Data21

Risks and Hidden Costs of ZIP Compression on z/OS

[2020 Update]

This paper exposes inherent liabilities of legacy z/OS ZIP compression solutions which negatively impact batch window utilization, MLC, SLA's, data security and regulatory compliance.

White Paper by
David Kennedy
Data 21, Inc.
VP of Technical Sales

Introduction

Despite the growth of computer storage capacity and network speeds, data compression remains an essential tool for storing and transmitting ever-larger collections of data. The .zip format is designed for cross-platform exchange and efficient data storage for a set of related files; combining 85% to 95% average data compression, file management, and data encryption within a portable archive format.

The ready presence of .zip compatible utilities and processes across virtually all computing platforms, and ease of use for end-users of all technical competency levels, makes .zip files a simple solution for quickly facilitating efficient and secure exchange within the enterprise and beyond. Alleviating the need for and complexity of specialized network infrastructures, file-transfer or security software at both ends of an exchange. ZIP Utilities also serve as a very efficient and secure file archiving methodology. Producing easily manageable and highly transportable compressed and encrypted archives of any size and number of files.

For the above reasons most z/OS operations have been employing zip file compression in production for many years. However, it is important to recognize that the environment has changed dramatically since such solutions were originally implemented. Most legacy products in operation today lack the 21st century technologies necessary to support strategic business and regulatory mandates, such as mainframe cost reduction and data privacy assurance and compliance, imposed upon today's Mainframe management and the Enterprise in general. The technologies at issue are:

- ☑ Strong AES Encryption
- ☑ zEnterprise® Data Compression (zEDC)
- ☑ **IBM**® z Integrated Information Processor (**zIIP**)

If your current z/OS zip solution does not check ALL THREE boxes, read on. If it does, you are almost certainly paying too much for it and could benefit by contacting Data 21 about lowering this cost.

Strong AES Encryption

The Zip format provides an easy to implement persistent data encryption feature known as *Password Protection*. The addition of a few parameters is all it takes to virtually eliminate the threat of unauthorized access of the data, in-transit and at rest. Assuming strong encryption is applied that is. And this is the rub. Virtually every Zip product on every other platform supports the Zip AES encryption specification; and for good reason. Most z/OS Zip solutions provide only an old weak form of password encryption known as Zip 2.0 Encryption. This encryption cannot be expected to secure confidential information, is not security regulation compliant, and does not take advantage of the Mainframes cryptographic hardware, making it very slow and costly. Completely secure zip files require two things, well constructed hard to guess pass-phrases, and strong (preferably 256bit) encryption. If confidential data is being shared via weak encrypted or unencrypted zip files, the organization could be subject to the following risks.

> Zip 2.0 encryption format is known to be relatively weak, and cannot be expected to provide protection from individuals with access to specialized password recovery tools.
>
> - WinZip Computing

Data Breach

IBM's 2018 Cost of a Data Breach Study defines a data breach as "an event in which an individual's name and a medical record and/or a financial record or debit card is potentially put at risk — either in electronic or paper format." Sighting as the three main causes: malicious or criminal attack, system glitch, or human error. The costs of data breach vary according to the cause and the safeguards in place at the time of the data breach. The study found that the average total cost of a data breach, the average cost for each lost or stolen record (per capita cost), and the average size of data breaches have all increased beyond the 2017 report averages.

> According to the findings, data breaches continue to be costlier and result in more consumer records being lost or stolen, year after *year.*

Strong AES Encryption (cont.)

- Average total cost of a data breach: $3.86 million
- Average total one-year cost increase: 6.4%
- Average cost per lost or stolen record: $148
- One-year increase in per capita cost: 4.8%
- Likelihood of a recurring material breach over the next two years: 27.9%
- Average increase in data breach size: 2.2%

Other recent survey results show that about 60% of the companies that were subject to a data breach did not encrypt their data. Therefore, it is very important to encrypt data at rest and during transmission.

According to the study, 48% of data breach incidents involved a malicious or criminal attack, 27% were due to negligent employees or contractors (human Factor) and 25% involved system glitches, both IT and business process failures. The per capita cost of each root cause sighted as $157, $131 and $128 respectively. The study found that extensive use of encryption is the second most effective factor in decreasing per capita cost - reducing it by $13.1.

Non-Compliance

The costs of non-compliance can be extremely steep. Recent research indicates that failure to comply has become more costly than ever for organizations, far exceeding the costs of compliance.

Based on a recent report by research firm the Ponemon Institute and security company GlobalScape, the annual cost of non-compliance to businesses now runs an average of $14.8 million, a 45% increase since 2011.
The range can be anywhere from $2.2 million to $39.2 million.

The penalties incurred for non-compliance, according to the Ponemon report, are 2.71 times that the cost of compliance.

Virtually all data protection regulations, such as HIPAA, GDPR, and PCI-DSS call for the encryption of regulated data. For example, encryption is specifically referenced in the EU's General Data Protection Regulation (GDPR). Article 32 (1)(a) of GDPR guidelines calls for the encryption of personal data.

Strong AES Encryption (cont.)

HIPAA requires organizations use data encryption technology to protect sensitive patient information. PCI-DSS requires encryption of card-holder data transmitted over open, public networks and protection of stored card-holder data. In other words, cardholder information must be encrypted whenever it is stored or transmitted. The non-compliance costs come from the expenses associated with business disruption, productivity losses, fines, penalties, and settlement costs, among others. The most obvious and straightforward way to protect against unauthorized access and associated risks is application of persistent encryption.

Unfortunately, encryption isn't a common feature for data at rest among cloud providers. According to a recent study by Skyhigh Networks, although 81.8 percent of cloud providers encrypt data that's in transit, only 9.4 percent of them encrypt data at rest on their servers. Therefore it is up to the data owner to ensure it.

Most organizations today recognize that protecting only the data that is required to achieve compliance is a minimum threshold and that a move from selective encryption (protecting only specific types of data) to pervasive encryption (encrypting all data) is needed. A recent Data 21 poll of its z/OS customers revealed that the majority polled routinely zip confidential data for transfer to servers located within and/or outside the company. Given the nature and percentage of enterprise data resident and processed on the Mainframe, this was not surprising. What was surprising, in light of the all the above, is in most cases these files are not being password encrypted. Given how easy it is to implement and the benefits gained, the question is why?

One reason is many organizations today are focused on *Transmission Protection* rather than *Data Protection*. The fact is that data is more vulnerable to unauthorized access while stored on a server than during transmission.

The fact is that data is more vulnerable to unauthorized access while stored on a server than during transmission.

Secure FTP and Virtual private Networks *(VPN's)* provide only transmission protection and therefore fall short of delivering complete privacy assurance. Zip AES Encryption secures confidential data during transmission and storage.

Another reason may be the time and cost of compressing and encrypting. This is the subject of the following section.

Additional Hidden Costs

Reducing the usage of General Processors (GP's) delivers immediate direct savings. BMC's recent 2019 global mainframe survey found mainframe capacity is continuing to grow. MIPS are trending upward, putting more pressure on the budgets of organizations that rely on the mainframe. More than 61 percent of respondents say mainframe cost reduction is a top priority. Therefore it is important that the solutions deployed incorporate zSeries technologies that directly support this priority.

zEnterprise® Data Compression (zEDC)

zEDC data compression provides up to 118X reduction in CPU and up to 24X throughput improvement. The new free "on chip" zEDC feature of the IBM z15 platform replaces the extra cost zEDC cards of the past, making zEDC freely available to all and un-enabled mainframe zip compression solutions obsolete. If your current mainframe zip solution does not support zEDC, and your current machine does, or if not, a z15 is in your future, replacement of the un-enabled solution with an enabled one should be seriously considered.

Up to 80% reduced CPU cost compared to non-enabled compression solutions.

The significantly lower compression cost and incredible compression speed of zEDC not only serves to improve all the metrics of mainframe zip processing, but enables a more pervasive use of native mainframe compression.

IBM® z Integrated Information Processor (zIIP)

If zEDC is not available in your environment, zIIP is the next best option for reducing compression cost. According to industry calculations, hardware plus software costs for a zIIP processor is $150 to $200 per MIPS compared with $2,200 to $3,400 for a general purpose processor. As processes go, data compression is one of the most cpu intensive. Offloading compression cycles to lower cost zIIP's is the next best thing to zEDC.

Furthermore, in cases where GP's are knee-capped, compression time may be reduced as well. Since most installations have zIIP's available, running a solution that does not support them represents a considerable extra cost over one that does.

zIIP eliminates associated MLC charges and frees up more expensive GP white-space.

Our Solution

ZIP/390 MP is a relatively low cost fully supported Zip compression solution for z/OS and USS that delivers all three key technologies presented in this White Paper, and more. Superior features and attractive competitive product replacement pricing makes MP the ideal replacement for more expensive and/or less technologically advanced solutions.

Visit the ZIP/390 Page for more information.

About Data 21

Data 21, Inc. has specialized in the development and support of IBM Mainframe software solutions continuously, and under the same management, since 1980. Data 21's commitment to timely implementation of relevant IBM zSeries hardware and software advances within its products, combined with highly competitive pricing, results in superior products which consistently deliver the best cost performance in their respective niches.