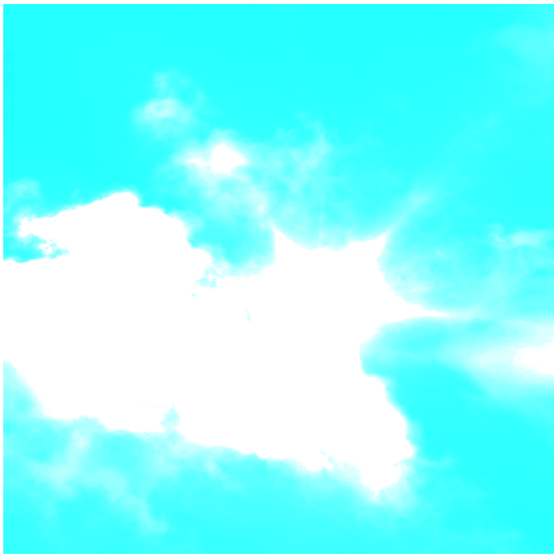
intronis
cloud backup + recovery

Measures of Success in Backup & Recovery



TECH GUIDE

Measures of Success in Backup & Recovery

Remote backup is one of the most popular items in a foundational service for many managed services providers (MSPs). The abilities to build comprehensive backup systems and ensure data is located across distributed physical locations are crucial challenges to many small and medium-sized business customers served by MSPs.

The service is becoming easier for MSPs to deliver, which means they have the option of working with vendors whose business models focus on hosted, online and cloud-based backup services aimed at SMB users and delivered via MSP channels.

While backup as a managed service is not commoditized, it has reached the point in the market at which simply offering the service is no longer a sufficient differentiator for most MSPs. Business continuity and disaster recovery (BCDR) is expected by clients and integral to the value MSPs provide in their overall practices.

How do MSPs demonstrate differentiated value in a service now seen as a market standard? The best method is to employ key metrics that monitor customer expectations and the recoverability of backed-up data. These metrics not only serve as vital underpinnings of a truly customized and highly valuable offering, they help MSPs explain and differentiate the value provided to their clientele more clearly than discussions of backup functionality and capacity.

Of BCDR performance and capability measures, the two that stand out for solution providers are recovery point objective (RPO) and recovery time objective (RTO). MSPs must understand these two key metrics to track and include them in their service-level agreements and put their unique stamp on this critical service.

In this tech guide, we will define the two backup measures, how they can be applied in a real-world context and how solution providers can use them as differentiators in their managed services practices.

HIGH COSTS OF DOWNTIME & LOST DATA

Given the high costs of downtime, a solid backup and recovery plan can drive a significant return on investment for customers. Recent studies show the average enterprise can lose more than $180,000 for each hour of data-center downtime (*Aberdeen Group, 2012*). Even small businesses can be on the hook for more than $12,000 (*Symantec, 2012*) in losses with just an hour's downtime. Those numbers are rising, with Aberdeen's research showing a 65 percent jump in the cost of downtime between 2010 and 2012.

If downtime is costly, data loss is downright devastating. Gartner research suggests only six percent of companies that suffer a "major loss" of data will survive two years, with 43 percent being put out of business immediately by such a loss.

Along with business concerns, an increasing number of regulations covers how much data must be retained and how quickly it must be handed over to authorities should the need arise. These regulations vary depending on industry/business sector (Gramm-Leach-Blilley Financial Services Modernization Act, Health Insurance Portability and Accountability Act) or can run across all businesses (Sarbanes-Oxley Act of 2002, The Patriot Act). These directives provide a baseline for backup requirements; customers' backup and disaster recovery plans must, at a minimum, meet regulatory requirements, which are increasing both in number and stringency.

MEASURING DATA PROTECTION

From the service providers' perspective, there are two main measurements for backup performance and value delivered:

RECOVERY TIME OBJECTIVE

RTO is the longest tolerable time a system, computer, application or network can be down after a failure or disaster before the business's operations are significantly impaired.

Different systems have radically different RTO measurements. It may be acceptable for a payroll system to be offline for a week or more, whereas sales order-processing systems being offline for a day could be catastrophic. Applied as part of a customer's SLA, RTO can express the maximum time a solution provider has to bring an application or system back online. Different applications or systems will have different RTO goals and should be based on individual customer requirements.

Determining appropriate RTO levels is key to developing a backup and disaster recovery strategy for a customer, and will call on a mix of knowledge of customer requirements and budgetary tolerances combined with deep understanding of the strengths and weaknesses of the backup and recovery options available on the market. Once these RTO goals are agreed upon, the solution provider can design and price services as part of an overall IT strategy for the customer.

RECOVERY POINT OBJECTIVE

RPO defines how much data a business can afford to lose – it is the time, relative to a disaster or failure, in which a business needs to recover its data.

There is usually much less variance with RPO than RTO; an organization that makes overnight backups will have an RPO for the end of the previous business day, meaning the most data lost as a result of a failure or downtime will be that generated between the previous day's backup and the time of the failure. But like RTO, different applications and business processes will have different levels of sensitivity.

For non-mission critical applications, losing a week's worth of data may be acceptable. For others, such as an enterprise resource-planning system, losing more than a few hours' worth of data – or any data at all – may be unacceptable.

Applied to a customer's SLA, RPO allows a solution provider to state the maximum amount of data that will be lost on a system-by-system basis in the event of an emergency. Determining appropriate and reasonable RPO goals for a customer depends on many variables, including the customer's business and budgetary needs and the available technology to support such goals.

OTHER CONSIDERATIONS

RTO and RPO do not necessarily reflect the importance of an application to a business and may be contingent on business processes. For example, a small business that receives most or all of its orders on paper and keys in ordering information at a later date may decide that having the last entries backed up as soon as they are entered is not necessary, as they still have paper-based backup should the application fail or data be lost.

COMBINING RTO & RPO

Applied together, RTO and RPO give a solution provider the ability to present in clear, contractual language the maximum amount of time a system will be down in the event of an emergency or disaster, and how much of the data produced or used by those systems will be preserved. They allow solution providers to document, in the form of an SLA, the answer to two of the most crucial questions customers will have on the protection of business systems and data.

When crafting a backup and disaster recovery policy, solution providers must consider the customer's tolerances and needs on an app-by-app basis. A checklist of major applications and application-driven business processes, complete with the company's tolerance for RTO and RPO, can determine the exact nature of the backup solution offered.

Doing a full rundown of the RTO and RPO requirements of a customer's infrastructure during initial business-impact assessments improves the value of the BCDR solution to the customer and helps the solution provider plan its investments and strategies to optimize margins for the services offered.

By showing the level of protection for critical data and the speed at which that data can be brought back in the event of an outage, solution providers are best able to demonstrate the return on customers' investment in backup and disaster recovery efforts.

BUILDING RTO & RPO INTO PROFESSIONAL SERVICES

To maximize the value, profitability and success of BCDR offerings, it is important solution providers think of BCDR not as a product sale, but as a complete professional service offering. The technologies used to enact BCDR services are important, but are merely tools in the hands of a skilled professional, as far as customers are concerned.

As with any sale of professional services, what is sold is an outcome, not necessarily the methodology used to achieve that outcome. Using RTO and RPO as key metrics in an SLA supports this backup approach by setting expectations for the overall BCDR solution and guaranteeing in writing the value of the provided services.

A wide variety of variables can shape the SLA covering an application or system in a customer's business. As discussed, the importance of availability and retention of records for a given application is foremost among those. Budget is, of course, a concern, but one that solution providers can navigate by understanding a client's business and revenue flows. An application that, if down, will cost a company tens of thousands of dollars an hour in lost revenues probably warrants a rock-solid BCDR solution and the low RTO and high RPO goals that come with it.

The flow of use for an application can also be closely matched to an SLA – it may, for example, be vitally important that a sales management application be up and running and data saved in as close to real time as possible between 6:00 am and 9:00 pm, but if the application sits unused outside that period, some flexibility can be built into the SLA.

Often, solution providers must take a view well beyond the individual system to be protected to get a real feel for attainable RTO and RPO metrics and craft the right SLA. For example, while the application to be protected may be back up and running in 45 minutes, if the network over which the application is accessed is non-functional, the application is still, in effect, down. It is important for solution providers to have a deep understanding of the customer's business needs, technology infrastructure, and connectivity to author an SLA that works for all involved.

BACKUP & RECOVERY IN SHARP FOCUS

The key metrics for determining the value and performance of a backup and recovery plan – recovery point objective and recovery time objective – combine to answer customers' two questions around their data backup services: "How soon will I be back up and running?" and "How much data will I lose?"

By focusing on these metrics in delivering a backup and recovery solution, solution providers will ensure their BCDR solutions align with customer priorities and needs, and will deliver the maximum return on investment for the customer and the maximum value for the partner.

ABOUT INTRONIS

Intronis Cloud Backup and Recovery is a world-class cloud backup solution for the IT channel. Intronis provides the industry's easiest-to-use secure data solution for offsite and local backup, which generates a monthly recurring revenue stream to add to your business. Intronis offers the best, deepest Exchange and SQL backup on the market, supports virtualized environments with native VMware backup and is integrated to major solutions in the MSP ecosystem. Partners receive expert customer support from our U.S.-based team. The solution has been field tested by thousands of MSPs, and the company has been awarded Best Revenue Generator seven times and Best Customer Support three times by members of ASCII.

For more information, please visit www.intronis.com