Amazon Web Services (AWS) customers rely on [Amazon Relational Database Service (Amazon RDS)](https://aws.amazon.com/rds/) to store their data for all kinds of workloads. For high availability (HA), you can use the Multi-AZ feature of Amazon RDS to provide additional resiliency by maintaining two copies of data across different Availability Zones (AZs).

Failures are rare, but as a best practice, applications should design around potential failures. The RDS Multi-AZ configuration is the recommended approach for production environments due to its ability to support low *RTO* (recovery time objective) and *RPO* (recovery point objective) requirements. RTO is the targeted amount of time for a recovery to complete in the event of failure. RPO is the targeted amount of time during which data is at risk for loss in the event of a failure.

**Single-AZ configurations** - With millions of active customers using AWS monthly, there are some customer workloads that do not require the level of HA provided by RDS Multi-AZ and the additional costs associated with it. These workloads might have more relaxed RTO and RPO requirements, and Single-AZ configurations might be sufficient to meet those needs.

**RTO** for recovery with an RDS Single-AZ instance failure can vary from minutes to hours. The duration depends on the size of the database and the failure and recovery approach required, as described later in this post.

**RPO** for recovery with an RDS Single-AZ instance failure is typically 5 minutes (the interval required for copying transaction logs to Amazon S3), but it can vary.

When we design and plan for failure with an RDS Single-AZ instance, we look at the following scenarios:

* **Recoverable instance failure** – The individual EC2 node suffered a hardware failure but could be recovered automatically by RDS.
* **Non-recoverable instance failure** – The individual EC2 node suffered a hardware failure but could *not* be recovered automatically by RDS.
* **EBS volume failure** – The EBS volume suffered a data loss failure.
* **Availability Zone disruption** – Failure at the Availability Zone level that would affect the RDS instance.

Multi-Site

Multi-Site is an active-active configuration DR approach, where in an identical solution runs on AWS as your on-site infrastructure. Traffic can be equally distributed to both the infrastructure as needed by using DNS service weighted routing approach.

In case of a disaster the DNS can be tuned to send all the traffic to the AWS environment and the AWS infrastructure scaled accordingly.

Preparation phase steps :

\* Set up your AWS environment to duplicate the production environment.

\* Set up DNS weighting, or similar traffic routing technology, to distribute incoming requests to both sites.

\* Configure automated failover to re-route traffic away from the affected site. for e.g. application to check if primary DB is available if not then redirect to the AWS DB

Somewhat this depends on your definition of RPO. Under most definitions of RPO it is the interval between backups and is measured in hours. It only applies to situations in which your live data is completely lost and you need to recover using a copy not maintained in real-time. Because the database also backs up the log file, RPO can be brought down to minutes (vs other kinds of data volumes). But the preferred mechanism is to use multiple synchronously maintained copies so that your RPO under all but the most extreme circumstances is 0.

If an RDS database instance's volumes were to be lost (logical or physical corruption), requiring recreating it from backup, then the RPO for Single-AZ, Multi-AZ, and even Aurora is typically around 5 minutes. That is the target interval for RDS to perform log backups to S3, so on a database volume loss you could have 5 minutes of log data that is also lost. There is no way to change the log backup interval, though that might be an interesting feature to add (hint: they would almost certainly have to charge for this as it would take a significant increase in resources behind the scenes to accomplish this at scale).

With Single-AZ the only live copy of your data is the EBS volume that holds the data for the instance. While EBS uses mirroring of data under the covers to provide durability and availability, there are several scenarios where you would have no choice other than to recover from backups. In this case you might want to apply the 5 minute log backup interval as your RPO.

With Multi-AZ the odds of data loss go way down because you have a separate synchronous copy of the volume being maintained in a separate data center (AZ). If your primary instance fails, you failover to the secondary instance with no data loss. There are far fewer scenarios where recreating the database from backup would be required, but there are still a few. Since volume-level replication is used, a corruption on the primary's volume may be replicated to the secondary's volume. And as rare as this scenario is, it would necessitate recovery from backups. I believe most customers think of Multi-AZ as having an RTO of 1-2 minutes and an RPO of 0, since they lose no data on any common failure. Again putting this into more traditional terms, even if a natural disaster were to destroy the data center housing the primary, the secondary would take over with no data loss. So assuming an RPO of 0 makes sense.

With Aurora the odds of data loss take another significant drop as it maintains 6 copies spread over 3 AZs, and it does that at a granularity of 10GB. So if something does become corrupt then it is a 10GB chunk of which there are 5 other copies plus backup information on S3, making it easy to transparently recover that one copy of the 10GB segment. There are almost no scenarios in which you would need to recreate the entire instance from backup. So truly an RPO of 0.

Bottom line is that I think for availability purposes RDS offers an RPO of 0 minutes. The next step would be to decide if you have a separate RPO for disaster recovery purposes, and what your disaster recovery plan looks like. Maybe it is just backups, or cross-region snapshot copies, or cross-region read replicas. None of these can achieve an RPO of 1 minute BTW, but DR strategies rarely require that.