

White Paper

Rocket Software Answers Mainframe Data Protection Needs with DASD Backup Supervisor

By Brian Garrett, VP ESG Lab with Jason Buffington, Principal Analyst

March 2016

This ESG White Paper was commissioned by Rocket Software and is distributed under license from ESG.



Contents

- Overview 3
- Priorities and Challenges 3
- Best Practices for Modernizing Mainframe Data Protection 4
 - People and Processes 4
 - Automation..... 5
 - Optimizing Data Set Level Recoveries 5
 - Point-in-time Snapshot Integration..... 5
 - Taking Advantage of the Speed and Density of the Latest Hardware..... 6
 - Maximizing Tape Media Utilization 6
 - Remote Tape Backup..... 7
- Introducing Rocket Software DASD Backup Supervisor 8
- The Bigger Truth 9

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.

Overview

The goal of this ESG White Paper is to help IT executives and backup administrators clearly understand the challenges and trends associated with protecting legacy business-critical and emerging next-generation application workloads running on IBM z Systems. The benefits of a modern mainframe data protection strategy powered by Rocket Software’s DASD Backup Supervisor offering will be highlighted.

Priorities and Challenges

For decades, enterprise-class organizations have counted mainframe backup and recovery among IT’s most essential responsibilities. Mainframe data protection has become even more critical in recent years within the growing number of organizations that leverage IBM z Systems as platforms for next-generation IT initiatives including Linux virtual server consolidation, enterprise mobility, big data, and analytics. In today’s information-driven world, the importance of this task has escalated—along with the negative legal, reputational, and fiscal consequences that arise when mainframe backup and recovery are *not* managed properly. These challenges are exacerbated by the costs and complexity associated with the never-ending growth of storage capacity.

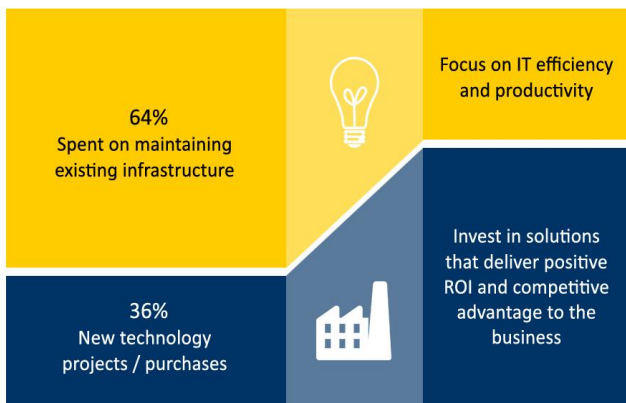
Before we review modern technologies and best practices that mainframe backup and recovery administrators are using to reduce costs and complexity, let’s take a look at some results from ESG’s annual survey of IT purchasing decision makers within enterprise-class organizations (e.g., organizations with 1,000 or more employees).

ESG’s 2016 annual IT spending intentions research survey indicates that security/risk management initiatives and cost reduction initiatives are the two business initiatives that the most respondents believed would drive their IT spending in 2016.¹ When asked about their most important IT priorities, managing data growth and improving backup and recovery were in the list of top five priorities with response rates of 22% and 20% respectively.²



In other words, risk management and cost reduction are the top initiatives for businesses, while improving backups and keeping up with data growth are top priorities for IT organizations. Mainframe backup administrators and their managers can align with these initiatives by investing in new technologies that reduce the costs and complexity of backup and recovery operations while minimizing the risks associated with mainframe application data loss.

An effective way for IT to save time and money is to invest in mainframe backup and recovery technologies that reduce complexity. When backup administrators are more productive, they need less time to maintain existing infrastructure. Reducing the number and severity of the issues associated with recovery frees up even more time—for backup administrators and the rest of the IT team.



The stark reality is that for most organizations, the bulk of the IT budget is spent “keeping the lights on,” rather than investing in new projects that deliver positive return on investment and a competitive advantage to the business (64% vs. 36% according to ESG survey respondents). Investing in mainframe backup and recovery modernization is one way that you can shift that ratio and become more strategic to the business.

¹ Source: ESG Research Report, *2016 IT Spending Intentions Survey*, to be published 2016.

² *ibid.*

Best Practices for Modernizing Mainframe Data Protection

IBM z System mainframes play a more vital and strategic role than ever before. Some of the largest organizations on the planet run their most mission-critical applications on mainframes. As a matter of fact, 92 of the largest 100 banks, all of the top 10 largest insurance companies, and 23 of the top 25 U.S. retailers rely on the multi-tenant performance, scalability, and reliability of IBM z Systems.³ A growing number of organizations are leveraging z Systems as a foundation for next-generation IT initiatives such as Linux virtual server consolidation, enterprise mobility, hybrid cloud, big data, and analytics.

As the strategic role of the mainframe has evolved in recent years, so too has the state of the art in mainframe data protection. For many organizations, it's no longer just a matter of protecting legacy mainframe applications. They also need to consider how to protect the mainframe middleware at the heart of their cloud, mobile, and big data initiatives. With these new initiatives driving towards always-available, 24x7 access and mobility, mainframe data protection is more important than ever. Let's take a look at some of the best practices that can be used to reduce the complexity, cost, and risk associated with mainframe data protection.

People and Processes

Organizations that want to improve the efficiency of their mainframe data protection services should begin with a holistic examination of people, processes, and technology. Start by identifying the team that's involved in mainframe backup and recovery operations. Training and skills development plans should be considered with an eye towards improving the efficiency of backup and recovery operations and reducing the risk associated with restore delays or failures. Retention and succession plans for key members of the team should be considered as well.

Next, an assessment of existing processes can be used to set a baseline for continuous improvement. Escalation procedures and service level agreements are a good area of focus for this exercise. Identifying the key performance indicators (KPIs) associated with mainframe backup and recovery can be helpful as well. KPIs may include:

- Backup duration (e.g., job run times).
- Backup administration (e.g., man hours per month).
- Restore requests (frequency and duration).
- Restore granularity (the data set needed, quickly and easily).
- Disaster recovery drills (frequency and duration).
- Recovery time objectives (RTO, or how long it takes to complete a restore request).
- Recovery point objectives (RPO, or how much time/data was missing after a restore).
- Capital equipment expenses (e.g., tape drives and media).
- Operational expenses (e.g., manpower, tape transport and vaulting fees, WAN fees).

For each of the topics in this paper, ESG will recommend actions intended to help you optimize your existing or new data protection solution.

Success in any business-critical data protection strategy starts with recognizing that “backup administrators” alone do not have the complete view of the business impact for data or productivity loss, nor the workload-protection/recovery requirements, such that they can unilaterally define and implement a data protection strategy that ensures the viability of the business. Therefore, executive stakeholders for the business units or core functions, application- or workload-specific experts who understand the data, and “data protection specialist(s)” need to be aligned on the strategy before attempting an implementation or evaluation.

³ IBM z System Fast Facts, <http://www-03.ibm.com/systems/z/#s-one>, Dec 2015

Automation

Automation that reduces complexity is one of the simplest ways to improve efficiency. Reducing the manual intervention associated with setting up and monitoring backup jobs is a good place to start. For example, automation that reduces the amount of time associated with editing legacy JCL or REXX scripts is a great way to improve efficiency. Automation that helps detect new applications and data set dependencies can also help improve the efficiency of the backup administrator. Moreover, it ensures that no critical steps are missed and reduces the risk of not having the data you need when you're restoring a critical application. Finally, look for technology and process improvements that automate and simplify *recovery* (vs. backup) operations since they can have the greatest impact on the business.

It is important to remember that critical personnel may not always be available for myriad reasons, including calamity, regional crises affecting their homes or the workplace, vacations, or simply dealing with other IT matters. The best time for applied expertise is in the planning and the preparation, not the execution, of a recovery plan. Everything that can be automated, from data restores to orchestration of restart tasks, as well as notifications and logging (of the recovery tasks as they execute), should all be automated wherever possible, such that the proper IT decision makers can hit the "easy button" to restore complex systems with confidence.

Optimizing Data Set Level Recoveries

The processes and time associated with servicing a routine request for a data set level restore is often a good candidate for efficiency improvement. Restoring a full volume to scratch disk to extract a missing data set gets the job done, but can be a waste of time for backup administrators and makes it harder to meet restore time service level agreements. Technology and process improvements that reduce the complexity and time associated with servicing data set restore requests should be considered.

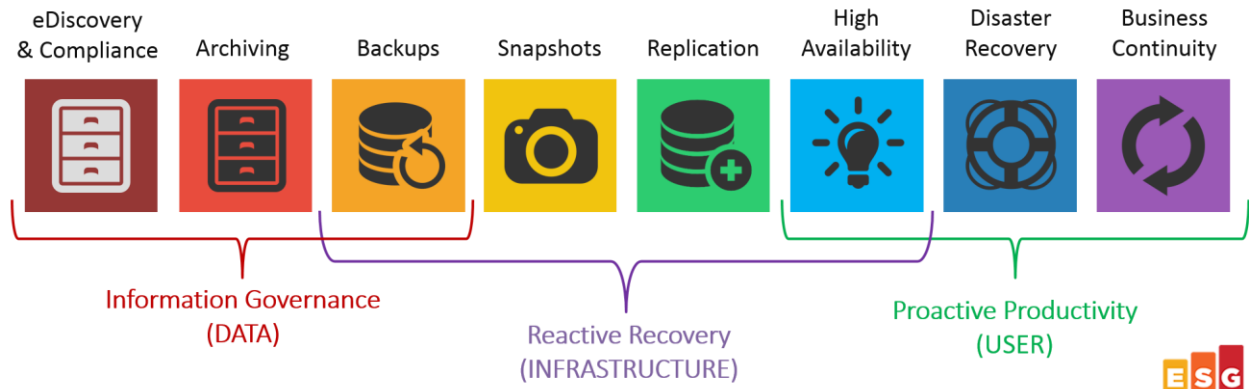
Don't underestimate the potential benefits of thorough protection and recovery planning. Testing one's recovery processes should always include a team-driven approach to considering what can be improved. These discussions will often reveal ways to automate tasks or reduce data sets to be recovered, and can even illuminate changes in protection methods that will result in more agile restores. Just as proper BC/DR planning will often reveal business processes that can be optimized, proper IT backup/restore planning will often provide opportunities for optimization.

Point-in-time Snapshot Integration

Integrating your backup processes with disk array-based snapshot technology (e.g., IBM FlashCopy) reduces the length of your backup window as it nearly instantaneously creates a capacity-efficient, point-in-time image of your applications. Legacy JCL or scripts that integrate API calls to create snapshots just before a backup job is run are effective, but they add complexity and risk for the backup administrator. Differences in the API calls between mainframe disk array vendors (such as IBM, EMC, HDS) exacerbate the complexity, especially for organizations that have inherited a heterogeneous mix of disk arrays from different vendors. Automation that can simplify this process should be considered.

"Data protection" is not just a synonym for "backup" but instead should be considered an overarching term that encompasses not only backups, but also snapshots and replication. In fact, ESG refers to the broad range of data protection methods and outcomes as a "Spectrum of Data Protection" (see Figure 1).

Figure 1. Spectrum of Data Protection



Source: Enterprise Strategy Group, 2016.

To be clear, the foundation of any “spectrum” or comprehensive approach to data protection starts with “backup.” But where applicable, in alignment with the diverse range of recoverability requirements that organizations have, backup alone may not be sufficient. Instead, consider strategies that leverage other recovery capabilities in complement to backup, ideally with automation or other integration between them.

Taking Advantage of the Speed and Density of the Latest Hardware

Upgrading the hardware that is used for mainframe backup and recovery adds upfront costs, but these costs are often offset by significant efficiency improvements and savings over time. For example, IBM’s latest tape library technology, the TS1150, is the fifth generation descendant of the IBM 3592 that supports up to 10 TB of native capacity per cartridge. It uses a 32-channel GMR head design and dual-port 8Gb FC to deliver up to 700 MBps of sustained performance with compression. That’s a 150% increase in capacity and a 44% increase in data rate compared to the previous generation technology. Supporting up to 16 drives per frame and 128 drives per library, a single library can store up to 526.5 petabytes of data. A tape library upgrade can be used to get backup and recovery jobs done faster, as well as to reduce the number of cartridges that need to be purchased, transported, and stored—all resulting in lower costs.

For the past two years, ESG’s annual IT spending intentions research has shown purchasing new technologies with better ROI as one of the top three most-cited planned methods of cost containment.⁴ While in years past, many cited cost containment strategies that involved slowing or abandoning efforts, modern IT organizations understand the value of embracing newer technologies that provide better agility while actually saving money well over any purchase price. Assessing the economic and operational value is equally as important as assessing the technical merits of any potential IT solution. In the meantime, do not presume that the status quo is less costly, or sufficient.

Maximizing Tape Media Utilization

Maximizing the amount of data that’s stored on each tape cartridge reduces mainframe backup and recovery costs (by requiring fewer cartridges) and increases the speed of backup and recovery jobs (by requiring fewer tape mounts). With these goals in mind, leveraging the almost nonexistent overhead compression that’s built into the latest enterprise-class tape libraries is an obvious best practice.

Tape stacking is another great way to increase the efficiency of your mainframe backup infrastructure. Tape stacking uses algorithms that optimize the number and variety of volumes stored on each cartridge with a goal of filling the tape as full as possible and making recovery operations run as fast as possible. State-of-the-art mainframe backup and recovery software with automated tape stacking support reduces costs and improves performance. It also makes the backup administrator more efficient since it reduces the time and complexity associated with

⁴ Source: ESG Research Report, 2016 IT Spending Intentions Survey, to be published.

setting up and executing “tape-stacked” backup and recovery jobs. A not so obvious benefit of maximizing tape media utilization is that fewer tapes are needed for off-site vaulting. This can result in substantial cost savings depending on the number of tapes sent off-site and managed by a third party.

With so much data being necessary for production and protection, many IT organizations are rediscovering the merits of modern tape solutions. As such, it exciting, albeit validating to industry veterans, to see continued innovation in tape cartridge speed, durability, and features, as well as enhanced access and usage methods (such as stacking and mountable file systems).

Remote Tape Backup

Remote tape backup is a term that’s often used to describe backup infrastructure and processes that leverage a tape library in a secondary data center that’s connected to a remotely mirrored storage array. This is a best practice that can reduce the amount of data loss after a disaster at a primary site. It can also be used to reduce the costs and risks associated with handling and transporting tapes.

Similar to the automation-related guidance earlier, one of the most impactful characteristics of a modern data protection strategy is the reduction of human interaction when possible (outside of expertise and assessment). Therefore, reducing tape handling through autoloaders on-premises, as well as remote tape copies (in lieu of packaging and transporting cartridges), will help ensure that the data is where it needs to be for whatever recovery is necessary for the business.

Multiple Backup Versions

Automation that simplifies the process of maintaining multiple backup versions adds another level of flexibility and recovery reliability. Multiple copies backup images on tape not only reduces the already low-risk of a data loss due to a media error during a recovery, it also simplifies the best practice of maintaining multiple copies of backups in multiple locations. While this best practice can be manually implemented with manual scripting, backup software that automates the creation, and tracking, of multiple backup versions adds another level of flexibility and reliability.

While it could sound trite to suggest making multiple copies under the pretext that “tape is cheap” there are certainly those who would dispute it based on the volume of data to be managed. That being said, it is undeniable that duplicate tapes achieved through automated or remote processes will undoubtedly be cheaper than the inability to restore due to media damage or misplacement.

Mirroring

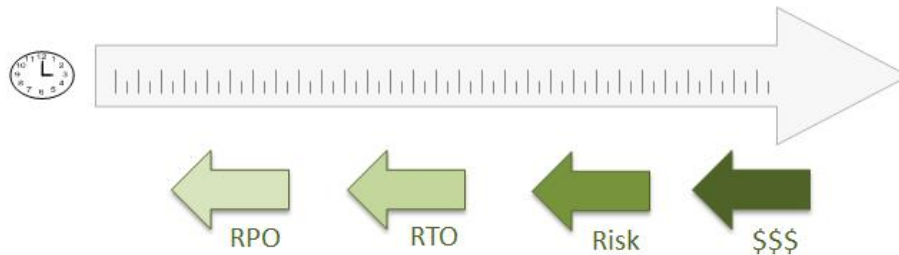
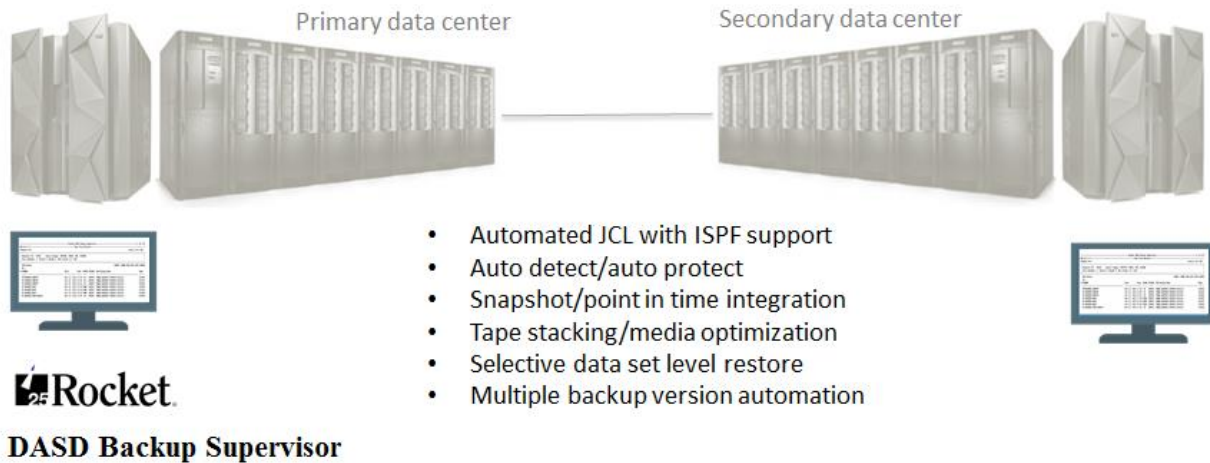
Many enterprises rely on data mirroring to another site as a disaster avoidance strategy. While mirroring is an effective component of an overall and comprehensive data protection strategy, enterprises should not rely on mirroring alone. Mirroring does not allow for easy restoration of individual data sets and mirroring will copy errors and corrupt data as well. A backup strategy should be implemented where multiple off-line backups are available so that enterprises can be more confident that a recent and clean copy of data is easily available for recovery.

Mirroring, which ESG’s spectrum would equate to “replication” combined with aspects of “availability,” can be very complementary to “backup” and “snapshot” mechanisms. By combining those technologies with business processes, one can achieve a diverse BC/DR capability that is unachievable with any single technology alone. As such, plan for “availability” of services and “preservation” of data in a comprehensive strategy.

Introducing Rocket Software DASD Backup Supervisor

DASD Backup Supervisor (DBS) is a state-of-the-art mainframe backup and recovery software solution. It runs on an IBM z Series mainframe in a primary and/or secondary data center to automate and optimize mainframe data protection services. ISPF with automated JCL support simplifies the job for backup admins as it reduces the risk of data loss for the business. DBS automates the detection of new DASD volumes, integration with disk-based snapshot technology (e.g., IBM FlashCopy), tape stacking, selective data set level restores, and multiple backup versions.

Figure 2. Rocket Software DASD Backup Supervisor



Source: Enterprise Strategy Group, 2016.

The benefits of modernizing mainframe backup and recovery with Rocket Software DASD Backup Supervisor and an optional tape hardware infrastructure upgrade are summarized in Table 1. The benefits can be simply summarized as less complexity, lower costs, shorter backup windows, and faster restores with less risk.

Table 1. Benefits of Modernizing Mainframe Data Protection with Rocket Software DASD Backup Supervisor

	Lower OpEx	Lower CapEx	Shorter Backup Window	Better RPO	Better RTO
Automated JCL with ISPF support	✓✓✓		✓	✓	✓
Auto detect/auto protect	✓✓✓			✓	✓
Snapshot integration			✓	✓✓✓	✓
Selective data set level restore		✓✓		✓✓	✓
Tape stacking				✓	✓✓✓
Tape infrastructure upgrade			✓	✓✓	✓✓✓

Source: Enterprise Strategy Group, 2016.

The Bigger Truth

Modernizing mainframe backup and recovery reduces risk and saves time and money as it enables IT administrators to spend more time on tasks that are strategic to the business, and less time on mundane jobs. With that in mind, here are some best practices to consider as you strive to reduce risk and cost with a modernized mainframe backup and recovery strategy:

1. Automate legacy JCL and scripting to save time and minimize mistakes.
2. Automate the detection of new DASD volumes to reduce complexity and improve recovery reliability.
3. Optimize how data is placed on tape cartridges (such as with tape stacking) to speed recoveries and reduce the number of tape cartridges you need to buy and transport.
4. Automate data set level restores for quick and easy operational recovery after an application error, data corruption, or accidental deletion.
5. Leverage remote tape backup with backup software running at a secondary data center to reduce not only the costs and risks associated with tape handling, but also the impact of data loss after a disaster at a primary site.
6. Upgrade your backup and recovery hardware to take advantage of the increased density, speed, and encryption capabilities of the latest tape libraries.
7. Automate point-in-time disk array snapshot integration (e.g., IBM FlashCopy) to shrink backup windows and enable faster recoveries with less data loss.
8. Automate the creation of multiple backup versions for increased flexibility and reliability.
9. Don't rely on data mirroring alone. While a great component of a comprehensive data protection strategy, mirroring replicates corrupted data and doesn't easily allow for granular data set restores.

If your organization relies on IBM z Systems as a platform for business-critical applications or a foundation for your next cloud, mobile, or big data initiatives, ESG recommends that you take a good look at how these best practices and DASD Backup Supervisor from Rocket Software can modernize your mainframe data protection strategy.



Enterprise Strategy Group | **Getting to the bigger truth.**