Zasady grupy – zaawansowane zastosowania

Wymagania:

- kontroler domeny na Windows Serwer 2012R2,
- dwa komputery klientów z Windows 10 – dołączone do domeny

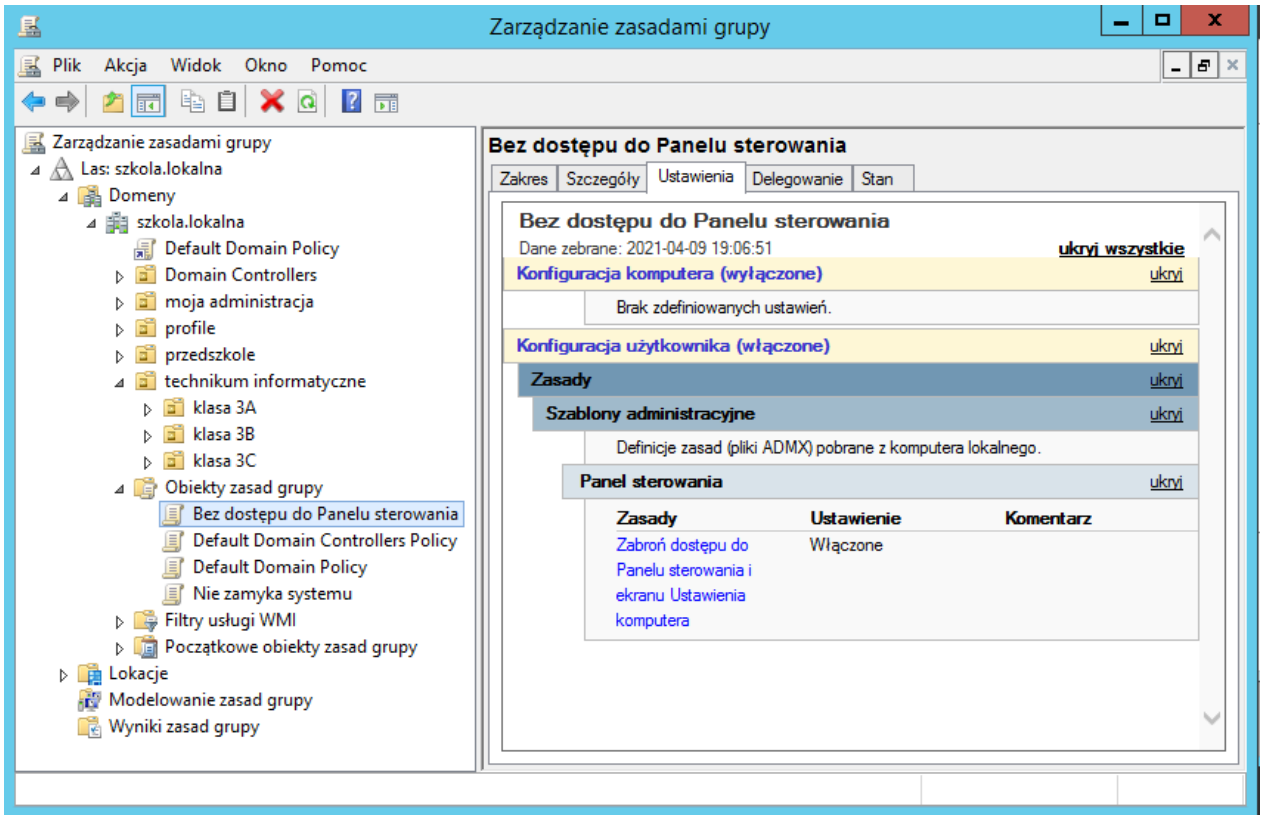
UWAGA

- **Najmniejszym obiektem AD z którym możemy połączyć obiekt zasady grupy jest jednostka organizacyjna.**
- **Jeden obiekt zasady grupy można połączyć z wieloma obiektami AD.**
- **Nie ma ograniczeń co do ilości utworzonych obiektów ZG.**
- **Pojedynczy obiekt ZG może zawierać jedną lub więcej zasad**
- **Domyślnie zasady grupy są dziedziczone we wszystkich obiektach podrzędnych AD**
- **Dziedziczenie ZG można zablokować na poziomie dowolnego obiektu AD**
- **Blokadę dziedziczenia można ominąć włączając wymuszenie działania na poziomie obiektu ZG**

I. W szkole „technikum informatyczne” tylko uczniowie klasy 3C mają dostęp do Panelu sterowania.
Problem można rozwiązać przynajmniej dwoma metodami.

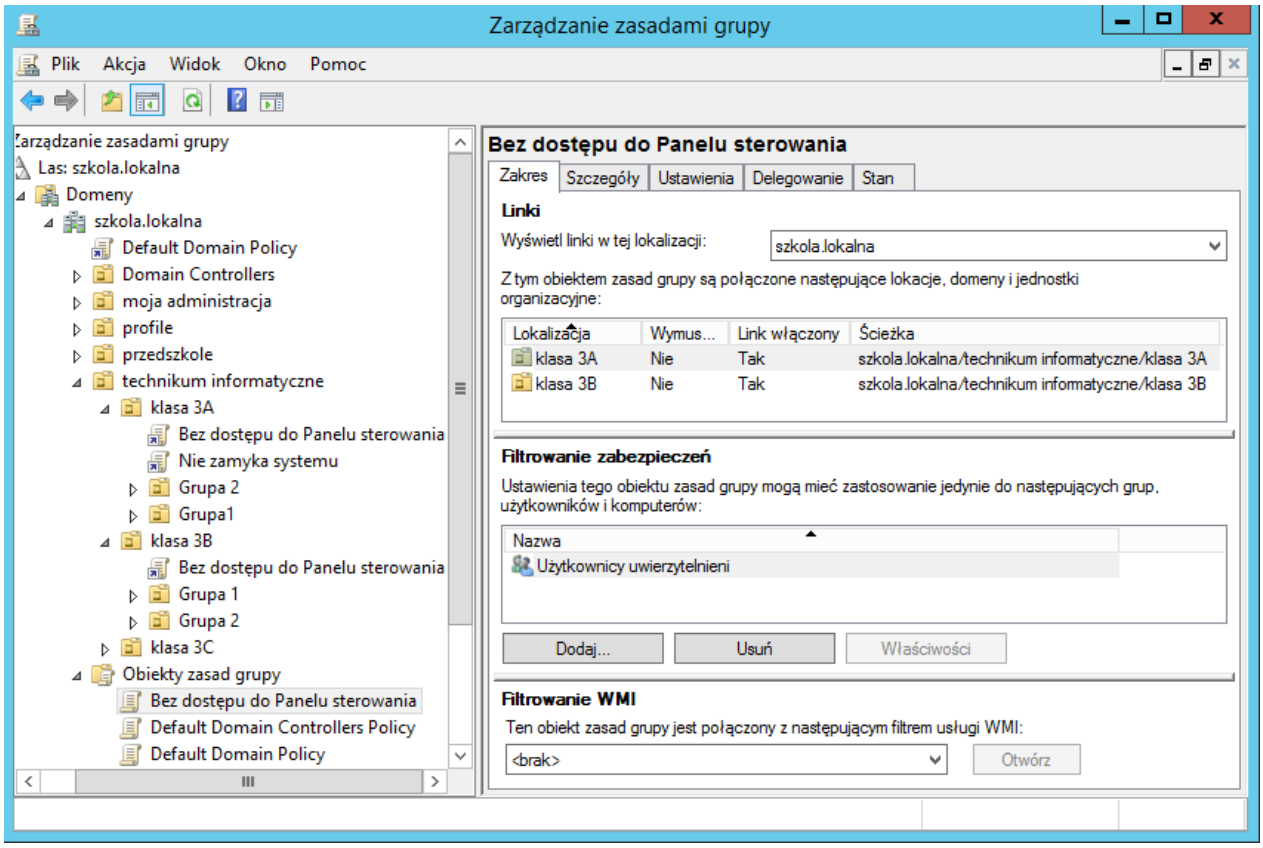
Metody rozwiązania problemu:

Tworzymy obiekt zasady grupy o nazwie np. **Bez dostępu do Panelu sterowania,** z włączoną zasadą **Zabroń dostępu do Panelu sterowania**….. Zgodnie z Wymaganiami zasada może być stosowana w Systemach Windows 2000 lub nowszych

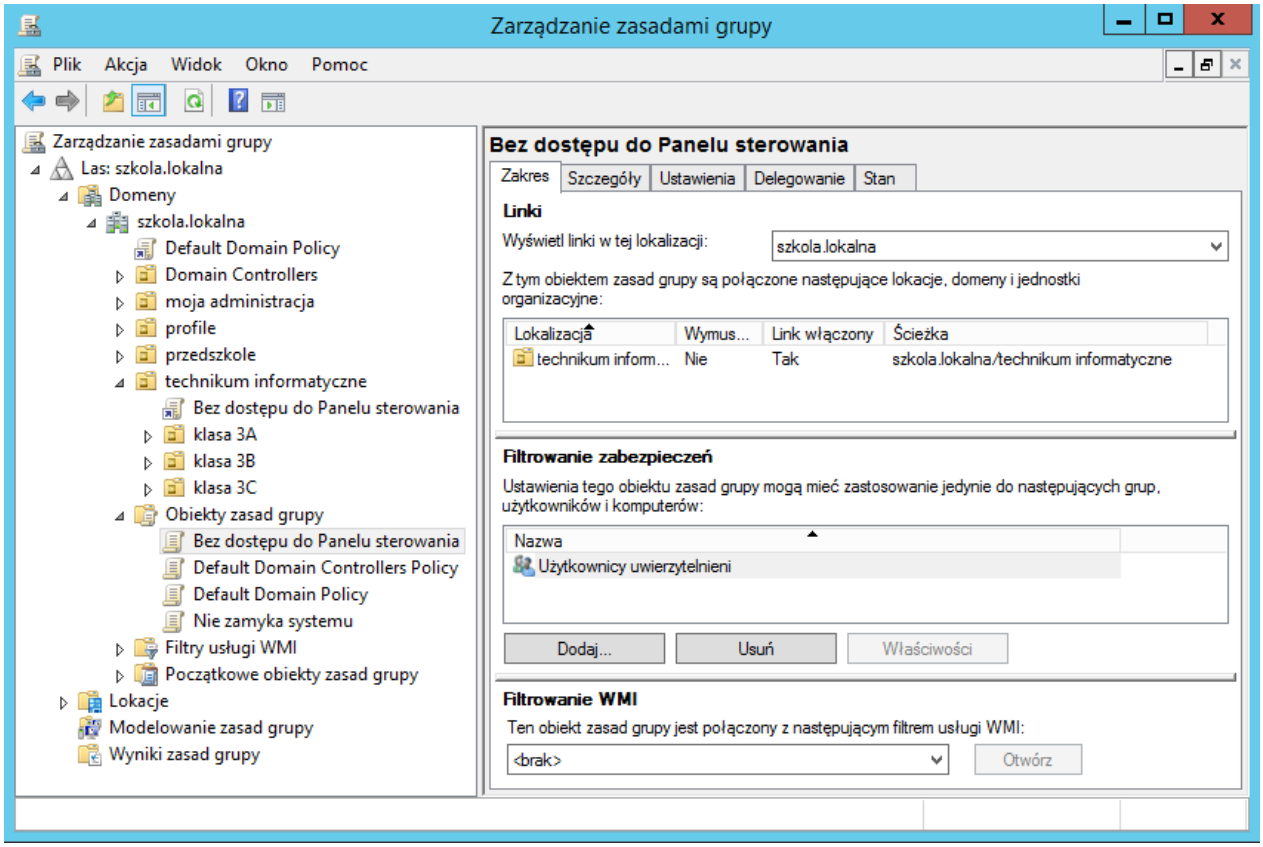


1. Pierwsza metoda - optymalna
    a. Jednostkę organizacyjną **klasa 3A** łączymy z utworzonym obiektem zasady grupy **Bez dostępu do Panelu sterowania**

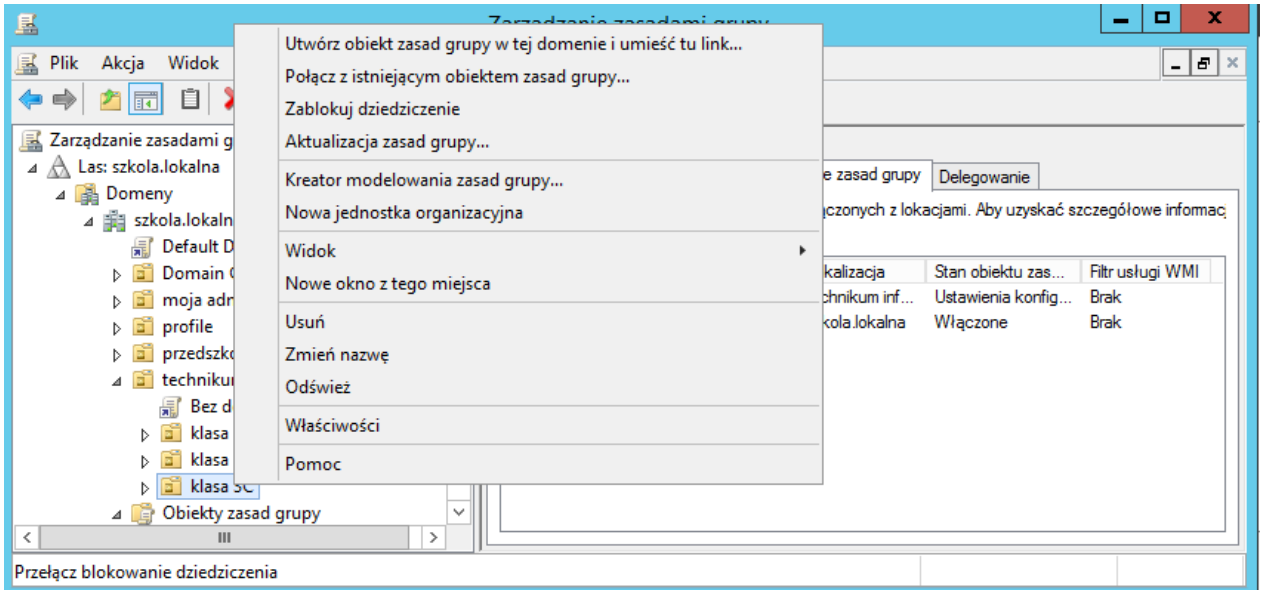
b. Jednostkę organizacyjną **klasa 3B** łączymy z utworzonym obiektem zasady grupy **Bez dostępu do Panelu sterowania**



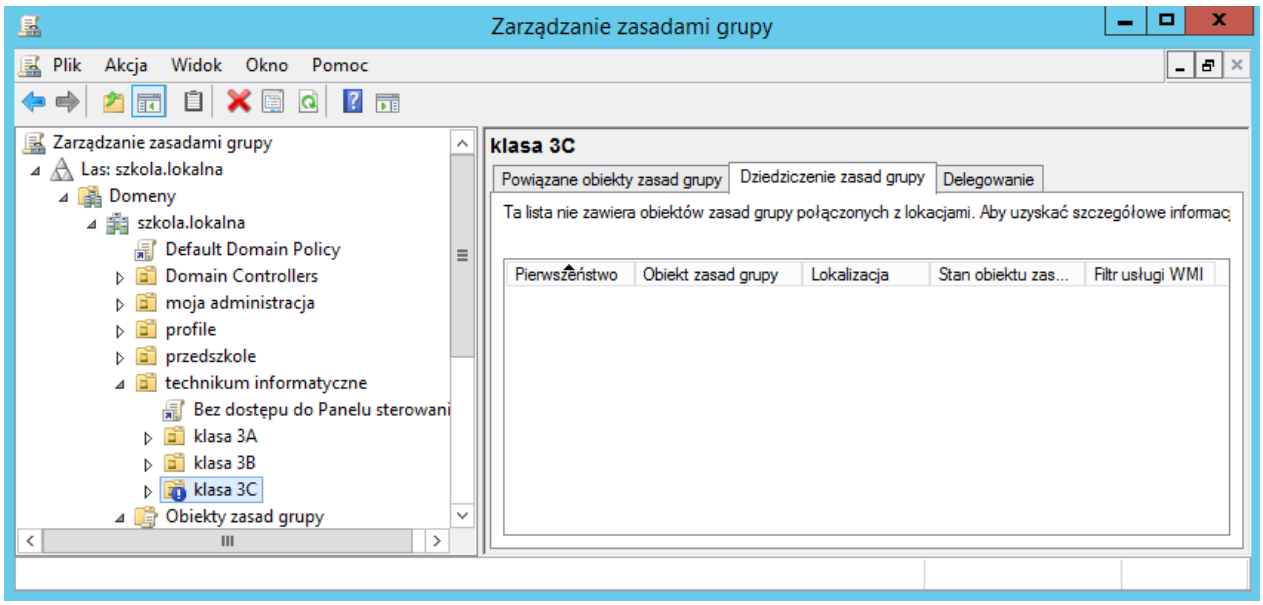
2. Druga metoda
   a. Jednostkę organizacyjną t**echnikum informatyczne** łączymy z utworzonym obiektem zasady grupy **Bez dostępu do Panelu sterowania**



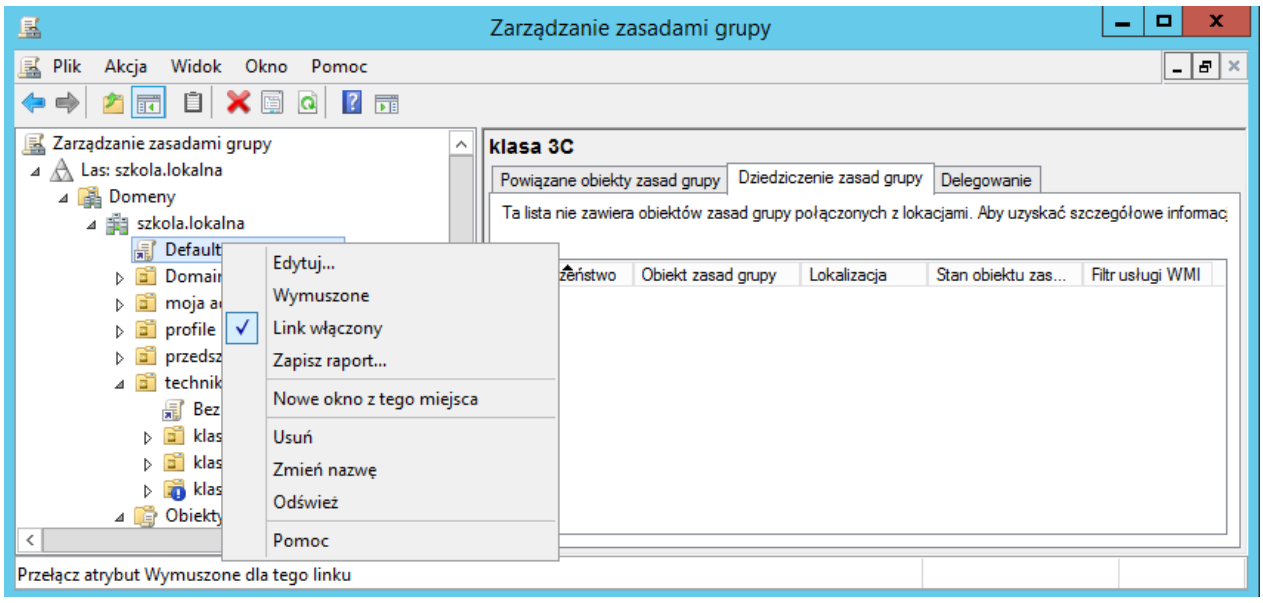
b. Blokujemy dziedziczenie zasad na poziomie jednostki organizacyjnej klasa 3C



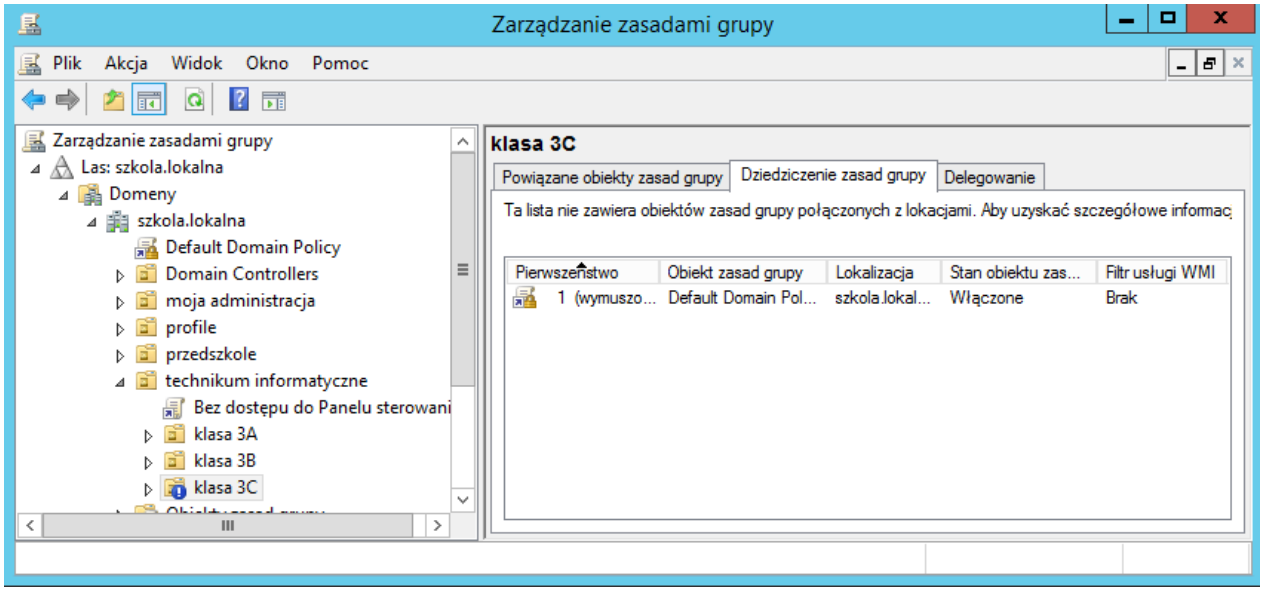
Jak widać jednostce organizacyjnej klasa3C nie działają żadne zasady



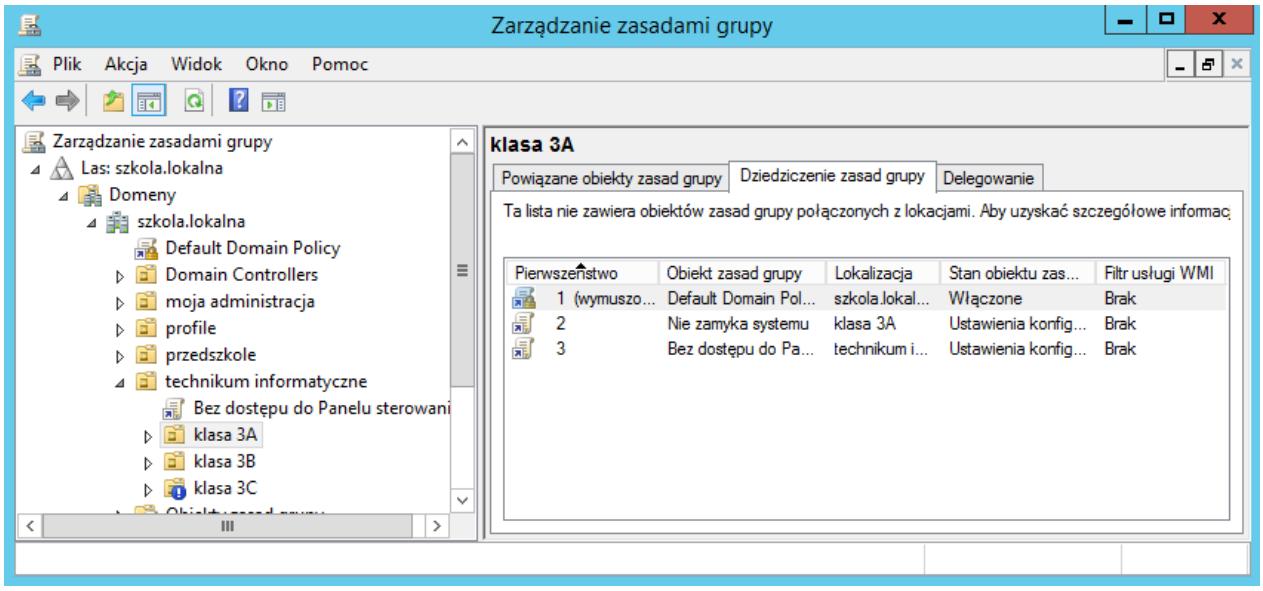
c. Wymuszamy działanie domyślnych zasad domeny



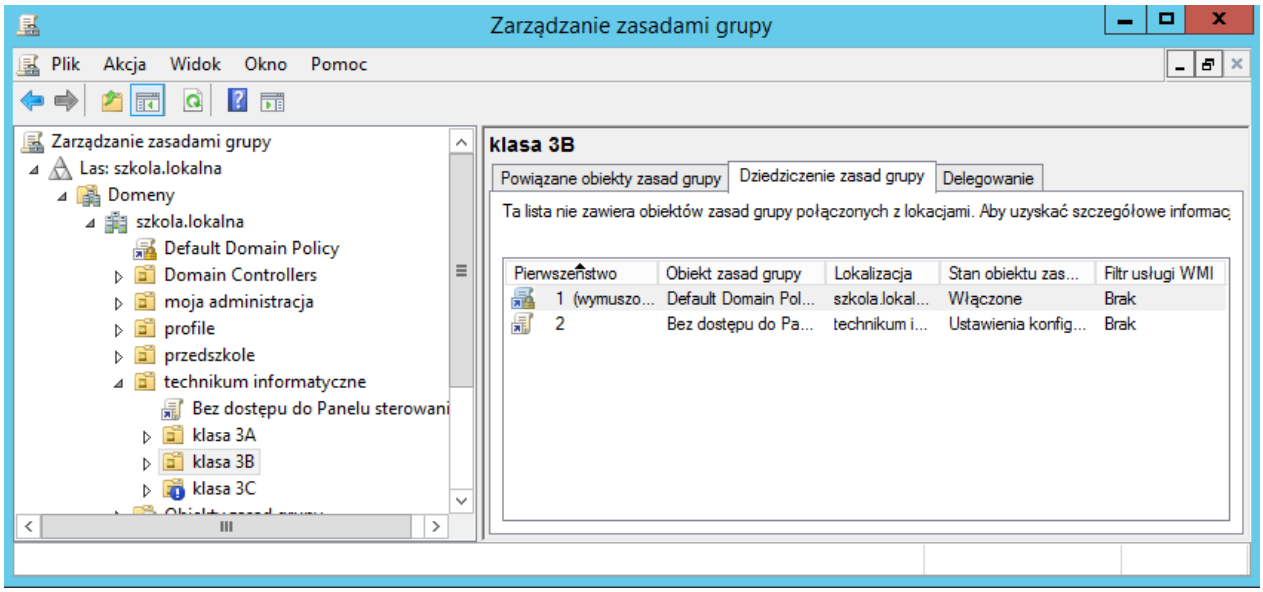
Domyślne zasady domeny obowiązują w jednostce organizacyjnej klasa 3C



W jednostce organizacyjnej klasa 3A obowiązują wszystkie wymagane zasady.



W jednostce organizacyjnej klasa 3B obowiązują wszystkie wymagane zasady.



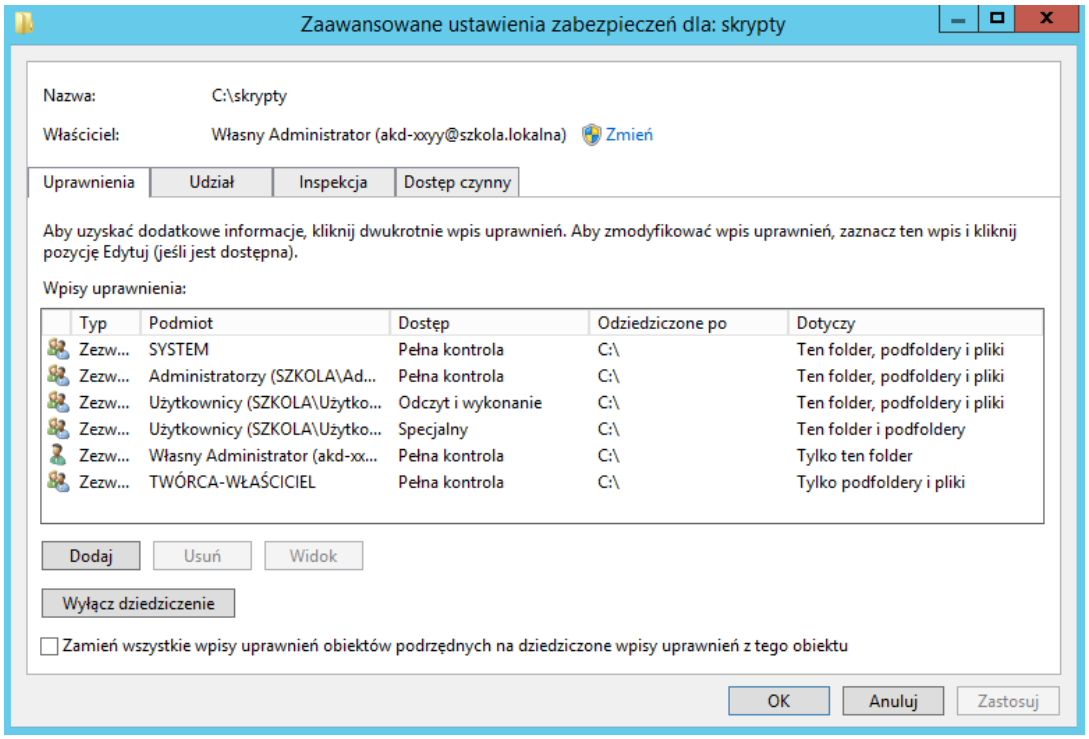
II. W przedszkolu użytkownicy z jednostki organizacyjnej *maluchy* nie mają prawa zapisywać na pulpicie. JO maluchy, znajduje się w JO przedszkole, a ta w domenie szkola.lokalna.

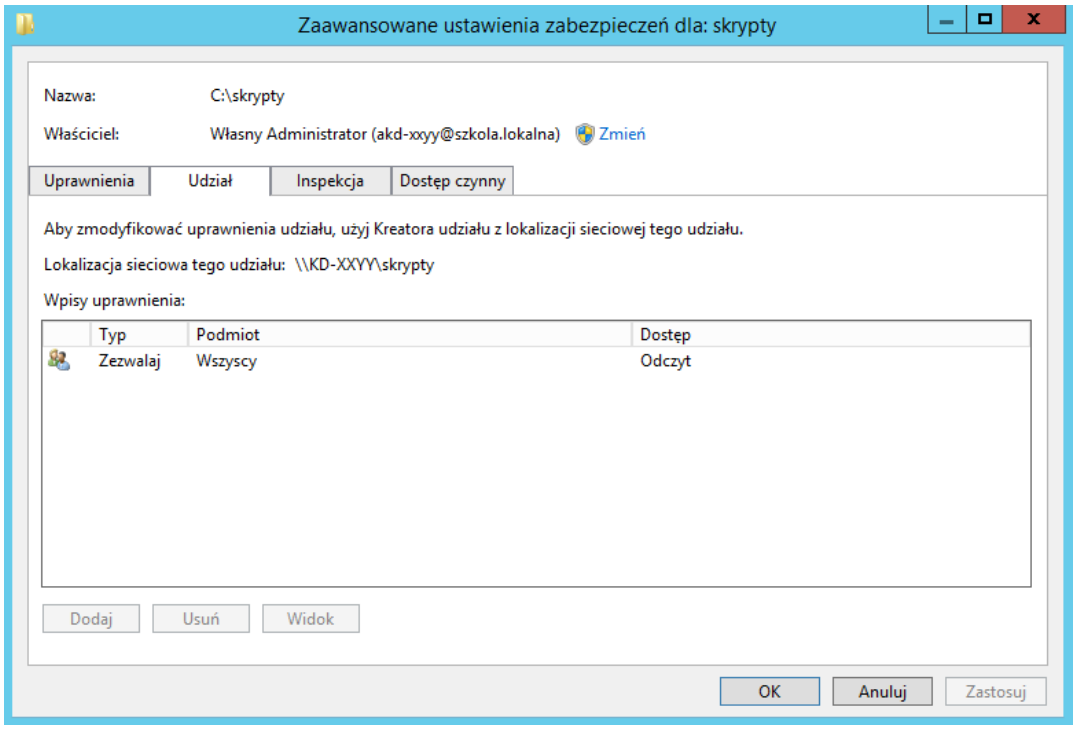
Aby użytkownik nie mógł zapisywać danych w jakiejś lokalizacji, nie może mieć uprawnień do zapisu. Pozostają tylko uprawnienia **Odczyt i wykonanie**.

Aby zrealizować to zadanie należy utworzyć:

- skrypt zmieniający uprawnienia dostępu do pulpitu użytkownika,
- zasadę grupy (GPO) która, podczas logowania użytkownika uruchomi powyższy skrypt.

Na dysku c: tworzymy katalog **skrypty.** Udostępniamy go w sieci z uprawnieniami domyślnymi.

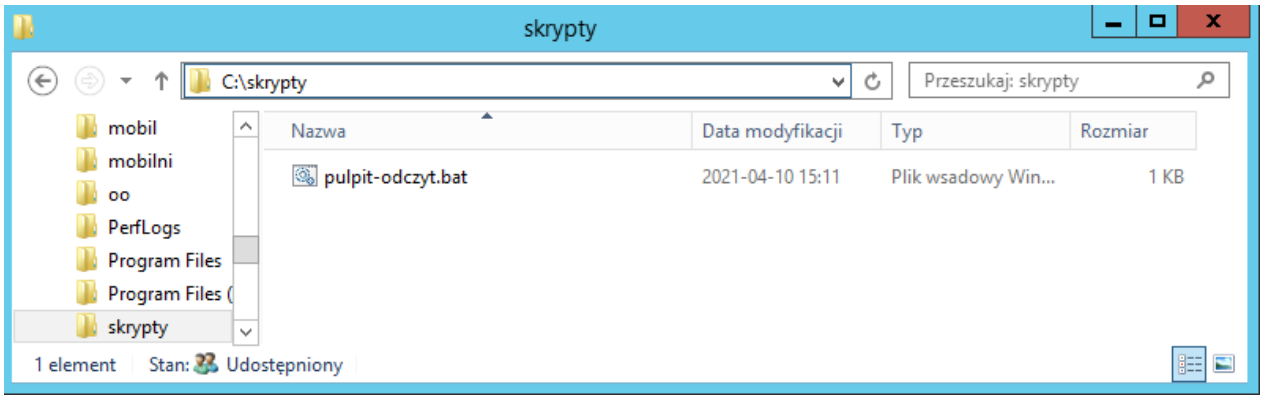




W notatniku tworzymy skrypt o nazwie **pulpit-odczyt.bat** o treści:

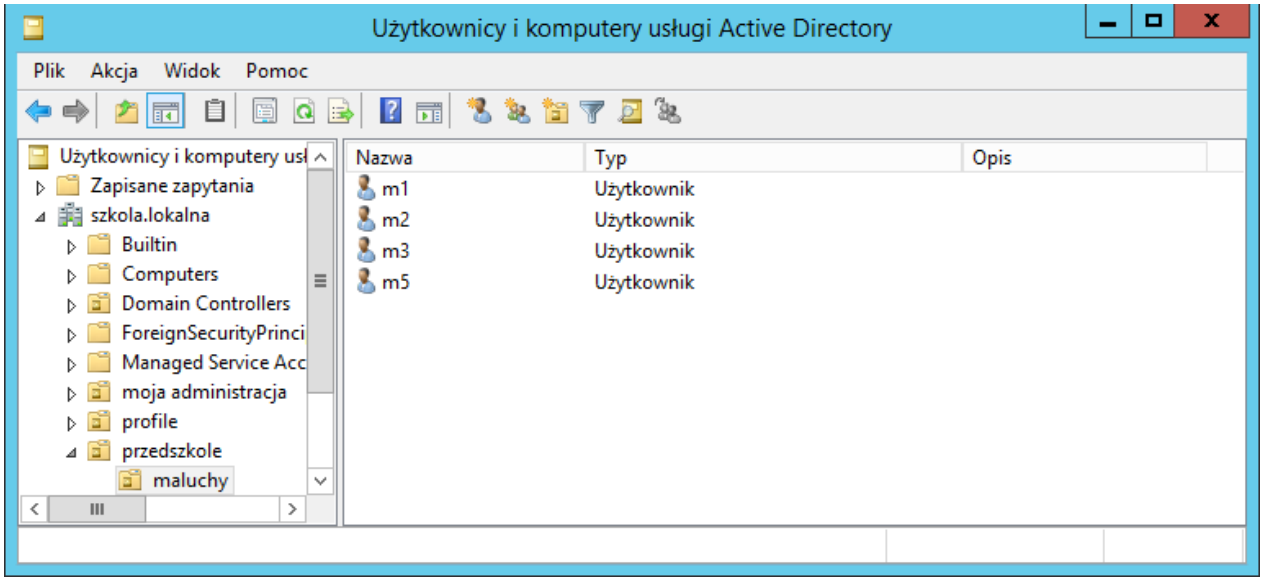
```
c:
cls
cd %userprofile%
echo t|icacls desktop /inheritance:d
echo t|icacls desktop /remove %username%
echo t|icacls desktop /grant:r %username%:(RX)
icacls desktop

pause
```

Skrypt zapisujemy w folderze **skrypty**.

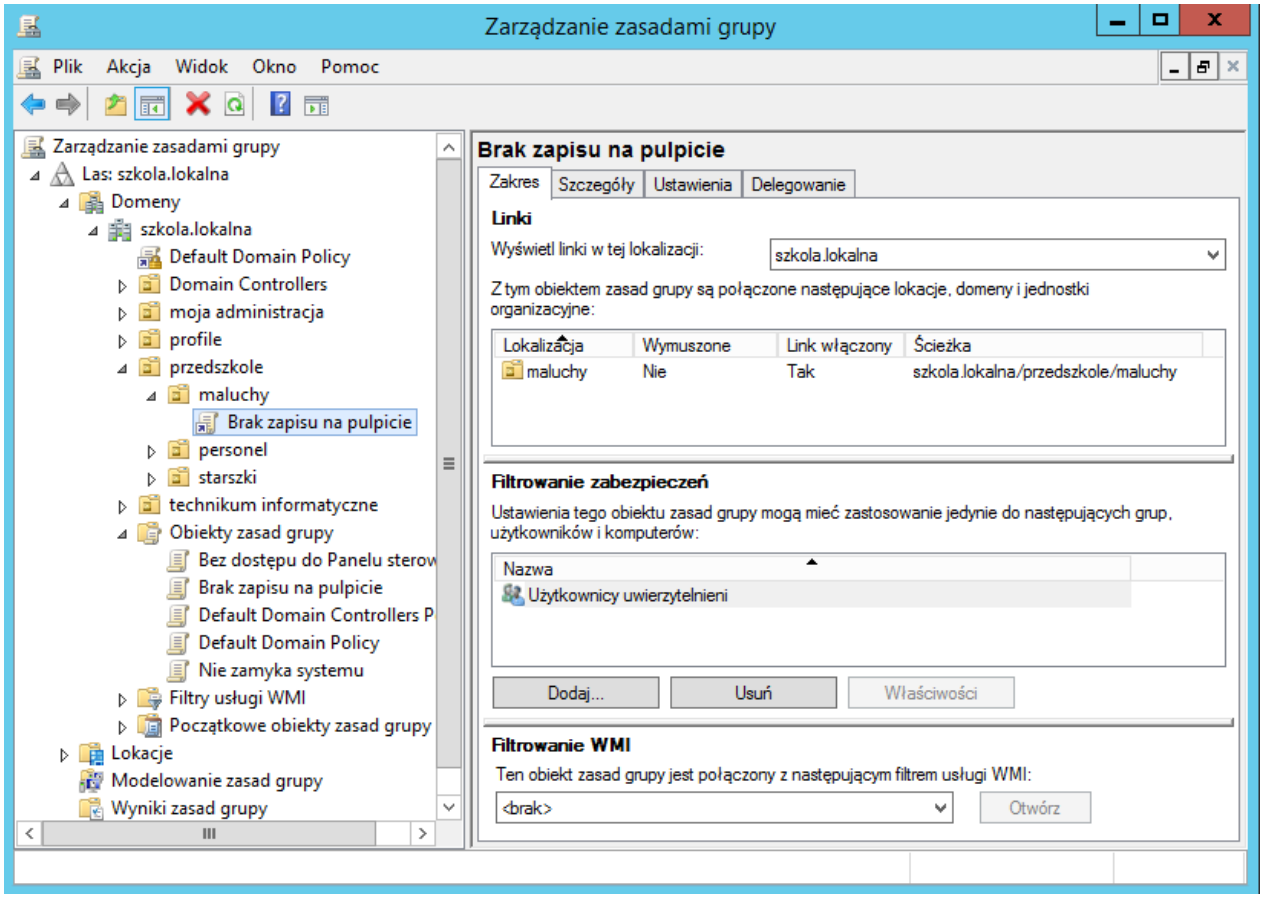


W przystawce **Użytkownicy i komputery usługi Active Directory** (AD):

- w domenie tworzymy JO **przedszkole**
- w JO **przedszkole** tworzymy JO **maluchy**
- w JO maluchy tworzymy min. trzy konta: m1, m2 i m3 z hasłem ZAQ!2wsx

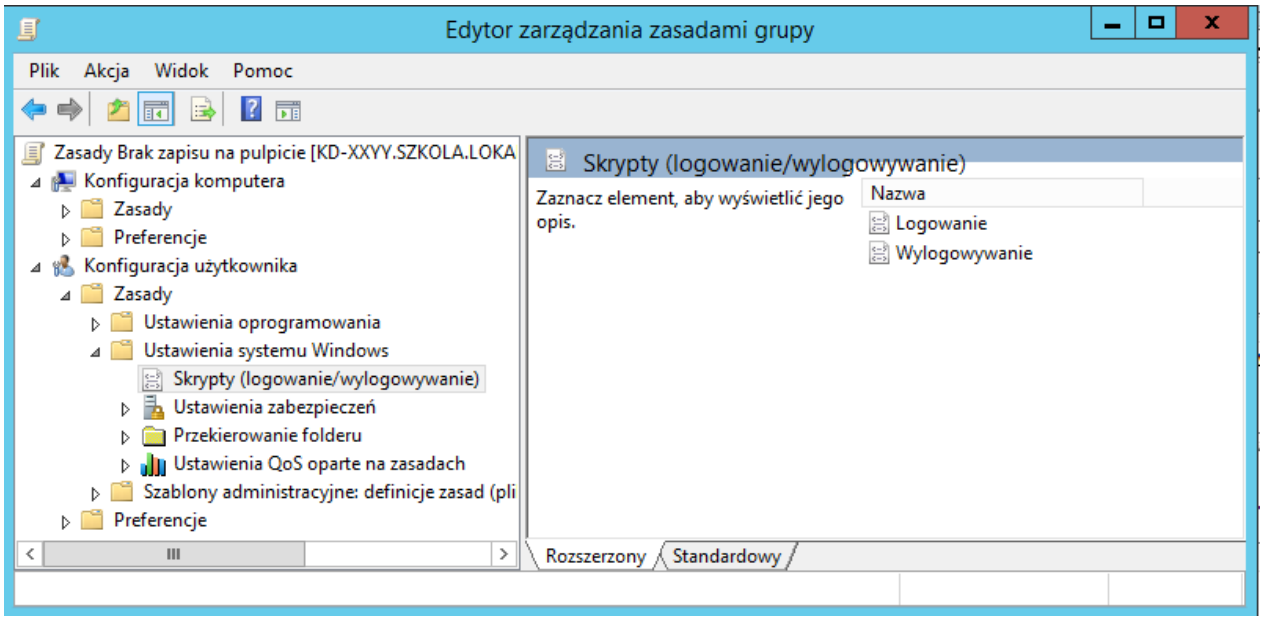


W przystawce **Zarządzanie zasadami grupy**, tworzymy GPO o nazwie **Brak zapisu na pulpicie**, powiązaną z jednostką organizacyjną maluchy

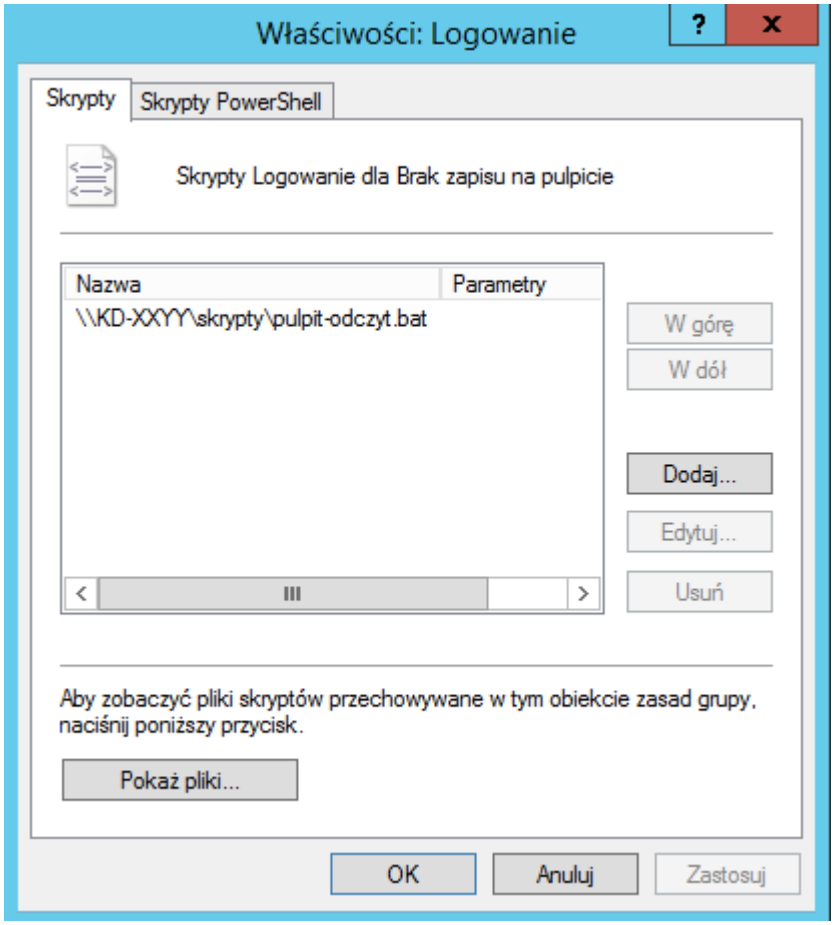


Edytujemy ten obiekt GPO i wybieramy

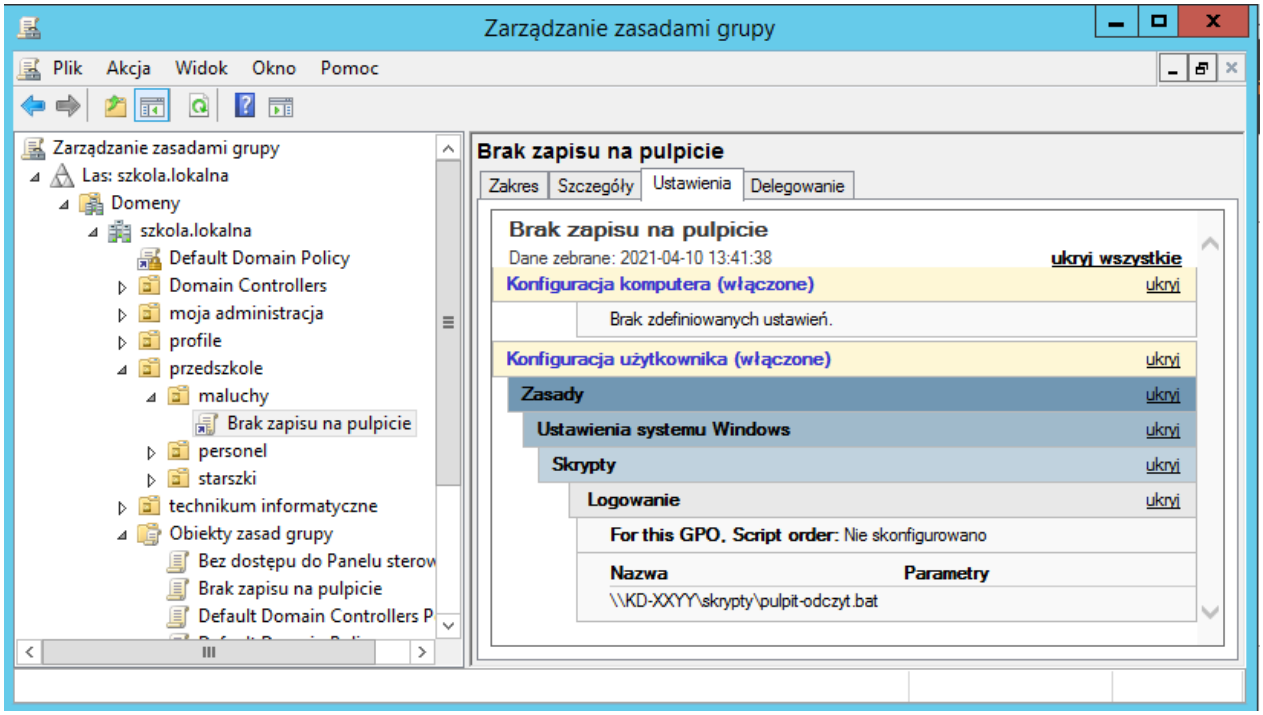
- Konfiguracja użytkownika
- Zasady
- Ustawienia systemu Windows
- Skrypty



Klikamy dwukrotnie w **Logowanie** i w oknie Właściwości : Logowanie wpisujemy ścieżkę UNC do naszego skryptu. Klikamy zastosuj i OK. Następnie zamykamy Edytor zarządzania GPO.



Wyświetlamy konfigurację naszego obiektu GPO



Możemy przystąpić do przetestowania działania, logując się na koncie np. m2 na desktopie.

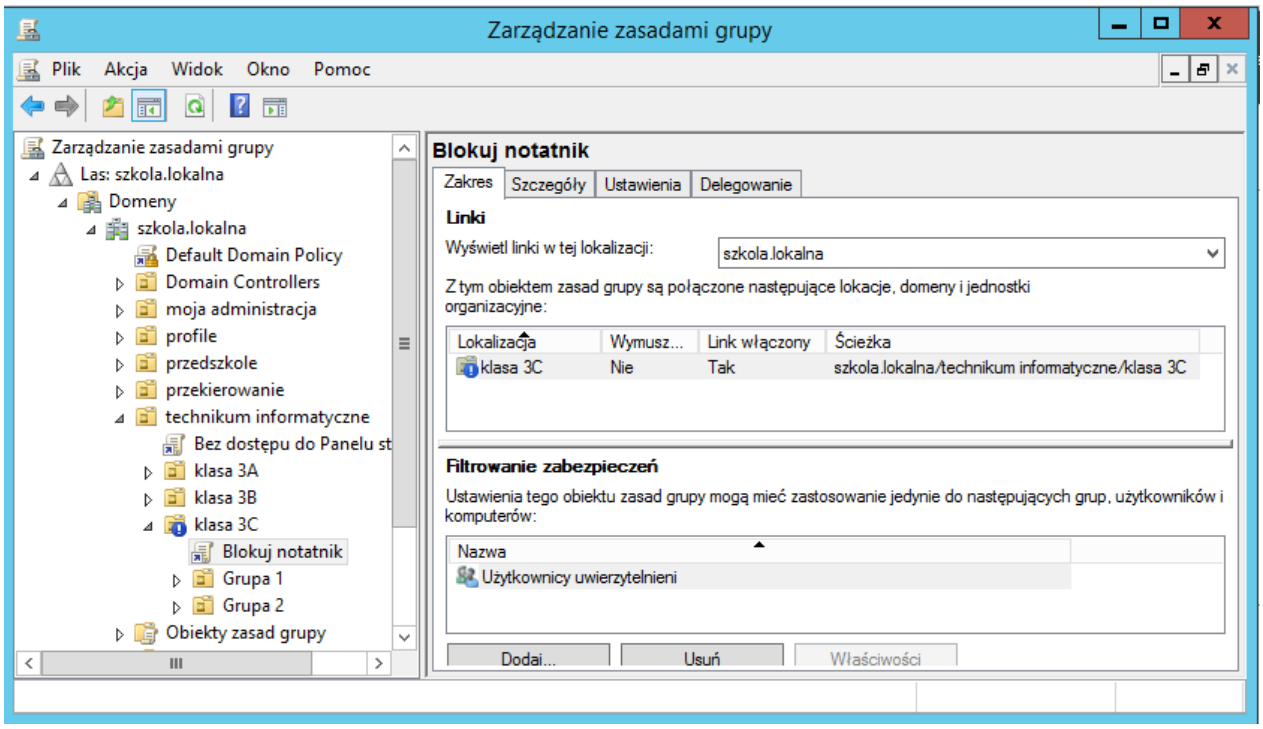
Zasady ograniczeń oprogramowania

Zabraniamy określonym użytkownikom, grupom dostępu do określonych programów. My zabronimy dostępu do notatnika :

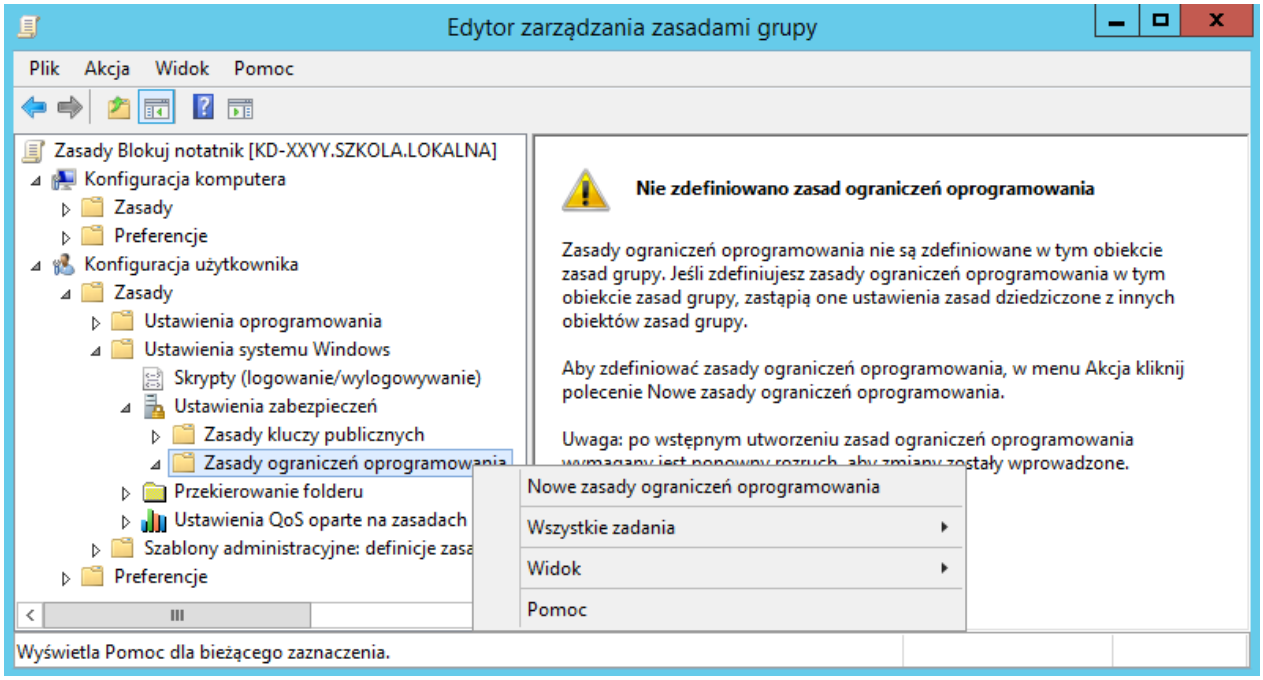
- użytkownicy JO klasa 3C zastosujemy regułę ścieżki
- użytkownicy JO klasa 3B zastosujemy regułę skrótu

Reguła ścieżki – użytkownicy JO klasa 3C

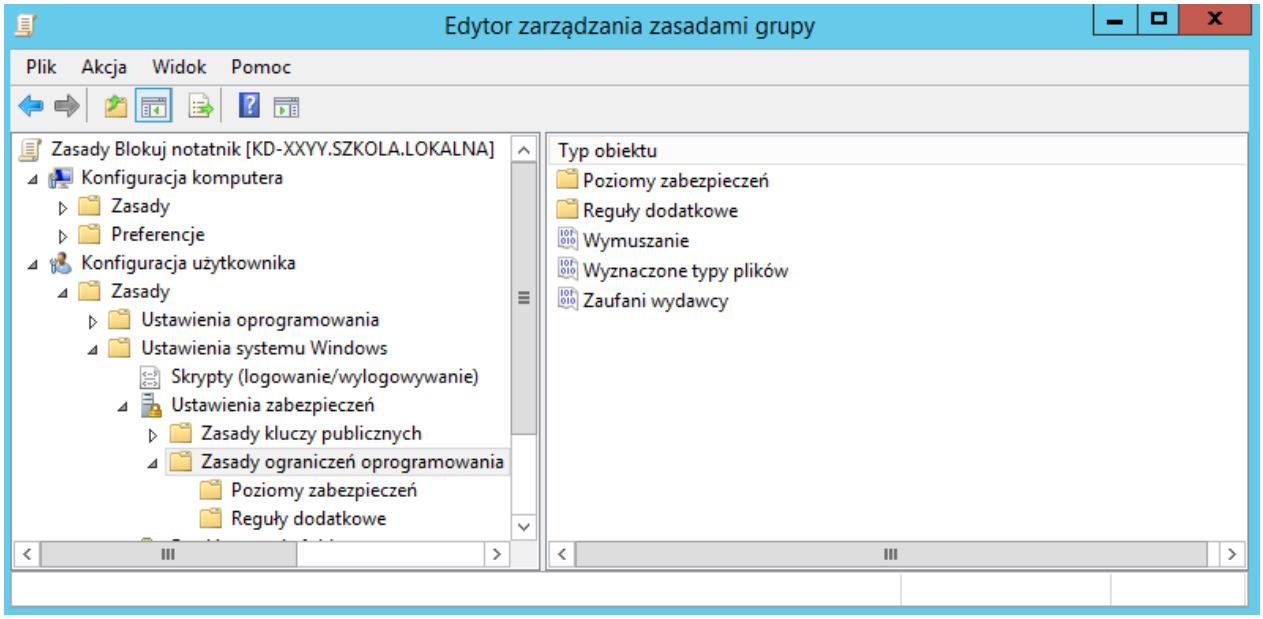
Tworzymy GPO **Blokuj notatnik** i łączymy go z JO **klasa 3C**



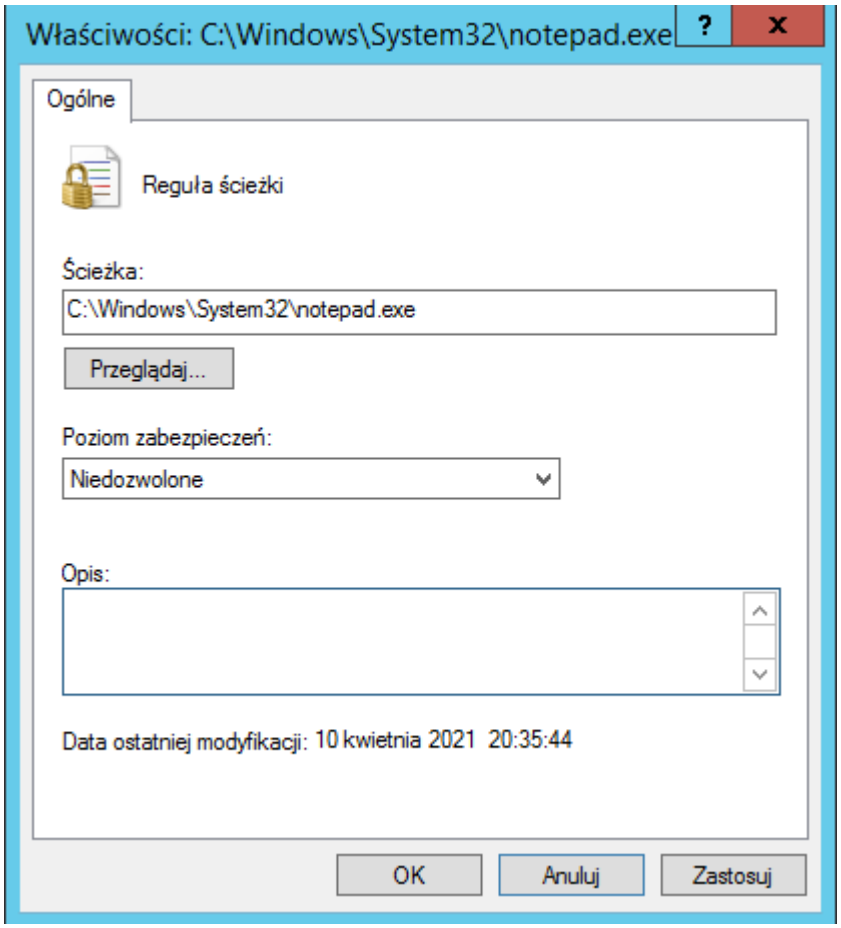
Przechodzimy do: Konfiguracja użytkownika -> zasady -> Ustawienia systemu Windows -> Ustawienia zabezpieczeń -> Zasady ograniczeń oprogramowania. Z menu podręcznego wybieramy **Nowe zasady ograniczeń oprogramowania**



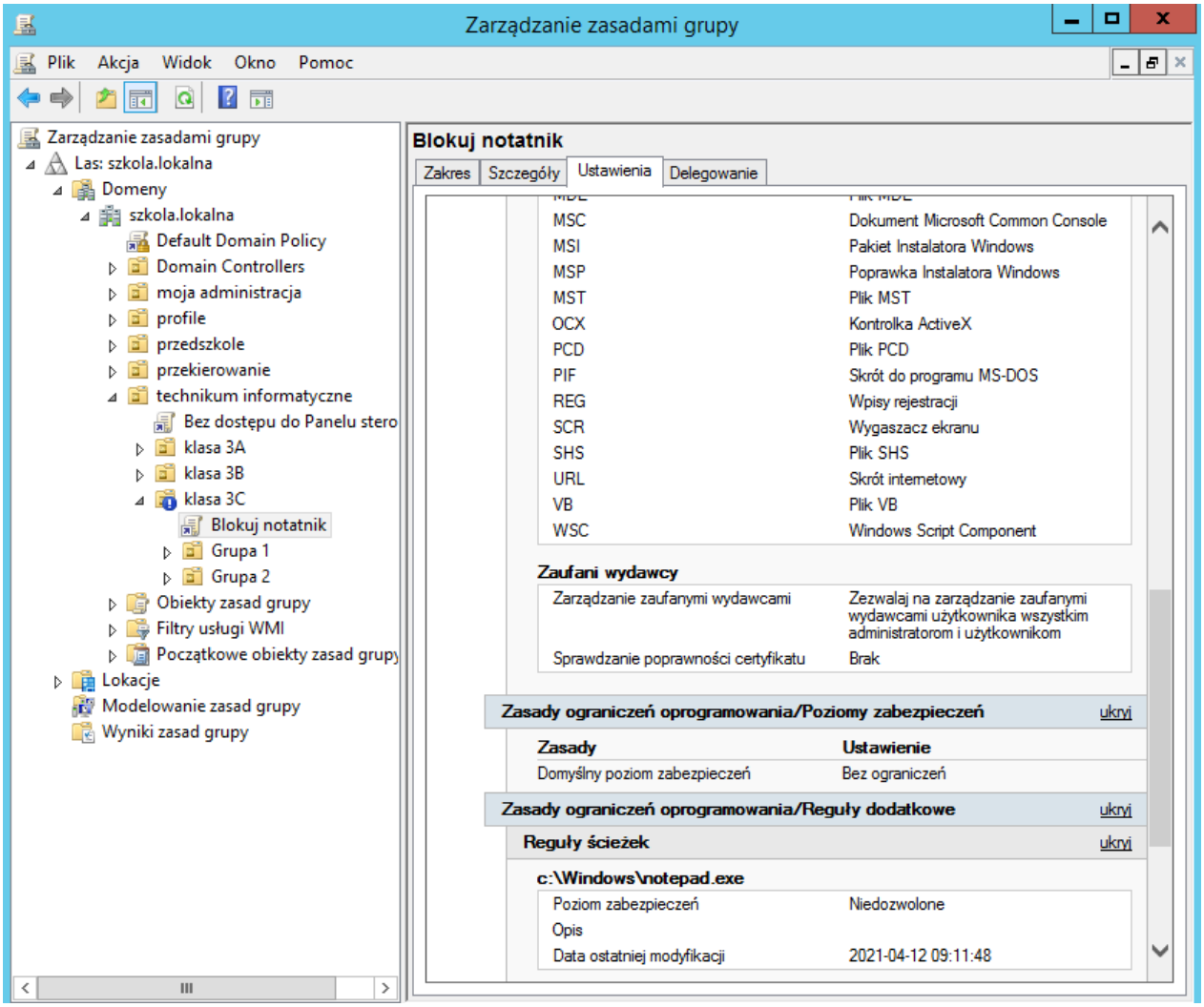
Przeglądamy dostępne opcje. Z menu podręcznego **Reguły dodatkowe** wybieramy **Nowa reguła ścieżki…**



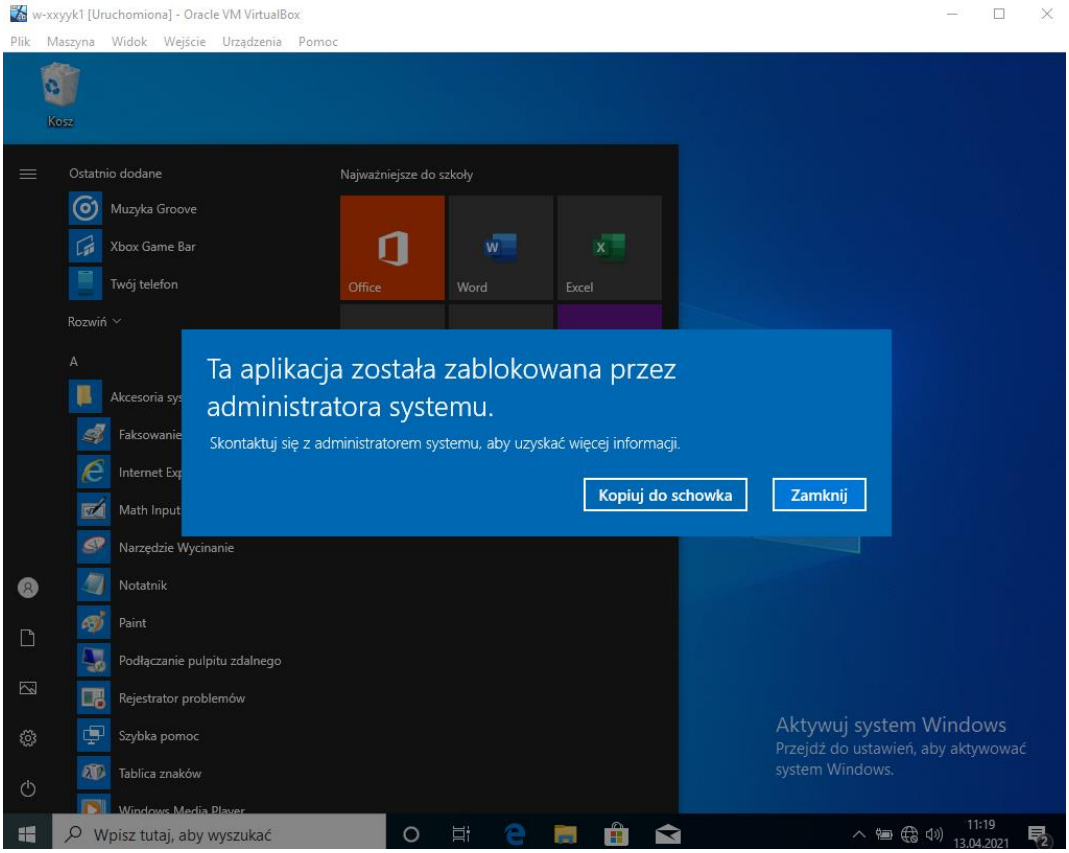
Klikamy przeglądaj i wyszukujemy notatnik (notepad.exe), klikamy zastosuj i OK. Zamykamy Edytor zarzadzania zasadami grupy.



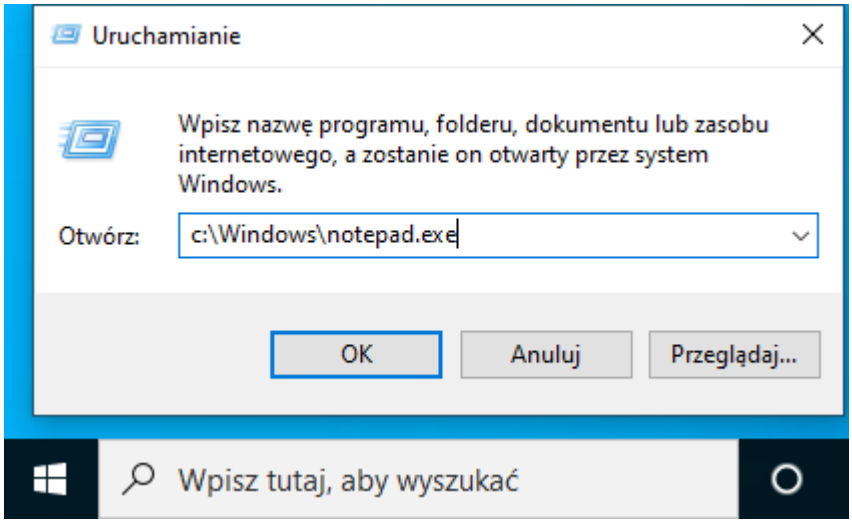
Weryfikujemy Ustawienia GPO **Blokuj notatnik**.



Logujemy się na kliencie na koncie np. 3c-k1 i weryfikujemy działanie GPO

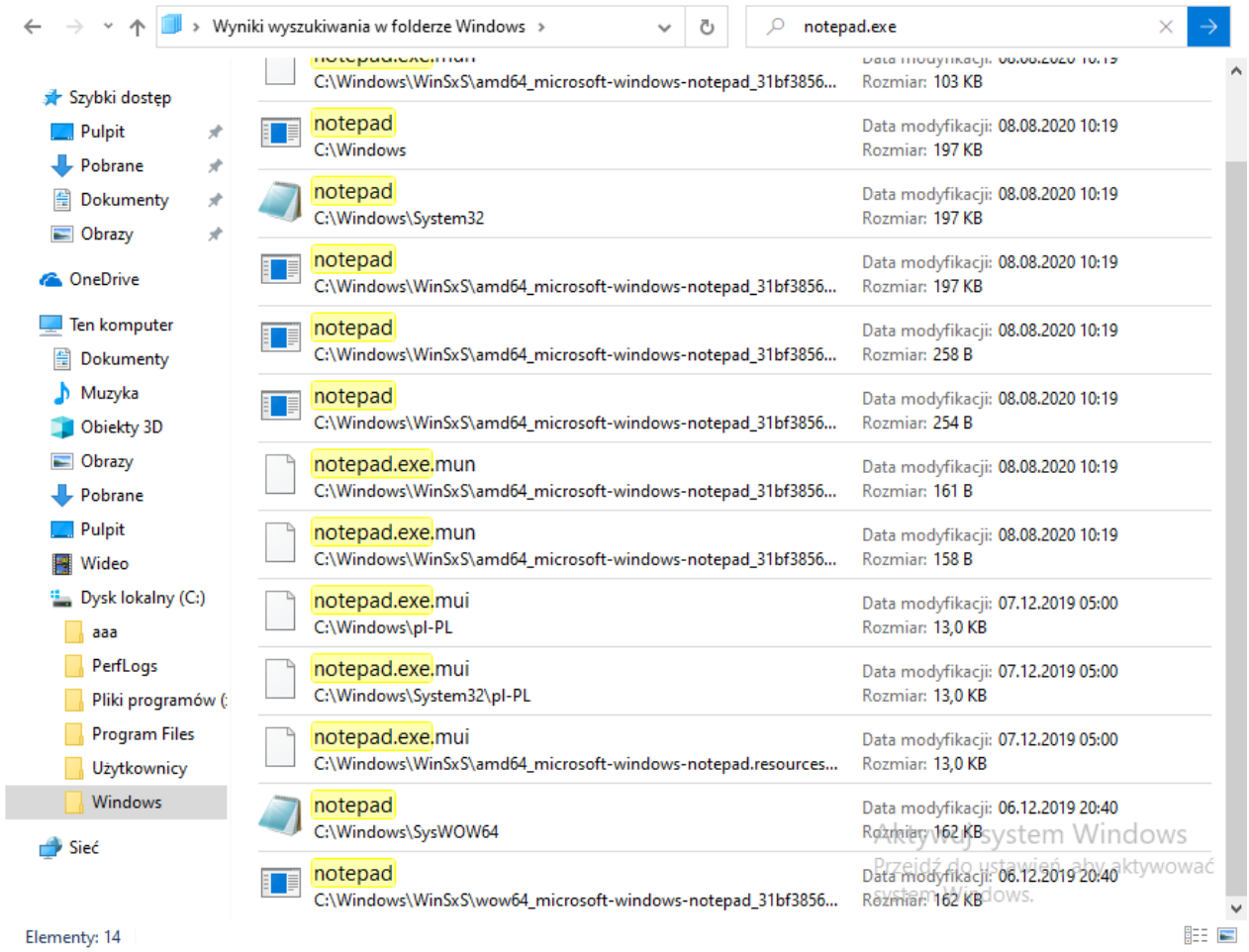


Sprawdzamy ścieżkę c:\Windows\notepad.exe.

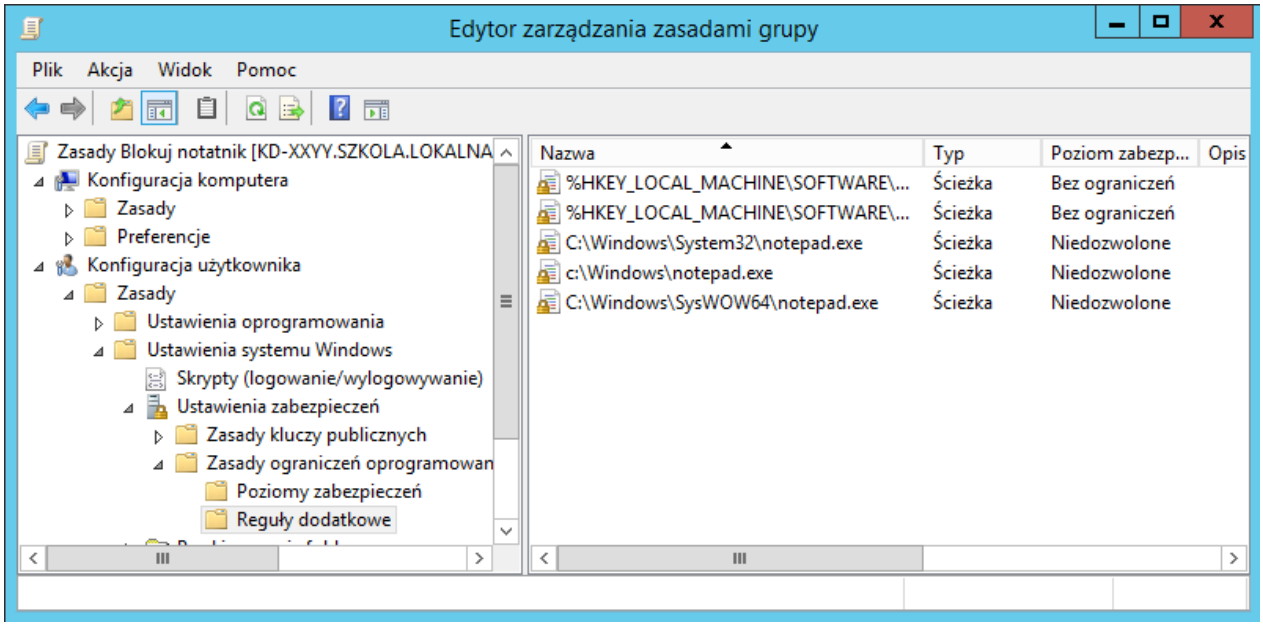


Okazuje się że notatnik się otwiera. Przeszukując katalog Windows okazuję się że taki wystąpień jest więcej.

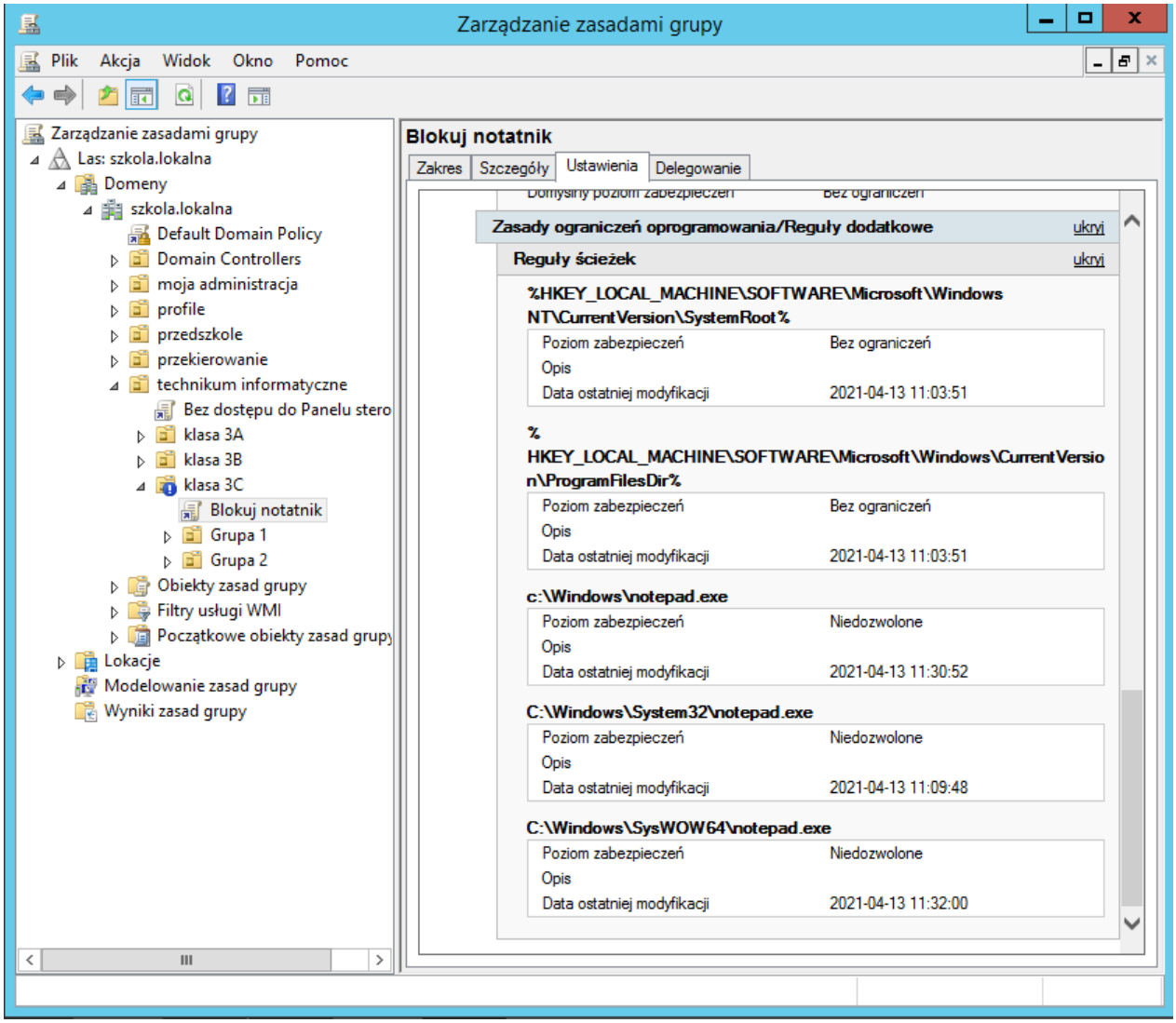
Należy dodać dodatkowe reguły ścieżki.



Dodajemy dodatkowe ścieżki. Zamykamy Edytor…



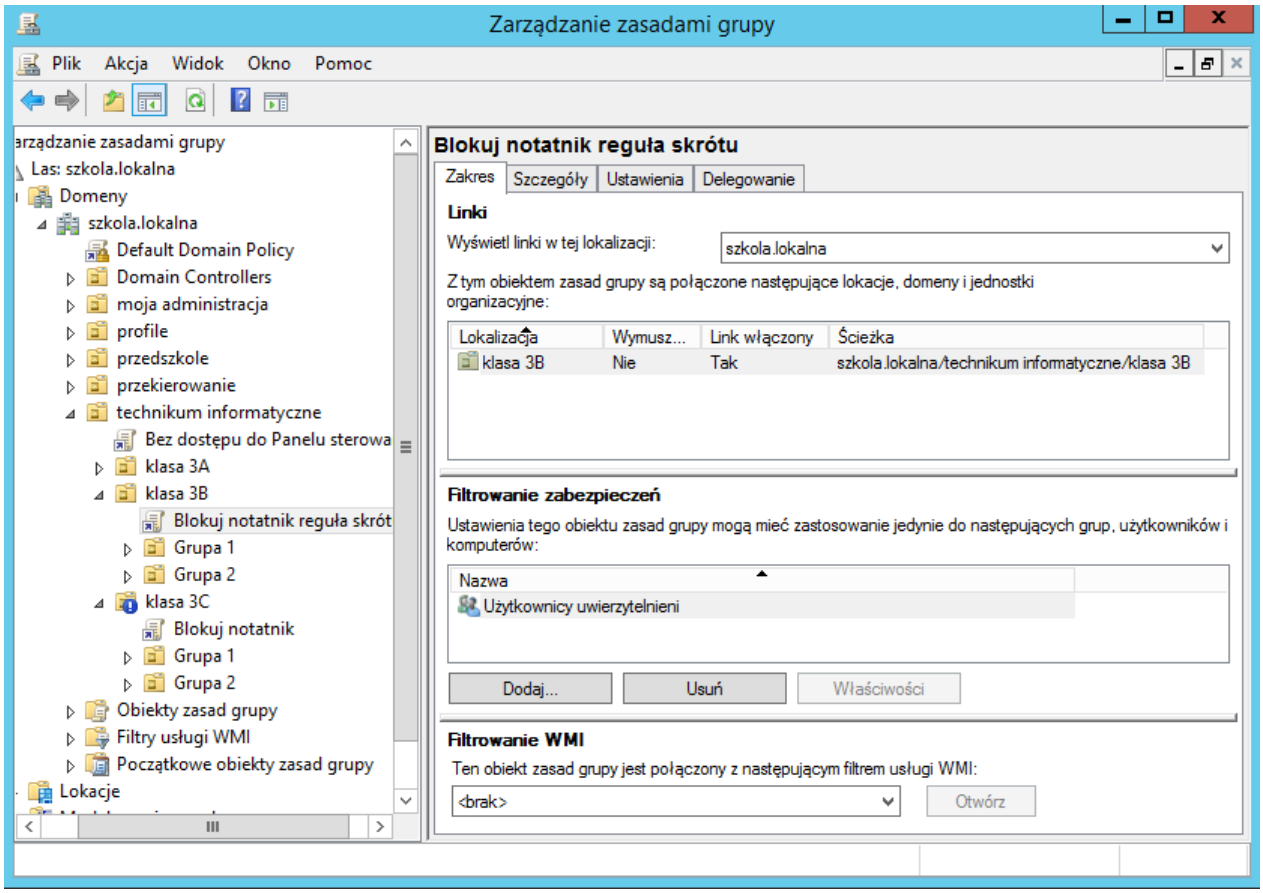
Weryfikujemy ustawienia



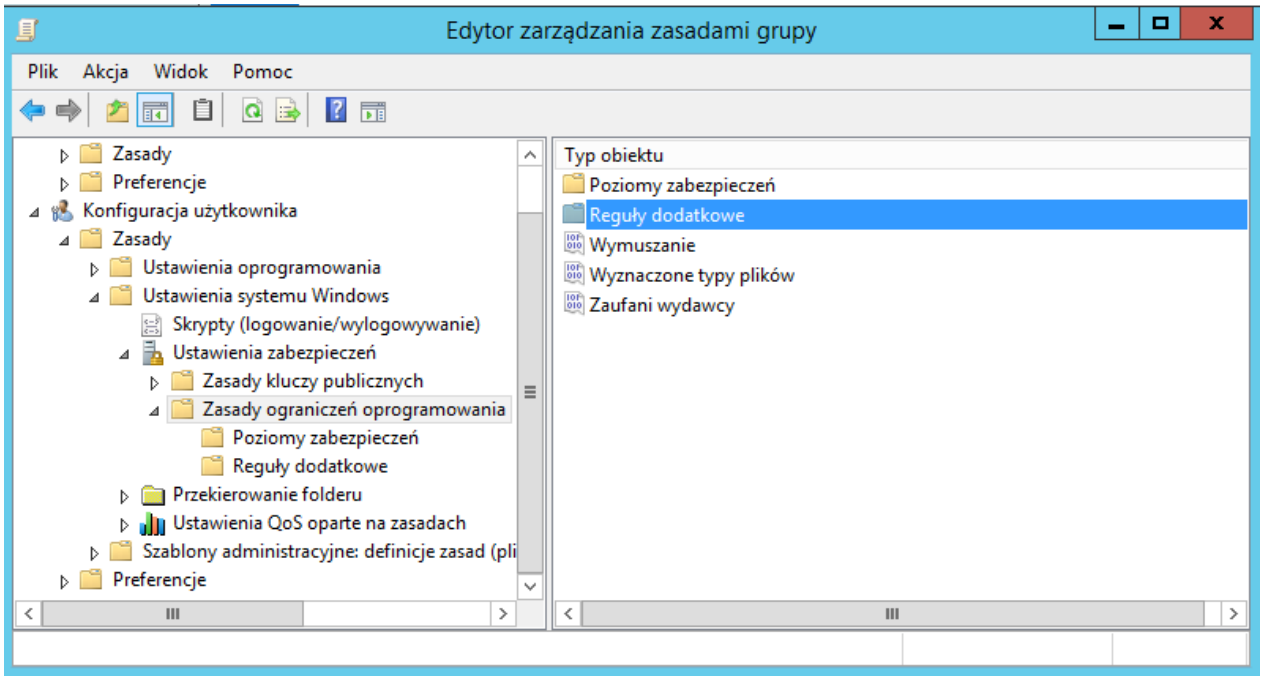
Logujemy się na kliencie i sprawdzamy skuteczność działania skonfigurowanego GPO.

Reguła skrótu -– użytkownicy JO klasa 3B

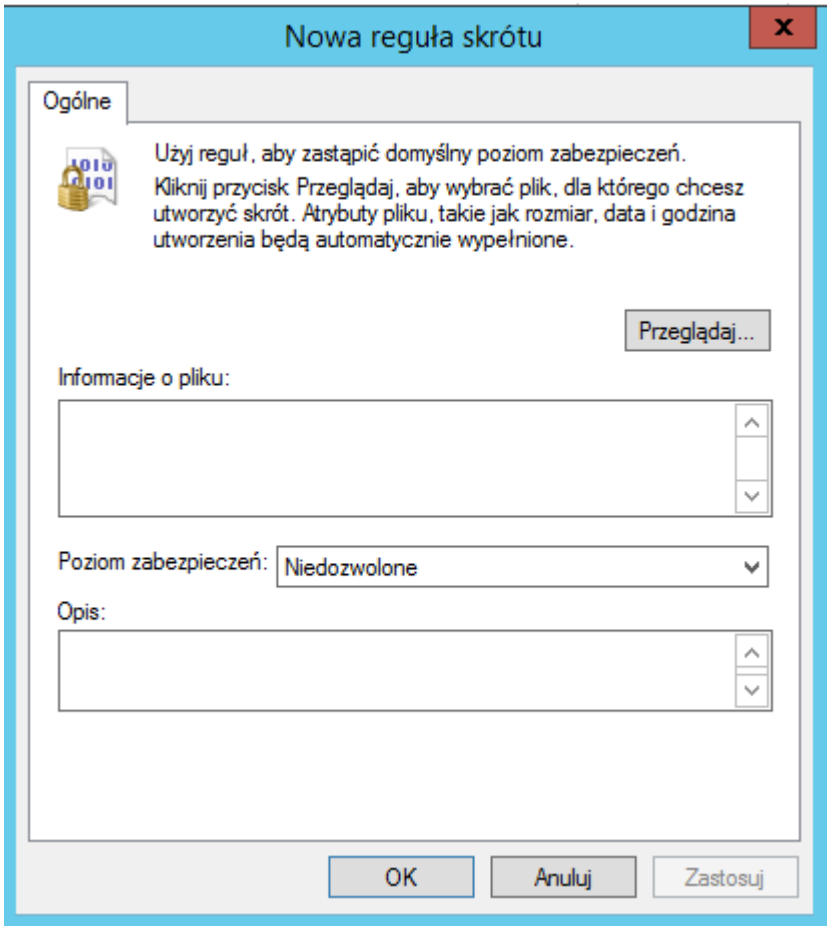
Tworzymy GPO **Blokuj notatnik reguła skrótu** i łączymy go z JO **klasa 3B**



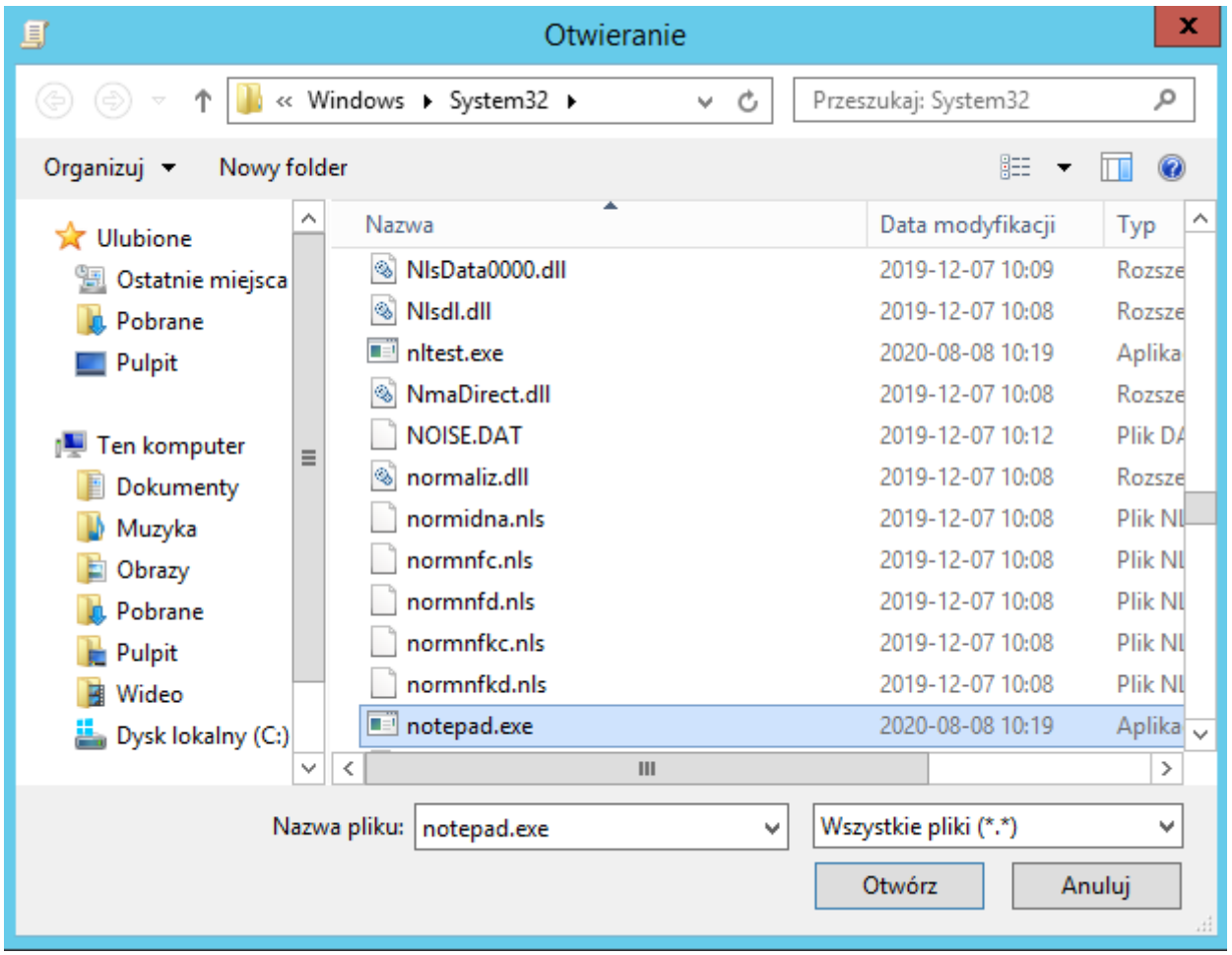
Edytujemy GPO **Blokuj notatnik reguła skrótu**. W **Reguły dodatkowe** wybieramy **Nowa reguła skrótu**



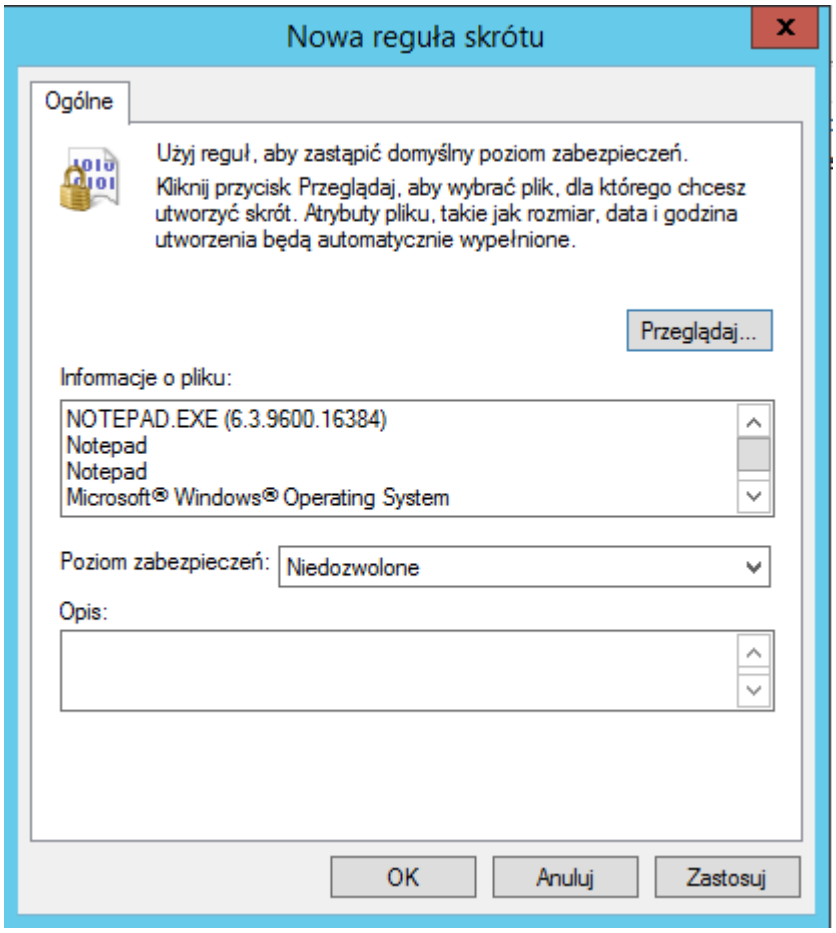
Klikamy przeglądaj



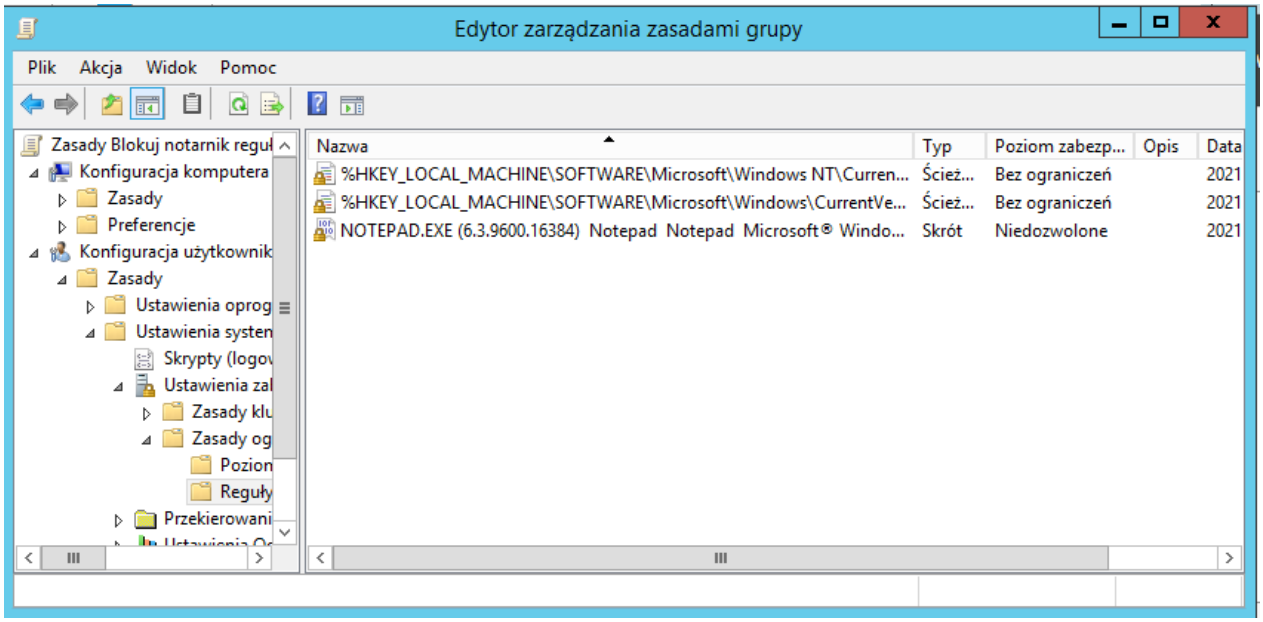
W katalogu System32 w polu Nazwa pliku wpisujemy notepad.exe i klikamy Otwórz



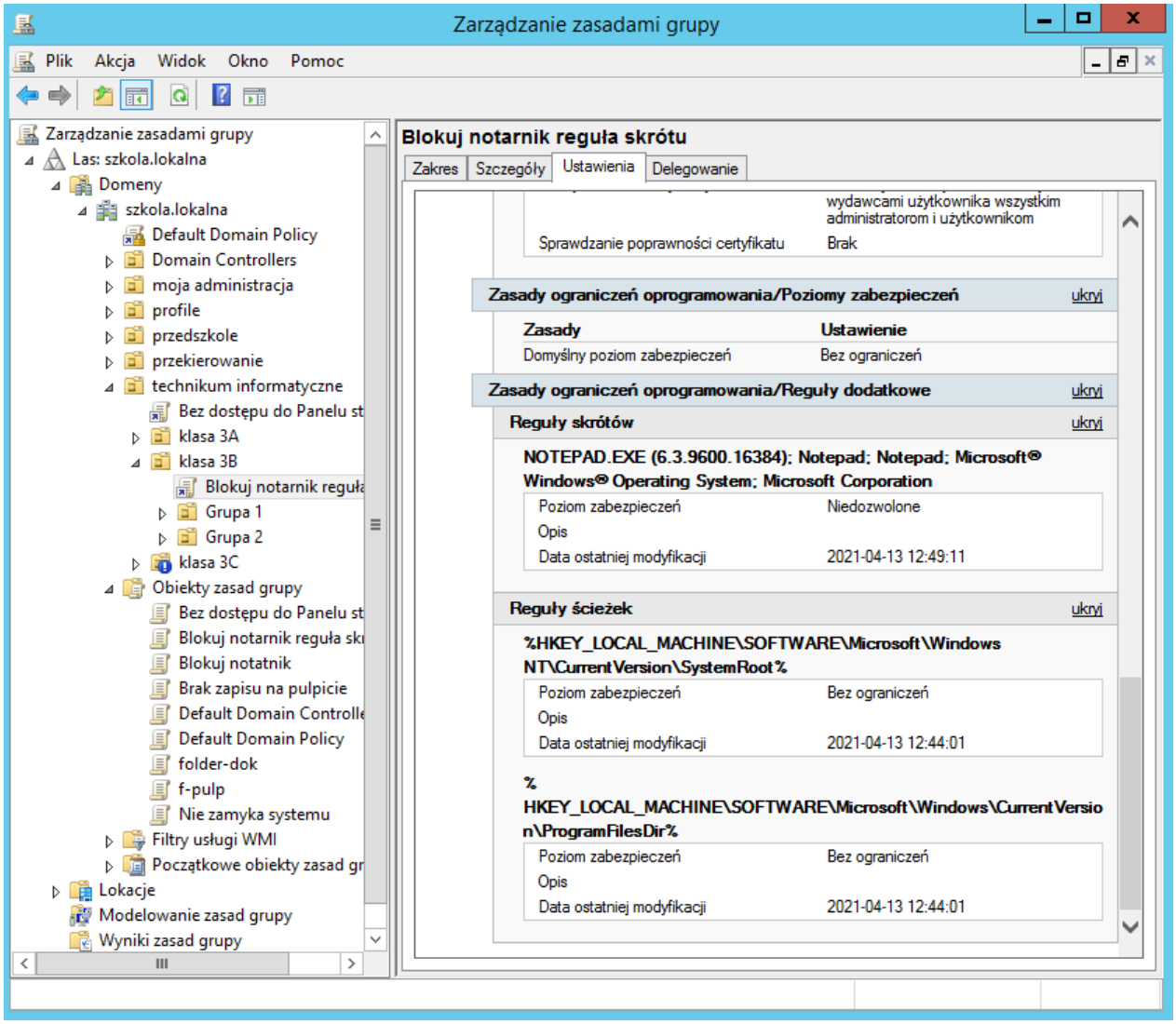
Przetworzone informacje o pliku zostały zapisane. W opisie można wpisać Windows Serwer 2012. Klikamy Zastosuj i OK



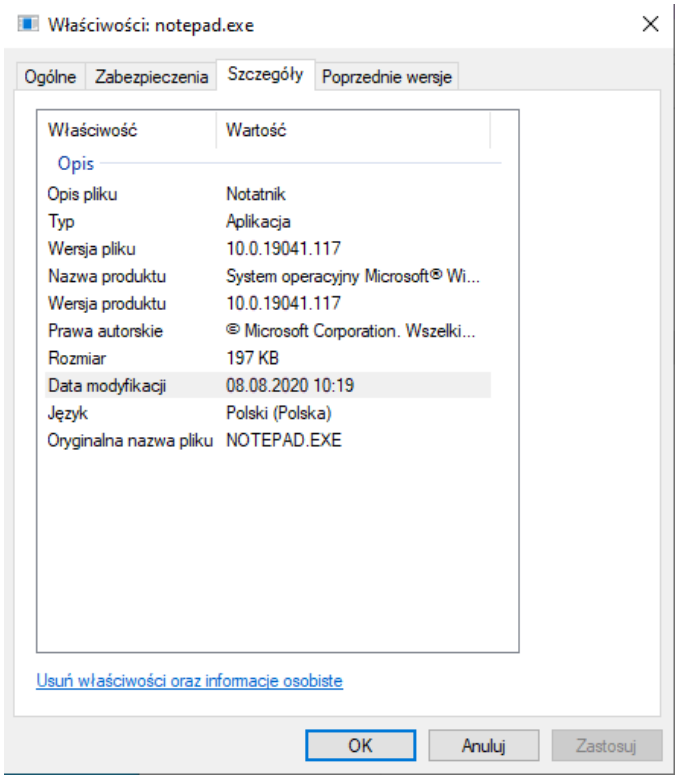
Reguła została zapisana



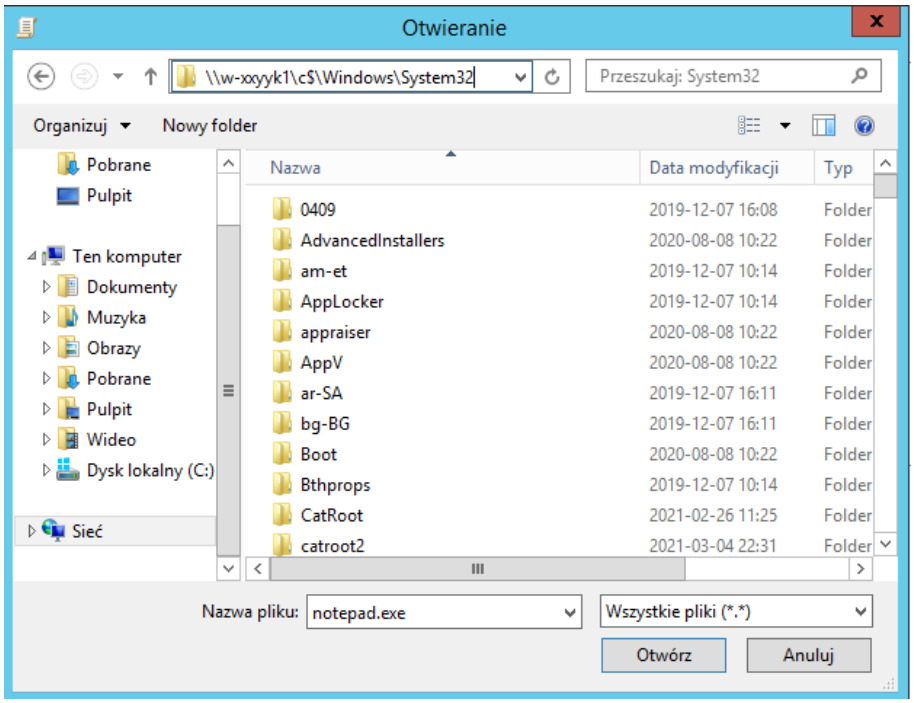
Weryfikujemy konfigurację e raporcie Ustawienia



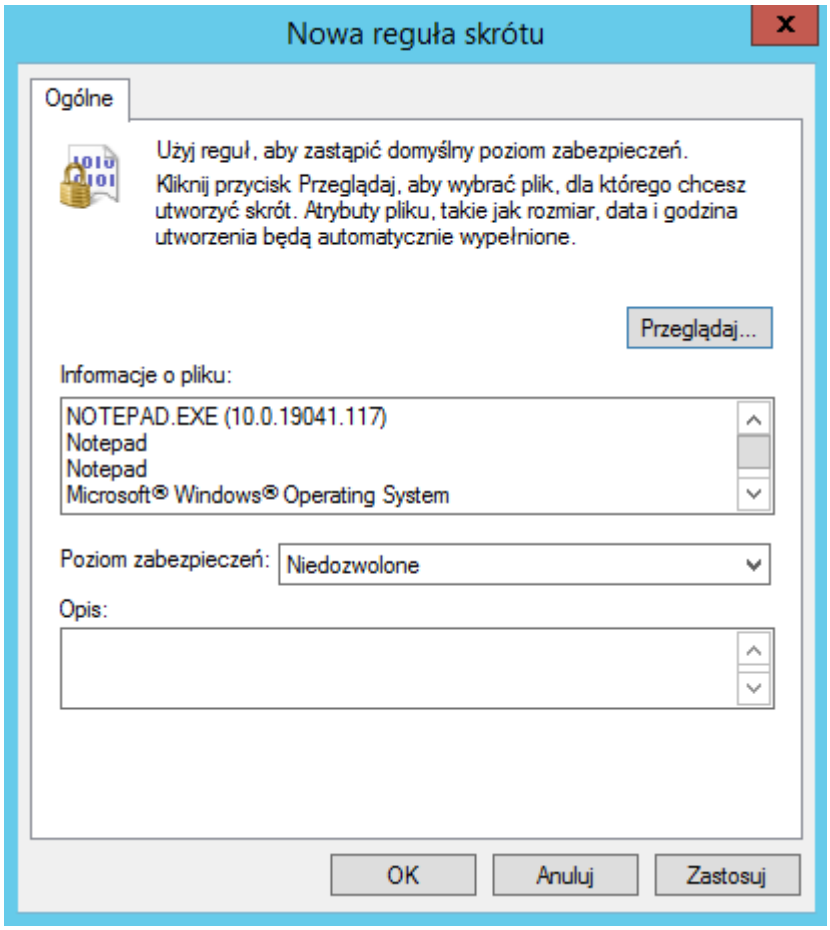
Sprawdzamy na kliencie użytkownika 3b-k1. Notatnik się otwiera. Odświeżmy zasady grupy wpisując w okienku Uruchom gpupdate.exe. Notatnik się otwiera. Sprawdzamy wersję notatnika. Jest inna.



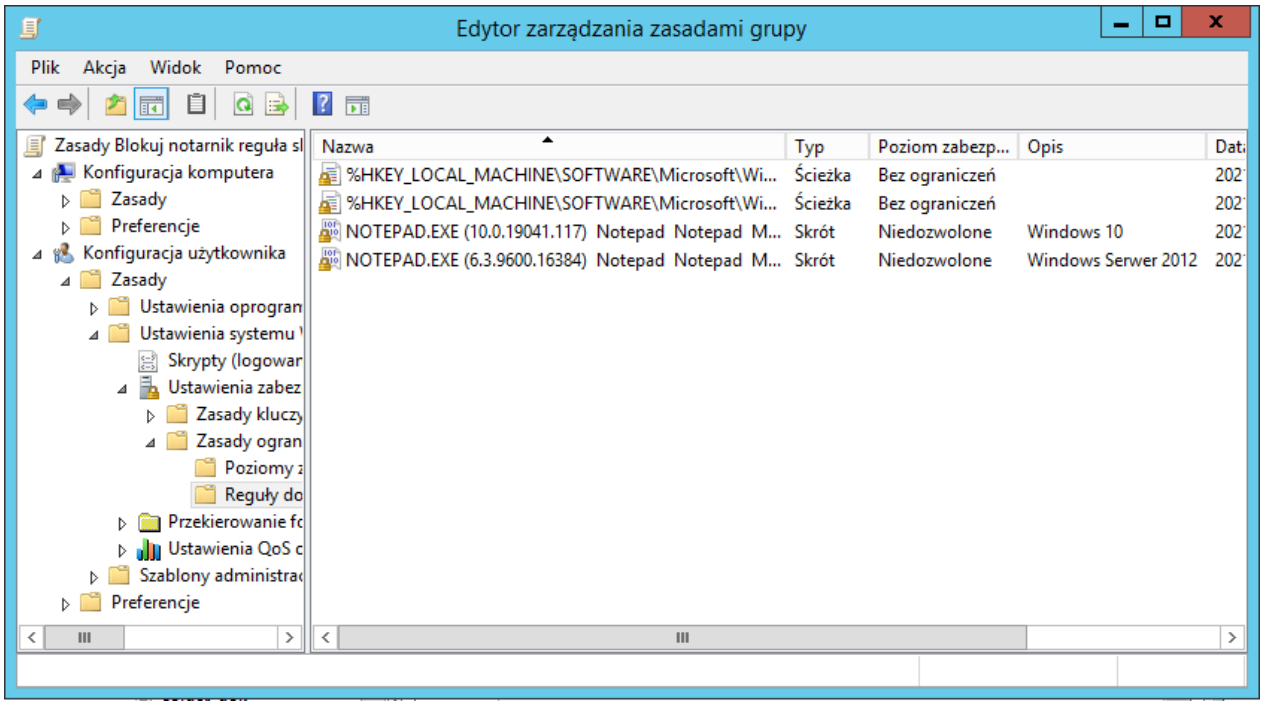
Wracamy na serwer. Wybieramy Nowa reguła skrótu. W oknie wyszukiwania pliku, wpisujemy ścieżkę UNC :do katalogu System32 na kliencie: \\w-xxyyk1\c$\Windows\System32 .W polu Nazwa pliku wpisujemy notepad.exe. Klikamy Otwórz



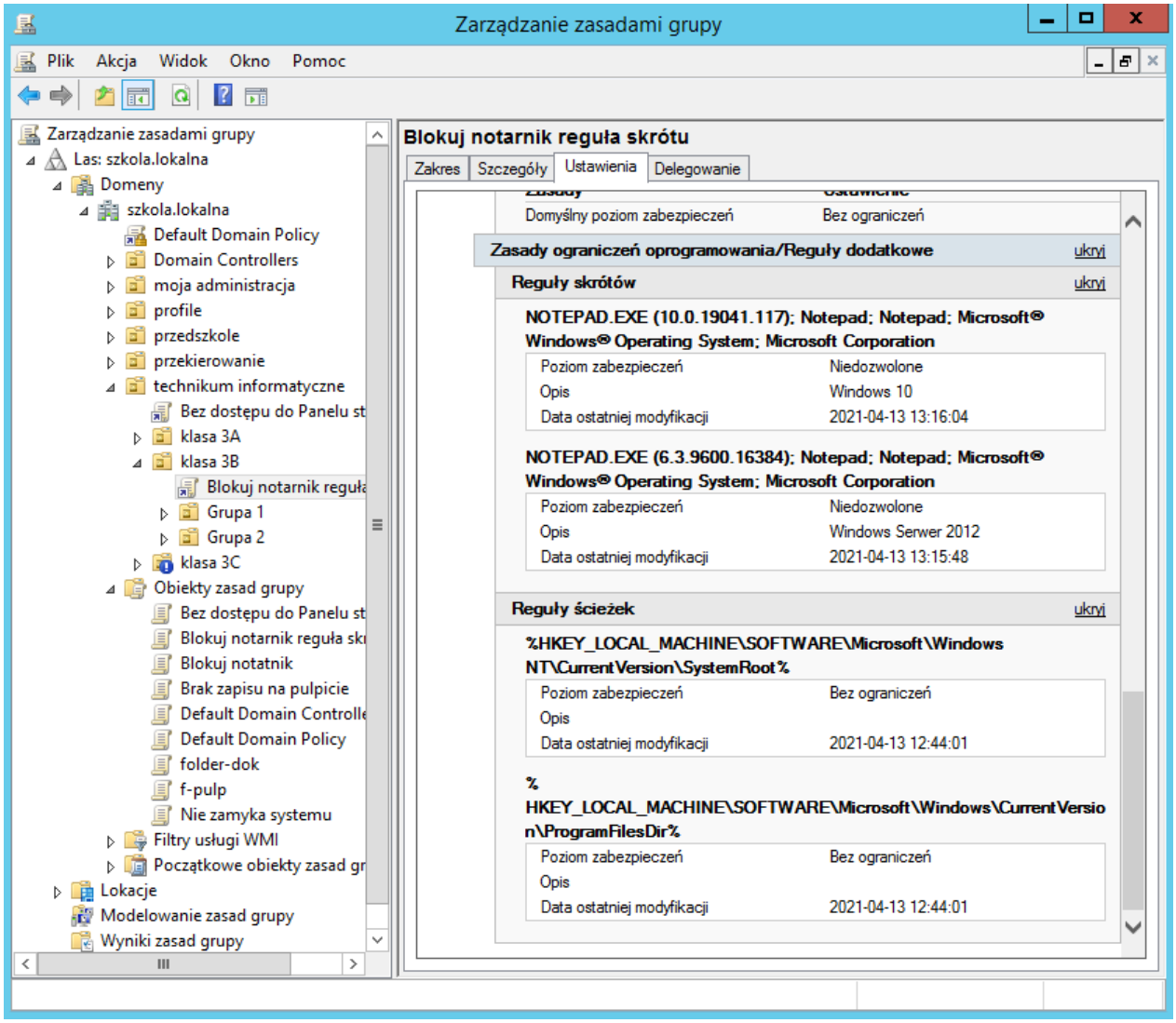
Informacja o pliku notepad.exe została wczytana. W opisie można wpisać Windows 10.



Mamy drugą regułę skrótu z inną wersją notatnika. Gdybyśmy mieli jeszcze inne wersje należy je wczytać. Po aktualizacji pliku też może się okazać, że nie działa i należy zasadę zaktualizować- dodać nową.



Weryfikujemy konfigurację przeglądają raport Ustawienia.



Wracamy na klienta.

Odświeżamy GPO uruchamiając gpupdate.exe i wszystko działa poprawnie.