

Spustite EventAnalyser kliknutím pravého tlačidla myši na ikonu C-monitora v lište a zvoľte Nástroje -> C-EventAnalyser.

	🗯 Odoslať a prijať						
	Zastaviť						
	Moduly •						
C-IPScanner	Nástroje 🕨 🕨						
C-EventAnalyser	🖳 Záznamy 🔹 🕨						
	📴 Scheduler - Monitor Console						
	Prepnúť na plochu interaktívnych služieb Vypnúť detekciu interaktívnych služieb						
	 Konfigurácia Potvrdzovať vzdialený prístup CM a Poruchy PC O aplikácii 						
	🖸 Koniec						
	 Zobraziť informačný panel Easyclick požiadavky Pomoc cez vzdialený prístup 						
	EN 🔺 💽 🕩 🏴 💾 14:16 23. 1. 2015						

Obrázek: Znázornenie ikonky C-Monitora pre otvorenie EventAnalyseru.

Nastavenie zobrazovania udalostí:

Vyberiete si, či chcete zobrazovať všetky typy udalostí, alebo iba tie, ktoré sú zaradené do kategórie dôležitých.

ŝ	Event Analys	er									
	🕝 🖉 🗐 🖣	a 🖻 😧 🛤 🍸 =	Default WIN7.2008	+ - AU	. .	Last 8 weeks events 🔹 💌	trieve Auto	G			
	🎩 Events List	Levents Statistic	s	Inc	ooftank						
	0 events										
ŀ	Туре	Date Time 🤝	Group	Event ID	Log Name	Task.	Description				
ŀ	7	7	7	T.	7	7	7				

Obrázek: Nastavovanie zobrazovania udalostí v EventAnalyseri

Zvolíte obdobie, za ktoré sa vám zobrazia všetky zozbierané udalosti.



Zobrazenie udalostí Publikováno z Customer Monitor

(https://www.customermonitor.cz)

Event Analy	ser						
🔁 🖗 🗐 🗆	h 🗐 😧 🕅 🍞 i	Default WIN7,2008	0+ ▼ [ALI	•	Last 8 weeks events 🛛 💌	😘 Retrieve 📃 Auto	Θ
Events List	📙 Events Statistic	:5			Last day events Last 3 days events		
0 events					Last 2 weeks events		
Туре	Date Time 🔝	Group	Event ID	Log Name	Last 4 weeks events	Description	
T	T	7	Ψ	T	Last 12 weeks events		
					All events		

Obrázek: Nastavovanie zobrazovania udalostí v EventAnalyseri

Udalosti na základe zvolených nastavení načítate tlačidlom **Retrieve**, a so získaným zoznamom viete ďalej pracovať. Pokiaľ chcete, aby EventAnalyser aktualizoval zoznam udalostí automaticky, zaškrtnite políčko Auto, a váš zoznam sa bude aktualizovať pravidelne každých 30 sekúnd.

C Event Analy	yser								x		
🔁 🕼 🐻	n 🖲 😧 🗚 🍸	Default WIN7.2008)+ ▼] (ALL	. ▼][Le	at 8 weeks events 🔹	😘 Retrie	ve 🔽 Auto		Θ		
Events Lis	II Events List Levents Statistics Automatically retrieve events every 30s										
0 events											
Туре	Date Time 🔝	Group	EventID	Log Name	Task		Description				
7	7	7	7	T	7		7				

Obrázek: Nastavovanie zobrazovania udalostí v EventAnalyseri

Zobrazenie podrobností konkrétnej udalosti:

Pre zobrazenie podrobnejšieho výpisu kliknite pravým tlačidlom myši na riadok s danou udalosťou a zvoľte možnosť Show event details prípadne použite dvojklik alebo stlačte Enter. V okne, ktoré sa vám zobrazí, si môžete prepínať medzi jednoduchým výpisom o udalosti, pôvodným výpisom tak, ako ho generuje Windows a XML zobrazením.





Obrázek: Otvorenie podrobného zobrazenia udalosti

Nastavenie filtrov

- Kliknutím na ikonu lievika v hornej lište zapnete filtrovací mód.
- Zvolíte si parameter(stĺpec) podľa ktorých chcete zo zoznamu udalostí filtrovať a kliknutím na ikonu lievika v danom stĺpci otvoríte okno pre nastavenie filtrovania.
- Nastavíte filtrovanie podľa potreby a kliknete OK. Zoznam udalostí, ktorý sa vám teraz zobrazuje obsahuje iba udalosti, ktoré vyhovujú nastaveným filtrom.
- Ak chcete filtrovať podľa viacerých parametrov súčasne, kliknite na ikonu lievika v ďalšom stĺpci a znovu zadajte nastavenie filtrovania. Po kliknutí OK bude zoznam udalostí obsahovať iba tie udalosti, ktoré vyhovujú všetkým zadaným filtrom.

C Event Analyser		_ — X
📑 🖉 🖬 🐚 🖄 📵 🖊 🝸	🕫 Default WIN7,2008+ 💌 ALL 💌 Last 8 weeks events 💌 🚱 Retrieve 📝 Auto	G
3 ALL Events List 14 ALL Event	s Statistics	
265 all events since 18. 6. 2014 0:00:00	UTC. Defeat/WIN7.2008+	
Type Date Time 🗢	Group EventID Log Name Task Description Key	y Words
Information 12.8.2014 9.2943 Image: Information 11.8.2014 13.09.08 Image: Information 11.8.2014 13.09.08 Image: Information 11.8.2014 13.09.08 Image: Information 11.8.2014 12.19.05 Image: Information 8.8.2014 22.42.33 Image: Information 8.8.2014 22.42.33 Image: Information 8.8.2014 22.19.35 Image: Information 8.8.2014 22.19.33 Image: Information 8.8.2014 22.19.32 Image: Information 8.8.2014 22.17.20 Image: Information 8.8.2014 22.17.15 Image: Information 8.8.2014 15.43.03 Image: Information 4.8.2014 15.43.03 Image: Information 4.8.2014 15.14.30 Image: Information 4.8.2014 15.13.47 Image: Information 4.8.2014 13.33.05 Image: Information 4.8.2014 13.33.05 Image: Information 4.8.2014 13.33.05	Powerkdion 12 System The openating system stafed at system inter 24147-0097-012TU229 Powerkdion Filter for "Group" Immediate at system inter 24147-0097-012TU229 Immediate at system inter 24147-0097-012TU229 Powerkdion Powerkdion Immediate at system inter 24147-0097-011118/21 Immediate at system inter 24147-0097-011118/21 Powerkdion Cal values Immediate at system inter 24147-0097-011118/21 Immediate 22147-0097-011118/21 Powerkdion Cal values Immediate at system inter 24147-0097-011118/21 Immediate at system inter 24147-0097-011118/21 Powerkdion Cal values Immediate at system inter 24147-0097-011118/21 Immediate at system inter 24147-0097-011118/21 Powerkdion Cal values Immediate at system inter 24147-0097-0101118/81 Immediate at system inter 24147-007-0100119/91 Powerkdion Login Login event Immediate at system inter 24147-007-0100119/91 Immediate at system inter 24147-007-0100119/91 Powerkdion Powerkdion Powerkdion Powerkdion Powerkdion Powerkdion Security event Immediate at system inter 24147-007-0111314 Immediate 24147-007-0111314 Powerkdion Verdegin ewent - Auditing	assic assic assic assic assic assic assic assic assic assic assic assic assic assic assic

Prispôsobenie zobrazovania udalostí v EventAnalyseri:

- Udalosti v zobrazenom zozname si môžete nechať zoradiť podľa ľubovoľného parametra kliknutím do príslušného políčka. Pri stĺpci, podľa ktorého je zoznam udalostí zoradený je zelená šípka(viď. červená šípka na obrázku).
- Jednotlivé stĺpce parametrov udalostí môžete preusporiadať, pridať ďalšie alebo niektoré odstrániť. Kliknite do ľubovoľného stĺpca pravým tlačidlom myši a zvoľte možnosť Select colums. V zobrazenej tabuľke máte vľavo celý zoznam stĺpcov, ktoré ešte môžete do vášho zobrazenia pridať, vpravo je zoznam aktuálne pridaných parametrov, môžete z nich niektoré odobrať, alebo ich preusporiadať.



Zobrazenie udalostí

Publikováno z Customer Monitor (https://www.customermonitor.cz)

Event Analy	/ser							L	x
ଟ 🏟 🖬	h 🖲 😣 🗛 [🍸 📪 🛛 Default WIN	7,2008+ 🔻 🛛	u 🔹	Last 8 weeks events 💌	😋 Retrieve	Auto		Θ
🧾 Events Lis	t 🐙 Events Stati	stics							
0 events									
Туре	Dote Time 🤝	Group	Event ID	Log Name	Task.	Des	cription		
7	T		- T	17	1	1			
	Select	Columns					×	Ŋ	
	Ave	ilable Columns			Selected Columns				
	Pro Pro Lev Do	arce rvider ID rsion val er Name main		Add->	Type Date Time Group Event ID Log Name Task	М	ove Up		
	Da Op Co Re Ori File Ful	te Time UTC er. Code mputer cord N. ginel Description Name I File Name	<	- Remove	Description Key Words	Mo	ve Down		
				Default					
						ок	Cancel		
Obrázek:	Nastavovar	nie zobrazo	vania st	ίρςον ν Ι	EventAnalvse	ri			

V EventAnalyseri si môžete pozrieť aj štatistiku výskytu udalostí za zvolené obdobie, zvoľte záložku **All Events Statistics** a uvidíte štatistické informácie o udalostiach: počet výskytov za zvolené obdobie, posledný výskyt a iné.

C)	Event Analyser											
2	🧬 🎲 🛃 🖹 😰 🛛 👫 🍞 👼 🛛 Default WIN7,2008+ 🔹 ALL 🔹 Last day events 🔹 🄄 Retrieve 📝 Auto											
E	I ALL Events List I ALL Events Statistics											
22	223 unique all events since 22. 1. 2015 15:17:54 UTC; Default WIN7,2008+											
Type Last Occurrence		rence	Group	Event ID	Description	Last Occur	rence UTC	Count 😎				
T		T		T	T	7	T		T			
1	Information	23.1.2015	16:19:14	NotImportant	5152	The Windows Filtering	23.1.2015	15:19:14	E	1,311		
	Information	23.1.2015	16:18:59	NotImportant	4656	A handle to an object w	23.1.2015	15:18:59	E	1,229		
1	Information	23.1.2015	15:38:01	NotImportant	5154	The Windows Filtering	23.1.2015	14:38:01	E	984		
1	Information	23.1.2015	16:17:34	FileAudit	4663	Account ***** Log	23.1.2015	15:17:34	E	528		
1	Information	23.1.2015	16:18:59	NotImportant	7036	The ***** service enters	23.1.2015	15:18:59	E	396		
1	Information	23.1.2015	15:38:02	NotImportant	5157	The Windows Filtering	23.1.2015	14:38:02	E	203		
	Information	23.1.2015	15:42:29	NotImportant	4719	System audit policy wa	23.1.2015	14:42:29		135		
1	Information	23.1.2015	15:44:34	NotImportant	4656	A handle to an object w	23.1.2015	14:44:34		120		
1	Information	23.1.2015	15:37:49	NotImportant	4957	Windows Firewall did n	23.1.2015	14:37:49	E	63		
1	Information	23.1.2015	15:39:23	Notimportant	2100	Received a Pnp or Pov	23.1.2015	14:39:23	E	44		

Obrázek: Príklad zobrazenia štatistiky udalostí

Exportovanie vybraných udalostí

- Zobrazené udalosti si môžete uložiť ako súbor programu C-EventAnalyser kliknutím na ikonu diskety v hornej lište, alebo ako Excelový súbor kliknutím na príslušnú ikonu vyznačenú na obrázku
- Pre uloženie len vybranej časti zoznamu, označte požadované udalosti a uložíte ich



Zobrazenie udalostí

Publikováno z Customer Monitor (https://www.customermonitor.cz)

C Event Analys	Event Analyser											
💣 🖗 🛃 🛙	2 🖻 🛛 🖊 🍸	Default WIN7,200	8+ ▼][AL	L •][La	st 2 weeks events 🔹	🖌 🕄 Retrieve	V Auto		Θ			
JALL Events List ALL Events Statistics												
49 all events since 30. 7. 2014 0.00:00 UTC; Default WIN7, 2008+												
Туре	Date Time 🤝	Group	EventID	Log Name	Task	Description						
7	7	PowerAction	7	7	7	7			Ξ			
 Information 	12.8.2014 9:29:43	PowerAction	12	System		The operating s	ystem started at	system time ?2014?-?08?-?12TI	07:2			
 Information 	11.8.2014 13:09:08	PowerAction	1074	System		The process C/	\Windows\syste	m32\winlogon.exe (DATASER)	/EF			
 Information 	11.8.2014 13:09:05	PowerAction	1074	System		The process Ex	plorer.EXE has i	nitiated the power off of compute	er D			
 Information 	11.8.2014 9:21:19	PowerAction	12	System	B. Com	T 1 C		pe ?2014?-?08?-?11Ti	07:2			
Information	8.8.2014 22:42:33	PowerAction	1074	System	ош Сору			ctri+c gon.exe (DATASER)	/EF			
Information	8.8.2014 22:42:30	PowerAction	1074	System	Copy de	etailed		power off of compute	er D			
Information	8.8.2014 21:48:45	PowerAction	12	System	Export s	selected events t	to EXCEL (XLS)	file) he ?2014?-?08?-?08T	19:4			
Obrázek: I	brázek: Exportovanie vybraných udalostívstem The process C \Windows \system 32 \window											

Date: 9.6.2015