

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.

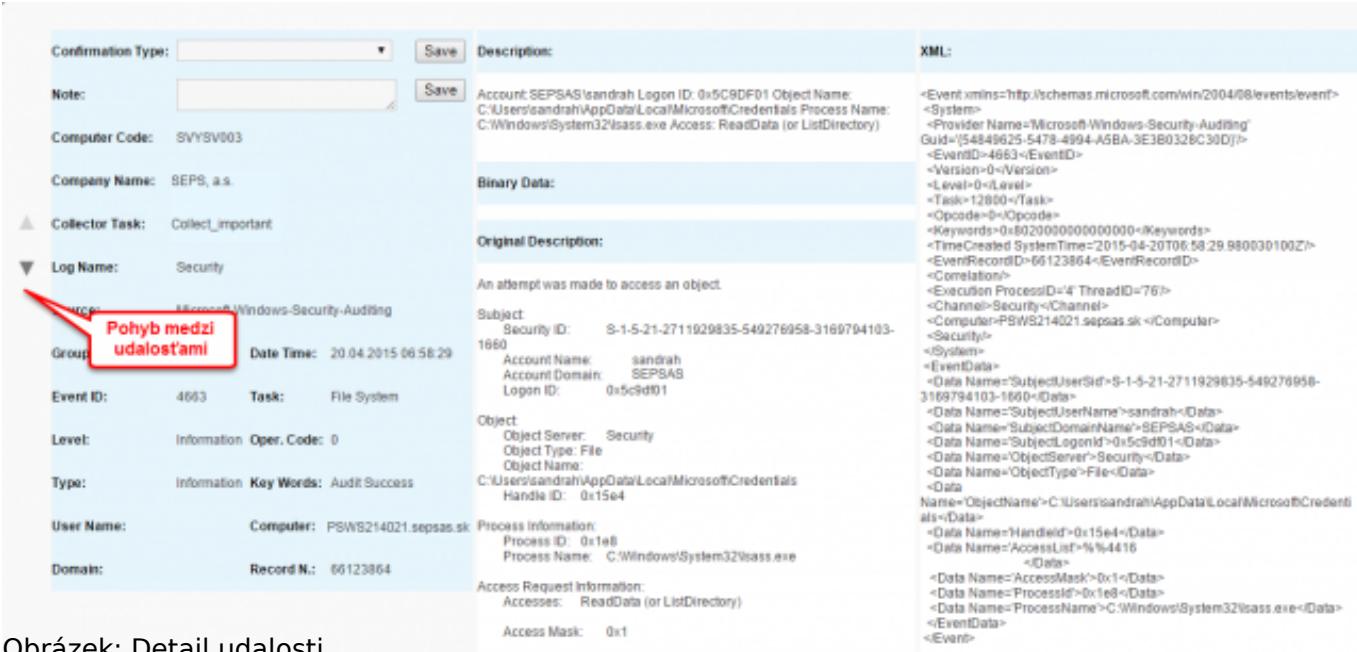
Stĺpce spoločnosť, počítač a názov zberu majú fixnú pozíciu a nedajú sa odstrániť. Pre lepšiu prehľadnosť sú sa však dajú skryť kliknutím na ikonu šípky, nachádzajúcu sa v ľavej časti zobrazenia.

Obrázek: 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 a detailed view of an event log entry. At the top, there are fields for 'Confirmation Type' (dropdown), 'Save' button, 'Description' (text area), and 'XML:' (button). Below these are sections for 'Note' (text area), 'Computer Code' (SVSYV003), 'Company Name' (SEPS, a.s.), and 'Collector Task' (Collect_Important). A 'Log Name' section shows 'Security'. The main event details are as follows:

- 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:** sandrah
- Computer:** PSWS214021.sepas.sk
- Domain:** Record N.: 66123864

Under 'Object' details:

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

Under 'Access Request Information':

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

The right side of the screen displays the XML representation of the event.

Obrázek: Detail udalosti

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

Date:
9.6.2015