu, obsahující naposledy spuštěný proces.

- PID

Udává identifikátor procesu (vlastnost *ProcessId*), který jednoznačně identifikuje proces. Má-li proces nějaké potomky (tj. z procesu byly spuštěny další procesy), zobrazuje se PID tučně. Pro aktuálně vybraný proces (označený řádek) je PID jeho přímého rodiče zvýrazněno červeně a PID rodičů tohoto přímého rodiče je zvýrazněno fialovou barvou. Zvýrazňování se dynamicky mění dle vybraného procesu. Tímto zvýrazňováním se částečně nahrazuje zobrazení procesů ve formě stromové struktury, kterou poskytují některé programy pro správu procesů (např. „Process Explorer“ od Marka Russinoviche, který je dostupný zdarma na adrese http://technet.microsoft.com/sysinternals/bb896653.aspx).

- PPID

Udává identifikátor rodičovského procesu (vlastnost *ParentProcessId*). Pokud již rodičovský proces neběží, zobrazuje se PPID světlou barvou. Pro aktuálně vybraný proces je PPID jeho přímých potomků zvýrazněno červeně a PPID potomků těchto přímých potomků je zvýrazněno fialovou barvou. Zvýrazňování se dynamicky mění dle vybraného procesu.

- Priorita

Označuje plánovací prioritu procesu v operačním systému (vlastnost *Priority*). Může nabývat těchto hodnot: 4=nízká, 6=nižší než normální, 8=*normální*, 10=vyšší než normální, 13=vysoká, 24=reálný čas. Výchozí normální priorita je 8 (označeno světlou barvou). Vyšší/nižší priorita je označena symbolem šipky nahoru/dolů pomocí podmíněného formátování. Důležité systémové procesy (smss.exe, csrss.exe, wininit.exe, services.exe, lsass.exe, winlogon.exe) mají vyšší prioritu a naopak např. procesy pro indexování souborů (SearchProtocolHost.exe, SearchFilterHost.exe) či procesy spuštěné pomocí *Plánovače úloh* mají prioritu nižší. Prioritu procesu lze změnit volbou „Nastavit prioritu“ v kontextovém menu.

- Uživatelské jméno

Sloupec zobrazuje uživatelský účet, pod nímž je proces spuštěn. Uživatelské jméno a název domény se získává pomocí metody *GetOwner*.

Uživatelské jméno lokálně přihlášeného uživatele (Interactive) je zvýrazněno zeleně a jméno uživatele připojeného přes vzdálenou plochu (RemoteInteractive) je zvýrazněno červeně. Toto se zjišťuje dle číselné hodnoty vlastnosti *LogonType* (2=Interactive, 10=RemoteInteractive) WMI třídy *Win32_LogonSession*. Pro funkčnost musí být cílový systém Windows verze Vista nebo novější. Propojení mezi třídami *Win32_Process* a *Win32_LogonSession* zajišťuje asociační třída *Win32_SessionProcess*. WQL dotaz pro WMI metodu *ExecQuery* vypadá takto:

```
ASSOCIATORS OF {Win32_Process=<PID>} WHERE
 ResultClass=Win32_LogonSession AssocClass=Win32_SessionProcess
```

- Relace

Číslo označující vlastníka procesu (vlastnost *SessionId*). Jestliže je přihlášeno více uživatelů, má každý z nich jedinečné číslo relace. Většina systémových procesů má relaci 0 (označeno světlou barvou). Šířka sloupce je standardně minimální.

- Příkazový řádek

Uvádí příkazový řádek použitý ke spuštění procesu (vlastnost *CommandLine*). Příkaz spuštěný volbou „Spustit příkaz“ nebo odinstalace software vyvolaná z listu Software volbou „Odinstalovat“ jsou zvýrazněny žlutou barvou pozadí v tomto sloupci.

- CPU

Zobrazuje průměrné využití procesoru (CPU) daným procesem od posledního obnovení. Intenzita barvy pozadí je dána velikostí hodnoty pomocí podmíněného formátování.

Jelikož třída Win32_Process neposkytuje informace o aktuálním využití CPU, musel jsem vymyslet vlastní způsob, jak získat kýžené údaje. Po prvním načtení údajů včetně spotřebovaných časů CPU (viz popis sloupce „Čas CPU“ níže) se chvíli počká, a poté se znovu načtou všechny spotřebované časy. Rozdíly časů všech procesů jsou sečteny a následně vyděleny dobou čekání. Takto získaná hodnota, uložená do proměnné „KorekceCPU“, vyjadřuje rychlost procesoru. Proměnná se poté používá při výpočtech využití CPU:

```
With objProcess
...
ModeTime = CSng(.KernelModeTime) + CSng(.UserModeTime)
VyuzitiCPU = 100 * (ModeTime - Bunka("ModeTime")) / KorekceCPU /
 RozdilSec
VyuzitiCPU = Round(VyuzitiCPU, 1)
If .Name <> "System Idle Process" Then
    Zapis "CPU", Replace(VyuzitiCPU, ",", "."), , , "0.0"
    CelkoveVyuzitiCPU = CelkoveVyuzitiCPU + VyuzitiCPU
End If
...
End With
```

- Čas CPU

Informuje o spotřebovaném čase procesoru daným procesem od jeho spuštění. Jedná se o součet hodnot (ve stovkách nanosekund) vlastností *KernelModeTime* a *UserModeTime*. Zobrazuje se ve formátu <*hodiny*>:<*minuty*>:<*sekundy*>.<*milisekundy*>. Hodnota se zapisuje také do pomocného skrytého sloupce „ModeTime“, který slouží pro výpočty využití CPU.

- Paměť

Udává velikost paměti používané procesem, kterou nelze sdílet s jinými procesy - soukromá pracovní sada (vlastnost *PrivatePageCount*). Intenzita barvy pozadí je dána velikostí hodnoty pomocí podmíněného formátování.

- Disk (čtení/zápis)

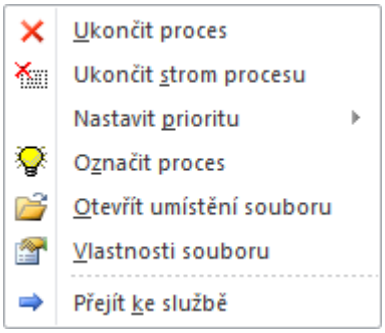
Tyto dva sloupce udávají objem přečtených/zapsaných bajtů dat (vlastnosti *ReadTransferCount* a *WriteTransferCount*). Počet červeně zvýrazněných číslic udává řád

průměrné rychlosti čtení/zápisu v bajtech za sekundu od posledního obnovení údajů. To se stanovuje na základě rozdílu nové a původní hodnoty za jednotku času.

- Čas spuštění

Zobrazuje datum a čas spuštění procesu (vlastnost *CreationDate*). U procesu spuštěného právě dnes se zobrazuje pouze čas. Seznam procesů je standardně seřazen podle pořadí jejich spuštění (pomocný skrytý sloupec „Pořadí“), což zpravidla odpovídá seřazení dle času spuštění procesů.

6.4.2 Kontextové menu



Obr. 6.3: Kontextové menu na listu Procesy

Popis položek kontextového menu listu Procesy:

- Ukončit proces

Tato volba ukončí vybraný proces. Ukončit lze také více procesů najednou jejich vybráním a stiskem klávesy Delete (předtím je vhodné vypnout automatické obnovování). Pro ukončení procesu se používá metoda *Terminate*. Ukončení je násilné, případná neuložená data procesu jsou ztracena. Při ukončení důležitého systémového procesu může dojít k nestabilitě nebo pádu operačního systému.

- Ukončit strom procesu

Umožňuje ukončit vybraný proces včetně všech jeho potomků (podprocesů), které tento proces přímo či nepřímo vyvolal. Pro ukončení hlavního procesu se použije stejná procedura jako u volby „Ukončit proces“. Následně se rekurzivně vyhledají a ukončí všichni jeho potomci.

- Nastavit prioritu

Rozbalovací nabídka pro nastavení priority procesu. Pro nastavení se používá metoda *SetPriority*, které se předává číselný parametr určující požadovanou prioritu (64=nízká, 16384=nižší než normální, 32=normální, 32768=vyšší než normální, 128=vysoká, 256=reálný čas).

- Označit proces

Tato možnost zapne/vypne označení procesu (zvýraznění žlutou barvou pozadí). Po ukončení běhu takto označeného procesu je zobrazeno informační upozornění.

- Otevřít umístění souboru

Otevře umístění souboru daného procesu v Průzkumníku Windows. Ke spuštění se používá příkaz `explorer.exe /separate,/select,<cesta>`.

Když je program AdminPC spuštěn pod jiným než přihlášeným uživatelem (z důvodu získání vyššího oprávnění), tak se Průzkumník (explorer.exe) spustí:

- Ve Windows 7 a výše pod přihlášeným uživatelem, tudíž cíl nemusí být dostupný z důvodu nedostatečného oprávnění (zobrazí se výzva k zadání přístupových údajů). Řešením je využít jiný souborový manažer, např. „Total Commander“ či „Explorer++“. Jejich použití je možné odkomentováním a případně upravením příslušné řádky kódu v proceduře *OtevritUmisteniSouboruNeboSlozky* v modulu „Module1“ editoru VBA.
- Ve Windows XP pod uživatelem, pod nímž program AdminPC běží, a to díky použití přepínače /separate, jinak by se Průzkumník vůbec nespustil.

Při používání 32-bitové verze Excelu pro práci s 64-bitovým systémem na lokálním počítači nejsou některé systémové soubory přístupné a zobrazí se zpráva „Soubor není dostupný“ (totéž platí pro volbu „Vlastnosti souboru“ níže). Při práci se vzdáleným počítačem toto omezení neplatí.

- Vlastnosti souboru

Zobrazí se vlastnosti souboru daného procesu. Jedná se o standardní dialog „Vlastnosti“, který lze vyvolat z kontextového menu souboru v Průzkumníku Windows. K zobrazení tohoto dialogu používám COM objekt *Shell.Application*:

```
CreateObject("Shell.Application").Namespace(0).ParseName(<cesta
 k souboru>).InvokeVerb "properties"
```

- Přejít ke službě

Tuto volbu lze použít u procesů služeb (zvýrazněny oranžovým vzorkem pozadí) pro přechod na list Služby a zobrazení příslušných služeb. Příslušnost se zjišťuje na základě shodnosti PID. Je-li nelezena pouze jedna související služba, aktivuje se řádka s touto službou. V případě zjištění více služeb (zejména u procesů „svchost.exe“) se odpovídající řádky vyfiltrují, hlavička prvního sloupce se zvýrazní modře a objeví se komentář „Pro zobrazení původního seznamu služeb zvolte Obnovit nebo stiskněte klávesu F5“.

6.4.3 Hlavní menu

Hlavní menu na listu Procesy obsahuje navíc tyto specifické položky:

- Filtrovat

Rozbalovací nabídka obsahuje následující předvolené filtry:

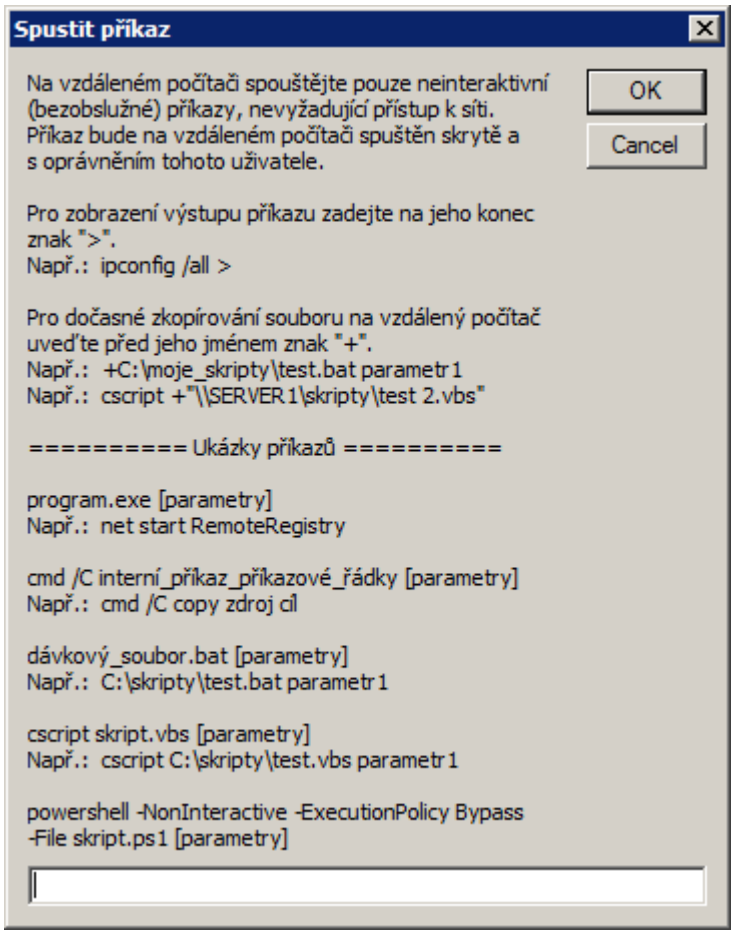
- Procesy lokálně přihlášených uživatelů
- Procesy služeb
- Zvýrazněné procesy

- Automatické obnovení

Tato volba zapíná/vypíná automatické obnovování údajů. Zapnutí je indikováno červenou barvou hlavičky sloupců a znakem „~“ na konci titulku okna. Automatické obnovení probíhá standardně každé dvě sekundy, ale lze to případně změnit úpravou konstanty „SetAutoRefreshTime“ v kódu listu Procesy. Při přepnutí na jiný list nebo do jiného sešitu v dané instanci Excelu se automatické obnovování dočasně pozastaví. K zajištění spouštění obnovovací procedury se využívá metoda Excelu *Application.OnTime*.

- Spustit příkaz

Umožňuje spuštění příkazu (procesu). Instrukce pro spuštění jsou součástí zadávacího dialogu (obr. 6.4). Spuštěný příkaz je zvýrazněn žlutou barvou pozadí ve sloupci „Příkazový řádek“. Po dobu běhu procesu se zapne automatické obnovování. Po ukončení procesu se zobrazí zpráva a případný chybový kód.



Obr. 6.4: Funkce „Spustit příkaz“

Pro spuštění příkazu se používá metoda *Create* třídy Win32_Process. Na lokálním počítači se takovýto příkaz spustí viditelně. Na vzdáleném počítači je však spuštěn skrytě, proto má význam spouštět pouze neinteraktivní (bezobslužné) příkazy. Spuštěný příkaz na vzdáleném počítači bohužel nemá přístup k síťovým zdrojům.

Pro schopnost získat ukončovací návratový kód (ExitStatus) příkazu jsem využil událostní WMI třídu *Win32_ProcessStopTrace*. Před vlastním spuštěním příkazu metodou *Create* se vytvoří speciální kolekce „colProcessStopTrace“, která zaznamenává údaje o ukončených procesech cílového počítače. Kód vypadá takto:

```
Set colProcessStopTrace = WMI.ExecNotificationQuery("SELECT * FROM
 Win32_ProcessStopTrace")

ReturnValue = WMI.Get("Win32_Process").Create(Prikaz,
 "C:\Windows\Temp", , SpustitPrikaz_ProcessId)
```

Po ukončení běhu příkazu se tento v kolekci „colProcessStopTrace“ vyhledá dle identifikátoru *ProcessId* a zjistí se hodnota vlastnosti *ExitStatus* (u starších systémů Windows XP a Windows Server 2003 není tato vlastnost dostupná). Kód vypadá takto:

```
Do
  With colProcessStopTrace.NextEvent
  If .ProcessId = SpustitPrikaz_ProcessId Then
    On Error Resume Next
    ExitStatus = .ExitStatus
    If Err Then ExitStatus = "XP"
    On Error GoTo 0

    Exit Do
  End If
  End With
Loop
```

Na základě hodnoty *ExitStatus* se zobrazí příslušná zpráva. Při hodnotě 0 se zobrazí „Příkaz byl úspěšně dokončen.“, jinak se vypíše zpráva s číslem chybového kódu. Pro starší nepodporovaný systém se zobrazí upozornění, že chybový kód nelze zjistit.

Často je žádoucí zachytit výstup konzolových příkazů. Umožnil jsem to pomocí zadání identifikačního znaku „>“ na konec příkazu (např. `ipconfig /all` **>**). Na základě toho se příkaz spustí prostřednictvím `cmd /U /C` *<příkaz>* `>output.txt 2>&1`. Tímto je standardní i chybový výstup příkazu přesměrován do souboru „output.txt“. Soubor se ukládá na cílovém počítači do složky „C:\Windows\Temp“, neboť příkaz se spouští metodou *Create*, které se předává tato složka v parametru *CurrentDirectory*. Po ukončení běhu příkazu se zobrazí dotaz, zda se má zobrazit výstup příkazu. V případě kladné odpovědi se otevře soubor „\\<*PC*>\C$\Windows\Temp\output.txt“. Tento dočasný soubor je poté odstraněn.

Na vzdáleném počítači je možné spustit také příkaz (program, dávkový soubor, skript), který je umístěn na lokálním počítači nebo v nějaké síťové složce. Stačí před ním uvést identifikační znak „+“ (např. `+C:\moje_skripty\test.bat parametr1` nebo `cscript +"\\SERVER1\skripty\test 2.vbs"`). Při detekování znaku „+“ se provede dočasné zkopírování souboru do složky „C:\Windows\Temp“ na vzdáleném počítači. Poté se cesta v příkazu náležitě upraví a příkaz se spustí.

6.5 List Služby

Zobrazuje služby nebo ovladače a poskytuje o nich důležité údaje. Zobrazení ovladačů místo služeb se zapíná/vypíná volbou „Zobrazit ovladače“ v hlavním menu. Umožňuje provádět operace: spuštění, zastavení, restartování, pozastavení, změna typu spouštění, odstranění. Také lze zobrazit závislosti služeb a ovladačů. V titulku okna je uveden počet spuštěných služeb resp. ovladačů a jejich celkový počet.

K práci se službami a ovladači se používají WMI třídy *Win32_Service* a *Win32_SystemDriver* z jmenného prostoru „root\CIMV2“.

Tab. 6.2: Vlastnosti a metody tříd Win32_Service a Win32_SystemDriver použité v programu

Vlastnost	**Popis**
Name	jedinečný název služby/ovladače
DisplayName	plný název služby/ovladače
Description	textový popis služby
StartMode	udává režim spouštění služby/ovladače
ProcessId	identifikátor procesu služby
PathName	příkazový řádek použitý ke spuštění služby nebo cesta k souboru ovladače
ServiceType	označuje typ služby poskytované volajícím procesům
StartName	název účtu, pod nímž je služba spuštěna
State	aktuální stav služby/ovladače
AcceptStop	označuje, zda může být služba/ovladač ukončen
AcceptPause	označuje, zda může být služba pozastavena
Metoda	
StartService	spustí službu/ovladač
StopService	zastaví službu/ovladač
PauseService	pozastaví běh služby
ResumeService	pokračuje v běhu služby
ChangeStartMode	změní režim spouštění služby/ovladače
Delete	odstraní službu/ovladač

Výsledkem operací se službami/ovladači jsou návratové kódy (ReturnValue) s čísly 0 až 24. Kód s číslem 0 znamená úspěšné provedení, ostatní čísla vyjadřují určitou chybu. Všem chybovým kódům jsem přiřadil příslušný český popis. Popisné texty jsem převzal z rozhraní WMI na Windows XP, které bylo lokalizováno do češtiny na rozdíl od novějších verzí Windows.

6.5.1 Sloupce

Sloupce na listu Služby jsou následující:

- Služba/Ovladač

Zobrazuje jedinečný název služby/ovladače (vlastnost *Name*). V komentáři je uvedena cesta k souboru služby/ovladače, získaná z řetězce příkazového řádku.

Při zvýrazňování se využívá pomocný skrytý sloupec „Stav“ (vlastnost *State*), který může nabývat těchto hodnot: Running, Stopped, Paused, Unknown, Start Pending, Stop Pending, Pause Pending, Continue Pending. Spuštěné (Running) služby/ovladače jsou zvýrazněny zeleně, pozastavené (Paused) služby modře a případný neznámý stav (Unknown) je indikován červeně. Aktuální provádění operace (… Pending) je zvýrazněno žlutou barvou pozadí.

Seznam služeb/ovladačů je standardně seřazen podle tohoto sloupce.

- Název

Uvádí plný název služby/ovladače (vlastnost *DisplayName*).

- Popis

Zobrazuje textový popis služby (vlastnost *Description*). Komentář obsahuje totéž. Šířka sloupce je standardně minimální, uzpůsobená pouze pro zobrazení komentáře po najetí kurzoru myši. Při zobrazení ovladačů je sloupec prázdný.

- Typ spouštění

Udává režim spouštění služby/ovladače (vlastnost *StartMode*). Originální názvy hodnot (Auto, Manual, Disabled) jsou překládány do češtiny.

Může nabývat těchto hodnot:

- Automaticky: automatický start během spuštění operačního systému
- Ručně: možnost ručního spuštění
- Zakázáno: zákaz spuštění (označeno světlou barvou)
- Boot: spuštění zavaděčem operačního systému (pouze pro ovladače)
- System: spuštění při inicializaci operačního systému (pouze pro ovladače)

Od Windows verze Vista přibyl ještě typ spouštění „Automaticky (Zpožděné spuštění)“. Tento nový typ však nelze pomocí WMI zjistit ani nastavit. Dalo by se to provést

přímým přístupem do registru (klíč „HKLM\SYSTEM\CurrentControlSet\services\<*služba*>“ a hodnota *DelayedAutoStart*), ale toto jsem nerealizoval.

- PID

  Udává identifikátor procesu spuštěné služby (vlastnost *ProcessId*). Při zobrazení ovladačů je sloupec prázdný, neboť ovladače žádné procesy nevytvářejí.

- Příkazový řádek

  Uvádí příkazový řádek použitý ke spuštění služby nebo cestu k souboru ovladače (vlastnost *PathName*).

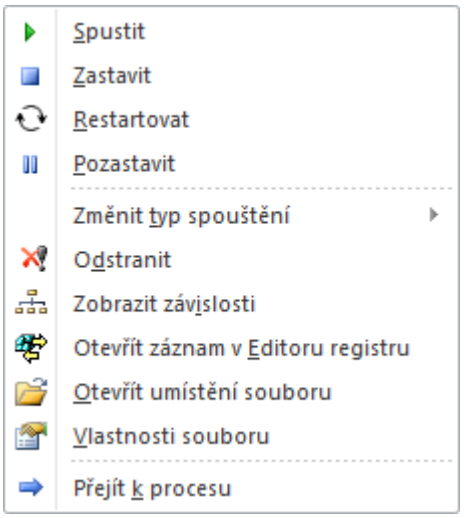
- Typ

  Označuje typ služby poskytované volajícím procesům (vlastnost *ServiceType*). U služeb to bývá typ „Own Process“ nebo „Share Process“ a u ovladačů typ „Kernel Driver“ nebo „File System Driver“.

- Účet pro přihlášení

  Zobrazuje název účtu, pod nímž je služba spuštěna (vlastnost *StartName*). Při zobrazení ovladačů je sloupec prázdný.

6.5.2 Kontextové menu



Obr. 6.5: Kontextové menu na listu Služby

Popis položek kontextového menu listu Služby:

- Spustit

Provede spuštění služby/ovladače metodou *StartService* nebo v případě pozastaveného stavu metodou *ResumeService*.

- Zastavit

Provede zastavení služby/ovladače metodou *StopService*.

Před zastavením nebo restartem služby/ovladače je nutné zastavit případné spuštěné závislé součásti. Je-li nějaká závislá součást spuštěna, zobrazí se před zastavením nebo restartem služby/ovladače dotaz s upozorněním „Budou zastaveny také následující závislé součásti a jejich případné podsoučásti“ následovaný výčtem těchto součástí. V případě potvrzení dotazu se rekurzivně vyhledají a ukončí všechny závislé součásti a nakonec i prvotní služba/ovladač.

Některé služby nejde z určitých důvodů zastavit/restartovat, např.: gpsvc (Klient zásad skupiny), Schedule (Plánovač úloh), PlugPlay (Plug and Play), eventlog (Protokol událostí systému Windows). Totéž platí také pro mnohé ovladače.

- Restartovat

Provede restart služby/ovladače. Přímá WMI metoda pro tuto operaci neexistuje, je tedy nutné vykonat zastavení, vyčkat na dokončení zastavení a následně službu/ovladač opět spustit. Pro zastavení platí totéž, co bylo popsáno u volby „Zastavit“ výše. Případné zastavené závislé součásti se po spuštění primární služby/ovladače opět spustí.

- Pozastavit/Pokračovat

Provede pozastavení/pokračování běhu služby metodou *PauseService*/*ResumeService*. Pozastavení je možné provést pouze u několika málo služeb, např. LanmanServer (Server) a LanmanWorkstation (Pracovní stanice).

- Změnit typ spouštění

Rozbalovací nabídka pro změnu typu spouštění. Pro nastavení se používá metoda *ChangeStartMode*. K dispozici jsou volby: *Automaticky* (Automatic), *Ručně* (Manual), *Zakázáno* (Disabled) a pro ovladače navíc *Boot* a *System*.

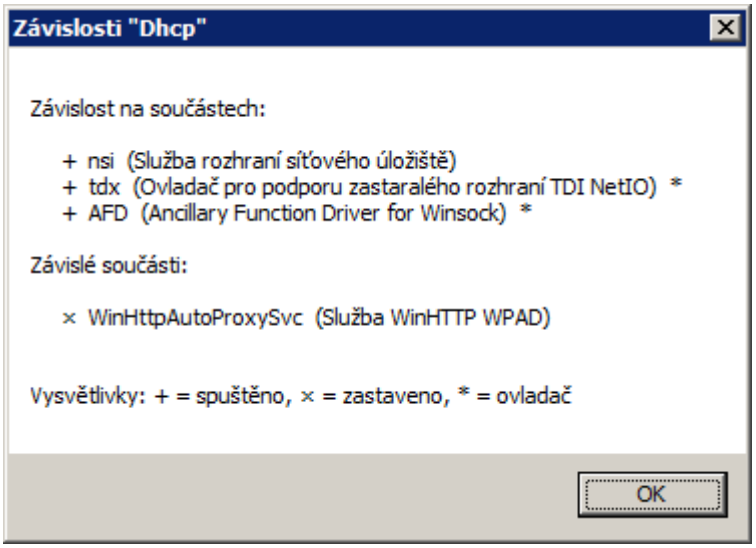
- Odstranit

Umožňuje odstranit službu/ovladač ze systému. Používá se k tomu metoda *Delete*. Dále se zobrazí dotaz, zda se má odstranit také příslušný související soubor. Pokud se spuštěnou službu/ovladač nepodaří momentálně zastavit, dojde k odstranění při nejbližším zastavení (např. při vypnutí počítače).

- Zobrazit závislosti

Zobrazí okno s přehledem závislostí pro danou službu/ovladač (obr. 6.6). Závislosti mapuje asociační WMI třída *Win32_DependentService*. Závislost služby/ovladače na součástech určuje vlastnost *Dependent* a závislé součásti definuje vlastnost *Antecedent*. WQL dotaz pro zjištění závislostí vypadá takto:

```
ASSOCIATORS OF {Win32_Service.Name="<služba/ovladač>"} WHERE
 AssocClass=Win32_DependentService Role=<Dependent/Antecedent>
```



Obr. 6.6: Ukázka závislostí pro službu „Dhcp“

- Otevřít záznam v Editoru registru

Tato volba otevře záznam služby/ovladače v Editoru registru. Jedná se o klíč „HKLM\SYSTEM\CurrentControlSet\services\<*služba/ovladač*>“, který obsahuje údaje o konfiguraci dané služby/ovladače. K otevření klíče v Editoru registru se používá pomocný skript „Tools\OpenInRegedit.vbs“ (viz kapitola **6.1 Soubory programu**).

- Otevřít umístění souboru

Otevře umístění souboru dané služby/ovladače v Průzkumníku Windows. Podrobněji popsáno u totožné volby pro procesy.

- Vlastnosti souboru

Zobrazí se vlastnosti souboru dané služby/ovladače. Podrobněji popsáno u totožné volby pro procesy.

- Přejít k procesu

Tuto volbu lze použít u spuštěných služeb (zvýrazněné zelenou barvou) pro přechod na list Procesy a aktivování řádky s příslušným procesem. Příslušnost se zjišťuje na základě shodnosti PID.

6.5.3 Hlavní menu

Hlavní menu na listu Služby obsahuje navíc tyto specifické položky:

- Filtrovat

Rozbalovací nabídka obsahuje následující předvolené filtry:

- Spuštěné služby
- Ručně spuštěné služby
- Automaticky spouštěné ale aktuálně zastavené služby
- Nezakázané služby

- Otevřít konzolu Služby

Otevře konzolu *Služby* příkazem `mmc` **`services.msc`** `/computer=<`*`PC`*`>`.

- Zobrazit ovladače

Tato volba zapne/vypne zobrazení ovladačů místo služeb. Tj. pro výčet se použije třída *Win32_SystemDriver* místo *Win32_Service*. Při zobrazení ovladačů je v titulku okna uveden text „Ovladače“ místo „Služby“ a první sloupec je nazván „Ovladač“ místo „Služba“.

6.6 List Software

Zobrazuje nainstalovaný software (program, aplikace, aktualizace) a poskytuje o něm důležité údaje. Umožňuje provádět operace: odinstalace, smazání odinstalačního záznamu, otevření odinstalačního záznamu v Editoru registru. V titulku okna se zobrazuje počet položek nainstalovaného software.

Informace o nainstalovaném software se získávají z registru z klíče „HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall“. V případě cílového počítače se 64-bitovým systémem se údaje o 32-bitovém software načítají z klíče „HKLM\SOFTWARE*Wow6432Node*\Microsoft\Windows\CurrentVersion\Uninstall“.
V těchto klíčích jsou podklíče nainstalovaného software, které obsahují potřebné hodnoty (ne vždy jsou všechny k dispozici).

Tab. 6.3: Hodnoty v podklíčích klíče „Uninstall“ použité v programu

Hodnota	**Popis**
DisplayName	název software
DisplayVersion	verze
Publisher	vydavatel
InstallDate	datum instalace ve formátu YYYYMMDD
InstallLocation	instalační složka
EstimatedSize	odhadovaná velikost na disku v kB
InstallSource	zdroj instalace
UninstallString	příkaz k odinstalaci
QuietUninstallString	příkaz k tiché (bezobslužné) odinstalaci

K práci s registrem se používá speciální WMI třída *StdRegProv* z jmenného prostoru „root\default“.

Tab. 6.4: Metody třídy StdRegProv použité v programu

Metoda	**Popis**
EnumKey	provede výčet podklíčů
GetStringValue	načte řetězcovou (REG_SZ) hodnotu
GetDWORDValue	načte číselnou (REG_DWORD) hodnotu
DeleteKey	odstraní klíč
ExecMethod_	alternativní způsob volání výše uvedených metod

Všechny metody třídy StdRegProv přijímají jako jeden z parametrů číselné označení kořenového klíče registru. Jelikož potřebný klíč *HKLM* je výchozí, uvádět se nemusel.

Pro možnost použít 32-bitovou verzi Excelu také pro práci s 64-bitovým systémem na lokálním počítači jsem musel použít alternativní způsob přístupu k údajům o 64-bitovém software pomocí metody *ExecMethod_*. Tento způsob je trochu pomalejší, ale použije se pouze v případě potřeby. Následuje zjednodušené porovnání kódu obou způsobů pro metodu *GetStringValue*:

```
Key = "SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\……"
ValueName = "DisplayName"
```

a) přímé volání metody:

```
objReg.GetStringValue , Key, ValueName, Value
```

b) využití metody *ExecMethod_* pro načtení 64-bitového údaje:

```
Set objCtx = CreateObject("WbemScripting.SWbemNamedValueSet")
objCtx.Add "__ProviderArchitecture", 64

Set InParams = objReg.Methods_("GetStringValue").InParameters
InParams.sSubKeyName = Key
InParams.sValueName = ValueName

Value = objReg.ExecMethod_("GetStringValue", InParams, ,
 objCtx).sValue
```

6.6.1 Sloupce

Sloupce na listu Software jsou následující:

- Software

Zobrazuje název nainstalovaného software (hodnota *DisplayName*) a v hranatých závorkách číslo verze (hodnota *DisplayVersion*). V komentáři je uveden název podklíče registru z klíče „Uninstall“. Seznam je standardně seřazen podle tohoto sloupce.

- Vydavatel

Uvádí jméno vydavatele (hodnota *Publisher*).

- Nainstalováno

Udává datum instalace software (hodnota *InstallDate*). Software nainstalovaný během posledních 14 dnů je zvýrazněn červenou barvou pozadí a instalace provedené během posledního půl roku žlutou barvou. Intenzita barvy pozadí je dána blízkostí data instalace.

- Instalační složka

  Zobrazuje cestu složky, obsahující nainstalovaný software (hodnota *InstallLocation*).

- Velikost

  Udává odhadovanou velikost software na disku (hodnota *EstimatedSize*). Nejedná se pouze o prostou velikost instalační složky. Intenzita barvy pozadí je dána velikostí hodnoty pomocí podmíněného formátování.

- Zdroj instalace

  Zobrazuje cestu složky, z níž byl software instalován (hodnota *InstallSource*).

- Odinstalace

  Uvádí příkaz k odinstalaci software (hodnota *UninstallString*). Software instalovaný pomocí balíčku MSI (Microsoft Windows Installer) se odinstaluje příkazem `MsiExec.exe /X{GUID}` (GUID je globálně jedinečný identifikátor). Občas je však v příkazu k odinstalaci uvedeno `MsiExec.exe /I{GUID}`, což slouží spíše k zobrazení nabídky ke změně/opravě/odstranění software. V tomto případě nahrazuji přepínač /I za /X.

- Tichá odinstalace

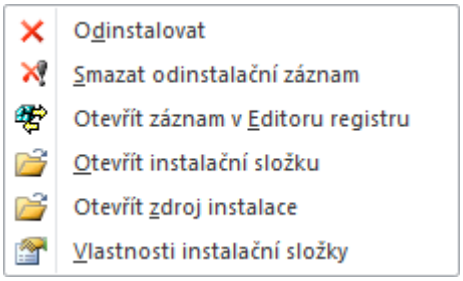
  Uvádí příkaz k tiché (bezobslužné) odinstalaci software (hodnota *QuietUninstallString*). K dispozici je jen zřídka. Software nainstalovaný pomocí balíčku MSI je však možné tiše odinstalovat přidáním přepínače /q za příkaz k běžné odinstalaci: `MsiExec.exe /X{GUID} /q`. Tyto příkazy jsou do sloupce dodatečně doplněny.

  Šířka sloupce je standardně malá, v případě existence tiché odinstalace je zobrazen pouze text „ANO“. Toto neplatí při zobrazení záznamů ve Formuláři, zde je viditelný kompletní příkaz k tiché odinstalaci.

- Platforma

  Rozlišuje platformu (32/64-bit) nainstalovaného software. V podstatě udává, ze kterého klíče registru byl záznam načten. Na cílovém počítači s 32-bitovým systémem se pochopitelně nalézá pouze 32-bitový software. Platforma 64-bit je zvýrazněna červeně.

6.6.2 Kontextové menu



Obr. 6.7: Kontextové menu na listu Software

Popis položek kontextového menu listu Software:

- Odinstalovat

Provede odinstalaci software. Na vzdáleném počítači je možné spustit pouze tichou (bezobslužnou) odinstalaci. Není-li příkaz pro tichou odinstalaci dostupný, odinstalaci software nelze vzdáleně provést. Při tiché odinstalaci se zobrazí průběh odinstalačního procesu na listu Procesy (využívá se část funkce „Spustit příkaz“).

Pokud je známa instalační složka a při odinstalaci software nebyla odstraněna (např. v ní zůstaly nějaké konfigurační soubory), zobrazí se dotaz, zda se má složka otevřít.

- Smazat odinstalační záznam

Smaže odinstalační záznamu software z registru. Prakticky jde o smazání příslušného podklíče v klíči „HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall“ nebo „HKLM\SOFTWARE*Wow6432Node*\Microsoft\Windows\CurrentVersion\Uninstall“.

- Otevřít záznam v Editoru registru

Tato volba otevře odinstalační záznam software v Editoru registru. Jedná se o příslušný podklíč klíče „HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall“ nebo „HKLM\SOFTWARE*Wow6432Node*\Microsoft\Windows\CurrentVersion\Uninstall“. K otevření klíče v Editoru registru se používá pomocný skript „Tools\OpenInRegedit.vbs“ (viz kapitola **6.1 Soubory programu**). Při používání 32-bitové verze Excelu nelze otevřít případný 64-bitový odinstalační záznam.

- Otevřít instalační složku

Otevře složku obsahující nainstalovaný software v Průzkumníku Windows. Ke spuštění se používá příkaz `explorer.exe /separate,<cesta>`. Podrobněji popsáno u obdobné volby „Otevřít umístění souboru“ pro procesy.

- Otevřít zdroj instalace

Otevře složku, z níž byl software instalován, v Průzkumníku Windows. Dále platí totéž, co je uvedeno u položky „Otevřít instalační složku“ výše.

- Vlastnosti instalační složky

Zobrazí se vlastnosti instalační složky. Podrobněji popsáno u obdobné volby „Vlastnosti souboru“ pro procesy.

6.6.3 Hlavní menu

Hlavní menu na listu Software obsahuje navíc tuto specifickou položku:

- Filtrovat

Rozbalovací nabídka obsahuje následující předvolené filtry:

- Software s tichou (bezobslužnou) odinstalací
- Skrýt aktualizace Office: skryje nainstalované aktualizace kancelářského balíku Microsoft Office 2007 a výše na základě výskytu textu „Oarpman.exe“ nebo „Oarpmany.exe“ v řetězci příkazu pro odinstalaci
- Skrýt všechny aktualizace Microsoft: skryje aktualizace systému Windows a dalších produktů od firmy Microsoft na základě výskytu řetězce „(KB“ v názvu software (slouží hlavně pro Windows XP, kde jsou aktualizace systému uvedeny v seznamu software)

Speciální volbu pro nainstalování nového software jsem nevytvářel, nicméně pro tento účel je možné využít funkci „Spustit příkaz“ v hlavním menu na listu Procesy. Většina programů pro Windows je dostupná ve formě instalačních balíčků MSI, které lze bezobslužně nainstalovat pomocí příkazu `msiexec /i <soubor *.msi> /q`. Jiné instalační balíčky (např. Inno Setup, InstallShield, Nullsoft Scriptable Install System) také většinou podporují přepínače pro tichou instalaci.

Závěr

Cílem této práce bylo ukázat možnostmi vzdálené správy a ovládání operačního systému Windows v lokální počítačové síti. Dále popsat prostředky, které vzdálenou správu usnadňují a automatizují.

Byly využity převážně nástroje, které jsou přímo součástí Windows. Příkazový řádek umožňuje spouštění příkazů a prostřednictvím dávkových souborů usnadňuje a automatizuje řadu činností. Mnoho příkazů umožňuje spravovat také vzdálené počítače. Rozhraní WMI je univerzálním prostředkem pro pokročilou správu Windows. Velkou výhodou je snadný a přirozený přístup ke vzdáleným počítačům. K rozhraní WMI lze přistupovat z různých skriptovacích a programovacích jazyků.

Pro některé účely je však vhodné či nutné použít další nástroje. Např. ke spouštění programů na vzdálených počítačích je výhodné použít utilitu PsExec ze sady PsTools [2]. Pro zapnutí (probuzení) počítače po síti existují též zdarma dostupné programy.

Úkolem praktické části bylo vytvořit dva nástroje. První (OnlinePC) pro zobrazení přehledu a informací o zapnutých/vypnutých počítačích s možností jejich ovládání. Druhý (AdminPC) pro zobrazení informací a správu jednotlivých vzdálených počítačů v oblastech: běžící procesy, služby, nainstalovaný software.

Nástroje (programy) jsem vytvořil v aplikaci Microsoft Excel za pomoci jazyka VBA. Využil jsem bohaté možnosti formátování, filtrování a seřazování, které Excel nabízí. Při programování jsem používal rozhraní WMI, funkce API a také objekty COM.

Během realizace programů jsem se občas potýkal s nestandardním chováním a nestabilitou Excelu. Plně se ztotožňuji s tím, co napsal velký znalec Excelu John Walkenbach: „Možná si myslíte, že produkty jako Excel (používané miliony lidí po celém světě) by měli být relativně bez chyb. Myslíte si to špatně. Excel je tak složitý kus softwaru, že se v něm chyby dají očekávat. A Excel skutečně má své slabé stránky.“ [7] Programy by asi bylo lepší vytvořit v nějakém plnohodnotném programovacím prostředí, ale těžko by se našla zobrazovací komponenta, která by se svými schopnostmi vyrovnala Excelu.

Program AdminPC bude funkční i v 64-bitové verzi Excelu, program OnlinePC však nikoliv. Bylo by nutné přinejmenším upravit deklarace všech funkcí API a funkčnost důkladně otestovat, což jsem z časových důvodů nerealizoval. Při psaní kódu jsem využíval nové funkce Excelu, tudíž programy nebudou funkční ve starých verzích 2003 a nižších.

Seznam literatury a informačních zdrojů

[1] BITTO, Ondřej. *Příkazový řádek Windows 7*. Brno: Computer Press, 2011. 231 s. ISBN 978-80-251-3506-8.

[2] Windows Sysinternals: PsTools. *Microsoft TechNet* [online]. May 2, 2014 [cit. 2014-12-17]. Dostupné z: http://technet.microsoft.com/sysinternals/bb896649.aspx

[3] RUSSINOVICH, Mark a Aaron MARGOSIS. *Windows sysinternals administrator's reference*. Redmond, Washington: Microsoft Press, 2011, xxviii, 462 p. ISBN 978-0-7356-5672-7.

[4] BOUŠKA, Petr. Články: Wake on LAN - lokální i vzdálený subnet. *SAMURAJ-cz.com* [online]. 10.8.2008 [cit. 2014-12-10]. Dostupné z: http://www.samuraj-cz.com/clanek/wake-on-lan-lokalni-i-vzdaleny-subnet/

[5] Wake On Lan. *Depicus* [online]. 2015 [cit. 2015-03-08]. Dostupné z: http://www.depicus.com/wake-on-lan/

[6] SOFER, Nir. *NirSoft - freeware utilities* [online]. 2015 [cit. 2015-03-07]. Dostupné z: http://nirsoft.net/

[7] WALKENBACH, John. *Microsoft Office Excel 2007: programování ve VBA*. Vyd. 1. Brno: Computer Press, 2008, 912 s. ISBN 978-80-251-2011-8.

[8] WEBER, Monika. *Excel VBA: velká kniha řešení*. 1. vyd. Brno: Computer Press, 2007, 867 s. ISBN 978-80-251-1453-7.

[9] How to ping an IP address with Visual Basic by using ICMP. *Microsoft Support* [online]. September 14, 2005 [cit. 2014-12-01]. Dostupné z: http://support.microsoft.com/en-us/kb/300197

Přílohy

Příloha A: Program OnlinePC - soubor „ZdrojPC.txt“

```
# soubor se zdrojem počítačů pro program OnlinePC
# určeno pro zadání:
# - změn výchozího nastavení programu
# - cest načítaných PC z Active Directory
# - jmen nebo IP adres PC či jiných síťových zařízení

# --- změna výchozího nastavení programu ---
# výchozí nastavení programu viz Visual Basic -> Module1 -> procedura VychoziNastaveni
# - obnovení po spuštění programu (0=ne, 1=ano)
#Obnovit=0
# - automatické obnovení (0=ne, 1=ano)
#AutomatickeObnoveni=1
# - rychlost automatického obnovení (počet sekund mezi postupným obnovením jednotlivých PC)
#AutomatickeObnoveni_Sekundy=1
# - ping timeout (počet milisekund)
#PingTimeout=1000
# - zjišťování MAC adres (0=ne, 1=vždy, 2=pouze u dosud nezjištěných)
#ZjistovatMAC=0
# - zjišťování a zobrazení přihlášených uživatelů (0=ne, 1=pomocí funkcí API, 2=stanice pomocí WMI a servery pomocí
 funkcí API)
#   při použití funkcí API se objeví v komentáři také vzdáleně přihlášení uživatelé, ale na stanici musí být
 povoleno vzdálené RPC např. příkazem:
#    reg add "\\<PC>\HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v AllowRemoteRPC /t REG_DWORD /d 1 /f
#ZjistovatUzivatele=1
# - vyloučení lokálního PC ze seznamu (0=ne, 1=ano)
#VyloucitLokalniPC=1
```

```
# --- zadání cest načítaných PC z Active Directory ---
# <cesta>;[<filtr>];[<scope>]
#   cesta: rozlišovací jméno kontejneru s PC (např. OU=Computers,DC=firma,DC=cz) nebo přímo ke konkrétnímu PC (např.
 CN=PC1,OU=Computers,DC=firma,DC=cz)
#   filtr: prohledávací LDAP filtr; standardně je již uplatněn filtr pro vyhledání nezakázaných a nainstalovaných PC
#   scope: rozsah hledání; standardně jsou prohledávány i případné podkontejnery (subtree), pro zrušení uveďte
 "onelevel" (např. OU=Computers,DC=firma,DC=cz;;onelevel)

# společný prohledávací LDAP filtr platný pro všechny níže uvedené cesty
#SpolecnyFiltr=<filtr>

# PŘÍKLADY:
# načtení PC z daného kontejneru, jejichž jména začínají znaky "A" nebo "B" a nemají vyplněn popis
#OU=Computers,DC=firma,DC=cz;(|(name=A*)(name=B*))(!description=*)
# načtení PC z daného kontejneru, které nemají nainstalován systém Windows 7 se Service Pack 1
#OU=Computers,DC=firma,DC=cz;(!(&(operatingSystem=Windows 7 *)(operatingSystemServicePack=Service Pack 1)))
# načtení PC z daného kontejneru (bez podkontejnerů - onelevel), které obsahují ve jméně text "SRV" nebo mají
 nainstalován systém Windows Server
#OU=Computers,DC=firma,DC=cz;(|(name=*SRV*)(operatingSystem=Windows Server*));onelevel
# načtení jednoho konkrétního PC
#CN=PC1,OU=Computers,DC=firma,DC=cz


# --- zadání jmen nebo IP adres PC či jiných síťových zařízení ---
# <jméno nebo IP adresa>;[<popis>];[<umístění>]

# PŘÍKLADY:
#PC1;uživatel Jan Novák;123, 1. patro
#SERVER1;doménový server
#10.1.1.1;router (GW)
```

Příloha B: Program OnlinePC - soubor „KontextoveMenu.txt“

```
# vlastní položky kontextového menu
# <název položky>;[<příkaz>];[<styl okna>];[<klávesová zkratka>]
#   název položky:
#     - název položky kontextového menu
#     - může to být: položka, podnabídka (nemá uveden příkaz), položka podnabídky (začíná jednou nebo více mezerami)
#     - znakem "&" před písmenem lze nastavit přístupovou klávesu
#     - pokud položka souvisí s přihlášeným uživatelem (má být zobrazena ikona "uživatel"), avšak v příkazu není
 %USER%, zadejte na konec názvu položky znak "*"
#   příkaz:
#     - cesta k souboru a jeho parametry
#     - v parametrech místo jména počítače zadejte %PC% (nebo !PC! pro vynechání kontroly jeho dostupnosti) a místo
 uživatele zadejte %USER%
#     - je-li v parametru uvedeno !PC!, bude zobrazena ikona "vypnutý a zapnutý počítač" a je-li v parametru %USER%,
 bude zobrazena ikona "uživatel"
#     - výchozí (nacestovanou) složkou je složka s programem OnlinePC, v příkazu lze tedy uvádět relativní cesty
 (např. Tools\soubor.bat)
#     - není-li příkaz zadán, považuje se položka za podnabídku
#   styl okna:
#     - styl okna spouštěného programu (pro konzoly MMC nefunkční)
#     - možné hodnoty: 3=MaximizedFocus, 2=MinimizedFocus, 6=MinimizedNoFocus, 4=NormalNoFocus, 0=Hide (hodnota 0
 použitelná pouze pro konzolové programy a dávkové soubory)
#   klávesová zkratka:
#     - zkratka pro spuštění příkazu
#     - přepínače: Shift=+, Ctrl=^, Alt=%
#     - speciální klávesy: např. {F1} až {F12}, {RIGHT}
#     - příklad: +^{RIGHT} znamená zkratku Shift+Ctrl+šipka vpravo
#     - více viz http://msdn.microsoft.com/library/office/ff197461(office.14).aspx#sectionToggle1
# pro zobrazení oddělovače mezi položkami menu vložte řádku s jednou nebo více pomlčkami
```

```
--- VLASTNÍ MENU ---;notepad KontextoveMenu.txt
-----
&AdminPC
  &Procesy;..\AdminPC\AdminPC.bat Procesy %PC%;0;%{F1}
  &Služby;..\AdminPC\AdminPC.bat Služby %PC%;0;%{F2}
  S&oftware;..\AdminPC\AdminPC.bat Software %PC%;0;%{F3}
-----
&Konzoly MMC
  &Správa počítače;compmgmt.msc /computer=%PC%;;^{F12}
  Prohlížeč &událostí;eventvwr \\%PC%
  &Sdílené složky;fsmgmt.msc /computer=%PC%
  &Místní uživatelé a skupiny;lusrmgr.msc /computer=%PC%
  S&lužby;services.msc /computer=%PC%
  &Zásady skupiny;gpedit.msc /gpcomputer:"%PC%"
  &Plánovač úloh;Tools\MMC\taskschd.msc /computer=%PC%
  &Certifikáty;Tools\MMC\certmgr.msc /computer=%PC%
Konzo&la ADUC
  Zobrazit objekt &počítače;Tools\ADUC.bat !PC!
  Zobrazit objekt &uživatele;Tools\ADUC.bat %USER%
-----
&Vzdálená plocha;mstsc /v:%PC% /f;;%{F12}
Vzdálená po&moc;Tools\nircmd.exe qbox "Nabídnout vzdálenou pomoc uživateli ~q%USER%~q na ~q%PC%~q?" "Vzdálená pomoc"
 msra /offerRA %PC%
&Otisk obrazovky*;Tools\PrintScreen.bat %PC%;0
-----
```

```
# když je program OnlinePC spuštěn pod jiným než přihlášeným uživatelem (z důvodu získání vyššího oprávnění), tak se
 explorer.exe spustí:
#  - ve Windows 7 pod přihlášeným uživatelem, tudíž cíl nemusí být dostupný z důvodu nedostatečného oprávnění
 (zobrazí se výzva k zadání přístupových údajů),
#    řešením je využít jiný souborový manažer, např. "Total Commander" či Explorer++ (viz níže)
#  - ve Windows XP pod uživatelem, pod nímž program OnlinePC běží, a to díky parametru /separate, jinak by se
 explorer.exe vůbec nespustil
Prů&zkumník;%windir%\explorer.exe /separate,\\%PC%
Průzkumník - disk (&C:);%windir%\explorer.exe /separate,\\%PC%\C$;;^o
#Total Commander;C:\totalcmd\TOTALCMD.EXE \\%PC%
#Explorer++;C:\Programy\Explorer++\Explorer++.exe \\%PC%
-----
&Editor registru;Tools\OpenInRegedit.vbs %PC%;;^r
E&ditor registru - klíč uživatele*;Tools\OpenInRegedit.vbs %PC% HKCU;;^+r
-----
&Informace
  &Systémové informace  (msinfo32);msinfo32 /computer %PC%
  S&ystémové informace  (systeminfo);cmd /C title Systémové informace &  systeminfo /S %PC%  & pause
  Informace o doménovém &uživateli  (net user <uživatel> /domain);cmd /C title Informace o doménovém uživateli &
 net user %USER% /domain  & pause
P&rocesy
  &Procesy  (tasklist);cmd /C title Procesy (%PC%) &  tasklist /S %PC%  & pause
  Procesy &uživatele  (tasklist);cmd /C title Procesy uživatele (%PC%) &  tasklist /S %PC% /FI "USERNAME eq %USER%"
 & pause
  Procesy &služeb  (tasklist);cmd /C title Procesy služeb (%PC%) &  tasklist /S %PC% /SVC | findstr /V /C:"Není k
 dispozici" /C:"N/A"  & pause
  Procesy - &cesty k souborům  (wmic);cmd /C title Procesy (%PC%) & mode con cols=300 &  wmic /node:%PC% process get
 ExecutablePath  & pause;3
  P&rocesy  (qprocess);cmd /C title Procesy (%PC%) &  qprocess /SERVER:%PC% *  & pause
  Pr&ocesy uživatele  (qprocess);cmd /C title Procesy uživatele (%PC%) &  qprocess /SERVER:%PC% %USER%  & pause
```

```
&Síťové nástroje
  &ping;cmd /C title ping (%PC%) &  ping -t !PC!
  pat&hping;cmd /C title pathping (%PC%) &  pathping !PC!  & pause
  &tracert;cmd /C title tracert (%PC%) &  tracert !PC!  & pause
  &netstat -b  (pomocí PsExec);cmd /C Tools\PsExec.exe \\%PC% -AcceptEula -e  netstat -b  2>NUL   & echo. & pause;3
  &ipconfig /all  (pomocí PsExec);cmd /C Tools\PsExec.exe \\%PC% -AcceptEula -e  ipconfig /all  2>NUL   & echo. &
 pause
  Network&AdapterConfiguration  (wmic);cmd /C title NetworkAdapterConfiguration (%PC%) &  wmic /node:%PC% path
 Win32_NetworkAdapterConfiguration where (IPEnabled=True) get /value  & pause;3
&Připojit
  &Web;http://%PC%
  &FTP;ftp %PC%
  &Telnet;telnet %PC%
  Windows Remote &Shell;winrs -remote:%PC% -noprofile -environment:PROMPT=%PC%\$P$G  cmd /K cd \
  &PowerShell;powershell -NoExit Enter-PSSession %PC%
-----
PsE&xec
  &Příkazový řádek;Tools\PsExec.exe \\%PC% -AcceptEula -e  cmd /K cd \
  Příkazový řádek s přístupem k síťovým &zdrojům (vyžaduje zadání hesla Vašeho uživ. účtu);cmd /C title \\%PC% &
 Tools\PsExec.exe \\%PC% -AcceptEula -u %USERDOMAIN%\%USERNAME% -e  cmd /K cd \
  Příkazový řádek s oprávněním uživatele &SYSTEM;Tools\PsExec.exe \\%PC% -AcceptEula -s  cmd /K cd \
Nástroje &NirSoft
  &TurnedOnTimesView;Tools\NirSoft\TurnedOnTimesView.exe /Source 2 /RemoteComputer %PC%;3
  &WinLogOnView;Tools\NirSoft\WinLogOnView.exe /Source 2 /Server %PC%;3
  &DevManView;Tools\NirSoft\DevManView.exe /LoadFrom 2 /ComputerName %PC%;3
  &USBDeview;Tools\NirSoft\USBDeview.exe /remote %PC%;3
  &MyEventViewer;Tools\NirSoft\MyEventViewer.exe /remote %PC%;3
  &AppCrashView;Tools\NirSoft\AppCrashView.exe /ProfilesFolder \\%PC%\C$\Users;3
  &BlueScreenView;Tools\NirSoft\BlueScreenView.exe \\%PC%\C$\Windows\Minidump;3
  Browsing&HistoryView;Tools\NirSoft\BrowsingHistoryView.exe /HistorySource 4 /HistorySourceFolder
 "\\%PC%\C$\Documents and Settings\%USER%";3
```

Příloha C: Program OnlinePC - dávkový soubor „Načíst MAC ze serveru DHCP.bat“

```
@echo off
title %~n0
cls

setlocal EnableDelayedExpansion

if NOT exist C:\Windows\System32\rsatclient.dll (
  echo Musí být nainstalován balík "Nástroje pro vzdálenou správu serveru".
  echo Pro Windows 7 je dostupný na adrese:
  echo http://www.microsoft.com/cs-cz/download/details.aspx?id=7887
  pause
  exit /b
)

if NOT exist C:\Windows\System32\dhcpmon.dll (
  set /P AN=Bude přidána funkce "Nástroje pro server DHCP", chcete pokračovat? [A,N]:
  if /I NOT "!AN!"=="a"  exit /b

  echo Přidávání funkce "Nástroje pro server DHCP"...
  :: Zapnout nebo vypnout funkce systému Widows > Nástroje pro vzdálenou správu serveru > Nástroje pro správu rolí > Nástroje pro
 server DHCP
  ocsetup RemoteServerAdministrationTools;RemoteServerAdministrationTools-Roles;RemoteServerAdministrationTools-Roles-DHCP
)

for /F "tokens=2 delims=:" %%A in ('"ipconfig /all | find "Server DHCP" "') do (
  set ServerDHCP=%%A
  set ServerDHCP=!ServerDHCP:~1!
)
if NOT "%ServerDHCP%"==""  set DEFAULT= (bez zadání = %ServerDHCP%)
set /P ServerDHCP=Zadejte jméno serveru DHCP%DEFAULT%:
if "%ServerDHCP%"==""  exit /b
```

```
netsh dhcp server \\%ServerDHCP% show scope  || (pause & exit /b)

echo.
echo.
echo Načítání MAC adres...

set TempFile=%TEMP%\MAC.txt

(for /F %%A in ('"netsh dhcp server \\%ServerDHCP% show scope | findstr "\-Aktivn" "') do  netsh dhcp server \\%ServerDHCP% scope
 %%A show clients 1) > %TempFile%

for %%A in (%TempFile%) do  if %%~zA==0 (
  echo Nebyly nalezeny žádné záznamy.
  goto K
)

echo.
echo Přidávání nových záznamů do souboru MAC.csv:

for /F "tokens=3-8,10* delims=-" %%A in ('find "  " %TempFile%') do (
  set MAC=%%A-%%B-%%C-%%D-%%E-%%F
  for /F "delims=." %%X in ("%%H") do  set PC=%%X
  set ZAZNAM=!PC: =!;!MAC: =!

  find /I "!ZAZNAM!" "%~dp0\MAC.csv" >NUL 2>&1 || (echo !ZAZNAM! & (echo !ZAZNAM!) >> "%~dp0\MAC.csv")
)

:K
del %TempFile%

echo.
pause
```

Příloha D: Program OnlinePC - konfigurační soubor pásu karet (kód RibbonX)

```
<customUI onLoad="RibbonOnLoad" xmlns="http://schemas.microsoft.com/office/2009/07/customui">
  <ribbon startFromScratch="false">
    <tabs>
      <tab id="MyCustomTab" label="OnlinePC" insertBeforeMso="TabHome" keytip="P">
        <group id="CustomGroup1">
          <button id="HlavniMenu" label="Hlavní menu" onAction="RibbonAction" imageMso="OutlineMoveDown" />
          <button id="KontextoveMenu" label="Kontextové menu" onAction="RibbonAction" imageMso="OutlineMoveDown" />
        </group>
        <group id="CustomGroup2">
          <button id="Zapnout" label="Zapnout" size="large" onAction="RibbonAction" imageMso="MacroPlay" keytip="+"
 />
          <button id="Vypnout" label="Vypnout" size="large" onAction="RibbonAction" imageMso="DeclineInvitation"
 keytip="-" />
          <button id="Restartovat" label="Restartovat" size="large" onAction="RibbonAction"
 imageMso="RecurrenceEdit" keytip="*" />
          <button id="OdhlasitUzivatele" label="Odhlásit uživatele" size="large" onAction="RibbonAction"
 imageMso="DistributionListRemoveMember" keytip="/" />
          <separator id="MySeparator1" />
          <button id="Obnovit" label="Obnovit" size="large" onAction="RibbonAction" imageMso="Refresh" keytip="O" />
          <button id="AutoRefresh" label="Automatické obnovení" size="large" onAction="RibbonAction"
 imageMso="RefreshAll" keytip="A" />
          <separator id="MySeparator2" />
          <button id="Formular" label="Formulář" size="large" onAction="RibbonAction" imageMso="DataFormExcel"
 keytip="F" />
          <button id="CelaObrazovka" label="Celá obrazovka" size="large" onAction="RibbonAction"
 imageMso="ViewFullScreenView" keytip="C" />
          <button id="UlozitNastaveni" label="Uložit nastavení" size="large" onAction="RibbonAction"
 imageMso="FileSave" keytip="U" />
```

```
          <button idQ="VisualBasic" size="large" keytip="V" />
          <button id="Napoveda" label="Nápověda" size="large" onAction="RibbonAction" imageMso="Help" keytip="N" />
          <separator id="MySeparator3" />
          <control idQ="ViewHeadings" label="Zobrazit záhlaví" keytip="B" />
          <control idQ="ReviewShowAllComments" label="Zobrazit komentáře" keytip="K" />
          <control idQ="ConditionalFormattingsManage" label="Podmíněné formátování"
 imageMso="ConditionalFormattingMenu" keytip="M" />
        </group>
      </tab>
    </tabs>
  </ribbon>

  <backstage>
    <button idMso="FileSaveAs" visible="false" />
    <button idMso="FileOpen" visible="false" />
    <button idMso="FileClose" visible="false" />
    <tab idMso="TabRecent" visible="false" />
    <tab idMso="TabNew" visible="false" />
  </backstage>
</customUI>
```