

Po kliknutí na položku menu CM IT Monitoring -> Event server -> Udalosti zo zberov sa vám zobrazí zoznam, obsahujúci udalosti nachádzajúce sa na serveri, zoradené od najnovších po najstaršie.

Vo vrchnej časti zobrazenia je možné filtrovať zobrazené udalosti na základe:

- názvu spoločnosti,
- názvu zberu,
- názvu počítača (CMID aj názov počítača),
- periody výskytu,
- užívateľa

V predvolenom zobrazení sú uvedené informácie (stĺpce):

- spoločnosť,
- počítač (CMID),
- názov zberu,
- typ udalosti,
- dátum a čas výskytu,
- skupina do ktorej daná udalosť patrí,
- stav udalosti (Potvrdenie),
- EventID udalosti,
- meno logu,
- popis udalosti (v skrátenom a zjednodušenom tvare),
- poznámka k udalosti.

Stĺpce spoločnosť, počítač a názov zberu majú fixnú pozíciu a nedajú sa odstrániť. Pre lepšiu prehľadnosť sú sa však dajú skryť kliknutím na ikonu šípky, nachádzajúcu sa v ľavej časti zobrazenia.

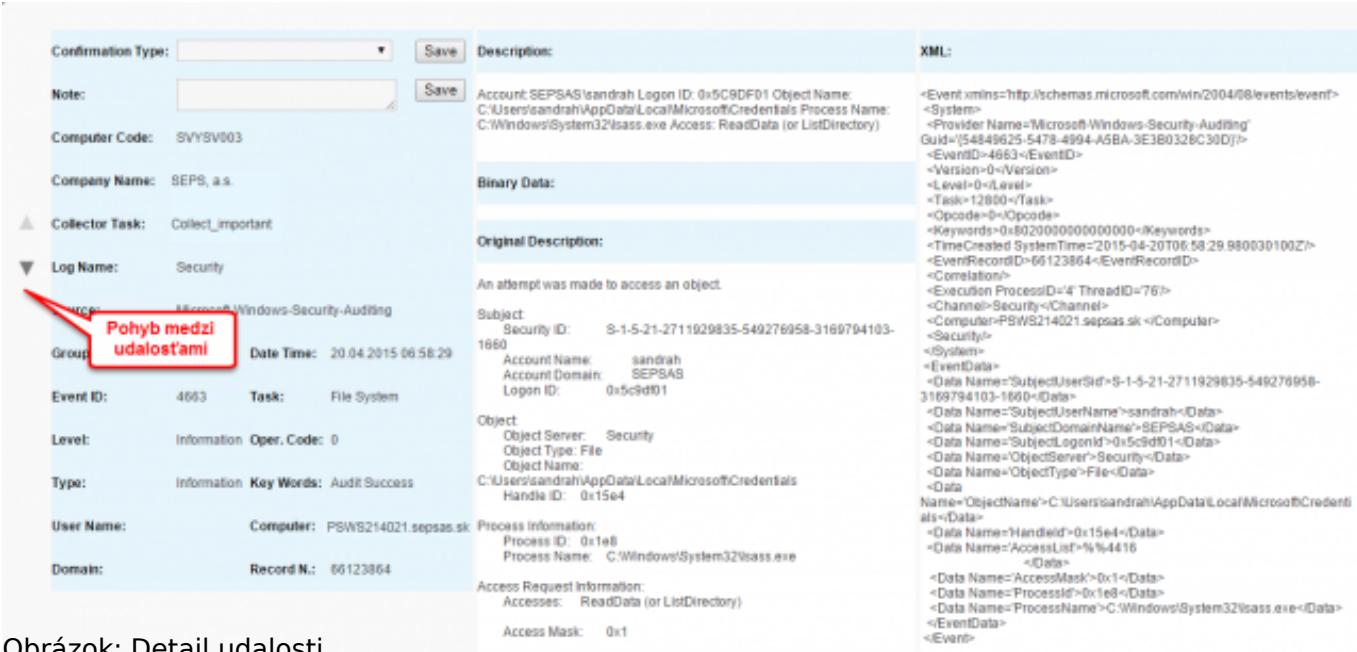
Company	Collector Task	Type	Date/Time	Group	Client ID	Confirmation	Log Name	Source	Task	Description
DEPS, a.s.	SYNTH003_ABK_col003	Information	29.04.2015 12:32:30	Logon	31	0 > [OP] M	Microsoft-Windows-Task	Microsoft-Windows-Task		Logged-on. SMBAccess: 35-45-14
DEPS, a.s.	SYNTH003_ABK_col003	Registry	20.04.2015 11:40:51	Install	0	0 > [OP] M	HKEY_LOCAL_MACHINE\Software\RegKey			Modified/unmodified registry key for 'OLV\MP\35-22-00_10-22-00' (0E322B86-3C71-4881-BF35-7988A9FAC3D)
DEPS, a.s.	SYNTH003_ZAKAD_00001	Critical	29.04.2015 07:52:15	Error	100	0 > [OP] M	Microsoft-Windows-Diagnostics	Microsoft-Windows-Diagnostics		System maintenance detected issues requiring your attention. A notification was sent to the Action Center.
DEPS, a.s.	SYNTH003_ZAKAD_00001	Critical	29.04.2015 07:52:18	Error	100	0 > [OP] M	Microsoft-Windows-Diagnostics	Microsoft-Windows-Diagnostics		System maintenance detected issues requiring your attention. A notification was sent to the Action Center.
DEPS, a.s.	SYNTH003_ZAKAD_00001	Critical	20.04.2015 07:52:18	Error	100	0 > [OP] M	Microsoft-Windows-Diagnostics	Microsoft-Windows-Diagnostics		System maintenance detected issues requiring your attention. A notification was sent to the Action Center.
DEPS, a.s.	SYNTH003_ZAKAD_00001	Critical	29.04.2015 06:40:15	Error	100	0 > [OP] M	Microsoft-Windows-Diagnostics	Microsoft-Windows-Diagnostics		System maintenance detected issues requiring your attention. A notification was sent to the Action Center.
DEPS, a.s.	SYNTH003_ABK_col003	Critical	20.04.2015 06:40:18	Error	100	0 > [OP] M	Microsoft-Windows-Diagnostics	Microsoft-Windows-Diagnostics		System maintenance detected issues requiring your attention. A notification was sent to the Action Center.
DEPS, a.s.	SYNTH003_ABK_col003	Critical	20.04.2015 06:40:19	Error	100	0 > [OP] M	Microsoft-Windows-Diagnostics	Microsoft-Windows-Diagnostics		System maintenance detected issues requiring your attention. A notification was sent to the Action Center.
DEPS, a.s.	SYNTH003_ABK_col003	Critical	20.04.2015 06:40:19	Error	100	0 > [OP] M	Microsoft-Windows-Diagnostics	Microsoft-Windows-Diagnostics		System maintenance detected issues requiring your attention. A notification was sent to the Action Center.
DEPS, a.s.	SYNTH003_ABK_col003	Critical	29.04.2015 06:40:19	Error	100	0 > [OP] M	Microsoft-Windows-Diagnostics	Microsoft-Windows-Diagnostics		System maintenance detected issues requiring your attention. A notification was sent to the Action Center.
DEPS, a.s.	SYNTH003_ABK_col003	Information	29.04.2015 05:38:38	Power UserLogon	4000	0 > [OP] M	Security	Microsoft-Windows-Security	Security State Change	Windows is starting up. The event is logged when L20000000 starts and the auditing subsystem is initialized.

Obrázok: Popis základného zobrazenia

Ak chcete zobraziť detailné informácie udalosti, kliknite na zvolený riadok. Otvorí sa vám dialógové okno v ktorom dodatočne vidíte (ak sú dostupné):

- rolovací zoznam pre zadanie stavu potvrdenia,
- užívateľa ktorý zadal posledný stav potvrdenia,
- údaj o dátume a čase poslednej zmeny stavu potvrdenia,
- zdroj z ktorého pochádza udalosť (Source),
- úlohu, ktorá vytvorila udalosť,
- úroveň výstrahy (level),
- operačný kód,

- kľúčové slová,
- užívateľské meno,
- názov počítača,
- doménu,
- číslo záznamu,
- popis udalosti v zjednodušenej podobe (a prípadne príslušné binárne dátumy),
- pole pre zadanie poznámky,
- originálne znenie udalosti (generované operačným systémom),
- XML znenie udalosti (generované operačným systémom).



The screenshot shows the 'Event Details' page of the Customer Monitor application. At the top, there are fields for 'Confirmation Type' (dropdown), 'Save' button, 'Description' text area, and an 'XML:' button. Below these are sections for 'Note' (dropdown), 'Computer Code' (SVSYV003), 'Company Name' (SEPS, a.s.), and 'Collector Task' (Collect_Important). A 'Log Name' section shows 'Security'. The main content area displays event details:

Event Details:

- Group:** Windows-Security-Auditing
- Date Time:** 20.04.2015 06:58:29
- Event ID:** 4663
- Task:** File System
- Level:** Information
- Oper. Code:** 0
- Type:** Information
- Key Words:** Audit Success
- User Name:** Computer: PSWS214021.sepsas.sk
- Domain:** Record N.: 66123864

Object:

- Object Server: Security
- Object Type: File
- Object Name: C:\Users\sandrah\AppData\Local\Microsoft\Credentials
- Handle ID: 0x15e4

Access Request Information:

- Accesses: ReadData (or ListDirectory)
- Access Mask: 0x1

Description:

An attempt was made to access an object.

Original Description:

```

<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
<System>
<Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-A5BA-3E3B0328C30D}">
<EventID>4663</EventID>
<Version>0</Version>
<Level>0</Level>
<Task>12800</Task>
<Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords>
<TimeCreated SystemTime="2015-04-20T06:58:29.980030100Z" />
<EventRecordID>66123864</EventRecordID>
<Correlation/>
<Execution ProcessID="4" ThreadID="76" />
<Channel>Security</Channel>
<Computer>PSWS214021.sepsas.sk</Computer>
<System/>
<EventData>
<Data Name="SubjectUserSid">S-1-5-21-2711929835-549276958-3169794103-1660</Data>
<Data Name="SubjectUserName">sandrah</Data>
<Data Name="SubjectDomainName">SEPSAS</Data>
<Data Name="SubjectLogonId">0x5c9d01</Data>
<Data Name="ObjectType">Security</Data>
<Data Name="ObjectName">File</Data>
<Data Name="ObjectName">C:\Users\sandrah\AppData\Local\Microsoft\Credentials</Data>
<Data Name="HandleId">0x15e4</Data>
<Data Name="AccessList">%4416</Data>
<Data Name="AccessMask">0x1</Data>
<Data Name="ProcessId">0x1e8</Data>
<Data Name="ProcessName">C:\Windows\System32\seass.exe</Data>
<EventData>
<Event>

```

Obrázok: Detail udalosti

V detaile udalosti je taktiež možný prechod na ďalšiu alebo predchádzajúcu udalosť a to pomocou smerových šípkov (▲ a ▼) nachádzajúcich sa v ľavej časti dialógového okna.

Date:
9.6.2015