



# PENERAPAN ENKRIPSI & PROTEKSI DATA PADA NON RELASIONAL

RPL318 – KEAMANAN BASIS DATA - PRAKTIKUM

## TUJUAN PEMBELAJARAN

Mahasiswa mampu menerapkan praktis dari prinsip-prinsip keamanan pada basis data non-relasional

# I. CONFIGURING AUTHENTICATION / AUTHORIZATION

Lakukan perubahan otentikasi pada `cassandra.yaml`

**Authenticator: PasswordAuthenticator**

**Authorizer: CassandraAuthorizer**

**Role\_manager: CassandraRoleManager**

Setelah restart, default superuser credentials (yaitu username: `cassandra`, password: `cassandra`) akan diaktifkan.

Kemudian lakukan perubahan default password menjadi jenis password level 2

## 2. IMPLEMENT ROLE-BASED ACCESS CONTROL

Sesuaikan dengan Topik PBL

- Create user
- Create role
- Grant permissions to that role & user

## 3. ENCRYPTION

Implementasikan Enkripsi SSL di Cassandra, yaitu:

1. Client to Node Encryption. Pastikan Generate Keystore dan Truststore, kemudian modifikasi Configuration melalui `Cassandra.yaml` (`client_encryption_options`)
2. Node to Node Encryption. Pastikan Generate Keystore dan Truststore, kemudian pastikan certificate ke semua nodes, dan modifikasi configuration melalui `Cassandra.yaml` (`server_encryption_options`)



Jadikan proses praktikum ini menjadi Laporan praktikum dengan bukti screenshot baik proses dan resultnya.

Penamaan File:

Praktikum06-Nim-Nama.pdf