IBM Education Assistance z/OS V2R3

DFSMS

Agenda

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

© 2017 IBM Corporation

Trademarks

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

© 2017 IBM Corporation

Session Objectives

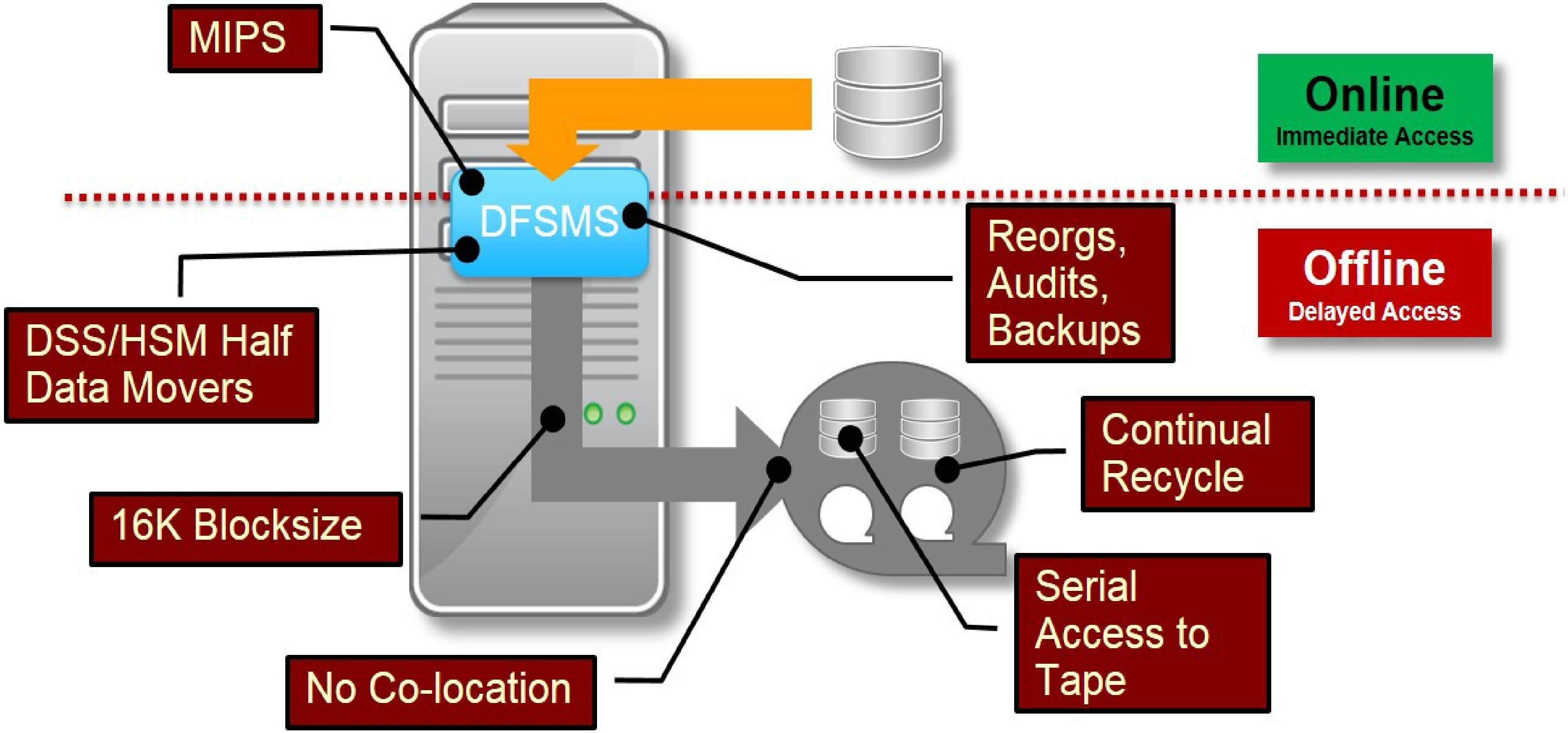
- **Overview Only of recently GA'd SPEs**
  - Transparent Cloud Tiering
  - zCDP Common Recover Queue
  - DS8K Thin Provisioning – Space Reclamation
  - DFSORT Enhancements
- **Details for DFSMS New Functions**
  - Data Set Level Encryption (V2R2 and V2R3)
  - Multiple OAM Address Spaces per LPAR
  - DFSORT UNICODE
  - RMM Enhancements
  - VSAM Enhancements
  - DFSMSdss Enhancements
  - VTOC Update Safe Interface and SMF Record

© 2017 IBM Corporation

Overview

Transparent Cloud Tiering

- **Problem** – Data Management still uses a 1970's architecture

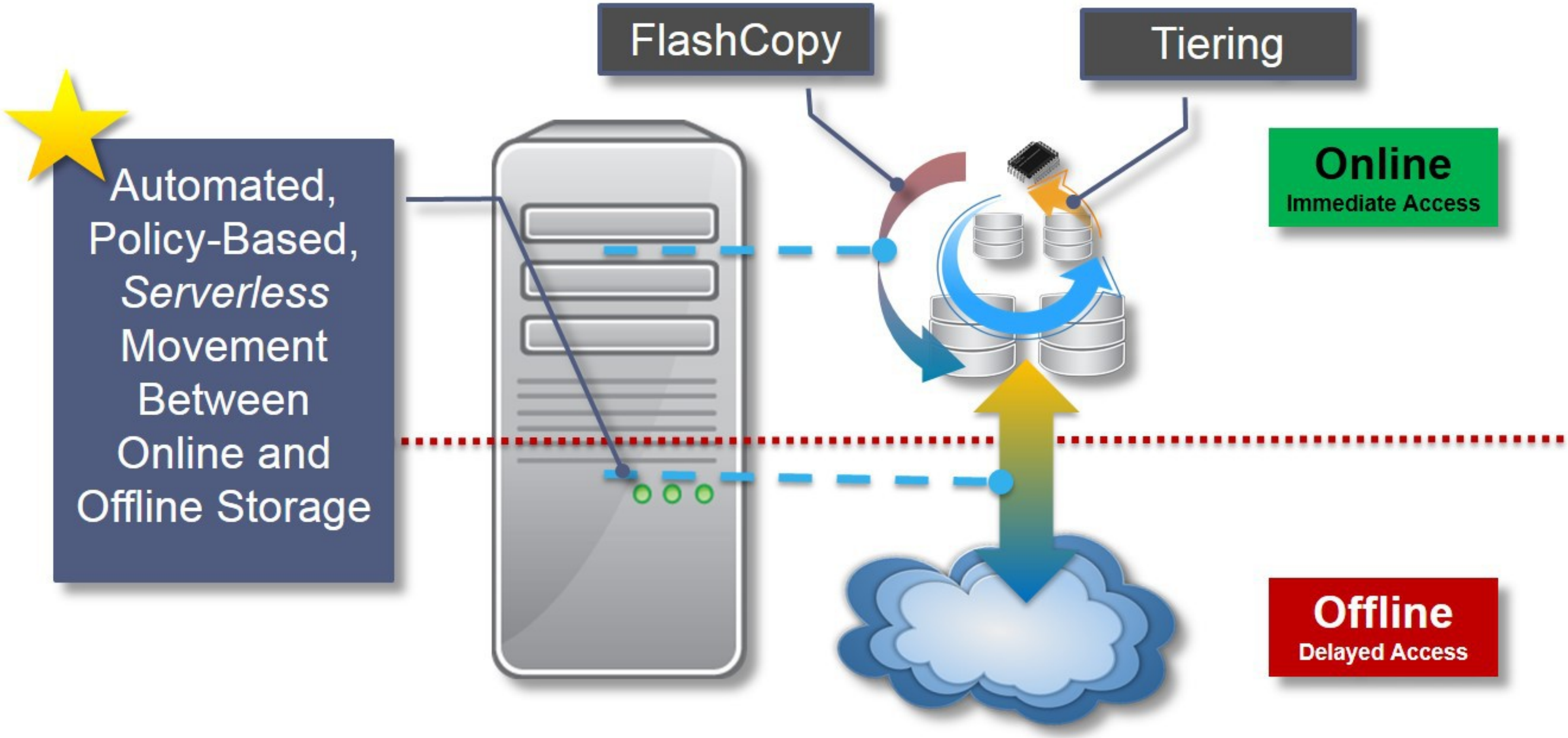


© 2017 IBM Corporation

Overview

Transparent Cloud Tiering

- **Solution** – Offload storage movement to storage controllers



© 2017 IBM Corporation

Overview

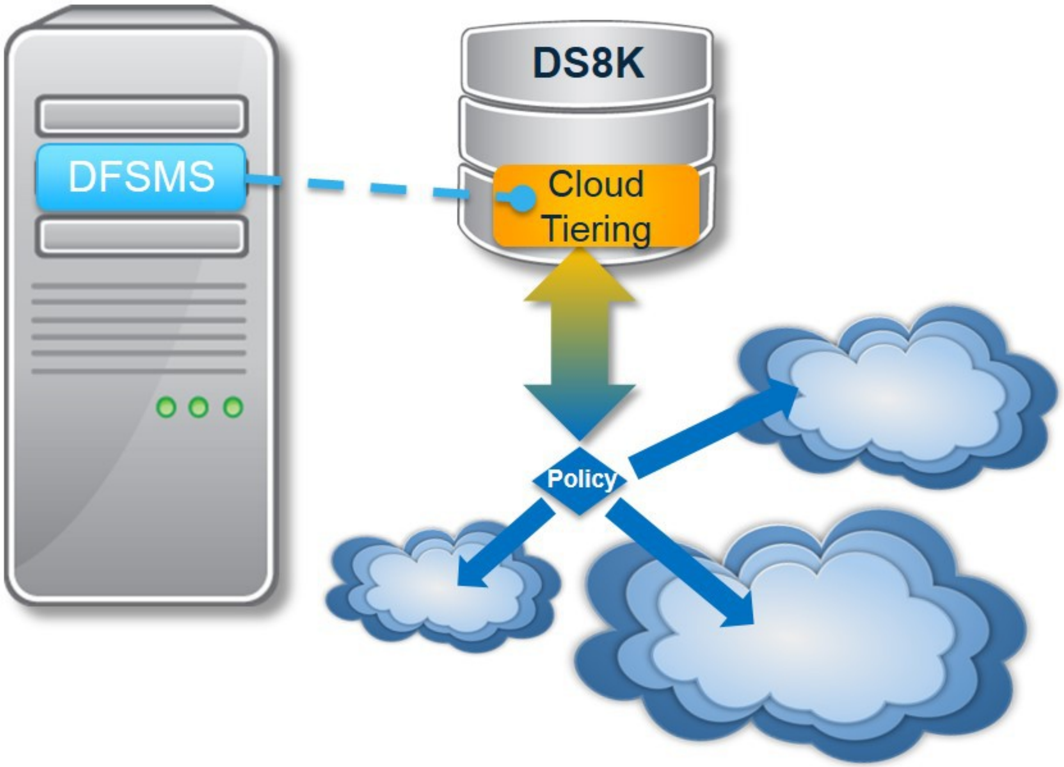
Transparent Cloud Tiering

- **Solution** – IBM DS8000 transparent cloud tiering
  OA51622 - 4th Quarter 2016 GA on z/OS V2R1 and DS8870 7.5
  OA50667 - 1st Quarter 2017 GA on z/OS V2R2
  Base on z/OS V2R3

★ Serverless, direct data movement between DS8000 & Cloud Storage

★ No additional appliance

★ Software Defined Microcode Update using existing Ethernet ports

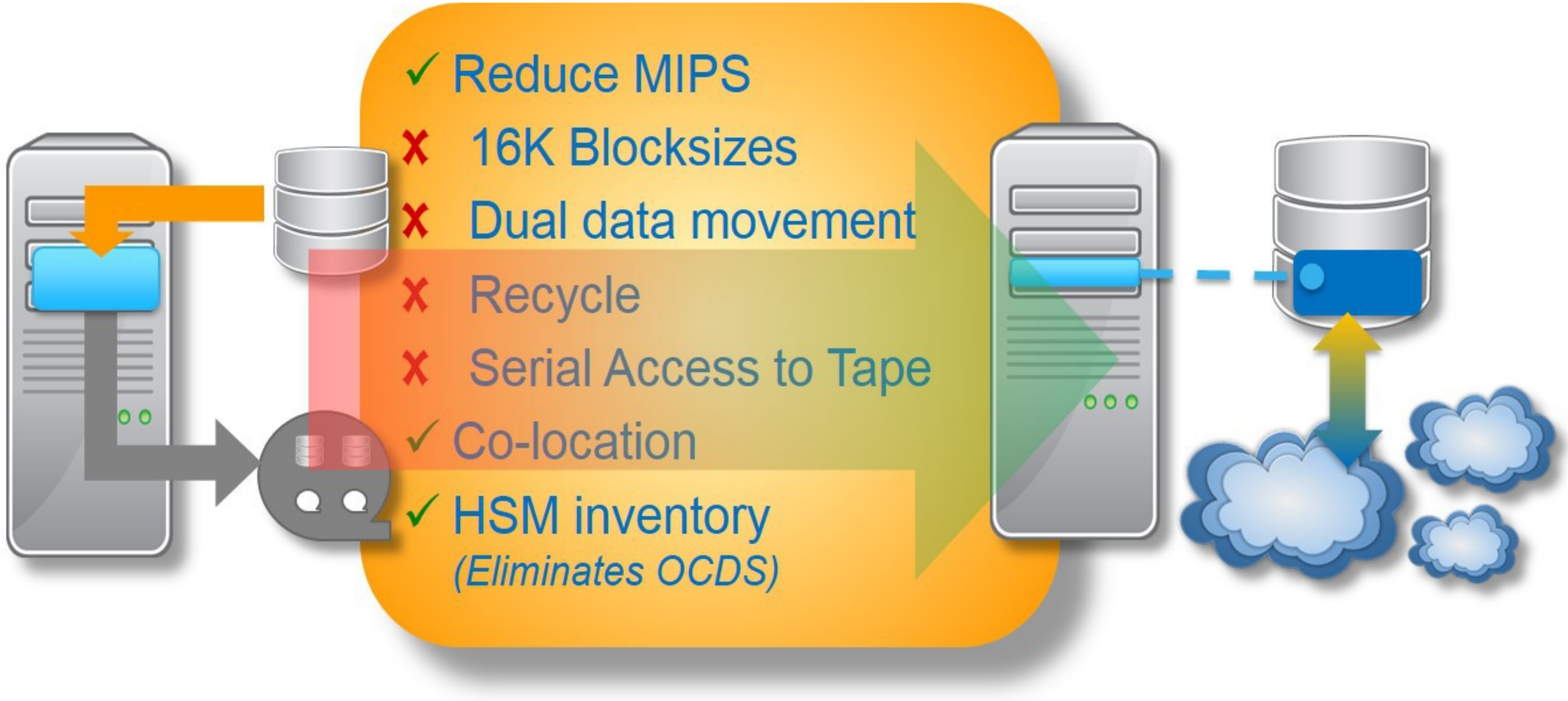


© 2017 IBM Corporation

Overview

Transparent Cloud Tiering

- **Benefit** – Eliminates today's constraints for managing data



✓ Reduce MIPS

✗ 16K Blocksizes

✗ Dual data movement

✗ Recycle

✗ Serial Access to Tape

✓ Co-location

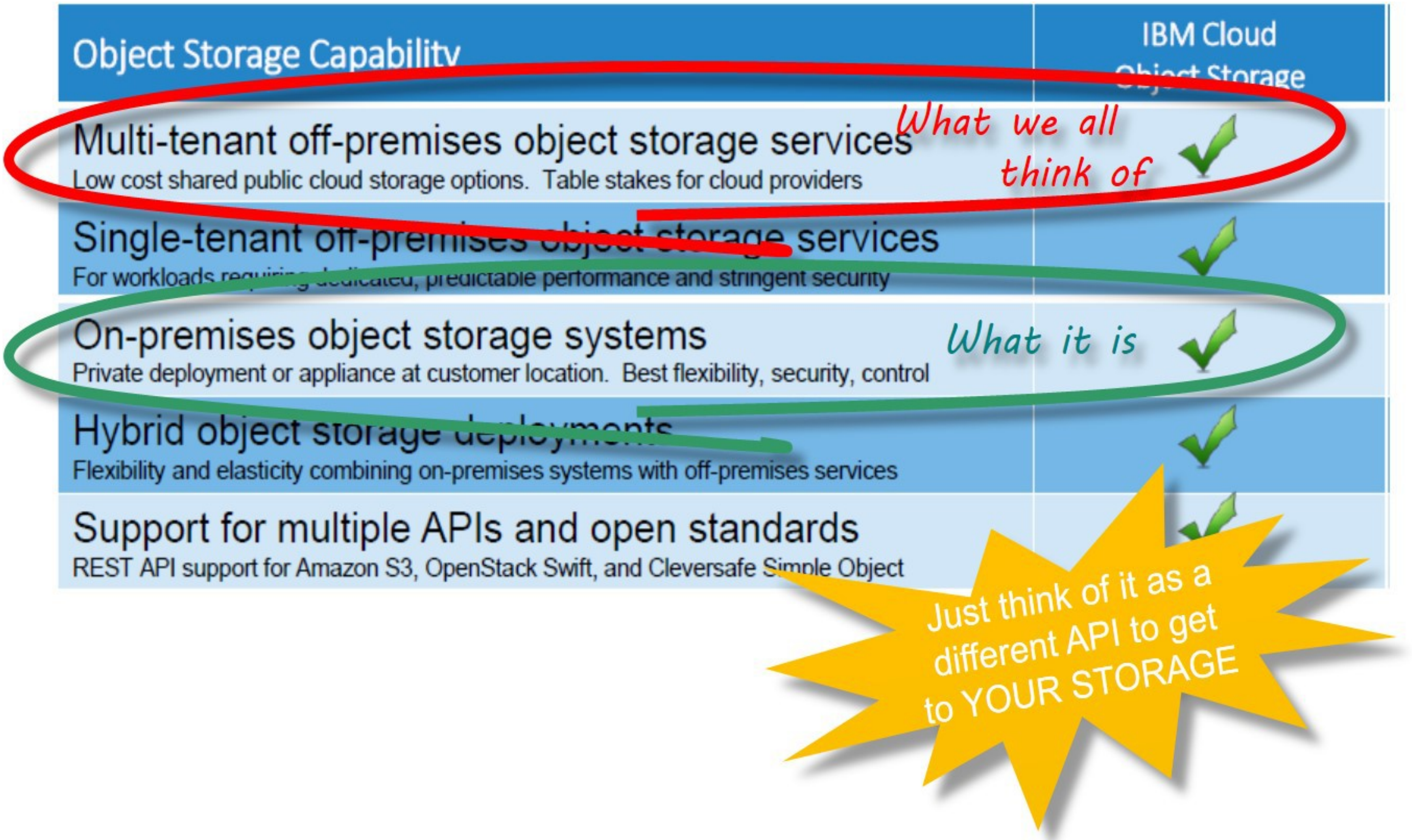
✓ HSM inventory
(Eliminates OCDS)

© 2017 IBM Corporation

Overview

Transparent Cloud Tiering

- **Benefit** – Cloud object storage can be private, on-premise storage



Object Storage Capability	IBM Cloud Object Storage
Multi-tenant off-premises object storage services Low cost shared public cloud storage options. Table stakes for cloud providers	✓
Single-tenant off-premises object storage services For workloads requiring dedicated, predictable performance and stringent security	✓
On-premises object storage systems Private deployment or appliance at customer location. Best flexibility, security, control	✓
Hybrid object storage deployments Flexibility and elasticity combining on-premises systems with off-premises services	✓
Support for multiple APIs and open standards REST API support for Amazon S3, OpenStack Swift, and Cleversafe Simple Object	✓

What we all think of

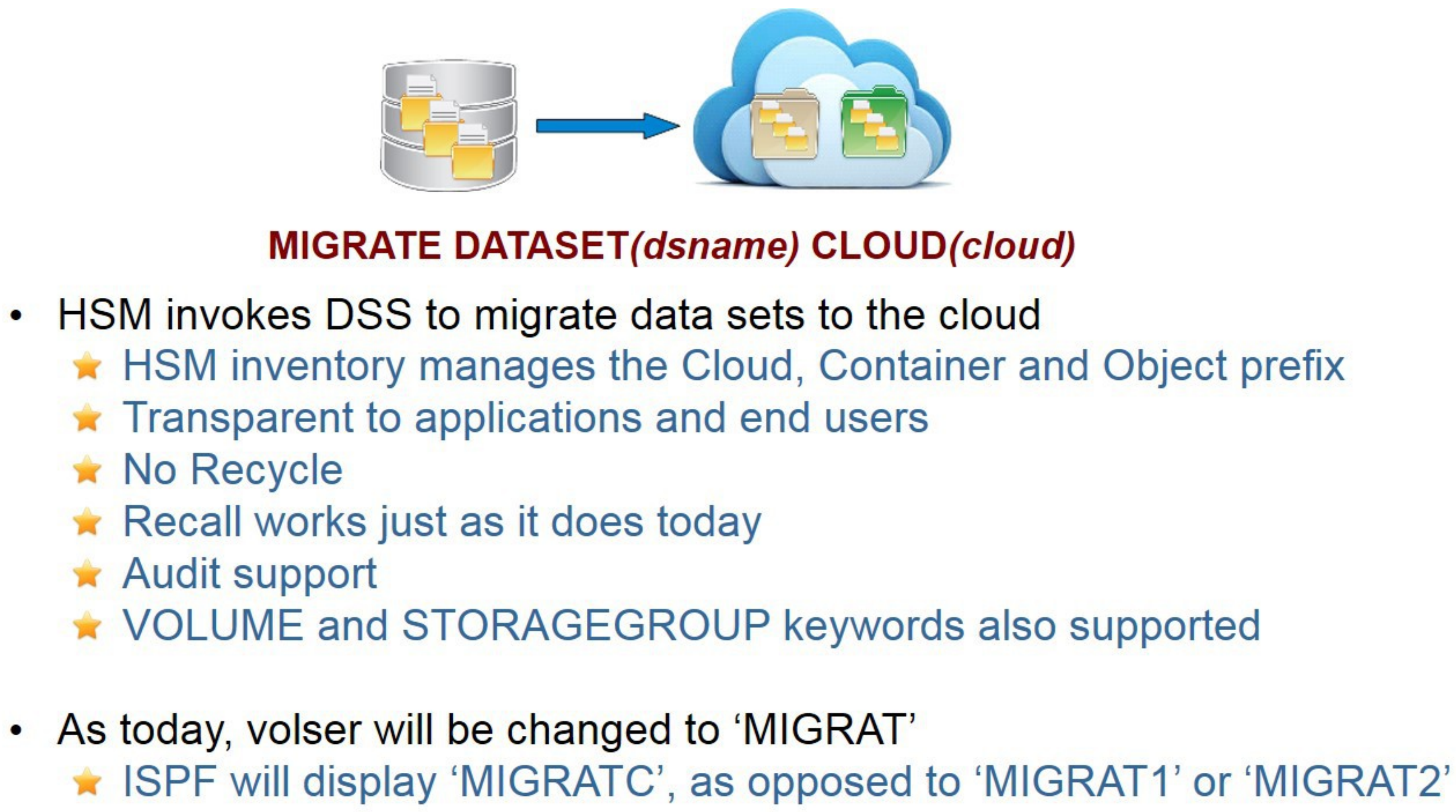
What it is

Just think of it as a different API to get to YOUR STORAGE

Overview

Transparent Cloud Tiering

- **Benefit** – Cloud Storage is just a new Migration Tier



MIGRATE DATASET*(dsname)* CLOUD*(cloud)*

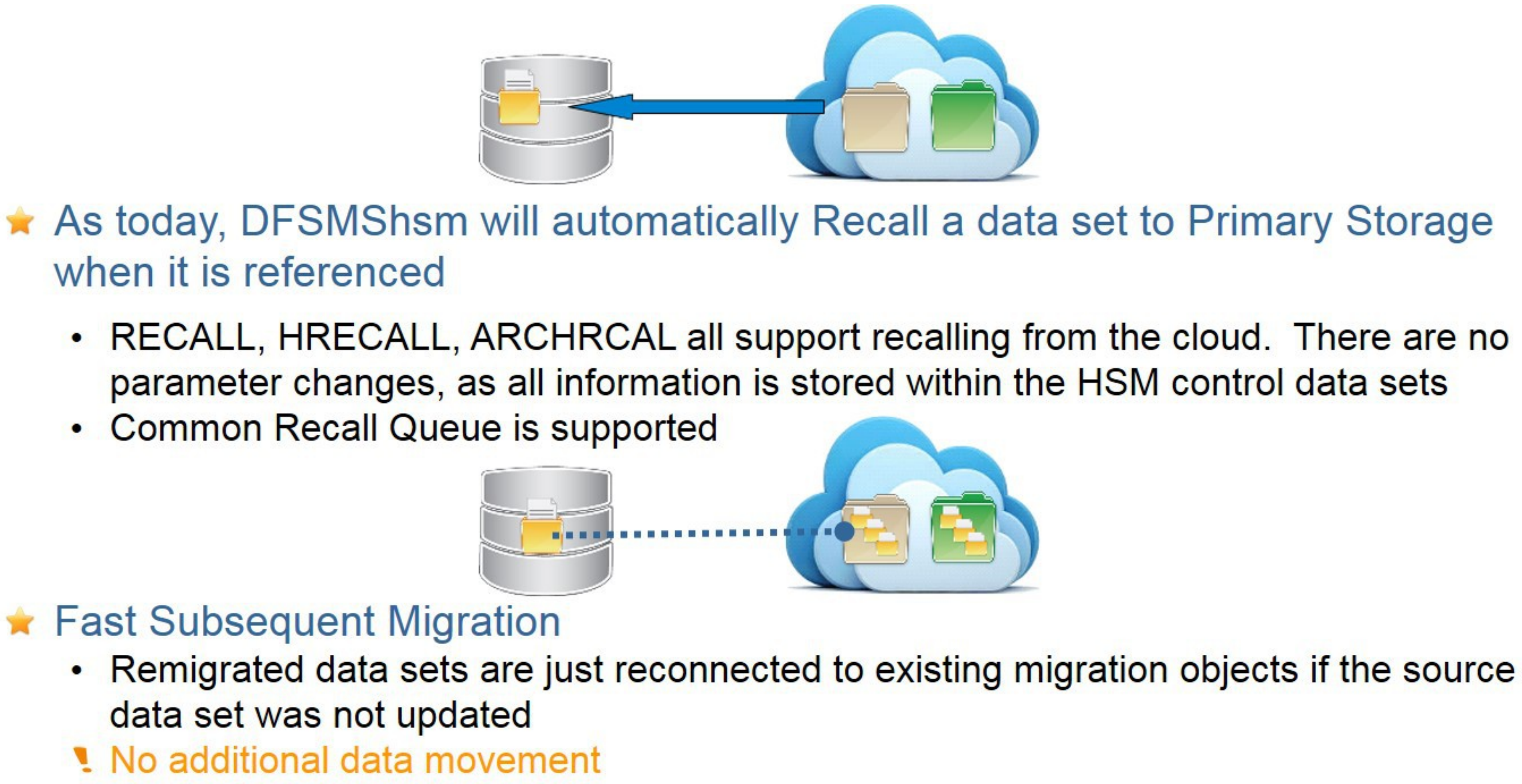
- HSM invokes DSS to migrate data sets to the cloud
  - HSM inventory manages the Cloud, Container and Object prefix
  - Transparent to applications and end users
  - No Recycle
  - Recall works just as it does today
  - Audit support
  - VOLUME and STORAGEGROUP keywords also supported

- As today, volser will be changed to ‘MIGRAT’
  - ISPF will display ‘MIGRATC’, as opposed to ‘MIGRAT1’ or ‘MIGRAT2’

Overview

Transparent Cloud Tiering

- **Benefit** – Recall from Cloud Storage is transparent for users and applications



★ As today, DFSMShsm will automatically Recall a data set to Primary Storage when it is referenced

- RECALL, HRECALL, ARCHRCAL all support recalling from the cloud. There are no parameter changes, as all information is stored within the HSM control data sets
- Common Recall Queue is supported

★ Fast Subsequent Migration

- Remigrated data sets are just reconnected to existing migration objects if the source data set was not updated

! No additional data movement

Overview

zCDP Common Recover Queue

- **Problem** – Exposure to malicious data corruption

AP: Regulators Looking to Strengthen Banks' Cyber Defenses

Marcy Gordon, AP Business Writer Updated 7:54pm, Wednesday, October 19, 2016

WASHINGTON — Federal regulators are looking to set up new standards for big banks' planning and testing for possible cyberattacks. The aim is to bolster the banking industry's defenses amid concern over periodic security breaches at U.S. Banks.

The move announced Wednesday by the Federal Reserve, the Federal Deposit Insurance Corp. and a Treasury Department banking agency is designed to get banks' senior executives and directors to pay closer attention to cybersecurity, agency officials said.

Fed Chair Janet Yellen has said that cybercrime is a "very significant threat." …

The banks should establish goals for how long it would take them to recover from a cyberattack, and should assess the potential for malware or corrupted data to spread through connected computer systems, the regulators said. …

Computers at the Fed were penetrated **dozens** of times between 2011 and 2015, according to House lawmakers. …

Overview

zCDP Common Recover Queue

- **Problem** – Exposure to malicious data corruption

FFIEC Appendix J: Strengthen Resiliency of Outsourced Technology Services

Federal Financial Institutions Examination Council

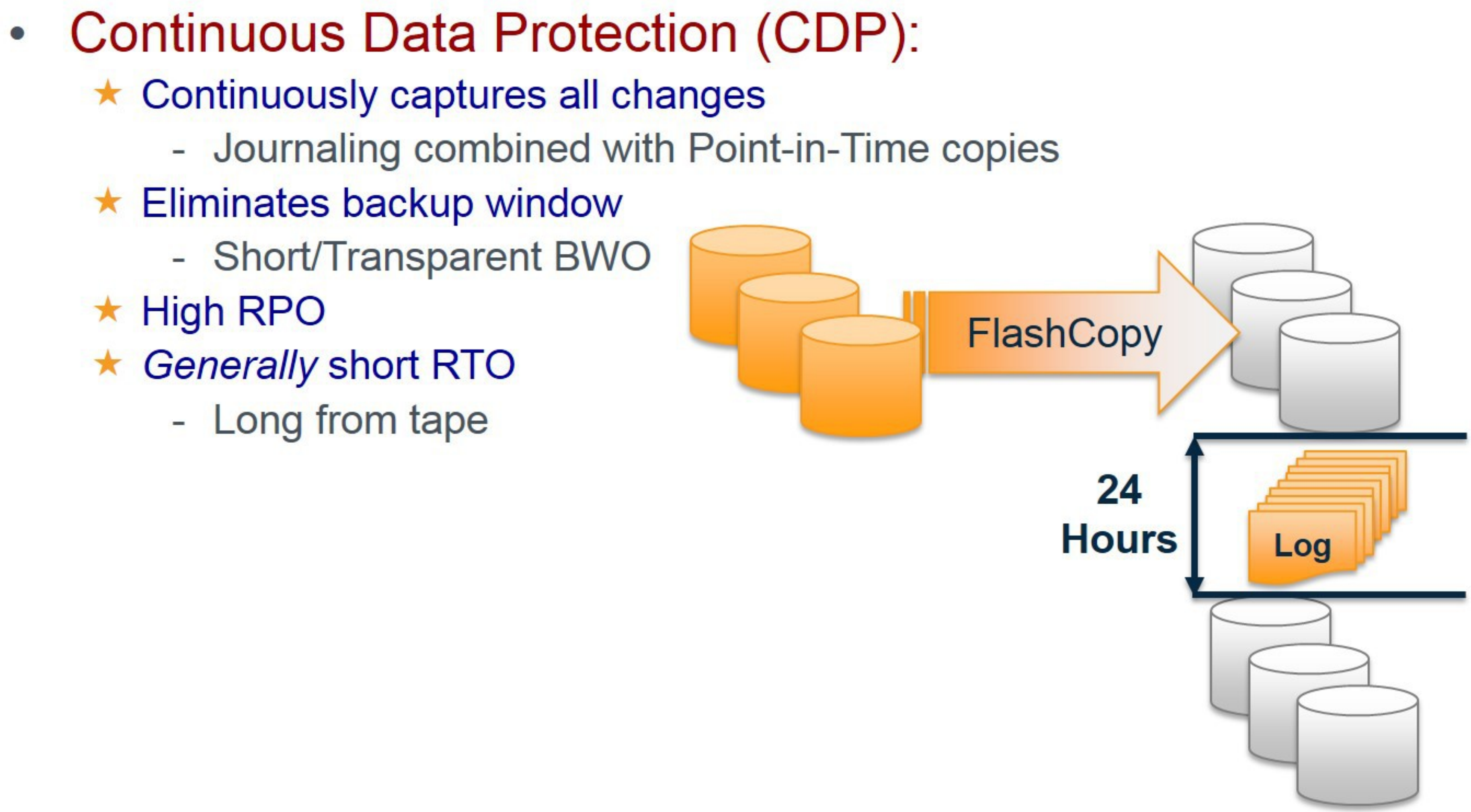
- **Cyber Resilience**
  - The increasing sophistication and volume of cyber threats and their ability to disrupt operations or corrupt data can affect the business resilience of financial institutions and Technology Service Providers. (TSPs)
  - Financial institutions, and their TSPs, need to incorporate the potential impact of a cyber event into their BCP process and ensure appropriate resilience capabilities
- **Risks**
  - Malware, Insider Threats, **Data or Systems Destruction and Corruption**, Communications Infrastructure Disruption, Simultaneous Attack on Financial Institutions and TSPs
- **Strategic Considerations – Cyber Resilience**
  - Data backup architectures and technology that minimize the potential for data destruction and corruption
  - Data integrity controls, such as check sums
  - Independent, redundant alternative communications providers
  - Layered anti-malware strategy
  - Enhanced disaster recovery planning to include the possibility of simultaneous attacks
  - Increased awareness of potential insider threats
  - Enhanced incident response plans reflecting the current threat landscape
  - Prearranged third-party forensic and incident management services

© 2017 IBM Corporation

Overview

zCDP Common Recover Queue

- **Problem** – zCDP for DB2 lacks the throughput capability to recover large DB2 environments from tape.

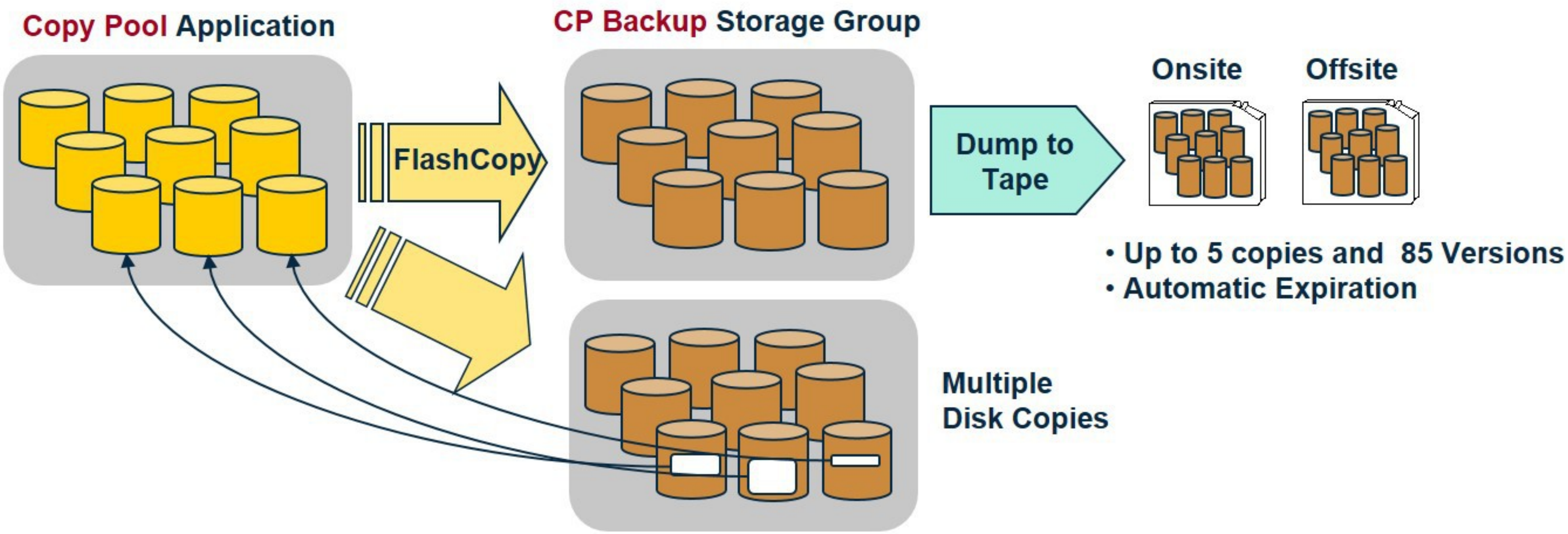


- Continuous Data Protection (CDP):
  - ★ Continuously captures all changes
    - Journaling combined with Point-in-Time copies
  - ★ Eliminates backup window
    - Short/Transparent BWO
  - ★ High RPO
  - ★ *Generally* short RTO
    - Long from tape

Overview

zCDP Common Recover Queue

- **Problem** – zCDP for DB2 lacks the throughput capability to recover large DB2 environments from tape because the requests can only be performed from a single system.



- Up to 5 copies and 85 Versions
- Automatic Expiration

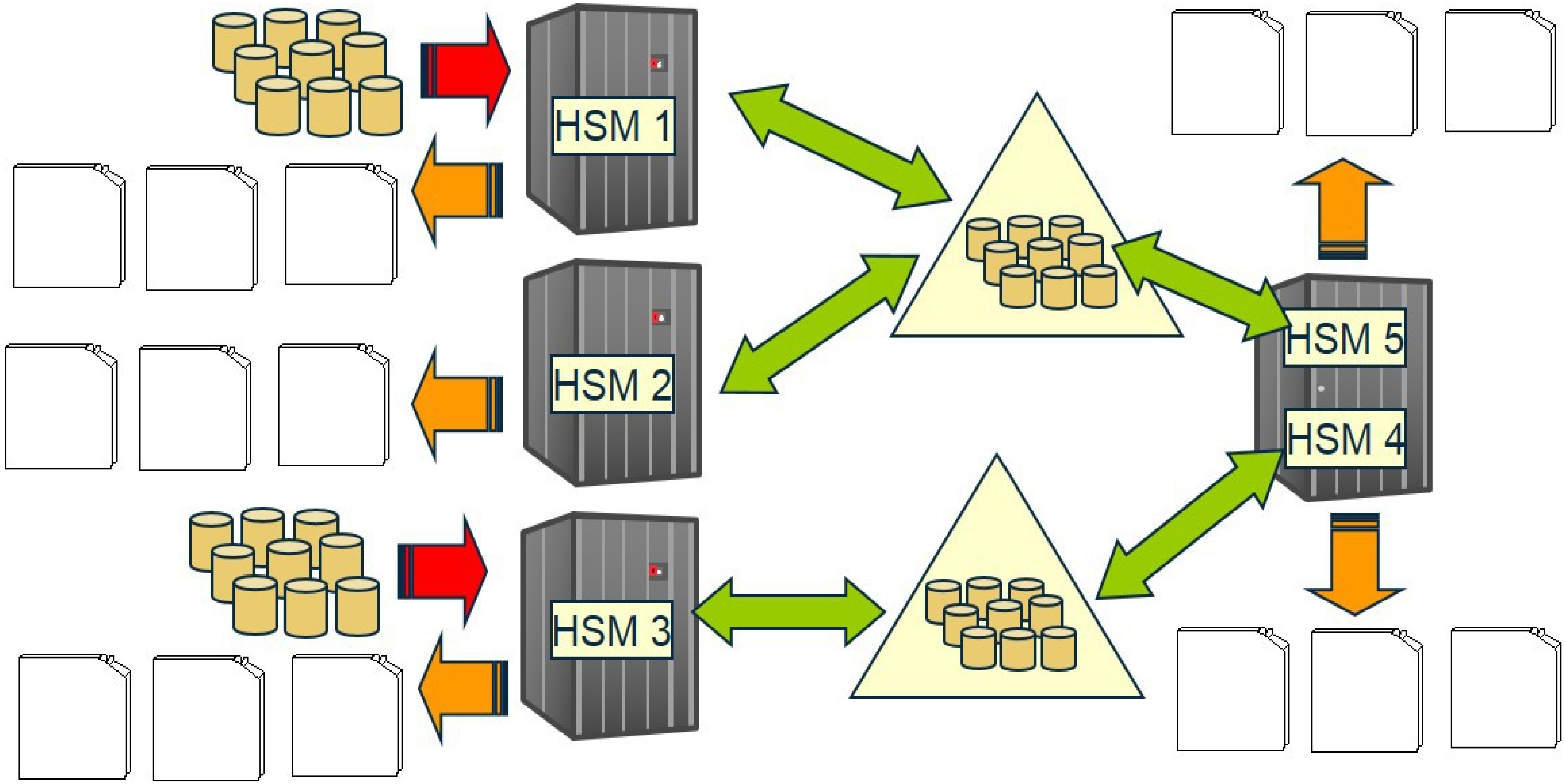
★Recovery at all levels from either disk or tape!

- Entire copy pool, individual volumes and …
- Individual data sets

Overview

zCDP Common Recover Queue

- **Problem** – DFSMShsm V2R2 Common Queue support was limited to the dump workload.

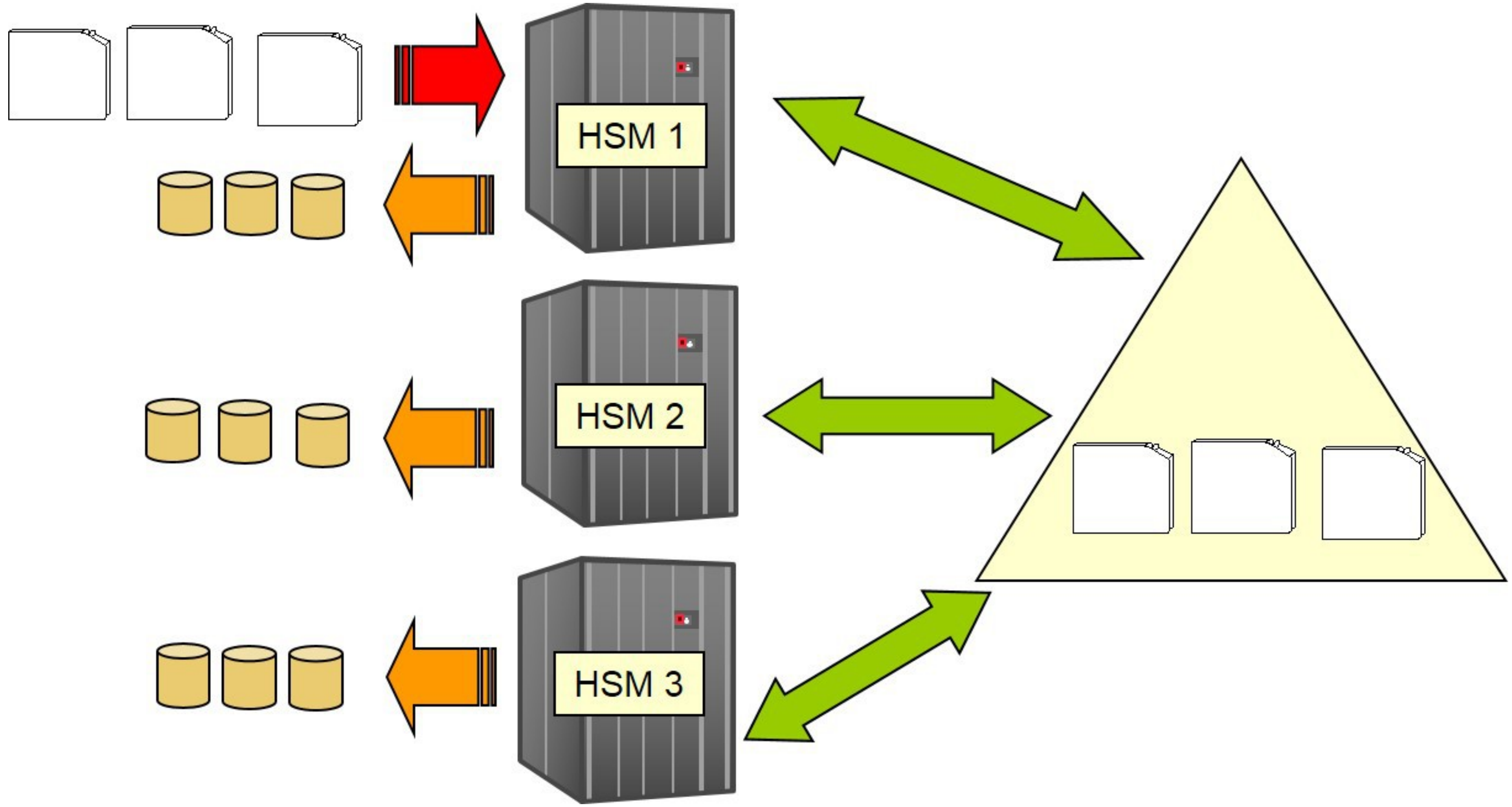


© 2017 IBM Corporation

Overview

zCDP Common Recover Queue

- **Solution** – DFSMShsm V2R2 **OA47904** Common Recover Queue



© 2017 IBM Corporation

Overview

zCDP Common Recover Queue

- **Benefits**
  - Significantly improve the overall throughput by distributing the workload across the entire sysplex
  - Flexible configurations
    - Systems can accept requests but do not have to actually process them
      - Enables systems to not require tape connectivity
      - Enables recovery workload to be kept off of critical production LPARs
    - Multiple HSM address spaces on the same LPAR can be started as needed to process requests

© 2017 IBM Corporation

Overview

DFSMSdss Space Reclamation Tool

- DS8K Extent Space Efficient (ESE) volumes are volumes that typically have no physical space allocated to them until the first write is done to the volume. Then physical space is allocated to the volume in extents from the extent pool where the volume is defined.
- **Problem Statement / Need Addressed**
  - There needs to be a way to release IBM DS8K ESE space that is no longer needed in order to avoid out of space conditions or to recover from out of space conditions after they occur.
- **Solution**
  - Full volume space release (DS8K 8.1.1) - ICKDSF INIT allows the space to be released for the entire volume. (GA July 2016; PI47180)
  - *Extent* level space release (DS8K 8.2) – DFSMSdss space release tool for z/OS will obtain volume free space extent information and allow unused space to be reclaimed. (GA Dec 2016; OA48710, OA48711, OA48709, OA48707)
- **Benefit / Value**
  - DFSMSdss space release tool provides storage administrators a command they can issue independently to release physical space extents (associated with free space tracks) from the specified non-SMS and SMS managed ESE volumes.

© 2017 IBM Corporation

Overview

DFSMSdss Space Reclamation Tool

- The new SPACEREL command determines the free space extents on the extent space efficient (ESE) volumes designated in the DDNAME, DYNAM, or STORGRP parameter and attempts to release the associated physical space to the extent pool.
  - DS8K will release space on the specified ESE volume
  - Command can be specified to fully provisioned volume (standard volume). No action will be performed. No error will be given.
  - DS8K only releases aligned full extent space.
  - Space release is allowed to a duplex metro mirror primary. Space release is not allowed on other replication types.
- The SPACEREL command performs physical volume processing.
- The volume must not be in use by any other jobs or systems during SPACEREL processing.
- Using the SPACEREL command might require RACF authorization. If your installation has defined the RACF FACILITY class profile, **STGADMIN.ADR.SPACEREL**, your user ID requires READ access to the profile.
- The SPACEREL command supports SMS and non-SMS managed ESE volumes with an indexed VTOC at the volume and storage group levels. Volumes with other VTOC formats are not supported.

© 2017 IBM Corporation

Overview

DFSORT E15/E35 Block Exit Support

- **Problem Statement / Need Addressed**
  - Updating E15/E35 exits to support the transfer of blocks of records between DFSORT and E15/E35 exits. With this new support for inserting blocks of records it will expand the functionality of the existing E15/E35 exits which will significantly reduce the number of calls of the E15/E35 exits, and will reduce the transfer of records between user's storage and DFSORT storage.
- **Solution**
  - DFSORT now supports passing blocks of records via the E15/E35 exits (GA Apr 2016; PI47000)
- **Benefit / Value**
  - Customers and applications, such as DB2 Utilities, can now reduce record processing time by passing blocks of records to the E15 and E35 exits

© 2017 IBM Corporation

Overview

DFSORT E15/E35 Block Exit Support

- **With this new E15/E35 block support allows users to:**
  - Blocks of records can be placed in any user's virtual storage (24/31/64) bit addressed.
  - E15/E35 block support can be used for DFSORT's COPY and SORT paths.
  - E15/E35 block support can be used for both FLR and VLR format of records.
  - Use of E15/E35 block support is initiated by use of the DFSORT's 64-bit Invocation Parameters List and 64-bit
  - E15/E35 exits parameters lists.
  - E15/E35 exits can have any addressing mode (AMODE 24/31/64) and can be specified in 64-bit invocation
  - Parameters List and with MODS control statement.
  - Block transfer of records can coexist with transfer of single records already existing in E15/E35 exits.

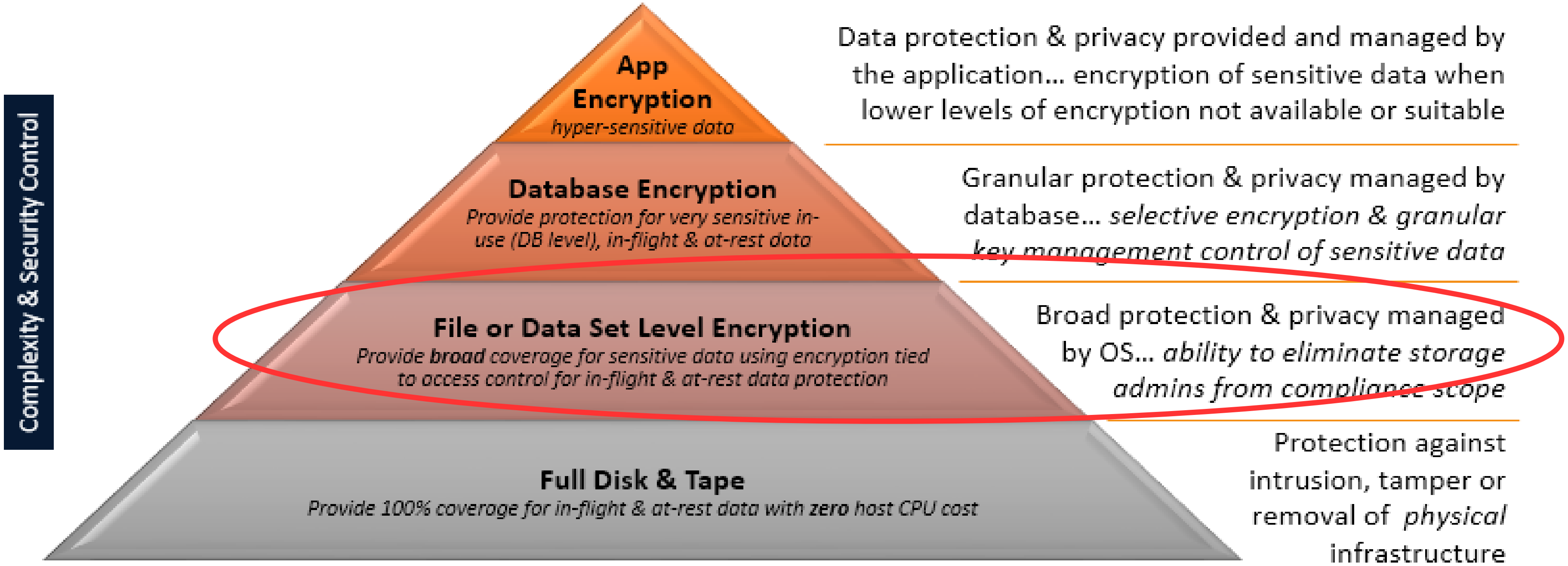
© 2017 IBM Corporation

Overview

Data Set Encryption

- **Problem Statement**
  - Various factors are driving the need for clients to adopt extensive use of encryption across their enterprises, including compliance mandates and the threat of data breaches.
  - Comprehensive data protection requires investment to deploy point solutions and/or enable encryption directly in applications. Clients need a better way to protect their data in the enterprise.

- **Solution**
  - z/OS data set encryption provides a simple, transparent and consumable approach to enable extensive encryption of data at rest for data on disk through DFSMS access methods



App Encryption
hyper-sensitive data

Data protection & privacy provided and managed by the application… encryption of sensitive data when lower levels of encryption not available or suitable

Database Encryption
Provide protection for very sensitive in-use (DB level), in-flight & at-rest data

Granular protection & privacy managed by database… *selective encryption & granular key management control of sensitive data*

File or Data Set Level Encryption
*Provide **broad** coverage for sensitive data using encryption tied to access control for in-flight & at-rest data protection*

Broad protection & privacy managed by OS… *ability to eliminate storage admins from compliance scope*

Full Disk & Tape
*Provide 100% coverage for in-flight & at-rest data with **zero** host CPU cost*

Protection against intrusion, tamper or removal of *physical* infrastructure

© 2017 IBM Corporation

Benefit / Value

Data Set Encryption

Clients who are required to protect customer data can leverage the z Systems hardware encryption for data at rest through existing policy management…*without application changes*.

- Data set level granularity
- Enabled through RACF and/or SMS policy
- No application changes required
- Supports separation of access control for data set and encryption key label

"IBM plans to deliver application transparent, policy-controlled dataset encryption in IBM z/OS®. IBM DB2® for z/OS and IBM Information Management System (IMS™) intend to exploit z/OS dataset encryption."

Statement of Direction in the Announcement letter IBM United States Software Announcement 216-392, dated October 4, 2016

https://www.ibm.com/common/ssi/rep_ca/2/897/ENUS216-392/ENUS216-392.PDF

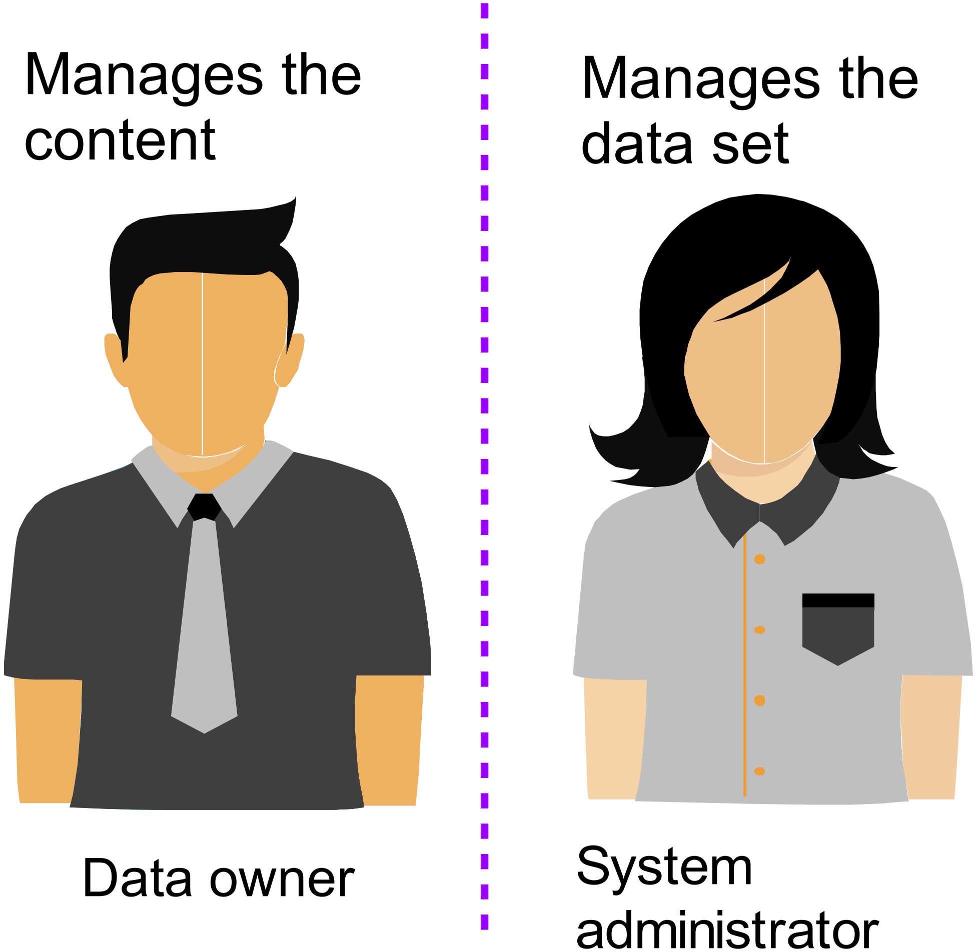
© 2017 IBM Corporation

Benefit / Value

Data Set Encryption

Helps with Segregation of Duties

- Data owners that *must* access content will need authority access to the data set as well as access to the the encryption key label
- Storage administrators who *manage only* the data sets need access to the data set but not access to the key label (thus protecting access to the content)
- Different keys can be used to protect different data sets – ideal for multiple tenants or data set specific policies.
- Prevent administrators from accessing the content
- Many utilities can process data preserving encrypted form
  - COPY, DUMP and RESTORE
  - Migrate/Recall, Backup/Recover, Dump/Data Set Restore
  - PPRC, XRC, FlashCopy®, Concurrent Copy, etc.



Manages the content

Manages the data set

Data owner

System administrator

© 2017 IBM Corporation

Usage & Invocation

Data Set Encryption

- DFSMS provides the ability to encrypt the following types of data sets
  - Sequential extended format data sets
    - Accessed through BSAM or QSAM
  - VSAM extended format data sets (KSDS, ESDS, RRDS, VRRDS, LDS)
    - Accessed through base VSAM or VSAM/RLS

    Note: Encrypted data sets must be SMS-managed extended format. They can be compressed or non-compressed format.
- To create an encrypted data set, a key label must be supplied on new data set allocation
  - Key label identifies a protected data key in the ICSF key repository (CKDS)
    - Encryption type supported: AES-256 bit data key (XTS, protected key).

© 2017 IBM Corporation

Usage & Invocation (Environment)

Data Set Encryption

- Before implementing z/OS data set encryption
  - Ensure that all systems in sysplex at minimum level
    - z/OS V2.3 or z/OS V2.2 + APARS
      - PTFs will be required on down level systems (V2.1) to support encrypted data sets.
      - A user cannot create a new encrypted data set on z/OS V2.1, but will be able to read from/write to an encrypted dataset created using z/OS V2.2 or V2.3
    - Refer to “Software / Hardware Dependencies” chart
  - Required maintenance is applied across all systems in the sysplex
    - Refer to “Installation” chart

Note: If your program must determine if the data set encryption function is installed on the system, a new flag is defined in the DFA (as mapped by IHADFA).

© 2017 IBM Corporation

Usage & Invocation (Setup)

Data Set Encryption

- Steps to implement data set encryption
  - Enable data set encryption
    - To allow the system to create encrypted data sets, the user must have at least READ authority to the following resource in the FACILITY class
      - **STGADMIN.SMS.ALLOW.DATASET.ENCRYPT**
  - Update ICSF segment of the covering profile (see Appendix for details)
  - Specify a key label through any of the following methods (see Appendix for details)
    - RACF Data set profile
    - JCL, Dynamic Allocation, TSO
    - SMS Data Class
    - IDCAMS DEFINE

  - Permit data owners access to the key label

© 2017 IBM Corporation

Usage & Invocation (Restrictions)

Data Set Encryption

- System data sets (such as Catalogs, SHCDS, HSM data sets) must not be encrypted, unless otherwise specified.
- Encrypted data sets only supported on 3390 device types
- Sequential (non-compressed) extended format data sets with a block size of less than 16 bytes cannot be encrypted
- DFSMSdss REBLOCK keyword is ignored on COPY and RESTORE functions.
- DFSMSdss ADRREBLK installation exit will not be called for encrypted data sets.
- Data sets used during IPL must not be encrypted.

Note: The following types of data sets cannot be extended format, therefore do not support data set encryption

- Temporary data sets
- SORTWK data sets

Usage & Invocation (Data Owners Role)

Data Set Encryption

- For data owners that must access data in encrypted data sets
  - They must have SAF authority to the data set and SAF authority to the key label (see Appendix for sample SAF setup for key labels)
  - With the proper authority, applications can transparently access the data in the clear without application changes:
    - Data is encrypted when written to disk
    - Data is decrypted when read from disk

© 2017 IBM Corporation

Usage & Invocation (Storage Admins Role)

Data Set Encryption

- For data managers (such as storage admins) that manage data sets (and not the data)
- They must have SAF authority to the data set but do not require SAF authority to the key label
  - The following types of functions maintain data in the encrypted form
    - During DFSMSdss functions, COPY, DUMP and RESTORE
    - During DFSMShsm functions, Migrate/Recall,Backup/Recover, Abackup/Arecover, Dump/Data Set Restore, FRBACKUP/FRRECOV DSNAME
    - During track based copy (PPRC, XRC, FlashCopy, Concurrent Copy, etc) operations

© 2017 IBM Corporation

Usage & Invocation (Identifying Encrypted Data Sets) Data Set Encryption

- Volume
  - IEHLIST LISTVTOC
- Catalog
  - LISTCAT
  - CSI (catalog search interface)
- SMS policy
  - ISMF Data set list panel
- BSAM/QSAM macro
  - ISITMGD
  -
- SMF Type 14/15 (BSAM/QSAM) and SMF Type 62 (VSAM) records
- DCOLLECT Record Types 'DC', 'D', 'M', and 'B'

See Appendix for samples

© 2017 IBM Corporation

Usage & Invocation (Converting to Encrypted Format) Data Set Encryption

Existing data sets can be copied to a new target data set allocated with encryption

- No utility available to perform a conversion without decrypting data from source and re-encrypting data onto target
- Standard utilities can be used to perform the copy, for example
  - ISPF 3.3 Copy data set
  - IDCAMS REPRO
  - IEBGENER

- **See Appendix for samples**

© 2017 IBM Corporation

Software / Hardware Dependencies

Data Set Encryption

- Software Dependencies
  - ICSF
    - HCR77C0, HCR77C1 or HCR77A0 through HCR77B1 with APAR OA50450
  - RACF based on z/OS V2R2

- Hardware Dependencies and feature codes
  - IBM zEnterprise® 196 / IBM zEnterprise (z196, z114) or later, CEX3 FC0864
  - IBM zEnterprise EC12 /IBM zEnterprise BC12 (zEC12, zBC12) require CEX3 FC0864 or CEX4 FC086
  - IBM z13, CEX5 FC0890
  - CPACF FC3863

© 2017 IBM Corporation

Migration Considerations

Data Set Encryption

- To support migration / coexistence / fallback, an enablement action is required to allow any data set encryption to occur.
  - Data set encryption is disabled by default

- To allow the system to create encrypted data sets, the user must have at least read authority to the following resource in the FACILITY class:
  - **STGADMIN.SMS.ALLOW.DATASET.ENCRYPT**
    - The system checks the RACF authority to this resource when the data set is first allocated (created).
    - One exception is when the key label is specified in the DFP segment in the RACF data set profile. In this case, the system does not require the user to have authority to this resource

Note: For years, IBM has recommended, and continues to recommend, that STGADMIN.* be defined with UACC(NONE)

© 2017 IBM Corporation

Coexistence Considerations

Data Set Encryption

- Coexistence PTFs will be required on downlevel systems (V2.1) to support encrypted data sets.
- Coexistence includes the ability to access existing encrypted data sets. That is, a user will not be able to create a new encrypted data set on a downlevel release (z/OS V2.1), but will be able to read from/write to an existing encrypted dataset which had been created on a z/OS V2.2 or V2.3 release.
- Although a user may not be able to create a new encrypted data set on a down level release, DFSMSdss will still be able to restore as an encrypted data set on a lower release. DFSMShsm will be able to recall and recover an encrypted data set on a lower release.
- ARECOVER ALLOCATE listed data sets that were backed up as an encrypted data set on zOS V2R2 or higher that are being recovered on an z/OS V2R1 system will be failed with a new error message, ADR6190E.

© 2017 IBM Corporation

Installation

Data Set Encryption

- This support is included in z/OS V2.3.
- This support is available in z/OS V2.2 with the following APARs:
  - DFSMS OA50569
  - RACF OA50512
  - ICSF OA50450
  - BCP SJF OA51076

© 2017 IBM Corporation

Appendix (Publications)

Data Set Encryption

- *z/OS DFSMS Introduction*
- *z/OS DFSMS Using the New Functions*
- *z/OS DFSMSdfp Storage Administration*
- *z/OS DFSMS Managing Catalogs*
- *z/OS DFSMS Access Method Services Command Reference*
- *z/OS DFSMS Using Data Sets*
- *z/OS DFSMS Macro Instructions for Data Sets*
- *z/OS DFSMSdfp Advanced Services*
- *z/OS DFSMSdfp Diagnosis*
- *z/OS DFSMSdss Storage Administration Reference*

Appendix (Publications)

Data Set Encryption

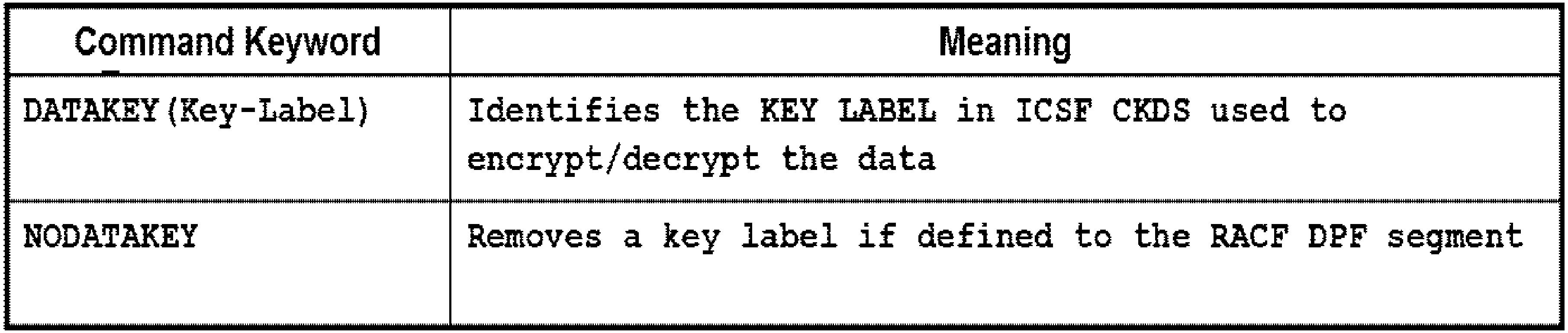
- *z/OS DFSMShsm Data Areas*
- *z/OS DFSMS Installation Exits*
- *z/OS MVS Initialization and Tuning Reference*
- *z/OS MVS System Commands*
- *z/OS MVS JCL Reference*
- *z/OS MVS System Management Facility (SMF)*
- *z/OS MVS System Messages Volume 1, 2, 6, 7 and 8*
- *z/OS MVS Programming: Authorized Assembler Services Guide*
- *z/OS Summary of Message and Interface Changes*
- *z/OS Migration*

© 2017 IBM Corporation

Appendix (Key Label supplied via RACF)

Data Set Encryption

- To specify key label via DFP segment in RACF data set profile
  - New keyword: DATAKEY



Command Keyword	Meaning
DATAKEY(Key-Label)	Identifies the KEY LABEL in ICSF CKDS used to encrypt/decrypt the data
NODATAKEY	Removes a key label if defined to the RACF DPF segment

Example:

```
ALTDSD 'PROJECTA.DATA.*' UACC(NONE) DFP(RESOWNER(iduser1))
DATAKEY(Key-Label)
```

Note: To use key label in RACF DS profile, ensure ACSDEFAULTS(YES) in SYS1.PARMLIB(IGDSMSxx).

© 2017 IBM Corporation

Appendix (Key Label supplied via JCL)

Data Set Encryption

- To specify key label via JCL, Dynamic Allocation and TSO Allocate
  - New JCL keyword: DSKEYLBL=key-label
    - DSKEYLBL is effective only if the new data set is on DASD. It is ignored for device types other than DASD, including DUMMY.

Example:

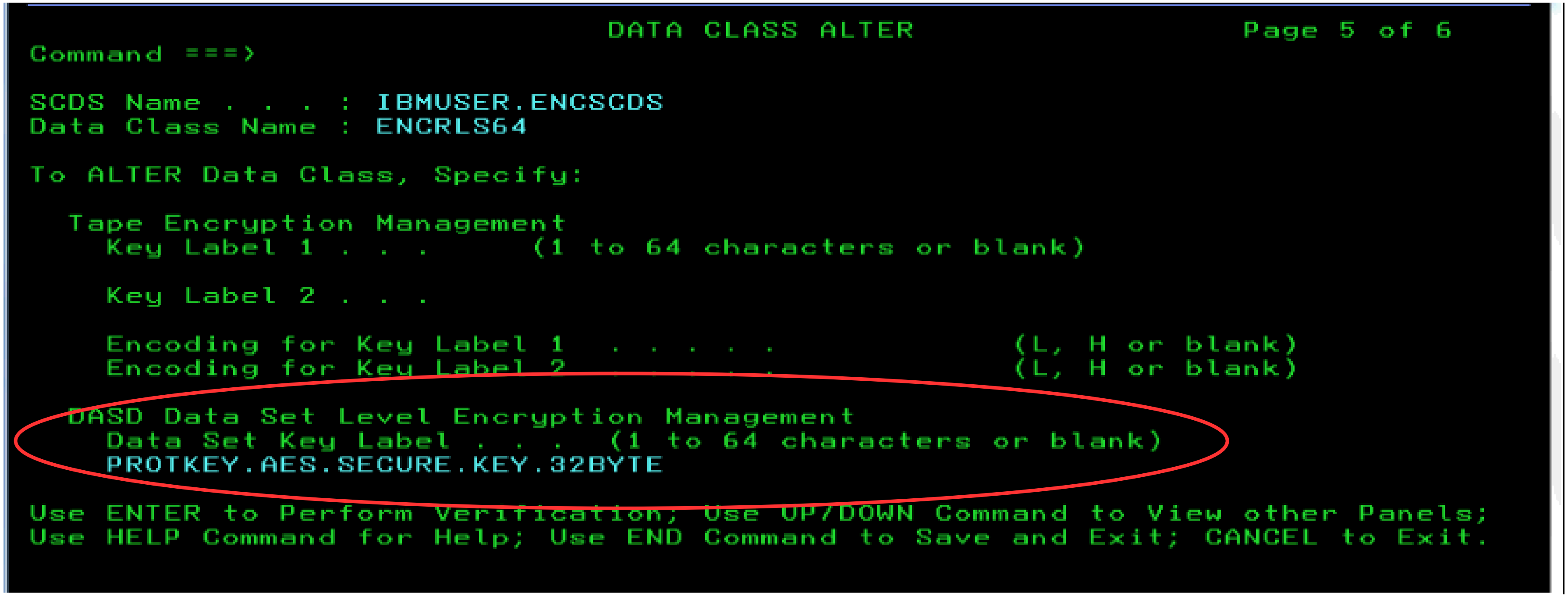
```
//DD1   DD   DSN=DSN1,DISP=(NEW,CATLG),DATACLAS=DSN1DATA,MGMTCLAS=DSN1MGMT,
//        STORCLAS=DSN1STOR,DSKEYLBL=’LABEL.FOR.DSN1’
```

© 2017 IBM Corporation

Appendix (Key Label supplied via SMS data class) Data Set Encryption

- To specify key label via SMS Data Class
  - New field: Data Set Key Label

Example:



```
                              DATA CLASS ALTER                          Page 5 of 6
Command ===>

SCDS Name . . . : IBMUSER.ENCSCDS
Data Class Name : ENCRLS64

To ALTER Data Class, Specify:

  Tape Encryption Management
    Key Label 1 . . .          (1 to 64 characters or blank)

    Key Label 2 . . .

    Encoding for Key Label 1  . . . . . .               (L, H or blank)
    Encoding for Key Label 2  . . . . . .               (L, H or blank)

  DASD Data Set Level Encryption Management
    Data Set Key Label . . .   (1 to 64 characters or blank)
    PROTKEY.AES.SECURE.KEY.32BYTE

Use ENTER to Perform Verification; Use UP/DOWN Command to View other Panels;
Use HELP Command for Help; Use END Command to Save and Exit; CANCEL to Exit.
```

© 2017 IBM Corporation

Appendix (Key Label supplied via IDCAMS)

Data Set Encryption

- To specify key label via AMS DEFINE for CLUSTER
  - New parameter: KEYLABEL=key-label
    - KEYLABEL only allowed on DEFINE CLUSTER.
    - All alternate indexes will use the same key label associated with the CLUSTER.

Example:

–

```
DEFINE CLUSTER -
 (NAME(DSN1.EXAMPLE.ESDS1) -
RECORDS(100 500) -
RECORDSIZE(250 250) -
KEYLABEL(LABEL.FOR.DSN1) -
NONINDEXED )
```

Appendix (ICSF Setup)

Data Set Encryption

- Prepare for accessing encrypted data sets by setting up access to the ICSF CKDS Key provisioning service invoked by the access methods
  - Security admin updates the following in the ICSF segment of the covering profile
    - SYMCPACFWRAP(YES)
    - SYMCPACFRET (YES)
  - Security admin sets up access to the ICSF CKDS Key Record Read2 (CSNBKRR2) service invoked by the access methods. For example,
    - Define the RACF profile such that no one has access to the ICSF services

      ```
      RDEFINE CSFSERV  * UACC(NONE)
      ```
    - Allow everyone to have access to the callable service CSNBKRR2

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

© 2017 IBM Corporation

Appendix (SAF setup)

Data Set Encryption

- Example of setting up SAF resources for the key label
  - Security Admin sets up profiles in the CSFKEYS general resource class based on installation requirements. The following are examples.
    - Define the RACF CSFKEYS profile such that no one has access to any key label

```
RDEFINE CSFKEYS * UACC(NONE)
```

    - To allow key label to be used by JOHN when accessed by any application

```
PERMIT key-label CLASS(CSFKEYS) ID(JOHN) ACCESS(READ)
```

    - To allow key label to be used by MIKE only when accessed by DFSMS

```
PERMIT key-label CLASS(CSFKEYS) ID(MIKE) ACCESS(READ)
WHEN(CRITERIA(SMS(DSENCRYPTION)))
```

    - To allow key label to be used by any user only when accessed by DFSMS

```
PERMIT key-label CLASS(CSFKEYS) ID(*) ACCESS(READ)
WHEN(CRITERIA(SMS(DSENCRYPTION)))
```

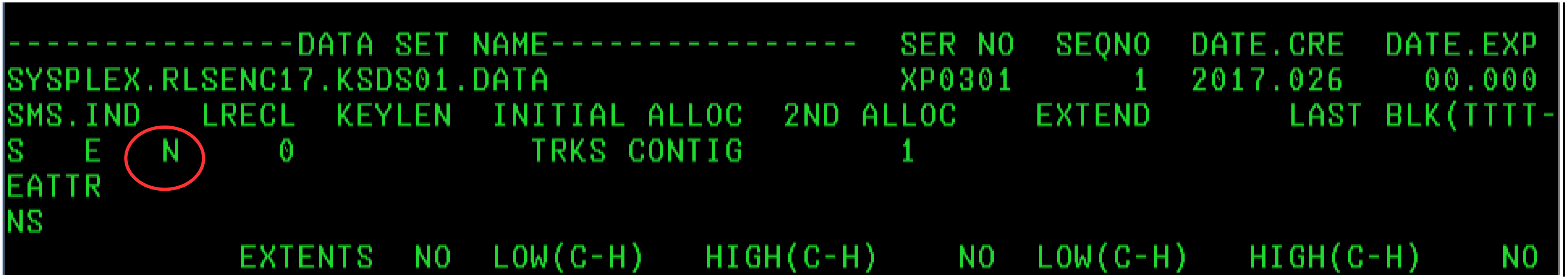
© 2017 IBM Corporation

Appendix (Identifying Encryption by Volume)

Data Set Encryption

- LISTVTOC – displays volume level information
  - Data set info includes new encryption attribute '**N**' under field SMS.IND
  -

Example



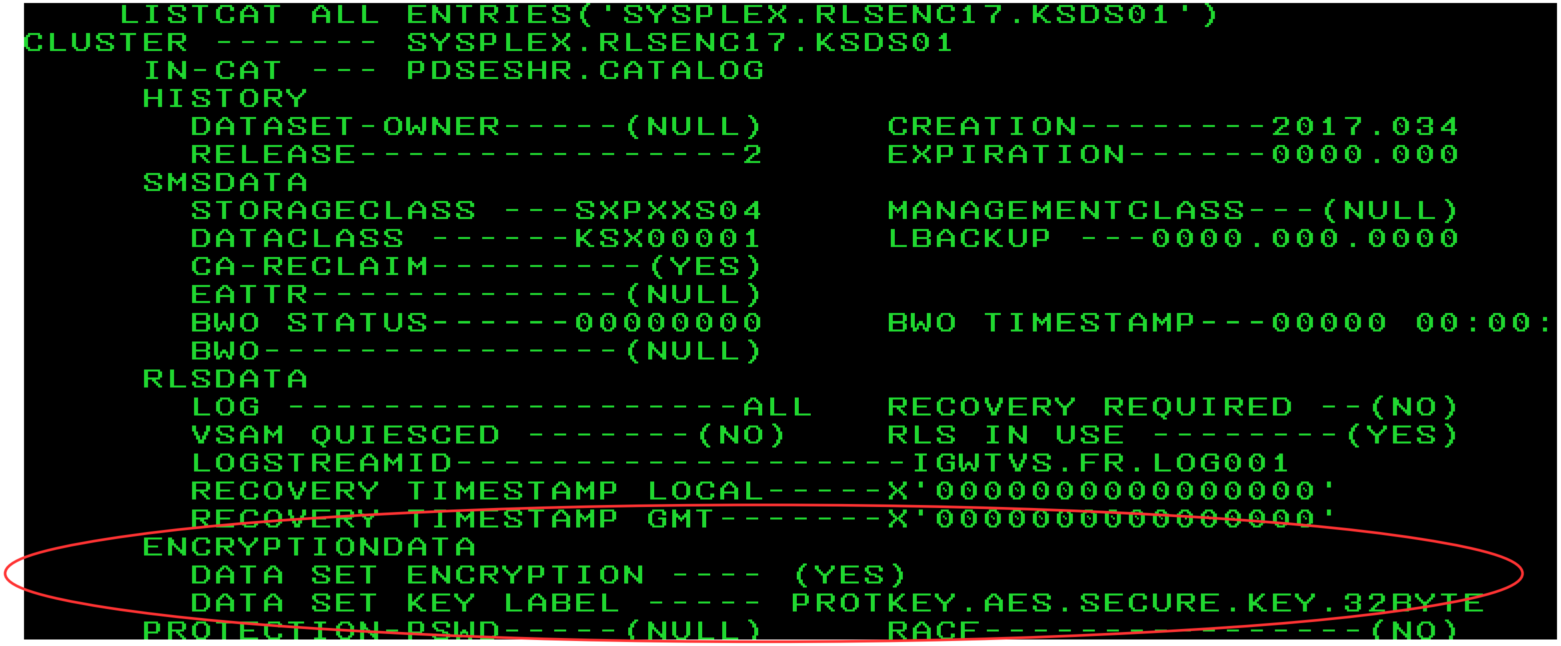
```
---------------DATA SET NAME----------------  SER NO  SEQNO  DATE.CRE  DATE.EXP
SYSPLEX.RLSENC17.KSDS01.DATA                  XP0301      1  2017.026    00.000
SMS.IND   LRECL  KEYLEN  INITIAL ALLOC  2ND ALLOC    EXTEND       LAST BLK(TTTT-
S   E   N     0            TRKS CONTIG        1
EATTR
NS
            EXTENTS  NO  LOW(C-H)   HIGH(C-H)    NO  LOW(C-H)   HIGH(C-H)    NO
```

Appendix (Identifying Encryption by Catalog)

Data Set Encryption

- LISTCAT – displays catalog level information
  - Data set info displays key label and Encryption flag

Example



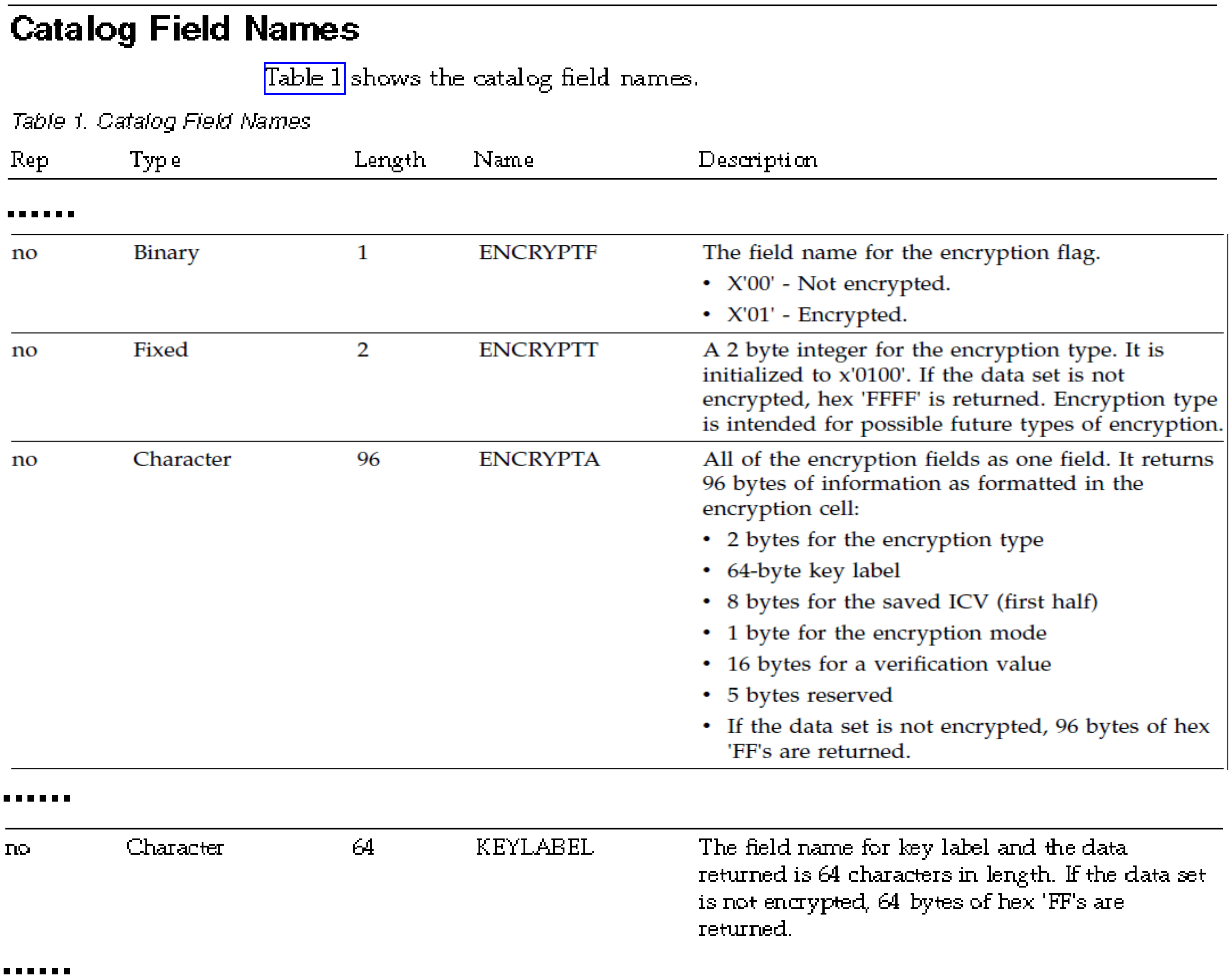
```
    LISTCAT ALL ENTRIES('SYSPLEX.RLSENC17.KSDS01')
CLUSTER ------- SYSPLEX.RLSENC17.KSDS01
     IN-CAT --- PDSESHR.CATALOG
     HISTORY
       DATASET-OWNER-----(NULL)     CREATION--------2017.034
       RELEASE----------------2     EXPIRATION------0000.000
     SMSDATA
       STORAGECLASS ---SXPXXS04     MANAGEMENTCLASS---(NULL)
       DATACLASS ------KSX00001     LBACKUP ---0000.000.0000
       CA-RECLAIM---------(YES)
       EATTR-------------(NULL)
       BWO STATUS------00000000     BWO TIMESTAMP---00000 00:00:
       BWO---------------(NULL)
     RLSDATA
       LOG -------------------ALL   RECOVERY REQUIRED --(NO)
       VSAM QUIESCED -------(NO)    RLS IN USE --------(YES)
       LOGSTREAMID-------------------IGWTVS.FR.LOG001
       RECOVERY TIMESTAMP LOCAL-----X'0000000000000000'
       RECOVERY TIMESTAMP GMT-------X'0000000000000000'
     ENCRYPTIONDATA
       DATA SET ENCRYPTION ---- (YES)
       DATA SET KEY LABEL ----- PROTKEY.AES.SECURE.KEY.32BYTE
     PROTECTION-PSWD-----(NULL)     RACF----------------(NO)
```

© 2017 IBM Corporation

Appendix (Identifying Encryption by Catalog)

Data Set Encryption

- CSI (catalog search interface)
  - Key label, Encryption flag/type, Encryption cell



Catalog Field Names

Table 1 shows the catalog field names.

Table 1. Catalog Field Names

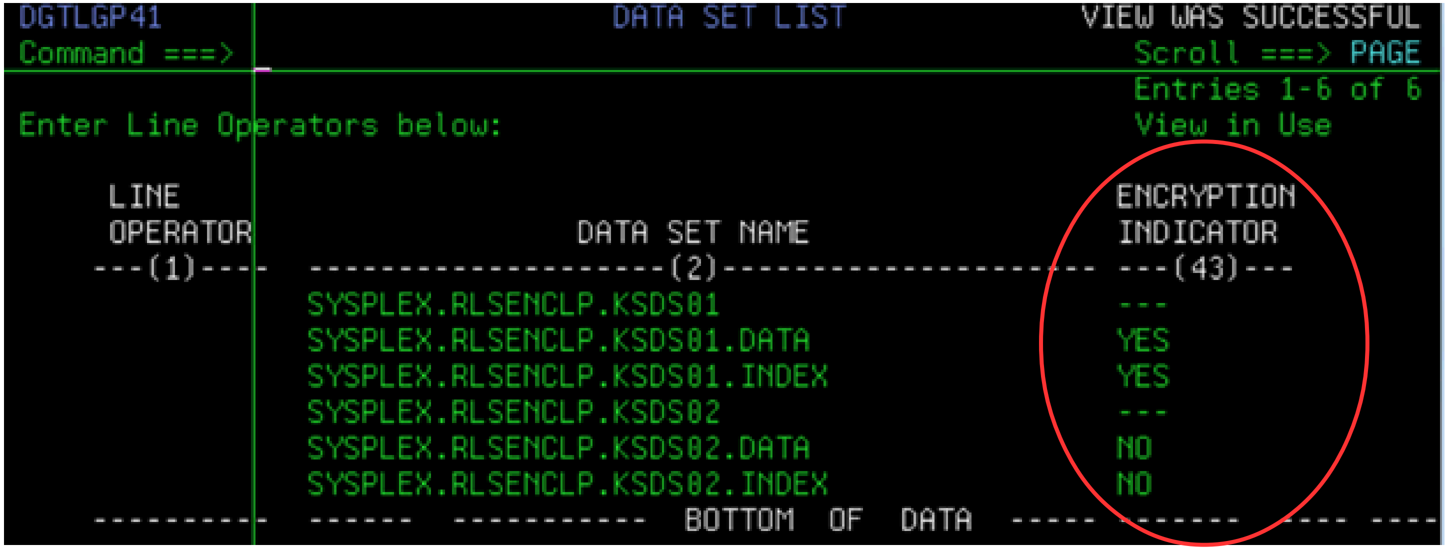
Rep	Type	Length	Name	Description
......				
no	Binary	1	ENCRYPTF	The field name for the encryption flag. • X'00' - Not encrypted. • X'01' - Encrypted.
no	Fixed	2	ENCRYPTT	A 2 byte integer for the encryption type. It is initialized to x'0100'. If the data set is not encrypted, hex 'FFFF' is returned. Encryption type is intended for possible future types of encryption.
no	Character	96	ENCRYPTA	All of the encryption fields as one field. It returns 96 bytes of information as formatted in the encryption cell: • 2 bytes for the encryption type • 64-byte key label • 8 bytes for the saved ICV (first half) • 1 byte for the encryption mode • 16 bytes for a verification value • 5 bytes reserved • If the data set is not encrypted, 96 bytes of hex 'FF's are returned.
......				
no	Character	64	KEYLABEL	The field name for key label and the data returned is 64 characters in length. If the data set is not encrypted, 64 bytes of hex 'FF's are returned.
......				

© 2017 IBM Corporation

Appendix (Identifying Encryption by SMS, BSAM / QSAM Macro)

Data Set Encryption

- SMS policy
  - ISMF Data set list panel
    - Encryption flag/type



```
DGTLGP41                      DATA SET LIST                VIEW WAS SUCCESSFUL
Command ===>                                                  Scroll ===> PAGE
                                                               Entries 1-6 of 6
Enter Line Operators below:                                    View in Use

     LINE                                                     ENCRYPTION
     OPERATOR                  DATA SET NAME                  INDICATOR
    ---(1)----  --------------------(2)---------------------  ---(43)---
                SYSPLEX.RLSENCLP.KSDS01                        ---
                SYSPLEX.RLSENCLP.KSDS01.DATA                   YES
                SYSPLEX.RLSENCLP.KSDS01.INDEX                  YES
                SYSPLEX.RLSENCLP.KSDS02                        ---
                SYSPLEX.RLSENCLP.KSDS02.DATA                   NO
                SYSPLEX.RLSENCLP.KSDS02.INDEX                  NO
    ----------  ------  -----------  BOTTOM  OF  DATA  -----  ------  ----  ----
```

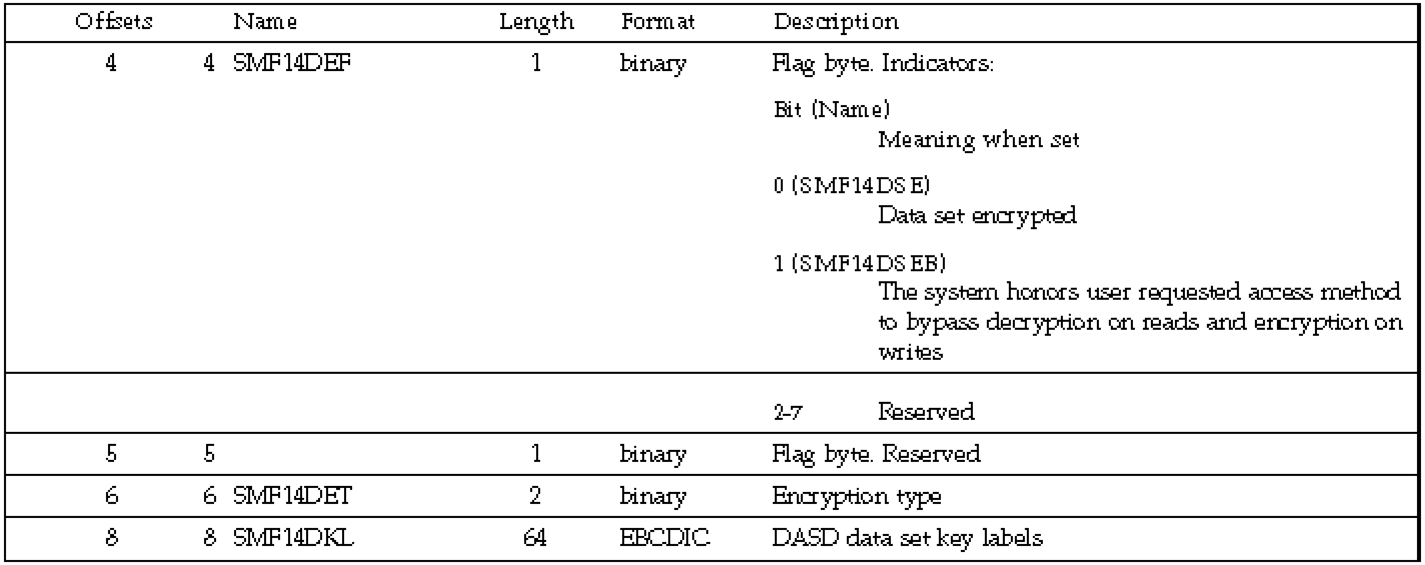
- BSAM/QSAM macro
  - ISITMGD – returns attributes related to sequential data sets
    - Encryption flag **ISMENCRP** ON if the DASD data set is encrypted by the access methods.

© 2017 IBM Corporation

Appendix (Identifying Encryption by SMF)

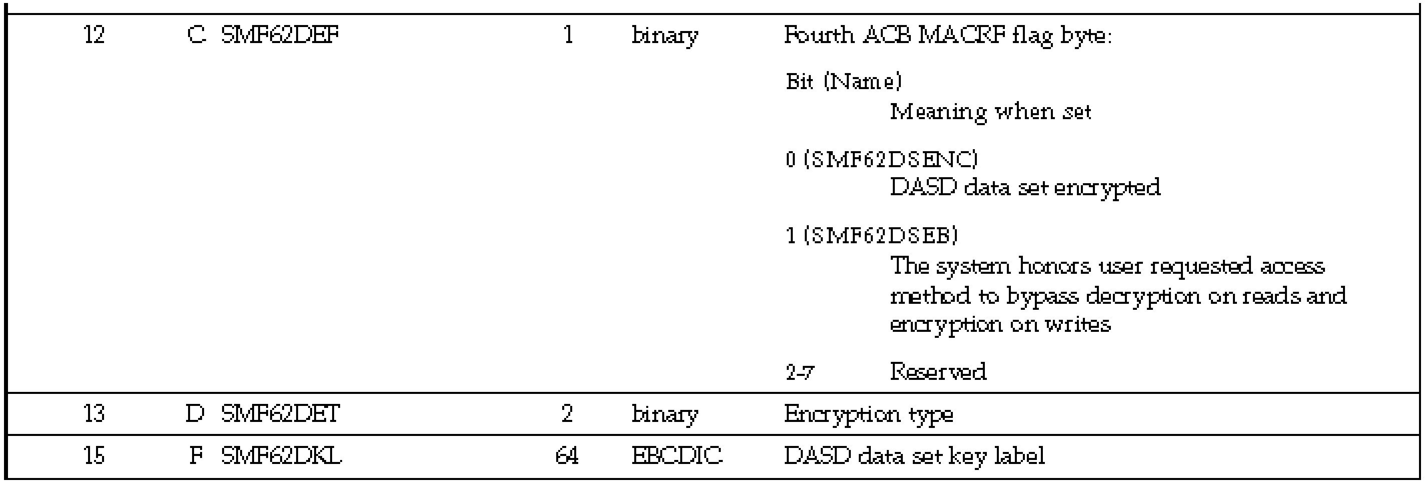
Data Set Encryption

- SMF Type 14/15 (New DASD Data Set Encryption Information Section



Offsets		Name	Length	Format	Description
4	4	SMF14DEF	1	binary	Flag byte. Indicators: Bit (Name) Meaning when set 0 (SMF14DSE) Data set encrypted 1 (SMF14DSEB) The system honors user requested access method to bypass decryption on reads and encryption on writes
					2-7 Reserved
5	5		1	binary	Flag byte. Reserved
6	6	SMF14DET	2	binary	Encryption type
8	8	SMF14DKL	64	EBCDIC	DASD data set key labels

- SMF Type 62 (VSAM data sets)

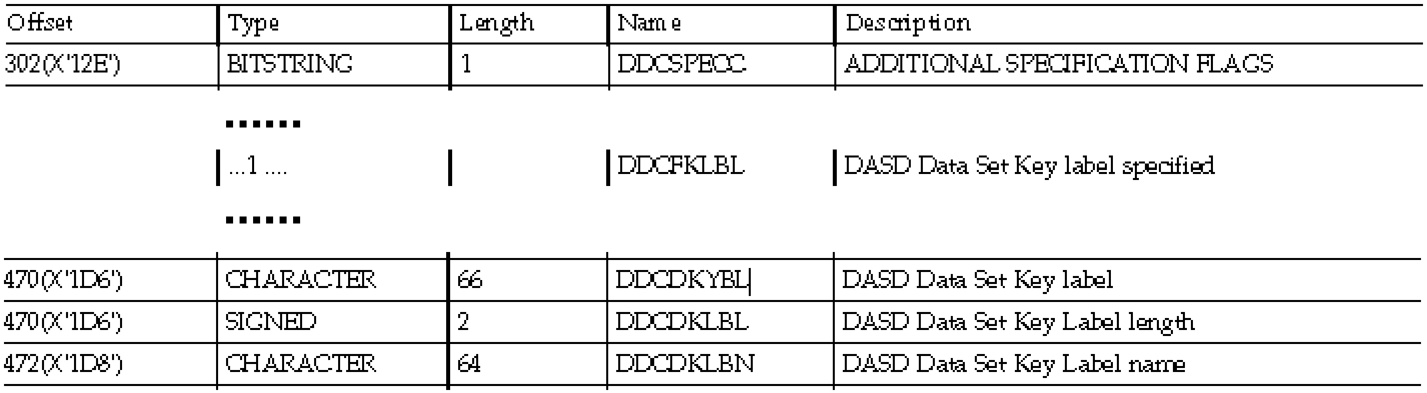


12	C	SMF62DEF	1	binary	Fourth ACB MACRF flag byte: Bit (Name) Meaning when set 0 (SMF62DSENC) DASD data set encrypted 1 (SMF62DSEB) The system honors user requested access method to bypass decryption on reads and encryption on writes 2-7 Reserved
13	D	SMF62DET	2	binary	Encryption type
15	F	SMF62DKL	64	EBCDIC	DASD data set key label

© 2017 IBM Corporation

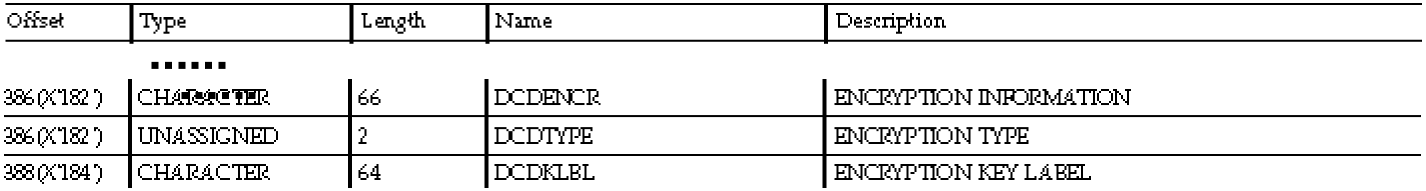
Appendix (Identifying Encryption by DCOLLECT) Data Set Encryption

- Data class definition record Type 'DC': New key label field



Offset	Type	Length	Name	Description
302(X'12E')	BITSTRING	1	DDCSPECC	ADDITIONAL SPECIFICATION FLAGS
	......			
	...1		DDCFKLBL	DASD Data Set Key label specified
	......			
470(X'1D6')	CHARACTER	66	DDCDKYBL	DASD Data Set Key label
470(X'1D6')	SIGNED	2	DDCDKLBL	DASD Data Set Key Label length
472(X'1D8')	CHARACTER	64	DDCDKLBN	DASD Data Set Key Label name

- Data set info record Type 'D': New key label field



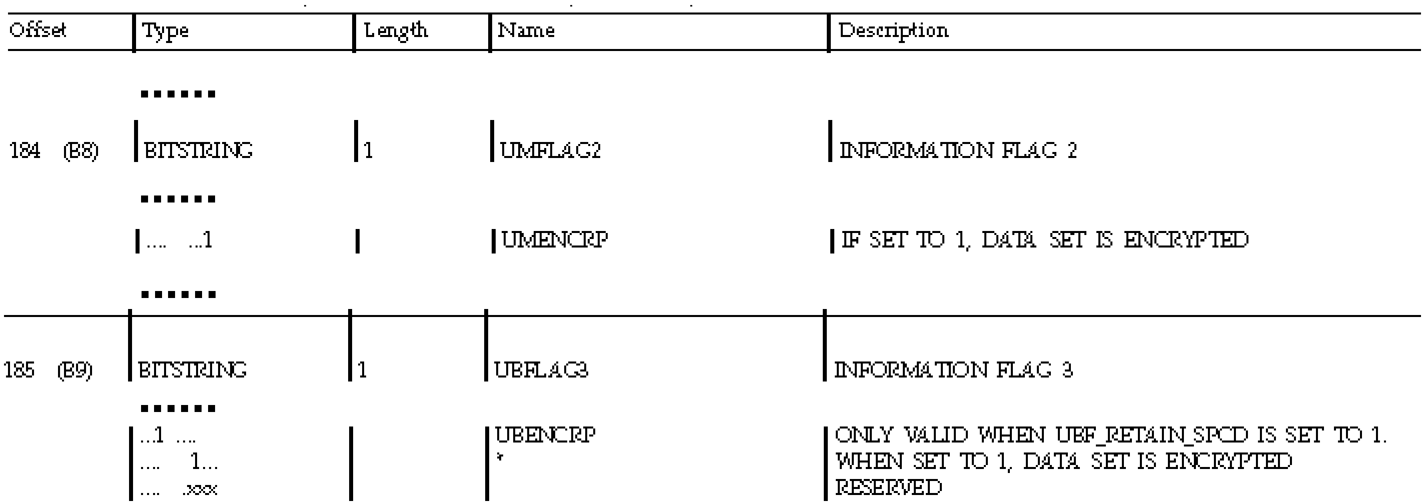
Offset	Type	Length	Name	Description
	......			
386(X'182')	CHARACTER	66	DCDENCR	ENCRYPTION INFORMATION
386(X'182')	UNASSIGNED	2	DCDTYPE	ENCRYPTION TYPE
388(X'184')	CHARACTER	64	DCDKLBL	ENCRYPTION KEY LABEL

© 2017 IBM Corporation

Appendix (Identifying Encryption by DCOLLECT)

Data Set Encryption

- HSM migration/backup record: Encryption flag



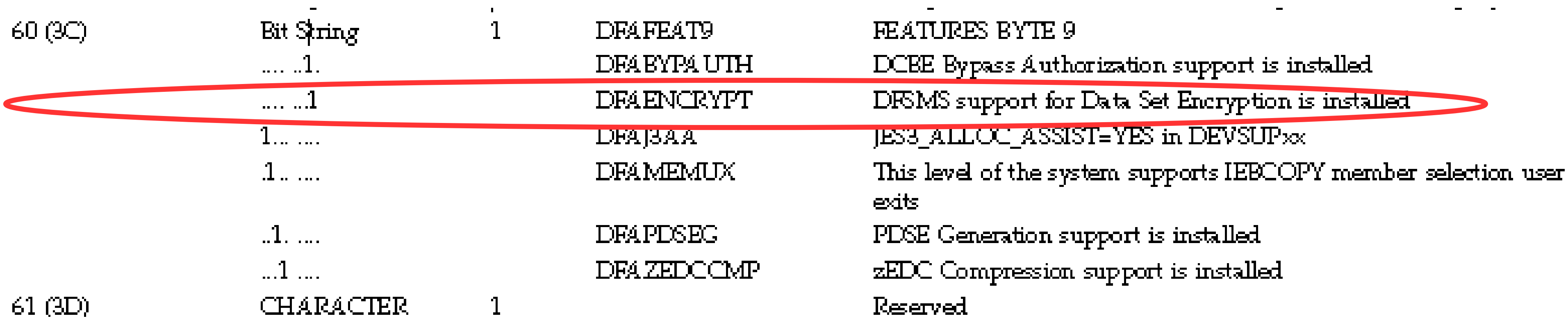
Offset	Type	Length	Name	Description
	▪▪▪▪▪▪			
184 (B8)	BITSTRING	1	UMFLAG2	INFORMATION FLAG 2
	▪▪▪▪▪▪			
	1		UMENCRP	IF SET TO 1, DATA SET IS ENCRYPTED
	▪▪▪▪▪▪			
185 (B9)	BITSTRING	1	UBFLAG3	INFORMATION FLAG 3
	▪▪▪▪▪▪			
	...1 .... 1... xxx		UBENCRP *	ONLY VALID WHEN UBF_RETAIN_SPCD IS SET TO 1. WHEN SET TO 1, DATA SET IS ENCRYPTED RESERVED

© 2017 IBM Corporation

Appendix (Determine Support)

Data Set Encryption

If a program must determine if data set encryption is supported, test for the new flag “DFAENCRYPT” (x'01') found in DFAFEAT9 (offset x'3C') in the DFA. This will be set on when this new function is available on the system.



60 (3C)	Bit String	1	DFAFEAT9	FEATURES BYTE 9
	.... ..1.		DFABYPAUTH	DCBE Bypass Authorization support is installed
	1		DFAENCRYPT	DFSMS support for Data Set Encryption is installed
	1...		DFAJBAA	JES3_ALLOC_ASSIST=YES in DEVSUPxx
	.1..		DFAMEMUX	This level of the system supports IEBCOPY member selection user exits
	..1.		DFAPDSEG	PDSE Generation support is installed
	...1		DFAZEDCCMP	zEDC Compression support is installed
61 (3D)	CHARACTER	1		Reserved

© 2017 IBM Corporation

Appendix (Converting to Encrypted)

Data Set Encryption

IEBGENER Example where SYSUT1 can be any sequential data set (compressed or non-compressed) and SYSUT2 is created with a DataClass containing key label

```
//SMITH2    JOB 1,GEOFF,MSGCLASS=X
//          EXEC PGM=IEBGENER
//SYSIN     DD DUMMY
//SYSPRINT DD SYSOUT=*
//SYSUT1    DD DISP=SHR,DSN=SMITH.SEQ.CLRDATA
//SYSUT2    DD DISP=(NEW,CATLG),
//    DSN=SMITH.SEQ.ENCDATA,STORCLAS=SCSEQ,
//    DATACLAS=DCENCRPT,SPACE=(CYL,100,10))
```

NOTE: DFSMSdss COPY does not convert target data set to encrypted since the target data set retains characteristics of the source data set.

© 2017 IBM Corporation

Overview

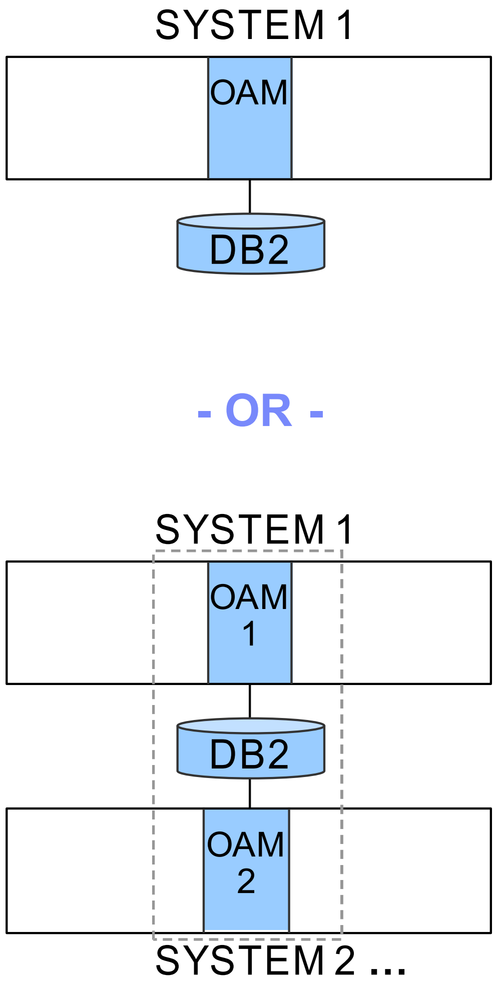
Multiple OAM Address Spaces per LPAR

- **Problem Statement / Need Addressed**
  - Need to host a “test” OAM (object support) instance and a “production” OAM (object support) instance on a single z/OS system.
  - Need to host multiple different “production” OAM (object support) instances on a single z/OS system.
  - Need to construct multiple OAMplex configurations each using one of the multiple OAM (object support) instances on each participating system.
- **Solution**
  - Provide new functionality that addresses customer needs by allowing Multiple OAM instances on a single system. V2R3 will allow the creation of up to 3 OAM subsystems (2 object, 1 tape) and 3 OAM address spaces (2 object, 1 tape).
- **Benefit / Value**
  - System programmers and storage administrators will be able to create multiple OAM instances to meet their unique business requirements. Application developers can exploit this functionality by directing OAM OSREQ application requests to a specific OAM (object support) instance. This will allow the ability for customers to deploy “production” and “test” capability for OAM or two separate “production” instances on the same system .

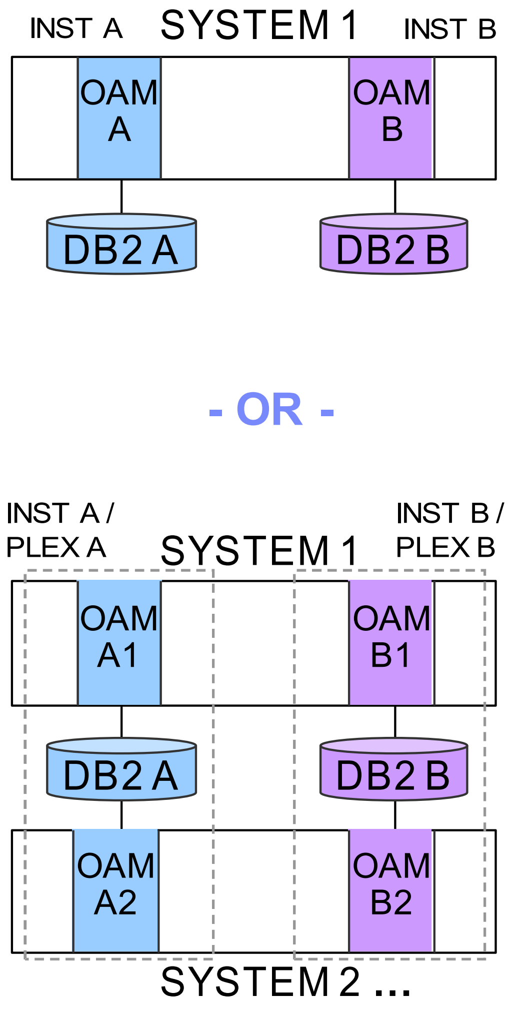
© 2017 IBM Corporation

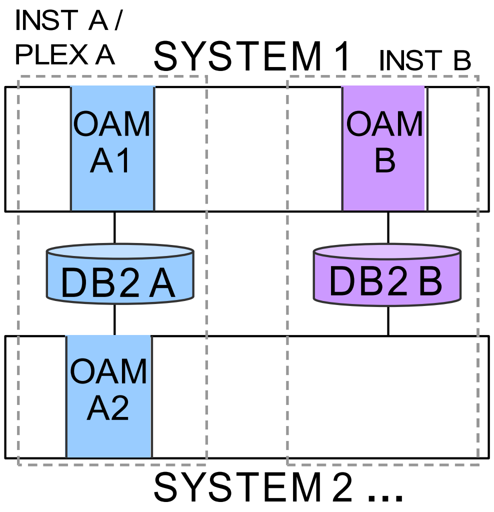
Multiple OAM Address Space Support

Today



z/OS V2R3





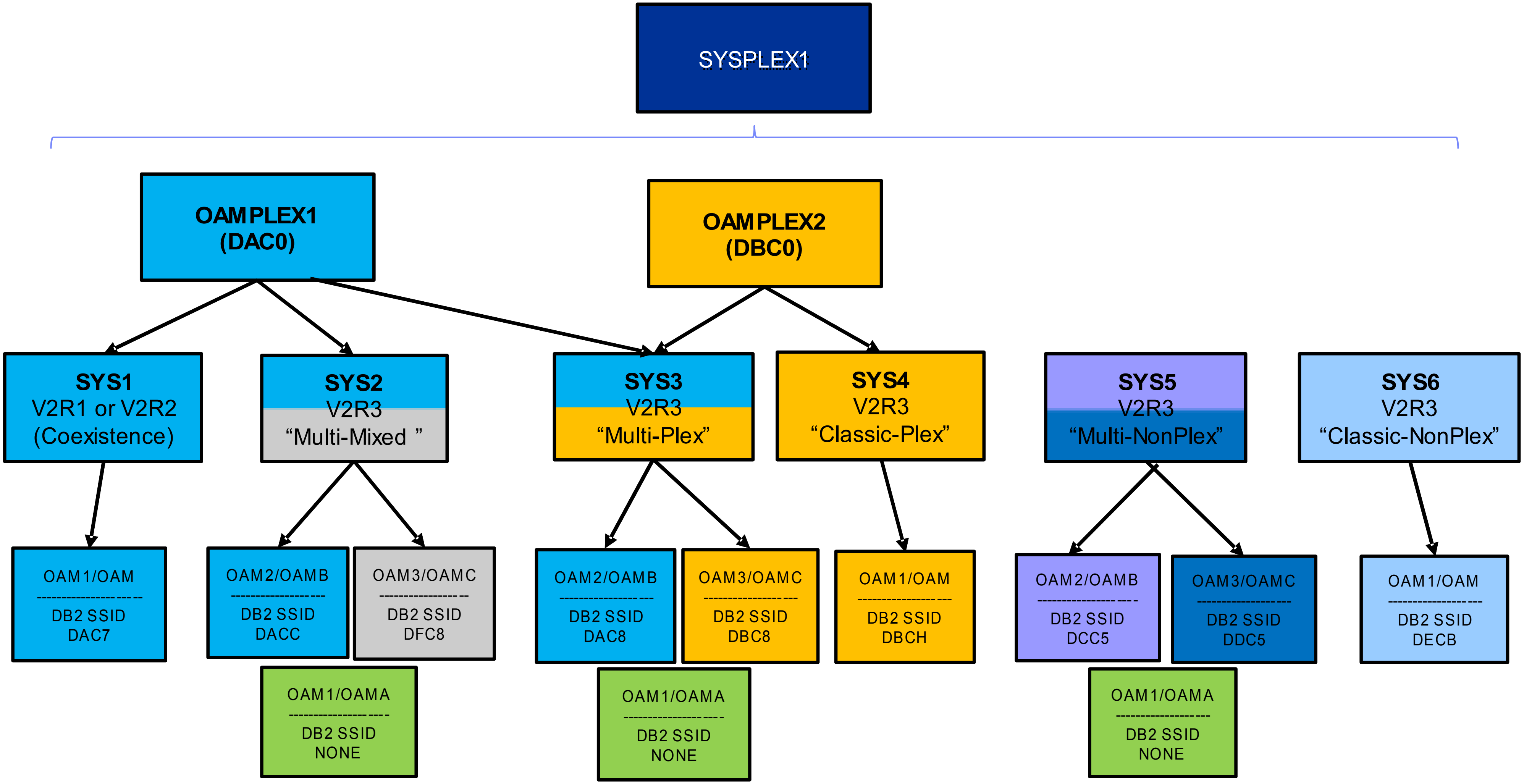
- ❑ Maximum of two OAM Object ‘instances’ per system (1 subsystem and 1 address space per ‘instance’)
- ❑ An optional tape library instance may also be used on each system for a total of 3 OAM instances per system

© 2017 IBM Corporation

Overview

Multiple OAM Address Spaces per LPAR

Example Configuration



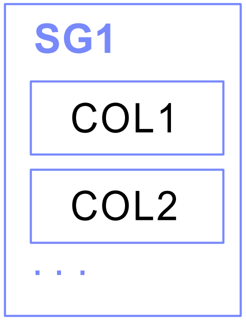
© 2017 IBM Corporation

Overview

Multiple OAM Address Spaces per LPAR

Collections

- Today OAM collections are maintained in two places, the catalog and in DB2
- With this support and with our coexistence support installed, OAM collections will no longer be maintained in two places
  - Now just in DB2
- This eliminates out of synch conditions and OAM having to maintain the information in two places
- New behavior is applicable when running in classic or in multiple mode



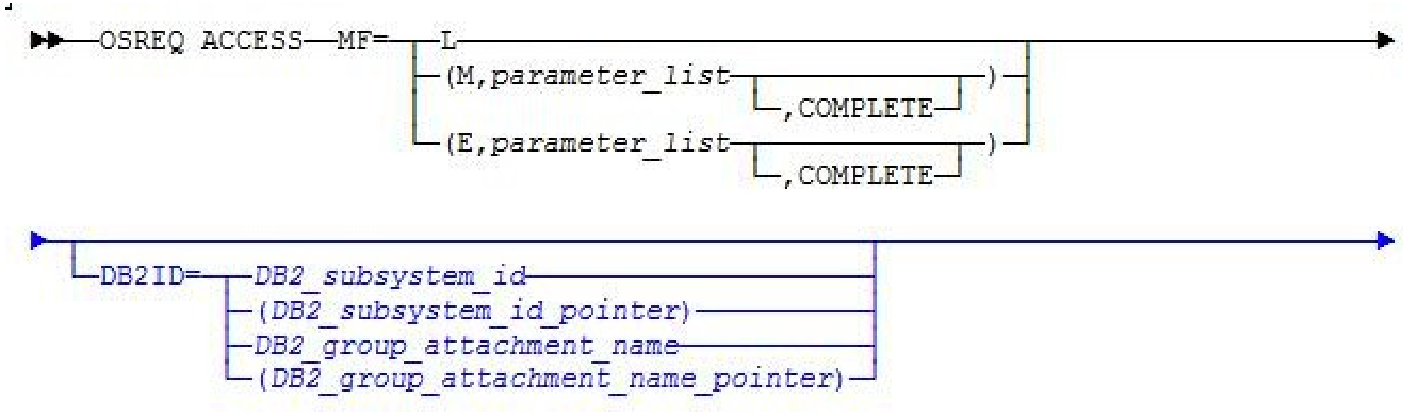
Logical grouping of objects; collection entry has default MC and SC

© 2017 IBM Corporation

Usage & Invocation

Multiple OAM Address Spaces per LPAR

OSREQ Interface (API)



```
►►─OSREQ ACCESS─MF=─┬─L──────────────────────────────────────┬──────────────►
                    ├─(M,parameter_list─┬───────────┬─)─┤
                    │                   └─,COMPLETE─┘    │
                    └─(E,parameter_list─┬───────────┬─)─┘
                                        └─,COMPLETE─┘

►─┬──────────────────────────────────────────────────────┬───────────────────►
  └─DB2ID=─┬─DB2_subsystem_id────────────────────────┤
           ├─(DB2_subsystem_id_pointer)──────────────┤
           ├─DB2_group_attachment_name───────────────┤
           └─(DB2_group_attachment_name_pointer)─────┘
```

- Identifies the DB2 subsystem (DB2 SSID or DB2 group attachment name if the DB2 subsystem is part of a data sharing group) to be used for processing this request

- For OSREQ applications that run in the (CICS or DSN) environment or when the IADDRESS keyword is specified, the DB2ID is not required since DB2 is already connected.
  - **No application changes** should be needed for customers using IBM Content Management and OnDemand since they already do the connection to the DB2 subsystem (enables us to determine which subsystem)

Usage & Invocation

Multiple OAM Address Spaces per LPAR

New Operator Command

DISPLAY OAM,CONFIG (within a “Multi OAM” environment)

```
CBR1960I OAM configuration data:
OAM   OAM       OAM       OAM       OAM   OAMPLEX   DB2   DB2   DB2
SUB   PROC      TASKID    STC#      TYPE  GROUP     ID    SSID  GATT
OAM1  OAMA      OAMA      STC00044  TLIB            NONE
OAM2  OAMB      OAMB      STC00052  OBJ             DB2   DB2   DBG1
OAM3  OAMC      OAMC      STC00053  OBJ             DB3   DB3   DBG2
```

Notes

- DISPLAY SMS commands get directed to tape library address space
- LIBRARY commands, as appropriate, get directed to tape library address space
- MODIFY *“OAM”,verb,operand* used to direct an OAM command to a particular object address space, for example …
  - MODIFY ***OAMB***,START,OSMC
  - MODIFY ***OAMB***,DISPLAY,OAM

DISPLAY OAM,CONFIG (within a “Classic OAM” environment)

```
CBR1960I OAM configuration data:
OAM   OAM       OAM       OAM       OAM   OAMPLEX   DB2   DB2   DB2
SUB   PROC      TASKID    STC#      TYPE  GROUP     ID    SSID  GATT
OAM1  OAM       OAM       STC00044  CLAS            DB2   DB2   DBG1
```

© 2017 IBM Corporation

Migration & Coexistence Considerations

Multiple OAM Address Spaces per LPAR

- No migration steps are required – the default values for all new options result in the same behavior as in prior releases.
- Coexistence APARs OA50220 (conditioning) and OA51229 (enablement) are required for pre-V2R3 systems operating in an OAMplex before introducing a V2R3 system.
  - Coexistence must be added within an OAMplex to allow lower level systems to now search for collection entries exclusively in DB2 tables since in V2R3 catalog use is removed.

© 2017 IBM Corporation

Installation

Multiple OAM Address Spaces per LPAR

Configuring OAM Multi

IEFSSNxx – for starting an OAM subsystem … OAM1, OAM2, ….

```
SUBSYS SUBNAME(OAM1) INITRTN(CBRINIT)
INITPARM('D=xxxx[,TIME=x][,MSG=x][,OTIS=x]
[,UPD=x][,MOS=nnnn][,LOB=x][,QB=x][,DP=x]')
```

Note: Specification of "D=" on 1st subsystem to initialize denotes "multi". Also, OTIS,MSG, and TIME from 1st subsystem to initialize apply to all subsystems.

'D=' Indicates the DB2 SSID, group attachment name or "NONE" for tape library support

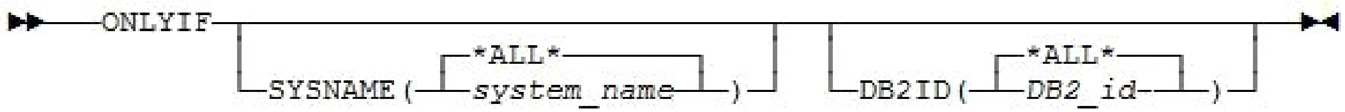
CBRAPROC – for starting an OAM address space … OAMA, OAMB, …

```
//OAM PROC OSMC=YES,MAXS=2,UNLOAD=9999,EJECT=LRW,REST=YES,DB2ID=DB2A
//IEFPROC EXEC PGM=CBROAM,REGION=0M,
//PARM=('OSMC=&OSMC,APLAN=CBROAM,MAXS=&MAXS,UNLOAD=&UNLOAD',
// 'EJECT=&EJECT,RESTART=&REST,D=&DB2ID')
//SYSABEND DD SYSOUT=A
```

'D=' indicates the DB2 SSID, group attachment name or "NONE" for tape library support

CBROAMxx - OAM Parmlib Member for tuning

ONLYIF statement syntax



'DB2ID' indicates the DB2 SSID, group attachment name or "NONE" for tape library support

Installation

Multiple OAM Address Spaces per LPAR

New Operator Command

MODIFY OTIS,DELSUB,[subsys|ALL]

- Support is added to the MODIFY OTIS command to allow OAM subsystems to be removed from the current OAM configuration. This is intended to provide support for changing between a classic OAM configuration and a multiple OAM configuration (or vice versa) or removing an incorrectly defined OAM subsystem without requiring an IPL.

subsys
Specifies the subsystem name of the OAM subsystem to be removed from the OAM configuration.

ALL
Specifies that all OAM subsystems that are in the OAM configuration should be removed from it.

“This command can be used to remove from the OAM configuration OAM subsystems that were defined in the IEFSSNxx member of PARMLIB or with a SETSSI ADD command. “

Note:

- A new OAM subsystem (or multiple OAM subsystems in a multiple OAM configuration) can be defined and added to the OAM configuration using the SETSSI ADD command, but because the removed subsystem remains defined to z/OS any newly added subsystem must use a different subsystem name.
- Precaution: The OAM address space, if any, and all other activity (e.g. OSREQ applications) associated with the OAM subsystem to be deleted should be stopped prior to issuing this command or unpredictable results could occur including abends.

© 2017 IBM Corporation

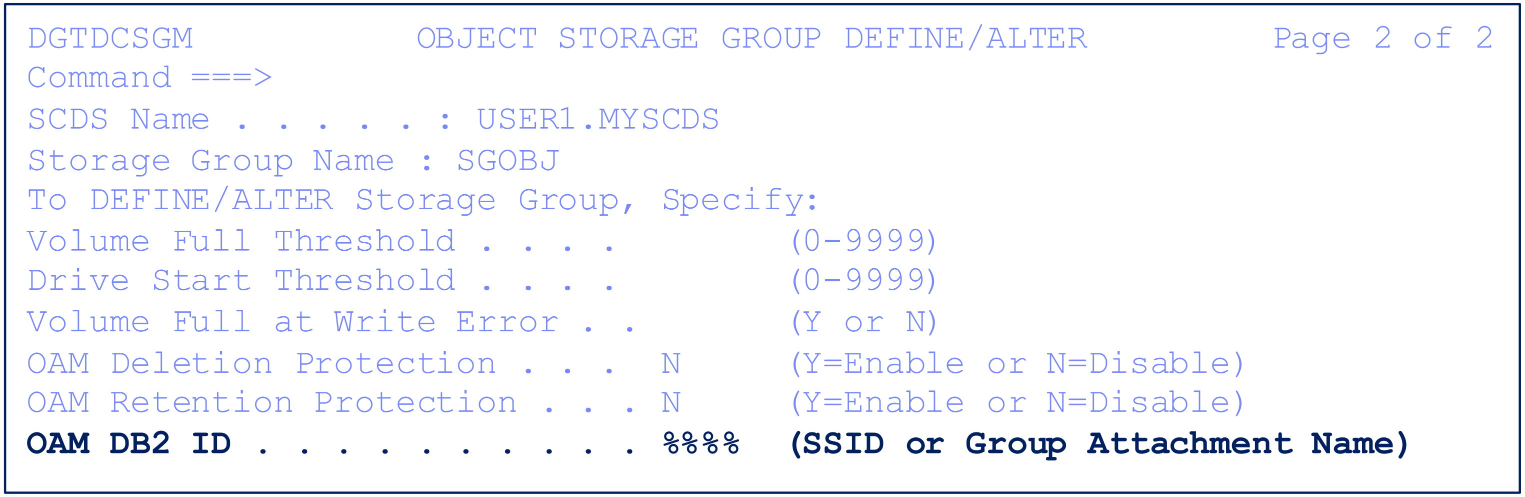
Installation

Multiple OAM Address Spaces per LPAR

SMS Configuration Changes

- **SMS Storage Group construct** “applicable in a multiple OAM configuration only; otherwise ignored” specifies the SSID(s) and/or Group Attachment Name(s) of the DB2 subsystem(s) associated with the OAM Object instance(s) in a multiple OAM configuration that can use this storage group name (wildcarding supported)

  Note: Where multiple OAM instances match the specified ID, all matching instances can use the same storage group name and values specified in the storage group definition. Each OAM instance is associated with a different DB2 subsystem, however, each instance will have a different set of DB2 tables and therefore data is not shared between OAM instances



```
DGTDCSGM          OBJECT STORAGE GROUP DEFINE/ALTER         Page 2 of 2
Command ===>
SCDS Name . . . . . : USER1.MYSCDS
Storage Group Name : SGOBJ
To DEFINE/ALTER Storage Group, Specify:
Volume Full Threshold . . . .         (0-9999)
Drive Start Threshold . . . .         (0-9999)
Volume Full at Write Error . .        (Y or N)
OAM Deletion Protection . . .   N     (Y=Enable or N=Disable)
OAM Retention Protection . . .  N     (Y=Enable or N=Disable)
OAM DB2 ID . . . . . . . . . .  %%%%  (SSID or Group Attachment Name)
```

- **SMS ACS routines** include a new &DB2SSID read-only variable that will be applicable in selected OAM environments
  - STORE, CHANGE, and CTRANS environments in the Storage Class and Management Class ACS routines
  - STORE environment in the Storage Group ACS routine

Appendix

Multiple OAM Address Spaces per LPAR

- z/OS DFSMS Object Access Method (OAM) Planning, Installation, and Storage Administration Guide for Object Support, SC23-6866
- z/OS DFSMS Object Access Method (OAM) Planning, Installation, and Storage Administration Guide for Tape Libraries, SC23-6867
- z/OS DFSMS Object Access Method (OAM) Application Programmer's Reference, SC23-6865
- z/OS DFSMSdfp Diagnosis, SC23-6863
- z/OS System Messages Vol 4 (CBD-DMO) , SA38-0671
- z/OS DFSMS Using the New Functions, SC23-6857
- z/OS DFSMSdfp Storage Administration Reference, SC23-6860
- Z/OS Summary of Message and Interface Changes, SA23-2300

© 2017 IBM Corporation

Overview

DFSORT UNICODE Support

- **Problem Statement / Need Addressed**
  - Unicode is the universal character encoding which provides the basis for processing, storage and interchange of text data in any language in all modern software and information technology protocols. As an application programmer, I want to be able to sort and merge Unicode data.
- **Solution**
  - DFSORT can now sort Unicode data in UTF8/UTF16/UTF32 encoding format
- **Benefit / Value**
  - With increased use of Unicode data worldwide, clients now can sort the Unicode data

© 2017 IBM Corporation

Usage & Invocation

DFSORT UNICODE Support

- With this line item customers now can
  - SORT/MERGE Unicode Data with control field length of 1 to 450 Unicode characters for UTF-8 format data.
  - SORT/MERGE Unicode Data with control field length of 1 to 450 Unicode characters for UTF-16 format data.
  - SORT/MERGE Unicode Data with control field length of 1 to 450 Unicode characters for UTF-32 format data.

- Examples :
  - SORT FIELDS=(1,450,UTF32,A)
  - SORT FIELDS=(12,16,UTF16,A,217,2,UTF16,D)
  - MERGE FIELDS=(9,2,UTF8,A,17,2,UTF8,A)

© 2017 IBM Corporation

Migration & Coexistence Considerations

DFSORT UNICODE Support

- The following are new DFSORT/ICETOOL reserved words which are no longer allowed as symbols: UTF8, UTF16 and UTF32
- If customers used any of these words as a symbol previously they must change them. For example, if they used UTF8, they can change it to utf8.

© 2017 IBM Corporation

Appendix

DFSORT UNICODE Support

- Publications
  - z/OS: DFSORT Installation and Customization (SC23-6881-03)
  - z/OS DFSORT Application Programming Guide (SC23-6878-03)
  - z/OS DFSORT Messages and Codes (SC23-6879-03)

- Web site: http://www.ibm.com/storage/dfsort

© 2017 IBM Corporation

Overview

RMM: UXTABLE Simplification

- **Problem Statement / Need Addressed**
  - Using the UXTABLE was the only alternative to modifying ACS routines and Management Classes if the clients wished to dynamically assign retention parameters such as the Retention Method to newly written tape data sets and volumes.
  - The existing UXTABLE is difficult to understand and to manage:
    - Needs manual compilation and understanding of RMM exits
    - No way to check the contents of the currently loaded UXTABLE
    - Difficult to alter, requires keeping the source code intact
    - No way to assign WHILECATALOG, Last reference days and RETAINBY using the UXTABLE
- **Solution**
  - The defaults table, which does the same thing as the UXTABLE, however is easier to manage
  - When a new file is written to tape, it is checked against the defaults table. If there is a match, the retention attributes specified in the table are used.

© 2017 IBM Corporation

Usage & Invocation

RMM: UXTABLE Simplification

- The internalized UXTABLE is called the Defaults Table, or DEFTABLE
- Defined in the EDGDEFxx PARMLIB member
  - EDGDEFxx suffix is specified in the DEFTABLE option of EDGRMMxx
- Simple to modify
  1) Edit the EDGDEFxx file
  2) Restart the RMM subsystem using F DFRMM,M=nn
- The **LISTCONTROL DEFTABLE** subcommand shows the currently loaded defaults table

© 2017 IBM Corporation

Usage & Invocation

RMM: UXTABLE Simplification

- **Sample Defaults**

PARMLIB(EDGRMMAA):

```
 OPTION  OPMODE(P) -
 SYSID(SYSTEM1) -
 TPRACF(N) -
 NOTIFY(Y) -
 MAXHOLD(100) -
 DEFTABLE(AA) -
 …
```

PARMLIB(EDGDEFAA):

```
 DEFAULT DSN(ABC.*) -
 JOB(JOB02) -
 KEYDATE(99001) -
 RETPD(100) -
 VX(NO) -
 RM(VRSEL)

 DEFAULT JOB(ABC*) -
 KEYDATE(99002) -
 RETPD(PERMANENT) -
 VRSVAL(M99002) -
 WHILECATALOG(ON) -
 RM(EXPDT) -
 RETAINBY(VOLUME)

 DEFAULT  -
 RETPD(5,OVERRRIDE) -
 VRSELEXCLUDE(YES) -
 LASTREF(20) -
 RETAINBY(SET)
```

© 2017 IBM Corporation

Usage & Invocation

RMM: UXTABLE Simplification

Selection and Criteria

- When a new tape data set is written, the defaults table is searched from the top down until a matching entry is found
- An entry only matches if all 3 selection criteria are satisfied
  - DSNAME mask – can contain wildcards. Default is **
  - JOBNAME mask – can contain wildcards. Default is *
  - KEYDATE – matched against the EXPDT value specified in the DD statement
    - Has the form yyddd, yy indicates years from 1900 to 1999, ddd indicates days from 0 to 365
    - The default is * to select all dates
    - NOKEYDATE only matches if a keydate is not specified. Any date present in KEYDATE(yyddd) anywhere in the defaults table is considered to be a keydate.

© 2017 IBM Corporation

Usage & Invocation

RMM: UXTABLE Simplification

- **Attributes that can be assigned**
  - Retention Period
  - VRSEL Exclude
  - VRS Management Value
  - Last reference days (valid for RM=EXPDT)
  - WHILECATALOG (valid for RM=EXPDT)
  - Retention Method
  - Retain By (valid for RM=EXPDT)

- If an attribute is not specified, it is not modified.

© 2017 IBM Corporation

Usage & Invocation

RMM: UXTABLE Simplification

Volume Specific Attributes

- only used if the matching data set is the first in the volume chain, and writing to a new or scratch volume.
- RETENTIONMETHOD or RM
  - EXPDT or VRSEL. VRSEL volumes are managed using VRSEL policies during housekeeping. EXPDT volumes are managed dynamically, and support WHILECATALOG and LASTREF.
- RETAINBY
  - SET, VOLUME, or FIRSTFILE. Is only used if the new volume has the EXPDT retention method.

© 2017 IBM Corporation

Usage & Invocation

RMM: UXTABLE Simplification

Data Set Attributes

- RETPD - 0 to 93000 or PERMANENT. Use RETPD(nnnnn,OVERRIDE) to override the RETPD value specified in the DD statement.
- VRSELEXCLUDE – Y or N. Y means the data set is excluded from VRSEL processing, saving time. Value for datasets on RM=EXPDT volumes is always Y.
- VRS Value – one to eight characters. This management value can be referenced in VRS policies
- Last Reference Days – 0 to 93000. Only used on RM=EXPDT volumes
- WHILECATALOG – ON, OFF, UNTILEXPIRED. Only used on RM=EXPDT volumes

© 2017 IBM Corporation

Usage & Invocation

RMM: UXTABLE Simplification

Priority

- Defaults table cannot be used together with the UXTABLE. Results in following message when starting RMM:

  DEFTABLE SPECIFIED IN PARMLIB WHILE UXTABLE IS DETECTED IN STORAGE. REPLY U TO USE THE UXTABLE, OR D TO USE THE DEFTABLE AND ERASE THE UXTABLE FROM STORAGE

- If a parameter is specified in several places,
  - Management Class has the highest priority
  - UX100 exit has the next highest priority
  - Defaults table has lower priority then MC and UX100
  - Global defaults in EDGRMMxx have the lowest priority

© 2017 IBM Corporation

Usage & Invocation

RMM: UXTABLE Simplification

Priorities for RETPD/EXPDT are handled differently:

- The RETPD/EXPDT value specified in the JFCB control block has the highest priority
    - Can be specified in the JCL
    - Can be specified in the DATACLASS
    - Can be modified using the UXTABLE or the EDG_EXIT100 exit
- The “Expire after Date/Days” value in the Management Class has the next highest priority
- RETPD in the defaults table has a lower priority. However, OVERRIDE can be used to override the JFCB value
- The global defaults REPTD value, along with RM=EXPDT specific global RETPD defaults have the lowest priority.

© 2017 IBM Corporation

Overview

RMM: SMS Management Class for Tape

- **Problem Statement / Need Addressed**
  - Clients would like to manage both their disk and their tape data sets using the same set of policies
  - However, the Management Classes used for disk data sets have limited influence on tape data
  - In V2R2, only RETPD and LASTREF could be assigned using the management class
- **Solution**
  - Add new tape specific attributes to the management class, that can be used by RMM
- **Benefit**
  - Single policy to manage both disk and tape data sets

© 2017 IBM Corporation

Usage & Invocation

RMM: SMS Management Class for Tape

Retention Method, Retain By, VRSEL Exclude, Whilecatalog

Now these attributes can be set using SMS Management Class!

The list of management class attributes assigned to tape data sets and volumes was expanded with:

Tape volumes attributes

- the ‘Retention Method’
- the ‘VRSEL EXCLUDE’ (for VRSEL retention method)

Tape data set attributes

- the ‘RETAIN BY’ (for EXPDT retention method)
- the ‘WHILECATALOG’ (for EXPDT retention method)

© 2017 IBM Corporation

Usage & Invocation

RMM: SMS Management Class for Tape

General requirements and specifications

- To assign a characteristic for a tape volume/data set using an SMS management class (MC), the following conditions must be met:
  - MC can apply to both system managed tape and non-system managed tape (using &ACSENVIR='RMMVRS)
  - The MC should exist and V2R3 is required
  - The created dataset should be SMS-supported and located on a TCDB volume
  - MGMTCLAS must be specified in JCL DD statement
  - When MCATTR=NONE, MC will not have any affect on an attribute
  - The following RMM PARMLIB options should be set:

SMSACS(YES) and MCATTR(ALL/VRSELXDI)

© 2017 IBM Corporation

Usage & Invocation

RMM: SMS Management Class for Tape

Description of Retention Method attribute

The retention method is an attribute of the volume. All volumes in a multivolume set have the same retention method. All data sets on a volume are managed with the same retention method as the volume on which they reside. Retention method is only used if writing to the first data set of the volume chain.

The possible values

EXPDT, VRSEL or blank.

Priority

The “Retention Method” for volumes can be taken from the following sources, listed in priority order, with the highest priority first

1) “Retention Method” in the Management Class

2) PL100_RETENTIONMETHOD, returned by the EDG_EXIT100 exit routine

3) RETENTIONMETHOD in the defaults table in EDGDEFxx.

4) The default EDGRMMxx parmlib OPTION RM

Compatibility with other attributes

This attribute is compatible with any other except VRSEL Exclude

Note

The retention method can also be specified manually in the ADDVOLUME or CHANGEVOLUME subcommands.

© 2017 IBM Corporation

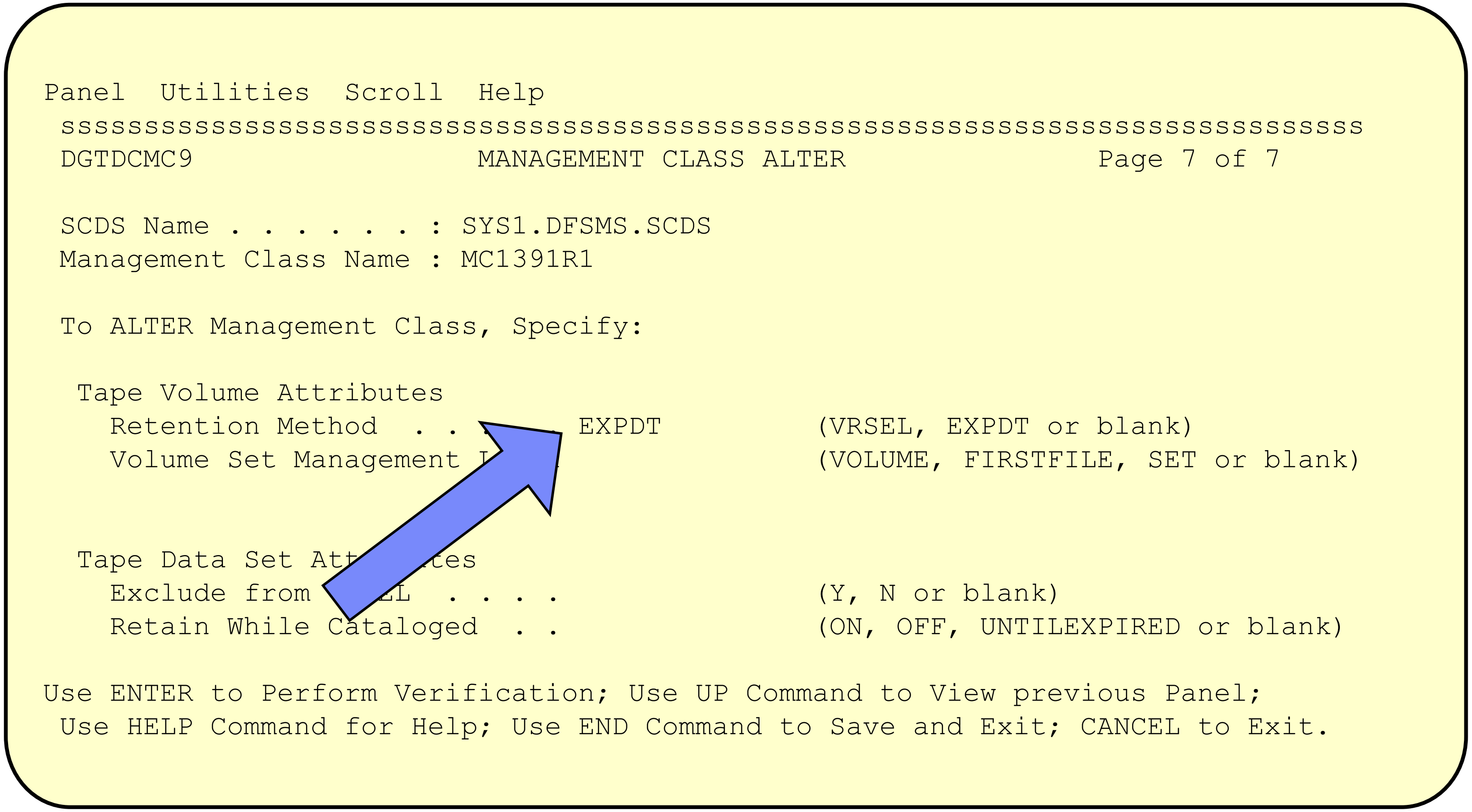
Usage & Invocation

RMM: SMS Management Class for Tape

Setting “Retention Method” using ISMF

Create a new MC or ALTER existing one.

To set “Retention Method“ select panel “MANAGEMENT CLASS ALTER” and type required value.



```
Panel  Utilities  Scroll  Help
 ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
 DGTDCMC9                 MANAGEMENT CLASS ALTER               Page 7 of 7

 SCDS Name . . . . . . . : SYS1.DFSMS.SCDS
 Management Class Name : MC1391R1

 To ALTER Management Class, Specify:

  Tape Volume Attributes
    Retention Method  . . .  . EXPDT          (VRSEL, EXPDT or blank)
    Volume Set Management L  .                (VOLUME, FIRSTFILE, SET or blank)


  Tape Data Set Att     tes
    Exclude from      EL  . . . .             (Y, N or blank)
    Retain While Cataloged  . .               (ON, OFF, UNTILEXPIRED or blank)

Use ENTER to Perform Verification; Use UP Command to View previous Panel;
 Use HELP Command for Help; Use END Command to Save and Exit; CANCEL to Exit.
```

Usage & Invocation

RMM: SMS Management Class for Tape

Description of RetainBy attribute

With the EXPDT retention method, volumes and volume sets can be retained as individual volumes, as volume sets, or based on the expiration date of the first file. The volume attribute related to the retention of a multivolume set is the “RetainBy” attribute. Retain By is only assigned if writing to the first data set of the volume chain.

The possible values

FIRSTFILE, VOLUME, SET or blank.

Priority

The “RETAINBY” for volumes can be taken from the following sources, listed in priority order, with the highest priority first

1) “RETAINBY” in the Management Class

2) RETAINBY in the defaults table in EDGDEFxx.

3) The default EDGRMMxx parmlib OPTION RM(EXPDT(RETAINBY(value)))

Compatibility with other attributes

This attribute is not compatible with RM(VRSEL) and VRS Exclude

Note

The “RetainBy” can also be specified manually in the ADDVOLUME subcommand using RETAINBY operand.

© 2017 IBM Corporation

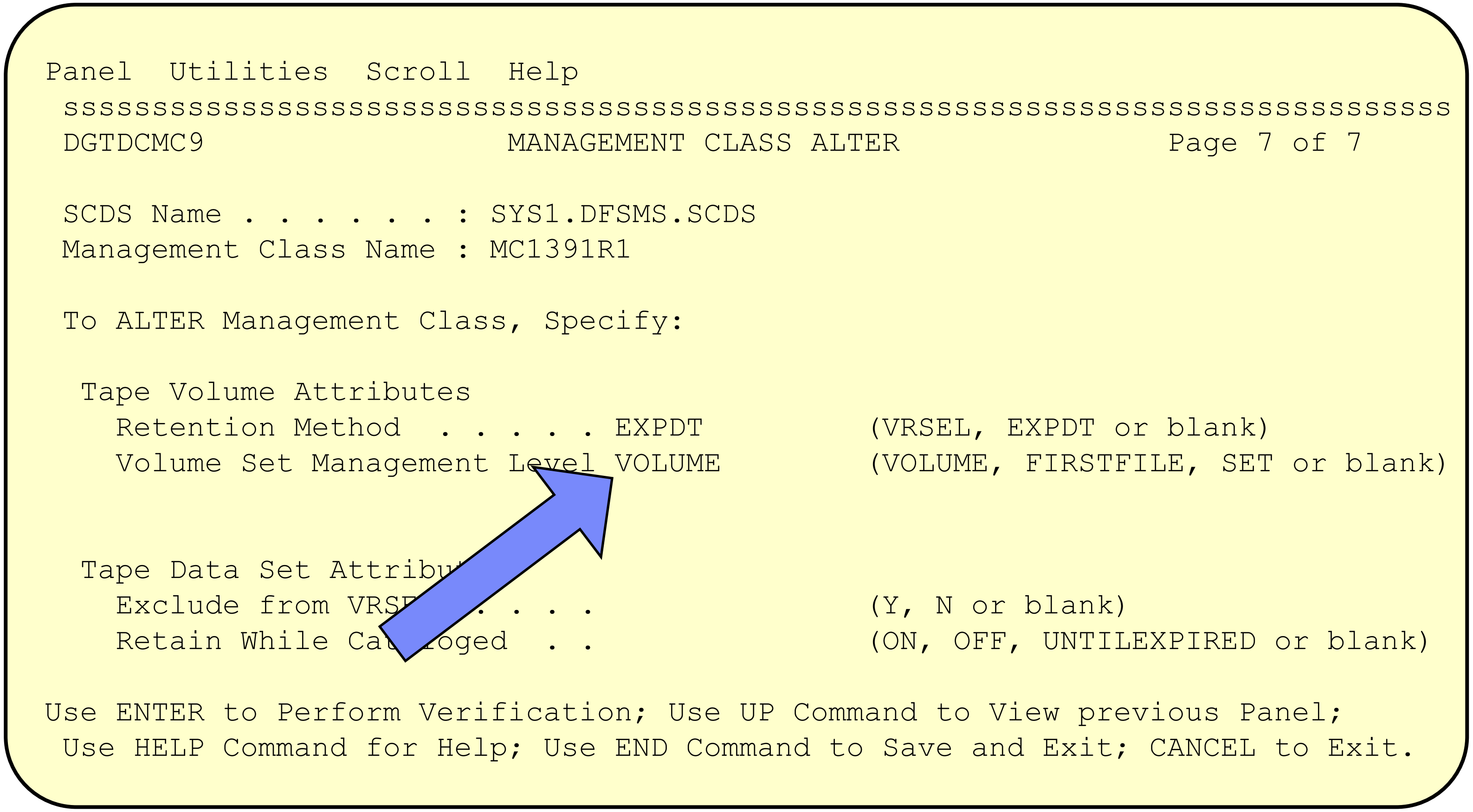
Usage & Invocation

RMM: SMS Management Class for Tape

Setting “Retain By” using ISMF

Create a new MC or ALTER existing one.

To set “Retain By“ select panel “MANAGEMENT CLASS ALTER” and type required value for “Volume Set Management Level” entry.



```
Panel  Utilities  Scroll  Help
 ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
 DGTDCMC9                 MANAGEMENT CLASS ALTER               Page 7 of 7

 SCDS Name . . . . . . : SYS1.DFSMS.SCDS
 Management Class Name : MC1391R1

 To ALTER Management Class, Specify:

  Tape Volume Attributes
    Retention Method  . . . . . EXPDT         (VRSEL, EXPDT or blank)
    Volume Set Management Level VOLUME        (VOLUME, FIRSTFILE, SET or blank)


  Tape Data Set Attributes
    Exclude from VRSEL  . . . .               (Y, N or blank)
    Retain While Cataloged  . .               (ON, OFF, UNTILEXPIRED or blank)

Use ENTER to Perform Verification; Use UP Command to View previous Panel;
 Use HELP Command for Help; Use END Command to Save and Exit; CANCEL to Exit.
```

Usage & Invocation

RMM: SMS Management Class for Tape

Description of VRSEL Exclude attribute

When a data set is created on a tape volume managed by the EXPDT retention method, the data set VRSELEXCLUDE attribute is automatically set as “Y”. If the data set is created on a tape volume managed by the VRSEL retention method, the VRSELEXCLUDE attribute can be set by a SMS MGMTCLAS VRSELEXCLUDE attribute

The possible values

Y, N or blank.

Priority

The “VRSELEXCLUDE” for a tape data set can be taken from the following sources, listed in priority order, with the highest priority first

1) “VRSELEXCLUDE” in the Management Class

2) VRSELEXCLUDE in the defaults table in EDGDEFxx.

3) VX in the EDG_EXIT100 installation exit.

Compatibility with other attributes

This attribute is compatible with RM(VRSEL) only.

© 2017 IBM Corporation

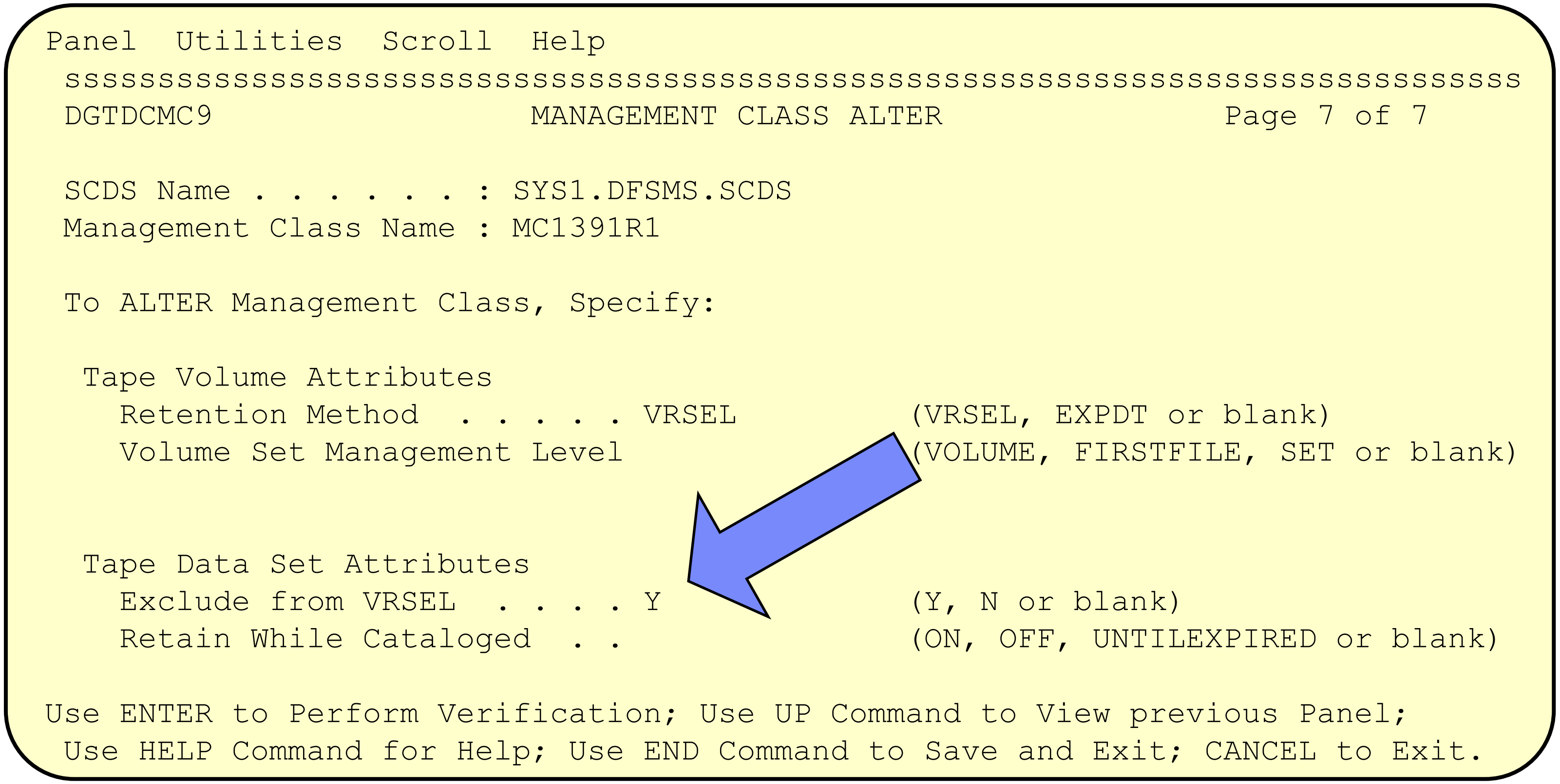
Usage & Invocation

RMM: SMS Management Class for Tape

Setting “VRSEL Exlude” using ISMF

Create a new MC or ALTER existing one.

To set “VRSEL Exclude “ select panel “MANAGEMENT CLASS ALTER” and type required value for “Exclude from VRSEL” entry.



```
Panel  Utilities  Scroll  Help
 ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
 DGTDCMC9                 MANAGEMENT CLASS ALTER               Page 7 of 7

 SCDS Name . . . . . . . : SYS1.DFSMS.SCDS
 Management Class Name : MC1391R1

 To ALTER Management Class, Specify:

  Tape Volume Attributes
    Retention Method  . . . . . VRSEL         (VRSEL, EXPDT or blank)
    Volume Set Management Level               (VOLUME, FIRSTFILE, SET or blank)


  Tape Data Set Attributes
    Exclude from VRSEL  . . . . Y             (Y, N or blank)
    Retain While Cataloged  . .               (ON, OFF, UNTILEXPIRED or blank)

Use ENTER to Perform Verification; Use UP Command to View previous Panel;
 Use HELP Command for Help; Use END Command to Save and Exit; CANCEL to Exit.
```

© 2017 IBM Corporation

Usage & Invocation

RMM: SMS Management Class for Tape

Description of WHILECATALOG attribute

A cataloged data set may prevent the volume from expiring on its expiration date if it has WHILECATALOG(ON). The date may decrease after a dataset with WHILECATALOG(UNTILEXPIRED) is uncataloged. WHILECATALOG attribute is used to set the WHILECATALOG attribute for a new data set on a EXPDT volume only.

The possible values

ON, OFF, UNTILEXPIRED or blank.

Priority

The “WHILECATALOG” for a tape data set can be taken from the following sources, listed in priority order, with the highest priority first

1) “WHILECATALOG” in the Management Class

2) WHILECATALOG in the defaults table in EDGDEFxx.

3) The default EDGRMMxx parmlib OPTION RM(EXPDT(GDG(WHILECATALOG(…)), NOGDG(WLCT(…)).

Compatibility with other attributes

This attribute is compatible with RM(EXPDT) only.

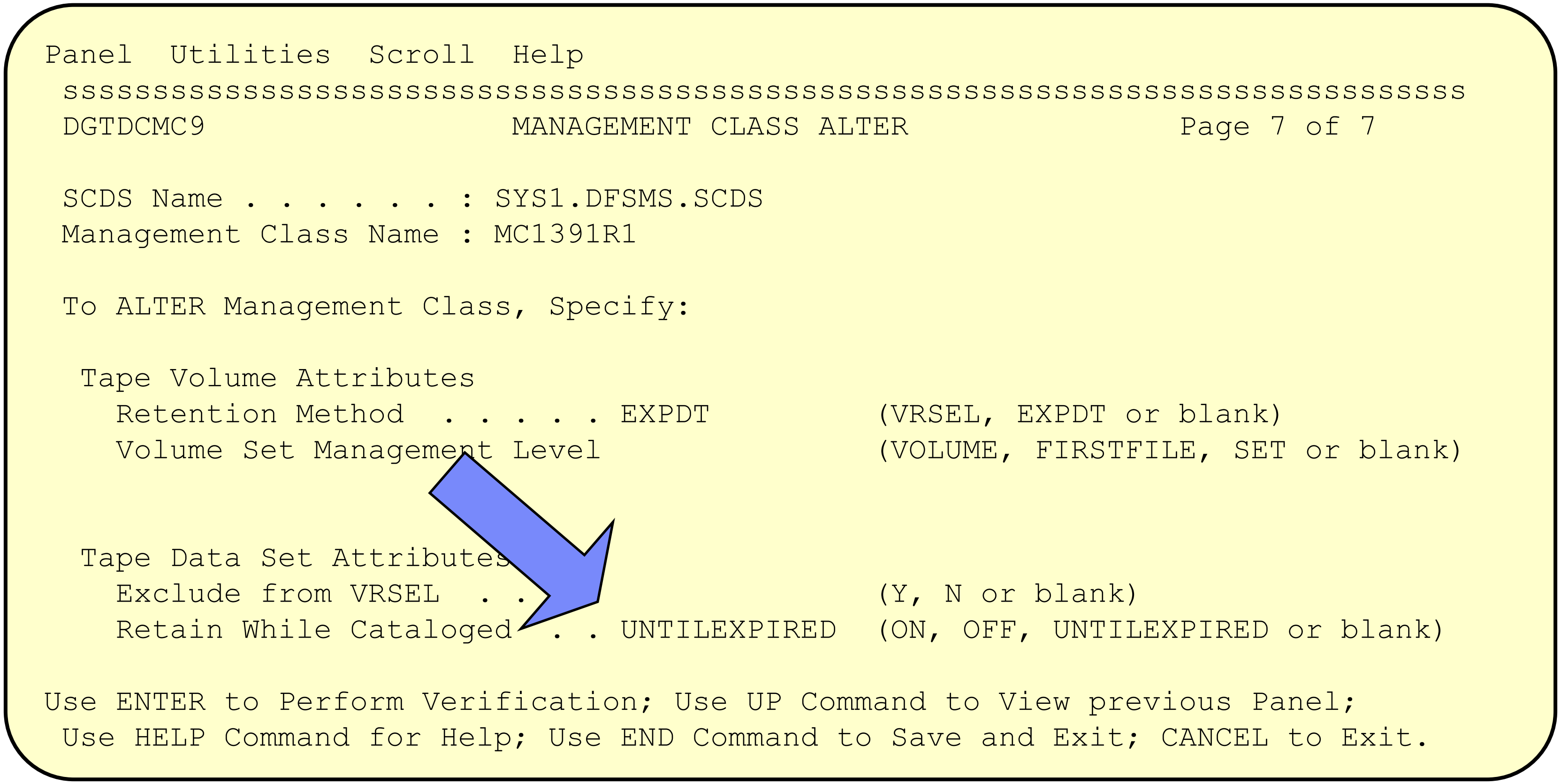
© 2017 IBM Corporation

Usage & Invocation

RMM: SMS Management Class for Tape

Setting “WHILECATALOG” using ISMF

- Create a new MC or ALTER existing one.
- To set “WHILECATALOG“ select panel “MANAGEMENT CLASS ALTER” and type required value for “Retain While Cataloged” entry.



```
Panel  Utilities  Scroll  Help
 ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
 DGTDCMC9                 MANAGEMENT CLASS ALTER                Page 7 of 7

 SCDS Name . . . . . . . : SYS1.DFSMS.SCDS
 Management Class Name : MC1391R1

 To ALTER Management Class, Specify:

  Tape Volume Attributes
    Retention Method  . . . . . . EXPDT         (VRSEL, EXPDT or blank)
    Volume Set Management Level                 (VOLUME, FIRSTFILE, SET or blank)


  Tape Data Set Attributes
    Exclude from VRSEL  . . .                   (Y, N or blank)
    Retain While Cataloged  . . UNTILEXPIRED  (ON, OFF, UNTILEXPIRED or blank)

Use ENTER to Perform Verification; Use UP Command to View previous Panel;
 Use HELP Command for Help; Use END Command to Save and Exit; CANCEL to Exit.
```

Usage & Invocation

RMM: SMS Management Class for Tape

Setting the management class attributes with NaviQuest

The following variables are used to call NaviQuest to set MC attribute:

Retention Method	RETMETHOD(EXPDT/VRSEL/blank)
Retain By	VOLSETMGL(FIRSTFILE/VOLUME/SET)
VRSEL Exclude	EXCLVRSEL(Y/N/blank)
WHILECATALOG	WHILECTLG(ON/OFF/UNTILEXPIRED/blank)

Corresponding changes included in the following samples of the SYS1. SACBCNTL:

ACBJBAIO, ACBJBAIQ, ACBJBAJ1

The following two slides show how to create or edit and activate a new or already existing Management Class using NaviQuest. The procedure consists of following steps:

a) DEFINE MC in temp data set (RMMUSER.TEST.ISPTABL) ;

b) ADD/ALTER it into ACS;

c) ACTIVATE new/altered MC.

© 2017 IBM Corporation

Usage & Invocation

RMM: SMS Management Class for Tape

Here is an example of MC creation with name **MCRLW** and attributes: RM(**EXPDT**),RETAINBY(**SET**),WHILECATALOG(**ON**)

```
//MCDEFINE JOB  (ACCT),'RMMUSER',MSGCLASS=H,
//      NOTIFY=RMMUSER,CLASS=A,MSGLEVEL=(1,1),TIME=(0,10)
//MYLIB JCLLIB ORDER=SYS1.SACBCNTL
//ALLOC   EXEC PGM=IEFBR14
//TABLES  DD DSN=RMMUSER.TEST.ISPTABL, UNIT=SYSDA,SPACE=(TRK,(9,1,4)),
//           DISP=(,CATLG),DCB=(LRECL=80,BLKSIZE=3120,RECFM=FB,DSORG=PO)
//********************************************************************
//*   DEFINE MANAGEMENT CLASS
//********************************************************************
//DEFINE EXEC ACBJBAOB,TABL2=RMMUSER.TEST.ISPTABL

//SYSUDUMP DD  SYSOUT=*
//TEMPFILE  DD  DSN=&&TEMPFILE,DISP=(MOD,PASS),UNIT=SYSDA,
// SPACE=(TRK,(1,1)),LRECL=300,RECFM=F,BLKSIZE=300
//SYSTSIN  DD *
 PROFILE PREFIX(SYS1)
 ISPSTART CMD(ACBQBAJ1 DEFINE SCDS(DFSMS.SCDS) +
 MGMTCLAS(MCRLW)   +
 RETMETHOD(EXPDT)  +
 VOLSETMGL(SET)    +
 WHILECTLG(ON))
/*
```

© 2017 IBM Corporation

Usage & Invocation

RMM: SMS Management Class for Tape

<continued from previous slide>

```
//*   EXECUTE THE DEFINE/ALTER **
//STEP3   EXEC ACBJBAOB,
//        TABL2=RMMUSER.TEST.ISPTABL
//SYSPROC  DD DSN=RMMTST.MAZ.EXEC,DISP=SHR,BLKSIZE=0
//         DD DSN=ISP.SISPCLIB,DISP=SHR
//         DD DSN=SYS1.DGTCLIB,DISP=SHR
//SYSUDUMP DD  SYSOUT=*
//SYSTSIN  DD DSN=&&TEMPFILE,DISP=(OLD,DELETE,DELETE)
//*   DELETE TEMP DATASET **
//TEMPDEL EXEC PGM=IDCAMS,COND=EVEN
//SYSPRINT DD  SYSOUT=*
 DELETE RMMUSER.TEST.ISPTABL
 SET MAXCC=0
/*
//*   Suspend processing for nn seconds (2 secs)  **
//RMMSLEEP EXEC  PGM=IKJEFT01,PARM='SLEEP 2',COND=EVEN
//SYSTSPRT DD  SYSOUT=*
//SYSTSIN  DD  DUMMY
/*
//ACTIVATE JOB (ACCT),'RMMUSER',MSGCLASS=H,PASSWORD=PERMPASS,
//      USER=RMMUSER,CLASS=A,MSGLEVEL=(1,1),TIME=(0,10)
//* THIS JOB ACTIVATES THE SCDS.                                     *
//SMSACT   EXEC PGM=XCONSOLE,PARM='SETSMS SCDS(SYS1.DFSMS.SCDS)'
```

© 2017 IBM Corporation

Overview

RMM: RAS Enhancements: External Data Manager

- **Problem Statement / Need Addressed**
  - When either OPEN and ABEND VRS's or RACF permissions are configured incorrectly a user can suffer because tapes being accidentally released by users they do not belong to.
- **Solution**
  - DFSMSrmm introduces a new feature for tapes created by programs that provide their own tape management. Such tapes will be referred to as EDM managed ones that means controlled by External Data Manager. The feature will affect the DFSMShsm, DFSMSdfp OAM and IBM Spectrum Protect components by preventing tapes from being accidentally released by users they do not belong to and will be referred to as EDM support.
- **Benefit / Value**
  - Prevent tapes from being incorrectly released and subsequently overwritten

© 2017 IBM Corporation

Usage & Invocation

RMM: RAS Enhancements: External Data Manager

EDM support is active by default. To deactivate the support the DFSMSrmm should be modified or restarted with the parmlib OPTION command operand EDM(NO).

Parmlib member EDGRMMxx OPTION command: operand EDM

```
>--+--------------------+-->
   |          |-YES-|   |
   |---EDM--(-+-----+-)-|
              |-NO--|
```

To enforce tape volumes to be considered as EDM managed or not, the following RMM CHANGEVOLUME subcommand operand can be used:

```
>-----+-----------+-- >
      |---EDM-----|
      |---NOEDM---|
```

EDM managed tape volumes can not be released via RMM DELETEVOLUME with RELEASE.

© 2017 IBM Corporation

Usage & Invocation

RMM: RAS Enhancements: External Data Manager

- The tape volume EDM attribute appears in the RMM LISTVOLUME output:

```
      Volume information:
Volume = A11572   VOL1  =          Rack  =           Owner   =
  Type = PHYSICAL         Stacked count  = 0         Jobname =
  Worldwide ID =                                     WORM    = N
Creation:  Date = 2016/173    Time = 03:15:51  System ID = W98MVS2
Assign:    Date = 2016/176    Time = 03:15:51  System ID =
. . . . . . . . . . .
Data set name =
Volume status:   EDM = N   Hold = N   File 1 Data set seq = 0
Status = SCRATCH   Availability =                   Label = SL
. . . . . . . . . . .
```

Migration & Coexistence Considerations

RAS Enhancements: External Data Manager

- z/OS releases V2R1 and V2R2 require coexistence PTFs - OA51654 - to be installed before exploitation of new functions is attempted on V2R3 and higher.
- The toleration/coexistence APAR OA51654 has been created to tolerate EDM support for V2R1 and V2R2 releases so that tape volumes with the EDM attribute set can not be expired and released by DFSMSrmm expiration process and RMM DELETEVOLEME with RELEASE.
- Migration action. None.

© 2017 IBM Corporation

Overview

RAS Enhancements: Report Generator

- **Problem Statement**

  ICETOOL allows displaying Maximum, Minimum, Average, values as well as counts. The report generator had no support for these statistics elements, forcing users to manually edit the report JCL.

- **Solution**

  You can define the needed statistics elements by typing “Y” against an appropriate field on the DFSMSrmm Report Definition panel.

  You may block calculating statistics for any numeric field by typing “N” on the DFSMSrmm Report Controls panel

- **Benefit / Value**

  Customizing reports made simpler

© 2017 IBM Corporation

Usage & Invocation

RMM: RAS Enhancements: Report Generator

You can define whether you need the amount of lines to be displayed in the report along with other needed statistics elements by typing “Y” against an appropriate field on the DFSMSrmm Report Definition panel

```
EDGPG050   DFSMSrmm Report Definition - COUNT06  Row 1 to 22 of 214

Command ===>                                  Scroll ===> PAGE

Report title . . . List of Data Sets (Size + Usage)   +
Report footer  . . in the CDS of RMM
Reporting tool . : ICETOOL                 Report width: 70
Show minimum values: (N/Y)        Show average values:  (N/Y)
Show maximum values: (N/Y)        Show totals        :  (N/Y)

Show counts        : (N/Y)
```

You may block calculating statistics for any numeric field by typing “N” against the Show statistics field on the DFSMSrmm Report Controls panel

```
EDGPG051            DFSMSrmm Report Controls - COUNT06

...

Column width . . .  10 Show statistics if numeric   n   Y or N
```

© 2017 IBM Corporation

Overview

RMM: Continuation of WHILECATALOG Support

- **Problem Statement / Need Addressed**
  - Not all RMM subcommands allow the specification of WHILECATALOG and expiration time
  - Not all attributes may be included in a search
- **Solution**
  - ADDDATASET supports WHILECATALOG and EXPTM
  - ADDVOLUME and GETVOLUME support EXPTM
  - SEARCHDATASET supports WHILECATALOG, Expiration time, Last Changed time, Catalog Retained status
  - SEARCHVOLUME supports Assigned Time, Expiration Time, Last Changed time, Catalog retained status
  - SEARCHVRS supports Time Last Referenced and Last Changed Time
- **Benefits**
  - Consistency
  - Extended searching capability

© 2017 IBM Corporation

Overview

RMM: Continuation of WHILECATALOG Support *(cont)*

- **Problem Statement / Need Addressed**
  - RETPD(PERMANENT) introduced in V2R2 but not supported in all options/subcomands
  - New WHILECATALOG default options introduced in V2R2 not viewable when examining dumps in IPCS
- **Solution**
  - RETPD(PERMANENT) allowed in ADDDATASET, ADDVOLUME, GETVOLUME, CHANGEDATASET, CHANGEVOLUME RMM subcommands and the global RETPD option in EDGRMMxx.
  - The IPCS RMMDATA VERBEXIT shows the following global options of RM(EXPDT): catalog days, RETPD and WHILECATALOG for GDG data sets, RETPD and WHILECATALOG for non-GDG datasets
- **Benefits**
  - Consistency
  - Simpler to debug RMM problems using dumps

© 2017 IBM Corporation

Migration & Coexistence Considerations

RMM

- In V2R3, Common Interface Module (CIM) support will be removed from DFSMSrmm.

© 2017 IBM Corporation

Installation

RMM

- Defaults table
  - To use the Defaults Table, the DEFTABLE(xx) option must be added to the EDGRMMxx parmlib member. The defaults table must be saved in the new EDGDEFxx parmlib member.
  - A new sample script, EDGRDEF, can be used to convert an existing UXTABLE into the defaults table format. The following UXTABLE options are not supported by the defaults table in V2R3, and as such cannot be converted: POOL, ACLOPT, F1ONLY, PGM
- EDM, Reports Generator, Management Class tape attributes, WHILECATALOG
  - None

© 2017 IBM Corporation

Appendix

RMM

Books and References

z/OS DFSMSrmm Managing and Using Removable Media	SC23-6873
z/OS DFSMSrmm Implementation and Customization Guide	SC23-6874
z/OS DFSMSrmm Reporting	SC23-6875

Some useful sources for help in using ISMF/Naviquest

- *"z/OS DFSMSdfp Storage Administration", SC26-7402.*
- *Victor Liang,* "Introduction to ISMF, NaviQuest & SMS", January 15, 2015.
- *Neal Bohling, "NaviQuest – Streamlining SMS", March 10, 2014.*
- *"DFSMSrmm Implementation and Customization Guide", SC23-6874,*
  Chapter 6. Organizing the removable media library.

© 2017 IBM Corporation

Overview

VSAM RLS Replacement of AIX Upgrade Lock

- **Problem Statement / Need Addressed**
  - To keep the VSAM RLS AIX upgrade set and the base cluster in sync, currently an upgrade lock is held on the sphere, in effect making the updates to the sphere single-threaded -- unacceptably slow in the advent of the big-data era.

    The AIX upgrade lock is an EXCL lock that is held across the AIX upgrade and the corresponding base cluster. The AIX upgrade is completed before the corresponding base cluster change is made.
- **Solution**
  - Replace the AIX upgrade lock with VSAM RLS redo on the AIX Control Intervals (CIs)
- **Benefit / Value**
  - Enables concurrent update requests to spheres to improve performance of all upgrade-set update processing

© 2017 IBM Corporation

Overview

VSAM Performance Enhancement

- **Problem Statement / Need Addressed**
  - As DB2 encourages clients to create one data set per DB2 table, DB2 tables are separated out into individual data sets and the number of data sets increases dramatically. This creates a need to increase the number and performance of allocating, opening and closing large numbers of data sets per DB2 region.
- **Solution**
  - VSAM OPEN will no longer call Catalog to check for RLS_IN_USE if the opening data set is a LDS since RLS does not support LDS.
VSAM OPEN will no longer obtain ENQ “N” to indicate non-RLS processing for LDS since RLS does not support LDS.
VSAM OPEN/CLOSE will no longer chain and unchain the AMBLs for LDS that are opened through MMSRV Connect.
VSAM OPEN will obtain LPMB storage in SP205 (which is owned by the address space rather than the job step TCB) when opening through MMSRV Connect. This will improve VSM performance when freeing the storage
- **Benefit / Value**
  - Improve performance of OPEN for LDSes opened with Media Manager Services CONNECT
  - Increase the number of data sets that can be opened concurrently

© 2017 IBM Corporation

Migration & Coexistence Considerations

VSAM/VSAM RLS

- **Coexistence support to z/OS V2R2 and V2R1**
  - Only V2R3 or above will be able to take advantage of this feature. Toleration APAR OA48980 will be needed to have lower releases coexist with V2R3. The toleration APAR obtains the AIX upgrade lock as well as doing redo
- **Migration actions**
  - None

© 2017 IBM Corporation

Overview

DFSMSdss RAS

- **Problem Statement / Need Addressed**
  - DFSMSdss users of Logical Dataset Dump are currently limited to processing up to 131,070 data sets that pass their INCLUDE/EXCLUDE filter criteria. If the user exceeds this limit message ADR865E is issued indicating they must narrow the scope of their, the dump is not processed
- **Solution**
  - Increase the number of data sets that may reside on the dump to a new logical limit of 2,147,483,392 data sets.
- **Benefit / Value**
  - Customers can have more flexibility in filtering data sets for logical data set dump

© 2017 IBM Corporation

Overview

DFSMSdss RAS

- **Problem Statement / Need Addressed**
  - DFSMSdss issues message ADR383W indicating a data set was not selected for processing. This message is issued for data sets that were specified in the INCLUDE/EXCLUDE filter. The message is issued for several reasons but **without** a reason code
  - Given the current message text there is no way to determine, for example, if the ADR383W was issued because the data set does not exist or the data set is migrated. This places a burden on users of DFSMSdss to try and determine the root cause of the ADR383W themselves.
- **Solution**
  - DFSMSdss was modified to issue, along with the existing text, a reason code to explicitly indicate the reason why a data set was not selected.
- **Benefit / Value**
  - This will greatly simplify the root cause analysis for users and applications that encounter this warning.

© 2017 IBM Corporation

Migration & Coexistence Considerations

DFSMSdss RAS

- **Coexistence support to z/OS V2R2 and V2R1**
  - APAR OA51382 enables V2R1 and V2R2 to Restore dumps
  - Creating >131K logical data sets in a dump is only supported on V2R3
- **Migration actions**
  - None

© 2017 IBM Corporation

Overview

VTOC Update Safe Interface

- **Problem Statement**
  - Today, there are many ways that callers can update DSCB records in the VTOC. None of them provide any checking to insure the caller did not accidentally change fields that could corrupt the VTOC or cause the Index to be disabled.
- **Solution**
  - A new CVAFDIR ACCESS=WRITE parameter will be provided that allows the caller to update an existing format 1/8/9/3 DSCB but not allow the modification of essential fields in this record.
- **Benefit / Value**
  - Using this new parameter provides a safer way to update DSCB records in the VTOC. This may prevent accidental VTOC corruption.

© 2017 IBM Corporation

Usage & Invocation

VTOC Update Safe Interface

- Today's CVAFDIR ACCESS=WRITE interface allows the user to write a single or multiple DSCBs to the VTOC.
  - A new parameter, VALIDATE=(YES,NO) will be added to indicate that the existing DSCB(s) will be read and compared to the ones passed by the user to insure essential fields are not being modified.
- Benefit / Value
  - Using this new interface provides a safer way to update DSCB records in the VTOC.
  - The addition of a new parameter allows current users of CVAFDIR ACCESS=WRITE to easily use a safer method for changes to the VTOC.

© 2017 IBM Corporation

Usage & Invocation

VTOC Update Safe Interface

- The following fields are not allowed to be modified:
  - Format 1/8 DSCB:
    - DS1DSNAM Data set name.
    - DS1FMTID Format identifier (X'F1' or X'F8').
    - DS1NOEPV Number of extents on volume.
    - DS1EXNTS Three extent fields.
    - DS1PTRDS Pointer to first format 3 or format 9, or zero.
  - Format 9 DSCB:
    - DS9KEYID Key identifier (X'09').
    - DS9SUBTY Subtype number for format 9 (currently always X'01').
    - DS9NUMF9 Number of format 9 DSCB's for this data set.
    - DS9FMTID Format identifier (X'F9').
    - DS9NUMF3 Number of format 3 pointers that follow.
    - DS9F3   Pointers to first to tenth format 3 DSCBs.
    - DS9PTRDS Pointer (CCHHR) to next format 9 DSCB, the first format 3 DSCB, or zero.
  - Format 3 DSCB:
    - No fields in the format 3 DSCB are allowed to be modified

© 2017 IBM Corporation

Usage & Invocation

VTOC Update Safe Interface

Important CVPL, BFLE fields and new CVSTAT code

- CVPL fields (macro ICVAFPL)
  - CVCLID (4 character EBCDIC field, new with z/OS R2V2) – identifier provided by the caller of ACCESS=WRITE. This identifier is used in SMF 42 subtype 27 record field SMF42FACT (EBCDIC activity type).
  - CVFL4 DS XL1 FOURTH FLAG BYTE
    - CV4VALID EQU X'03' VALIDATE WAS SPECIFIED FOR CVAFDIR WRITE
- New CVSTAT code (passed back in the CVPL):
  - 88 - An essential field was attempted to be updated using CVAFDIR ACCESS=WRITE and VALIDATE=YES. No write occurred.
- New flag byte in the BFLE (ICVAFBFL) to indicate which buffer had the invalid update
    - BFLEVLER EQU X'40' VALIDATION ERROR OCCURRED ON THIS BUFFER

© 2017 IBM Corporation

Usage & Invocation

VTOC Update Safe Interface

Example of CVAF call with new VALIDATE parameter

```
DIRWRITE DS    0H
         CVAFDIR  ACCESS=WRITE,DEB=(R4),BUFLIST=BUFLHDR,MAPRCDS=YES,   X
               DSN=DSNAME,MF=(E,CVAFDIR),VALIDATE=YES,                 X
               MULTIPLEDSCBS=YES,EADSCB=OK
CVAFDIR  CVAFDIR MF=L              CVAFDIR MACRO PARM LIST
```

Usage & Invocation

VTOC Update Safe Interface

1. Pass a literal in the list format:

```
CVAFDIR  CVAFDIR MF=L,CVCLID='LIST',PLISTVER=2
```

2. Pass an address in the immediate format:

```
          CVAFDIR  ACCESS=WRITE,DEB=(R4),BUFLIST=BUFLHDR,MAPRCDS=YES,   X
               DSN=DSNAME,MF=I,CVCLID=CARRIEID,PLISTVER=2
          CARRIEID DC    CL4'CVN2'              MY ID
```

3. Pass a register in the execute format:

```
         LA    R11,CARRIEID            GET ADDR OF 4BYTE ID
         CVAFDIR  ACCESS=WRITE,DEB=(R4),BUFLIST=BUFLHDR,MAPRCDS=YES,   X
              DSN=DSNAME,CVCLID=(R11),MF=(E,CVAFDIR)
         CARRIEID DC    CL4'CVN2'              MY ID
         CVAFDIR  CVAFDIR MF=L,PLISTVER=2
```

Overview

VTOC Update Safe Interface

- **Problem Statement**
  - If a VTOC gets corrupted, or if something unexplained happens to a data set, it is detected far after the actual error and there is no 'real' evidence of what occurred. This makes it extremely hard to diagnose the cause.
- **Solution**
  - V2.2 provided a new SMF Record 42 sub-type 27 for DASD VTOC Operations. It captures updates to the VTOC for IBM and Vendor-built channel programs.
  - V2.3 enhances that record to provide all DSCBs that are affected by the write.
- **Benefit / Value**
  - Provides an audit log for VTOC updates
  - Helps diagnose problems when VTOC is compromised
  - Provides a comprehensive 'life of a dataset' footprint.

© 2017 IBM Corporation

Usage & Invocation

VTOC Update Safe Interface

- Writes to the VTOC are detected by DADSM and CVAF. The following functions write the enhanced SMF record:
  - DADSM functions
    - Create – shows the new DSCBs created
    - Rename – shows the format 1/8 DSCB before and after the Rename
    - Extend – shows the changed DSCBs before and after the Extend
    - Partial Release – shows the changed DSCBs before and after the release
    - Scratch – shows the DSCBs being deleted
  - CVAFDIR WRITE function – shows the DSCB(s) before and after the write. Note: The CVCLID field can be passed to CVAF to uniquely identify the writer.
- For these records, the SMF42PSV (version number) field will contain a value of 2. When the version number is 2, all DSCBs affected by the activity will be recorded. There is a DSCB change section for the OLD and the NEW DSCBs.

© 2017 IBM Corporation

Usage & Invocation

VTOC Update Safe Interface

New or enhanced SMF 42 sub-type 27 fields

Changed fields (changes in *italics*):

- SMF4227R4 - Offset to *Old* DSCB section from start of record, including record descriptor word (RDW).
- SMF4227R5 - Length of *Old* DSCB section
- SMF4227R6 - Number of *Old* DSCB sections
- SMF4227R7 - Offset to *New* DSCB section from start of record, including record descriptor word (RDW).
- SMF4227R8 - Length of *New* DSCB section
- SMF4227R9 - Number of *New* DSCB sections

New fields:

- SMF42RDSCB - Complete DSCB field added to address the entire DSCB instead of the key and the data fields having to be addressed separately.
- SMF42RDSI - Data set indicators:

	Value	Meaning
SMF42RRSV	X’80’	Data set is erase on scratch

© 2017 IBM Corporation

Installation

VTOC Update Safe Interface

- PARMLIB member SMFPRMXX keyword NOTYPE is used to identify Record Subtypes that should not be recorded.
  - Specify NOTYPE(42(27)) to disable VTOC Audit logging

© 2017 IBM Corporation

Session Summary

VTOC Update Safe Interface

- When using CVAFDIR to update existing DSCBs, use the new VALIDATE=YES parameter to safeguard from accidental modification of key DSCB fields that could result in a VTOC corruption and the inability to get to any data on that volume.
- Use CVCLID parameter to identify your CVAF updates in the SMF42/27 records.
- Record SMF 42/27 records to create an audit record of VTOC DSCB updates.

© 2017 IBM Corporation

Appendix

VTOC Update Safe Interface

Documentation:

How to use the CVAFDIR function can be found in Chapter 1. 'Using the Volume Table of Contents' of the z/OS DFSMSdfp Advanced Services book (SC23-6861)

The layout of the SMF 42/27 record can be found in z/OS MVS System Management Facilities (SMF) (SA22-7630)

© 2017 IBM Corporation

Session Summary

- **Overview of recently GA'd SPEs**
  - Transparent Cloud Tiering
  - zCDP Common Recover Queue
  - DS8K Thin Provisioning – Space Reclamation
  - DFSORT Enhancements
- **Details for DFSMS New Functions**
  - Data Set Level Encryption (V2R2 and V2R3)
  - Multiple OAM Address Spaces per LPAR
  - DFSORT UNICODE
  - RMM Enhancements
  - VSAM Enhancements
  - DFSMSdss Enhancements
  - VTOC Update Safe Interface and SMF Record

© 2017 IBM Corporation