Univerzitet u Novom Sadu

Fakultet tehničkih nauka

Osnove informacione bezbednosti u infrastrukturnim sistemima

PR 87/2020 NEVENA ĆULIBRK
PR 95/2020 KRISTINA SRETENOVIĆ
PR 103/2020 ANABELA ZONAI

UVOD

Ovaj dokument opisuje implementaciju servisa koji pruža usluge korišćenja baze podataka, namenjenog različitim vrstama klijentskih aplikacija. Servis koristi interfejs IDatabaseManagement i omogućava manipulaciju podacima u tekstualnom fajlu koji predstavlja bazu podataka. Ova implementacija pruža siguran i efikasan mehanizam za upravljanje podacima uz poštovanje principa sigurnosti, autorizacije i autentifikacije. Servis je dizajniran kako bi zadovoljio potrebe različitih tipova klijentskih aplikacija, omogućavajući im pristup i upravljanje podacima u skladu sa njihovim ulogama i permisijama.

OPIS PROJEKTNOG ZADATKA

U okviru našeg projekta zadatak je bio da implementiramo servis koji pruža usluge korišćenja i upravljanja tekstualnom bazom podataka. Baza podataka sadrži informacije o identifikatoru, regionu, gradu, godini i potrošnji električne energije po mesecima tokom godine.

Postoje tri tipa klijentskih aplikacija:

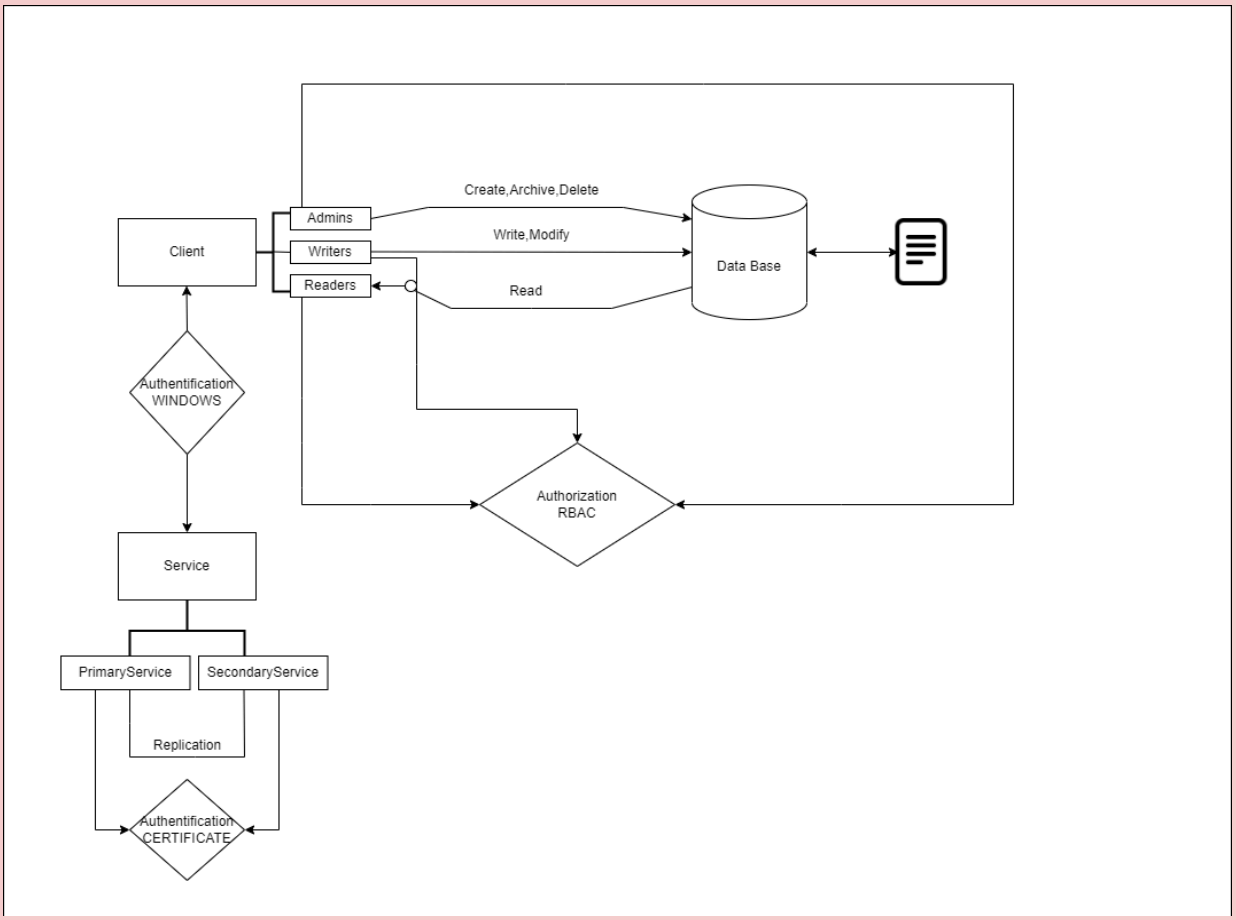
- Admins mogu kreirati, arhivirati i brisati bazu podataka. Mogu obrisati bazu prilikom arhiviranja ili na zahtev, bez prethodnog arhiviranja.
- Writers mogu upisivati i modifikovati bazu podataka.
- Readers mogu čitati informacije iz baze podataka. Mogu dobiti srednju potrošnju za određeni grad ili region, kao i pronaći najvećeg potrošača u određenom regionu.

Autentifikacija se vrši preko Windows autentifikacionog protokola, a autorizacija se zasniva na RBAC autorizacionoj šemi.

Podaci se repliciraju na sekundarni server (BackupService). Autentifikacija između primarnog i sekundarnog servera se postiže sertifikatima, a poruke između njih se šifruju AES algoritmom.

Sve akcije, uključujući autentifikaciju, autorizaciju i rad nad bazom podataka, se loguju u Windows Event Log putem specifičnog log fajla.

DIJAGRAM



OPIS DIJAGRAMA AKTIVNOSTI

Client izvršava Login u ulozi admin-a, writer-a ili reader-a. Na osnovu toga se vrši Windows autentifikacija. Na osnovu uloge koju klijent ima, vrši se autorizacija i klijent dobija različite permisije vezane za tu ulogu koje može da izvršava nad bazom podataka koja je u vidu XML File-a. Postoje 2 vrste service-a, Backup i Service gde se podaci repliciraju sa primarnog(Service) na sekundarni servis (Backup Service), dok su poruke šifrovane, a autentifikacija se vrši preko sertifikata.

OPIS TEHNOLOGIJA

Za implementaciju projekta korišćene su neke od sledećih tehnologija:

- Programski jezik C# korišćen je za implementaciju servisa i klijentske aplikacije
- WCF (Windows Communication Foundation) korišćen je radi ostvarenja komunikacije između servisa i klijentske aplikacije
- Windows autentifikacija i preko sertifikata
- RBAC autorizacija
- AES algoritam za enkripciju podataka

OPIS KOMPONENTI APLIKACIJE

Common - Realizovan je kao ClassLibrary koji sadrži klase i interfejse.
Klase:
DatabaseEntry - klasa za kreiranje objekta koji će biti serijalizovan u bazu i deserijalizovan iz nje. Sadrži polja id, region, grad, godina i ukupna potrošnja električne energije.
AES - Klasa u kojoj su definisane metode za enkripciju (EncryptStringToBytes_Aes()) i dekripciju (DecryptBytesToString_Aes) podataka Aes algoritmom u CBC modu.
SecretMask - klasa koja XOR operacijom kriptuje kljuc (key) i IV vektor

Interfejsi:
IDatabaseManagement - služi za povezivanje klijenta i servera preko WCF-a. Sadrži metode koje će admin, writer i reader koristiti.
IBackupService - služi za povezivanje servisa sa backup servisom. Sadrži metodu PullDatabase() koja će imati kriptovane podatke i slati ih na backup servis da se dekriptuju.

CertificateManager - Realizovan je kao ClassLibrary koji sadrži klase koje su vezane za sertifikate u našoj aplikaciji.
Klase:
ServiceCertValidator i BackupServiceCertValidator - funkcije za proveru jel serverski sertifikat self-signed i da li je klijentski sertifikat potekao od istog izvora kao i serverski.
CertManager - klasa koja pronalazi instalirane sertifikate na našem računaru.

SecurityManager - Realizovan je kao ClassLibrary koji sadrži klase koje su vezane za autorizaciju.
Sadrži klase koje proveraju identitete, kojim oni grupama pripadaju i koje su njihove permisije, jer koristimo RBAC autorizaciju. U .resx fajlu su definisane grupe i permisije koje svaka grupa poseduje.

Service - Konzolna aplikacija
Program.cs - definiše se binding za klijenta i backupservice i otvara se endpoint.
Između klijenta i servisa je windows autentifikacija i autorizacija RBAC modelom, a između servisa i backupservisa je autentifikacija pomoću sertifikata (ChainTrust).
Definiše se i instanca Audit klase koja će služiti za upravljanje logovima aplikacije.
DatabaseService.cs - klasa koja implementira sve funkcije iz IDatabaseManagement interfejsa.
U svakoj funkciji proverava identitet korisnika koji pokušava da pristupi metodi i gleda da li ima ulogu koja mu dozvoljava pristup toj metodi. To se radi imperativnom proverom privilegija uz pomoć metode IsInRole().
Na početku ove klase je deklarisana i baza, tačnije njegova putanja u kojoj će se čuvati svi podaci. Baza se može kreirati, arhivirati i brisati ukoliko klijent ima Administrate privilegiju. Klijent u bazu može da upiše podatke i da ih modifikuje ukoliko ima Write privilegiju ili da čita iz baze ako ima Read privilegiju.

Client - konzolna aplikacija
ClientProxy.cs - otvara se kanal za komunikaciju sa servisom.
Definisana je autentifikacija (Windows). Klijentu se prilikom pokretanja nudi meni sa izborom akcija koje može da uradi.

BackupService - konzolna aplikacija
Otvara se kanal za komunikaciju sa servisom i definiše se autentifikacija pomoću sertifikata. Takođe na backup servisu se dešava dešifrovanje podataka i njihovo ponovno upisivanje u bazu (BackupDatabase.xml).

AuditManager - Zapisivanje bezbednosnih događaja u Windows aplikativnu log datoteku. Definiše nam da li će autentifikacija i autorizacija biti uspešna ili neuspešna. Proverava uspešnost i neuspešnost i svih ostalih akcija u aplikaciji kao sto su: kreiranje, arhiviranje i brisanje baze, pisanje i modifikovanje baze i pokušaji čitanja podataka iz iste.

ZAKLJUČAK

Implementacija servisa za upravljanje bazom podataka predstavlja bezbedno rešenje koje omogućava klijentskim aplikacijama efikasan pristup i manipulaciju podacima. Kroz primenu Windows autentifikacionog protokola i RBAC autorizacione šeme, obezbeđena je visoka sigurnost sistema.

Implementirana je replikacija podataka na sekundarni servis, pružajući redundanciju sistema.

Kriptovanje poruka između primarnog i sekundarnog servisa dodatno povećava sigurnost komunikacije.

Logovanje svih akcija, uključujući autentifikaciju, autorizaciju i sve operacije nad bazom podataka, omogućava praćenje i analizu aktivnosti sistema.

Implementacija servisa pridržava se najviših standarda sigurnosti, omogućavajući klijentima da efikasno upravljaju podacima uz jasnu podelu odgovornosti i prava među različitim tipovima klijentskih aplikacija.