Diagnozowanie awarii w Windows Server

Serwerowe systemy operacyjne muszą cechować się ciągłą i stabilną pracą. Można sobie bowiem wyobrazić przypadek, gdy w hucie szkła albo na linii produkcyjnej samochodów nagle przestaje działać oprogramowanie zależne od serwera tylko dlatego, że system na nim „zawiesił się". Straty przez tego typu awarię liczy się przeważnie w milionach (zatrzymanie linii, czas potrzebny wznowienie jej pracy itp.). Dlatego administratorzy serwerów muszą potrafić potrafić szybko znaleźć potencjalne źródła problemów i jeszcze szybciej je eliminować.

Niestety Windows Server jest jednym z bardziej kapryśnych serwerowych systemów operacyjnych. Same jego domyślne usługi potrafią ciągle zgłaszać ostrzeżenia i błędy, z których niektóre producent systemu doradza „spokojnie ignorować". Oczywiście względem pierwszych wersji systemów z rodziny NT dokonał się niebywały postęp pod względem stabilności produktu firmy Microsoft. W teorii system ten może teraz działać bez okresowych ponownych uruchomień (zalecane było dokonywanie restartu co 30 dni), więcej operacji może zostać zastosowanych bez ponownego uruchomienia systemu itd. System nadal jest jednak oparty o konfigurację rejestru systemowego, którego jakakolwiek zmiana wymaga restartu (a przynajmniej wylogowania/zalogowania jeżeli tyczy się tylko zmiany na koncie danego użytkownika); to samo tyczy się wdrażania jakichkolwiek łatek systemowych dostępnych przez Windows Update. Tak więc wymóg ponownego uruchomienia został zastąpiony planowanymi uruchomieniami wdrażającymi łatki i nowe konfiguracje systemowe.

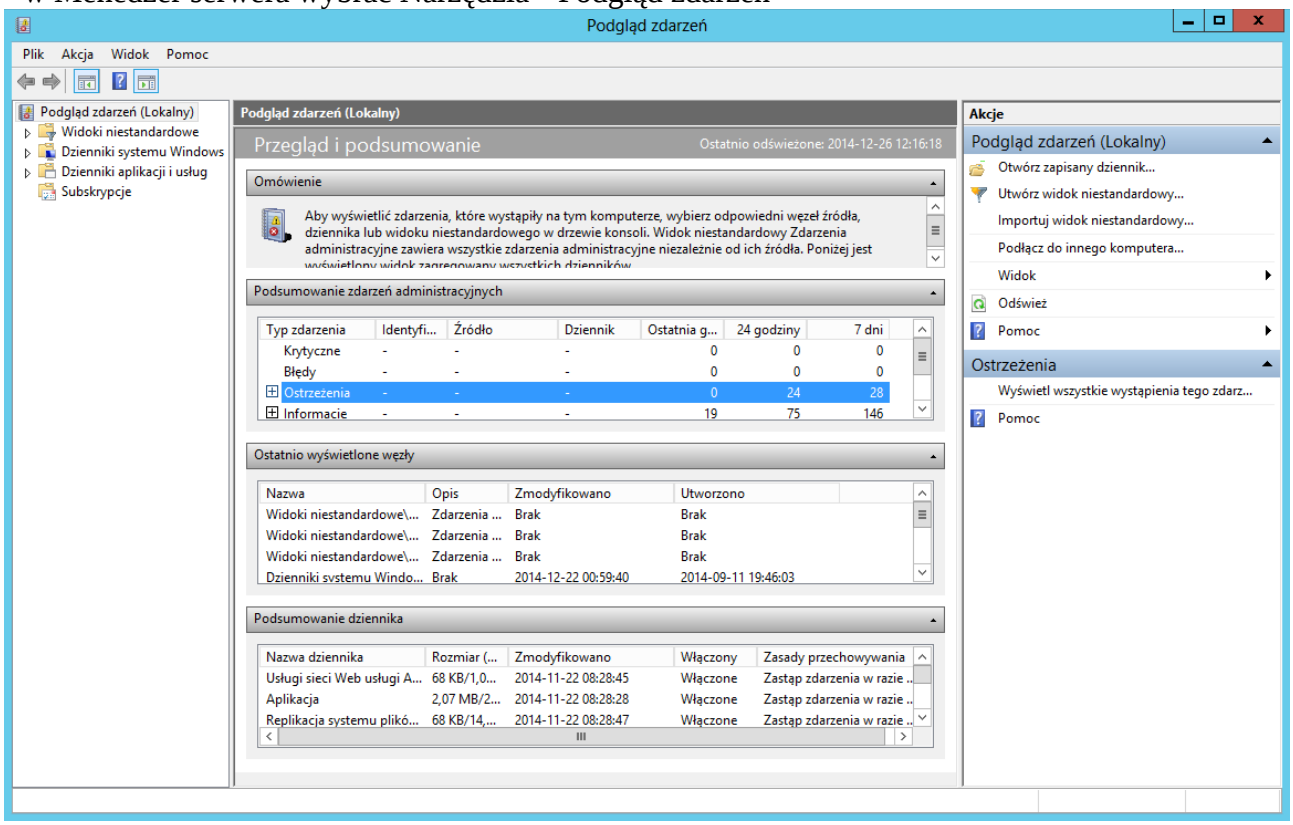
Trzeba pamiętać, że im więcej usług i ról posiada Windows Server, tym więcej potencjalnych błędów może być generowanych przez system, a to z kolei może prowadzić do niestabilności systemu. Przykładowo jeżeli system pełni rolę serwera terminali to jego „piętą achillesową" mogą stać się użytkownicy. Jeżeli nie zablokujemy użytkownikom możliwości Wstrzymywania sesji to może zdarzyć się, że system po iluś godzinach/dniach pracy odmówi jakichkolwiek logowań do systemu i będziemy zmuszeni do ręcznego restartu systemu. Dzieje się tak dlatego, że wstrzymywana sesja zamraża wszystkie otwarte przez użytkownika procesy i aplikacje. Jeżeli są one wadliwe (mają np. wycieki pamięci) to zajmują one coraz więcej i więcej pamięci systemowej. System, do czasu aż aplikacja jest otwarta, przydziela jej coraz więcej pamięci aż w końcu zajmie ona całą dostępną przestrzeń, po czym zacznie być wykorzystywany plik wymiany. Do tego należy pamiętać iż Windows czasami „zapomina" zwolnić niepotrzebną mu pamięć operacyjną, przez co również rośnie zapotrzebowanie na nią (na to pomaga tylko restart lub odpowiednie oprogramowanie)

Oczywiście przedstawiony powyżej problem to tylko jeden z wielu, z jakimi mierzą się na co dzień administratorzy serwerów. Trzeba pamiętać, że poszczególne usługi mogą posiadać wystawione czasowe certyfikaty (ich wygaśnięcie może powodować ostrzeżenie/błąd aplikacji), niektóre usługi mogą działać wadliwie gdyż inna usługa działa wadliwie (łańcuch powiązanych usług – np. Sharepoint w podstawowej wersji wymaga IIS, SQL oraz 3 swoich własnych procesów by działać prawidłowo; błąd którejkolwiek z wymienionych powoduje przypadkowe/losowe błędy całej aplikacji), jeszcze inne mogą być źle napisane (i zgłaszać wyjątki) – a wszystko to ma niestety niebagatelny wpływ na funkcjonowanie systemu serwerowego.

System Windows Server, jak każdy inny system, monitoruje działanie swojej pracy. Jeżeli serwer zachowuje się w sposób nieoczekiwany, często się restartuje albo zawiesza to istnieje duża szansa, iż mamy do czynienia z jednym/wieloma zdarzeniem/zdarzeniami opisanymi powyżej. System Windows (nie tylko Server) posiada specjalną, systemową usługę, uruchamianą wraz z systemem (ma ona jeden z wyższych priorytetów wśród usług niekrytycznych) – EventLog (w wersji polskiej nazywa się Dziennik zdarzeń systemu Windows). Rejestruje ona błędy zarówno systemowe, jak i programów/aplikacji działających w systemie. Domyślnie rejestrowane są zdarzenia systemu oraz aplikacji działających jako aktywne procesy (także te w tle – np. poprzez harmonogram zadań).

Praca z dziennikami zdarzeń

Domyślnie system do poglądu/zarządzania zdarzeniami posiada narzędzie Podgląd zdarzeń. Uruchomić można je np. poprzez:
- polecenie Uruchom – eventvwr.msc
- Panel sterowania->Narzędzia administracyjne->Podgląd zdarzeń
- w Menedżer serwera wybrać Narzędzia->Podgląd zdarzeń



Po lewej stronie mamy dostępne drzewo posegregowanych zdarzeń. Domyślnie ustawione są 3 katalogi. Jeżeli będziemy otwierali zapisane dzienniki to będą otwierane jako kolejne katalogi.

- Widoki niestandardowe – tutaj narzędzie umieszcza przefiltrowane widoki na zdarzenia. Administrator, tworząc taki widok, może widzieć tylko interesujące go ostrzeżenia/błędy zebrane od wybranych aplikacji/usług systemowych oraz ustalić np. z której godziny interesują go takie raporty. Istnieje również możliwość ręcznego pisania takowego filtru oraz filtrowania już stworzonego widoku. Niektóre role systemu dodają własne widoku darzeń (w celu lepszego śledzenia ich działania)

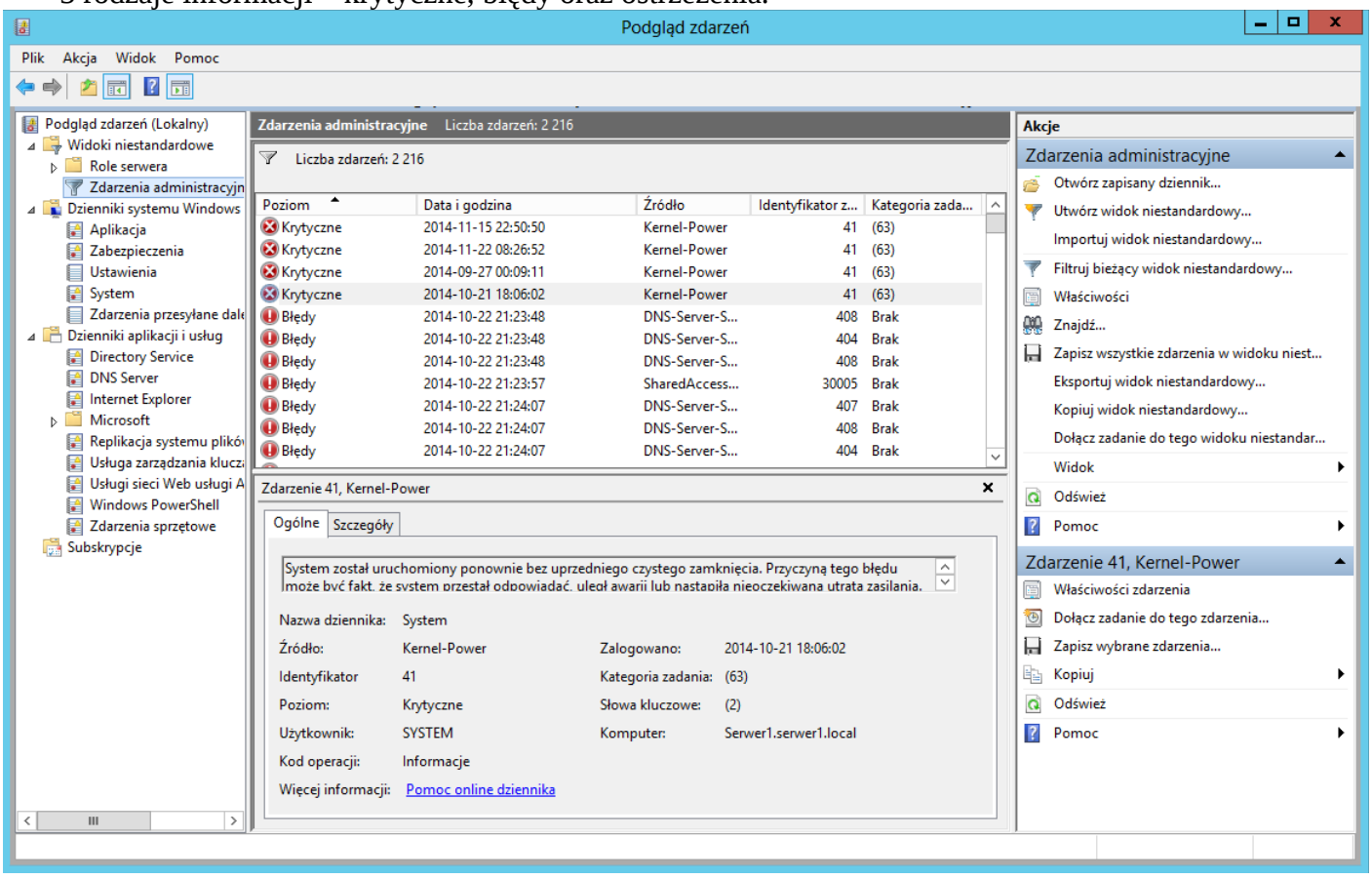
- Dzienniki systemu Windows – w tej gałęzi mamy dostępne standardowe zbiory (dzienniki) ze zdarzeniami systemowymi.
a) Aplikacja – w tym dzienniku zapisywane są wszelkie informacje dotyczące stanu uruchamianych aplikacji systemowych, jak WMI, Menedżera pulpitu, Zabezpieczeń, Podsystemu zdarzeń, Usługi Profilów i innych. Przeważnie są to komunikaty informacyjne (o powodzeniu/niepowodzeniu uruchomienia aplikacji, jej stanie itp.)
b) Zabezpieczenia – tutaj zbierane są informacje z Audytu zabezpieczeń systemu Windows, takich jak logowanie użytkowników do systemu, logowaniach zdalnych, spełnieniu/niespełnieniu warunków zabezpieczeń przez klientów i inne.
c) Ustawienia – tutaj zbierane są głównie informacje dotyczące ustawień systemu Windows. Przykładem takich ustawień mogą być np. aktualizacje poszczególnych usług poprzez Windows Update, informacje czy dany pakiet wymaga ponownego uruchomienia, czy jego aktualizacja się powiodła itp.

d) System – narzędzie umieszcza w tym dzienniku informacje dotyczące działania samego systemu (jądro, sterowniki) oraz usług krytycznych dla systemu (menedżer sterowników, klient DHCP, usługa aktualizacji czasu itp.). Możemy tutaj znaleźć informacje co działo się podczas startu systemu, jaki stan raportuje aktualny system plików (najczęściej NTFS), czy działa usługa wirtualnych dysków twardych itd.
e) Zdarzenia przesyłane dalej – tutaj system serwerowy zbiera informacje/błędy/ostrzeżenia od systemów kooperujących z nim (będące w sieci i np. dołączone do domeny AD). Przykładowo to tutaj trafiają informacje o stanie audytu zabezpieczeń klienta domeny (dopuszczony/odrzucony z dostępu do sieci/intranetu/internetu), o aktualizacjach przesyłanych do klientów (Windows Server Update Services) i inne.

- Dzienniki aplikacji i usług – tutaj znajdują się wszystkie zdarzenia pochodzące od poszczególnych usług i programów działających w systemie Windows. Należy pamiętać, że aplikacja musi współpracować z dziennikiem systemu Windows by wyświetlać komunikaty. Drugim wymogiem jest włączenie przez administratora niektórych zdarzeń (bo np. nikt normalnie nie potrzebuje wychwytywać zdarzeń Wordpada czy informacji o zmianie kolorów systemu Windows). Gałąź ta dostarcza sporej ilości informacji na temat wszystkiego, co dzieje się w systemie. Niektóre zdarzenia włączane są do domyślnego, niestandardowego widoku Zdarzenia administracyjne.

- Subskrypcje – specjalna zakładka pozwalająca na zarządzanie zdarzeniami, które mają być przesyłane danej (do innych komputerów). Szczególnie przydatne w przypadku, gdy administrujemy rozległą siecią i potrzebujemy widzieć poszczególne błędy z różnych komputerów w jednym czasie np. na serwerze. Innym zastosowaniem tej funkcji jest przypadek gdy posiadamy kilka/kilkanaście serwerów Windows, a chcemy, logując się na jeden z nich, posiadać informacje o interesujących nas błędach w jednym miejscu.

Przyjrzyjmy się niestandardowemu widokowi Zdarzenia administracyjne. W nim spotkamy 3 rodzaje informacji – krytyczne, błędy oraz ostrzeżenia.



Na powyższym zrzucie widzimy dwa rodzaje błędów – Krytyczne (czerwone z krzyżykiem) oraz po prostu Błędy (czerwone z wykrzyknikiem). Krytyczne błędy na 99,9% notowane są przed zawieszeniem się systemu/restartem/wyłączeniem się komputera. Dotyczą przede wszystkim jądra systemu i jeżeli często się powtarzają świadczyć to może o poważniejszym uszkodzeniu systemu/podzespołów komputera. Prezentowany wyżej błąd krytyczny jest akurat w tym wypadku „niegroźny" - po prostu system został wyłączony sprzętowo. W tym wypadku administrator może ignorować ten błąd (wyłączenie przez przycisk na obudowie), jednak jeżeli niespodziewanie system kilkukrotnie monituje o takim zdarzeniu, a nie my odłączyliśmy go od prądu to świadczyć to może o uszkodzonym zasilaczu/płycie głównej.

Dwa kolejne błędy na zrzucie to odpowiednio błąd usługi serwera DNS oraz dostępu do sieci współdzielonej. Pierwszy z nich wskazuje, że serwer DNS nie mógł odnaleźć żadnych nadrzędnych serwerów DNS na wskazanym interfejsie sieciowym (w tym wypadku słusznie – dotyczy interfejsu wewnętrznego), drugi z nich natomiast mówi, iż dwa interfejsy sieciowe znajdują się w obrębie tej samej sieci współdzielonej (NAT). System Windows zablokował widoczność systemu na jednym z interfejsów by komputery błędnie nie odwoływały się do niego naprzemiennie (gubienie pakietów). Błędy tego typu nie powodują przeważnie unieruchomienia serwera, mogą jednak wiele mówić administratorowi dlaczego niektóre usługi są niedostępne/działają nieprawidłowo. Niektóre z tych błędów mają status „bezpiecznego ignorowania" - pojawiają się, jednak można się nimi nie przejmować. Niektórzy, zresztą słusznie, że jeżeli błędy nie są ważne powinny mieć zamieniony status na Ostrzeżenie (żółte tło z wykrzyknikiem).

System rozróżnia jeszcze zdarzenia inspekcji bezpieczeństwa (ikona klucza), które można znaleźć w dzienniku Zabezpieczenia i dotyczą przede wszystkim nadawania/odmawiania uprawnień do korzystania z serwera/poszczególnych usług dla poszczególnych użytkowników.

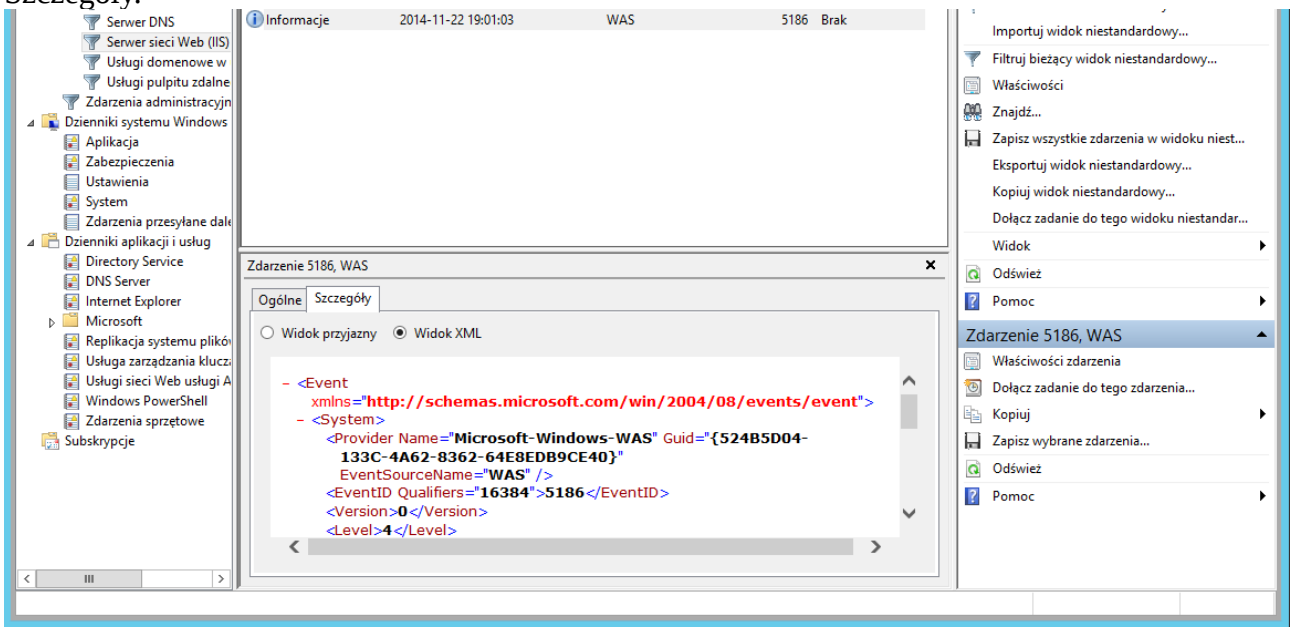
Ostatnim rodzajem zdarzeń jest informacja (ikona szarego koła z niebieską literą i). Informuje ono o pewnych zdarzeniach w systemie, które mogą, lecz nie muszą mieć jakiegokolwiek znaczenia dla administratora systemu. Informacje te mogą jedynie naprowadzać do rozwiązania problemu, który klasyfikowany jest jako błąd (często błędy wywoływane są przez pewne, określone zachowania aplikacji bądź użytkowników systemu, które są zgłaszane właśnie jako informacje). Z informacji można się przykładowo dowiedzieć, że dany użytkownik o wskazanej godzinie zawiesił swoją sesję bądź został wylogowany przez innego użytkownika/usługę systemu. Informacjami są także zdarzenia z Windows Update czy instalacji kolejnych pakietów dodatkowych do systemu Windows.

Dochodzenie do przyczyn konkretnych błędów.

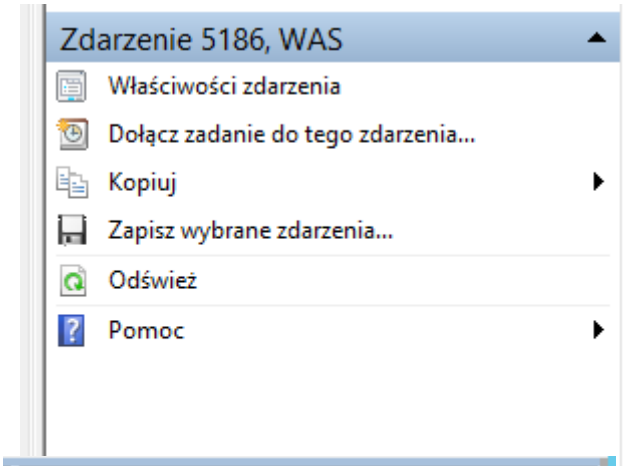
W przypadku, gdy dany błąd jest niepożądany/uciążliwy bądź destabilizujący nasz system, musimy poszukać rozwiązania dla niego – może to być pewne ustawienie w systemie, aplikacja/szereg aplikacji powodująca jego wystąpienie bądź po prostu błąd ze strony firmy Microsoft (który albo trzeba zgłosić, albo istnieje na niego odpowiednia aktualizacja).

Ponieważ lista „co to może być" jest długa, dlatego najlepszym sposobem jest wyszukać tematów pomocy poprzez wyszukiwarkę internetową (nomen omen lepiej radzi sobie np. Google niż Bing od Microsoft...). Aby dowiedzieć się np. czegoś więcej o błędzie krytycznym z poprzedniego zrzutu wystarczy w wyszukiwarce wpisać/wkleić zawartość Źródła błędu (Kernel-Power) oraz jego identyfikator (Event ID, w tym wypadku 41). W zasadzie tyle wystarczy by odnaleźć informacje, przyczyny oraz ewentualne kroki zaradcze by błąd się więcej nie pojawił. Oczywiście rozwiązań może być kilka/kilkanaście (jak to w systemie Windows) dlatego należy wybrać najbardziej prawdopodobny scenariusz pojawiania się błędu, zastosowaniu się do jego rozwiązania i obserwowaniu systemu. Jeżeli rozwiązanie nic nie zmieni – trzeba szukać dalej aż do skutku. Czasami może też się zdarzyć, że błąd oczekuje na rozwiązanie – wtedy pozostaje jedynie czekać (i czasami się nie doczekać, jak np. w wersjach SBS z panelem administracyjnym zgłaszającym błąd do jądra systemu). Niekiedy na stronach firmy Microsoft znajdziemy rozwiązanie jak dany błąd wyłączyć z raportowania (jeżeli faktycznie nie jest ważny).

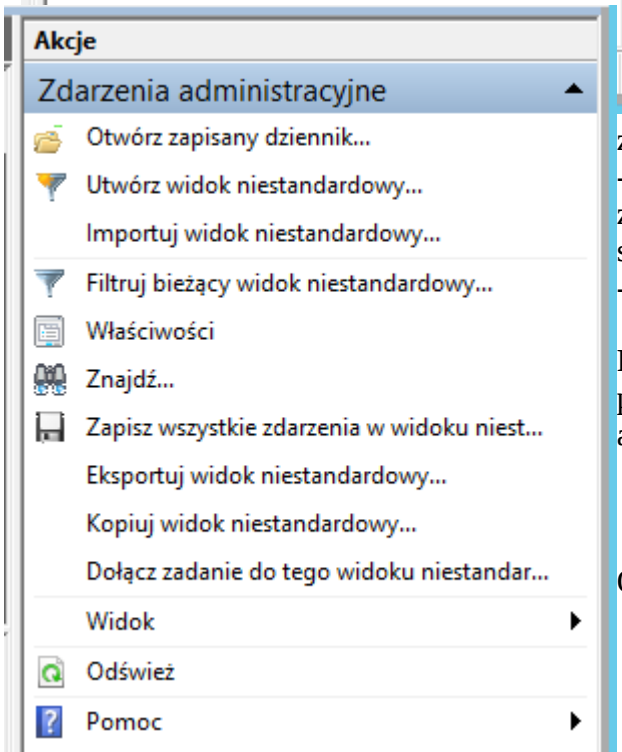
W niektórych wypadkach, szczególnie gdy będziemy błąd raportować do firmy Microsoft, należy podać więcej szczegółów wystąpienia błędów. Wtedy należy skorzystać z zakładki Szczegóły.



W tym wypadku zawsze, ale to zawsze powinien interesować nas Widok XML (przyjazny jest... mało czytelny i niespecjalnie nadaje się do przenoszenia).
Do kopiowania można zaznaczyć tekst/fragment i po prostu kliknąć skrót klawiaturowy [CTRL]+[C], można też posłużyć się specjalną opcją dostępną po prawej stronie okna:



- Właściwości zdarzenia – pozwalają na wyświetlenie opisu zdarzenia w osobnym oknie
- Dołącz zadanie do tego zdarzenia... - pozwala na wykonanie dodatkowej, automatycznej akcji przez system w przypadku, gdy to zdarzenie będzie miało miejsce. Przykładowo możemy kazać zamknąć jakąś aplikację, zrestartować system, uruchomić napisany skrypt/uruchomić aplikację itp.
- Kopiuj – tutaj mamy możliwość skopiowania informacji o zdarzeniu (gdy nie lubimy skrótów klawiaturowych)
- Zapisz wybrane zdarzenie... - zapisuje to zdarzenie (w przypadku wybrania widoku/dziennika zapisuje wszystkie zdarzenia w nich zebrane) w pliku evtx (rozszerzenie dziennika zdarzeń w systemie Windows).
- Odśwież – pozwala na odświeżenie zawartości zdarzenia/dziennika zdarzeń/widoku (samoczynnie się nie odświeża)
- Pomoc – wyświetla pomoc systemową



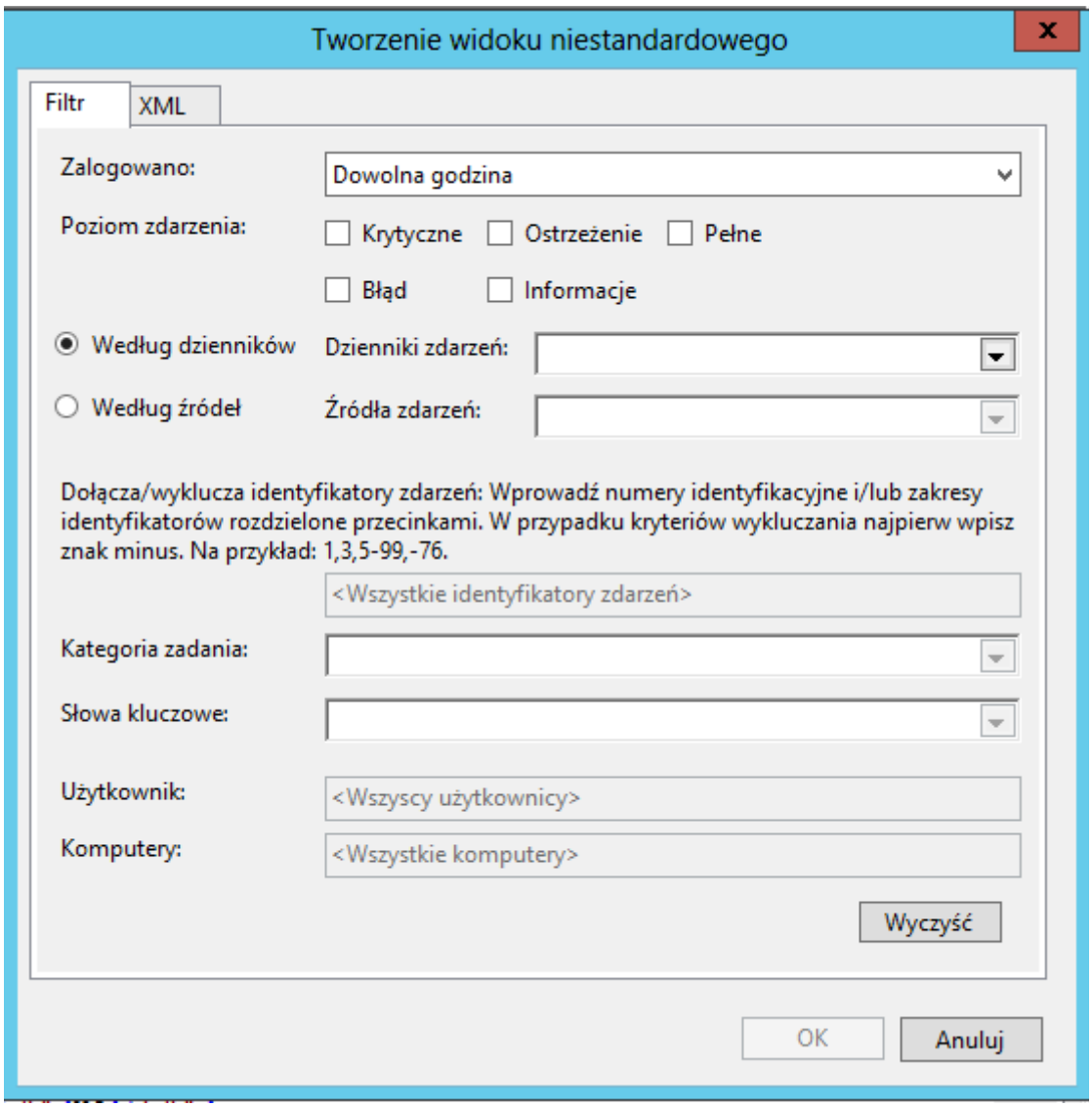
Pozostałe opcje dziennika zdarzeń (tutaj w przypadku wybrania widoku Zdarzenia administracyjne):

Otwórz zapisany dziennik... - otwiera wcześniej

zapisany dziennik zdarzeń (plik evtx). Można otworzyć dziennik przeniesiony z innego komputera
- Utwórz widok niestandardowy... - pozwala na utworzenie własnego widoku, który będzie zawierał interesujące nas zdarzenia (mogą być wybrane z dowolnego dziennika/innego widoku).
- Importuj widok niestandardowy... - dodaje do dziennika utworzony wcześniej widok (może być z innego systemu). Trzeba jednak pamiętać, by widok był zapisany w postaci XML (można np. skopiować jego kod XML z zakładki)
- Filtruj bieżący widok niestandardowy... - pozwala na zmianę ustawień filtrowania w wybranym widoku. Można dokonywać zarówno zmian w widoku kreatora jak i bezpośrednio w kodzie XML
- Właściwości – pozwala na zmianę i opis widoku/dziennika; ponadto pozwala na zmianę filtracja (opis wyżej)
- Znajdź... - wyszukiwarka konkretnego zdarzenia (po nazwie, ID, fragmencie ciągu itd.)
- Zapisz wszystkie zdarzenia w widoku niestandardowy(dzienniku)... - zapisuje wszystkie zdarzenia aktualnie wyświetlanie na liście zdarzeń (dostępne w widoku/dzienniku).
- Eksportuj widok niestandardowy... - eksportuje do pliku XML aktualny widok niestandardowy
- Kopiuj widok niestandardowy... - kopiuje aktualnie wybrany widok niestandardowy jako nowy widok niestandardowy (np. by zachować jego pewne cechy, a pewne poddać modyfikacjom)
- Dołącz zadanie do tego widoku niestandardowego(dzinnika)... - pozwala na utworzenie zdania, które będzie powiązane z danym widokiem/dziennikiem (np. wywołanie określonej czynności w systemie gdy pojawi się nowe zdarzenie)
- Widok – tutaj możemy wybierać co ma być pokazywane w oknie (domyślnie jest tylko podgląd) oraz w jaki sposób mają być domyślnie sortowane listy, grupy itd.
- Odśwież – odświeża aktualnie wybrany widok/dziennika
- Pomoc – pomoc systemowa

Tworzenie niestandardowego widoku.

Czasami zachodzi potrzeba przeglądania tylko wybranych, najważniejszych dla nas zdarzeń z różnych dzienników/aplikacji. Gdybyśmy musieli robić to ręcznie to znalezienie/analizowanie takich zdarzeń byłoby uciążliwe. Jednak możemy utworzyć specjalny widok, w którym będziemy obserwować tylko istotne dla nas informacje.
Okno tworzenia widoku niestandardowego przezentuje się następująco:



- Zalogowano – możemy wybrać przedział czasu, z jakiego interesują nas zdarzenia (domyślnie jest to dowolna godzina, można jednak zawęzić czas do godziny, dnia, tygodnia czy utworzyć nowy, własny przedział)
- Poziom zdarzenia – które zdarzenia mają być wyświetlane w widoku (Pełne oznacza, że wszystkie zdarzenia będą dodawane)
- Według dzienników – możemy wybrać z których dzienników będziemy pobierać zdarzenia (można wybrać kilka lub wszystkie)
- Według źródeł – pozwala na wybranie źródła jako konkretnej usługi, aplikacji bądź systemowego składnika, dla którego zdarzenie zostało zarejestrowane

Dołącza/wyklucza identyfikatory zdarzeń – w tym polu można podać konkretne numery ID zdarzeń, które będą dodawane do widoku (znacznie polepsza czytelność w przypadku poszukiwania konkretnych zdarzeń)

- Kategoria zadania – pozwala na wybranie zdarzeń generowanych tylko przy wykonywaniu określonych zadań (np. przy pobieraniu pliku, otwieraniu strony itp.)
- Słowa kluczowe – pozwala wybrać tylko te zdarzenia, które posiadają konkretne słowa kluczowe (można je wybrać z konkretnej listy przypisanej do dziennika/widoku)
- Użytkownik – można wybrać użytkownika, który dla którego zdarzenie występuje (lub przez którego występuje)
- Komputery – można wybrać, dla których komputerów zdarzenie ma być rejestrowane (bądź przez które zostało wywołane).

Zadania do wykonania:

1. Należy utworzyć nowy widok, w którym będą wyświetlane zdarzenia z zapory sieciowej Windows oraz z Shell-Core.
2. Utworzyć widok, w którym będą widziane tylko zdarzenia dla jądra systemu Windows. Proszę zawęzić zakres do zdarzeń 42 oraz 410
3. Należy włączyć rejestrowanie zdarzeń dla aplikacji Wordpad.
4. Proszę z widoku administracyjnego wybrać wszystkie rodzaje zdarzeń. Następnie należy odnaleźć informacje o tych zdarzeniach (groźne/niegroźne dla systemu, jakie są ewentualnie możliwości wyeliminowania ich pojawiania się w przyszłości).

Dodatkowe
5. Proszę spróbować dodać zadanie do zdarzenia, kiedy to system zostanie wyłączony fizycznie (ID 42 Kernel-power). Zadanie to ma wysyłać pocztę na wskazany adres e-mail z wiadomością o wystąpieniu błędu. Podpowiedź: http://blogs.iis.net/rickbarber/archive/2012/10/26/send-an-email-when-an-event-is-logged.aspx