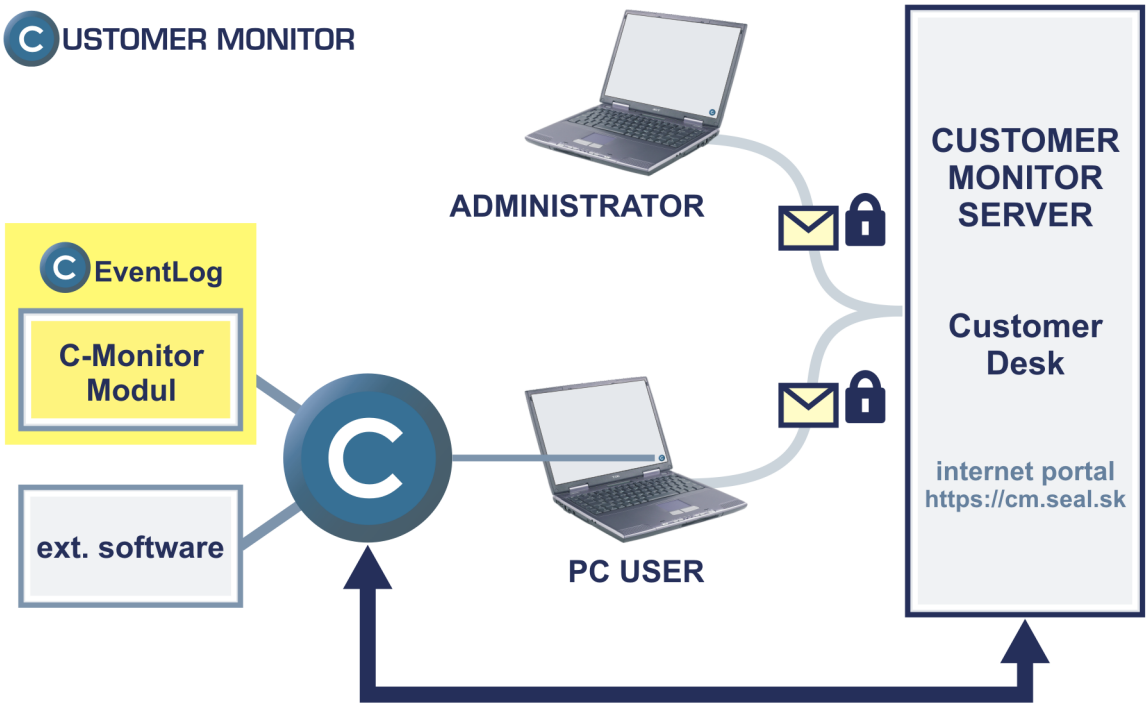
Používateľská príručka

C-EventLogConsole

verzia 2.0.0.206

C-EventLogConsole je nástroj na prezeranie a vyhľadávanie udalostí (events). Jeho funkcia je podobná nástroju Prehliadač udalostí (Event Viewer), ktorý je súčasťou nástrojov pre správu. Tento nástroj pracuje iba na platforme MS Windows NT (XP, 2003). Aplikácia dokáže pracovať v interaktívnom aj neinteraktívnom režime.



Obsah

1 Základné informácie

1.1 Princíp činnosti

Aplikácia načíta zoznam všetkých udalostí zvoleného druhu, a na základe používateľom zadanej podmienky (skriptu) v ňom vyhľadá všetky udalosti ktoré tejto podmienke vyhovujú. Takto získaný „zoznam nájdených udalostí“ je možné prezerať, prípadne ukladať vo viacerých formátoch. Nástroj funguje v interaktívnom režime s používateľským rozhraním alebo v neinteraktívnom režime, v závislosti od parametrov príkazového riadku.

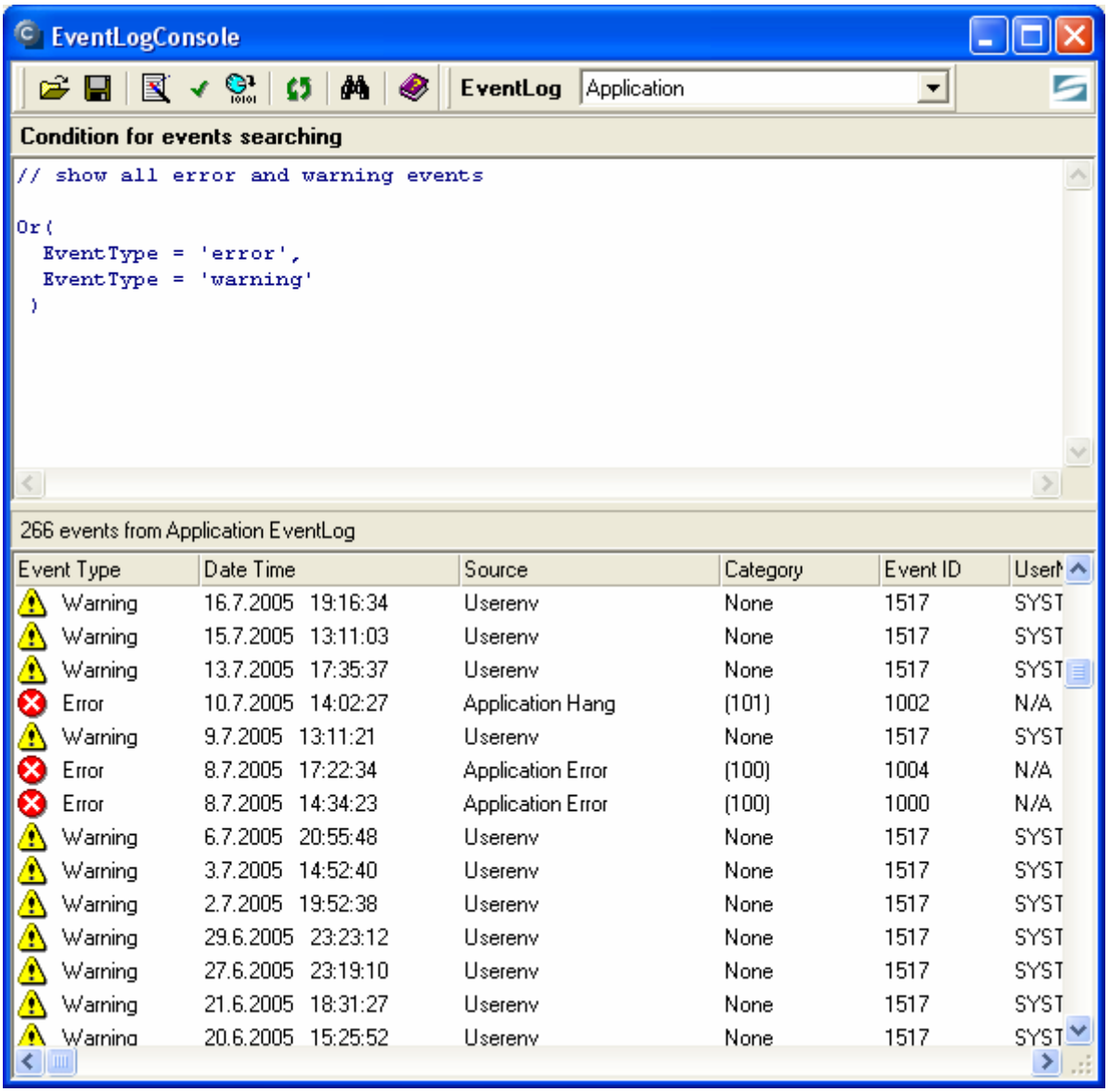
1.2 Licencia

Licencia je súčasťou licencie pre C-Monitor, a nachádza sa v súbore „**License.apk**“, ktorý sa musí nachádzať v tej zložke kde sa nachádza „EventLogConsole.exe“, v jej podzložke „**Cnf**“, v jej ľubovoľnej nadzložke alebo podzložke „**Cnf**“ niektorej jej nadzložky.
Aby aplikácia pracovala, licencia musí byť platná. Aby ale technik mohol používať aplikáciu so svojou licenciou na inom počítači v interaktívnom režime, aplikácia v interaktívnom režime pracuje aj ak je licencia technická a platná pre iný (technikov) počítač.

Príklad typického umiestnenia:
C:\CMonitor\Cnf\License.apk
C:\CMonitor\Modules\EventLog\EventLogConsole.exe

2 Popis použitia, okna aplikácie

Okno aplikácie je rozdelené na niekoľko oblastí – panel nástrojov, pod ním textové pole pre zápis podmienky pre výber udalostí, a dole sa nachádza zoznam vybraných udalostí.



2.1 Typický scenár použitia, práce s týmto oknom

2.1.1 Získanie zoznamu udalostí spĺňajúcich určité kritériá

1. Ak majú byť vybrané iba niektoré udalosti, podmienka pre výber sa buď načíta zo súboru (ak je už pripravená v nejakom súbore, stlačením tlačítka a zvolením príkazu „Load Condition“), alebo sa priamo napíše (skúsení používatelia), alebo sa vytvorí pomocou dialógu spusteného tlačítkom . Je tiež možné použiť príklad a ten upraviť. (príklad sa vloží stlačením tlačítka / Examples / ...).

2. V prípade, že podmienka pre výber udalostí bola priamo napísaná, je doporučené jej zápis skontrolovať stlačením tlačítka - po stlačení tlačítka sa urobí syntaktická kontrola zapísanej podmienky a namiesto zoznamu udalostí sa zobrazí výsledok, prípadné chyby sú vypísané.

3. V rozbaľovacom zozname „EventLog“ na paneli nástrojov sa vyberie zdroj (typ) udalostí, v ktorom sa bude hľadať. Ak v dôsledku výberu zdroja dôjde k načítaniu udalostí, krok 4. je možné vynechať.

4. Stlačením tlačítka sa načítajú všetky udalostí daného typu (vybraného v rozbaľovacom zozname „EventLog“ na paneli nástrojov), a v nich sa vyhľadajú udalosti určené zapísanou podmienkou.

5. Zoznam udalostí sa uloží do súboru stlačením tlačítka a zvolením príkazu „Save Events“.

2.1.2 Vyhľadávanie udalostí spĺňajúcich určité kritériá

1. Ak sa majú vyhľadávať aktuálne udalosti, v rozbaľovacom zozname „EventLog“ na paneli nástrojov sa vyberie požadovaný zdroj (typ) udalostí, v ktorom sa bude hľadať. Ak pri výbere zdroja nedošlo k načítaniu zoznamu udalostí, stlačí sa tlačítko na načítanie tohto zoznamu.

   V prípade, že sa majú vyhľadávať udalosti, informácie o ktorých sú uložené v „*.sel“ súbore, súbor so zoznamom udalostí sa načíta stlačením tlačítka a zvolením príkazu „Load Events“.

2. Ak majú byť vybrané iba niektoré udalosti, podmienka pre výber sa buď načíta zo súboru (ak je už pripravená v nejakom súbore, stlačením tlačítka a zvolením príkazu „Load Condition“), alebo sa priamo napíše (skúsení používatelia), alebo sa vytvorí pomocou dialógu spusteného tlačítkom . Je tiež možné použiť príklad a ten upraviť. (príklad sa vloží stlačením tlačítka / Examples / ...).

3. Stlačením tlačítka sa z načítaného / zo súboru nahratého zoznamu vyhľadajú udalosti určené zapísanou podmienkou.

4. Ak je zoznam nájdených udalostí neprehľadný, stlačením záhlavia príslušného stĺpca je možné tento zoznam usporiadať. Stlačením tlačítka je možné zobraziť dialóg pre vyhľadávanie požadovaného reťazca.

5. Detaily o nájdenej udalosti je možné prezrieť v dialógu, ktorý sa otvorí dvojklikom na požadovanú udalosť.

2.2 Základné okno aplikácie

2.2.1 Popis tlačítiek panela nástrojov

načítanie podmienky (skriptu) alebo zoznamu nájdených udalostí zo súboru. Po stlačení tlačítka sa rozbalí menu, ktoré obsahuje príkazy:

- „**Load Condition**“ - načítanie podmienky (skriptu) zo súboru
- „**Load Events**“ - načítanie zoznamu nájdených udalostí zo súboru

uloženie podmienky (skriptu) alebo zoznamu udalostí do súboru. Po stlačení tlačítka sa rozbalí menu, ktoré obsahuje nasledovné príkazy:

- „**Save Condition**“ - uloženie podmienky (skriptu) do súboru
- „**Save Events**“ - uloženie zoznamu nájdených udalostí do súboru

zobrazenie dialógu pre „zostavenie podmienky“ – popis dialógu je v samostatnej kapitole.

syntaktická kontrola podmienky – slúži na kontrolu toho, ako aplikácia spracovala zadanú podmienku, či je podmienka syntakticky správne napísaná, či neobsahuje formálne chyby. V dôsledku stlačenia tohto tlačítka sa namiesto zoznam nájdených udalostí zobrazí výsledok syntaktickej kontroly podmienky, ukážka je pri popise tohto poľa („Condition syntax check result“).

vyhľadanie tých udalostí z naposledy načítaného zoznamu všetkých udalostí, ktoré vyhovujú zadanej podmienke. Z dôvodu, že tento príkaz pracuje nad už načítaným zoznamom všetkých udalostí, jeho vykonanie je rýchle, a preto je tento príkaz vhodný na testovanie a ladenie podmienok. Načítanie zoznamu všetkých udalostí je časovo oveľa náročnejšie ako vyhľadanie udalostí z neho na základe podmienky.
Pracuje sa podľa opakovaného scenára „načítaj zoznam všetkých udalostí, vyhľadaj požadované, vyhľadaj požadované, vyhľadaj požadované,...“

V prípade, že je definícia podmienky v poriadku, zobrazí sa v dolnej časti okna zoznam nájdených udalostí, v prípade, že podmienka nie je zadaná správne (obsahuje syntaktické chyby), zobrazí sa namiesto zoznamu nájdených udalostí pole „**Condition syntax check result**“, ukážka je pri popise tohto poľa.

načítanie zoznamu všetkých udalostí a vyhľadanie tých z nich, ktoré vyhovujú zadanej podmienke. Pracuje podobne ako predošlý príkaz  , avšak pretože načítanie zoznamu všetkých udalostí môže byť časovo náročné, jeho vykonanie môže trvať niekoľko násobne dlhšie. Oproti príkazu  pracuje vždy nad najnovšími údajmi.
Pracuje sa podľa opakovaného scenára „načítaj zoznam všetkých udalostí a vyhľadaj požadované, načítaj zoznam všetkých udalostí a vyhľadaj požadované, načítaj zoznam všetkých udalostí a vyhľadaj požadované,...“

V prípade, že je definícia podmienky v poriadku, zobrazí sa v dolnej časti okna zoznam nájdených udalostí, v prípade, že podmienka nie je zadaná správne (obsahuje syntaktické chyby), zobrazí sa namiesto zoznamu nájdených udalostí pole „**Condition syntax check result**“, ukážka je pri popise tohto poľa.

vyhľadávanie textu v zozname nájdených udalostí

zobrazenie menu obsahujúceho príkaz

- „**About**“ - zobrazenie informácií o aplikácií
- „**Condition Definition**“ - krátky návod na písanie podmienky
- „**Examples**“ - v tomto podmenu je niekoľko príkladov podmienok

2.2.2 EventLog

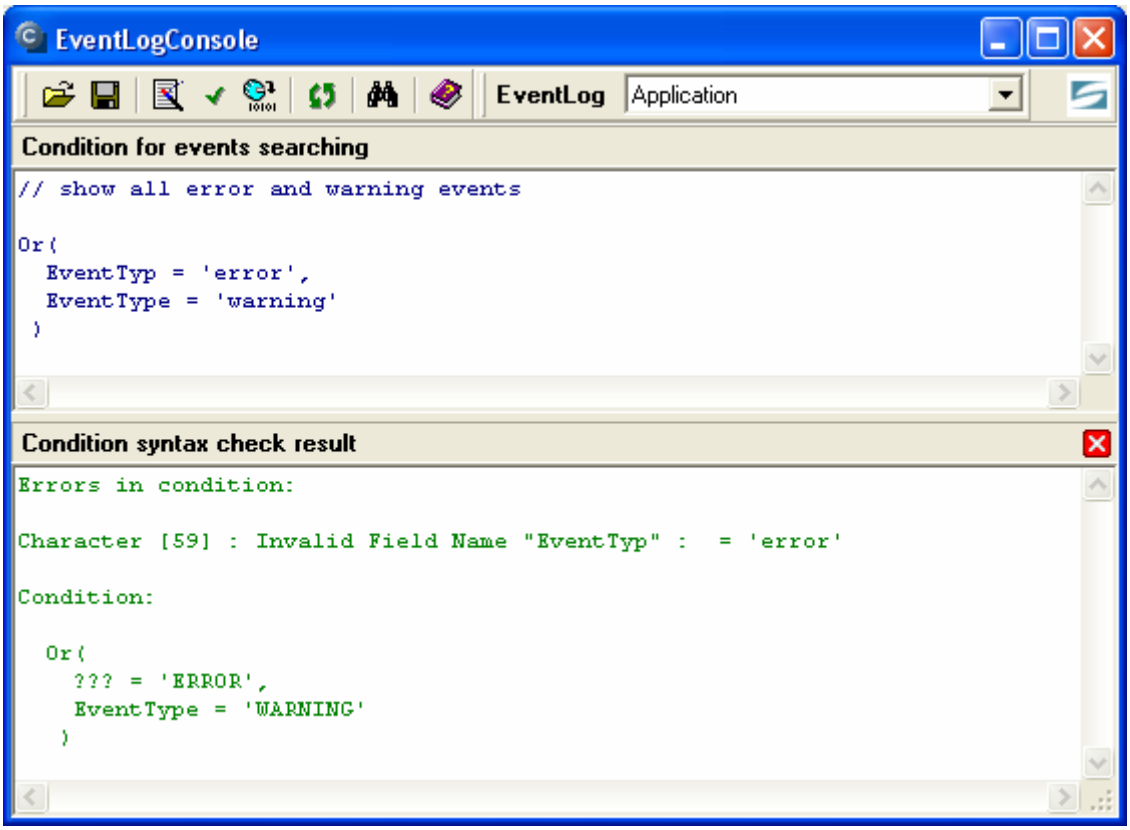
Toto pole slúži na výber druhu udalostí, tento zoznam ponúka všetky dostupné druhy udalostí (na základe informácií získaných zo systému). Pri výbere druhu udalostí sa automaticky načíta zoznam všetkých udalostí vybratého druhu a vyhľadajú sa udalosti vyhovujúce zadanej podmienke.

2.2.3 Condition for events searching

Toto pole je určené pre zápis podmienky pre vyhľadanie udalostí, ak sa ponechá prázdne, sú do výsledku zahrnuté všetky udalosti. Popis syntaxe podmienky je v samostatnej kapitole.

2.2.4 Condition syntax check result

V tomto poli sa zobrazujú informácie o spracovaní podmienky. Zobrazujú sa tu podmienky tak, ako im aplikácia porozumela, a tiež sa tu zobrazujú syntaktické či iné chyby súvisiace so spracovaním podmienky.



Toto pole sa automaticky zobrazí namiesto zoznamu udalostí vždy, keď je nejaký problém so spracovaním podmienky (po stlačení tlačítka , resp. , výbere zdroja / typu udalostí), a vždy po syntaktickej kontrole vynútenej stlačením tlačítka .

Stlačením tlačítka dôjde k prepnutiu na zoznam nájdených udalostí.

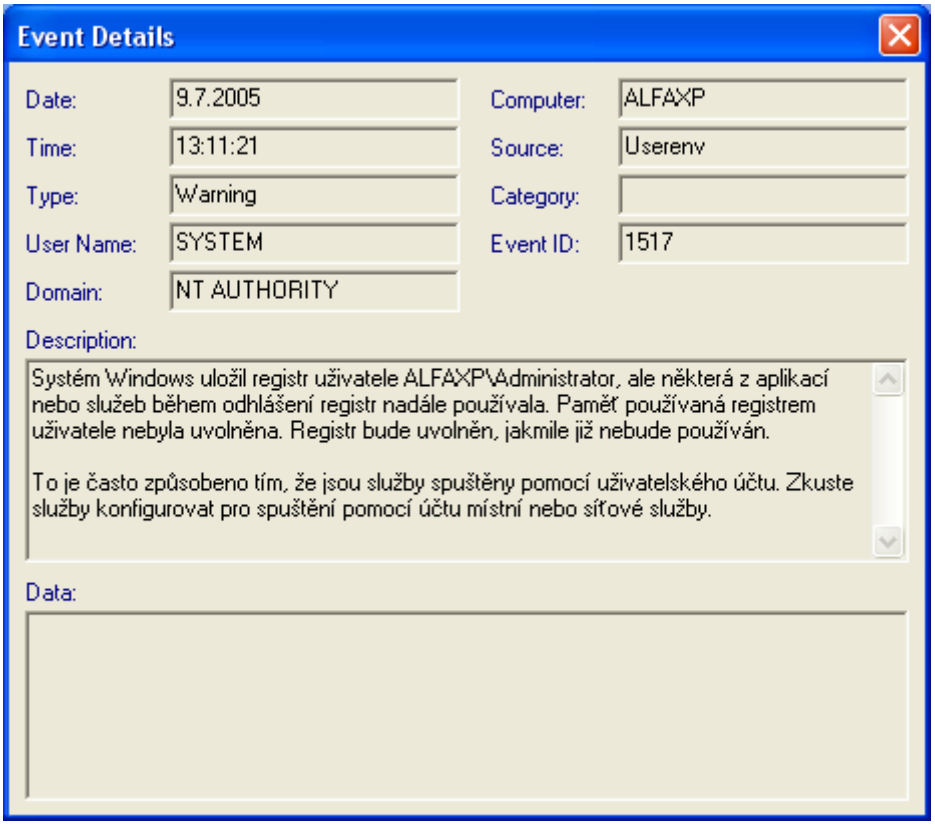
2.2.5 Zoznam nájdených udalostí

Tento zoznam obsahuje také udalosti zo zoznamu všetkých udalostí, ktoré vyhovujú zadanej podmienke. Tento zoznam možno usporiadať stlačením záhlavia stĺpca, smer usporiadania je indikovaný zelenou šípkou - vzostupne , zostupne . Smer usporiadania sa mení na opačný po každom ďalšom stlačení toho istého záhlavia.
Dvojklikom na požadovanú udalosť alebo stlačenie klávesy „**Enter**“ na požadovanej udalosti spôsobí zobrazenie okna s detailmi o vybratej udalosti. Vybratím inej udalosti sa automaticky v okne detailov o nej zobrazia detaily.

2.3 Okno detailov udalosti

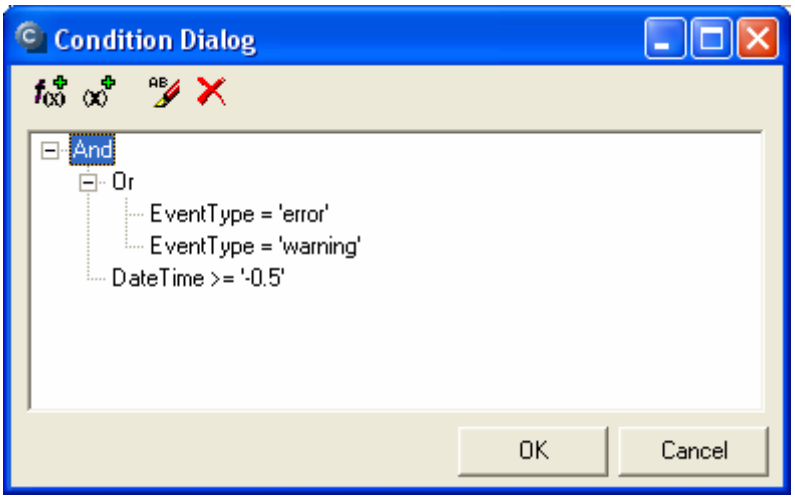
Okno detailov udalosti sa otvorí dvojklikom na požadovanú udalosť, alebo stlačením klávesy „**Enter**“ na tejto udalosti.

Toto okno je plávajúce, zobrazuje detailné informácie o práve vybratej udalosti v zozname nájdených udalostí. Pri výbere inej udalosti v zozname nájdených udalostí sú informácie v tomto okne automaticky aktualizované, platí to aj pri výbere udalosti počas vyhľadávania (dialóg pre vyhľadávanie sa zobrazí stlačením tlačítka). Toto okno nie je nutné pred výberom inej udalosti zatvoriť.



2.4 Dialóg pre zostavenie podmienky

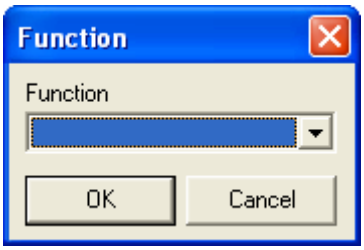
Po stlačení tlačítka sa spracuje zadaná podmienka, a v prípade, že neobsahujú syntaktické či iné chyby, zobrazí sa dialóg pre zostavenie podmienky. V prípade, že zadaná podmienka chyby obsahuje, do poľa „Condition syntax check result“ (Výsledok syntaktickej kontroly podmienky) sa tieto chyby vypíšu a **dialóg sa nezobrazí**.



Podmienky sa zobrazujú v stromovej štruktúre, ktorá vyjadruje logiku spracovania. Ako je vidieť na obrázku – funkcia „**Or**“ má operandy dve podmienky „**EventType = ‘error’**“ a „**EventType = ‘warning’**“, a funkcia „**And**“ má operandy uvedenú funkciu „Or“ a podmienku „**DateTime >= ‘-0.5’**“

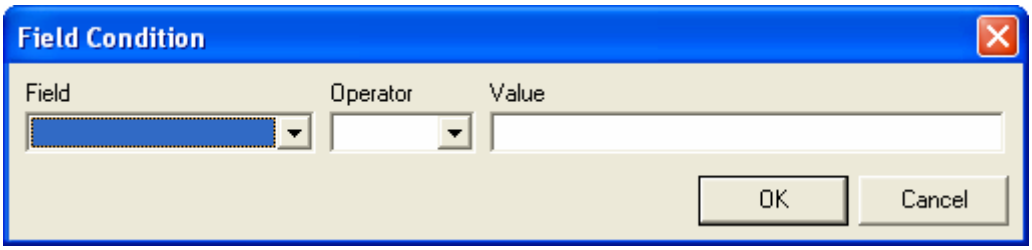
2.4.1 Popis tlačítiek

pridanie „**zloženej podmienky**“ (funkcie). Po stlačení tohto tlačítka sa zobrazí dialóg pre výber funkcie („**And**“, „**Or**“, „**NAnd**“, „**Nor**“), po stlačení „**OK**“ sa vybraná funkcia pridá ako **operand**. Pre situáciu ako je na ilustračnom obrázku by sa funkcia pridala ako operand funkcie „**And**“, Ak by bola vybratá niektorá podmienka, funkcia by sa pridala ako jej „sesterský“ operand.



pridanie „**jednoduchej podmienky**“ . Po stlačení tohto tlačítka sa zobrazí dialóg pre vytvorenie podmienky. V poli „**Field**“ je treba vybrať ktorá hodnota, parameter z udalosti sa bude skúmať, v poli „**Operator**“ je potrebné vybrať operátor, a do poľa „**Value**“ zadať požadovanú hodnotu. Po stlačení „**OK**“ sa vybraná podmienka pridá ako **operand**. Pre situáciu ako je na ilustračnom obrázku by sa podmienka pridala ako

operand funkcie „**And**“, Ak by bola vybratá niektorá podmienka, funkcia by sa pridala ako jej „sesterský“ operand.



Poznámka
výklad pojmov „**Field**“, „**Operator**“, „**Value**“ sa nachádza v kapitole „**Popis syntaxe podmienky (skriptu)**“ podkapitole „**Popis prvkov syntaxe**“


modifikácia podmienky. Podľa toho, čo je vybraté – zložená podmienka (funkcia) alebo jednoduchá podmienka, sa po stlačení tohto tlačítka zobrazí príslušný dialóg, v ktorom je možné zloženú podmienku (funkciu) alebo jednoduchú podmienku zmeniť.


odstránenie podmienky. Ak sa maže zložená podmienka (funkcia), vymažú sa aj všetky jej operandy.

Tlačítko „**OK**“	uloženie, potvrdenie zmien, zatvorenie dialógu.
Tlačítko „**Cancel**“	stornovanie zmien a zatvorenie dialógu.

3 Neinteraktívny režim

C-EventLogConsole je možné spúšťať aj v neinteraktívnom režime, ak je potrebné vyhľadať udalosti podľa určitej podmienky, a ich zoznam uložiť do súboru, a to bez interakcie s používateľom. Popis parametrov príkazového riadku sa nachádza v samostatnej kapitole.

4 Popis parametrov príkazového riadku

Či aplikácia pobeží v interaktívnom alebo neinteraktívnom režime určujú parametre príkazového riadku, s ktorými bude spustená.

Ak sú uvedené 3 alebo 4 parametre, aplikácia bude pracovať v neinteraktívnom režime – t.j. nevytvorí sa žiadne okno, bude sa pracovať iba nad súbormi určenými parametrami..

4.1 Spustenie v interaktívnom režime

EventLogConsole.exe [<udalosti>]

[<udalosti>] nepovinný parameter, meno „***.sel**“ súboru so zoznamom udalostí. Po spustení aplikácie sa uvedený súbor sa načíta do zoznamu nájdených udalostí.

Príklad:

spustenie aplikácie a načítanie súboru “c:\appevents.sel”

EventLogConsole.exe c:\appevents.sel

4.2 Spustenie v neinteraktívnom režime

EventLog.exe <typ_udalostí> <podmienka> <udalosti> [<formát>]

<typ_udalostí> určuje druh udalostí v ktorom sa má vyhľadávať, nad ktorými sa pracuje. Môže mať nasledovné hodnoty:

apps - udalosti aplikácií
system - udalosti systému
security - udalosti zabezpečenia

alebo táto hodnota musí byť podkľúčom nasledovného kľúča v registry databáze

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog

<podmienka> meno textového súboru, v ktorom je zapísaná podmienka pre vyhľadanie udalostí zo zoznamu všetkých udalostí. V prípade, že sa majú do výstupu zahrnúť všetky udalosti, je možné ako hodnotu uviesť "**N/A**".

<udalosti> meno súboru, do ktorého sa má uložiť zoznam nájdených udalostí. Výstupný súbor je uložený buď vo formáte XML (ak je uvedený prepínač „**-xml**"), alebo v systémovom formáte v nekomprimovanom tvare (prepínač „**-sel**"), alebo v komprimovanom tvare (prepínač „**-selc**"). Predvolený formát je komprimovaný systémový, t.j. ak sa neuvedie žiaden prepínač, výstupný súbor bude uložený v systémovom komprimovanom formáte.

[<formát>] tento parameter je nepovinný, určuje formát výstupného súboru, a môže to byť jedna z nasledovných hodnôt „**-xml**", „**-sel**", „**-selc**".

-xml ak je uvedený prepínač „**-xml**", výstupný súbor <Udalosti> bude uložený vo formáte XML.

-sel ak je uvedený prepínač „**-sel**", výstupný súbor <Udalosti> bude uložený v systémovom nekomprimovanom formáte.

-selc ak je uvedený prepínač „**-selc**", výstupný súbor <Udalosti> bude uložený v systémovom komprimovanom formáte. Ak sa neuvedie iný prepínač, výstupný súbor bude uložený v tomto formáte.

Po spustení sa načítajú všetky udalosti zvoleného druhu „**<typ_udalostí>**", a vyhľadajú sa také z nich, ktoré spĺňajú podmienku načítanú zo súboru „**<podmienka>**" a uložia sa do súboru určeného menom „**<udalosti>**".

Príklad:

uloženie všetkých udalostí aplikácií do súboru „c:\appevents.xml" vo formáte XML

EventLogConsole.exe apps N/A c:\appevents.xml –xml

uloženie všetkých systémových udalostí ktoré spĺňajú podmienky zapísané v súbore „c:\conditions.txt" do súboru „c:\sysevents.sel" v systémovom komprimovanom tvare

EventLogConsole.exe system c:\conditions.txt c:\sysevents.sel

5 Popis syntaxe podmienky (skriptu)

Podmienky pre vyhľadanie udalostí sa zapisujú vo forme textu do poľa na to určeného („Condition for events searching“).

Buď nemusí byť zadaná „**žiadna podmienka**“, alebo môže byť zadaná jedna „**jednoduchá podmienka**“, alebo môže byť zadaná jedna „**zložená podmienka**“.

5.1 Žiadna podmienka

Ak nie je zadaná žiadna podmienka, vyhľadajú sa všetky udalosti.

5.2 Jednoduchá podmienka

Jednoduchá podmienka má syntax

<Pole><Operátor><Hodnota>

Vyhľadajú sa iba tie udalosti, ktoré vyhovejú tejto podmienke.

Napr.

EventType = 'error'

spôsobí vyhľadanie tých udalostí, ktoré majú typ udalosti „error“.

Poznámka
výklad pojmov „<Pole>“, „<Operátor>“, „<Hodnota>“ sa nachádza v podkapitole „**Popis prvkov syntaxe**“

5.3 Zložená podmienka (funkcia)

Zložená podmienka má syntax

<Funkcia>**(**<Operand>[**,**<Operand>]**)**

<Funkcia> je jedna z logických funkcií

„And“, „Or“, „NAnd“, „NOr“

(na veľkosť písmen sa neprihliada, neprihliada sa ani na medzery vyskytujúce sa medzi jednotlivými symbolmi)

<Operand> je buď jednoduchá alebo zložená podmienka.

Jednotlivé „Operandy“ sú oddelené čiarkou, ich počet nie je obmedzený, a sú uzavreté do jednoduchých zátvoriek.

Či je podmienka splnená alebo nie, závisí od typu funkcie, a či sú „splnené“ jej operandy alebo nie (toho, ako sa operandy vyhodnotia).

Napr.

Or(EventType = ‘Error‘, EventType = ‘Warning‘)

Poznámka
výklad pojmov „<Funkcia>“, „<Operand>“ sa nachádza v podkapitole „**Popis prvkov syntaxe**“

5.4 Popis prvkov syntaxe

5.4.1 Pole (parameter udalosti), tiež „Field“

Pri písaní jednoduchých podmienok <Pole> značí názov poľa, je to text, ktorý nie je uzavretý do zátvoriek ani apostrofov.

Každá udalosť má nasledovné polia (parametre), ktorých požadovanú hodnotu možno ošetriť podmienkami, čím sa vlastne rozhoduje o tom, či tá ktorá udalosť bude vyhľadaná alebo nie.

5.4.1.1 „EventType“ (typ udalosti)

nadobúda jednu z nasledovných hodnôt

„Unknown“ - neznámy typ
„Error“ - chyba
„Warning“ - upozornenie
„Information“ - informácia
„AuditSuccess“ - úspešný audit
„AuditFailure“ - neúspešný audit

Ako hodnotu pri jednoduchej podmienke má teda zmysel používať iba niektorú z uvedených hodnôt (textov), pričom pri vyhodnocovaní podmienky sa na veľkosť písmen neprihliada.

5.4.1.2 „DateTime“ (dátum a čas udalosti)

má formát YYYY.MM.DD/HH:NN:SS:ZZZ kde

YYYY je rok (4 cifry)
MM mesiac (2 cifry)
DD deň v mesiaci (2 cifry)
HH hodina (2 cifry)
NN minúta (2 cifry)
SS sekunda (2 cifry)
ZZZ tisícina sekundy (3 cifry)

Napr. 2004.12.31/23:59:59:999

Ako hodnotu pri jednoduchej podmienke je možné zadať hodnotu dátumu a času udalosti niektorým z nasledovných spôsobov:

Konkrétny dátum a čas

Iba dátum, napr. **2004.12.31** znamená 2004.12.31/00:00:00:000
Dátum a jednoduchý čas, napr. **2004.12.31/23:59:59** znamená 2004.12.31/23:59:59:000
Dátum a kompletný čas, napr. **2004.12.31/23:59:59:999**

Relatívne k aktuálnemu dátumu a času

(N je celé číslo, F je desatinné číslo)

+N napr. **+2** ak je aktuálny dátum a čas 2004.12.20/15:45:00:000 znamená 2004.12.22/00:00:00:000

-N napr. **-2** ak je aktuálny dátum a čas 2004.12.20/15:45:00:000 znamená 2004.12.18/00:00:00:000

+F napr. **+2.5** ak je aktuálny dátum a čas 2004.12.20/15:45:00:000 znamená 2004.12.23/03:45:00:000, lebo 2.5 dňa je 60 hodín (2.5 x 24h)

-F napr. **-2.5** ak je aktuálny dátum a čas 2004.12.20/15:45:00:000 znamená 2004.12.18/03:45:00:000, lebo 2.5 dňa je 60 hodín (2.5 x 24h)

5.4.1.3 „Source“ (zdroj udalosti)

môže to byť akýkoľvek text

Ako hodnotu pri jednoduchej podmienke má teda zmysel používať akýkoľvek text, pričom pri vyhodnocovaní podmienky sa na veľkosť písmen neprihliada.

5.4.1.4 „Category“ (kategória udalosti)

môže to byť akýkoľvek text, ak nie je žiadna, hodnota je „**None**“.

Ako hodnotu pri jednoduchej podmienke má teda zmysel používať akýkoľvek text, pričom „**None**“ značí nedefinovanú / neurčenú kategóriu, a pri vyhodnocovaní podmienky sa na veľkosť písmen neprihliada.

5.4.1.5 „EventID“ (identifikačné číslo udalosti)

môže to byť celočíselná kladná hodnota

Ako hodnotu pri jednoduchej podmienke má teda zmysel používať iba celé čísla.

5.4.1.6 „UserName“ (meno používateľa)

môže to byť akýkoľvek text, ak nie je žiadny, hodnota je „**N/A**“.

Ako hodnotu pri jednoduchej podmienke má teda zmysel používať akýkoľvek text, pričom „**N/A**“ značí nedefinovaného / neurčeného používateľa, a pri vyhodnocovaní podmienky sa na veľkosť písmen neprihliada.

5.4.1.7 „Domain“ (doména)

môže to byť akýkoľvek text

Ako hodnotu pri jednoduchej podmienke má teda zmysel používať akýkoľvek text, pričom pri vyhodnocovaní podmienky sa na veľkosť písmen neprihliada.

5.4.1.8 „Computer“ (počítač)

môže to byť akýkoľvek text

Ako hodnotu pri jednoduchej podmienke má teda zmysel používať akýkoľvek text, pričom pri vyhodnocovaní podmienky sa na veľkosť písmen neprihliada.

5.4.1.9 „Description“ (popis)

môže to byť akýkoľvek text

Ako hodnotu pri jednoduchej podmienke má teda zmysel používať akýkoľvek text, pričom pri vyhodnocovaní podmienky sa na veľkosť písmen neprihliada.

5.4.1.10 „BinaryData“ (binárne údaje)

môže to byť akýkoľvek text

Ako hodnotu pri jednoduchej podmienke má teda zmysel používať akýkoľvek text, pričom pri vyhodnocovaní podmienky sa na veľkosť písmen neprihliada.

5.4.2 Operátor, tiež „Operator“

Pri písaní jednoduchých podmienok <Operátor> značí operátor, je to text, ktorý nie je uzavretý do zátvoriek ani apostrofov.

Operátor určuje požadovaný vzťah medzi „poľom“ (parametrom udalosti) a jeho „hodnotou“

5.4.2.1 „=“ (rovnaká hodnota)

určuje, že daný parameter **má mať** práve takúto hodnotu

5.4.2.2 „<>“ (rôzna hodnota)

určuje, že daný parameter **nemá mať** takúto hodnotu

5.4.2.3 „<“ (menšia hodnota)

určuje, že daný parameter **má mať menšiu** hodnotu

5.4.2.4 „<=“ (menšia alebo rovnaká hodnota)

určuje, že daný parameter **má mať menšiu alebo práve takúto** hodnotu

5.4.2.5 „>“ (väčšia hodnota)

určuje, že daný parameter **má mať väčšiu** hodnotu

5.4.2.6 „>=“ (väčšia alebo rovnaká hodnota)

určuje, že daný parameter **má mať väčšiu alebo práve takúto** hodnotu

5.4.2.7 „%“ ()

určuje, že v danom parametri (jeho hodnote) **sa má nachádzať** táto hodnota

5.4.2.8 „!%“ ()

určuje, že v danom parametri (jeho hodnote) **sa nemá nachádzať** táto hodnota

5.4.3 Hodnota, tiež „Value“

Pri písaní jednoduchých podmienok <Hodnota> značí hodnotu, s ktorou sa operátorom porovnáva hodnota toho ktorého pola (parametra) udalosti , je to text, ktorý je uzavretý do apostrofov.

Hodnoty pre jednotlivé polia sú popísané v podkapitole „**Pole (parameter udalosti), tiež „Field“**“

5.4.4 Funkcia, tiež „Function“

funkciou sa rozumie logická funkcia, ktorou je možné vytvárať zložené podmienky

5.4.4.1 And (a súčasne)

Podmienka je splnená vtedy, ak sú splnené všetky podmienky predstavujúce jej operandy

5.4.4.2 Or (alebo)

Podmienka je splnená vtedy, ak je splnená aspoň jedna z podmienok predstavujúcich jej operandy.

5.4.4.3 NAnd (nie a súčasne)

Podmienka je splnená vtedy, ak nie je splnená aspoň jedna z podmienok predstavujúcich jej operandy.

5.4.4.4 NOr (nie alebo)

Podmienka je splnená vtedy, ak nie je splnená ani jedna z podmienok predstavujúcich jej operandy.

5.4.5 Operand

je jednoduchá alebo zložená podmienka.

5.5 Príklady podmienok

5.5.1 Vyhľadanie všetkých udalostí

Ako podmienku treba zadať prázdny text

5.5.2 Vyhľadanie všetkých udalostí typu „Chyba“

EventType = ‘Error’

5.5.2.1 Vyhľadanie všetkých udalostí typu „Chyba“ a „Upozornenie“

Or(EventType = ‘Error’, EventType = ‘Warning’)

5.5.2.2 Vyhľadanie udalostí typu „Chyba“ za posledných 5 dní

And(EventType = ‘Error’, DateTime >= ‘-5’)

5.5.2.3 Vyhľadanie udalostí typu „Chyba“ za posledných 48 hodín

And(EventType = ‘Error’, DateTime >= ‘-2.0’)

5.5.2.4 Vyhľadanie udalostí typu „Chyba“ alebo „Upozornenie“ za posledných 5 dní

And(Or(EventType = ‘Error’,

```
        EventType = ‘Warning’ ),
DateTime >= ‘-5’ )
```