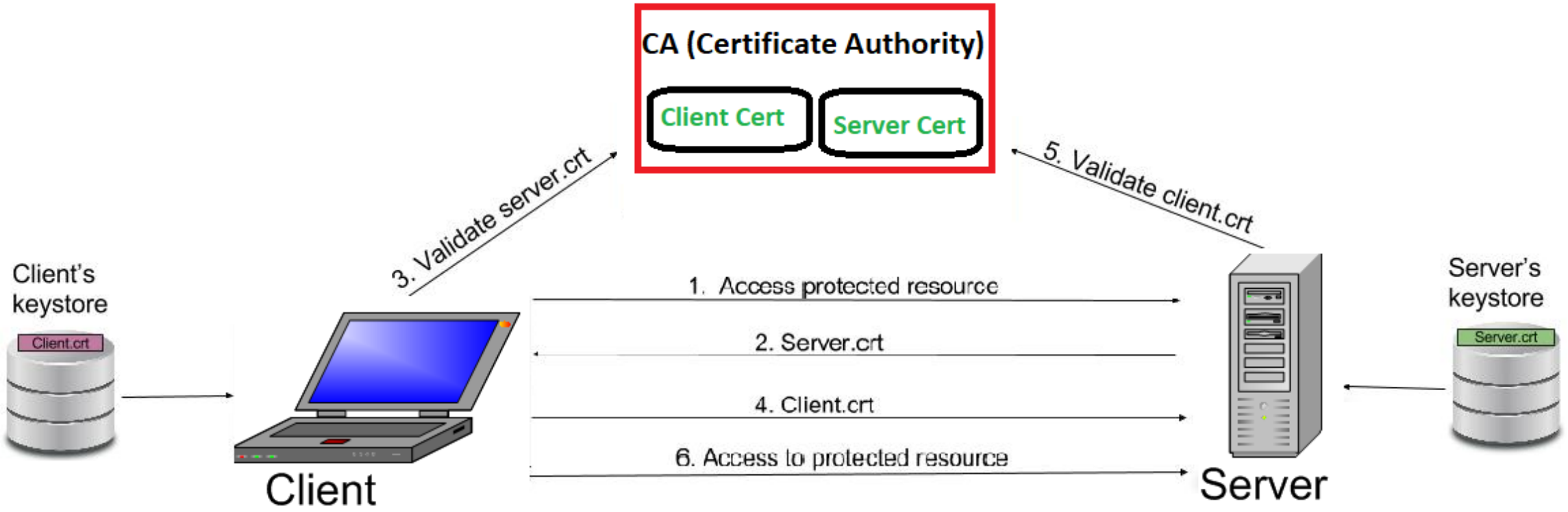
Securing Apache Kafka

Preparing SSL

Tos

1. Generate certificate (X509) in broker key store
2. Generate certificate authority (CA) for signing
3. Sign broker certificate with CA
4. Import signed certificate and CA to broker key store
5. Import CA to client trust store
6. 2-way authentication: generate client certificate in a similar way



Configuring SSL

Tos

- No client code change; just configuration change.

Client/Broker

```
ssl.keystore.location =
/var/private/ssl/kafka.server.keystore.jks
ssl.keystore.password = test1234
ssl.key.password = test1234
ssl.truststore.location =
/var/private/ssl/kafka.server.truststore.jks
ssl.truststore.password = test1234
```

Broker

```
listeners = SSL://host.name:port
security.inter.broker.protocol = SSL
ssl.client.auth = required
```

Client

```
security.protocol = SSL
```

Authorization

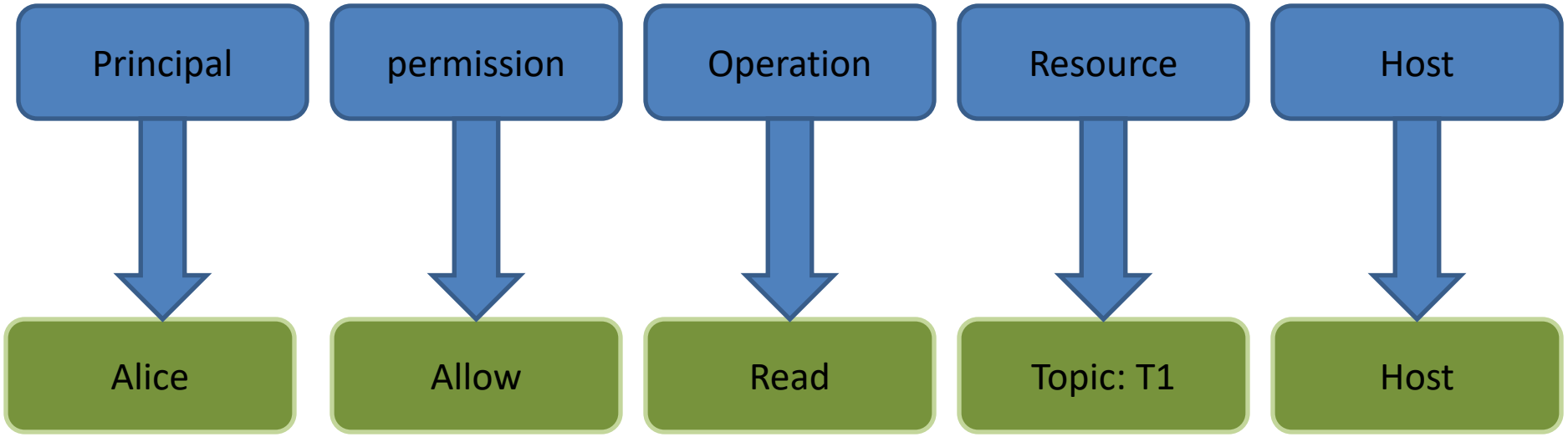
Tos

- Control which permission each authenticated principal has
- Pluggable with a default implementation

ACL

Tos

Alice is Allowed to Read from topic T1 from Host1



Operations and Resources

Tos

- Operations
  - Read, Write, Create, Describe, ClusterAction, All
- Resources
  - Topic, Cluster and ConsumerGroup

Operations	Resources
Read, write, Describe (Read, Write implies Describe)	Topic
Read	Consumer Group
Create, ClusterAction(communication between controller and brokers)	Cluster

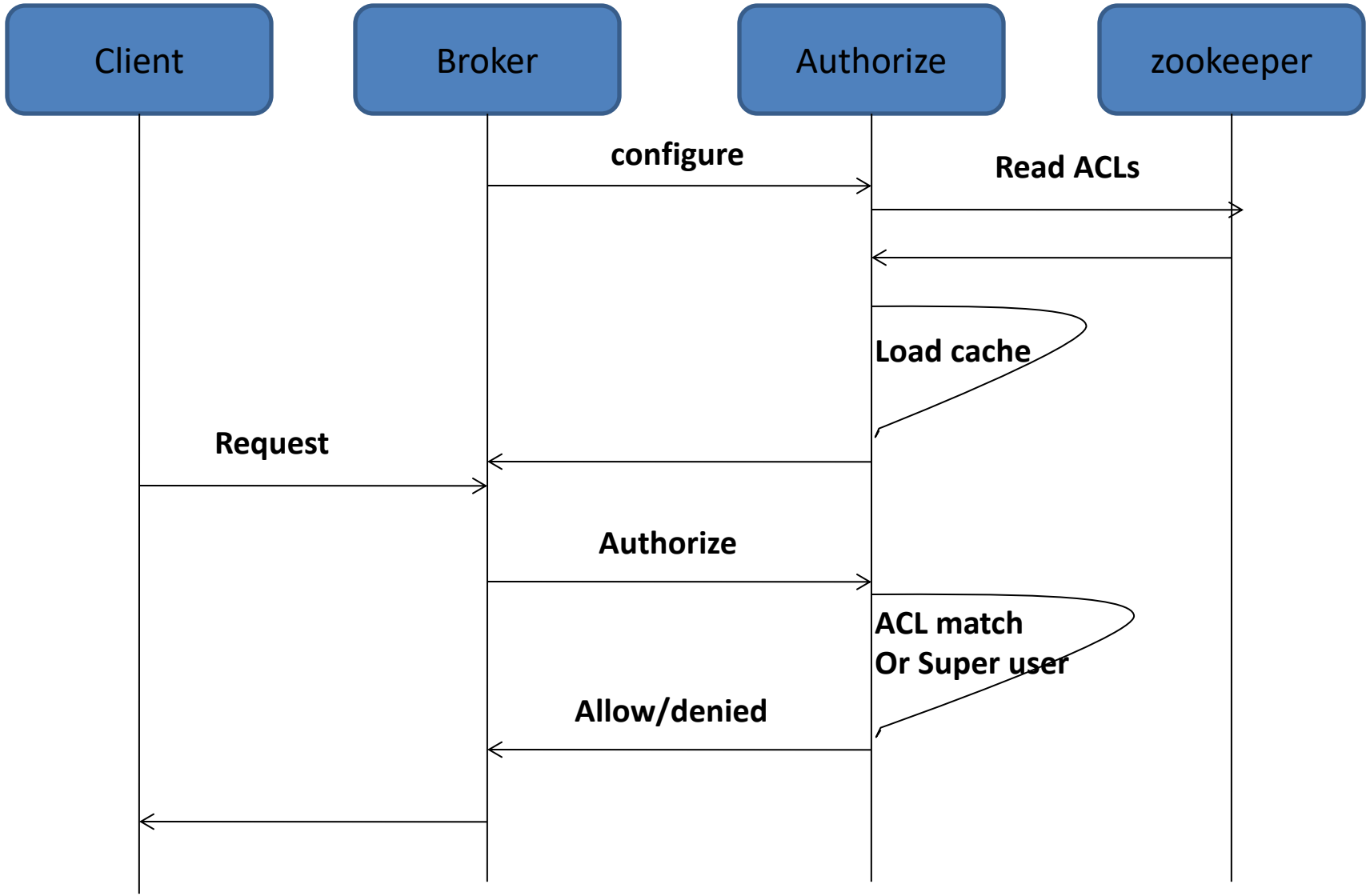
SimpleAclAuthorizer

Tos

- Out of box authorizer implementation.
- CLI tool for adding/removing acls
- ACLs stored in zookeeper and propagated to brokers asynchronously
- ACL cache in broker for better performance

Authorizer Flow

Tos



Configure broker ACL

Tos

- authorizer.class.name=kafka.security.auth.SimpleAclAuthorizer

- Make Kafka principal super users
  - Or grant ClusterAction and Read all topics to Kafka principal

Configure client ACL

Tos

- Producer
  - Grant Write on topic, Create on cluster (auto creation)
  - Or use --producer option in CLI

***bin/kafka-acls --authorizer-properties zookeeper.connect=localhost:2181 ***
--add --allow-principal User:Bob --producer --topic t1

- Consumer
  - Grant Read on topic, Read on consumer group
  - Or use --consumer option in CLI

***bin/kafka-acls --authorizer-properties zookeeper.connect=localhost:2181 ***
--add --allow-principal User:Bob --consumer --topic t1 --group group1

Lab : - Securing Kafka