druva

The ultimate guide to achieving RPO/RTO

Definitions, calculations, and cloud data protection best practices

INTRODUCTION | DEFINING RTO — GETTING BACK TO BUSINESS | DEFINING RPO — HOW MUCH DATA CAN YOU LOSE? | ESSENTIAL FACTORS FOR CALCULATING RTO/RPOS | COST-EFFECTIVELY REDUCING RTO/RPOS | ACTUALS — TESTING IS IMPERATIVE | IMPORTANT TERMS AND ACRONYMS | OPTIMIZE RTO/RPOS WITH CLOUD DATA PROTECTION | ADDITIONAL RPO/RTO RESOURCES | CONCLUSION

Introduction

At some point, your organization will suffer outages and data loss because of a natural disaster, ransomware, or even a disgruntled employee. It's an inevitable part of doing business and as an IT professional, you know that preparing for the unexpected is one of your core responsibilities.

Your organization's data protection solution is what ensures that when that loss occurs, the impact on your business operations is minimal. To find the right solution that reliably and cost-effectively protects your valuable data, you need to fully understand two concepts:

- **Recovery time objective (RTO)** — how long you can afford to take to get systems up-and-running again after a loss event.
- **Recovery point objective (RPO)** — how much un-backed-up data your business can afford to lose because of a loss event.

Data protection solutions come in different shapes and sizes and your particular RTO/RPOs dictate the solution your organization needs. This eBook is an overview of what RTO/RPOs are and what they entail, the importance of testing, and a glimpse of how Druva's cloud data protection solves data protection challenges and optimizes RTO/RPOs, while reducing both costs and complexity.

Defining RTO — getting back to business

An RTO is a goal for how long it takes to resume a system after a loss event. It includes getting infrastructure and applications online as well as restoring lost data and files. If a burst pipe floods an on-premises data center, RTO includes the time it takes for repairs, move in new servers, get applications up, and reconnect with good data.

Typically, you'll have very different RTOs for different parts of the business. You'll set up different recovery tiers according to how important it is for a process to get back online:

- HR, PR, marketing? The RTO may be 12 hrs.
- Development and production? The RTO may be three hrs.
- Online sales and customer support? The RTO may be near zero.

An RTO doesn't include the time it takes to catch up with lost work and to straighten out whatever mess has been left behind from the loss. The RTO plus this work recovery time (WRT) equals the maximum tolerable downtime (MTD).

> **"When you come from a legacy background, a truly cloud-native solution can be difficult to wrap your head around. [Druva] is the only service we need for full and incremental server backups.**
>
> — CIO, Northgate Markets

Defining RPO — how much data can you lose?

A recovery point is the elapsed time between a backup and a loss event. Any data accumulated between the last backup and the loss event is unrecoverable. Generally speaking, your RPO is your backup frequency: if you back up every six hours, you stand to lose up to six hours of data. If a loss event occurs immediately after a backup, you're lucky.

Both RTO and RPO are measured in time, but RTO is about processes: getting things back on track. RPO is about data: ensuring you don't lose it, or at least don't lose too much. As with RTOs, you'll probably have multiple RPOs for different business processes. Your highest-priority, data-centric applications will have short or, perhaps, near-zero RPOs.

Of course, many will say, "I can't lose any of my data." This may well be true, but generally a useful RPO requires realistic assessments that consider both data and your budget.

> **"Thanks to the visibility Druva offers relating to all backups — VMs, physical file servers, Oracle and SQL databases, and EC2 instances — we were able to cut our backups in half, and, leveraging Druva's solution for Oracle, achieve a four times reduction in EBS storage consumption.**
>
> — Cloud Infrastructure Services Leader, Suez Water Technologies & Solutions

Essential factors for calculating RTO/RPOs

So how does your organization calculate these objectives? Ultimately, it takes spreadsheets of data that objectify value by business process and estimate detailed costs for their loss and remediation. It's not a simple or quick task. And it's not always necessary. If you approach the problem from the standpoint of optimizing your data protection architecture, optimal RTO/RPOs are likely to follow.

The factors that most effect calculating RTO/RPOs revolve around three components:

- **Storage** — on-premises hardware, offsite repositories, and private/public clouds.
- **Network speed and bandwidth** — LAN and WAN capacities.
- **Human factors** — complexity of tasks and degrees of automation.

Increasingly, IT groups are ensuring availability, while minimizing capital expenditures and maintenance overhead by moving data storage to cloud services such as AWS. This enables instant scalability with virtually infinite capacity for ever-increasing volumes of enterprise data.

In some instances, the trade-off for cloud storage is in network speed and bandwidth. Nothing is faster for restoring data than a cached backup on a server sitting next to your operations. Whether the incremental speed differential makes a significant difference for your RTO/RPOs depends on your particular needs and requires testing.

Unless you implement a highly automated cloud solution, human factors are critically important. Staff needs training, hardware has to be maintained, backup protocols need to be stringently adhered to, and your efforts will only be as strong as the weakest link — typically, human error.

> **"We tested the speed of SQL database backups and restores to remote offices and immediately found that Druva in the cloud was 30% faster to backup and restore than our on-premises [other vendor] grids.**
>
> — Senior Network Engineer, Premier Networks

Cost-effectively reducing RTO/RPOs

Can you achieve RTO/RPOs of zero? Yes (virtually), but it's expensive. A continuous availability architecture duplicates all operational components at least once. Business processes and transactions take place in at least two places simultaneously and if there's an outage at one site, business continues at another site without missing a beat. When was the last time you couldn't immediately buy something on Amazon?

For many organizations, near-zero RTO/RPOs are practical goals for highest-priority use cases such as web order entry or something involving highly regulated data. Still expensive, it's achievable using hardware such as flash storage arrays either on-premises or in the cloud.

RTO/RPOs measured in hours or minutes are adequate for most use cases and there are a number of ways to configure a solution. Cloud storage is almost always the most cost-effective approach for several reasons. You can take advantage of tiered pricing for high-availability hot, medium-availability warm, and cold storage. Note that for the hottest access, you can pay almost 100x what the coldest access costs.

> **"What we were interested in was something that was truly born in the cloud and was optimized to handle the efficiencies of cloud as an infrastructure.**
>
> — CIO, TRC Companies

Actuals — testing is imperative

Professional athletes spend much more time training and practicing than they do competing. Likewise, rehearsing and testing for outages is the only way to have real confidence in RTO/RPOs. Perhaps an application update in one system changed things in another, an infrequently accessed hardware connection failed, or a key team member left and an intern is filling in.

Simulating an IT failure or other disruption is the only way to expose the unexpected and fix shortfalls before a real loss event occurs. You have to test the storage, the network, and how well your staff is performing. And testing needs to occur regularly — at least several times a year.

Testing and trials are also the only way you can accurately evaluate the performance of a prospective data protection solution in your particular environment. Seeing the actual product working in your actual environment with your actual data is what counts. A trial run with whatever solution you're considering is essential to achieving realistic RTO/RPOs.

> **"Druva's backup technology is truly revolutionary. With its speed, scalability, and TCO savings, we now make decisions based on our business objectives rather than the restrictions of our legacy backup solution.**
>
> — IT Admin, AmorePacific

Important terms and acronyms

Any discussion of backup/restore, business continuity, or disaster recovery will include a number of concepts (and acronyms) you should learn:

- **Backup** — Maintaining copies of data in a separate environment.
- **Continuous availability** — Eliminating downtime using architectures such as massively parallel processing.
- **MTD** — Maximum tolerable downtime, how long operations can be down before incurring unacceptable losses. MTD = RTO + WRT.
- **Recovery** — Recovering select files or data needed to resume work.
- **Restore** — Restoring entire systems needed to resume operations.
- **RPA** — Recovery point actual, showing how accurate your RPO is when tested.
- **RPO** — Recovery point objective, how much business data your business can afford to lose because of a loss event.
- **RTA** — Recovery time actual, showing how accurate your RTOs are when tested.
- **RTO** — Recovery time objective, how long it really takes to restore systems after a loss event.
- **WRT** — Work recovery time, how long it takes for operations to "catch up" after systems and data have been restored.

> **Druva's built-in global deduplication, which is delivering a 10.5X reduction in storage for our hybrid cloud data, helps us reduce TCO.**
>
> — ISO, Network and System Administrator, Office of Governor Newsom

Optimize RTO/RPOs with cloud data protection

It's a mistake to calculate RTO/RPOs based on the limitations of legacy backup hardware. Rather, the solution must reliably enable your RTO/RPOs and protect your business needs. Fortunately, modern born-in-the-cloud applications have matured into services that protect all of your data and let you quickly recover content and restore systems.

Natively integrated with S3/AWS, Druva brings the simplicity and scale of the cloud to enterprise backup and data management, protecting all of your data across data centers, cloud applications, and endpoints.

The key benefits available with cloud-native Druva SaaS data protection include:

- **Reduced operational expenses and total-cost-of-ownership (TCO)** — consumption vs. subscription pricing; elastic auto-scaling and automated tiered storage; and no software maintenance and associated complexity.
- **Increased cyber resilience and compliance for all your data assets** — air-gapped, highly-available storage with the highest level of security; ransomware identification and forensics capabilities; and governance features to quickly find and act on sensitive data.
- **The ability to accelerate cloud projects globally** — robust interoperability with modern cloud tools and tech stacks; infrastructure readiness for new cloud apps; and, the ability to instantly scale for improved business agility.

Plus, organizations can speed RTOs by using geographically close storage resources. Druva is configurable in 15 AWS regions today including the AWS GovCloud (US).

> **"We reduced our backup time by 95 percent because of the simplicity and automation of Druva...**
>
> — Lead Infrastructure Engineer, Incyte Diagnostics

Additional RPO/RTO resources

Understanding RPO and RTO

Data management essentials: RPO and RTO

Why data backup in the cloud can help you reach your RPO/RTO

Understanding recovery objectives for enterprise data protection

Meet your recovery time objectives with Druva and AWS

RPO/RTO glossary page

> **Druva is a win-win for the district and for our team [...] We're using our budget wisely, and now we can spend time on strategic projects instead of troubleshooting backups.**
>
> — Network Engineer, Ellington Public Schools

Conclusion

Now you understand the basics of RTO/RPOs — what they are, how they're calculated, and how you can improve them. Also keep in mind that selecting the right cloud data protection solution is the most critically important factor in quickly getting back in business after disasters, ransomware, and other inevitable outages and data loss.

Druva's cloud-native approach to data protection enables the fastest RTO/RPOs at the least-possible cost regardless of your organization's data architecture. If your data demands continuous availability and on-premises backup hardware, the Druva cloud cache enables zero RTO/RPOs, while maintaining the 3-2-1 rule that dictates maintaining off-site backups. You can also eliminate on-premises backup hardware entirely, enabling optimal RTO/RPOs via automatically tiered AWS S3 storage.

Discover how Druva solves your data protection challenges with cloud-native expertise — reducing both costs and complexity.

Optimize RTO/RPOs and calculate your TCO savings with cloud backup

aws partner network

Advanced Technology Partner

- Storage Competency
- Digital Workplace Competency
- Government Competency
- SaaS Partner
- Marketplace Seller

aws marketplace

Find Druva in AWS Marketplace

Get started

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: +81-3-6890-8667
Singapore: +65 3158-4985
Australia: +61 1300-312-729

Druva® delivers Data Protection and Management for the cloud era. Druva Cloud Platform is built on AWS and offered as-a-Service; customers drive down costs by up to 50 percent by freeing themselves from the burden of unnecessary hardware, capacity planning, and software management. Druva is trusted by thousands of companies worldwide, including over 50 of the Fortune 500. Druva is a privately held company headquartered in Sunnyvale, California, and is funded by Sequoia Capital, Viking Global Investors, CDPQ, Neuberger Berman, Tenaya Capital, Riverwood Capital, and Nexus Partners. Visit druva.com and follow us on LinkedIn, Twitter, and Facebook.

Q122-20270