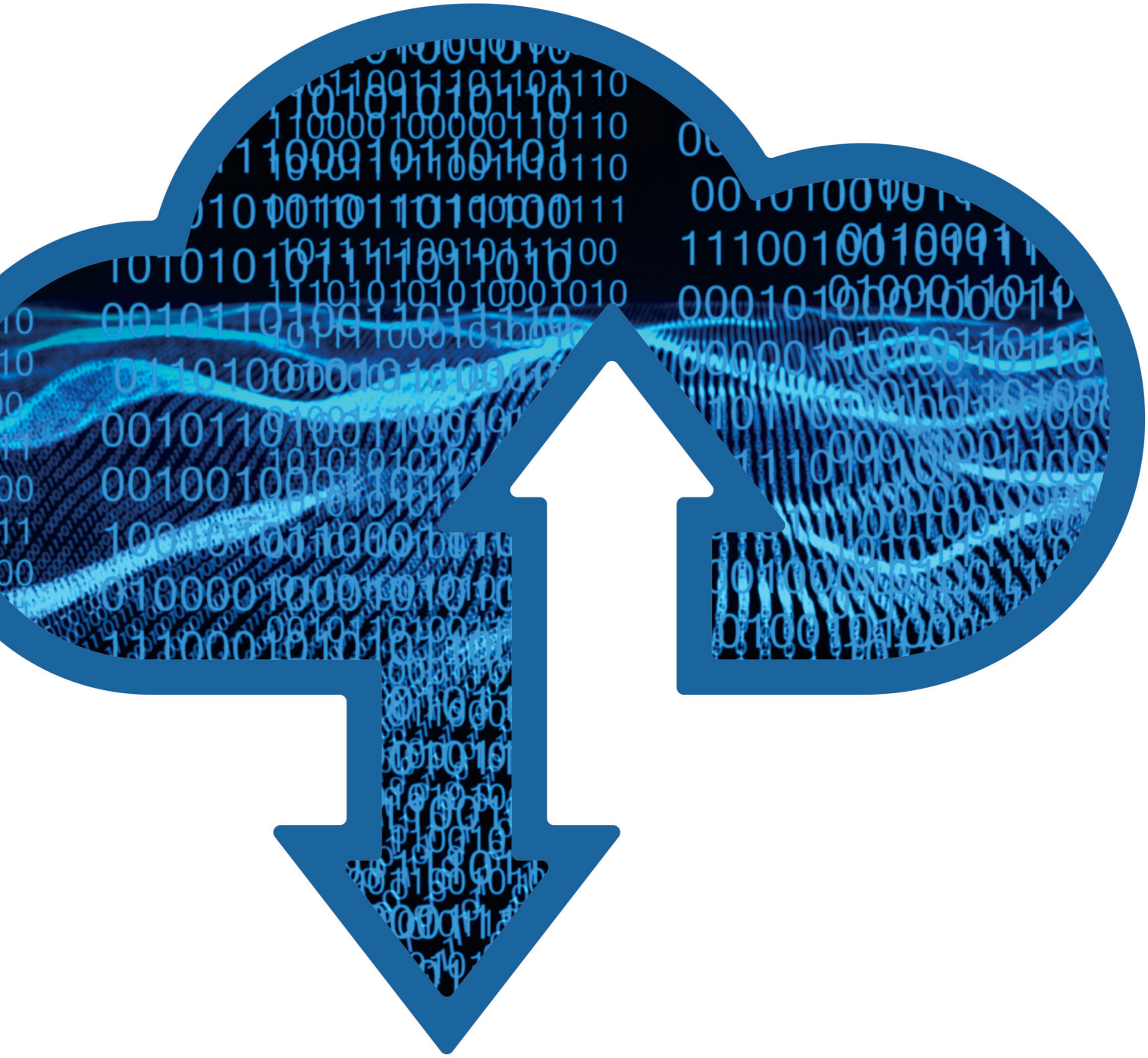
WHITE PAPER

IBM Power Systems
Backup in the Cloud



Data Storage CORPORATION

CMA

Contents

Introduction: IBM Power Systems Backup in the Cloud

Does your current IBM backup strategy still meet your organization's needs? Even with a myriad of backup and restore technologies to choose from, many IBM Power shops are still using tape backup strategies that were originally deployed in the 1960s.

Meanwhile, organizational needs and outside groups are spurring change, especially in the following areas:

- ***Regulations and service level agreements (SLAs) that require backup changes, including encrypted backups, off-site storage, and other mandatory backup and recovery modifications.*** Regulatory standards such as the United States' Health Insurance Portability and Accountability Act of 1996 (HIPAA), Sarbanes-Oxley (SOX), and the European Union's General Data Protection Regulation (GDPR) contain requirements that affect your IBM i, AIX, and Linus backup and recovery solutions. Customer SLAs may also require modifications to protect data integrity and security.
- ***Physical issues requiring geographical backup and recovery solutions.*** 2017 showed how futile local backup and recovery solutions can be when entire metropolitan and regional areas are devastated (such as when Hurricanes Harvey, Irma, and Marie caused massive destruction in Houston, Miami, and Puerto Rico). Some organizations discovered that both their production environments and their backup strategies can be wiped out by a regional disaster.
- ***Data corruption issues that may take weeks or months to discover.*** Viruses, application errors, deleted files, and internal mistakes can be deadly for data integrity, requiring archived backup versions of applications and data to resolve.

The need to modernize and move away from old fashioned 1980s era backup solutions is critical and becoming more urgent. This white paper shows the benefits and steps needed to modernize your IBM i, AIX, and Linux backup and recovery solutions, and how modernization can benefit your organization in the areas of availability, data integrity, security, and regulatory compliance.

What a backup and recovery system needs to do

An effective backup and recovery strategy meets the following goals:

1. *It provides **application and data availability** during and after a disaster or equipment failure, so that you can maintain operations, process orders, and continue running your business.*
2. *It protects **data integrity**, avoiding financial issues, legal liability, and operational mistakes by allowing for recovery when data corruption occurs because of an attack, input mistakes, or application errors.*
3. *It helps **secure data from unauthorized access**, to prevent internal or external bad actors from stealing or accessing unencrypted backups.*
4. *It enables **regulatory and Service Level Agreement (SLA) compliance**, to avoid incurring regulation violations, penalties, or lost business when your backup and restore strategy does not meet requirements.*

There is set of common metrics that can help you judge the efficiency and accuracy of an IT backup and recovery system. These metrics are listed in the sidebar below and will be referenced as we discuss each goal.

Let's look at how improving your backup and recovery systems can help accomplish organizations accomplish their backup and recovery goals.

Critical Metrics for IT Backup and Recovery

Successful IT recovery services are judged by the following metrics, created in conjunction with their organization's business needs.

Recovery Point Objective (RPO) – How closely a target system's data is synchronized with its companion source system data. An RPO of five minutes for example, means target system data is synchronized with its source system to within the last five minutes. RPOs designate how much data an organization would lose if they have to switch processing from a source to a target system during a disaster.

Recovery Time Objective (RTO) – The organizational target for how quickly processing can be switched from a production source system to a backup target system. It specifies how long it should take for a target machine to assume production processing, if the source machine goes away.

Recovery Time Actual (RTA) – The actual measured time it takes to move production from a source machine to a target machine during testing or an emergency. This estimates how long you can actually expect an emergency production transfer to occur.

The Backup and Recovery Roadmap for IBM Power Systems

Most organizational IBM Power backup and recovery strategies fall into one of the nine steps listed in our backup and recovery roadmap in figure 1. Each step lists the common stages and actions organizations take to achieve their backup and recovery goals. As a rule, the farther up the roadmap an organization moves, the better their solution satisfies the essential goals of a backup system and protects their organization. This roadmap can be used to identity the current state of an organization's backup and recovery solution and to pinpoint the next step to take to improve that solution.

Figure 1: The nine steps in the IBM Power Backup & Recovery Roadmap

Let's review each step and discuss how it can improve your backup and recovery solution and the benefits each step provides.

Nine Steps in the Backup and Recovery Roadmap

Step 1: Local tape-based backups

Tape-based backup is older than most people reading this white paper, and many organizations are still using it as either a primary or secondary backup solution. With tape backup systems, data and systems are backed up to magnetic media and stored locally off-site in a (hopefully) secured tape storage facility.

Tape backup utilizes a tape rotation strategy where a specific number of tapes are kept for daily, weekly, monthly, and yearly backup. When disaster hits, the correct tapes are recovered and your systems and data are rebuilt from tape.

Backup tapes must be managed. Tapes require equipment (tape drives) and the number of tapes stored off-site quickly multiplies. A tape backup strategy requires resources for moving tapes in and out of tape drives and for transporting, inventorying, and retrieving tapes from off-site. Many organizations use a tape-management vendor for tape pickup, storage, and retrieval. Other organizations may store tapes off-site in other buildings they own.

There are a number of common problems associated with local tape-based backup, as shown in the accompanying sidebar. Any of these problems can lead to backup and recovery failure, where critical system and data backups aren't available when needed.

For most organizations, a local tape backup and restore system is no longer adequate on its own to meet all their backup goals. Traditional tape backup scenarios allow you to recover systems and data in a disaster but they don't generally meet the other critical backup and recovery goals. Tape backup has a high RPO (restored data is usually 1 or more days old) and a high RTO/RTA, where full system recovery from tape can take between 72 hours and 5-7 days.

Common problems with using local tape-based backups

1. Tapes are usually stored in the same geographical area as the system they back up, and your tapes may not be available during a local or regional disaster, such as a hurricane, tornado, earthquake, flood, or terrorist attack.
2. Mechanical failures can cause backups to be skipped or fail.
3. Tapes can get lost, misplaced, or mislabeled.
4. Tapes are easy to steal.
5. Tapes are physically delicate, and are susceptible to humidity, heat, and magnetic interference.
6. Lengthy restore times make it difficult to meet RPO and RTO/RTA goals.
7. Tapes degrade, wear out with use, and are susceptible to electromagnetic charges.
8. Older tapes may have been produced on drives that are no longer available or maintained, making restores extremely difficult.

Step 2: Realizing your tape backup strategy must change

Organizations in this step realize that their current tape backup strategy no longer meets their needs. This step is commonly spurred on by new requirements or backup and recovery failures, including:

- The organization has a tape restore failure, where they can't recover corrupted or missing data or an entire partition.
- A new requirement is defined by a regulatory entity or law, such as Sarbanes-Oxley (SOX), the Payment Card Industry Data Security Standard (PCI DSS), or the European Union's General Data Protection regulation (GDPR).
- A new requirement is specified by a Service Level Agreement (SLA), a large customer, or from an audit point.
- A regional disaster such as Hurricane Irma occurs, where their local backup solution is destroyed along with the production system it protects.
- A hack, virus infection, or ransomware attack hits their system and corrupts their files, and large-scale file restores must occur.
- They experience unintended data corruption or deleted objects that may take days, weeks, or months to discover and recover from.

An organization's backup and recovery system is their last line of defense for protecting data availability and integrity. At some point, organizations realize that tape backup can no longer satisfy all their backup and recovery needs by itself, and begin upgrading their backup and recovery strategy.

Step 3: Implementing multi-tiered backups using the 3-2-1 strategy

The next step is to modify your backup strategy to provide multi-tier onsite and offsite backups. This is frequently done according to the 3-2-1 backup strategy shown in figure 2, which specifies the following backup and recovery features.

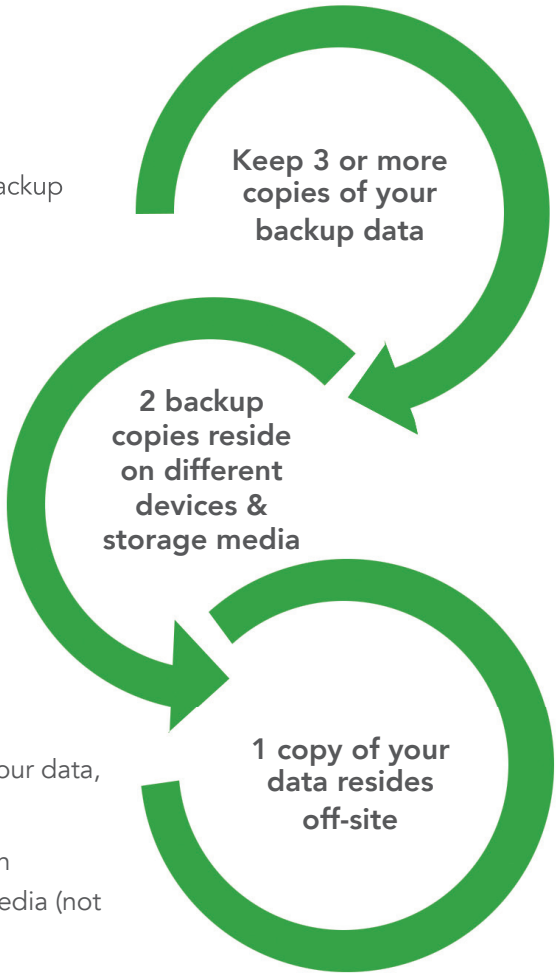


Figure 2: The 3-2-1 backup strategy

- You always keep at least 3 total copies of your data, including the current data.
- 2 copies of your data are local but reside on different devices, using different storage media (not on the same disk array or device).
- 1 copy of your data resides off-site.

For example, organizations implementing a 3-2-1 ERP backup strategy on an IBM Power System would have the original (current) copy of its system and data on its IBM connected disk drives. A second copy would be saved on a nightly, weekly, monthly or yearly schedule to another system, such as external storage or another IBM i, AIX, or Linux partition on a different machine. A third copy would be produced on tape, automatically vaulted, or replicated to the cloud. The second copy provides fast local restore capability if your current ERP data is damaged or corrupted. The third copy protects against a local disaster if the first two copies are destroyed or corrupted.

A 3-2-1 backup strategy ensures you have quick access to recovery data through your local backups. It also ensures that you have multiple copies of your data in different locations, protecting your data no matter what happens. Many of the other steps in the backup roadmap support a 3-2-1 strategy.

Step 4: Improving efficiency by replacing tape backup with disk backup

The next step is to move your backups away from movable media, such as tape drives. Implementing the 3-2-1 strategy, you can deploy local disk-to-disk backups, where your systems and data are stored on another device's storage. Disk-to-disk backup offers several efficiencies over disk-to-tape backup, including:

- Local disk-based backups insure that you'll always have an on-site copy of your data for quick restores.
- Disk backup is much faster than comparable backups to tape. Disk restore is also significantly quicker than tape restore operations.
- Technologies such as data deduplication, archiving, and using image backup software can significantly drive down backup costs. They can also reduce the amount of storage needed to contain multiple backups.
- Disk backups can easily be moved between devices, as needed.

Disk-to-disk backup provides efficiencies in terms of backup time needed, it significantly reduces storage costs over tapes, it provides the ability to recreate backups from different points in time, and it allows you to quickly move backups between devices and networks.

Step 5: Improving security through encryption

For many companies, data and backup encryption is no longer an option. It's a requirement for many different regulatory standards.

Encryption is not just a regulatory issue. It's also a data protection issue, as encrypted backups are nearly impossible to read (as opposed to an unencrypted backup, which only requires tape drive hardware to read). Encryption not only enhances security for portable backup media such as tapes, it also enhances security for transmitted backup sets such as disk-to-disk backups, where backup sets can be accessed and stored remotely.

Data can be encrypted in your source IBM i, AIX, and Linux libraries and folders, or it can be encrypted and decrypted on the fly, as you write data to and restore data from your backups. Library and folder encryption is much more secure as it protects on-line production data as well as backed up data, whereas backup encryption only protects your backed up data.

Step 6: Improving recovery time through local backup replicated to the cloud

Local backup to disk using advance technologies is the most efficient backup strategy. However, for increased protection, at least one backup copy of your data and systems should be stored off-site, preferably in a geographically distant area to insure your data isn't lost in a local or regional disaster.

Local backup appliances can perform encrypted IBM i, AIX, and Linux backups which can be replicated to cloud storage vaulting. This provides organizations the benefit of efficient local backup that can also be stored geographically distant in the cloud. Offsite cloud backup can also scale with growth and it uses technologies such as deduplication and compression backup to reduce backup and recovery times. IBM and several third-party vendors offer vaulting technology that enables this cloud and hybrid backup technology (local appliance backup replicated to the cloud). Cloud and hybrid technology satisfies the 3-2-1 strategy to have at least two backups of your data on different machines and media.

Step 7: Improving recovery point objectives through replication

Data and system changes can be immediately copied to different systems in different locations using software-based and hardware-based replication technologies. Because replication takes place in real-time as data is written and updated, replication technologies can shrink your RPO to provide a near real-time backup set. Replication can also provide significant recovery time improvements over using tape recovery.

It's important to understand that because data is replicated in real-time, replication does not provide a point-in-time backup. Rather, it provides an almost current copy of your data from the source to the backup system. Mistakes made on the source system will automatically be replicated to the backup system, making replication a poor choice for correcting data errors, as errors will exist in both the source and the backup data.

Recovery time for a continuously replicating system can be as short as 15 minutes, while tape backup recovery can take anywhere from 72 hours to 5-7 days.

For IBM Power systems, IBM offers a Capacity Backup (CBU) for Power Enterprise servers, which can be used as a standby server for production partitions. The CBU is an IBM Power system that is exclusively designated for IBM I, AIX, and Linux partitions for disaster recovery and high availability.

IBM also offers storage-based replication offerings for its Power systems, where an exact bit-by-bit replica of your primary storage is created on geographically remote system hardware. This storage replica can be activated to run the primary system when a hardware failure occurs.

Step 8: Providing availability through the cloud

Whatever backup technologies you use, it's important to implement standby compute, storage, and network infrastructure resources that can provide turn-key access to your applications and data, even when your primary system is not available.

When standby compute, storage, and network infrastructure resources are deployed in the cloud, you can provide geographical high availability. Production workloads can be instantly switched to the cloud, complete with all the networking needed to present and run your workloads transparently for both your internal and external customers. Your applications run on the standby resources, allowing your customers to continue using these apps when the production system is down.

Step 9: Eliminate organization-hosted resources through cloud deployment

The final step in our backup and recovery roadmap is to eliminate all your organization-hosted resources and instead use Infrastructure as a Service (IaaS) to deploy your production environment in the cloud. In an IaaS scenario, your vendor takes over all aspects of your application environment, including hardware lifecycle management, maintenance, and public Internet access with VPN or secured private access using a private cloud. The vendor will usually provide a backup strategy complete with availability options.

With IaaS, you no longer need to maintain and backup the equipment and the network it runs on. The vendor will do it for you. A secondary benefit is that you can reduce staff requirements because the vendor performs all the maintenance and availability functions that your IT operations staff previously performed.

What to look for when upgrading data backup and recovery systems

Here are some important questions you should consider when using a vendor to upgrade your IBM Power backup and recovery systems.

1. ***How quickly will you be able to recover from a disaster?*** What RTOs and RPOs can you reasonably expect from your backup and recovery solution? If implementing a vendor solution, what does the vendor's customer history look like in providing these services?
2. ***Does the vendor offer well-defined Service Level Agreements (SLAs) that enforce your RTO and RPO targets?*** How does the vendor guarantee that you'll meet your availability, data integrity, security, and regulatory compliance goals? If you're unable to quickly recover your systems after a disaster, it affects your entire business. All backup and recovery options should be explicitly covered by SLAs and your preferred recovery performance should be guaranteed by the SLA. Make sure your vendor puts your recovery targets in writing with guarantees and penalties if your goals aren't met.
3. ***Can you test your recovery solution without affecting production performance?*** Testing your backup and recovery systems isn't an option; it's a requirement. Many companies have great disaster recovery plans that have never been tested. Remember: if you haven't tested your recovery plan, you don't have a recovery plan. Test your backup and recovery solution early and often.
4. ***Will your data be encrypted end-to-end?*** Is your data encrypted on your production system? If not, will it be encrypted before it's transferred to tape, backed up to disk, or replicated to another system. Many regulatory standards require encryption when moving data between systems.
5. ***When moving to the cloud, does the vendor provide pre-configured network access and VPN access?*** In the event of a failover during a disaster, does the vendor provide a pre-configure network and VPN access that mimics your production access, so that production can be quickly restarted.

The Next Step

There are a number of options for efficiently and effectively updating your backup and recovery solution. It's all a matter of knowing where you're currently at and where you want your backup to achieve. An experienced business partner like Computer Management & Marketing Associates, Inc. can help organizations select and implement the backup and recovery technology that's right for their business, no matter what the company's size and budget.

Please feel free to contact CMA, if you have any questions about improving your backup and recovery strategy.

Computer Management & Marketing Associates, Inc.

107 N. Commerce Way Suite 100A
Bethlehem, PA 18017
Tel: (610) 837-8262
cmma.com
Email: sharkins@cmma.com

Data Storage CORPORATION

IBM Gold Business Partner™