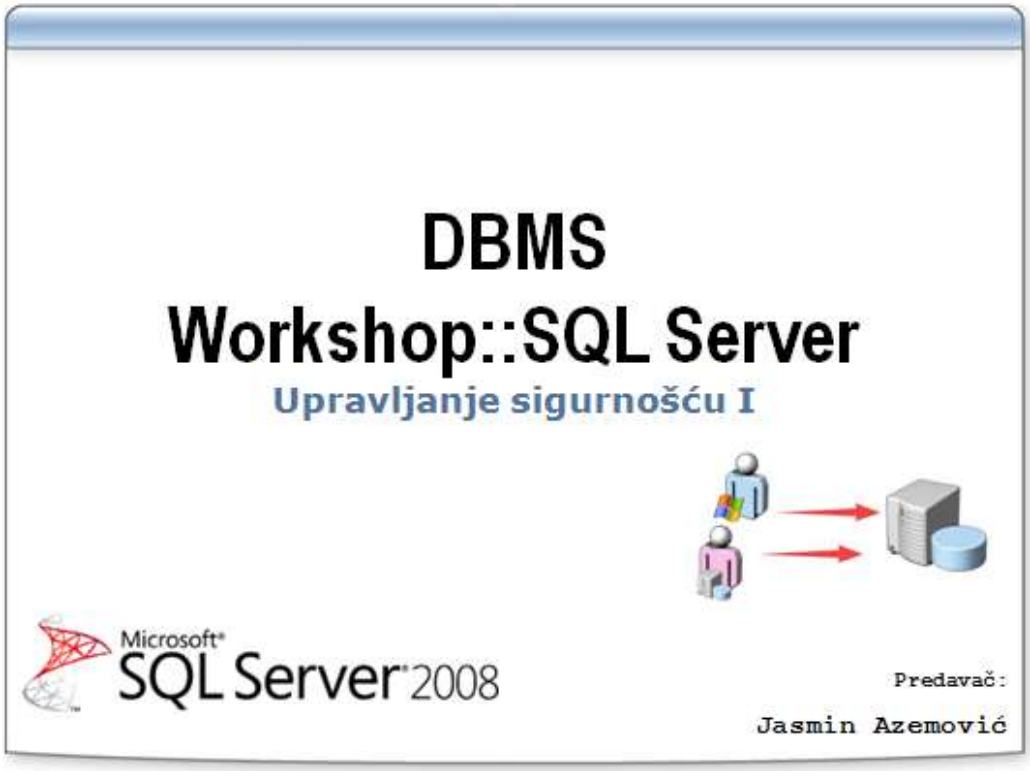
Datum:13.04.2010

Upravljanje sigurnošću

I dio



Današnja lekcija obrađuje izuzetno važan segment baza podataka, a to je sigurnost. Sigurnost se generalno proteže kroz sve faze razvoja i slojeve informacionih sistema. Međutim, baza podataka i server baza podataka su zadnje linija odbrane. U slučaju kada napadač prođe sve barijere, između njega i podataka stoji vrlo jaka prepreka. Barijera se sastoji iz dvije pod linije odbrane i to:

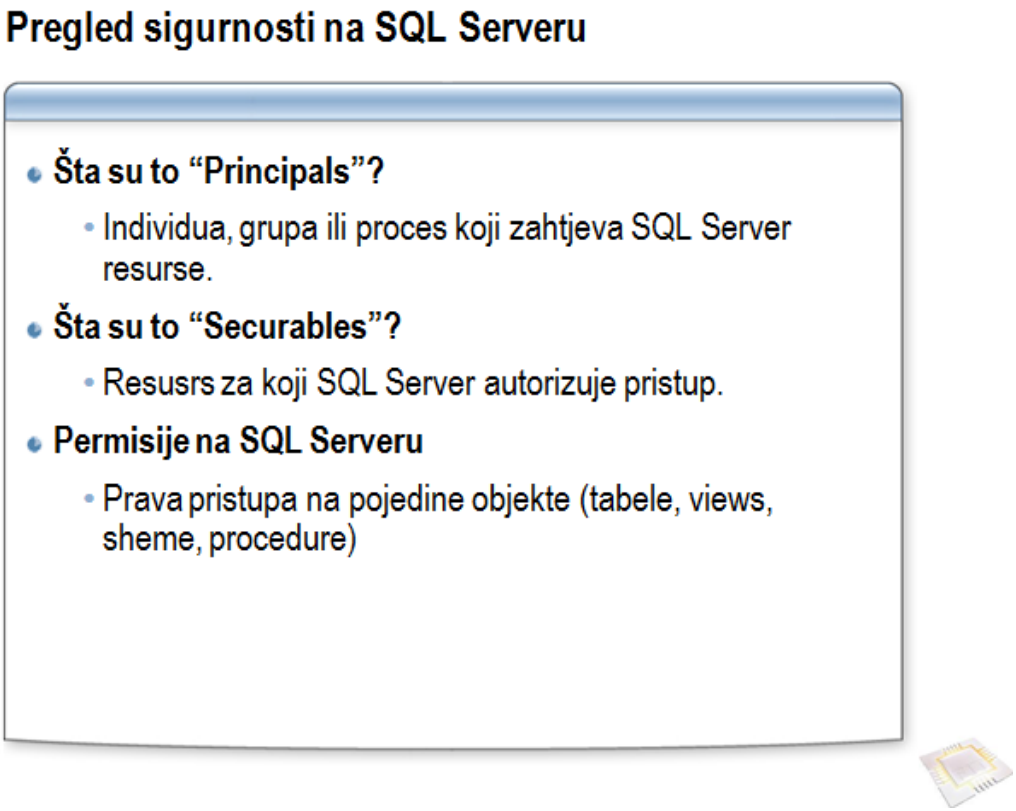
- Sigurnost sa aspekta servera
- Sigurnost sa aspekta baze podataka

Samim time smo ovu lekciju podjeli na dva dijela jer se u radi o odvojenim aspektima sigurnosti, ali istovremeno i povezanim jer funkcionišu u konjukciji

Ali krenimo redom, današnja lekcija se fokusara na sljedeća dva elementa:

- Pregled sigurnosti na SQL Serveru;
- Sigurnosni elemetni na nivou servera

Pregled sigurnosnih elemenata



Kompletan koncepit sigurnost se vrti oko tri elementa:

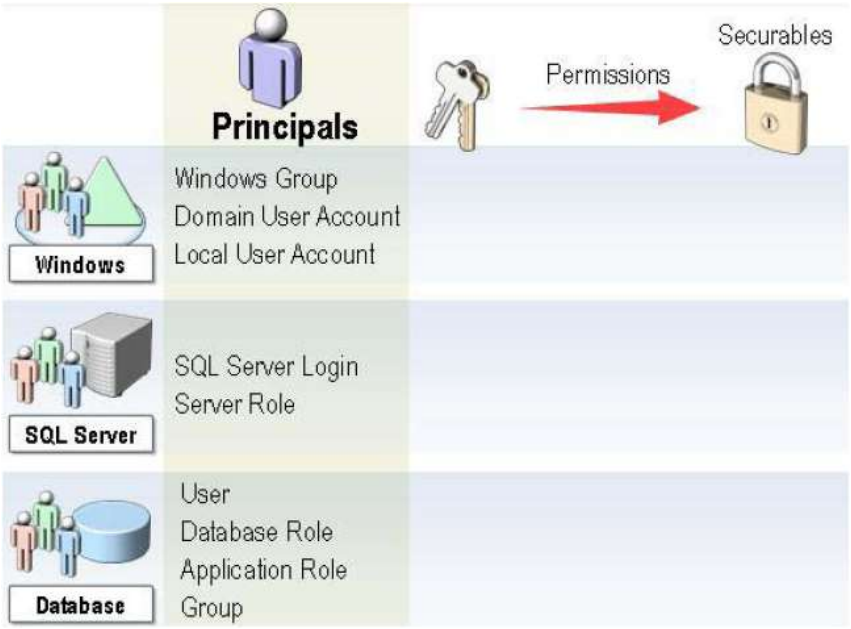
- Principals;
- Securables;
- Permisije;

Principals

Pricnipals su entiteti (individue, grupe, procesi i/ili aplikacije) koji zahtjevaju određene resurse na SQL Serveru. Logično je zaključiti da je model autorizacije pricipala zasnovan hijerarhijski (kao i čitav koncept sigurnosti u IT-u). Opseg uticaja *principala* zavisi od definisanih prava pristupa, bez obzira o kome se radi:

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

Svaki principal, bez obzira sa kojeg od navedenih nivoa dolazi, ima svoj identifikator (SID) - secure ID.

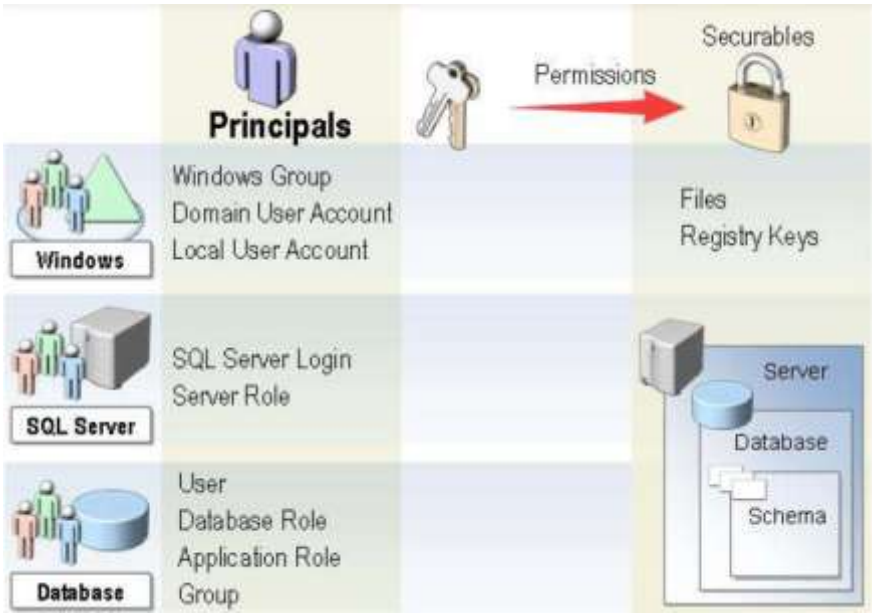


Slika 1. *Hijerarhija principala*

Slika 1 jasno prikazuje položaj principala u hijerarhiji sigurnosti.

Securables

Securables (približan prevod bio bi osiguranici) su resursi **za koje** SQL Server autorizuje pristup. Opseg osiguranika je takođe hijerarhijskii i kreće se od servera preko baza podataka (tabela, views..) pa sve do nivou kolone u tabeli. Mada je ubičajeno da se osiguranicima smatraju objeti u bazama podataka, ali sada smo naučili da je ta paleta i malo šira.



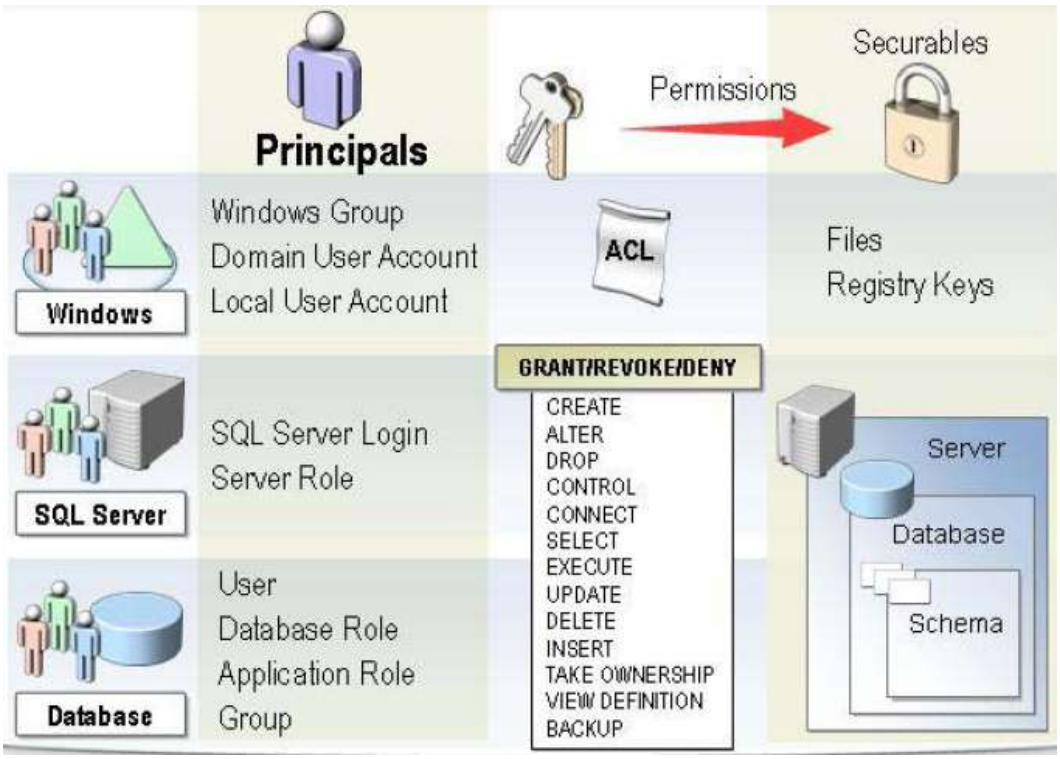
Slika 2. *Hijerarhija osiguranika*

Permisije

Ono što veže principala i osiguranika jeste permisija (dozvoljene aktivnosti nad objektima i podacima u bazi podataka). Opseg dozvola je jako širok, neke od njih mogu biti:

- kreiranje baze na serveru;
- rad sa sigurnosnim elementima
- promjena definicije objekata
- SELECT, INSERT, UPDATE, DELETE
- Itd.

Kompletna lista svih prava pristupa se može naći u BooksOnline:



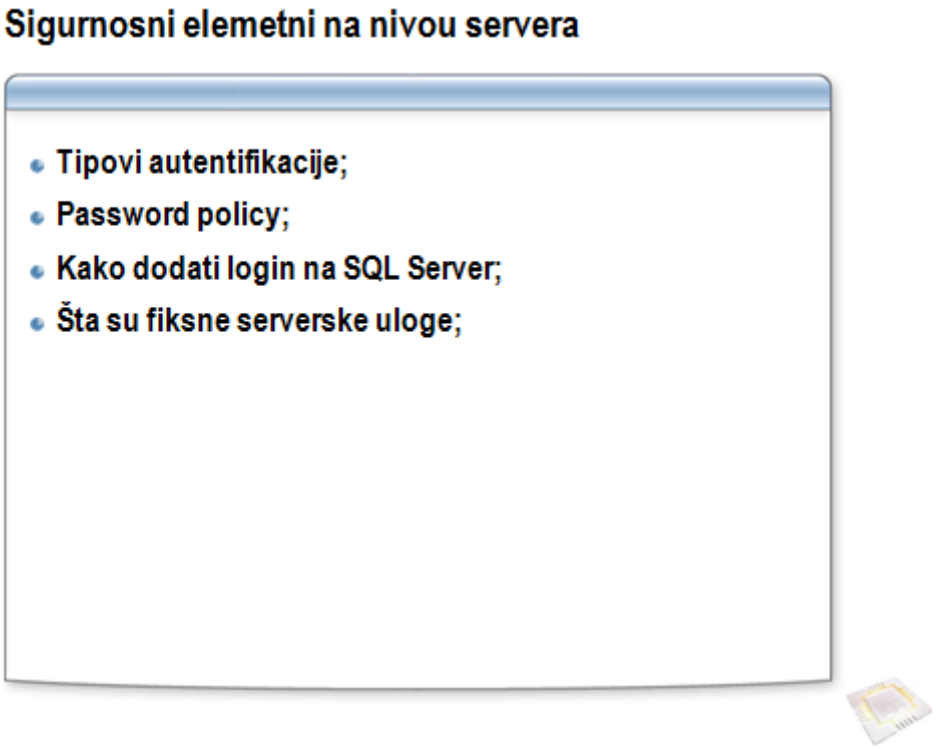
Slika 3. *Kompletna slika sa principalima, osiguranicima i vezom u obliku permsija.*

Tek na slici 3 se vidi puna sprega na relaciji: Principal→Permisija→Securables. **Principal sam za sebe ne može uraditi ništa nad bilo kojim osiguranim resursom bez odgovarajuće permisije**.

Npr. Redovni studenti u Mostaru su na dobili permisiju (CREATE DATABASE) kako bi uspješno kreirali baze podataka na workshop djelu nastave.

Neke od navedenih permisija (slika 3) su u domenu servera, a neke u domeni baze podataka. Malo kasnije više o tome.

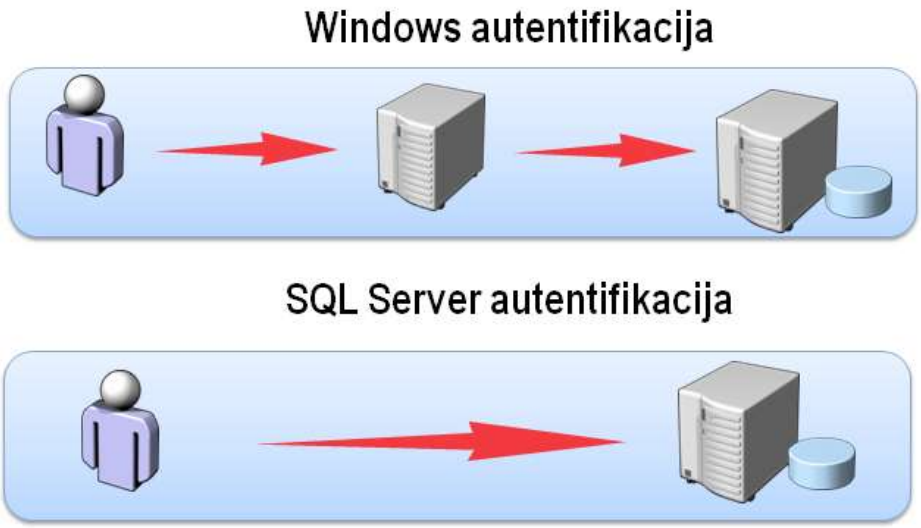
Server side security



U nastavku lekcije ćemo se upoznati sa sigurnosnim elementima (mehanizmima) na SQL Serveru koji omogućavaju funkcionisanje lanca **Principal→Permisija→Securables**. Krenimo redom.

Tipovi autentifikacije

O tipovim autentifikacije smo govorili u lekciji Modul.1. Sada ćemo malo proširiti postojeće znanje.



Slika 4. *Tipovi autentifikacije*

Kao i svaki drugi servis SQL Server zahtjeva od klijenta (principal) proces autentifikacije i autorizacije prije nego dozvoli pristup svojim resursima.

Autentifikacija – proces identifikacije korsnika tj. da li je to neko za koga se predstavlja. Ovo je operacija koja se izvršava prilikom pristupa (logiranja). Uspješna autentifikacija NE znači da imate pristup određenom resursu. Tada na scenu stupa:

Autorizacija - procedura provjere šta autentificirani korisnik smije da radi tj. kojim resursima i pod kojim pravima im može pristupiti (čitanje podata u tabelama, modifikacija, brisanje, konfiguracijske postavke servera i sl.)

U tu svrhu SQL Server koristi dva tipa autentifikacije korisnika.

- **Windows ili trusted autentifikacija** preko domen kontrole (Active Directory) ili preko lokalnog Windows naloga
- **SQL Server autentifikacija** gdje se podaci o korisniku i lozinkama nalaze direktno u master bazi SQL Servera

Prvi korak, prije nego što možete pristupiti SQL Server-u, jeste Vaše autorizovanje tj. provjera; Ko ste Vi ? Da bi taj korak bio izvodiv, na SQL Serveru se mora nalaziti login (ne korisnik) koji mapira domenski nalog (Windows autentifikacija) ili SQL Server nalog. Dakle, student sa domenskim nalogom FIT\945 želi pristupiti SQL Serveru. Prvi korak koji administrator mora uraditi jeste kreirati login na serveru i mapirati ga (dodjeliti) domenskom nalogu. SQL Server to naziva LOGIN. Login može nositi isto ime kao i domenski, ali nije obavezno.

U slučaju da nemamo mogučnost korištenja domenskog okruženja, tada možemo uključiti MIXED mod autentifikacije (Windows i SQL Server). SQL Server može raditi samo u Windows ili Mixed modu. Dakle dolazimo do zaključka da nije moguće raditi samo sa SQL Server modom autentifikacije. SQL Server autentifikacija je najmjenjena onim sistemima i klijentima koji dolaze iz **ne**-Domenskog okruženja. Npr. Linux klijent bi sa ovim tipom autentfikacije mogao pristuputi serveru i eventualno bazi podataka ako tako definišemo.
Ovo je zgodno mjesto da napomenemo jednu vrlu bitnu stvar. Ako korisniku dodjelite login na SQL Server to ne znači niti garantuje da ima pristup bilo kojem resursu na serveru. Ovo zapamtite dobro jer većina grešaka se pravi na ovom nivou. Da budemo još preciziniji, ako domenskom korisniku FIT\945 kreirate login na serveru (i ništa više) FIT\945 nakon uspješne prijave na SQL Server nema pristup niti jednom resursu (securables). Gledano sa aspekta servera to su baze podataka.

Ako se pitate kako da kod kuće i na Vašim lokalnim instalacijama imate pristup SQL Serveru bez da se logirate i svim njegovim resursima (uključujući i baze podataka), pogledajte sliku 5.

Slika 5. *Čvor security*

Ako ste administrator na Vašoj mašini (u 99 % situacija jeste) onda imate nešto slično kao na slici 5. Login, BUILTIN\Administrators je automatski dodao sve lokalne admine i dodjelio im sa (sysadmin) permisije tj. pristup svim elemtima SQL Servera. Zašto se od Vas ne traži nikakva lozinka tj. ona koju unosite prilikom logiranja na Windows XP/2003, objašnjenje leži u slici 6.

Slika 6. *Logiranje na lokalnu instancu preko Windows autentifikacije*

Razlog je taj što ste već prijavljeni na sistem (logirali ste se na Vaš Windows OS) i SQL Server vjeruje (trusted connection) da ste to Vi. Naravno, ako nekome drugom date Vaš password od OS-a, to je Vaš problem, a ne RDBMS-a.

Primjetite da su polja User name i Password „siva" (disabled) tj. Nemate mogučnost da uneste bilo šta u njih. User name već ima prikazano korisničko ime sa Windows sesije i ako je isti mapiran kao SQL Serve login, onda je prijava na RDBMS zagaratovana.

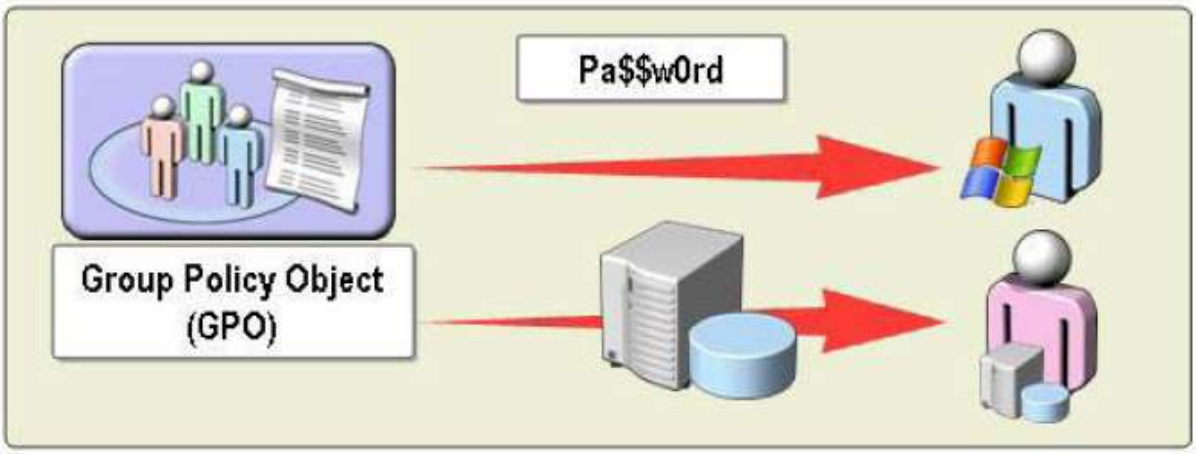
U slučajevima kada koristimo Mixed mod (SQL Server autentifikaciju) onda je moguće unijeti korisničko ime i lozinku tj. podatke od logina koji je kreiran na SQL Serveru.

Slika 7. *Logiranje na lokalnu instancu preko SQL Server autentifikacije*

Preporuka je da se koristi Windows autentifikacija iz razloga što user name i lozinka ne „putuju" mrežom i samim time nisu potencijalna meta mrežnim uljezima. Ovaj problem se može riješiti kritpovanjem komunikacije klijenta i servera.

Password policy

Opšte poznata činjenica je da u lancu sigurnosti korisnik nosi najveći rizik i to u svim segmetnima. Jedan od elemenata jeste i lozinka. Korisnici obično ne žele da pamte „jake" (strong) lozinke i za iste odabiru opšte poznate pojmove iz života. U velikoj većini slučajeva je to samo ime korisnika ili pojam koji je usko vezan za istog (imena članova porodice, datumi rođenja i sl.)

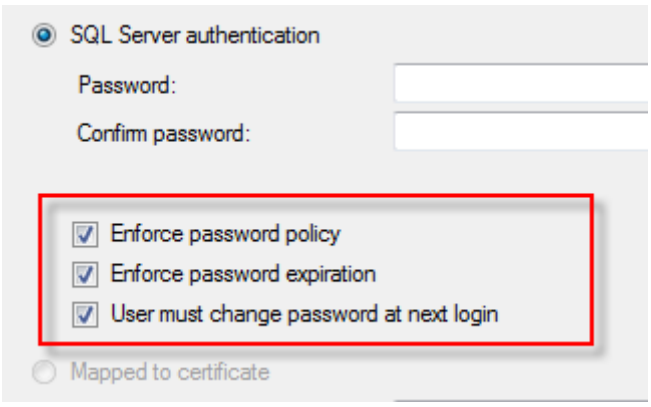


Slika 8. *Šema password policy arhitekture*

Ako pogledamo sliku 8 shvatiti ćemo da i SQL Server ima ugrađene mehanizme koji se brinu da korisnik **mora** definisati **jaku** lozinku.

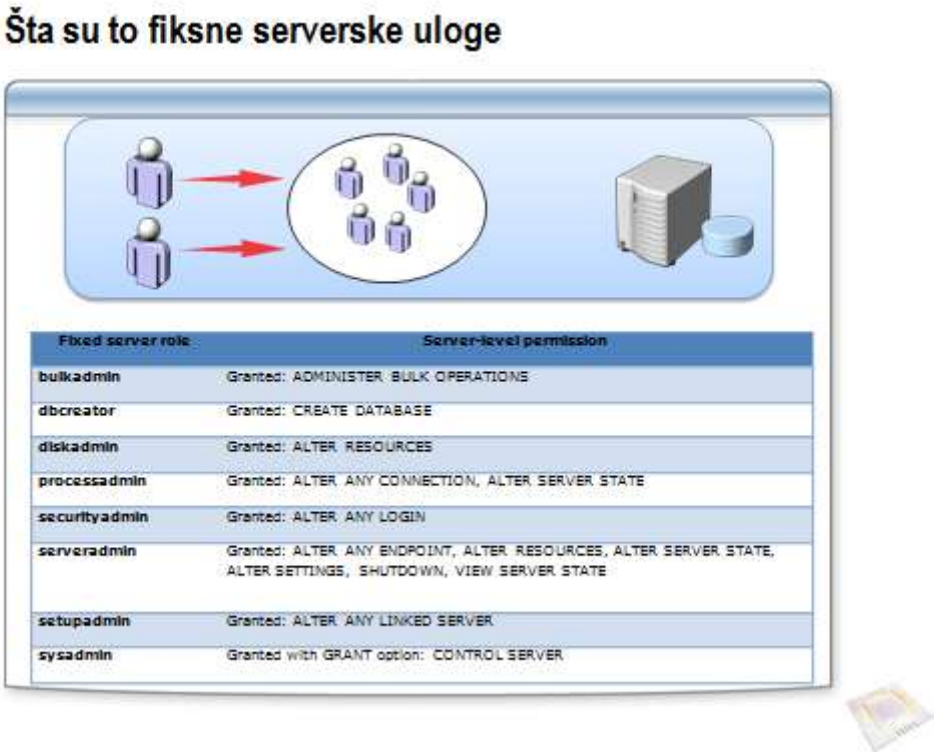
U slučaju Windows autentifikacije, korisnika autorizuje domen kontroler. Ako je, administrator domene omogućio (default je **on**), password policy se provjerava na tom mjestu. Već smo rekli da u slučaju Windows autentifikacije, SQL Server ne provjerava korisnika taj zadatak radi domen kontroler (Active Directory).

Međutim, ako koristite SQL Server login, tada jačinu lozinke mora provjeriti sam SQL Server. To je moguće samo ako je RDBMS instaliran na Windows 2003 Server i više verzije. Slika 9 prikazuje koje sve elemente vezane za lozinku možemo definisato na SQL Server loginu.



Slika 9. *Password policy*

Fiksne serverske uloge



Već smo rekli da login na SQL Serveri ne garantuje pristup niti permisije na bilo koji resurs. Naravno, prilikom kreiranja logina možeme definisati koje aktivnosti na nivou servera taj login može vršiti. Ovo je potpuno opcionalno. U produkcijskim okuženjima nije baš često praksa dodjele serverskih uloge korisnicima. U svakom slučaju postoji 8 unaprijed definisanih **fiksnih** serverskih uloga koje možete dodjeliti loginima na SQL Serveru.

Fiksna serverska uloga	Permisije
bulkadmin	Granted: ADMINISTER BULK OPERATIONS
dbcreator	Granted: CREATE DATABASE
diskadmin	Granted: ALTER RESOURCES
processadmin	Granted: ALTER ANY CONNECTION, ALTER SERVER STATE
securityadmin	Granted: ALTER ANY LOGIN
serveradmin	Granted: ALTER ANY ENDPOINT, ALTER RESOURCES, ALTER SERVER STATE, ALTER SETTINGS, SHUTDOWN, VIEW SERVER STATE
setupadmin	Granted: ALTER ANY LINKED SERVER
sysadmin	Granted with GRANT option: CONTROL SERVER

U sljedećoj lekciji objašnjavamo kako loginima sa servera dozvoliti pristup u baze podataka.