EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

jihomoravský kraj

OPERAČNÍ SYSTÉMY

Pokročilá práce s protokoly ve Windows

Metodický list

Autor: Ing. Marek Kocan, Metodik: Ing. Roman Koláčný

Recenzent: Mgr. Jiří Činčura

Rok vydání: 2023

Pokročilá práce s protokoly ve Windows podléhá licenci CC BY-SA 4.0 International License (Offline use: http://creativecommons.org/licenses/by-nc-sa/4.0/).

Obsah

Cíle

Studenti se seznámí s teoretickými základy v oblasti protokolů u operačních systémů Windows a osvojí si dovednosti pro pokročilou práci s protokoly, a to na základě konkrétních příkladů předvedených vyučujícím i na základě samostatně vyzkoušených úkolů.

Student bude schopen vlastními slovy vysvětlit co jsou protokoly, co je základem protokolů ve Windows, kde se protokoly ve Windows nachází a jak v základu protokoly ve Windows fungují. V dlouhodobém horizontu bude student schopen samostatně využít nové znalosti a dovednosti pro zjednodušení správy operačního systému.

Dovednosti

Student bude schopen vypsat obsah hlavních protokolů operačního systému i vyhledávat podle obsahu, druhu i závažnosti. Dále student zvládne i pokročilou práci, například navázání události na plánovač úloh. V dlouhodobém horizontu bude student schopen aplikovat získané dovednosti pro efektivní práci s protokoly operačního systému.

Pracovní prostředí

Výuku lze realizovat v prostředí:

- Cylab JCEKB, operační systém Windows 10

Pro práci postačí standardní nástroje, některé další budou v rámci průběhu scénáře nainstalovány.

1 Práce s protokoly ve Windows – teoretický základ

Obdobně jako každý moderní operační systém i operační systémy Windows pracují s tzv. protokoly událostí (logy). Záznamy (tedy události) v protokolech mohou vytvářet jak hlavní komponenty OS, tak i služby a aplikační programy, případně jako reakce na uživatelskou aktivitu.

1.1 Protokoly ve Windows

Protokoly ve Windows – v terminologii tohoto operačního systému logy událostí (Event Log) – se člení do řady kategorií/skupin a jsou ukládány ve strukturované podobě. Součástí Windows je nástroj *Prohlížeč událostí*, který umožňuje interaktivní práci s jednotlivými skupinami protokolů. Mezi základní kategorie patří:

- *Systém* – události spojené s operačním systémem a jeho jednotlivými částmi
- *Aplikace* – události spojené s jednotlivými uživatelskými aplikacemi
- *Zabezpečení* – události spojené s bezpečností operačního systému
- *Instalace* – události spojené s instalací operačního systému
- *Předané události* – události předané z ostatních počítačů ve stejné síti

Zápis událostí mají na starosti tzv. poskytovatelé/zdroje (Event Log Providers) a může jít například o službu, program či ovladač. Existují různé typy – *vyučující dle zkušeností a plánu zmíní MOF, WPP, Manifest, TraceLogging*).

Anglický pojem *log* je v kontextu operačního systému linuxového typu využíván jak pro označení jednotlivého záznamu v souboru s protokolem, tak i pro samotný soubor protokolu. Operační systémy Windows pracují s pojmy události a protokoly.

2 Pokročilá práce s protokoly ve Windows – praktické ukázky a cvičení

V této části vyučující představí jednotlivé příklady pokročilé práce s protokoly. Na tyto ukázky bude průběžně navazovat samostatná práce studentů (kontrolní body).

2.1 Pracovní prostředí

Výuku lze realizovat v prostředí Cylab JCEKB, operační systém Windows.

3 Prohlížeč událostí

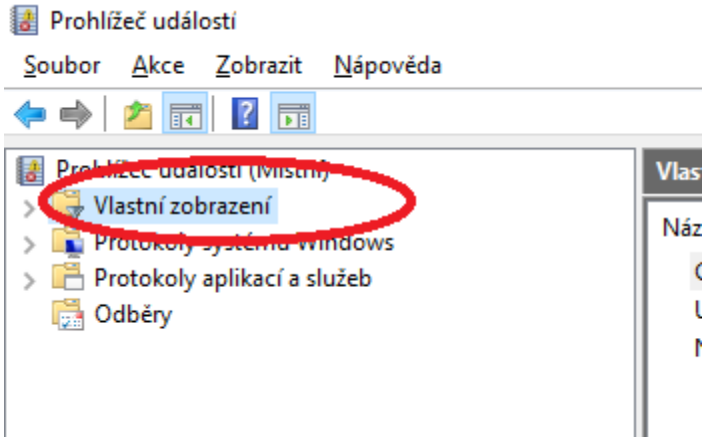
V aktuálních verzích operačního systému Windows je k dispozici nástroj *Prohlížeč událostí*.

Vyučující vysvětlí možnosti spuštění (přímo přes nabídku Start v rámci vyhledávání Prohlížeč událostí, eventvwr.exe). Dále vyučující předvede základní ovládání tohoto nástroje.

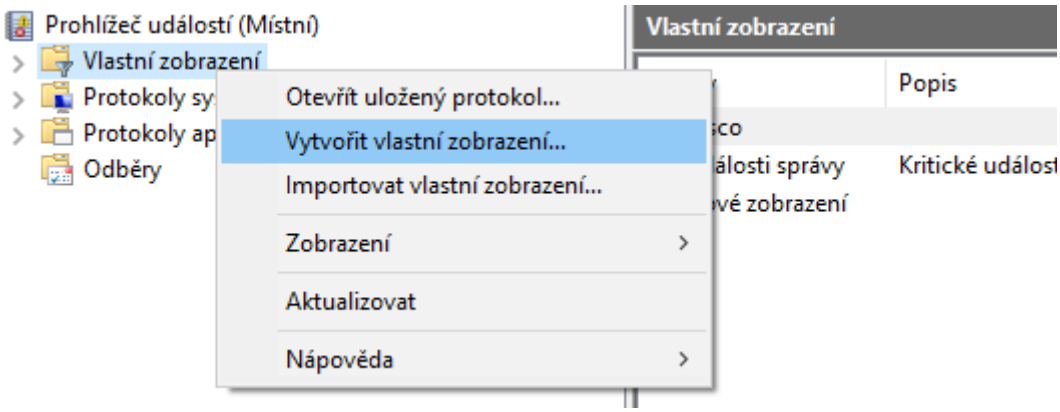
3.1 Vlastní zobrazení

V následujícím postupu je předvedeno využití vlastního zobrazení. Jde o inspiraci, vyučující může předvést reálný příklad na základě svých zkušeností nebo představ.

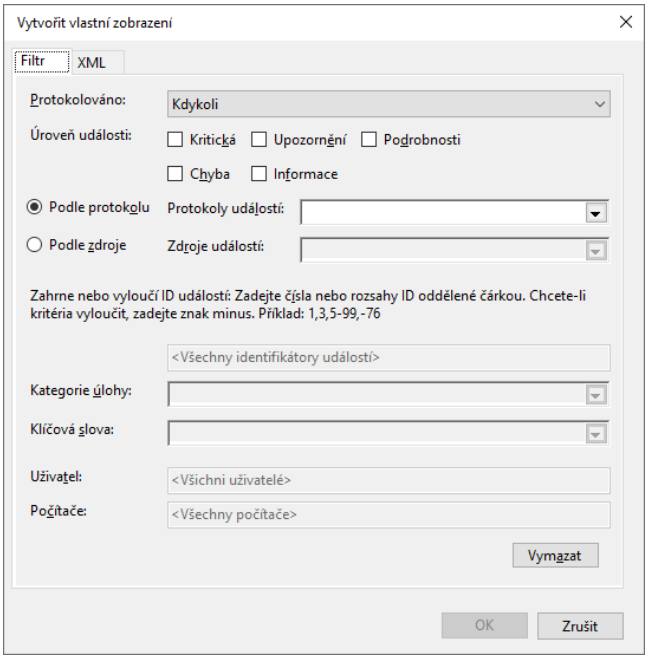
Na samém začátku je vhodné ukázat, kde se vlastní zobrazení nachází:



Po stisku pravého tlačítka myši na položce *Vlastní zobrazení* se objeví následující kontextová nabídka, v rámci které je pro tento scénář důležitá položka *Vytvořit vlastní zobrazení*:



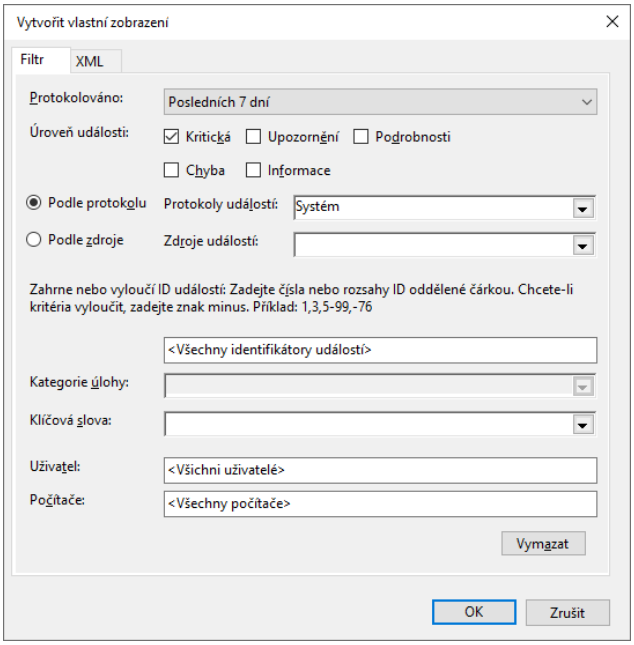
Vyučující vysvětlí jednotlivé položky dialogu Vytvořit vlastní zobrazení:



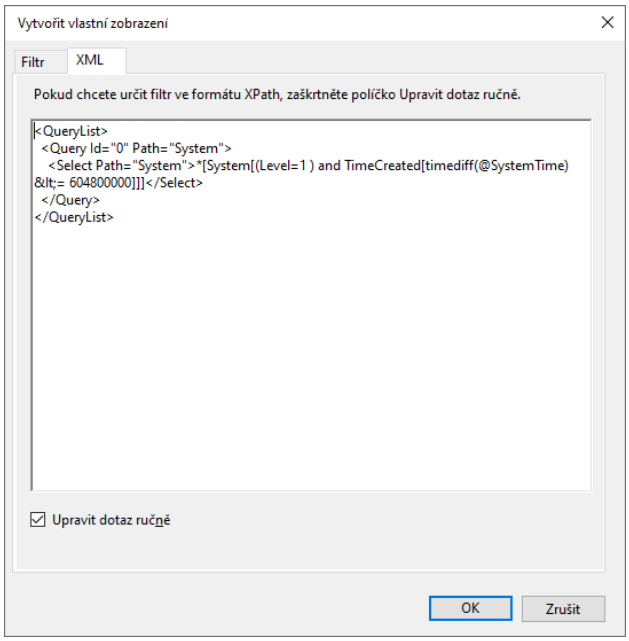
V rámci tohoto scénáře jsou důležité položky:

- *Protokolováno* – definuje podmínky podle časového rozmezí vzniku záznamu (události) protokolu
- *Úroveň události* – umožňuje ovlivnit výběr událostí podle tzv. severity, tedy závažnosti, od informativních událostí až po kritické.
- *Podle protokolu* – umožňuje určit, jaké protokoly budou pro vlastní zobrazení využité. Protokolů je možné vybrat více (rozumně až 10, poté může dojít k varování či zpomalení odezvy).
- *Podle zdroje událostí* – umožňuje určit, jaké zdroje budou pro vlastní zobrazení využité. Zdrojů je možné vybrat více (rozumně až 10, poté může dojít k varování či zpomalení odezvy). *Vyučující upozorní na to, že je možné pracovat buď s protokoly nebo se zdroji událostí.*

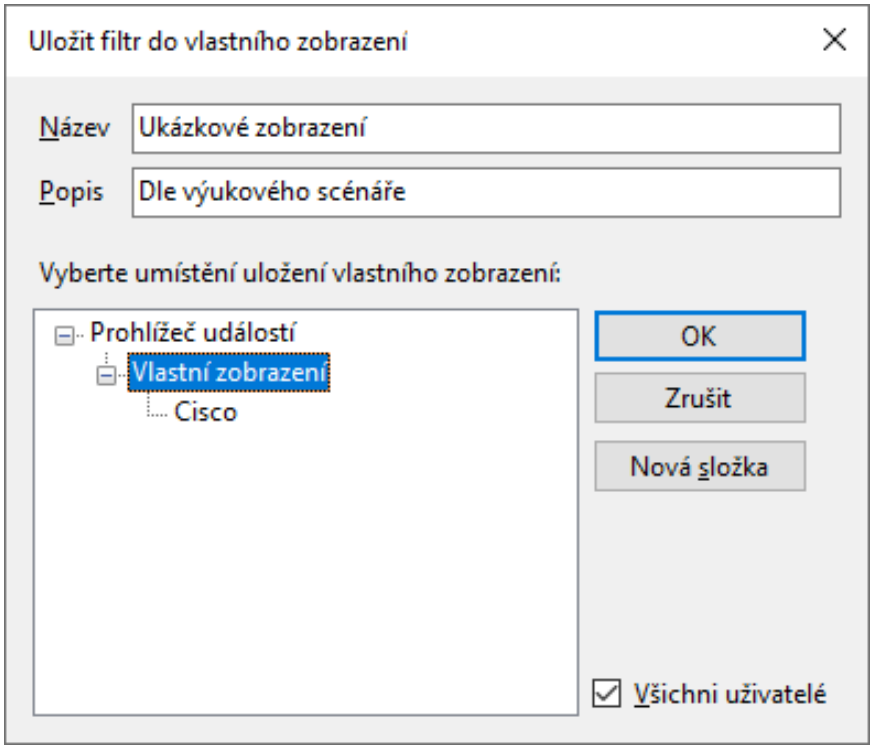
Pro předvedení bude použita následující konfigurace vlastního zobrazení:



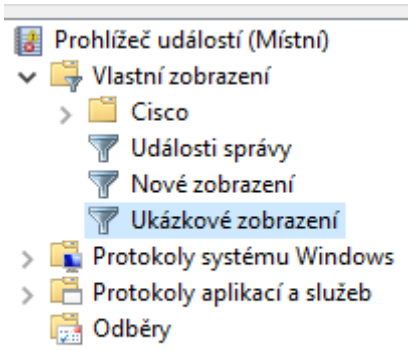
Vyučující dále předvede zobrazení XML, případně dle svých zkušeností vysvětlí i možnost ruční editace.



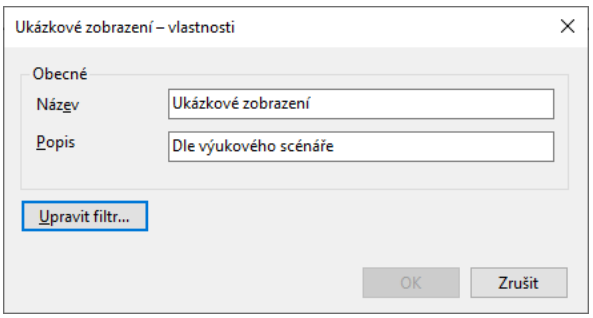
K druhému kroku ve vytváření vlastního zobrazení dojde po stisku tlačítka *OK*, po kterém se objeví následující dialog (již jsou předvyplněné hodnoty dle záměru scénáře).



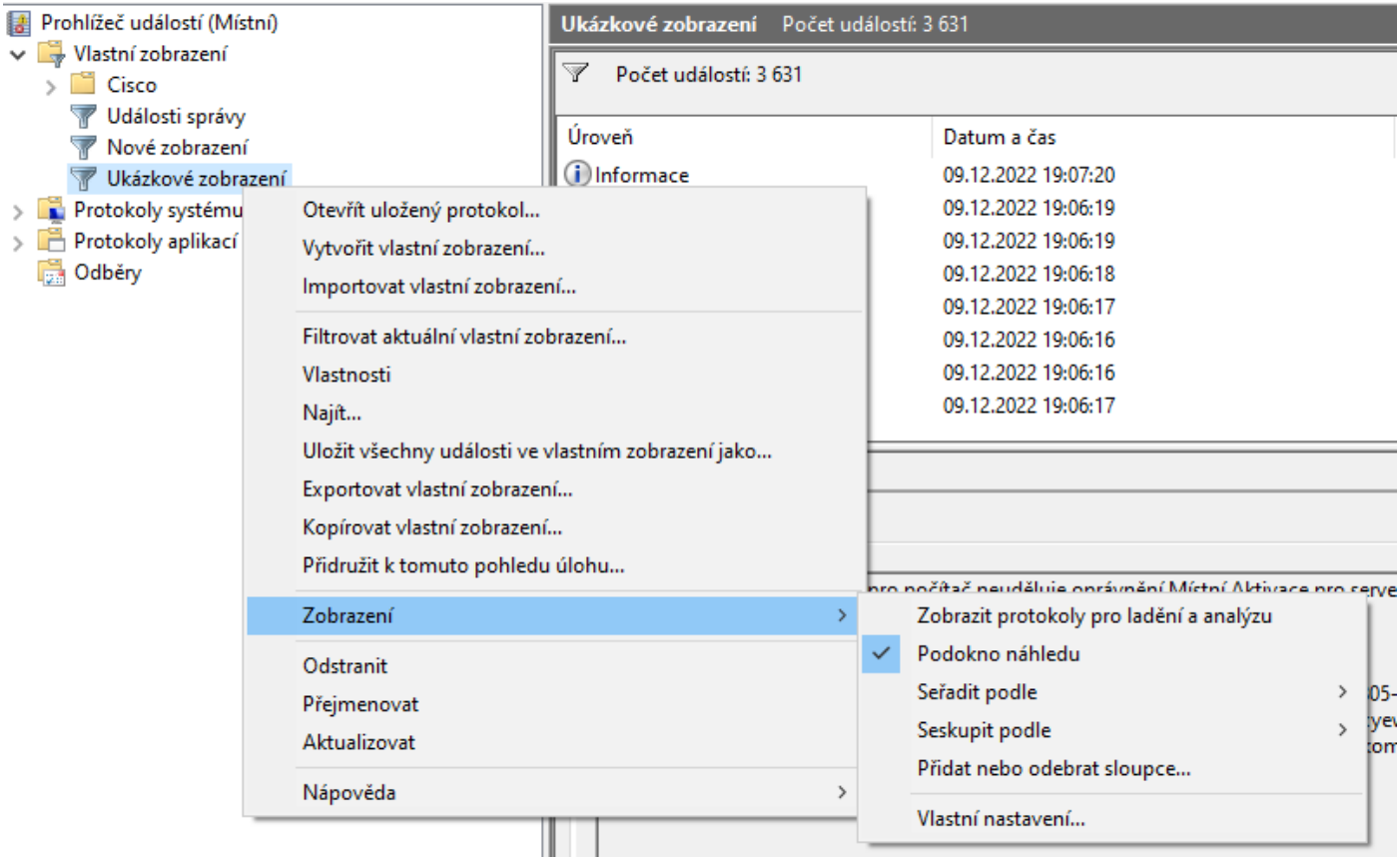
Po stisku tlačítka *OK* dojde k vytvoření požadovaného vlastního zobrazení a k jeho začlenění do struktury na požadované místo. Současně jsou vyfiltrovány ovlivněné události (*vyučující může ukázat jak prázdný výsledek, tak i vliv změny jednotlivých parametrů definice vlastního zobrazení. Toto je vhodné si vyzkoušet před výukou*).



Úpravu vlastního zobrazení je možné provést například z kontextové nabídky nad příslušným vlastním zobrazení, a to *Vlastnosti*, následně tlačítko *Upravit filtr*.



Dle potřeby dále vyučující vysvětlí další položky kontextové nabídky pro příslušné vlastní zobrazení:



Cílem této části (vlastní zobrazení) není poskytnout studentům vyčerpávající přehled možní, ale pouze seznámení s možností vytvořit si vlastní zobrazení jako základ pro případnou optimalizaci administrátorských činností využívajících GUI.

Kontrolní bod

Studenti si vytvoří vlastní zobrazení v rámci Prohlížeče událostí; zváží vhodná nastavení a parametry

4 Pokročilé možnosti při využití technologie PowerShell

Velmi silnou stránkou objektového shellu PowerShell (například viz samostatný scénář) je efektivní práce s protokoly. V této části scénáře jsou zahrnuty základní techniky, které mohou vyučující i studenti dále rozvíjet dle specifických požadavků dané hodiny.

Vyučující předvede spuštění pracovního prostředí PowerShell (v rámci tohoto scénáře Spustit jako správce).

4.1 Základní výpisy protokolů

Následující konstrukce vypíše jednotlivé protokoly dostupné v rámci lokálního počítače.

```
PS c:\Users\syadmin> Get-WinEvent -ListLog * -ComputerName localhost
```

Výstup (dle skutečného obsahu, zkráceno):

```
LogMode   MaximumSizeInBytes RecordCount LogName
-------   ------------------ ----------- -------
Circular           15728640        1855 Windows PowerShell
Circular           20971520       34288 System
Circular           20971520       31036 Security
Circular            1052672        3177 OAlerts
Circular           20971520           0 Key Management Service
Circular            1052672           0 Internet Explorer
...
```

Vyučující vysvětlí jednotlivé sloupce (typ protokolu – zde kruhový, maximální velikost protokolu, stávající počet záznamů a název protokolu; další trvalý a automaticky zálohovaný). Dle uvážení předvede vazbu na Prohlížeč událostí.

Shodného výsledku je možné dosáhnout použitím IP adresy 127.0.0.1, případně jakékoli jiné loopback adresy.

```
PS c:\Users\syadmin> Get-WinEvent -ListLog * -ComputerName 127.0.0.90
```

Výstup (dle skutečného obsahu, zkráceno):

```
LogMode   MaximumSizeInBytes RecordCount LogName
-------   ------------------ ----------- -------
Circular           15728640        1855 Windows PowerShell
Circular           20971520       34288 System
Circular           20971520       31036 Security
Circular            1052672        3177 OAlerts
Circular           20971520           0 Key Management Service
Circular            1052672           0 Internet Explorer
...
```

Vyučující upozorní na možnost zobrazení protokolů i ze vzdáleného počítače.

Následující konstrukce omezí pomocí `Where-Object` výpis pouze na ty protokoly, které nejsou prázdné (*vyučující následně dle potřeby zmíní i jiné zápisy, např.* `Get-WinEvent -ListLog * -ComputerName 127.0.0.90 | Where-Object { $_.RecordCount -gt 0}`). Konstrukce podmínky vyhodnocuje, zda existuje alespoň nějaký záznam v jednotlivém protokolu (*u příkladu vyučujícího pak, zda je počet větší nule*).

```
PS c:\Users\syadmin> Get-WinEvent -ListLog * -ComputerName 127.0.0.90 | Where-Object { $_.RecordCount }
```

Výstup (dle skutečného obsahu, zkráceno):

```
LogMode   MaximumSizeInBytes RecordCount LogName
-------   ------------------ ----------- -------
Circular            15728640        1855 Windows PowerShell
Circular            20971520       34288 System
Circular            20971520       31007 Security
Circular             1052672        3177 OAlerts
Circular             4000000        5186 Cisco AnyConnect Secure Mobility Client
Circular            20971520       17002 Application
Circular             1052672          97 Setup
...
```

Kontrolní bod

Studenti s vyučujícím diskutují, jak by ještě mohla vypadat podmínka pro Where-Object. Nejde o syntaxi, ale nápady.

4.2 Základní výpisy protokolu – záznamů

Následující konstrukce vypíše všechny události z protokolu *System*, a to pro jednotlivé providery/zdroje (vyučující upozorní na *Get-WinEvent -ListProvider **).

```
PS c:\Users\syadmin> Get-WinEvent -LogName System
```

Výstup (dle skutečného obsahu, zkráceno):

```
ProviderName: Microsoft-Windows-Time-Service

TimeCreated                     Id LevelDisplayName Message
-----------                     -- ---------------- -------
09.12.2022 20:51:47            158 Informace        The time provider 'VMICTimeProvider'
has indicated that the current hardware and operating environment is not supported and has
stopped. This behavior is expected for VMICTimeProvi...


   ProviderName: Microsoft-Windows-Kernel-General

TimeCreated                     Id LevelDisplayName Message
-----------                     -- ---------------- -------
09.12.2022 20:51:47              1 Informace        Systémový čas se změnil
09.12.2022 20:51:47             24 Informace        Informace o časovém pásmu byly
aktualizovány s důvodem pro ukončení 0. Aktuální posun časového pásma je -60.
...
```

Vyučující předvede a vysvětlí následující konstrukce:

- `Get-WinEvent -LogName System -MaxEvents 5` – vypíše pět nejnovějších událostí z protokolu System
- `Get-WinEvent -LogName System -MaxEvents 5 | Select-Object TimeCreated, ID, ProviderName, LevelDisplayName, Message` – vypíše pět nejnovějších událostí z protokolu System (předá je pomocí roury do dalšího zpracování s výběrem atributů `TimeCreated, ID, ProviderName, LevelDisplayName, Message` a vypíše je v skupení podle jednotlivých událostí.

Dále vyučující ke druhému z výše uvedených příkladů dodá přesměrování v rouře do úpravy zobrazení `| Format-Table -AutoSize` a `| Out-GridView`. *Vyučující se studenty blíže diskutuje vliv na výsledné zobrazení.*

Kontrolní bod

Studenti vypíší 15 nejnovějších událostí souvisejících s bezpečností do gridu

(řešení: `Get-WinEvent -LogName Security -MaxEvents 15 | Out-GridView`)

Následující konstrukce omezí výpis pouze na ty události, které v textovém popisu obsahují řetězec USB.

```
PS c:\Users\syadmin> Get-WinEvent -LogName System | Where {$_.Message -like "*USB*"}
```

Výstup (dle skutečného obsahu, zkráceno):

```
ProviderName: Microsoft-Windows-Ntfs

   ProviderName: Microsoft-Windows-Kernel-PnP

TimeCreated                     Id LevelDisplayName Message
-----------                     -- ---------------- -------
16.12.2022 16:37:35            219 Upozornění       The driver \Driver\WudfRd failed to
load for the device USB\VID_08E6&PID_3437\7&2e44c8bd&0&3.
15.12.2022 20:26:52            219 Upozornění       The driver \Driver\WudfRd failed to
load for the device USB\VID_08E6&PID_3437\7&2e44c8bd&0&3.
12.12.2022 5:29:46             219 Upozornění       The driver \Driver\WudfRd failed to
load for the device USB\VID_08E6&PID_3437\7&2e44c8bd&0&3.
11.12.2022 20:06:47            219 Upozornění       The driver \Driver\WudfRd failed to
load for the device USB\VID_08E6&PID_3437\7&2e44c8bd&0&3
...
```

Vyučující vybere vhodnou událost a pokusí se ji se studenty identifikovat i v Prohlížeči událostí. V návaznosti na své znalosti rozebere se studenty detail záznamu.

Následující konstrukce vypíše 5 nejnovějších událostí, a to pouze chyby (level=2). *Vyučující upozorní na jiný formát zápisu pomocí FilterHashtable*.

```
PS c:\Users\syadmin> Get-WinEvent -MaxEvents 5 -FilterHashtable @{LogName="System";level=2}
```

Výstup (dle skutečného obsahu, zkráceno):

```
ProviderName: Service Control Manager

TimeCreated                     Id LevelDisplayName Message
-----------                     -- ---------------- -------
12.12.2022 5:29:48            7000 Chyba            Služba DgiVecp neuspěla při spuštění v
důsledku následující chyby: ...
11.12.2022 20:06:51           7000 Chyba            Služba DgiVecp neuspěla při spuštění v
důsledku následující chyby: ...


   ProviderName: Server

TimeCreated                     Id LevelDisplayName Message
-----------                     -- ---------------- -------
11.12.2022 16:54:38           2505 Chyba            Server nemohl vytvořit vazbu na přenos
\Device\NetBT_Tcpip_{56859541-D195-4641-9A1C-9B74C882EC2B}, protože jiný počítač v síti má
stejný název. Server nelze spustit.
11.12.2022 16:54:38           2505 Chyba            Server nemohl vytvořit vazbu na přenos
\Device\NetBT_Tcpip_{FC22C78F-8C34-4FB1-9831-447B932D04E2}, protože jiný počítač v síti má
stejný název. Server nelze spustit.
11.12.2022 16:54:38           2505 Chyba            Server nemohl vytvořit vazbu na přenos
\Device\NetBT_Tcpip_{56859541-D195-4641-9A1C-9B74C882EC2B}, protože jiný počítač v síti má
stejný název. Server nelze spustit.
```

```
11.12.2022 16:54:38           2505 Chyba           Server nemohl vytvořit vazbu na přenos
\Device\NetBT_Tcpip_{FC22C78F-8C34-4FB1-9831-447B932D04E2}, protože jiný počítač v síti má
stejný název. Server nelze spustit.
11.12.2022 16:54:38           2505 Chyba           Server nemohl vytvořit vazbu na přenos
\Device\NetBT_Tcpip_{56859541-D195-4641-9A1C-9B74C882EC2B}, protože jiný počítač v síti má
stejný název. Server nelze spustit.
...
```

Vyučující vysvětlí jednotlivé levely a předvede výše uvedenou konstrukci pro upozornění (level 3).

Jednotlivé úrovně:

1 – kritická událost

2 – chyba

3 – upozornění

4 – informace

5 - podrobnosti

Vyučující dále dle svých znalostí může zmínit, jak definovat úrovně protokolování (včetně hodnoty 0 pro všechny události).

4.3 Export a konverze událostí

Pomocí PowerShellu je velmi snadné události exportovat, a to včetně konverze do vybraného formátu. Následující příkaz vypíše pět nejnovějších událostí z protokolu *Systém* a provede jejich konverzi do formátu CSV včetně uložení do souboru:

```
PS c:\Users\syadmin> Get-WinEvent -LogName System -MaxEvents 5 | Export-Csv logy.csv
```

Výstup předvede vyučující zobrazením souboru logy.csv a ukáže i další možnost konverze do XML.

```
PS c:\Users\syadmin> Get-WinEvent -LogName System -MaxEvents 5 | Export-Clixml logy.xml
```

Konverzi lze provádět i bez uložení do souboru, například do formátu HTML:

```
PS c:\Users\syadmin> Get-WinEvent -LogName System -MaxEvents 5 | ConvertTo-Html
```

Výstup (dle skutečného obsahu, zkráceno):

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<title>HTML TABLE</title>
</head><body>
<table>
<colgroup><col/><col/><col/><col/><col/><col/><col/><col/><col/><col/><col/><col/><co
l/><col/><col/><col/><col/><col/><col/><col/><col/><col/><col/><col/><col/><col/></colgroup
>
<tr><th>Message</th><th>Id</th><th>Version</th><th>Qualifiers</th><th>Level</th><th>Task</t
h><th>Opcode</th><th>Keywords</th><th>RecordId</th><th>ProviderName</th><th>ProviderId</th>
<th>LogName</th><th>ProcessId</th><th>ThreadId</th><th>MachineName</th><th>UserId</th><th>T
```

```
imeCreated</th><th>ActivityId</th><th>RelatedActivityId</th><th>ContainerLog</th><th>Matche
dQueryIds</th><th>Bookmark</th><th>LevelDisplayName</th><th>OpcodeDisplayName</th><th>TaskD
isplayName</th><th>KeywordsDisplayNames</th><th>Properties</th></tr>
<tr><td>Režim spuštěn&#237; služby Služba inteligentn&#237;ho přenosu na pozad&#237; byl
změněn z spouštěn&#237; na vyž&#225;d&#225;n&#237; na automatick&#233;
spouštěn&#237;.</td><td>7040</td><td>0</td><td>16384</td><td>4</td><td>0</td><td>0</td><td>
-9187343239835811840</td><td>37963</td><td>Service Control Manager</td><td>555908d1-a6d7-
4695-8e1e-26931d2012f4</td><td>System</td><td>820</td><td>1784</td><td>DESKTOP-
Q7RIU78</td><td>S-1-5-18</td><td>12.12.2022
17:42:41</td><td></td><td></td><td>System</td><td>System.UInt32[]</td><td>System.Diagnostic
s.Eventing.Reader.EventBookmark</td><td>Informace</td><td></td><td></td><td>System.Collecti
ons.ObjectModel.ReadOnlyCollection`1[System.String]</td><td>System.Collections.Generic.List
`1[System.Diagnostics.Eventing.Reader.EventProperty]</td></tr>
...
```

Vyučující dále předvede možnost přesměrování výše uvedené konverze do souboru (`Get-WinEvent -LogName System -MaxEvents 5 | ConvertTo-Html | Out-File logy.html`) a předvede další možnosti konverze do Csv (`ConvertTo-Csv`).

4.4 Zapsání události

Následující příklad demonstruje možnost zapsání události do protokolu, a to konkrétně události s ID 40961 při využití poskytovatele Microsft-Windows-PowerShell.

```
PS c:\Users\syadmin> New-WinEvent -ProviderName Microsoft-Windows-PowerShell -Id 40961
```

Následující výpis potvrdí vložení události:

```
PS c:\Users\syadmin> Get-WinEvent -ProviderName Microsoft-Windows-PowerShell -MaxEvent 1
```

Výstup:

```
ProviderName: Microsoft-Windows-PowerShell

TimeCreated                     Id LevelDisplayName Message
-----------                     -- ---------------- -------
12.02.2023 17:54:13          40961 Informace        PowerShell console is starting up
```

Vyučující předvede nalezení události v prohlížeči událostí, např.:

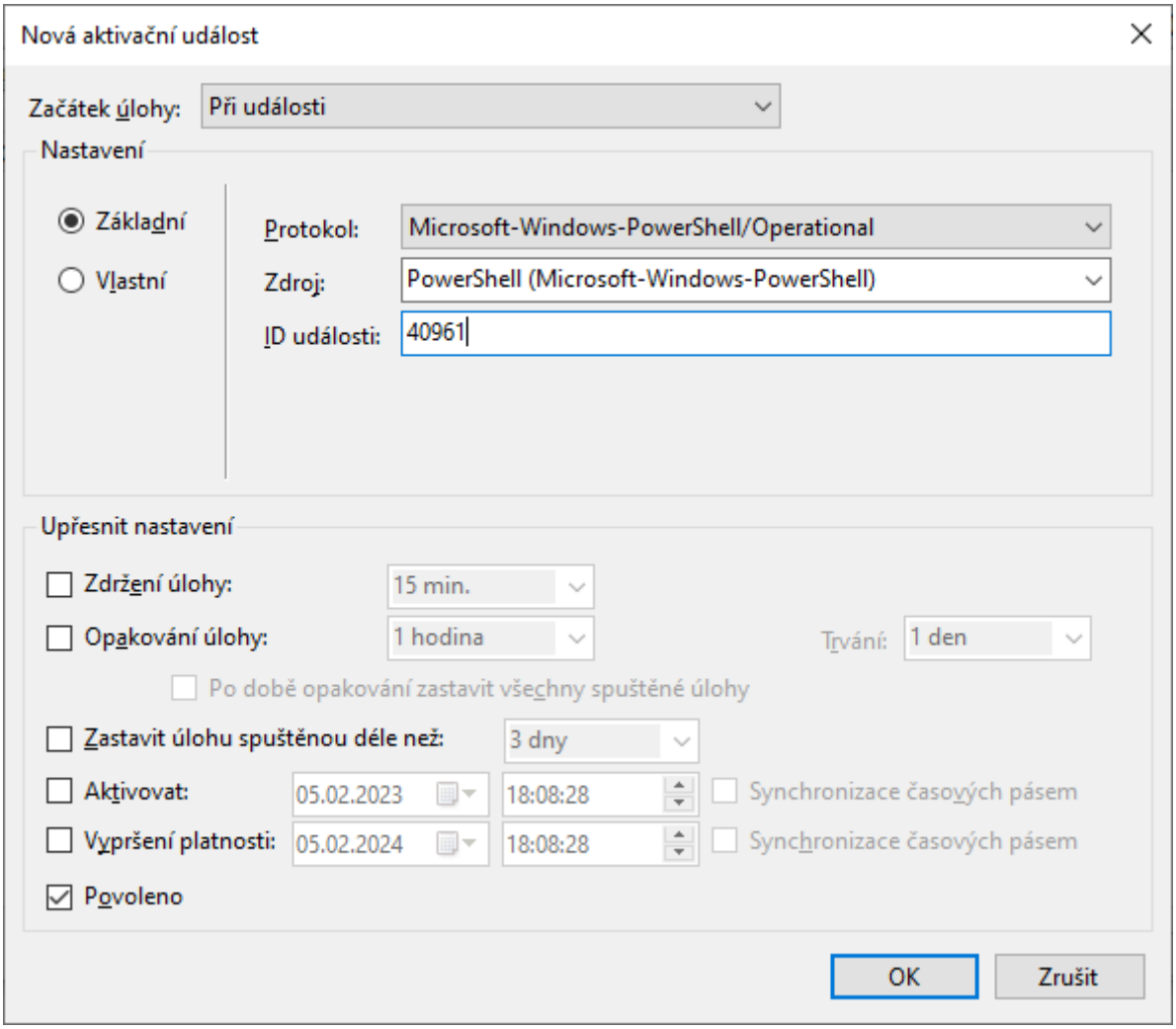
`Prokoly aplikací a služeb -> Windows -> PowerShell->Operational`

Kontrolní bod

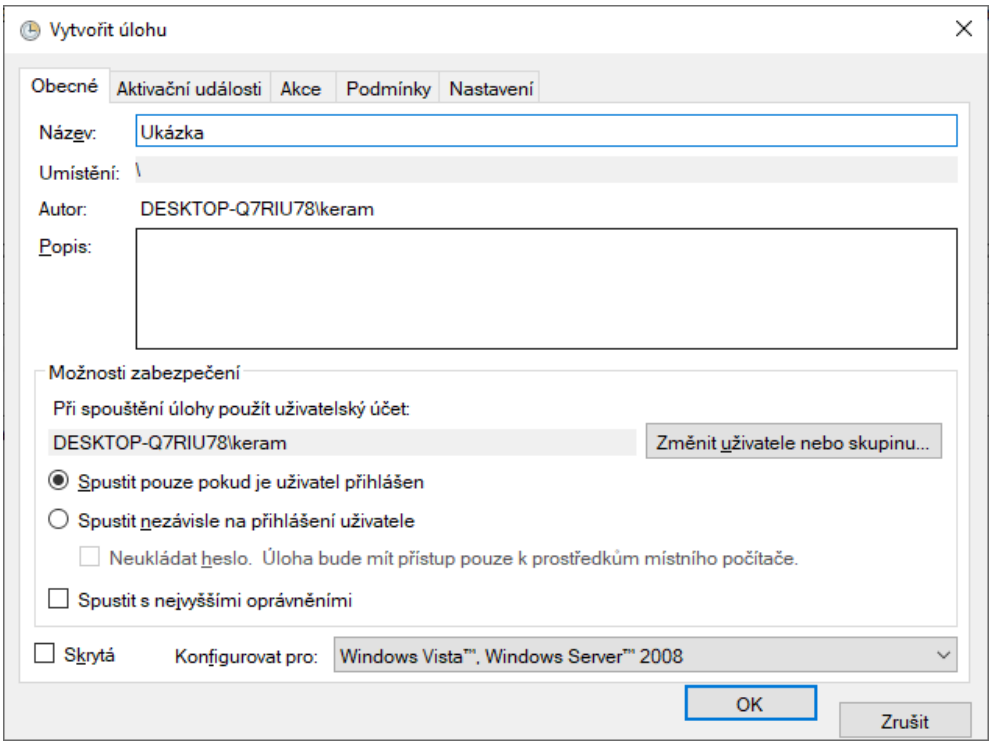
Studenti si sami ověří zapsání a zobrazení události pro Microsoft-Windows-PowerShell a ID 40961, a to bez zobrazení předchozího příkladu (vyučující dle svého uvážení může poskytnout nápovědu).

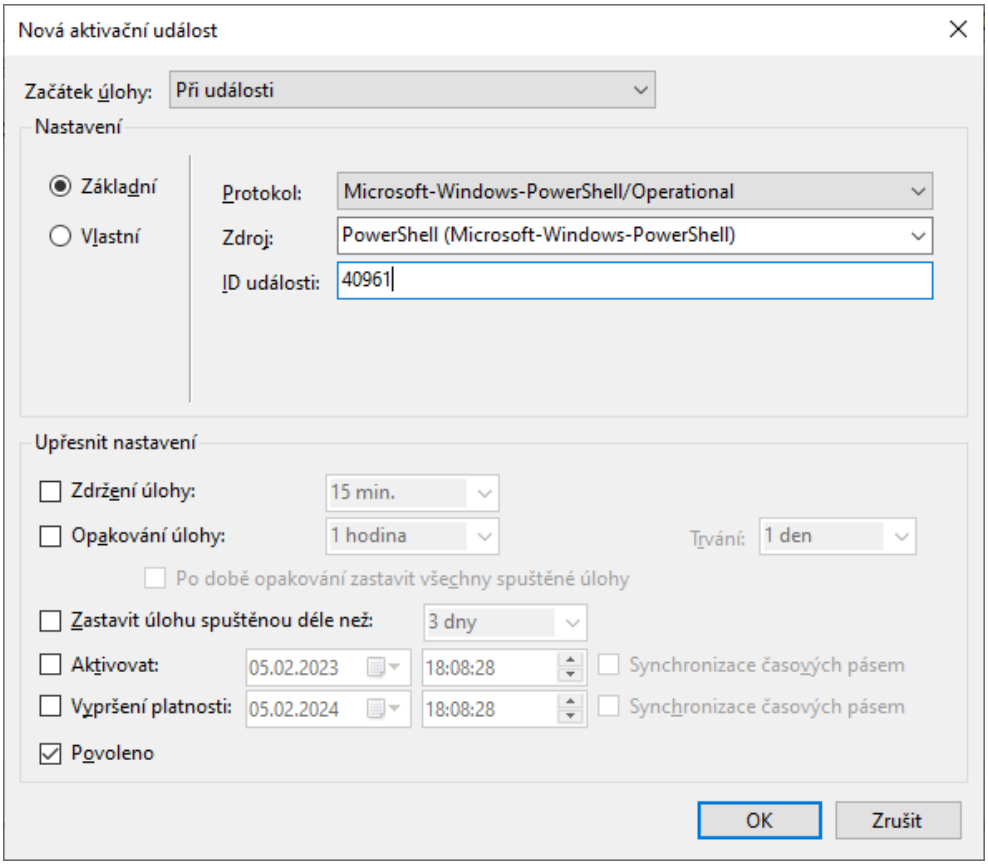
5 Propojení s Plánovačem úloh

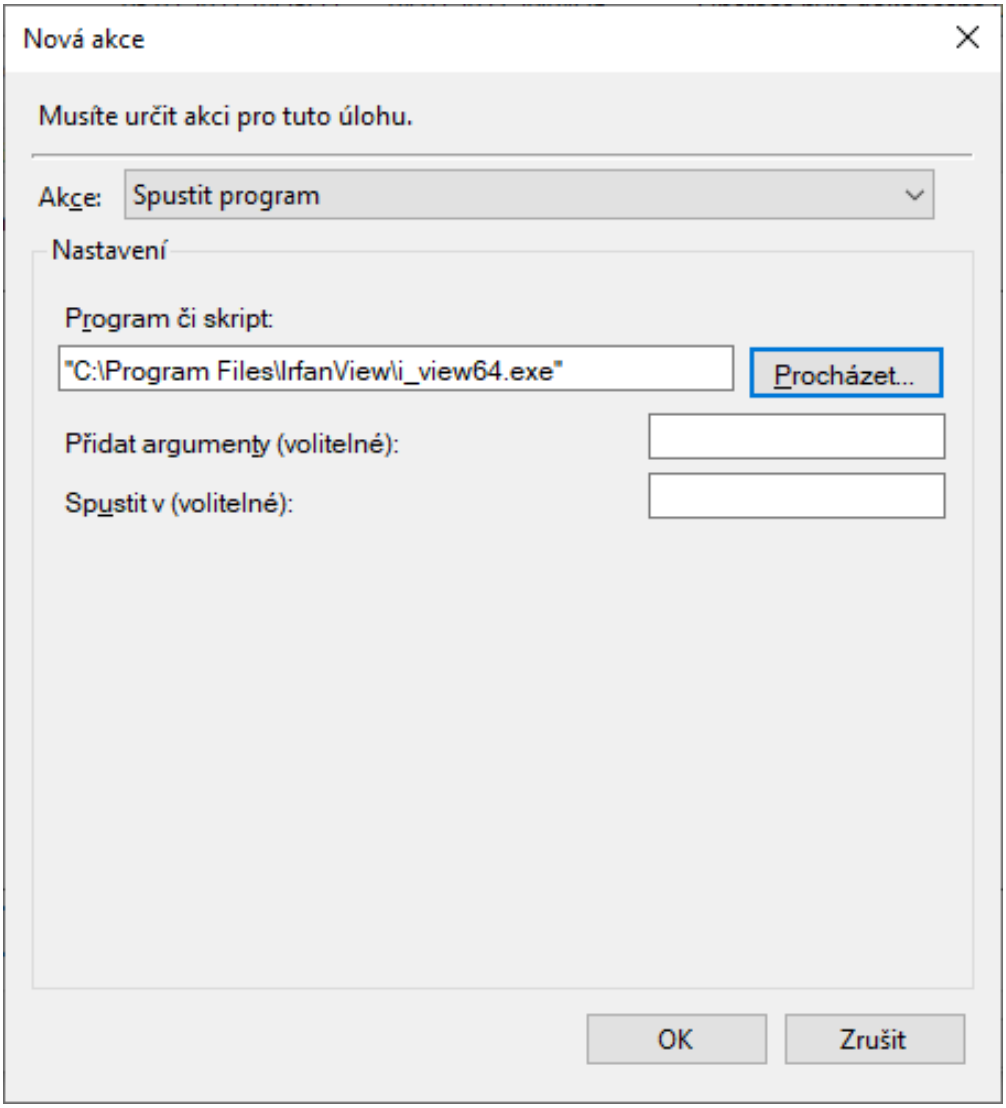
Události ve Windows je možné využít také jako aktivaci v rámci Plánovače úloh. Při vytváření nové úlohy může definice vypadat například následujícím způsobem, kdy je aktivace navázána na výskyt události zapsané do protokolů dle kapitoly *4.4 Zapsání událostí*.



Celý postup po spuštění Plánovače úloh demonstrují následující snímky a vyučující jej aktivně využije pouze za předpokladu, že studenti jsou již s plánováním úloh obeznámeni.




Nová aktivační událost
Začátek úlohy:
Při události
Nastavení
Základní
Vlastní
Protokol:
Microsoft-Windows-PowerShell/Operational
Zdroj:
PowerShell (Microsoft-Windows-PowerShell)
ID události:
40961
Upřesnit nastavení
Zdržení úlohy:
15 min.
Opakování úlohy:
1 hodina
Trvání:
1 den
Po době opakování zastavit všechny spuštěné úlohy
Zastavit úlohu spuštěnou déle než:
3 dny
Aktivovat:
05.02.2023
18:08:28
Synchronizace časových pásem
Vypršení platnosti:
05.02.2024
18:08:28
Synchronizace časových pásem
Povoleno
OK
Zrušit



S tímto minimálním nastavením lze provázat událost se spuštěním programu, v tomto konkrétním případě prohlížeče obrázků. *Vyučující demonstruje použití a diskutuje nad dalšími způsoby využití takového provázání (například reakce na bezpečnostní události apod.).*

Shrnutí a závěr

Studenti se seznámili jak se základy protokolů v operačních systémech Windows, tak i s technikami práce za využití PowerShellu. Dle svého uvážení může vyučující připravit pro studenty například test, a to jak z pohledu teorie, tak i praktického opakování nad zdokumentovanými postupy.

Seznam použitých zdrojů

Learn. *Dokumentace k prostředí PowerShell*. Dostupné z: https://learn.microsoft.com/cs-cz/powershell/

Nápověda Windows. Dostupné z operačního systému.