Data Provenance for Multi-Database Servers Enterprise Architecture

James R. Tapsell - Supervised by: Konstantinos Markantonakis and Raja Naeem Akram

Information Security Group, Smart Card and IoT Security Centre

ROYAL HOLLOWAY UNIVERSITY OF LONDON

The Smart Card and Internet of Things Security Centre

Objectives

This project builds upon my earlier work[1] on collecting provenance information from MongoDB, adding the following aims:

- Collection in clustered environments.
- Low overhead to the overall cluster
- No single point of failure

Introduction

The previous project[1] recorded provenance for a single server database. This worked well but a large amount of systems now use multiple servers in a cluster. This gives the following benefits:

- Data is not lost if a single server dies
- Data can be sharded to allow for more data than 1 server can hold
- Multiple servers can be reading from replicated data at the same time
- Sharding can speed up queries
- Data can be replicated in different locations to reduce latency

The cluster automatically balances out the shards so that they are all used, preventing all of the data from being held on one shard which would decrease how effectively the resources are used as some nodes would be idle.

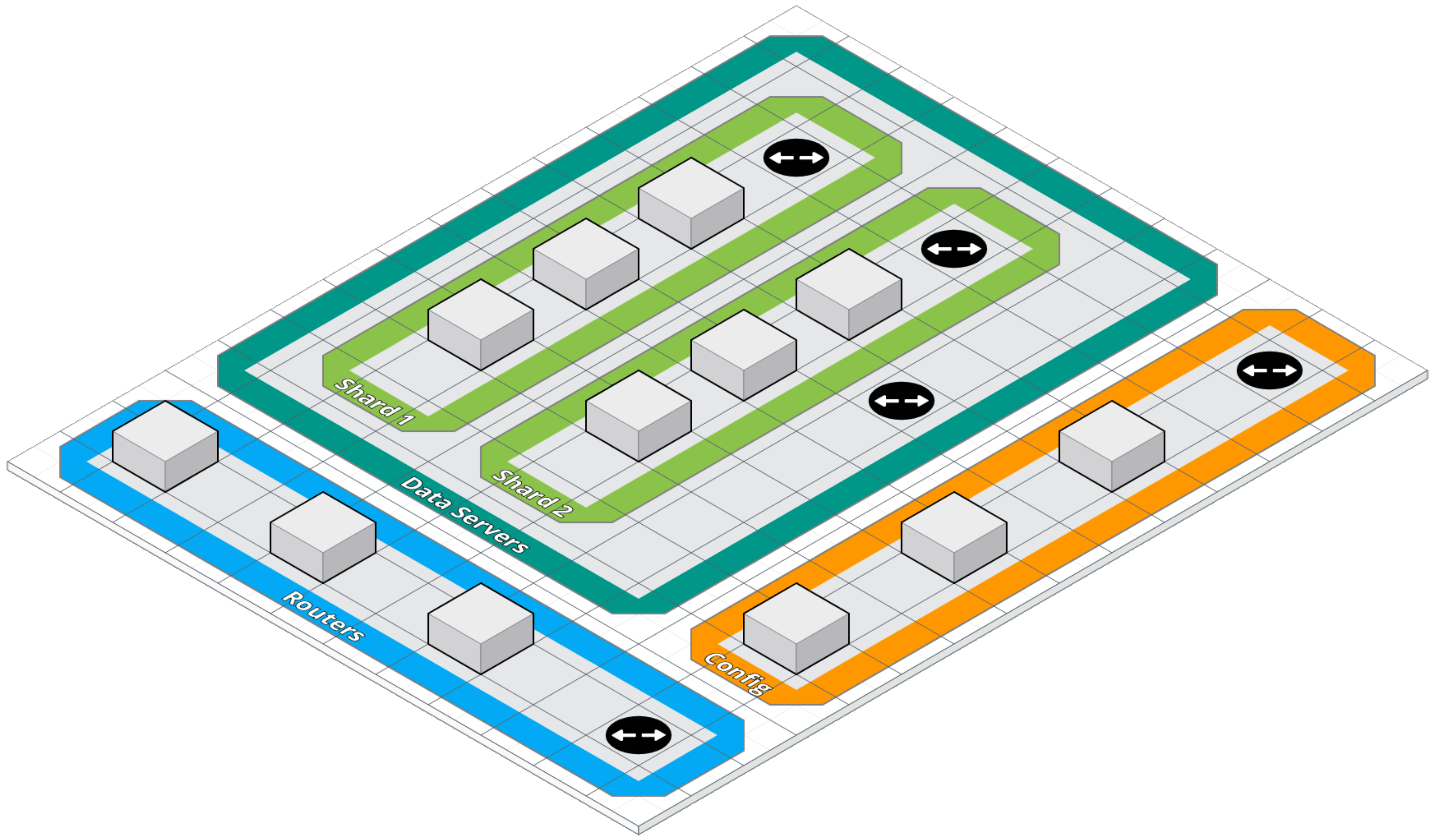
Demo Cluster

The demo cluster I used had the following configuration:

- Data servers - 2 shards, of 3 each servers each
- Configuration servers - 3 configuration servers
- Routers - 2 routers

This required 11 servers which were created as docker containers, spinning up these containers was controlled by Docker Compose, and configuring them once they existed was managed by a NodeJS script.

Cluster diagram



MongoDB Limits

The following limits are set by MongoDB.

- Nodes in a replica set[2]
  This is a hard limit at 50, although the amount of voting nodes is limited to 7
- Configuration sets per cluster[2]
  There can only be one configuration set, which has to keep to the limit for replica sets as well
- Shards per cluster
  This seems to have no limit (although the shard details do have to be stored in the configuration servers)
- Routers per cluster
  There appears to be no limit on this, routers just act as a proxy which allows access to the database

Provenance in Clusters

As the data and queries are spread over the shards, recording provenence on any of these shards would only give the provenance for that shard alone, rather than the whole cluster. In order to work around this limitation, provenance will be recorded in the router layer instead, where queries and answers are received and sent in a single transaction.

This still leaves the problem of keeping the nodes in sync, but this should be simple, as the nodes already need to have synchronised clocks. It should be less difficult to organise the events from however many routers are used, rather than from each single node in each shard individually.

Additional Information

This project is related to the EPSRC funded project *Data to Improve Customer Experience (DICE)*. The project is particularly interested in personal data, and is using rail passengers as a specific focus of interest. The overall aims of the project are:

- To understand the role that personal data plays in enhancing the user experience of rail passengers
- To develop technical solutions to data privacy
- To develop an evaluation framework that can be implemented so passengers can understand how their data is used and how they can control and verify its use

The project started in October 2016, and runs for three years to September 2019. For more information about the project, please visit the dice website[3].

References

[1] Blockchain data provenance - urop 2017 | james tapsell. *https://www.jrtapsell.co.uk/urop-2017-bc.html*.

[2] Mongodb limits and thresholds. *https://docs.mongodb.com/manual/reference/limits/*.

[3] Data to improve the customer experience (dice). *http://www.dice-project.org*.

Acknowledgements

We acknowledge the support of the ISG-SCC for the summer internship program and EPSRC funded project. The views and opinions expressed in this poster are those of the authors and do not necessarily reflect the position of DICE project or any of partners associated with this project.

Contact Information

- Web: www.jrtapsell.co.uk/intern-2018.html
- Email: papers@jrtapsell.co.uk