Addressing Mainframe Data Management and Protection Challenges

Controlling escalating data center costs is one of the top concerns of IT executives today regardless of whether the data center is in a physical or cloud environment. There is constant pressure to do more with less and strict SLAs must be met, all while ensuring data security. Mainframe compression and encryption consumes valuable CPU and storage, in turn jeopardizing SLAs and increasing hardware and software costs. What’s more, encrypted data can’t be compressed resulting in more data and increased costs. Many organizations bypass data management and encryption in order to reduce CP consumption. Fortunately, PKWARE provides alternatives to control these costs.

PKWARE created the ZIP standard in 1986 and has a rich 27-year history of innovation built on its flagship products, PKZIP and SecureZIP. PKWARE’s customers use PKZIP and SecureZIP to reduce the cost of processing, moving and storing data and to eliminate the risks and costs associated with security breaches.

PKZIP provides data management and file compression, which makes reduces the size of large files while aggregating many files into a single zip file, simplifying data exchange minimizing the storage footprint.

SecureZIP adds strong security to the data management and compression capabilities of PKZIP by supporting encryption with PKI with X.509 digital certificates and PGP keys. File integrity is ensured with digital signing and authentication.

Leveraging the encryption capabilities of SecureZIP and System z®

SecureZIP for z/OS® has support for all hardware crypto capabilities on System z®, including clear key, secure key and protected key. Clear key uses CPACF, a set of cryptographic instructions available on all CPs. Secure key uses the CryptoExpress3 and 4S cards. Protected key uses a combination of CryptoExpress3 and 4S cards and CPACF. CPACF on all the machines has been enhanced to include support for the Advanced Encryption Standard (AES) for 128, 192 and 256-bit keys along with the Secure Hash Algorithm-1 (SHA-1) and SHA-2 (256, 384 and 512), and Pseudo Random Number Generation (PRNG).

SecureZIP for z/OS allows you to protect all your data using symmetric and asymmetric encryption as well as digital signing and authentication, using hardware that comes built into System z. This allows you to protect all your data on z/OS with very minimal overhead on your system.
ENCYPTHING WITH PASSPHRASES – SYMMETRIC KEY

With symmetric key cryptography, the key must be known to only the recipient and sender because the same key is used to encrypt and decrypt the data. This type of encryption is often referred to as “Passphrase” encryption because the key is essentially a passphrase that is shared with both parties. Symmetric key encryption is a simple and relatively fast method of encryption from a processing perspective, but requires exchanging the secret key ahead of time. This key exchange needs to be done through a pre-arranged, separate channel like email, phone, a separate FTP, etc. There is some risk involved in exchanging the key and it’s important that both parties keep the key safe because anyone who accesses it can decrypt the data.

ENCYPTHING WITH PUBLIC/PRIVATE KEY PAIRS – ASYMMETRIC KEY

Asymmetric key cryptography is where the enciphering key is different from, but closely related to, the deciphering key. This pair of keys is mathematically related such that data encrypted using one can only be decrypted using the other member of the pair. The key pair consists of what is known as a public key and a private key. As its name suggests, the public key is publicly viewable and can be freely given to others to encrypt information for the key owner who provided the public key. Distributing the public key is safe. It can only be used to encrypt for you or to authenticate your digital signature. The private key however, is a protected key used by the key owner to decrypt information encrypted using the matching public key. It is held in confidence and never shared with another user. Public/private key encryption makes it easier and safer for co-workers and business partners to encrypt data because it isn’t necessary to arrange the exchange of passphrase keys.

DIGITAL SIGNING AND AUTHENTICATION

Digital signing and authentication is often used with public/private key encryption. A digital signature is an electronic signature that validates data integrity and sender authenticity thereby providing trust in the information stored or transferred. Digital signing occurs when the data is hashed using a defined algorithm, for example SHA-1. The hash is encrypted using the sender’s private key and the digital signature is then packaged with the data. For authentication, the recipient would use the sender’s public key to verify the identity of the sender and decrypt the hash value. A new hash value is calculated from the data received and is compared to the hash from the sender. If they match, the data content is unchanged.
New Ways to Get More Out of Your Mainframe

IBM® recently announced a new solution to save storage space and improve wall clock time for compression. The announcement includes new hardware; the zBC12 and zEC12 GA2; a new operating system, z/OS v2.1; and the zEDC (zEnterprise Data Compression). PKWARE was selected as one of ten strategic partners included in the IBM announcement which outlines how customers will benefit from a significant increase in compression rates to manage data on z/OS in physical and cloud environments.

BOOST ELAPSED TIME PERFORMANCE UP TO TENFOLD WITH PKZIP AND SECUREZIP v15 WITH ZEDC SUPPORT

PKWARE was selected as one of ten strategic partners included in the IBM announcement which outlines how customers will benefit from a significant increase in compression rates to manage data on z/OS in physical and cloud environments. The zEDC is similar to the zIIP engine in that it allows customers to offload workloads without impacting CP consumption. The difference between the zIIP engine and the zEDC is that the elapsed time performance of compression is boosted up to tenfold with the zEDC. Support for the zEDC will be available in the fall of 2013 with PKZIP and SecureZIP v15 and includes accelerated deflate compression and automatic detection of the zEDC, meaning there is no requirement for existing PKZIP / SecureZIP customers to change JCL during the upgrade process. The z10-EC, z10-BC, z196, z114, zEC12 and zBC12 all support CP Assist for Cryptographic Functions (CPACF) and Cryptographic Express3 Coprocessor (CEX3C). The zEC12 and zBC12 additionally support the Cryptographic Express4 Coprocessor or CEX4C.

OFFLOAD PROCESSING TO LOWER THE COST OF COMPUTING WITH PKZIP AND SECUREZIP v14 WITH ZIIP SUPPORT

With the IBM® z Integrated Information Processors (zIIP), organizations can offload select workloads by making them zIIP eligible to free up general computing capacity and lower overall total cost of computing. The zIIP specialty engine is less expensive than general CP and doesn’t increase the MSUs/MIPS on the box. System z includes extensive hardware crypto capabilities, which reduce the overhead cost of encryption because sensitive data can be protected in an efficient way on the mainframe, rather than sending it to another server for encryption. 90% of compression processing is zIIP eligible, which translates to significant cost savings. Additionally, after compression, there is less data to encrypt. Support for the zIIP specialty engine is available today with PKZIP and SecureZIP v14 as well as all the hardware cryptographic support.
Real World Results

A LARGE COMMERCIAL BANK REDUCES A THREE HOUR PROCESSING WINDOW TO FOURTEEN MINUTES

A large financial institution that provides commercial banking services processes customer data on a daily basis. The Bank was delayed in delivering large reports to partners, missing SLAs. Their mainframe was running at peak capacity and the three hour SLA window was completely consumed by the processing of 100 files totaling 5GB in size. Each missed SLA resulted in a $1,000 penalty, adding up to $10,000/month.

With PKZIP v15 and the IBM zBC12 and zEDC, the Bank is now compressing files at 70% which takes one elapsed minute and 13 minutes to transfer. The bank is now easily meeting its three hour SLA window and fines associated with missed SLAs have disappeared. The bank can also now accommodate restarts and delays, a luxury that wasn’t an option when their entire SLA window was consumed by processing.

SECURING HEALTH CARE MAINFRAME DATA IN THE CLOUD

Our customer is a major health care provider. The organization processes massive amounts of Protected Health Information (PHI) on the mainframe. Faced with increasing costs, the health care provider began looking at the public cloud as an alternative; however they were concerned that the mainframe data could not be processed in a cloud environment.

SecureZIP provides the health care provider with efficient network transfer and storage while protecting sensitive PHI data in the cloud. Metadata is stored in the ZIP archive, allowing data structures that are foreign to non-mainframe platforms to be stored in the public cloud. When the health care provider restores the data to its mainframe, SecureZIP dynamically reallocates the data sets. In a sense, the SecureZIP archive is like a portable file system, allowing mainframe data to be consumed on other platforms, including the cloud. In addition, the organization can rest assured that the sensitive PHI data is secure.

ABOUT PKWARE: PKWARE, the industry leader in enterprise data security products, has a history rooted in innovation, starting with the creation of the .ZIP file in 1986. Since then, PKWARE has been at the forefront of creating products for reducing and protecting data — from Mainframes and zLinux to servers to desktops and into virtual and cloud environments.