PART 3. DATA STORAGE AND FLOW MANAGEMENT

Sangmi Lee Pallickara
Computer Science, Colorado State University
http://www.cs.colostate.edu/~cs435

Today’s topics
- FAQs
- Dynamo: Key-Value storage

FAQs
- Why $O(\log N)$ for lookup process?
- Quiz 8?

Key Value Stores: Dynamo

This material is built based on,

(2) High Availability for writes

<table>
<thead>
<tr>
<th>Problem</th>
<th>Technique</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1) Membership</td>
<td>Consistent hashing</td>
</tr>
<tr>
<td>(2) High Availability for writes</td>
<td>Vector clocks with reconciliation during reads</td>
</tr>
<tr>
<td>(3) Handling temporary failures</td>
<td>Sleepy Gauss and reliablekadet</td>
</tr>
<tr>
<td>(4) Recovering from permanent failures</td>
<td>Archeology using Merkle tree</td>
</tr>
<tr>
<td>(5) Membership and failure detection</td>
<td>Group-based membership protocol and failure detection</td>
</tr>
</tbody>
</table>
Replication (1/3)

- Dynamo replicates its data on multiple hosts
  - Each data item is replicated at \( R \) hosts, where \( R \) is a parameter configured “per-instance”
- Each key \( k \) is assigned to a coordinator node
  - The coordinator is managing the replication of the data items that fall within its range
  - Stores at the \( R \)th clockwise successor nodes in the ring
  - Each node is responsible for the region of the ring between it and its \( R \)th predecessor

Replication (2/3)

Machine D will store the keys, \([A,B), [B,C), \) and \([C,D)\)

Replication (3/3)

- Preference list
  - The list of nodes that is responsible for storing a particular key
- Node failures
  - Preference list contains more than \( R \) nodes
- Virtual nodes can reduce actual number of machines in “\( R \) nodes”
  - The preference list for a key is constructed only by distinct physical nodes

Data Versioning

- Dynamo provides eventual consistency
  - Allows for updates to be propagated to all replicas asynchronously
  - A put call may return to its caller before the update has been applied to all the replicas

“Add to Cart” example

- The shopping cart application requires that an “Add to Cart” operation can never be forgotten or rejected
  - If the most recent cart is not available and user makes changes to an old version of the cart
    - Still the change should be meaningful and preserved
  - “add to cart” and “delete item from cart” should be translated into put operation to Dynamo
  - The divergent versions are reconciled later

Maintaining vector clock

- Dynamo treats the result of each modification as a new and immutable version of the data
  - Multiple version of data can be in the system
- Version branching
  - Due to the failure(s) in node(s), there are conflicting versions of an object
- Merging
  - Collapses multiple branches of data evolution back into one
  - Semantic reconciliation
  - e.g. merging different versions of shopping cart and preserving all of the items those client put into the cart
Vector clocks

- Used to capture causality between different versions of same object
- Two versions of object are on parallel branches or have a causal ordering
- Vector clock
  - A list of (node, counter) pairs
  - One vector clock is associated with every version of every object

Definition of the vector clocks

- $VC(x)$ denotes the vector clock of event $x$
- $VC(x)_z$ denotes the component of that clock for process $z$
- $x \rightarrow y$ denotes that event $x$ happens before event $y$
- If $x \rightarrow y$, then $VC(x) < VC(y)$

$$VC(x) < VC(y) \iff \forall z \left[ VC(x)_z \leq VC(y)_z \right] \land \exists z' \left[ VC(x)_z < VC(y)_{z'} \right]$$

Examples

- $VC(D1)=([Sx, 3], [Sy, 2], [Sz, 2], [Sq, 2])$
- $VC(D2)=([Sx, 3], [Sy, 2], [Sz, 2], [Sq, 1])$
- $VC(D3)=([Sx, 3], [Sy, 2], [Sq, 1])$
- $VC(D4)=([Sx, 3], [Sy, 3], [Sz, 2], [Sq, 1])$

- Is $VC(D1) > VC(D2)$? YES
- Is $VC(D3) > VC(D2)$? NO (VC(D2) > VC(D3) is not true as well)
- Is $VC(D4) > VC(D2)$? YES

Properties of the vector clocks

- If $VC(a) < VC(b)$, then $a \rightarrow b$
- Antisymmetry:
  - If $VC(a)<VC(b)$ then NOT $VC(b) < VC(a)$
- Transitivity
  - If $VC(a)<VC(b)$ and $VC(b)<VC(c)$, then $VC(a)<VC(c)$
Execution of **get** and **put** operations

- Users can send the operations to **any storage node** in Dynamo.
- Coordinator:
  - A node handling a read or write operation
  - The top $N$ nodes in the preference list
- Client can select a coordinator:
  - Route its request through a generic load balancer
  - Use a partition-aware client library
  - Directly access the coordinators

Using quorum-like system

- $R$: Minimum number of nodes that must participate in a successful read operation
- $W$: Minimum number of nodes that must participate in a successful write operation
- Setting $R$ and $W$:
  - $R + W > N$
  - $W > N/2$
- The latency of a get (or put) operation is dictated by the slowest of the $R$ (or $W$) replicas
  - $R$ and $W$ are configured to be less than $N$

**put request**

- Coordinator node
  1. Generates the vector clock
     - For the new version
  2. Writes the new version locally
  3. Sends the new version to the $N$ highest-ranked reachable nodes
     - Along with the new vector clock

**get request**

- The coordinator requests all existing versions of data for that key from the $N$ highest-ranked reachable nodes
  - In the preference list
  - Waits for $R$ responses
  - If multiple versions of the data are collected:
    - Returns all the versions it deems to be causally unrelated
    - The reconciled version superseding the current versions is written back

(3) Handling temporary failures

<table>
<thead>
<tr>
<th>Technique</th>
<th>Practice</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1) Partitioning</td>
<td>Consistent hashing</td>
</tr>
<tr>
<td>(2) High Availability for writes</td>
<td>Vector clocks with reconciliation during reads</td>
</tr>
<tr>
<td>(3) Handling temporary failures</td>
<td>Sloppy quorum and hinted handoff</td>
</tr>
<tr>
<td>(4) Recovering from permanent failures</td>
<td>Anti-entropy using Merkle tree</td>
</tr>
<tr>
<td>(5) Membership and failure detection</td>
<td>Gossip-based membership protocol and failure detection</td>
</tr>
</tbody>
</table>

Sloppy quorum

- All read and write operations are performed on the **first $N$ healthy nodes** from the preference list
  - May not always be the first $N$ nodes on the hashing ring
- Hinted handoff
  - If a node is temporarily unavailable, data is propagated to the next node in the ring
  - Metadata contains information about the originally intended node
  - Stored in a separate local database and scanned periodically
- Upon detecting that the original node is recovered,
  - A data delivery attempt will be made
  - Once the transfer succeeds, the data at the temporary node will be removed
Example

The data will be sent to the node D
If C is temporarily down
This data contained in C's metadata
node where it was supposed to be stored
After the recovery, D will send data to C
Then, it will remove the data.

What if W is 1?

- Applications that need the highest level of availability can set W as 1
  - Under Amazon’s model
  - A write is accepted as long as a single node in the system has durably written the key to its local store
  - A write request is rejected,
  - Only if all nodes in the system are unavailable

Anti-entropy protocol

- Replica synchronization protocol
- Hinted replica can be lost before they can be returned to the original replica node
- Detect inconsistencies between the replicas faster
- Minimize the amount of transferred data
- Dynamo uses Merkle tree

Merkle tree

- Hash tree where leaves are hashes of the values of individual keys
- Parent nodes are hashes of their respective children
- Each branch of the tree can be checked independently
  - Without requiring nodes to download the entire tree or dataset
- If the hash values of the root of two trees are equal
  - The values of the leaf nodes in the tree are equal
  - No synchronization needed

Uses of Merkle tree

- Merkle trees can be used to verify any kind of data stored, handled and transferred.
  - Used in a peer-to-peer network
- Trusted computing systems
  - Sun’s ZFS (Zeta File System)
- Git
- Cassandra and Dynamo
- Bittorrent protocol
How Merkle tree works

- Hash of Data 1: H1
- Hash of Data 2: H2
- Hash of Data 3: H3
- Hash of Data 4: H4
- Hash of (H1+H2): H5
- Hash of (H3+H4): H6

Top Hash: H13

How Dynamo uses Merkle tree

- Each node maintains a separate Merkle tree for each key range
- Two nodes exchange the root of the Merkle tree corresponding to the key ranges they host in common
- Node performs tree traversal and determines if there is any difference
- Perform the appropriate synchronization action

Disadvantage
- When a new node joins or leaves
  - Tree needs to be recalculated

How Merkle tree works for Dynamo

1. Compare Top hashes
2. If top hashes did not match, compare H5 vs. H13 and H6 vs. H14
3. If H6 and H14 did not match, compare H3 vs. H12 and H4 vs. H13

Ring Membership

- A node outage should not result in re-balancing of the partition assignment or repair of the unreachable replicas
- A node outage is mostly temporary

- Gossip-based protocol
  - Propagates membership changes
  - Maintains an eventually consistent view of membership

- Each node contacts a peer every second
  - Random selection
  - Two nodes reconcile their persisted membership change history

Logical partitioning

- Almost concurrent addition of two new nodes
  - Node A joins the ring
  - Node B joins the ring

- A and B consider themselves members of the ring
  - Yet neither would be immediately aware of each other
  - Logical partitioning
External Discovery

- Seeds
  - Discovered via an external mechanism
  - Known to all nodes
  - Statically configured (or from a configuration service)

- Seed nodes will eventually reconcile their membership with all of the nodes

Communication failure

- Attempts to
  - Communicate with unreachable peers during a `get` or `put` operation
  - Transfer partitions and hinted replicas

- Detecting communication failures
  - When there is no response to an initiated communication

- Responding to communication failures
  - Sender will try alternate nodes that map to failed node’s partitions
  - Periodically retry failed node for recovery