|  |  |  |
| --- | --- | --- |
|  | UNIVERZITET U NOVOM SADU  FAKULTET TEHNIČKIH NAUKA  NOVI SAD |  |

Grupa 11

Aleksandra Jagodić PR 161/2017

Irina Jovanović PR 11/2015

Marija Vukomanović PR 67/2015

Petar Stančov E3 16/2014

Zadatak 25

Sigurnost i bezbednost u elektroenergetskim sistemima

* Primenjeno softversko inženjerstvo -

Novi Sad, 16.11.2018

Sadrzaj

[1. OPIS REŠAVANOG PROBLEMA](#__RefHeading___Toc209_3190288126) 3

[2. TEORIJSKE OSNOVE](#__RefHeading___Toc211_3190288126) 4

[3. DIZAJN IMPLEMENTIRANOG SISTEMA](#__RefHeading___Toc321_3190288126) 5

[4. TESTIRANJE SISTEMA](#__RefHeading___Toc215_3190288126) 6

# OPIS REŠAVANOG PROBLEMA

Zadatak projekta je pravljenje sigurnosne komunikacije između klijenta i servera za upravljanje bazom podataka (.txt fajl) .

Podržane su autentifikacija, autorizacija, replikacija podataka na sekundarni server i failover mehanizam. Korisnik je povezan sa privilegijama posredstvom Windows grupa koje su mu dodeljene tako što podržava RBAC šemu.

U zavisnosti od tipa klijentske aplikacije, odnosno različitih vrsta klijenta korisnici imaju određena prava. Klijenti tipa Admin imaju pravo kreiranja, arhiviranja i brisanja baze podataka. Klijenti tipa Writer imaju pravo upisa i modifikacije podataka, dok klijenti tipa Reader imaju pravo čitanja iz baze (srednja potrošnja za određeni grad, srednja potrošnja za određeni region i pronalazak najvećeg potošača za određeni region).

Replikator replicira podatke koji se ne nalaze na drugom serveru, odnosno šaljemo samo razliku podataka.

FailOver mehanizam u slučaju otkaza primarnog servera omogućava neometan rad klijenta , jer njegovu ulogu preuzima sekundarni server. U slučaju da klijent pokušava da se konektuje na server koji je nedostupan, automatski će pokušati da se konektuje na drugog servera.

Projekat takođe podržava zapis događaja u specifični *Windows Event Log* za centralizovano logovanje pomoću metoda implemetiranih u **CustomAuditBehavior** klasi.

# TEORIJSKE OSNOVE

**Autentifikacija** je jedan od osnovnih bezbednosnih mehanizama kojim se obezbeđuje validacija identiteta u okviru informacionog sistema. U ovom zadatku se koristi Windows autentifikacija.

Windows autentifikacioni model je zasnovan na SPNEGO (Simple and Protected GSS API negotiation mechanism) mehanizmu za pregovaranje između različitih realnih autentifikacionih mehanizama u zavisnosti od okruženja. SSPI (Security Support Provider Interface) je Windows API koji implementira SPNEGO i predstavlja zajednički interfejs za različite Windows autentifikacione protokole (Secure Service Provider). Negotiate SSP je aplikativni protokol kojim je implementirano pregovaranje u Windows-u. Trenutno podržani protokoli su NTLM i Kerberos.

**NTLM** (NT Lan Manager) je autentifikacioni protokol zasnovan na *challenge-response* autentifikacionoj šemi, čime je omogućena autentifikacija bez slanja poverljivih podataka (šifre). Iako challenge-response spada u jake autentifikacione šeme jer nema razmene poverljivih podataka, problem ovakvih protokola je činjenica da servis mora da zna originalnu šifru svakog klijenta kako bi mogao da validira pristigli response. Dodatno, u ovako definisanom autentifikacionom protokolu izostaje verifikacija servisnog identiteta od strane klijenta, odnosno ovakav protokol ne omogućuje obostranu autentifikaciju

**Kerberos** je dvosmerni autentifikacioni protokol koji se zasniva na trećoj strani od poverenja i razmeni ticketa u cilju uspostavljanja bezbedne obostrane autentifikacije učesnika u komunikaciji bez razmene šifri. Kako bi se obezbedili sigurniji protokoli, uvodi se treća strana od poverenja odnosno entitet kome veruju svi ostali učesnici u komunikaciji.

Bezbednosni događaji mogu biti kako uspešno izvršene akcije u sistemu, tako i neuspešni pokušaji pristupa resursima. Audit log predstavlja zapis bezbednosno relevantnih događaja u sistemu. S obzirom da audit log predstavlja vremenski obeležene zapise o aktivnostima u sistemu, učesnici ne mogu naknadno poricati izvršene akcije čime se obezbeđuje neporecivost. Integritet, odnosno tačnost podataka koje sadrže audit logovi se obezbeđuje primenom mehanizama kontrole pristupa logovima, digitalnim potpisima, itd. Analizom prikupljenih informacija moguće je detektovati kako uspešne tako i neuspešne pokušaje kako redovnih tako i malicioznih aktivnosti u sistemu, odnosno naknadno utvrditi uzroke grešaka ili otkaza u sistemu.

Korišćeni bezbednosni mehanizam za logovanje je *Windows Event Log*. Ugrađeni .NET mehanizam za logovanje i audit koristi log datoteke *Windows* operativnog sistema za zapis različitih tipova događaja: sistemskih (generisanih od strane operativnog sistema), aplikativnih i bezbednosnih – tzv. *Microsoft Windows Event Log*.

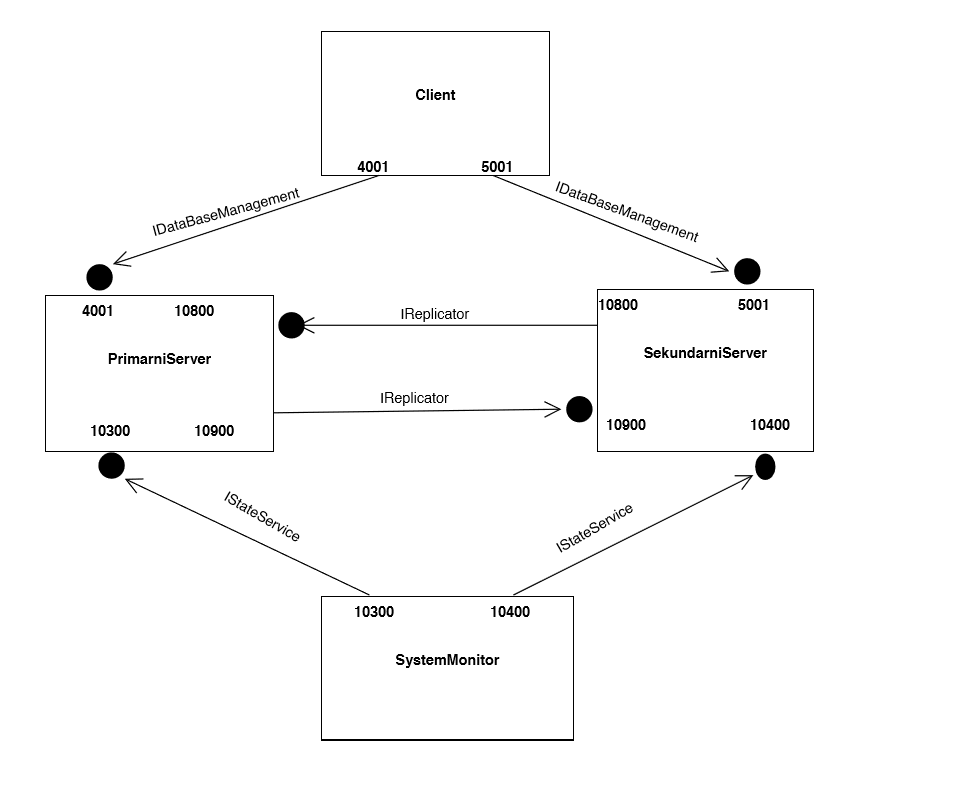
Korišćeni bezbednosni mehanizam za autorizaciju je **RBAC** autorizaciona šema. Kontrola pristupa zasnovana na ulozi (**RBAC**) je neutralan mehanizam kontrole pristupa koji je definisan ulogama i privilegijama. Komponente RBAC-a, kao što su dozvole i uloge korisnika, olakšavaju izvršavanje korisničkih zadataka. Upotrebom RBAC-a olakšava se upravljanje korisničkim privilegijama.

**Autorizacija** je proces definisanja ovlašćenja validnim entitetima u sistemu, kao i proces odlučivanja kojim resursima tog sistema entitet može da pristupi i koje operacije nad resursima može da izvrši.

# DIZAJN IMPLEMENTIRANOG SISTEMA

Projekat se sastoji iz sledećih komponenti :

* Client –klijentska aplikacija koja omogućava korisniku autentifikaciju i komunikaciju sa serverom
* Common –biblioteka koja sadrži sve potrebne klase i interfejse IDatabaseManagement i IStateService
* Server – sadrži implementaciju interfejsa IdatabaseManagement,IstateService..takođe Replikacija je odrađena na samom serveru
* SystemMonitor –otpornost na otkaze.



Tehnologija korišćena za komunikaciju između klijenta i servera je WCF (Windows Communication Foundation). WCF je deo .NET razvojnog okruženja za pisanje distirbuiranih, servisno-orijentisanih aplikacija. Mehanizmi bezbednosti primenjeni u zadatku su autentifikacija i autorizacija, kao i audit za praćenje događaja. Klijent ima mogućnost da se autentifikuje preko Windows kredencijala. Server izlaže interfejs *IdataBaseManagment klijentu*  koji omogućava rad sa bazom.

Interfejs *IdataBaseManagment*  nudi sledeće metode:

* AddConsumer – *Write* privilegija
* ModificationConsumer – *Write* privilegija
* CityConsumtion – *Read* privilegija
* MaxRegionConsumation – *Read* privilegija
* RegionConsumtion – *Read* privilegija
* CreateFile – *Administrate* privilegija
* RemoveConsumation – *Administrate* privilegija
* ArchiveConsumation– *Read* privilegija

# TESTIRANJE SISTEMA

Prikaz rezultata testiranja. Očekuju se prikazi pozitivnih i negativnih (npr. neuspešna autentifikacija, neuspešna autorizacija, itd.) test scenarija.