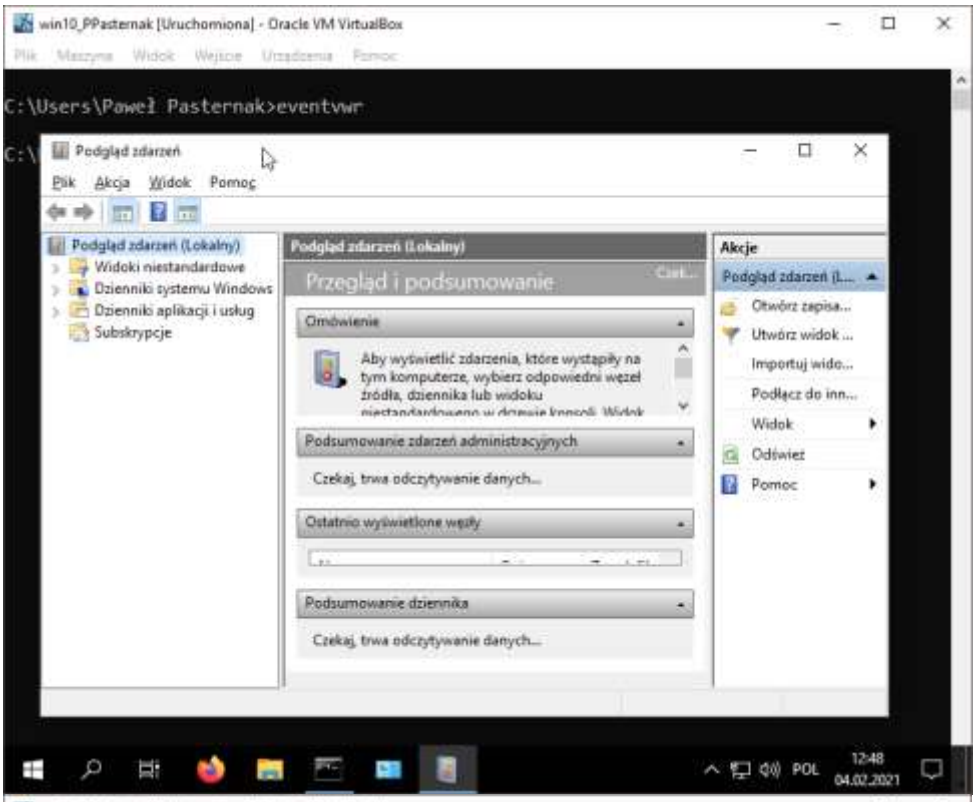
Dziennik Zdarzeń

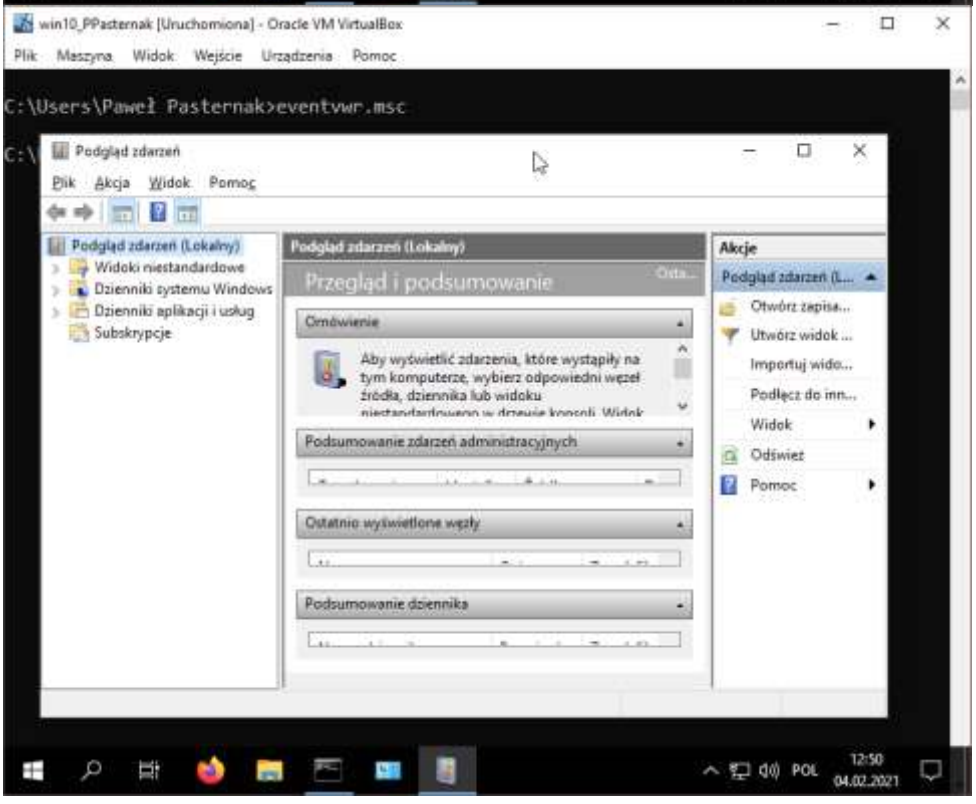
Spis treści

1. Zadanie

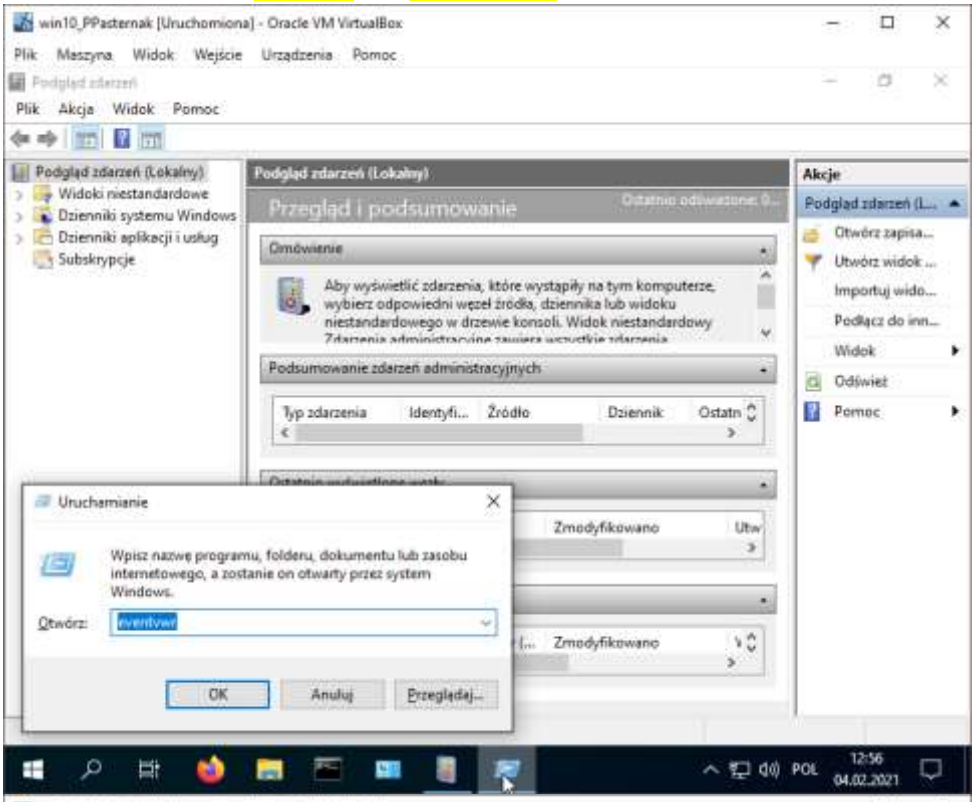
- Jakim poleceniem można otworzyć dziennik zdarzeń za pomocą CMD

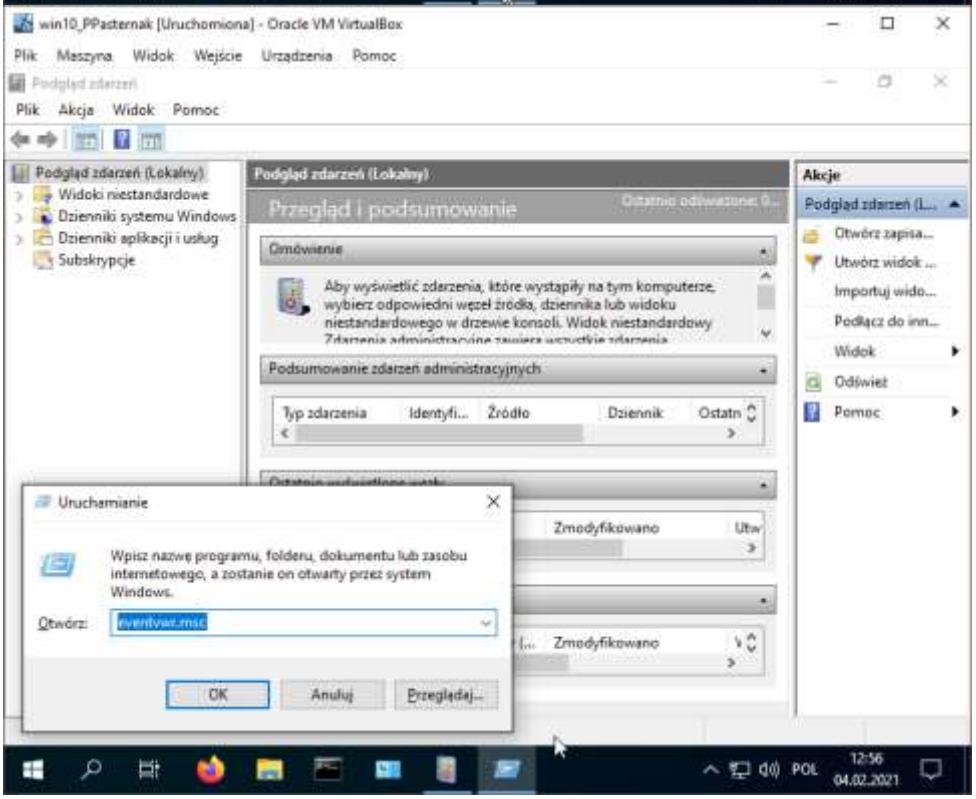
Polecenie: ***eventvwr*** albo ***eventvwr.msc***



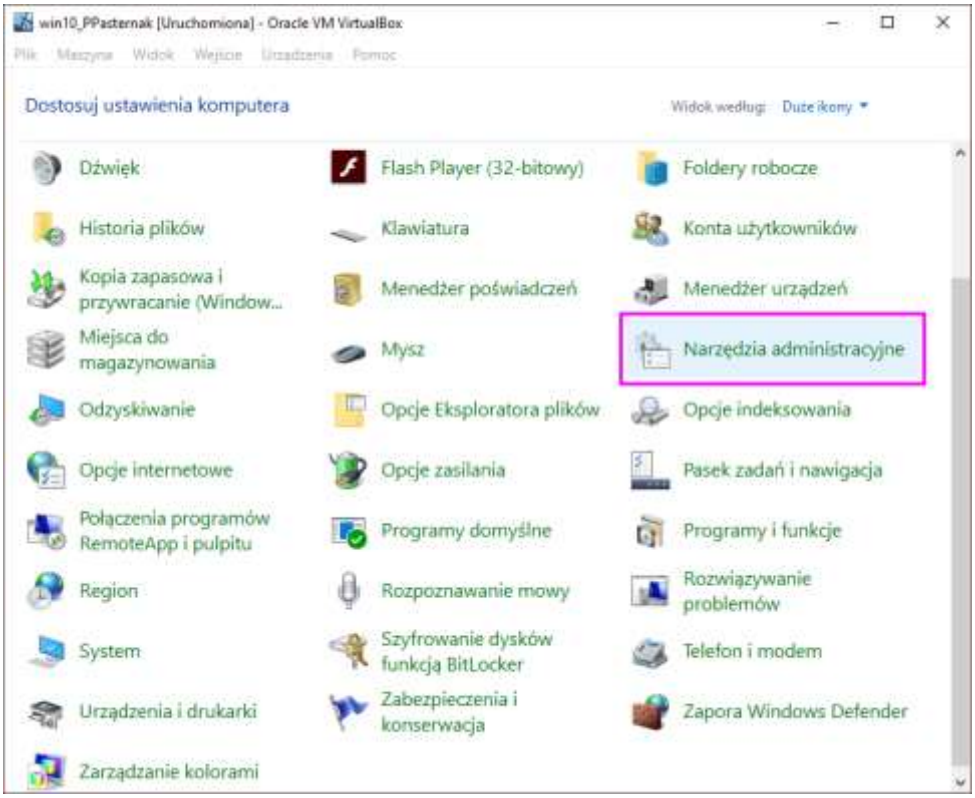


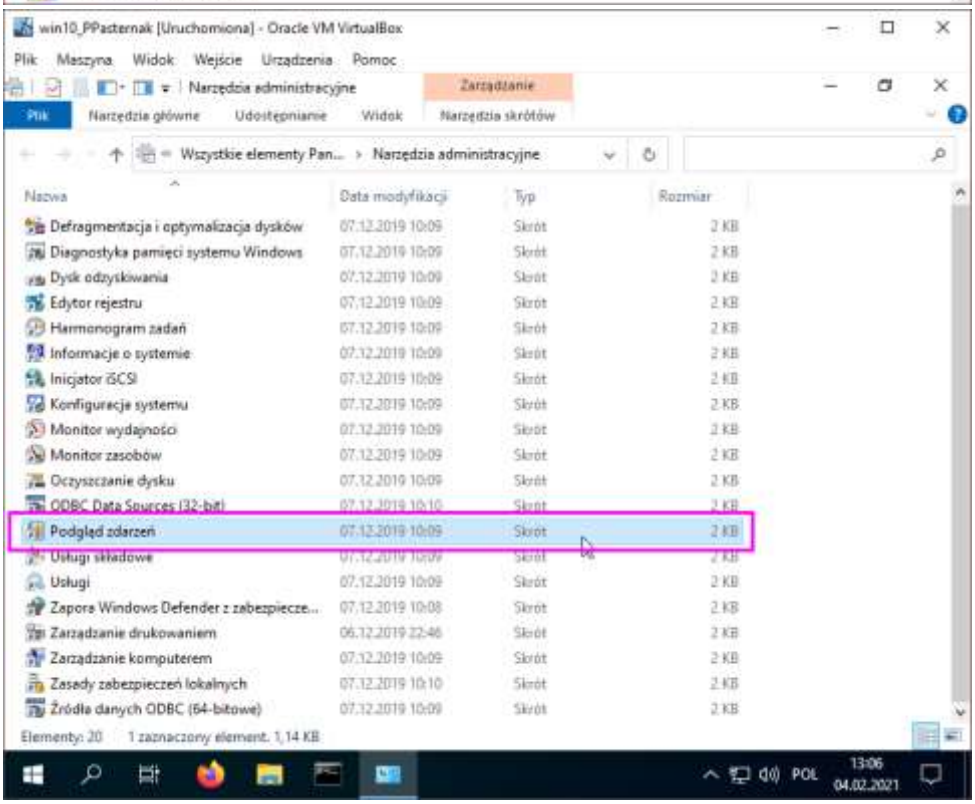
- Jak jeszcze można otworzyć dziennik zdarzeń
  - Za pomocą aplikacji „Uruchamianie”, którą możemy otworzyć skrótem ***win+r***, a następnie użyciu komendy: ***eventvwr*** albo ***eventvwr.msc***



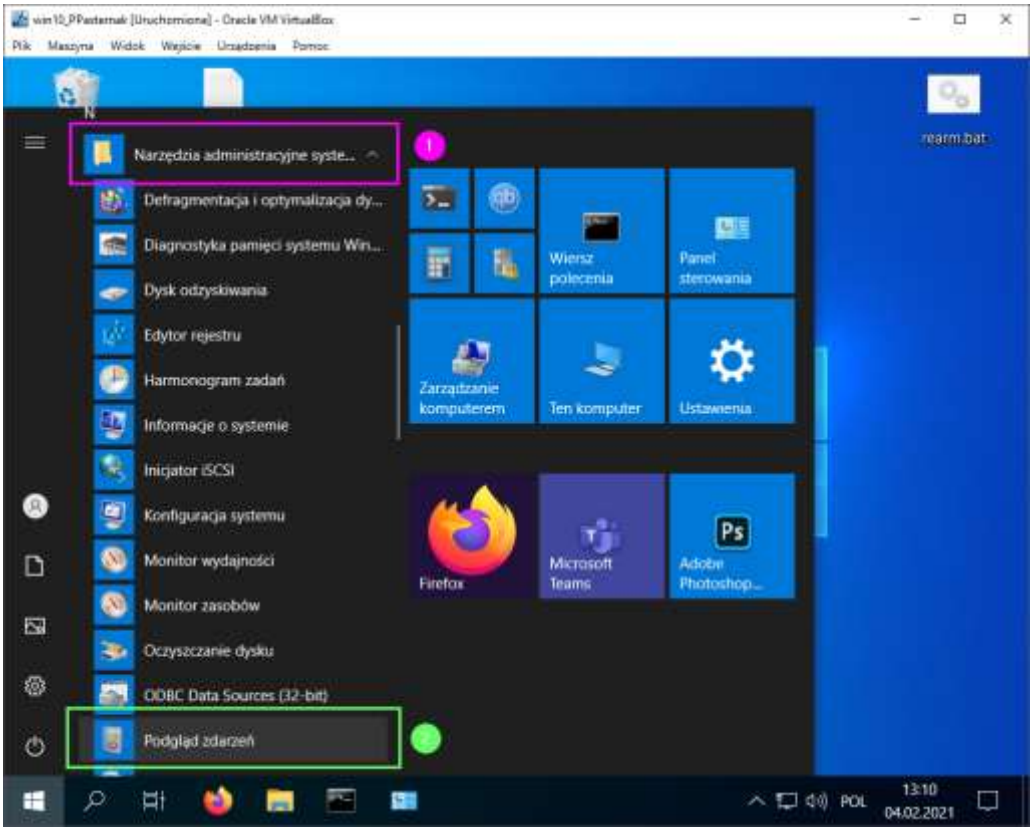


- Z panelu sterowania -> Narzędzia administracyjne -> Podgląd Zdarzeń

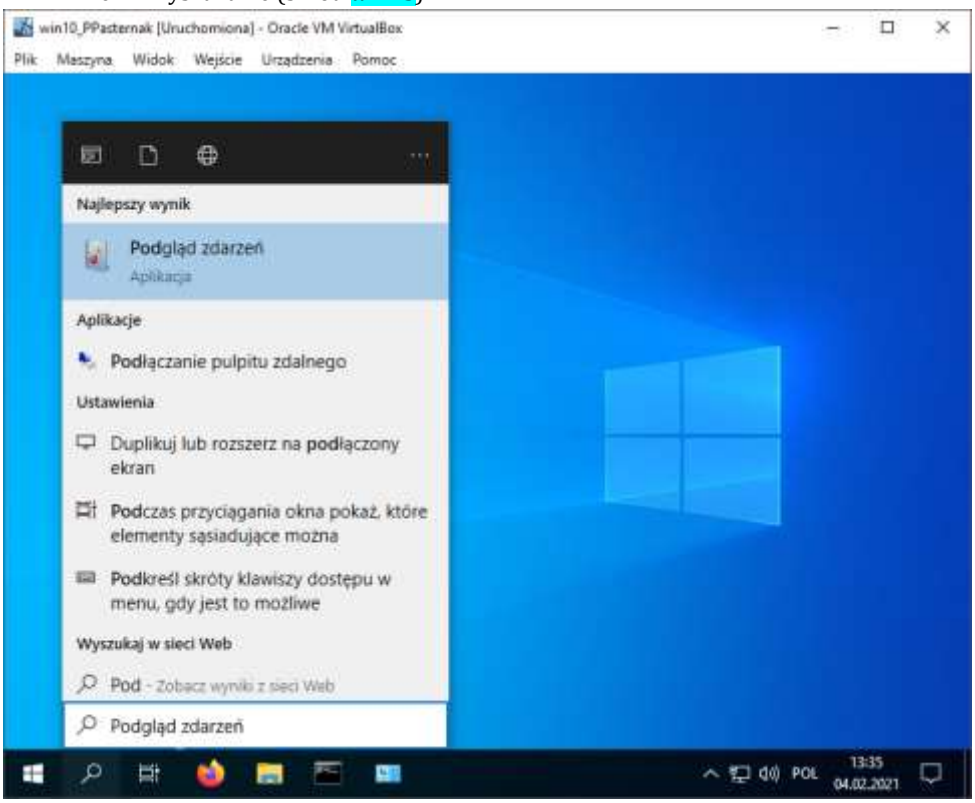




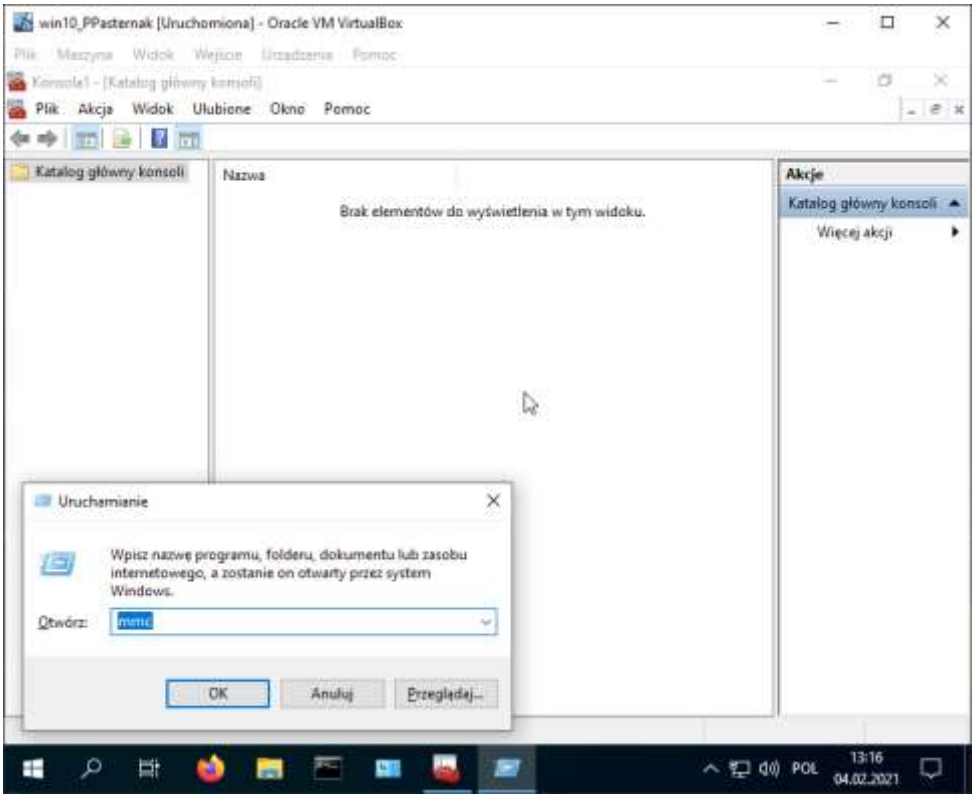
- Z menu start -> Narzędzia administracyjne systemu Windows -> Podgląd Zdarzeń

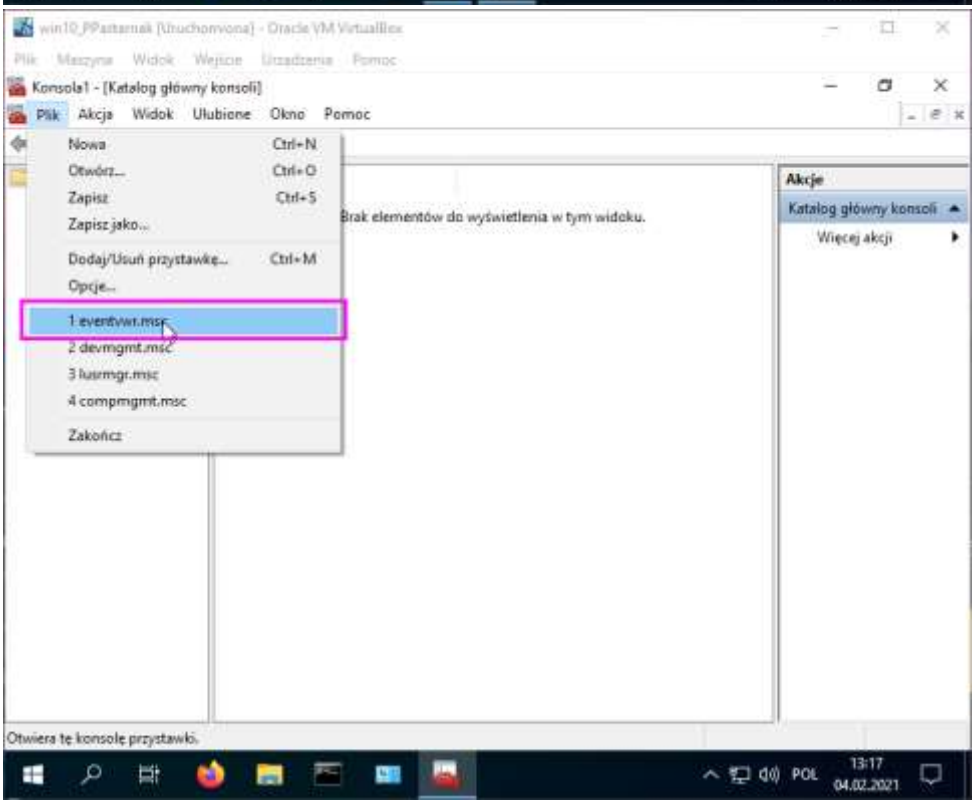


- Wyszukanie (skrót: ***win+s***)

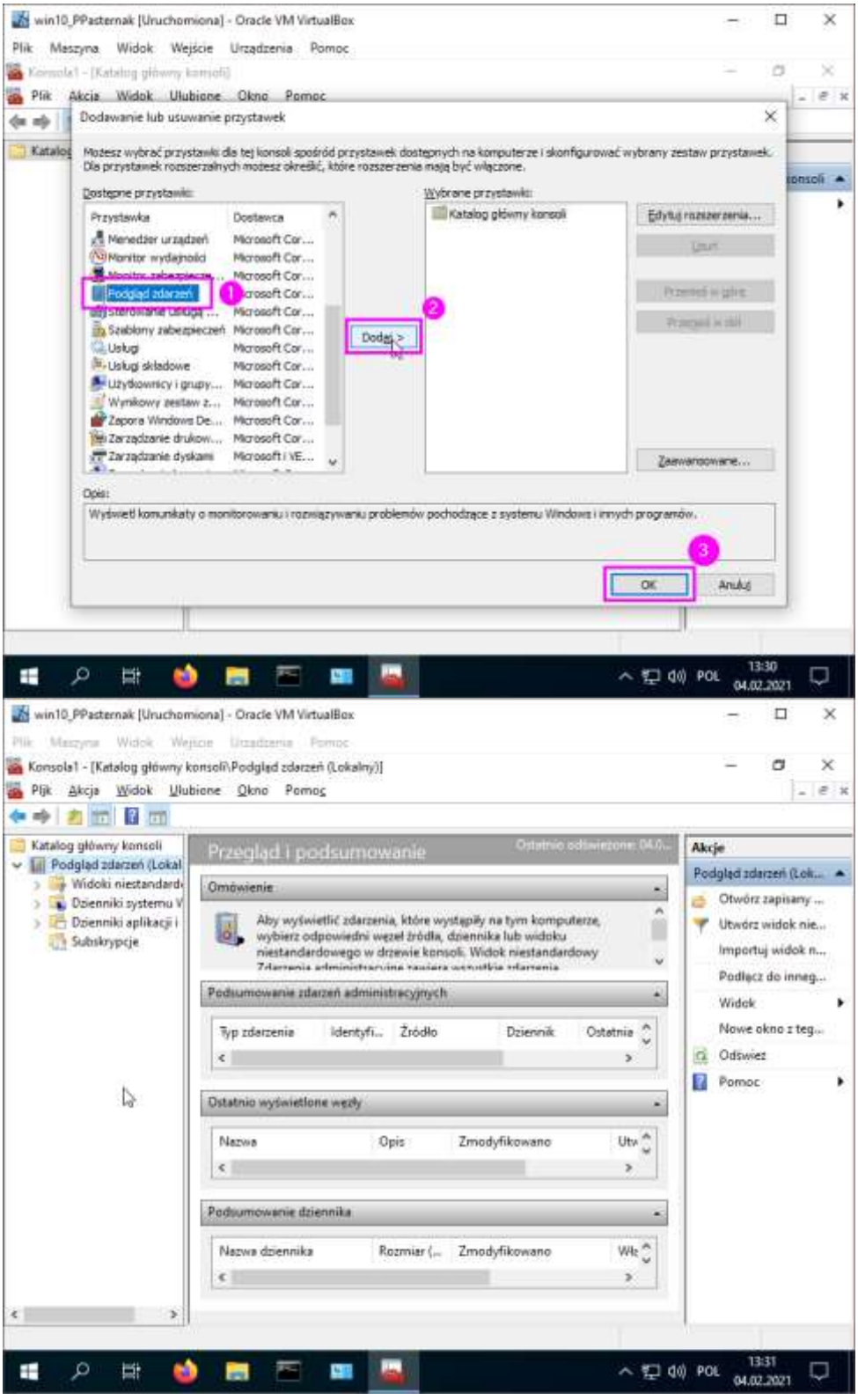


- Poprzez konsole MMC -> Plik -> 1 eventvwr.msc





- Poprzez konsole MMC -> Plik -> Dodaj/Usuń przystawkę…



- Jakie jest przeznaczenie „Subskrypcji zdarzeń”

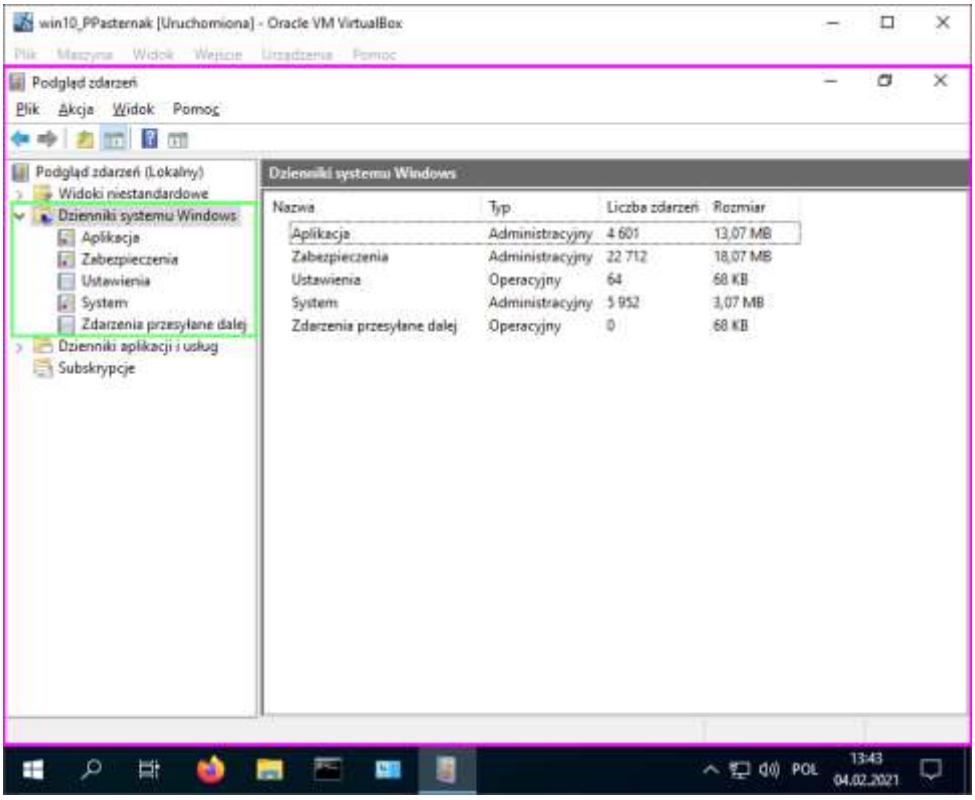
Podgląd zdarzeń umożliwia wyświetlanie zdarzeń na pojedynczym komputerze zdalnym. Jednak rozwiązywanie problemów może wymagać przeanalizowania zestawu zdarzeń zapisanych w wielu dziennikach na wielu komputerach.

System Windows umożliwia zbieranie kopii zdarzeń z wielu komputerów zdalnych i przechowywanie ich lokalnie. Aby określić, które zdarzenia mają być zbierane, należy utworzyć subskrypcję zdarzeń. Oprócz innych szczegółów subskrypcja określa dokładnie, które zdarzenia będą zbierane i w którym dzienniku będą lokalnie przechowywane. Po uaktywnieniu subskrypcji i rozpoczęciu zbierania zdarzeń można wyświetlać te zdarzenia i manipulować nimi tak, jakby były to dowolne inne lokalnie przechowywane zdarzenia.

Funkcja zbierania zdarzeń wymaga skonfigurowania zarówno komputera przekazującego, jak i zbierającego. Funkcjonalność ta zależy od usług Zdalne zarządzanie systemem Windows (WinRM) i Kolektor zdarzeń systemu Windows (Wecsvc). Obie te usługi muszą być uruchomione na komputerach uczestniczących w procesie przekazywania i zbierania.

Źródło: https://forsenergy.com/pl-pl/eventviewer/html/4aa6403f-d4b8-43a4-a70d-ceb7f88c524e.htm

- Jakie są działy „Dziennika Systemu Windows”



- Aplikacja

Dziennik aplikacji rejestruje zdarzenia związane z programami zainstalowanymi w systemie.

- Zabezpieczenia

Gdy rejestrowanie zabezpieczeń jest włączone (jest domyślnie wyłączone w systemie Windows), ten dziennik rejestruje zdarzenia związane z bezpieczeństwem, takie jak próby logowania i dostęp do zasobów.

- System

Dziennik systemu rejestruje zdarzenia związane ze składnikami systemu Windows, takimi jak sterowniki i wbudowane elementy interfejsu.

- Ustawienia

Wiadomości generowane podczas instalowania i uaktualniania systemu operacyjnego Windows. Jeśli system Windows jest kontrolerem domeny, te komunikaty również są tutaj rejestrowane.

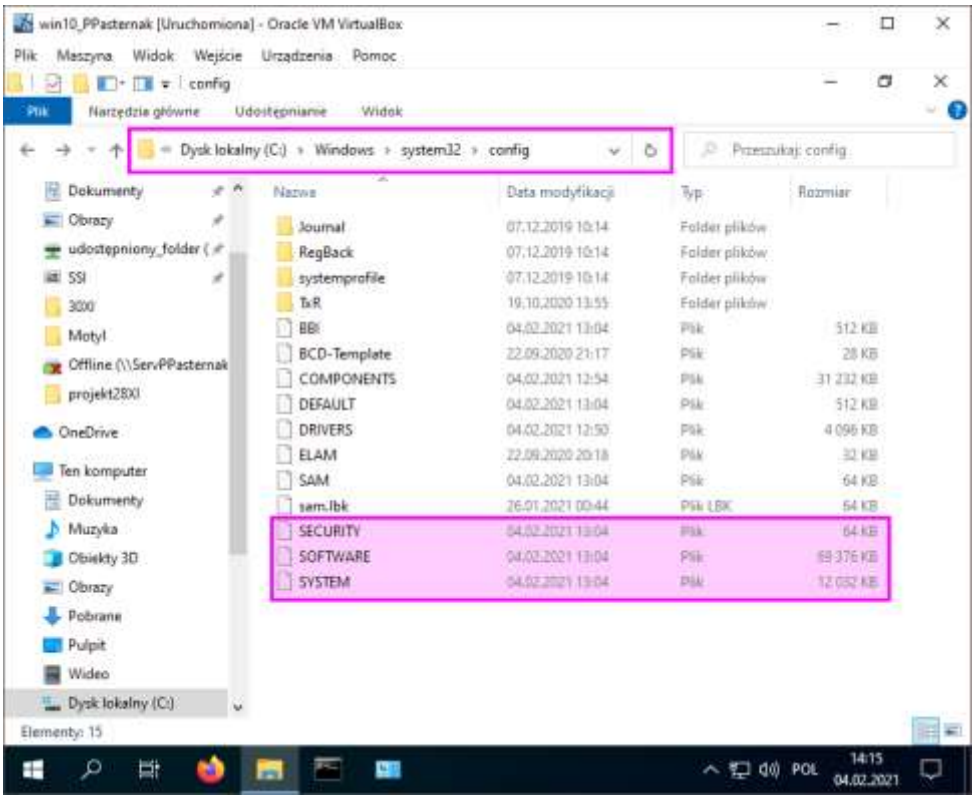
- Przesłane dalej

Zdarzenia przekazywane przez inne komputery, gdy komputer lokalny działa jako centralny subskrybent.

Źródła:
https://www.howtogeek.com/123646/htg-explains-what-the-windows-event-viewer-is-and-how-you-can-use-it/
https://www.loggly.com/ultimate-guide/windows-logging-basics/
http://math.uni.lodz.pl/~robpleb/pzwdz.pdf

- Jaka jest fizyczna ścieżka wszystkich działów „Dziennika Systemu Windows”

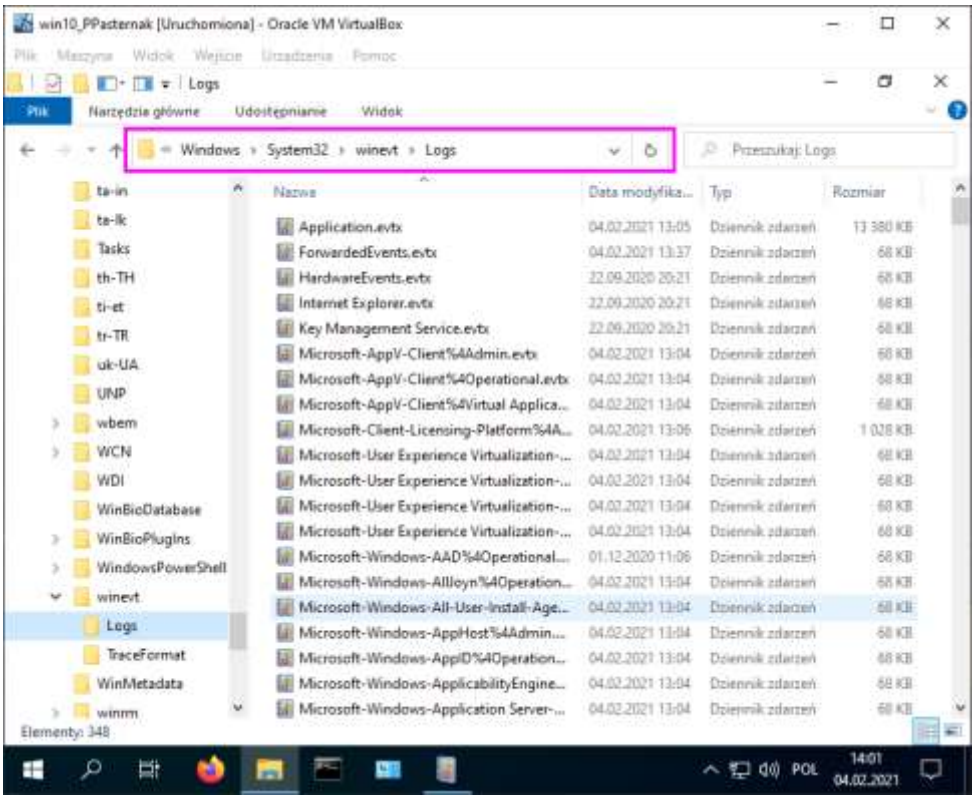
C:\Windows\System32\config albo %SystemRoot%\System32\Config



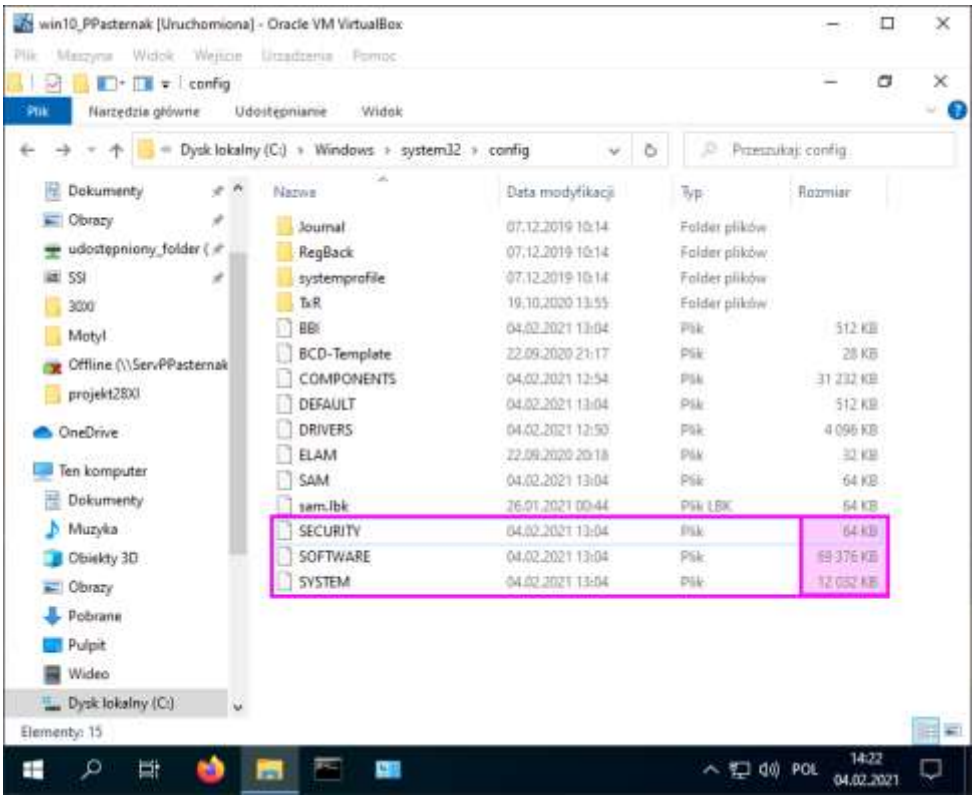
Źródło: https://docs.microsoft.com/en-us/troubleshoot/windows-server/application-management/move-event-viewer-log-files#:~:text=By%20default%2C%20Event%20Viewer%20log,location%20of%20the%20log%20files.

- Lokalizacja logów dziennika

C:\Windows\System32\winevt\Logs albo %SystemRoot%\System32\Winevt\Logs



- Jaka jest domyślna wartość wielkości poszczególnych działów dziennika

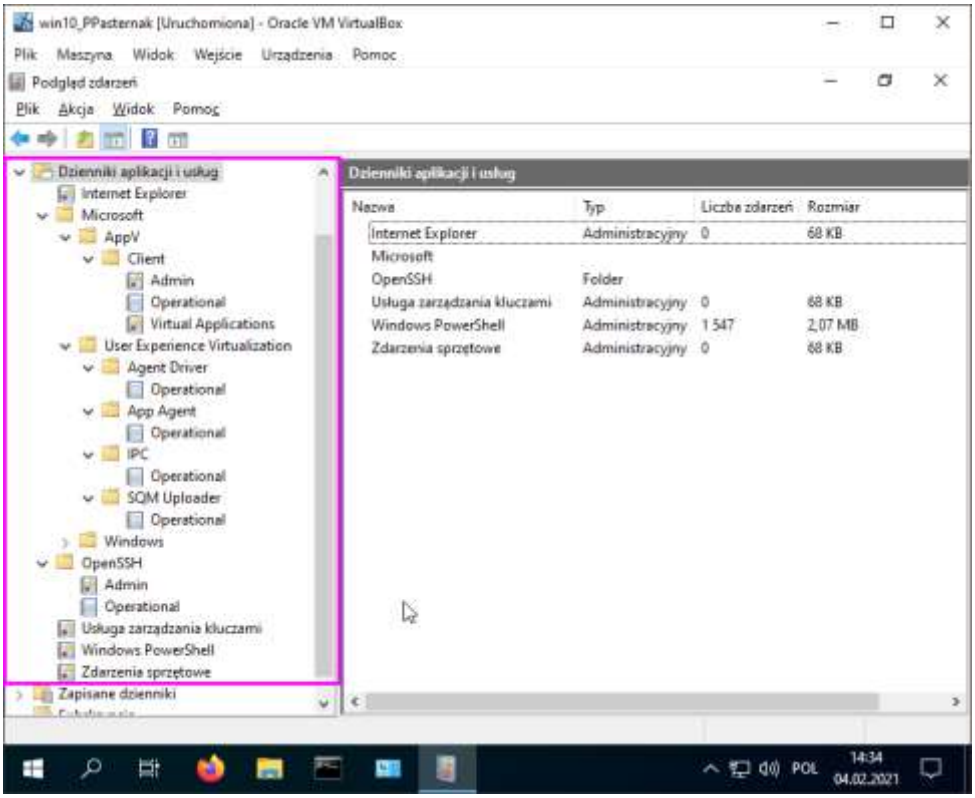


Security = 64kB

Software = 69,376mB

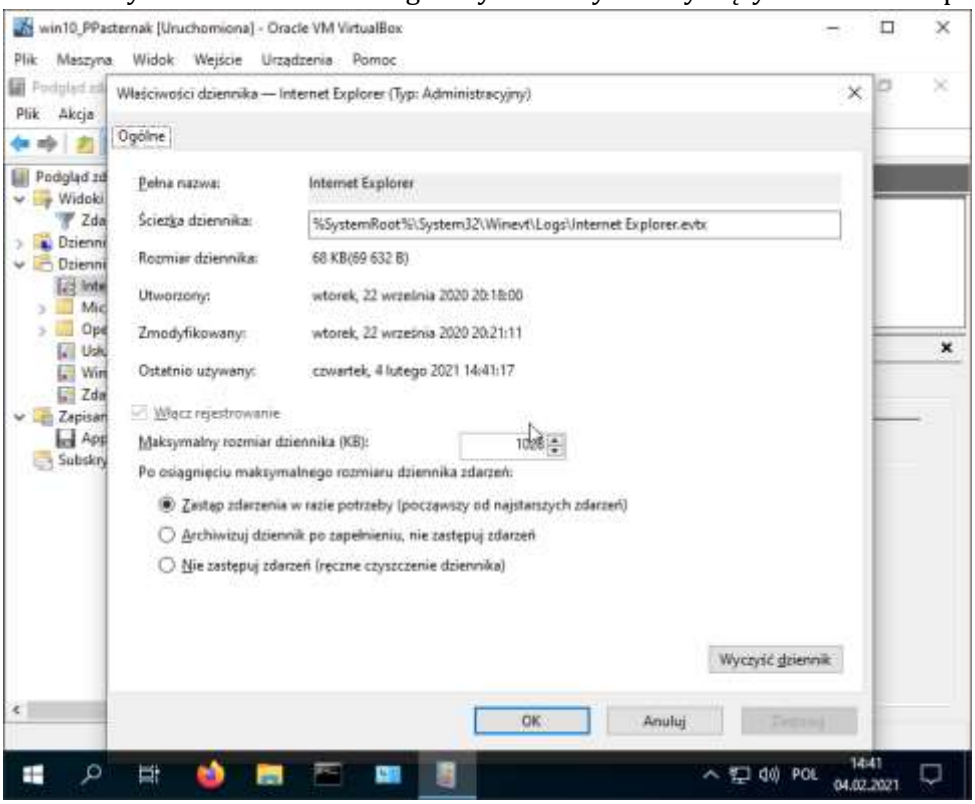
System = 12,032mB

- Jakie inne dzienniki są rejestrowane przez system ? pokaż konkretne przykłady



Dzienniki aplikacji i usług. Np.: Internet Explorer, Usługa zarządzania kluczami, Windows PowerShell, Zdarzenia sprzętowe, OpenSSH, itd.

- Wyświetl właściwości logów systemowych dotyczących Internet Explorera



- Jaka jest klasyfikacja wagi zdarzeń w systemie „Poziom” ?

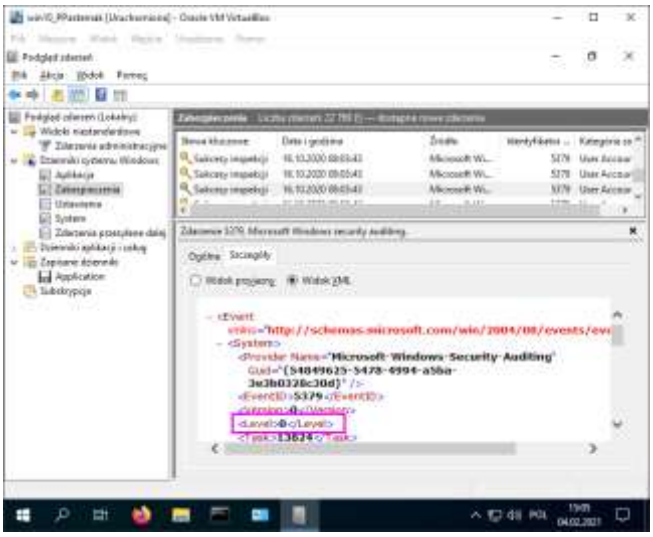
Sukces inspekcji - 0

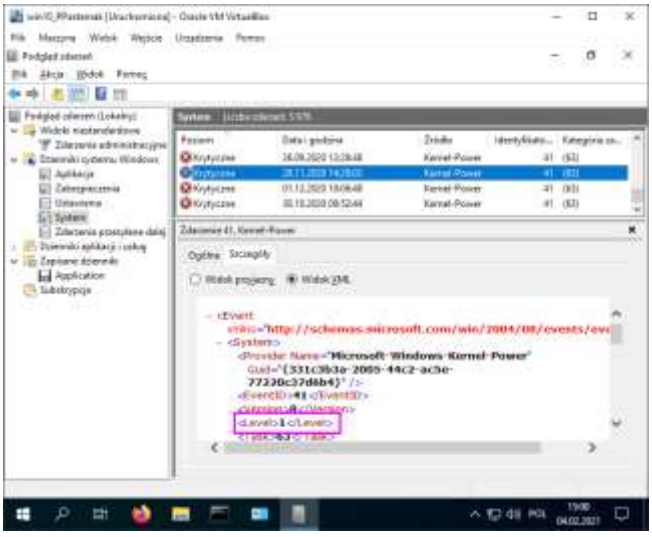
Critical – Krytyczny - 1

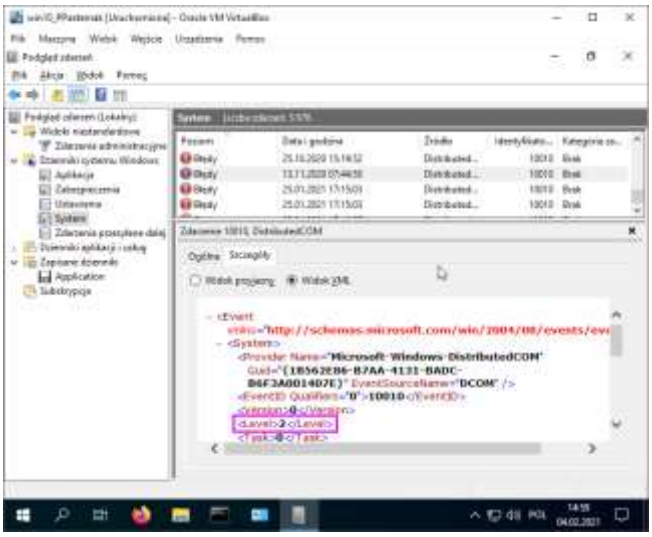
Error – Błąd - 2

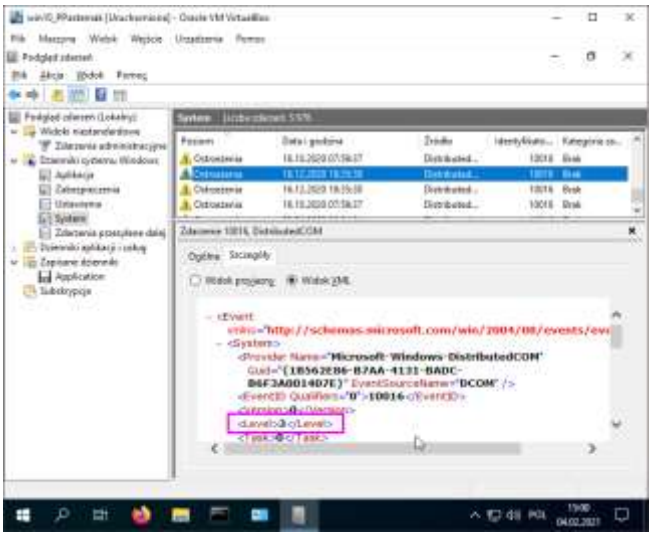
Warming – Ostrzeżenie – 3

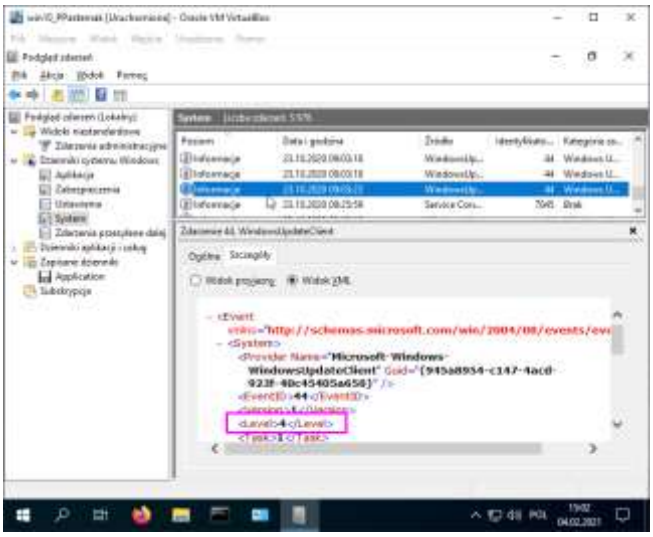
Information – Informacje - 4



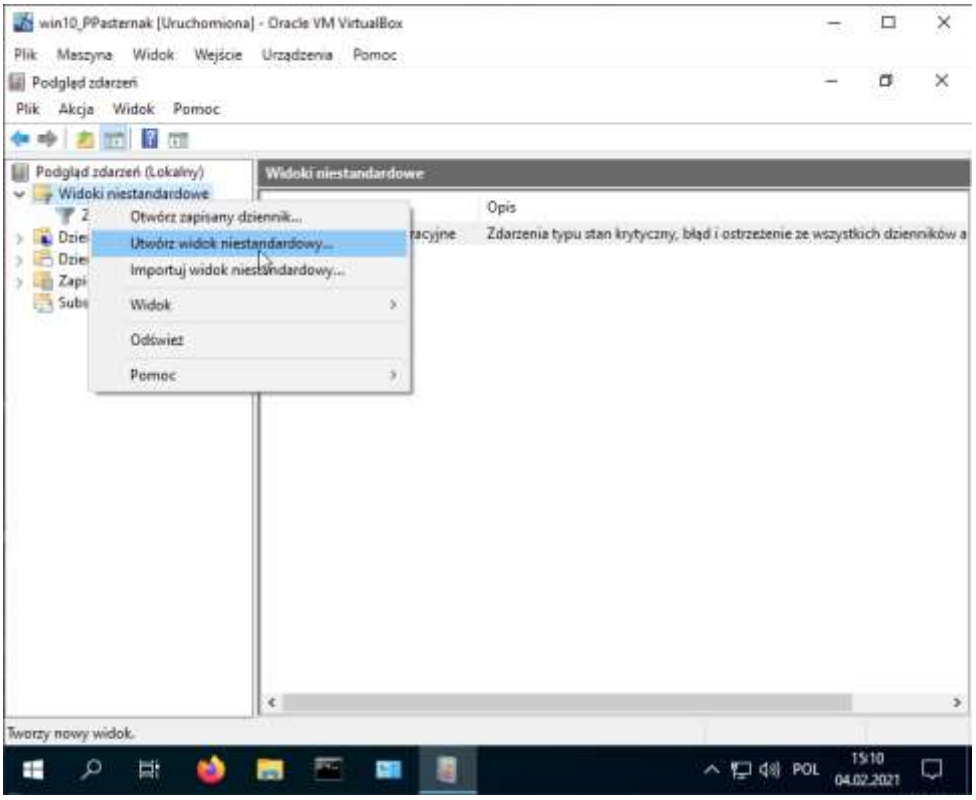




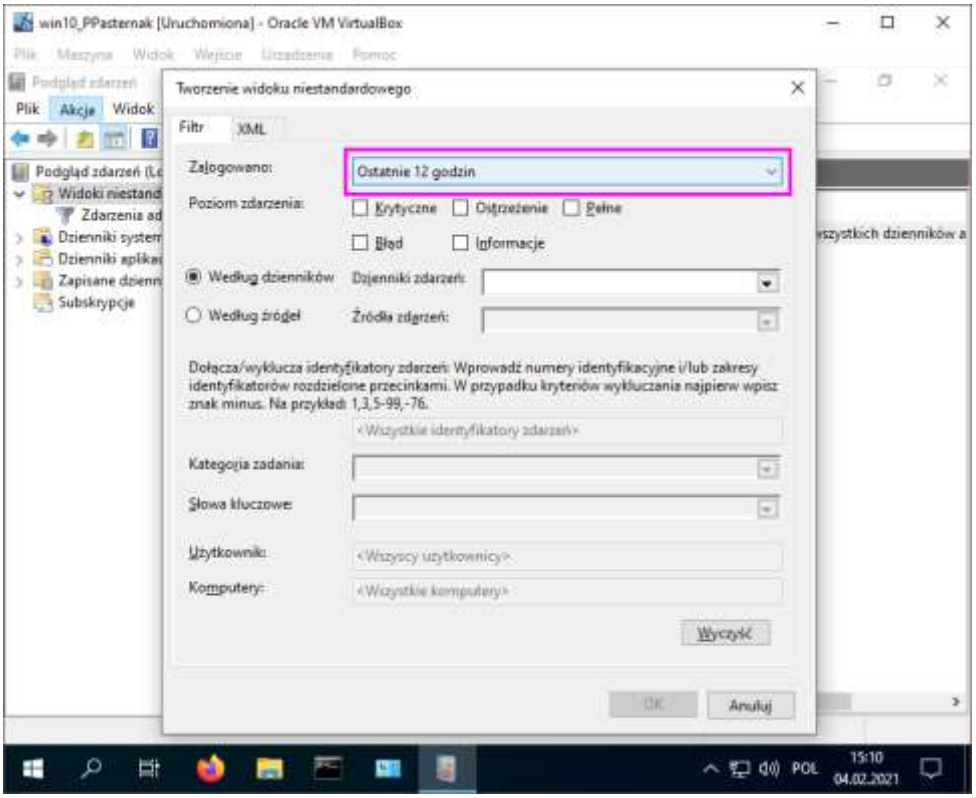



Podgląd zdarzeń
Plik Akcja Widok Pomoc
Podgląd zdarzeń (Lokalny)
Widoki niestandardowe
Dzienniki systemu Windows
Aplikacja
Zabezpieczenia
Instalacja
System
Zdarzenia przesyłane dalej
Dzienniki aplikacji i usług
Zapisane dzienniki
Application
Subskrypcje
System Liczba zdarzeń: 5 570
Poziom
Data i godzina
Źródło
Identyfikator...
Kategoria za...
Informacje
Informacje
Informacje
Informacje
Service Con...
7045
Brak
Zdarzenie 44, WindowsUpdateClient
Ogólne
Szczegóły
Widok przyjazny
Widok XML
- <Event
xmlns="http://schemas.microsoft.com/win/2004/08/events/eve
- <System>
<Provider Name="Microsoft-Windows-
WindowsUpdateClient" Guid="{945a8954-c147-4acd-
923f-40c45405a658}" />
<EventID>44</EventID>
<Level>4</Level>
<Task>3</Task>
POL
19:02
04.02.2021

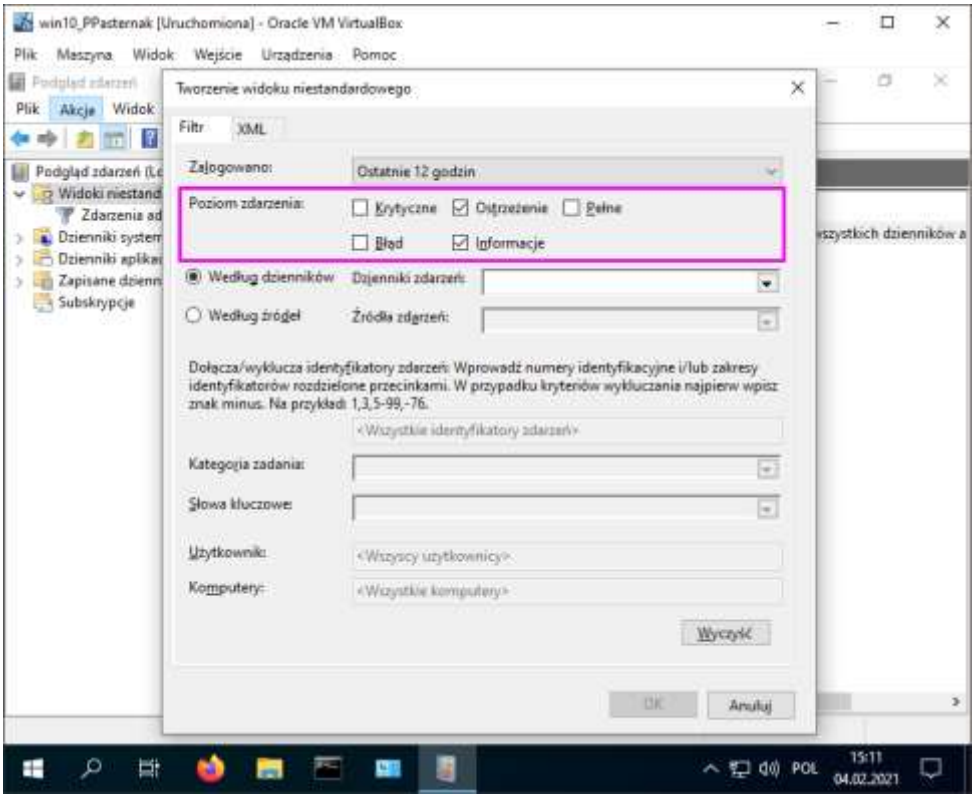
2. Należy utworzyć widok niestandardowy (nowy dziennik który będzie zbierał następujące informacje)



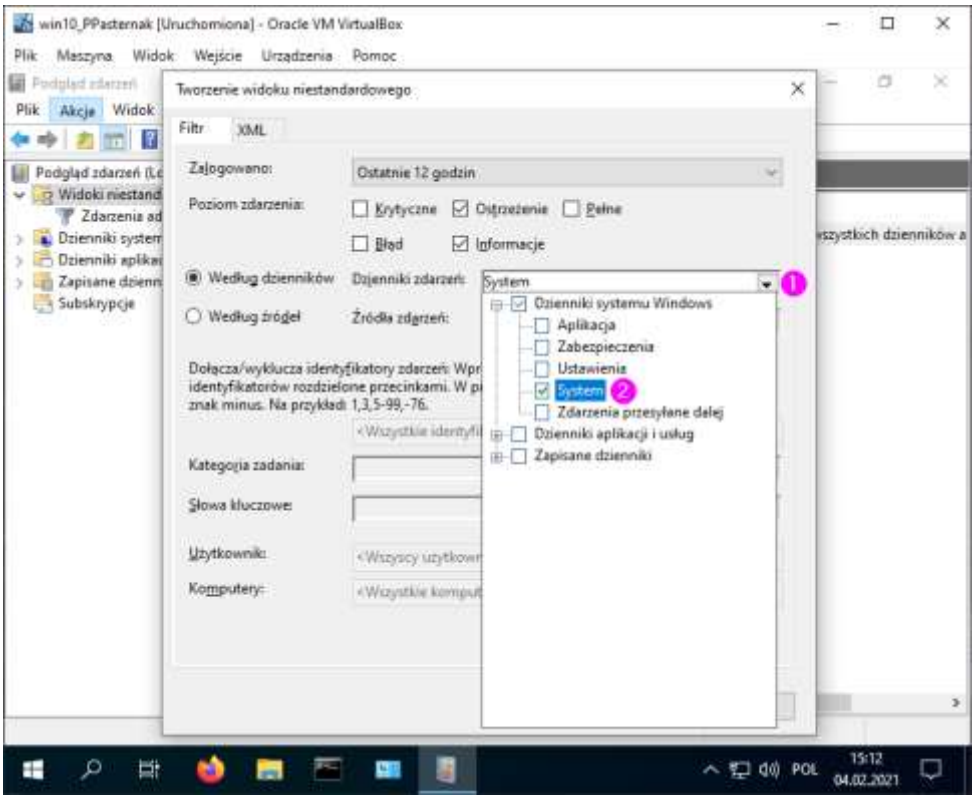
- Wyświetl ostatnie 12 godzin

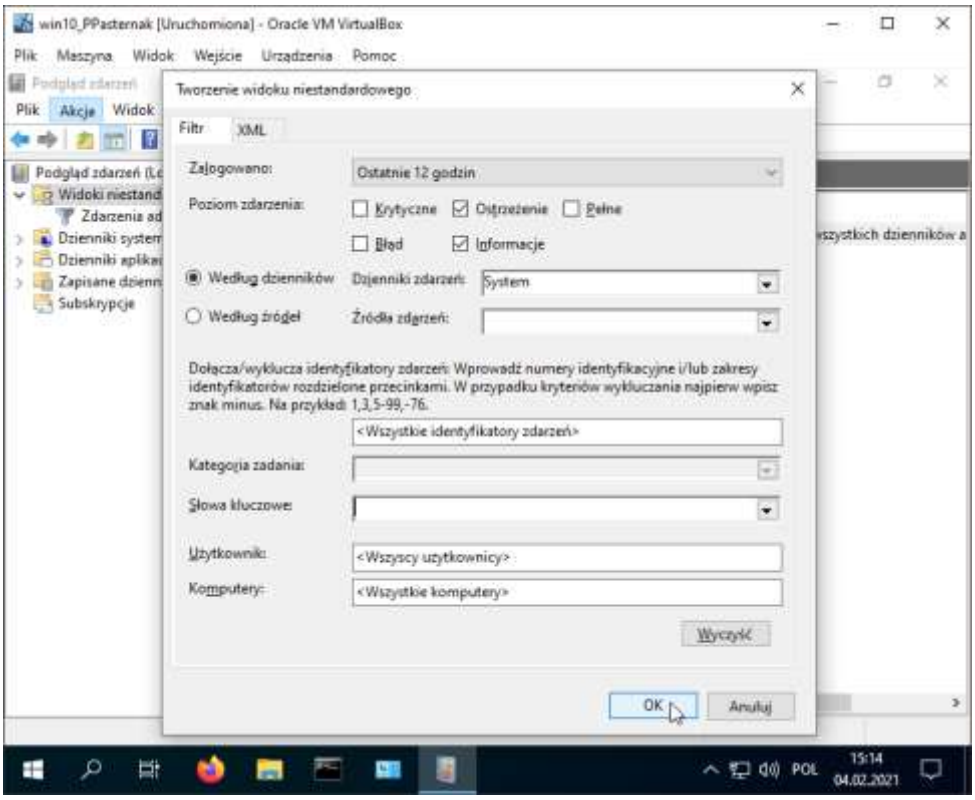


- Informacje oraz ostrzeżenia -podaj sensowny przykład

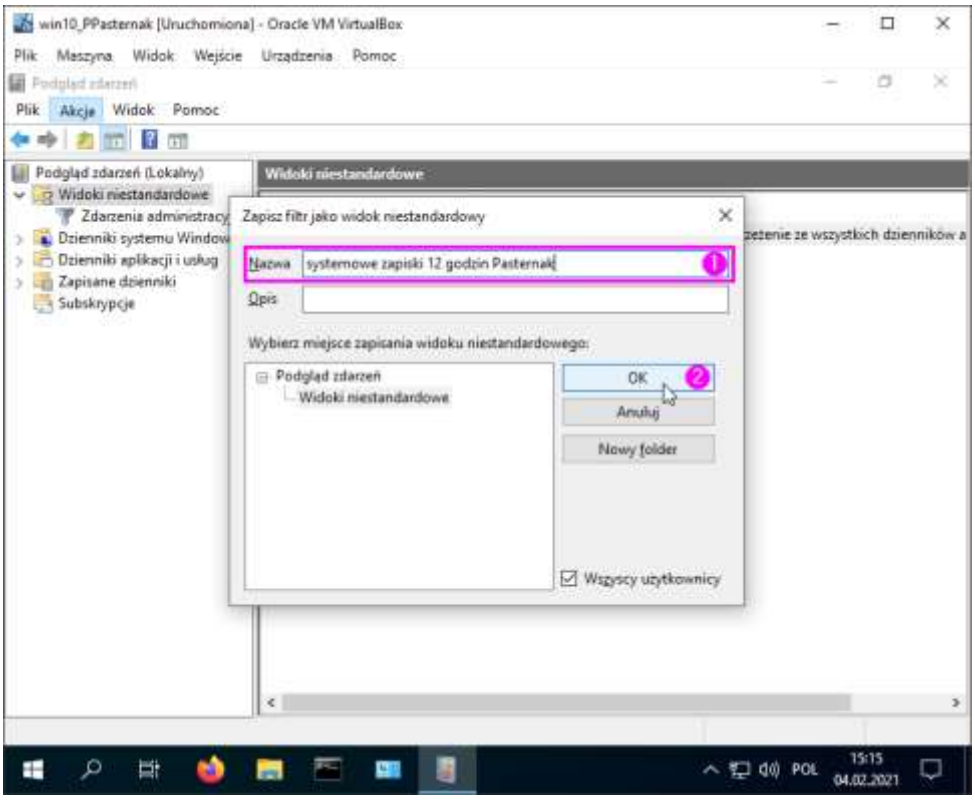


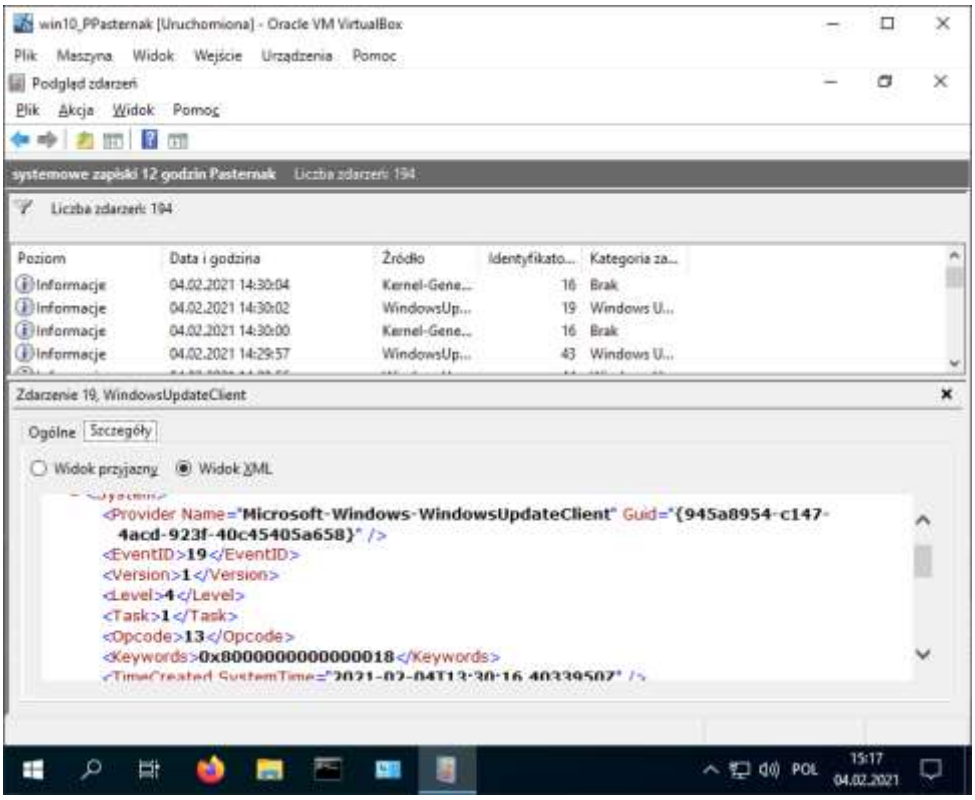
- zdarzenia z kategorii System -podaj sensowny przykład



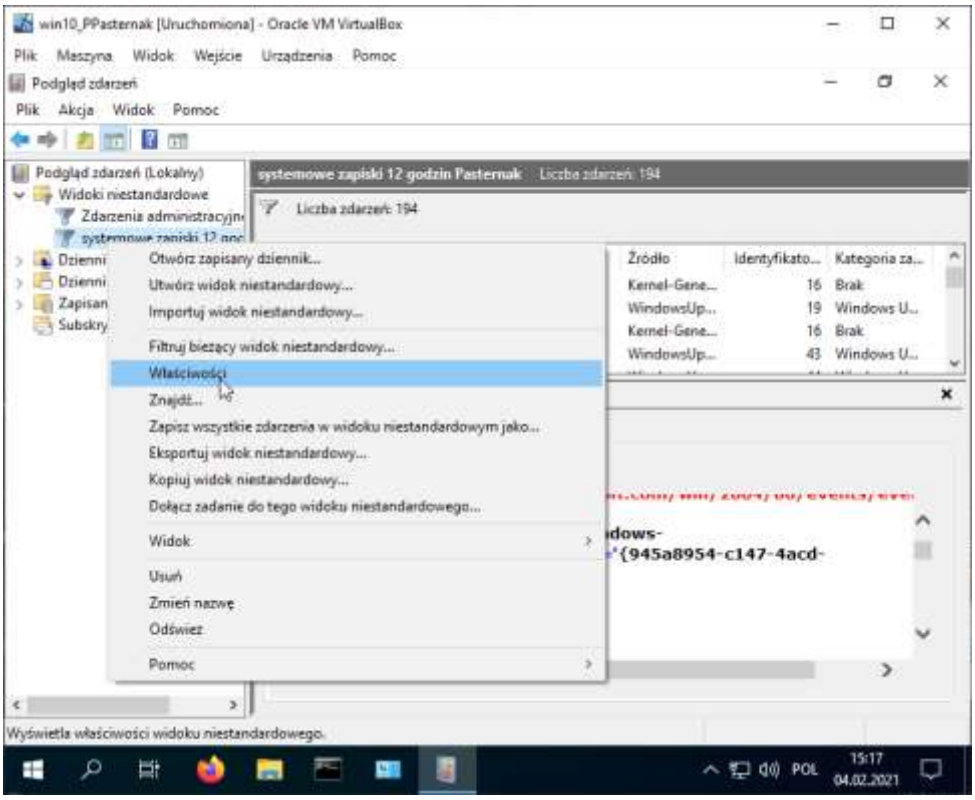


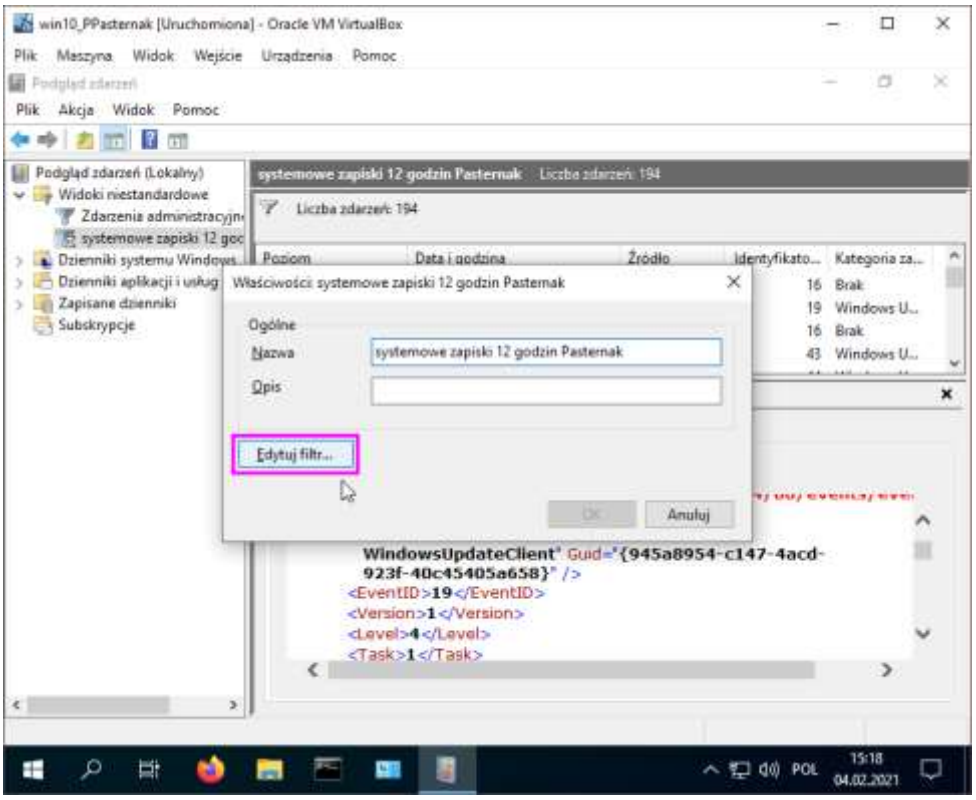
- Zapisanie pod nazwą „systemowe zapiski 12 godzin nazwisko”

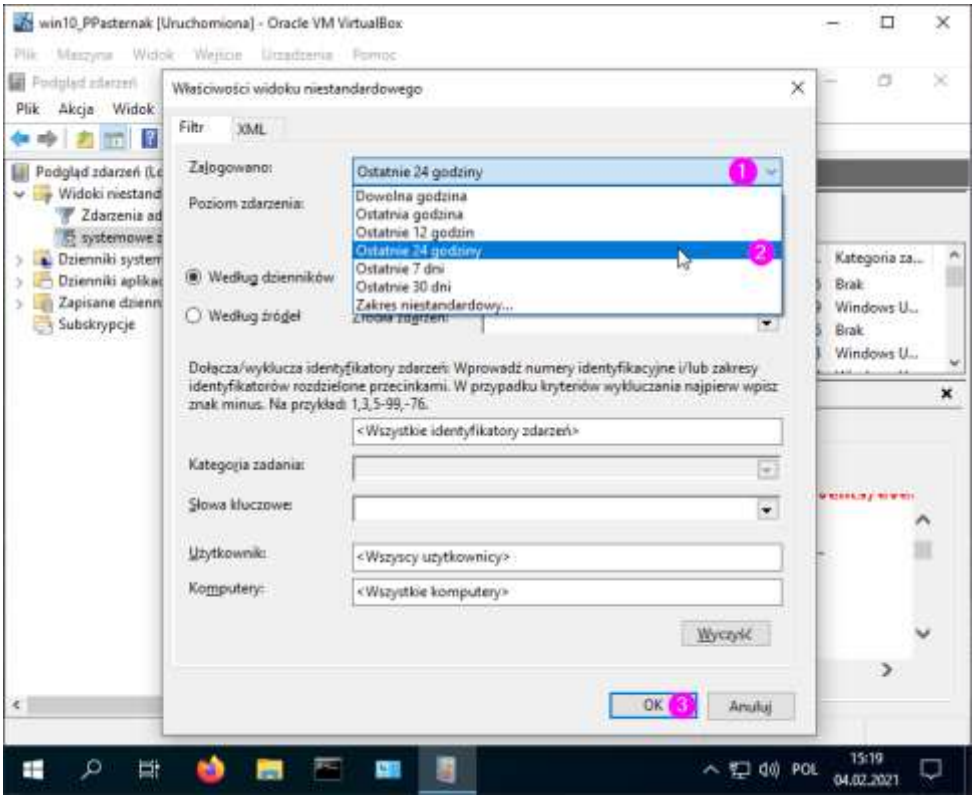




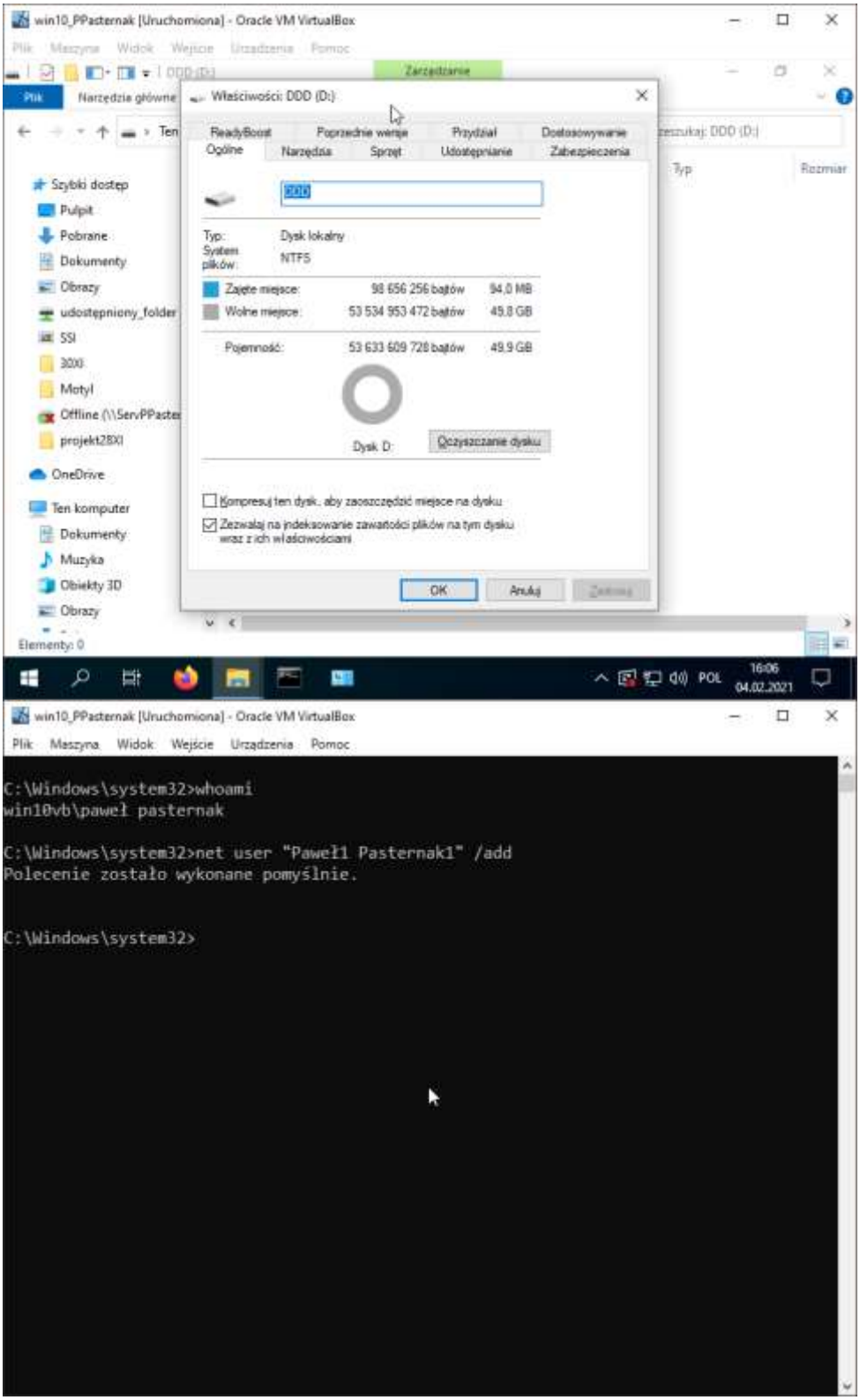
- w jaki sposób można zmienić – dany dziennik tak by pobierał informację z 24 godzin



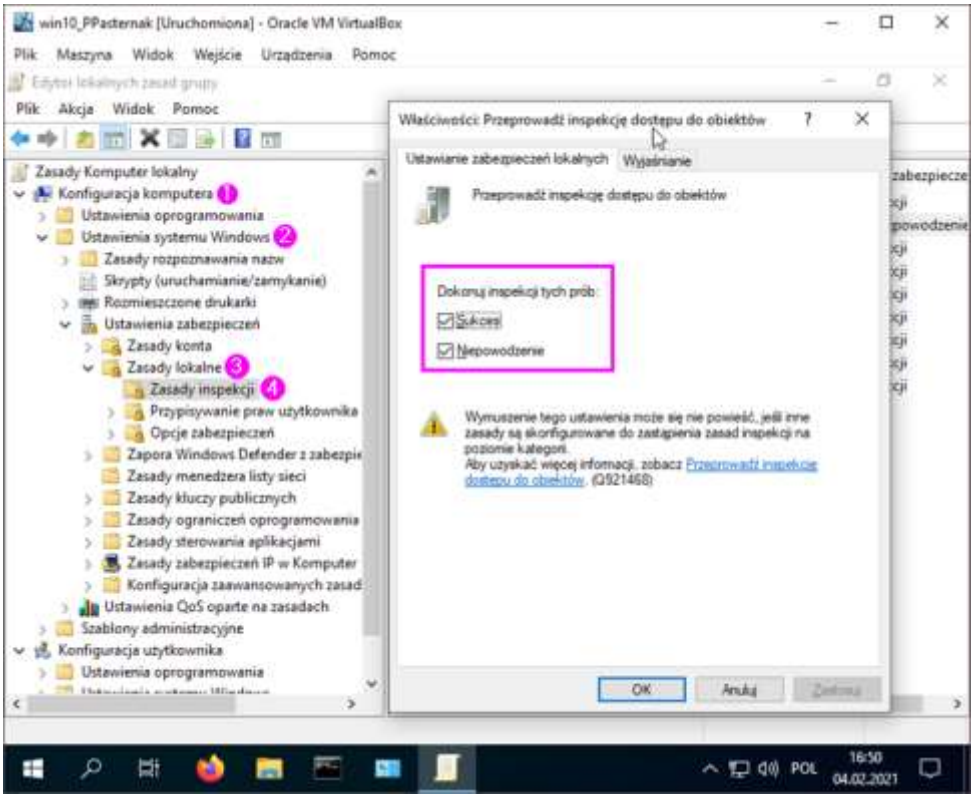

win10_PPasternak [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc
Podgląd zdarzeń
Plik Akcja Widok Pomoc
Podgląd zdarzeń (Lokalny)
Widoki niestandardowe
Zdarzenia administracyjne
systemowe zapiski 12 goc
Dzienniki systemu Windows
Dzienniki aplikacji i usług
Zapisane dzienniki
Subskrypcje
systemowe zapiski 12 godzin Pasternak Liczba zdarzeń: 194
Liczba zdarzeń: 194
Poziom Data i godzina Źródło Identyfikato... Kategoria za...
16 Brak
19 Windows U...
16 Brak
43 Windows U...
Właściwości: systemowe zapiski 12 godzin Pasternak
Ogólne
Nazwa systemowe zapiski 12 godzin Pasternak
Opis
Edytuj filtr...
OK Anuluj
WindowsUpdateClient' Guid='{945a8954-c147-4acd-923f-40c45405a658}' />
<EventID>19</EventID>
<Version>1</Version>
<Level>4</Level>
<Task>1</Task>
POL 15:18 04.02.2021


win10_PPasternak [Uruchomiona] - Oracle VM VirtualBox
Właściwości widoku niestandardowego
Filtr XML
Zalogowano: Ostatnie 24 godziny
Poziom zdarzenia:
Dowolna godzina
Ostatnia godzina
Ostatnie 12 godzin
Ostatnie 24 godziny
Ostatnie 7 dni
Ostatnie 30 dni
Zakres niestandardowy...
Według dzienników
Według źródeł
Dołącza/wyklucza identyfikatory zdarzeń: Wprowadź numery identyfikacyjne i/lub zakresy identyfikatorów rozdzielone przecinkami. W przypadku kryteriów wykluczania najpierw wpisz znak minus. Na przykład 1,3,5-99,-76.
<Wszystkie identyfikatory zdarzeń>
Kategoria zadania:
Słowa kluczowe:
Użytkownik: <Wszyscy użytkownicy>
Komputery: <Wszystkie komputery>
Wyczyść
OK Anuluj
POL 15:19 04.02.2021

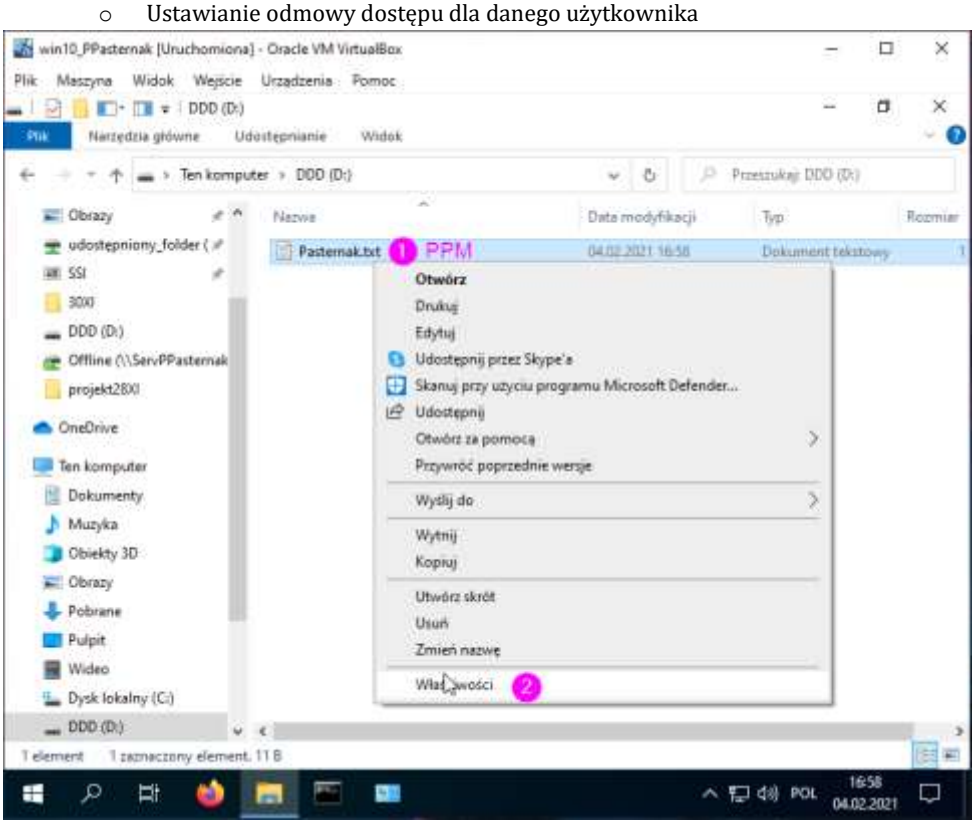
3. Wprowadzić takie ustawienia by możliwe było rejestrowanie sukcesy i niepowodzenia (inspekcja) pliku o nazwie nazwisko (na dysku :D - jeżeli nie ma utworzyć dysk D dodając przestrzeń 10 GB).

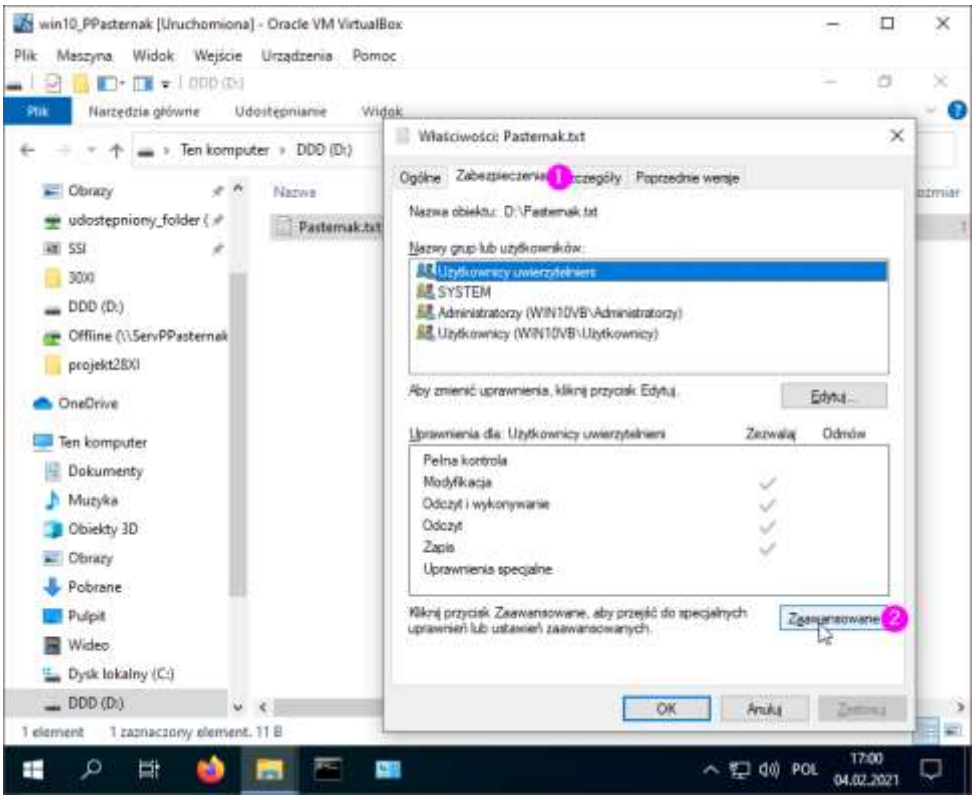


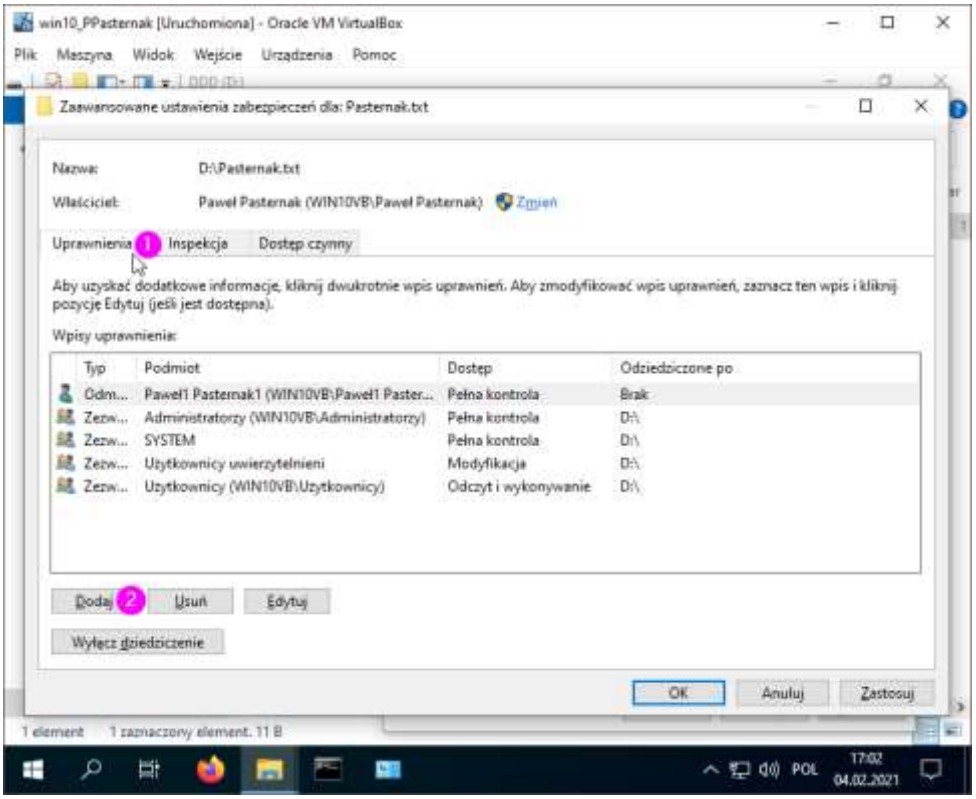
- Włączenie inspekcji

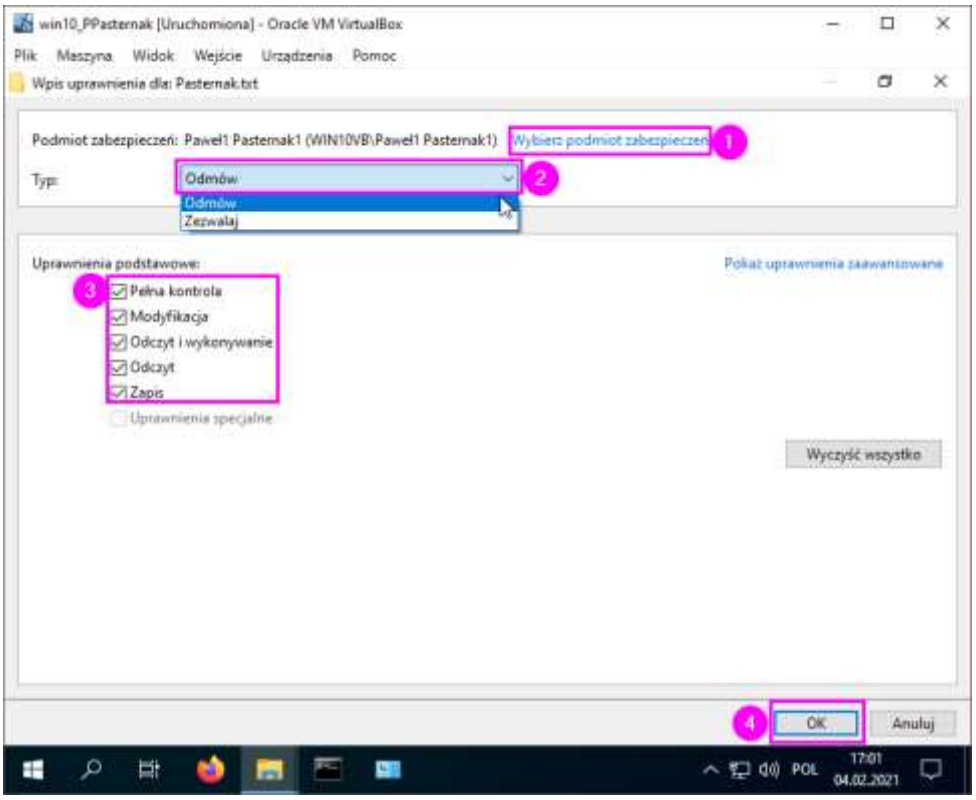


- Ustawianie odmowy dostępu dla danego użytkownika

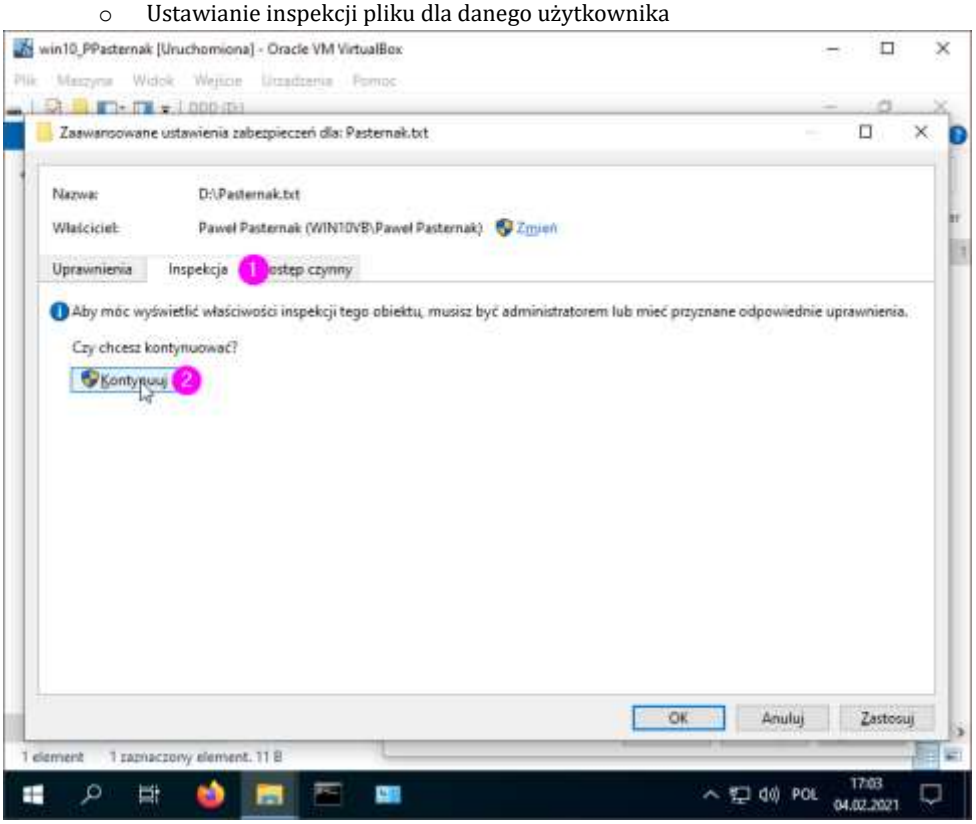


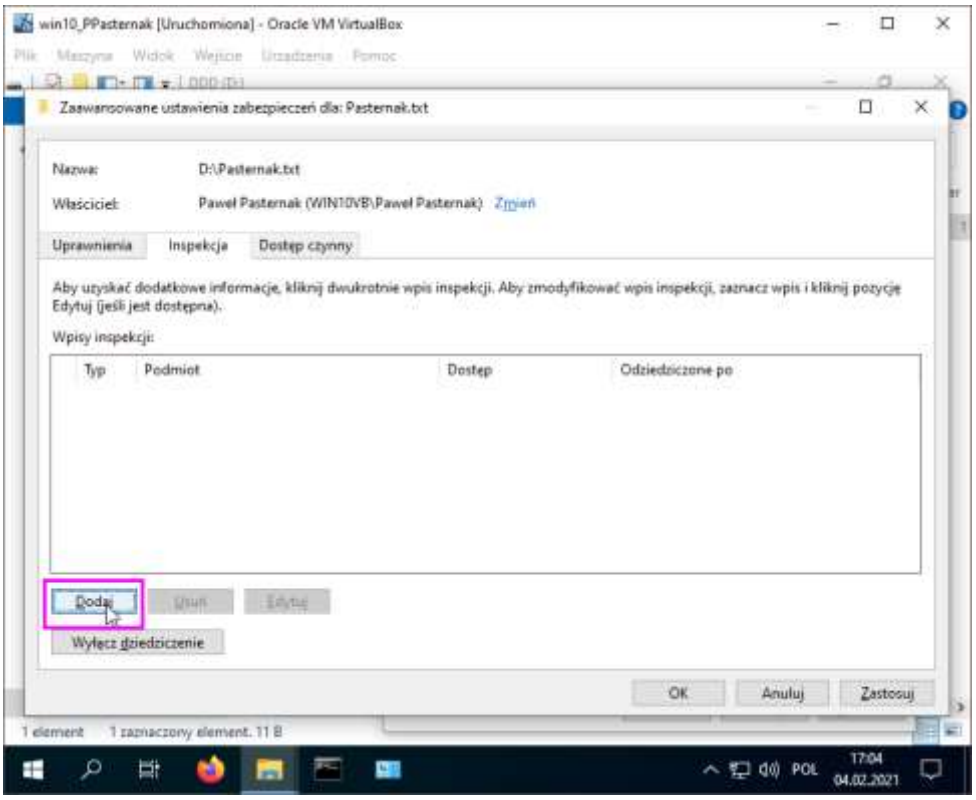

win10_PPasternak [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc
Właściwości: Pasternak.txt
Ogólne Zabezpieczenia Szczegóły Poprzednie wersje
Nazwa obiektu: D:\Pasternak.txt
Nazwy grup lub użytkowników:
Użytkownicy uwierzytelnieni
SYSTEM
Administratorzy (WIN10VB\Administratorzy)
Użytkownicy (WIN10VB\Użytkownicy)
Aby zmienić uprawnienia, kliknij przycisk Edytuj.
Edytuj...
Uprawnienia dla: Użytkownicy uwierzytelnieni
Zezwalaj
Odmów
Pełna kontrola
Modyfikacja
Odczyt i wykonywanie
Odczyt
Zapis
Uprawnienia specjalne
Kliknij przycisk Zaawansowane, aby przejść do specjalnych uprawnień lub ustawień zaawansowanych.
Zaawansowane
OK
Anuluj
Zastosuj
1 element 1 zaznaczony element. 11 B
POL
17:00
04.02.2021

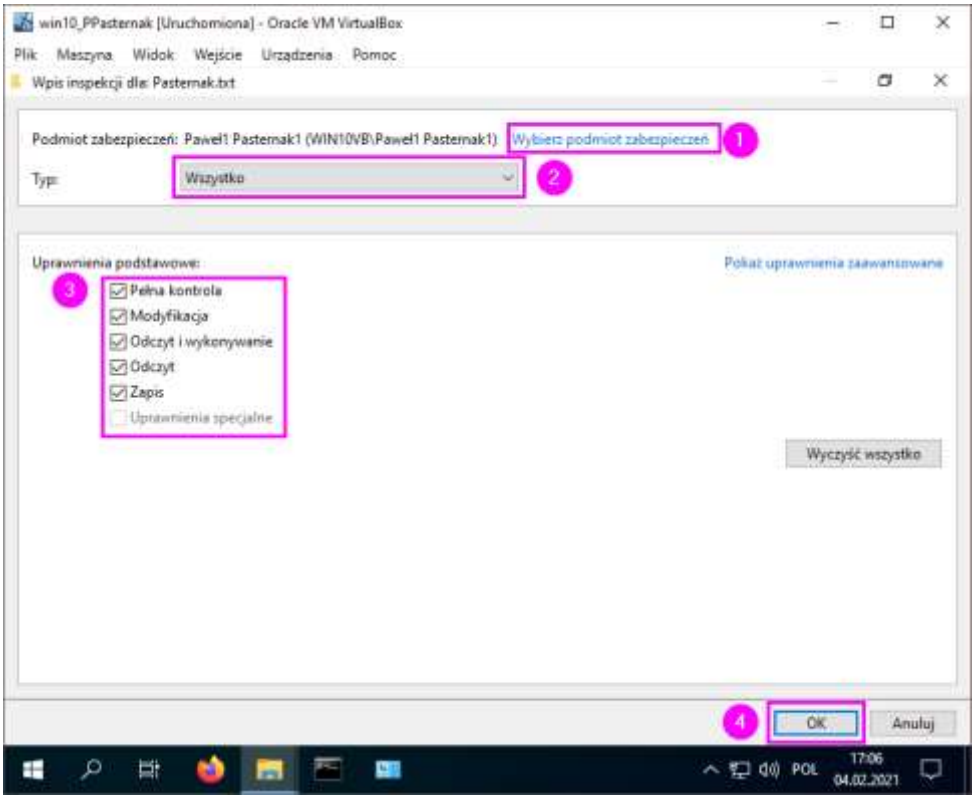

win10_PPasternak [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc
Zaawansowane ustawienia zabezpieczeń dla: Pasternak.txt
Nazwa: D:\Pasternak.txt
Właściciel: Paweł Pasternak (WIN10VB\Paweł Pasternak) Zmień
Uprawnienia Inspekcja Dostęp czynny
Aby uzyskać dodatkowe informacje, kliknij dwukrotnie wpis uprawnień. Aby zmodyfikować wpis uprawnień, zaznacz ten wpis i kliknij pozycję Edytuj (jeśli jest dostępna).
Wpisy uprawnienia:
Typ
Podmiot
Dostęp
Odziedziczone po
Odm... Paweł1 Pasternak1 (WIN10VB\Paweł1 Paster... Pełna kontrola Brak
Zezw... Administratorzy (WIN10VB\Administratorzy) Pełna kontrola D:\
Zezw... SYSTEM Pełna kontrola D:\
Zezw... Użytkownicy uwierzytelnieni Modyfikacja D:\
Zezw... Użytkownicy (WIN10VB\Użytkownicy) Odczyt i wykonywanie D:\
Dodaj
Usuń
Edytuj
Wyłącz dziedziczenie
OK
Anuluj
Zastosuj
1 element 1 zaznaczony element. 11 B
POL
17:02
04.02.2021

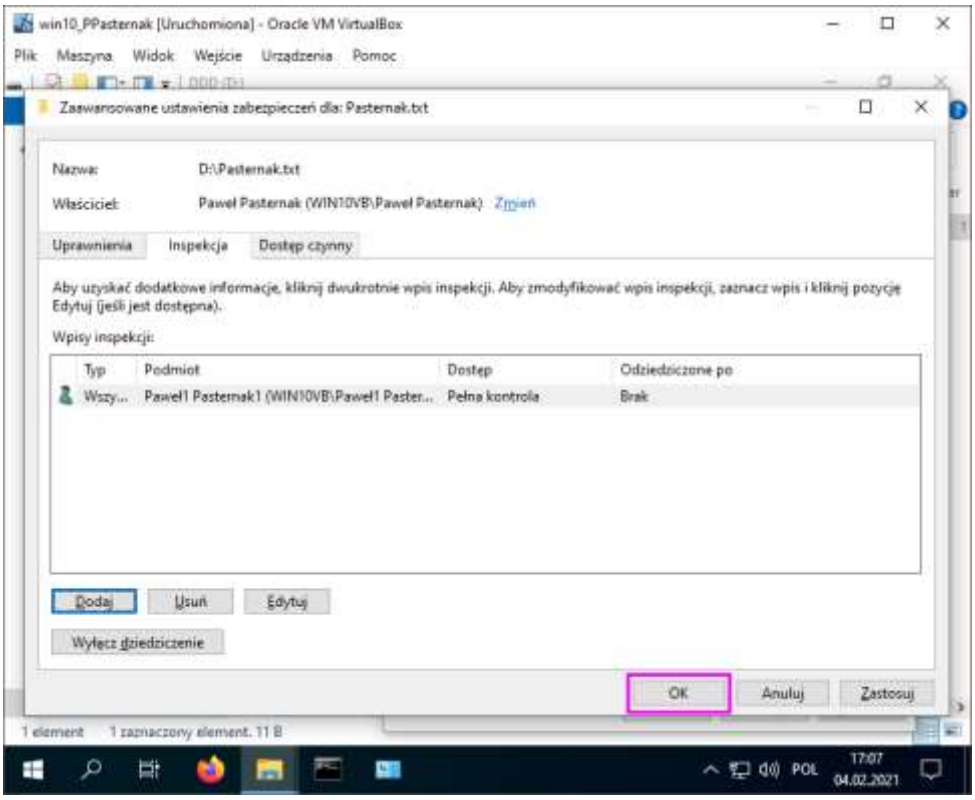


- Ustawianie inspekcji pliku dla danego użytkownika

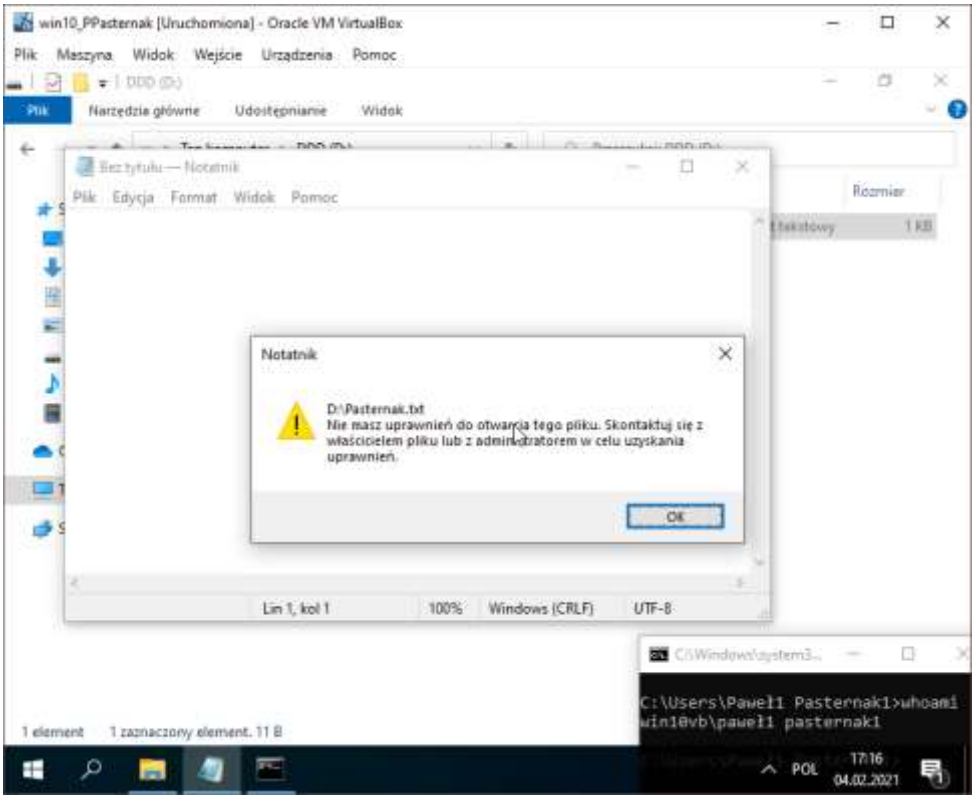


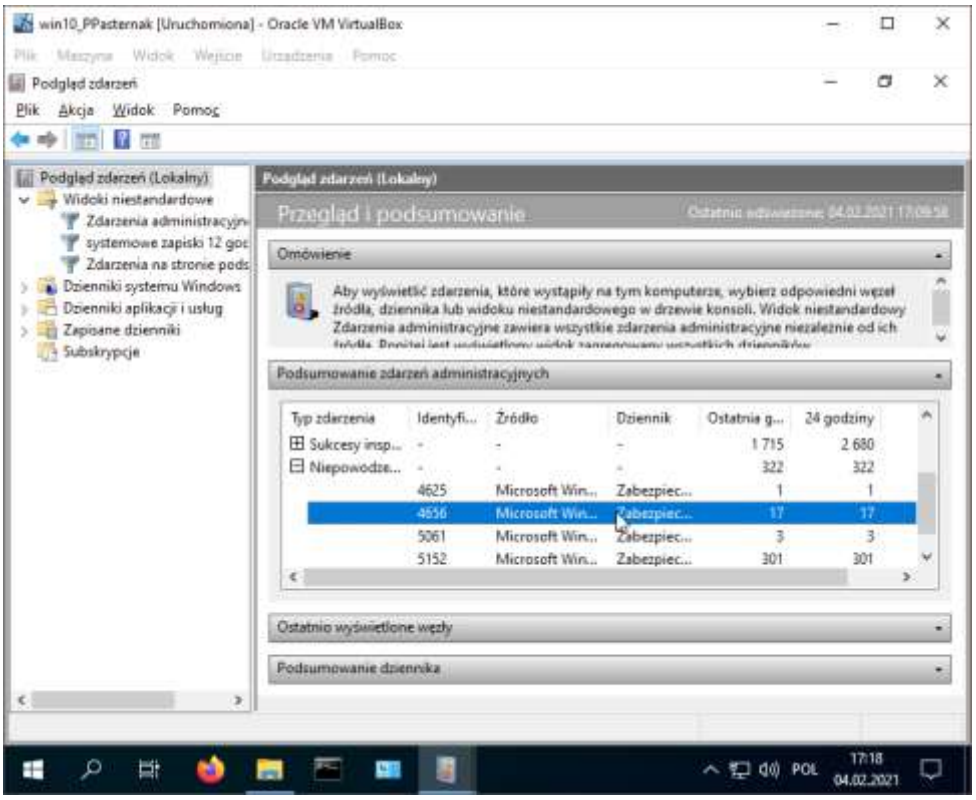

win10_PPasternak [Uruchomiona] - Oracle VM VirtualBox
Zaawansowane ustawienia zabezpieczeń dla: Pasternak.txt
Nazwa: D:\Pasternak.txt
Właściciel: Paweł Pasternak (WIN10VB\Paweł Pasternak) Zmień
Uprawnienia
Inspekcja
Dostęp czynny
Aby uzyskać dodatkowe informacje, kliknij dwukrotnie wpis inspekcji. Aby zmodyfikować wpis inspekcji, zaznacz wpis i kliknij pozycję Edytuj (jeśli jest dostępna).
Wpisy inspekcji:
Typ
Podmiot
Dostęp
Odziedziczone po
Dodaj
Usuń
Edytuj
Wyłącz dziedziczenie
OK
Anuluj
Zastosuj
1 element
1 zaznaczony element. 11 B
POL
17:04
04.02.2021

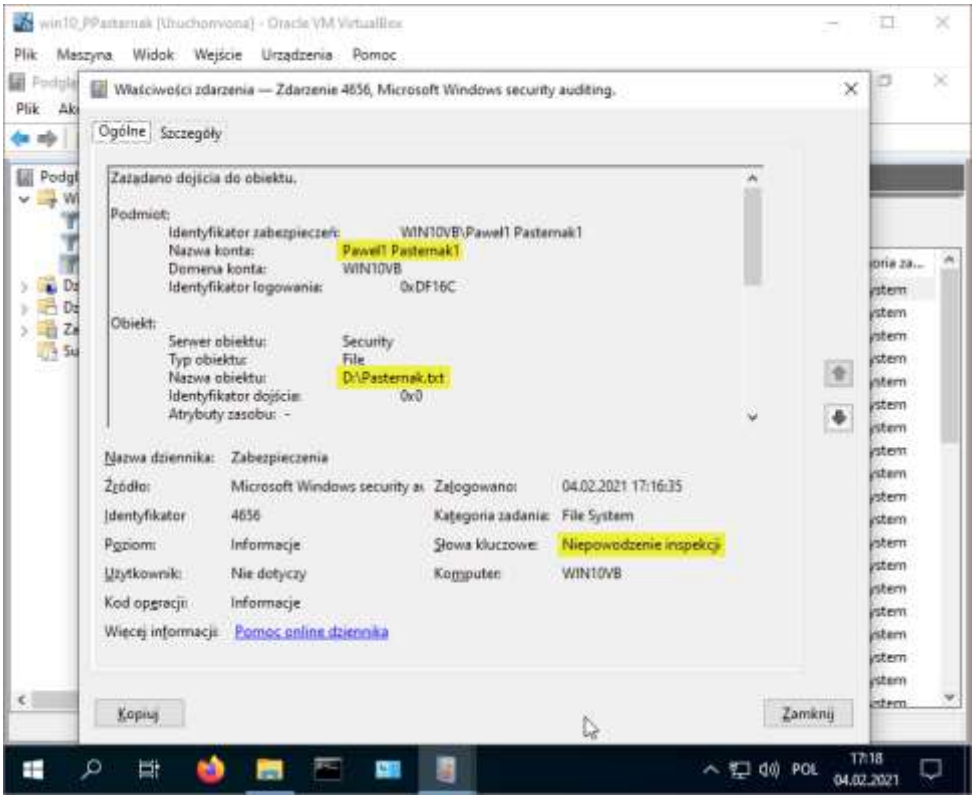

win10_PPasternak [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc
Wpis inspekcji dla: Pasternak.txt
Podmiot zabezpieczeń: Paweł1 Pasternak1 (WIN10VB\Paweł1 Pasternak1)
Wybierz podmiot zabezpieczeń
1
Typ:
Wszystko
2
Uprawnienia podstawowe:
3
Pełna kontrola
Modyfikacja
Odczyt i wykonywanie
Odczyt
Zapis
Uprawnienia specjalne
Pokaż uprawnienia zaawansowane
Wyczyść wszystko
4
OK
Anuluj
POL
17:06
04.02.2021



- co najmniej 2 użytkowników (Imię, Nazwisko i Imię1 Nazwisko 1) ograniczyć uprawnienia do pliku użytkownikowi nazwisko a następnie spróbować ograniczonym użytkownikiem dokonać jakichś zmian w pliku – wykazać taką sytuację w dziennikach zdarzeń (Nazwa użytkownika, konkretny plik)

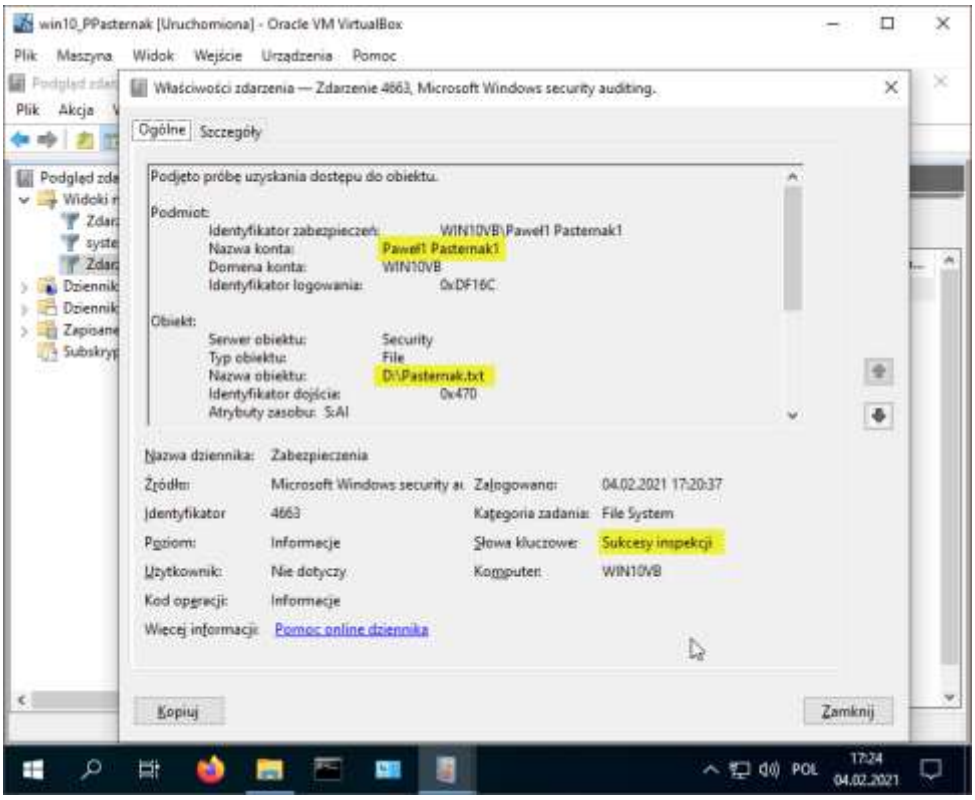






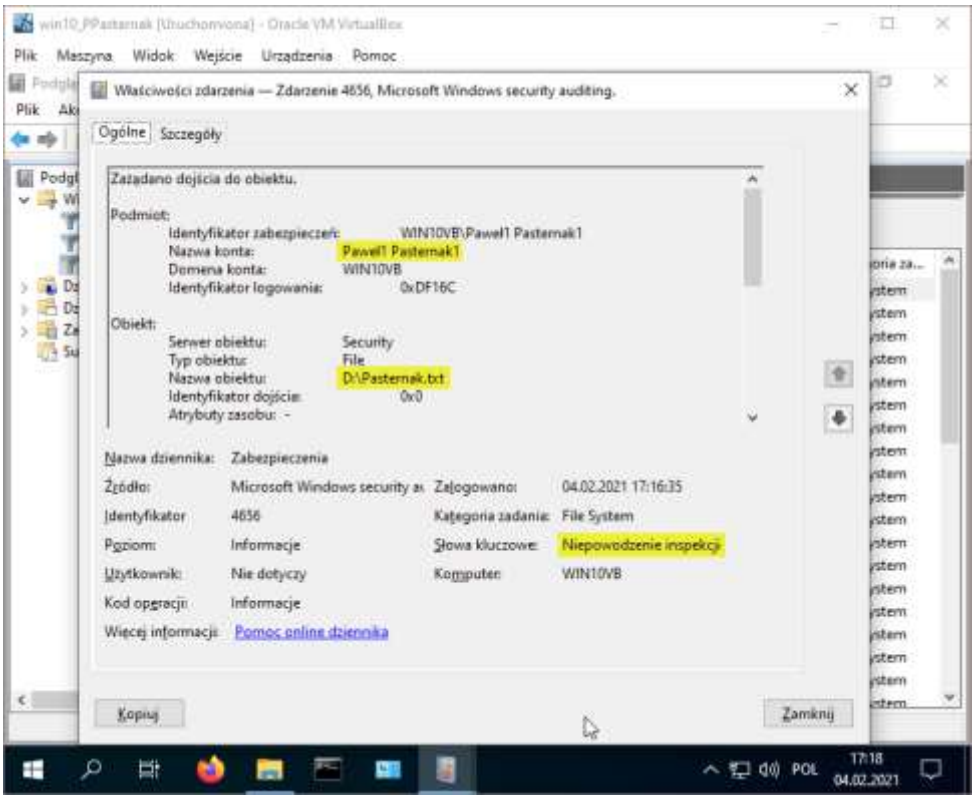
- czym różnią się od siebie Inspekcja sukcesów, inspekcja niepowodzeń (wymienić zdarzenia jakie mogą być oznaczone)
    - Inspekcja sukcesów

-zdarzenie opisujące pomyślne zakończenie zdarzenia dotyczącego zabezpieczeń, które jest objęte inspekcją. Przykład: zdarzenie typu Inspekcja sukcesów jest rejestrowane w przypadku zalogowania się użytkownika do komputera.

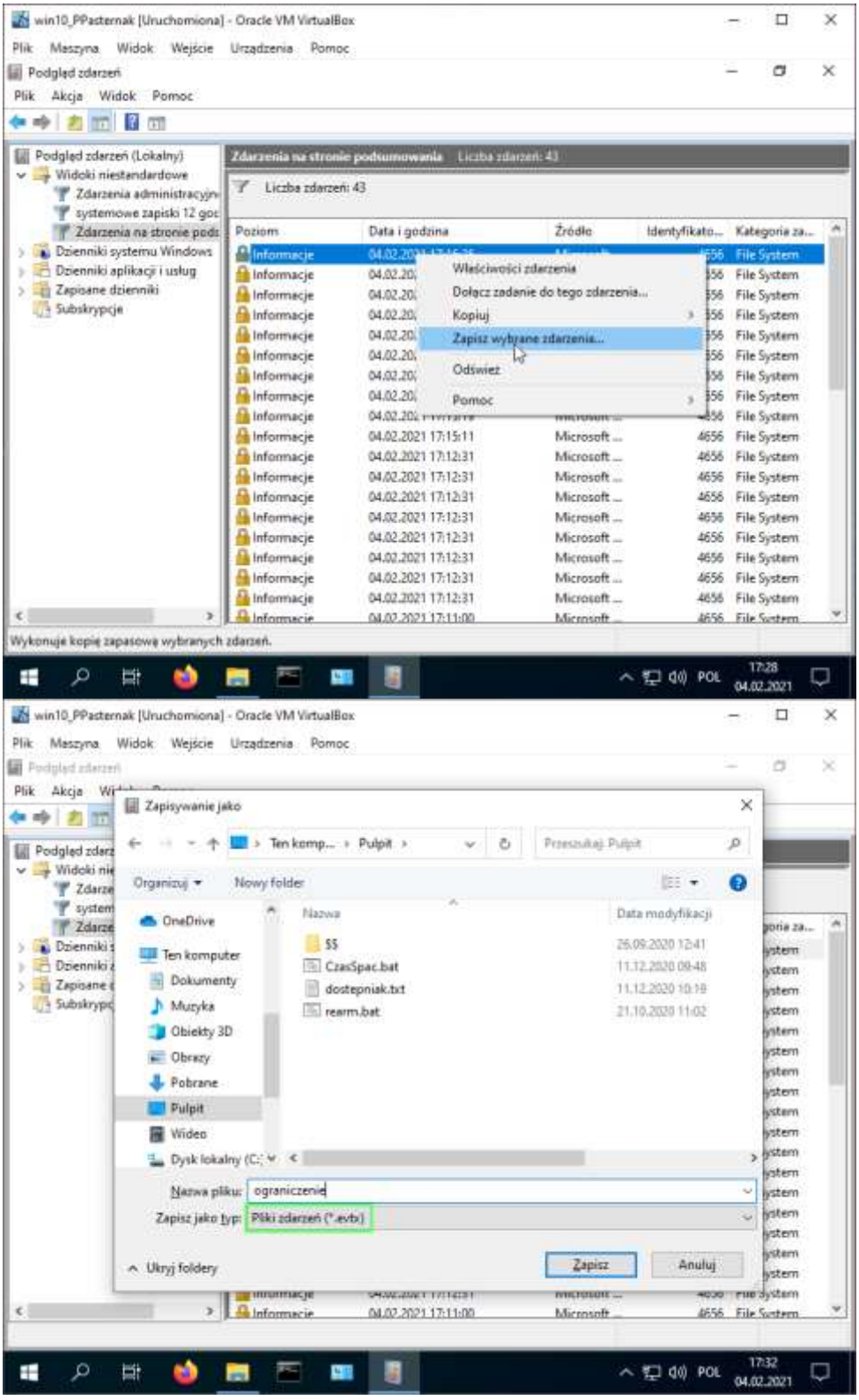


- Inspekcja niepowodzeń

- zdarzenie opisujące niepomyślne zakończenie zdarzenia dotyczącego zabezpieczeń, które jest objęte inspekcją. Przykład: zdarzenie typu Inspekcja niepowodzeń jest rejestrowane w sytuacji, gdy użytkownik nie może uzyskać dostępu do dysku sieciowego.



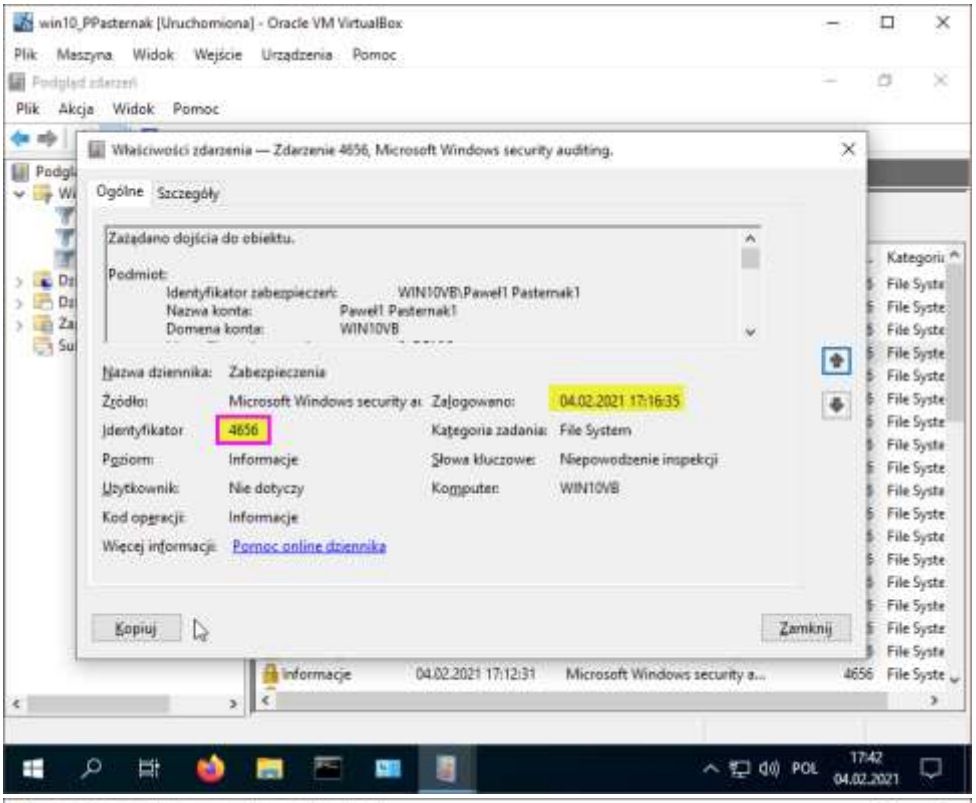
- zapisać jedno wybrane takie zdarzenie na pulpicie o nazwie ograniczenie (jakie rozszerzenie mają zapisane zdarzenia)

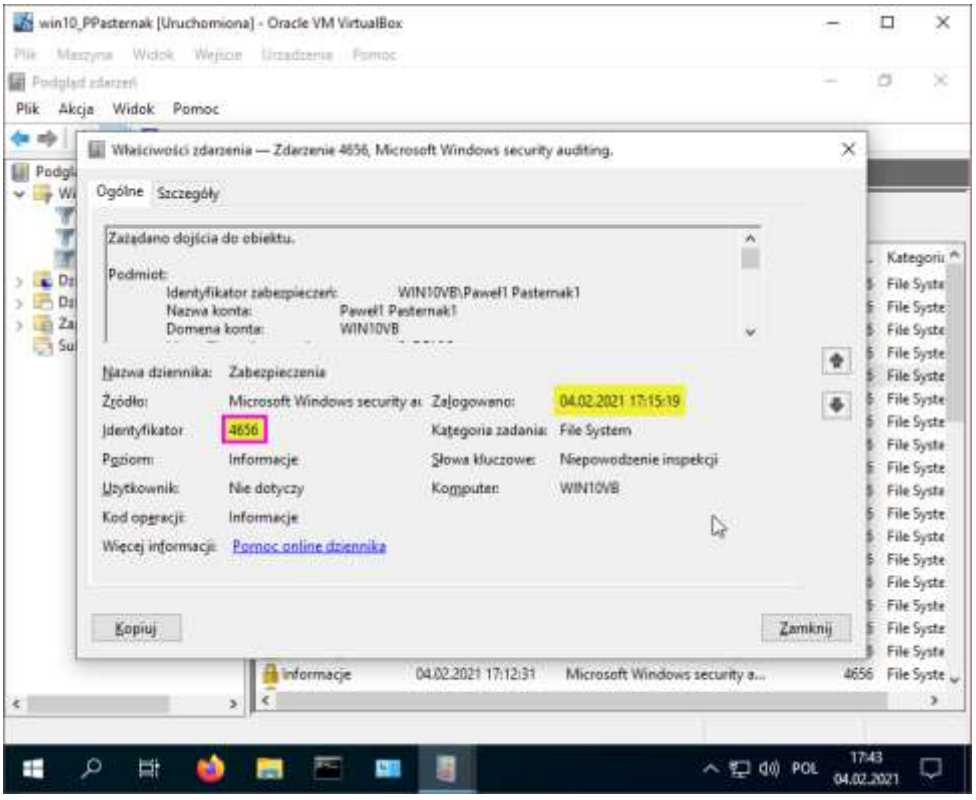


Mają rozszerzenie *.evtx

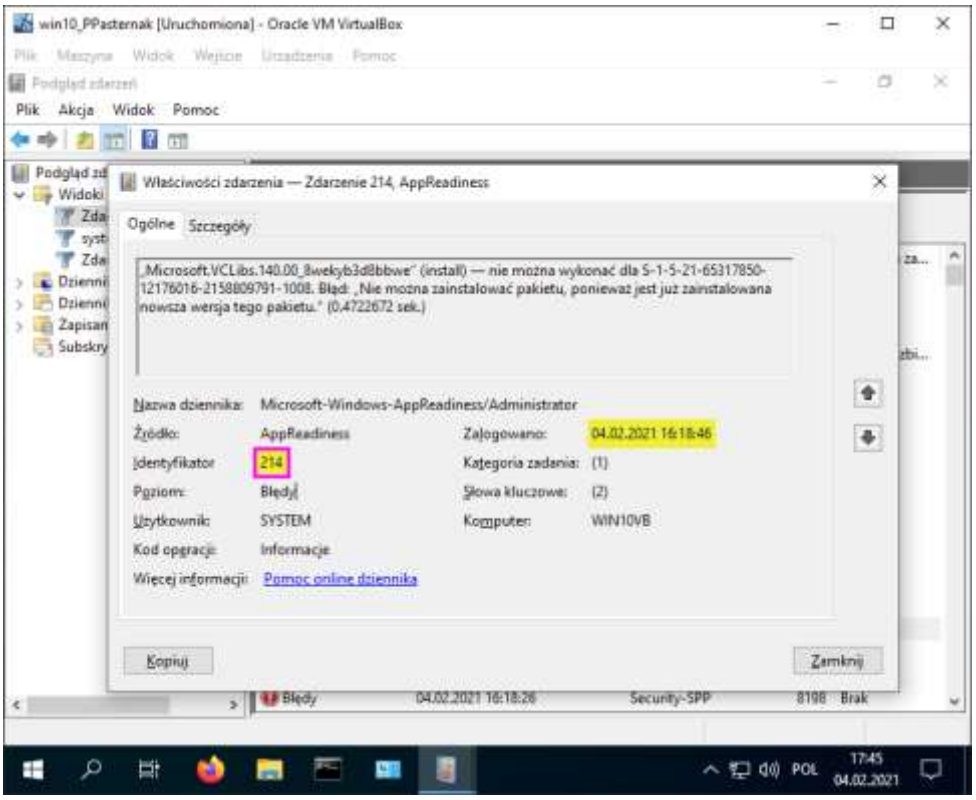
- jakie znaczenie ma Identyfikator zdarzenia do czego może nam się przydać ? podaj kilka przykładów z dziennika zdarzeń

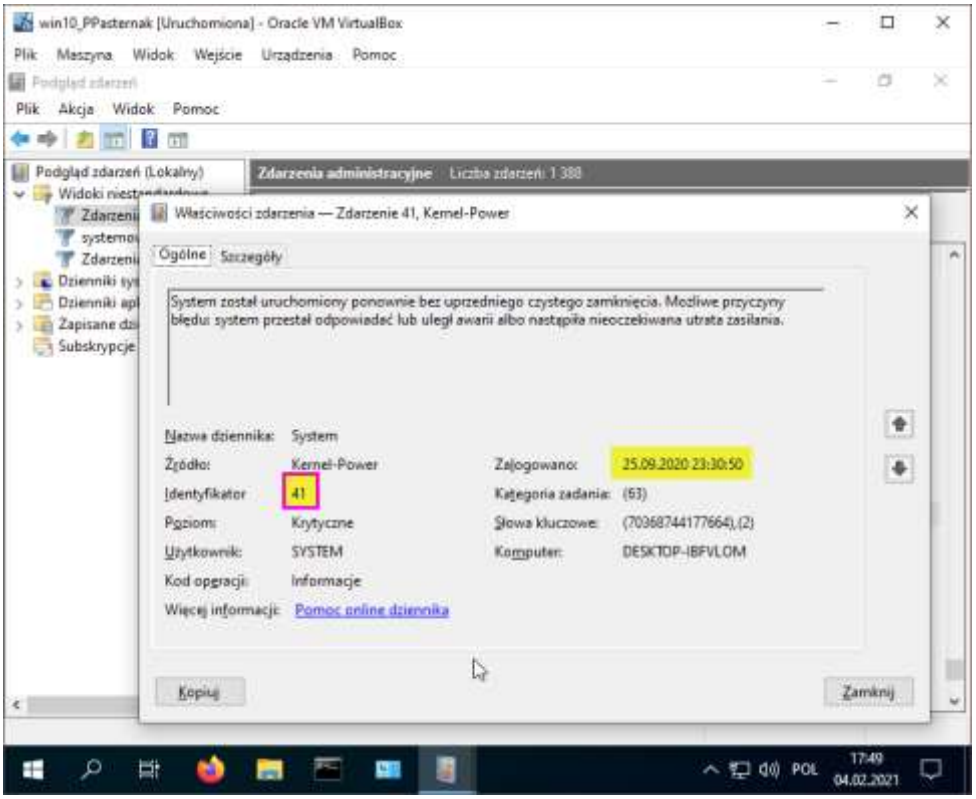
Identyfikator zdarzenia może pomóc przedstawicielom pomocy technicznej danego produktu w zidentyfikowaniu zdarzenia lub znalezieniu przez nas rozwiązania dotyczącego tego problemu, np.: w pomocy czy na forach, gdzie ktoś miał podobny problem.

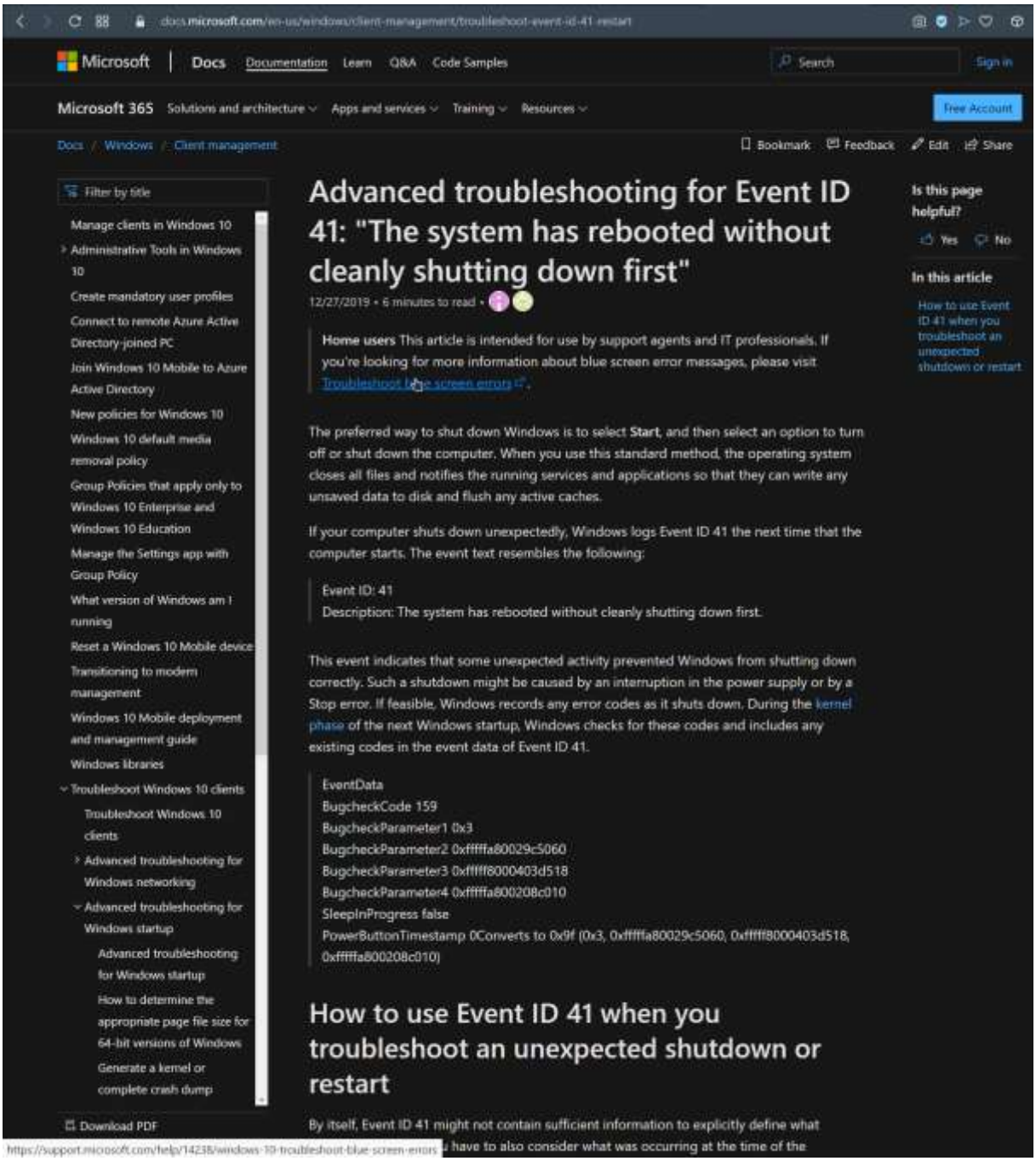




Te same problemy mają ten sam identyfikator.

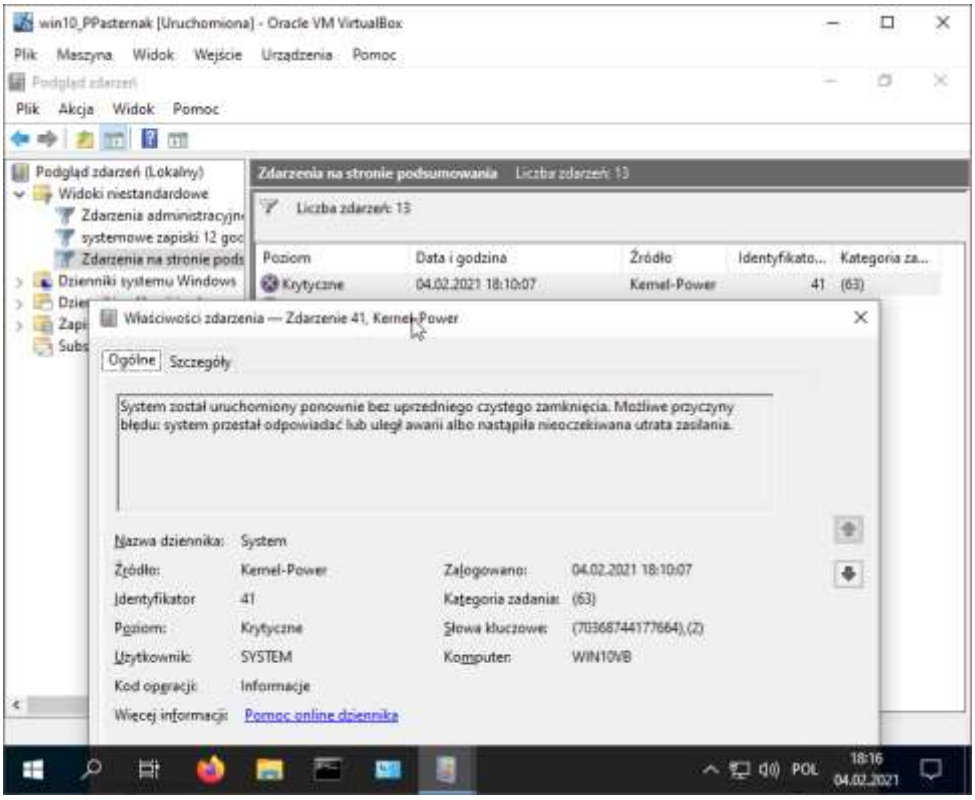

win10_PPasternak [Uruchomiona] - Oracle VM VirtualBox
Plik Akcja Widok Pomoc
Właściwości zdarzenia — Zdarzenie 214, AppReadiness
Ogólne Szczegóły
„Microsoft.VCLibs.140.00_8wekyb3d8bbwe" (install) — nie można wykonać dla S-1-5-21-65317850-12176016-2158809791-1008. Błąd: „Nie można zainstalować pakietu, ponieważ jest już zainstalowana nowsza wersja tego pakietu." (0.4722672 sek.)
Nazwa dziennika: Microsoft-Windows-AppReadiness/Administrator
Źródło: AppReadiness
Zalogowano: 04.02.2021 16:18:46
Identyfikator: 214
Kategoria zadania: (1)
Poziom: Błędy
Słowa kluczowe: (2)
Użytkownik: SYSTEM
Komputer: WIN10VB
Kod operacji: Informacje
Więcej informacji: Pomoc online dziennika
Kopiuj
Zamknij
Błędy 04.02.2021 16:18:26 Security-SPP 8198 Brak
POL 17:45 04.02.2021


win10_PPasternak [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc
Plik Akcja Widok Pomoc
Podgląd zdarzeń (Lokalny)
Zdarzenia administracyjne Liczba zdarzeń: 1 388
Właściwości zdarzenia — Zdarzenie 41, Kernel-Power
Ogólne Szczegóły
System został uruchomiony ponownie bez uprzedniego czystego zamknięcia. Możliwe przyczyny błędu: system przestał odpowiadać lub uległ awarii albo nastąpiła nieoczekiwana utrata zasilania.
Nazwa dziennika: System
Źródło: Kernel-Power
Zalogowano: 25.09.2020 23:30:50
Identyfikator: 41
Kategoria zadania: (63)
Poziom: Krytyczne
Słowa kluczowe: (70368744177664),(2)
Użytkownik: SYSTEM
Komputer: DESKTOP-IBFVLOM
Kod operacji: Informacje
Więcej informacji: Pomoc online dziennika
Kopiuj
Zamknij
POL 17:49 04.02.2021



Strona pomocy dla błędu 41

4. Wyłączyć komputer (niestandardowo – gniazdka – wirtualna maszyna – reset) wykazać takie zdarzenie w dziennikach zdarzeń



Samo zdarzenie o identyfikatorze 41 może nie zawierać wystarczających informacji, aby jednoznacznie określić, co się stało. Zwykle trzeba również wziąć pod uwagę, co się działo w momencie nieoczekiwanego wyłączenia (na przykład awaria zasilania). Skorzystaj z informacji zawartych w tym artykule, aby zidentyfikować podejście do rozwiązywania problemów, które jest odpowiednie w danych okolicznościach:

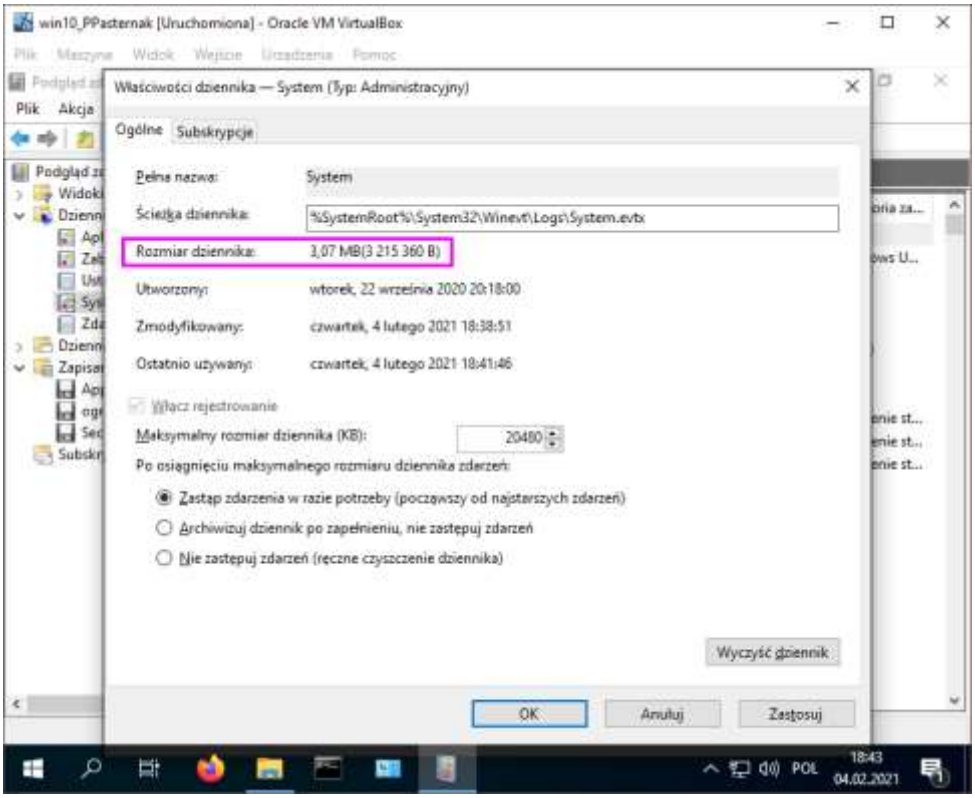
Scenariusz 1: komputer uruchamia się ponownie z powodu błędu zatrzymania, a identyfikator zdarzenia 41 zawiera kod błędu zatrzymania (sprawdzania błędów)

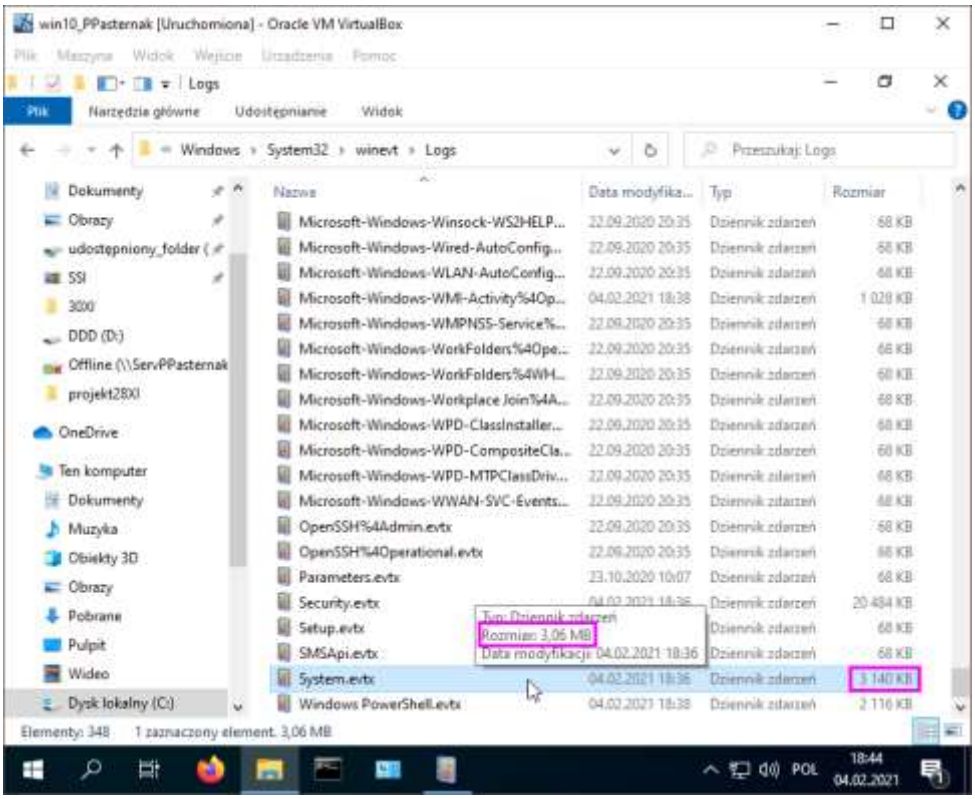
Scenariusz 2: Komputer uruchamia się ponownie, ponieważ został naciśnięty i przytrzymany przycisk zasilania

Scenariusz 3: komputer nie odpowiada lub losowo uruchamia się ponownie, a identyfikator zdarzenia 41 nie jest rejestrowany lub wpis o identyfikatorze zdarzenia 41 zawiera wartości kodów błędów równe zero

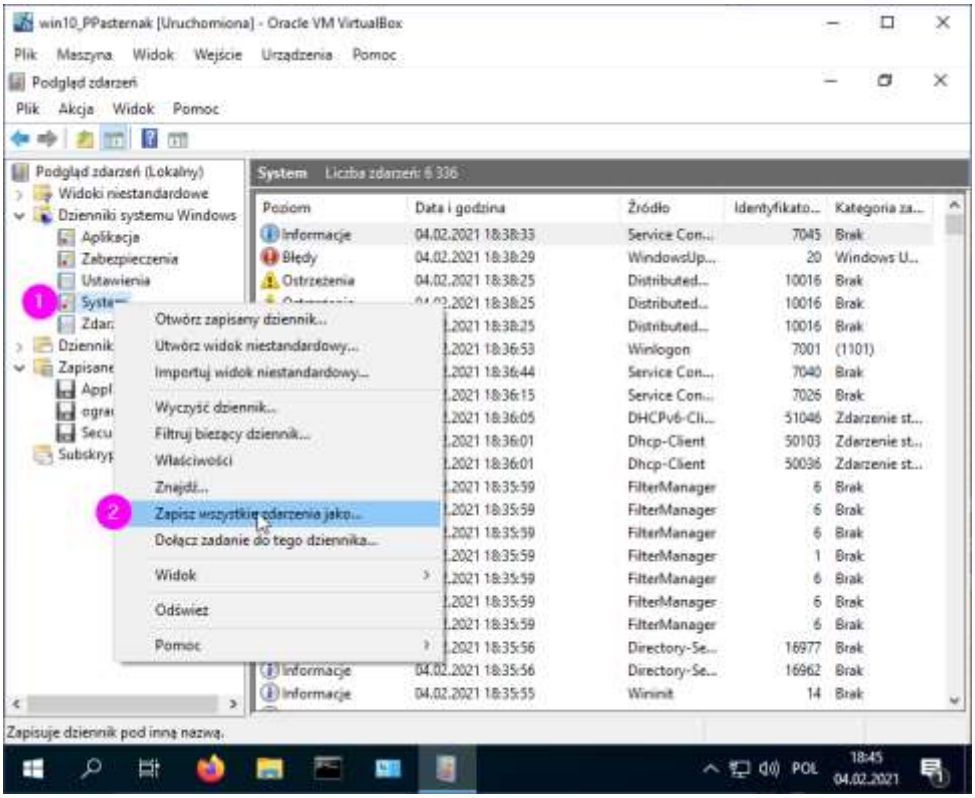
Źródło: https://docs.microsoft.com/pl-PL/windows/client-management/troubleshoot-event-id-41-restart

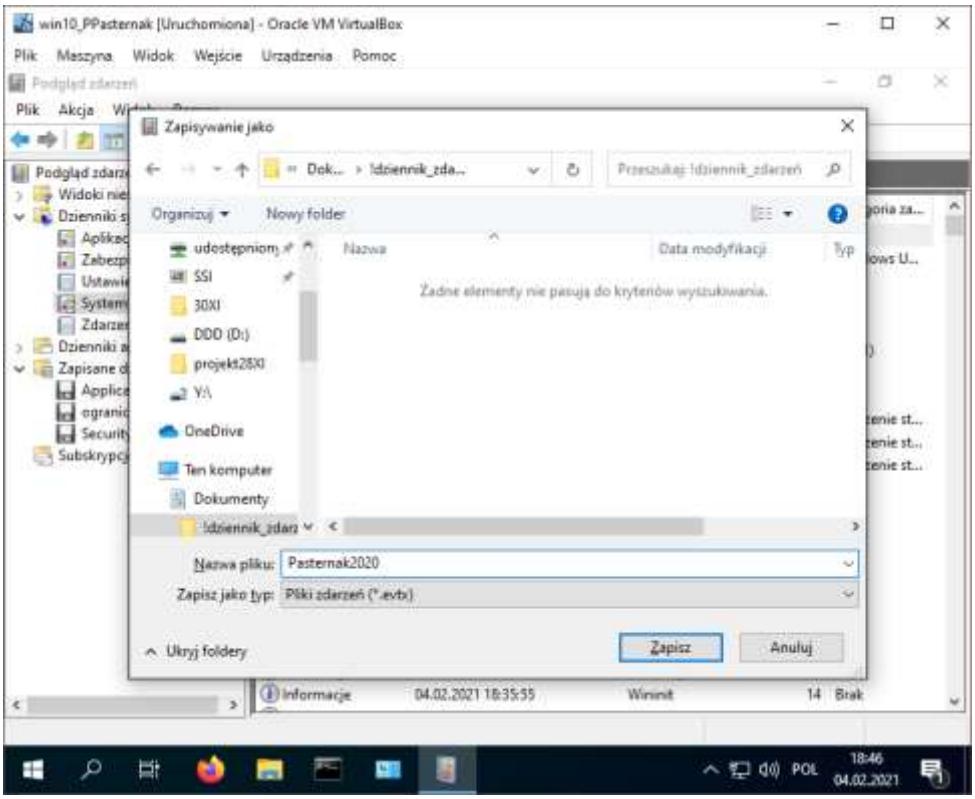
5. Wskazać jak wielki jest plik danego działu dziennika



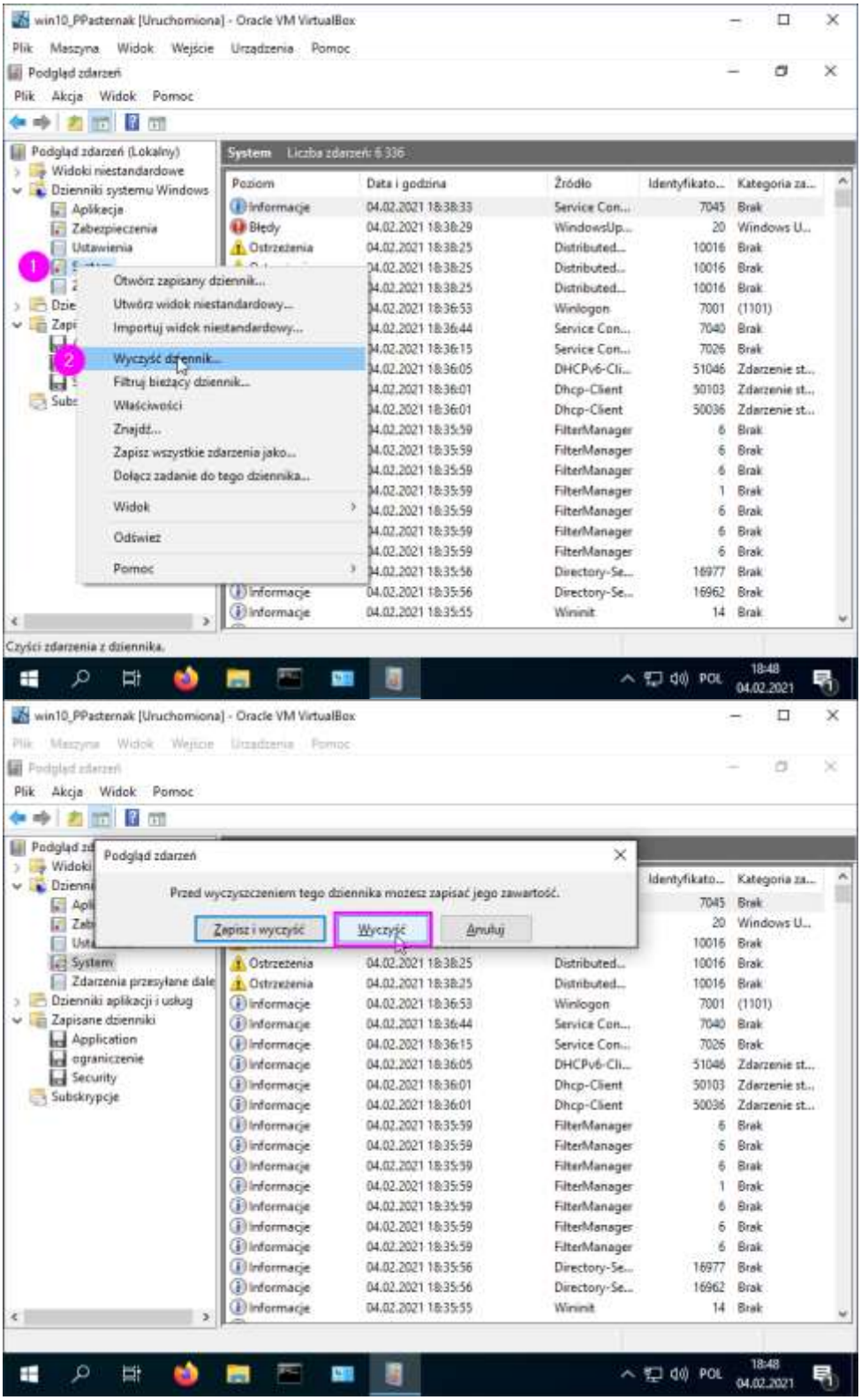


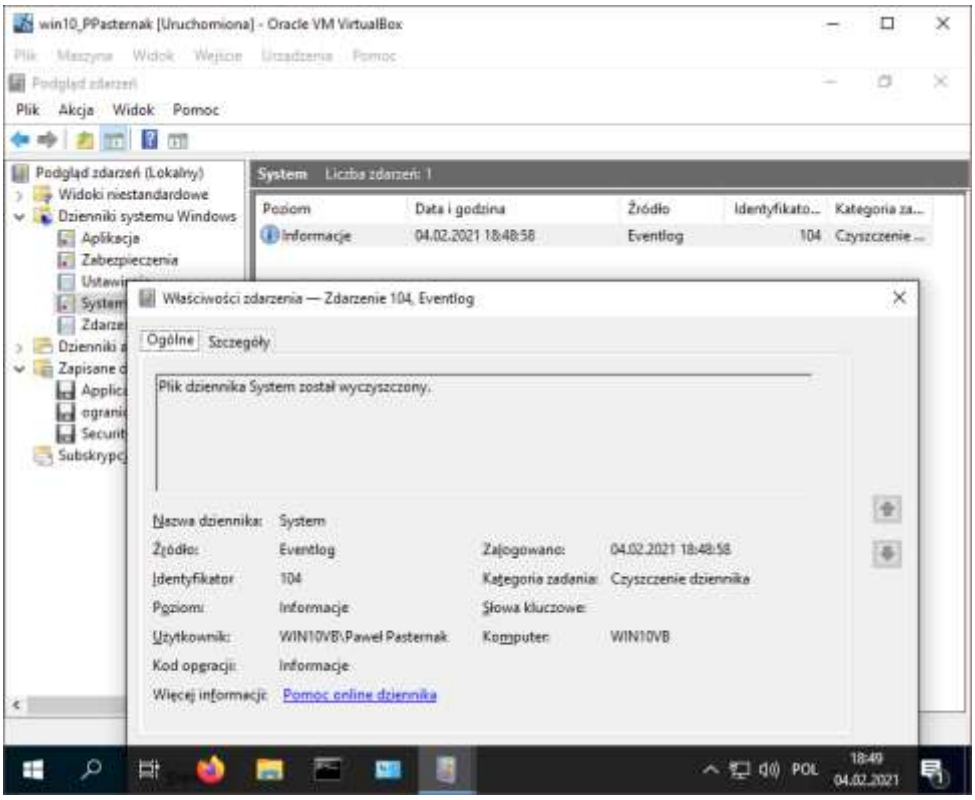
6. Zapisać dziennik „System” pod nazwą Nazwisko2020



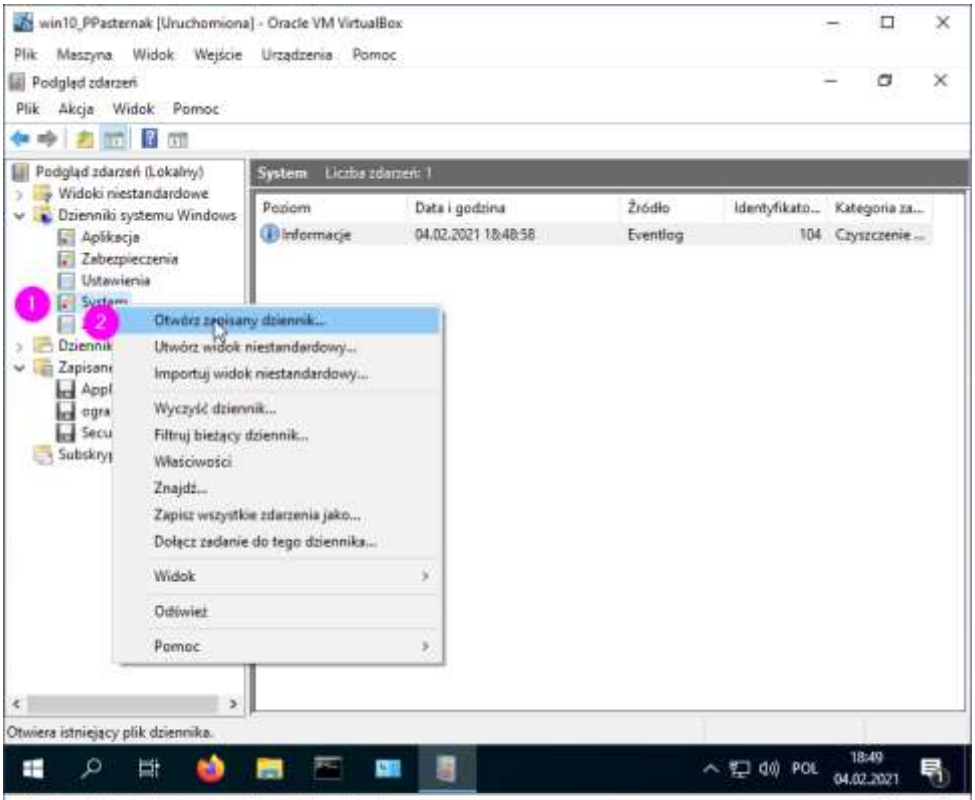


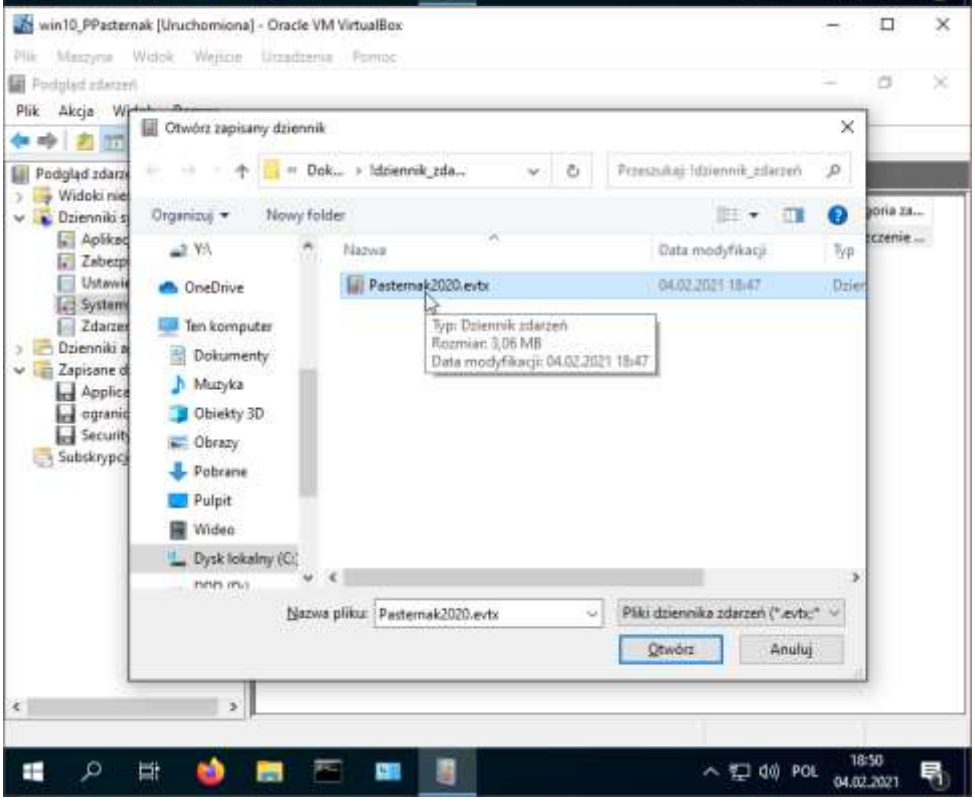
- Wyczyścić dany dziennik System np.

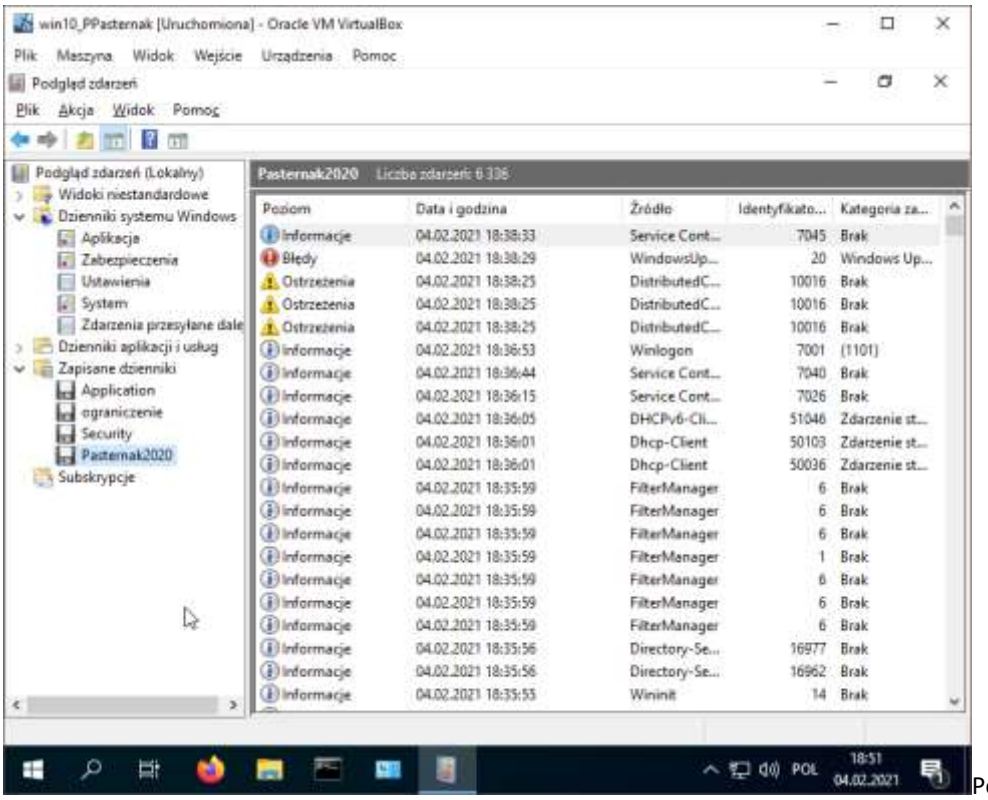



win10_PPasternak [Uruchomiona] - Oracle VM VirtualBox
Podgląd zdarzeń
Plik Akcja Widok Pomoc
Podgląd zdarzeń (Lokalny)
Widoki niestandardowe
Dzienniki systemu Windows
Aplikacja
Zabezpieczenia
System
System Liczba zdarzeń: 1
Poziom Data i godzina Źródło Identyfikato... Kategoria za...
Informacje 04.02.2021 18:48:58 Eventlog 104 Czyszczenie ...
Właściwości zdarzenia — Zdarzenie 104, Eventlog
Ogólne Szczegóły
Plik dziennika System został wyczyszczony.
Nazwa dziennika: System
Źródło: Eventlog
Zalogowano: 04.02.2021 18:48:58
Identyfikator 104
Kategoria zadania: Czyszczenie dziennika
Poziom: Informacje
Słowa kluczowe:
Użytkownik: WIN10VB\Paweł Pasternak
Komputer: WIN10VB
Kod operacji: Informacje
Więcej informacji: Pomoc online dziennika
POL
18:49
04.02.2021

- Zaimportować dziennik - w którym miejscu znajduje się dziennik po importowaniu



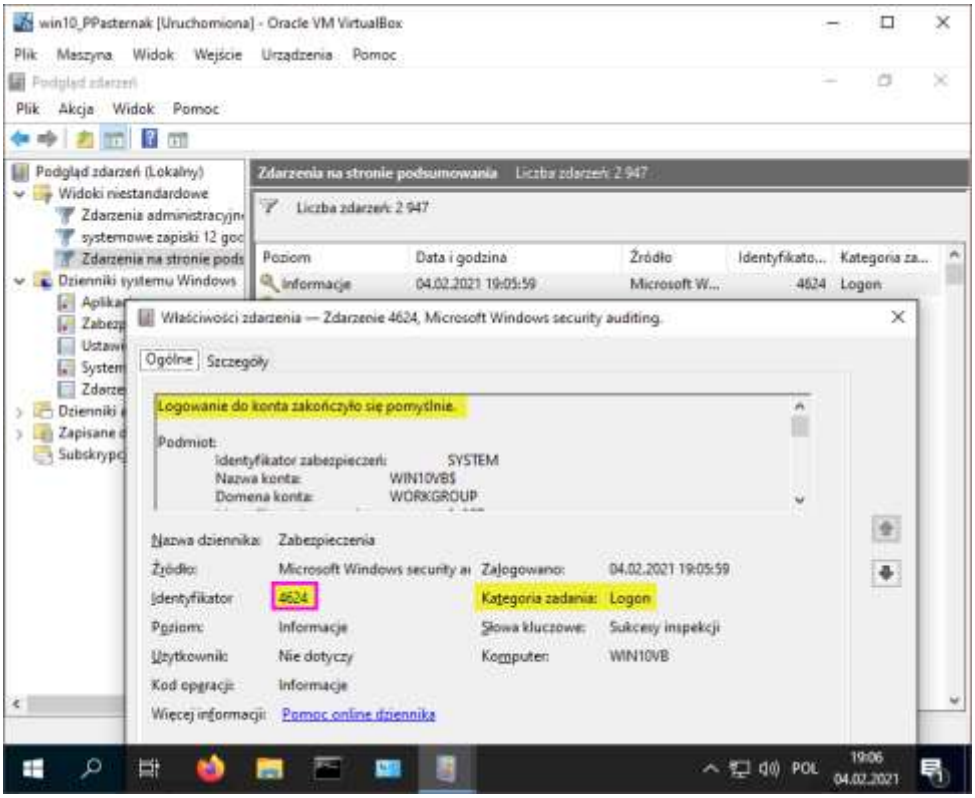




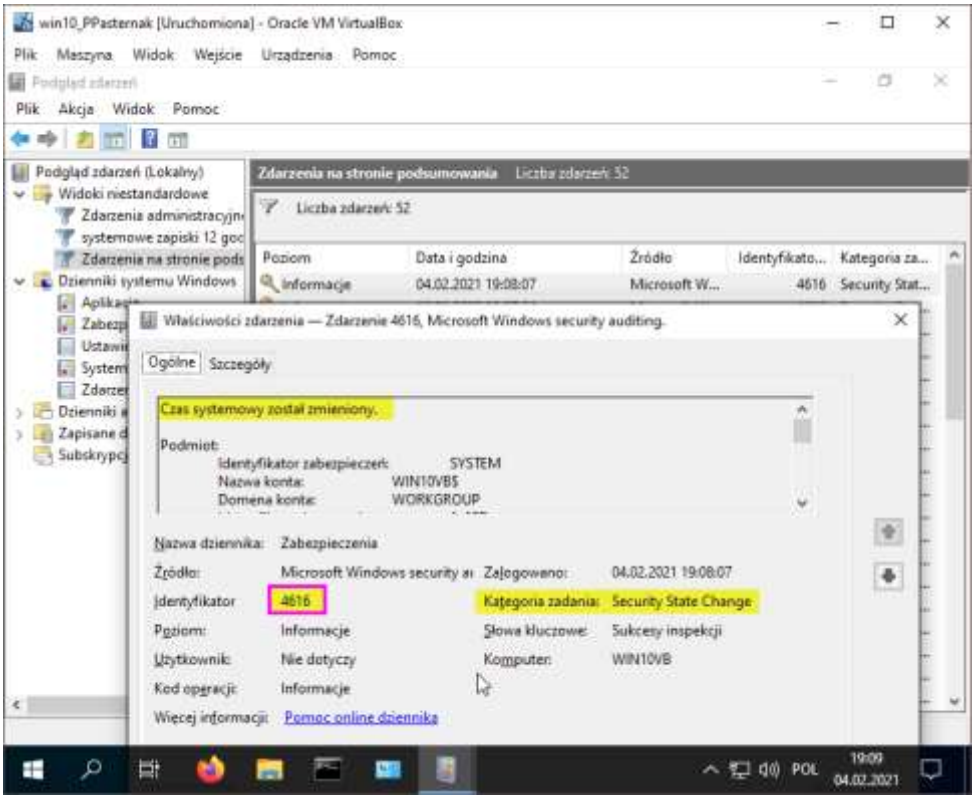
Po zaimportowaniu dziennik znajduje się w zapisanych dziennikach, a nie w oryginalnej lokalizacji.

7. Wykaż jaki jest numer identyfikatora dla takich zdarzeń jak

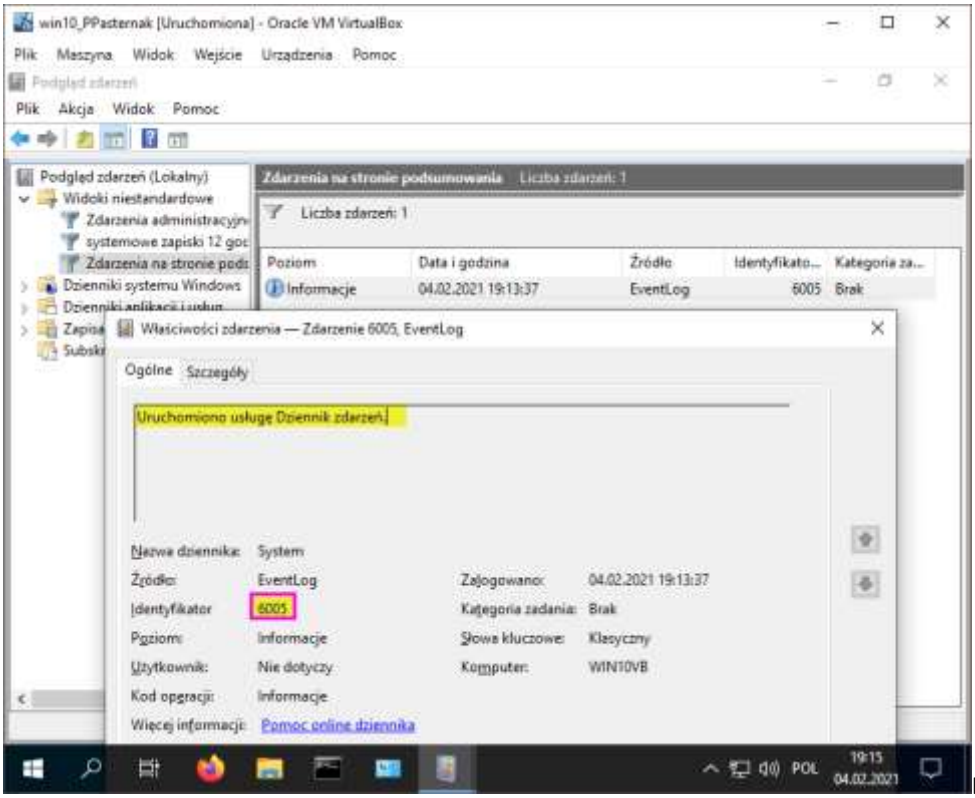
- Sukces- zalogowania się na koncie - **4624**



- Zmiana czasu systemowego - **4616**

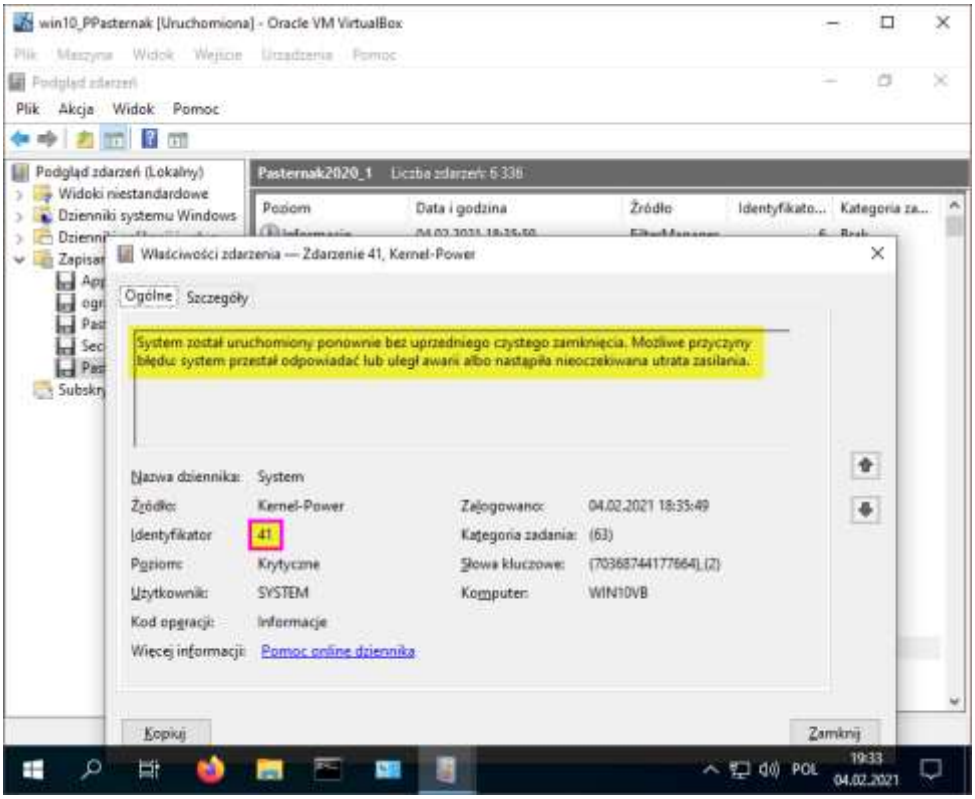


- Uruchamianie systemu Windows - **6005**

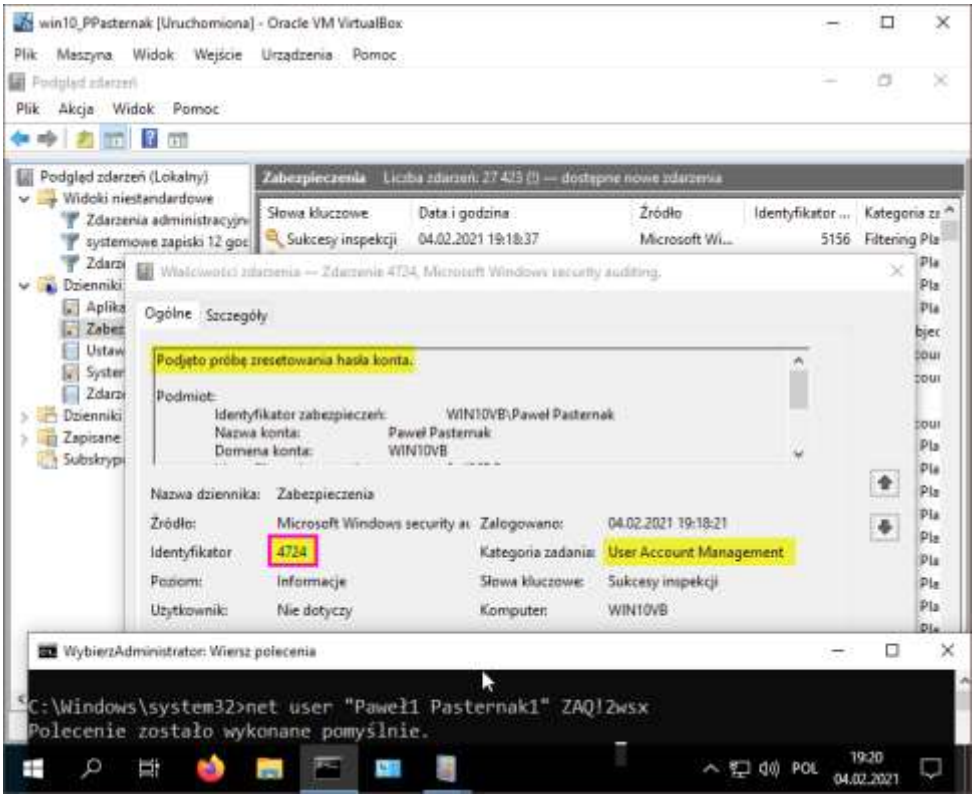


Dziennik zadań uruchamia się zaraz po uruchomieniu komputera.

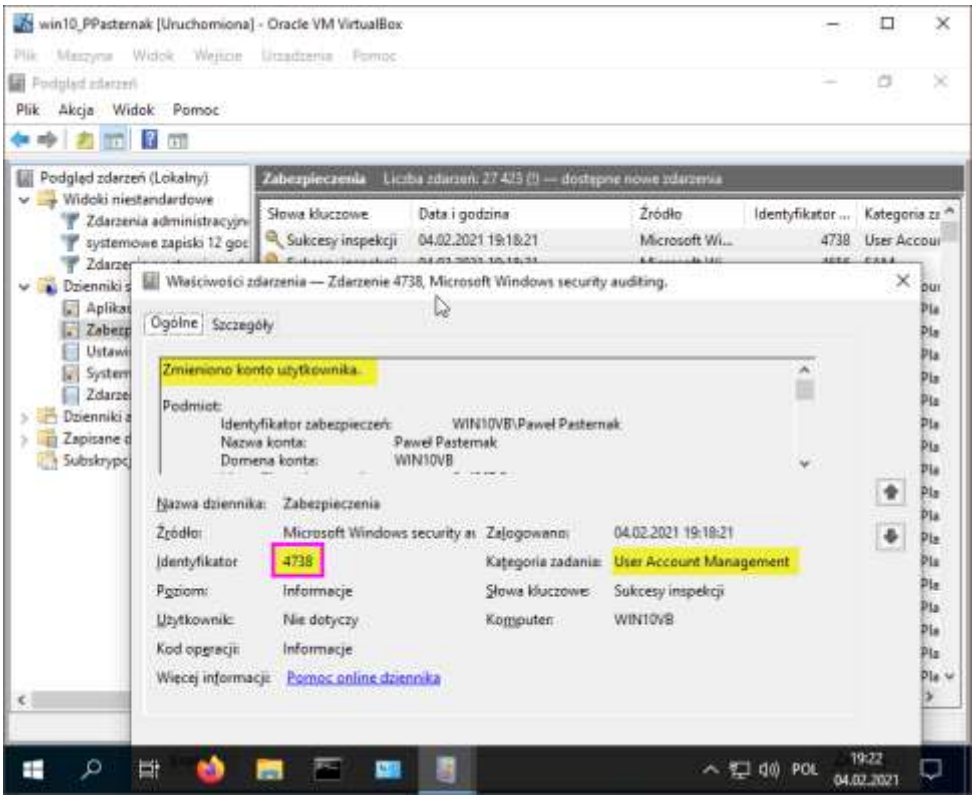
- Nieprawidłowe wyłączenie komputera - **41**



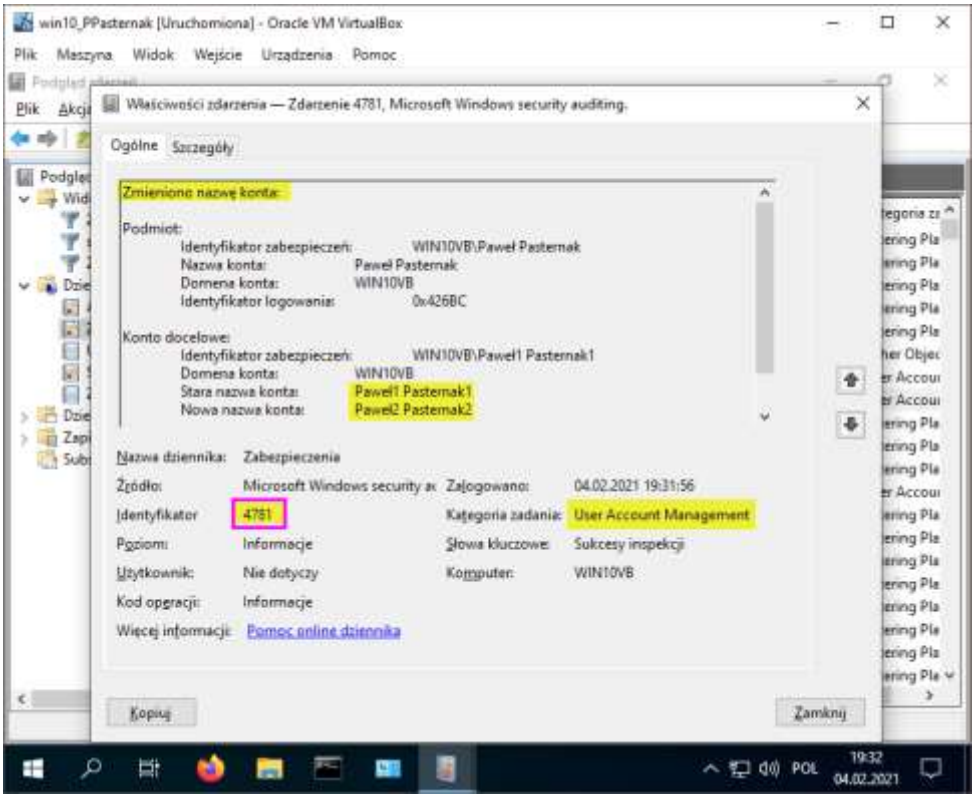
- Podjęcie próby zresetowania hasła - **4724**



- Zmieniono konto użytkownika - **4738**

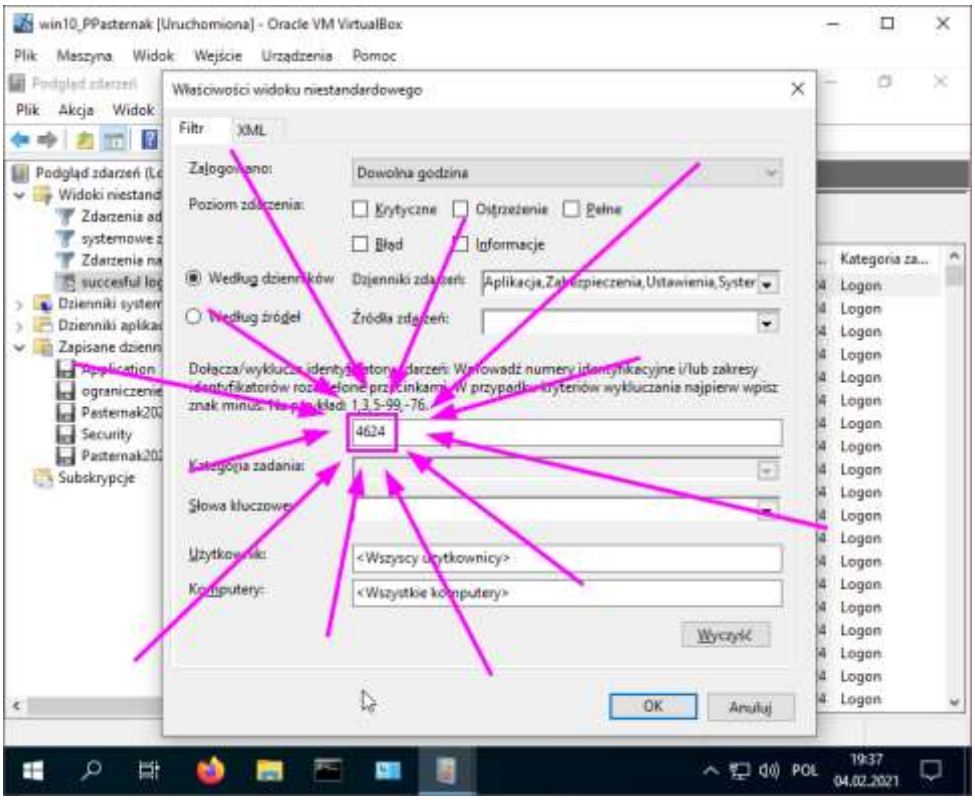


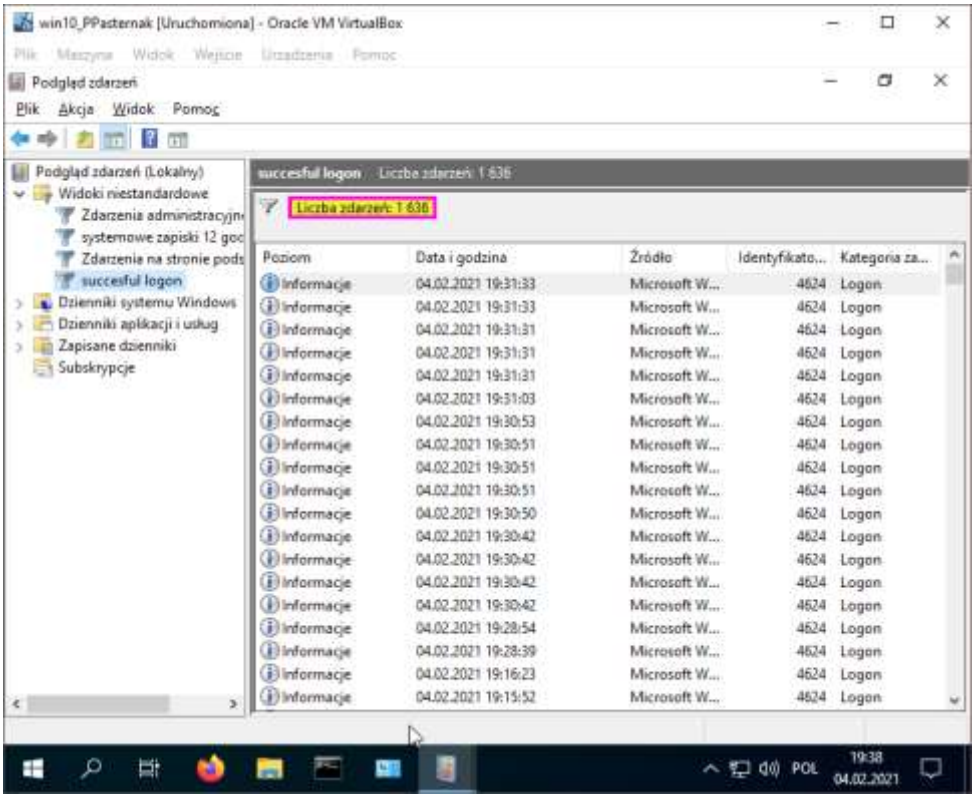
- Zmieniono nazwę konta - **4781**



8. Określ ile razy zarejestrowano sukces w logowaniu się na koncie od początku rejestrowania zdarzeń

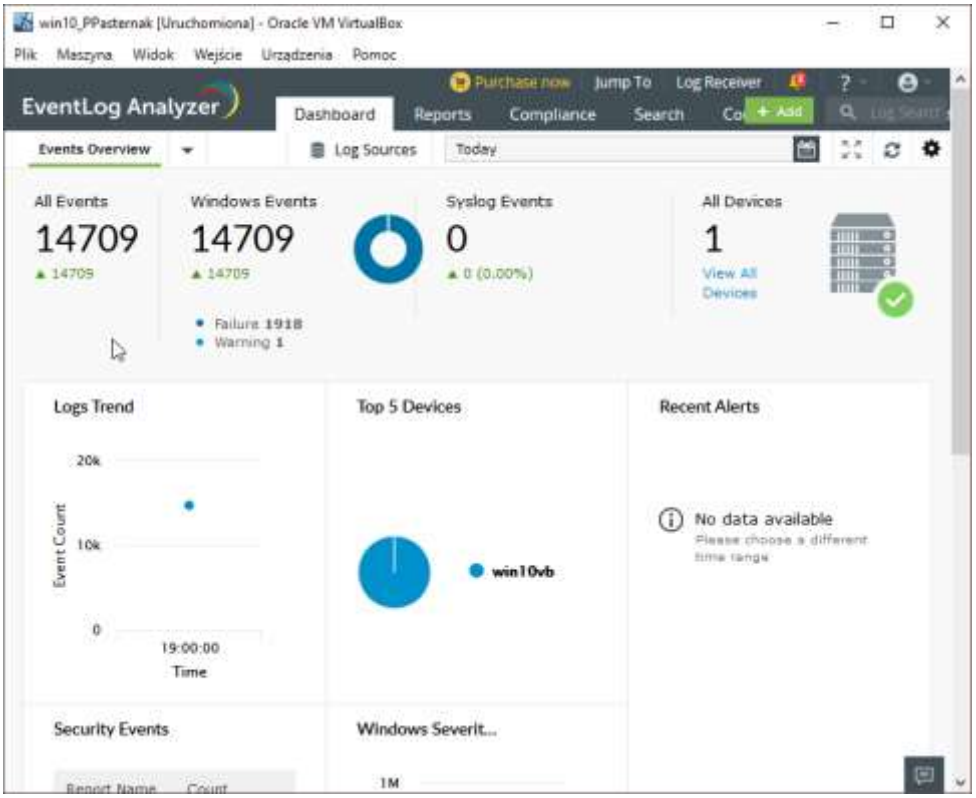
Od początku rejestrowania zdarzeń zalogowałem się 1636 razy 😁



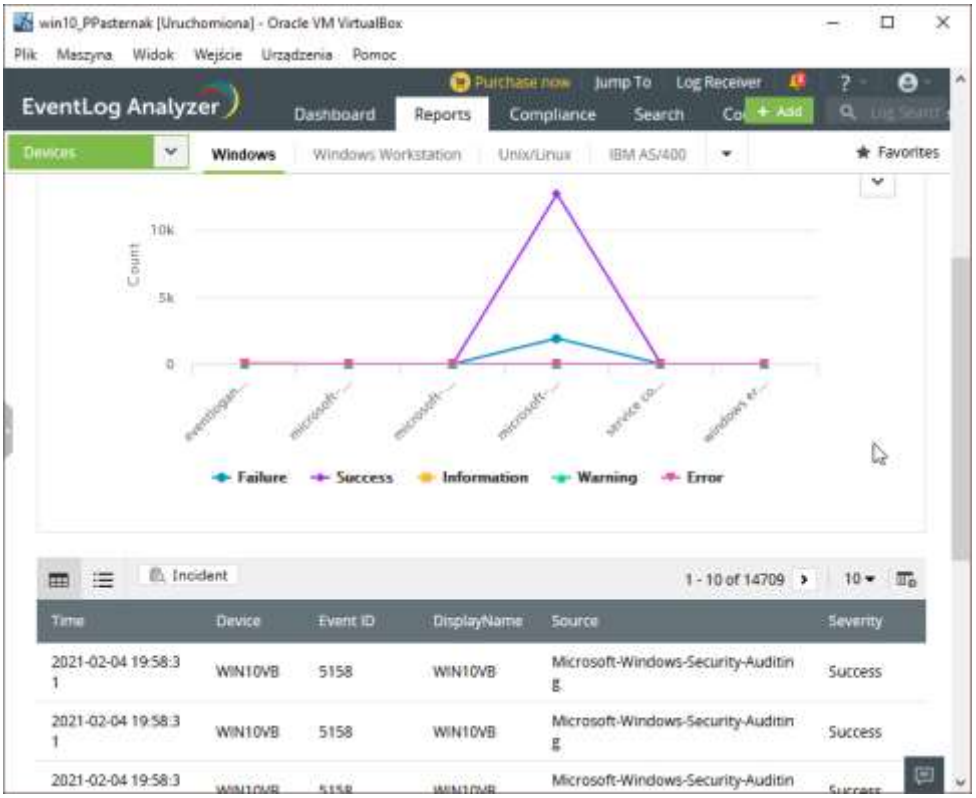


9. Znajdź 5 programów (pokaż ich działanie) które służą do zestawień, raportów dot zdarzeń systemowych, logów

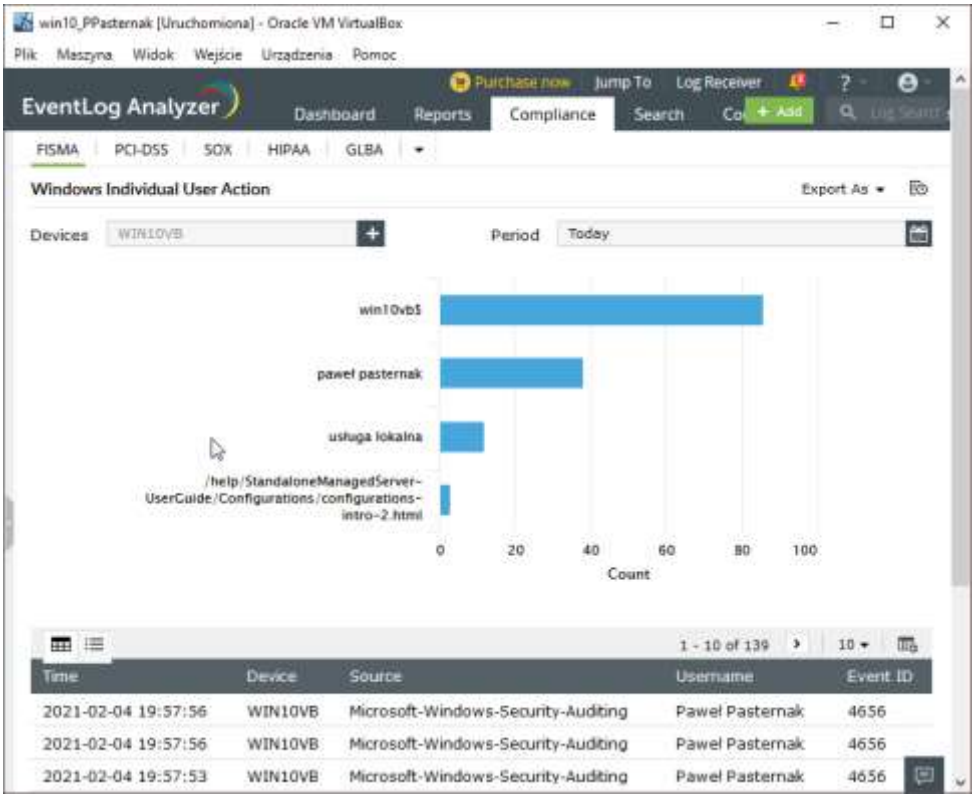
- EventLog Analyzer



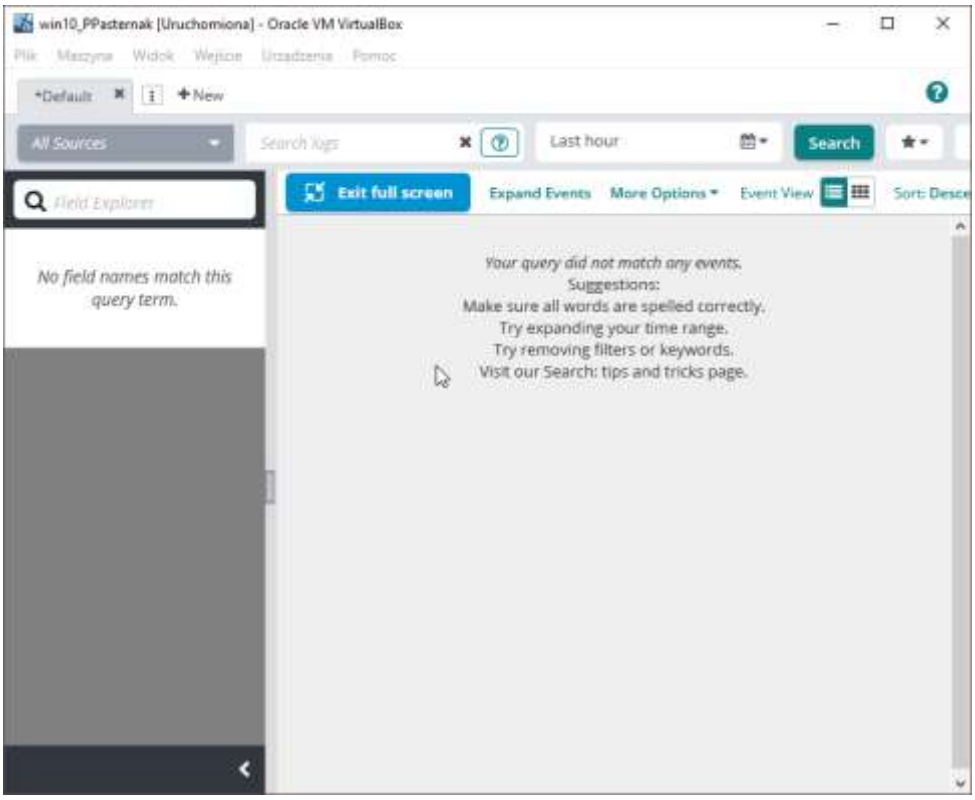
Raport

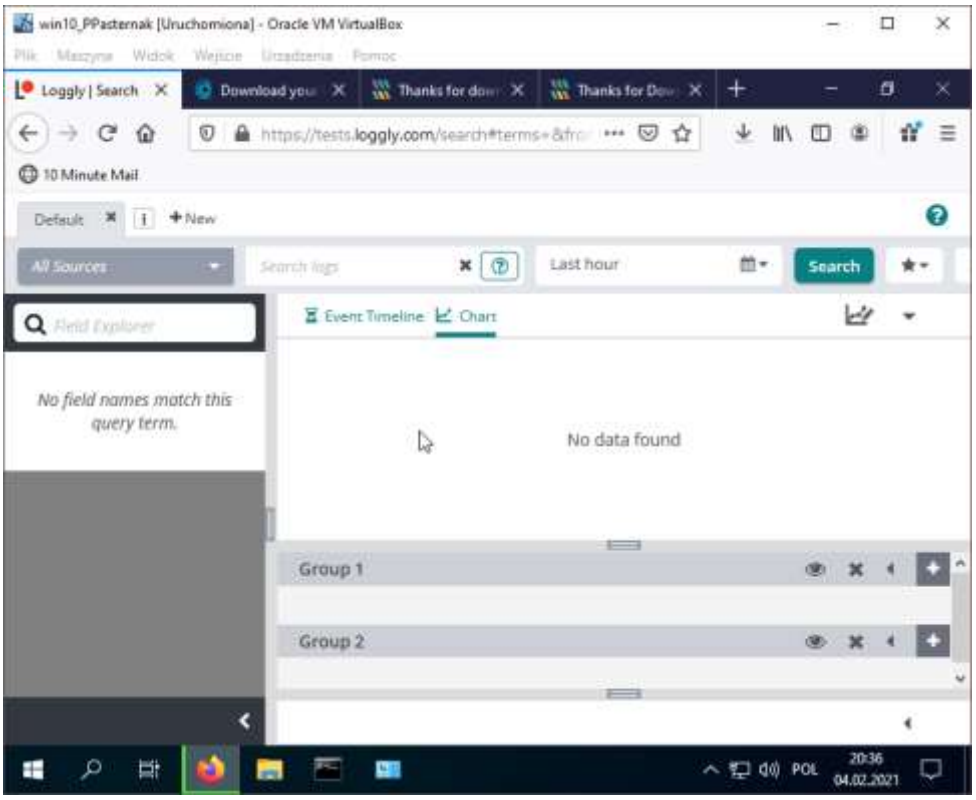


Zestawienie



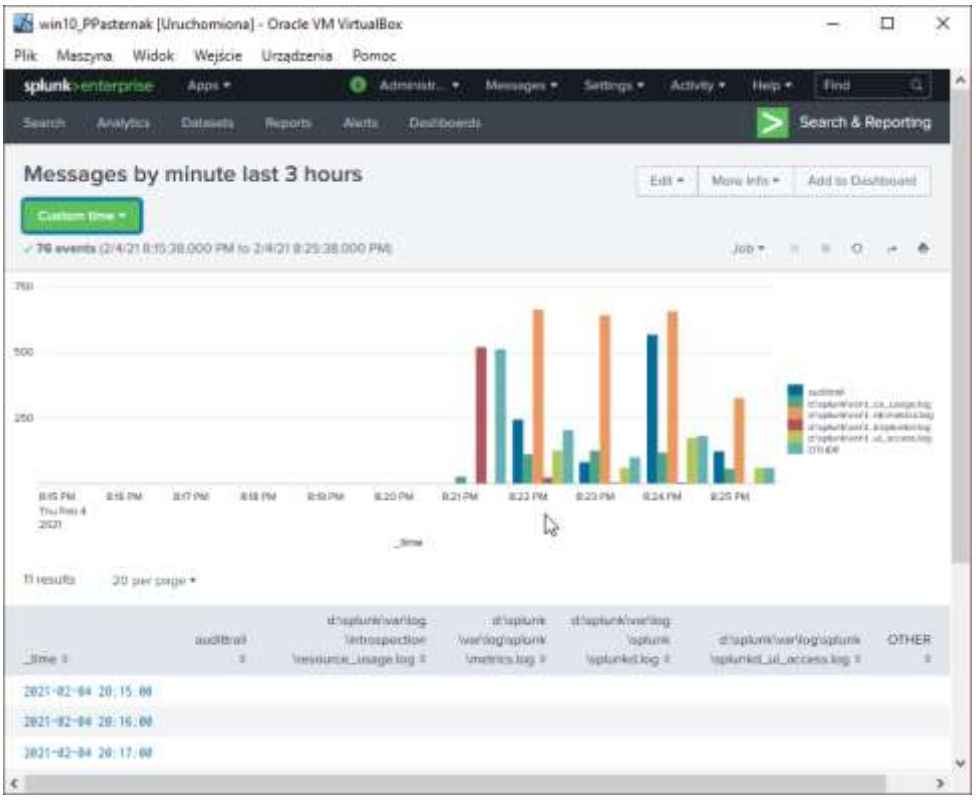
- Loggly



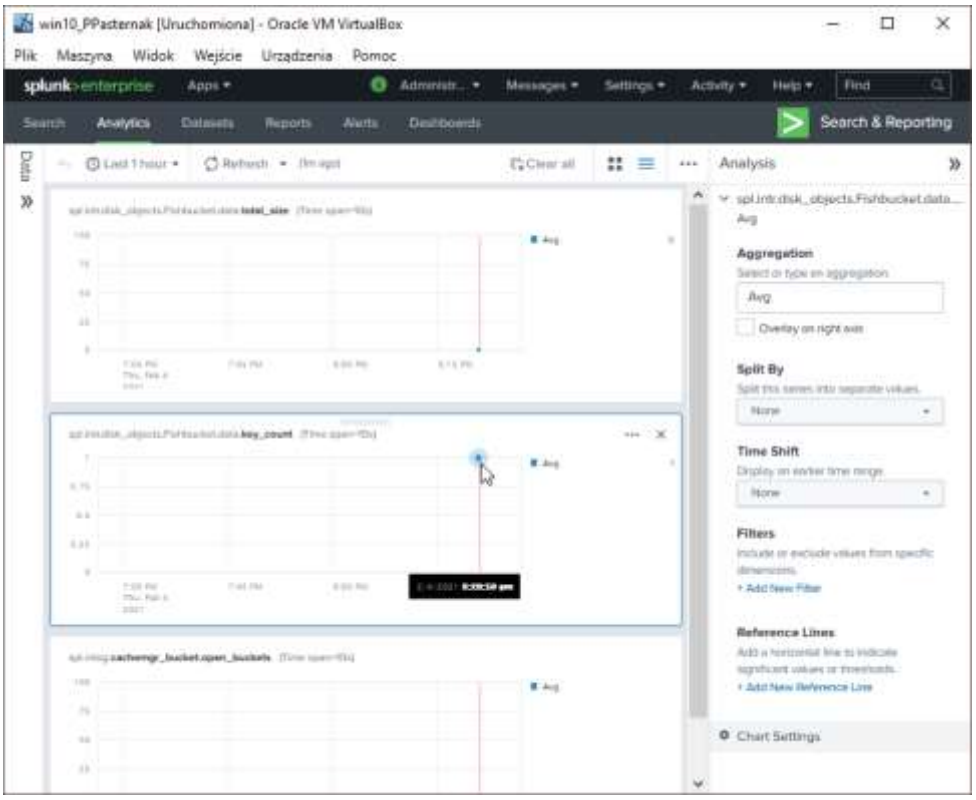


- Splunk

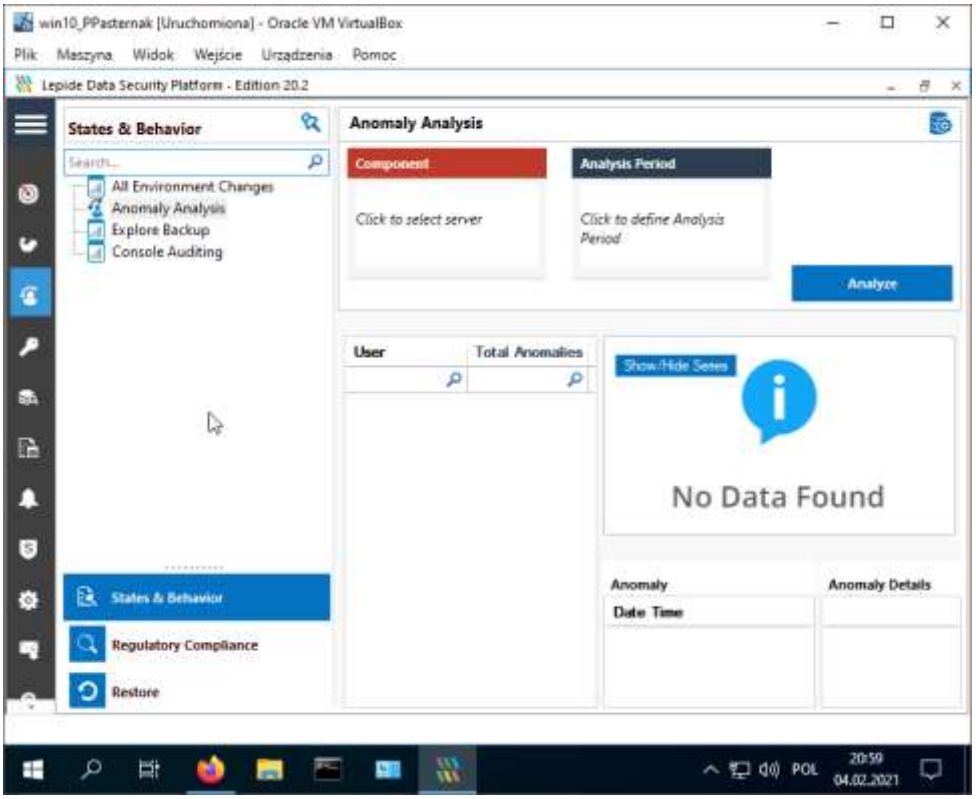
Raport

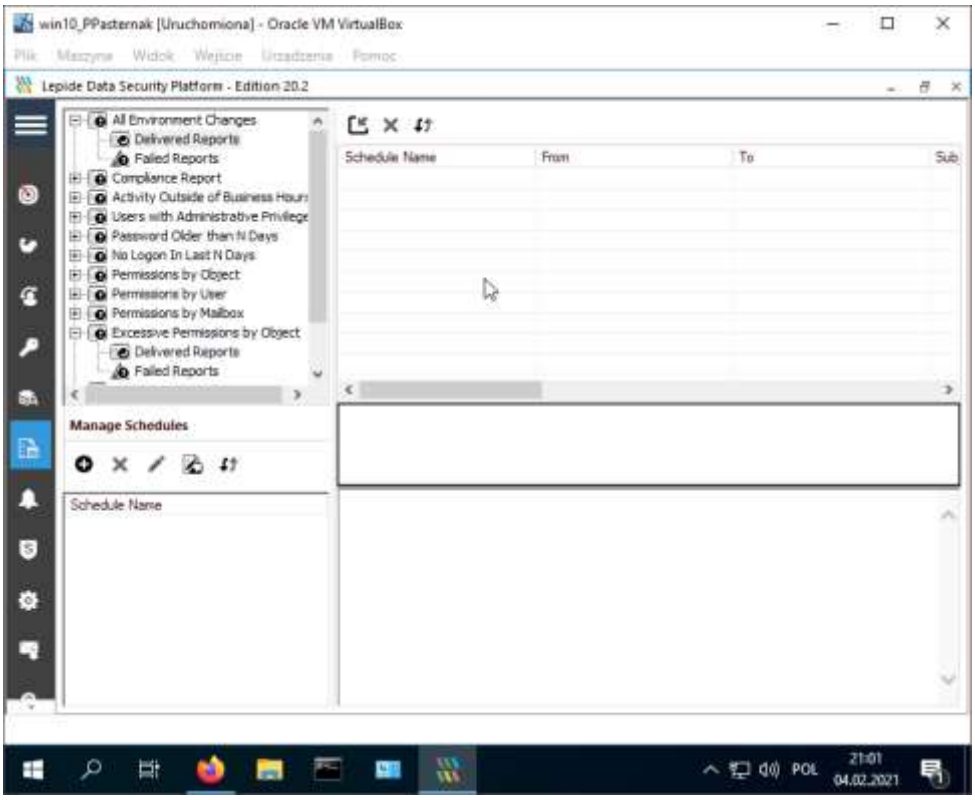


Analiza

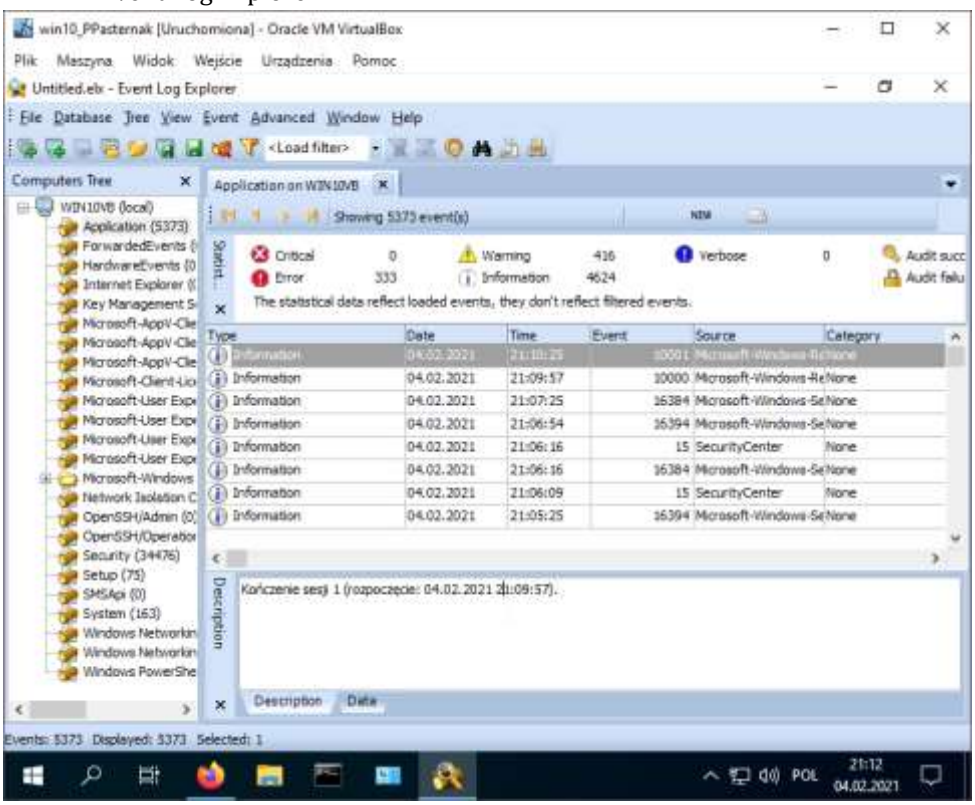

win10_PPasternak [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc
splunk>enterprise
Search & Reporting
Analysis
Aggregation
Split By
Time Shift
Filters
Reference Lines
Chart Settings

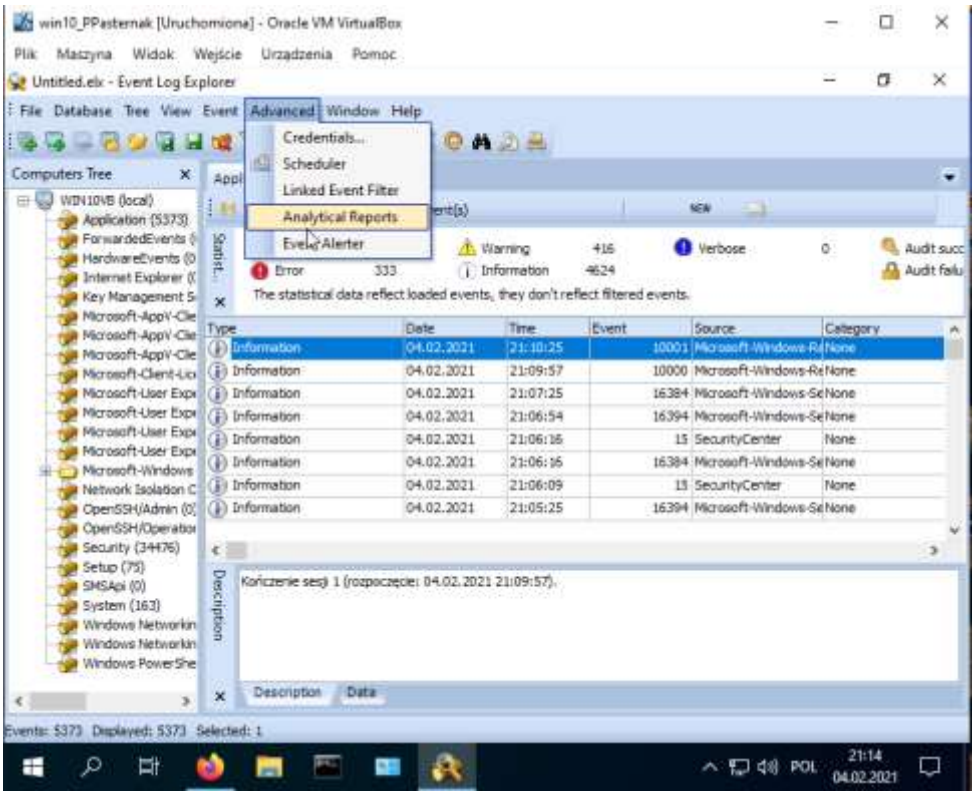
- Lepide

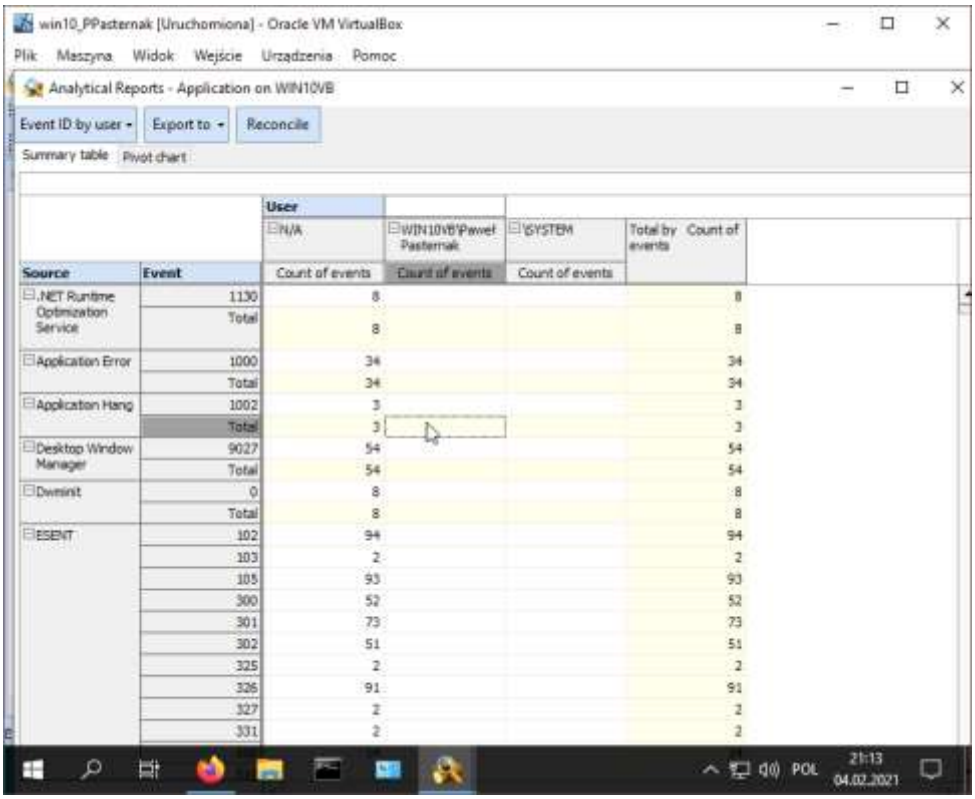

win10_PPasternak [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc
Lepide Data Security Platform - Edition 20.2
States & Behavior
All Environment Changes
Anomaly Analysis
Explore Backup
Console Auditing
Anomaly Analysis
Component
Click to select server
Analysis Period
Click to define Analysis Period
Analyze
User
Total Anomalies
Show/Hide Series
No Data Found
Anomaly
Date Time
Anomaly Details
States & Behavior
Regulatory Compliance
Restore
POL
20:59
04.02.2021



- Event Log Explorer




win10_PPasternak [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc
Untitled.elx - Event Log Explorer
File Database Tree View Event Advanced Window Help
Credentials...
Scheduler
Linked Event Filter
Analytical Reports
Event Alerter
Computers Tree
WIN10VB (local)
Application (5373)
Warning 416
Verbose 0
Error 333
Information 4624
The statistical data reflect loaded events, they don't reflect filtered events.
Type Date Time Event Source Category
Information 04.02.2021 21:10:25 10001 Microsoft-Windows-R None
Information 04.02.2021 21:09:57 10000 Microsoft-Windows-Re None
Information 04.02.2021 21:07:25 16384 Microsoft-Windows-Se None
Information 04.02.2021 21:06:54 16394 Microsoft-Windows-Se None
Information 04.02.2021 21:06:16 15 SecurityCenter None
Information 04.02.2021 21:06:16 16384 Microsoft-Windows-Se None
Information 04.02.2021 21:06:09 15 SecurityCenter None
Information 04.02.2021 21:05:25 16394 Microsoft-Windows-Se None
Description
Kończenie sesji 1 (rozpoczęcie: 04.02.2021 21:09:57).
Description Data
Events: 5373 Displayed: 5373 Selected: 1
POL 21:14 04.02.2021


win10_PPasternak [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc
Analytical Reports - Application on WIN10VB
Event ID by user
Export to
Reconcile
Summary table Pivot chart
User
N/A
WIN10VB\Paweł Pasternak
\SYSTEM
Total by Count of events
Source Event Count of events Count of events Count of events
.NET Runtime Optimization Service 1130 8 8
Total 8 8
Application Error 1000 34 34
Total 34 34
Application Hang 1002 3 3
Total 3 3
Desktop Window Manager 9027 54 54
Total 54 54
Dwminit 0 8 8
Total 8 8
ESENT 102 94 94
103 2 2
105 93 93
300 52 52
301 73 73
302 51 51
325 2 2
326 91 91
327 2 2
331 2 2
POL 21:13 04.02.2021

10. Czy istnieje potrzeba archiwizowania danych z dziennika - uzasadnij swoją decyzję

Według mnie archiwizowanie danych z dziennika zdarzeń może być bardzo przydatne. Pozwoli ono w razie, np. uszkodzenia danych lub ich zaszyfrowania, na sprawdzenie co lub kto majstrował przy naszym komputerze, a w dodatku kiedy. Umożliwi ono też porównanie danych z różnych okresów czasu, itd…