

Štatistiky a exporty

V menu „Admin zóna -> Events Server -> Štatistiky a reporty“ si môže operátor zobrazíť súhrnné informácie za dané obdobie. Zvolené informácie si môžete samozrejme aj filtrovať a to podľa názvu zberu, konkrétneho počítača, stavu, EventID a ďalších.

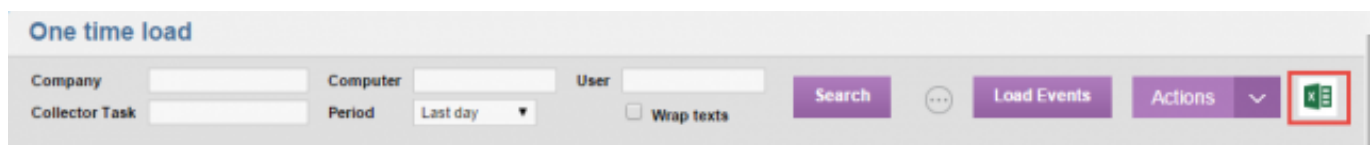
Štatistiky sa zobrazujú pre výskyt udalosti a niektoré detaily sú zanedbané (ako napr. súbor nad ktorým sa vykonala zmena alebo užívateľ ktorý sa prihlasoval), čo je v detaile udalosti zobrazené opakovaným znakom „*“. Aktualizácia údajov štatistík je na dennej báze, prostredníctvom samostatných (skrýtych) zberov, čo dovoľuje efektívne generovanie reportov za určité obdobie.

Ak si chcete vygenerovať report za zvolené obdobie, zadajte časový rozsah a vami vybranú skupinu počítačov a kliknite *Zobraziť*. Následne je možné report vyexportovať do XLS súboru pomocou príslušnej ikony nachádzajúcej sa v pravom hornom rohu.

Type	Date	Group	Event ID	Log Name	Total Count	Description
Information	01.04.2015	FileAudit	4663	Security	3367255	Account: ***** Logon ID: ***** Object Name: ***** Process Name: ***** Access: *****
Information	01.04.2015	FileAudit	4663	Security	3372296	Account: ***** Logon ID: ***** Object Name: ***** Process Name: ***** Access: *****
Information	01.04.2015	NotImportant	4656	Security	3351828	A handle to an object was requested. Subject: Security ID: ***** Account Name: ***** Account Domain: *****
Information	04.04.2015	FileAudit	4663	Security	620144	Account: ***** Logon ID: ***** Object Name: ***** Process Name: ***** Access: *****
Information	04.04.2015	FileAudit	4663	Security	960075	Account: ***** Logon ID: ***** Object Name: ***** Process Name: ***** Access: *****
Information	04.04.2015	NotImportant	4656	Security	899186	A handle to an object was requested. Subject: Security ID: ***** Account Name: ***** Account Domain: *****
Information	18.04.2015	FileAudit	4663	Security	117802	Account: ***** Logon ID: ***** Object Name: ***** Process Name: ***** Access: *****
Information	27.03.2015	FileAudit	4663	Security	99139	Account: ***** Logon ID: ***** Object Name: ***** Process Name: ***** Access: *****
Information	23.04.2015	FileAudit	4663	Security	98927	Account: ***** Logon ID: ***** Object Name: ***** Process Name: ***** Access: *****
Information	09.04.2015	FileAudit	4663	Security	64061	Account: ***** Logon ID: ***** Object Name: ***** Process Name: ***** Access: *****
Information	07.04.2015	FileAudit	4663	Security	33032	Account: ***** Logon ID: ***** Object Name: ***** Process Name: ***** Access: *****

Obrázok: Zobrazenie štatistík

Export dát je dostupný v prípade Jednorazového načítania, Udalostí zo zberov a Súhrnných štatistík. V prípade ak chcete exportovať dáta, vyhovujúce aktuálne nastaveným filtrom (filter udalostí a zároveň vrchný filter) kliknite na ikonu „MS Excel“ v pravej časti horného menu.



Obrázok: Tlačidlo slúžiace na export dát

Nastavenia EventServer

Nastavenia modulu Events Server sa nachádzajú v menu CM IT Monitoring -> Events Server, ktoré ďalej obsahuje podmenu:

- [Správa zberov](#) [1],
- [Správa potvrďovacích pravidiel](#) [2],
- [Štatistiky a reporty](#) [3],
- [Všeobecné nastavenia](#) [4],

Táto kapitola obsahuje podrobný popis sekcie *Všeobecné nastavenia* (pod účtom správcu: Admin zóna -> Môj profil, globál. nastavenia -> Events Collector).

Voľba „Aktualizovať súbory s pravidlami na počítačoch“ slúži na automatickú distribúciu súborov s pravidlami. Pravidlá sa distribuujú rýchlosťou 100 klientov / 10 minút, čo môže určitú dobu trvať.

Sekcia „Súbory so základnými pravidlami“ slúži na nahrávanie .elr súborov, ktoré sú spoločné pre všetky zbery a sú v nich zadefinované pravidlá kategorizácie udalostí. Tieto pravidlá je samozrejme možné neskôr na jednotlivých počítačoch upraviť ale odporúčame v prvom rade v sieti rozdistribuovať preddefinovaný súbor pravidiel ako základ zberov.

V sekcii „Súbory s potvrdzovacími pravidlami“ je možné nahráť na server preddefinované sady potvrdzovacích pravidiel. Tieto preddefinované sady vám neskôr uľahčia prácu pri filtrácii a vyhodnocovaní udalostí. Ako príklad si môžeme uviesť nahranie súboru kde bude zadefinované čítanie súborov v umiestnení Public užívateľom Everyone ako „OK“ a prihlásenie sa konta s oprávnením administrátora ako „Problem“ (čiže určené na preverenie). Tieto pravidlá je možné pridávať pre každú vytvorenú skupinu, pričom preddefinované skupiny sú PC, NB a SV.

Aktualizácia súborov s pravidlami Uložiť

Po nahrať alebo zmazať nejakého súboru s pravidlami prebehne aktualizácia automaticky. Aktualizácia prebieha po častiach a môže trvať aj niekoľko hodín v závislosti od počtu počítačov.

Aktualizovať súbory s pravidlami na počítačoch ☐

Súbory s kategorizačnými pravidlami

Elr súbor pre Windows Vista a novší
Vybrať súbor Nie je vybratý žiadny súbor Stiahnuť súbor (7 KB)
☐ Zmazať súbor

Elr súbor pre Windows XP, 2003 a 2000
Vybrať súbor Nie je vybratý žiadny súbor
☐ Zmazať súbor

Súbory s potvrdzovacími pravidlami

Elr súbor pre (PC)
Vybrať súbor Nie je vybratý žiadny súbor
☐ Zmazať súbor

Elr súbor pre (NB)
Vybrať súbor Nie je vybratý žiadny súbor
☐ Zmazať súbor

Elr súbor pre (SV)
Vybrať súbor Nie je vybratý žiadny súbor
☐ Zmazať súbor

Uložiť

Obrázok: Všeobecné nastavenia

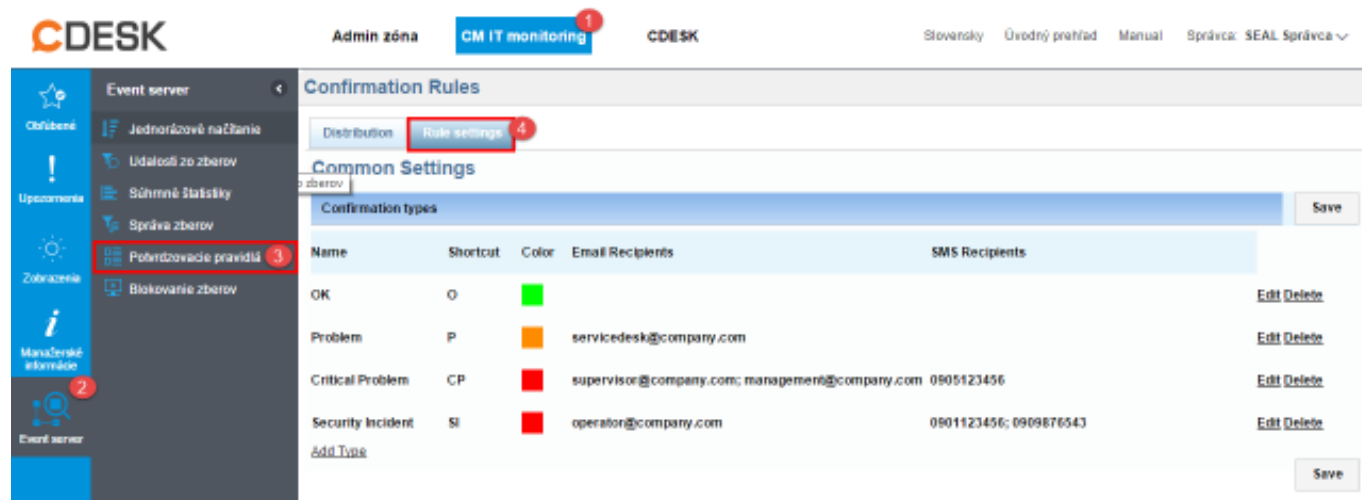
V prípade ak chcete editovať alebo pridávať nové stavy potvrdenia udalostí, táto funkcionlita sa nachádza v CM IT Monitoring -> Event server -> Potvrdzovacie pravidlá -> Záložka Rule settings. Nastavenie stavov potvrdenia pozostáva z tabuľky, v ktorej jeden riadok predstavuje jeden stav potvrdenia aj s príslušnou konfiguráciou.

V tejto sekcii je možné nastaviť:

- Názov stavu potvrdenia
- Skratku pre výpis (maximálne 3 znaky),
- Zobrazovanú farbu (vyberte zo zoznamu),
- Konfiguráciu E-Mailových notifikácií:
 - Príslúchajúce e-mailové adresy pre notifikácie,
 - Predmet E-mailu (je možné použiť premenné)
 - Obsah tela E-mailu (je možné použiť premenné)
- Konfiguráciu SMS notifikácií

- Prislúchajúce telefónne čísla pre SMS notifikácie,
- Text SMS správy s počítadlom znakov (je možné použiť premenné)

Na vytvorenie nového stavu potvrdenia slúži tlačidlo „Add type“, pričom tlačidlá „Edit“ a „Delete“ slúžia na manipuláciu už existujúceho pravidla.



Obrázok: Konfigurácia stavov potvrdenia

V nastaveniach predmetu a obsahu e-mailu a textu SMS správy je možné používať premenné ktoré budú v čase odoslania nahradené príslušným textom.

Date:

9.6.2015

Odkazy

[1] https://customermonitor.sk/ako-funguje-cm/eventanalyser/serverova-cast/sprava-zberov-pravidiel#sprava_zberov

[2] https://customermonitor.sk/ako-funguje-cm/eventanalyser/serverova-cast/sprava-zberov-pravidiel#sprava_pravidiel

[3] <https://customermonitor.sk/ako-funguje-cm/eventanalyser/serverova-cast/statistiky-nastavenia#statistiky>

[4] https://customermonitor.sk/ako-funguje-cm/eventanalyser/serverova-cast/statistiky-nastavenia#vseobecne_nastavenia_EA