

Ako bolo už uvedené, každá udalosť obsahuje informáciu o jej stave (stĺpec "Potvrdenie" a "Stav potvrdenia" v detaile udalosti). Stav udalosti indikuje, či už bola udalosť preskúmaná a poverená osoba zaznačila svoje rozhodnutie o rizikovosti udalosti.

Predvolené stavy udalostí sú:

- "OK" nie je primárne potrebná žiadna ďalšia aktivita operátorov. Tento stav je možné neskôr prípadne eskalovať na iný a slúži primárne na zaznačenie ošetrenia výskytu istej udalosti,
- "Problem" stav indikujúci, že udalosť je určená na ďalšie preskúmanie zodpovednou osobou. Povereným operátorom bude odoslaná e-mailová notifikácia,
- "Critical Problem" stav udalosti ktorý indikuje závažný problém vyžadujúci okamžitú pozornosť poverenej osoby. V prípade týchto udalostí je vhodné zabezpečiť eskaláciu do Service Desk. Povereným operátorom bude odoslaná e-mailová a SMS notifikácia,
- "Security Incident" stav udalosti ktorý indikuje bezpečnostný incident vyžadujúci okamžitú pozornosť poverenej osoby. V prípade týchto udalostí je vhodné zabezpečiť eskaláciu do Service Desk. Povereným operátorom bude odoslaná e-mailová a SMS notifikácia.

V prípade, že je veľa stavu potvrdenia uvedené "[M]", tak bol tento nastavený ručne, ak sa tam text nenachádza bol stav nastavený pravidlom (viď <u>Potvrdenie s nastavením opakovania</u> [1]).

						dmin zó	na	CM IT monitor	ring CDESK		Slovensky	Úvodný prehľad Manual	Správca: EA Spravca \checkmark
19	•	ł	Event	s fr	om collector	tasks	isks						
Oblübené	Nibené 17		Company		Compute		ter	Use Line -1		Search 💬		Filter 🗸	Confirm 🗸
1			CONNECTOR	Task		Penod	Case	s caste 🖃	Wrap texts				
Upozomenia				Гуре	Date Time	Group	Event ID	Confirmation	Log Name	Descrip	ption		
-(ó)-				Ŧ.	8	Ŧ	Ŧ			Y			
Zobrazonia			E 6	nor	23.04.2015 10:22:13	Error	3002	Problem [M]	Microsoft-Windows-CodeIntegr	ty/Operational Code Inte	egrity is unable to verify the in	nage integrity of the file 'Device/Har	ddisk//olume2/Mindows/Syster
i			E •	TOP	23.04.2015 10:22:13	Error	3002	01910915	Microsoft-Windows-CodeIntegr	ty/Operational Code Inte	egrity is unable to verify the in	mage integrity of the file 'Device'Har	ddisk//olume2//ilindows/Syster

Obrázek: Indikácia manuálneho potvrdenia

Každá zmena stavu udalosti je zaznačená v detaile udalosti (pod aktuálnym stavov) aj s menom operátora a časom kedy bola vykonaná.

Jednorázové potvrdenie

Stav udalosti je možné zadať rôznymi spôsobmi. Prvým spôsobom je kliknutie na želaný stav v riadku udalosti (stĺpec "Potvrdenie") v zobrazení *CM IT Monitoring -> Event server -> Správa načítaných udalostí*. Ak daná udalosť nemá pridelený stav, sú v stĺpci zobrazené všetky stavy potvrdenia pomocou nastavených skratiek, čiže v základnej konfigurácii uvidíte **O | P | CP | SI**. Po nastavení stavu sa v stĺpci nachádza iba plné znenie stavu (v príslušnej farbe).



Potvrdzovanie udalostí

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

CD	ESK	Admin zó	Admin zóna CM IT monitoring			CDESK Slovensky				Manual Sprävca: EA Sprav	ial Správca: EA Spravca 🗸		
10	Event server C	Events fr	rom collecto	r tasks									
Obřúbené	🐺 Jednorázové načítanie	Company Collector Tasi		Comp	uter Last 3	3 days 🔻	Iser 🗹 Wrap texts	Search	••••••••••••••••••••••••••••••••••••••	iller 🗸 Confirm	~		
Upozomenia	 Súhmné štatistiky Správa zberov 	Type	▼Date Time	Group	Event ID	Confirmation	Log Name	Source	Task	Description	Note		
Zobranenia 1 Manaferniké informácie	 Pohrtičovacie pravidla Blokovanie zberov 	> Ener	23.04 2015 20:15:11	Emor	1001	O P CP SI	Microsoft-Windows- Dhop-Client/Admin	Microsoft-Windows- Dhop-Client	Address Configuration State Event	Your complete was ret as spired as address hum as spired as address hum benering for the Network Card with retwork address bothCARCESECCAR. The following error occurred both Var computer will continue to try and obtain as address to its own than the network address (DHCP) server.	n.		
Event server		> > • • • • • •	23.04 2015 28:15:10	Enar	1001	0 P CP SI	Microsoft-Windows- Dhop-Clant/Admin	Microsoft-Windows- Dhop-Client	Address Configuration State Event	Your competer was eit assigned as address hism the network (by the DPCCP) Savers for the Network Card with retwork address to DCPP/sc30 t832. The following error occurred by 75, Viser competer will continue to try and obtain as address a fit own from the network address (DHCP) server.			

Obrázek: Možnosti stavu potvrdenia

Ďalšou možnosťou je zaznačenie stavu v detaile konkrétnej udalosti. V rolovacom zozname si vyberte jeden zo stavov "OK", "Problem", "Critical Problem" alebo "Security Incident" a následne kliknite na tlačidlo uložiť.

	Confirmation Type:	▼ Save	Description:	XML:
	Note: Computer Code:	OK Protein Critical Problem Security Incident SVYSV003	Account: SEPSAS (sandrah Logon ID: 0x5C9DFD1 Object Name: C:Users/sandrah/AppData/Local/MicrosoffCredentals Process Name: C:Windows/System32(sass.exe Access: ReadData (or ListDirectory)	<event xmins="http://schemas.microsoft.com/win/2004/08/events/event"> <system> <provider <br="" name="Microsoft-Windows-Security-Auditing">Guid#\[54849625-5478.4994.ASBA-3E380328C30D]/> <eventdia4633<eventdia< th=""></eventdia4633<eventdia<></provider></system></event>
	Company Name:	SEPS, a.s.	Binary Data:	<version>0</version> <level=0< level=""> <task=12800< task=""></task=12800<></level=0<>
*	Collector Task:	Collect_important	Original Description:	<pre>«Opcode=0=/Opcode» «Keywords=0=8020000000000000=/Keywords» <timecreated systemtime="2015-04-20106;58/29.980030100Z/"></timecreated></pre>
۳	Log Name:	Security	An attempt was made to access an object.	<eventrecordid=66123864< eventrecordid=""> <correlation></correlation> <execution processid="# ThreadID=767></th></tr><tr><th></th><th>Source:</th><th>Microsoft-Windows-Dhcp-Client</th><th>Subject
Security ID: S-1-5-21-2711929835-549276958-3169794103-
1660</th><th colspan=5><Computer-Security-commerce
<Security/-
<Security/-
<Security/-</th></tr><tr><th></th><th>Group:</th><th>Error Date Time: 23.04.2015 20:15:11</th><th>Account Name: sandrah
Account Domain: SEPSAS</th><th>«EventData»
«Data Name=SubjectUserSid»S-1-5-21-2711929835-549276958-</th></tr><tr><th></th><th>Event ID:</th><th>4663 Task: File System</th><th>Object</th><th>3169794103-1660-/Data>
«Data Name='SubjectUserName'>sandrah-/Data></th></tr><tr><th></th><th>Levet</th><th>Information Oper. Code: 0</th><th>Object Server: Security
Object Type: File</th><th><Data Name=" subjectdomainname"="">BEPSAS-(Data> <data data="" name="SubjectLogon(i>us/scbt01-(Data>
<Data Name='ObjectServer'>Security-(Data></th></tr><tr><th></th><th>Type:</th><th>Information Key Words: Audit Success</th><th>C:Userstandrah/UppData/Local/MicrosoffiCredentials
Handle ID: 0x15e4</th><th><Data Name='ObjectType'>File</Data>
<Data
Name='ObjectName'>C:\Users\sandrah\AppData\Local\MicrosoftCredenti</th></tr><tr><th></th><th>User Name:</th><th>Computer: PSW8214021.sepsas.sk</th><th>Process Information:
Process ID: 0x1e8
Process Name: CMMedical Public 2016 as an</th><th>ats="> =Data Name="Handleid"=0x15e4=\Data> =Data Name="AccessList="%%4416</data></execution></eventrecordid=66123864<>
	Domain:	Record N.: 66123864	Access Request Information:	<data> <data name="AccessMask">0x1</data> <data name="ProcessMask">0x1</data> <data name="ProcessMask">0x1a</data></data>
			Accesses: ReadData (or ListDirectory) Access Mask: 0x1	Data Aname = ProcessName > C.Windows/System32lisass.exe

Obrázek: Nastavenie potvrdenia v detaile udalosti

Vyššie spomenutá metóda je vhodná hlavne pre udalosti typu "Problem", "Critical Problem" alebo "Security Incident" vzhľadom na ich povahu a prípadnú potrebu preskúmať detailné informácie. Avšak pri uvádzaní väčšieho množstva udalostí do konkrétneho stavu potvrdenia, by sa jednalo o zdĺhavý a namáhavý proces. Pre tento prípad je možné označiť viacero udalostí zaškrtnutím políčka na začiatku riadku.

V pravom hornom rohu kliknite na tlačidlo *"Confirm" a* vyberte z ponúkaných možností *"One Time",* pričom vám bude v ďalšom kroku ponúknutý stav do ktorého chcete udalosti uviesť.



Potvrdzovanie udalostí

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

CD	ES	К		Ad	dmin zói	na 🤇	CM IT monitor	ing CDES	к		Slovensky	Úvodný prehľad	Manual	Správca: EA Spravca \checkmark
_^o	0	Eve	nts fr	om collector	tasks									
Obříbené !		Collec	any tor Task		Compu	Lost 3	days 🖃	r 🖵 Wrap texts						Continuitor
Upozomenie		•	туре Т	Date Time	Group	Event ID	Confirmation	Log Name		Description				Create fore
Zobrazenia		R					0 P CP SI	Microsoft-Windows-Co		Code integrity is unable				ddisk://olume21/Vindows/System
i		R					01P1CP1SI			Code integrity is unable				idisk:/olume21/Vindows/System
Manaženské informácie		R					0 P CP SI	Microsoft-Windows-Co		Code integrity is unable				ddiskt/olume2tWindowstSystem
		7		23.04 2015 10:01:14			0191C915	Microsoft-Windows-Co		Code Integrity is unable				ddisk//olume20/Vindows/System
Event server		Ē					0 P CP SI	Microsoft-Windows-Co		Code Integrity is unable				idisk:/olume21/Vindows/System
		Г		23.04.2015 10:01:14			01				-8			idisk://olume21/Vindows/System
					Error		Choose	confirmation type:	OK OK	2	()	age integrity of the fi	e Cevice/Har	ddiak /olume2Windows/System
		п					01		Critical Problem Security Incident		ie im			ddisk:/okume21/Vindows/System

Obrázek: Hromadné manuálne potvrdenie udalostí

Ak neskôr narazíte na udalosť ktorej stav potvrdenia chcete zmeniť, je potrebné túto zmenu vykonať v detaile udalosti alebo hromadným nastavením, avšak už vygenerované notifikácie sa odstrániť nedajú.

Potvrdenie s nastavením opakovania

Pre udalosti ktorých výskyt sa opakuje a viete, že ich uvediete vždy do toho istého stavu, je možné vytvoriť tzv. "pravidlá potvrdzovania". Tieto pravidlá sa dajú nastaviť na jednotlivé udalosti alebo prípadne aj na celý zber. Jednotlivé skupiny potvrdzovacích pravidiel je potom možné spájať do stromovej štruktúry.

Vytvorenie pravidla vykonáte v menu "CM IT Monitoring -> Event server -> Správa načítaných udalostí" prípadne z "CM IT Monitoring -> Event server -> Jednorazové načítanie", kde si pomocou filtra určíte kritéria vyhľadávania a zaškrtnutím udalosti vyberiete len konkrétne, na ktoré sa majú pravidlá aplikovať (alebo všetky). Následne v pravom hornom rohu kliknite na tlačidlo "Confirm -> Create rule" resp. "Actions -> Create Confirmation rule" v jednorazovom načítaní.

Zobrazí sa vám dialógové okno, obsahujúce tabuľku v ktorej sú po riadkoch načítané udalosti vrátane ich detailov (okrem *"Description"* a *"Poznámky"*). Každý z údajov, je editovateľný kliknutím na príslušnú hodnotu, pričom je možné používať regulárne výrazy a prázdne pole znamená nepodstatný údaj.

Prepísaním hodnoty môžete vytvárať pravidlá, ktoré sa budú vzťahovať na rôzne inštancie danej udalosti. Ako príklad si môžeme uviesť udalosť, ktorá oznamuje, že sa daný užívateľ prihlásil na *zariadenie* ako *DOMAIN\USER* – v prípade ak chcete filtrovať iba užívateľov z konkrétnej domény tak do poľa *DOMAIN* zaznačte názov príslušnej domény a do poľa *USER* zadajte znak * (alebo ju ponechajte prázdnu). Ostatné položky nechajte nastavené na pôvodnú hodnotu.

V zozname zaznačte každej udalosti stav do ktorého bude automaticky uvedená, prípadne sa nad zoznamom udalostí nachádza rolovací zoznam so stavmi *"Choose confirmation type for all:"*, ktorý slúži na hromadné nastavenie stavov potvrdenia.

Jednotlivé riadky s pravidlami môžete presúvať na vyššie alebo nižšie pozície pomocou smerových šípok (\blacktriangle a \bigtriangledown) resp. pridávať a odoberať pomocou tlačidiel *"Delete"* a *"Add"*.



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

Rele Narbei Inkuerses Posum pravidla mižšie/vyššie		-	-	Pomenovanie prav	idla		Hromadné nastaven	ie stavuCk	0K •					
			E	Ci Imer	Log Name	Source	User Name	Castom Group	Task	Confirmation Type	Note			
	Onlete	Ņ	Error			0	System	Microsoft Windows-HIRPSv:		Erv .		0K •		
	Detete		Drev.			81	Microsoft-Vindous-Dircp-Cit	Mercoult-Windows-Dhep-Cik	LOCAL SERVICE	Сям	Address Configuration State E	Problem •		
	Delete		Breat				Marwoll Visions Hanetter	Maronall Medices HameOn	LOCAL SERVICE	less.		Pulan •		
	Delete		Error			81	System	Service Control Manager		Erre .		Critical Problem	escalate to	50 1
	Delete		Erece.			8	System	Service Control Manager		Če v		ОК •		
	Add	6	stränen	ie riadku										
		1	Pride prézdi riad	nie neho ku										Save

Obrázek: Detail potvrdzovacieho pravidla

Do súboru pravidla je automaticky pridaný operátor ktorý ho vytvoril aj s časom vytvorenia. Pred uložením odporúčame súbor pravidiel pomenovať jednoznačným menom (v ľavom hornom rohu), čo vám uľahčí neskoršiu identifikáciu. Po ukončení úprav pravidlá uložte do interného repozitára servera tlačidlom "*Uložiť*".

Po uložení súboru pravidiel budete presmerovaný na obrazovku v ktorej môžete súbory s pravidlami spájať a vykonať záverečné úpravy (pre viac informácii viď <u>Správa pravidiel</u> [2]). Po vykonaní úprav zvoľte zariadenia na ktoré chcete súbor pravidiel distribuovať a kliknite na tlačidlo *"Distribute file"*. Date:

9.6.2015

Odkazy

[1] https://www.customermonitor.cz/ako-funguje-cm/eventanalyser/serverova-cast/potvrdzovanie-udalosti#confirm_rule

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