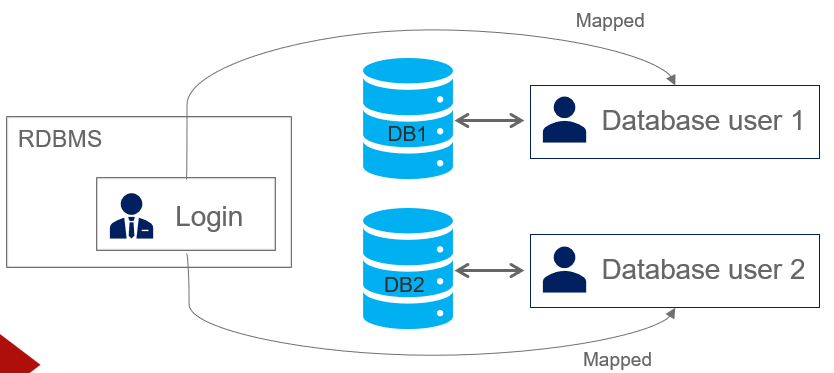
**Deel 4 - Security**

**Logins**

* Twee belangrijke concepten in security
  + Authenticatie => Wie ben je?
  + Autorisatie => Wat mag/kan je doen?



* SQL Server werkt op 2 niveaus voor authenticatie
  + Niveau van de database server Login
  + Niveau van de database Database user
* SQL Server voorziet 2 soorten logins
  + Windows login
  + SQL login
* Keuze uit 2 authentication modes in SQL Server
  + Windows Authentication mode alleen Windows logins
  + Mixed mode Windows logins en SQL logins

**Windows login**

* Bestaande accounts bewaard in Windows
* Windows zal verantwoordelijk zijn om de authenticiteit van de login te valideren

**SQL Login**

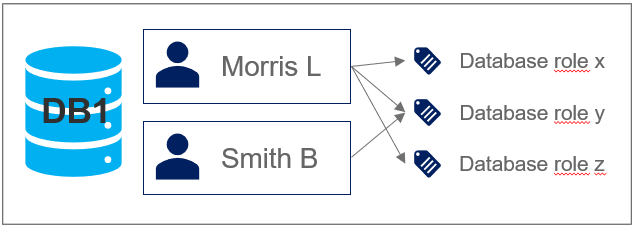
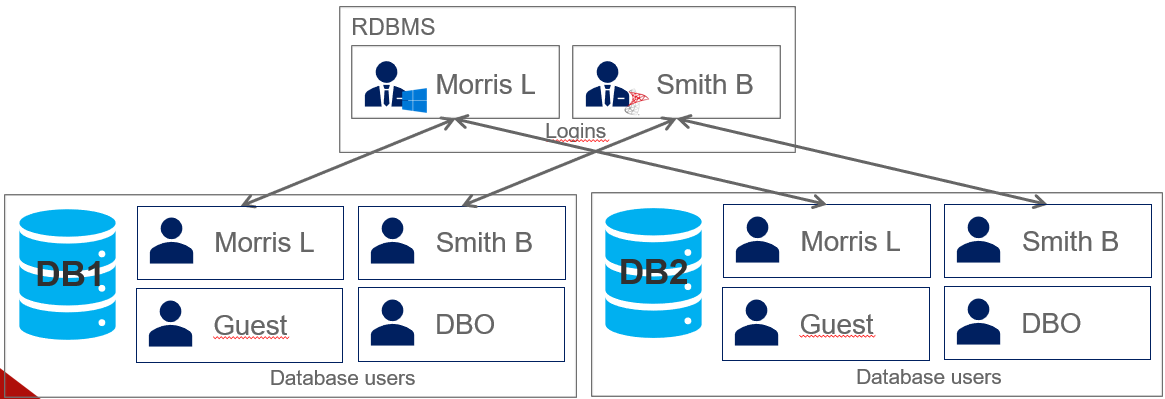
* Accounts bestaan niet in windows

**Server rollen**

* Een rol is een set van vooraf gedefinieerde permissies
* Server rol bepaalt wat je mag op niveau van de SQL Server instance
* Login kan een of meerdere rollen toegewezen krijgen
* Login erft de permissies van de toegewezen rol(len)
* Een server rol kan fixed of user-defined zijn
  + **Fixed** => Bijhorende permissies kunnen niet gewijzigd worden
  + **User-defined** => Bijhorende permissies kunnen wel geconfigureerd worden
* **Dbcreator** => Kan eender welke database creëren, droppen, wijzigen en terugzetten
* **Public** => De “Public” rol kan elke database zien (lezen)
* **Securityadmin** => Kan logins en permissies beheren
* **Sysadmin** => Kan eender welke taak uitvoeren in SQL Server

**Database users**

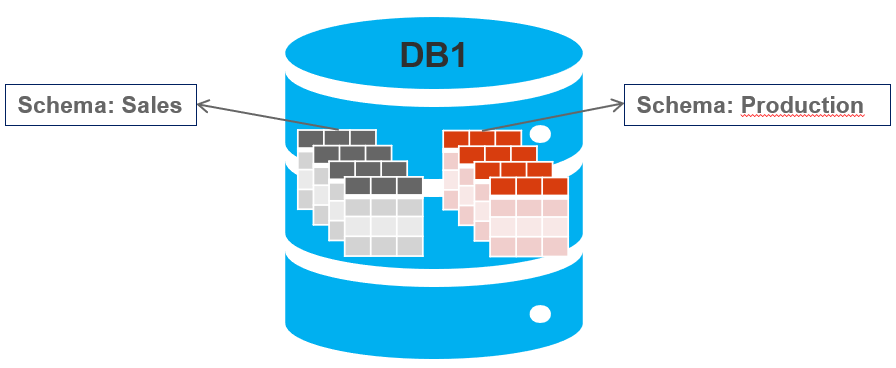
* Worden gedefinieerd binnen een database en bestaan enkel daar
* Worden gebruikt om toegang tot database objecten in te stellen
* Database user is geassocieerd (gemapped) met een login
* Aan 1 login kan voor elke database 1 database user gekoppeld worden
* Authenticatie
  + Is niet van toepassing voor een database user
  + Gebeurt overkoepelend via de Login die geassocieerd wordt met de database user
* By default 2 database users in een database
  + Guest
  + DBO (DataBase Owner)



**Database rollen**

* Bepaalt wat je mag op niveau van de database
* Database user kan een of meerdere rollen toegewezen krijgen
* Een database rol is “Fixed” of “User-defined”
* db\_accessadmin (toevoegen/verwijderen toegang voor Logins)
* db\_backupoperator (Het recht om een database te back-uppen)
* db\_datareader (alle user tabellen lezen)
* db\_denydatareader
* db\_datawriter (schrijven naar alle user tabellen)
* db\_denydatawriter
* …
* Ook op dit niveau is er een onderscheid tussen fixed en user-defined database rollen
* **Fixed database rollen** 
  + Zijn minder flexibel om in te stellen wat iemand (niet) mag
* **User-defined database rollen** 
  + Bieden grotere controle over het beheren van permissies en toegang tot resources in de database

**Database schema**

* Container die een aantal database objecten bevat
* Schema heeft een naam (bv. Production)
* Schema heeft slechts één eigenaar (Database user of database Role)
* Elk database object (beveiligbaar) behoort tot één Schema
* Een gebruiker kan gedefinieerd worden met een default Schema
* De eigenaar van het Schema heeft alle permissies voor de objecten die dit schema bevat
* De volledige naam van een object is = schemaname.objectname  
  Bv. Production.persons

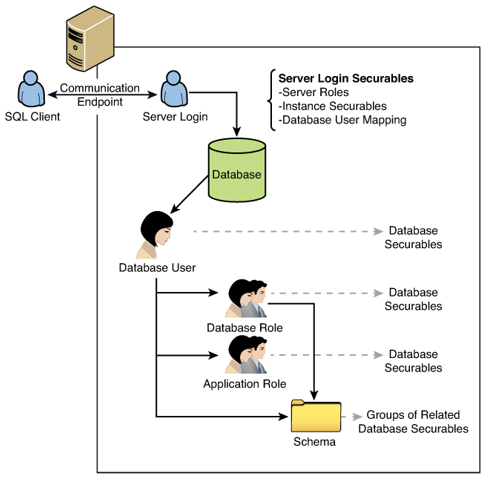
**Expliciet instellen permissies**

**DENY:** Het verbieden van een bepaalde permissie. Hierdoor wordt expliciet aangegeven dat een bepaalde permissie niet toegekend wordt aan een principal.  
Als de permissie impliciet zou worden toegekend zal Deny ervoor zorgen dat dit alsnog overruled wordt.

**GRANT:** Wil zeggen dat je de permissie die je zelf hebt ook kan doorgeven aan anderen.

**REVOKE:** Het intrekken van een reeds toegekende permissie.

**Schematisch overzicht**



**Geef de login/user gepaste permissies om:**

**=>** Zijn/haar werk te kunnen doen