CA View®

Release Notes

r11.6

technologies

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be disclosed by you or used for any purpose other than as may be permitted in (i) a separate agreement between you and CA governing your use of the CA software to which the Documentation relates; or (ii) a separate confidentiality agreement between you and CA.

Notwithstanding the foregoing, if you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

CA Technologies Product References

This document references the following CA products:

- CA ACF2
- CA Deliver™
- CA Mainframe Software Manager (CA MSM)
- CA Output Management Web Viewer
- CA Top Secret®

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: Introduction

This document provides information about the new features and functions in CA View r11.6.

It also includes the supported environments, new functionality, system changes, how to configure CA View for encryption, JCL and module setting changes, new messages, and how to use this document in conjunction with the existing documentation set.

Important! Be aware that release 11.6 is built on CA View r11.5, and includes changes or updates that are directly connected to encryption, use of ESD PAX or MSM installation, and Health Checks; therefore, with the exception of the information contained in this document, all pre-existing product documentation is accurate and timely. Changes that affect other documents in the set are included in sections in the CA View Parameter and Setting chapter.

The encryption feature *does not* support Centera storage. This will be added in an APAR or future release.

This section contains the following topics:

New Features

CA View r11.6 is a feature-specific release built on CA View r11.5. It provides the following:

- The strong encryption needed to support PCI (Payment Card Industry) compliance

  Note that this encryption is found across our suite of interactive products which also includes CA Spool, CA Dispatch, CA Bundl, CA DRAS, and CA Deliver.

- The ability to use Electronic Software Delivery (ESD) PAX—the installation process that lets you install directly from DASD.

- Large Data Set Support
- Improved STATUS command
- An encryption health check
- Backward compatibility with CA View r11.0 and r11.5

Note that with the exception of the information contained in this document, all pre-existing product documentation is accurate and timely.

Data Encryption

Protecting your data is of utmost importance. Customers who store credit card data must abide by Payment Credit Industry (PCI) compliance. One of the most important factors in this compliance is to provide optimum security, that is, *data at rest must be encrypted through strong encryption.*

CA View provides support for encryption and decryption of data using the AES encryption algorithm and management of encryption keys with the CA Encryption Key Manager and IBM Integrated Cryptography Service Facility products. The encryption feature is enabled with the ENCRYPT initialization parameter. CA View will encrypt report and report index data in the database and on tape which includes the primary, duplex, and DR tapes.

Note: For more information, see the chapter Data Encryption in the *Reference Guide*.

Encryption Keys

We are integrating with the IBM CPACF and ICSF services for encryption. You activate encryption using a simple initialization parameter. The process is as follows:

1. Based on a client-specified interval, key labels and encryption keys are written to the ICSF Key Store Data Set (CKDS).
2. A Call is sent to ICSF to obtain a proper key.
3. CPACF or ICSF is invoked to perform the AES encryption.

Important! If you are sharing the ICSF CKDS data set between multiple z/OS systems, the ICSF SYSPLEXCKDS(YES,FAIL(xxxx)) parameter *must be specified in the ICSF installation options data set.* This allows newly created keys to be shared with other systems running ICSF. Without this parameter, the ICSF in-memory copy of the CKDS will be out of sync between the systems and result in reports being encrypted with one key and later incorrectly decrypted with another key. When this occurs, the original keys are replaced with keys from another system. Reports using the original keys can no longer be decrypted.

Be aware of the following:

- When the encryption feature is enabled, all report and index data will be encrypted on both disk and tape.

  This includes the CA View database, backup, duplex, and DR (Disaster Recovery).
- Existing backup tapes can be encrypted by using the CA View SARPAC utility.
- Reloading an older report back to disk will automatically encrypt the disk copy.
- Copying the database will encrypt all reports on the copied database.

Note: See Supported Cryptographic Hardware, Encrypt the Data, and Decrypt the Data for more information.

Important! CA View *does not keep* a local copy of the encryption key; it stores a clear 256 bit encryption key in the ICSF Key store (CKDS). CA View only accesses the CKDS via the ICSF services – it does not require any security permissions to access this data set. We recommend that you use your external security package to prevent unauthorized browsing of the CKDS data set.

Currently CA View uses ICSF as a key store. Future releases will provide support for other third party key managers including any CA products that provide this functionality.

Supported Cryptographic Hardware

Two cryptographic hardware choices are available for use on various systems:

- Cryptographic Coprocessor Facility (CCF) A standard component on z900 and a no-cost option for z800. On z800 and z900 systems, ICSF requires CCF.
- CP Assist for Cryptographic Functions (CPACF) A standard component on z9 and z10 and a no-cost option for z890 and z990

Other available cryptographic hardware components do not necessarily improve encryption performance, as described in the following list:

- Peripheral Component Interconnect (PCI)-based coprocessors (PCICC, PCIXCC, and Crypto Express2), which provide secure key storage, hardware hashing, and SSL support.

- PCI-based accelerators (PCICA, Crypto Express2 configured in accelerator mode), which provide high performance SSL assistance.

Note: Because CA View uses a clear key, it does not require the use of the Cryptographic Express2 coprocessor (CEX2C). To run ICSF without a CEX2C coprocessor, you will need ICSF release FMID HCR7751or higher.

If you are running an older release of ICSF, you will be required to purchase a CEX2C coprocessor because older releases of ICSF required that hardware to initialize the CKDS data set.

Encrypt the Data

Encryption is enabled by a SARINIT parameter. See the Procedure to Configure CA View for Encryption section for information about set up.

The sequence to encrypt is as follows:

1. Run SARINIT with ENCRYPT=ICSF

   See the Configuration chapter for more information about the ENCRYPT parameter.

2. When CA View collects reports, it will encrypt them on both tape and disk if the ENCRYPT parameter is set to ICSF.

3. Depending on your hardware, encryption is done using the Advanced Encryption Standard (AES) with 128 or 256 bit keys.

Important! Changes to the ENCRYPT parameter will not take effect until the collectors are stopped and restarted. For reports archiving "DIRECT TO VIEW," encryption is determined by the value of the ENCRYPT parameter when the report was opened by the application program.

Decrypt the Data

The decryption process might be needed if you need to view or print data from a 3270 or web interface.

The decryption process is as follows:

1. CA View finds the data, which has a scrambled key.

2. CA View unscrambles the key.

3. CA View calls one of the following for decryption:
   - Hardware (first)
   - Software (ICSF) – If Crypto Assist hardware is not installed
4. The data is decrypted and presented to the user.

Merged Databases and Encryption

Merging encrypted and non-encrypted databases does not automatically encrypt or decrypt all reports on the merged database.

Be aware that encrypted reports are merged in encrypted format and non-encrypted reports are not encrypted.

Important! The setting of the ENCRYPT parameter on the merged database is based on the setting found on the last merged database (SARMERGn).

IEBGENER Considerations

IEBGENER can no longer be used to print a report from a backup tape since data is now stored in encrypted format.

Encryption and Decryption Software Considerations

Be aware that if you use z/OS software encryption and decryption, the time the CPU uses to encrypt or decrypt data will increase the CPU time consumed by the job or started task.

Our tests have shown that encryption using the Crypto Assist Facility (CPACF) has the smallest amount of overhead. We experienced an increase of 1/10 of a CPU second for every million lines archived or browsed.

What Gets Encrypted

In CA View all report data and report index data get encrypted. Panels, banner pages, and resource data is not encrypted.

Terminology

You may encounter the following terms and abbreviations:

- AES – Advanced Encryption Standard
- Asymmetric key – A different key is used for encryption and decryption. Thought of as a public key and a private key.
- CKDS – ICSF Cryptographic Key Data Set is the storage vehicle for symmetric keys
- CPACF – CP Assist for Crypto Functions
- DSS – Data Security Standard
- IBM CPACF and ICSF services
- ICSF – Integrated Cryptographic Service Facility
- MSM – CA Mainframe Software Manager
- PAX – UNIX file system archive file
- PCI – Payment Card Industry
- PCI compliance – Meeting the standards that were created to help organizations that process card payments by preventing credit card fraud through increased controls around data and its exposure to compromise
- Symmetric Key – Same key is used for both decryption and encryption

Large Data Set Support

The size of a database extent is no longer limited to 4369 cylinders. Now a database extent can allocate an entire 3390 mod 27 (32,760 cylinders) as one database extent. This increases the maximum database size from 1,114,095 to 8,353,800 cylinders.

If your site consolidates the CA View database into as few extents as possible, you will see the following benefits:

- Increased database capacity - Over 8 million cylinders as opposed to 1 million in previous releases
- Lower below-the-line storage requirements allowing a single XMS region to process more users
- Faster log ons to CA View because fewer extents are being accessed

Note: Large data sets cannot be versioned back to release 11.5. If you decide to fall back to release 11.5 or 11.0 and you have allocated one or more large data sets, you must do the following:

1. Unload the database.
2. Allocate a new database that does not contain any large data sets.
3. Load the unload tape to the new database and version back to release 11.5 or release 11.0.

Improved STATUS Command

Because of a change in the database structure, The online STATUS command now provides a quick and accurate allocation percentage for the database. To take advantage of the feature, the database must be versioned to the 11.6 release level.

In release 11.0, the response time for this command was slow, but it provided accurate allocation percentages. In release 11.5 the response time for this command was quick, but it only produced an approximate allocation percentage for the index.

Environment

This section discusses the current operating systems supported, scalability, compatibility, and the security interfaces.

Supported Operating Systems

The minimum hardware required to run this release of the product and meet the performance requirements is IBM z/OS 1.9 and higher.

Scalability, Availability, and Prior Versions

CA View r11.6 will have the same scalability as previous versions.

Availability should be almost 24x7 except for periodic maintenance which will vary in frequency according to the needs of your site.

Note the following:

- CA Deliver allows concurrent archiving to CA View r11.0, r11.5, and r11.6..
- The release 11.6 XMS and DRAS tasks allow concurrent viewing of CA View r11.0, r11.5, and r11.6 databases.

Compatibility

This section discusses compatibility with prior releases and backward compatibility and encryption.

Backward Compatibility and Encryption

CA View r11.6 will be able to read prior versions of report data found on disk and tape.

Important! CA View r11.6 encryption does not have backward compatibility to allow previous releases to access encrypted data. Once you start to use encryption, you cannot read the encrypted tapes in a prior release.

To fall back to Release 11.5, you must do the following:

1. Set ENCRYPT=NO to disable encryption in release 11.6.
2. Run the batch job SARPAC to COPY the encrypted tapes and remove the encryption from any tape reports.
3. Run SARDBASE to COPY the database and remove the encryption from any disk reports.
4. Ensure the PTF RO17278 is applied to release 11.5; this will ensure that non-encrypted tapes can be read by release 11.5.

To fall back to Release 11.0, you must do the following:

1. Set ENCRYPT=NO to disable encryption in 11.6.
2. Run the batch job SARPAC to COPY the encrypted tapes and remove the encryption from any tape reports.
3. Run SARDBASE to COPY the database and remove the encryption from any disk reports.
4. Ensure the PTF RO17241 is applied to release 11.0; this will ensure that non-encrypted tapes can be read by release 11.0.

Compatibility with Prior Releases

If prior releases of CA Deliver are running on your systems, release 11.7 compatibility PTFs must be applied as follows:

- If you are running CA Deliver r11.0/EBC r11.0, apply PTF RO19371, RO12652, and RO29509
- If you are running CA Deliver r11.5/EBC r11.5, apply PTF RO19402, RO13763, and RO31766
- If you are running CA Deliver r11.6/EBC r11.6, apply PTF RO26210

Security and Privileges

Once reports are encrypted, they are secure. We are using AES encryption with 256 or 128 bit keys.

External security interface is provided to CA Top Secret, CA ACF2, and IBM RACF.

Chapter 2: Installation and Upgrade

CA View is installed using the MSM or ESD PAX process.

For the CA View installation steps see your 11.5 CA View Installation Guide and the following sections in this guide:

- CA View Installation Guide - Chapter 3
- Upgrade Considerations in this guide.

This section contains the following topics:

The ESD PAX Installation Process

You can obtain CA View in a compressed format (pax.Z file) that enables you to install directly from DASD. This is known as the ESD PAX process.

To install CA View using the ESD PAX process, see the *CA View Installation Guide.*

Upgrade Considerations

CA View r11.6 is available to all CA View customers with active maintenance contracts. There is no specific license required to upgrade to release 11.6.

CA View r11.6 is backward compatible with CA View r11.0 and r11.5. XMS and CA Deliver direct archival can concurrently browse or archive to CA View r11.6, r11.5, and r11.0 databases.

See Backward Compatibility for information about encryption compatibilities.

Chapter 3: Configuration

This section provides information about the new initialization parameters and how to configure CA View r11.6.

This section contains the following topics:

The Initialization Parameters and Options

The following parameters are added to CA View.

- ENCRYPT=NO (Default)
- ENCRYPT=ICSF,nnn

Procedure to Configure CA View for Encryption

CA View r11.6 gives you the ability to enable AES encryption of reports stored in CA View.

To set up encryption in CA View

1. Determine if your hardware has the CPACF Crypto assist facility installed.

   Note that ICSF can perform encryption without this hardware, but it is extremely CPU intensive.

2. Review the encryption information.

   IBM's z9 hardware only supports 128 bit AES, however z10 hardware supports 256 bit. Be aware of the following:

   - If z9 and a hardware assist is present, encrypt/decrypt using 128 bits and the CPACF instruction set (hardware).
   - If z9 and no hardware assist is present, ICSF is called (software encrypt/decrypt) using 256 bit AES.
   - If z10 and a hardware assist is present, encrypt/decrypt using 256 bits and the CPACF instruction set (hardware).
   - If z10 and no hardware assist is present, ICSF is called (software encrypt/decrypt) using 256 AES

- A health check will also be triggered if encryption is enabled and CPACF hardware is not available. This is because software AES encryption is extremely CPU intensive.

3. Install CA View r11.6 using MSM or normal SMPE methods.

4. Set the ENCRYPT=ICSF,nnn initialization parameter and restart CA View.

   Reports archived from this point forward will be encrypted. Any reports that are reloaded from tape to disk will be encrypted. SARPAC will encrypt older reports as tapes are processed.

Chapter 4: CA View Parameter, Setting, and Information Changes

CA View r11.6 is built upon CA View r11.5.

Important! This document assumes the availability of the complete CA View r11.5 documentation set. Release Notes does not replace the Reference Guide, Messages Guide, or Best Practices documentation, it provides the updated information that will guide you as you install using CA MSM or ESD PAX and as you configure and use the new encryption functionality.

This Release Notes document contains updates to CA View parameters and settings, and additional information for the following documents:

The CA View Reference Guide

- Chapter 2
- Chapter 7
- Appendix B

The CA View Message Guide

- Chapter 3

The CA View Best Practices Guide

This section contains the following topics:

CA View Reference Guide

The sections that follow describe release 11.6 changes that have been made for the CA View Reference Guide.

Chapter 2. Initialization Parameters

Add the following parameter to Initialization Parameter Descriptions.

SARINIT Encryption Parameter ENCRYPT=

ENCRYPT=

Syntax

```
ENCRYPT=NO | ICSF,nnn
```

Description

This parameter specifies whether view data should be encrypted or not. Valid values are:

- NO—Report data is not encrypted
- nnn—Report data is encrypted using the ICSF AES algorithm. The encryption key is stored in the IPCS CKDS data set and is changed every nnn days throughout the year. Valid values are 1-366.

Chapter 7. Database Utilities

Replace the following in the Database Control Statements for the ADDDS statement.

ADDDS

The ADDDS control statement is used to create a new database, to add additional space to an existing database, or to add a new index file data set. Space is added by creating a new data set and formatting it with fixed-length blocks.

Database Extent Considerations

- For data sets that are 4,369 or fewer cylinders, the data sets are to be allocated as an IBM direct access data set.
- For data sets that are more than 4,369 cylinders, the data sets are to be allocated as physical sequential data sets due to IBM restrictions.

Note: The physical sequential data sets are accessible via standard utilities and ISPF. It is recommended that you use the CA View Systems Extension Data Set Security Feature to limit access to these data sets or implement encryption to secure the data.

To minimize contention, we recommend that each database extent be placed on a separate dedicated volume. Where possible, the size of the volume should match the size of the database extent. A matching database extent prevents I/O for multiple extents from queuing on the same device address.

Also, the first extent of the index and the database must be placed on separate dedicated volumes because the RESERVE processing uses the dataset name and volume of the first extent to serialize all accesses.

The high-level name of the database must have previously been defined with the NAME control statement (or the PARM parameter of the EXEC JCL statement).

Note: The allocation of a new index and/or data extent might not take effect immediately if archival tasks are active. (These archive tasks are SARSTC, FSS Collectors, or CA Deliver Direct-to-View.) Be aware of the following:

- The archival task does not need to be recycled for either a new index or data extent allocation to take effect.
- The new extent becomes active to an archival task when that processor makes a space allocation request.
- A newly allocated data extent becomes active to an archival task when a new Sysout is archived
- A newly allocated index extent becomes active to an archival task when the index is expanded by an index space allocation (cylinder allocation) request.

Syntax

```
ADDDS   ABOVE
        BLKSIZE=
        CYLINDER=
        DATACLASS=
        INDEX|DATA
        MGMTCLAS=
        STORCLAS=
        UNIT=
        VOLSER=
```

Where:

ABOVE

Indicates that the data set being added to the database can be allocated above the 64K cylinder line on a 3390-A device. Data sets that are allocated above the 64K cylinder line are allocated in increments of 21 cylinders so the final data set allocation is rounded up to the next multiple of 21 cylinders. This parameter is optional.

BLKSIZE=

Specifies the block size to be used in the data sets.

The minimum is 3476; the maximum is 32760. The default block size for the database index file data sets is 8906, and the default block size for the database data file data sets is 3768. The block size for an existing database cannot be changed, so this operand is only valid when you create a new database. After a database has been created, any subsequent use of the block size parameter is ignored.

Note: For more information about determining the block size to use, see Estimating DASD Requirements For a Database later in this chapter.

CYLINDER=

Specifies the number of contiguous cylinders to allocate to the data set. A maximum of 32,760 cylinders can be allocated to one data set.

DATACLASS=

Specifies the data class of an SMS dataset

INDEX|DATA

Specifies whether an index file or a data file data set is to be added to the database. INDEX indicates the addition of an index file data set suffixed with Innnnnnnn. DATA indicates a data file data set suffixed with Dnnnnnnnn. Either INDEX or DATA is required.

MGMTCLAS=

Specifies the management class of an SMS data set

STORCLAS=

Specifies the storage class of an SMS data set

UNIT=

Specifies the unit name to be used to dynamically allocate a new data set

VOLSER=

Specifies the volume serial number on which to allocate the new data set

All of the ADDDS keywords can be abbreviated to the fewest number of characters that makes them unique.

SMS and Non-SMS: Specifying Parameters

The following table summarizes the interdependency of the ADDDS parameters for SMS and non-SMS data sets:

Parameter	Non-SMS Data Set	SMS Data Set
BLKSIZE	Optional	Optional
CYLINDER	Required	Required
DATACLAS	Omit	Optional
MGMTCLAS	Omit	Optional
STORCLAS	Omit	Optional
UNIT	Optional	Omit

Parameter	Non-SMS Data Set	SMS Data Set
VOLSER	Optional	Omit

Estimating DASD Requirements for a Database

There is no way to know the exact amount of space that a database might require.

These formulas can be used to approximate the space needed (for this approximation, a block size of 3768 is used):

- If you are installing a new database, you must allocate 100 cylinders of INDEX for every 45,000 reports, including reports on tape. This allocation gives a 50 percent buffer to do standalone reorganization.
- CA View writes fixed-length blocks to its database. (You can specify a block size from 3476 through 32760.)
- For a block size of 3768, 195 blocks are contained in one cylinder of a 3390, 165 blocks are contained in one cylinder of a 3380, and 130 blocks are contained in one 3350 cylinder.
- Repetitive characters are compressed, giving, on the average, a 60 to 70 percent reduction in space requirements.
- The space required for the master index is minimal compared to the space required for the SYSOUT data; a minimum of one cylinder is required for the master index.

Procedure to Estimate Database Space

Using the previous information, you can use this procedure to approximate the amount of space required for your database.

1. Take the maximum lines archived to disk in one generation (that is, one day).
2. Multiply the number of lines by the average line length.
3. Divide by 3 (for compression).
4. Divide by 3768 to get number of blocks.
5. Divide by 195 (for a 3390) or 165 (for a 3380) or 130 (for a 3350) to get number of cylinders.
6. Multiply the result by the number of generations to be retained on disk.
7. To allow for growth, add 10 percent to the result.

Example

Assume that a site produces 1,000,000 lines of SYSOUT in one day to be archived on disk. The average line length of the SYSOUT is 121 bytes, and three days' worth of SYSOUT is going to be kept on disk.

Using the method described on the previous page, space requirements can be approximated as follows:

- 1,000,000 lines (per generation)
- 1,000,000 lines * 121 bytes/line = 121,000,000 bytes
- 121,000,000 bytes / 3 = 40,333,333 bytes (compressed)
- 40,333,333 bytes / 3768 bytes/block = 10,705 blocks
- A block size of 3768 is assumed for this example. Consult your DASD administrator to choose an optimal block size.
- 10,705 blocks / 195 3390-cylinders = 55 3390-cylinders
- 55 3390-cylinders * 3 generations = 165 3390-cylinders
- 165 3390-cylinders + 17 3390-cylinders (10%) = 182 3390-cylinders

Appendix B. CA View Health Checks

The VIEW_OPT_ENCRYPT@STCname Health Check has been added to CA View.

The following health check is provided for the encryption function.

VIEW_OPT_ENCRYPT@STCname

Description

This health check warns that the CA View database xxxxxxxxxx has detected a setting of ENCRYPT=ICSF, but encryption hardware is not installed on this machine.

If CPACF status is absent, the optimum encryption hardware is not available for use in encryption processing. Be aware that CA View can encrypt and decrypt reports without encryption hardware, but emulating encryption hardware is very CPU intensive and will use CPU resources that might be needed for production applications.

This could potentially delay those applications.

Best Practice

Important! We recommend that all archiving and browsing tasks for encrypted databases be run on a machine that supports hardware encryption.

System Programmer Response

For optimal encryption performance, use the CPACF hardware in your system. If you do not have CPACF enabled, contact IBM to determine if the no-cost CPACF option can be made available for your system.

If possible, run the following tasks on a machine that supports hardware encryption – SARSTC, FSS collectors, and SARXMS.

Note: CP Assist for Cryptographic Functions (CPACF) is a standard component on z9 and z10 and a no-cost option for z890 and z990 processors.

To disable encryption, run SARINIT and set ENCRYPT=NO. After setting the option, cycle the SARSTC started task and any SARFSS collectors.

Parameters Accepted

None

Reference

See the Configuration section earlier in this guide for more information.

Messages

The following messages are generated:

- SARH005E
- SARH005I

CA View Message Guide

The section that follows describes the release 11.6 changes that have been made for the CA View Message Guide.

Chapter 3. Messages

Add the following messages:

SARDBA46

Large format data sets only supported for a release 11.6 or higher database

Reason:

The SARDBASE ADDDS statement specified to add a large format data set (data set with more than 4369 cylinders) to an 11.5 or earlier release level database. Large format data sets are only supported for 11.6 or higher release level databases.

Action:

Version the database level of the database to 11.6 with the SARDBASE VERSION statement prior to adding the large format data set or reduce the number of cylinders on the SARDBASE ADDDS statement.

SARDBC10

Release 11.5 or earlier database cannot be copied to database with large format data sets

Reason:

The SARDBASE COPY statement specified to copy an 11.5 or earlier release level database to a new database that contains a large format data set (data set than with more 4369 cylinders). Large format data sets are only supported for 11.6 or higher release level databases.

Action:

Version the database level of the "FROM" database to 11.6 with the SARDBASE VERSION statement or recreate the "TO" database with data sets that have 4369 cylinders or less prior to copying the database.

SARDBM10

Release 11.5 or earlier database cannot be loaded/merged to database with large format data sets

Reason:

The SARDBASE LOAD or MERGE statement specified to load or merge an 11.5 or earlier release level database to a new database that contains a large format data set (data set with more than 4369 cylinders). Large format data sets are only supported for 11.6 or higher release level databases.

Action:

Recreate the new database with data sets that have 4369 cylinders or less prior to loading or merging the database. Alternatively, version the old 11.5 or earlier release level database(s) to 11.6 with the SARDBASE VERSION statement, perform a new unload the database(s), and then load or merge the database(s).

SARDBR10

Release 11.5 or earlier database cannot be restored to database with large format data sets

Reason:

The SARDBASE RESTORE statement specified to restore an 11.5 or earlier release level database to a new database that contains a large format data set (data set with more than 4369 cylinders). Large format data sets are only supported for 11.6 or higher release level databases.

Action:

Recreate the new database with data sets that have 4369 cylinders or less prior to loading or merging the database.

SARDBT23

Database with large format data sets cannot be versioned to release 11.5 or earlier

Reason:

The SARDBASE VERSION statement is being used to version a database to release level 11.5 or earlier but the database contains a large format data set (data set with more than 4369 cylinders). Large format data sets are only supported for 11.6 or higher release level databases and cannot be versioned to release 11.5 or earlier.

Action:

To be compatible with the 11.5 or earlier database structure, the 11.6 or higher release level database will have to be recreated. A new database will have to be created with data sets that have 4369 cylinders or less. The 11.6 or higher release level database will have to be copied or loaded into the new database. After the copy or load, the database can be versioned to the 11.5 or earlier database release level.

SARH005E

CA View database "xxxxxxxxxx" has detected a setting of ENCRYPT=ICSF, but encryption hardware (CPACF) is not installed on this machine.

Reason:

This message is informational, but be aware that CA View can encrypt and decrypt reports without encryption hardware, but emulating encryption hardware is very CPU intensive.

Action:

See the CA View Health Checks section earlier in this guide for more information.

SARH005I

CA View database "xxxxxxxxxx" has detected a setting of ENCRYPT=ICSF. This machine has the recommended hardware encryption support to optimize encryption performance.

Reason:

This message is informational.

Action:

None.

SARICF01

ICSF key(s) generated - be sure to backup ICSF CKDS data

Reason:

New keys have been placed in the ICSF CKDS data set. This data set should be backed up as soon as possible.

Action:

CA View has updated encryption keys in the ICSF CKDS dataset. These keys will be required when encrypting and decrypting report data. To insure that these keys are available, this data set should be backed up and sent to your disaster recovery site.

SARICF02

CSF error - Service=xxxxxxxx RC=nnn Reason=nnn Entry=nnn

Reason:

ICSF has returned an error code. The return and reason codes are described in Appendix A of the IBM publication ICSF Application Programmers Guide (SA22-7522).

xxxxxxxx is the name of the ICSF service that failed.

Action:

Contact CA Technical Support.

SARICF03

ICSF not active - Service=xxxxxxxx RC=nnn Reason=nnn

Reason:

xxxxxxxx is the name of the ICSF service that failed.

ICSF has returned an error code. The return and reason codes are described in Appendix A of the IBM publication ICSF Application Programmers Guide (SA22-7522).

Action:

Insure that ICSF is running on the machine where the error occurred.

SARICF04

ICSF not installed - Service=xxxxxxxx Entry=nnn

Reason:

xxxxxxxx is the name of the ICSF service that failed, CA-View failed to load the above ICSF service.

Action:

Contact CA Technical Support.

SARICF05

ICSF key not found - Key=xxxxxxxx Entry=nnn

Reason:

Xxxxxxxx is the name of the missing key

CA View has requested the above key from the ICSF key store (CKDS) and it was not found. This type of error occurs when the CKDS has been restored to an old version or multiple CKDS datasets are used for the same CA-View database.

Action:

Contact CA Technical Support to determine if the key can be recovered and the extent of the data loss.

SARICF06

Invalid entry code nnn

Reason:

An internal error has occurred within CA View.

Action:

Contact CA Technical Support.

SARPAM30

External key manager error obtaining key for database ¢ - Reply R (retry) or T (terminate)

Reason:

The direct to CA View archival feature is attempting to write report data to an encrypted database but the external key manager product (ICSF) is not active, not installed, or rejected the service request to obtain the encryption key. This write to operator message will be preceded by a SARICF message that identifies the specific error.

Action:

The SARICF message will specifically identify the nature of the error. If the SARICF error message identifies a return and reason code, a description of the code can be found in Appendix A of the IBM z/OS Cryptographic Service Application Programmer's Guide.

Once the problem is resolved and the external key manager product is active, reply "R" to the SARPAM30 to resume direct to CA View archival for the job. The direct to CA View archival interface will attempt to reestablish communication with the external key manager product every minute. If connection is reestablished, the SARICF and SARPAM30 messages will be deleted. If the external key manager product error cannot be resolved in the near term, the job can be terminated by replying "T" to the SARPAM30 message. If this is the case, it may also be desirable to turn off direct to CA View archival or turn off encryption to the affected database(s).

SARSTC42

Encryption enabled for xxx…xxx

Reason:

xxx…xxx is the name of the CA-View database.

This is a confirmation that reports are being encrypted.

Action:

None.

SARXTD23

CSVDYLPA macro failed for module xxxxxxxx, R15=xxxx R0=xxxx FLAGS=xxxx PROCESSING CONTINUES

Reason:

SARXTD was unable to add the above module to the MLPA CDE directory. This is only needed by product support and does not affect normal product performance.

Action:

Contact CA Technical support.

CA View Best Practices Guide

The section that follows describes the release 11.6 change that has been made for the CA View Best Practices Guide.

Data Encryption

Use the CA View ENCRYPTION feature to secure and protect your data.

Business Value:

Protecting your data is of utmost importance. Customers that store credit card data must abide by PCI compliance. One of the most important factors in this compliance is to provide optimum security–data at rest must be encrypted via strong encryption. Reports are encrypted on both disk and tape.

More Information:

For more information about Encryption, see the CA View r11.6 Release Notes.

Index