

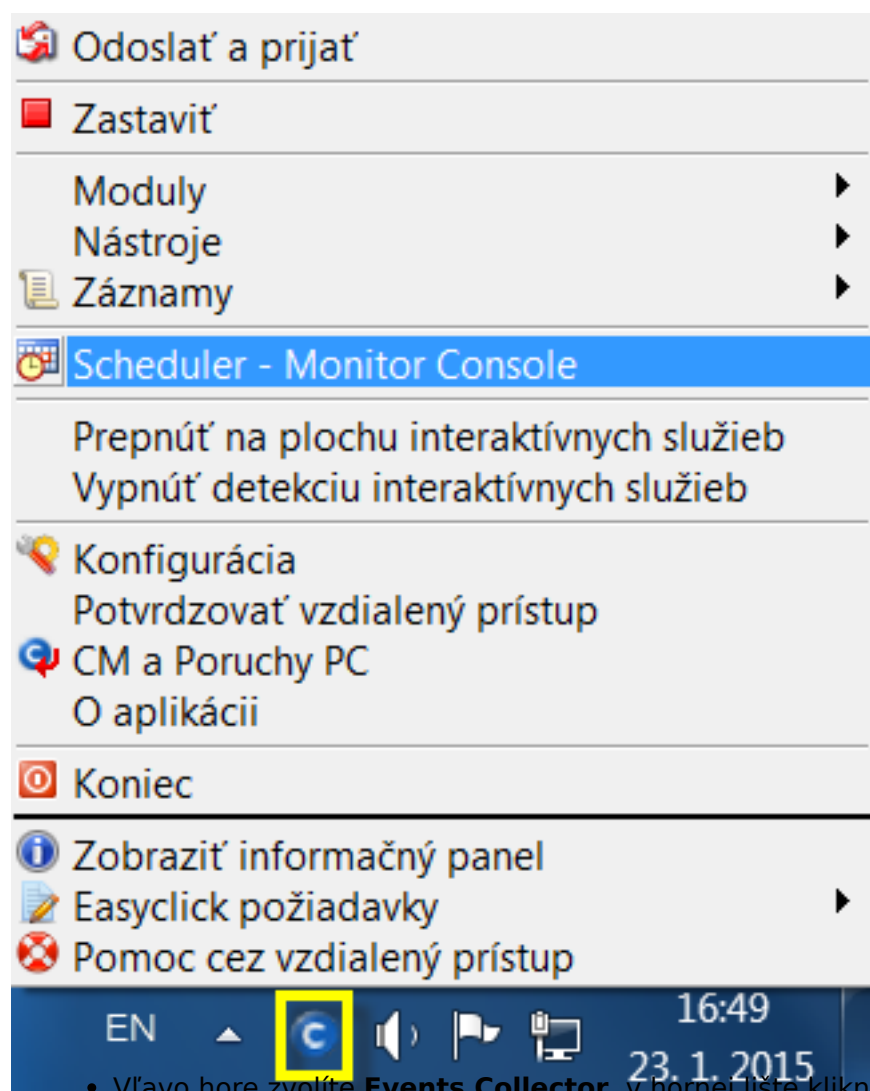
Events Collector je súčasť C-Monitora, pomocou ktorej môžete zbierať udalosti vyhovujúce zadaným filtrom a ukladať ich v rôznych formátoch na vami zvolenom mieste.

- **Nastavenie filtrov pre zber udalostí:**

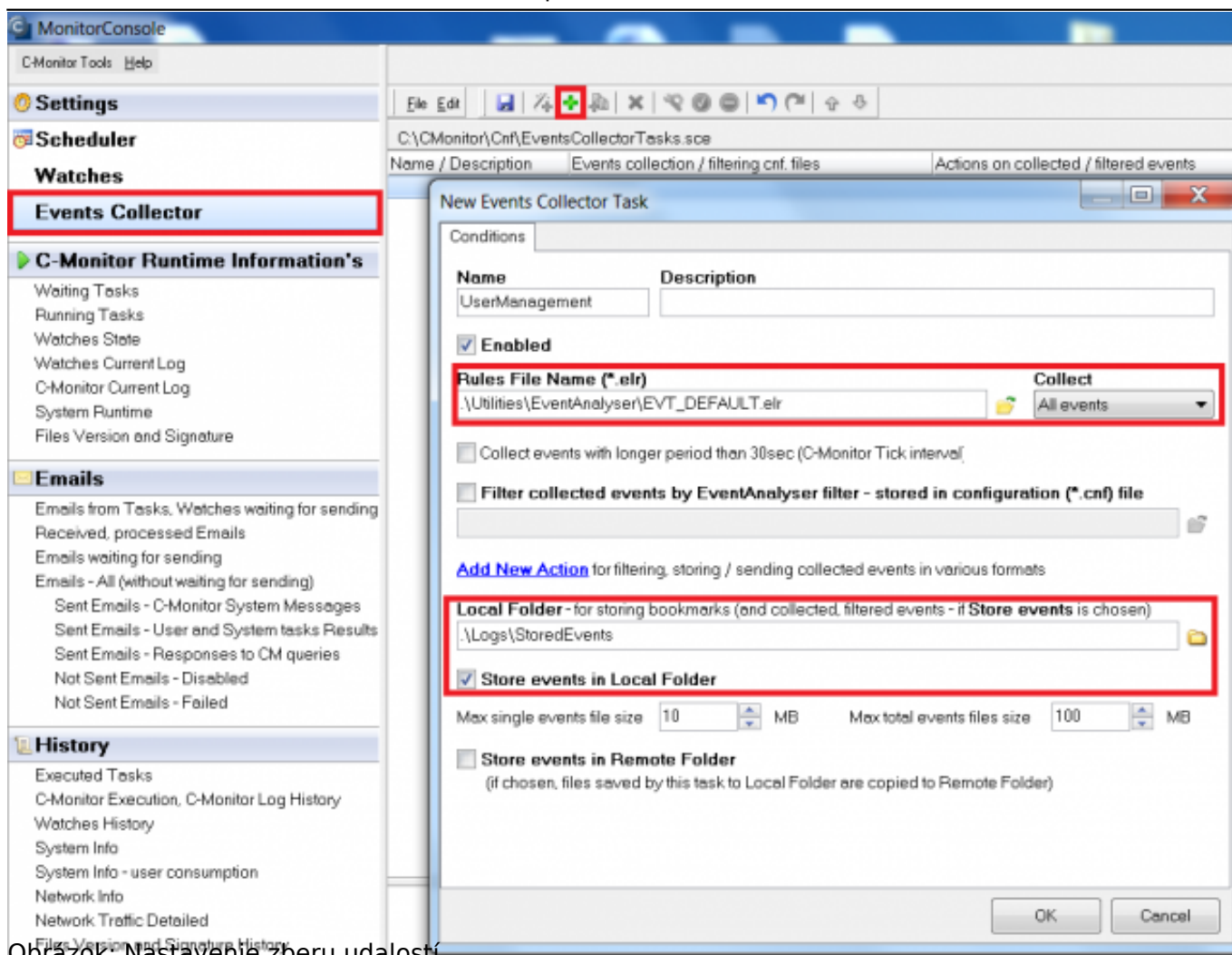
Otvoríte si EventAnalyser a nastavíte filter tak, aby mu vyhovovali len udalosti, ktoré chcete zbierať. Po nastavení filtrov zatvorte EventAnalyser. Vaše nastavenie sa týmto uloží do súboru LastSettings.cnf, ktorý budeme potrebovať neskôr.

- **Nastavenie zberu udalostí:**

Pravým tlačidlom myši kliknite na ikonu C-Monitora a otvorte Monitor Console.

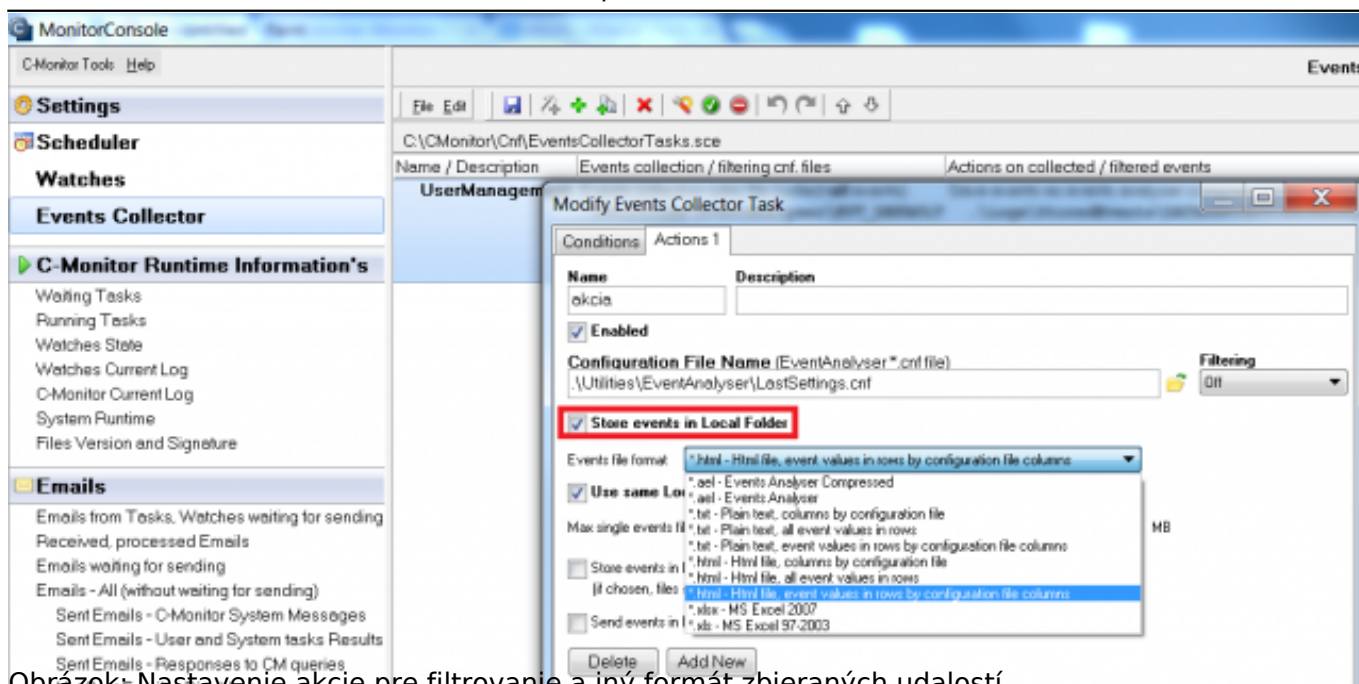


- Vľavo hore zvolíte **Events Collector**, v hornej lište kliknete na zelené plus(Add new events collector task) a vyskočí vám okno s nastaveniami.
- Zvolíte názov úlohy a jej popis, pod tým pre políčko **Rules File Name** zvolíte pravidlá(napr. EVT_DEFAULT.elr).
- Vyberiete, či chcete zbierať len dôležité udalosti alebo všetky.
- Teraz kliknete na políčko **Store events in Local folder**, a vyberiete miesto, kam chcete aby sa zozbierané udalosti ukladali a kliknete OK.
- Zmeny potvrdíte kliknutím na ikonu diskety v hornej lište.



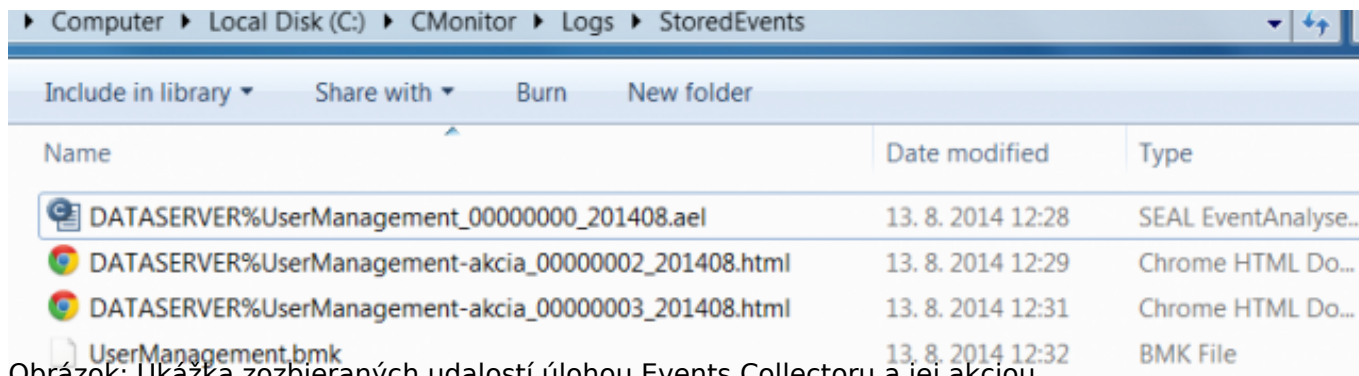
Obrazok: Nastavenie zberu udalostí

- Pokiaľ chcete udalosti ukladať v inom formáte, alebo z nich filtrovať len niečo konkrétne, môžete k existujúcej úlohe pridať akciu.
- Kliknite pravým tlačidlom myši na vytvorenú úlohu a zvolíte **Edit Events Collector Task**, otvorí sa vám okno, kde ste nastavovali úlohu, tam kliknete na **Add New Action**.
- Vyplníte názov akcie, popis a zvolíte konfiguračný súbor, ktorý vytriedi len požadované udalosti, v tomto prípade **LastSettings.cnf** (v ňom sú uložené údaje o filtrovaní, ktoré ste nastavili v EventsAnalyseri).
- Kliknite na Events file format a vyberte si jednu z možností, v akom formáte sa budú filtrované udalosti ukladať.
- Zaškrtnite políčko **Store Events in Local Folder**, následne buď nastavíte iný adresár ako pre samotnú úlohu, alebo zaškrtnete možnosť **Use same Local Folder as current collector task**, a všetky udalosti sa budú ukladať do toho istého adresára.



Obrázok: Nastavenie akcie pre filtrovanie a iný formát zbieraných udalostí

- Zmeny uložíte kliknutím na ikonu diskety.
- Ak ste pri nastavovaní úlohy nezadali inak, zbierané udalosti sa aktualizujú každých 30 sekúnd.
- Ukladať môžete nechať buď len filtrované udalosti z akcie vo vami zvolenom formáte, alebo aj zo samotnej úlohy v prednastavenom .ael formáte.
- Otvorením takto zozbieraných súborov sa podľa zvoleného formátu otvorí program, v ktorom si môžete prezrieť zoznam udalostí(EventAnalyser, Notepad, Excel, Browser).



Obrázok: Ukážka zozbieraných udalostí úlohou Events Collectoru a jej akciou

Zber udalostí v sieti

Nastavenie filtrov pre zber udalostí:

- Otvoríte si EventAnalyser a nastavíte filter tak, aby mu vyhovovali len udalosti, ktoré chcete zbierať. Po nastavení filtrov zatvorte EventAnalyser. Vaše nastavenie sa uloží do súboru *LastSettings.cnf*, ktorý budeme potrebovať neskôr.

Nastavenie zberu udalostí:

- Otvorte si MonitorConsole, vľavo hore zvolíte **Events Collector**, v hornej lište kliknete na zelené plus(Add new events collector task) a vyskočí vám okno s nastaveniami.
- Nastavíte názov úlohy, pravidlá a ostatné veci rovnako ako v predchádzajúcom prípade.
- Zaškrtnite políčko **Store events in Remote Folder**

-
- Zobrazia sa vám nové textové polia,
 - **Remote Folder** - Cesta ku vzdialenému priečinku, do ktorého chcete ukladať zozbierané udalosti. Priečinko na vzdialenom počítači musí byť zdieľaný a musíte mať k nemu oprávnenie na zápis.
 - **User Name** - Používateľ, cez ktorého sa bude súbor na vzdialenom počítači ukladať
 - **Domain** - Doména vzdialeného používateľa
 - **Password** - Heslo k účtu vzdialeného používateľa, cez ktorého sa bude súbor na vzdialenom počítači ukladať.

Po správnom nastavení sa začnú vyhovujúce udalosti ukladať na umiestnenie vo vzdialenom počítači.

Notifikácia na udalosti pomocou e-mailu

V prípade ak chcete byť na niektoré typy udalostí notifikovaný e-mailom, pripravte si podľa predchádzajúcich pokynov filter na želané udalosti. Následne pri vytváraní novej úlohy v Event Collectore kliknite na Add New Action (viď. obrázok).

New Events Collector Task

Conditions

Name

UserManagement

Description

☒ Enabled

Rules File Name (*.elr)

.\\Utilities\\EventAnalyser\\EVT_DEFAULT.elr

Collect

Important events

☐ Collect events with longer period than 30sec (C-Monitor Tick interval)

☒ Filter collected events by EventAnalyser filter - stored in configuration (*.cnf) file

.\\Utilities\\EventAnalyser\\LastSettings.cnf

Add New Action

 for filtering, storing / sending collected events in various formats

Local Folder - for storing bookmarks (and collected, filtered events - if Store events is chosen)

☐ Store events in Local Folder

Note: Events collection is active from 5 min after the operating system start.

OK

Cancel

Obrázok: Pridanie novej akcie

Budete presmerovaný na dialóg v ktorom môžete pridať druhý (dodatočný) filter na selektovanie iba konkrétnych udalostí zberu. Zaškrtnite prosím, *Send events in E-Mail to custom E-Mail Addresses*.

Následne vám bude umožnené zadať e-mailovú adresu alebo adresy na ktoré sa bude notifikácia posilať, predmet a text správy, formát zasielaných udalostí a aj spôsob zasielania udalostí (obyčajný súbor / ZIP súbor / Pripojiť k telu správy).

New Events Collector Task

ConditionsActions 1

Name

SendByMail

Description

Send e-mail with notification

☒ Enabled

Configuration File Name (EventAnalyser *.cnf file)

.\\Utilities\\EventAnalyser\\LastSettings.cnf

Filtering

by configuration file

☐ Store events in Local (Remote) Folder

☒ Send events in E-Mail to custom E-Mail Addresses

For E-Mail sending will be used C-Monitor SMTP settings

From:

\$DefaultNotificationSendFrom\$

To:

\$DefaultNotificationSendTo\$

Subject:

Notification warning

Please read the events provided in appendix.

Events send format

*.xlsx - MS Excel 2007

Events send mode

Send events as attachment

Max attachment size

10

MB

Note:

E-Mail will be sent via CM Server (http transfer to CM). Max 2 MB.

Test Send E-Mail

Delete

Add New

OK

Cancel

Obrázok: Nastavenie notifikácií na udalosť e-mailom

Po úspešnom nastavení budete notifikovaný e-mailom na každý výskyt vami vybraných udalostí.
Date:

9.6.2015