Baze podataka II
Modul 10 – Jezik SQL

Administracija DBMS okruženja

Sigurnosni mehanizmi

Summary

- Sigurnosni koncepti
- Sigurnosni mehanizmi na nivou servera
- Sigurnosni mehanizmi na nivou baze podataka

Lekcija 1: Sigurnosni koncepti

- Sigurnost
- CIA
- Autentifikacija
- Autorizacija
- SQL::DCL

Sigurnost

- **Sigurnost je proces, a ne krajnje stanje.**
- **Informacijska sigurnost je disciplina fokusirana na konkretnu zaštitu podataka unutar samih informacijskih sistema**
  - DB Sigurnost – zaštita podataka od bilo kojeg autorizovanog i neautorizovanog pristupa
- **Nivo baze podataka**
- **Nivo operativnog sistema**
- **Mrežni sloj**
- **Fizički nivo**
- **Čovjek je najslabija karika u lancu sigurnosti.**

CIA

- **Confidentiality: prevencija neautorizovanog čitanja informacija:**
  - Kriptografija;
- **Integrity: detekcija neautorizovanog pisanja informacija**
  - Kriptografija
- **Availability: Podaci trebaju biti dostupni kada su potrebni**
  - Jedan od novih sigurnosnih elemenata
  - Disaster recovery procedure
  - BackUp/Restore
  - ...

Autentifikacija

- **Provjera identiteta korisnika**
  - Ko si ti?
  - Da li si to **zaista** ti?
- **Lozinke su trenutno jedan od najraširenijih oblika autentifkacije, ali su podložne mrežnom „prisluškivanju“ i re-emitovanju**
- **Challenge-response (izazov-odgovor)**
  - Korisnik dobiva „izazov“
  - Izazov se enkriptuje (ili hash-uje) skupa sa lozinkom i šalje nazad.
  - Druga strana verifikuje odgovor
- **Digitalni potpisi se koriste kako bi se verifikovala autentičnost strana u komunikaciji**

Autorizacija

- **Proces provjere šta korisnik smije da radi u sistemu**
- **Oblici autorizacije na nivou podataka:**
  - **Read** authorization – samo čitanje podataka
  - **Insert** authorization – samo dodavanje bez izmjena.
  - **Update** authorization – dozvola izmjena, ali ne i brisanja.
  - **Delete** authorization – dozvola za brisanje podataka
- **Oblici autorizacije na nivou šeme baze podataka**
  - **Create** authorization
  - **Alter** authorization
  - **Drop** authorization

SQL::DCL

- **Definisanje prva pristupa objektima baze podataka i podacima (autorizacija);**
  - GRANT
  - DENY
  - REVOKE

Lekcija 2: Sigurnosni mehanizmi na nivou servera

- Šta su *principals*?
- Šta su *securables*?
- Šta su permisije ?
- Tipovi autentifikacije;
- Password policy;
- SQL Server Logins;
- Primjeri;
- Fiksne serverske uloge;

Šta su principals?

Principals

Windows

Windows Group
Domain User Account
Local User Account

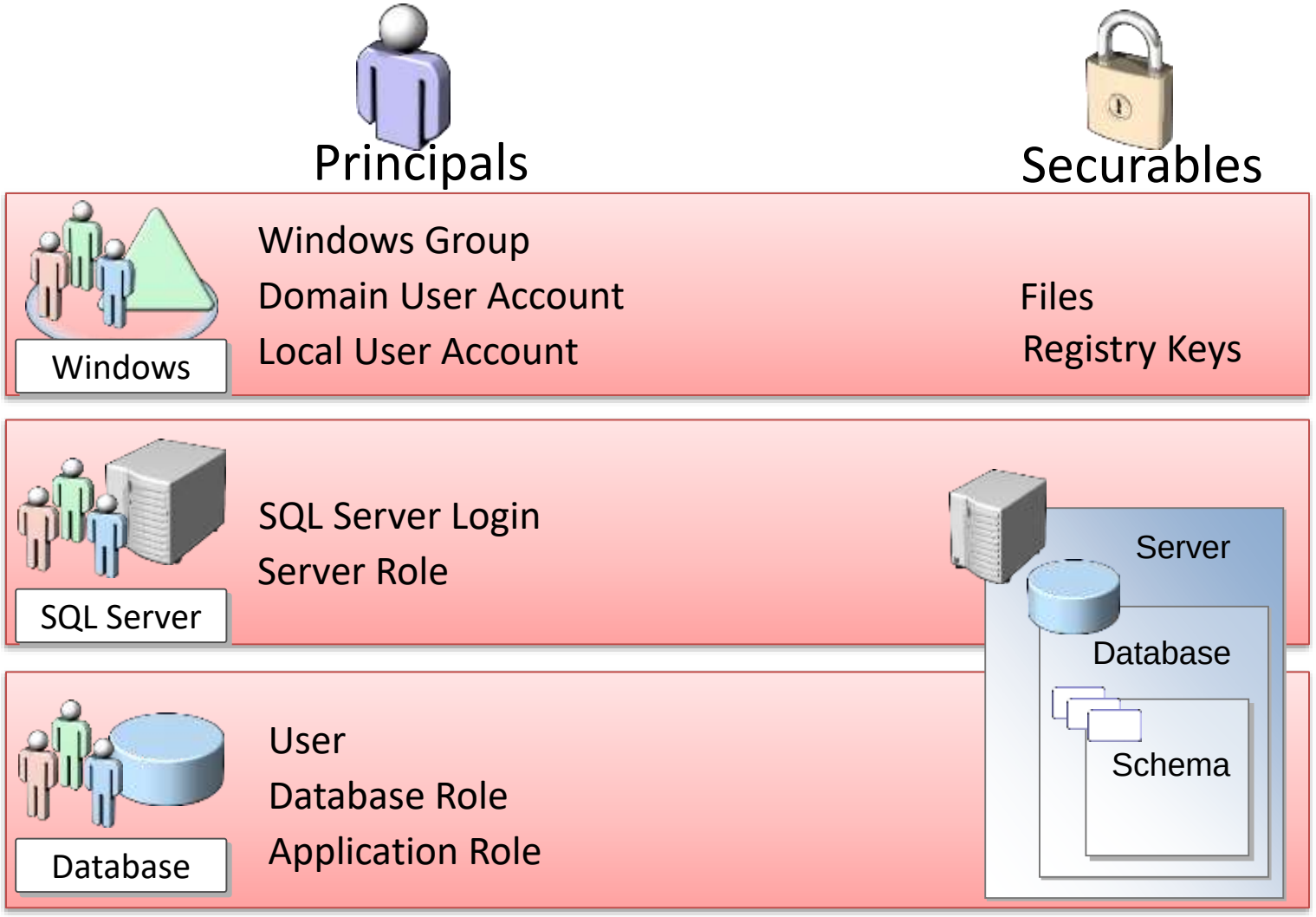
SQL Server

SQL Server Login
Server Role

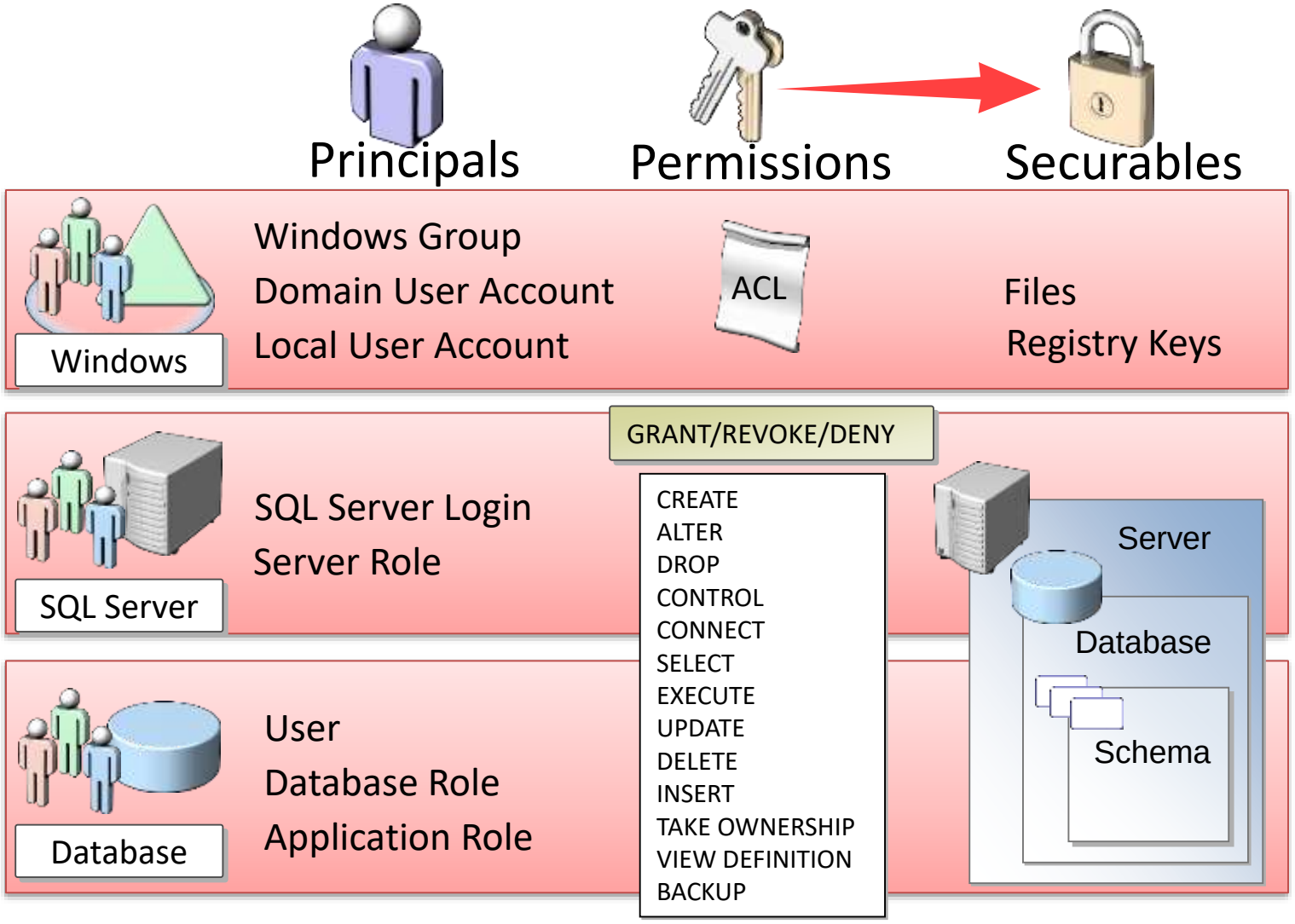
Database

User
Database Role
Application Role

Šta su securables?

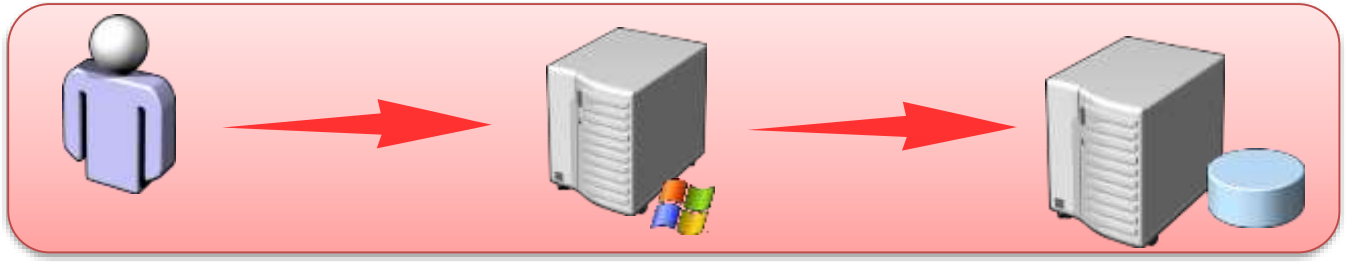


Šta su permisije?

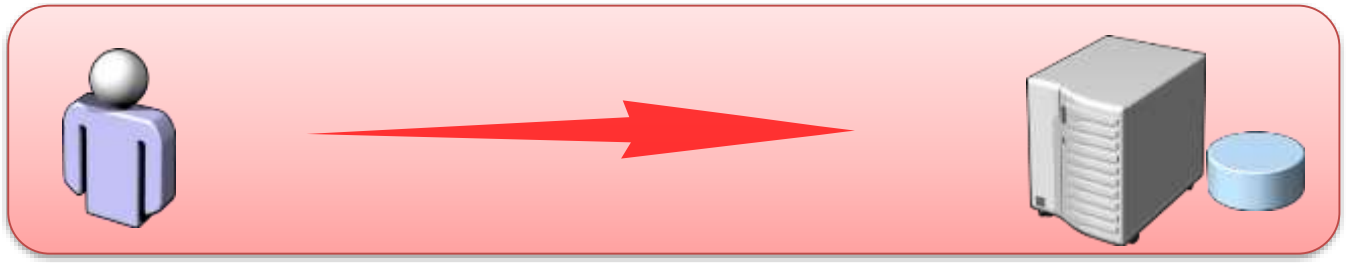


Tipovi autentifikacije

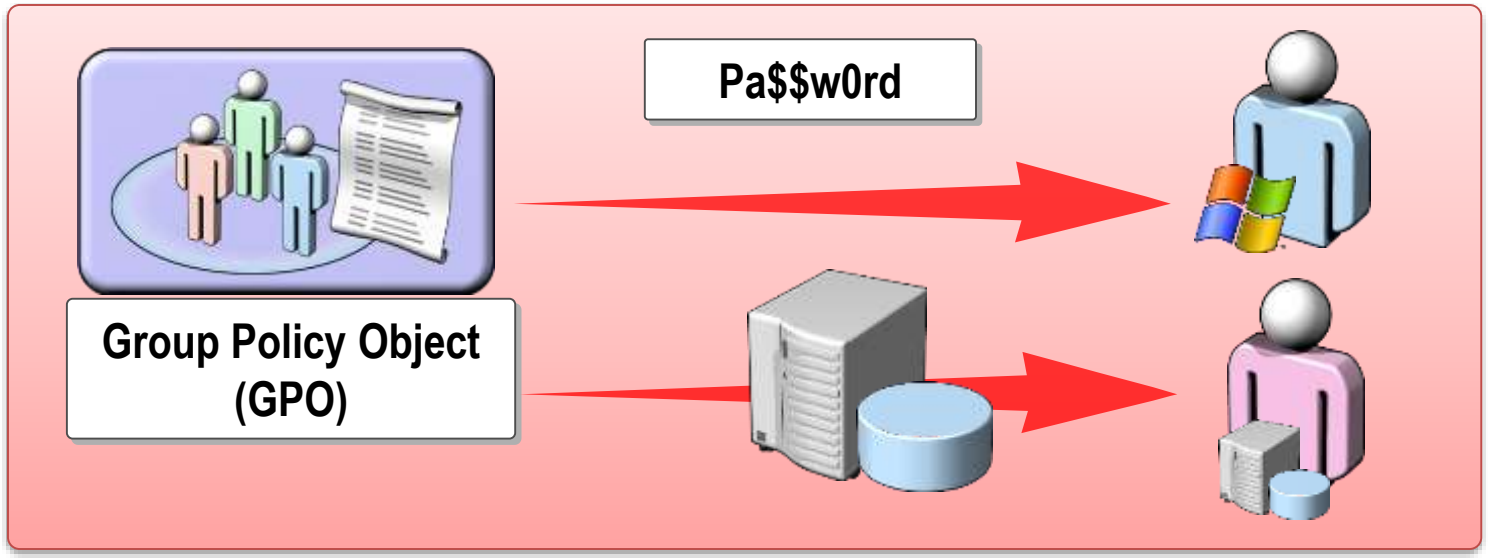
- **Windows autentifikacija – *trusted***
  - Korisnik je autentificiran od strane Windows OS-a
  - Korisnici pristupaju putem logina koji su mapirani na njihove Windows naloge



- **SQL Server autentifikacija - *nontrusted***
  - Korisnike se autentifikuje od strane SQL Server okruženja



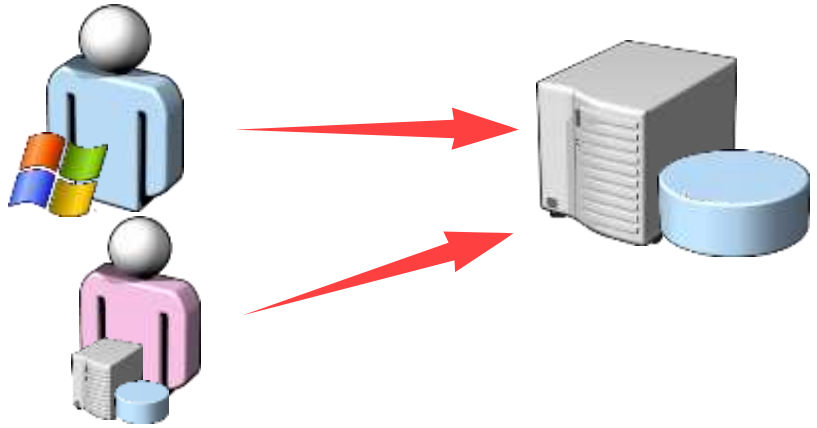
Password policy

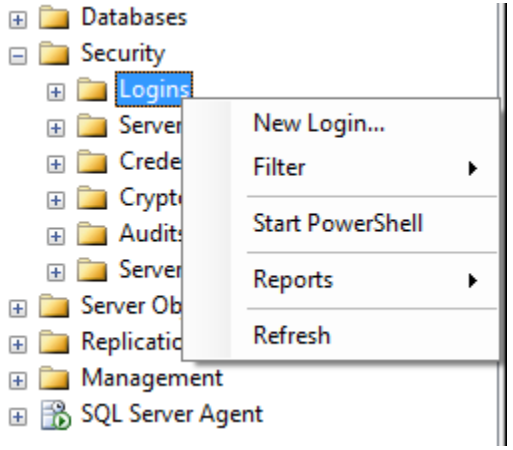


- GPO se koristi na nivou OS i/ili domene
- SQL Server također posjeduje password policy za SQL Server autentifikaciju

SQL Server Logins

- **Preko SSMS**
  - Security→Logins →New Login
    - Odabrati Windows ili SQL Server login
- **SQL kod**
  - CREATE LOGIN






```
CREATE LOGIN login_name
{ WITH SQL_login_options
| FROM WINDOWS [ WITH windows_login_options ] }
```

Primjeri

```
/* Windows lokalni ili domenski nalog*/
CREATE LOGIN [SERVER\Jasmin]
FROM WINDOWS
WITH DEFAULT_DATABASE = AdventureWorks2014
```

```
/* SQL Server login*/
CREATE LOGIN Selver
WITH PASSWORD = 'Pa$$w0rd',
DEFAULT_DATABASE = pubs
```

```
--Izmjena
ALTER LOGIN Sara WITH PASSWORD = 'NewPa$$w0rd'
--Brisanje
DROP LOGIN [SERVER\Jasmin]
```

```
CREATE LOGIN Imran
WITH PASSWORD = 'password',
DEFAULT_DATABASE =
AdventureWorks2014,
CHECK_EXPIRATION = OFF,
CHECK_POLICY = OFF
```

Fiksne serverske uloge

Role	Description	Server-level Permission
sysadmin	Perform any activity	CONTROL SERVER (with GRANT option)
dbcreator	Create and alter databases	ALTER ANY DATABASE
diskadmin	Manage disk files	ALTER RESOURCES
serveradmin	Configure server-wide settings	ALTER ANY ENDPOINT, ALTER RESOURCES, ALTER SERVER STATE, ALTER SETTINGS, SHUTDOWN, VIEW SERVER STATE
securityadmin	Manage and audit server logins	ALTER ANY LOGIN
processadmin	Manage SQL Server processes	ALTER ANY CONNECTION ALTER SERVER STATE
bulkadmin	Run the BULK INSERT statement	ADMINISTER BULK OPERATIONS
setupadmin	Configure replication and linked servers	ALTER ANY LINKED SERVER

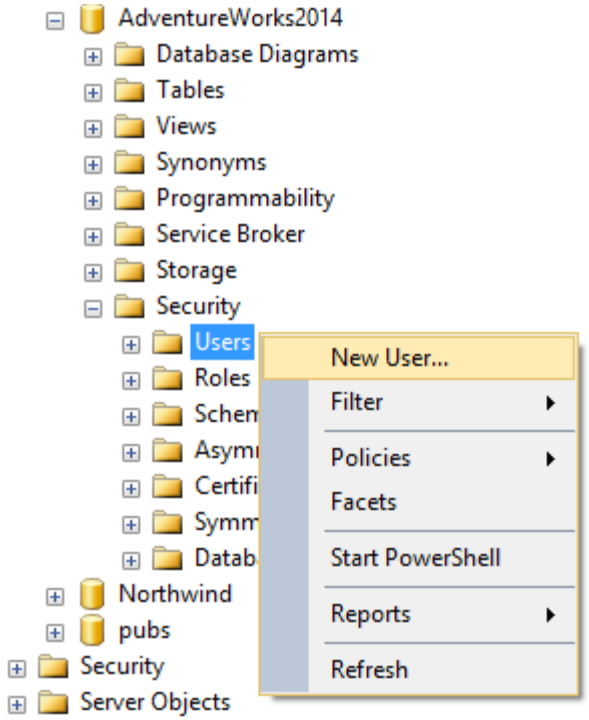
Lekcija 3: Sigurnosni mehanizmi na nivou baze podataka

- Upravljanje korisnicima;
- Primjeri;
- Specijalni tipovi korisnika;
- Fiksne database uloge;
- Šta su šeme?
- Primjena šema i prednosti;
- Primjeri upotrebe šema;

Upravljanje korisnicima

- **Preko SSMS**
  - Database→Security→Users →New User
- **SQL kod**
  - CREATE USER

```
CREATE USER user_name
    [
        { FOR | FROM } LOGIN login_name
    ]
    [ WITH <limited_options_list> [ ,... ] ]
[ ; ]
```



Primjeri

```
-- Kreiranje korisnika za login sa istim imenom

CREATE USER Jasmin
```

```
/* Kreiranje korisnika sa drugim imenom u odnosu na
mapirani login */

CREATE USER Student_1458 FOR LOGIN [FIT\1458]
```

```
-- Kreiranje korisnika sa default shemom

CREATE USER Denis FOR LOGIN [FIT\Denis]
WITH DEFAULT_SCHEMA = profesori
```

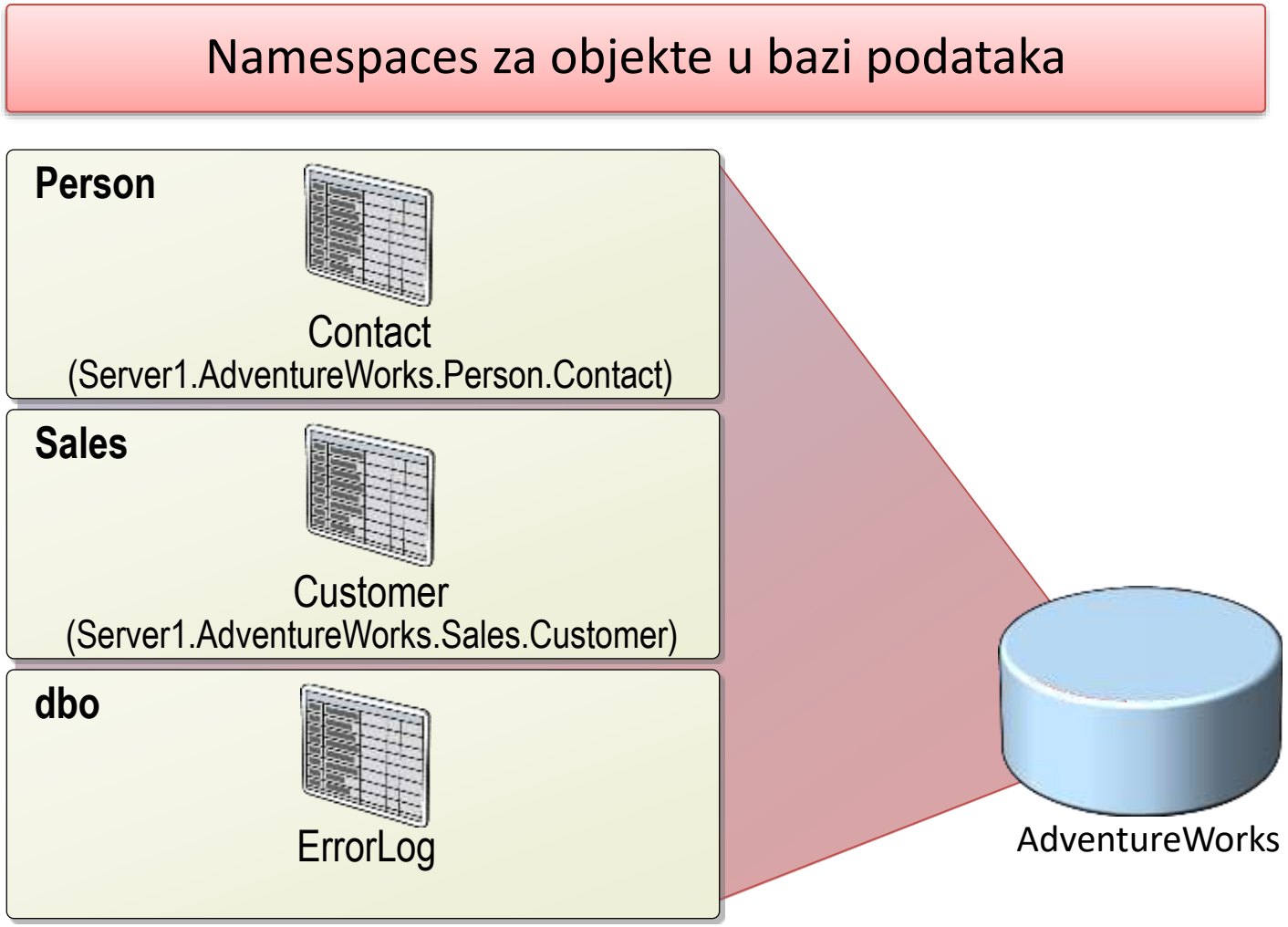
Specijalni tipovi korisnika

- **dbo user**
  - Postoji u svakoj bazi podataka;
  - Članovi **sysadmin** uloge i **sa** logina, mapiranu su na **dbo** korisnika;
  - Svaki objekta kreiran od strane **sysadmin** članova pripada **dbo** korisniku
  - Brisanje nije moguće;
- **guest user**
  - Postoji u svakoj bazi podataka
  - Disabled (default)
  - Omogučava da logini koji nemaju korisnički nalog u bazi imaju “pristup”;

Fiksne database uloge

Role	Description
db_owner	Perform any configuration and maintenance activities on the DB and can drop it
db_securityadmin	Modify role membership and manage permissions
db_accessadmin	Add or remove access to the DB for logins
db_backupoperator	Back up the DB
db_ddladmin	Run any DDL command in the DB
db_datawriter	Add, delete, or change data in all user tables
db_datareader	Read all data from all user tables
db_denydatawriter	Cannot add, delete, or change data in user tables
db_denydatareader	Cannot read any data in user tables

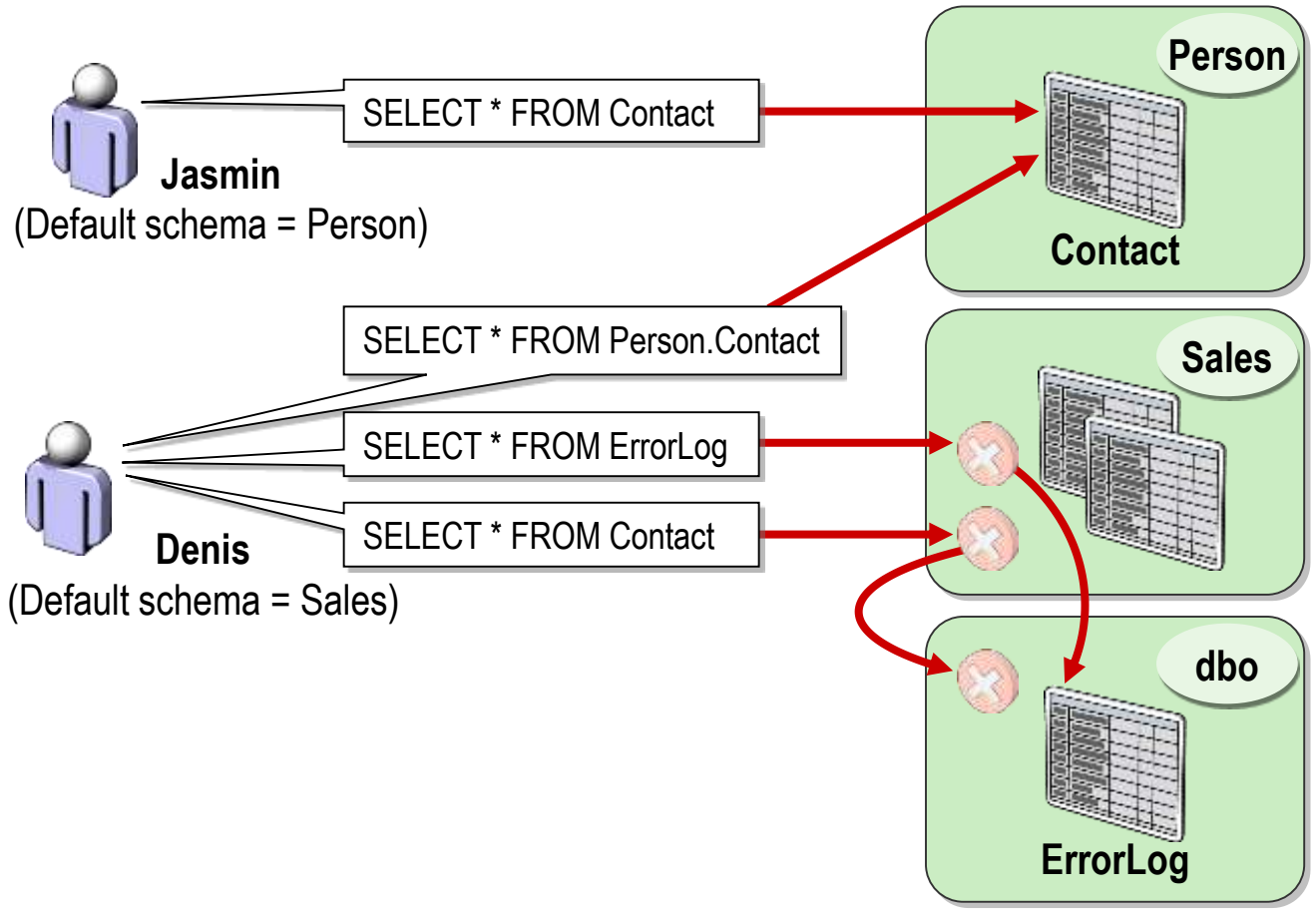
Šta su šeme?



Primjena i prednosti

- **Puno ime objekta je u formatu:**
  - `server.database.schema.object`
  - unutar baze može i `schema.object`
- **Primjer baze AdwentureWorks**
  - `HumanResources, Person, Production, Purchasing, Sales`
- **Svaka baza podataka ima default shemu (dbo)**
  - Ako se prilikom kreiranja objekta ne specificira drugačije, objekat nasljeđuje dbo šemu
- **Veća organizovanost objekata baze i nezavisnost od korisnika;**
- **Jednostavnije dijeljenje permisija;**
- **Lakše upravljanje sa objektima**

Primjeri upotrebe šema



Pitanja