IBM Education Assistance for z/OS V2R3

Log stream and DIV data set level encryption support

Element/Component: BCP system logger and DIV

Agenda

- Trademarks
- Session Objectives
- Overview
- Usage & Invocation
- Interactions & Dependencies
- Migration & Coexistence Considerations
- Installation
- Session Summary
- Appendix

Trademarks

- See url http://www.ibm.com/legal/copytrade.shtml for a list of trademarks.
- Additional Trademarks:
  - None

Session Objectives

Understand:

z/OS v2r3 system logger and DIV enhancements / changes:

- Basics of data set level encryption
- Considerations for encrypting log stream data sets
- Considerations for DIV encrypted data sets

Overview – data set level encryption for log stream data sets

- Problem Statement / Need Addressed
  - Access method data set level encryption support is being provided in z/OS v2r3 and on z/OS v2r2
  - Without any enhancements, system logger and DIV will not be able to access any encrypted data sets
  - Will result in exploiters not being able to use their log stream or DIV resources, leading to numerous failed processing situations

- Solution (in z/OS v2r3 release, with roll down to z/OS v2r1)
  - Provide the system logger and DIV enhancements necessary to make use of encrypted (log stream) data sets that are established via new policies and specifications

- Benefit / Value
  - Clients will be able to enhance data security for their sensitive data that is housed in encrypted data sets

Usage & Invocation

- **Log stream** data set encryption can be enabled by naming ***key labels*** that identify cryptographic keys to be used for data set level encryption through:
  - DFSMS data class definitions or ACS routines — DATA SET KEY LABEL ke*ylabel*
  - JCL, dynamic allocation or TSO/E allocate — DSKEYLBL(*keylabel*), DALDKYL (8032)
  - RACF data set profile - this takes precedence — DATAKEY(*keylabel*)

- ***key labels***
  - string from 1 to 64 characters (bytes)
  - identifies a protected data key in the ICSF repository
  - type of encryption: *AES*-256 *XTS* protected key

- Once the key label is derived for the data set during new data set allocation, the encryption info will be maintained in the catalog:
  - ***key label***, encryption type and mode
  - this Catalog info cannot be overridden or replaced

Usage & Invocation (continued)

Setup and use for significant areas:

- ICSF setup
- RACF setup
- DFSMS setup
- System logger setup and use

Usage & Invocation (continued)

ICSF setup

see Installation topic for PTFs and hardware requirements

- Activating the ICSF address space is required
- For information about ICSF, see *zOS Cryptographic Services Integrated Cryptographic Service Facility Administration Guide*
- Set up and maintain cryptographic keys and the KEYLABELS to be used for data set level encryption
- Ensure the Sysplex ICSF repository (database) is shared and maintained across all systems in the sysplex, and on any recovery site systems, so that any use of the data set key labels are consistent across the sysplex for encrypting and de-crypting
- Ensure the catalogs are also shared across these same systems when data set level encryption is used

Usage & Invocation (continued)

ICSF setup (continued)

- For the ICSF segment of the covering profile must be updated with the following new options to ensure wrapped keys can be returned:
  - SYMCPACFWRAP(YES) to allow key label to be wrapped
  - SYMCPACFRET (YES) to allow the service to return the wrapped key
- For protected keys,
  - set up profiles in the CSFKEYS general resource class and set up groups and users to allow system logger address space (IXGLOGR) access to the key labels
  - refer to sections
    - "Setting up profiles in the CSFKEYS general resource class"
    - "Enabling use of encrypted keys in Symmetric Key Encipher and Symmetric Key Decipher callable services”
- Sample:

```
RDEFINE CSFKEYS * UACC(READ) ICSF(SYMCPACFWRAP(YES) SYMCPACFRET(YES))
```

Usage & Invocation (continued)

RACF setup

You can optionally use a key label in RACF DS profiles

- For information about RACF, see *z/OS Security Server RACF Security Administrator's Guide.*
- Create RACF data set profiles, in the DFP Segment specify desired key label
  - **DATAKEY(*key-label-value*)**
    - identifies the KEY LABEL in ICSF CKDS
    - used to encrypt/decrypt the data

Usage & Invocation (continued)

DFSMS setup

- Access method data set encryption is restricted to:
  - SMS managed data sets that are Extended Format on 3390 device types.
- Activate the SMS address space
- Ensure **ACSDEFAULTS(YES)** in SYS1.PARMLIB(IGDSMSxx) member
- For information about DFSMS, see *z/OS DFSMS Using the Interactive Storage Management Facility*

- You can optionally use a key label in DFSMS Data Classes with Extended format option using the Interactive Storage Management Facility (ISMF) panels or ACS routines
- DFSMS data class:
  - Data Set Name Type "EXT" (extended format)
  - **Data Set Key Label** ***key-label-value***
- refer to log stream definition STG_DATACLAS and LS_DATACLAS values

Usage & Invocation (continued)

System Logger setup and use

- When using data set level encryption for log stream data sets:
  - Define read access to RESOURCE(CSFKRR2) CLASS(CSFSERV)
  - Define read access to the profiles covering any ICSF key labels used for encrypting log stream data sets in the general CSFKEYS class.

- If using the data class approach:
  - update the intended log stream definitions to specify the appropriate **STG_DATACLAS** and **LS_DATACLAS** values
  - remember to use different class definitions since the Control Interval (CISIZE) settings are:
    - 4K for staging data sets (required)
    - 24K for offload data sets (recommended)

Usage & Invocation (continued)

System Logger setup and use (continued)

- There is a new system logger WTOR message IXG079E (see next pages)
  - So automation might be affected

- **NO** other setup changes to system logger are required, including:
  - LOGR CDS (couple data set)
  - log stream definitions
  - IXGCNFxx parmlib specifications

Usage & Invocation (continued)

New system logger messages IXG079E (WTOR), IXG080I and IXG290I:

- when attempting to open an encrypted log stream data set and ICSF is not available:
  - IXG290I LOGSTREAM DATASET OPEN PENDING
    FOR DSN=*dsname*
    WAITING ON SYSTEM SERVICES AVAILABILITY: ICSF
  - IXG079E ICSF IS NOT ACTIVE. ACTIVATE ICSF, OR REPLY
    WITH ANY CHARACTER FOR LOGGER TO CONTINUE REGARDLESS.
- when attempting to open an encrypted log stream data set and ICSF is not available:
  - IXG080I LOGGER NO LONGER WAITING ON ICSF,
    a) SINCE ICSF IS NOW AVAILABLE
    b) AS A RESULT OF THE IXG079E MESSAGE REPLY
    c) UNEXPECTED ICSF STATE CHANGE
- If 2nd open attempt fails, then existing system logger error messages will be issued and the existing error handling for the failed access with result

Usage & Invocation (continued)

To stop using log stream data set encryption:

- *take action to stop system logger from creating new encrypted log stream data sets, based on how you enabled encryption:*
  - update your log stream definition to use a different DFSMS data class definition
  - change the DFSMS data class definition or ACS routine to no longer specify a data set key label
  - remove DATAKEY specification from RACF profiles covering log stream data sets
- *since the above does not alter any existing encrypted data sets, take action to cause existing log stream data sets to be deleted:*
  - *depending upon each log stream exploiter, your options to cause the deletion of existing log stream data sets can vary greatly*
  - *for example, you may need to disconnect from the log stream from all the connected systems in the sysplex, or you may need to delete the log stream entirely*
- *you could alternatively rename the existing (encrypted) log stream and define a new instance with the original name*
  - *in case of need to keep original encrypted log stream data sets*
  - *but will need encrypted environment enabled to access any of that log data*

Usage & Invocation - DIV

- Data in Virtual
  - Supports mapping virtual storage to a Linear VSAM data set, referred to as a DIV object
  - DIV objects on extended format data sets may be encrypted
    - when a data set is newly created as per the policy or specification intent
    - via RACF profile, JCL – dynamic allocation – TSO/E Allocate (**DSKEYLBL**), DFSMS data class or ACS routines, etc.
  - DIV application need not be aware of this – no changes to the interface other than possible failure scenarios.

- DIV ACCESS – open the data set
  - DIV application not SAF authorized to use ICSF services
    - ABEND08D, RSN=xxxx0055
  - DIV application not SAF authorized to access the key label
    - ABEND08B, RSN=xxxx0056
  - ICSF is not available
    - Return code 'C'x, RSN=xxxx0809

Usage & Invocation - DIV (continued)

- DIV ACCESS errors *(continued)*
  - Key associated with key label not found
    - Return code 'C'x, reason xxxx080A
  - Co-processor needed to process the request not available
    - Return code 'C'x, reason xxxx080C
  - Failure due to some other ICSF or cryptographic hardware related problem
    - Return code 'C'x, reason xxxx080B
    - MMSPL Media Manager parameter list is traced

- DIV SAVE errors
  - DIV could not obtain storage for encryption buffers
    - Return code '8'X, reason xxxx004E

Interactions & Dependencies

The following key enhanced areas are required to take advantage of this new function:

- DFSMS Access Method Data Set Level Encryption
  - see PTFs for anchor APAR **OA50569** for pre-z/OS v2r3 support
- JCL and dynamic allocation enhancements for data set level encryption
  - (pertinent for DIV)
- Catalog support for data set level encryption
- RACF support for data set level encryption
  - The Systems Access Facility (SAF) security server (RACF element) provides secure, high-speed cryptographic services in the z/OS environment
- Integrated Cryptographic Service Facility (ICSF)
  - ICSF is the software element of z/OS that works with the hardware cryptographic features

Interactions & Dependencies (continued)

- z/OS system logger and DIV make use of the DFSMS media manager for their respective data set access
- Enhancements in system logger and DIV were required in order to access (log stream) data sets that are defined/created as encrypted data sets
- DFSMS media manage will interact with ICSF to obtain data set key label encryption information when a log stream data set is opened (media manager connect request)
- Therefore, the ICSF address space must be activated

<u>For system logger:</u>

- If the ICSF address space is not available when system logger opens a log stream data set, then a new WTOR message IXG079E is issued
- System logger will wait for an ENF signal if/when ICSF becomes available or a reply to the message
- Either response will cause message IXG079E to be cleared (DOMed), and then system logger will retry one more time to open the data set

Migration & Coexistence Considerations

Since encrypted log stream data sets will be able to be established on z/OS V2R3 and z/OS V2R2 release level systems with all the appropriate support applied and required hardware installed,
coexistence support is also being provided on z/OS V2R1 for mixed release level sysplex configurations.

- Requires PTFs on z/OS v2r2 and z/OS v2r1
- Appropriate minimum hardware and features must be installed
- Do not allow encryption for any log stream data sets unless:
  - all systems in the sysplex, and on any recovery site systems for the sysplex are at the same functional and definitional levels

Installation

- Support is inherent in z/OS v2r3 when it is generally available
- ensure required hardware and features are installed
  - For protected keys, the minimum processor hardware is z196 or higher processor with CEX3 or later
    - z196/z114 require CEX3 (feature 0864)
    - zEC12/zBC12 require CEX3 (feature 0864) or CEX4 (feature 0865)
    - z13 - CEX5 (feature 0890)
- Apply PTFs and all related requisites for:
  - system logger APAR **OA52047**
  - DIV APAR **OA52093**
  - refer to PTFs for DFSMS APAR **OA50569** and all its If-reqs & Pre-reqs
  - and DFSMS media manager APAR **OA51052**

Session Summary

You should now be aware of:

z/OS v2r3, z/OS v2r2 and z/OS v2r1 system logger and DIV enhancements / changes:

- Basics of data set level encryption
- Considerations for encrypting log stream data sets
- Considerations for DIV encrypted data sets

Appendices

- Appendix A: publications

Appendix A: publications

z/OS V2R3 Introduction and Release Guide

z/OS V2R3 Summary of Message and Interface Changes

z/OS MVS Setting Up a Sysplex

z/OS MVS System Messages, Vol 10 (IXC-IZP)

z/OS MVS System Codes

z/OS MVS Programming: Assembler Services Guide

z/OS MVS Programing: Assembler Services Reference, Volume 1 (ABE-HSP)