Secure zOS Backup Data with SecureZIP Encryption

Z/OS backup processing is commonly done using such tools as FDR (Innovation) and DFSMSdss (IBM). This document highlights ways that you can integrate SecureZIP encryption into your existing z/OS backup procedures, including full volume backups done with FDR and DFSMSdss.

A Note Before We Start: Lowering the Cost of Encryption

Encryption isn't free. Encrypting (or decrypting) a file involves performing complex mathematical operations on every byte of data in the file. These operations inevitably add some processing cost.

The key to minimizing the overhead of encrypting is to be selective about what you encrypt. Customers tell us that less than 20% of the data in a typical backup is sensitive information that requires encryption. A much larger portion consists of such things as operating system and application program files that are not confidential and do not need to be encrypted.

You can distinguish sensitive data from data that is not confidential by classifying the data to be backed up. Various approaches to classifying data are possible, and the popular backup tools provide you with ready-made classification schemes. SecureZIP's powerful file selection features work with any classification system to help you select just the files you need to encrypt.

Specifying Files to Encrypt with SecureZIP

SecureZip provides sophisticated features for selecting files for encryption based on data classification or business continuity planning. You can specify an individual file name or use wildcard characters to specify a filename pattern, you can recurse directories, and so on. With SecureZIP, you can set selection filters on the files in your file system. Only files that match the specification criteria are included; files that don't match are skipped.

Wildcard characters enable you to use a single name containing wildcard characters to specify multiple data sets. The wildcard characters (?, *, and **) can be used in place of some or all of the characters in the name to match a range of filename characters instead of just a single, fixed character.

SecureZIP also enables you to set filters to specify cataloged files to exclude. These exclusion filters exclude matching files from the set of files to be encrypted when you request data sets for encryption processing through the catalog.

Working with DFSMS Classes

IBM's Data Facility Storage Management Subsystem (DFSMS) is an operating environment that is part of the base z/OS system and helps automate and centralize the management of storage. DFSMS provides control over the SMS classes, notably, the *data class*, the *storage class*, and the *management class*.

- The *data class* is a collection of allocation and space attributes z/OS uses when creating a data set. The data class allows the storage administrator to simplify and standardize the allocation of new data sets.

  When creating a data set, SecureZIP uses default values that are defined in SecureZIP installation parameters. These default values can be overridden by particular SecureZIP commands that provide allocation parameters. SecureZIP also provides commands that request DFSMS data classes to provide allocation parameters. DFSMS local installation rules can also override allocation commands, DD card parameters and data class selections in SecureZIP.
- The *storage class* provides the criteria that DFSMS uses in determining an appropriate location to place a data set or object. It is a collection of performance goals and device availability requirements that the storage administrator defines. Examples of storage class criteria include: the device performance, the amount of space available on the volume, and the availability of a data set or object on the device.
- The *management class* is a collection of management attributes, such as retention, migration, backup and unused space management. The storage administrator can associate a level of service with a data set or object that is independent of the physical location of the data set.

Organizations that use DFSMS classifications to select data for backup can use the SecureZip commands listed below to specify classes to include or exclude when creating or updating encrypted archives:

–ARCHIVE_DATACLASS,
–ARCHIVE_STORCLASS
–ARCHIVE_MGMTCLASS

Consolidating Sensitive Data

With SecureZIP, you can designate a volume or group of volumes as the target location in which to create an archive. This enables you to locate sensitive, encrypted data in a particular place, for easier management.

Options for Integrating Encryption

SecureZip can run as multiple, concurrent jobs to encrypt data into individual archives. Parallelizing encryption enables you to reduce the time required to encrypt.

SecureZip can also be integrated into application job streams so that the applications themselves take responsibility for doing encryption.

SecureZIP Encryption with DFSMSdss and FDR

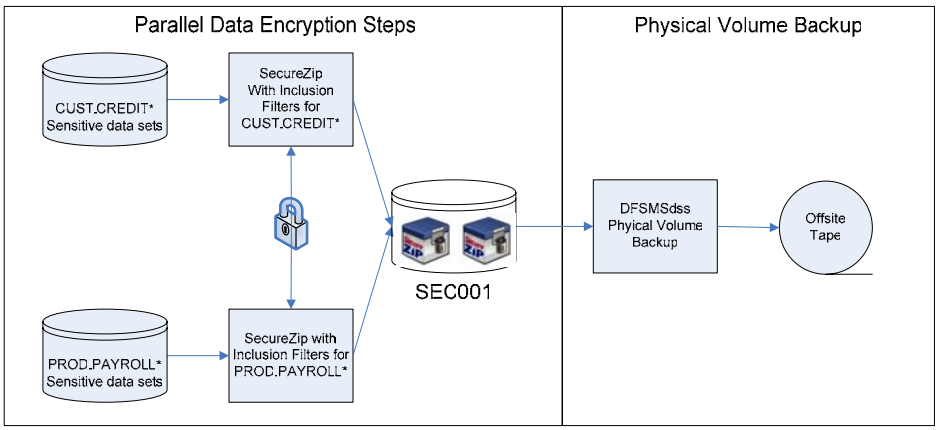
IBM's Data Facility Storage Management Subsystem Data Set Services (DFSMSdss; also referred to as DFDSS) is an optional feature of DFSMS that provides host system backup and recovery functions.

DFDSS and FDR offer two processing methods, *logical* and *physical*. The physical processing method accesses the data at the track-image level of the device. The logical processing method accesses the data at the data-set level, independent of the physical medium in which the data is stored.

SecureZIP can be used with either processing method, with either DFDSS or FDR. In each case, you first use SecureZIP to encrypt sensitive data to a designated location. You then run DFDSS or FDR to do the backup, including the encrypted archives.

Physical Volume Backups

The diagram below shows SecureZIP integrated into a backup that uses the physical processing method.



In this example, two SecureZip jobs run in parallel to encrypt sensitive data using inclusion and exclusion filters.

The first SecureZIP job encrypts all the data sets that start with CUST.CREDIT* into a single encrypted archive and places the archive on the SEC001 disk volume.

The second SecureZIP job encrypts data sets that start with PROD.PAYROLL* into a single encrypted archive and places the archive on the same SEC001 disk volume.

DFSMSdss or FDR then does a physical volume backup of SEC001 to tape. The parallelization of the SecureZIP jobs to encrypt the data, along with the file name inclusion and exclusion filters, enable storage administrators to back up only the sensitive data, thus helping to keep the size of the backup window to a minimum. A DFSMSdss or FDR physical volume backup also keeps tape utilization to a minimum.

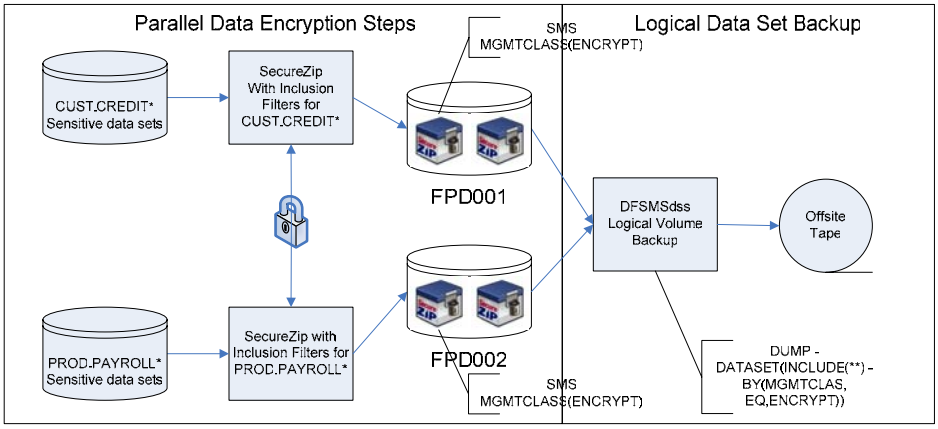
As a variation on this approach, you can include the SecureZIP command

–ARCHIVE_STORCLASS(ENCRYPT)

and then perform physical volume backups on the volumes included in the ENCRYPT storage class.

Logical Processing Method

SecureZIP encryption can be parallelized when the logical processing method is used, too. Here the backup level of granularity is the data set rather than the physical device. The following diagram shows SecureZIP integrated into a logical processing model.



In this example, multiple SecureZIP data encryption jobs still take place in parallel. The same inclusion and exclusion filters are used as in the physical processing method example. The biggest difference is that we specify

–ARCHIVE_MGMTCLASS(ENCRYPT)

to assign an SMS management class of ENCRYPT to all the encrypted archives. We include all data sets with an SMS management class of ENCRYPT.

Whatever backup approach you use, SecureZIP enables you to add secure encryption of sensitive data with no radical change to your existing procedures.