Quiz 10: Highly Available Services

Due Jul 27 at 11:59pm **Points** 100 **Questions** 2
Available Jul 21 at 8am - Jul 27 at 11:59pm 7 days **Time Limit** 60 Minutes

This quiz was locked Jul 27 at 11:59pm.

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	27 minutes	45 out of 100

Score for this quiz: **45** out of 100
Submitted Jul 27 at 11:21am
This attempt took 27 minutes.

Question 1

15 / 50 pts

Suppose we are doing state machine replication with voting, allowing for up to F process failures.

1. How many replicas do we require to achieve a write quorum despite failures?
2. When can the client application report that the operation is finished? In other words, what is the commit point for the protocol?
3. Suppose the coordinator (for an update) and several replicas crash. What guarantees that at least one of the surviving replicas will know of the update?
4. Suppose two clients perform updates U1 and U2 concurrently on the same replicas. What guarantees that U1 and U2 will be delivered in the same order at all replicas?
5. What failure model does state machine replication with voting assume? Why may the protocol block?

Your Answer:

1. We require enough replicas to achieve Qw + Qr > F and Qw + Qw > F and that there are at least 1 of Qwrite and Qread.

2. The client application can report that the operation is finished and the protocol is at the commit point when all the group members voted at voted to commit the updates in timestamp order.

3. If a coordinator and several replicas crash, the surviving replicas will still have a pending vote/update for the process and won't discard it until it verifies that its vote wasn't counted.

4. If two clients perform updates U1 and U2 concurrently on the same replicas, the timestamp and version number of the updates guarantees that U1 and U2 are delivered in the same order at all replicas

5. State machine replication with voting assumes Byzantine failure model. The protocol may block because all machines need to be on the same update order.

1. 2F+1 replicas for a write quorum 2. Ack once a write quorum acks confirm/commit message from coordinator (client) at end of voting protocol 3. No more than F failures, but ack from write quorum ensures that at least one of the quorum survives with the update. 4. Voting protocol has servers in write quorums choose same timestamp for an update for all servers in its quorum. Since W + W > N, these write quorums must overlap, and one update has higher timestamp than the other update at all these replicas. 5. Assumes fail stop (or crash-stop) failure model. May block if a coordinator (client) crashes during the voting protocol.

Question 2

30 / 50 pts

Suppose we are using viewstamp replication, allowing for up to F process failures.

1. How many replicas do we require?
2. When does the primary server acknowledge the update back to the client?

3. Suppose the primary and several replicas crash. What guarantees that at least one of the surviving replicas will know of the update?
4. Suppose the new primary was not one of the replicas contacted by the old primary to perform the update. How will the new primary learn of the update?
5. What failure model does viewstamp replication assume? Why is this assumption necessary?

Your Answer:

1. Viewstamp replication requires 2f+1 replicas.

2. The primary server acknowledges the update back to the client when all replicas respond to the commit.

3. If the primary and several replicas crash, at least one of the surviving replicas still knows about the updates because they have an active log of the changes (like operation number) that they notify the new primary server once they reconnect.

4. The new primary learns of the new update by asking for a log from all the replicas and checking for the log that has the most recent updates.

5. Viewstamp replication assumes a crash stop failure model. This assumption is necessary because the primary server needs to read the logs of the replicas to know the most recent update number.

2. Ack once F backups acknowledge PREPARE message (so F+1 servers are prepared) 3. No more than F failures, but ack from primary means F+1 servers (primary and F backups) received the update, so there must be at least one surviving replica that has the update 5. Assumes fail stop failure model. This is necessary to avoid split brain problem of backup taking over while primary is still running.

Quiz Score: **45** out of 100