

Administracija Baza podataka

Sigurnost i zaštita baza podataka

Sigurnost - Pojam

- ❑ Zaštita baza podataka od neovlašćenog korišćenja.
- ❑ Razlozi:
 - Zakonski propisi, društveni odnosi i etičke norme nalažu da se spreči neovlašćeno korišćenje podataka.
 - Podaci u kompanijama, državnim institucijama i drugim organizacijama moraju biti zaštićeni.
 - U okviru samog SUBP podaci, a i korisnički nalozi i lozinke moraju biti zaštićeni.

Sigurnost i zaštita Baza podataka

- ❑ Administracija sigurnosti je jedan od ključnih zadataka administracije baza podataka.
- ❑ Razumevanje mogućnosti zaštite koje neki SUBP podržava je ključan za obezbeđivanje integriteta kompletnog okruženja baze podataka.
- ❑ Dobra implementacija i rukovanje modelom zaštite pomaže u smanjenju ranjivosti osetljivih podataka u bazi, a povećavaju ukupnu skalabilnost i pouzdanost kompletnog okruženja baze podataka.

Koncepti sigurnosti baze podataka

- ❑ Zaštita baze podataka od neovlašćenog korišćenja odvija se na više nivoa:
 - Zaštita celog sistema;
 - Zaštita na nivou mreže;
 - Zaštita na nivou operativnog sistema;
 - Zaštita na nivou aplikacije;
 - Zaštita unutar same baze podataka.

Sigurnost celog sistema

- ❑ Sigurnost celog sistema podrazumeva sprečavanje pristupa neovlašćenoj osobi celokupnom sistemu baze podataka, obično se koriste korisnička imena i lozinke.
- ❑ Ovaj koncept obuhvata i sprečavanje fizičkog pristupa mestu gde se nalazi baza podataka.

Sigurost baze podataka

- ❑ Neki od pristupa koji bazu podataka mogu učiniti sigurnijom:
 - Ograničiti pristup važnim resursima koji mogu biti pogrešno korišćeni – zlonamerno ili slučajno;
 - Onemogućiti nepotrebne komponente i servise sistema za upravljanje bazom podataka;
 - Ukloniti ili onemogućiti predefinisane korisničke naloge;
 - Izvršavati procese baze podataka pod namenskim neprivilegovanim nalogima.
 -

Načelo najmanjih ovlašćenja i razdvajanje

❑ Načelo najmanjih ovlašćenja (*least privilege*)

- Korisnik ima minimalni skup dozvola koje su neophodne za obavljanje tekućeg zadatka
- Pojedinaac ima različite nivoe ovlašćenja u različito vreme zavisno od zadatka ili funkcije koju obavlja;
- Sprečavanje obavljanja nepotrebnih i eventualno štetnih akcija.

❑ Razdvajanje dužnosti (*Separation Of Duty – SoD*)

- Osetljive zadatke ne može u celini obavljati jedan korisnik;
- Na taj način se smanjuje mogućnost zloupotrebe.

Mehanizmi zaštite na nivou SUBP

- ❑ Identifikacija i dokazivanje autentičnosti (predstavljanje onoga ko pristupa sistemu);
- ❑ Autorizacija i kontrola pristupa (ko nešto može da uradi);
- ❑ Enkripcija podataka (odredjivanje ko podatke može videti);
- ❑ Praćenje pristupa podacima i zapisivanje (prećenje ko je šta i kada uradio):
 - Upis izvornog teksta korisničkog zahteva;
 - Upis identifikatora klijanta/terminala sa kojeg je pristupljeno;
 - Upis datuma i vremena pristupa bazi;
 - Upis relacije, n-torke i atributa kojima je pristupano;
 - Upis starih i novih vrednosti podataka.

Model sigurnosti same baze podataka

- ❑ Osnovni model sigurnosti se može predstaviti preko skupa autorizacija, koje predstavljaju uredjene četvorke:

Autorizacija (Korisnik, Objekat, Operacija, Uslov)

- ❑ SUBP mora da omogući implementaciju i realizaciju opisanog koncepta autorizacije.
- ❑ Deo SUBP koji obavlja ovaj zadatak naziva se podsistem sigurnosti ili podsistem autorizacije.

Sigurnost baze podataka

KONTROLA PRISTUPA

Kontrola pristupa

- ❑ Kontrola pristupa je deo sigurnosne politike koja je prisutna u gotovo svakom sistemu.
- ❑ Kad se spominje kontrola pristupa, uzimaju se u obzir četiri situacije:
 - Sprečavanje pristupa;
 - Ograničavanje pristupa;
 - Dozvola pristupa;
 - Oduzimanje prava pristupa

Kontrola pristupa

- 🔒 Korisnicima se dodeljuju ovlašćenja (eng. privileges) za povezivanje na bazu i rad sa njenim objektima.
- 🔒 Ovlašćenja korisnicima može dodeljivati administrator baze, vlasnik objekata ili neki drugi autorizovani korisnik kome je dato to pravo.
- 🔒 Ovlašćenja omogućavaju korisnicima da obavljaju određene akcije nad serverom baze i samom bazom podataka (sistemska ovlašćenja) ili objektima baze (objektni ovlašćenja).

Sistemska ovlašćenja

- 🔒 Sistemska ovlašćenja najčešće dodeljuje administrator baze podataka.
- 🔒 U ova ovlašćenja spadaju, npr. CREATE DATABASE, CREATE TABLE, CREATE VIEW i CREATE USER, koja dozvoljavaju korisniku da kreira novu bazu podataka, tabelu, pogled i novi korisnički nalog.

Objektna ovlašćenja

- 🔒 Objektna ovlašćenja korisniku omogućavaju da izvrši operacije nad konkretnim objektima baze (kao što su određena baza, tabele, obeležja, pogledi...).
- 🔒 Ako korisnik treba da vidi podatke neke tabele, potrebno mu je dodeliti SELECT ovlašćenje nad tom tabelom (isto važi za INSERT, UPDATE, DELETE, ...).

Modeli kontrole pristupa

- ❑ Modeli kontrole pristupa u bazama podataka zasnovani su na generalnoj teoriji zaštite u računarskim sistemima.
- ❑ Modeli kontrole pristupa dele se u dve grupe:
 - 🔒 Modeli zasnovani na mogućnostima i
 - 🔒 Modeli zasnovani na listama kontrole pristupa (*ACL – Access Control List*), kojima se definiše lista dozvola nad nekim objektom.

Modeli kontrole pristupa

Kontrola pristupa deli se i prema metodama implementacije na:

- ❑ Diskrecioni model (*DAC – Discretionary Access Control*),
- ❑ Mandatorni model (*MAC – Mandatory Access Control*) i
- ❑ Model grupa i uloga (*RBAC – Role-based access control*)

Model zasnovani na mogućnostima

- 🔒 Na primer, neka postoji računarski sistem u kojem program, da bi pristupio određenom objektu, mora imati posebnu oznaku (eng. token). Oznaka (token) određuje objekat i pruža programu (subjektu) dovoljna ovlašćenja za izvođenje određenog skupa akcija, kao što su čitanje ili pisanje, nad tim objektom.
- 🔒 Mogućnosti se mogu delegirati i kopirati.

Liste kontrole pristupa (ACL)

- ☐ Lista kontrole pristupa je uređeni skup podataka o ovlašćenjima ili pravima pristupa svih subjekata (korisnika ili programa) nad bazom podataka.
- ☐ Svaki korisnik ili grupa korisnika ima određena prava pristupa i ovlašćenja nad specifičnim objektom.
- ☐ U sistemima koji imaju velik broj korisnika i gde se stalno menjaju korisnici, nije preporučljivo koristiti liste kontrole pristupa.
- ☐ Diskrecioni i mandatorni modeli mogu koristiti liste kontrole pristupa u svojim implementacijama.

Diskrecioni model sigurnosti (*DAC*)

- ❑ *DAC* je sigurnosni model gde se prava pristupa daje na osnovu korisničkog identiteta.
- ❑ Svakom korisniku se daju specifična prava pristupa za različite objekte.
- ❑ Kreiranje autorizacije:




GRANT<lista privilegija> ON <objekat baze>
TO <identifikator(i) korisnika>
[WITH GRANT OPTION]

- ❑ Privilegije: SELECT, UPDATE, INSERT, DELETE, ALL PRIVILEGES...
- ❑ Objekti: TABLE i DOMAIN

Diskrecioni model sigurnosti (DAC)

 Opozivanje privilegije:

**REVOKE [GRANT OPTION FOR] <lista privilegija>
ON <objekat baze> FROM <identifikator(i) korisnika>
[RESTRICT | CASCADE]**

-  Opcija GRANT OPTION FOR se koristi kada se opoziva mogućnost prenosa privilegija.
-  RESTRICT – onemogućava opozivanje privilegija ukoliko su prenete drugim korisnicima.
-  CASCADE – opoziva pored navedenih privilegija i sve prenete privilegije.

Diskrecioni model sigurnosti (DAC)

- ❑ Napomena: Vlasnik šeme baze podataka (korisnik koje je kreirao šemu) ima sve privilegije u njoj.

Primer: *User1* je vlasnik šeme *Drzava*.

Drzava(DID, Naziv, Uredjenje)

Grad(DID, GID, Naziv)

1. GRANT SELECT, INSERT ON Drzava TO *User2*
WITH GRANT OPTION

2. GRANT SELECT, UPDATE ON Grad To *User3*

Mandatorni model (MAC)

- ❑ *MAC* je sigurnosni model gde korisnicima prava na resurse može da da samo administrator ili operativni sistem.
- ❑ Subjektima i objektima je dodeljen skup sigurnosnih prava ili klasifikacija.
- ❑ Pristup određenim resursima dozvoljen je samo subjektima s dodeljenom klasifikacijom.
- ❑ Mandatorni model pristupa koristi se kod obrađivanja vrlo osetljivih podataka, kao što su poverljive informacije vladinih i vojnih organizacija.

Model zasnovan na ulogama (RBAC)

- ❑ *Role Based Access Control (RBAC)* – Način kontrole pristupa zasnovan na ulogama i pravima.
- ❑ U ovom sigurnosnom modelu, pristup resursima je baziran na ulozi korisnika koju je dobio od administratora.
- ❑ Administrator dodeljuje ulogu koja dolazi sa već određenim pravima i privilegijama, i korisnik može da vrši samo akcije dodeljene pravilima uloge.
- ❑ *RBAC* je novija alternativa *DAC* i *MAC*.
- ❑ *RBAC* model nudi mogućnost implementacije i *MAC* modela i *DAC* modela kontrole pristupa.

Princip minimalnih ovlašćenja

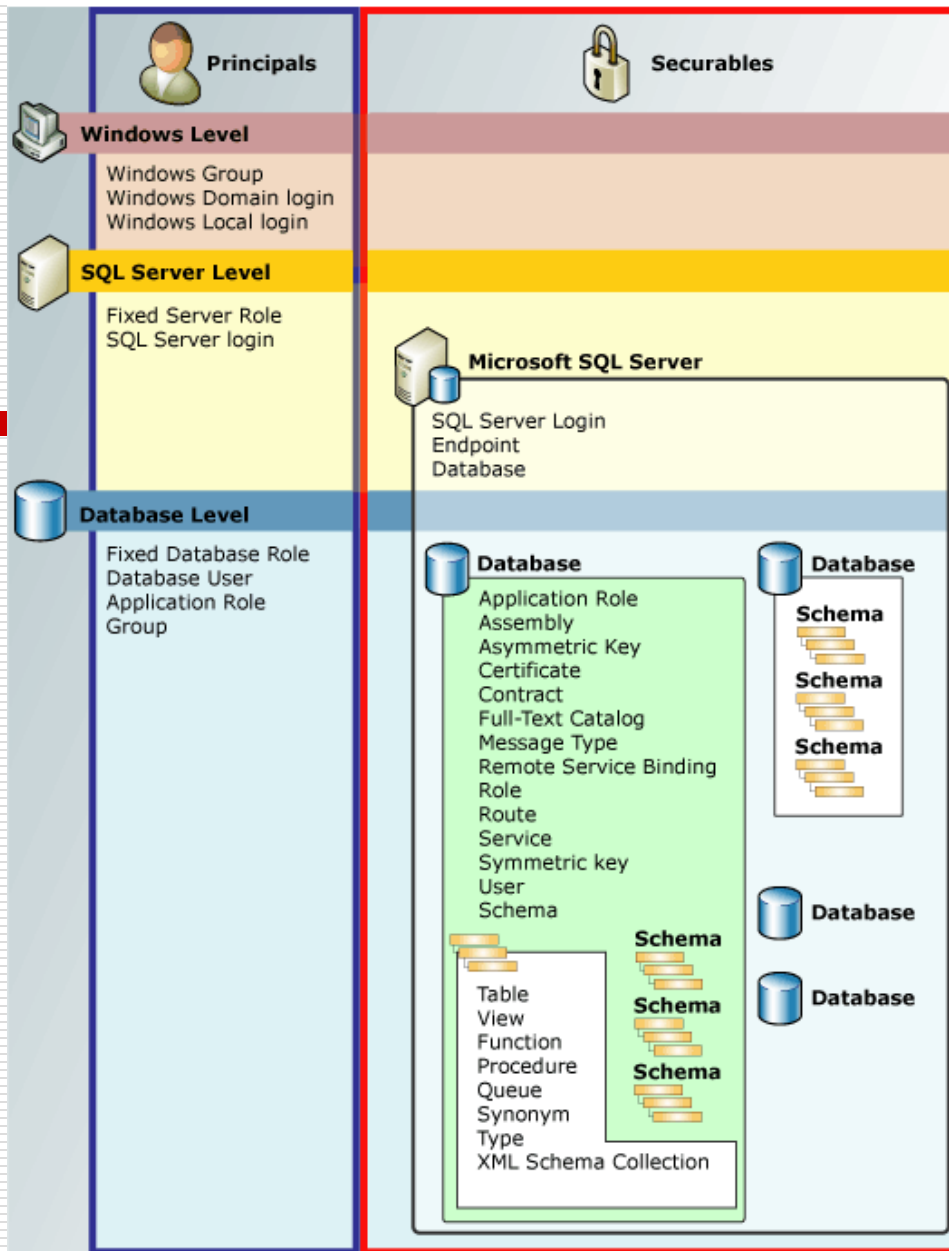
- ❑ Princip minimalnih ovlašćenja predviđa da korisnicima treba dodeliti samo minimum ovlašćenja potrebnih za obavljanje njihovih poslova nad bazom. To takođe predviđa:
 - Upotrebu uloga, koje sadrže grupe (skup) ovlašćenja i olakšavaju administraciju;
 - Upotrebu pogleda, koji ograničavaju pristup na definisane podskupove postojećih podataka;
 - Upotrebu uskladištenih procedura čijom se upotrebom može izbeći dodela konkretnih prava nad baznim tabelama korisnicima.

Sigurnost baze podataka

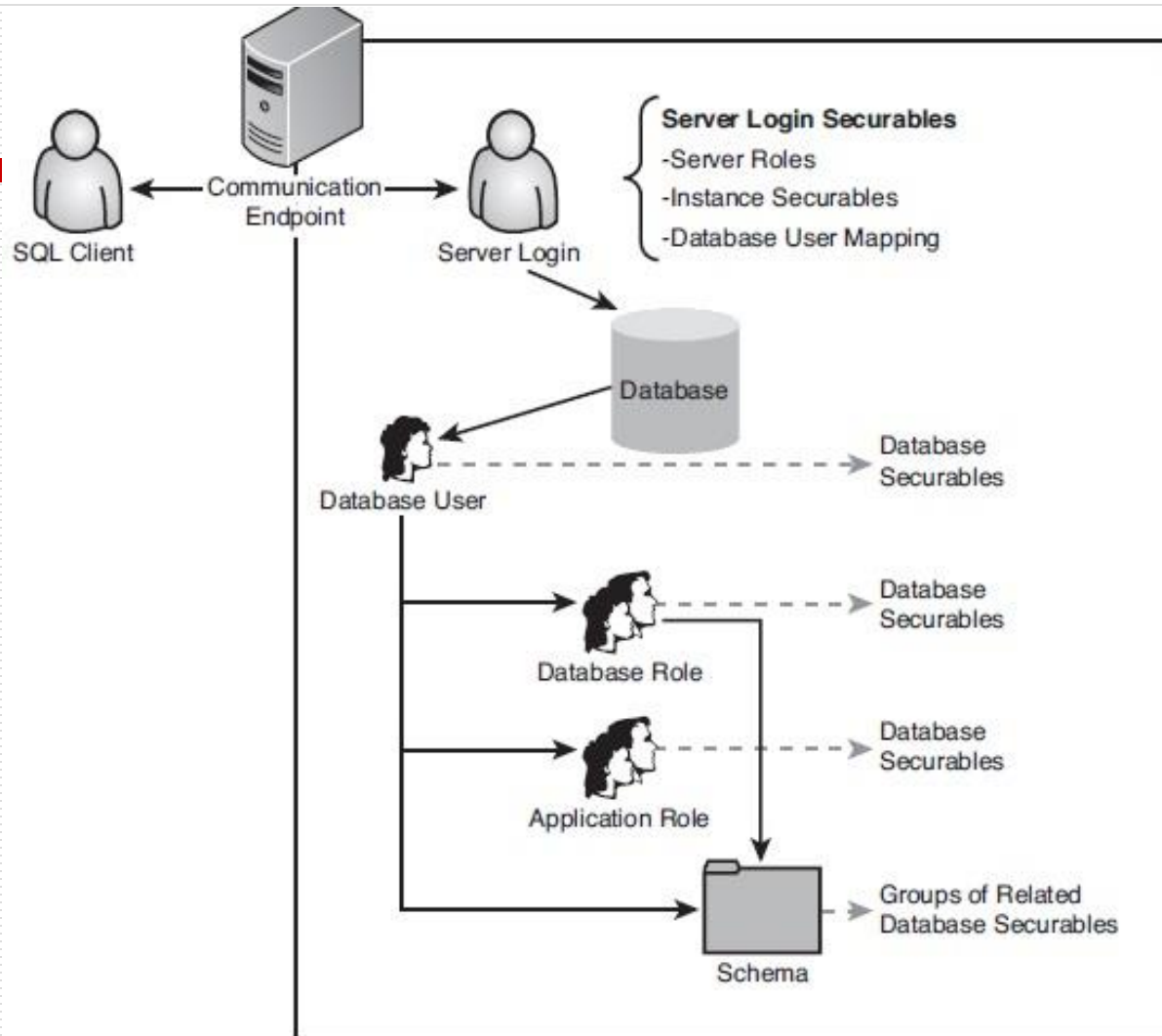
SIGURNOST kod MICROSOFT SQL SERVERA

SQL Server Security Overview

- ❑ Višenivojski model zaštite (*Layered Security Model*):
 - Windows Level
 - SQL Server Level
 - Database
 - Schemas (for database objects)
- ❑ Terminologija:
 - Principals – Objekti BP kojima se dodeljuju prava
 - Securables – Objekti baze podataka koji se štite
 - Permissions – Dozvole (prava pristupa)
 - Scopes and Inheritance



MS SQL Server - Security



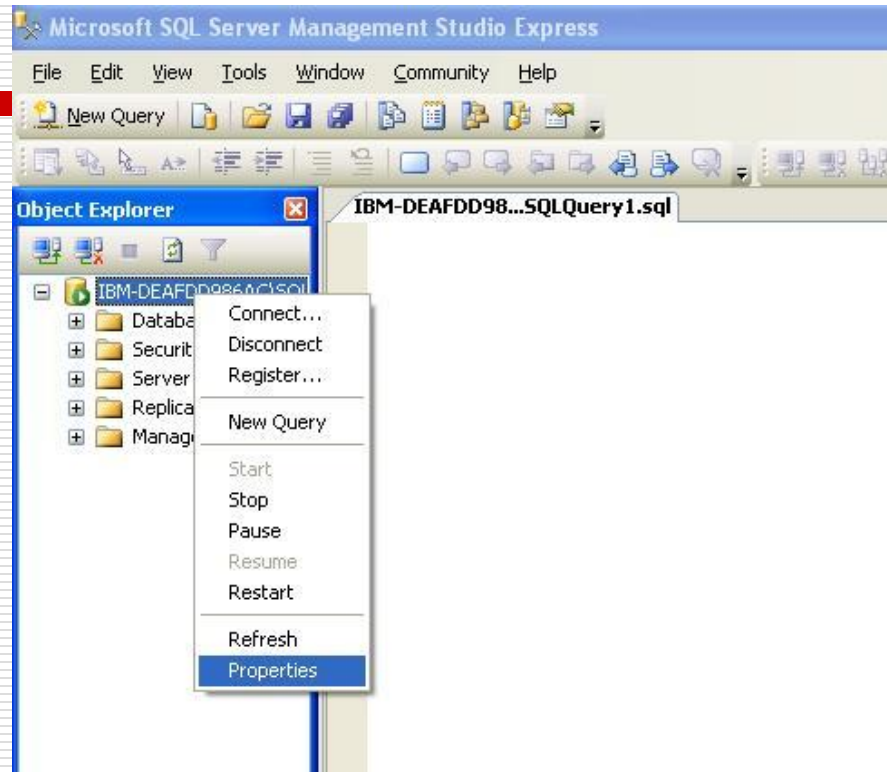
Preporuke - najbolja praksa -

- ☐ Administracija zaštite baze podataka treba da bude deo procesa standardne administracije baze podataka.
- ☐ Koristiti princip najmanjih privilegija.
- ☐ Implementirati dubinsku zaštitu na više nivoa.
- ☐ Dozvoliti (*enejblovati*) samo potrebne servise i komponente.
- ☐ Redovno pratiti podešavanja zaštite.
- ☐ Obučavati korisnike o važnosti zaštite.
- ☐ Definirati zaštitne uloge u sistemu na osnovu poslovnih pravila koja važe u sistemu.

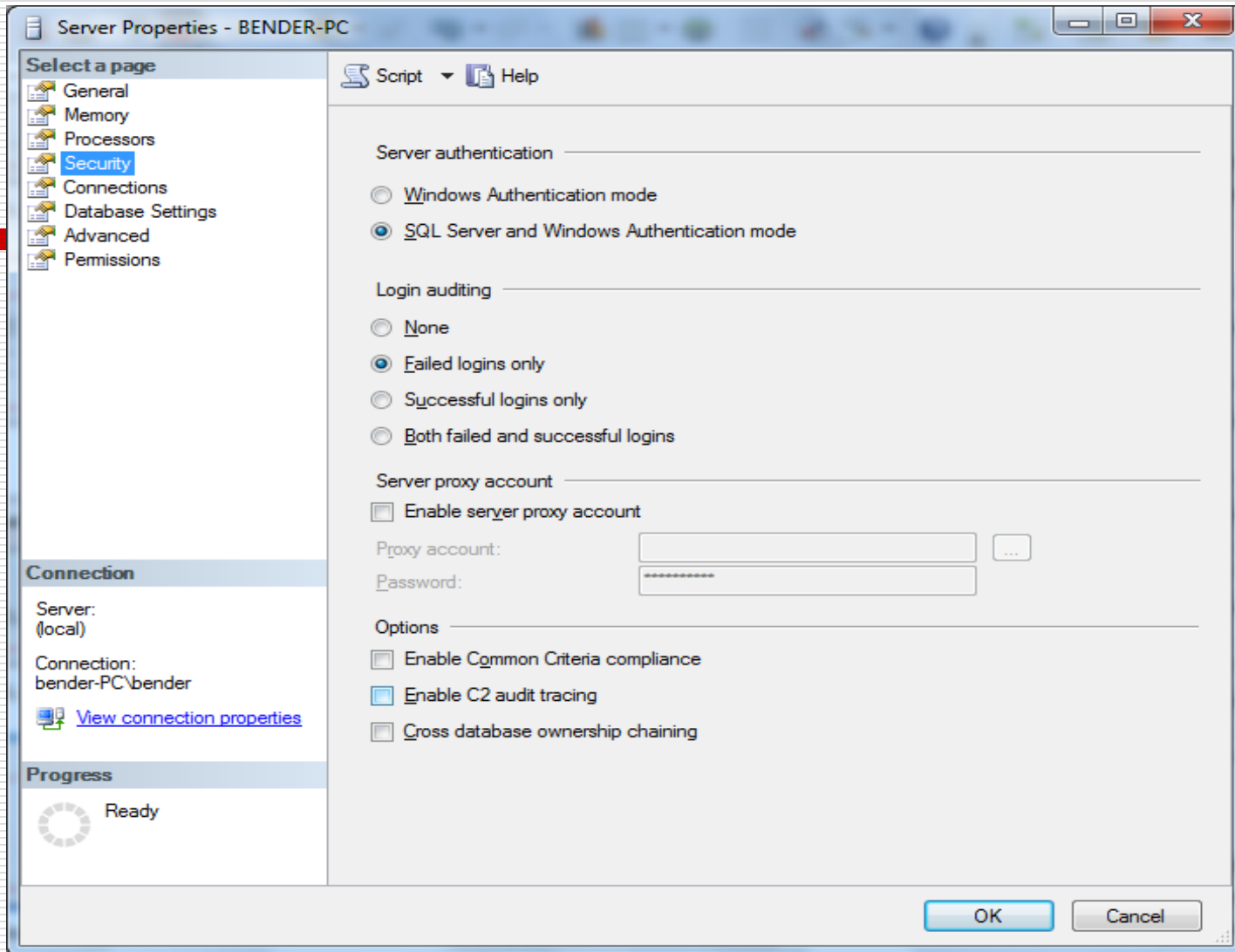
MS SQL Server - Režimi bezbednosti

- ❑ SQL Server poseduje dva načina na koje se korisnik (takođe i aplikacija ili Web sajt), može povezati.
 - SQL Server autentifikacija
 - Windows autentifikacija
 - ❑ Način autentifikacije se definiše pri instalaciji ali se može promeniti promenom parametara konfiguracije SQL Servera.
-

Konfigurisanje SQL Servera



Promena načina Autentifikacije



SQL Server autentifikacija

- ❑ Znači da je potrebno upisati korisničko ime i šifru za povezivanje.
 - ❑ Ovaj način povezivanja se koristi u slučaju peer to peer mreža, bez centralizovane lokacije na kojoj se čuvaju korisnički računi – aktivni direktorijum.
-

Windows autentifikacija

- ☐ Koristi se ime korisnika i šifra preko kojih se korisnik ulogovao na Windows.
 - ☐ Ideja iza ovoga je da jednom prijavljen korisnik na Windows mrežu, iste kredencijale koristi i za prijavu na SQL Server.
 - ☐ U predhodnom nastavku smo prilikom instalacije dodali korisnika Administrator, što znači da svako ko se na Windows prijavi kao administrator, automatski ima prava prijave i na SQL Server.
 - ☐ Ovo se može uraditi za bilo koji korisnički račun ili grupu na lokalnom računaru, kao i u domenskoj mreži.
-

Pristup MS SQL Serveru

- ❑ Bez obzira na način prijave koji je izabran, pre svega je neophodno uneti ime SQL Servera na koji želimo da se povežemo.
 - Standardno, ime SQL Servera je isto kao ime računara na koji je instaliran. Isto važi i za njegovu IP adresu.
 - ❑ Osnovni protokol koji koristi SQL Server je TCP/IP na portu 1433, što je značajan podatak u slučaju da postoji FireWall.
 - ❑ Umesto Imena SQL Servera na koji se vezujemo uvek se može uneti njegova IP adresa, kao i ime računara na kojem je instaliran (što se opet prevodi u njegovu IP adresu). Izuzetak od ovoga je slučaj kada se SQL Server nalazi na Internetu i tada se mora uneti njegova IP adresa.
-

Pristup MS SQL Serveru

- ❑ Postoje i dve skraćenice kada je u pitanju lokani SQL Server. Može se upisati (**local**) ili jednostavno tačka(.).
- ❑ Obe skraćenice se interno prevode na IP adresu **127.0.0.0** što označava lokalnu IP adresu lokalnog računara.
- ❑ SQL Server Express edition po inicijalnoj instalaciji predstavlja mali izuzetak od ovog pravila jer se njegovo ime formira po sistemu **ImeRačunara\SQLEXPRESS** kako bi se razlokovalo od "velikog" SQL Servera.

Logins and Users

- ❑ Kod SQL Servera postoje dva nivoa provere prava pristupa:
 1. Logins – Korisnički nalog na nivou cele instance SQL Servera.
 2. Users – Korisnički nalozi za posebnu bazu podataka kojom rukuje instanca SQL Servera.

Logins and Users

- ❑ Da bi se uspešno povezao sa SQL Serverom korisnik koji se povezuje na SQL Server mora imati oba naloga:
 - Login nalog za instancu SQL Servera i
 - User nalog za bazu podataka.
- ❑ U protivnom neće moći da se konektuje na SQL Server.
- ❑ Pored toga postoje i Windows korisnički nalozi kojima se rukuje na nivou domena mreže i za njih nije odgovoran DBA već Administrator sistema.

Dozvola pristupa servisima SQL Servera

- ❑ Dozvola pristupa servisima SQL Servera izvodi se u četiri koraka:
 1. Kreira se Login nalog.
 2. Kreira se User nalog – jedan za svaku bazu podataka kojoj se zahteva pristup.
 3. Pridruživanje Login naloga User nalogu.
 4. Definisanje prava pristupa i uloga (*Roles*) User nalogu.

System Administrator (sa) Login

- ☐ U procesu instalacije SQL Servera, ako se izabere *Mixed Mode authentication*, sistem zahteva da se postavi *Password* za **sa** predefinisani administrativni *Login* nalog.
- ☐ Potrebno je u procesu instalacije odmah dodeliti *Password* za **sa** Login nalog da bi se sprečio neautorizovani pristup instanci SQL Server-a korišćenjem **sa** *Login* naloga.
- ☐ Ukoliko se pri instalaciji izabere *Windows Authentication* mod potrebno je posle instalacije dodeliti *Password* za **sa** *Login* nalog da bi osigurali da **sa** *Login* nalog ima *Password* u slučaju da se kasnije promeni način autentifikacije u *Mixed Mode authentication*.
- ☐ Ne koristiti *blank password*.

System Administrator (sa) Login

- ❑ *System administrator (sa)* se koristi da bi se obezbedila kompadibilnost sa prethodnim verzijama softvera.
- ❑ Inicijalno *Login nalogu (sa)* se pridružuje **sysadmin** *fixed server role* i to se ne može menjati. Iako je **sa** *built-in administrator login* ne treba ga rutinski koristiti. Umesto toga potrebno je kreirati poseban administratorski login i pridružiti ga **sysadmin** serverskoj ulozi.
- ❑ **sa** *built-in login* nalog koristiti samo kada nema drugog načina da se pristupi instanci SQL Server-a.

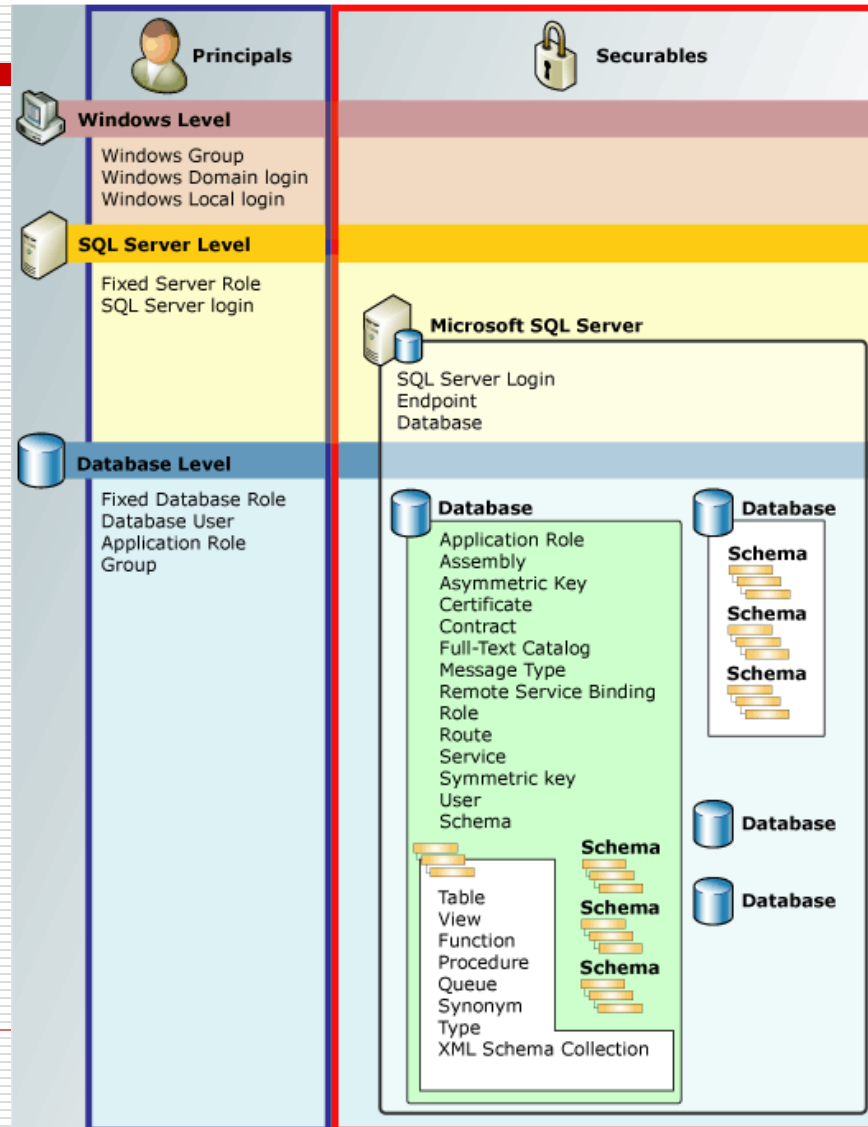
Identity and Access Control

- Kod SQL Server-a postoje različite metode i alati za konfigurisanje zaštite za korisnike, servise i druge naloge za pristup sistemu.
- Ovde su dati osnovni pojmovi koji se tiču rukovanja zaštitom kod SQL Server-a koje je potrebno poznavati
 - *Principals* (korisnici i korisnički nalozi)
 - *Roles* (groups of *Principals*);
 - Objekti zaštite (*Securables*)i
 - Dozvole (*Permissions*)
- *Principals* - Opisuju entitete koji mogu zahtevati resurse SQL Servera
- *Server-Level Roles* – Opisuju uloge na nivou SQL Server-a.
- *Database-Level-Roles* – Opisuju uloge u SQL Serveru na nivou Baze podataka.

Identity and Access Control

- ❑ *Principals* – Subjekti kojima se dodeljuju prava pristupa.
- ❑ *Securables* – Objekti čija zaštita se vrši.
- ❑ *Permissions* – Dodeljena prava pristupa subjektima nad objektima zaštite.

Identity and Access Control



Principals (Database Engine)

- ❑ *Principals* – entiteti koji mogu zahtevati resurs SQL Servera.
- ❑ Kao i kod drugih komponenti autorizacionog modela SQL Servera *Principals* mogu biti hijerarhijski organizovani.
- ❑ Svaki Principal ima svoj *Security Identifier (SID)*.

Principals

- ❑ *Windows-level principals*
 - Windows Domain Login
 - Windows Local Login
 - ❑ *SQL Server-level principal*
 - SQL Server Login
 - ❑ *Database-level principals*
 - Database User
 - Database Role
 - Application Role
-

Database Users- Korisnici Baze podataka

- ❑ Korisnik (*User*) baze podataka je *Principal* na nivou baze podataka. Svakom korisniku baze podataka je dodeljena ***public role***.
- ❑ Pri kreiranju baze podataka po *default*-u se kreira korisnik ***guest***. Prava pristupa dodeljena ***guest*** user-u se dodeljuju korisnicima koji nemaju korisnički nalog u bazi podataka.
- ❑ ***guest*** user se ne može ukloniti (izbrisati) ali se mogu ukinuti prava konekcije.
- ❑ Dozvola konekcije se može ukinuti izvršavanjem REVOKE CONNECT FROM GUEST u bilo kojoj bazi podataka SQL Servera osim u ***master*** ili ***tempdb*** sistemskim bazama podataka.

Server-Level Roles - Uloge na nivou Servera

- ❑ Da bi se jednostavnije dodeljivala prava na nivou SQL Servera, SQL Server obezbeđuje nekoliko uloga (*roles*). Uloge su slične grupama kod Windows operativnog sistema.
 - ❑ Serverskim ulogama se dodeljuju prava pristupa na nivou instance SQL Servera.
-

Mogućnosti uloga na nivou servera(1)

- ❑ **sysadmin** – Članovi ove uloge mogu izvršavati bilo koju aktivnost na nivou servera.
- ❑ **serveradmin** – Mogu menjati širok skup konfiguracionih parametara servera i vršiti zaustavljanje rada servera.
- ❑ **securityadmin** – Mogu upravljati login nalozima i njihovim parametrima. Članovi ove uloge mogu izvršavati GRANT, DENY, i REVOKE naredbe za prava pristupa na nivou servera. Osim toga mogu resetovati password za login naloge SQL Server-a.

Mogućnosti uloga na nivou servera(2)

- ❑ **processadmin** – Članovi ove uloge mogu upravljati procesima koji se izvršavaju u okviru instance SQL Server-a.
 - ❑ **setupadmin** – Članovi ove uloge mogu dodavati i uklanjati povezane servera.
-

Mogućnosti uloga na nivou servera(3)

- ❑ **bulkadmin** – Članovi ove uloge mogu izvršavati BULK INSERT naredbe.
 - ❑ **diskadmin** – Ova serverska uloga se koristi za upravljanje datotekama baze podataka na disku.
 - ❑ **dbcreator** – Članovi ove uloge mogu vršiti kreiranje, izmenu, uklanjanje i vršiti *restore* bilo koje baze podataka.
 - ❑ **public** – Svaki login nalog SQL Servera pripada *public* serverskoj ulozi. Kada subjekt na nivou servera (*principal*) nema dodeljena i zabranjena neka posebna prava nad objektima zaštite, korisnik nasledjuje prava dodeljena *public* ulozi nad tim objektom.
-

Database-Level Roles

- Kod SQL Servera postoje dve grupe uloga na nivou baze podataka:
 - Fiksne uloge koje su unapred definisane u bazi podataka i
 - Promenljive uloge na nivou baze podataka koje se mogu kreirati od strane administratora.

Database-Level Roles

- ❑ Fiksne uloge na nivou baze podataka postoje u svakoj bazi podataka. Članovi ***db_owner*** i ***db_securityadmin*** mogu upravljati pridruživanjem fiksnih uloga baze podataka korisnicima baze podataka. Međutim, samo članovi uloge ***db_owner*** mogu pridruživati članove u fiksnu ulogu ***db_owner*** baze podataka. Osim toga, u *msdb* sistemskoj bazi podataka postoje neke uloge posebne namene.
 - ❑ ***db_owner*** – Članovi ove uloge mogu izvršavati sve konfiguracione aktivnosti nad bazom podataka, mogu izvršavati i *Drop Database* naredbu.
 - ❑ ***db_securityadmin*** – Članovi ove uloge baze podataka mogu modifikovati pripadnost korisnika baze podataka ulogama i upravljati pravima pristupa (privilegijama).
-

Database-Level Roles

- ***db_accessadmin*** – Članovi ove uloge mogu dodavati ili uklanjati pravo pristupa bazi podataka za Windows login naloge, Windows grupe i SQL Server login naloge
- ***db_backupoperator*** – Članovi ove uloge mogu vršiti uzimanje rezervnih kopija baze podataka (*Backup*)
- ***db_ddladmin*** – Članovi ove grupe imaju pravo izvršavanja bilo koje DDL naredbe nad bazom podataka.

Database-Level Roles

- ***db_datawriter*** – Članovi ove uloge mogu dodavati, brisati ili menjati podatke u svim korisničkim tabelama baze podataka.
- ***db_datareader*** – Članovi ove uloge imaju pravo čitanja iz svih korisničkih tabela baze podataka.

Prava nad objektima

- Three separate object permissions exist in SQL Server:
 - 1. Grant** – can perform action
 - 2. Deny** – cannot perform action (strong). This applies even if the user account is a member of a role which has been granted the permission.
 - 3. Revoke** – cannot perform action (weak). This will be overridden by a grant to a role which the user account is a member of.
- So Grant and Revoke are the same as in oracle. The additional Deny command is an extra strong form of Revoke.

Application Roles

- *Application role* je *principal* baze podataka koji omogućava aplikaciji da se aplikacijama dodeljuju dozvole (prava) kao korisnicima baze podataka
- Ova uloga omogućava pristup podacima samo onim korisnicima koji se na bazu podataka konektuju preko neke aplikacije.
- Za razliku od uloga baze podataka aplikacione uloge ne sadrže članove i nisu aktivne po default-u. Rade u oba režima autentifikacije SQL Servera.
- Aplikacione uloge se enejbluju korišćenjem ***sp_setapprole***, koja zahteva *password*.

Application Roles

- Obzirom da je *application role* uloga na nivo baze podataka, preko nje se može pristupiti drugim bazama podataka samo na osnovu dozvola koje su u toj bazi podataka dodeljene **guest** korisniku.
 - Zbog toga, neće se moći pristupiti drugoj bazi podataka preko *application role* ako je u noj disejblovan **guest** korisnik.
-

Connecting with an Application Role

- The following steps make up the process by which an application role switches security contexts:
 - A user executes a client application.
 - The client application connects to an instance of SQL Server as the user.
 - The application then executes the **sp_setapprole** stored procedure with a password known only to the application.

Connecting with an Application Role

- If the application role name and password are valid, the application role is enabled.
- At this point the connection loses the permissions of the user and assumes the permissions of the application role.
- The permissions acquired through the application role remain in effect for the duration of the connection.

How to: Create a SQL Server Login

- Most Windows users need a SQL Server login to connect to SQL Server. This topic shows how to create a SQL Server login.
- To create a SQL Server login that uses Windows Authentication (SQL Server Management Studio)

How to: Create a SQL Server Login

1. In SQL Server Management Studio, open Object Explorer and expand the folder of the server instance in which to create the new login.
2. Right-click the Security folder, point to New, and then click Login.
3. On the General page, enter the name of a Windows user in the Login name box.
4. Select Windows Authentication.
5. Click OK.

How to: Create a SQL Server Login

- To **create a SQL Server login that uses SQL Server Authentication** (SQL Server Management Studio)
 1. In SQL Server Management Studio, open Object Explorer and expand the folder of the server instance in which to create the new login.
 2. Right-click the Security folder, point to New, and then click Login.
 3. On the General page, enter a name for the new login in the Login name box.
 4. Select SQL Server Authentication. Windows Authentication is the more secure option.
 5. Enter a password for the login.
 6. Select the password policy options that should be applied to the new login. In general, enforcing password policy is the more secure option.
 7. Click OK.

How to: Create a Database User

- To create a database user using SQL Server Management Studio
 1. In SQL Server Management Studio, open Object Explorer and expand the Databases folder.
 2. Expand the database in which to create the new database user.
 3. Right-click the Security folder, point to New, and then click User.
 4. On the General page, enter a name for the new user in the User name box.
 5. In the Login name box, enter the name of a SQL Server login to map to the database user.
 6. Click OK.

How to: Create a Database User

- Kreiranje korisnika baze podataka korišćenjem Transact-SQL naredbe
 1. Potrebno je u *Query Editor*-u izvršiti konekciju na bazu podataka u kojoj želimo da kreiramo novog korisnika baze podataka izvršavanjem sledeće Transact-SQL komande:

USE <database name> GO

1. Kreiranje korisnika baze podataka može se izvršiti sledećom Transact-SQL naredbom:

CREATE USER <new user name>
FOR LOGIN <login name>

Kreiranje korisnika baze podataka(1)

- Administracija korisnika baze podataka može se vršiti korišćenjem:
 - Transact-SQL komande ili
 - SQL Server Management Studio

Kreiranje korisnika baze podataka(2)

- Korisnik je subjekt zaštite (Principal) na nivou baze podataka.
- Login nalozi se mapiraju korisnike baze podataka da bi se izvršila konekcija na bazu.
- Login nalozi mogu se mapirati na različite baze podataka preko različitih korisnika, ali se na svaku od baza mogu mapirati kao samo jedan korisnik u svakoj bazi podataka.

Kreiranje korisnika baze podataka(3)

- Ukoliko je u bazi podataka *enejblovan* korisnik **guest**, Login nalog koji nije mapiran na korisnika baze podataka može bazi podataka pristupiti kao **guest** korisnik .
- Napomena – **guest** korisnik je inicijalno *disejblovan* i ne treba ga *enejblovati* ukoliko to nije neophodno.
- Da bi se konektovalo na neko od baza podataka instance SQL Servera Login nalog mora biti mapiran na korisnika baze podataka.
- Dozvole, odnosno prava pristupa dodeljuju se korisnicima baze podataka a ne Login nalozima.

Using SQL Server Management Studio

- To create a database user
 1. In Object Explorer, expand the Databases folder.
 2. Expand the database in which to create the new database user.
 3. Right-click the Security folder, point to New, and select User....
 4. In the Database User – New dialog box, on the General page, select one of the following user types from the User type list: SQL user with login, SQL user without login, User mapped to a certificate, User mapped to an asymmetric key, or Windows user.

Using SQL Server Management Studio

5. In the User name box, enter a name for the new user. If you have chosen Windows user from the User type list, you can also click the ellipsis (...) to open the Select User or Group dialog box.
6. In the Login name box, enter the login for the user. Alternately, click the ellipsis (...) to open the Select Login dialog box. Login name is available if you select either SQL user with login or Windows user from the User type list.

Using SQL Server Management Studio

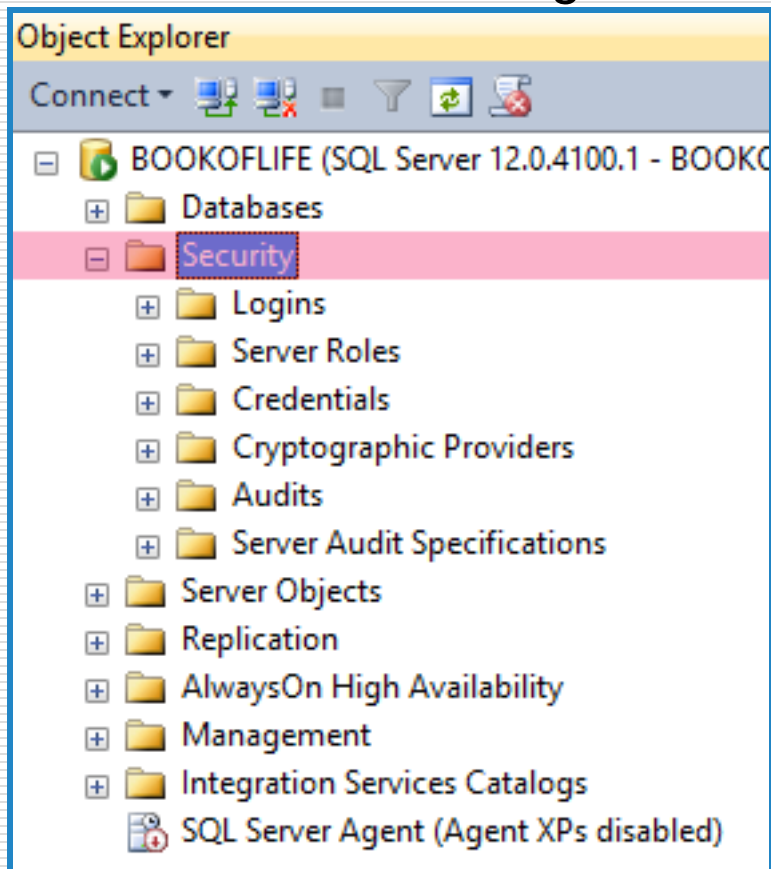
- In the Default schema box, specifies the schema that will own objects created by this user. Alternately, click the ellipsis (...) to open the Select Schema dialog box. Default schema is available if you select either SQL user with login, SQL user without login, or Windows user from the User type list.
- In the Certificate name box, enter the certificate to be used for the database user. Alternately, click the ellipsis (...) to open the Select Certificate dialog box. Certificate name is available if you select User mapped to a certificate from the User type list.

Administracija sigurnosti kod SQL Servera

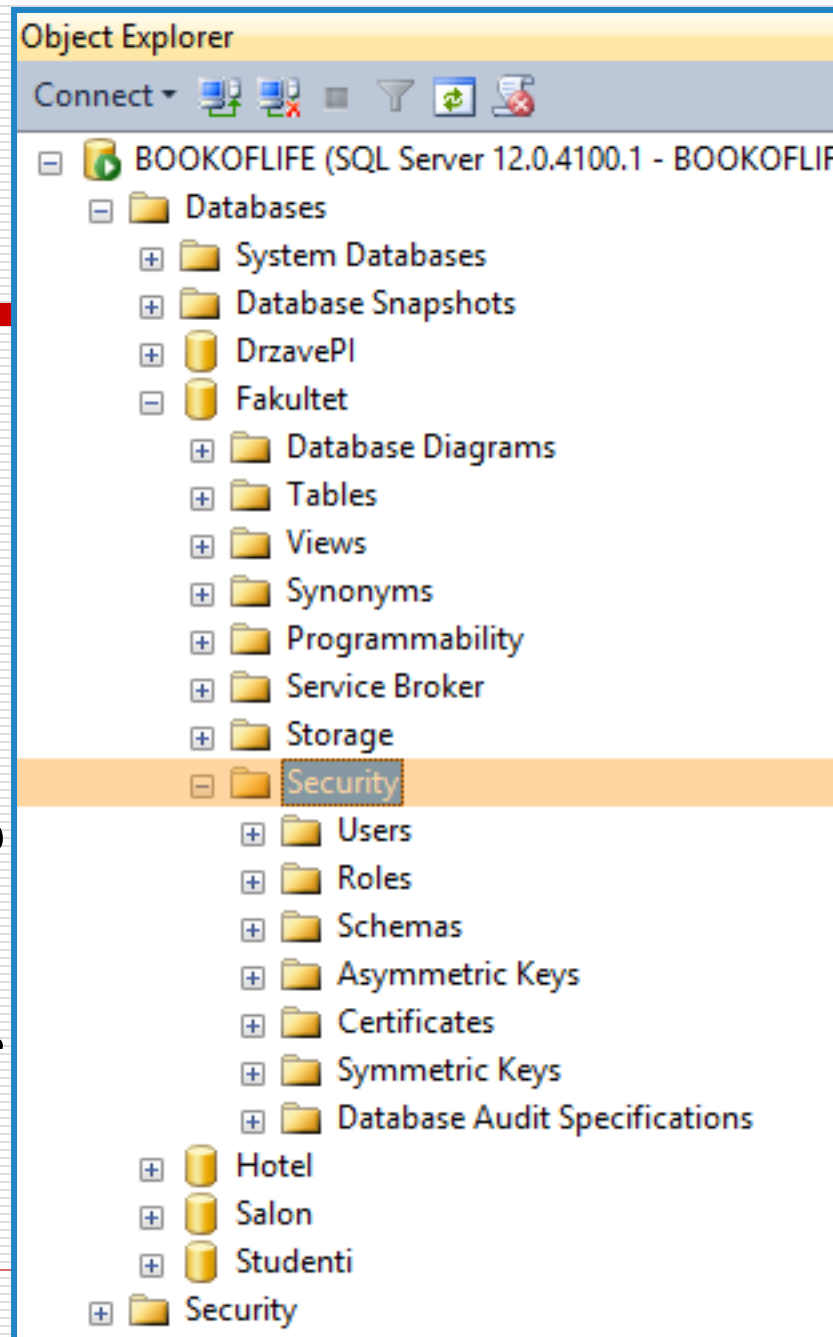
Korišćenje SQL Server Management Studio-a

Sistemska i objektna sigurnost

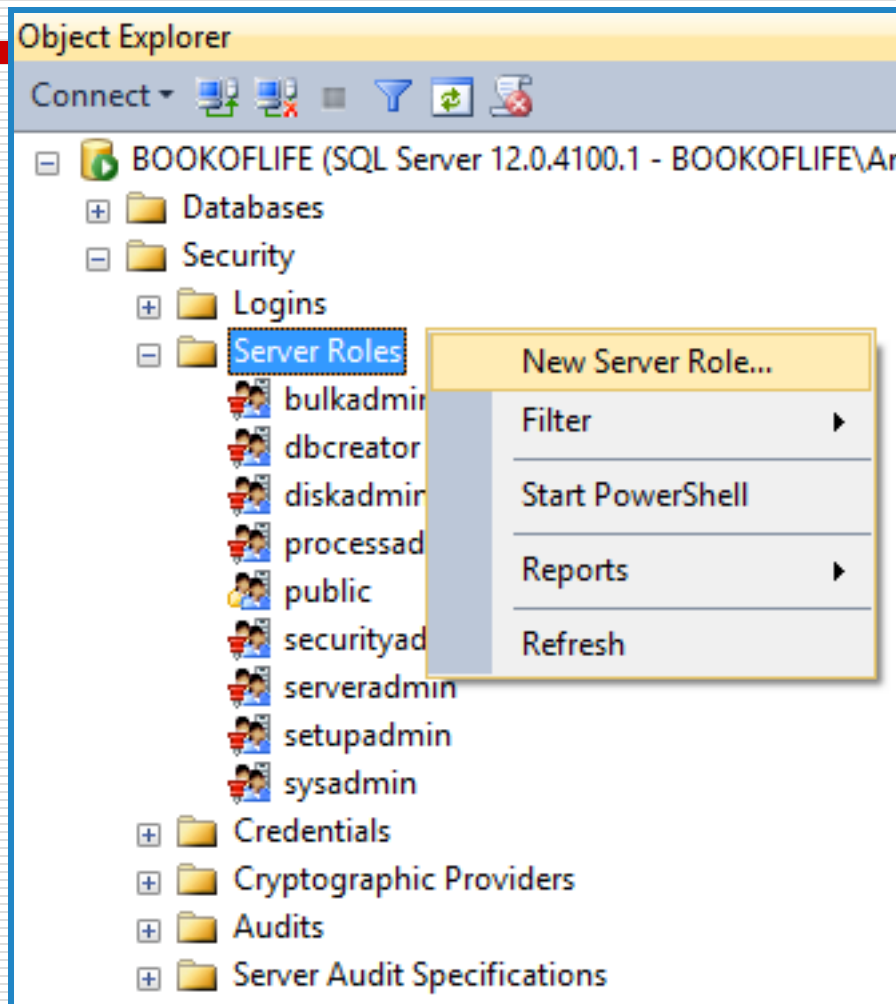
Slika 1: Sistemska sigurnost



Slika 2: Objektna sigurnost nad BP

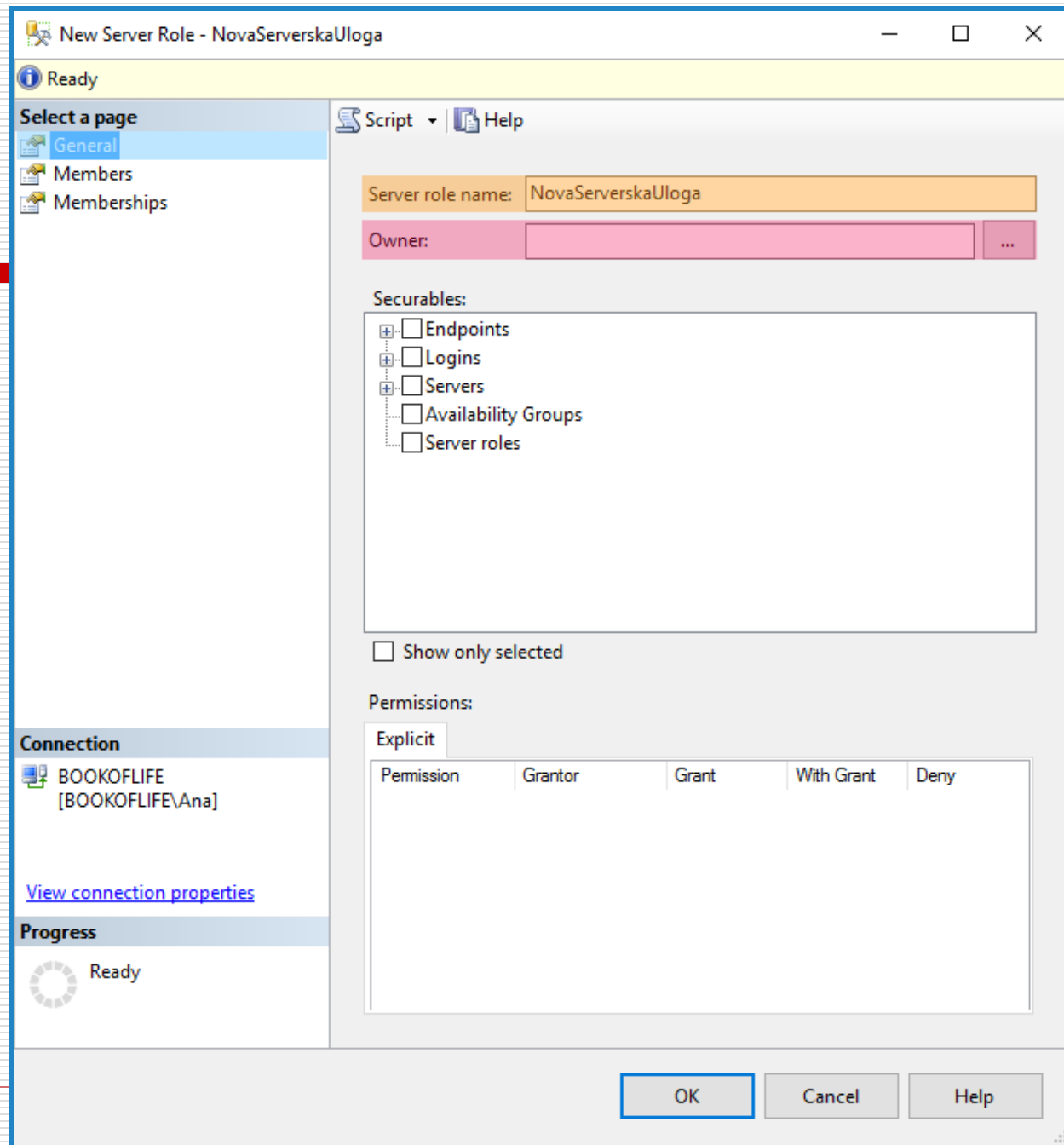


Sistemska sigurnost: kreiranje serverske uloge



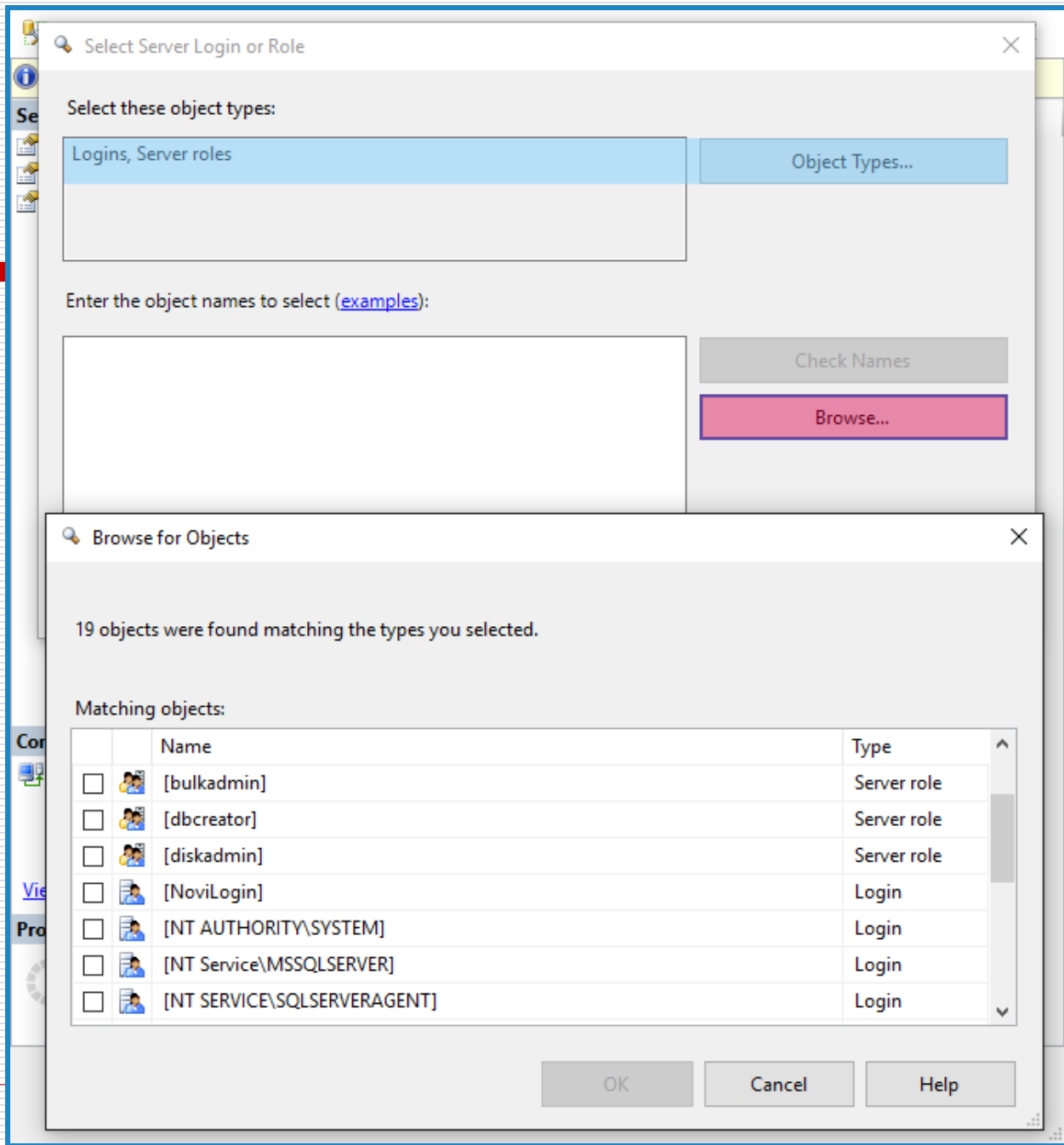
Slika 3: New Server Role

Sistemska sigurnost: kreiranje serverske uloge



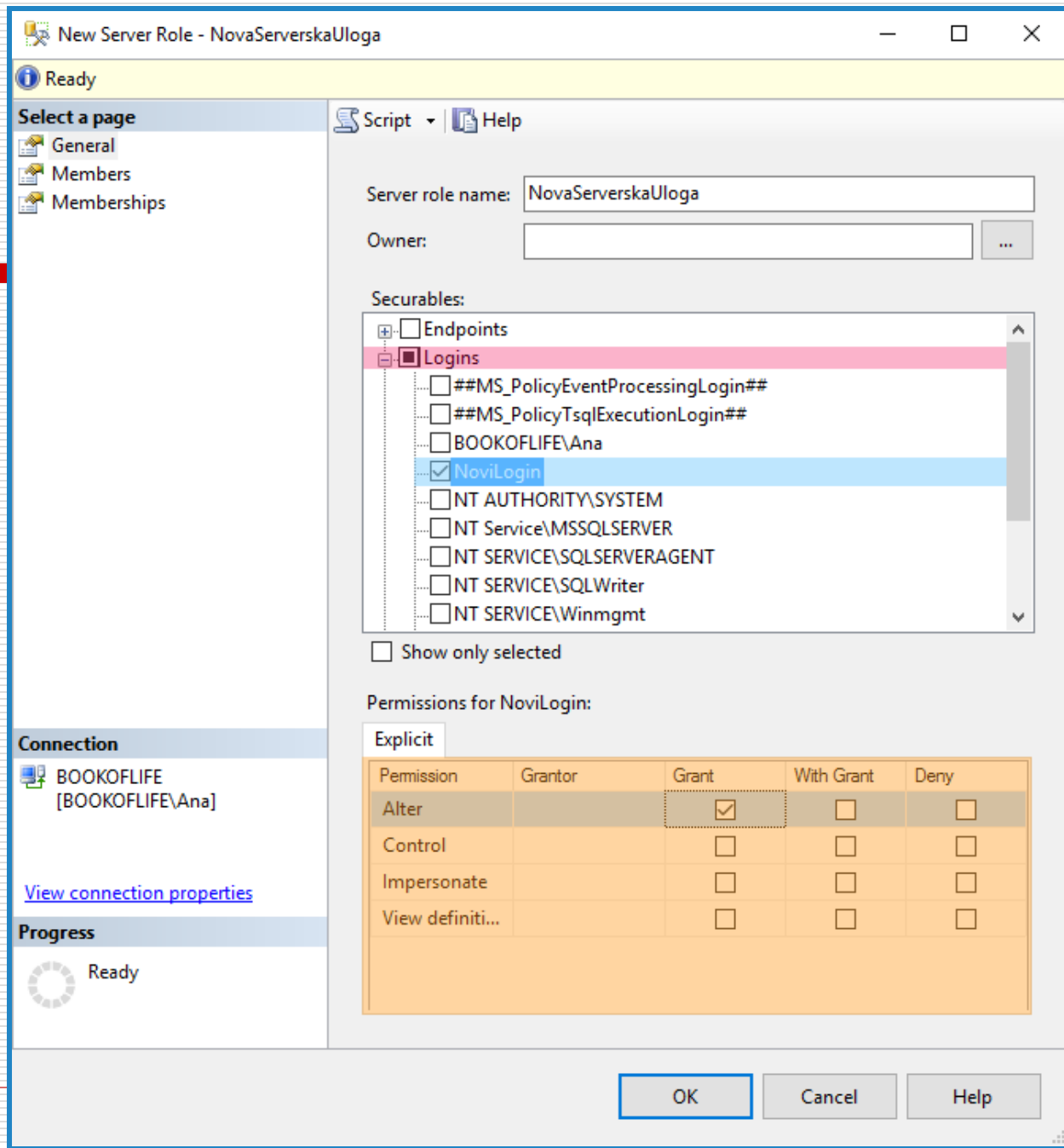
Slika 4: New Server Role

Sistemska sigurnost: kreiranje serverske uloge



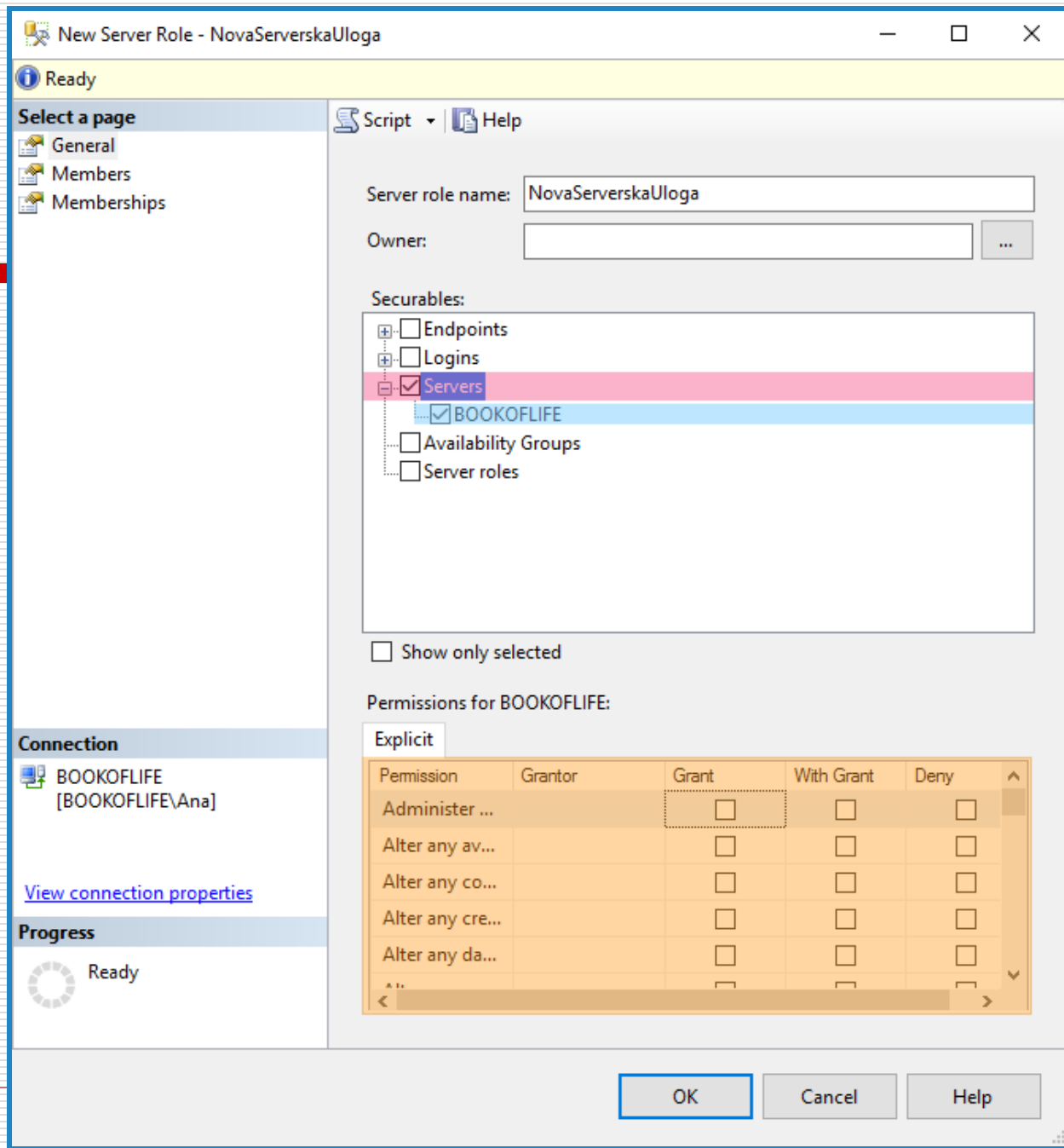
Slika 5: New Server Role

Sistemska sigurnost: kreiranje serverske uloge



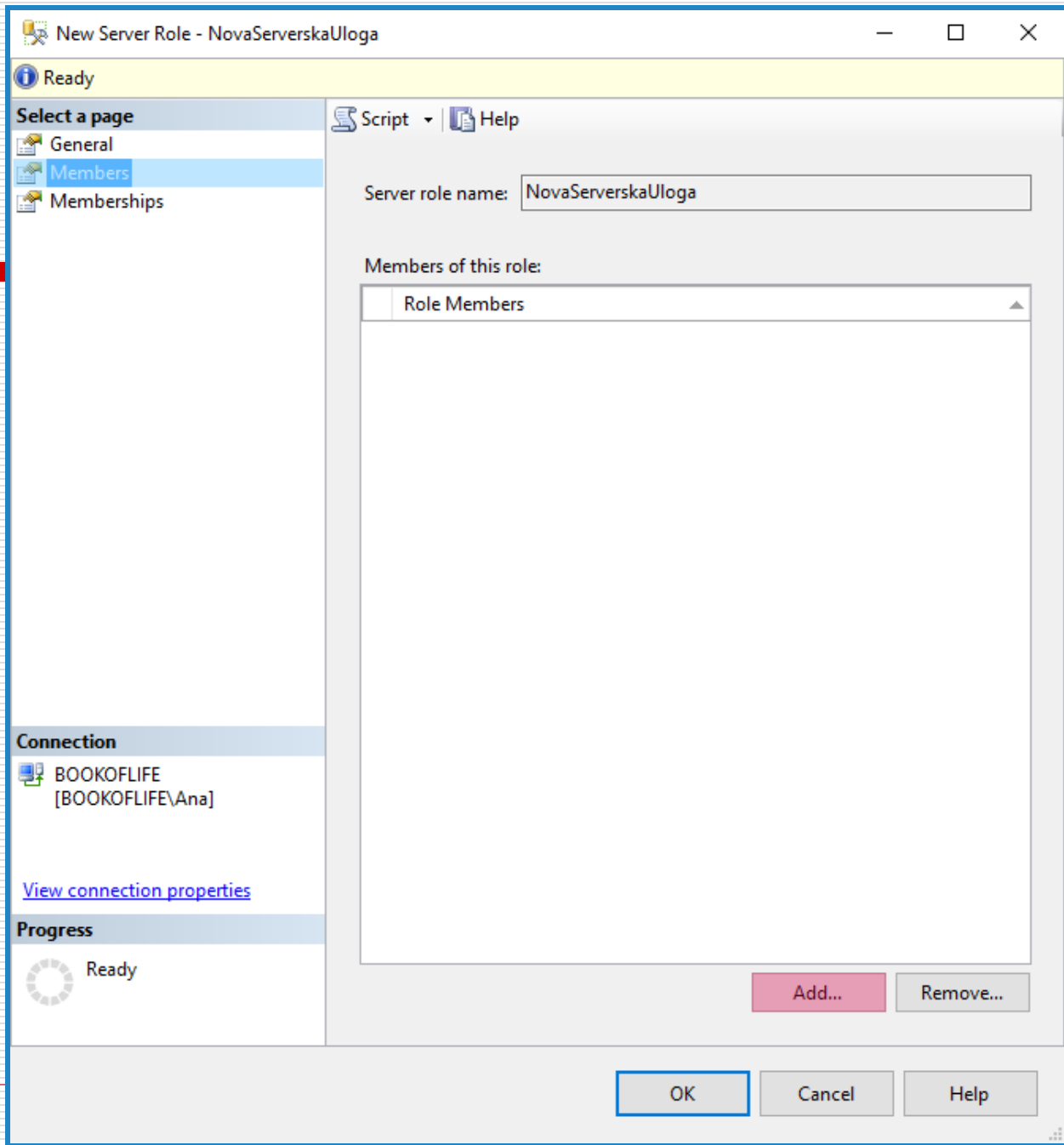
Slika 6: New Server Role

Sistemska sigurnost: kreiranje serverske uloge



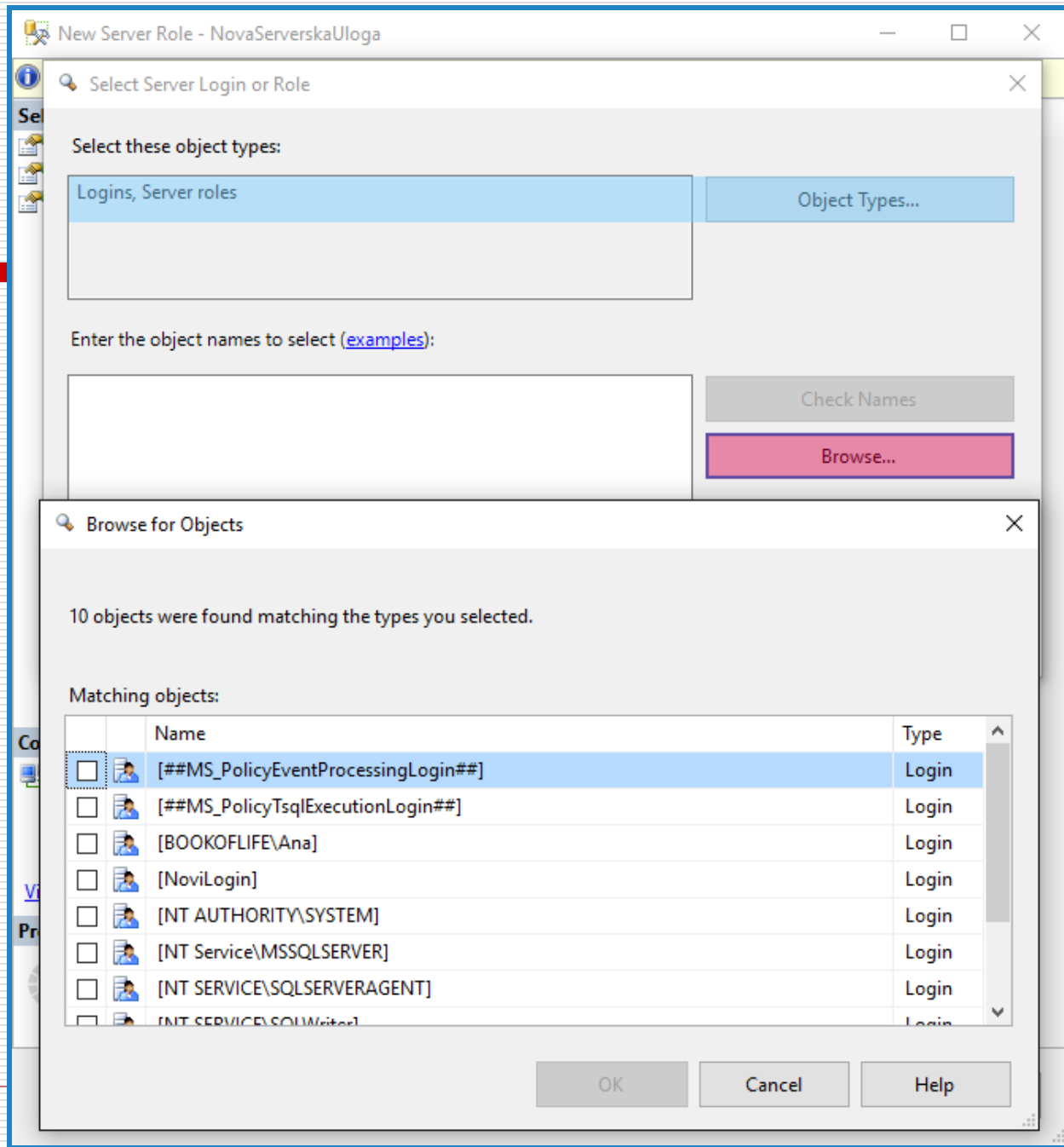
Slika 7: New Server Role

Sistemska sigurnost: kreiranje serverske uloge



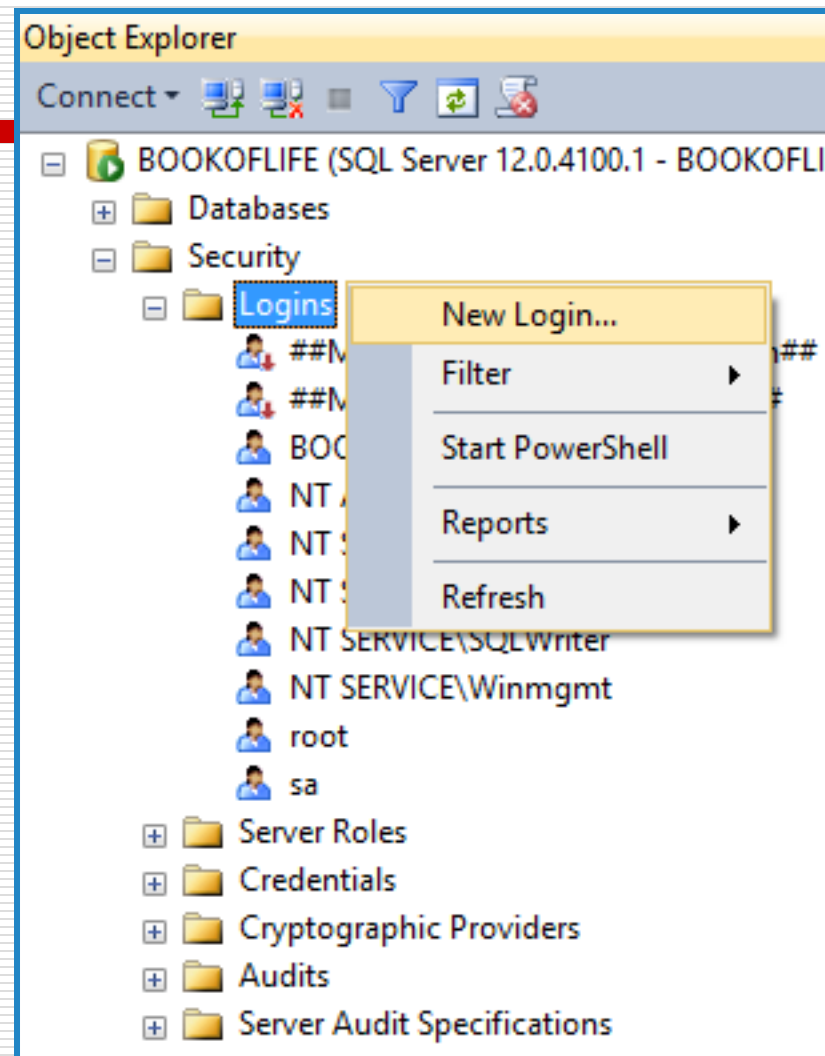
Slika 8: New Server Role

Sistemska sigurnost: kreiranje serverske uloge



Slika 9: New Server Role

Sistemska sigurnost: kreiranje login-a



Slika 10: New Login

Sistemska sigurnost: kreiranje login-a

Login - New

Select a page

- General
- Server Roles
- User Mapping
- Securables
- Status

Script Help

Login name: NoviLogin Search...

☐ Windows authentication

☒ SQL Server authentication

Password:

Confirm password:

☐ Specify old password

Old password:

☒ Enforce password policy

☒ Enforce password expiration

☒ User must change password at next login

☐ Mapped to certificate

☐ Mapped to asymmetric key

☐ Map to Credential

Mapped Credentials

Credential	Provider
------------	----------

Add

Remove

Default database: master

Default language: <default>

OK Cancel

Server: BOOKOFLIFE

Connection: BOOKOFLIFE\Ana

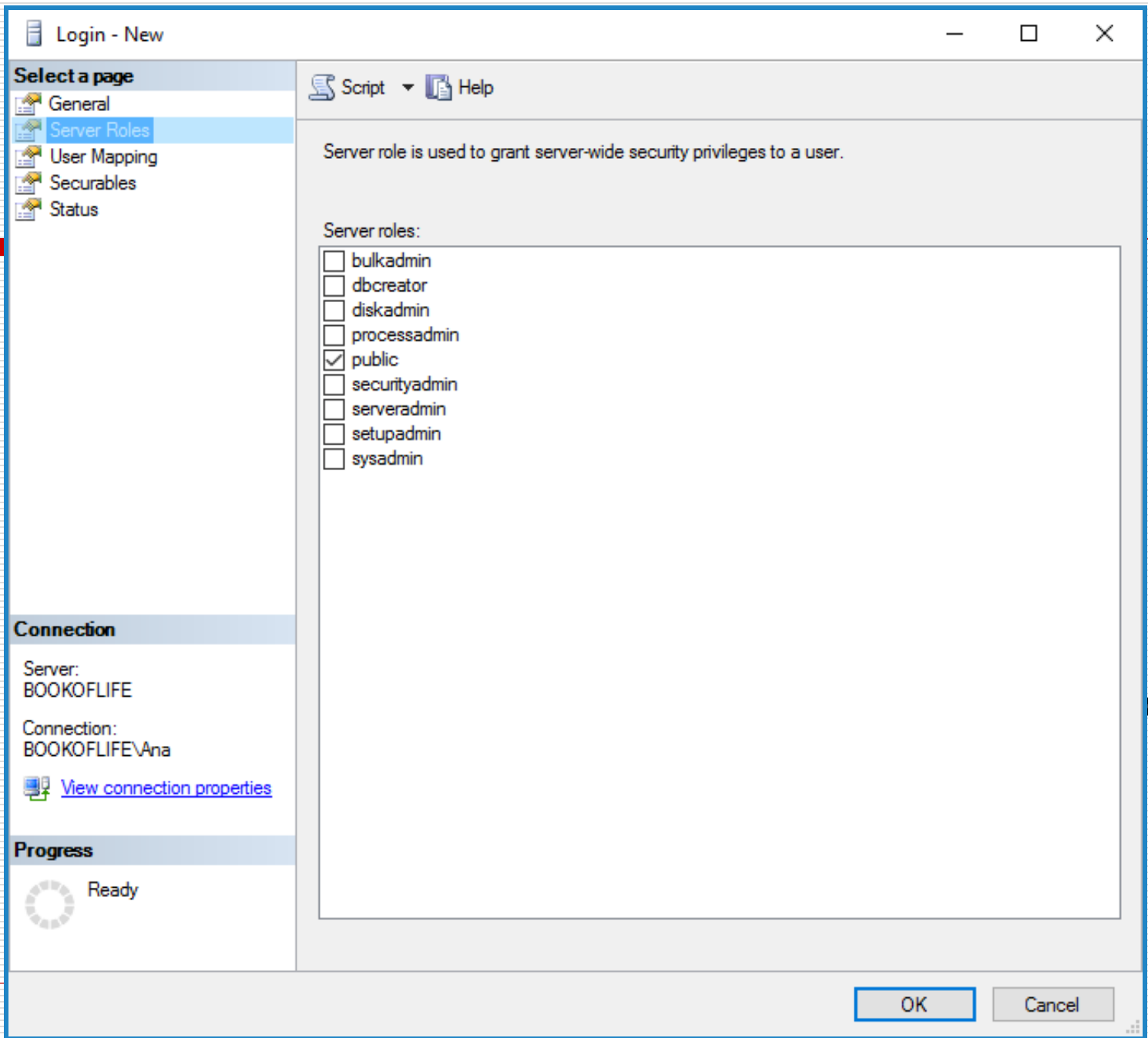
[View connection properties](#)

Progress

Ready

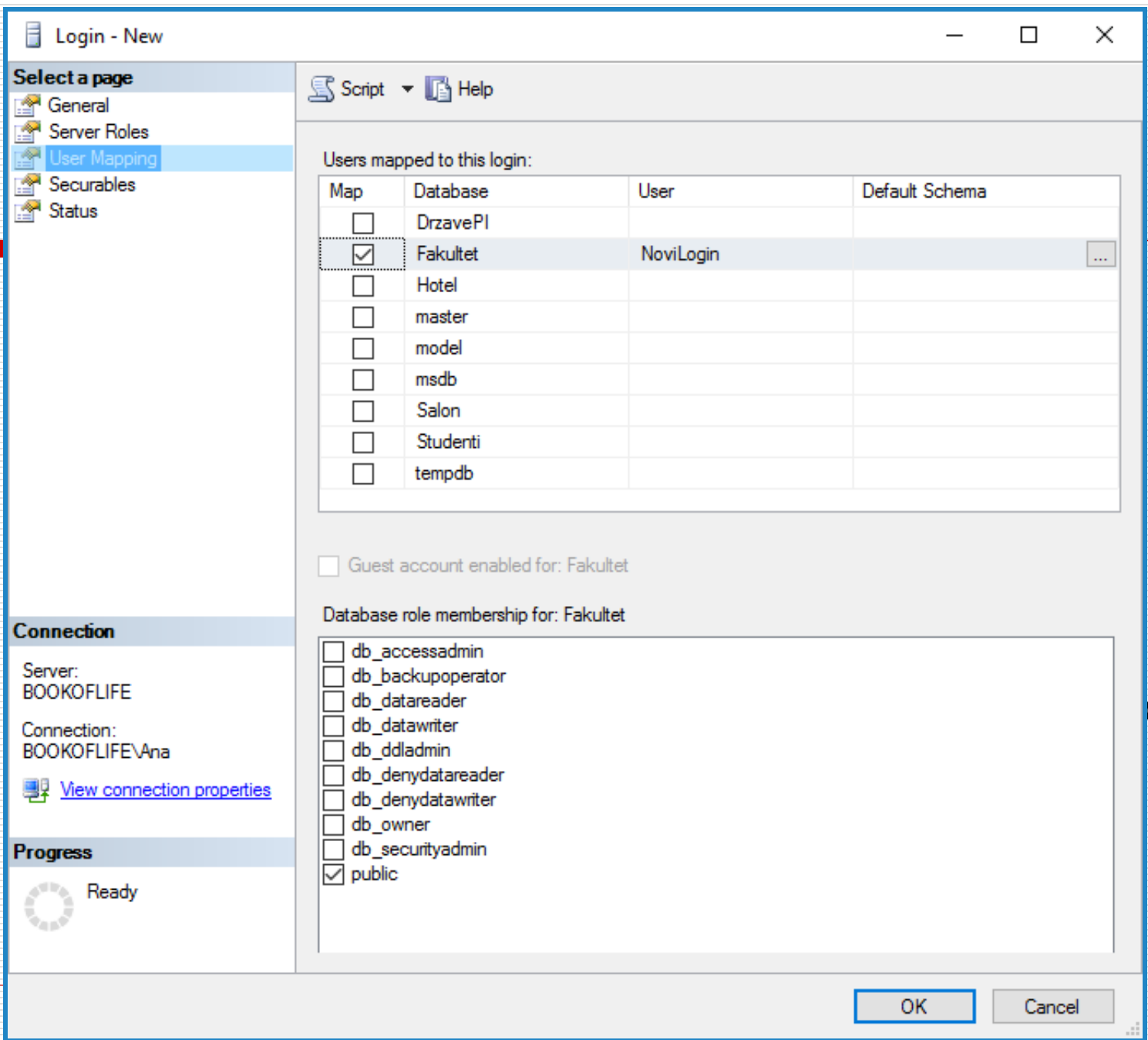
Slika 11: New Login

Sistemska sigurnost: kreiranje login-a



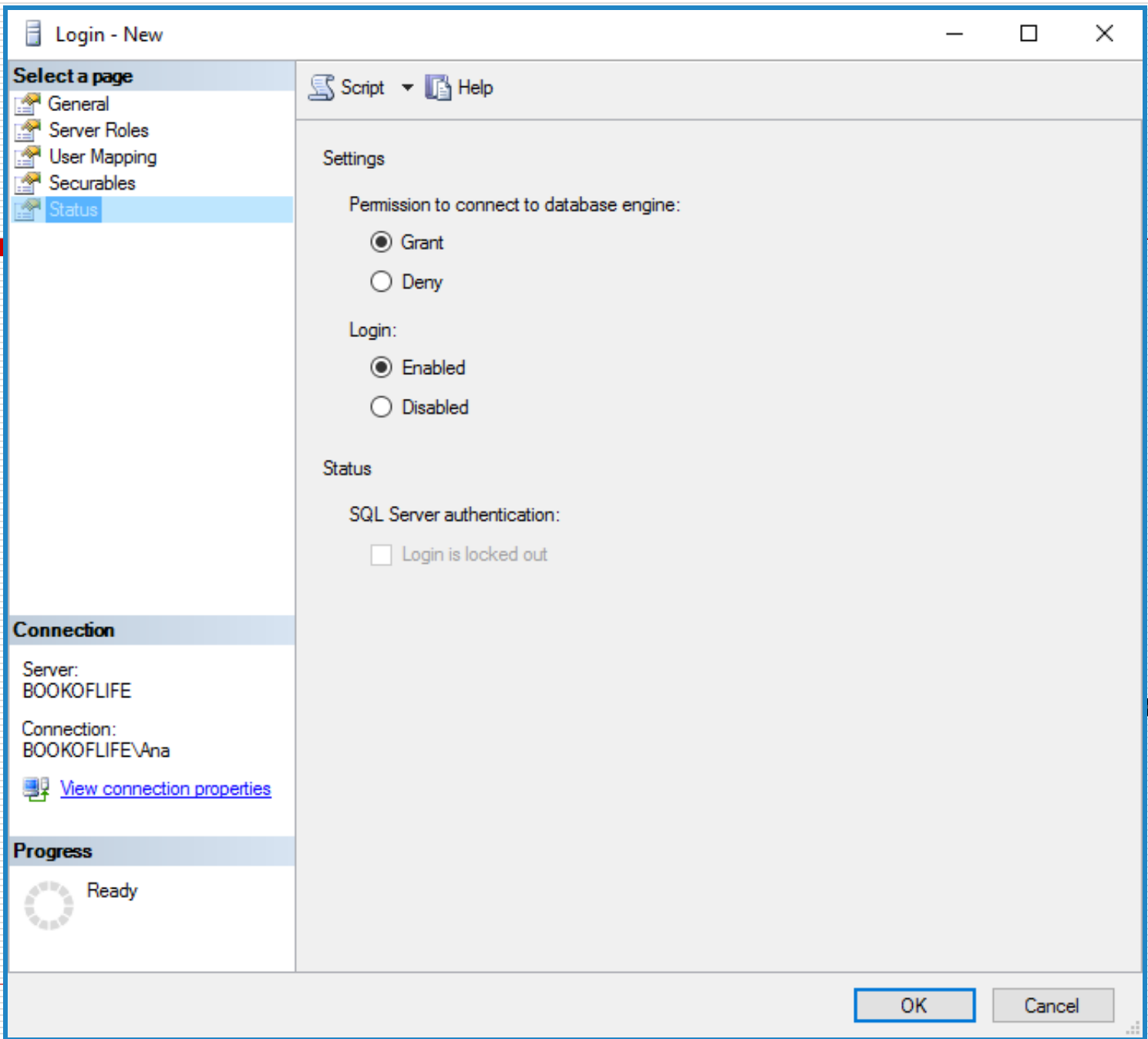
Slika 12: New Login

Sistemska sigurnost: kreiranje login-a



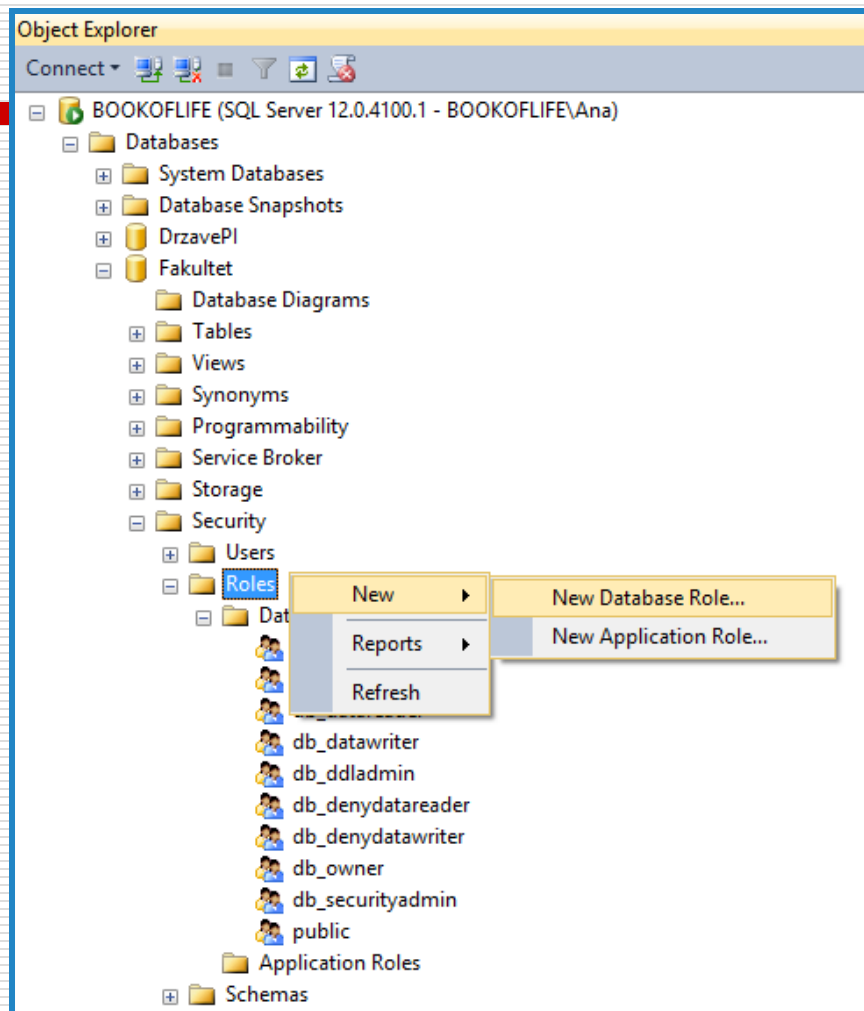
Slika 13: New Login

Sistemska sigurnost: kreiranje login-a



Slika 14: New Login

Objektna sigurnost: kreiranje uloge



Slika 15: New Database Role

Objektna sigurnost: kreiranje uloge

Database Role - New

Select a page

- General
- Securables
- Extended Properties

Script Help

Role name: NovaUloga

Owner:

Schemas owned by this role:

	Owned Schemas
<input type="checkbox"/>	db_accessadmin
<input type="checkbox"/>	dbo
<input type="checkbox"/>	db_securityadmin
<input type="checkbox"/>	sys
<input type="checkbox"/>	db_owner
<input type="checkbox"/>	db_backupoperator

Members of this role:

Role Members

Add... Remove

OK Cancel

Connection

Server: BOOKOFLIFE

Connection: BOOKOFLIFE\Ana

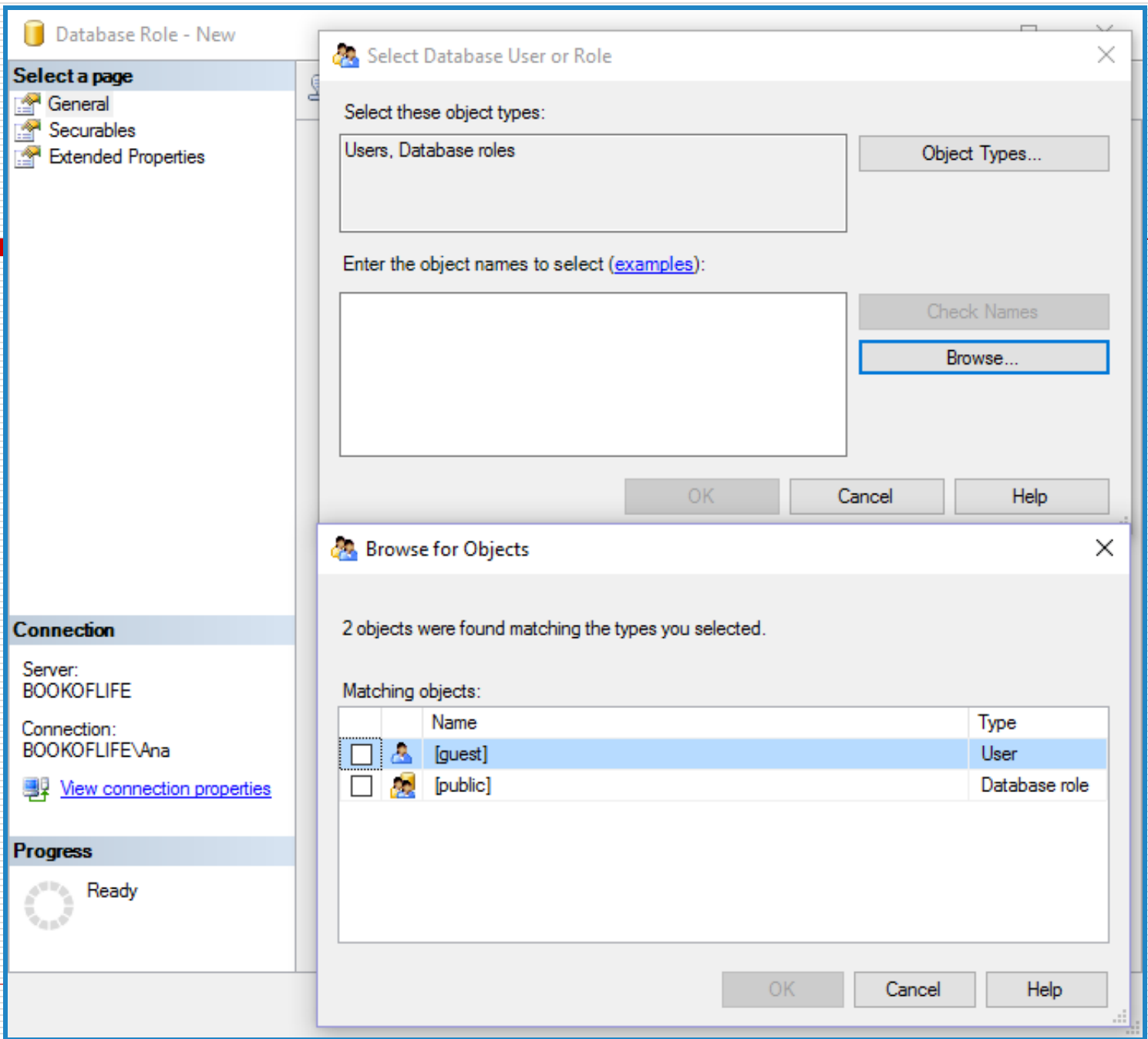
[View connection properties](#)

Progress

Ready

Slika 16: New Database Role

Objektna sigurnost: kreiranje uloge



Objektna sigurnost: kreiranje uloge

Application Role - New

Select a page

- General
- Securables
- Extended Properties

Script Help

Role name: NovaUlogaZaAplikaciju

Default schema:

Password: *****

Confirm password: *****

Schemas owned by this role:

	Owned Schemas
<input type="checkbox"/>	db_accessadmin
<input type="checkbox"/>	db_backupoperator
<input type="checkbox"/>	db_datareader
<input type="checkbox"/>	db_datawriter
<input type="checkbox"/>	db_ddladmin
<input type="checkbox"/>	db_denydatareader
<input type="checkbox"/>	db_denydatawriter
<input type="checkbox"/>	db_owner
<input type="checkbox"/>	db_securityadmin
<input type="checkbox"/>	dbo
<input type="checkbox"/>	guest
<input type="checkbox"/>	INFORMATION_SCHEMA
<input type="checkbox"/>	sys

Connection

Server: BOOKOFLIFE

Connection: BOOKOFLIFE\Ana

[View connection properties](#)

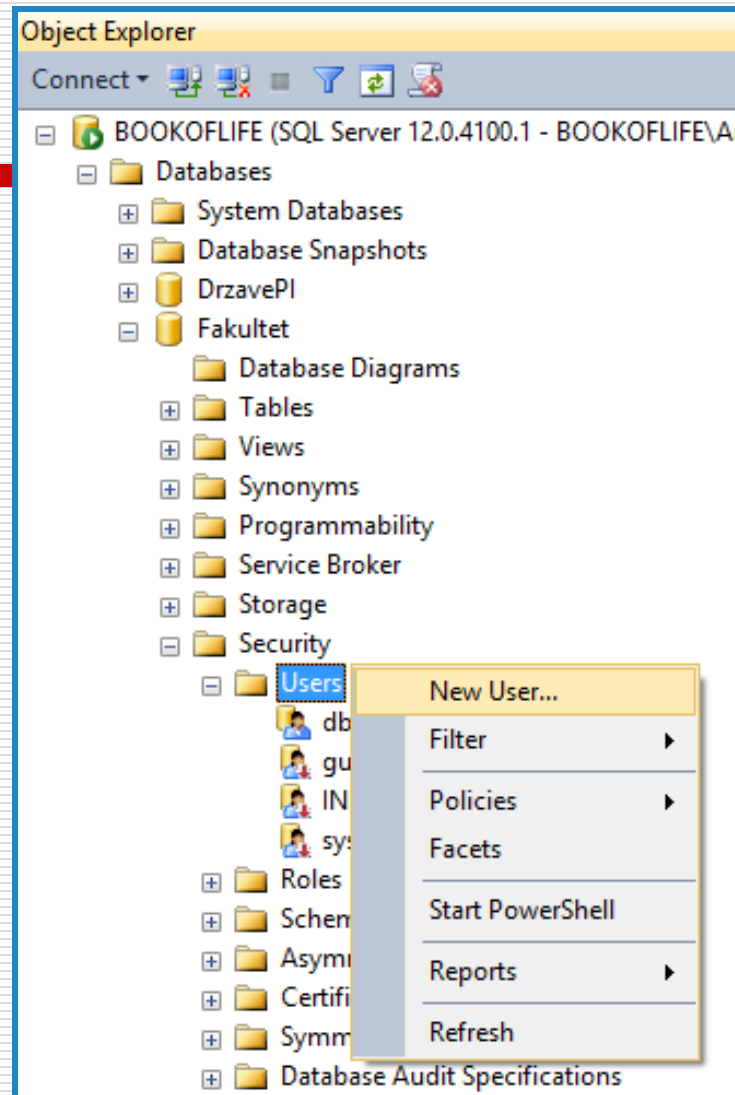
Progress

Ready

OK Cancel

Slika 18: New Application Role

Objektna sigurnost: kreiranje korisnika



Slika 19: New User

Objektna sigurnost: kreiranje korisnika

Database User - New

Select a page

- General
- Owned Schemas
- Membership
- Securables
- Extended Properties

Script Help

User type:
SQL user with login

User name:
NoviKorisnik

Login name:

Default schema:

Connection

Server:
BOOKOFLIFE

Connection:
BOOKOFLIFE\Ana

[View connection properties](#)

Progress

Ready

OK Cancel

Slika 20: New User

Objektna sigurnost: kreiranje korisnika

Database User - New

Select a page

- General
- Owned Schemas
- Membership
- Securables
- Extended Properties

Script Help

User type:

- SQL user with login
- SQL user with login
- SQL user without login
- User mapped to a certificate
- User mapped to an asymmetric key
- Windows user

Login name:

Default schema:

Connection

Server: BOOKOFLIFE

Connection: BOOKOFLIFE\Ana

[View connection properties](#)

Progress

Ready

OK Cancel

Slika 21: New User

Objektna sigurnost: kreiranje korisnika

Database User - New

Select a page

- General
- Owned Schemas
- Membership
- Securables
- Extended Properties

Script Help

User type:
SQL user with login

User name:
NoviKorisnik

Login name:

Default schema:

Connection

Server:
BOOKOFLIFE

Connection:
BOOKOFLIFE\Ana

[View connection properties](#)

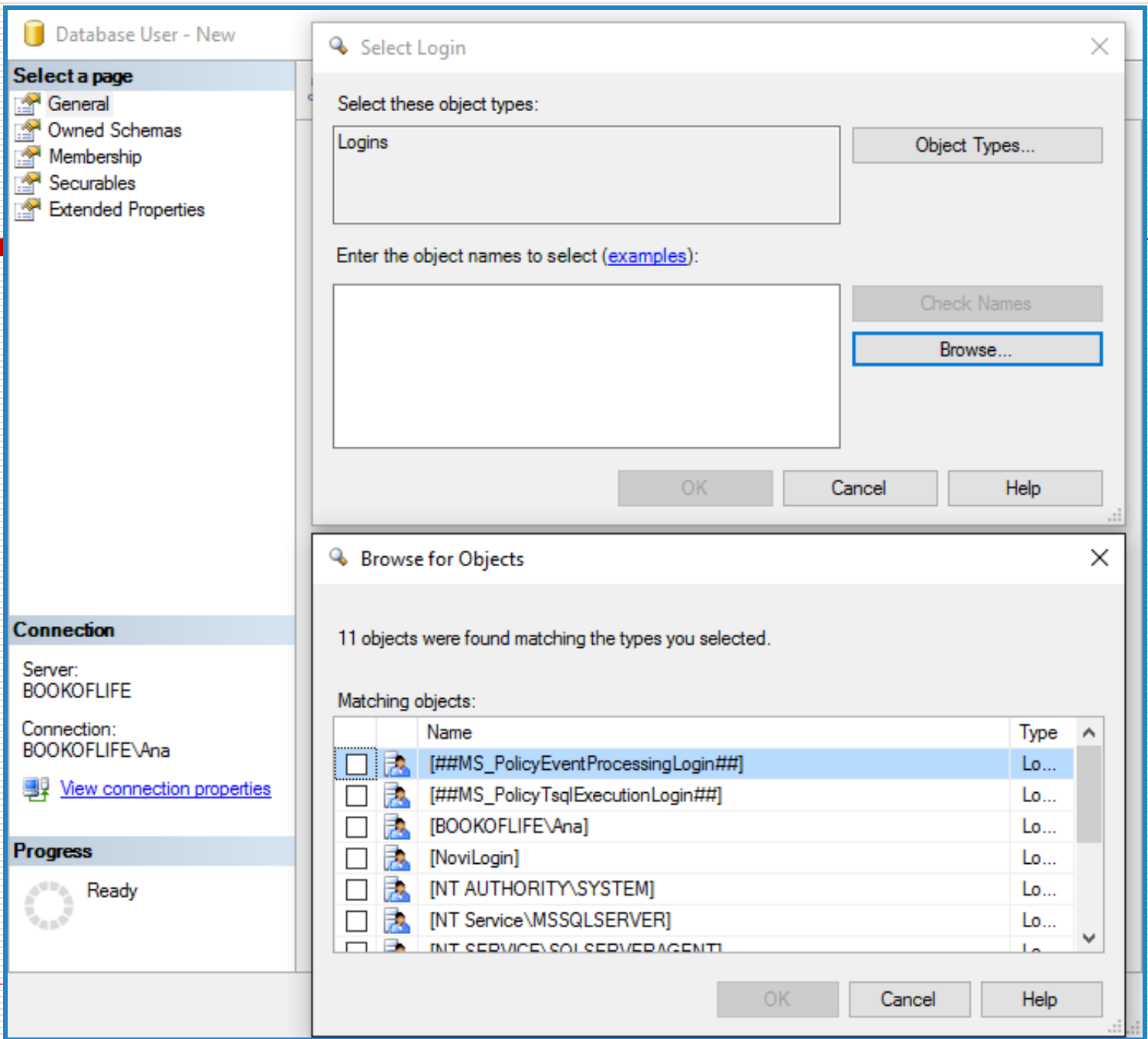
Progress

Ready

OK Cancel

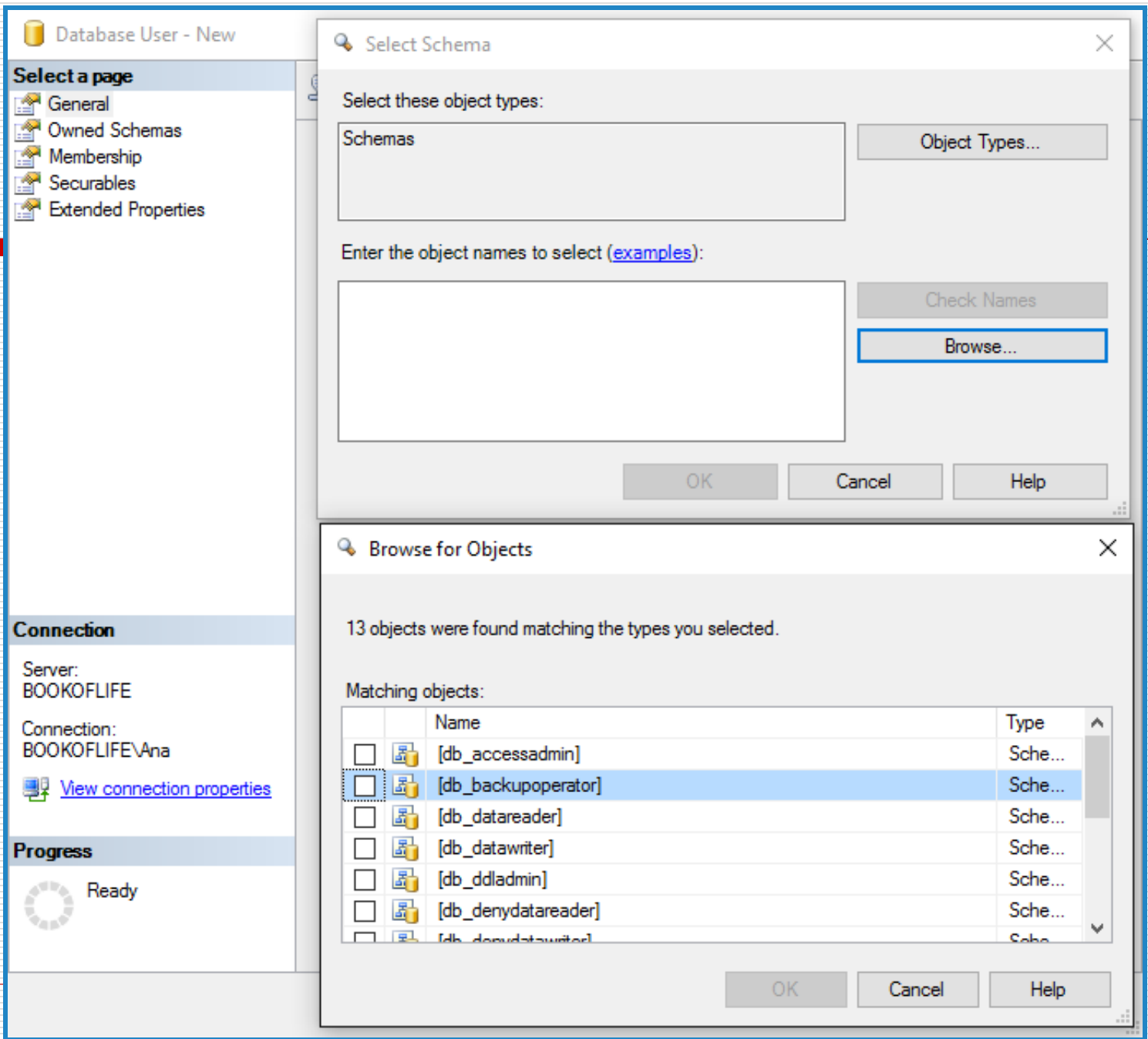
Slika 22: New User

Objektna sigurnost: kreiranje korisnika

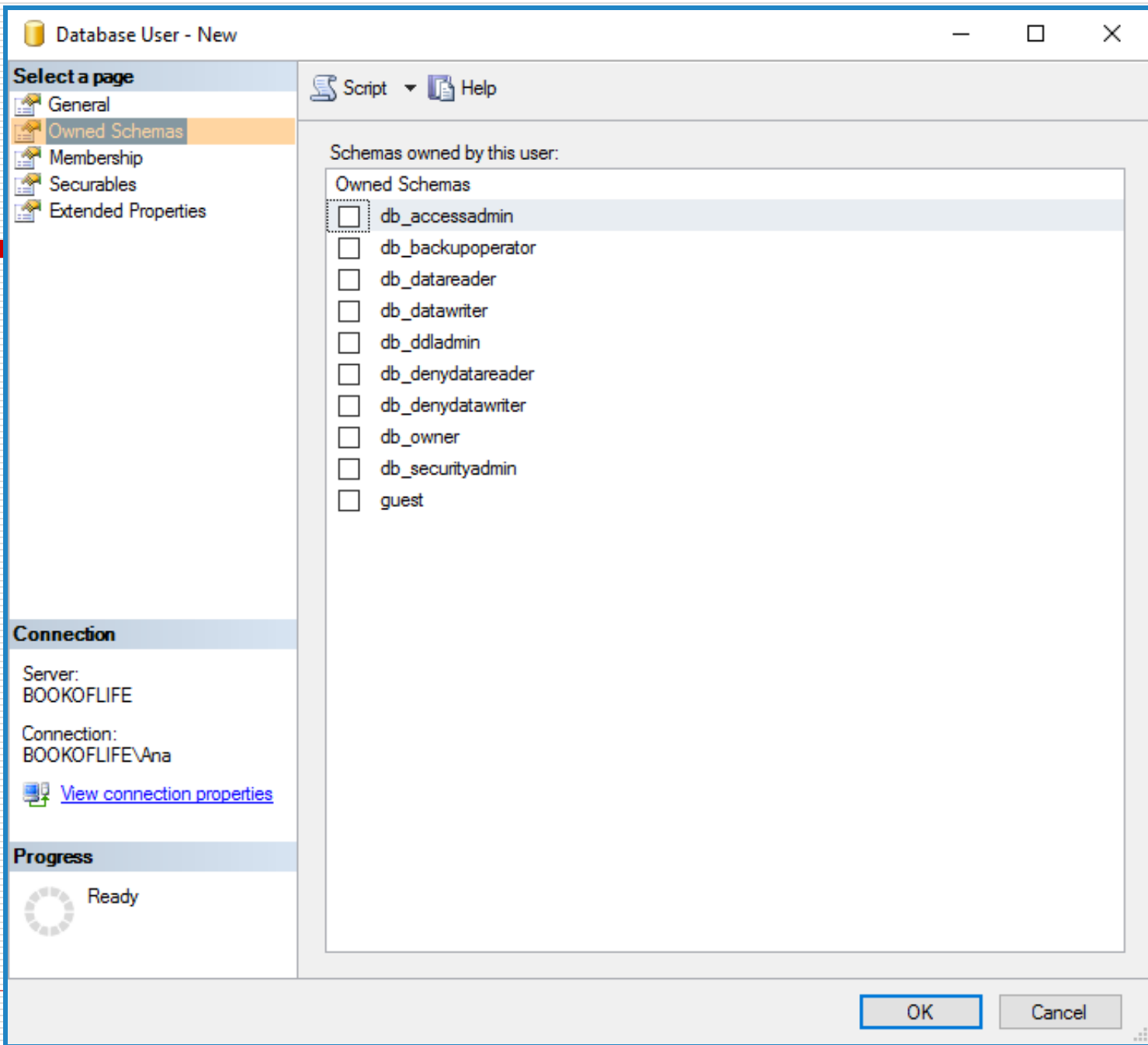


Slika 23: New User

Objektna sigurnost: kreiranje korisnika

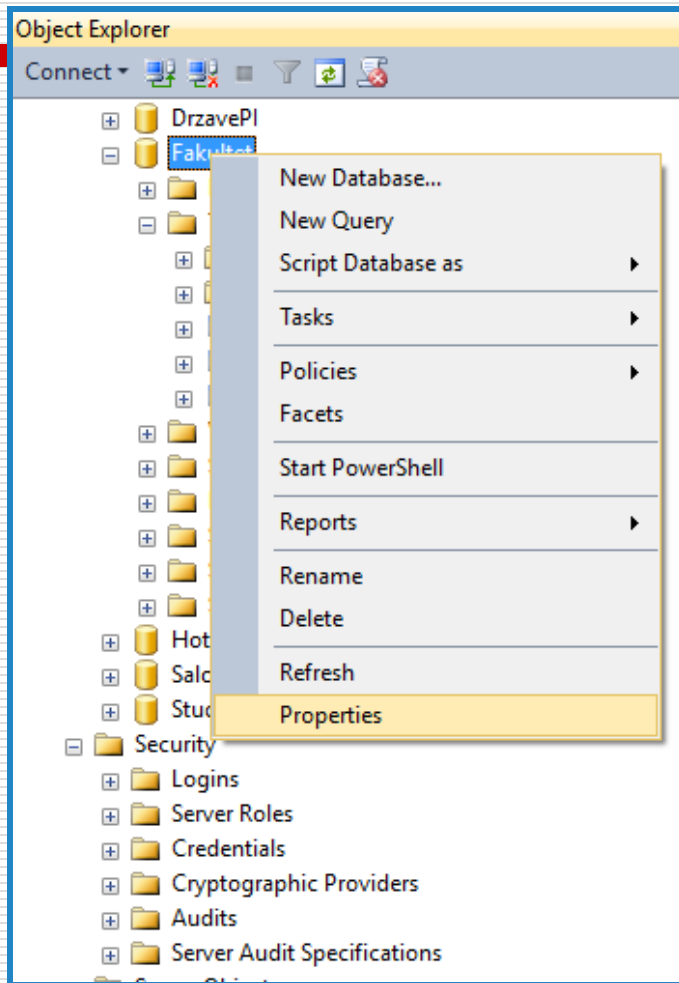


Objektna sigurnost: kreiranje korisnika

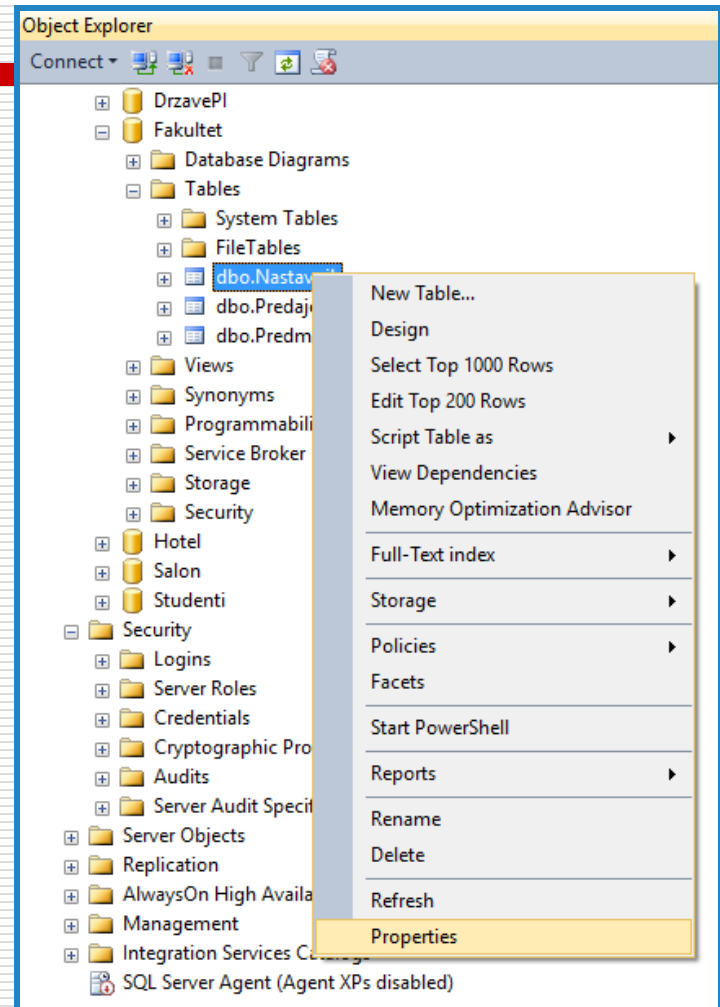


Slika 25: New User

Objektna sigurnost: dozvole nad bazom ili tabelom

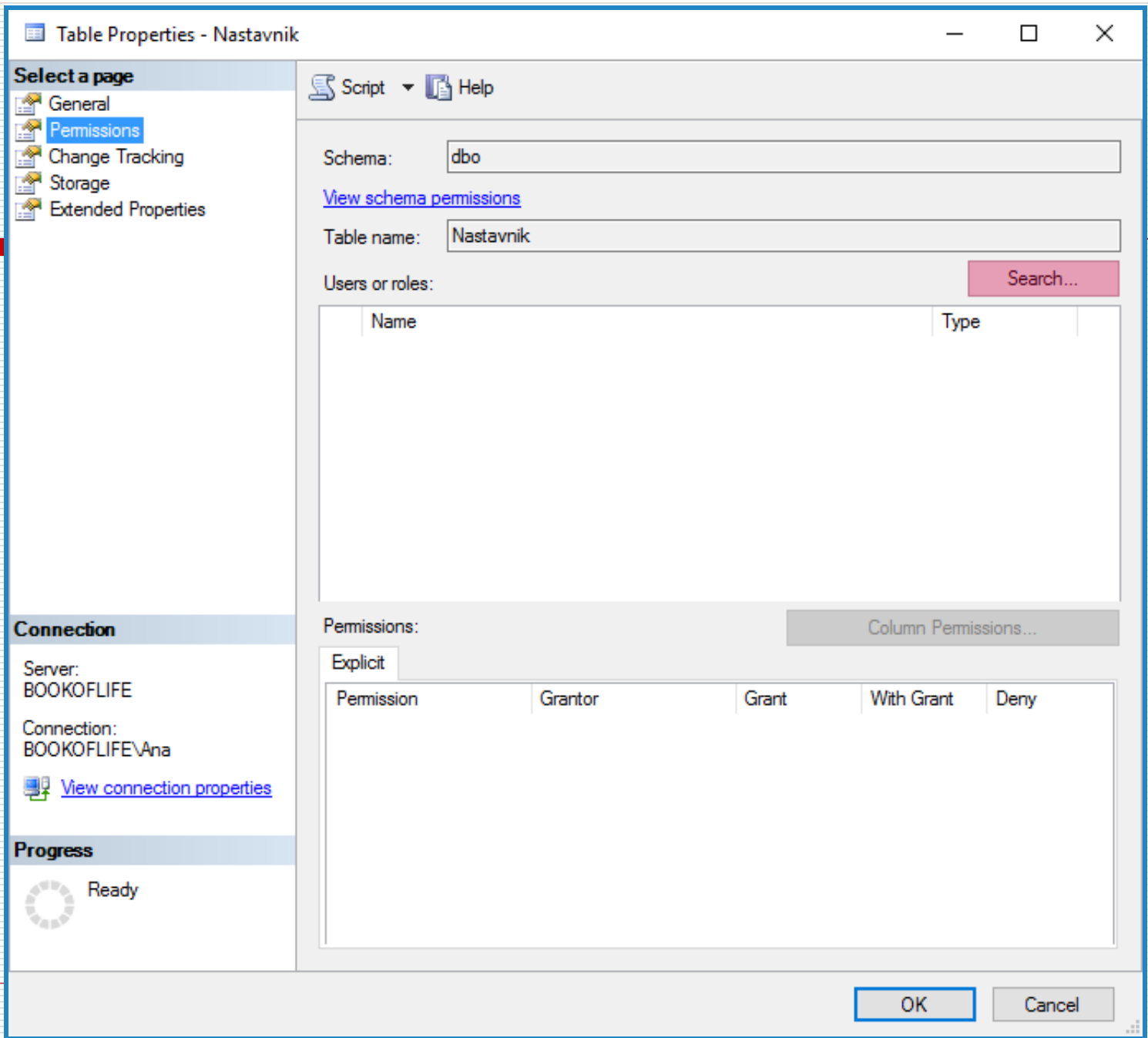


Slika 26: Permissions



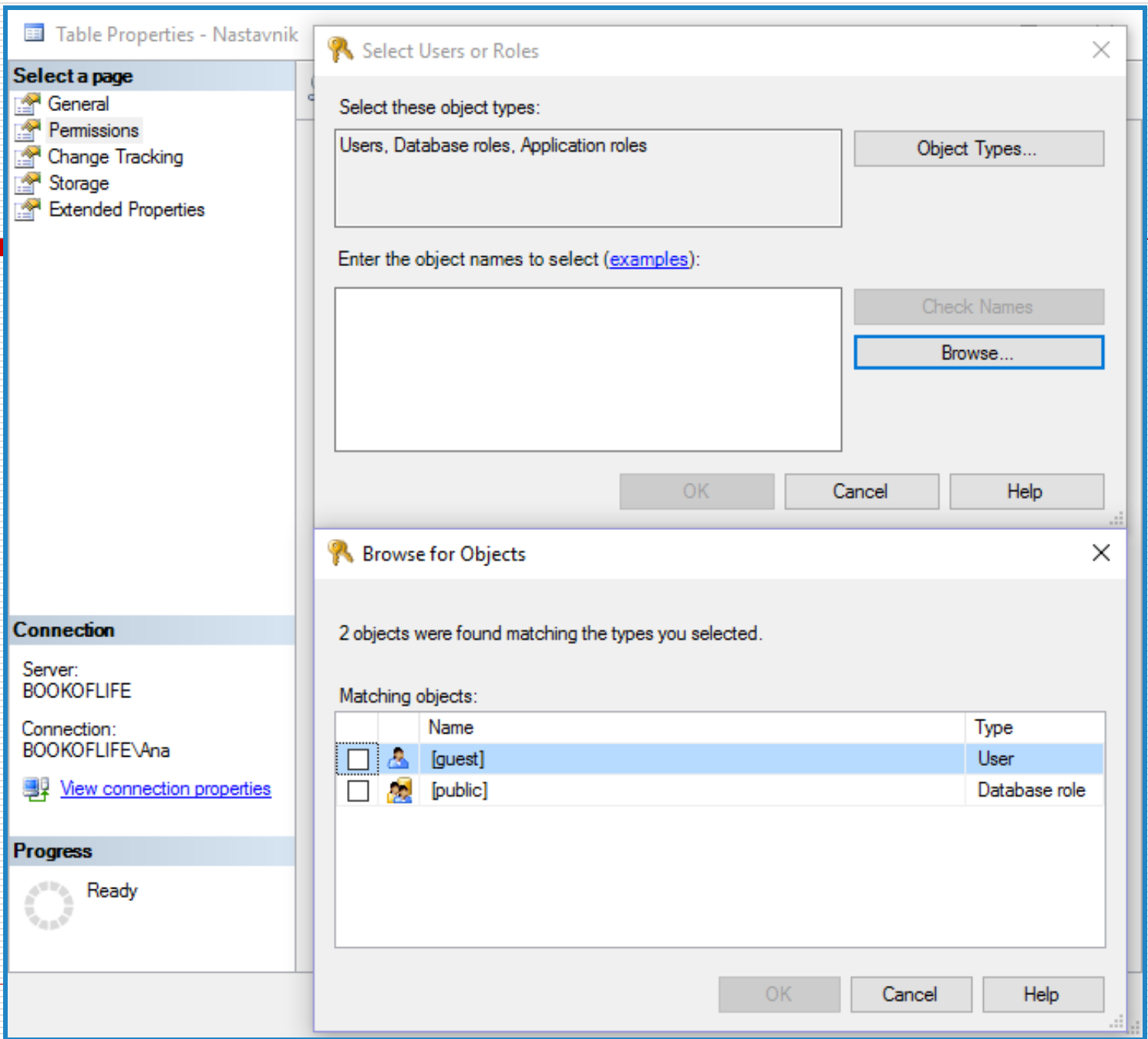
Slika 27: Permissions

Objektna sigurnost: dozvole nad bazom ili tabelom



Slika 28: Permissions

Objektna sigurnost: dozvole nad bazom ili tabelom



Objektna sigurnost: dozvole nad bazom ili tabelom

Table Properties - Nastavnik

Select a page

General

Permissions

Change Tracking

Storage

Extended Properties

Connection

Server: BOOKOFLIFE

Connection: BOOKOFLIFE\Ana

View connection properties

Progress

Ready

Script


Help

Schema:

[View schema permissions](#)

Table name:

Users or roles:

Name	Type
 guest	User

Permissions for guest:

Column Permissions...

Explicit

Effective

Permission	Grantor	Grant	With Grant	Deny
Alter		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Control		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Delete		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Insert		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
References		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Select		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Take ownership		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

OK

Cancel