

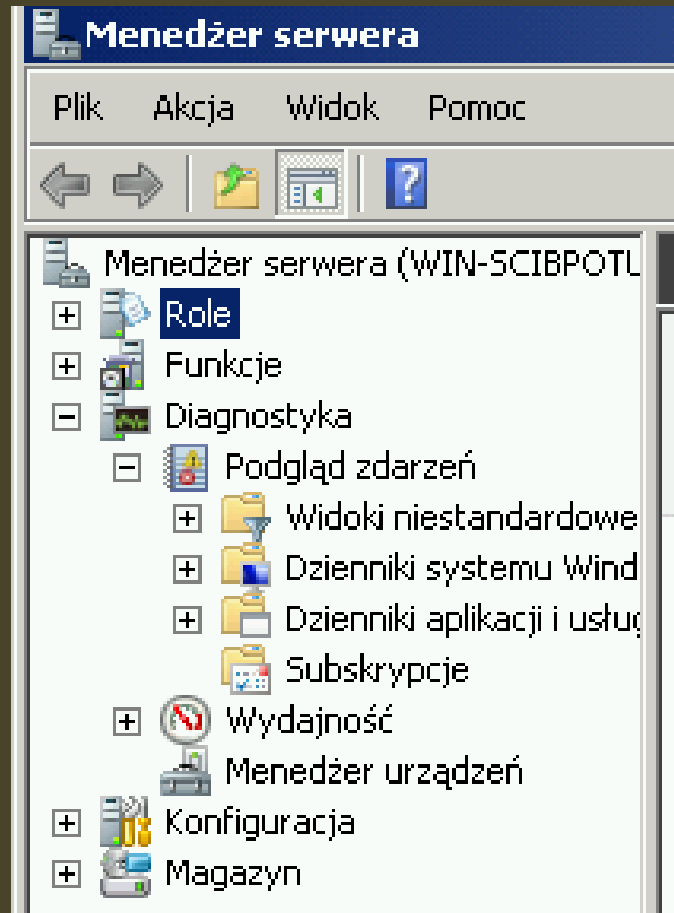
**Inspekcja systemu
(Windows Server 2008R2)
Dziennik zdarzeń**



Po co dziennik zdarzeń?

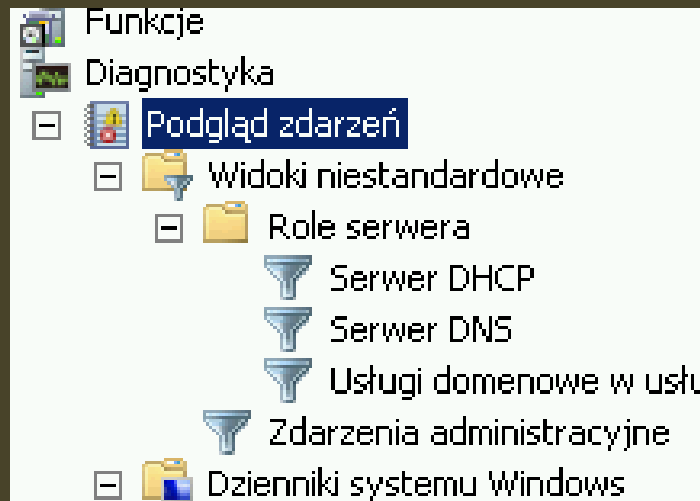
- wiedza na temat tego co dzieje się w systemie
- bezpieczeństwo
- zapobieganie awariom
-jakieś pomysły....?

Dziennik zdarzeń



Menedżer serwera -> Diagnostyka -> Podgląd zdarzeń

Dziennik zdarzeń – role serwera



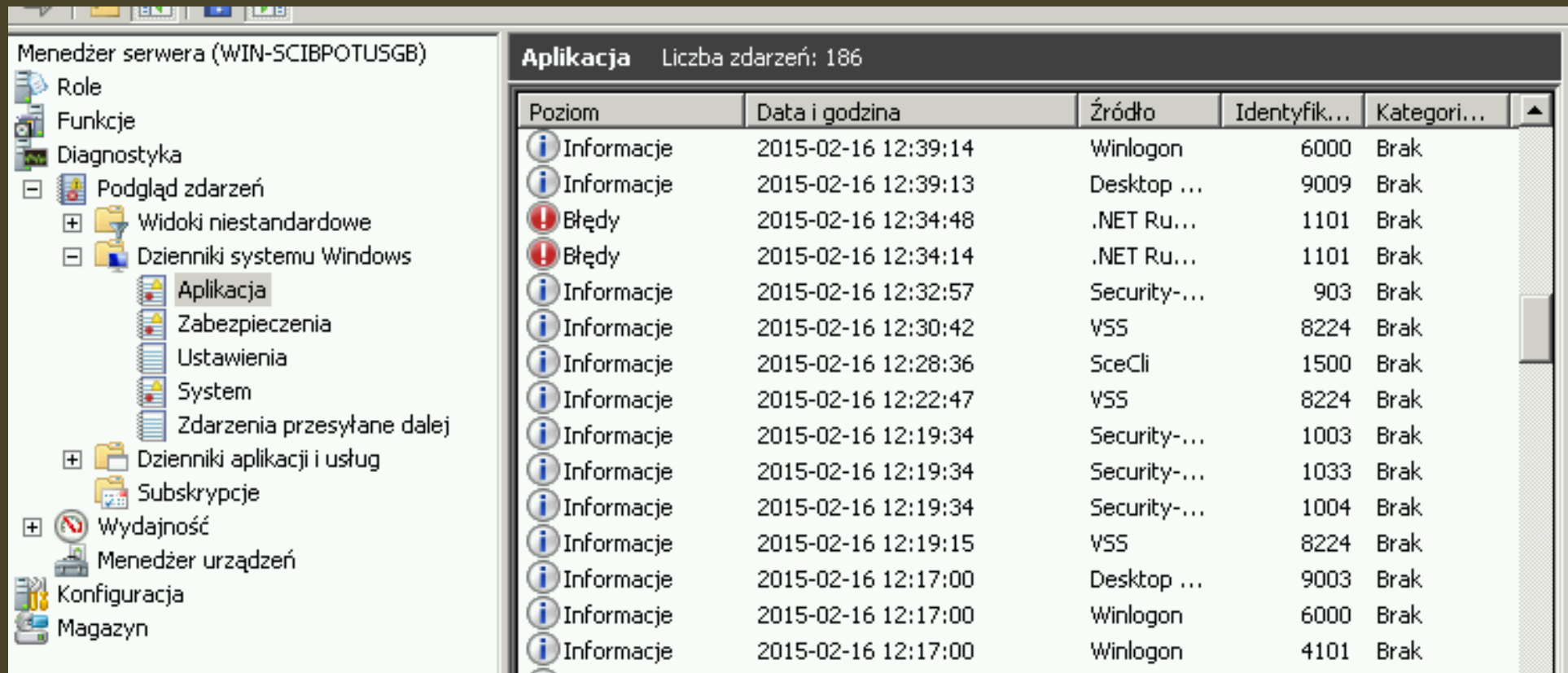
edźer serwera (WIN-SCIBPOTUSGB)
Role
Funkcje
Diagnostyka
Podgląd zdarzeń
Widoki niestandardowe
Role serwera
Serwer DHCP
Serwer DNS
Usługi domenowe w usługach
Zdarzenia administracyjne

Serwer DHCP Liczba zdarzeń: 6

Liczba zdarzeń: 6

Poziom	Data i godzina	Źródło	Identyfik...	Kategori...
Informacje	2015-02-16 12:47:38	DHCP-Se...	1044	Brak
Błędy	2015-02-16 12:47:38	DHCP-Se...	1059	Brak
Błędy	2015-02-16 12:47:38	DHCP-Se...	1046	Brak
Błędy	2015-02-16 12:47:38	DHCP-Se...	1059	Brak
Ostrzeżenia	2015-02-16 12:47:38	DHCP-Se...	10020	Brak
Ostrzeżenia	2015-02-16 12:47:38	DHCP-Se...	1056	Brak
















Dziennik zdarzeń – dziennik systemu Windows



Menedżer serwera (WIN-SCIBPOTUSGB)

- Role
- Funkcje
- Diagnostyka
 - Podgląd zdarzeń
 - Widoki niestandardowe
 - Dzienniki systemu Windows
 - Aplikacja**
 - Zabezpieczenia
 - Ustawienia
 - System
 - Zdarzenia przesyłane dalej
 - Dzienniki aplikacji i usług
 - Subskrypcje
 - Wydajność
 - Menedżer urządzeń
- Konfiguracja
- Magazyn

Aplikacja Liczba zdarzeń: 186

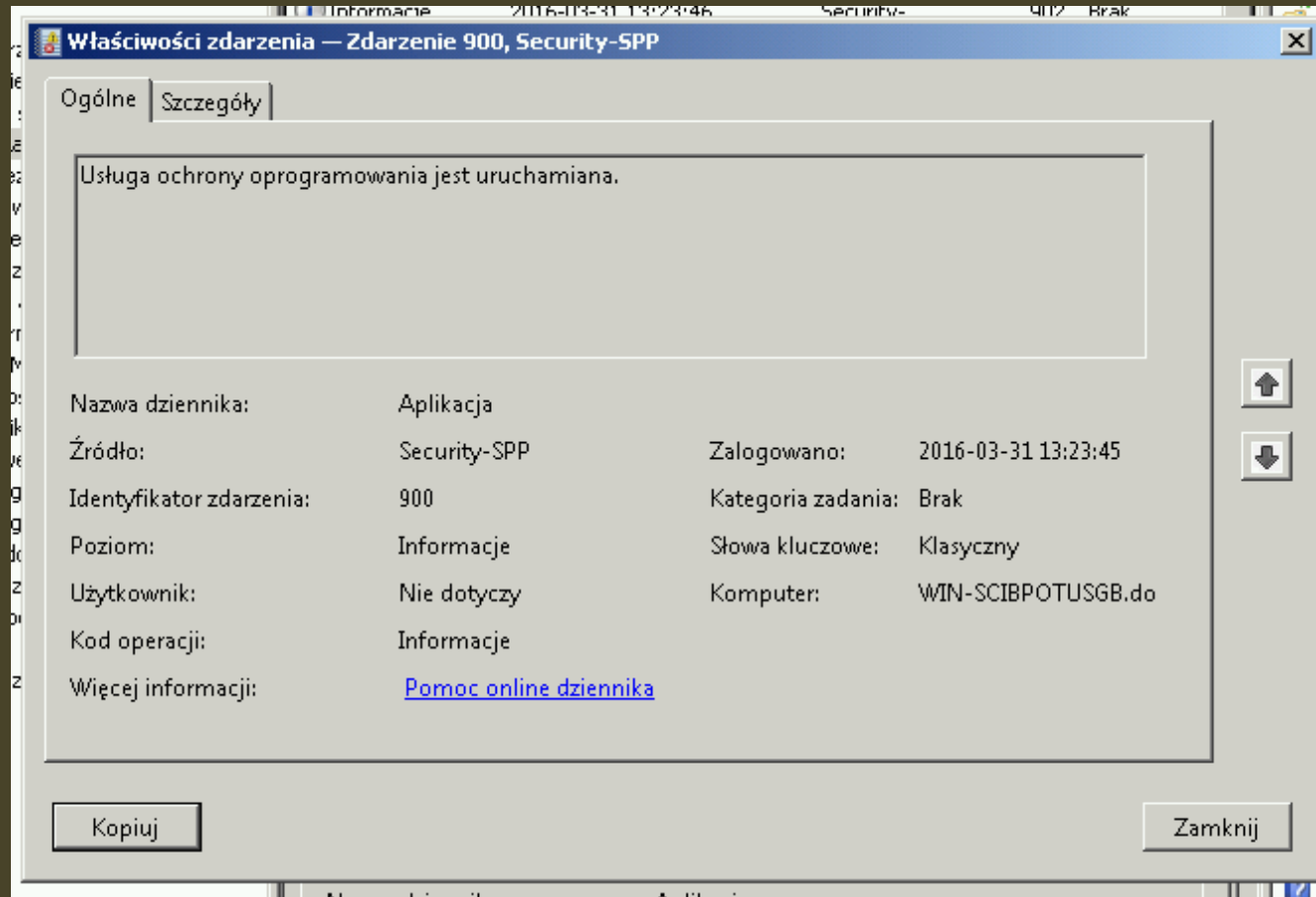
Poziom	Data i godzina	Źródło	Identyfik...	Kategori...
 Informacje	2015-02-16 12:39:14	Winlogon	6000	Brak
 Informacje	2015-02-16 12:39:13	Desktop ...	9009	Brak
 Błędy	2015-02-16 12:34:48	.NET Ru...	1101	Brak
 Błędy	2015-02-16 12:34:14	.NET Ru...	1101	Brak
 Informacje	2015-02-16 12:32:57	Security-...	903	Brak
 Informacje	2015-02-16 12:30:42	VSS	8224	Brak
 Informacje	2015-02-16 12:28:36	SceCli	1500	Brak
 Informacje	2015-02-16 12:22:47	VSS	8224	Brak
 Informacje	2015-02-16 12:19:34	Security-...	1003	Brak
 Informacje	2015-02-16 12:19:34	Security-...	1033	Brak
 Informacje	2015-02-16 12:19:34	Security-...	1004	Brak
 Informacje	2015-02-16 12:19:15	VSS	8224	Brak
 Informacje	2015-02-16 12:17:00	Desktop ...	9003	Brak
 Informacje	2015-02-16 12:17:00	Winlogon	6000	Brak
 Informacje	2015-02-16 12:17:00	Winlogon	4101	Brak

Dziennik zdarzeń – dziennik aplikacji i usług

The screenshot displays the Windows Event Viewer interface. The left-hand navigation pane shows the tree structure: 'Menedżer serwera (WIN-SCIBPOTUSGB)' > 'Diagnostyka' > 'Dzienniki aplikacji i usług' > 'Internet Explorer'. The main pane shows a table with the following columns: 'Poziom', 'Data i godzina', 'Źródło', 'Identyfik...', and 'Kategori...'. The table is currently empty, with a status bar at the top indicating 'Liczba zdarzeń: 0'. On the right side, there is a vertical 'Akcje' (Actions) pane with various icons for filtering and viewing events.

Poziom	Data i godzina	Źródło	Identyfik...	Kategori...
--------	----------------	--------	--------------	-------------

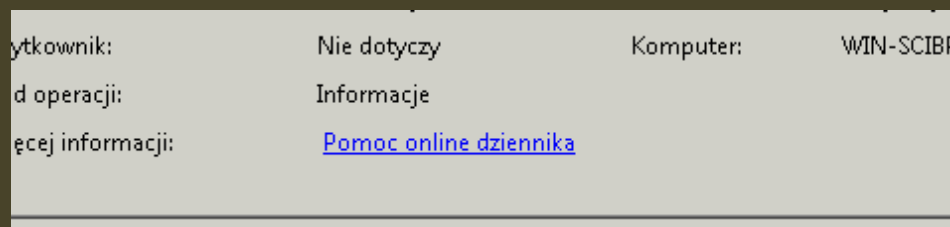
Dziennik zdarzeń – interpretacja wyników



Ogólne informacje o zdarzeniu

Dziennik zdarzeń – interpretacja wyników

Jeśli zachodzi potrzeba rozwiązania błędu, który się pojawia cyklicznie, a sam opis nic nam nie mówi, zawsze można skorzystać z pomocy online dziennika lub google'a...

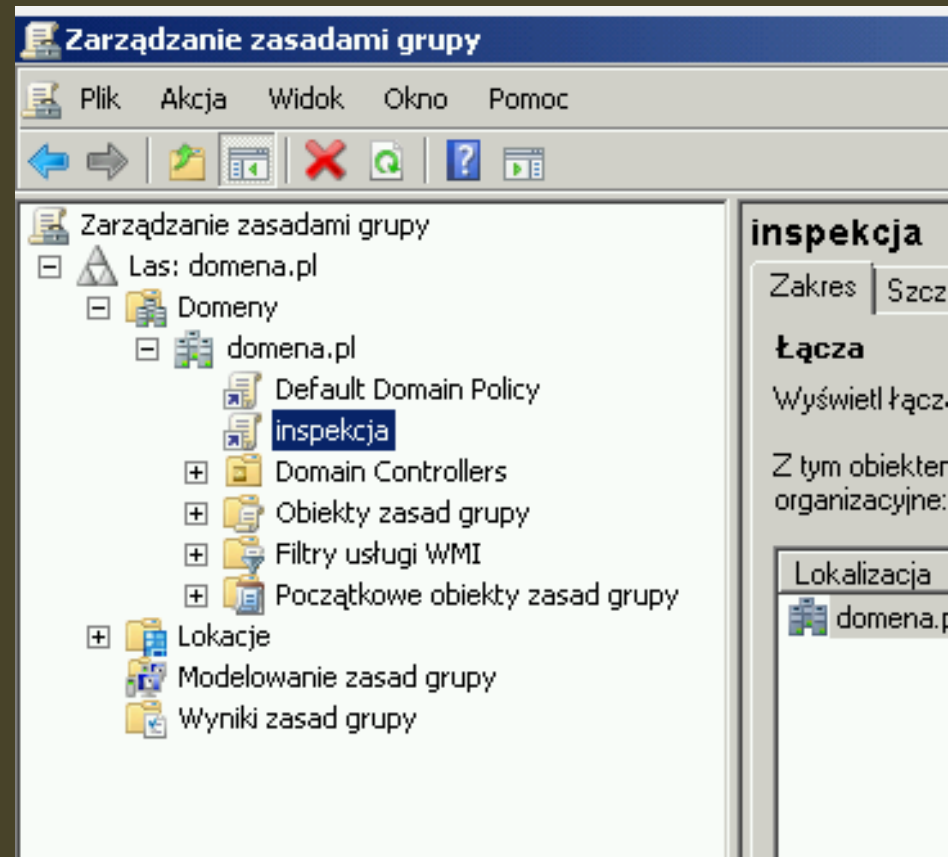


Warto pamiętać szukając informacji o błędzie w Google o tym, że istotne są: **Nazwa dziennika**, **Źródło** oraz **Identyfikator zdarzenia**

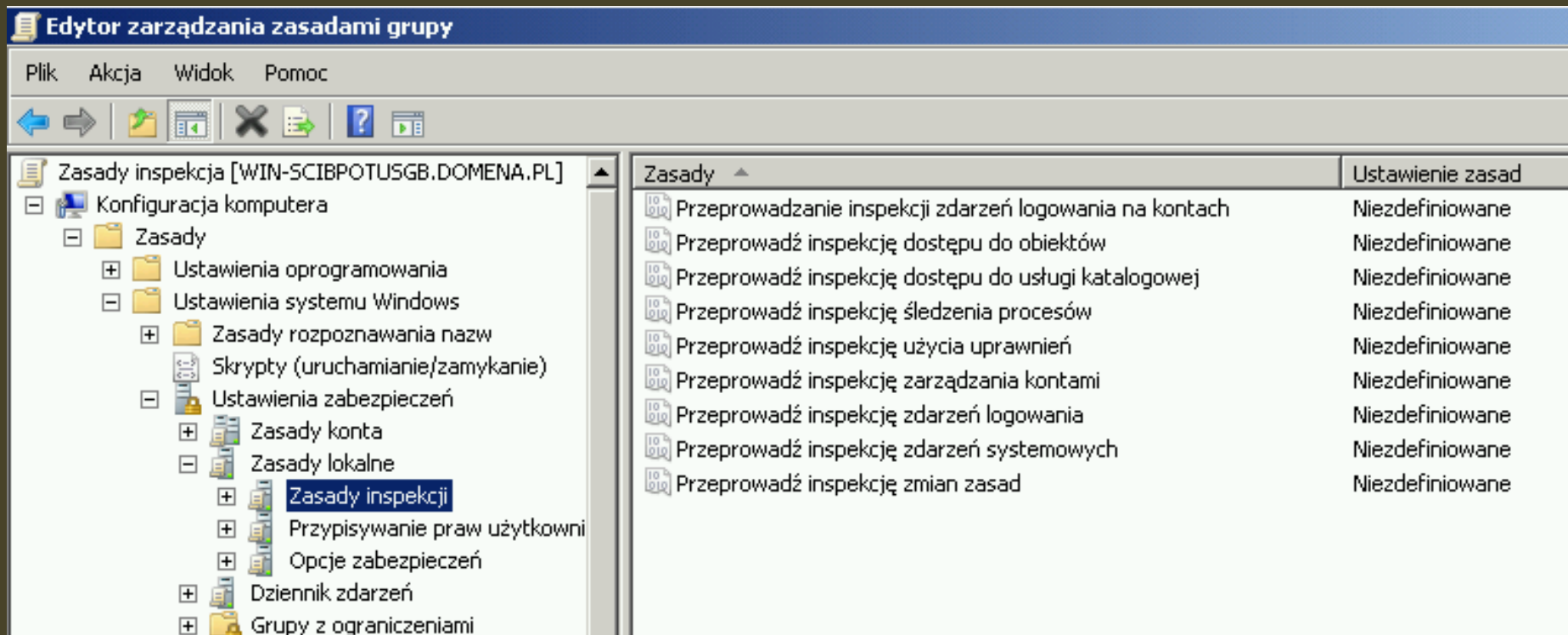
Pytanie: Jak konfigurować inspekcje?

Odpowiedź: GPO...

**Warto utworzyć na okoliczność
każdej z opcji inspekcji osobny
obiekt lub jeden wspólny dla
wszystkich zasad inspekcji
(kwestia gustu) – wiele obiektów
dla poszczególnych elementów
inspekcji dają większą kontrolę.**



Jeśli mamy już obiekt GPO można go wymedytować:



Konfiguracja komputera -> Ustawienia systemu Windows ->
Ustawienia zabezpieczeń -> Zasady inspekcji

Przeprowadź inspekcję zdarzeń logowania na kontach

To ustawienie zabezpieczeń określa, czy każda weryfikacja poświadczeń konta na tym komputerze ma być poddawana inspekcji w systemie operacyjnym.

Jeśli to ustawienie zasad jest zdefiniowane, administrator może określić, czy inspekcji mają być poddawane wyłącznie sukcesy, wyłącznie niepowodzenia, zarówno sukcesy, jak i niepowodzenia, czy te zdarzenia wcale nie będą poddawane inspekcji (ani sukcesy, ani niepowodzenia).

Przeprowadź inspekcję dostępu do obiektów

To ustawienie zabezpieczeń określa, czy próby uzyskania dostępu przez użytkownika do obiektów spoza usługi Active Directory mają być poddawane inspekcji w systemie operacyjnym. Inspekcja jest generowana jedynie w przypadku obiektów, dla których określono systemowe listy kontroli dostępu (SACL), i tylko wtedy, gdy typ żądanego dostępu (np. zapis, odczyt lub modyfikacja) oraz konto zgłaszające żądanie są zgodne z ustawieniami na liście SACL.

Przeprowadź inspekcję dostępu do usługi katalogowej

To ustawienie zabezpieczeń określa, czy próby uzyskania dostępu przez użytkownika do obiektów usługi Active Directory mają być poddawane inspekcji w systemie operacyjnym.

Przeprowadź inspekcję śledzenia procesów

To ustawienie zabezpieczeń określa, czy zdarzenia związane z procesami, takie jak utworzenie procesu, zakończenie procesu, duplikacja uchwytu i pośredni dostęp do obiektu, mają być poddawane inspekcji w systemie operacyjnym.

Przeprowadź inspekcję użycia uprawnień

To ustawienie zabezpieczeń określa, czy każdy przypadek skorzystania z prawa użytkownika ma być poddawany inspekcji.

Przeprowadź inspekcję zarządzania kontami

To ustawienie zabezpieczeń określa, czy każde zdarzenie zarządzania kontami na komputerze ma być poddawane inspekcji.

Przykłady zdarzeń zarządzania kontami są następujące:

Utworzenie, zmiana lub usunięcie konta użytkownika lub grupy. Zmiana nazwy, wyłączenie lub włączenie konta użytkownika. Ustawienie lub zmiana hasła.

Przeprowadź inspekcję zdarzeń logowania

To ustawienie zabezpieczeń określa, czy każda próba zalogowania się na tym komputerze lub wylogowania się podjęta przez użytkownika ma być poddawana inspekcji w systemie operacyjnym.

Przeprowadź inspekcję zdarzeń systemowych

To ustawienie zabezpieczeń określa, czy następujące zdarzenia mają być poddawane inspekcji w systemie operacyjnym:

- **Próba zmiany czasu systemowego**
- **Próba uruchomienia lub zamknięcia systemu zabezpieczeń**
- **Próba załadowania składników uwierzytelniania rozszerzonego**
- **Utrata zdarzeń poddawanych inspekcji z powodu awarii systemu inspekcji**
- **Rozmiar dziennika zabezpieczeń przekraczający skonfigurowany próg ostrzegawczy**

Przeprowadź inspekcję zmian zasad

To ustawienie zabezpieczeń określa, czy każda próba zmiany zasad przypisywania praw użytkownika, zasad inspekcji, zasad konta lub zasad zaufania ma być poddawana inspekcji w systemie operacyjnym.


Dodatkowo w GPO można definiować zaawansowane zasady inspekcji

The screenshot shows the Windows Group Policy Editor interface. On the left, the tree view is expanded to 'Zasady inspekcji systemu — lokalne'. The right pane shows the configuration for 'Logowanie na kontach' (Logon on accounts), which is currently set to 'Nie skonfigurowano' (Not configured).

Konfiguracja

Wprowadzenie

Ustawienia konfiguracji zaawansowanych zasad inspekcji umożliwiają skutecznych ataków na sieć i zasoby użytkownika oraz sprawdzanie zgodności.

 Jeśli używane są ustawienia konfiguracji zaawansowanych zasad inspekcji, system Windows V wymusi ustawienia podkategorii zasad inspekcji (system Windows V ścieżce Zasady lokalne/Opcje zabezpieczeń).

[Wiecej informacji](#)

[Które wersje systemu](#)

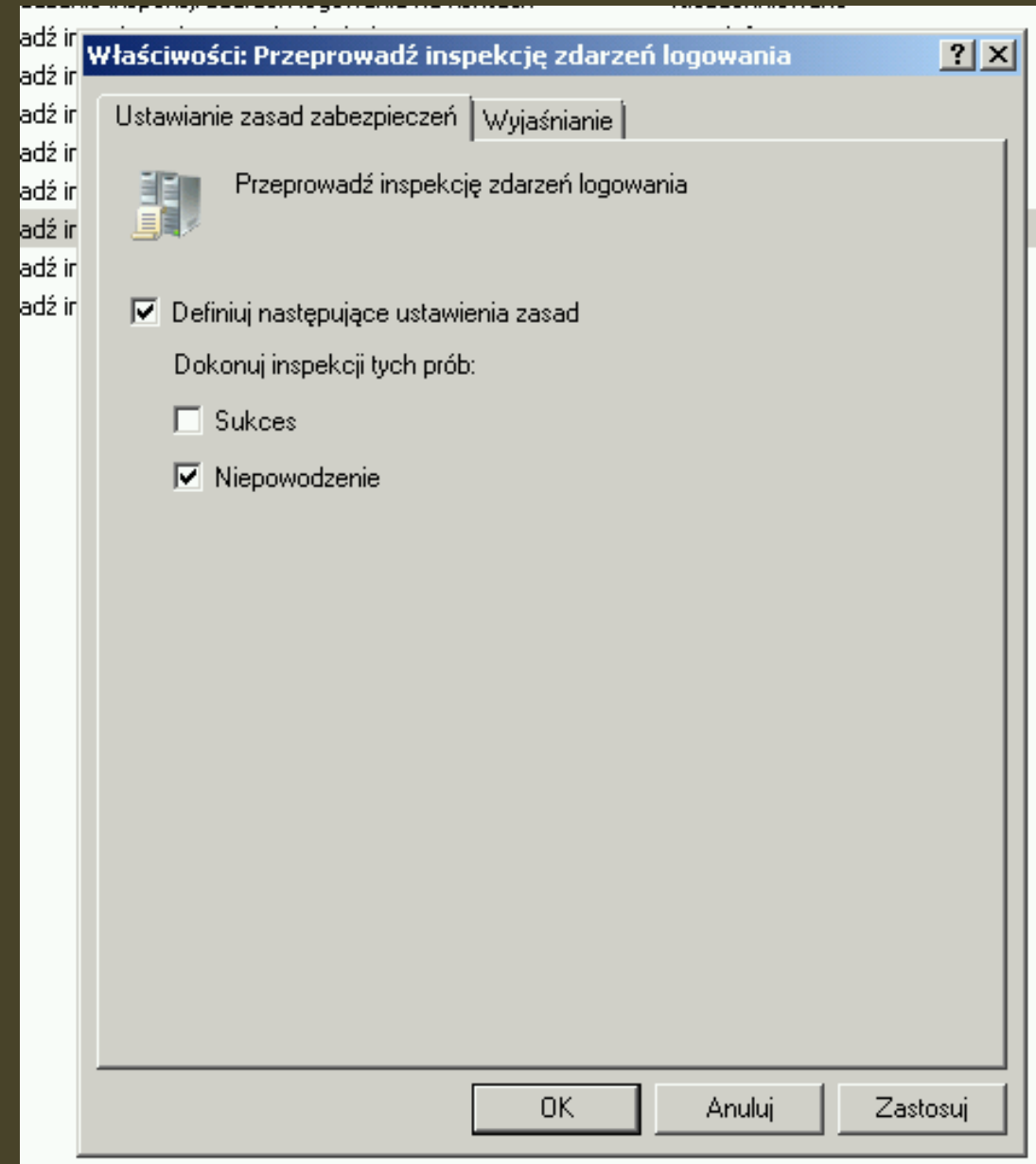
Poniżej

Kategorie	Konfiguracja
Logowanie na kontach	Nie skonfigurowano
Zarządzanie kontami	Nie skonfigurowano
Szczegółowe śledzenie	Nie skonfigurowano
Dostęp do usługi katalogowej	Nie skonfigurowano
Logowanie/wylogowywanie	Nie skonfigurowano
Dostęp do obiektów	Nie skonfigurowano
Zmiana zasad	Nie skonfigurowano
Wykorzystanie uprawnień	Nie skonfigurowano
System	Nie skonfigurowano
Inspekcja globalnego dostępu do obiektów	Nie skonfigurowano

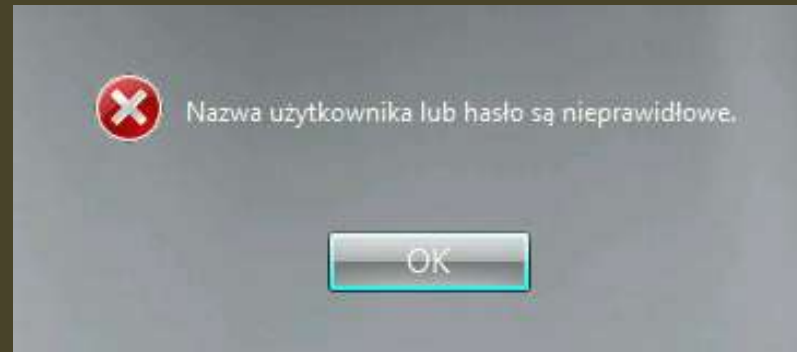
W praktyce...

Przykład 1

Inspekcja niepowodzenia podczas logowania



Próba nieudanego logowania – błędne hasło



Menedżer serwera

Plik Akcja Widok Pomoc

Menedżer serwera (WIN-SCIBPOTL)

- Role
- Funkcje
- Diagnostyka
 - Podgląd zdarzeń
 - Widoki niestandardowe
 - Dzienniki systemu Wind
 - Aplikacja
 - Zabezpieczenia
 - Ustawienia

Zabezpieczenia Liczba zdarzeń: 2 557

Słowa kluczowe	Data i godzina	Źródło	Identyfikator...
Sukcesy inspekcji	2016-03-31 14:21:10	Microsoft Wi...	4624
Sukcesy inspekcji	2016-03-31 14:21:10	Microsoft Wi...	4672
Niepowodzenie inspekcji	2016-03-31 14:20:53	Microsoft Wi...	4625
Sukcesy inspekcji	2016-03-31 14:20:51	Microsoft Wi...	4634
Sukcesy inspekcji	2016-03-31 14:20:51	Microsoft Wi...	4624
Sukcesy inspekcji	2016-03-31 14:20:51	Microsoft Wi...	4672
Sukcesy inspekcji	2016-03-31 14:20:51	Microsoft Wi...	4634

Właściwości zdarzenia — Zdarzenie 4625, Microsoft Windows security auditing.

Ogólne | Szczegóły

Logowanie na koncie nie powiodło się.

Podmiot:
Identyfikator zabezpieczeń: SYSTEM
Nazwa konta: WIN-SCIBPOTUSGB\$\br/> Domena konta: DOMENA
Identyfikator logowania: 0x3e7

Nazwa dziennika: Zabezpieczenia

Źródło: Microsoft Windows security Zalogowano: 2016-03-31 14:20:53

Identyfikator zdarzenia: 4625 Kategoria zadania: Logowanie

Poziom: Informacje Słowa kluczowe: Niepowodzenie inspek

Użytkownik: Nie dotyczy Komputer: WIN-SCIBPOTUSGB.do

Kod operacji: Informacje

Więcej informacji: [Pomoc online dziennika](#)

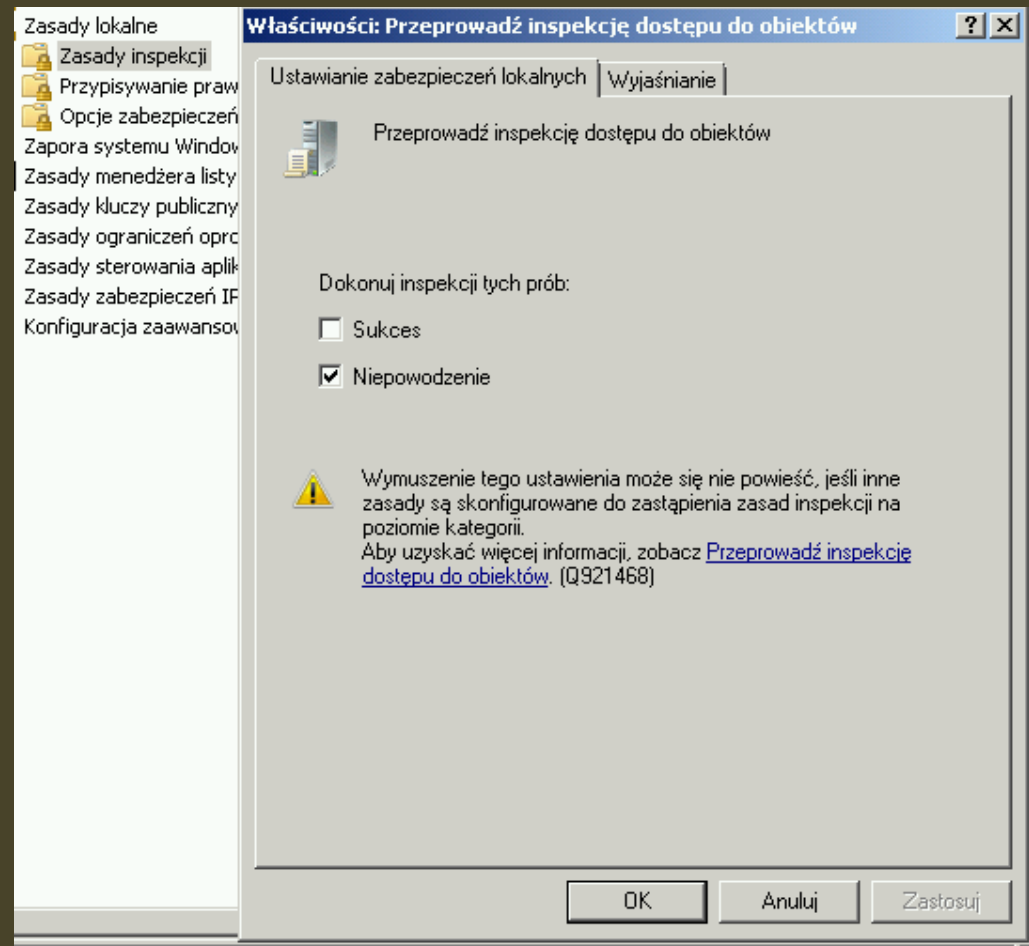
Kopiuuj Zamknij

Źródło: Microsoft Windows security Zalogowano: 2016-03-31 14

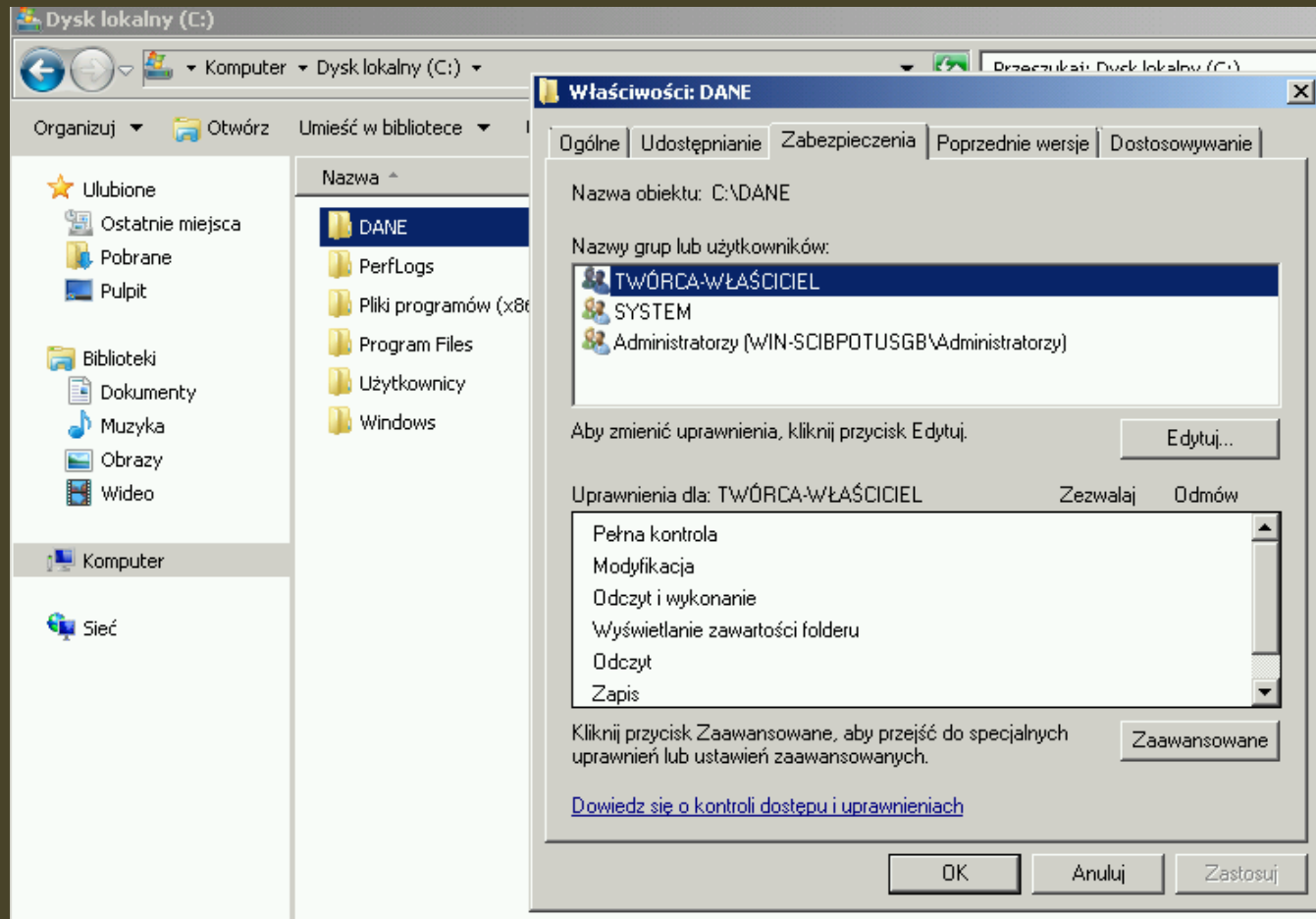
Przykład 2

Inspekcja dostępu do zasobów (pliki, foldery)

**W tym wypadku śledzone
będą jedynie
niepowodzenia (nieudane
próby dostępu do zasobu)**



Określenie Praw Dostępu do katalogu



Dla uproszczenia – tylko administratorzy mają dostęp do katalogu

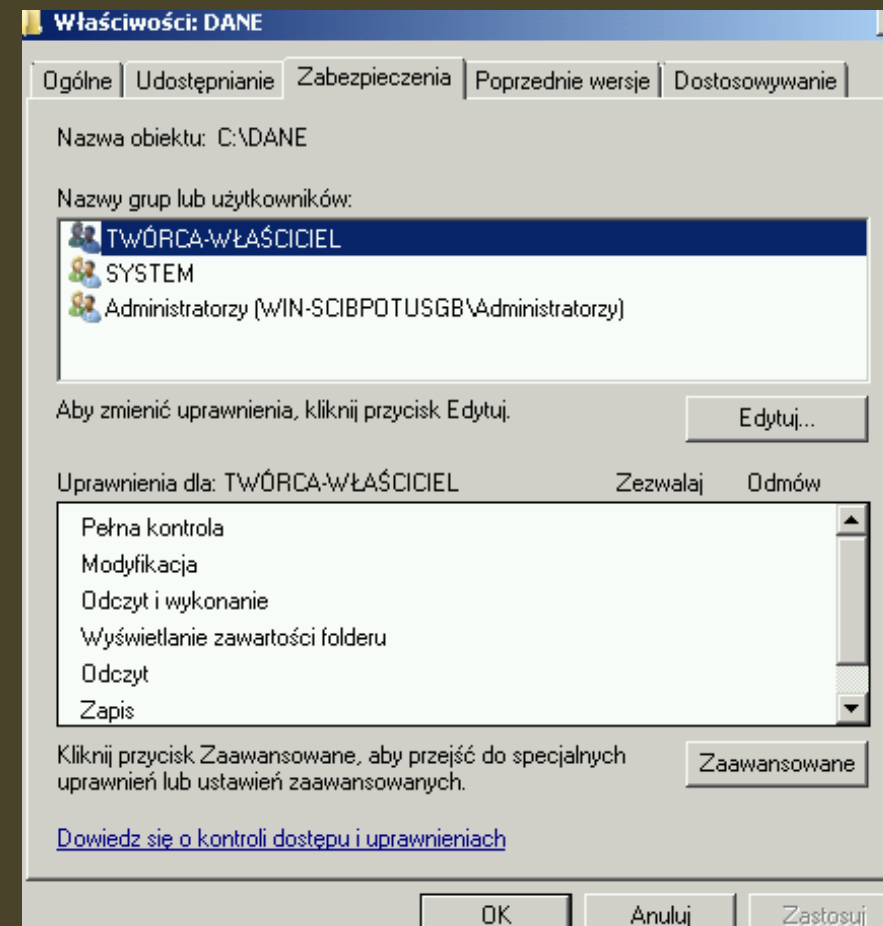
UWAGA: w tym wypadku nie wystarczy włączyć inspekcje z poziomu GPO – dodatkowo trzeba określić dla jakich grup/użytkowników i na okoliczność jakich zdarzeń chcemy przeprowadzać inspekcję...

Należy wykonać następującą czynność/czynności:

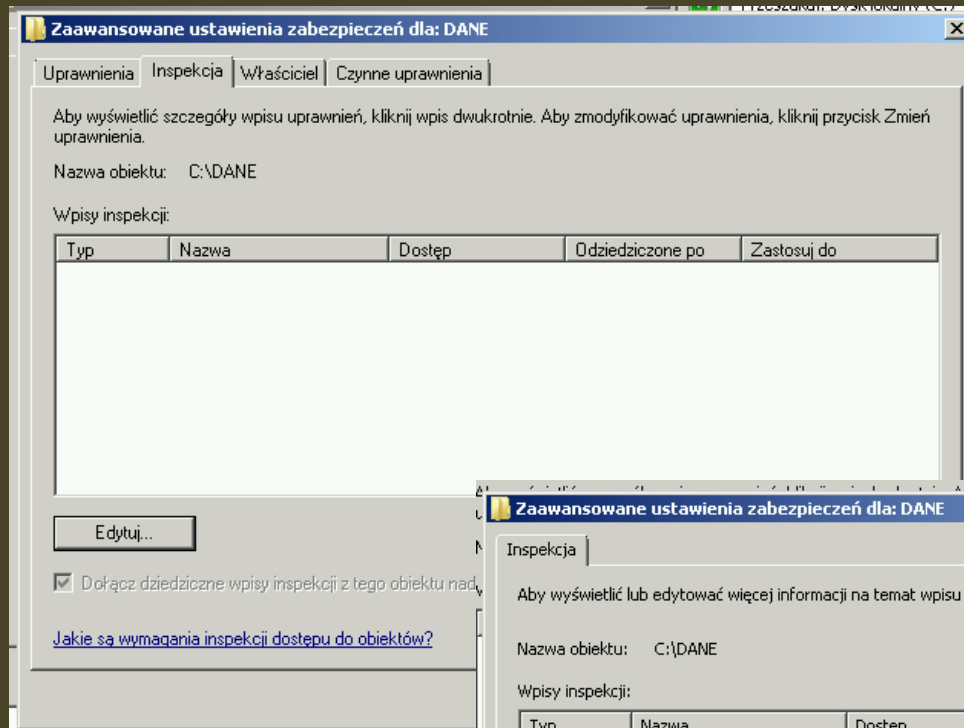
OBIEKT* -> Właściwości ->

Zabezpieczenia -> Zaawansowane

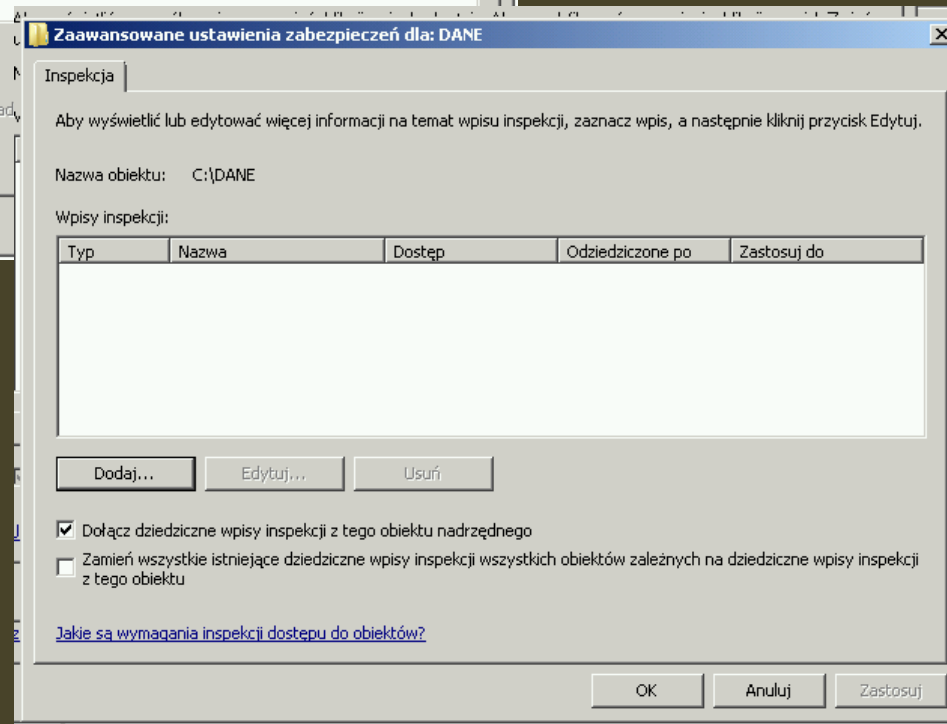
***(w tym wypadku katalog DANE)**



Następnie należy dodać wpis dotyczący inspekcji

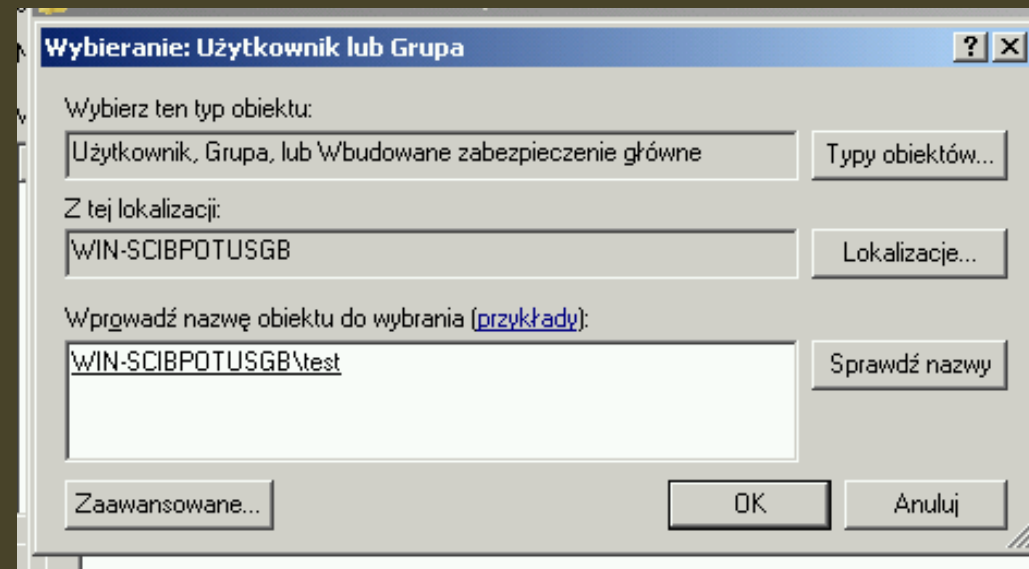


Inspekcja -> Edytuj



➔ DODAJ

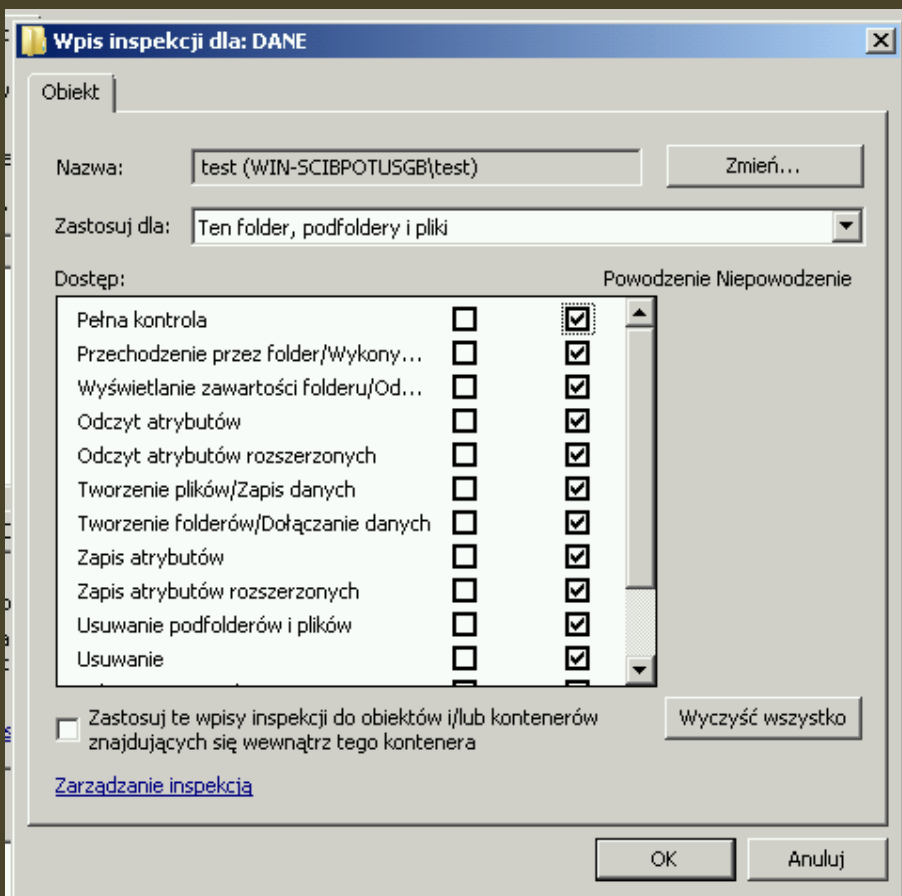
Określamy dla jakich GRUP/UŻYTKOWNIKÓW ma być prowadzona inspekcja ORAZ w jakim wypadku



UWAGA:

**1kolumna dotyczy powodzenia;
2kolumna niepowodzenia**

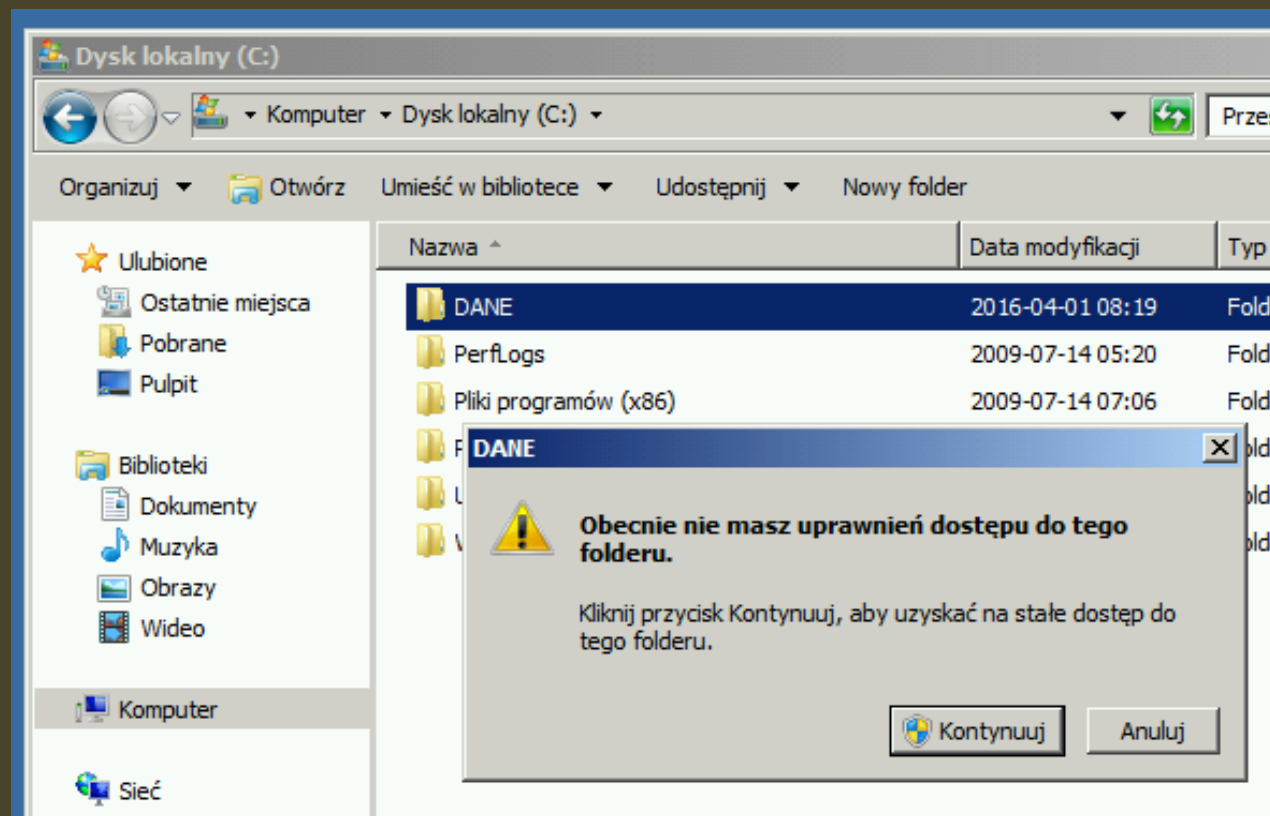
W tym wypadku dla ułatwienia interesuje mnie inspekcja niepowodzeń w dostępie do katalogu DANE przez użytkownika TEST w dowolnym zakresie (próba wglądu do katalogu, zmiany parametrów etc...).



Logowanie na konto TEST i próba wglądu do katalogu...



Oczywiście brak dostępu
(zgodnie z listą ACL)



Wynik Inspekcji:

The screenshot displays the Windows Security Auditing interface. On the left is a navigation pane with categories like 'Funkcje', 'Diagnostyka', and 'Magazyn'. The main window shows a list of events under the 'Zabezpieczenia' (Security) category. A specific event is selected, and its properties are shown in a dialog box.

Zabezpieczenia Liczba zdarzeń: 292 (!) — dostępne nowe zdarzenia

Słowa kluczowe	Data i godzina	Źródło	Identyfikator z...	Kategoria zadania
Niepowodzen...	2016-04-01 08:37:08	Microsoft Wind...	5152	Porzucanie pakie...
Niepowodzen...	2016-04-01 08:37:07	Microsoft Wind...	5152	Porzucanie pakie...

Właściwości zdarzenia — Zdarzenie 4656, Microsoft Windows security auditing.

Ogólne | Szczegóły

Zaądzano dojścia do obiektu.

Temat:

Identyfikator zabezpieczeń: WIN-SCIBPOTUSGB\test
Nazwa konta: test
Domena konta: WIN-SCIBPOTUSGB
Identyfikator logowania: 0x11a0f3

Nazwa dziennika: Zabezpieczenia

Źródło: Microsoft Windows security Zalogowano: 2016-04-01 08:37:03

Identyfikator zdarzenia: 4656 Kategoria zadania: System plików

Poziom: Informacje Słowa kluczowe: Niepowodzenie inspek

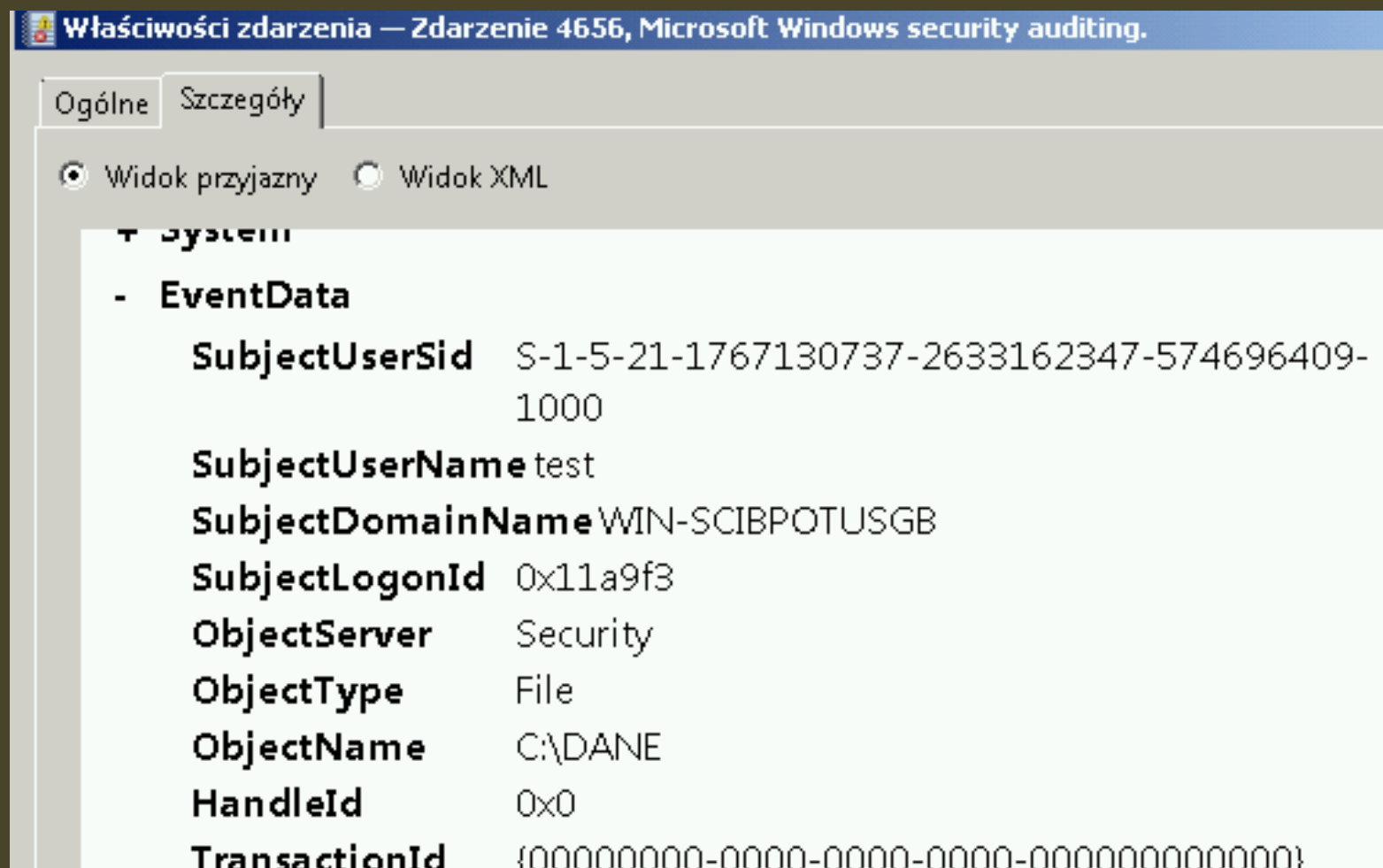
Użytkownik: Nie dotyczy Komputer: WIN-SCIBPOTUSGB

Kod operacji: Informacje

Więcej informacji: [Pomoc online dziennika](#)

Zamknij

Wiadomo, że użytkownik TEST nie uzyskał dostępu do katalogu C:\DANE



Identyfikator zdarzenia to: 4656 - > oznacza, że „Zażądano dojście do obiektu.”

