Prawa dostępu do serwera.

Nadawanie i odbieranie uprawnień –DCL.

Użytkownicy a role

Na SQL Server możemy wyróżnić trzy rodzaje ról:

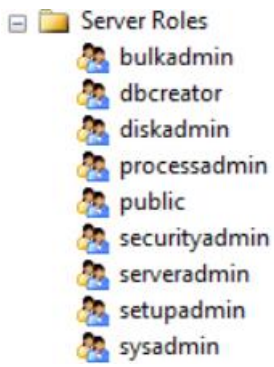
- Serwerowe
- Bazodanowe
- Zdefiniowane przez użytkownika

Role pozwalają grupować użytkowników, którzy mają mieć takie same prawa dostępu. Role serwerowe służą do przyznawania uprawnień operatorom serwera. Role bazodanowe wykorzystuje się do nadania użytkownikom standardowych zasad dostępu do baz danych. Możemy też tworzyć własne role - te role reprezentują najczęściej klasę pracowników w firmie i definiują ich dostęp do aplikacji ulokowanej w konkretnej bazie danych. takie role znacznie ułatwiają administracje aplikacją biznesową, Np. jeżeli pracownik zmienia stanowisko wystarczy przypisać go do nowej roli i odebrać mu poprzednią, a nie nadawać mu bardzo dużo uprawnień oddzielnie. Dodatkowo jeżeli zmieniają się uprawnienia dla zadanej klasy pracowników wystarczy zmienić uprawnienia dla roli, a nie oddzielnie dla np. tysiąca pracowników.

Poniższa tabela zawiera listę wszystkich ról serwerowych

sysadmin	Może wykonywać każdą czynność związaną z administrację serwerem
dbcreator	Może tworzyć i zmieniać ustawienia baz danych
diskadmin	Może zarządzać plikami dyskowymi
processadmin	Może zarządzać procesami SQL Servera
serveradmin	Może konfigurować ustawienia serwera.
setupadmin	Może zainstalować replikację.
securityadmin	Może zarządzać loginami na SQL Serverze.
bulkadmin	Może wykonywać BULK INSERT.

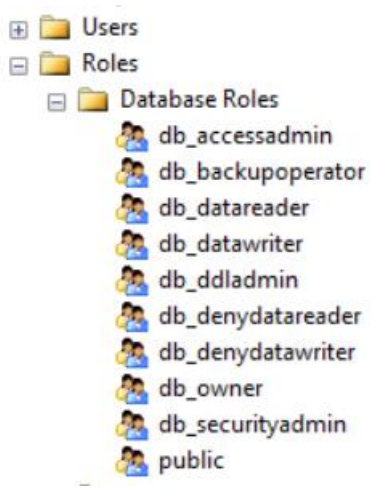
BULK INSERT - Za jego pomocą możemy wykonać szybki, masowy import danych z pliku tekstowego do istniejącej tabeli w bazie danych – z poziomu skryptu T-SQL



Role bazodanowe:

public	Posiada wszystkie publiczne uprawnienia

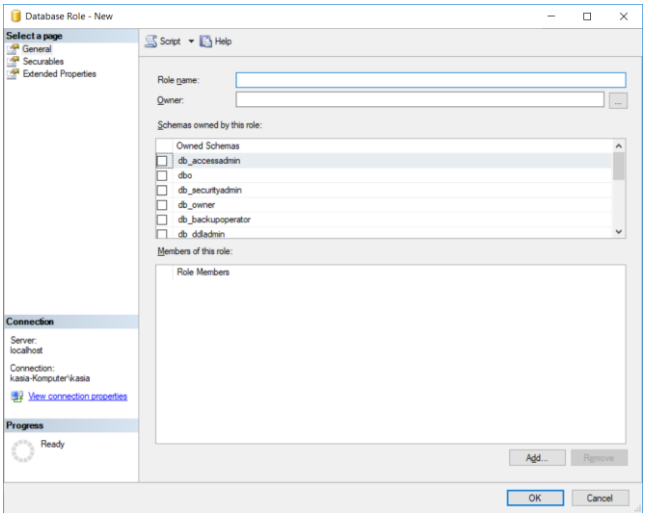
db_owner	Może przeprowadzić każde działanie na bazie danych
db_accessadmin	Może dodawać, kasować użytkowników baz danych, grupy i role użytkownika
db_ddladmin	Może tworzyć, modyfikować i kasować obiekty baz danych
db_securityadmin	Może zarządzać uprawnieniami systemowymi i obiektowymi
db_backupoperator	Może archiwizować bazę danych
db_datareader	Może czytać z każdej tabeli.
db_datawriter	Może pisać do każdej tabeli.
db_denydatareader	NIE może czytać z żadnej tabeli.
db_denydatawriter	NIE może pisać do żadnej tabeli.



Stworzenie własnej roli w bazie na SQL Serverze pozwala na grupowanie użytkowników z identycznymi uprawnieniami. Takie role powinno się tworzyć:

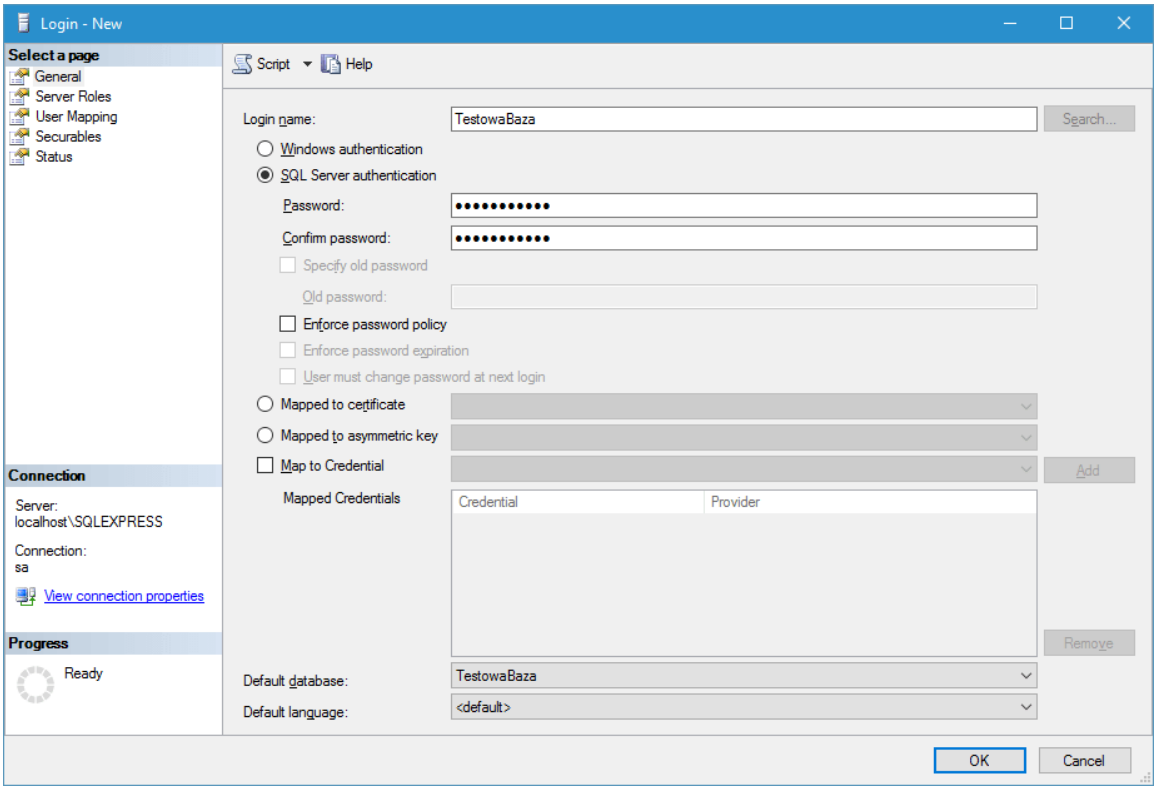
- Kiedy grupa ludzi powinna wykonywać te same czynności na SQL Serverze, a nie istnieje taka grupa w systemie Windows
- Kiedy nie mamy uprawnień do zarządzanie kontami systemu Windows

Grupy zdefiniowane przez użytkownika pozwalają na grupowanie uprawnień i łatwe zarządzanie nimi. Nową rolę możemy utworzyć korzystając z Enterprise Managera - w bazie danych wybieramy zakładkę Roles i wybieramy New



Jak w MS SQL stworzyć użytkownika i nadać prawa do bazy danych

Aby to uczynić należy wpierw otworzyć SQL Server Management Studio i podłączyć się do wybranej instancji. Następnie trzeba rozwinąć sekcję serwera oraz pozycję Security, a następnie kliknąć prawym klawiszem na pozycji Logins. W menu podręcznym które zostanie wyświetlone wystarczy wybrać New Login… co otworzy okno tworzenia nowego loginu.



Teraz trzeba podać jego nazwę w polu Login name oraz hasło w polach Password i Confirm password. Można także odznaczyć opcję Enforce password policy. Alternatywnie można pozostawić tę opcję zaznaczoną, ale odznaczyć dwie następne: Enforce password expiration oraz User must change password at the next login.

Dodatkowo w polu Default database należy wybrać bazę danych do której dostęp ma mieć tworzony użytkownik.

Na koniec konieczne jest jeszcze przejście do widoku User Mapping gdzie w górnej części okna trzeba zaznaczyć to której bazy użytkownika ma mieć dostęp: TestowaBaza. Następnie w dolnej części okna zaznaczyć np.role db_datawriter i db_datareader czy db_owner.

Konto specjalne - dbo

Jest to konto specjalne, członkowie grupy Sysadmin są mapowanie automatycznie na to konto.

Uprawnienia na SQL Server

Po zmapowaniu loginów na użytkowników i przypisaniu ich do ról nadszedł czas aby przypisać im uprawnienia bezpośrednio. Uprawnienia przypisuje się tak samo użytkownikom i rolom stworzonym przez użytkownika. Uprawnienia specyfikują z jakich obiektów i co z tymi obiektami mogą robić użytkownicy. Uprawnienia użytkownika w danej bazie danych zależą od uprawnień jakie ma konto tego użytkownika i uprawnienia jakie mają role, do których należy ten użytkownik.

Na SQL Serwerze istnieją dwa rodzaje uprawnień systemowe i obiektowe. Systemowe to np:

- CREATE DATABASE
- CREATE TABLE
- CREATE VIEW
- CREATE PROCEDURE
- CREATE FUNCTION
- CREATE RULE
- CREATE DEFAULT
- BACKUP DATABASE

Uprawnienia obiekotwe na tabeli i perwspektywie to:

- SELECT
- INSERT
- DELETE
- UPDATE

Uprawnienia obiektowe na kolumnie to:

- SELECT
- UPDATE
- REFERENCES

Uprawnienia obiektowe na procedurze to:

- EXECUTE

Przyznawanie uprawnień

Przyznawanie uprawnień na SQL Serwerze jest trzy stopniowe. Uprawnienia mogą być przyznane (granted), zabronione (denied), albo odebrane (revoked). Uprawnienia, które nie zostały nadane, ani zabronione są neutralne - czyli zachowują się jakby były odebrane. Poniższa tabel podsumowuje stany uprawnień.

przyznane granted	**-**	**Użytkownik może przeprowadzić zadaną akcję.**
zabronine - deny		Użytkownik nie może wykonać zadanej operacji. Ta opcja jest nadrzędna
revoke	**-**	Użytkownik nie może wykonać zadanej operacji, ale może to być nadpisane poprzez

odebrane	przynależność do roli.

Uprawnienia przyznane (granted) kumulują się więc, czyli użytkownik może wykonać każdą operacje jaka została jemu przyznana plus operacja, na które mają uprawnienia role, do których należy. Jak użytkownik ma DENY na jakimś uprawnieniu to to ustawienie nadpisuje wszystkie inne. Użytkownik ma prawo do wykonywania operacji jeśli obydwie poniższe reguły są prawdziwe:

- Uprawnienie zostało nadane bezpośrednio bądź poprzez rolę, do której należy użytkownik.
- Uprawnienie nie zostało zabronione bezpośrednio użytkownikowi, ani żadnej grupie, do której należy.

Archwizacja baz danych

Każdy administrator powinien pamiętać o tym jak ważne jest wykonywanie archwizacji baz danych. Jednymi z powodów są:

- Zabezpieczenie przed przypadkowym wykoaniem instrukcji DELETE badź UPDATE - np.
- Zabezpieczenie przed wirusami
- Zabezpieczenie przed żywiołami
- Zabezpieczenie przed kradzieżą

Podstawowa zasada dotycząca archiwizacji to : Wykonywać ją regularnie!!

Każda baza danych na SQL Server ma przypisany Recovery Model. W zależności od tego ustawienia mamy różne możliwości dotyczące rchiwizacji. Na SQL Server mamy moliwo ustawienia trzech rodzajw Revore Model:

- Full Recovery
- Bulk Logged
- Simple

Full Recovery tego trybu powinno się używać dla najważniejszych baz w przedsiębiorstwie. W tym trybie SQL Server zapisuje wszystkie zmiany jakie zaszły w bazie danych, łącznie z operacjami typu BULK i tworzeniem indeksów. Dzięki temu SQL Server jest w stanie odtworzyćwszystkie dane do chwili awarii, oprócz transakcji, które akurat trwały podczas awarii. Jedynym minusem tego trybu jest duży rozmiar transactional logu.

Bulk Logged tryb ten podobny jest do Full Recovery, natomiast złużywa on mniej przestrzeni Transactional Log, gdyż nie loguje takich operacji jak tworzenie indeksu, operacje typu BULK, procedure WRITETEXT.

Simple Recovery ten tryb jest dobry dla małych baz danych, w których dane nie zmianiają się za często. Ten try pozwala odtworzyć tylko dane do ostatniej archiwizacji.