Understanding RPO and RTO

Recovery Point Objective (RPO) and Recovery Time Objective (RTO) are two of the most important parameters of a disaster recovery or data protection plan. These are objectives which can guide enterprises to choose an optimal data backup plan.

The RPO/RTO, along with a business impact analysis, provides the basis for identifying and analyzing viable strategies for inclusion in the business continuity plan. Viable strategy options include any which would enable resumption of a business process in a time frame at or near the RPO/RTO.

At first glance these two terms appear to be quite similar. The best way to understand the difference between them is to associate the “RP” in “RPO” by imagining that they stand for “Rewrite Parameters” and the “RT” in “RTO” as “Real Time.”

RPO: Recovery Point Objective

Recovery Point Objective (RPO) describes the interval of time that might pass during a disruption before the quantity of data lost during that period exceeds the Business Continuity Plan’s maximum allowable threshold or “tolerance.”

Example: If the last available good copy of data upon an outage is from 18 hours ago, and the RPO for this business is 20 hours then we are still within the parameters of the Business Continuity Plan’s RPO. In other words, it the answers the question – “Up to what point in time could the Business Process’s recovery proceed tolerably given the volume of data lost during that interval?”

RTO: Recovery Time Objective

The Recovery Time Objective (RTO) is the duration of time and a service level within which a business process must be restored after a disaster in order to avoid unacceptable consequences associated with a break in continuity. In other words, the RTO is the answer to the question: “How much time did it take to recover after notification of business process disruption?”

RPO designates the variable amount of data that will be lost or will have to be re-entered during network downtime. RTO designates the amount of “real time” that can pass before the disruption begins to seriously and unacceptably impede the flow of normal business operations.

There is always a gap between the actuals – Recovery Time Actual (RTA) and Recovery Point Actual (RPA) – and objectives introduced by various manual and automated steps to bring the business application up. These actuals can only be exposed by disaster and business disruption rehearsals.

Some examples

Traditional Backups: In traditional tape backups, if your backup plan takes 2 hours for a scheduled backup at 0600 hours and 1800 hours, then a primary site failure at 1400 hours would leave you with an option to restore from 0600 hours backup, which means RPA of 8 hours and 2 hours RTA.

Continuous Replication: Replication provides higher RPO guarantees as the target system contains the mirrored image of the source. The RPA values depend upon how fast the changes are applied and if the replication is synchronous or asynchronous. RPO is dependent on how soon can the data on target/replicated site be made available to the application.

Learn more about cloud disaster recovery and how Druva brings together backup, disaster recovery and archival for data center workloads.

druva Sales: +1 888-248-4976 | sales@druva.com

Americas: +1 888-248-4976
Europe: +44 (0) 20-3750-9440
India: +91 (0) 20 6726-3300

Japan: japan-sales@druva.com
Singapore: asean-sales@druva.com
Australia: anz-sales@druva.com

Druva is the industry’s leading SaaS platform for data resiliency, and the only vendor to ensure data protection across the most common data risks backed by a $10 million guarantee. Druva’s innovative approach to backup and recovery has transformed how data is secured, protected and utilized by thousands of enterprises. The Druva Data Resiliency Cloud eliminates the need for costly hardware, software, and services through a simple, and agile cloud-native architecture that delivers unmatched security, availability and scale. Visit druva.com and follow us on LinkedIn, Twitter, and Facebook.