Data set encryption for IBM® z/OS® V2.2 Frequently Asked Questions

Contents

OVERVIEW

An overview of data set encryption related to IBM z/OS V2.2.

What is data set encryption provided in the updates to IBM z/OS V2.2?

Extensive use of encryption is one of the most effective ways to help reduce the risks and financial losses of a data breach and help meet complex compliance mandates.

Enhanced data protection for many z/OS data sets gives users the ability to encrypt data without needing to make changes to applications to embed encryption APIs within applications.

z/OS data set encryption, through z/OS system authorization facility (SAF) controls and RACF® or equivalent function along with SMS policies, allows you to identify new data sets or groups of data sets to be encrypted. This means that you are able to protect data residing on disk from being viewed by unauthorized users in the clear.

Authorization is based on access to the key label that is associated with the data set and used by the access methods to encrypt and decrypt the data.

z/OS data set encryption supports VSAM and sequential extended format data sets. Supported databases and middleware data sets appear elsewhere in this document.

What are some of the design advantages built into z/OS data set encryption?

z/OS data set encryption:

- Uses CPACF and protected key, which means that key material is not visible in clear text format, offering a higher level of protection along with the high throughput of encryption using CPACF
- Is designed to protect data in a way that is aligned with customers' current access control mechanisms offering a more straightforward configuration experience
- Is designed to perform efficiently at speed
- Has the ability to enable encryption without requiring application or database changes
- Allows data to remain encrypted throughout its journey. For instance, with z/OS data set encryption any data replicated through PPRC or XRC, or backed up or migrated, remains encrypted
- In-memory buffer content is not encrypted which means that every data access does not require an encrypt or a decrypt operation; this design helps reduce the overall cost of encryption
- Can be configured such that encryption keys are owned and managed by logical organizational environment (e.g., production versus test) providing cryptographic separation from other environments
- Can help simplify compliance efforts

How is data set encryption different from other encryption software that IBM offers?

Data set encryption enables encryption of files in bulk through the access method as opposed to encrypting a single field or row at a time. z/OS data set encryption is designed to offer high throughput, low cost encryption. It is intended to be more accessible to the organization than many other forms of encryption. For instance, z/OS data set encryption is designed to be transparent to the application, requiring no changes to application code. z/OS data set encryption enables customers to encrypt data at course scale without the need to perform data identification and classification first.

Is data set encryption a separately priced feature?

No, data set encryption is delivered through the base DFSMS™ component of z/OS V2.2. Refer to the REQUIREMENTS and SUPPORT section on page 3 for requisite service to z/OS V2.2 related to data set encryption.

Clients are advised to order a Crypto Express Adapter priced feature in order to use protected key.

REQUIREMENTS and SUPPORT

Hardware and software service requirements for data set encryption related to z/OS V2.2.

What are the crypto adapter requirements for z/OS data set encryption?

Data set encryption always uses CPACF protected keys for keys in memory. Protected keys ensure the key is not visible to applications or to the operating system.

Protected keys, based on secure keys, offer the security capabilities of the Crypto Express adapter along with the performance characteristics of on-chip crypto using CPACF. It is strongly recommended to use the Crypto Express adapter to protect secured keys. A Crypto Express 3 or higher level adapter is required for this purpose.

What Crypto Express "mode" is required to support z/OS data set encryption? Is it possible to have another mode configured concurrently on the same Crypto Express adapter?

z/OS data set encryption requires the Crypto Express feature to be configured as a CCA coprocessor. A given Crypto Express feature may be configured as a CCA coprocessor, an EP11 coprocessor, or an accelerator, but can only be configured as one type at a time.

What is the minimum and recommended hardware (HW) for z/OS V2.2 data set encryption?

Table 1 Minimum and Recommended Hardware for data set encryption for z/OS V2.2

IBM Z	CPACF	Crypto Express[1]	
	Notes	*Minimum Required*	*Recommended*
z196, z114 or later	FC 3863	CEX3 FC 0864 or FC 0871	CEX3 FC 0864 or FC 0871
EC12, BC12 (zEC12, zBC12)	FC 3863	CEX3 FC 0864 or FC 0871 CEX4S FC 0865	CEX4S FC 0865
z13	FC 3863	CEX5S FC 0890	CEX5S FC 0890
z14	FC 3863	CEX5S FC 0890 or CEX6S FC 0893	CEX6S FC 0893

[1] Secure-key is *strongly recommended* for production environments. Clear key can be used in dev/test

What is the required z/OS software for z/OS V2.2 data set encryption?

Data set encryption for z/OS V2.2 is available via OA50569, "NEW FUNCTION - THE DFSMS Z/OS DATA SET ENCRYPTION ENHANCEMENT," available at the following URL: http://www-01.ibm.com/support/docview.wss?crawler=1&uid=isg1OA50569.

OA50569 has two applicable component levels: one for z/OS V2.2 (R220 PSY UA92779) and one for z/OS V2.1 toleration (R210 PSY UA92778).

*Note: The DFSMS portion of APAR OA50569 pulls in the pre/co-req APAR(s) along with dependency APAR(s); however, depending on the level of service already on a system, additional service may be required. SMP/E APPLY or REPORT MISSINGFIX can be used to identify service needed for the fix category IBM.Function.DataSetEncryption. For more information on fix categories, refer to the resource, *IBM Fix Category Values and Descriptions for z/OS*.

What does toleration/coexistence support for z/OS V2.1 mean?

z/OS V2.1 with service applied is designed to be able to support z/OS data set encryption in toleration mode, meaning it can read from and write to encrypted data sets but not create new encrypted data sets.

Toleration/coexistence PTFs are available via the z/OS V2.2 data set encryption APAR provided in the previous question.

What changes are needed to make sure that encrypted data sets created on a current IBM Z server are accessible to down-level servers with prior cryptographic capabilities?

IBM Z encryption hardware (Crypto Express and CPACF) is typically downward compatible. If prior generation IBM Z servers meet the minimum hardware and software requirements for z/OS data set encryption, they would be able to access encrypted data sets produced by z/OS data set encryption.

What files and databases can leverage z/OS data set encryption?

z/OS data set encryption supports sequential extended format data sets accessed through BSAM and QSAM, as well as VSAM extended format data sets accessed through base VSAM and VSAM RLS.

This is aligned with clients' most immediate need to protect data associated with databases, CICS® VSAM applications, and batch workloads.

Data set encryption is transparent to applications and data bases that call documented access method APIs for VSAM, QSAM and BSAM access methods. Applications that use the licensed Media Manager interfaces to access encrypted data sets require changes.

Are there plans for IBM CICS Transaction Server to support z/OS data set encryption?

Yes, all in-service releases of CICS Transaction Server for z/OS (CICS TS) will support data set encryption, and do not require CICS product APARs or PTFs to support data set encryption.

CICS TS V5.4 planning and using information for data set encryption is available at the following CICS TS Knowledge Center link: https://www.ibm.com/support/knowledgecenter/SSGMCP_5.4.0/configuring/cics/data-set-encryption-process.html.

Note: The planning and using information at the CICS TS V5.4 Knowledge Center is applicable to all in-service releases of CICS TS.

Are there plans for IBM Db2 to support z/OS data set encryption?

Yes, IBM Db2 is designed to transparently encrypt data at rest without database downtime or requiring the administrator to redefine objects, which could cause disruption to operations. This includes the ability to transparently encrypt its logs, catalog, directory, tables and indices including all data types such as large binary objects transparently. In addition, for maximum availability, rekeying of data keys can be performed non-disruptively without taking Db2 databases offline.

IBM Db2 for z/OS v11 for z/OS and IBM Db2 v12 for z/OS (at M100 level) support z/OS V2.2 data set encryption with the following Db2 service:

- Db2 V11 APAR PI81900, "DB2 11 FOR Z/OS NEW FUNCTION"
- Db2 V12 APAR PI81907 (for M100 –M501 level), "DB2 FOR Z/OS NEW FUNCTION"

Db2 planning and using information for data set encryption is available at the following Db2 Knowledge Center links:

- https://www.ibm.com/support/knowledgecenter/SSEPEK_11.0.0/seca/src/tpc/db2z_dfsmsencryptionsupport.html (Encrypting your data with z/OS DFSMS data set encryption, Db2 V11 Knowledge Center)
- https://www.ibm.com/support/knowledgecenter/SSEPEK_12.0.0/seca/src/tpc/db2z_dfsmsencryptionsupport.html (Encrypting your data with z/OS DFSMS data set encryption, Db2 V12 Knowledge Center)

Are there plans for IBM IMS to support z/OS data set encryption?

Yes, Information Management System (IMS) V13, V14, and V15 support z/OS V2.2 data set encryption.

IMS V13, V14, and V15 do not require IMS product APARs or PTFs to support data set encryption.

IMS planning and using information for data set encryption is available at the following IMS Knowledge Center links:

- https://www.ibm.com/support/knowledgecenter/SSEPH2_15.1.0/com.ibm.ims15.doc.sag/system_admin/ims_dataset_encryption.htm
- https://www.ibm.com/support/knowledgecenter/SSEPH2_14.1.0/com.ibm.ims14.doc.sag/system_admin/ims_dataset_encryption.htm
- https://www.ibm.com/support/knowledgecenter/SSEPH2_13.1.0/com.ibm.ims13.doc.sag/system_admin/ims_dataset_encryption.htm

Note: The information at the IMS Knowledge Center also summarizes IMS data sets that do and do not support data set encryption.

Are there plans for IBM MQ to support z/OS data set encryption?

Yes, IBM MQ versions 8.0.0 and 9.0.0 (Long Term Support and Continuous Delivery Release) supports z/OS V2.2 data set encryption.

MQ versions 8.0.0 and 9.0.0 (LTS and CDR) do not require MQ product APARs or PTFs to support data set encryption.

The following information summarizes MQ data sets that do and do not support data set encryption.

VSAM and sequential datasets used in an MQ subsystem, such as the BSDS, sequential files holding system configuration (MQSC) commands read at startup via CSQINPx DDNAMEs and the MQ archive logs, often used for long term archival of MQ log data for audit purposes, can be encrypted via data set encryption by allocating a data set with key label.

The z/OS dataset encryption feature can be applied to archive logs for queue managers running at V8 or later. These archive logs must be allocated using Automatic Class Selection (ACS) routines to a data class defined with EXTENDED attributes and a data set key label that ensures the data is AES encrypted.

The MQ data sets which provide the primary storage of message data cannot be encrypted using data set encryption. These are:

- Page sets
- Active logs
- Shared Message Data sets

Customers requiring encryption of message data at rest are encouraged to use IBM MQ's Advanced Message Security (AMS) offering which provides policy based, application transparent, end-to-end encryption of message payload throughout an MQ network.

It is not possible to use DSE to encrypt MQ archive logs prior to MQ V8.

For more information on MQ and z/OS V2.2 data set encryption, refer to the MQ Knowledge Center at https://www.ibm.com/support/knowledgecenter/en/SSFKSJ_9.0.0/com.ibm.mq.pro.doc/q004180_.htm
.

Are there plans for IBM zSecure support for z/OS data set encryption?

Yes, IBM Security zSecure suite V2.3 helps administer and audit data set encryption capabilities. zSecure allows clients to immediately audit and monitor usage of data set encryption features. zSecure can help customers understand which systems and which users can decrypt data, aiding in the administration and control of data set encryption. zSecure also helps with direct navigation from data set encryption key labels to the administration of key label protection profiles. In addition, key labels can be enriched with selectable key algorithms and key length fields. zSecure also collects, formats and enriches data set encryption information that is sent to SIEMs including IBM QRadar® for enhanced enterprise-wide security intelligence.

The information listed next are the zSecure products that support z/OS V2.2 data set encryption, listed by zSecure product/program ID:

- 5655-N16 IBM Security zSecure Admin 2.3.0
- 5655-N17 IBM Security zSecure Audit for RACF 2.3.0
- 5655-N17 IBM Security zSecure Audit for ACF2 2.3.0
- 5655-N17 IBM Security zSecure Audit for Top Secret 2.3.0
- 5655-N19 IBM Security zSecure Command Verifier 2.3.0
- 5655-N20 IBM Security zSecure Visual 2.3.0
- 5655-N21 IBM Security zSecure Alert for RACF 2.3.0
- 5655-N21 IBM Security zSecure Alert for ACF2 2.3.0
- 5655-AD8 IBM Security zSecure Adapters for SIEM - ACF2 2.3.0
- 5655-AD8 IBM Security zSecure Adapters for SIEM - RACF 2.3.0
- 5655-AD8 IBM Security zSecure Adapters for SIEM - Top Secret 2.3.0

The zSecure products listed previously are also available as the following zSecure 2.3.0 bundles:

- 5655-N23 IBM Security zSecure Administration
- 5655-N24 IBM Security zSecure Compliance and Auditing
- 5655-N25 IBM Security zSecure Compliance and Administration

Are there plans for IBM QRadar support for z/OS data set encryption?

IBM QRadar is a Security Information Event Manager (SIEM). It allows for enterprise collection of all security events which are then stored to be monitored, analyzed and reported on. When events are sent to QRadar a device support module (DSM) specific to the device parses and normalized the event data into QRadar terms. There are plans for the new data set encryption event types, key label, key algorithm and key algorithm to be supported by the IBM z/OS DSM. This support will enable QRadar monitoring, analyzing and reporting on pervasive encryption statistics. At this time there is sample support available upon request. Please contact David Rossi at dzrossi@us.ibm.com for more details.

Would customers be able to use both encryption and compression?

Yes. Since encrypted data does not compress, data must be compressed first before it is encrypted. For encrypted, compressed data sets the access methods perform both compression and encryption operations and will compress data before the data is encrypted, and decrypt data before it is decompressed.

Where do I find publication information for z/OS V2.2 for data set encryption?

Publication information for z/OS V2.2 data set encryption is provided as a single PDF document with the associated data set encryption APAR. The following list provides both a direct link the PDF and a link to the associated z/OS data set encryption APAR:

- http://publibz.boulder.ibm.com/zoslib/pdf/OA50569.pdf
- http://www-01.ibm.com/support/docview.wss?crawler=1&uid=isg1OA50569

Where can I learn more about crypto and data set encryption?

To learn more about data set encryption, refer to the following page at the IBM Crypto Education Wiki: *Pervasive Encryption – Data Set Encryption*. This resource provides information related to configuring Crypto Express cards, configuring and starting the IBM Integrated Cryptographic Service Facility (ICSF), loading AES master key, initializing the Cryptographic Key Data Set (CKDS), generating a secure AES data key, protecting data sets with secure keys, authorizing users to keys, allocating encrypted data sets, and reading/writing encrypted data sets.

OPERATIONAL CONSIDERATIONS

Operational considerations for data set encryption related to z/OS V2.2.

How should my customer modify their cryptographic environment to prepare for z/OS data set encryption?

Customers can install Crypto Adapters on supported servers and can also plan to configure their environment to support protected key environments. Customers need to install and configure ICSF. ICSF callable services and programs help users generate, maintain, and manage keys. ICSF provides APIs by which applications request cryptographic services. Customers must also configure a CKDS data set to store keys. Data set encryption requires the use of AES master keys.

Is there CPU overhead when using z/OS data set encryption?

Encryption typically consumes processor cycles. z/OS data set encryption is designed for performance and efficiency offering design elements to reduce cost. For instance, z/OS data set encryption is performed at the I/O buffer write level in order to keep encryption more cost effective than encrypting a single record at a time. The use of the Crypto Express adapter is optimized and is used initially at data set open time to handle processing of the key after which CPACF is used for high performance and efficient data set encryption. ICSF is also optimized to cache keys so that when a data set is re-opened, the protected key is accessible, avoiding additional I/O costs. An enhanced zBNA tool is available to help users and IBMers estimate the CPU cost of encryption as part of their planning efforts.

Is it possible to backup and restore encrypted data sets "as-is," without decryption?

Yes, DFSMSdss™ and DFSMShsm™ provide a number of utilities and copy functions such as copy, dump, restore, PPRC and more that support encrypted data sets without the need to access data in the clear. Data sets remain encrypted throughout this processing. The ability to perform these utility functions without requiring key label access to decrypt data is an advantage and can help with compliance efforts.

Are there any planned tools to assist clients with estimating the CPU cost of encryption?

Yes. The zBNA tool, which is a customer accessible tool, has been enhanced to help estimate additional CPU incurred when enabling encryption for certain workloads. It can also be used to help estimate CPU costs for both data set encryption and also for coupling facility encryption. Customers will need to use the zBNA V1.8.1 tool with DFSMS, RMF™, and XES PTFs applied.

> Note: Before zBNA can be used for data set encryption estimation, the requisite PTFs must be applied. The requisite PTFs ensure the SMF data that is generated for the tool contains the appropriate fields needed to do the estimation.

IBM z Systems Batch Network Analyzer (zBNA) Tool official website: http://www-03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/PRS5132

How can I avoid delays in z/OS initialization and termination when using data set encryption?

Customers need to ensure that ICSF is started early in the IPL process to avoid delays in z/OS initialization and termination. This is especially true if customers plan to encrypt SMF data sets or other data sets used during z/OS initialization. As such, it is highly recommended the command **S CSF,SUB=MSTR** (or appropriate PROC name) is placed early in the COMMNDxx member to ensure there is minimum delay in z/OS initialization. Specifying SUB=MSTR is necessary to allow ICSF to start before JES. Furthermore, during z/OS system shutdown, ICSF should be one of the last features to be terminated so that dependent functions are not impacted. It is highly recommended that ICSF be brought down after terminating the JES address space and after initiating SMF halt processing. Note that since ICSF is brought down after SMF is halted, there may not be an SMF record cut for the termination of ICSF.

Can troubleshooting data be sent to IBM when using z/OS data set encryption?

Yes, troubleshooting data can be sent to IBM when using z/OS data set encryption; however, to ensure that IBM Support is able to read the data that is in the encrypted data sets, refer to the information in the following IBM Technote (prior to sending troubleshooting data): Sending troubleshooting data to IBM when using z/OS data set encryption.

KEYS and KEY MANAGEMENT

Keys and key management considerations for data set encryption related to z/OS V2.2.

Does z/OS data set encryption allow for the use of different keys to protect different data sets?

Yes, customers can assign different keys using different RACF profiles and DFSMS classes. Customers do not need to define a unique key for each and every data set encrypted, and groups of data sets can share common keys. This can help simplify administration.

How do customers create keys and key labels?

Clients will be able to define, generate and store a key in ICSF. ICSF web deliverable HCR77C1, available later in 2017, offers enhancements to help simplify key management. The CKDS browser is designed to make it easier for ICSF administrators to manage the life cycle of their cryptographic key material that resides in the CKDS. The CKDS browser can help customers new to ICSF provision encryption keys for applications and for use by z/OS.

Clients can also use EKMF to generate and manage keys. Once the key label is defined, the key label would be associated with a particular data set or group of data sets through several methods offering flexibility and choice. Clients can also use ICSF services to help manage keys.

What type of encryption does z/OS data set encryption use?

z/OS data set encryption is designed to use AES 256, considered one of the strongest.

Is it possible to expire, revoke, and/or reissue keys related to z/OS data set encryption?

Newer versions of ICSF support key record metadata for expiring and archiving encryption keys. Enterprise key management systems can also provide this capability. It will be possible to rekey data by generating a new key and key label, assigning a new key label to a new data set and migrating data encrypted under old key to the new key by copying the data set to the newly created data set.

SERVICES

Services considerations for data set encryption related to z/OS V2.2.

Are there IBM resources available to help clients assess their readiness for data set encryption and to assist in addressing any gaps?

A. Yes, the IBM Systems Lab Services team will assess your needs for dataset encryption and provide the appropriate deployment for your situation. You can contact IBM Systems Lab Services via the internet at https://www.ibm.com/it-infrastructure/services/lab-services or send an email to ibmsls@us.ibm.com.

ADDITIONAL INFORMATION

Additional information for data set encryption related to z/OS V2.2

Are there restrictions specific to data set encryption for z/OS V2.2?

Yes, the following list are restrictions related to z/OS V2.2 data set encryption:

- The z/OS Distributed File Service (DFS) Server Message Block (SMB) server does not support access to encrypted data sets. This is a permanent restriction. SMB is being stabilized and no new support is being added
- z/OS Network File System will not support access to encrypted z/OS data sets regardless of the z/OS NFS Server configuration based on its "security" site attribute. The restriction will be lifted in APAR OA53223 in 4Q2017 for z/OS NFS Server configured with "security(saf)" or "security(safexp)"
- zFS file system encryption is only allowed for a z/OS 2.3 site. zFS file systems should never be encrypted unless every system at a customer site is z/OS 2.3 or later that will access that file system and the customer is confident that they will not need to migrate back to a prior release of z/OS. zFS will not allow any encrypted file system to be mounted on a z/OS 2.2 or prior release

Do non-IBM vendor products support z/OS V2.2 data set encryption?

For non-IBM vendor product support related to z/OS V2.2 data set encryption, please check with your vendor or ISV.

What is the difference between data set encryption in z/OS V2.2 and pervasive encryption in the July 2017 IBM Z announcements?

Data set encryption, which is one aspect of pervasive encryption, is available in z/OS V2.2 when the requisite service is applied. Refer to the REQUIREMENTS and SUPPORT section on page 3 for requisite service to z/OS V2.2 related to data set encryption.

For what was announced related to pervasive encryption, refer to the July 17, 2017, software announcement*, IBM z/OS Version 2 Release 3 - Engine for digital transformation*.

IBM Corporation
New Orchard Road
Armonk, NY 10504

U.S.A.

Produced in the United States of America,
08/2017

All statements regarding IBM’s future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates. It is the user’s responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.