High-Availability Algorithms for Distributed Stream Processing

Jeong-Hyon Hwang, Magdalena Balazinska, Alexander Rasin Uğur Çetintemel, Michael Stonebraker and Stan Zdonik

Presented by: Anand Subramanian
anand@cs.uwaterloo.ca

Classical HA - DBMS

The Five Nines

*The five nines refers to how much percent of uptime you need per year.

<table>
<thead>
<tr>
<th></th>
<th>Percent Uptime</th>
<th>Downtime per year</th>
</tr>
</thead>
<tbody>
<tr>
<td>One Nine</td>
<td>90.000%</td>
<td>36 days per year</td>
</tr>
<tr>
<td>Two Nines</td>
<td>99.000%</td>
<td>3.65 days per year</td>
</tr>
<tr>
<td>Three Nines</td>
<td>99.900%</td>
<td>8 hours per year</td>
</tr>
<tr>
<td>Four Nines</td>
<td>99.990%</td>
<td>52 minutes per year</td>
</tr>
<tr>
<td>Five Nines</td>
<td>99.999%</td>
<td>5 minutes per year</td>
</tr>
</tbody>
</table>

The more nines, the higher the cost.
System Model

Node N_u is upstream of N
Node N_d is downstream of N

HA applied to DSMSs

- Types of Recovery
  - Precise Recovery – recover entire state of the “old” Primary node
  - Rollback Recovery – tends to be almost equivalent to being Precise (can produce duplication of tuples etc.)
  - Gap Recovery – dropping of state, data is tolerated

Gap Recovery

- Amnesia
  - Processing continues from the state when primary broke off...from empty state
  - …with state lost of course
  - Zero recovery time
  - Not useful if you want lossless HA or in a critical setup
Rollback Recovery

Passive Standby
- Recovery node receives a checkpoint, informs upstream node about its state
- Recovery node N requests N_u to resend tuples from its output queues

Upstream Backup
- Upstream neighbor acts as backup, logs tuples till they have been processed by N
- Secondary receives ACKs
- Secondary rebuilds Primary’s state based on logged tuples from upstream neighbor

Active Standby
- Secondary is active along with the Primary
- Secondary receives and processes tuples in parallel
- Secondary logs tuples in its output queues
- Upon Failover:
  - Secondary can continue processing tuples
  - But from which point?
    - high watermark associated with each tuple
    - Secondary queues are trimmed to omit duplicates
Results (Runtime overhead vs. recovery time)

Upstream Backup:
- Overhead ~0
- WINNER
- But
- Slowest recovery

Active Standby:
- 100% overhead
- BUT
- ~0
- Recovery time

Checkpointing interval: 25-50-100-150-200 ms

Discussions

- Failover Detection not accounted for – this is very important as a HA metric
- Mappings used for level-0 and level-1 ACKS add a lot of overhead – IGNORED
- For Active Standby – add a second set of indicators – lot of overhead again
- Focus should be only on recovery time, not overhead – given the powerful systems today
- Query network type/state experiments are unclear
- The state of the primary denotes much more than just the state of the operator queues and the last dequeued position - system buffers or caches that are used by the primary, scheduling of operators, resource usage states amongst a good many factors