

Prava pristupa (Microsoft SQL Server)

SOFTVERSKI ALATI BAZA PODATAKA

Sadržaj

- Login
- User
- Role
- Schema
- Authorization
- Prava pristupa
- Hijerarhija prava pristupa

Login

Login omogućava konekciju sa serverom. Pomoću login-a moguće je pristupiti samo onome čemu ima pravo pristupa public rola.

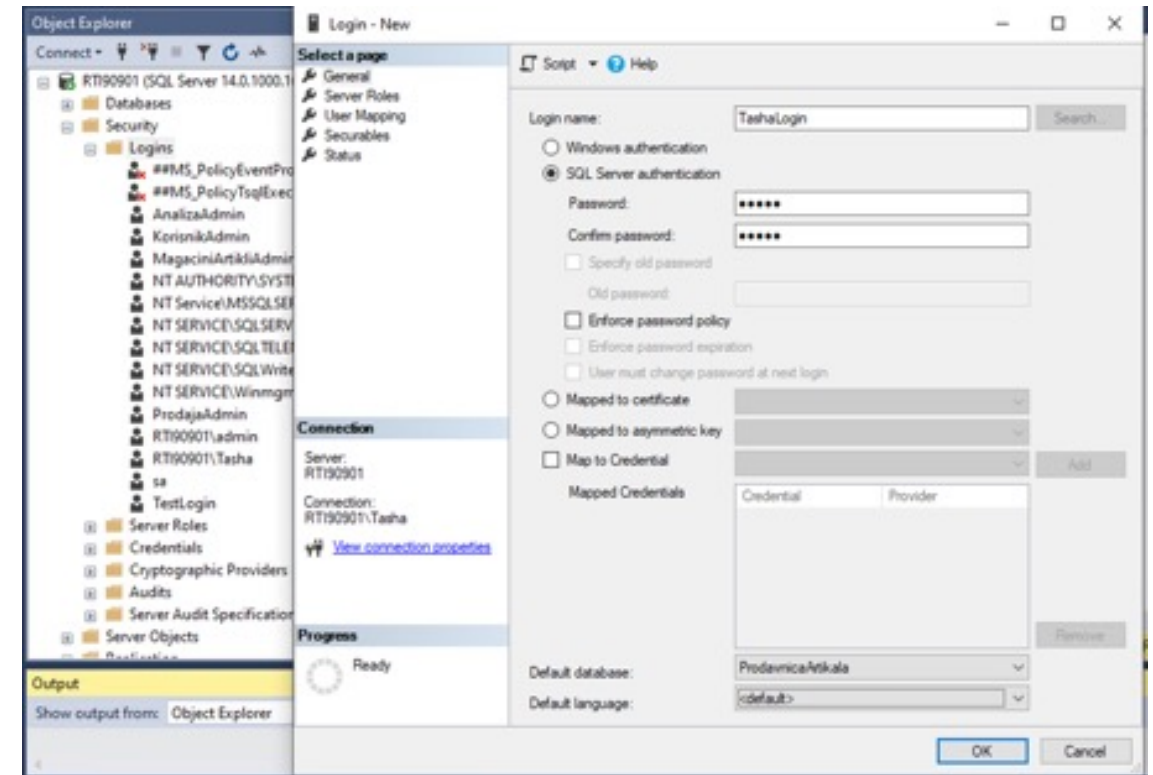
Primer kreiranja login-a:

```
CREATE LOGIN TashaLogin
```

```
WITH PASSWORD = 'tasha'
```

Link:

<https://learn.microsoft.com/en-us/sql/t-sql/statements/create-login-transact-sql?view=sql-server-ver16>



User

User omogućava pristup konkretnoj bazi podataka. Kako bi user uopšte mogao da pristupi bazi podataka, potrebno je definisati i na koji način će pristupiti serveru.

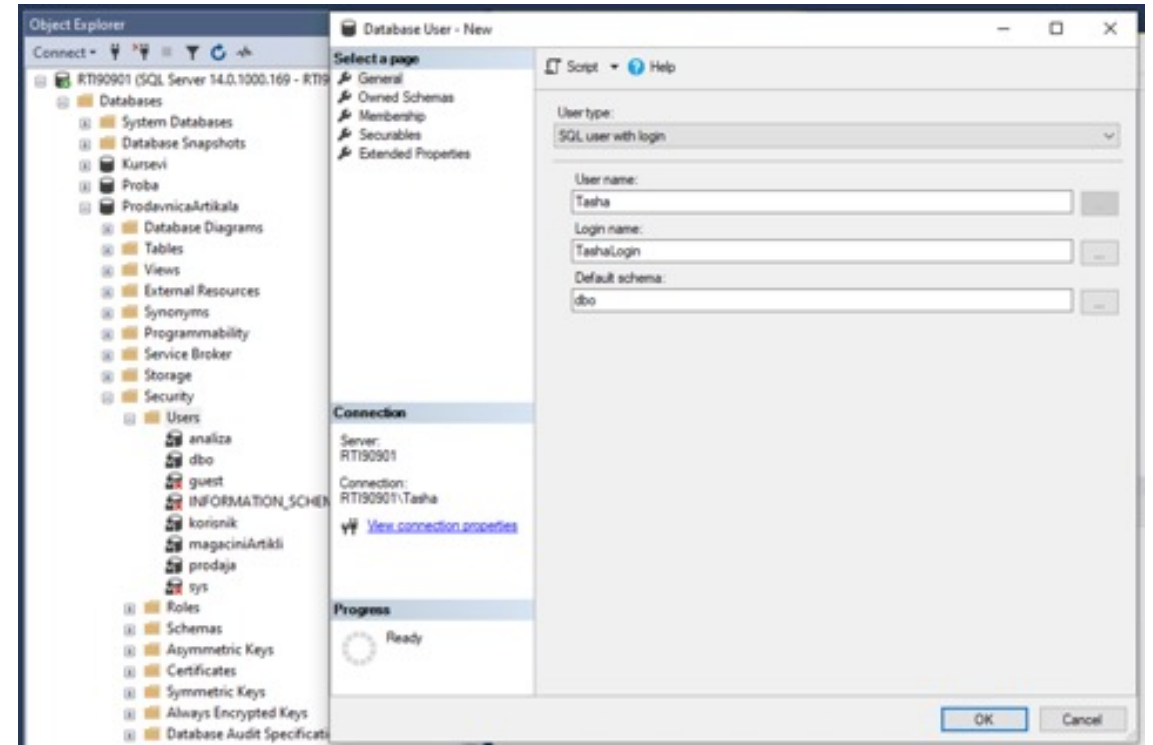
Primer kreiranja user-a:

CREATE USER Tasha

FOR LOGIN TashaLogin

Link:

<https://learn.microsoft.com/en-us/sql/t-sql/statements/create-user-transact-sql?view=sql-server-ver16>



Role

Nad Role-ma se definišu prava pristupa unutar neke baze. Nakon toga je moguće određenim korisnicima dodeljivati određene role.

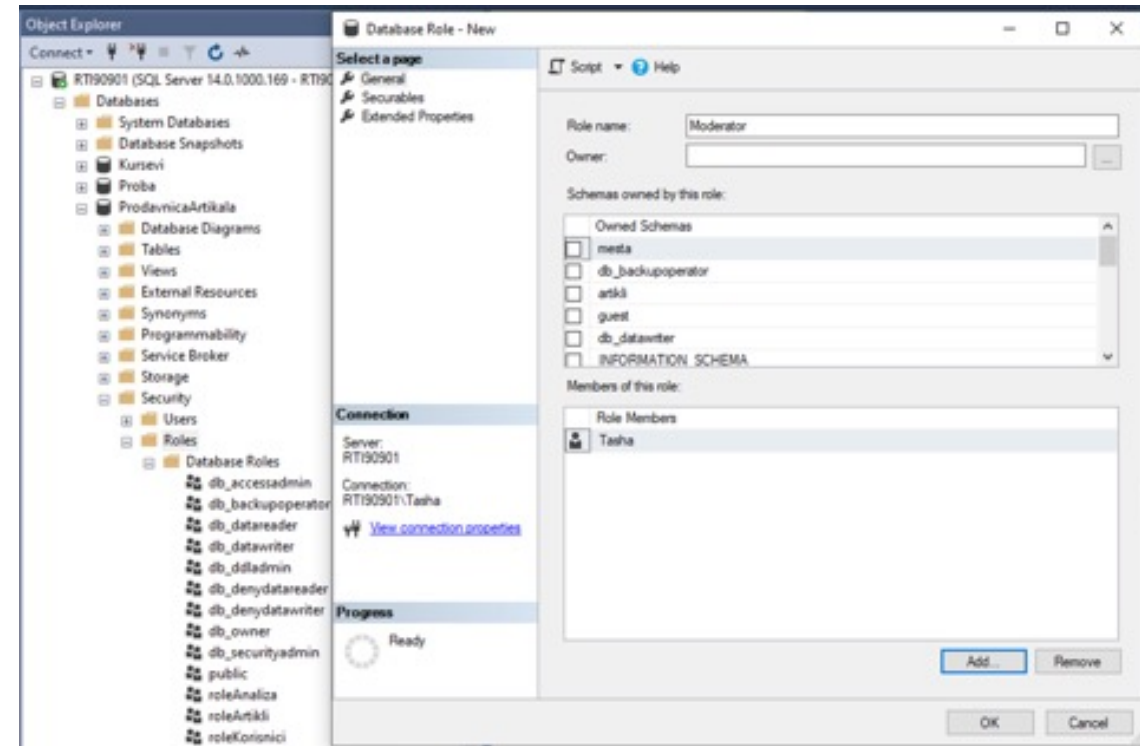
Primer kreiranja role-a i dodeljivanje role korisnicima:

CREATE ROLE Moderator

ALTER ROLE Moderator **ADD MEMBER** Tasha

Link:

<https://learn.microsoft.com/en-us/sql/t-sql/statements/create-role-transact-sql?view=sql-server-ver16>



Schema

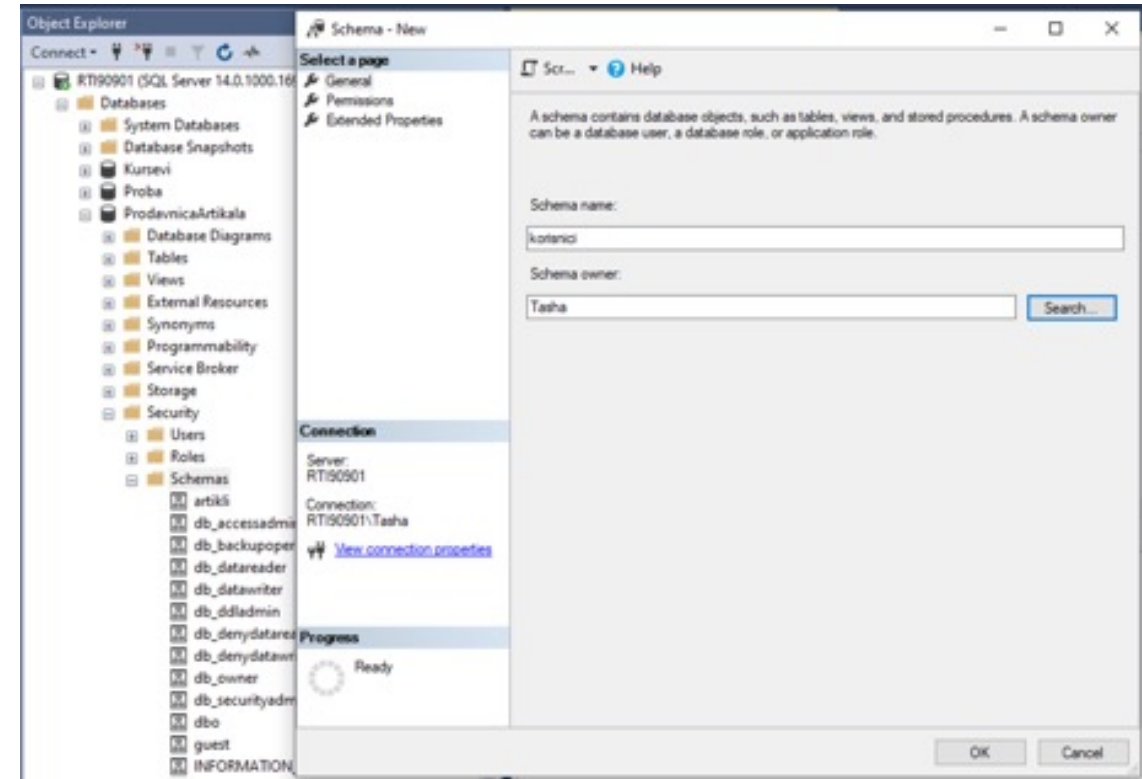
Schema predstavlja logičku celinu unutar baze podataka. Unutar njih se nalaze objekti baze podataka. Podrazumevano se objekti nalaze unutar dbo schema-e.

Primer kreiranja schema-e:

CREATE SCHEMA korisnici

Link:

<https://learn.microsoft.com/en-us/sql/t-sql/statements/create-schema-transact-sql?view=sql-server-ver16>



Schema

Objekti se mogu kreirati unutar zadate scheme i mogu se premeštati iz jedne u drugu schema-u.

Primer premeštanja objekta iz jedne schema-e u drugu:

```
ALTER SCHEMA korisnici TRANSFER OBJECT::dbo.Kupac
```

Link:

<https://learn.microsoft.com/en-us/sql/t-sql/statements/alter-schema-transact-sql?view=sql-server-ver16>

Authorization

Svaka schema i svaki objekat ima svog vlasnika. Podrazumevano vlasnik je dbo user.

Primer kreiranja schema-e sa zadatim vlasnikom i promena vlasnika schema/e i tabele:

```
CREATE SCHEMA korisnici AUTHORIZATION Tasha
```

```
ALTER AUTHORIZATION ON SCHEMA::korisnici TO Tasha
```

```
ALTER AUTHORIZATION ON OBJECT::korisnici.Kupac TO Tasha
```

Link:

<https://learn.microsoft.com/en-us/sql/t-sql/statements/alter-authorization-transact-sql?view=sql-server-ver16>

Prikaz informacija

Informacije o postojećim login-ovima, user-ima, role-ama, schema-ma i objekata moguće je dohvatiti korišćenjem sistemskih pogleda.

Primer:

```
SELECT * FROM sys.sql_logins
```

```
SELECT * FROM sys.database_principals where type = 'S' or type = 'U'
```

```
SELECT * FROM sys.database_principals where type = 'R'
```

```
SELECT * FROM sys.schemas
```

```
SELECT * FROM sys.objects where type = 'U'
```

Link:

<https://learn.microsoft.com/en-us/sql/relational-databases/system-compatibility-views/system-compatibility-views-transact-sql?view=sql-server-ver16>

Prava pristupa

Prava pristupa moguće je davati (GRANT) i oduzimati (DENY) na nivou baze, schema-e i objekta. Ona se dodeljuju role-ama. Moguće je i ukidanje postojećeg prava pristupa pomoću naredbe REVOKE.

Moguće je dodeljivati sveobuhvatno pravo pristupa, kao i parvo na samo čitanje, kreiranje, dodavanje, brisanje, izvršavanje,...

Link:

<https://learn.microsoft.com/en-us/sql/relational-databases/security/permissions-database-engine?view=sql-server-ver16>

<https://learn.microsoft.com/en-us/sql/t-sql/statements/grant-transact-sql?view=sql-server-ver16>

<https://learn.microsoft.com/en-us/sql/t-sql/statements/deny-transact-sql?view=sql-server-ver16>

<https://learn.microsoft.com/en-us/sql/t-sql/statements/revoke-transact-sql?view=sql-server-ver16>

Prava pristupa

Primeri:

```
GRANT CONTROL ON SCHEMA::Mesta TO Moderator
```

```
GRANT CONTROL ON SCHEMA::Mesta TO Admin WITH GRANT OPTION
```

```
GRANT SELECT ON OBJECT::korisnici.korisnik TO Moderator
```

```
DENY SELECT ON OBJECT::korisnici.korisnik(sifra) TO Moderator
```

```
GRANT EXECUTE ON OBJECT::dbo.brojKorisnikaPoGradu TO Moderator
```

Hijerarhija prava pristupa

Prava pristupa se mogu dodeljivati na različitim nivoima. Prava se proveravaju od manje specifičnim ka specifičnijim. Uspešnost izvršavanja upita zavisi od dozvole ili zabranu pristupa na koju se prvo naiđe.

Primer:

```
GRANT SELECT ON SCHEMA::korisnici TO roleKorisnici
```

```
DENY SELECT ON OBJECT::korisnici.korisnik TO roleKorisnici
```

```
GRANT SELECT ON OBJECT::korisnici.korisnik(email) TO roleKorisnici
```

RoleKorisnici će imati pravo samo da selektuje email, dok ostalim kolonama neće imati pristup, zato što select pravo pristupa nad tabelom predstavlja zapravo select pravo pristupa nad svim njenim kolonama.

Link:

<https://learn.microsoft.com/en-us/sql/relational-databases/security/permissions-hierarchy-database-engine?view=sql-server-ver16>