



BAZY DANYCH

WYKŁAD II

MECHANIZM UPRAWNIENÍ W MSSQL SERVER

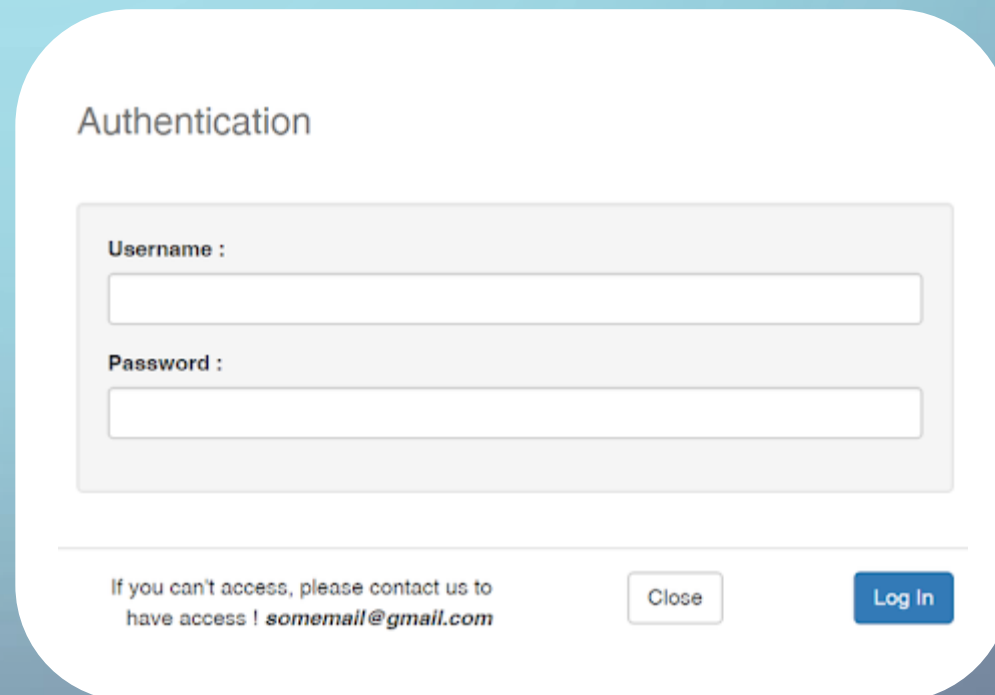
MS SQL SERVER

SQL Server jest systemem zarządzania relacyjną bazą danych opracowanym, wspieranym i rozpowszechnianym przez Microsoft. W bardzo prostym rozumieniu jest to relacyjny system baz danych, za pomocą którego zarządzamy elementami bazy takimi jak tabele, widoki, elementy programistyczne. System charakteryzuje się tym, iż jako język zapytań używany jest przede wszystkim Transact-SQL, który stanowi rozwinięcie standardu ANSI/ISO (SQL Server posiada wysoką zgodność ze standardem SQL).

SQL Server 2019 (Express?) + SQL Server Management Studio (SSMS) 18.10

UWIERZYTELNIANIE I AUTORYZACJA SQL SERVER

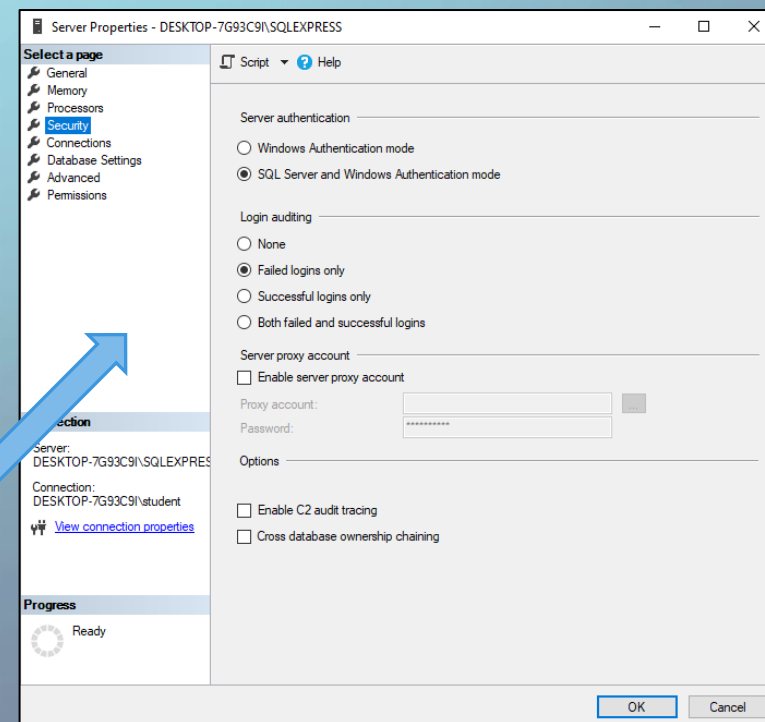
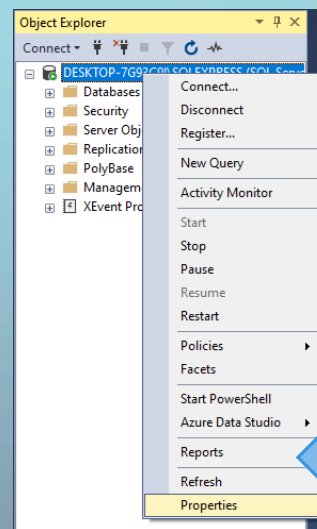
- Ochrona danych
- Uwierzytelnianie użytkowników
- Autoryzacja dostępu do danych.

A white authentication dialog box with rounded corners. It has a title 'Authentication' at the top. Below the title, there are two input fields: 'Username :' and 'Password :'. At the bottom, there is a line of text: 'If you can't access, please contact us to have access ! *somemail@gmail.com*'. To the right of this text are two buttons: 'Close' and 'Log In'.

TRYBY UWIERZYTELNIANIA W MS SQL SERVER

Microsoft SQL Server oferuje administratorom dwie możliwości implementacji sposobu uwierzytelniania użytkowników przez system:

- tryb uwierzytelniania systemu Windows
- tryb mieszanego uwierzytelniania



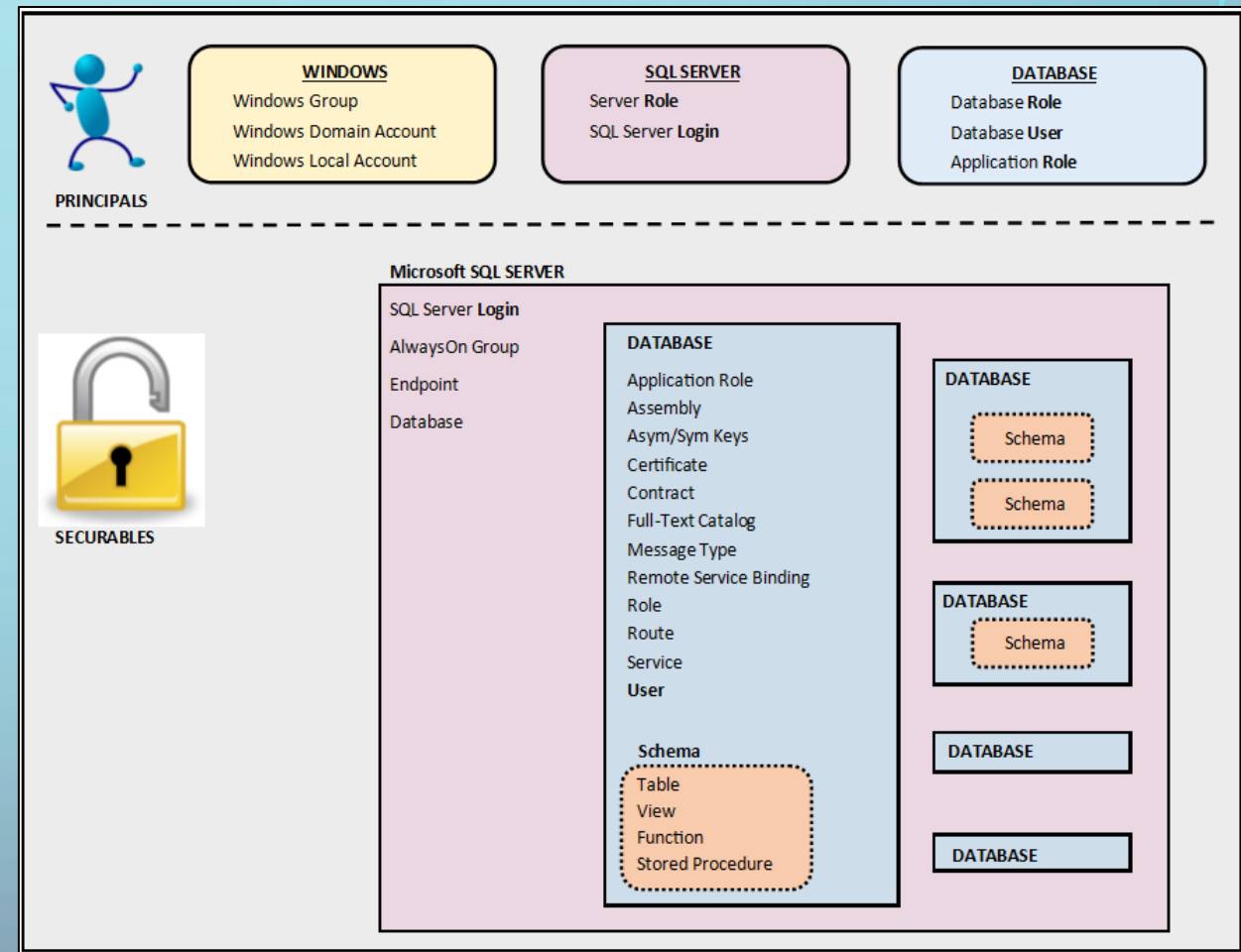
TRYBY UWIERZYTELNIANIA W MS SQL SERVER

Uwierzytelnianie systemu Windows oznacza, że SQL Server sprawdza tożsamość użytkownika, używając tylko jego nazwy użytkownika i hasła Windows. Jeśli użytkownik został już uwierzytelniony przez system Windows, SQL Server nie pyta o hasło.

Tryb mieszany oznacza, że SQL Server umożliwia uwierzytelnianie systemu Windows i uwierzytelnianie serwera SQL. Uwierzytelnianie serwera SQL tworzy loginy użytkownika niepowiązane z systemem Windows.

KONTROLA DOSTĘPU

Istnieje wiele podmiotów (bytów, tłum. z *Principals*) mogących żądać zasobów programu SQL Server. Podobnie jak inne składniki modelu autoryzacji SQL Server podmioty te mogą występować pojedynczo lub być zorganizowane w hierarchię.



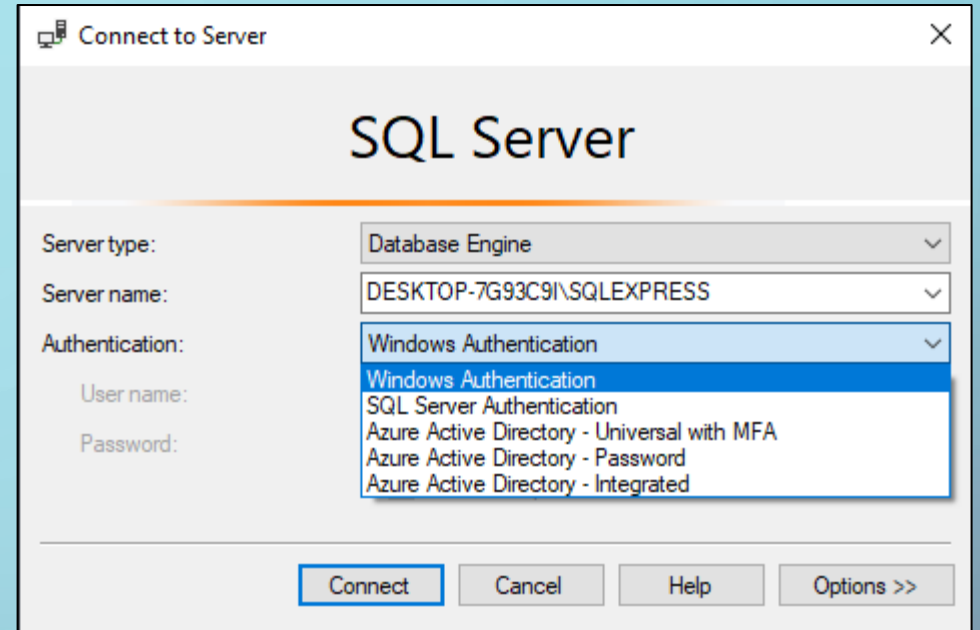
TOŻSAMOŚĆ I KONTROLA DOSTĘPU

- Principals – to byty żądające zasobów, np. użytkownicy baz danych, konta logowania,
- Securables – to obiekty, które mogą być chronione, np. tabele, procedury, funkcje,
- Roles - stałe role serwera, role bazy danych, role użytkowników,
- Permissions - przywileje, które principal otrzymuje do danego securable.

PRINCIPALS

Podmioty na poziomie serwera
(SQL Server-level principals)

- Login w SQL Server,
- Logowanie w systemie Windows,
- Grupa w systemie Windows,
- Logowanie w Azure Active Directory dla użytkownika AD,
- Logowanie w Azure Active Directory dla grupy AD,
- Rola Serwera



PRINCIPALS

Podmioty na poziomie bazy danych (Database-level principals)

- Użytkownik bazy danych (Jest 12 typów użytkowników),
- Rola bazy danych,
- Rola Aplikacji.

! SCHEMAT - kontener składający obiekty (tabele, widoki, funkcje, procedury, etc)

SECURABLES

Obiekty tworzące środowisko serwera i bazy danych. Obiekty można podzielić na trzy hierarchiczne poziomy:

- Zabezpieczenia na poziomie serwera obejmują takie obiekty, jak bazy danych i grupy dostępności.
- Zabezpieczane na poziomie bazy danych obejmują takie obiekty, jak schematy i katalogi pełnotekstowe.
- Zabezpieczane na poziomie schematu obejmują takie obiekty, jak tabele, widoki, funkcje i procedury składowane.

Poziomy: serwer, baza danych, schemat

PUBLICZNE ROLE BAZY DANYCH I SERWERA

Każda instancja SQL Server zawiera stałą rolę serwera *public*, a każda baza danych (w tym bazy danych systemowych) zawiera stałą rolę bazy danych *public*. Wszystkie loginy należą do roli serwera *public*, a wszyscy użytkownicy bazy danych należą do roli bazy danych *public*. Nie można usunąć żadnej roli, ani dodawać członków ani usuwać członków z żadnej roli.

Silnik bazy danych domyślnie przypisuje zestaw uprawnień do ról. Loginy dziedziczą wszystkie uprawnienia przyznane roli serwera *public*, chyba że dane logowania zostały wyraźnie przyznane lub odrzucone. To samo dotyczy roli *public* bazy danych. Użytkownicy dziedziczą wszystkie uprawnienia, chyba że uprawnienia specjalnie im przyznano lub odmówiono.

PUBLICZNE ROLE BAZY DANYCH I SERWERA

Aby wyświetlić uprawnienia przypisane do roli *public* serwera, należy wykonać odpowiednią instrukcję:



SQLQuery1.sql - DE...93C9I\student (55))* -p X

```
SELECT pm.state_desc,  
       pm.permission_name,  
       pm.class_desc,  
       pm.major_id,  
       ep.name  
FROM sys.server_permissions pm  
JOIN sys.server_principals pr  
     ON pm.grantee_principal_id = pr.principal_id  
LEFT JOIN sys.endpoints ep  
     ON pm.major_id = ep.endpoint_id  
WHERE pr.name = 'public';
```

100 %

Results Messages

	state_desc	permission_name	class_desc	major_id	name
1	GRANT	VIEW ANY DATABASE	SERVER	0	NULL
2	GRANT	CONNECT	ENDPOINT	2	TSQL Local Machine
3	GRANT	CONNECT	ENDPOINT	3	TSQL Named Pipes
4	GRANT	CONNECT	ENDPOINT	4	TSQL Default TCP
5	GRANT	CONNECT	ENDPOINT	5	TSQL Default VIA

STAŁE ROLE BAZY DANYCH I SERWERA

Aby łatwo zarządzać uprawnieniami w bazach danych, SQL Server udostępnia kilka ról, które są podmiotami zabezpieczeń grupującymi inne podmioty. Są jak grupy w systemie operacyjnym Microsoft Windows. Role na poziomie bazy danych obejmują zakres uprawnień obejmujący całą bazę danych.

Istnieją dwa typy ról zdefiniowanych w bazie danych: stałe role (fixed-database role), które są predefiniowane w bazie danych oraz role zdefiniowane przez użytkownika.

Stałe role są definiowane na poziomie bazy i istnieją w każdej bazie danych. Członkowie roli bazy danych *db_owner* mogą zarządzać członkostwem w roli stałej bazy danych.

STAŁE ROLE BAZY DANYCH (FIXED-DATABASE ROLES)

db_owner – Członkowie stałej roli bazy danych *db_owner* mogą wykonywać wszystkie czynności związane z konfiguracją i konserwacją bazy danych, a także mogą usuwać bazę danych w programie SQL Server. (W SQL Database i Azure Synapse niektóre działania konserwacyjne wymagają uprawnień na poziomie serwera i nie mogą być wykonywane przez *db_owners*).

db_securityadmin – członkowie zarządzają uprawnieniami, członkostwem w rolach, mogą modyfikować członkostwo w rolach tylko dla ról niestandardowych i zarządzać uprawnieniami. Członkowie tej roli mogą potencjalnie podnieść swoje uprawnienia, a ich działania powinny być monitorowane.

db_accessadmin - Członkowie stałej roli bazy danych *db_accessadmin* mogą dodawać lub usuwać dostęp do bazy danych dla logowania Windows, grup Windows i logowania SQL Server.

STAŁE ROLE BAZY DANYCH

db_backupoperator – Członkowie stałej roli bazy danych *db_backupoperator* mogą tworzyć kopię zapasową bazy danych.

db_ddladmin – członkowie mogą wykonać dowolną instrukcję języka DDL w danej bazie.

db_datawriter – członkowie mogą wykonać dowolną instrukcję języka DML w danej bazie

db_datareader - Członkowie stałej roli bazy danych *db_datareader* mogą odczytywać wszystkie dane ze wszystkich tabel i widoków użytkownika. Obiekty użytkownika mogą istnieć w dowolnym schemacie z wyjątkiem sys i *INFORMATION_SCHEMA*.

db_denydatawriter – Członkowie stałej roli bazy danych *db_denydatawriter* nie mogą dodawać, modyfikować ani usuwać żadnych danych w tabelach użytkowników w bazie danych.

db_denydatareader – Członkowie stałej roli bazy danych *db_denydatareader* nie mogą odczytywać żadnych danych z tabel i widoków użytkownika w bazie danych.

STAŁE ROLE SERWERA

sysadmin – Członkowie stałej roli serwera *sysadmin* mogą wykonywać dowolne działania na serwerze.

serveradmin – Członkowie stałej roli serwera *serveradmin* mogą zmieniać opcje konfiguracji całego serwera i wyłączać serwer.

securityadmin – Członkowie zarządzają dowolnymi kontami logowania, użytkownikami, uprawnieniami, członkostwem w rolach.

setupadmin - Członkowie stałej roli serwera *setupadmin* mogą dodawać i usuwać serwery połączone za pomocą instrukcji języka Transact-SQL. (członkostwo *sysadmin* jest wymagane podczas korzystania z Management Studio).

STAŁE ROLE SERWERA

dbcreator – członkowie zarządzają dowolną bazą w instancji (mogą tworzyć, zmieniać, usuwać i przywracać dowolną bazę danych).

diskadmin – członkowie zarządzają plikami baz danych na dysku.

bulkadmin – członkowie mogą uruchomić instrukcje BULK INSERT

processadmin - członkowie zarządzają procesami instancji

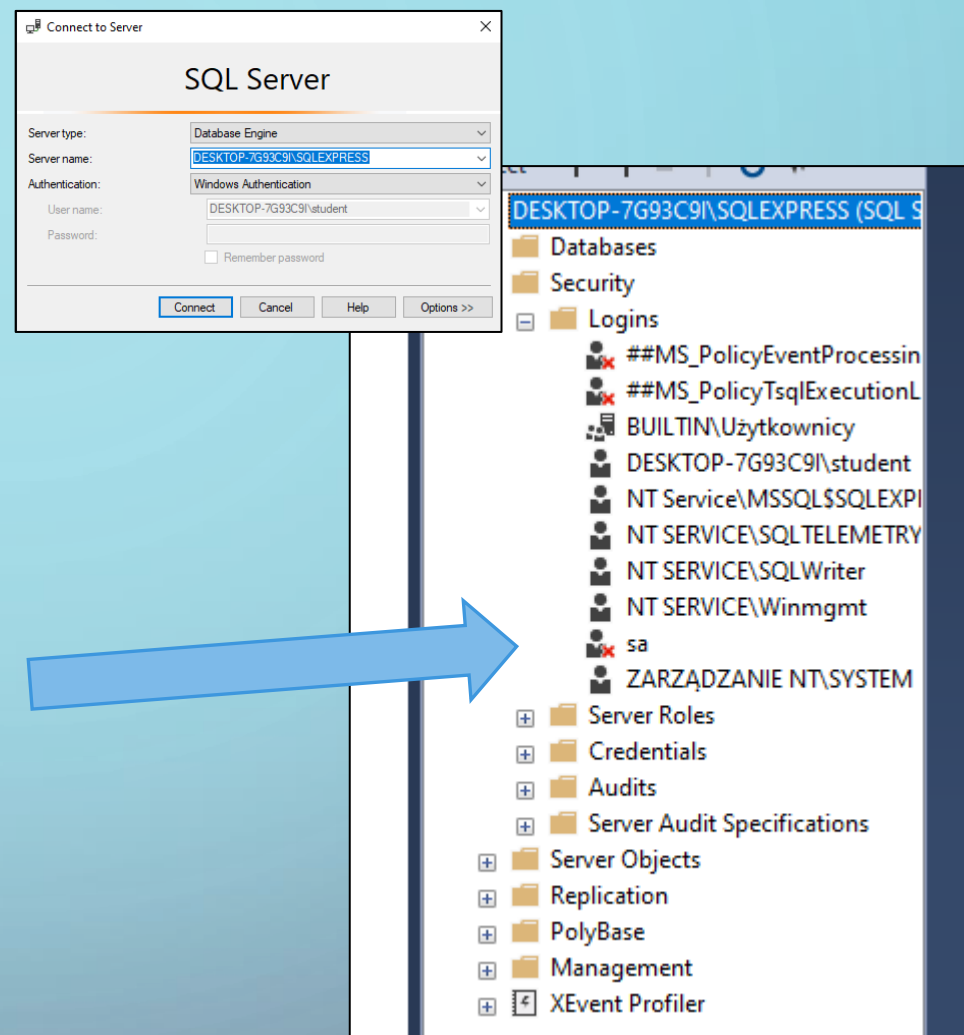
public – członkowie widzą bazy danych w instancji

PREDEFINIOWANE KONTA UŻYTKOWNIKÓW

SQL Server posiada użytkowników, predefiniowane konta użytkowników oraz stałe role bazy danych.

Użytkownik 'sa'

sa (system administrator) to podmiot z poziomu serwera (server-level). Jest automatycznie dodawany jako członek *sysadmin* (roli serwera) i posiada wszystkie uprawnienia do tej instancji co umożliwia mu wykonywanie dowolne działania.



Użytkownik 'sa'

Można sprawdzić, czy logowanie sa jest wyłączone, wysyłając odpowiednie zapytanie do sys.server.principals.

```
SQLQuery1.sql - DE...93C9\student (54))* -> X
USE master;
GO
SELECT principal_id, type_desc, is_disabled
FROM sys.server_principals
WHERE name = 'sa';
```

100 %

Results Messages

	principal_id	type_desc	is_disabled
1	1	SQL_LOGIN	1

Można zweryfikować członkostwo podmiotu sa

```
SQLQuery1.sql - DE...93C9\student (54))* -> X
SELECT member.name
FROM sys.server_role_members rm
JOIN sys.server_principals role
ON rm.role_principal_id = role.principal_id
JOIN sys.server_principals member
ON rm.member_principal_id = member.principal_id
WHERE role.name = 'sysadmin';
```

100 %

Results Messages

	name
1	sa
2	DESKTOP-7G93C9\student
3	NT SERVICE\SQLWriter
4	NT SERVICE\Winmgmt
5	NT Service\MSSQL\$SQLEXPRESS

Podmiot można włączyć

Object Explorer

Connect

- DESKTOP-7G93C9\SQLEXPRESS (SQL S)
- Databases
- Security
 - Logins
 - ##MS_PolicyEventProcessin
 - ##MS_PolicyTsqlExecutionL
 - BUILTIN\Uzytkownicy
 - DESKTOP-7G93C9\student
 - NT Service\MSSQL\$SQLEXP
 - NT SERVICE\SQLTELEMETRY
 - NT SERVICE\SQLWriter
 - NT SERVICE\Winmgmt
 - sa
 - ZARZĄDZANIE NT\SYSTEM
 - Server Roles
 - Credentials
 - Audite

```
SQLQuery1.sql - DE...93C9\student (54))* -> X
USE master;
GO
ALTER LOGIN sa ENABLE;
GO
ALTER LOGIN sa WITH PASSWORD = 'haslo!';
GO
```

100 %

Messages

Commands completed successfully.

Completion time: 2021-10-21T09:33:16.4146S28+02:

Użytkownik 'sa'

SQLQuery1.sql - DESKTOP-7G93C9\SQLEXPRESS.master (DESKTOP-7G93C9\student (54))* - Microsoft SQL Server Management Studio

File Edit View Query Project Tools Window Help

Object Explorer

Connect - DESKTOP-7G93C9\SQLEXPRESS (SQL S

SQLQuery1.sql - DE...93C9\student (54))*

```
SELECT * FROM sys.server_principals;
```

Results Messages

	name	principal_id	sid	type	type_desc	is_disabled	create_date	modify_date	default_database_name	default_language_name	credential_id	owning_principal_id
1	sa	1	0x01	S	SQL_LOGIN	1	2003-04-08 09:10:35.460	2021-10-20 23:32:24.250	master	us_english	NULL	NULL
2	public	2	0x02	R	SERVER_ROLE	0	2009-04-13 12:59:06.030	2009-04-13 12:59:06.030	NULL	NULL	NULL	1
3	sysadmin	3	0x03	R	SERVER_ROLE	0	2009-04-13 12:59:06.030	2009-04-13 12:59:06.030	NULL	NULL	NULL	1
4	securityadmin	4	0x04	R	SERVER_ROLE	0	2009-04-13 12:59:06.030	2009-04-13 12:59:06.030	NULL	NULL	NULL	1
5	serveradmin	5	0x05	R	SERVER_ROLE	0	2009-04-13 12:59:06.030	2009-04-13 12:59:06.030	NULL	NULL	NULL	1
6	setupadmin	6	0x06	R	SERVER_ROLE	0	2009-04-13 12:59:06.030	2009-04-13 12:59:06.030	NULL	NULL	NULL	1
7	processadmin	7	0x07	R	SERVER_ROLE	0	2009-04-13 12:59:06.030	2009-04-13 12:59:06.030	NULL	NULL	NULL	1
8	diskadmin	8	0x08	R	SERVER_ROLE	0	2009-04-13 12:59:06.030	2009-04-13 12:59:06.030	NULL	NULL	NULL	1
9	dbcreator	9	0x09	R	SERVER_ROLE	0	2009-04-13 12:59:06.030	2009-04-13 12:59:06.030	NULL	NULL	NULL	1
10	bulkadmin	10	0x0A	R	SERVER_ROLE	0	2009-04-13 12:59:06.030	2009-04-13 12:59:06.030	NULL	NULL	NULL	1
11	##MS_SQLResourceSigningCertificate##	101	0x010600000000000009010000001E501960278B270FD3419142...	C	CERTIFICATE_MAPPED_LOGIN	0	2019-09-24 14:21:16.390	2019-09-24 14:21:16.390	master	us_english	NULL	NULL
12	##MS_SQLReplicationSigningCertificate##	102	0x01060000000000000901000000ED1B6318A0592D96CE6D14...	C	CERTIFICATE_MAPPED_LOGIN	0	2019-09-24 14:21:16.390	2019-09-24 14:21:16.390	master	us_english	NULL	NULL
13	##MS_SQLAuthenticatorCertificate##	103	0x01060000000000000901000000FB236D83A8DC8E7DE549C5...	C	CERTIFICATE_MAPPED_LOGIN	0	2019-09-24 14:21:16.390	2019-09-24 14:21:16.390	master	us_english	NULL	NULL
14	##MS_PolicySigningCertificate##	105	0x01060000000000000901000000B81B6130E13E5B67B7BD49...	C	CERTIFICATE_MAPPED_LOGIN	0	2019-09-24 14:21:16.393	2019-09-24 14:21:16.393	master	us_english	NULL	NULL
15	##MS_SmoExtendedSigningCertificate##	106	0x01060000000000000901000000CDFCE5B748D5515E793FC...	C	CERTIFICATE_MAPPED_LOGIN	0	2019-09-24 14:21:16.393	2019-09-24 14:21:16.393	master	us_english	NULL	NULL
16	##MS_PolicyEventProcessingLogin##	256	0x5681CCE7A1F1FF41B2F95CED7D792E70	S	SQL_LOGIN	1	2019-09-24 14:21:53.563	2021-10-20 23:32:24.337	master	us_english	NULL	NULL
17	##MS_PolicyTsqExecutionLogin##	257	0x27578D8516843E4094EFA2CEED085C82	S	SQL_LOGIN	1	2019-09-24 14:21:53.570	2021-10-20 23:32:24.330	master	us_english	NULL	NULL
18	##MS_AgentSigningCertificate##	258	0x010600000000000009010000004C1967C27FEB2EAD332894C...	C	CERTIFICATE_MAPPED_LOGIN	0	2019-09-24 14:21:58.890	2019-09-24 14:21:58.897	master	us_english	NULL	NULL
19	DESKTOP-7G93C9\student	259	0x01050000000000000515000000275503B645E45C2ED6ECC77...	U	WINDOWS_LOGIN	0	2021-10-20 23:32:24.170	2021-10-20 23:32:24.180	master	us_english	NULL	NULL
20	NT SERVICE\SQLWriter	260	0x01060000000000000550000000732B9753646EF90356745CB6...	U	WINDOWS_LOGIN	0	2021-10-20 23:32:24.183	2021-10-20 23:32:24.193	master	us_english	NULL	NULL
21	NT SERVICE\Wingmt	261	0x010600000000000005500000005A048DFF9C7430A8450D4...	U	WINDOWS_LOGIN	0	2021-10-20 23:32:24.190	2021-10-20 23:32:24.200	master	us_english	NULL	NULL
22	NT SERVICE\MSSQL\$SQLEXPRESS	262	0x01060000000000000550000000703344E71D40B7FFB884456...	U	WINDOWS_LOGIN	0	2021-10-20 23:32:24.200	2021-10-20 23:32:24.210	master	us_english	NULL	NULL
23	BUILTIN\Uzytkownicy	263	0x0102000000000000052000000021020000	G	WINDOWS_GROUP	0	2021-10-20 23:32:24.207	2021-10-20 23:32:24.213	master	us_english	NULL	NULL
24	ZARZADZANIE NT\SYSTEM	264	0x01010000000000000512000000	U	WINDOWS_LOGIN	0	2021-10-20 23:32:24.213	2021-10-20 23:32:24.220	master	us_english	NULL	NULL
25	NT SERVICE\SQLTELEMETRY\$SQLEXPRESS	265	0x010600000000000005500000002C4559766DEF9A2F8E23EA8...	U	WINDOWS_LOGIN	0	2021-10-20 23:32:25.117	2021-10-20 23:32:25.123	master	us_english	NULL	NULL

Query executed successfully.

DESKTOP-7G93C9\SQLEXPRESS ... | DESKTOP-7G93C9\student ... | master | 00:00:00 | 25 rows

Ready

Ln 1 Col 37 Ch 37 INS

Wpisz tu wyszukiwane słowa

09:29 21.10.2021

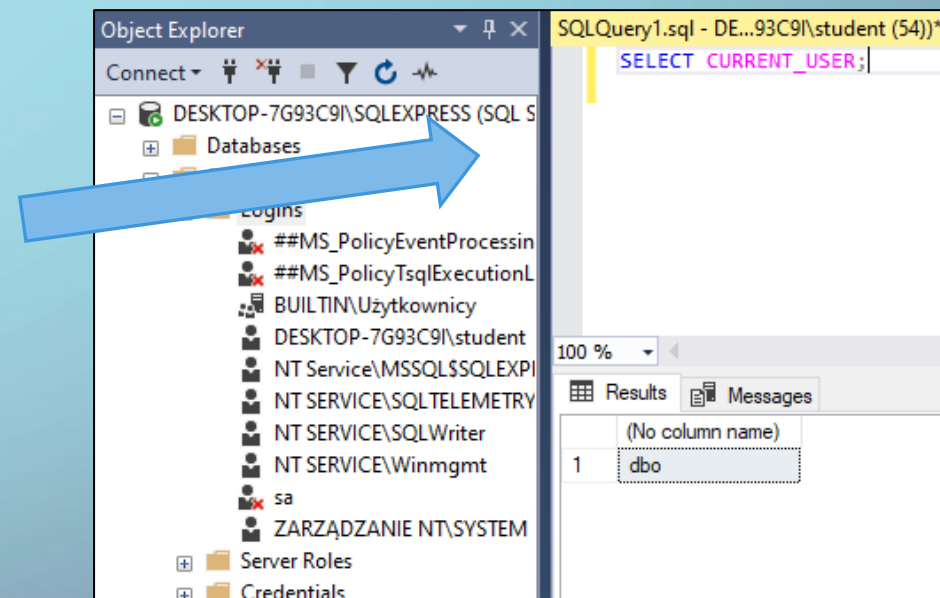
Duże możliwości 😊

Użytkownik 'dbo' oraz schemat 'dbo'

Użytkownik *dbo* jest specjalnym podmiotem w każdej bazie danych. Administratorzy Serwera SQL, członkowie stałej roli *sysadmin*, podmiot *sa* oraz właściciele bazy danych tworzą bazy jako użytkownik *dbo*. Podmiot ten posiada wszystkie uprawnienia w bazie danych i nie może być ograniczany ani usunięty. Podmiot *dbo* jest właścicielem bazy danych ale nie odzwierciedla stałej roli *db_owner*. Użytkownik *dbo* jest właścicielem schematu *dbo*. Schemat *dbo* jest domyślnym schematem dla wszystkich użytkowników, o ile nie podano innego schematu. Nie można usunąć schematu *dbo*.

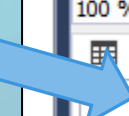
Użytkownik 'dbo' oraz schemat 'dbo'

SQL Server automatycznie mapuje podmiot *sa*, właściciela bazy danych i członków roli serwera *sysadmin* serwera na konto użytkownika *dbo* w każdej bazie danych. Można to sprawdzić poprzez wykonanie zapytania z funkcją `CURRENT_USER`.



Użytkownik 'dbo' oraz schemat 'dbo'

Aby zweryfikować nazwę logowania i domyślną bazę danych skojarzoną z użytkownikiem *dbo*, należy uruchomić odpowiednie zapytanie w jednej z baz danych:



```
USE master;
GO
SELECT USER_SNAME(sid) login_name, default_schema_name
FROM sys.database_principals
WHERE name = 'dbo';
```

	login_name	default_schema_name
1	sa	dbo

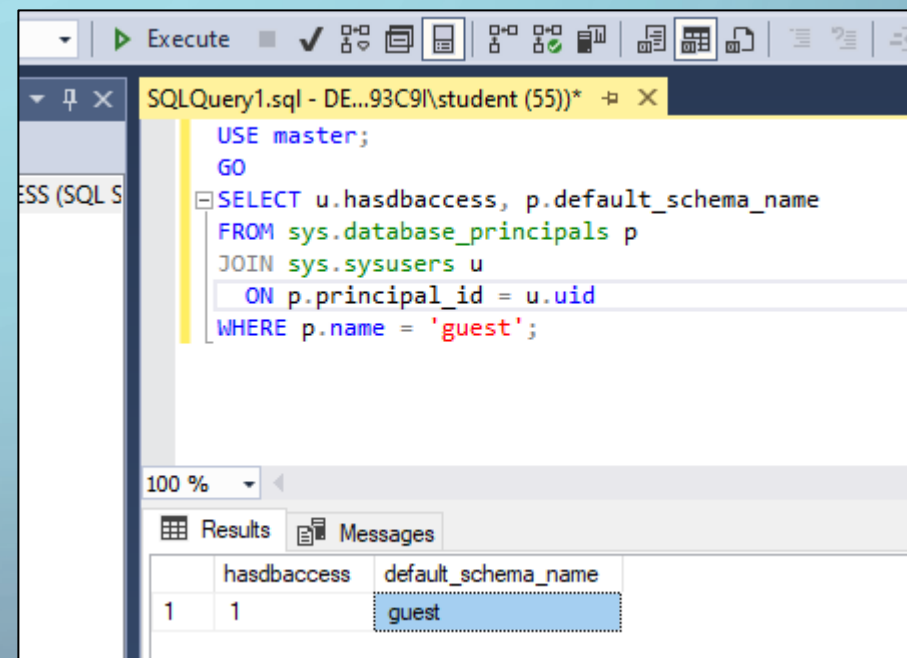
Użytkownik 'guest' oraz schemat 'guest'

Podobnie jak w przypadku *dbo*, każda baza danych zawiera użytkownika i schemat *guest*. Można użyć użytkownika *guest* po to, aby przyznać dostęp do bazy danych loginom, które nie są skojarzone z kontami użytkowników w tej bazie danych (tej strategii raczej powinno się unikać).

Użytkownika *guest* nie można usunąć, ale domyślnie jest on wyłączony i nie ma przydzielonych żadnych uprawnień (czy aby na pewno?). Jeśli ten podmiot jest włączona, loginy, które nie powinny mieć dostępu do bazy danych, będą miały dostęp. Użytkownik *guest* jest właścicielem schematu *guest*. Podobnie jak użytkownika, schematu także nie można usunąć.

Użytkownik 'guest' oraz schemat 'guest'

Aby sprawdzić, czy użytkownik *guest* jest włączony, uruchom następujące zapytanie:



```
SQLQuery1.sql - DE...93C9I\student (55))* X
USE master;
GO
SELECT u.hasdbaccess, p.default_schema_name
FROM sys.database_principals p
JOIN sys.sysusers u
ON p.principal_id = u.uid
WHERE p.name = 'guest';
```

100 %

Results Messages

	hasdbaccess	default_schema_name
1	1	guest

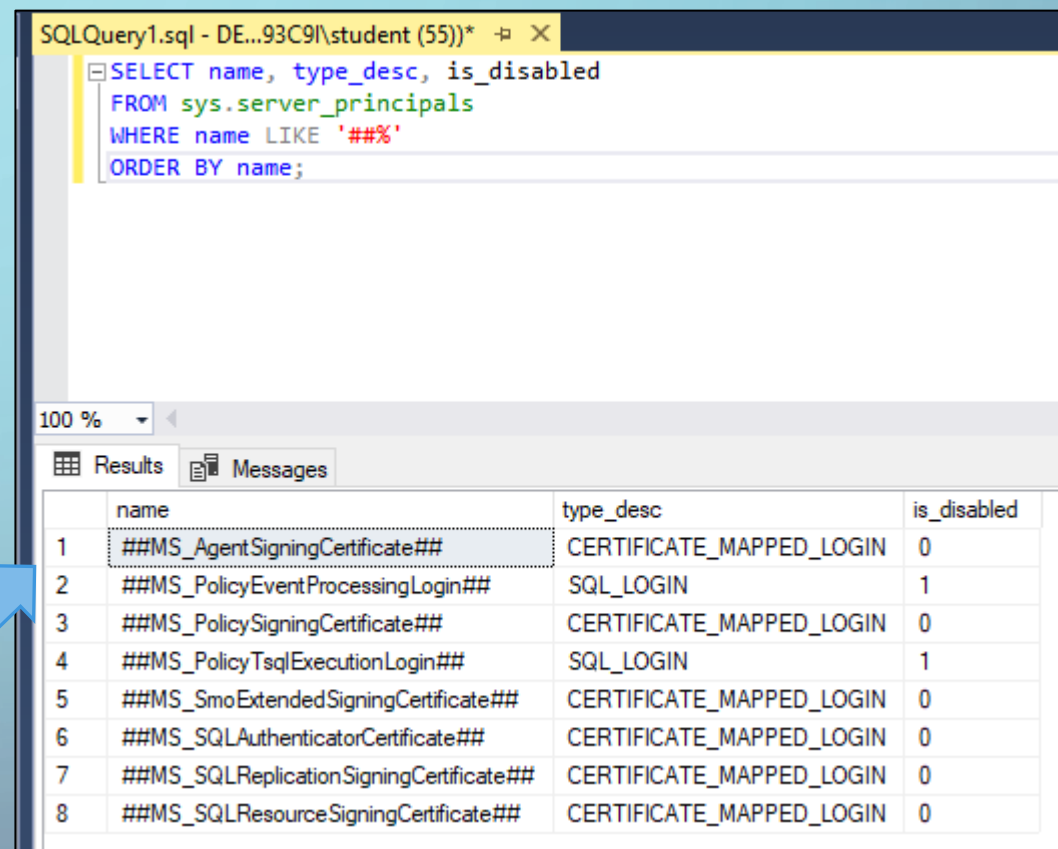
'sys' oraz 'INFORMATION_SCHEMA'

Każda baza danych zawiera podmioty widniejące jako użytkownicy: INFORMATION_SCHEMA oraz sys. Podmioty te są używane do użytku wewnętrznego przez silnik bazy danych. Nie można ich modyfikować ani usuwać.

LOGOWANIE OPARTE NA CERTYFIKATACH

SQL Server zawiera także grupę podmiotów których nazwy zaczynają się i kończą podwójnymi znakami hash (przykład ##MS_PolicySigningCertificate##). Loginy to konta mapowane na certyfikaty używane przez silnik bazy danych do celów wewnętrznych. Nie należy ich usuwać.

Aby pobrać listę logowań opartych na certyfikatach należy wykonać odpowiednie zapytanie:



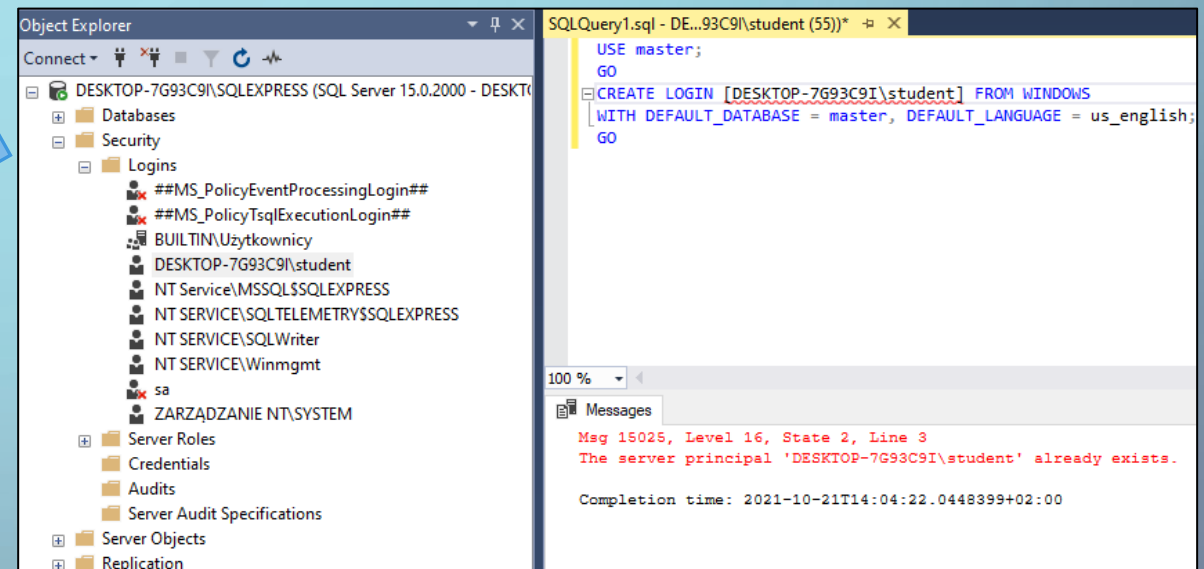
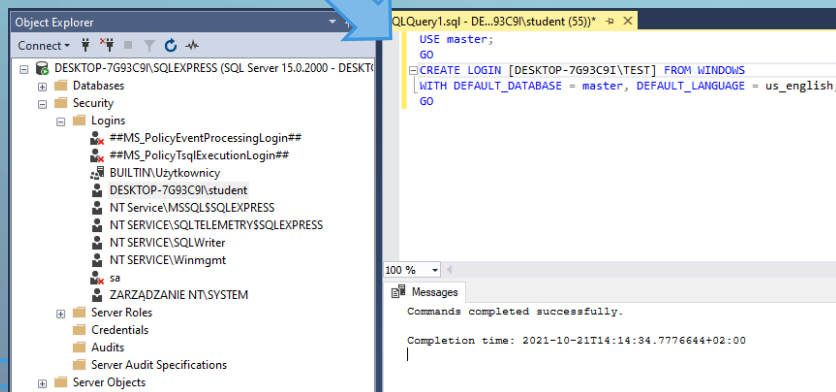
```
SQLQuery1.sql - DE...93C9\student (55))* -p X
SELECT name, type_desc, is_disabled
FROM sys.server_principals
WHERE name LIKE '##%'
ORDER BY name;
```

	name	type_desc	is_disabled
1	##MS_AgentSigningCertificate##	CERTIFICATE_MAPPED_LOGIN	0
2	##MS_PolicyEventProcessingLogin##	SQL_LOGIN	1
3	##MS_PolicySigningCertificate##	CERTIFICATE_MAPPED_LOGIN	0
4	##MS_PolicyTsqlExecutionLogin##	SQL_LOGIN	1
5	##MS_SmoExtendedSigningCertificate##	CERTIFICATE_MAPPED_LOGIN	0
6	##MS_SQLAuthenticatorCertificate##	CERTIFICATE_MAPPED_LOGIN	0
7	##MS_SQLReplicationSigningCertificate##	CERTIFICATE_MAPPED_LOGIN	0
8	##MS_SQLResourceSigningCertificate##	CERTIFICATE_MAPPED_LOGIN	0

PRZYKŁAD:

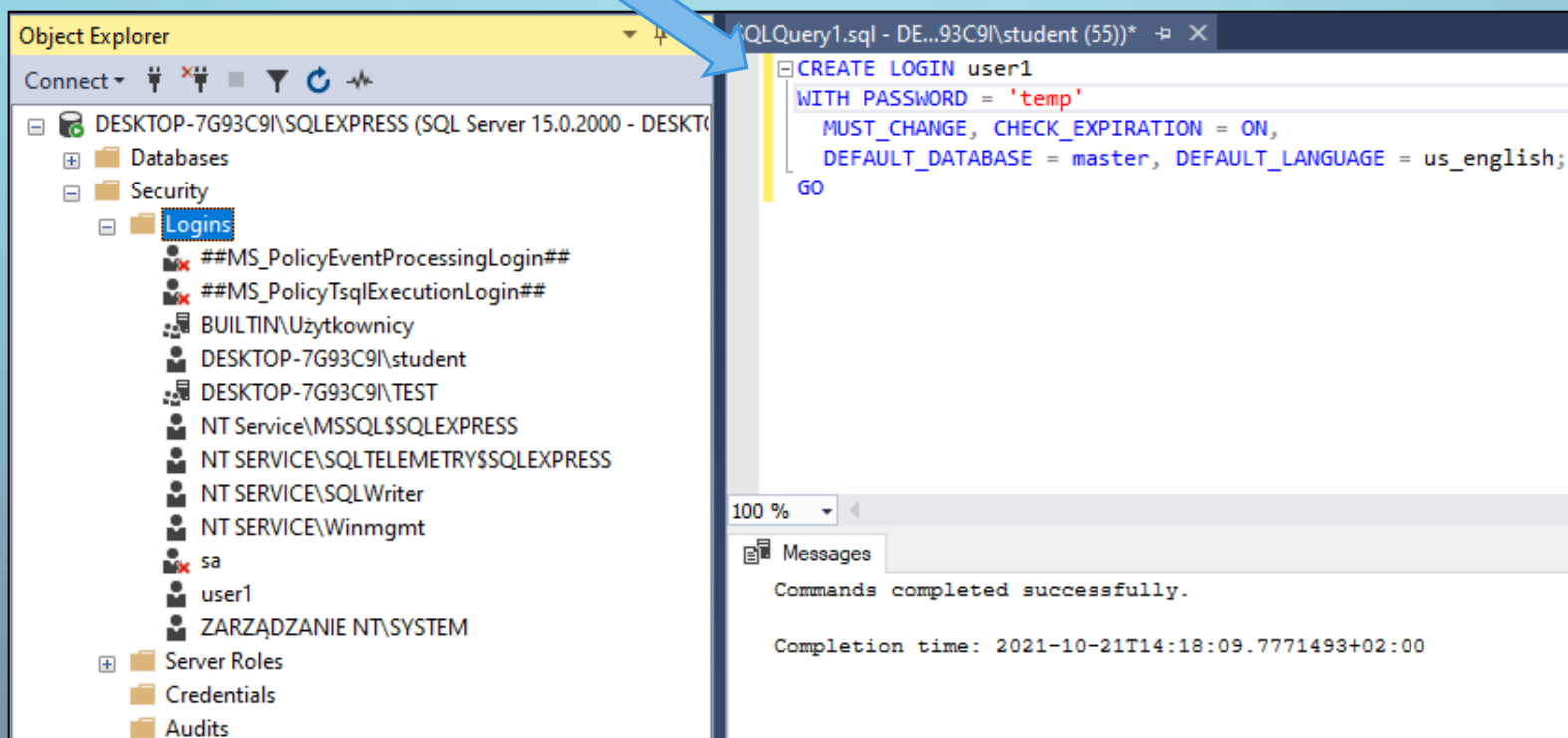
Instrukcja definiuje logowanie na podstawie lokalnego konta *student* na komputerze o nazwie DESKTOP-7G93C9I:

Przydzielenie dostępu dla grupy
Windows



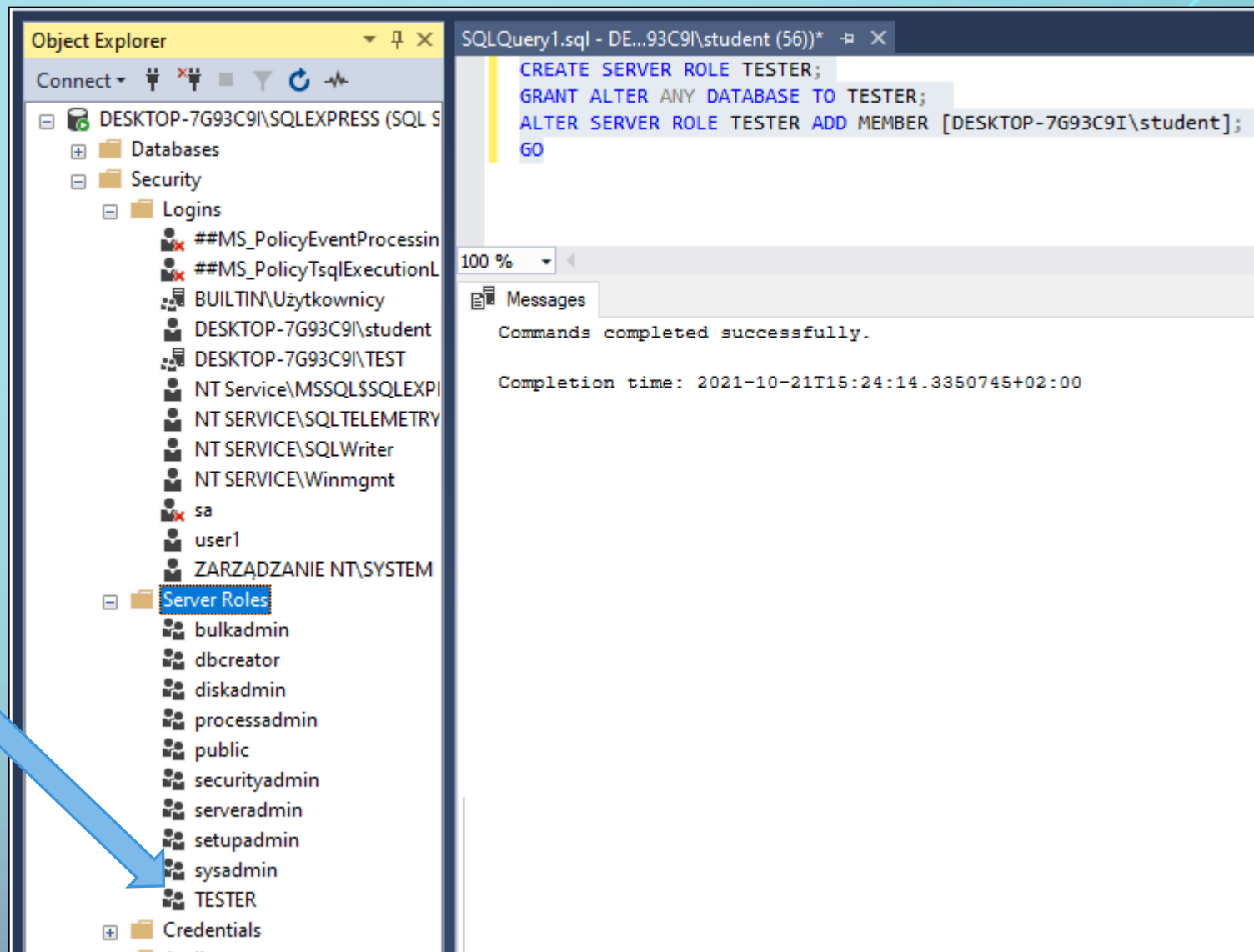
PRZYKŁAD:

Instrukcja definiuje login do serwera SQL:



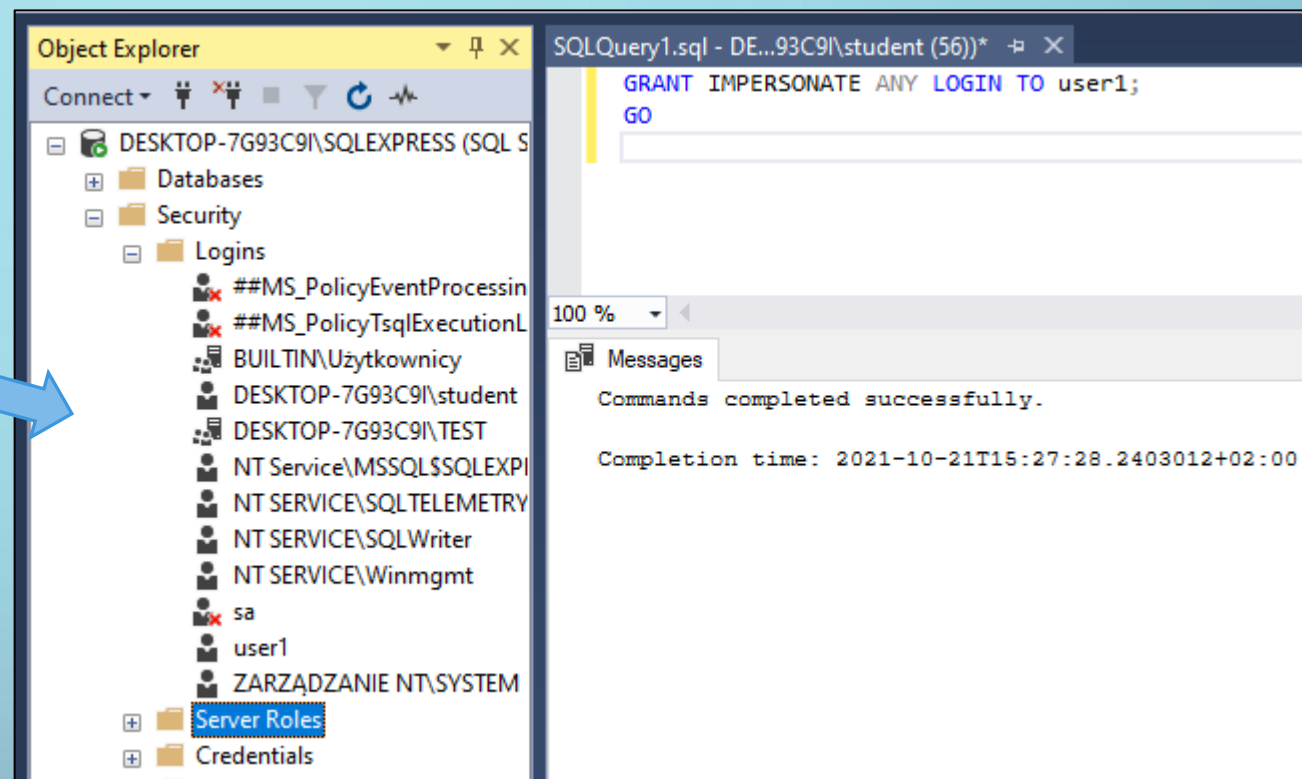
PRZYKŁAD:

Instrukcja definiuje rolę w SQL Server:



PRZYKŁAD:

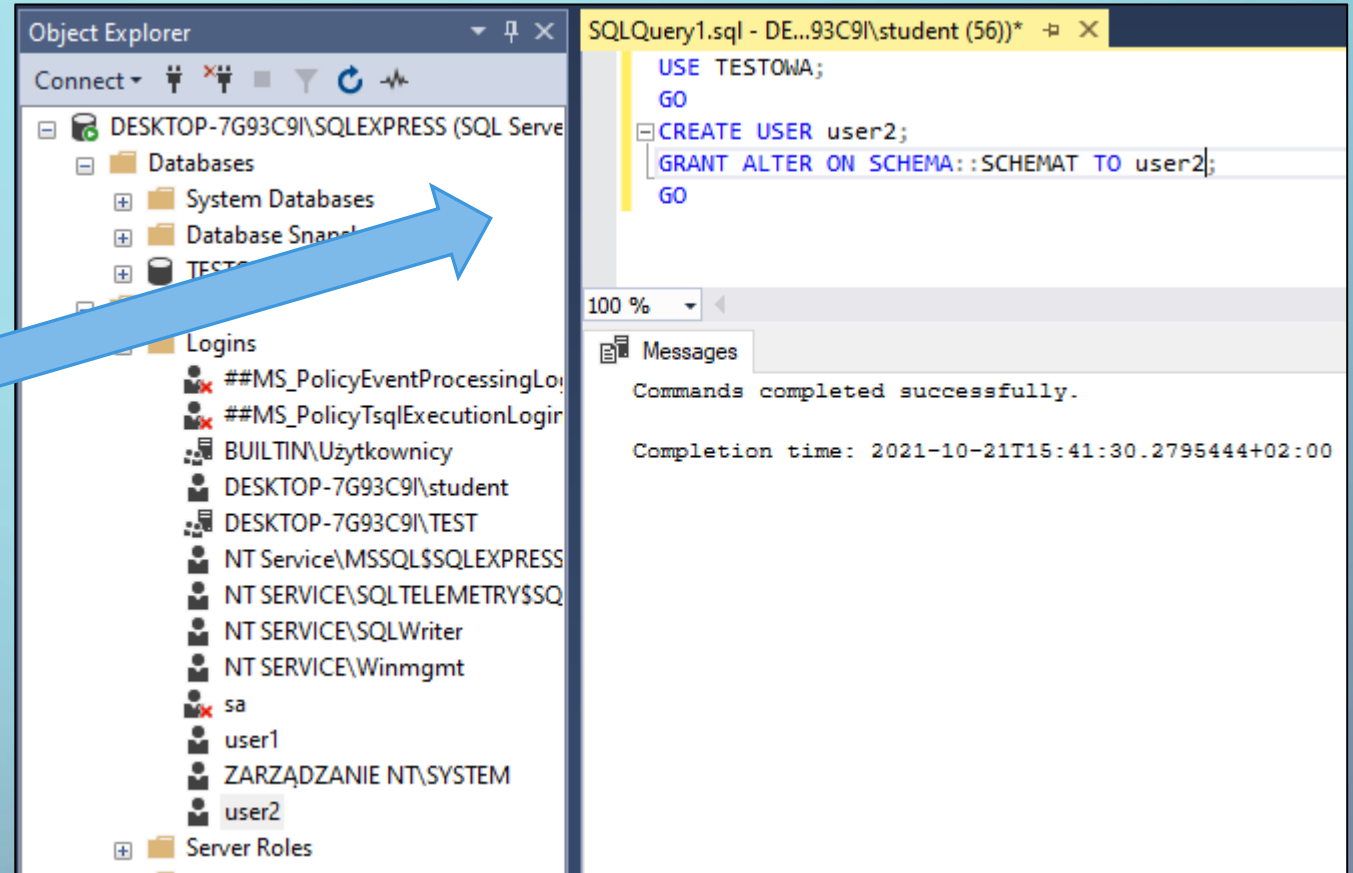
Instrukcja definiuje uprawnienia
w SQL Server:



PRZYKŁAD:

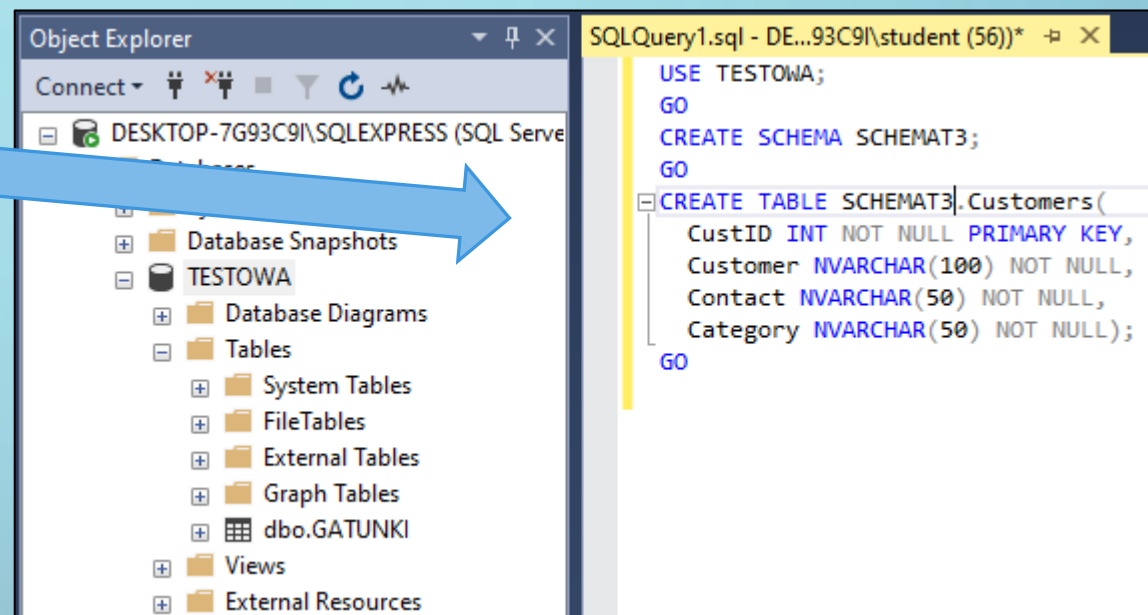
Tworzenie użytkownika i przydzielenie do schematu SCHEMAT.

Należy pamiętać o stworzeniu Loginu.



PRZYKŁAD:

Tworzenie schematu i tabeli.



DZIĘKUJĘ ZA UWAGĘ