z/OS
Version 2 Release 4

Pervasive Encryption for IBM Z

Note

Before using this information and the product it supports, read the information in “Notices” on page 17.

© Copyright International Business Machines Corporation 2019, 2019.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

About the Pervasive Encryption for IBM Z Content Solution

This information supports z/OS® (5650-ZOS) and contains information about pervasive encryption for IBM Z®.

Purpose of this information This information is a collection of the information that you need to understand to exploit pervasive encryption for IBM Z®. Some of the information contained in this content solution also exists elsewhere in the z/OS library.

Who should read this information This information is intended for z/OS administrators who are responsible for encryption of files in bulk using z/OS data set encryption, encryption of data structures through the Coupling Facility, cryptographic state of connections through z/OS Communications Server, and anyone who manages cryptographic keys.

Related information

For an interactive starting point, and access to a variety of resources related to Pervasive Encryption for IBM Z, see Pervasive Encryption for IBM Z (www.ibm.com/support/z-content-solutions/pervasive-encryption/).

© Copyright IBM Corp. 2019, 2019

How to send your comments to IBM

We appreciate your input on this information. Please provide us with any feedback that you have, including comments on the clarity, accuracy, or completeness.

Use one of the following methods to send your comments:

Important: If your comment regards a technical problem, see instead "If you have a technical problem" on page vii.

- Send an email to mhvrcfs@us.ibm.com.
- Send an email from the Contact the z/OS team web page (www.ibm.com/systems/campaignmail/z/zos/contact_z).

Include the following information:

- Your name and address
- Your email address
- Your phone or fax number
- The title:

  Pervasive encryption for IBM Z Content Solution
- The topic and page number or URL of the specific information to which your comment relates
- The text of your comment.

When you send comments to IBM®, you grant IBM a nonexclusive right to use or distribute the comments in any way appropriate without incurring any obligation to you.

IBM or any other organizations use the personal information that you supply to contact you only about the issues that you submit.

If you have a technical problem

Do not use the feedback methods that are listed for sending comments. Instead, take one or more of the following actions:

- Visit the IBM Support Portal (support.ibm.com).
- Contact your IBM service representative.
- Call IBM technical support.

© Copyright IBM Corp. 2019, 2019

Chapter 1. Introduction to pervasive encryption for IBM Z

What is pervasive encryption for IBM Z?

Related information

Pervasive Encryption for IBM Z is a consumable approach to enable extensive encryption of data in-flight and at-rest to substantially simplify encryption, and reduce costs associated with protecting data.

Pervasive Encryption for IBM Z can be used in conjunction with full disk and tape encryption, database encryption, and application encryption.

Full disk and tape encryption
Full disk and tape encryption protects against intrusion, tamper or removal of physical infrastructure.

File or data set encryption
File or data set encryption is managed through z/OS, and provides simple policy controls that allow clients to protect data in mission critical databases including DB2®, IMS and VSAM. Additionally, "z/OS data set encryption" on page 3 gives clients the ability to eliminate storage administrators from the compliance scope.

Database encryption
Database encryption provides selective encryption and granular key management control of sensitive data.

Application encryption
Application encryption is used to encrypt sensitive data when lower levels of encryption are not available or suitable.

z/OS provides the following capabilities for pervasive encryption: "z/OS data set encryption" on page 3, "z/OS Coupling Facility encryption" on page 13, and "z/OS Encryption Readiness Technology (zERT)" on page 13.

For access to interactive resources related to Pervasive Encryption for IBM Z, see Pervasive Encryption for IBM Z (www.ibm.com/support/z-content-solutions/pervasive-encryption/).

© Copyright IBM Corp. 2019, 2019

Chapter 2. IBM Z pervasive encryption with z/OS data set encryption

z/OS data set encryption

Introduction to z/OS data set encryption

z/OS data set encryption enables encryption through the DFSMS access methods. You can use z/OS data set encryption to encrypt the following types of data sets:

- Sequential extended format data sets, accessed through BSAM and QSAM
- VSAM extended format data sets (KSDS, ESDS, RRDS, VRRDS, LDS), accessed through base VSAM and VSAM RLS

Encrypted data sets must be SMS-managed extended format. They can be compressed format, also.

Data set encryption relies on ICSF and AES 256 bit encryption DATA keys stored in a CKDS. In addition, data set encryption takes advantage of the security capabilities of the Crypto Express® adapter along with the performance characteristics of on-chip crypto using CPACF.

Application or component specific requirements

Refer to the following resources for IBM application or component specific requirements and exploitation of data set encryption:

- Considerations for encrypting log stream data sets
- Encrypting and compressing zFS file system data
- Security concepts in IBM MQ for z/OS (www.ibm.com/support/knowledgecenter/en/SSFKSJ_9.0.0/com.ibm.mq.pro.doc/q004180_.htm)
- Encrypting data sets (www.ibm.com/support/knowledgecenter/SSGMCP_5.4.0/configuring/cics/data-set-encryption-process.html)
- Data set encryption support for IMS (www.ibm.com/support/knowledgecenter/SSEPH2_15.1.0/com.ibm.ims15.doc.sag/system_admin/ims_dataset_encryption.htm)
- Encrypting your data with z/OS DFSMS data set encryption (www.ibm.com/support/knowledgecenter/SSEPEK_11.0.0/seca/src/tpc/db2z_dfsmsencryptionsupport.html). Refer to the “IBM Db2 support for z/OS data set encryption” on page 12 section for details.

Core infrastructure requirements

The recommended platform for dataset encryption is z14, CPACF, and CryptoExpress 6s, with z/OS 2.3, and ISCF HCR77C1. Using the highest levels of hardware, firmware, and software ensures the most scalable performance and enhanced system and security management. Data set encryption is also available on earlier processors with CPACF and the appropriate Crypto Express co-processors. Implementing data set encryption on earlier processors will provide a base for establishing appropriate processes and procedures prior to enabling data set encryption.

IBM Integrated Cryptographic Service Facility (ICSF), IBM Crypto Express cards, and a supported System Authorization Facility (SAF) (e.g. IBM RACF® or equivalent product), are required for data set encryption.

For an introduction to ICSF, refer to *z/OS Cryptographic Services ICSF System Programmer's Guide* , and the *z/OS Cryptographic Services ICSF Administrator's Guide*.

If ICSF is not installed, refer to the following resources for planning and installation information:

- Steps prior to starting installation

© Copyright IBM Corp. 2019, 2019

- Installation, initialization, and customization

Additional ICSF configuration and starting information is available at the IBM Crypto Education Wiki page, IBM Crypto Education Community (www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/W7df80301055d_495b_bb88_a0a2f84757c5).

If you have installed Integrated Cryptographic Service Facility (ICSF) function modification identifier (FMID) HCR77C1, then refer to the ICSF documentation resources at z/OS Cryptographic Services publications for ICSF FMID HCR77C1 (www.ibm.com/servers/resourcelink/svc00100.nsf/pages/zOSICSFFmidHCR77C1Publications?OpenDocument). See the z/OS Downloads (www-01.ibm.com/servers/resourcelink/svc00100.nsf/pages/zosDownloads?OpenDocument#crypto-sep-2017) page for information about downloading and installing ICSF FMID HCR77C1.

Additional ICSF consideration

If you plan to encrypt SMF data sets or other data sets used during z/OS initialization, you must ensure that ICSF is started early in the IPL process to avoid delays in z/OS initialization and termination. As such, it is highly recommended that the command S CSF,SUB=MSTR is placed early in the COMMNDxx member to ensure 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 must be one of the last features to stop so that dependent functions are not impacted. It is highly recommended that you shut down ICSF after terminating the JES address space and after initiating SMF halt processing. Note when ICSF is stopped after SMF is halted, that there might not be an SMF record cut for the termination of ICSF. (The ability to start ICSF with SUB=MSTR is available on all supported releases of ICSF.)

Hardware and software requirements

Hardware requirements Data set encryption requires IBM Enterprise z196 or later as well as the following cryptographic hardware features:

- Crypto Express3 Coprocessor or later
- Feature 3863, CP Assist for Cryptographic Functions (CPACF)

Operating System requirements

- ICSF is installed and configured with a CKDS and AES master key loaded. See ICSF planning and installation for more information.

Coexistence requirements

- On a z/OS V2R2 system with OA50569, you can create encrypted data sets as well as access encrypted data sets created on a z/OS V2R2 (with OA50569) or later system.
- On a z/OS V2R1 system with OA50569, you cannot create encrypted data sets. However, you can access encrypted data sets created on a z/OS V2R2 (with OA50569) or later system.

  Note: The minimum software release that can support encrypted data sets is z/OS V2R1 with OA50569. An attempt to access an encrypted data set on a lower release will result in loss of access to the data. Ensure that all systems are at the minimum hardware and software levels before encrypting any data sets.

z/OS data set encryption for V2R2

Data set encryption for z/OS V2R2 is available. See OA50569: NEW FUNCTION - THE DFSMS Z/OS DATA SET ENCRYPTION ENHANCEMENT (www.ibm.com/support/docview.wss?crawler=1&uid=isg1OA50569).

The DFSMS APAR OA50569 pulls in the pre-req/co-req APAR(s) along with dependency APAR(s); however, depending on the level of service already on a system, additional service can 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, see IBM Fix Category Values and Descriptions (www-01.ibm.com/support/docview.wss?uid=isg3T1027683).

A collection of frequently asked questions and answers for z/OS V2.2 data set encryption is available in the IBM Techdocs: Data Set Encryption for IBM z/OS V2.2 Frequently Asked Questions (www-03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/FQ131494).

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)

Additional data set encryption information

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): Search support or find a product: Search support or find a product Search Sending troubleshooting data to IBM when using z/OS data set encryption (www-01.ibm.com/support/docview.wss?uid=isg3T1025650).

Planning z/OS data set encryption

Considerations when planning for data set encryption

- Encrypted data sets must be extended format. Refer to Extended-Format VSAM Data Sets and Processing Extended-Format Sequential Data Sets for information on allocating extended format data sets, including guidelines and restrictions.
- Sequential extended format data sets can be version 1 or 2. When allocating an encrypted sequential extended format data set, the system creates the data set as an extended format version 2 data set, regardless of the user's specification for version number on DSNTYPE or the PS_EXT_VERSION keyword in the IGDSMSxx member in PARMLIB.
- Encrypted data do not compress. Therefore, encrypted extended format data sets might not benefit from storage savings when relying on disk and tape device compression, as well as other areas in the infrastructure that attempt to compress data. Where possible, consider using compressed format data sets. When data set level compression is requested along with encryption, access methods handle compression before encryption for encrypted compressed format data sets. Refer to Compressed Data and Allocating Compressed-Format Data Sets for information on allocating compressed format data sets, including guidelines and restrictions.
- When processing encrypted extended format data sets, the access methods may use additional internal system buffers during read and write processing. For optimal performance, consider increasing memory to your partition as your use of encrypted data sets increases.

Restrictions for encrypted data sets

- System data sets (such as Catalogs, SMS control data sets, SHCDS, HSM data sets) must not be encrypted, unless otherwise specified in product documentation.
- Data sets used during IPL must not be encrypted.
- Encrypted data sets only supported on 3390 device types.
- Sequential (non-compressed) data sets with a BLKSIZE of less than 16 bytes cannot be extended format.

For potential restrictions associated with other products, consult the corresponding product documentation.

Setting up z/OS data set encryption

Importance of host based compression

It is recommended that clients who use host-based encryption, also use host-based compression before data encryption. If the data is not compressed prior to encryption, there can be consequences to other parts of the client infrastructure. For example, replicated data that is being compressed in the SAN infrastructure by DWDM technology will no longer effectively compress encrypted data. If the data is not compressed before it is encrypted, additional bandwidth might be required.

Additionally, tape systems might require extra capacity in terms of disk space, in the case of virtual tape or tape cartridges. If data deduplication is supported, host-based encryption can prevent data deduplication from working. Therefore, where possible, use compressed format data sets. With encrypted compressed format data sets, the access methods perform compression before encryption. Refer to "Considerations when planning for data set encryption" on page 5.

To create an encrypted data set, a key label must be supplied on new data set allocation. The key label must point to an AES-256 bit encryption DATA key within the ICSF key repository (CKDS) to be used to encrypt or decrypt the data. For each encrypted data set, its key label is stored in the catalog. The key label is not sensitive information; it identifies the encryption key, which is sensitive; therefore, IBM recommends only using secure keys. For more information, see *z/OS Cryptographic Services ICSF System Programmer's Guide*.

Before enabling this function

Because data set encryption has both hardware and software requirements, you must consider all systems that share data with a system on which you plan to enable data set encryption before creating an encrypted data set. This includes backout software levels, backup systems, read-only systems, replication target systems and disaster recovery systems. Before encrypting data sets other than those used for testing, be sure that all the systems that must access encrypted data sets are capable of doing so by meeting the required hardware and software requirements. In addition to the hardware and software requirements that must be available on every system that will access the encrypted data sets, all key labels and encryption keys associated with the encrypted data sets must also be available.

Take the following steps to make data set encryption unavailable to users who are not explicitly authorized to use it:

- Define the STGADMIN.SMS.ALLOW.DATASET.ENCRYPT profile in the FACILITY class, and set the universal access to NONE:

```
RDEFINE FACILITY STGADMIN.SMS.ALLOW.DATASET.ENCRYPT UACC(NONE)
```

- If the FIELD class is active, check for any profile that would allow any user without SPECIAL attribute access to the DATASET.DFP.DATAKEY. If there are none, no additional action is needed. If there is any profile that would allow access to DATASET.DFP.DATAKEY, create a DATASET.DFP.DATAKEY profile in the FIELD class with a UACC of NONE:

```
RDEFINE FIELD DATASET.DFP.DATAKEY UACC(NONE)
```

Taking the above steps is intended to assure that only authorized users are allowed to use data set encryption. Such users should be made aware that until the decryption functions are available on all sharing systems, backup systems, and disaster recovery systems, access to encrypted data can be lost at any time.

Tasks for setting up z/OS data set encryption

This section assumes that the following "Core infrastructure requirements" on page 3 are already in place, or are understood by the user:

- ICSF installation, configuration, administration ICSF AES master key(s) populated
- Crypto Express hardware cards installed, configured, and known to ICSF
- RACF installation, configuration, administration, or equivalent SAF product
- Basic knowledge or understanding of AES keys, data keys, key labels, ICSF and RACF in a sysplex.

Create key labels and encryption keys

To create an encrypted data set, a key label must be assigned to the data set. The key label and its associated AES-256 bit encryption key must exist in the CKDS by the time the data set is opened. To create keys in the CKDS, refer to *z/OS Cryptographic Services ICSF System Programmer's Guide*. IBM recommends the use of secure keys.

Set up CSFKEYS

To control which users can use which keys, protect resources CSFKEYS class. The CSFKEYS class controls access to cryptographic keys identified by the key label.

To enable the use of ICSF keys:

1. Grant the user READ authority to the resource key-label in the CSFKEYS class. This authority can be granted for all uses of the key-label or only when the use of the key-label is permitted when using the a CRITERIA value of DSENCRYPTION for SMS.

   - if the class has not already been enabled for generics

   ```
   SETROPTS GENERIC(CSFKEYS)
   ```

   - Define profiles in the CSFKEYS class to protect key labels

   ```
   RDEFINE    CSFKEYS  profile-name UACC(NONE)
              ICSF(SYMCPACFWRAP(YES)   SYMCPACFRET(YES))
   ```

   - Give the users (preferably groups) access to the profiles

   ```
   PERMIT profile-name CLASS(CSFKEYS)
          ID(name)    ACCESS(READ)
   ```

   or

   ```
   PERMIT profile-name CLASS(CSFKEYS)
          ID(name)    ACCESS(READ)
          WHEN(CRITERIA(SMS(DSENCRYPTION)))
   ```

2. Define the ICSF information for the key with SYMCPACFWRAP(YES) and SYMCPACFRET(YES), if it was not specified on the DEFINE

   ```
   RALTER CSFKEYS profile-name
          ICSF(SYMCPACFWRAP(YES)   SYMCPACFRET(YES))
   ```

3. Set RACF options

   - if the CSFKEYS class is not already active

   ```
   SETROPTS CLASSACT(CSFKEYS)
   ```

   - if the CSFKEYS class has not already been RACLISTed

   ```
   SETROPTS RACLIST(CSFKEYS)
   ```

   - or if the CSFKEYS class has already been RACLISTed

   ```
   SETROPTS RACLIST(CSFKEYS) REFRESH
   ```

Set up CSFSERV

Important: The following setup is required only if CHECKAUTH(YES) is specified on the ICSF installation options data set. CHECKAUTH(NO) is the default.

Protect the resources CSFSERV class. ICSF controls access to cryptographic services through the CSFSERV resource class. For more information, see *z/OS Cryptographic Services ICSF Administrator's Guide* .

The following table summarizes the CSFSERV resource required for processing encrypted data sets.

Table 1. CSFSERV resource required for data set encryption

Function	ICSF callable service	Resource
CKDS Key Record Read2	CSNBKRR2	CSFKRR2

If the user does not have sufficient access, open processing will fail. An informational message ICH408I (which indicates insufficient authorization) might be issued.

1. Grant the user READ authority to the resource CSFSERV class:

   - if the class has not already been enabled for generics

   ```
   SETROPTS GENERIC(CSFSERV)
   ```

   - Define profiles in the CSFSERV class to protect key labels

   ```
   RDEFINE CSFSERV * UACC(NONE)
   ```

   - Define profile CSFKRR2 if it does not exist

   ```
   RDEFINE CSFSERV CSFKRR2 UACC(NONE)
   ```

   - Give the users (preferably groups) access

   ```
   PERMIT CSFKRR2 CLASS(CSFSERV) ID(groupid) ACCESS(READ)
   ```

2. Set RACF options:

   - if the CSFSERV class is not already active

   ```
   SETROPTS CLASSACT(CSFSERV)
   ```

   - if the CSFSERV class has not already been RACLISTed

   ```
   SETROPTS RACLIST(CSFSERV)
   ```

   - or if the CSFSERV class has already been RACLISTed

   ```
   SETROPTS RACLIST(CSFSERV) REFRESH
   ```

Create an encrypted data set

To create an encrypted data set, you must assign a key label to the data set when it is newly allocated (data set create). A key label can be specified through any of the following methods:

- RACF data set profile
- JCL, dynamic allocation, TSO ALLOCATE, IDCAMS DEFINE
- SMS data class

To specify a key label using the DFP segment in the RACF data set profile, use keyword DATAKEY(Key-Label). The system will use this key label for extended format data sets that are created after DATAKEY is added to the data set profile. Use keyword NODATAKEY to remove a key label, if defined, from the RACF DFP segment. The key label is ignored for a data set that is not a DASD data set.

To specify a key label using JCL, dynamic allocation, and TSO allocate, use JCL keyword DSKEYLBL='key-label', dynamic allocation text unit DALDKYL, or TSO allocate DSKEYLBL(label-name). DSKEYLBL parameter is effective only if the new data set is on DASD. The key label is ignored for a data set that is not a DASD data set.

See details about the DSKEYLBL parameter (key-label) keyword on the JCL DD statement in *z/OS MVS JCL Reference*.

To specify a key label using SMS data class, use the *Data Set Key Label* field on the ISMF DEFINE/ALTER panel. The system will use this key label for extended format data sets that are created after the data set key label is added to the data class. The key label is ignored for a data set that is not a DASD data set.

See details on using the Data Set Key Label field in the ISMF panels in *z/OS DFSMS Using the Interactive Storage Management Facility*.

To specify a key label using the DEFINE CLUSTER command for a VSAM CLUSTER, use the KEYLABEL parameter; for example, KEYLABEL(MYLABEL). Any alternate index associated with the CLUSTER will also be encrypted and use the same key label as specified for the CLUSTER. The key label is ignored for a data set that is not a DASD data set.

For more information on using DEFINE CLUSTER command for a VSAM CLUSTER, see *z/OS DFSMS Access Method Services Commands*.

When a key label is specified on more than one source, the key label is derived from one of the above sources only on the initial data set allocation (on data set create). The key label is derived in the following order of precedence:

1. From DFP segment in the RACF data set profile.
2. Explicitly specified on the DD statement, dynamic allocation text unit, TSO ALLOCATE command, or DEFINE CLUSTER control statement.
3. From the data class that applies to the current DD statement.

   Note: The REFDD and LIKE JCL DD statement keywords do not cause a key label from the data set referred to be used when allocating a new data set.

On successful allocation of an encrypted data set, the following message is issued:

```
IGD17150I DATA SET dsname IS ELIGIBLE FOR ACCESS METHOD ENCRYPTION
KEY LABEL IS (key_label)
```

Specifying a key label for a non-extended format data set

If an encryption key label is specified for a DASD data set that is not extended format, the key label is ignored and the data set is successfully created as non-encrypted non-extended format data set. In addition, SMS message IGD17156I is issued (or if using IDCAMS DEFINE and data set is non-SMS managed, message IDC3040I is issued) indicating that the key label is ignored. Instead to have the system fail the allocation, the user must have at least READ authority to the resource in the FACILITY class: STGADMIN.SMS. FAIL.INVALID.DSNTYPE.ENC

If this facility class resource exists and the user has at least read authority, SMS will fail the allocation and issue message IGD17151I (or if using IDCAMS DEFINE and non-SMS managed data set request, message IDC3039I is issued).

Enable data set encryption

An enablement action is required to allow the creation of encrypted data sets when the key label is specified through a method outside of the DFP segment in the RACF data set profile.

To allow the system to create encrypted data sets using a key label specified through a method other than through the DFP segment in the RACF data set profile, the user must have at least READ authority to the following resource in the FACILITY class:

```
STGADMIN.SMS.ALLOW.DATASET.ENCRYPT
```

Note: IBM recommends that you define STGADMIN.* with UACC(NONE).

The system checks the user's authority to access this resource when a data set to be encrypted is first allocated (that is, created). It is not checked again before encrypting a data set.

Allocation processing

SMS allocation processing determines if a data set can be allocated as an encrypted data set. Under certain conditions, you can specify how the allocation should proceed. The following tables summarize the system behavior during SMS allocation processing for a new data set based on specific FACILITY class resources and the user's authorization to the resource.

On a z/OS V2R2 system (with OA50569) and later, the following table describes the result of an allocation request for an extended format data set when a key label has been specified. On a successful allocation,

the resulting data set will be an encrypted extended format data set. Other factors not described in this table (such as lack of space) might cause the allocation to fail.

Table 2. SMS Allocation Processing Based on System Levels and Allocation Request (z/OS V2R2 with OA50569)

FACILITY class resource	**STGADMIN.SMS.ALLOW.DATASET.ENCRYPT**			
Access	**Not defined OR not authorized**		**At least authorized for READ**	
Allocation type	**JCL**	**IDCAMS DEFINE**	**JCL**	**IDCAMS DEFINE**
Key label from DFP segment of RACF DS profile	Allocation continues with IGD17150I	Allocation continues with IGD17150I	Allocation continues with IGD17150I	Allocation continues with IGD17150I
Key label from a source other than DFP segment of RACF DS profile	Allocation fails with IGD17155I	Allocation fails with IDC3038I	Allocation continues with IGD17150I	Allocation continues with IGD17150I

On a z/OS V2R2 system (with OA50569) and above, the following table describes the result of an allocation request for a DASD non-extended format data set when a key label has been specified from any source. On a successful allocation, the resulting data set will be a non-encrypted non-extended format data set. Other factors not described in this table (such as lack of space) might cause the allocation to fail.

Table 3. SMS Allocation Processing Based on System Levels and Allocation Request (z/OS V2R2 with OA50569)

FACILITY class resource	**STGADMIN.SMS. FAIL.INVALID.DSNTYPE.ENC**			
Access	**Not defined OR not authorized**		**At least authorized for READ**	
Allocation type	**JCL**	**IDCAMS DEFINE**	**JCL**	**IDCAMS DEFINE**
SMS mgd	Allocation continues with IGD17156I	Allocation continues with IGD17156I	Allocation fails with IGD17151I	Allocation fails with IGD17151I
non-SMS mgd	Allocation fails with IGD17156I	Allocation fails with IDC3040I	Allocation fails with IGD17151I	Allocation fails with IDC3039I

On a z/OS V2R1 system (with OA50569), the following table describes the result of an allocation request for a DASD data set (extended format and non-extended format) when a key label has been specified from any source. On a successful allocation, the resulting data set will be a non-encrypted data set since you cannot create new encrypted data sets on a z/OS V2R1 system. Other factors not described in this table (such as lack of space) might cause the allocation to fail.

Table 4. SMS Allocation Processing Based on System Levels and Allocation Request (z/OS V2R1 with OA50569)

FACILITY class resource	**STGADMIN.SMS. FAIL.INVALID.DSNTYPE.ENC**			
Access	**Not defined OR not authorized**		**At least authorized for READ**	
Allocation type	**JCL**	**IDCAMS DEFINE**	**JCL**	**IDCAMS DEFINE**
Key label specified on JCL (DSKEYLBL)	Job fails with IEFC630I	N/A	Job fails with IEFC630I	N/A

Table 4. SMS Allocation Processing Based on System Levels and Allocation Request (z/OS V2R1 with OA50569) (continued)

FACILITY class resource	**STGADMIN.SMS. FAIL.INVALID.DSNTYPE.ENC**			
Access	**Not defined OR not authorized**		**At least authorized for READ**	
Allocation type	**JCL**	**IDCAMS DEFINE**	**JCL**	**IDCAMS DEFINE**
Key label specified on IDCAMS DEFINE (KEYLABEL)	N/A	Allocation fails with IDC3211I	N/A	Allocation fails with IDC3211I
Key label from DFP segment of RACF DS profile or from data class)	Refer to the following two rows			
SMS mgd	Allocation continues with IGD17156I	Allocation continues with IDC3040I	Allocation fails with IGD17154I	Allocation fails with IDC0017I
non-SMS mgd	Allocation continues with IGD17156I	Allocation continues with IDC3040I	Allocation fails with IGD17154I	Allocation fails with IDC0017I

Accessing encrypted data sets

Applications that use standard BSAM, QSAM, and VSAM APIs do not require changes to access encrypted data sets. The user data transferred between the application and the access methods is in the unencrypted form. The access method encrypts the data when writing to DASD and decrypts the data when reading from DASD. For encrypted compressed format data sets, the access method compresses the data before encrypting it on output. On input, the access method decrypts the data before decompressing it.

Considerations regarding ICSF startup and shutdown

If you plan to encrypt SMF data sets or other data sets used during z/OS initialization, you must ensure that ICSF is started early in the IPL process to avoid delays in z/OS initialization and termination. As such, it is highly recommended the command S CSF,SUB=MSTR is placed early in the COMMNDxx member to ensure that 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 must be one of the last features to stop so that dependent functions are not impacted. It is highly recommended that you shut down ICSF after terminating the JES address space and after initiating SMF halt processing. Note when ICSF is stopped after SMF is halted, that there might not be an SMF record cut for the termination of ICSF. (The ability to start ICSF with SUB=MSTR is available on all supported releases of ICSF.)

Considerations regarding backup/migration/replication functions

Key label authorization

The following system functions maintain data in the encrypted form. Therefore, users performing these functions do not require authorization to the key label associated with the data sets being processed with these functions:

- DFSMSdss functions: COPY, DUMP, and RESTORE
- DFSMShsm functions: migrate/recall, backup/recover, abackup/arecover, dump/data set restore, FRBACKUP/FRRECOV DSNAME

- Track based copy (PPRC, XRC, FlashCopy®, concurrent copy) operations

Other considerations

- DFSMSdss REBLOCK keyword is ignored on COPY and RESTORE functions for encrypted data sets.
- DFSMSdss ADRREBLK installation exit will not be called for encrypted data sets.
- DFSMSdss does not support VALIDATE processing when backing up encrypted indexed VSAM data sets. VALIDATE will be ignored.
- Backup and migration of encrypted data sets may impact expected savings with disk or tape device compression. Where possible, convert to compressed format data sets. When data set level compression requested, access methods handle compression before encryption for compressed format encrypted data sets.

IBM Db2 support for z/OS data set encryption

IBM Db2 supports z/OS data set encryption. IBM Db2 is designed to transparently encrypt data at rest without database downtime or requiring the administrator to redefine objects, which can 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, re-keying 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) supports z/OS V2.2 data set encryption with the following Db2 service:

- PI81900: DB2 11 FOR Z/OS NEW FUNCTION (www-01.ibm.com/support/docview.wss?uid=swg1PI81900)
- PI81907: DB2 FOR Z/OS NEW FUNCTION (www-01.ibm.com/support/docview.wss?uid=swg1PI81907)

Chapter 3. IBM Z pervasive encryption with z/OS CF encryption and zERT

z/OS Encryption Readiness Technology (zERT)

z/OS Encryption Readiness Technology (zERT) is provided by the z/OS V2R3 Communications Server. With zERT, the TCP/IP stack acts as a focal point in collecting and reporting the cryptographic security attributes of IPv4 and IPv6 application traffic that is protected using the TLS/SSL, SSH and IPSec cryptographic network security protocols. The collected connection level data is written to SMF in new SMF 119 subtype 11 records for analysis.

For an expanded zERT overview, along with tables for planning, enabling, and using zERT, refer to z/OS Encryption Readiness Technology (zERT) (www.ibm.com/support/knowledgecenter/SSLTBW_2.3.0/com.ibm.zos.v2r3.halg001/nfsrgvhzert23.htm).

z/OS Coupling Facility encryption

On systems at the z/OS V2R3 level and above, list and cache structure entry and entry adjunct data can be encrypted while the data is being transferred to and from the coupling facility and while the data resides in the coupling facility structure. List and cache structure services use secure cryptographic key tokens obtained from the z/OS Integrated Cryptographic Service Facility (ICSF) software element to encrypt and decrypt user provided structure data. Encryption of structure data can be controlled on a structure-by-structure basis.

For system and XCF requirements, sysplex coexistence considerations, and additional information related to Coupling Facility encryption, refer to Encrypting coupling facility structure data (www.ibm.com/support/knowledgecenter/SSLTBW_2.3.0/com.ibm.zos.v2r3.ieaf100/encryptstrdat.htm).

© Copyright IBM Corp. 2019, 2019

Chapter 4. Related tools and information for IBM Z pervasive encryption

Other resources

Related information for IBM Z® hardware and software products that support IBM Z® pervasive encryption can be found in the following resources:

- The IBM Crypto Education Community (www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/W7df80301055d_495b_bb88_a0a2f84757c5) provides information and sample code 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.
- The IBM Techdocs IBM Techdocs: Data Set Encryption for IBM z/OS V2.2 Frequently Asked Questions (www-03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/FQ131494) provide an essential list of frequently asked questions and answers.
- IBM Trusted Key Entry (TKE) securely manages multiple cryptographic coprocessors and keys on various generations of IBM Z and other platforms, from a single point of control, see z/OS Trusted Key Entry Workstation (TKE) (www.ibm.com/support/knowledgecenter/SSLTBW_2.3.0/com.ibm.zos.v2r3.izst100/abstract.htm).
- The IBM QRadar SIEM offering adds analytics and intelligence to IBM z® sourced event notifications, see QRadar on Cloud documentation (www.ibm.com/support/knowledgecenter/en/SSKMKU/com.ibm.qradar.doc_cloud/cloud_kc_welcome.html).
- IBM Z Batch Network Analyzer (zBNA) Tool (www-03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/PRS5132) helps estimate additional CPU that is incurred when enabling encryption for certain workloads. It can also be used to help estimate CPU costs for both data set encryption and for coupling facility encryption. zBNA V1.8.1 tool can be used with DFSMS, RMF, and XES PTFs applied.

  Note: Before zBNA can be used for 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. The zBNA Tool is available in the IBM Techdocs Library at IBM Z Batch Network Analyzer (zBNA) Tool (www-03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/PRS5132).

New and changed messages for z/OS data set encryption

This topic lists new, changed, and deleted messages and codes for BCP (MVS™), DFSMSdfp, DFSMSdss, DFSMShsm, DFSMSrmm, and DFSMStvs. All the messages and codes in this section are grouped together, without distinction as to element or feature.

z/OS MVS System Messages, Vol 1 (ABA-AOM)

The following messages are updated:

- ADR380E
- ADR439E
- ADR447I
- ADR518I
- ADR519E
- ADR778E

© Copyright IBM Corp. 2019, 2019

z/OS MVS System Messages, Vol 2 (ARC-ASA)

The following message is updated:

- ARC6190E

z/OS System Messages Volume 6 (GOS-IEA)

The following messages are new:

- IDC0017I
- IDC3038I
- IDC3039I
- IDC3040I

The following message is updated:

- IDC3009I

z/OS MVS System Messages, Vol 7 (IEB-IEE)

The following messages are updated:

- IEC036I (new reason codes added)
- IEC143I (new reason codes added)
- IEC150I (new reason codes added)
- IEC161I (new reason codes added)

z/OS MVS System Messages, Vol 8 (IEF-IGD)

The following messages are new:

- IGD17150I
- IGD17151I
- IGD17152I
- IGD17153I
- IGD17154I
- IGD17155I
- IGD17156I

The following messages are updated:

- IGD17269I
- IGD17279I
- IGD17345I

z/OS MVS System Messages, Vol 9 (IGD-IWM)

The following message is updated:

- IGW640I

Notices

This information was developed for products and services that are offered in the USA or elsewhere.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
United States of America

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

This information could include missing, incorrect, or broken hyperlinks. Hyperlinks are maintained in only the HTML plug-in output for the Knowledge Centers. Use of hyperlinks in other output formats of this information is at your own risk.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Site Counsel
2455 South Road

© Copyright IBM Corp. 2019, 2019

Poughkeepsie, NY 12601-5400
USA

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

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

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

IBM Online Privacy Statement

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user, or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

Depending upon the configurations deployed, this Software Offering may use session cookies that collect each user's name, email address, phone number, or other personally identifiable information for purposes of enhanced user usability and single sign-on configuration. These cookies can be disabled, but disabling them will also eliminate the functionality they enable.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM's Privacy Policy at ibm.com/privacy and IBM's Online Privacy Statement at ibm.com/privacy/details in the section entitled "Cookies, Web Beacons and Other Technologies," and the "IBM Software Products and Software-as-a-Service Privacy Statement" at ibm.com/software/info/product-privacy.

Policy for unsupported hardware

Various z/OS elements, such as DFSMSdfp, JES2, JES3, and MVS, contain code that supports specific hardware servers or devices. In some cases, this device-related element support remains in the product even after the hardware devices pass their announced End of Service date. z/OS may continue to service element code; however, it will not provide service related to unsupported hardware devices. Software problems related to these devices will not be accepted for service, and current service activity will cease if a problem is determined to be associated with out-of-support devices. In such cases, fixes will not be issued.

Minimum supported hardware

The minimum supported hardware for z/OS releases identified in z/OS announcements can subsequently change when service for particular servers or devices is withdrawn. Likewise, the levels of other software products supported on a particular release of z/OS are subject to the service support lifecycle of those products. Therefore, z/OS and its product publications (for example, panels, samples, messages, and product documentation) can include references to hardware and software that is no longer supported.

- For information about software support lifecycle, see: IBM Lifecycle Support for z/OS (www.ibm.com/software/support/systemsz/lifecycle)

- For information about currently-supported IBM hardware, contact your IBM representative.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at Copyright and Trademark information (www.ibm.com/legal/copytrade.shtml).

Product Number: 5650-ZOS