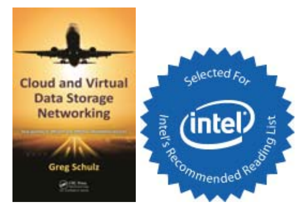
Complements of StorageIO

This chapter download from the book "Cloud and Virtual Data Storage Networking" (CRC Press) by noted IT industry veteran and Server StorageIO founder Greg Schulz is complements of The Server and StorageIO Group (StorageIO). Learn more about the techniques, trends, technologies and products covered in this book by visiting storageio.com and storageioblog.com and register for events and other promotions. Follow us on twitter @storageio or on Google+ among other social media venues.

Visit storageio.com/events to see upcoming seminars and activities



Cloud and Virtual Data Storage Networking has been added to the Intel Recommended Reading List (IRRL) for Developers. Click on the image below to learn more about the IRRL.

The Recommended Reading List is a valuable resource for technical professionals who want to thoroughly explore topics such as software threading, wireless technologies, power management, and more. Dozens of industry technologists, corporate fellows, and engineers have helped by suggesting books and reviewing the list.

Learn more about Cloud and Virtual Data Storage Networking (CRC Press) by visiting storageio.com/books

/ƒĂŎ KŜŊŜ ŰƵ ƚŜI·ŊYY ƵŊŜ I·ŌƵdzŰ 5Ŝƒƒ . I·Ŏdzǈ¦ ó . I·ŎdzǈI·YŘ 5I·ŰI· tŊƵŰŜŎŰƛƵY
¦ YƛØŜŊăƛŰèú ƛYŎƒdzŘƛYƎ ǿŜŌƛYI·Ŋă ƵYƒƛYŜ ŎƵYØŜŊăI·ŰƛƵYã I·YŘ I·ŘŘƛŰƛƵYI·ƒ ŎƵYŰŜYŰ
ǿǿǿăƵŦŰǿI·ŊŜŘŜƒŎƵY ĸŌI·ŎdzǈdzÍ

Chapter 5

Data Protection: Backup/Restore and Business Continuance/ Disaster Recovery

Information security: To protect, preserve, and serve.

– Greg Schulz

In This Chapter

- The difference between business continuance (BC) and disaster recovery (DR)
- The importance of an effective data protection plan and strategy
- Why it is time to modernize backup and data protection
- How to reduce costs by using tiered data protection and different technologies

This chapter looks at issues, challenges, and opportunities for protecting data in cloud, virtual, and data storage networks. The focus of data protection in this chapter is on maintaining availability and accessibility of both active and inactive data. In the context of this chapter, data protection builds on the previous chapter's subject of security by expanding our focus to information accessibility and maintenance of data integrity. Key themes, buzzwords, and trends addressed in this chapter include high availability (HA), backup and restore, business continuance (BC) and disaster recovery (DR) along with replication and snapshot-related technologies.

5.1. Getting Started

Mention "DP" to people in IT and, depending on their area of interest and their length of experience, you may get answers such as Dual Platter, Dedupe Performance, Data Processing, Double or Dual Parity, or perhaps even Dance Partner from someone more creatively inclined. For the purposes of this chapter, DP is data protection.

"Data loss" can be a misleading idea: If your data is intact but you cannot get to it when needed, is the data really "lost"? There are many types of data loss, including loss of accessibility or availability and complete loss. Loss of data availability means that somewhere—perhaps off-line on a removable disk, optical drive, tape, or at another site on-line, near-line, or off-line—your data is still intact, but you cannot get to it. There is also real data loss, where both your primary copy and backup as well as archive data are lost, stolen, corrupted, or never actually protected.

Protection of data and information services delivery applies to:

- Workgroups, departments, and remote offices/branch offices (ROBOs)
- Enterprise, small to medium-size business (SMB)
- Small office/home office (SOHO) and consumer environments
- Workstations, laptops, and mobile devices
- Physical and virtual servers, workstations and desktops
- Managed service providers, public and private clouds
- Integrated stacks, converged and unified solutions

5.2. Data Protection Challenges and Opportunities

IT organizations of all sizes are tasked with the basic responsibilities of protecting, preserving, and serving information services when needed. Since new data is continuously created while old data must continuously be handled, there is more data to process, move, and store for longer periods of time than there was even yesterday. Consumers of IT services are dependent on applications and data being readily available and protected by BC and DR activities. A challenge for many organizations is how to balance the cost to protect against various threat risks, regulatory and other compliance requirements, and the demand to protect, preserve, and serve more data for longer periods of time in an economical manner.

Data protection trends and challenges include:

- More data to process, move, protect, preserve, and serve
- Shifting data lifecycle and access patterns while retaining data longer
- Continued focus on cost containment or reductions
- Reliance on information services accessible when and where needed
- Increase in mobile-generated and -accessed information services
- Cloud, virtualized, dynamic, and flexible computing
- Outages resulting from human error or design deficiency

There are other challenges related to protecting data and applications in physical, virtual, and cloud environments. For example, in a nonvirtualized server environment, the loss of a physical server impacts the applications running on that server. In a highly aggregated or consolidated environment, the loss of a physical server supporting many virtual machines (VMs) has a much more significant impact, affecting all the applications supported by the virtual servers. Another challenge is protecting the growing amount of structured and unstructured data in primary data centers along with data in ROBOs, workgroups, field offices, and other locations.

Data protection opportunities include:

- Stretch available budgets further to protect and preserve more data longer.
- Maximize return on investment (ROI) in capital and operating expenditures.
- Improve quality of service (QoS), service-level agreements (SLAs) and service-level objectives (SLOs), including recovery-time objectives (RTOs) and recovery-point objectives (RPOs).
- Modernize data protection including backup/restore and BC/DR.
- Reduce cost of services delivered via improved efficiencies.
- Provide protection of cloud, virtual, and physical resources.
- Leverage cloud and virtualization technologies to mask complexities.
- Reconcile and streamline protection frequencies and retention cycles.

5.3. Protect, Preserve, and Serve Information Services

Disaster recovery (DR) can mean different things to different people; however, for the purposes of this chapter it will mean two things. The first is an overall process, paradigm, or set of best practices that spans across different technology groups and organizational boundaries. The second are the steps taken as a last resort to reconstruct or rebuild, reconfigure, restore, reload, rollback, restart, and resume information and organizational services or functionality in the event of a severe incident or catastrophe. Business continuance (BC) and DR are often used interchangeably to mean the same thing. We will treat them separately, with business continuance focused on disaster prevention, surviving a disaster or incident, and keeping the business running, and disaster recovery as the process of putting all of the pieces back together again if HA, BC, and other steps were either not taken or failed.

Threat risks to information services delivery requiring data protection include:

- More data being generated, stored, and used remotely
- Funding constraints coupled with increased demands
- Accidental or intentional deletion and data corruption
- Operating system, application software, server, or storage failure
- Loss of access to site, servers, storage, or networking resources
- Acts of nature or acts of man, headline and nonheadline incidents
- Local site, campus, metropolitan, regional, or global incidents

- Business or regulatory compliance requirements
- Increased awareness of threat risks and reliance on information services
- Technology failure or inappropriate configuration design
- Planned or scheduled and unscheduled downtime
- Network or communications disruptions including cables being cut
- Problems introduced via configuration changes

Table 5.1 shows various situations or scenarios in which information services have been or could be impacted. The scenarios or situations are categorized into different levels that can be used to help determine what type of data protection to apply to counter applicable threat risks.

Table 5.1 Protecting Against Various Levels of Threats and Impending Risks

Level	Description of Incident or Scenario
1	Systems are running alerts warning of potential threat and disruption received
2	Hardware, software, network, or facilities component has failed
3	Single system or application disruption
4	Single major disruption or multiple lower-level incidents
5	Metropolitan or campus disaster
6	Major local or regional disaster

- *Level 1: Systems are running; alerts or advance warning of potential threat and disruption have been received.* Notification or indications of possible threat or service disruption have been received, ranging from a virus or security issue to a system potentially being compromised or a hardware device logging errors or software indicating that consistency checks should be taken. Weather reports might indicate an approaching storm, or acts of civil unrest or other threats may be anticipated. Left unchecked, or not corrected, Level 1 threats may escalate to a higher threat level or, worse, a rolling disaster.
- *Level 2: A hardware, software, or network/facilities component has failed.* Business functionality has not yet been disrupted. Business functions, information services, and their applications remain operational. The incident might be a failure in a component such as a disk drive, storage controller, server, network path, power supply, or other item that is being protected by redundancy and automatic failover. The threat might also be a virus, software, or data correctable error leveraging a translation log or journal rollback. There is vulnerability of a multiple failure during the repair process escalating into a disaster.
- *Level 3: Single system or application disruption.* Overall business or information services remain available, but some functionally is not currently available. An entire system or application (hardware, software, and network) may have failed or been shut down due to a facilities issue such as circuit breaker or zone cooling issue. Some disruption may occur during failover to a standby site if available

or, if the disruption will be extensive in length, restoration from backup media. Failback occurs when resources are ready, safe, and stable. Databases may be read-only until updates can resume.

- *Level 4: Single major disruption or multiple lower-level incidents.* The data center exists and most systems are functional, but some Level 2 or 3 scenarios may be occurring. Performance may be slow due to rebuild, failover, or loss of primary systems placing heavy demand on standby resources. Disruption may be hardware-, applications-, or data-related. Resolution may require failover to a standby system with good data or restoration from a known good copy or snapshot.
- *Level 5: Metropolitan or campus disaster.* The data center, information, and resources are intact, but access to them has been lost for some period of time due to a localized incident. If a standby or failover site is available in a different location, service may resume; otherwise, recovery occurs elsewhere.
- *Level 6: Major local or regional disaster.* Loss or damage to facilities and related infrastructure, including power, water, communications, or personnel, due to acts of nature (flood, earthquake, hurricane) or acts of man, including terrorism. A determination is made that the primary site will not be available/accessible for an extended period of time, resulting in major disruption to business function for any applications not protected via HA or BC.

Different types or levels (Table 5.1) of disasters or incidents can be localized to a given site, campus, metropolitan, regional, or global basis. Understanding the applicable data protection threat risks or scenarios along with the likelihood of their occurrence and subsequent impact to the business is part of technology or service alignment. The importance of technology and data protection service alignment is to make sure that an appropriate level of protection is applied when and where needed to stretch available budgets as far as possible.

Figure 5.1 shows how distance can be part of enabling business or information services survivability to different threat risks for some environments or applications. If applications or services are focused only on a local or metropolitan audience, then regional or global forms of protection may not be required. Granted, they may be nice to have, and if affordable, then practical.

Distance is important for enabling data protection and survivability. While distance is often thought of in terms of physical space, time can also be a function of distance. This means being able to go back to a particular place or point from which data was copied or protected—known as a recovery-point objective (RPO).

Physical distance can be measured in inches, feet or meters, kilometers or miles. How would distance of inches be enough to enable data protection? By having data on two different storage devices located next to each other in case one fails. However, there would still be a point of failure if the server or storage system in which they were installed failed. The next logical step would be to have data on two different storage devices, which might be feet or meters apart in the same facility, to isolate and protect against device failure. Here the single point of failure would be the site or facility; this can be mitigated by having copies of data on different systems spread across a campus, metropolitan area, and region or on a global basis.

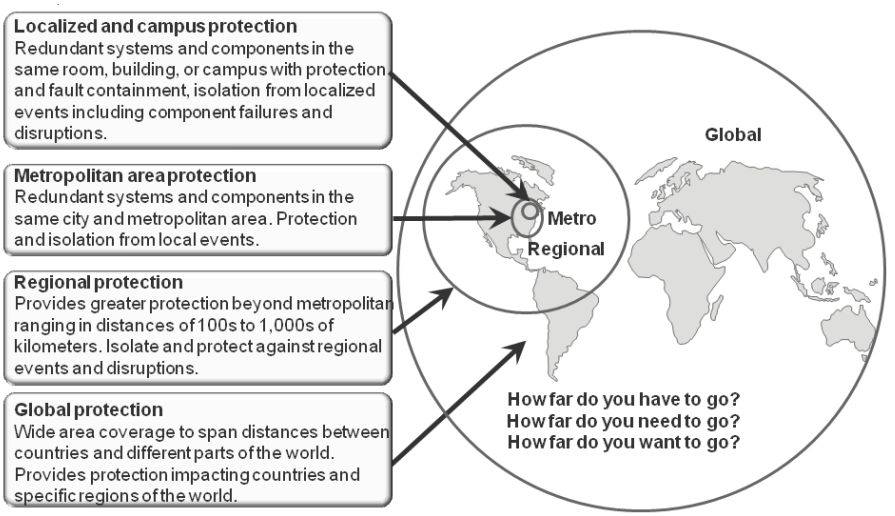


Figure 5.1 Protecting against various threat risks to data and information services.

5.3.1. Basic Information Reliability–Availability–Serviceability (RAS)

As the name implies, basic information services availability means limited or no data protection. This could mean that backups occur now and then with no recurring or regular frequency. Availability may be limited to servers or storage that lack failover or redundancy components, for example, storage that lacks RAID (redundant array of independent disks) data availability capabilities or redundant power supplies and cooling fans. Basic availability can be enhanced by increasing the frequency of backups, ensuring that important information is copied to different locations.

In addition to making copies of data that are stored in different locations (a local copy on disk, another copy on a fileserver, another stored at an off-site cloud or managed service provider site), retention is also important. Retention means how long those copies are kept before being deleted or destroyed. For example, if you have multiple copies of data that all expire after 14 days and you are only making copies of data once a week, if something goes wrong with the last backups, you may be facing a disaster situation. On the other hand, having too many copies for too long adds to the cost of protecting data. Managing threat risks needs to be balanced with available budgets as well as business needs.

Other common constraints for data protection include:

- Growing amount of data to protect and preserve
- Time including backup or protection windows
- Budgets (capital and operating)
- Technology interoperability or interdependencies
- Software license restrictions

- Lack of automation, reporting, or analytics for data protection
- False positives when diagnosing problems
- Staffing and in-house expertise
- Cross-technology ownership issues
- Upper management buy-in, support, or sign-off
- Policies or lack there of
- Workflow and paperwork overhead

Items that need to be addressed or included in a data protection plan include:

- Facilities—Floor space, primary and secondary power, cooling, fire suppression
- Networking services—LAN, SAN, MAN, and WAN voice and data services
- Security—Physical and logical security including encryption key management
- Monitoring and management—Infrastructure resource management (IRM)
- Diagnostics tools—End-to-end tools for analysis and troubleshooting
- Software—Applications, middleware, databases, operating systems, hypervisors
- Hardware—Servers, storage, networking, workstations, and desktops
- High availability, backup/restore, snapshots and replication, media maintenance
- Best practices—Documentation, communication, change control
- Testing and audits—Review of plans and processes, random testing of activities

5.3.2. High Availability and Business Continuance

Think of high availability (HA) and business continuance (BC) as disaster prevention. Disaster prevention refers to containing or isolating faults from rolling into a larger event or disaster scenario. Essentially, enabling HA and BC means taking adequate steps within reason as well as budget constraints to eliminate or minimize the impacts of various incidents on information services delivery—in other words, enabling information services to actually service in the face of a disaster. Disaster recovery (DR), on the other hand, involves rebuilding, restoring, recovering, restarting, and resuming business after an incident that could not, within reason or budget, be contained.

Enabling HA and BC involves eliminating single points of failure and containing or isolating faults from spreading by using redundant components and failover software. In addition to hardware, software, and networking redundancy on a local as well as remote basis, another important aspect of both IRM in general and data protection specifically is change control. Change control means testing and validating hardware, software, application, or other configuration changes before they are implemented, updating applicable documents as part of workflow management, and having a plan in case the change does not work.

Having a fallback plan or process to back out of the change quickly can help keep a minor incident from escalating. A simple approach to change management is to have multiple copies of the configurations, applications, or data that is being updated, which can be reapplied if needed. Part of change control management should also be a determination of the interdependences of a change and associated remediation.

Not all incidents or outages are the result of a major disaster. As mentioned above, some can be the result of component failures or faults that were left uncontained and therefore expanded into a disaster. There is also the possibility that an IT environment can be reduced to physical ruins by a fire, flood, hurricane, tornado, or explosion caused by an accident or act of man. In other situations, an IT environment may be completely intact but not usable as a result of loss of access to a facility. For example, an area might be evacuated due to a chemical spill from a truck or railroad car. If the site is automated, with intervention available via remote access, the disruption may be minimal to nonexistent unless utilities were also cut. Having on-site standby electrical power and self-contained cooling would mitigate those risks; however, what about communications for networks along with adequate fuel supplies for backup generators and cooling water?

In other, less drastic, incidents, all hardware, networks, and software may be intact but a data corruption or error occurs, requiring rapid restoration to a previous point in time. If a recent snapshot can be rapidly recalled and restored, log or journal files applied, and integrity and consistency checks completed, the outage can be kept to a minimum. If, instead, you have to wait for data to be brought back on-site, reloaded, and then rollbacks along with consistency checks performed, that will take more time. This is where data protection comes back to a balance of cost versus risk to the business and the value of time. Not all applications will have the same time sensitivity, so not all data and applications should be protected the same way. Aligning the data protection strategy with the sensitivity of the data is one way of maximizing budgets and resources.

5.3.3. Disaster Recovery

As mentioned earlier, disaster recovery can be thought of in two ways, one being the overall process of ensuring business and organizational survivability and the other being the activities involved in reconstructing an environment after an incident. Basic RAS (reliability–availability–serviceability), HA, and BC can all be considered part of enabling an overall DR plan and strategy. The last line of defense to various threat levels (Table 5.1) in DR is the process of reconstructing, restoring, and resuming after a major disaster or incident beyond the abilities of HA and BC to cope (Figure 5.2).

What could cause a disaster and what would create only a minor inconvenience to information services delivery? For example, would a short outage of a few minutes result in any data loss, or simply loss of access to data for a short period of time? What would happen if the short outage turned into a day or longer? Figure 5.2 shows examples of normal running states with various forms of data protection occurring at different frequencies and retention lengths to combat various incidents or disaster scenarios.

Part of supporting growth or increasing business demands while reducing costs and maintaining or enhancing quality of service involves aligning the applicable level of data protection to the likely threat risk scenario. What threats or incidents are most likely to occur, and what would be the impact on your organization if they were not remedied? How much protection do you want, how much do you need, and what can

you afford? Put a different way, what can you afford not to do, and what is the subsequent impact to specific information services, applications, functions, or the entire business or organization?

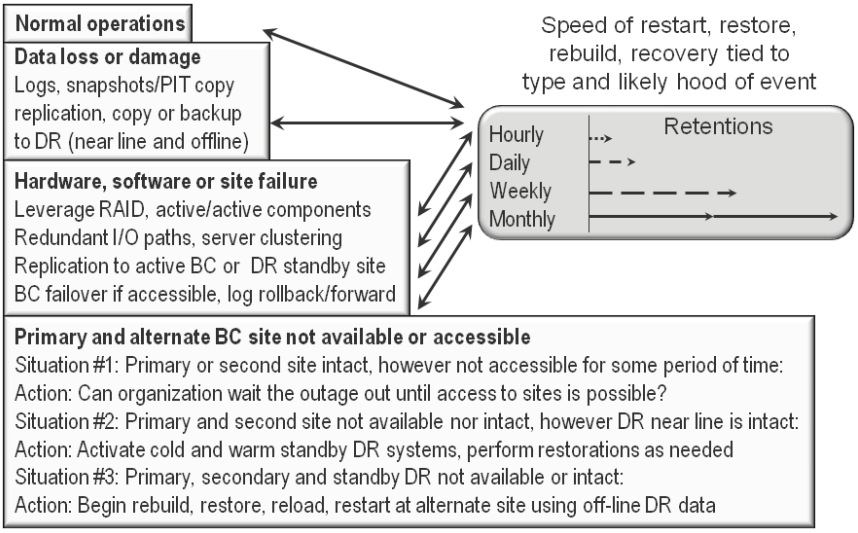


Figure 5.2 RAS, HA, BC, and DR as part of a data protection strategy.

5.3.4. Data Protection vs. Preservation (Backup vs. Archive)

While the two functions are related, backup is focused on protecting data with the intention of it being usable for recovery to a given point in time (the RPO), and archiving is aimed at preserving the state of data or an application for possible future use. They may sound similar, but they differ in retention cycles and in the frequency or interval at which backups are made versus archives.

Archives are usually retained for longer periods of time, such as years, while backups are typically retained for days, weeks, or months. Archives can be established for regulatory compliance purposes as well as to preserve intellectual property (IP) or project data for possible future use. Additionally, archives are used as part of data footprint reduction (DFR) as a means of migrating less frequently used or accessed data off-line or to another medium such as disk, tape, or cloud to reduce online or active storage space needs. The benefit of archiving databases, email, and Microsoft SharePoint or file systems is to free up space while reducing the amount of data that needs to be backed up or protected.

Backups and archives can use the same software and target hardware or service while implementing different policies and business practices. The main difference is that archiving is focused on saving the context of data and applications as of a point in time for long-term retention in case it's needed. Backup, on the other hand, preserves the context of data and applications as of a point in time for routine restoration of a

single file or dataset object or database table. Archiving as a tool to optimize storage capacity will be discussed further in Chapter 8.

5.4. SLO and SLAs: How Much Availability Do You Need vs. Want

Costs associated with data availability need to be understood to determine availability objectives. Vendors use terms such as "five 9s," "six 9s," or higher to describe their solutions' availability. It is important to understand that availability is the sum of all components combined with design for fault isolation and containment. Seconds of downtime per year are shown in Table 5.2. How much availability you need and can afford will be a function of your environment, application and business requirements, and objectives.

Availability is only as good as the weakest link in a chain. In the case of a data center, that weakest link might be the applications, software, servers, storage, network, facilities, processes, or best practices. This means that, for example, installing a single converged SAN and LAN networking switch with "five 9s" or better availability could create a single point of failure. Keep in mind that the failure may be technology-related, a configuration issue, a software update failure, or something as simple as someone unplugging a physical network connection cable. Virtual data centers rely on physical resources to function; a good design can help eliminate unplanned outages to compensate for failure of an individual component. A good design removes complexity while providing scalability, stability, ease of management and maintenance, as well as fault containment and isolation. Design for both maintenance and to contain or isolate faults from spreading, as well as to balance risk, or the likelihood of something happening to required service levels and cost.

Table 5.2 Availability Expressed as a Number of "9s"

Availability (%)	Number of 9s	Amount of Downtime Per Year
99	Two	3.65 days
99.9	Three	8.77 hours
99.99	Four	52.6 minutes
99.999	Five	6.26 minutes
99.9999	Six	31.56 seconds
99.99999	Seven	3.16 seconds
99.999999	Eight	½ second

5.4.1. RTO and RPO: Balancing Data Availability vs. Time and Budgets

Figure 5.3 shows a timeline example that includes a gap in data coverage between where and when data was last protected and where it can be recovered. Also shown are

various component recovery time objectives, such as when hardware becomes available for use for operating systems or hypervisors, data, and applications. While server hardware, hypervisor, and operating system RTOs are important, as are storage and data restoration RTOs, the overall application RTO is what matters to the consumer of the information service or application. Figure 5.3 shows that there are different RTOs that need to be aligned to meet the cumulative service objective for a given class or category of service.

If a given application or information service has, as an example, a 4-hour RTO, it is important to understand what that RTO means. Make sure you know whether the 4-hour RTO is cumulative and when application users or consumers of services can expect to be able to resume work, or whether the RTO is for a given component (Figure 5.3). If the RTO of 4 hours is cumulative, then all other sub-RTOs for data restoration, operating system and hypervisors, database rebuilds or rollbacks, and verification must fit within that 4-hour window.

A common mistake is that multiple groups learn that the RTO is, continuing the example, 4 hours and assume that means they each have 4 hours to complete their required tasks. While some tasks may be done in parallel, some—such as data restoration followed by database verification or rebuild and application verification—are usually done serially; if each team assumes they have 4 hours to complete their task, the 4-hour cumulative RTO cannot be achieved.

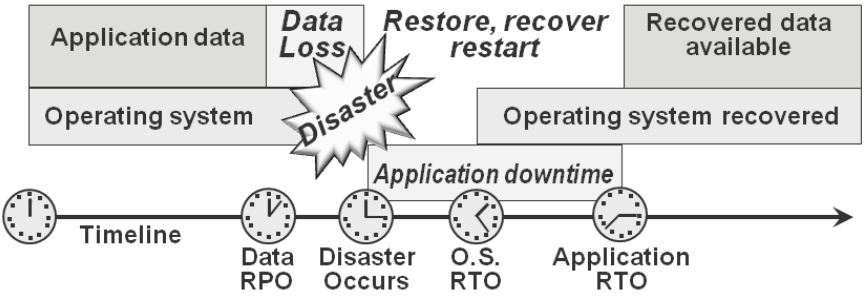


Figure 5.3 End-to-end recovery-time objectives.

5.4.2. Reconciling and Assessing RTO and RPO Requirements

Earlier, we discussed the importance of not treating all applications or data the same so as to do more with what you have while enhancing quality of service. For data protection and availability this is also true, in that an incorrect assumption as to what level of service is desired vs. what is required can increase costs. This means assessing actual availability requirements against what would be nice to have, to be able to align the applicable classes or categories of service and underlying technologies to a given situation.

With a continued industry trend toward using disk-to-disk (D2D) backup for more frequent and timely data protection, tape is finding a renewed role in larger, more infrequent backups for large-scale disaster recovery supporting long-term archiving and

data preservation of project data and compliance data. For example, D2D, combined with compression and de-duplication disk-based solutions, is used for local, daily and recurring backups that have shorter retention but that have more granularities (Figure 5.4). Meanwhile, weekly or monthly full backups are sent to disk at a secondary location, cloud server, or to tape, to free disk space as well as address PCFE concerns. These copies occur less often so there are not as many of them, but they are retained for longer periods of time.

By reconciling and tuning data protection frequencies along with retention cycles (Figure 5.4), the overhead of protecting data can be reduced while increasing survivability in a cost-effective manner. The principal idea is that for more commonly occurring incidents, recovery or restart occurs more often, faster, and with more ease than traditional data protection. D2D data protection combined with data footprint reduction (DFR) techniques means more copies of protected data can be kept closer to where it will be needed at a lower cost. Meanwhile, copies of data that are less likely to be accessed occur in longer cycles and are sent to off-line or cloud facilities.

By not aligning the applicable service level along with reviewing service-level objectives (SLOs) and service-level agreements (SLAs), situations where two parties wrongly assume what the other wanted or needed can be avoided. For example, IT or a service provider assumes that a given application requires the highest level of availability and data protection because that is what the business unit, customer liaison, advocate, or consumers indicated that they would like. However, the consumers or customer representatives thought that they would need the highest level of service without considering the cost ramifications or verifying what they actually needed. Upon review of what is actually required, there is sometimes a difference from the level of service being delivered. When questioned about SLOs or SLAs, business or IT services consumers may want to have the higher level of service, but some due diligence may show that they do not actually need it, and this can help stretch their budget.

The previous is an example of a disconnect between customer/consumer and IT services management. If IT understands their services and costs and works with their customers, the applicable level of capabilities can be delivered. In some cases IT services customers may be surprised to find that IT-provided services are cost effective when compared to cloud and MSP solutions on the same SLO and SLA services basis.

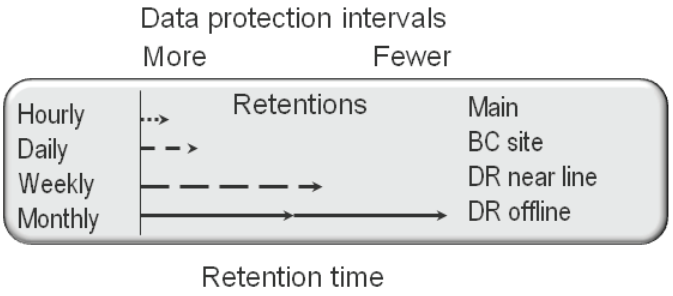


Figure 5.4 Reconciling and tuning data protection intervals and retention cycles.

have a small business and, practicing what I preach, have implemented a multitier data protection strategy including D2D, D2D2C, and D2D2D on a local, remote, as well as with removable technologies. I leverage a cloud backup MSP where encrypted data gets sent even while I am traveling (I have done backups from commercial aircraft using Gogo WiFi), as well as having local copies on disk. Additionally, I have a master copy off-site in a vault that gets routinely updated using removable hard disk drives. There are many different tools, with more on the way, some which will be available by the time you read this. Check my blog and website for news, announcements, and discussions on related topics, trends, and techniques.

What are some key steps or questions to ask when choosing an on-line or cloud MSP for backup or archive services? Balance the cost or fees of the service with the available functionality, SLAs, hidden fees for accessing your data, import or export charges, options for what locations or regions where your data can be stored, and reporting. For example, I get a daily backup report via email from my service provider that I can check manually or set up a script to scan for exceptions. Also look into how your data is reduced using data footprint reduction techniques before transmission, to either move more data in a given amount of time, or with less network bandwidth capability. Also test how long restores take, to avoid surprises when time may be of the essence, and look into options to get larger quantities of data restored in a shorter period of time.

5.10. Chapter Summary

HA, BC, DR, and backup/restore are changing with evolving and maturing techniques and technologies. Clouds and virtualization need to be protected, but, at the same time, they can be used for enhancing protection.

General action items include:

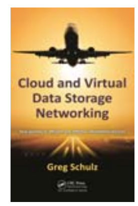
- Avoid treating all data and applications the same.
- Apply the applicable level of data protection to required needs.
- Modernize data protection to reduce overhead, complexity, and cost.
- Combine multiple data protection techniques in a cost-effective manner.
- Don't be afraid of cloud and virtualization, but have a plan.

The bottom line: For now, if you are putting data into any cloud, have a backup or a copy elsewhere. Likewise, if you have local or even remote data, consider using a cloud or managed service provider as a means of parking another copy of backups or archives. After all, any information worth keeping should have multiple copies on different media in various venues.

Complements of StorageIO

This chapter download from the book “Cloud and Virtual Data Storage Networking” (CRC Press) by noted IT industry veteran and Server StorageIO founder Greg Schulz is complements of The Server and StorageIO Group (StorageIO). Learn more about the techniques, trends, technologies and products covered in this book by visiting storageio.com and storageioblog.com and register for events and other promotions. Follow us on twitter @storageio or on Google+ among other social media venues.

Visit storageio.com/events to see upcoming seminars and activities



Cloud and Virtual Data Storage Networking has been added to the Intel Recommended Reading List (IRRL) for Developers. Click on the image below to learn more about the IRRL.

Learn more about Cloud and Virtual Data Storage Networking (CRC Press) by visiting storageio.com/books