

UNIVERSITY PIERRE ET MARIE CURIE

INTERNSHIP INTER-REPORT

MASTER'S DEGREE

Java Driver for Apache Cassandra

Author :
Kevin GALLARDO

Supervisors :
University : Sebastien
MONNET
Company : Shannon
DENNIS

30 août 2015

Introduction

This inter-report describes the content of this internship made at *DataStax* , UK, London. The internship was supervised by Shannon Dennis (Senior Director Engineer) and Olivier Michallat (Software Engineer) on the *DataStax* side, by Sebastien Monnet (Associate Professor) and Julien Sopena (Associate Professor) on the University side.

The intern will be joining the Drivers and Tools Developers Team. The main tasks will be to contribute to the *DataStax Java Driver* for *Apache Cassandra* , he will help develop new features in the Driver, fix found issues, execute performance tests and resolve performance issues.

In this inter-report I will first make a description of *Apache Cassandra* including some additional research work on software technologies used by *Apache Cassandra* . Then, I will make a description of how the *DataStax Java Driver* works. After that I will describe the tasks currently achieved. I will finally conclude with making statement on what is envisaged to do for the rest of this internship.

Apache Cassandra

Apache Cassandra is a distributed No-SQL database created by *Facebook* providing high availability and scalability, developed to handle heavy workload produced by their large amount of users and data. *Apache Cassandra* has a master/slave-free architecture which allows it to provide linear scalability and helps instant recovery on hardware and software failures.

The purpose in the following is not to make an entire technical description of *Apache Cassandra* since on the one hand, the internship doesn't involve me on the internal development of *Apache Cassandra*. On the other hand, understanding all concepts of *Apache Cassandra* is crucial to be able to handle correctly the interaction with an *Apache Cassandra* cluster and thus, be as efficient as possible in the development of the *DataStax Java Driver*.

General Concept

With *Apache Cassandra*, each node on a cluster of machines is responsible of a part of the data. Thus, a set of data is represented by a Partition Key, and this Partition Key indicates on which node it will be stored, since at each node is attributed the responsibility of a range of Partition Keys. The data can (and is supposed to) be replicated among other nodes with a coefficient of replication that involves different policies of consistency and load balancing. All *Apache Cassandra* nodes will then refer to these policies to manage data among all other nodes.

Writing on a replicated data introduces consistency challenges and is handled in *Apache Cassandra* by broadcasting the write operations on all replicas and then waiting on a quorum of replicas to confirm that changes have been applied. A default setting on an *Apache Cassandra* node is to set this quorum's size to $N/2$ (N is the number of nodes owning a replica of the data). Reads on replicated data can be configured according to the client's requirements. Each Cassandra node is aware of all the other nodes, and each node is responsible of the replication of the data in his range of Partition Keys.

Advanced Description

The following section will describe more precisely some of the key features that allows *Apache Cassandra* to achieve its high availability and scalability characteristics.

We will also make some comparison with other database systems that have different behaviors regarding these characteristics.

Transactions

Apache Cassandra version 2.0 introduced a system to handle distributed transactions which, for instance allows clients using CQL operations like :

Listing 2.1– CQL Update Example

```
1 UPDATE ExampleTable
   SET variable = NEW_VAL
3 IF variable = OLD_VAL;
```

This *IF* condition may not be a big constraint when developing a relational database, but with a fully distributed database, this precondition causes several complications :

- How to achieve linearizability and consistency with distributed transactions ? Use Consensus.
- How to keep an acceptable throughput with a Consensus algorithm ? *Paxos* [1].

But, building these types of transactions involved the need to add some extra-phases to the original *Paxos* algorithm. Here we won't recall *Paxos* 's proofs that define the Consensus guaranties when a majority of nodes responds positively in the *Accept* phase. But original *Paxos* algorithm allows to agree on one value that won't be changed, besides that, what we want to do in *Apache Cassandra* is to achieve linearizability on a suite of operations (or we can say 'values'). Nodes would then be sure of the consistency of the data since every node would have executed operations on its replica in the same order.

To do so, a node must find a way to 'restart' the algorithm in order to make a new decision on another value and chain the algorithm executions. First way to do that would be to build a distributed edit log file based on successive Consensuses made with *Paxos* (a brief review of *Google's* solution to do that later). To chain *Paxos* execution in *Apache Cassandra* the idea has been to add an extra phase to the algorithm called *commit* phase which simply sends *commit* messages to all nodes to notify them the end of the algorithm.

Another point about using *Paxos* algorithm in our context is that our need is to execute a *compare-and-set-like* operation, whereas *Paxos* algorithm allows to only *set* a value without making the comparison.

Making this possible implied adding another extra-phase to the original *Paxos* algorithm, which is, after receiving a majority of responses from the *prepare* phase. The newly decided coordinator will send a request to all nodes to get their local value of the replica. If the expected value match, the node proceeds to the following of the algorithm (*accept*), if not, the algorithm stops and the value is not updated. With these solutions, *Apache Cassandra* simply implements *compare-and-set* distributed operations on multiple variables sequentially with the guaranties of the *Paxos* algorithm. With the cost of the overhead produced by the 2 extra-phases.

Google's distributed edit log file

Google's approach to build a distributed fault-tolerant database based on *Paxos* was described in their paper *Paxos Made Live*. It actually explains that even if *Paxos* algorithm could be easily described in one page of algorithmic instructions, engineering a production-ready software based on it, is not so simple.

Indeed, to be fault-tolerant an application has to rely on the hypothesis that a machine doesn't have unlimited memory, and that it can suffer of hard disk failures. Also, the implementation has to be adaptable to different hardware infrastructures since real systems are rarely specified precisely.

The approach taken here was to build a *fault-tolerant* log file that will describe the operations to be applied on a replica of data. All the replicas hosts would then agree with *Paxos*'s Consensus on the content of this log file and each one would keep locally a version of it. Building a file log of sequential operations implies to chain *Paxos* executions, which are called *instances* (the same idea described earlier for *Apache Cassandra*).

In order to increase throughput and performance of the *instances*, two additional concepts came up in the paper :

- When a coordinator sends data in an *Accept* message, it can concern not only one variable, and update multiple set of variables. So when the *Accept* message is acknowledged by a majority of nodes, all the values will be modified at the same time.
- To avoid as much *Propose* messages overhead as possible, the algorithm could state that a coordinator, once it has passed the *Accept* phase with his value on a previous instance, can stay *elected* for certain period of time. And thus, it can chain *Accept* phases for as long as he is coordinator. He is then called *master*. After that, when a node starts a new instance of *Paxos* algorithm, it first tries to grant a lease from the coordinator (*master*) of the last instance and sets it as his coordinator for this new instance.

Master leases doesn't corrupt the *Paxos* algorithm since a *master* is elected it can fail, and after a certain period of time (*heartbeats*), a new instance will be run and will elect a new *master*.

Besides that, *master leases* improve performance with the fact that when a *master* is elected by a majority of replicas, the *compare* of a *compare-and-set* operation on a *master* can be done locally since once it knows that it has been elected, the *master* knows no other node is going to acknowledge *Propose* messages from another coordinator. Each time a *Paxos* instance is ran, replicas *grant* a lease from the *master* of the previous instance. For *Google*, this implementation of *Paxos* was used as backend of *Chubby*, a *fault-tolerant master-slave* distributed locking system which during its computation stores *Chubby* lock files in a distributed database with replication, and that was then, using this implementation of *Paxos*. This way, *Chubby masters* and *Paxos masters* could be correlated to improve throughput of the application.

Since the log file concerns actions to be applied on a certain data structure, the data structure's history has to be saved, so as for the log file, in case of when a replica fails and has to recover. To handle limited memory restrictions, persistent state's history has been achieved by making *snapshots*. With a proper *snapshot* algorithm the data could be saved in a period of time related to the memory capacity and the log file can also be truncated since it only needs to contain the operations executed since the last *snapshot*.

Implementing these concepts and other technical details allowed to build distributed fault tolerant database relying on *Paxos* .

Apache Cassandra local persistence

To achieve local persistence of writes on data in the most efficient way, *Apache Cassandra* rely on some principles that helps acquiring better performance and safety. Each write operation involves a new entry in a local commit file. The write in this file is persisted and it is assumed in *Facebook's* paper on *Cassandra* that this commit file is stored on a dedicated hard disk used only for this purpose, to maximize throughput in regard of the sequential constraints of this one.

To optimize response time on a *read* request, *Apache Cassandra* first does a lookup in the in-memory data structure of most recent data, and if not present, do a lookup on persistent storage. Data is stored in many files on a disk, (ordered from newest to oldest) each part of the data represented by a key. To prevent browsing files that do not contain the needed key, each file owns an index which describes all the keys the file is composed of. This index is called *bloom filter*.

Gossip membership protocol and possible ATTACKS!

With *Apache Cassandra* , since the data is distributed and replicated, each node maintains locally the situation it is aware of each other node in the *ring* (the *ring* represents the nodes organized according the distribution of the tokens).

To maintain a coherent distribution of the tokens, in case of when a node fails, a membership protocol called *Gossip protocol* runs regularly to keep the ring coherent. In short, this protocol consists of : an *initiator* node starting a *gossip* round by sending a *receiver* node his current view of all the nodes. The *receiver* updates his view according to the initiator's view (assuming that there's a additional technical process that can insure that a view is more recent than another). And if the view also needs to be updated on the *initiator*, the *receiver* sends the updates in an *ack* message. The *initiator* then updates his views and acknowledges them to the *receiver*.

After explaining that this protocol brings a great benefit to the consistency of the system, we will see that some experiences proved that in some cases it can also become a weakness...

This[3] paper explains the vulnerabilities to such a protocol, stating that, in the *gossip* protocol, there is no concern about the about what could happen if the information in these *gossip* messages are false, corrupted. With this statement, we can imagine 2 types of attacks involving a byzantine node that's purpose is to send wrong information among the network.

A first *attack* would be to make some nodes (even maybe all) believe that a node is *down* while he is not. Sending a message to a *receiver* node, falsely up-to-date, saying that a node is *down* can lead the *receiver* node to update his view with a wrong information. The second *attack* is the opposite of the first one, a byzantine node waits for a node to fail, and while the node is failed, the byzantine one sends *gossip* messages to every other saying that for it (the last updated view) the node is still up. This kind of *attacks* can have a big impact on the performance of the database when there's big loads of data to handle.

It could in the first case, contradict load balancing policies by lowering the usage of

the *faked* node, in the second case, involve a great number of lost requests. The paper reports a percentage of up to 83% of lost requests when disseminating up to 75% byzantine nodes in the network, using the *ALL* consistency level. It also describes a *relatively low* performance impact solution to the excess of trust in the *gossip* protocol. It consists in adding an encryption layer to the protocol, allowing to insure that information provided is not from a byzantine node. A little bit like Byzantine *Paxos* [4], with the cost of encryption.

Java Driver for Apache Cassandra

THE *DataStax Java Driver* defines a high level API to handle interaction with an *Apache Cassandra* node. The *DataStax Java Driver* is based on the CQL query language and communicates with a *Apache Cassandra* using the *Native Protocol*.

CQL

The CQL query language is a database query language dedicated to *Apache Cassandra*. Hence its goal is to fit the most possible to the existing universal *SQL* query language, and in the same time providing *Apache Cassandra* specific functionalities. With CQL a client can then set specific replication factor when adding data or consistency level in a query.

Native protocol

The *Native protocol* is a network applicative protocol built on *TCP*. The *Native protocol* is fully asynchronous, hence, on the driver side it allows to accumulate queries on a single connection without consistency issues. *Native protocol* also allows security functionalities like authentication and SSL encryption.

The *DataStax Java Driver* 's task is to interact with a node by encoding and decoding messages from a node using the *Native protocol*.

Connection

Connecting a client to a node with the driver is subject to many optimizations. To make a connection to a host, the top-level API for a client is to use an object named *Session*. The *Java driver* aggregates this object with *Connections*. When a *session* is created, the driver established connections to all nodes of a cluster (discovering the list of hosts relies on the *gossip*). In addition to that, the *Java driver* creates a *pool* of connections on each node. This is made for multiple purposes : if a connection is closed, we can rely on another connection from the pool to keep communicating with a node. Also, because the *Native protocol* is asynchronous, we can pile up multiple requests on a connection, but with a limit number of maximum requests. If a client exceeds this limit, the pool provides another connection to enqueue new requests. Since the driver maintains connection on multiple hosts of a cluster of nodes, we can define policies to balance requests among all the nodes, and avoid bottlenecks. Getting together local connection informations to the hosts and *gossip* informations

helps keeping a consistent state of the nodes in the cluster. The driver also defines a set of different policies like *retry on deconnection* policies.

Processing responses

The *Native protocol* being fully asynchronous, a client has the possibility to process results of its queries either synchronously or asynchronously. Internally, everything is handled asynchronously, every request implies the creation of a *Future* object from the Java API's Future interface. On these *Futures* we define callbacks to fill the data when a connection notifies its activity. Since internal processing in the driver is asynchronous, most part of the code is multi-threaded and thread-safe.

Achieved work

The main purpose of this internship at DataStax is to contribute to the active development of the open-source *DataStax Java Driver* for *Apache Cassandra*. This includes aggregating the client's API with new functionalities to fit *Apache Cassandra* functionalities, internal operation of the driver, improving Query Builder¹ and Object Mapper² functions, resolving reported internal driver's issues and suggestions. I will then, give a brief description of some of the most significant tasks I have been working on since now. I have also been assigned to build a new *DataStax*'s tool called *Cassandra Detection Tool* (described later).

Java-Driver

Refactoring Integration Tests Class

The test architecture for the *DataStax Java Driver* is composed of both unit and integration test. Those test are ran 24/7 for continuous integration by *Jenkins* servers. To simplify building these tests, a big number of integration tests are classes that extend an *all-configured* class which has the responsibility to create the necessary connections and configurations with a test cluster using DataStax's specific tools for automating *Apache Cassandra* cluster creation.

The previous behavior was that inheriting this all-configured implied the need to recreate a new cluster each time. The process was simplified by creating a generic class that initiates a cluster and stays instanciated for all classes inheriting it, adding a thread-safe need for this class. Integration tests suite runs approximately 30% faster.

Manual Paging

Requests on *Apache Cassandra* that generate a large amount of data are transferred in network applicative frames called *pages*. These pages are identified by *Apache Cassandra* and are communicated through the *Native protocol*. The goal of this improvement was to give client the possibility to handle themselves the *paging state* of a request. Thanks to his *paging state* the client start fetching some data from the server, stop processing, and re-send a new request but with the *paging state* information

1. Query Builder is a library developed for the Java Driver allowing clients to build query in an Object Oriented way. Example : `Statement statement = QueryBuilder.select().all().from(keyspace, table);`

2. Object Mapper is an Object Relational Mapping tool developed for the Java Driver.

which allows him to continue its processing from where he had stopped. Giving the possibility to the driver to be used in a entirely stateless environment. This task involved studying *Native protocol* and gathering information by manually decoding frames, changing the internal use of the *paging state* in the driver and understanding *Apache Cassandra* 's usage of the *paging state*.

Asynchronous host pools creation

Until now, creating a pool of connection to a *Apache Cassandra* node was all made sequentially. Moreover, making an authenticated connection on a *Apache Cassandra* cluster implies a certain overhead due to password verification. Therefore, when the driver has to make sequentially a pool of authenticated connections it could imply too much latency on a cluster with a large number of nodes.

The solution was to make the pool creation entirely asynchronous. Thus, all connection pools are made in parallel, and the driver worker only have to wait for all connections to be established. Since we are in a HIGHLY concurrent part of code, lots of issues were produced when adding this feature and needed a big part of refactoring of code. Temporary tests report a improvement 8x the time for the driver to connect to a 40 nodes cluster.

Cassandra Detection Tool

Cassandra Detection Tool is a software I have been asked to contribute to that's main function is to provide to customers all useful *Apache Cassandra* information we can gather concerning a given a range of IPs. Customers owning a (*very*) large number of clusters among its network sometimes isn't even sure how much nodes are running. *Cassandra Detection Tool* makes then, a clean and concise description of the *Apache Cassandra* instances. A first prototype of the tool has been made by *Martin Van Ryswyk*, our Executive Vice President in Engineering, and my work have been to build a final working solution of the software.

It turned out that I changed almost all the code conserving the original conception design. Technically the process was to first, use asynchronous Java sockets to try to establish connection on all of the given IP, all tries made in parallel. Thanks to that the software could establish a list of UP nodes running a *Apache Cassandra* instance. Moreover, the app use the *DataStax Java Driver* and the *Java Thrift API*³ to connect to running hosts and gather all the node information possible. Information concerns : token map, cluster's hosts, keyspaces and all types of versions. To be more efficient in case of a *big* list of hosts (we can aim for a class B network) to connect to, the application creates a dynamic sized thread pool and then tries to use drivers to gather information. Also, to avoid the need for a thread in the pool (*worker*) to have to, let's say, send gathered information to a main worker that processes all the results and etc... the information was stored in *static* (shared) data structures so it was highly concurrent because a certain number of nodes can be located on the same cluster,

3. Apache Thrift is a network applicative protocol originally used for Cassandra but got replaced by the Native protocol because of performance issues and also because the Java API for Thrift was really hard to use and not well designed. It is still available (but not updated) and Deprecated but I use it here for compatibility with clusters potentially using an old version of Cassandra.

and modifying the list of nodes in this *Cluster* object has to be doable concurrently. As a result, the code is thread-safe.

It was great to have the opportunity to build this software on my own, and also I'll have the chance to make a video presentation to clients and sales team people on how to use the software (even though I tried to make a GUI as clean as possible).

What's next

For the following of the internship I will continue to contribute to the *Java driver* bringing new functionalities and trying to understand more and more of its code in order to be able to handle more easily the development process.

Bibliographie

- [1] Leslie Lamport. *Paxos Made Simple*. ACM SIGACT News (Distributed Computing Column), 2001.
- [2] Tushar Chandra, Robert Griesemer, Joshua Redstone. *Paxos Made Live - An Engineering Perspective*. June 20, 2007.
- [3] Leonardo Aniello, Silvia Bonomi, Marta Breno, Roberto Baldoni. *Assessing Data Availability of Cassandra in the Presence of non-accurate Membership*. University of Rome, Italy, 2013.
- [4] Jean-Philippe Martin, Lorenzo Alvisi. *Fast Byzantine Paxos*.