

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.

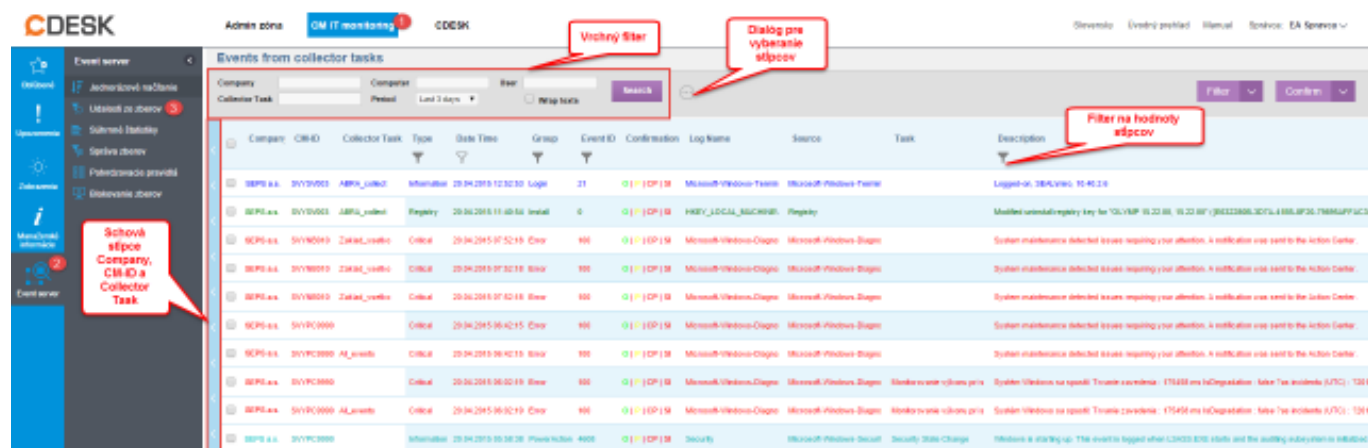
Vo vrchnej časti zobrazenia je možné filtrovať zobrazené udalosti na základe:

- názvu spoločnosti,
- názvu zberu,
- názvu počítača (CMID aj názov počítača),
- periódy 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.

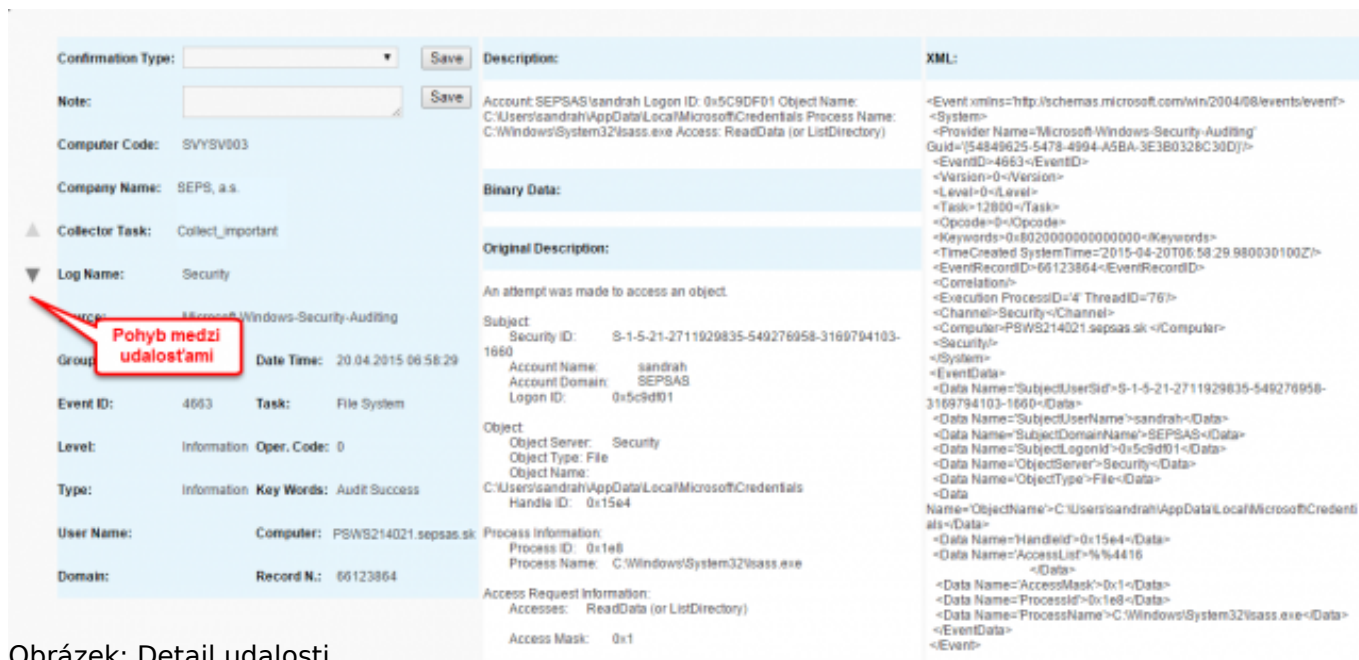


Obrázek: Popis základného zobrazenia

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 dáta),
- pole pre zadanie poznámky,
- originálne znenie udalosti (generované operačným systémom),
- XML znenie udalosti (generované operačným systémom).



The screenshot displays the 'Detail udalosti' (Event Detail) window. On the left, there's a form with fields for 'Confirmation Type', 'Note', 'Computer Code' (SVYSV003), 'Company Name' (SEPS, a.s.), 'Collector Task' (Collect_important), 'Log Name' (Security), and 'Group' (Microsoft Windows-Security-Auditing). A red box with the text 'Pohyb medzi udalosťami' (Move between events) points to the up and down arrow buttons next to the 'Log Name' field. Below these are fields for 'Event ID' (4663), 'Task' (File System), 'Level' (Information), 'Oper. Code' (0), 'Type' (Information), 'Key Words' (Audit Success), 'User Name', 'Computer' (PSVWS214021.sepsas.sk), and 'Domain'. The right side of the window shows the 'Description' (An attempt was made to access an object.), 'Binary Data', 'Original Description', and 'XML' (XML representation of the event).

Obrázek: Detail udalosti

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

Date:

9.6.2015