MAINFRAME BEST PRACTICES FOR AFFORDABLE BACKUP AND EFFICIENT RECOVERY

Mainframe teams these days are expected to contain backup and archiving costs while ensuring minimum downtime, especially in disaster recovery situations. While full-blown disasters may be rare, costly outages and interruptions are not, and a 2022 ITIC survey reveals just how expensive they are: 91 percent of mid-sized and large enterprises said that a single hour of downtime costs over $300,00, with 44% reporting that the cost was $1-5 million.

When designing a data management solution, it is important to explore cost-effective backup options that allow efficient recovery to cope with the enormous amounts of generated data. At the same time, it is also important to look into how to improve recovery efficiency, even if it might increase the direct backup costs.

Reducing backup costs

The total cost of ownership (TCO) of mainframe data management consists of several direct and indirect costs. Using the following methods, an organization can reduce backup costs while still meeting demanding recovery requirements:

- **Incremental backup:** Instead of backing up all data sets, implement solutions that support incremental backups and only back up data sets that have changed since the previous backup process.

- **Deduplication:** Significant storage space can be saved by eliminating duplicate copies of repeating data. It is therefore recommended to enable deduplication if your target storage system supports it.
- **Compression:** Another way to contain data management costs is to ensure that backup data is compressed before it is sent over the network to the storage system.
- **Leveraging commodity storage:** Maintaining tape-related hardware and software imposes substantial costs. Instead, a cost-efficient data management solution like BMC AMI Cloud Data securely delivers mainframe data to any cloud or on-prem storage system. This makes it possible to benefit from pay-as-you-go cloud storage instead of stocking up on tapes and VTLs.

On top of the above-mentioned practices to reduce the TCO of the data management continuum, one should also factor in the costs of archiving data for longer periods of time to meet regulatory requirements. For example, banks have to keep masses of archived data for many years to comply with regulations, most of which will never be accessed. As explained in this blog post, selecting the right kind of storage for this type of data can significantly affect backup costs.

Improving recovery efficiency

A more efficient recovery often requires additional measures in the backup stage, which might actually increase backup costs. However, the staggering costs of unplanned downtime alone can justify the investment, not to mention the heavy non-compliance fees. The following methods can be used for a more efficient recovery:

- **Write Once Read Many (WORM) storage:** Keeping backups on WORM storage in the cloud or on-premises prevents accidental or malicious erasure and tampering that will make recovery difficult, more expensive or subject to ransom. In the case of an event, immutable backup data in the cloud is available as soon as the system is up and running without needing to wait for archived data.
- **Multiple snapshots:** Taking snapshots, also known as flash copies, of volumes and data sets at regular intervals helps to maintain data set versioning, which is important for automated recovery processes. Snapshots also make it possible to recover a data set in case of logical failure.
- **Stand-alone restore:** Stand-alone restore allows bare-metal recovery from tape or cloud in cases of cyberattacks, disasters, and errors. Cloud-based backup platforms like BMC AMI Cloud enable initial program load (IPL) from a cloud server for a quick recovery that significantly reduces unplanned downtime.
- **End-to-end encryption:** End-to-end encryption reduces the risk of malicious data corruption that could cause logical failures and other problems making recovery scenarios more complex and more expensive. Encryption is also critical for meeting regulatory requirements regarding data security and privacy.