Hazelcast Certification – Code Challenge

Design & Implementation

# Introduction

This document contains the technical description of the solution’s components.

The TPS scalability and latency, the sizing of the cluster and the

Durability and availability of the system is also discussed in this document.

# Design of distributed data structure

The distributed data structure selected for the solution is an IMap with a credit card number as the key of the entry and the list of its associated transactions as the value.



1. Map definition in ‘IMDGCertification’ class

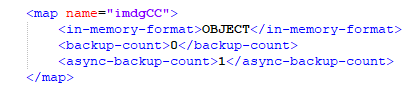
The main reason to use this data structure is that contains, in a single entry, all the historical transactions for a credit card. In consequence we assure that, when the fraud detector makes its calculations, the data needed is in the same member, so operations can be executed without the cost of extra network calls.

As map entries are not related among themselves there's no need to change Hazelcast default's partitions distribution.

As we are going to see in the next chapter of this document, an Entry Processor is used to perform the fraud detection process, this is the reason why it is used OBJECT as the in-memory-format in the Map in order to minimize serialization cost.

In the same way, the synchronous backup is disabled and a single asynchronous backup is configured to improve the speed of processing without losing data safety.

There is no a specific need to persist data so no map loader nor map store is used.

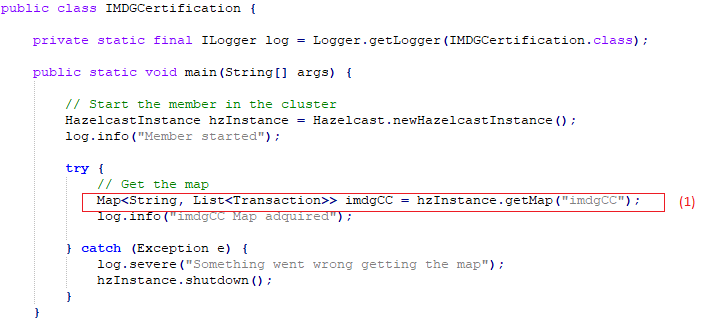


1. Map configuration in ‘hazelcast.xml’ configuration file

# Components used in the solution

## Cluster members

Cluster members are implemented by the **‘IMDGCertification’** class included in the ‘com.hazelcast.certification.cluster’ package.



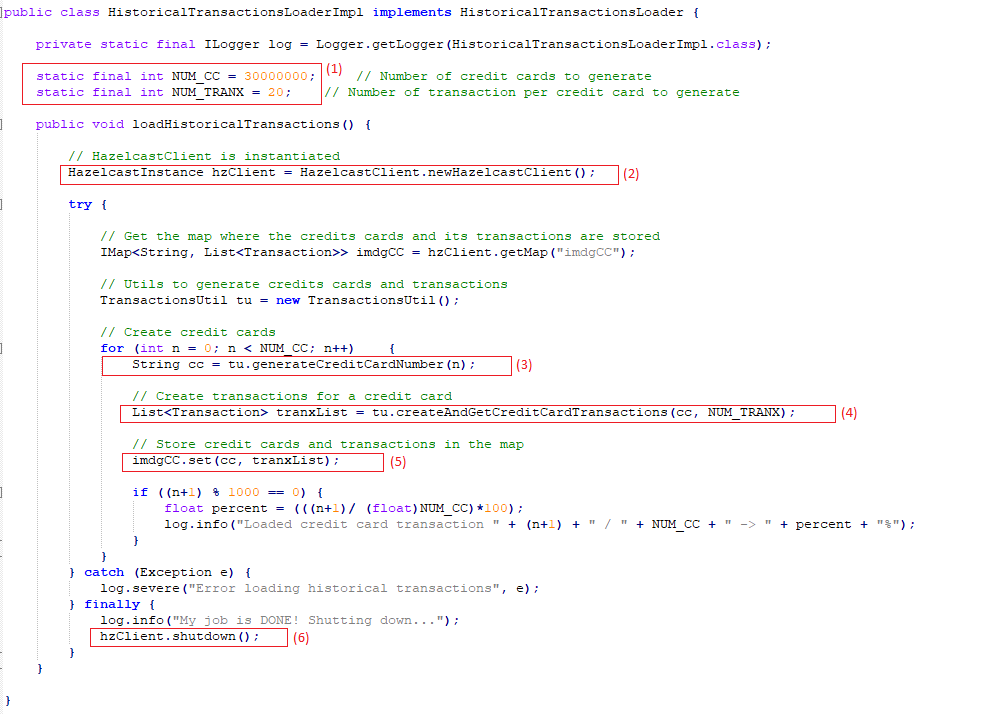
1. ‘IMDGCertification’ class

It’s a Hazelcast instance which its main objectives are: bring support to the IMap data structure described above and perform the fraud detection process using an Entry Processor. (1)

This class can be instantiated as many time as needed to achieve the optimal cluster performance.

## Historical transactions loader

Historical transactions loader process is implemented by the **‘HistoricalTransactionsLoaderImpl’** class included in the ‘com.hazelcast.certification.process’ package.



1. ‘HistoricalTransactionsLoaderImpl’ class

It’s a Hazelcast client that implements the **‘HistoricalTransactionsLoader’** interface, generating the historical data and loading it into the cluster’s Map. (2)

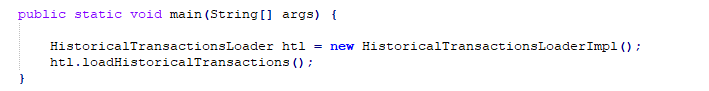
Credit cards numbers and historical transactions are generated using **'TransactionsUtil'** methods. (3) and (4)

The set method is used, instead of put, to store data in the Map to be more efficient because we don't need the stored value to be returned. (5)

Once all the data is stored in the Map the client shutdowns itself. (6)

The amount of data to load is controlled by the constants NUM\_CC and NUM\_TRANX. This is useful for testing purposes. (1)

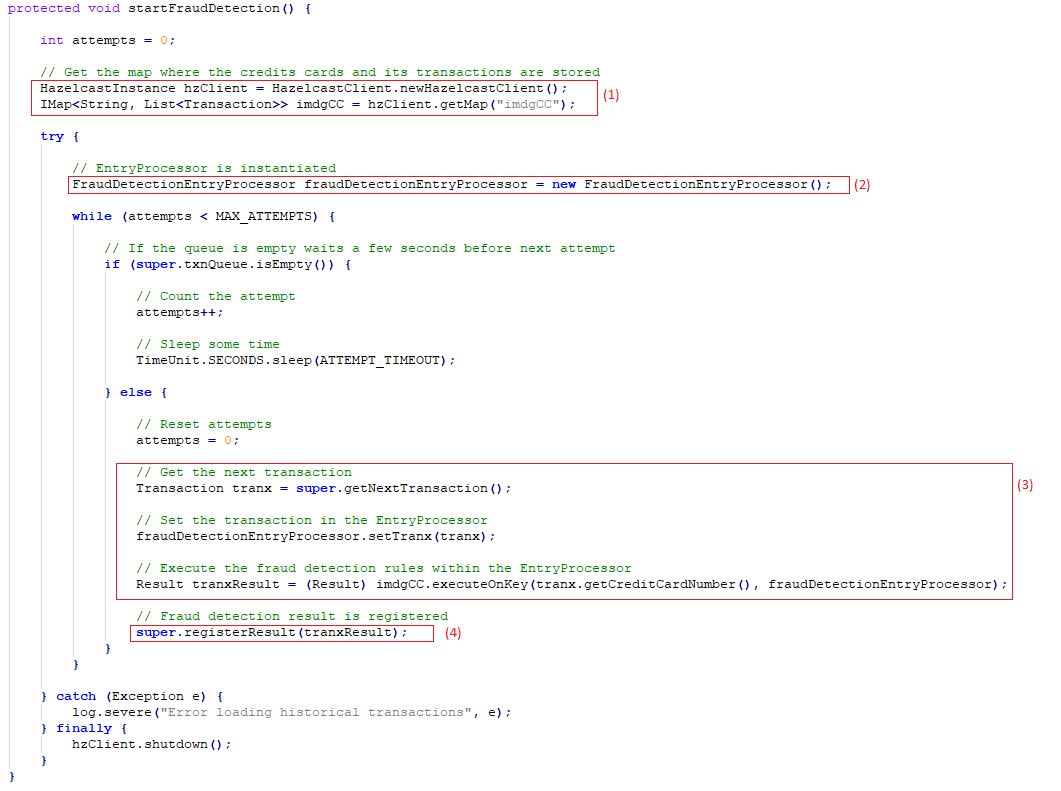
**‘Historical Transaction Runner’** class is in charge of putting the loader process in motion.



1. ‘HistoricalTransactionRunner’ class

## Fraud detection process

The business logic of the fraud detection process is implemented by the **‘FraudDetectionImpl’** class included in the ‘com.hazelcast.certification.process.impl.executorService’ package.



1. ‘FraudDetectionImpl’ class

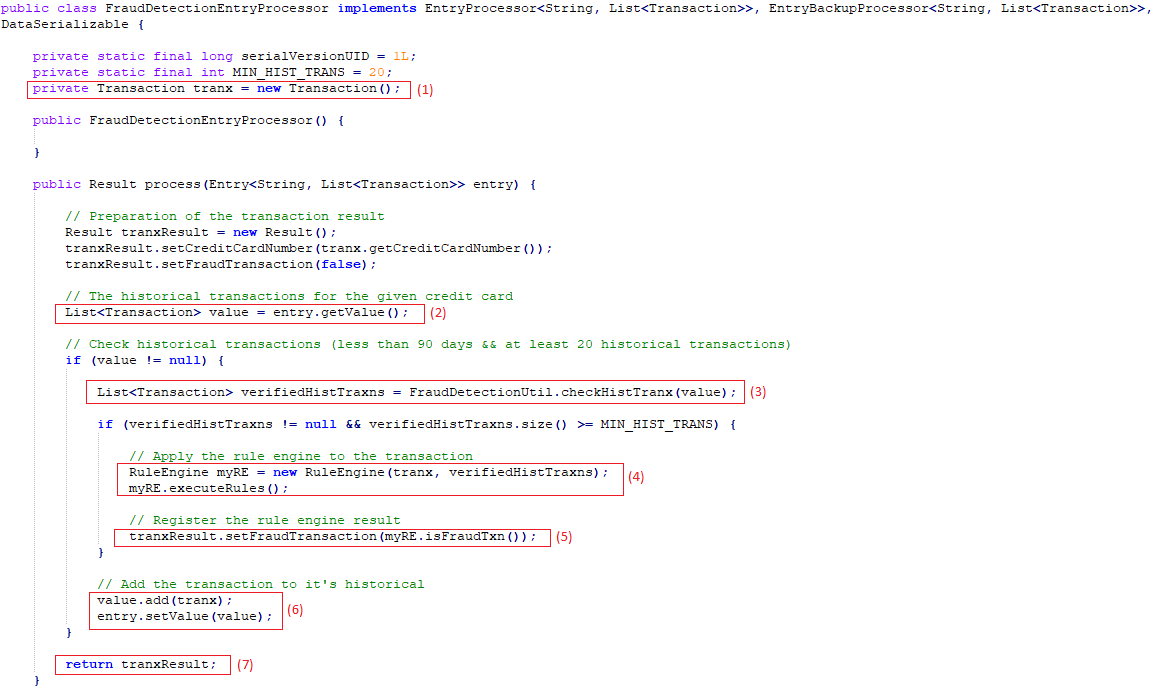
It’s a Hazelcast client that extents the **‘FraudDetection’** class, implementing the startFraudDetection method. (1)

Due that the fraud detection process basically consist on reading from the Map, modify the value, and putting the entry back in the Map an **Entry Processor** is chosen to perform this operations. The entry processor executes a read and updates upon the member where the data resides and this eliminates costly network hops. (2)

For each incoming transaction that is received from the transactions generator, the process sets the transaction in the entry processor and rely on it to execute the fraud detection process of the given transaction’s credit card number. (3)

The result of the fraud detection process is registered. (4)

The entry processor is implemented by **‘FraudDetectionEntryProcessor’** class and it’s applied on the key that contains the credit card’s transaction.



1. ‘FraudDetectionEntryProcessor’ class

As mentioned before, the Entry Processor contains the transaction that is going to be processed. (1)

The process verifies if the transactions of the entry’s credit card meets the requirements of number (at least 20 historical transactions) and age (with less than 90 days). To verify the age of the historical transactions a ‘checkHistTranx’ method is created in the **‘FraudDetectionUtil’** class and it is used by the entry processor. (2) and (3)

Historical transactions that don't meet the requirements don't participate in fraud detection process. The current transaction neither participates.

Rule engine for fraud detection process is provided with validated historical transactions of the credit card. (4)

The result of the fraud detection process is registered and the transaction is added to the collection of historical transactions of a credit card. (5), (6) and (7)

# TPS scalability and latency

Over time the system’s amount of data will grow and the fraud detection process will be more costly. For that reason it’s very important that the system can be easily scalable so it can have enough resources to store new data and perform the fraud detection operations with low latency.

Because cluster members are responsible for storing credit card and transactions data and performing fraud detection operations, the scalability of the system is achieved by being able to increase the number of cluster members or by increasing the resources (CPU, RAM) of existing members.

Adding new members to the cluster (horizontal scalability) is the easiest way using Hazelcast, since it allows increasing the total amount of RAM memory in the cluster to store more data and increase the capacity of transaction processing.

To maintain a low-latency system the configured backup is asynchronous as explained below in more detail.

# Sizing of the cluster to achieve a particular performance

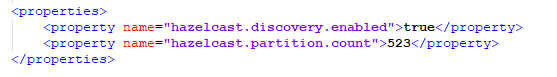
As detailed in appendix 1, the size of the initial amount of data that the cluster have to store is 51 GB approximately.

This implies that the minimum configuration of the cluster must allow the storage of those 51 GB of data plus those corresponding to the asynchronous backup that has been defined.

In addition, it is necessary to take into account the expected data growth so that the system can store them and perform the fraud detection operations.

To achieve a particular performance, the cluster has to be configured in such a way that the combination of RAM and processing capacity will allow to reach the objective.

On the other hand, we need to increase the partition count to the point where data load per-partition is under 100 MB. That gives us the number of **523 partitions**, which is also a prime number, and that’s mean that the data will be distributed to the members almost evenly.



1. Partition count in ‘hazelcast.xml’ configuration file

However, with 523 as partition count, the partition size is too close to the limit of 100 MB. A forecast of the projected data growth would be necessary to calculate to resize the number of partitions.

# Durability and availability of the application

As it was mentioned in the design of distributed data structure section, the map that stores the credits cards and transactions data is configured to have one asynchronous backup.

The backup allows to maintain a copy of the data and restore them if any member of the cluster goes down. As we want to prioritize performance over the backing up, the asynchronous backup is chosen because don’t block operations.

On the other hand the durability of the data is not ensure because no map store is used for data persistence. If all nodes fails or are shut down, the data will be lost.

# Success criteria completion

## Application must store 30 million credit cards before commencing Fraud Detection for incoming transactions

This criteria was accomplish in an Amazon AWS environment with 11 members of the clusters running the IMDG process (runIMDG.sh) and one client running the historical transaction loader process (runHistTxnLoader.sh). The 12 instance types used were m5.4xlarge with 16 vCPUs and 64 GB of RAM memory.

Credit cards numbers are generated using the generateCreditCardNumber method of the TransactionsUtil class within the historical transaction loader process (HistoricalTransactionsLoaderImpl.java).

## Each credit card must also have 20 historical transactions, generated in past 90 days

This criteria were accomplished along with the previous one by using the createAndGetCreditCardTransactions method of the TransactionsUtil class within the historical transaction loader process (HistoricalTransactionsLoaderImpl.java).

## Each incoming transaction that is received from TransactionsGenerator gets added to the collection of historical transactions of a credit card

FraudDetectionEntryProcessor class is the responsible to store the transaction received and processed to the historical transactions of the entry's credit card.

## Rule Engine for fraud detection process requires historical transactions (excluding current transaction) of a credit card. Therefore, RuleEngine must be provided with the current transaction that is received from TransactionsGenerator and all historical transactions of the same credit card

For every transaction received the FraudDetectionImpl class set the transaction into the FraudDetectionEntryProcessor class. The Entry Processor then gets the credit card of the transaction and uses it to obtain the historical transactions of the given credit card from the map. Transaction and historical transactions are provided to the rule engine to perform the fraud detection process.

## No historical transaction will be valid for more than 90 days i.e. any historical transaction that has passed its expiry must not participate in Fraud Detection process.

Once the FraudDetectionEntryProcessor gets the historical transactions, first it excludes the transactions with more than 90 days old (using checkHistTranx method of the FraudDetectionUtil class). Then it checks that the credit card has at least 20 valid historical transactions (not including the transaction given for fraud detection process).

## Result of every transaction that was read by invoking getNextTransaction() must be registered with the application (registerResult()) after running fraud detection process.

This was perform by the FraudDetectionImpl class.

# Appendix

## Appendix 1. Partition count calculation

### Historical data size

Number of credits cards: 30 million

Size of one credit cards: 14 chars \* 2 bytes = 28 bytes

**Total size of the credits cards: 28 bytes \* 30 million = 801 MB**

Number of initial transactions for each credit cards: 20 transactions

Size of one transaction: 90 bytes

* creditCardNumber: 28 bytes
* timestamp: 8 bytes
* countryCode: 6 bytes
* responseCode: 4 bytes
* txnAmount: 10 bytes
* txnCurrency: 6 bytes
* txnCode: 10 bytes
* merchantType: 8 bytes
* txnCity: 10 bytes

**Total size of transactions: (90 bytes \* 20 transactions) \* 30 million = 50,29 GB**

**Total size of historical data: 801 MB + 50,29 GB = 51,07 GB**

### Partition count

**Partition count: 51,07 GB / 100 MB = 523 partitions**