UNIVERZITET U NIŠU
ELEKTRONSKI FAKULTET
Katedra za računarstvo

APACHE CASSANDRA – SIGURNOST BAZE PODATAKA

SISTEMI ZA UPRAVLJANJE BAZAMA PODATAKA

-SEMINARSKI RAD-

Student:
Marijana Cvetković, br. ind. 1431

Mentor:
Doc. dr Aleksandar Stanimirović

Uvod

- Sigurnost baze podataka
  - Sigurnosni ciljevi
  - Pretnje bezbednosti baze podataka
  - Kako obezbediti server baze podataka
  - Saveti očuvanja bezbednosti baze podataka
  - Kontrole i politike
- Sigurnost Cassandra baze podataka
  - Autentifikacija
  - Autorizacija
  - SSL enkripcija
  - Opšte mere bezbednosti
  - Keširanje

SIGURNOST BAZE PODATAKA

- Bezbednost baze podataka se odnosi na mere koje se koriste za zaštitu i obezbeđenje baze podataka ili softvera za upravljanje bazom podataka od nezakonite upotrebe i zlonamernih sajber pretnji i napada.

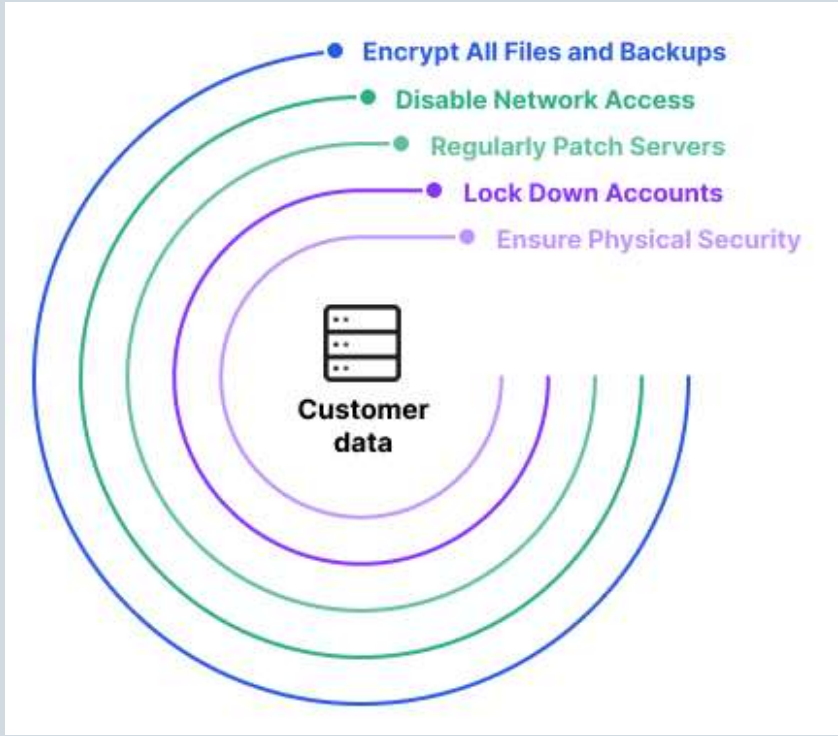
- Načini kojima se analizira i implementira bezbednost baze podataka uključuju:
  - Ograničavanje neovlašćenog pristupa i korišćenja primenom jakih i višefaktorskih kontrola pristupa i upravljanje podacima.
  - Testiranje opterećenja/stres i testiranje kapaciteta baze podataka kako bi se osiguralo da se ne sruši u napadu distribuiranog uskraćivanja usluge ili preopterećenju korisnika.
  - Fitička sigurnost servera baze podataka i rezervne opreme od krađe i elementarnih nepogoda. Redovne rezervne kopije podataka mogu se planirati kao deo bezbednosnog protokola baze podataka, a više kopija se može uskladištiti van lokacije da bi se obezbedila redudantnost i hitan oproravak.
  - Pregled postojećeg sistema za sve poznate ili nepoznate ranjivosti i definisanje i implementacija mape puta/plan za njihovo ublažavanje.
  - Šifrovanje podataka može da obezbedi nivo bezbednosti za zaštiti integiteta i poverljivosti podataka.

Pretnje bezbednosti baze podatka

- Insajderske pretnje
- Ljudska greška
- Iskorišćavanje ranjivosti softvera baze podatka
- Napadi prekoračenja bafera
- Napadi uskraćivanja usluge
- Zlonamerni programi
- Razvojno IT okruženje

Bezbednost servera baze podataka

- Obezbediti fizičku bezbednost baze podataka
- Zaključati naloge i privilegije
- Redovno zakrpiti serevere baze podataka
- Onemogućiti pristup javnoj mreži
- Šifrovanje svih datoteka i rezervnih kopija



Saveti za bezbednost baze podataka

- Aktivno upravljanje lozinkama i korisničkim pristupom
- Testiranje bezbednosti baze podataka
- Korišćenje praćenja baze podataka u realnom vremenu
- Korišćenje zaštitinih zidova za veb aplikacije i baze podataka

Politike bezbednosti baze podataka treba da budu integrisane i podržavaju opšte poslovne ciljeve, kao što su zaštita kritične intelektualne svojine i politike sajber bezbednosti i politike bezbednosti u oblaku. Bezbednosne kontrole, programi obuke i edukacije o svesti o bezbednosti, kao i strategije za testiranje penetracije i procene ranjivosti treba da budu uspostavljene kao podrška formalnim bezbednosnim politikama.

SIGURNOST CASSANDRA BAZE PODATAKA

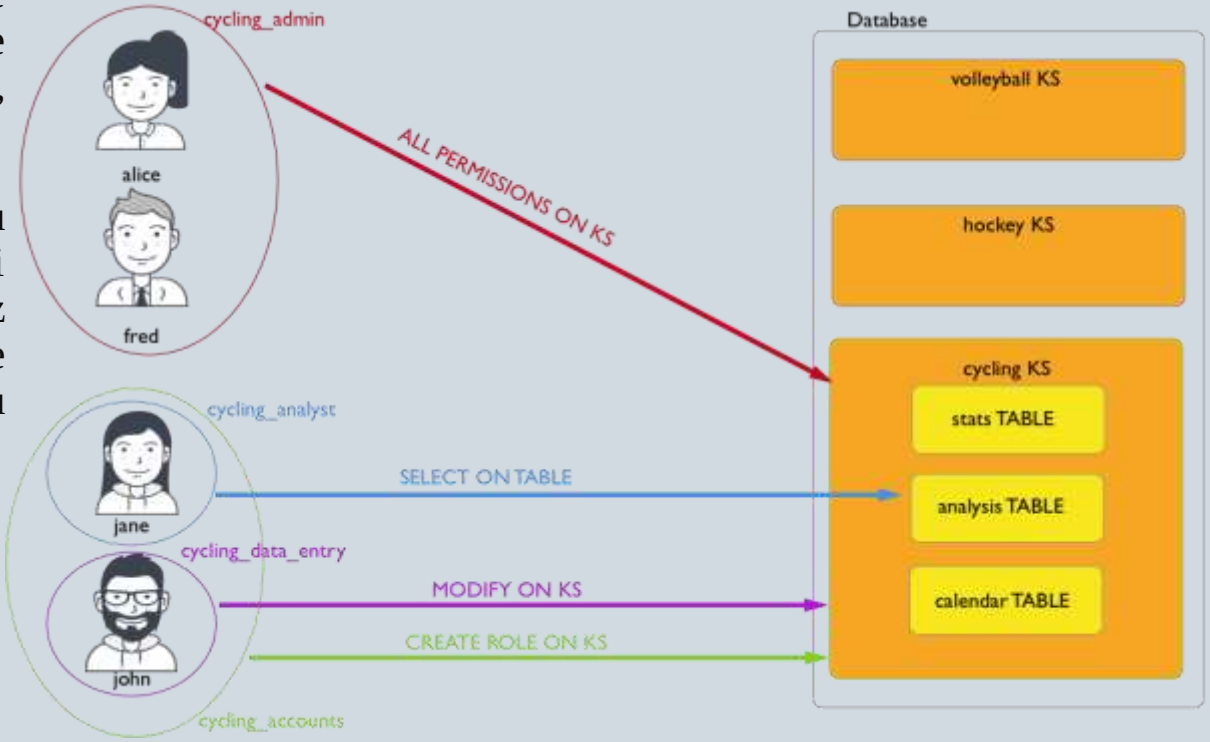
Cassandra pruža ove bezbednosne funkcije zajednici otvorenog koda:

- Autentifikacija zasnovana na interno kontrolisanom imenu uloge/lozinki
- Autorizacija zasnovana na upravljanju dozvolama za objekte
- Autentifikacija i autorizacija na osnovu JMKS korisničkog imena/lozinke
- SSL enkripcija
- Opšte mere bezbednosti.

1) Autentifikacija zasnovana na interno kontrolisanom imenu uloge/imena

Cassandra autentifikacija je zasnovana na ulogama i interno se čuva u sistemskim tabelama Cassandre. Administratori mogu da kreiraju, menjaju, ispuštaju ili listaju uloge koristeći CQL komande, sa pridruženom lozinkom. Uloge se mogu kreirati sa privilegijama superkorisnika, nesuperkorisnika i privilegijama za prijavu.

Cassandra koristi imena uloga i lozinke za internu autentifikaciju. Potvrda identiteta zasnovana na ulozi obuhvata i korisnike i ulog da bi se autorizaciji doneo niz korisnih funkcija. Uloge mogu predstavljati ili stvarne pojedinačne korisnike ili uloge koje ti korisnici imaju u administrisiranju i pristupu Cassandra klasteru.



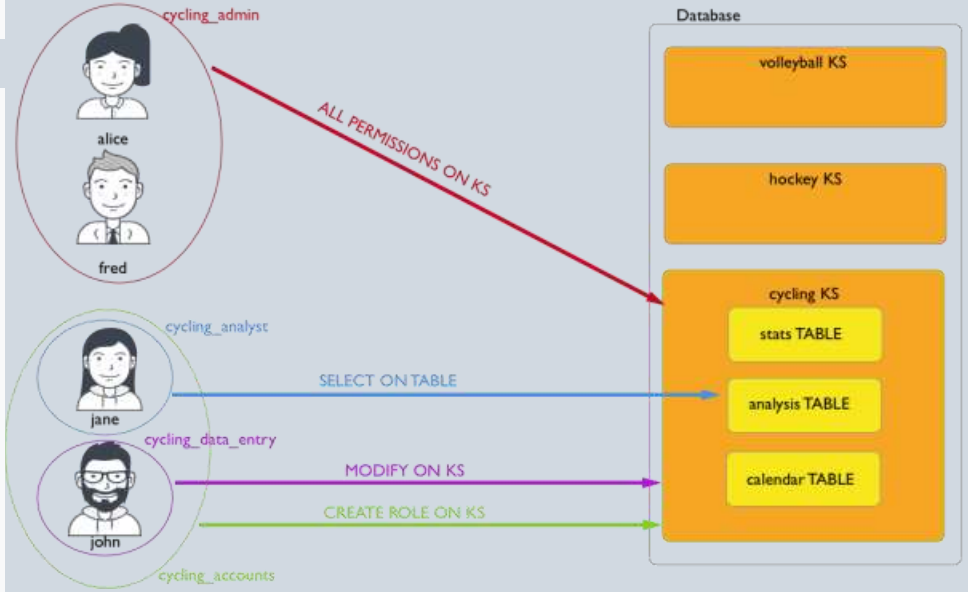
```
CREATE ROLE alice WITH PASSWORD = 'enjoyLife' AND LOGIN = true;
```

```
CREATE ROLE cycling_admin WITH PASSWORD = '1234abcd';
```

```
GRANT ALL PERMISSIONS ON KEYSPACE cycling TO cycling_admin;
```

```
GRANT cycling_admin TO alice;
```

```
CREATE ROLE cycling_analyst WITH PASSWORD =
'zyxw9876';
GRANT SELECT ON TABLE cycling.analysis TO
cycling_analyst;
CREATE ROLE hockey_analyst WITH PASSWORD =
'Iget2seeAll';
GRANT SELECT ON TABLE hockey.analysis TO
hockey_analyst;
GRANT hockey_analyst TO cycling_analyst;
GRANT cyclist_analyst TO jane;
```



-Konfigurisanje autentifikacije-

Autentifikacija se može priključiti na Cassandri i konfiguriše se korišćenjem *authenticator* podešavanja u *cassandra.yaml*. Podrazumevano, Cassandra je konfigurisana tako *AllowAllAuthenticator* da ne vrši proveru autentifikacije i stoga ne zahteva nikakve akreditive.

Autentifikacija neophodan uslov Cassandrinog podsistema dozvola, tako da ako je autentifikacija onemogućena, zapravo su i dozvole.

- Promena u datoteci cassandra.yaml

```
authenticator: PasswordAuthenticator
```

```
AllowAllAuthenticator
```

- Podrazumevano korišćenje ime superkorisnika i lozinke

```
cqlsh -u cassandra -p cassandra
```

- Da bi se sprečilo narušavanje bezbednosti, zamena podrazumevanog superkorisnika, cassandra, drugim superkorisnikom sa drugim imenom:

```
cqlsh> CREATE ROLE <new_super_user> WITH PASSWORD =
 '<some_secure_password>'
AND SUPERUSER = true
AND LOGIN = true;
```

2) Autorizacija

Autorizacija daje privilegije pristupa operacijama Cassandra klastera na osnovu autentifikacije uloge. Autorizacija može dati dozvolu za pristup celoj bazi podataka ili ograničiti ulogu na pristup pojedinačnoj tabeli. Uloge mogu da daju ovlašćenje za autorizaciju drugih uloga. Uloge se mogu dodeliti ulogama. CQL komande GRANT i REVOKE se koriste za upravljanje autorizacijom.

Dozvole za objekte mogu biti dodeljene korišćenjem Cassandrinog internog mehanizma autorizacije za sledeće objekte: keyspace, table, funkcija, agregat, uloge i Mbeans (u Cassandra 3.6 i novijim verzijama)

Dozvole se čuvaju u Cassandrinim tabelama. Dozvola se može konfigurisati sa CQL komandama CREATE, ALTER, DROP, SELECT, MODIFY i DESCRIBE, koje se koriste za interakciju sa bazom podataka. Komanda EXECUTE se može koristiti za davanje dozvole ulozi za komande SELECT, INSERT i UPDATE. Pored toga, AUTHORIZE komanda se može koristiti za davanje dozvole za ulogu GRANT, REVOKE ili AUTHORIZE dozvole druge uloge.

-Konfiguracija interne autorizacije-

CassandraAuthorizer je jedna od mogućih implementacija IAuthorizer

```
authorizer: CassandraAuthorizer
```

```
permissions_validity_in_ms: 2000
```

```
permissions_update_interval_in_ms: 2000
```

```
GRANT permission ON resource TO user
```

```
Create user laura with password 'newhire';
grant all on dev.emp to laura;
revoke all on dev.emp to laura;
grant select on dev.emp to laura;
```

```
cqlsh:dev> select * from emp_bonus;
Bad Request: User laura has no SELECT permission on <table dev.emp_bonus> or any of its parents
```

3) Autentifikacija i autorizacija na osnovu JMX korisničkog imena/lozinke

JMX (Java Managment Extensions) tehnologija pruža jenostavan i standardan način upravljanja i nadgledanja resursa koji se ondose na instancu Java virtuelne mašine (JVM). Ovo se postiže instrumentiranjem resursa sa Java objektima poznatim kao Managed Beans (MBeans) koji su registrovani na Mbean serveru. JMX autentifikacija čuva korisničko ime i povezane lozinke u dve datoteke, jednu za lozinke i jednu za pristup.

U Cassandri 3.6 i novijim verzijama, JMX autentikacija i autorizacija se mogu pronaći korišćenjem Cassandrinih internih mogućnosti autentifikacije i autorizacije.

- Nodetool sa autentifikacijom
- Jconsole sa autentifikacijom.

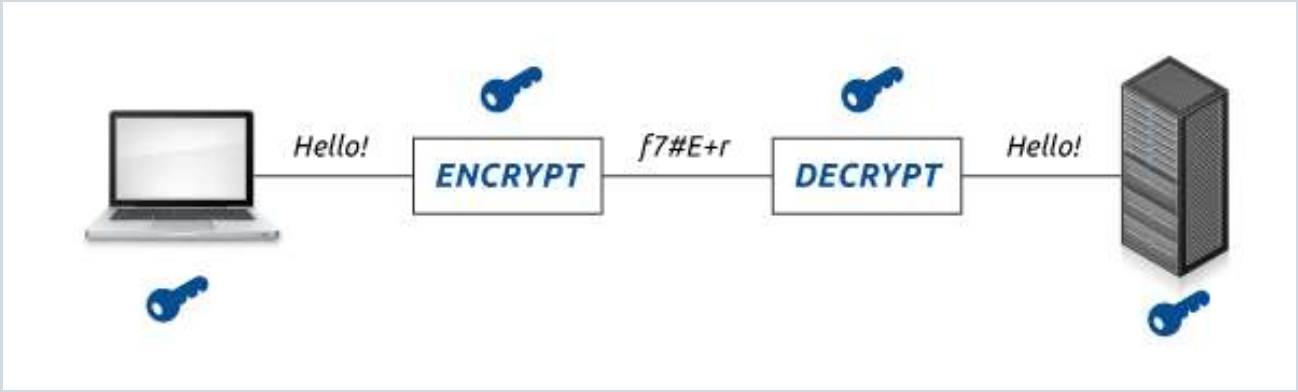
```
if [ "$LOCAL_JMX" = "yes" ]; then

  JVM_OPTS="$JVM_OPTS -
Dcassandra.jmx.local.port=$JMX_PORT -
XX:+DisableExplicitGC"
```

4) SSL enkripcija

Cassandra obezbeđuje bezbednu komunikaciju između klijenata i klastera baze podataka, kao i između čvorova u klasteru. Omogućavaje SSL enkripcije osigurava da podaci u letu nisu ugroženi i da se bezbedno prenose. Šifrovanje od klijenata do čvora i od čvora do čvora se neizvesno konfiguriše. Cassandra alati se mogu konfigurisati da koriste SSL enkripciju.

Sloj bezbedne utičnice (SSL) je kriptografski protokol koji se koristi za obezbeđenje komunikacije između računara. Podaci se šifruju tokom komunikacije kako bi se sprečili slučajni ili namerni pokušaji čitanja podataka.

Za sisteme koji koriste autoritet sertifikata (CA), skladište poverenja može da skladišti sertifikate koje je potpisao CA radi verifikacije. I skladišta ključeva i skladišta poverenja imaju dodeljene lozinke, koje se nazivaju keypass i storepass.



Apache Cassandra pruža ove funkcije SSL enkripcije:

- Šifrovana komunikacija od čvora do čvora – Šifrovanje od čvora do čvora se koristi za obezbeđenje podataka koji se prenose između čvorova u klasteru.
- Šifrovana komunikacija klijent-čvor – Šifrovanje od klijenata do čvora se koristi za obezbeđenje podataka prosleđenih između klijentskog programa, kao što je cqlsh, DevCenter ili nodetool, i čvorova u klasteru.

```
$keytool -genkey -keyalg RSA -alias node0 -validity 36500 -keystore keystore.node0
```

```
$keytool -genkey -keyalg RSA -alias node0 -keystore keystore.node0 -storepass cassandra -keypass cassandra -dname "CN=172.31.10.22, OU=None, O=None, L=None, C=None"
```

```
$keytool -export -alias cassandra -file node0.cer -keystore .keystore
```

```
$keytool -import -v -trustcacerts -alias node0 -file node0.cer -keystore truststore.node0
```

```
keytool -importkeystore -srckeystore keystore.node0 -destkeystore node0.p12 -deststoretype PKCS12 -srcstorepass cassandra -deststorepass cassandraopenssl pkcs12 -in node0.p12 -nokeys -out node0.cer.pem -passin pass:cassandraopenssl pkcs12 -in node0.p12 -nodes -nocerts -out node0.key.pem -passin pass:cassandra
```

5) Opšte mere bezbednosti

Javni port

Broj porta	Opis
22	SSH port

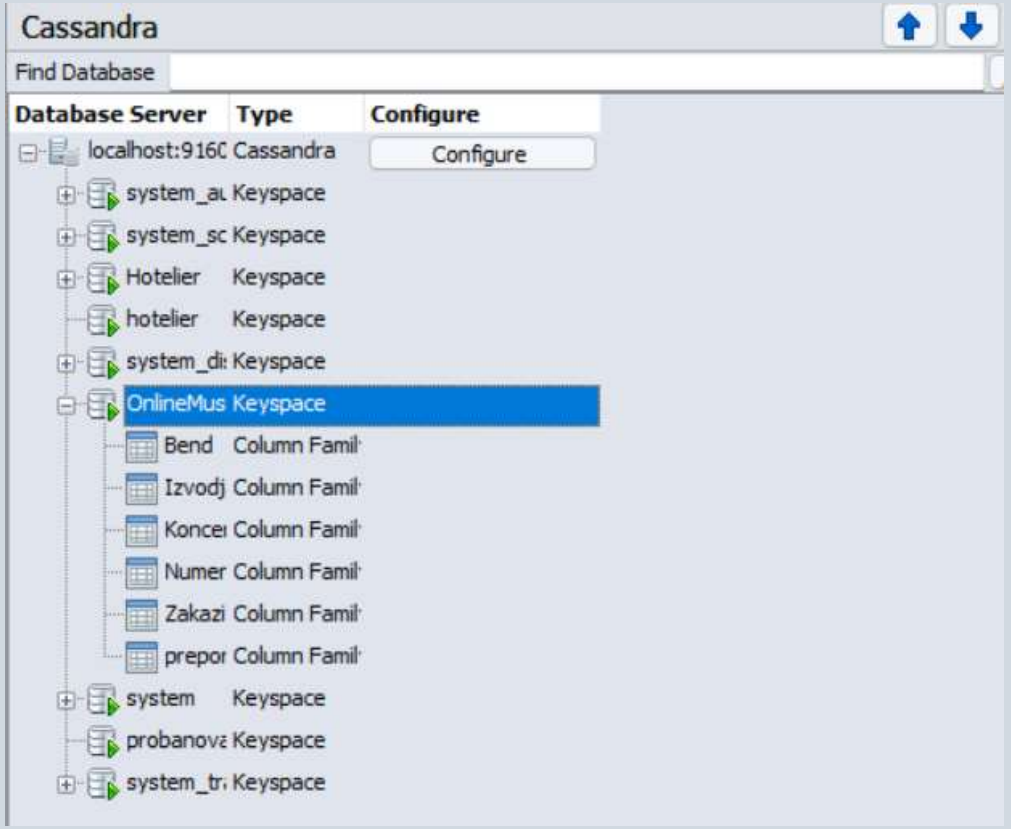
Cassandra inter-node portovi

Broj porta	Opis
7000	Cassandra inter-node klister komunikacija
7001	Cassandra SSL komunikacija klastera među čvorovima
7199	Cassandra JMKS port za nadgledanje

Cassandra klijent portovi

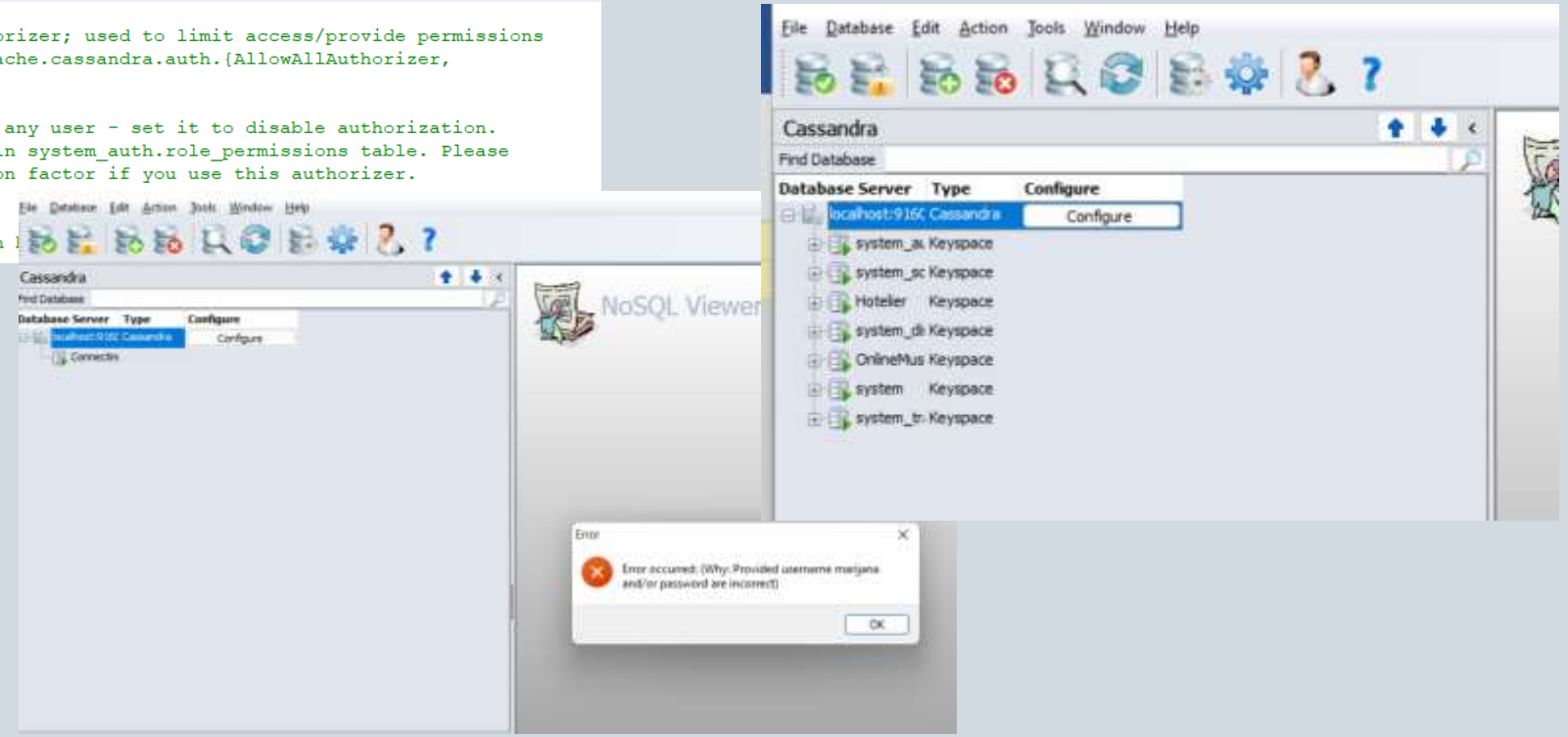
Broj porta	Opis
9042	Cassandra klijent port
9160	Cassandra klijent port
9142	Podrazumevano za native_transport_port_ssl, korisno kada us potrebne i šifrovane i nešifrovane veze

Praktična primena



Praktična primena-mere sigurnosti nad bazom podataka

```
# - PasswordAuthenticator relies on username/password pairs to authenticate
#   users. It keeps usernames and hashed passwords in system_auth.roles table.
#   Please increase system_auth keyspace replication factor if you use this authenticator.
#   If using PasswordAuthenticator, CassandraRoleManager must also be used (see below)
authenticator: PasswordAuthenticator

# Authorization backend, implementing IAuthorizer; used to limit access/provide permissions
# Out of the box, Cassandra provides org.apache.cassandra.auth.{AllowAllAuthorizer,
# CassandraAuthorizer}.
#
# - AllowAllAuthorizer allows any action to any user - set it to disable authorization.
# - CassandraAuthorizer stores permissions in system_auth.role_permissions table. Please
#   increase system_auth keyspace replication factor if you use this authorizer.
authorizer: CassandraAuthorizer

# Part of the Authentication & Authorization
```



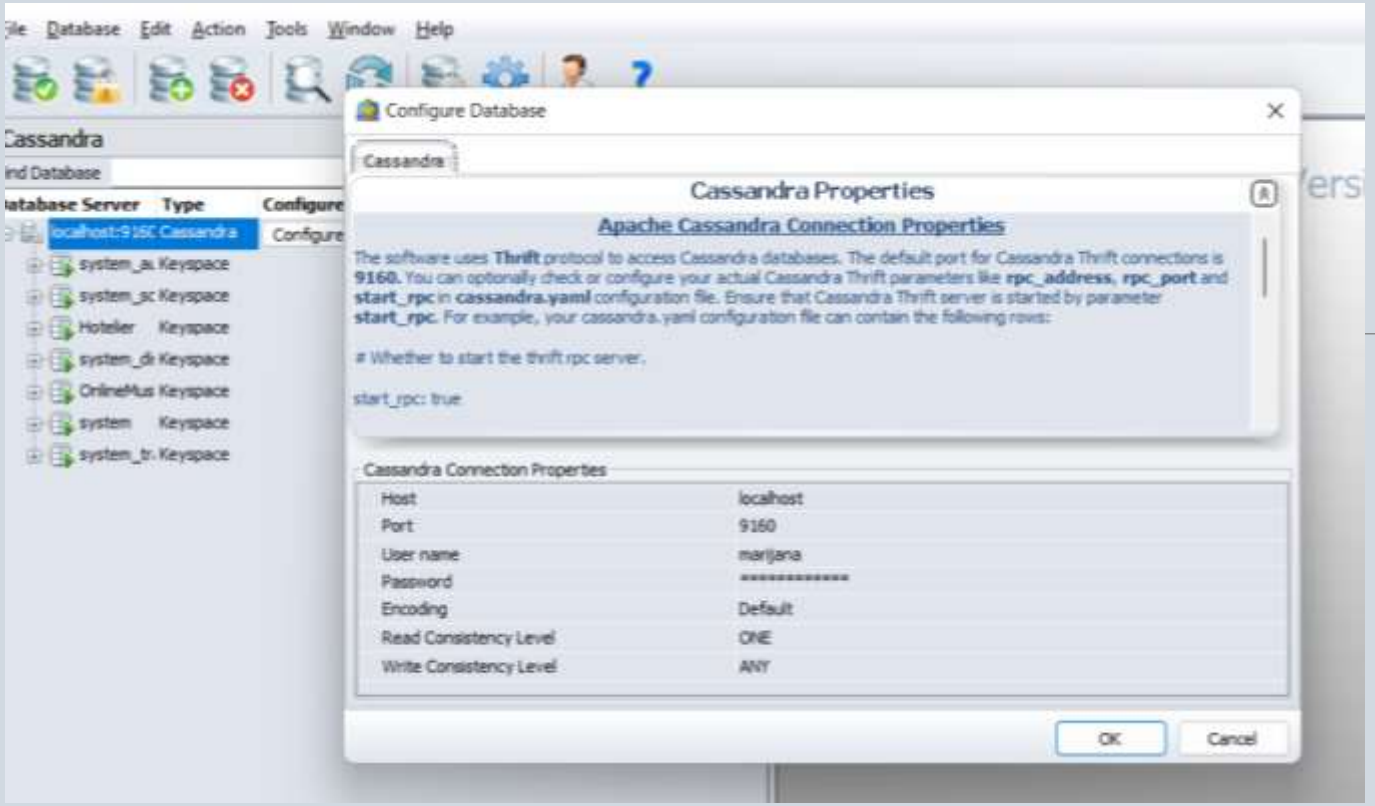
```
ALTER USER cassandra WITH PASSWORD 'cassandra123'
```

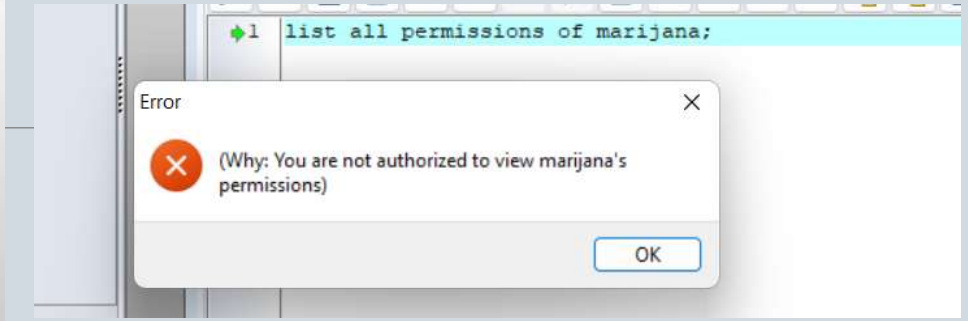
```
CREATE ROLE marijana WITH PASSWORD = 'marijanaa123' AND LOGIN = true;
```

```
CREATE ROLE base_admin WITH PASSWORD = '1234abcd';
```

```
GRANT ALL PERMISSIONS ON KEYSPACE “OnlineMusicConcert” TO base_admin;
```

```
GRANT base_admin TO marijana;
```






```
CREATE ROLE base_analyst WITH PASSWORD = 'zyxw9876';
****GRANT SELECT ON TABLE OnlineMusicConcert.koncert TO base_analyst;
CREATE ROLE second_analyst WITH PASSWORD = 'Iget2seeAll';
****GRANT SELECT ON TABLE OnlineMusicConcert.koncert TO second_analyst;
GRANT second_analyst TO base_analyst;
CREATE ROLE jovan WITH PASSWORD = 'jovan123' AND LOGIN = true;
GRANT base_analyst TO jovan;
```

HVALA NA PAŽNJI!

Marijana Cvetković, br. ind. 1431