

5 Best Practices for Leveraging Backup and Recovery as a Service for True Business Continuity and Resiliency

The advent of cloud has been both a curse and a blessing for businesses when it comes to backup and recovery. It is a curse because too many organizations assume that cloud backup as a service (BaaS) is all they need: they can access their backup data from anywhere, so they neglect the details of disaster recovery planning. But the cloud is also a blessing because, once companies realize the danger of ignoring disaster recovery, they can leverage the new cloud-based recovery as a service (RaaS) options available to them to complement their cloud backup as a service. Whereas BaaS provides data only, RaaS provides data and compute resources in the cloud.

Here are five best practices to leverage BaaS and RaaS together for true business continuity and resiliency.

1

Put recovery at the forefront – don't make it an afterthought

Most companies understand the importance of backup. They may even have regulatory requirements in place that provide guidelines as to what kind of backup, for what data, on what schedule, and for how long.

The disconnect happens if these same companies do not take the next step: considering what *actually* happens if an interruption or incident occurs. Certainly, the data is backed up. But is the business *recoverable*? A backup

copy of data is just that: a backup copy of data. The fact that a business has a backup copy doesn't provide the what, how, who, when, and where of getting the business back online. As a result, having data effectively backed up can't – by itself – guarantee the real business goal: end-user satisfaction, resiliency, agility, and risk mitigation. For that, companies need disaster recovery and operational recovery to be fully integrated with their backup solutions.

EMC²

Together, Sungard Availability Services and EMC² deliver fully-integrated backup as a service and disaster recovery as a service solutions:

- Experience the optimum mix of flexibility and scale.
- Take advantage of affordable pricing options.
- Leverage a tiered approach that matches the right availability solution to each application's recovery time and recovery point needs.



SUNGARD®
AVAILABILITY
SERVICES™

EXECUTIVE BRIEF

2

Select BaaS and RaaS vendors with an eye to the past, the present, and the future

Choosing a BaaS and RaaS provider carries with it a financial and operational investment. To ensure that investment delivers an ROI, companies should seek for BaaS and RaaS providers who bring:

- **Experience.** This is a look at the past. Longevity is a good indicator that a cloud backup as a service or disaster recovery as a service vendor has the expertise necessary to handle customer requirements.
- **Maturity.** This is a look at the present. End-to-end resiliency requires BaaS and RaaS maturity, which is characterized by a defined and proven methodology. Companies should inquire carefully as to how a vendor approaches backup and recovery, and should ask about the results their clients have had.
- **Flexibility.** This is a look at the future. The economy, the market, technology, and each individual business will inevitably experience change. It is essential to have a cloud BaaS/RaaS provider who will adapt with change. Companies should look for a full suite of solutions, a pattern of regular additions or enhancements to services, and a strong set of business partners: all these are indicators of a vendor's commitment to flexibility.

3

Be certain to back up system state information as well as data

All too often, companies back up only their raw data – forgetting that without all the systems to support it, that data is useless and recovery is impossible. As an example, people will back up their Windows data, but forget to back up the system state information necessary to restore the entire server. On an AS/400, people will not do a SAVSYS. On HP/UX, people often forget to document their volume group listing. A RaaS provider will work with the BaaS vendor to ensure that this type of critical omission does not happen.



4

Don't rely on partial tests alone

Partial tests have a very definite place in a testing regimen. They help ensure that critical applications are recoverable at all times, and they verify that newly-added applications or processes are seamlessly incorporated into the disaster recovery plan.

However, partial tests may not reveal the dependencies of one tier of applications on another tier of applications or sphere of infrastructure. Such dependencies could derail disaster recovery efforts during a true incident or crisis.

For example, suppose a company has a SQL cluster – a database clustered across three or four servers. In a partial test, the company may attempt to bring up one server. The test will probably be successful: they can see the server, they can ping it, so the test is checked off as completed on the testing matrix.

But then a disaster occurs. The company goes to bring up the server, but they can't access their backup data because the server is part of a cluster. All the servers in the cluster need to be restored before any of the servers will work. Missing this critical dependency can add hours to the recovery process.

5

Make BaaS and RaaS part of a larger business continuity program

The very terms “cloud backup as a service” and “cloud recovery as a service” communicate a very important point: these services are provided by vendors who are *external* to the client company. As such, the services they provide are only going to be as good as the *internal* business continuity program of the company.

For example, suppose a company adds three new servers. If they do not communicate with the BaaS vendor that there are new servers requiring backup, then critical data and applications could be missed.

Likewise, if the company adds new processes, new personnel, new products, etc., but fails to tell the RaaS vendor, then these new items will not be incorporated into the disaster recovery plans.

Put simply, having BaaS or RaaS vendors does not negate the fact that business continuity is, ultimately, the responsibility of each company.

True business continuity and resiliency

Cloud backup as a service and recovery as a service vendors can be crucial partners for a company seeking to achieve true business continuity and resiliency. By leveraging the five principles provided here, companies can be assured that the BaaS and RaaS providers they choose will deliver a solid ROI financially and operationally should a crisis, incident, or interruption occur.

The perfect partnership

Sungard AS and EMC² work together to provide companies with true business continuity and resiliency:

Looking to protect tier 1 production data? Sungard AS' Managed Enterprise Storage Replication offers a target EMC environment, a second site to host it, and management of the recover point replication process. Data is fully hydrated and ready to mount, giving you a low RTO!

Looking for tape-free data protection? Sungard AS Managed Backup and Vaulting for Avamar provides a true opex utility model for protecting data. This service includes the Avamar software, Avamar hardware (source and target), and a hosted target location to store data off-site. Perfect to recover tier 2 and tier 3 applications.

Looking to manage your own backups, but you also want disaster recovery capabilities? Sungard AS allows for the hosting of a target Data Domain or Avamar solution within the Sungard AS recovery center.

Looking for 4-hour automated server recovery? Sungard AS' R2C-Server Replication and R2C-Site Recovery Manager provide automated continuous data protection and push-button recovery of production servers onto EMC storage within the Sungard AS recovery cloud.

Looking for a fully-managed disaster recovery program? Sungard AS Managed Recovery Program (EMC) is available with any of the above services and provides recovery experts to create a recovery plan, execute recovery testing, and manage the recovery lifecycle to ensure that your recovery is as successful as possible.

For more information
please visit our website at:
[www.sungardas.com/
disaster-recovery](http://www.sungardas.com/disaster-recovery) or call
us at 1-866-714-7209.

About Sungard Availability Services

Sungard Availability Services provides managed IT services, information availability consulting services, business continuity management software, and disaster recovery services.

To learn more, visit www.sungardas.com
or call 1-888-270-3657

Trademark information

Sungard Availability Services is a trademark of SunGard Data Systems Inc. or its affiliate used under license. The Sungard Availability Services logo by itself is a trademark of Sungard Availability Services Capital, Inc. or its affiliate. All other trade names are trademarks or registered trademarks of their respective holders.

Connect with Us

