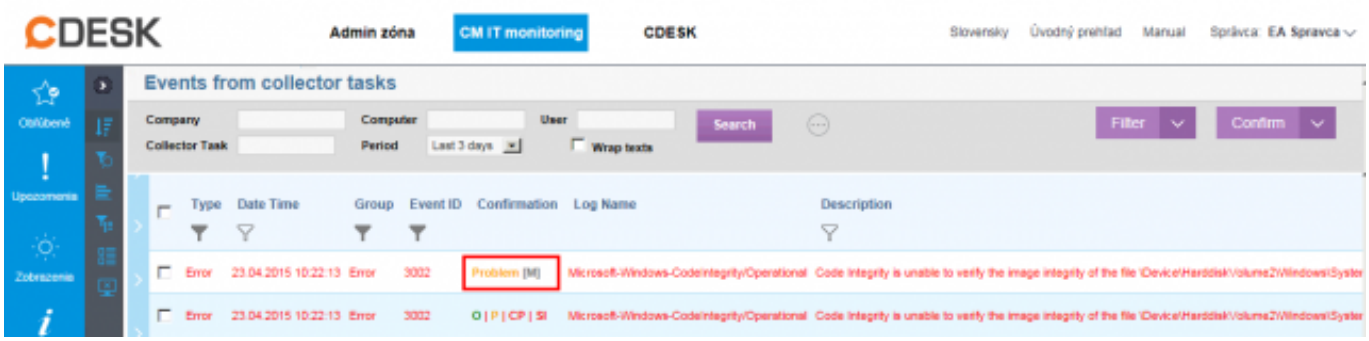
Ako bolo už uvedené, každá udalosť obsahuje informáciu o jej stave (stĺpec „Potvrdenie“ a „Stav potvrdenia“ v detaile udalosti). Stav udalosti indikuje, či už bola udalosť preskúmaná a poverená osoba zaznačila svoje rozhodnutie o rizikovosti udalosti.

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 Potvrdenie s nastavením opakovania [1]).

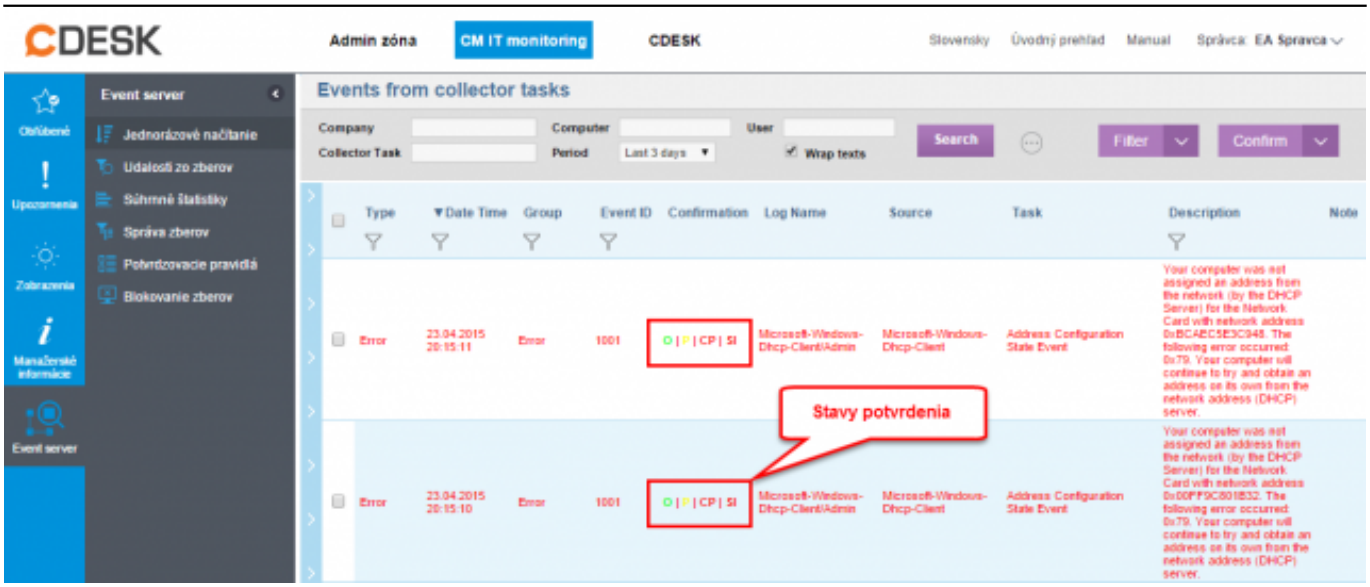


Obrázok: Indikácia manuálneho potvrdenia

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

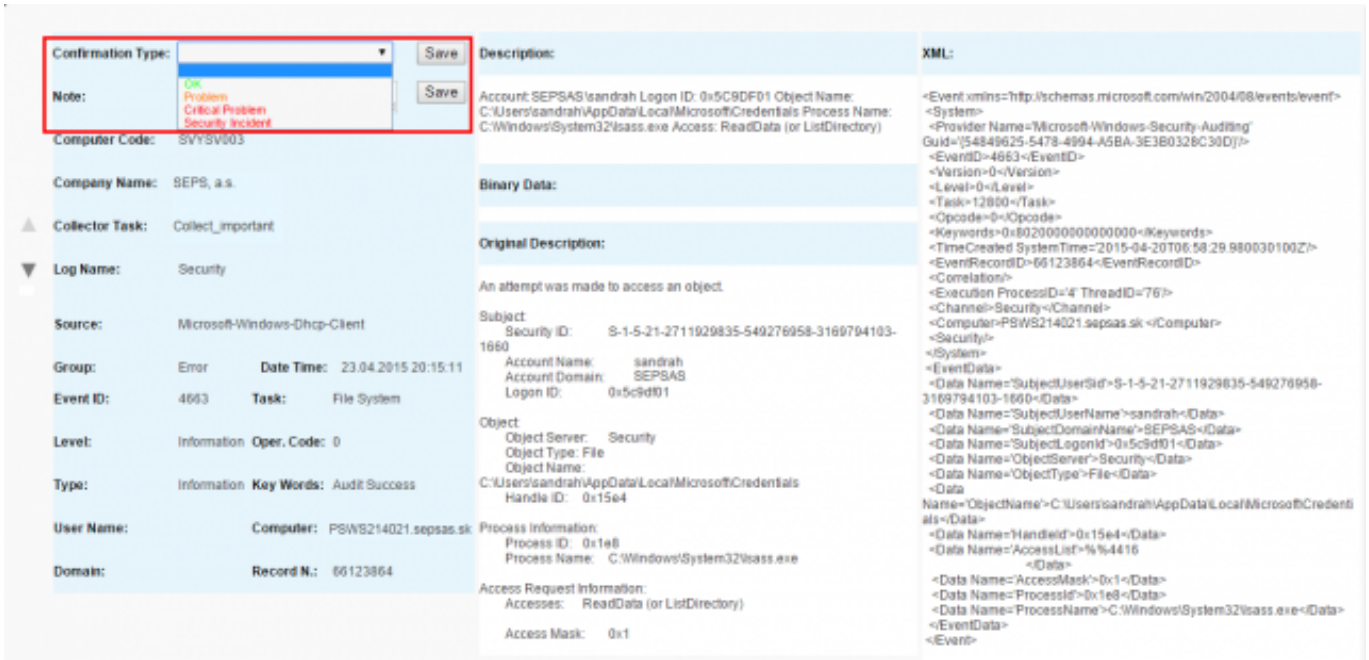
Jednorázové potvrdenie

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).



Obrázok: Možnosti stavu potvrdenia

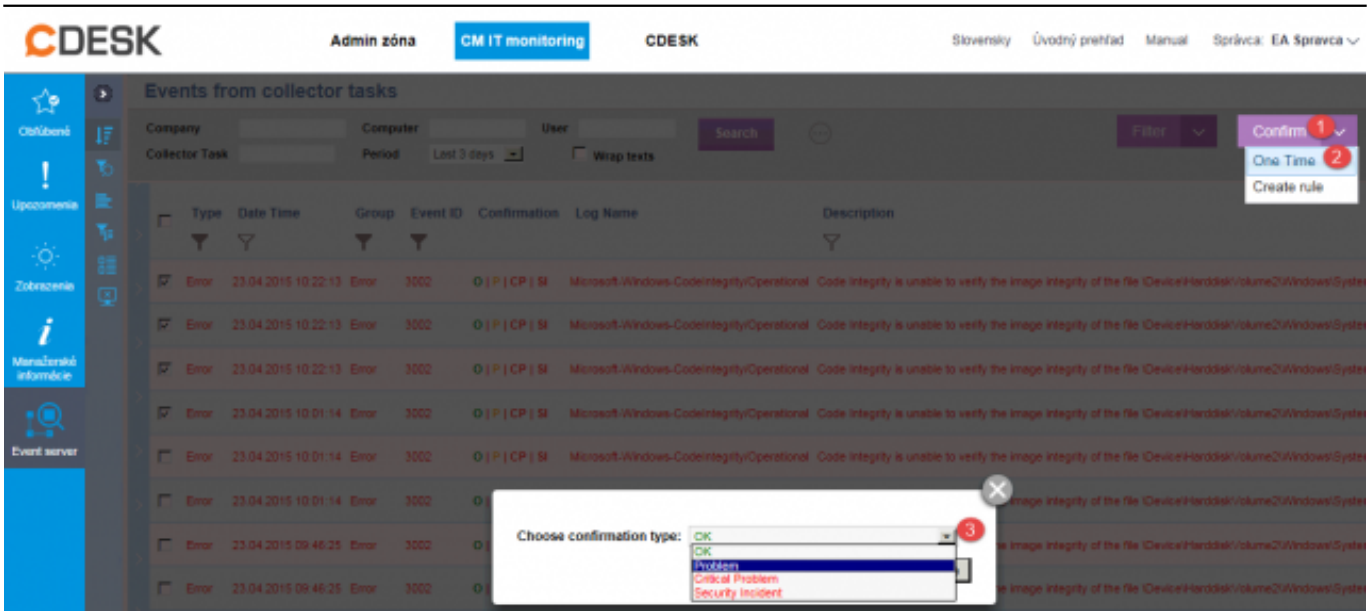
Ďalšou možnosťou je zaznačenie stavu v detaile konkrétnej udalosti. V rolovacom zozname si vyberte jeden zo stavov „OK“, „Problem“, „Critical Problem“ alebo “Security Incident“ a následne kliknite na tlačidlo uložiť.



Obrázok: 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.



Obrázok: 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.

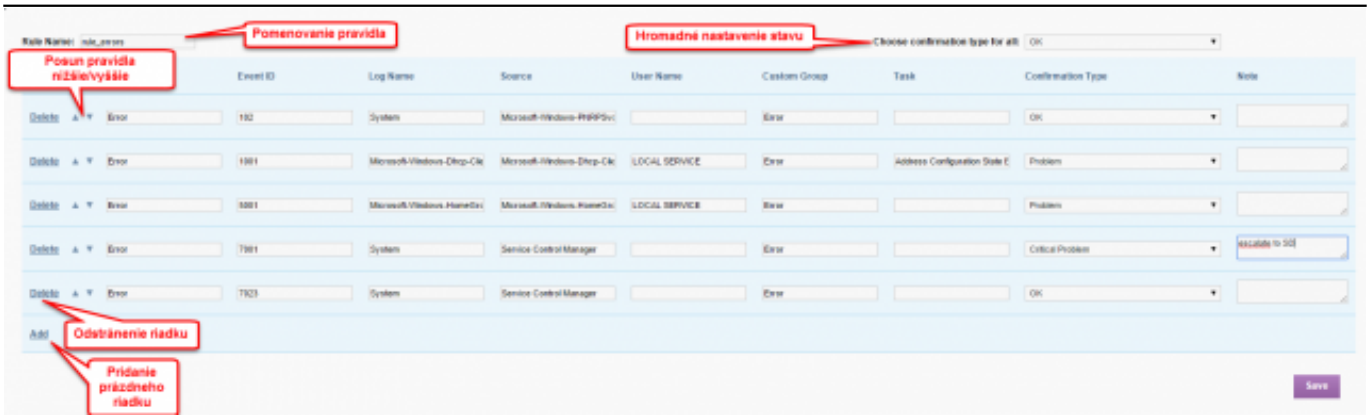
Vytvorenie pravidla vykonáte v menu *„CM IT Monitoring -> Event server -> Správa načítaných udalostí“* prípadne z *„CM IT Monitoring -> Event server -> Jednorazové načítanie“*, kde si pomocou filtra určíte kritéria vyhľadávania a zaškrtnutím udalosti vyberiete len konkrétne, na ktoré sa majú pravidlá 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 (▲ a ▼) resp. pridávať a odoberať pomocou tlačidiel *„Delete“* a *„Add“*.



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