OA66198 DFSMShsm S3 protocol support Publication Updates

Version 1.0

DFSMShsm

June 24, 2025

Table of Contents

Overview

This document describes IBM publication changes for the DFSMShsm S3 protocol support.

APAR OA66198 provides a hybrid cloud storage solution for backup and archive leveraging z/OS DFSMSdfp Cloud Data Access (CDA) to communicate with the object storage using standard S3 protocols.

z/OS DFSMShsm Implementation and Customization Guide (SC23-6869)

Chapter 12. DFSMShsm and Cloud Storage

When you prepare to use the cloud as a target for DFSMShsm functions, consider the configuration options and their supported solutions. The z/OS DFSMSdfp Cloud Data Access (CDA) can be used to manage the credentials and transfer objects. DFSMShsm requires OMVS, TCP/IP, and the CP Assist for Cryptographic Functions to be enabled for this support.

DFSMShsm supports cloud storage as a target tier for migration and full volume dump using the following solutions:

- TS7700 advanced object storage with transparent cloud tiering (TCT)
- Traditional cloud object storage with transparent cloud tiering (TCT)
- Traditional cloud object storage with CDA direct-to-cloud

OMVS segment

OMVS segment for DFSMShsm

The DFSMShsm started task user ID must have an OMVS segment defined to it. See “Identifying DFSMShsm to z/OS UNIX System Services” for details. This is required for DFSMShsm to communicate with the cloud over TCP/IP.

DFSMShsm connection to OMVS

During processing to the cloud, DFSMShsm uses services that are provided by OMVS. This causes a connection to OMVS, and DFSMShsm prevents OMVS from performing a shutdown.

If OMVS needs to be shut down for maintenance, the DFSMShsm address space must first be stopped. If OMVS is unavailable, the functions that interact with cloud are unavailable.

The DISPLAY OMVS,A=ALL console command can be used to see whether the ARCCTL load module is known to OMVS and prevents OMVS shutdown.

If DFSMShsm is started while OMVS is shut down, but cloud services are needed, the SETSYS CLOUD(NAME(*cloud_name*) REFRESH) command can be issued to reconnect DFSMShsm with OMVS and allow the functions that interact with cloud to be used.

TS7700 advanced object store with transparent cloud tiering

Tiering data to a TS7700

DFSMS can use a DS8000 to transparently tier data to a TS7700 Virtualization Engine as the object storage target. To enable TCT to a TS7700, define a cloud construct in an SMS network connection construct with the DS8000 as the endpoint or in a CDA provider file to take advantage of the multiple endpoints support. All object requests originating from DFSMS are routed through the DS8000 onto the TS7700.

TCT supports compression of data stored on the TS7700 object store. DFSMS detects data that is already compressed or encrypted with z/OS host-based methods and does not compress it.

Related reading:

- See *z/OS DFSMSdfp Storage Administration* for information on how to setup a DS8000 as an object proxy server in an SMS network connection construct.
- For information about enabling or disabling the TCT compression feature (TCTCOMPRESS) and the AOM496I status message on the console for TCT operations (AOM496I) by specifications in the DEVSUPxx member of the SYS1.PARMLIB, see *z/OS MVS Initialization and Tuning*. For using the F DEVMAN command to display or modify DEVSUP settings, see the *z/OS MVS System Commands*.
- For more information about the TS7700 object storage support, see hardware RPQ 8B3867 FC 0005 DS8000 Offload.

Using multiple endpoints

When multiple endpoint support for TCT TS7700 advanced object store is enabled, DFSMShsm allows you to specify multiple endpoints in a CDA provider file for TCT TS7700 advanced object store and provides failover function. If one endpoint failed with HWTHCONN or HTTP 500-511 Internal Server Error, DFSMShsm can get a new endpoint for this cloud and retry the failed cloud process.

The following changes are necessary to enable multiple endpoints support for TCT TS7700 advanced object store:

1. **Specify the configuration in a CDA provider file**

   You need to specify the configurations previously in the SMS network connection construct in a CDA provider file with keys including 'host', 'port', 'tctType', 'sslKey', 'sslVersion'. The 'host' key allows specifying multiple end points within 'preferred' or 'backup' JSON objects.

```
"host": {
"preferred": [
"sample.url.1",
"sample.url.2"],
"backup": [
"https://sample.url.3:8000,*AUTH",
"https://sample.url.4"]
},
"port": "8000",
"tctIdentity": "userid",
"tctType": "TAPE-OBJECT",
"sslKey": "*AUTH*/*",
"sslVersion": "TLSV12"
}
```

   A similar sample CDA provider file with required DFSMSdss json key/value pairs can be found in /usr/lpp/dfsms/dss/samples where 'cloudName', 'enableDFSMSdss', and 'supportedOperations' are not required for DFSMShsm. This sample provider file is provided as a simple example; the files in

/usr/lpp/dfsms/gdk/providers directory should be used as prevailing examples for future enhancements.

The keys, 'host', ‘tctIdentity’, 'tctType' and 'sslVersion' are required. 'port' and 'sslKey' are optional only when all of URLs specified in 'host' have them embedded. All the keys and values are case-sensitive.

This support needs CDA credentials, TCT full volume dump restore (OA60278), and multiple endpoints (OA66197) functions. When these functions have been installed on all systems in the HSMplex, include the following patch in the DFSMShsm's parmlib member ARCCMDxx for every DFSMShsm host, and restart DFSMShsm.

```
PATCH .ARCCVT.+5D7 BITS(1.1.....)
```

2. **Define the cloud provider to DFSMShsm after DFSMShsm restarts:**

   - Issue SETSYS CLOUD(NAME(*cloudname*) CDAPROVIDER) on one DFSMShsm host. If 'tctType' in the provider file is "TAPE-OBJECT', multiple endpoints support for this cloud will be enabled after creating or updating the cloud provider record based on the corresponding CDA provider file.

     If SETSYS CLOUD(NAME(*cloudname*) CDACREDENTIALS) is specified and the *cloudname*.json file is empty, or the 'tctType' is 'TCT', DFSMShsm will continue to search for the cloud definition in SMS network connection constructs.

   - Issue SETSYS CLOUD(NAME(*cloudname*) REFRESH) on all other hosts in the HSMplex.

   When the CDA provisioned password is changed or the CDA *cloudname*.json file is updated,

   - Issue SETSYS CLOUD(NAME(*cloudname*) CDAPROVIDER) on one host in the HSMplex
   - Issue SETSYS CLOUD(NAME(*cloudname*) REFRESH) on other hosts in the HSMplex.

3. **Set the maximum number of retries retrieving a new endpoint during failover processing**

   You can set the maximum number of retries retrieving a new endpoint during failover processing for a TCT TS7700 advanced object store which is defined using CDA provider file. Multiple endpoint support for TCT TS7700 advanced object store allows users to specify multiple endpoints in a CDA provider file. If one endpoint failed, DFSMShsm can get another new endpoint and retry the failed cloud process. When there are no more endpoints available, the message ARC1593I is issued. When the maximum retry times is reached or there are no more endpoints available, the corresponding cloud process will continue with the last failed endpoint.

   ```
   PATCH .MCVT.+5DC X'nn'
   ```

   The default value is X'08' (8 times of RETRY, total 9 endpoints can be used).

   Optionally, users can dictate the preference DFSMShsm uses when connecting to TCT TS7700 endpoints marked as 'Preferred', or 'Backup' in the CDA provider file with the following:

   ```
   PATCH .MCVT.+24F BITS(.......1)
   ```

   The default is OFF, meaning DFSMShsm will only use the endpoints dictated by the system symbol TCTREGION=PROD | DR where PROD indicates to use Preferred endpoints, and DR indicates to use Backup endpoints. When turned ON, DFSMShsm may use both types of endpoints (Preferred or Backup) but will favor the type indicated by system symbol TCTREGION=PROD | DR. You can define the system symbol TCTREGION in IEASYMxx parmlib member, for example:

   ```
   SYSDEF SYMDEF(&TCTREGION='PROD')
   ```

Related reading: For more information about tuning patches to enable the multiple endpoints support for TS7700 advanced object store, see the following sections in this *DFSMShsm Implementation and Customization Guide*, “tuning patches supported by DFSMShsm”.

- Allowing multiple endpoints support for TCT TS7700 advanced object store (tape object)
- Setting the maximum number of retries for retrieving a new endpoint for TCT TS7700 advanced object store

Traditional cloud object store with transparent cloud tiering

Tiering data to an S3 compatible object storage cloud

DFSMS can use a DS8000 to transparently tier data to an object storage cloud that exposes an S3 compatible API. To enable transparent cloud tiering to an S3 cloud, you can define a cloud configuration using a CDA provider file or in an SMS network connection construct.

Using CDA provider files

You can define cloud connection properties in a CDA provider file, *cloudname*.json, and designate TCT. When you specify CDAPROVIDER keyword on the SETSYS CLOUD command, it tells DFSMShsm to use the CDA provider file and CDA will obtain the credentials from the key file. When you specify “tctType”: “TCT” in the *provider*.json file, metadata objects will be transferred through CDA, and data extent objects are transferred to cloud through the DS8000.

Using SMS network connection constructs

When you define a SWIFT cloud provider in an SMS network connection construct with the DS8000 as the endpoint, all object requests originating from DFSMS are routed through the DS8000 onto the S3 cloud. The SMSPROVIDER CDACREDENTIALS keywords on the SETSYS CLOUD command tells DFSMShsm to obtain the credentials from CDA.

Provider file

The sample CDA provider files in /usr/lpp/dfsms/gdk/samples/providers directory may be used as examples. For example, *IBMCOS.json*. Specify the keys, “host”, “port”, and “region” to values of your cloud provider. To designate TCT, specify key-value pairs “tctType”: “TCT”. All the keys and values are case-sensitive.

Related reading:

- For information on how to set up a DS8000 as an object proxy server and configure in an SMS network connection construct, see *z/OS DFSMSdfp Storage Administration*.
- For more information about z/OS DFSMSdfp Cloud Data Access services and how to set up a CDA configuration, see *z/OS MVS Programming: Callable Services for High-Level Languages*.
- For information about DFSMShsm SETSYCLOUD options, see *z/OS DFSMShsm Storage Administration*.

Communicating the cloud password to DFSMShsm using CDACREDENTIALS

DFSMShsm uses the password for the user ID that is configured in the SMS network connection construct or the CDA provider file to communicate with the cloud. To communicate the cloud password to DFSMShsm with z/OS CDA, issue the SETSYS CLOUD(NAME(*cloudname)* CDACREDENTIALS) command.

Note: When the CDAPROVIDER keyword is specified on the SETSYS CLOUD command, the CDACREDENTIALS keyword is not applicable, and CDA will obtain credentials from the key file.

Security configuration for cloud storage

To allow the DFSMShsm address space to access cloud storage that uses the CDA services, the Security Server (RACF) or equivalent security product must be configured to provide both a z/OS Unix System Services group (with an associated group ID) and user (with an associated user ID) for the DFSMShsm started procedure. With CDA running in the DFSMShsm address space, access to CDA security and configuration files and encryption services must be provided by using a RACF user ID. Complete the following steps to grant CDA, DFSMShsm, and appropriate administrators access to the CDA files and encryption services.

Create the HSM home directory

1. Create a home directory for the DFSMShsm user.

   ```
   mkdir HSM_home_dir_name
   ```

2. Create subdirectories for cloud data access configuration files.

   ```
   mkdir /HSM_home_dir_name/gdk
   mkdir /HSM_home_dir_name/gdk/providers
   ```

   Note: You should use owner, group and permissions for these directories and files as recommended in “Secure the HSM home directory” on page xxx.

Create RACF HSM user and group

RACF (or equivalent) user and group IDs for DFSMShsm must be created and configured. If these steps are completed from a prior DFSMShsm file system level setup, ensure that the existing user IDs FILEPROCMAX and PROCUSERMAX settings are 50 if using both file system and cloud levels simultaneously. Otherwise, ensure that FILEPROCMAX and PROCUSERMAX are set to 25. If this user ID is to be shared across multiple DFSMShsm address spaces, the FILEPROCMAX and PROCUSERMAX settings should be 50 (or 25) multiplied by the number of HSMs sharing the user ID.

The following are example RACF commands that can be used to accomplish these steps:

1. Create a group specifically for DFSMShsm usage with a unique GID.

   ```
   ADDGROUP hsmgrpOMVS(GID(gid))
   ```

2. Create a user ID for DFSMShsm with a unique UID and assign it to the group above. Use a setting of 50 per HSM address space for both FILEPROCMAX and PROCUSERMAX if the HSM file system level is being used with the cloud level, otherwise a setting of 25 per HSM address space, if using just the cloud support. A home directory is needed to store CDA (cloud data access) configuration files.

   ```
   ADDUSER hsmDFLTGRP(hsmgrp) OWNER(hsmgrp) NAME('HSM Address Space')
   NOPASSWORD OMVS(UID(uid) FILEPROCMAX(fff) PROCUSERMAX(ppp)
   HOME(HSM_home_dir_name))
   ```

3. Associate the DFSMShsm started task with the HSM group.

```
RDEFINE STARTED HSM*.HSM* STDATA(USER(=MEMBER) GROUP(hsmgrp))
```

4. Refresh the RACF (or equivalent) profile.

```
SETROPTS RACLIST(STARTED) REFRESH
```

5. Validate the RACF (or equivalent) profile.

To validate the DFSMShsm RACF user ID UNIX setup, issue the following TSO command:

```
LISTUSER hsm OMVS
```

Example Output:

```
USER=hsm NAME=hsm                   OWNER=user   CREATED=18.337
 DEFAULT-GROUP=HSMGRP   PASSDATE=N/A    PASS-INTERVAL=N/A PHRASEDATE=N/A
 ATTRIBUTES=PROTECTED
 REVOKE DATE=NONE   RESUME DATE=NONE
 LAST-ACCESS=20.272/11:07:04
 CLASS AUTHORIZATIONS=NONE
 NO-INSTALLATION-DATA
 NO-MODEL-NAME
…
OMVS INFORMATION
----------------
UID= 0000012345
HOME= HSM_home_dir_name
CPUTIMEMAX= NONE
ASSIZEMAX= NONE
FILEPROCMAX= 00000050
PROCUSERMAX= 00000050
THREADSMAX= NONE
MMAPAREAMAX= NONE
```

To validate that the RACF user ID and group for DFSMShsm are correctly associated with the HSM address space, check the following message in the system log during DFSMShsm initialization:

```
IEF695I START HSM      WITH JOBNAME HSM      IS ASSIGNED TO USER hsm, GROUP hsmgrp
```

Create the RACF HSM administrator group

Create a RACF group for HSM administrators with a unique GID. For example, :

```
ADDGROUP hsmadminOMVS(GID(gid))
```

Add the appropriate users to this group, which includes:

1. A system administrator who is responsible for maintaining the CDA (cloud data access) configuration file in the */HSM_home_dir_name/gdk* directory. For more information, see Alter configuration file.

   /HSM_home_dir_name/gdk

2. A storage administrator who is responsible for updating the CDA (cloud data access) provider definition files that are located in */HSM_home_dir_name/gdk/providers* directory. For more information, see Alter cloud provider definition file.

   /HSM_home_dir_name/gdk/providers

3. A security (or storage) administrator is responsible for adding cloud provider access keys using the CDA (cloud data access) ISPF panels. For more information, see Add cloud provider keys.

To prevent unauthorized users from accessing DFSMShsm file system objects, you should use a separate DFSMShsm administrator group.

Copy cloud data access configuration files

Copy the CDA sample JSON files to the HSM home directory:

1. */usr/lpp/dfsms/gdk/samples/gdkconfig.json*

   should be copied to

   /HSM_home_dir_name/gdk/config.json

2. */usr/lpp/dfsms/gdk/samples/gdkkeyf.json*

   should be copied to

   /HSM_home_dir_name/gdk/gdkkeyf.json

3. */usr/lpp/dfsms/gdk/samples/providers/IBMCOS.json*

   should be copied to

   /HSM_home_dir_name/gdk/providers/IBMCOS.json

All file names, fields, and values that are contained within are case-sensitive.

Secure the HSM home directory

Configure the HSM home directory with a Unix owner, group, and permissions that allows only the HSM user ID and HSM administrator group access to the directory and files.

1. Change the permissions of the HSM home directory to 770 to allow only the owner and group read, write, and execute authority.

   ```
   chmod -R 770 /HSM_home_dir_name
   ```

2. Change the HSM home directory group to the HSM administrator group.

   ```
   chgrp -R hsmadmin /HSM_home_dir_name
   ```

3. Change the owner of the HSM home directory to the HSM user ID.

   ```
   chown -R hsm /HSM_home_dir_name
   ```

Configure the CSFKEYS general resource class

The CSFKEYS RACF (or equivalent) general resource class must be configured to allow CDA to use encryption services.

1. The CSFKEYS general resource class must be active and RACLISTed.
2. The ICSF segment of the CSFKEYS class profile CSF-PROTECTED-KEY-TOKEN (or its generic equivalent) must contain SYMCPACFWRAP(YES).

3. The DFSMShsm user ID must have READ access to the CSF-PROTECTED-KEY-TOKEN profile (or its generic equivalent).
4. Define a profile for CSFKEYS resources beginning with GDK with a universal access (UACC) of NONE.
5. The DFSMShsm user ID must have READ access to the new CSFKEYS profile for resources beginning with GDK.
6. The security administrator that enters the cloud provider keys must have READ and WRITE access to the new CSFKEYS profile for resources beginning with GDK.HSM. For more information, see “Add cloud provider keys” on page xxx.
7. The DFSMShsm user ID must have UPDATE access to the ARC. The *cloudname* key label (or all of the ARC.* key labels) in the CSFKEYS class.

Add SSL certificates

All required cloud provider SSL certificates must be added to RACF (or equivalent). The DFSMShsm user ID must be given READ access to the key ring where the certificates are stored. Only a secure HTTPS connection to the cloud provider is supported.

CDA configuration for cloud storage

CDA must be configured to provide information about and access to the cloud provider or providers that are used by DFSMShsm for cloud storage.

CDA panel library

Ensure that SYS1.DFQPLIB is part of the ISPPLIB concatenation or that the following members located in SYS1.DFQPLIB are added to an ISPPLIB library:

- GDKAPPOP
- GDKAUTHK
- GDKAUTHL
- GDKAUTHP
- GDKMAINP
- GDKOBJAC
- GDKOBJAL

Create a RACF (or equivalent) profile to ensure that only authorized users have access to these members.

Alter configuration file

The CDA configuration file, config.json, contains settings that alter CDA behavior. Currently, the only value is related to logging and error capture.

Use the default value, NONE, for the log-level setting. If necessary, DFSMShsm or CDA support requests that this value be changed to assist with problem diagnosis.

Alter cloud provider definition file

The sample cloud provider definition file, IBMCOS.json, contains fields and values which describe settings and supported operations that are related to the cloud storage provider. There can be multiple

provider definition files which might be used to define different cloud storage providers or multiple versions of the same provider (for example, an east and west region of the same provider).

Related reading: See the *z/OS MVS Programming: Callable Services for High-Level Languages* for descriptions of the keys and values.

Add cloud provider keys

Before starting this step, ensure that the security (or storage) administrator who is entering the cloud provider keys has sufficient authority to write to the *gdkkeyf.json* file *(/HSM_home_dir_name/gdk/gdkkeyf.json*) and the CSFKEYS profile for resources beginning with GDK. For more information, see “Secure the HSM home directory” and “Configure the CSFKEYS general resource class”.

From the TSO command line, issue the following command:

```
EX 'SYS1.SAXREXEC(GDKAUTHP)'
```

This starts a CDA panel where the S3 key pair is encrypted and saved.

1. Select the cloud provider that is associated with the key pair that is added by entering the associated number under the "Select Cloud Provider" heading.
2. Enter the RACF (or equivalent) user ID associated with DFSMShsm into the UserID field under the "Encryption Parameters" section.
3. If this key pair is intended to be used with a specific bucket, enter a ‘/’ followed by the bucket name in the Resource field under the "Encryption Parameters" section. Otherwise, enter a ‘/’ to indicate that this key pair is valid for any bucket that is associated with this cloud provider.

   Both specific and generic keys can be added and CDA attempts to use specific keys that are tied to buckets before using the generic key for the provider.

   Note: Only 1 generic key is used per provider. If a second is entered, it overwrites the first.
4. Press Enter to save the values.
5. Enter an ‘O’ on the top Option line to continue to the next panel.
6. Enter the Key and Secret key values into the associated fields under the “Authorization Parameters” section. Press Enter. The characters are not echoed to the screen and are displayed as * when enter is pressed.
7. Enter an ‘S’ on the top Option line to encrypt and save the key pair.

Note: The first time this panel is executed, the user can receive the following warning messages:

```
ERROR: getpwnam() error: EDC5121I Invalid argument.

ERROR: getpwnam() error: EDC5129I No such file or directory.
```

This behavior is expected because the UserID field is not populated. When the DFSMShsm user ID is created in “Security configuration for cloud storage” on page 254, “Create RACF HSM user and group” is specified at least one time, the warning messages are no longer displayed.

Delete cloud provider keys (optional)

From the TSO command line, issue the following command:

```
EX 'SYS1.SAXREXEC(GDKAUTHP)'
```

This starts a CDA panel where the S3 key pair is deleted:

1. Select the cloud provider associated with the key pair that is being removed by entering the associated number under the "Select Cloud Provider" heading.
2. Enter the RACF (or equivalent) user ID associated with DFSMShsm into the UserID field under the “Encryption Parameters” section.
3. Enter an ‘L’ on the top Option line.
4. Enter a ‘/’ next to the key to be removed.
5. Enter a ‘1’ to confirm the delete action.

Backup cloud data access files

When CDA (cloud data access) is configured, make sure that the DFSMShsm administrator makes a backup of all the files contained within the */HSM_home_dir_name/gdk* directory.

DFSMShsm configuration for cloud storage

DFSMShsm is ready to use the CDA credentials manager. Specify the SETSYS CLOUD(NAME(*network_connection_construct_name*) CDACREDS) to request DFSMShsm to provision the password that is entered by the security administrator and stored within CDA. This example of an SMS network connection definition is called PRODCLOUD. The following command allows the storage administrator to request CDACREDS option for PRODCLOUD to DFSMShsm:

```
F DFHSM,SETSYS CLOUD(NAME(PRODCLOUD) CDACREDENTIALS)
```

For more information about SETSYS CLOUD command parameters, see Cloud password in *z/OS DFSMShsm Storage Administration*.

Using CDACREDENTIALS without a Crypto Express

You might want to use the CDA support, but do not have a Crypto Express card that is installed in the processor. A flag in the MCVT can be patched ON to indicate that it is accepted that the cloud credentials are less protected by not having the encryption key that is wrapped by the main AES key in the crypto express. By patching this flag on, it indicates that you can have the encryption key that is stored in the clear in the ICSF CKDS.

To request allowing encryption key to be stored in the clear in the ICSF CKDS, issue the following PATCH command:

```
PATCH .MCVT.+597 BITS(.....1.)
```

The patch to revert this option is:

```
PATCH .MCVT.+597 BITS(.....0.)
```

Communicating the cloud password to DFSMShsm using CLOUDCREDENTIALS

DFSMShsm uses the password for the user ID that is configured in the SMS network connection construct to communicate with the cloud. To communicate the password to DFSMShsm, issue the SETSYS CLOUD command. DFSMShsm stores the password in encrypted form, in one of the control data sets, so that you can specify it only once.

Here is an example of an SMS network connection definition called PRODCLOUD. The following command allows the storage administrator to communicate the password for PRODCLOUD to DFSMShsm:

```
F DFHSM,SETSYS CLOUD(NAME(PRODCLOUD) CCREDENTIALS)
```

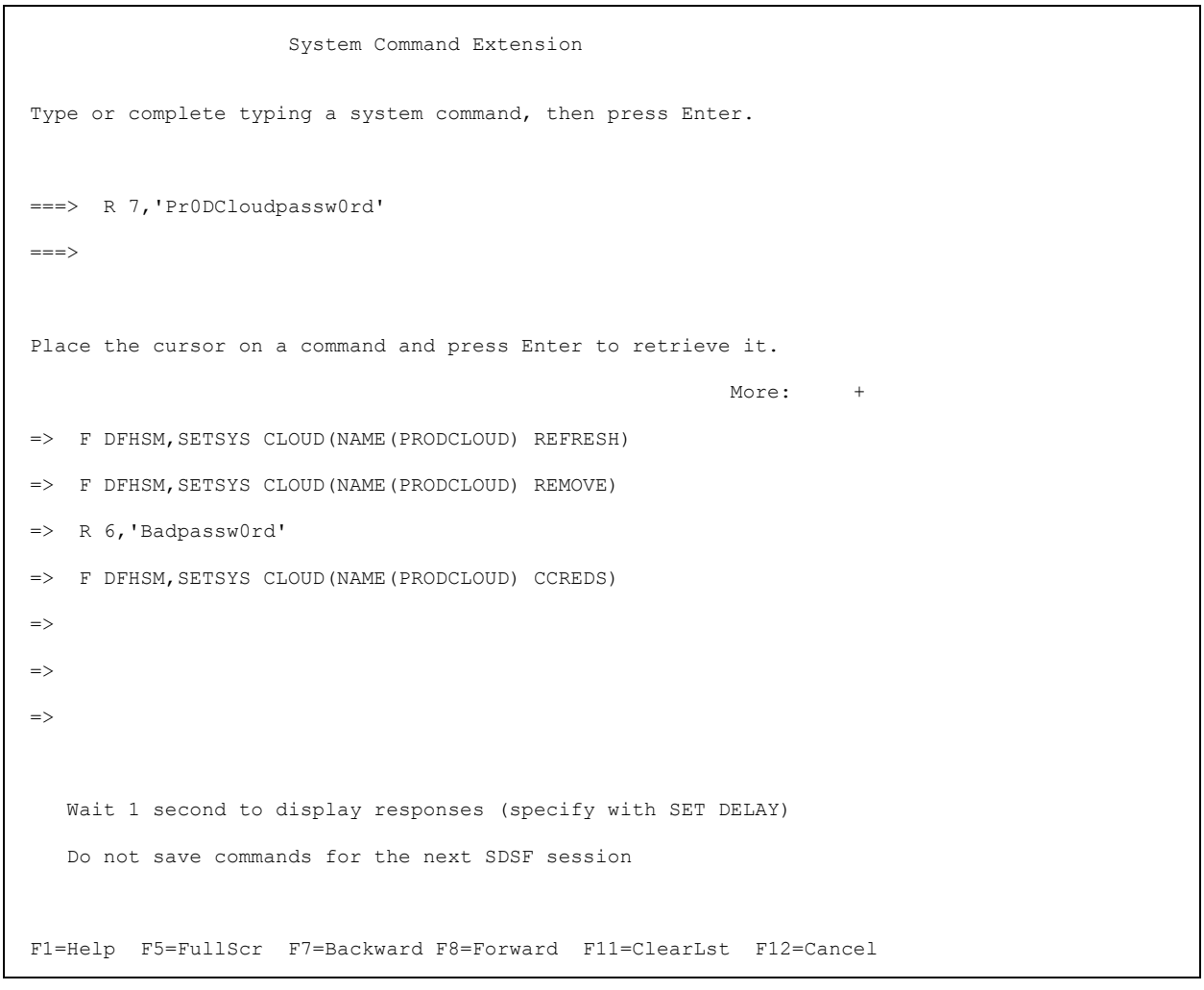
A WTOR is issued to request the password that is associated with PROCDLOUD

*0007 ARC1585A ENTER PASSWORD FOR CLOUD PRODCLOUD

Issue a reply to the WTOR from the SDSF SYSLOG system command extension. The password is case sensitive. For example, if the password for PRODCLOUD includes uppercase and lowercase letters, you must surround the password with single quotation marks and issue the request from the system command extension. Any WTOR reply that is issued from the SDSF SYSLOG is folded to uppercase by the system, regardless of the single quotation marks.

Note: Entering a forward-slash on the command input line in the SDSF SYSLOG and pressing Enter opens the system command extension.

Example:



DFSMShsm attempts to authenticate with the Cloud using the specified password. If the password is incorrect, an error message is issued. See *z/OS DFSMShsm Diagnosis* for other errors and messages that might be issued.

```
ARC1581I UNEXPECTED HTTP STATUS 401 DURING A POST FOR URI
ARC1581I (CONT.) http://prodcloud.ibm.com/v2.0/tokens/ ERRTEXT HTTP/1.1 401
ARC1581I (CONT.) Unauthorized
```

Changing the cloud password

When the password for a cloud is changed, the storage administrator must update the password that is stored by DFSMShsm. When you issue the SETSYS CLOUD(NAME(PRODCLOUD) CCREDS) command and enter the new password in response to the WTOR, the previous password is overwritten. In a multiple-image environment (multiple DFSMShsm hosts), to ensure that all DFSMShsm hosts have the updated encrypted password, you can issue the SETSYS CLOUD(NAME(PRODCLOUD) REFRESH) command to each host. Issuing this command causes the updated encrypted password to be read.

For z/OS CDA provisioned passwords, issuing the SETSYS CLOUD(NAME(PRODCLOUD) CDACREDS) or SETSYS CLOUD(NAME(PRODCLOUD) REFRESH) command will reestablish the password from z/OS CDA and update the host-encrypted password that is held in storage for this cloud provider. With the REFRESH option specified, all the passwords from z/OS CDA are reestablished.

Cleaning up the cloud password

It might become necessary to clean up some of the DFSMShsm stored information for cloud. For passwords provisioned with the CCREDS keyword (WTOR), the information is stored in the MHCR record. A storage administrator can use the FIXCDS S MHCR DISPLAY command to display the MHCR. The cloud information entries can be found at the end of the record, where the cloud name is in plain text, and the password is encrypted.

The SETSYS CLOUD(NAME(*OldEntry*) REMOVE) command can be used to remove entries from the cloud information that is known to DFSMShsm.

The SETSYS CLOUD(NAME(*AnyEntryName*) REFRESH) command is used to refresh all in storage cloud information that is known to DFSMShsm. The basis for the refresh is the current MHCR records or the S XC-*cloudname* records in the MCDS. These records describe cloud information that is known to DFSMShsm.

Traditional cloud object store with CDA

You can define cloud connection properties in a CDA provider file and designate a direct-to-cloud connection. When you specify the CDAPROVIDER keyword on the SETSYS CLOUD command, it tells DFSMShsm to use the CDA provider file and CDA will obtain the credentials from the key file.

Before defining the cloud provider to DFSMShsm, some configuration needs to be performed to set up and use CDA services. The security configurations are similar to the setup steps described in the “traditional cloud object store with TCT” section. The following sections describe the requirements for using CDA.

Note: This support requires the CDA credentials and TCT full volume dump restore functions be enabled through the patch below in the ARCCMDxx parmlib member for all hosts in the HSMplex:

```
PATCH .MCVT.+5D7 BITS(1.......)
```

Using CDA – security administrator

Follow the “system administrator configuration quick-start” steps 1 and 2 in the *z/OS MVS Programming: Callable Servies for High-Level Languages* to set up the following:

1. Configure the CSFKEYS general resource class to protect the keylabels created by CDA

```
/* Define a generic label with UACC(NONE) so default access is NONE */
RDEFINE CSFKEYS GDK.** UACC(NONE) ICSF(SYMCPACFWRAP(YES) SYMCPACFRET(YES))

/* Define a generic label specific to the DFSMShsm user ID */
RDEFINE CSFKEYS GDK.DFHSM.** UACC(NONE) ICSF(SYMCPACFWRAP(YES) SYMCPACFRET(YES))

/* Permit both the DFSHSMuser ID and the user ID configuring CDA to their keylabels */
PERMIT GDK.DFHSM.** CLASS(CSFKEYS) ID(DFHSM) ACCESS(UPDATE)
PERMIT GDK.DFHSM.** CLASS(CSFKEYS) ID(storage_admin) ACCESS(UPDATE)
SETROPTS RACLIST(CSFKEYS) CLASSACT(CSFKEYS) REFRESH
```

2. PERMIT read access to the following CSFSERV class resources to both DFSMShsm user ID and the user ID configuring CDA on behalf of the DFSMShsm user ID
   - CSFKGN
   - CSFRNGL
   - CSFKRD
   - CSFKRC2
   - CSFOWH (CSFKTB2 if ALLOW_NO_CEX)
   - CSFRNG
   - CSFIQA

Note: You might need to add root and any intermediate certificates that signed the cloud storage provider certificates to your security product.

Using CDA – storage administrator

Configure CDA for the user ID the DFSMShsm started task is running under.

CDA uses the following files during its processing:

Key file contains the encrypted cloud credentials for the user.

gdkkeyf.json

1. Create a gdk/ directory in the DFSMShsm user ID’s home directory and set the permissions to 770.
2. Copy /usr/lpp/dfsms/gdk/samples/gdkkeyf.json to ~/gdk/gdkkeyf.json and set the permissions to 660.

Config file contains some configuration used during the saving of the cloud credentials.

config.json

1. Copy /usr/lpp/dfsms/gdk/samples/gdkconfig.json to ~/gdk/config.json and set the permissions to 660.

Provider file contains configuration specific to a Cloud Object Store provider.

provider.json

1. Create a providers/ directory in the DFSMShsm user ID's home directory and set permissions to 770.
2. Create your *cloudname.json* and set permissions to 660. There are several samples provided in /usr/lpp/dfsms/gdk/samples/providers

Note:

The permissions described above are different than what are documented in the *z/OS MVS Programming: Callable Servies for High-Level* Languages because you are setting this up for the user ID the DFSMShsm server runs under.

The user ID that is configuring CDA for DFSMShsm must be part of group that has write access to the DFSMShsm user ID home directory and the files created underneath it.

Related reading: See "user configuration quick-start" in the *z/OS MVS Programming: Callable Servies for High-Level Languages*.

Provider file

The sample provider files in /usr/lpp/dfsms/gdk/samples/providers directory may be used as examples. For example, *IBMCOS.json*. Specify the keys, "host", "port", and "region" to values of your cloud provider. To designate a **direct-to-cloud** connection, do not specify key-value pairs for "tctType". All the keys and values are case-sensitive.

The following supportedOperations must be present:

- GETOBJECT
- GETLARGEOBJECT
- WRITEOBJECT
- WRITELARGEOBJECT
- LISTOBJECT
- DELETEOBJECT
- CREATEBUCKET
- DELETEBUCKET
- LISTBUCKETS

If you encounter memory shortages during direct-to-cloud data transfer operations, the "multipartChunksize" and "multipartThreshold" values may be reduced to 5 megabytes from the values used in the sample provider file:

```
"httpMethod": "GET",
```

```
"multipartChunksize": "5242880",
  :
"name": "WRITELARGEOBJECT",
"multipartChunksize": "5242880",
"multipartThreshold": "5242880",
```

If you encounter errors during direct-to-cloud data transfer operations due to large data extents, the “multipartChunksize” and “multipartThreshold” values in the provider fil may be increased to process large data objects.

```
"name": "GETLARGEOBJECT",
"multipartChunksize": "22020096",
"multipartThreshold": "8388608",
  :
"name": "WRITELARGEOBJECT",
"multipartChunksize": "22020096",
"multipartThreshold": "8338608",
```

Configure cloud credentials

From the TSO command line, issue the following command:

```
EX 'SYS1.SAXREXEC(GDKAUTHP)'
```

This starts a CDA Authorization Utility panel where the S3 key pair is encrypted and saved.

1. Select the cloud provider that is associated with the key pair that is added by entering the associated number under the "Select Cloud Provider" heading.
2. Enter the RACF (or equivalent) user ID associated with DFSMShsm into the UserID field under the "Encryption Parameters" section.
3. Enter an ‘O’ on the top Option line to continue to the next panel.
4. Enter the Key and Secret key values into the associated fields under the “Authorization Parameters” section. Press Enter. The characters are not echoed to the screen and are displayed as * when enter is pressed.
5. Enter an ‘S’ on the top Option line to encrypt and save the key pair.

   CDA will encrypt the username and password with a keylabel it creates, and the key is stored in ICSF. By default, it will ‘wrap’ the key used to encrypt the credentials using the master key of a Crypto Express adapter.

```
                  z/OS Cloud Data Access Authorization Utility
Option  ===> S
    S Save Resource Authorization            C Clear Secret Key Field
                                                (for hidden input)
Encryption Parameters
   Provider . . . S3CLOUD
   KeyLabel . . . GDK.DFHSM.S3CLOUD
   Keystore . . . /u/dfhsm/gdk/gdkkeyf.json
   Resource . . . /


Authorization Parameters
   Key  .  userid

   Secret Key . ********



Enter the Key and Secret Key used to access the specified Cloud Provider.
```

Using CDA credential store without Crypto Express

If the system does not have any Crypto Express configured as CCA co-processor, you might see an error when saving the resource authorization.

```
ERROR: encryptKeys: Unable to generate a key. CSNBKGN rc: 12, rsn:0000
```

If you see this error, you can set allow-no-CEX to true in config.json, then CDA will store the key in ICSF in the clear in the ICSF CKDS.

If you don't have CEX adapters and set allow-no-CEX to true but still see this `CSNBKGN rc: 12, rsn:0000` error, it could be caused by using a fixed length record format. You can check the format of your CKDS with LISTCAT.

If SETSYS CLOUD failed with message ARC1584I below, you can request allowing encryption key to be stored in the clear in the ICSF CKDS.

```
ARC1584I SETSYS CLOUD - NO CRYPTO EXPRESS CARD IS INSTALLED
```

To request allow-no-CEX, issue the following DFSMShsm PATCH command:

```
PATCH .MCVT.+597 BITS(......1.)
```

The patch to revert this option is:

```
PATCH .MCVT.+597 BITS(......0.)
```

Diagnosing errors when accessing the cloud

Incorrect CDA credentials

CDA credentials are used for various cloud operations. If a denied access response (HTTP 403) is received during SETSYS CLOUD command processing, it might be caused by incorrect CDA credentials. For example:

```
SETSYS CLOUD(NAME(IBMCOS) CDAPROVIDER)
```

```
ARC0300I **OPER** ISSUED===>SETSYS CLOUD(NAME(IBMCOS) CDAPROV)
ARC1594I Z/OS CLOUD . ACCESS ENCOUNTERED AN ERROR
ARC1594I (CONT.) WHILE PERFORMING GDKLIST  SERVICE, RETURN CODE=901
ARC1594I (CONT.) RETURN CODE TRANSLATION=Denied access (HTTP 403)
ARC1594I (CONT.) FOR CLOUD IBMCOS
ARC1594I (CONT.) CONTAINER /
ARC0100I SETSYS COMMAND COMPLETED - CLOUD(NAME(IBMCOS...
```

Related reading: For other errors and messages that might be issued, *see DFSMShsm Diagnosis*.

DFSMSdss is unable to read the key file

If the required setup has not been completed, DFSMSdss might not be able to locate the gdkkeyf.json file. For example, the user ID of DFSMShsm is DFHSM, whereas DFSMSdss is not running under the user ID DFHSM while running in cross memory mode. The cloud operation might fail with the following error:

```
ADR617E (001)-CDAI (08), Z/OS CLOUD DATA ACCESS ENCOUNTERED AN ERROR
WHILE PERFORMING A GDKINIT SERVICE, RETURN CODE 100
        RETURN CODE TRANSLATION: Unable to read the keyfile
```

Ensure the following setup has been completed for DFSMShsm to invoke DFSMSdss in cross-memory mode.

- Configure DFSMShsm to invoke DFSMSdss as a started task.
- Create a profile under the RACF ‘STARTED’ class.
- Name of the profile should be ARC*.*, because the address space identifiers are ARC*n*MIGR for migration function, ARC*n*DUMP for full volume dump, and ARC*n*RST*y* for full volume restore in cross-memory mode, where ‘n’ = Host ID.
- Refresh the STARTED class after adding this new profile to activate it.

Related reading: For more information, see “configuring DFSMShsm to invoke DFSMSds as a started task” and “DFSMSdss address spaces started by DFSMShsm” sections in the z/OS DFSMShsm Implementation Guide

Data object size exceeds the size limit

CDA uses the multipartChunksize and multipartThreshold values specified in the provider file when retrieving or sending an object. If the data object size exceeds the size limit imposed by the provider file specifications, the cloud operation might fail with the following error:

```
ADR617E (001)-CDAI (02), Z/OS CLOUD DATA ACCESS ENCOUNTERED AN ERROR
WHILE PERFORMING A GDKWRITE SERVICE, RETURN CODE 801
        RETURN CODE TRANSLATION: Web toolkit returned a bad return code
        FOR OBJECT: objprefix/dsn/DTPVOLD01/NVSM/EXTENTS
        HWTHRQST RETURN CODE: 00000106
        HWTHRQST DIAGAREA: Socket closed by remote partner
```

Related reading: For more information about z/OS DFSMSdfp Cloud Data Access services and provider file, see *z/OS MVS Programming: Callable Services for High-Level Languages*.

Using cloud object store in DFSMShsm functions

You can define cloud properties in CDA provider files or SMS network connection constructs. DFSMShsm uses the attributes of a specified cloud definition to manage data set migration, recall, full volume dump restore, and provide secondary functions.

- The SETSYS CLOUD command parameters further designate a particular cloud configuration that DFSMShsm uses to store migration copies of data sets and dump copies of full volumes. The SETSYS CLOUD CDAPROVIDER option tells DFSMShsm to use the CDA provider file and CDA will obtain the credentials from the key file. The SETSYS CLOUD command supports the SMSPROVIDER CDACREDENTIALS option to request that DFSMShsm obtain the password from CDA for the cloud defined in an SMS network connection construct.

  Enable the CDACREDENTIALS and cloud full volume dump support by specifying the following PATCH in the ARCCMDxx parmlib member for all hosts in an HSMplex, then restart the DFSMShsm hosts:

  ```
  PATCH .MCVT.+5D7 BITS(1.......)
  ```

  If you have multiple DFSMShsm hosts in an HSMplex, SETSYS PLEXNAME(*hsmplex_suffix*) must be specified in the ARCCMDxx parmlib member following the PATCH described above. Specify the same *hsmplex_suffix* name for all non-FILE mode hosts in the HSMplex.

  The SETSYS optional parameters CLOUDMIGRATION allow specification of fast subsequent migration (FSM) for data set migrated to storage in the cloud.

- The MIGRATE and HMIGRATE commands include an optional keyword, CLOUD(*cloudname*). When this keyword is specified, the named data set, or data sets on the named volume is migrated to the requested cloud. The *cloudname* specified must match an existing SMS cloud network connection name or an existing CDA provider file name.

  Automatic space management uses SMS management class to manage data set migration. The management class attributes can designate a cloud object store as migration target. Secondary space management can manage cloud migration dump copies and delete inactive empty migration containers.

- The DEFINE DUMPCLASS command includes optional keywords, TAPE | CLOUD(*cloudname*) and UNASSIGNTAPE. TAPE | CLOUD specifies whether the volumes should be dumped to tape or offloaded to the designated cloud object store. UNASSIGNTAPE specifies that DFSMShsm unassign any TAPE dump volumes that are empty and are currently added to this (existing) dump class.

  Note: The CLOUD(*cloudname*) specified on the DEFINE DUMPCLASS command must have already been defined to DFSMShsm via a prior SETSYS CLOUD command.

- The BACKVOL DUMP, RECOVER FROMDUMP, FRBACKUP DUMP | DUMPONLY, FRRECOV FROMDUMP, and automatic dump functions will dump to or restore from cloud object store when designated by a CLOUD dump class. When multiple dump copies are made concurrently, each copy is associated with a different dump class. DFSMShsm supports up to 5 TAPE dump classes in a dump generation whereas dumping to cloud object store supports a single CLOUD dump class in a dump generation. Multiple CLOUD dump classes and mixed CLOUD and TAPE dump classes within a dump generation are not supported. Data set restore from a full-volume CLOUD dump copy is not supported.

- The DDELETE command can be used to delete specified non-copy pool dump copies residing in cloud storage. This command is intended for occasional cloud dump copy deletion and is not designed for bulk deletion. Use of automatic dump expiration to manage dumps and inactive empty dump container deletion is recommended.

- The LIST commands display information about data sets migrated to cloud storage, volumes dumped to cloud storage, as well as the cloud storage that DFSMShsm has used. The CLOUD optional

keyword for DATASET SELECT will cause DFSMShsm to list only those data sets that have been migrated to cloud storage.

- The QUERY NETWORK command displays TS7700 TAPE-OBJECT cloud endpoint statistics known to DFSMShsm. It does not display endpoints for S3 cloud providers.
- The REPORT command can display information about data sets migrated to cloud storage. The TOCLOUD and FROMCLOUD optional parameters on MIGRATION and RECALL respectively allow selection of records where cloud storage was involved.
- AUDIT command processing includes migrated data sets and full volume dumps that are stored in the cloud storage. AUDIT MEDIACONTROLS supports the CLOUD(*cloudname*) parameter. This function audits control information contained in migration copies and dump copies that reside in the cloud storage. The cloudname refers to a defined SMS network connection construct name or CDA provider file name.

Related reading: See z/OS *DFSMShsm Storage Administration* for information about the commands and parameters.

Enabling fast subsequent migration to cloud

With fast subsequent migration, data sets that are recalled from the cloud (but not changed or re-created), can be reconnected to the original migration copy in the cloud. This reconnection eliminates unnecessary data movement that results from remigration. Reconnection can occur during individual data set migration, or during volume migration. Reconnection is supported only in a SETSYS USERDATASETSERIALIZATION environment.

To enable fast subsequent migration for data sets that are recalled from the cloud, you can issue the SETSYS CLOUDMIGRATION(RECONNECT(ALL)) command.

Note: DFSMShsm performs fast subsequent migration only when the data set has not changed since recall. DFSMShsm determines this change based on flags in the format 1 DSCB that are set when the data set is recalled. This allows DFSMShsm to be compatible with other backup applications, as DFSMShsm no longer relies on the change bit in the format 1 DSCB, which can be set or reset by other data set backup products.

Special considerations

Using CDA configuration or SMS configuration

You can define cloud object storage for DFSMShsm use with one of the following two configuration methods. Consider the solutions supported by each configuration method:

- CDA provider file
  - TS7700 TAPE-OBJECT storage with TCT with multiple endpoints support. With DS8000 as an object proxy, all objects are transferred through the DS8000.
  - Traditional cloud object store with TCT. Metadata objects are transferred through CDA. Data extent objects are transferred to cloud through the DS8000.
  - Traditional cloud object store with CDA direct-to-cloud. All objects are transferred through a direct-to-cloud connection.

  With a CDA cloud configuration, DFSMShsm does not store the credentials for traditional cloud providers. DFSMShsm will store the password obtained from CDA for a TS7700 cloud provider in the same ways as the CDACREDENTIALS option. IBM recommends the CDA configuration method.

- SMS network connection construct
    - TS7700 TAPE-OBJECT storage with TCT. Multiple endpoints support is unavailable. With the DS8000 as an object proxy, all objects are transferred through the DS8000.
    - Traditional cloud object store with TCT. With the DS8000 as an object proxy, all objects are transferred through the DS8000.

  With an SMS cloud configuration, DFSMShsm supports CDACREDENTIALS or CLOUDCREDENTIALS options to manage passwords.

    - CDACREDENTIALS – DFSMShsm obtains the password for the cloud construct from CDA where the password has been entered by the security administrator. DFSMShsm will store the encrypted password for future cloud requests. IBM recommends the CDACREDS option when using an SMS cloud configuration.
    - CLOUDCREDENTIALS – DFSMShsm requests the password associated with the object storage account from the security administrator using WTOR. DFSMShsm will encrypt and store the password for future cloud requests.

Related reading:

- For information on how to set up a DS8000 as an object proxy server in an SMS network connection construct, see *z/OS DFSMSdfp Storage Administration*.
- For more information about z/OS DFSMSdfp Cloud Data Access services and how to set up a CDA configuration, see *z/OS MVS Programming: Callable Services for High-Level Languages*.
- For information about DFSMShsm SETSYCLOUD options, see *z/OS DFSMShsm Storage Administration*.

Incompatibilities caused by cloud provider configuration changes

When the cloud provider properties are changed, it could cause incompatibilities resulting in loss of access to data processed before the configuration changes. IBM recommends defining a new cloud provider name when the changes are incompatible.

SMS configuration and CDA configuration

DFSMShsm does not support transitioning an existing cloud defined in the SMS network connection construct with SWIFT protocol to a CDA cloud provider file with a same name using TCT or DIRECT, or vice versa. For example, if you REMOVE the existing cloud definition and define the same cloud name in CDA configuration, DFSMShsm will no longer be able to recall or restore objects previously migrated or dumped with the SMS cloud definition.

Recommendation: Define the SMS cloud network connection and CDA provider file under different cloud names.

CDA TCT and DIRECT data movement methods

Data moved with CDA TCT and DIRECT are incompatible because the data formats are different.

Recommendation: Use different CDA provider file names for CDA TCT and DIRECT data transfer methods.

Regions and endpoints in provider files

If you change the region in an existing cloud provider file, you might lose access to the existing buckets created using previously specified region.

Recommendation:

- Use multi-region endpoints or cross-region global endpoints when they are available.
- Use different cloud provider names for different regions.

z/OS DFSMShsm Managing Your Own Data (SC23-6870)

Chapter 23. HMIGRATE: Migrating data sets

Optional parameters

CLOUD: Specifying migration of a data set directly to cloud storage

Explanation

CLOUD is an optional parameter specifying that a data set migrates from an SMS managed volume to the requested cloud storage. The specified *cloud_name* is the CDA provider file name or the name of the network connection construct. When the cloud name is specified, the data set is migrated to the requested cloud storage regardless of the data set management class attributes, with the exception when migration is not allowed. The CLOUD parameter is valid only for SMS-managed data sets.

The CLOUD parameter cannot be specified with the following parameters:

MIGRATIONLEVEL1, MIGRATIONLEVEL2, and CONVERT.

Note: When you perform a Migrate to cloud storage, the following DFSMShsm SETSYS settings do not apply:

COMPACT, COMPACTPERCENT, COMPACT(ALL)

Migrating a data set to cloud storage ignores any current COMPACT setting. If the data set is being migrated to a cloud object storage that supports transparent cloud tiering compression, the data set can be compressed by TCT compression if it is not already compressed, encrypted, or compressed and encrypted.

CONVERSION(REBLOCKTOANY)

Because data movement is not performed by the host, there is no opportunity to perform re-blocking of a data set.

CONCURRENT

Migrating a data set to cloud storage ignores any current setting that relates to CONCURRENT.

Chapter 29. Using DFSMShsm user macros

ARCHMIG: Migrating data sets

Optional parameters

<Update the description of CLOUD parameter as shown below. This text includes the OA67601 DOC update.>

CLOUD

specifies the address of a 32-byte area containing a 2-byte field indicating the length of the cloud name followed by a 30-byte field indicating the cloud name. The specified cloud name must match the name of a CDA provider file or an SMS network connection construct.

The data is migrated to the specified cloud storage which overrides any other specification in the management class of the data set other than eligibility for migration. Non-SMS managed data sets are not eligible for migration to cloud storage. The name must be left-aligned and padded with blanks. The CLOUD keyword cannot be specified with MIGLVL.

z/OS DFSMShsm Storage Administration (SC23-6871)

Chapter 2. Space management of SMS-managed storage

Automatic space management operation examples

Automatic primary space management

Compaction or zEDC compression during migration

Update the first sentence of the existing last paragraph and add a new paragraph about SETSYS ZCOMPRESS(CLOUDMIGRATE(YES)) as shown below:

...

If the data set is being migrated to a cloud object store defined in the SMS network connection construct that supports transparent cloud tiering compression, then the data set can be compressed by TCT compression if it is not already compressed, encrypted, or compressed and encrypted. If the migrated data set is TCT compressed, then the percentage of space saved for the data set is stored in the MCDS and FSR records. DFSMS selects a TCT compression capable primary volume when the TCT compressed migrated data set is recalled.

If the data set is being migrated to a DIRECT cloud provider defined with a CDA provider file and SETSYS ZCOMPRESS(ALL | CLOUDMIGRATE(YES)) has been specified, DFSMShsm will request CDA compression to be used during migration.

Command space management tasks

Reconnecting data sets using fast subsequent migration

Add the following bullet item under “requirements that must be satisfied when a fast subsequent migration reconnect is attempted on the data set are:”

- The cloud provider definition has not changed since the previous migration, or the cloud provider properties remain compatible.

Chapter 4. Other space management considerations

Object storage in the cloud

DFSMShsm can use object storage in the cloud as a destination for migrated data set images. When data movement is offloaded to the storage controller, other management functions are performed directly using the z/OS Client Web Enablement Toolkit or the z/OS DFSMSdfp Cloud Data Access (CDA) services. Using object storage in the cloud allows DFSMShsm to avoid extra processing such as RECYCLE.

System set up to use the cloud

For DFSMShsm to use the cloud, you must first set up your system. You can find the requirements and configuration options in the *z/OS DFSMShsm Implementation and Customization Guide*.

- For transparent cloud tiering (TCT), DASD volumes in a DS8700 or higher with TCT need to be attached to the system. Only data sets that reside on a device with transparent cloud tiering can be migrated to the cloud through DFSMShsm.
- <Delete the bullet item about configuring SMS.>

DASD volumes

For TCT, ensure that the first volume in an LSS that other volumes are attached from is attached to the system. Failure to do this can lead to attention messages from the DS8000 being missed.

SETSYS

<No change to the existing text.>

When DFSMShsm is enabled, it reconnects eligible data sets without performing data movement. If SETSYS CLOUDMIGRATION(RECONNECT(NONE)) is in effect, a subsequent migration of a data set that was otherwise eligible to be reconnected, causes the previous migration copy to be deleted and a new migration copy created.

Cloud password

With an SMS cloud configuration, DFSMShsm supports CDACREDENTIALS or CLOUDCREDENTIALS options to manage passwords.

- CDACREDENTIALS – DFSMShsm obtains the password for the cloud construct from CDA where the password has been entered by the security administrator. DFSMShsm will store the encrypted password for future cloud requests. IBM recommends the CDACREDS option when using an SMS cloud configuration.

- CLOUDCREDENTIALS – When the CLOUDCREDENTIALS option is specified on the SETSYS CLOUD command to provide DFSMShsm with the cloud password for the user ID that is defined in the SMS network connection construct, great care needs to be taken with this password. DFSMShsm keeps the password in encrypted form for later use. Anyone with access to this password can access the cloud directly and delete the migration copies, thus making DFSMShsm unable to recall those data sets. It is recommended that the security administrator issue this command to protect the access to the cloud.

With a CDA provider configuration, DFSMShsm does not store the credentials for traditional cloud providers. DFSMShsm will store the password obtained from CDA for a TS7700 cloud provider in the same way as the CDACREDENTIALS option.

Using the cloud

Workload distribution with TCT

<Existing text is not changed.>

Chapter 40. DEFINE command

Optional parameter of the DEFINE command

DUMPCLASS(CLOUD | TAPE): Specifying where the dump copies to reside

<Update the existing description of the CLOUD parameter. Delete “(when OA66197 enabled)”.>

DUMPCLASS(TAPE | CLOUD): Specifying where the dump copies to reside

<**Delete this section** located before the “examples of how to code the DEFINE command” heading. It is a duplicate of the ‘DUMPCLASS(CLOUD | TAPE) section.>

DUMPCLASS(ZCOMPRESS): Specifying whether to use zEDC Services on the dump data

<Add new paragraphs about CDA compression to the existing descriptions of the ZCOMPRESS parameter as shown below :>

Explanation: ZCOMPRESS is an optional subparameter specifying whether DFSMSdss is to use zEDC Services on the dump data.

Subparameter	Explanation
ZCOMPRESS(YES)	**DUMPCLASS(ZCOMPRESS(YES))** When YES is specified, compression with zEDC will be performed if this function is

	supported by the system. If zEDC Services are not available, the other compression type will be used. For a CLOUD dump class, CDA compression with zEDC Services will be used when a DIRECT cloud provider is specified in the CLOUD parameter.
ZCOMPRESS(NO)	**DUMPCLASS(ZCOMPRESS(NO))** When NO is specified, compression with zEDC will not be performed. ZCOMPRESS(NO) can be specified to override an existing setting of ZCOMPRESS(YES). For a CLOUD dump class, CDA compression will not be used when a DIRECT cloud provider is specified in the CLOUD parameter.

Default: When ZCOMPRESS is not specified and was not previously set in the existing dump class definition, NO is used by default.

Chapter 58. QUERY command

Optional parameter of the QUERY command

<Update the NETWORK description with a “Note” item after “Defaults”.>

NETWORK: Displaying cloud endpoint statistics known to DFSMShsm

Explanation: NETWORK is an optional parameter requesting DFSMShsm to output informational statistical data about known cloud endpoints.

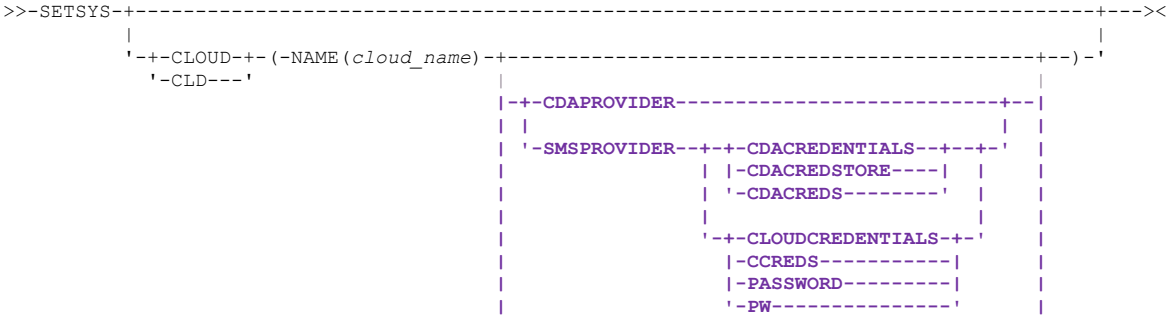
Defaults: None.

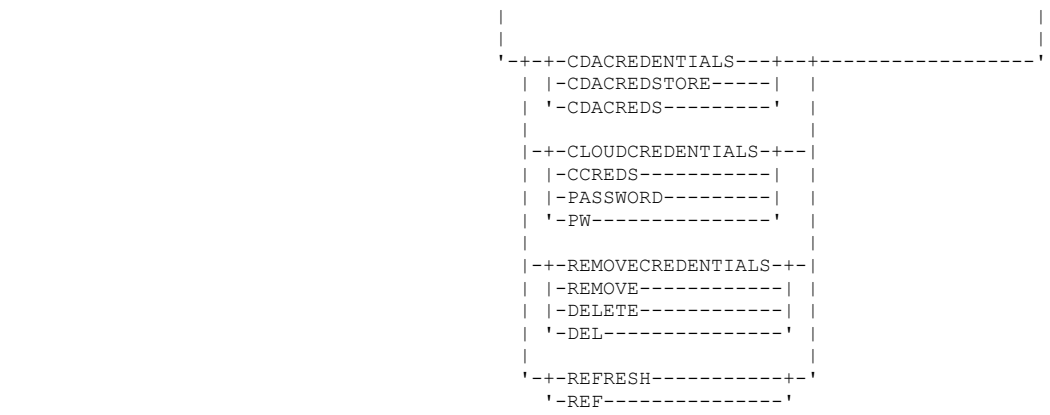
Note: DFSMShsm does not display endpoints information for S3 cloud providers.

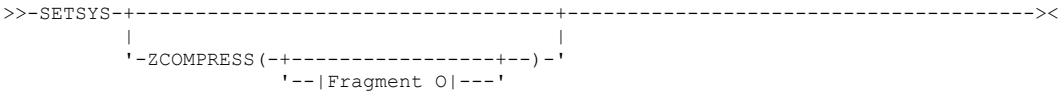
Chapter 65. SETSYS command

<Update the syntax diagram of SETSYS CLOUD and ZCOMPRESS command parameters as shown below.>

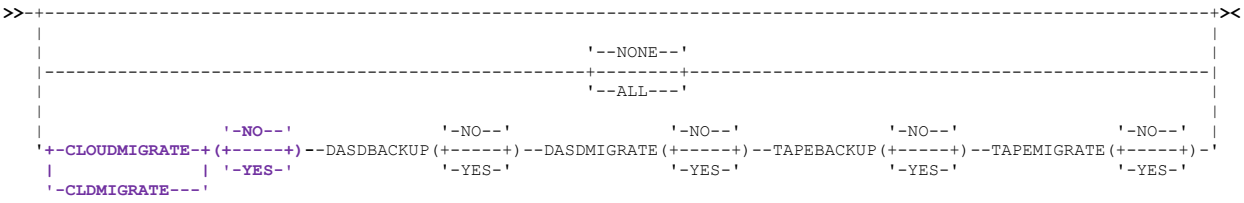
Syntax of the SETSYS command







O: ZCOMPRESS optional parameters



Optional parameter of the SETSYS command

CLOUD: Specifying CLOUD properties

<Update the existing keyword descriptions and add new optional keywords, CDAPROVIDER and SMSPROVIDER, as described below. The updates are highlighted in purple.>

CLOUD is an optional parameter that allows specification of properties specific to a particular Object Storage that DFSMShsm uses to store full volume dump and migration copies of data sets. If specified in a DFSMShsm parmlib member, this parameter is ignored.

The following are required and optional keywords for the CLOUD parameter*:*

NAME(*cloud_network_connection_name*)

cloud_network_connection_name is the name of a defined SMS Cloud Construct or a CDA provider file. This is an optional parameter when REFRESH is specified. Otherwise, this is a required parameter.

If the specified name does not exist in the current SMS configuration nor in the CDA providers directory, the command does not succeed.

CDACREDENTIALS

<No change.>

CLOUDCREDENTIALS

<No change.>

REMOVECREDENTIALS

<No change.>

REFRESH

<No change.>

CDAPROVIDER and SMSPROVIDER

CDAPROVIDER and SMSPROVIDER are mutually exclusive keywords specifying whether DFSMShsm should look for cloud information in a CDA provider file or an SMS network connection construct. When REMOVE or REFRESH is specified along with CDAPROVIDER or SMSPROVIDER, CDAPROVIDER and SMSPROVIDER keywords are ignored.

CDAPROVIDER specifies cloud provider properties are defined in a CDA provider file. DFSMShsm looks for a CDA provider file with the specified CLOUD name. When a valid, non-empty provider file is found, DFSMShsm will use CDA API for cloud operations. If a valid CDA provider file is not found, the SETSYS CLOUD command fails.

When DFSMShsm is obtaining information from a CDA provider file, the **tctType** key field is checked to determine how to connect to the cloud object store.

- **TAPE-OBJECT:** When tctType value specifies “TAPE-OBJECT” in the CDA provider file, it describes a TS7700 advanced object store. DFSMShsm supports multiple endpoints for TS7700 advanced object store if the functionality has been enabled. All data is moved through the DS8000 cloud proxy using either FICON or Ethernet connections.
- **TCT:** When tctType value species “TCT” in the CDA provider file, the connection type is CDA TCT. All user data is moved through the DS8000 cloud proxy using FICON connections. All metadata and utility operations go through the storage cloud via Ethernet instead of using the DS8000 proxy.
- When tctType is not specified in the CDA provider file, the connection type is **DIRECT to cloud**. DFSMShsm uses CDA API to transfer both metadata and user data extents via Ethernet connections.

Alias: CDAPROV

SMSPROVIDER specifies cloud provider properties are defined in an SMS network connection construct and DFSMShsm should not look for a valid, non-empty CDA provider file. When SMSPROVIDER is specified, either CCREDS or CDACREDS must also be specified.

Alias: SMSPROV

Defaults: When neither CDAPROVIDER nor SMSPROVIDER is specified, DFSMShsm does the following when the designated cloud is a TS7700 TAPE-OBJECT store:

- When multiple endpoints support functionality has been enabled, DFSMShsm first looks for a valid, non-empty CDA provider file with the name of a TS7700 TAPE-OBJECT store in order to provide multiple endpoints support. If a valid, non-empty CDA provider file is not found, DFSMShsm will continue to look for an SMS network connection construct for the specified cloud, and multiple endpoints support is unavailable.
- When multiple endpoints support is not enabled, DFSMShsm uses cloud information defined in the SMS network connection construct.

Related reading:

- For more information about multiple endpoints support, see *z/OS DFSMShsm Implementation and Customization Guide*, “Allowing multiple endpoints support for TCT TS7700 advanced object store”.
- For more information about using CDA provider files and associated key credentials, see *DFSMShsm Implementation and Customization*, Chapter 12 “DFSMShsm and cloud storage”

DSSXMMODE: Specifying whether DFSMSdss will be loaded in its own address space using the cross memory interface, or in the DFSMShsm address space

<Add a new note item as shown below.>

Notes:

4. When migrating, dumping, or restoring data using CDA DIRECT cloud connections, DFSMSdss will always be loaded in its own address space.

DUMPIO: Specifying the DFSMSdss DASD I/O buffering technique

<Add a new note item as shown below.>

Notes:

5. DUMPIO applies to migration and full volume dump to DIRECT cloud connections. It is ignored during other cloud operations.

ZCOMPRESS: Specifying when compression with zEDC should be done

<Add new optional subparameter “CLOUDMIGRATE(YES | NO)” to the list in the existing ZCOMPRESS parameter descriptions as shown below:>

Explanation: ZCOMPRESS is an optional parameter that you use to specify the type of compression used during migration or backup for all data sets.

The subparameters of the ZCOMPRESS parameter follow this discussion in alphabetical order. The following are optional subparameters:

- ALL | NONE
- CLOUDMIGRATE(YES | NO)
- DASDBACKUP (YES | NO)
- DASDMIGRATE (YES | NO)
- TAPEBACKUP (YES | NO)
- TAPEMIGRATE (YES | NO)

<Add a new “ZCOMPRESS(CLOUDMIGRATE(NO | YES))” section as described below before the existing “ZCOMPRESS(DASDBACKUP(NO | YES))” section.>

ZCOMPRESS(CLOUDMIGRATE(NO | YES)): Specifying whether to use CDA compression for data sets during migration to DIRECT cloud connections

Explanation: CLOUDMIGRATE (NO | YES) are mutually exclusive, optional subparameters of the ZCOMPRESS parameter, specifying whether or not to use CDA compression with zEDC Services when DFSMShsm migrates to DIRECT cloud.

Subparameter	Explanation
CLOUDMIGRATE(NO)	DFSMShsm does not use CDA compression for migration to DIRECT cloud connections.
CLOUDMIGRATE(YES)	DFSMShsm will use CDA compression with zEDC Services during migration to DIRECT cloud connections, if this function is supported by the system. If CDA compression is unavailable, the data sets will not be compressed during migration to DIRECT cloud connections.

SMS relationship: SMS-managed data sets are supported for migration to CLOUD. This parameter is inapplicable for non-SMS-managed data sets.

SETSYS default: None.

DFSMShsm default: If you do not specify either subparameter on any SETSYS ZCOMPRESS command, the DFSMShsm default is CLOUDMIGRATE(NO).

Notes:

1. As compressed-format data sets are already compressed, they are not compressed with CDA compression during migration to DIRECT cloud connections.
2. Since encrypted data sets do not compress, CDA compression will not be used during migration to DIRECT cloud connections.
3. You can run the SETSYS ZCOMPRESS(CLOUDMIGRATE(NO|YES)) command in the ARCCMDxx parmlib member conditionally by specifying ONLYIF HSMHOST. This allows you to run the command only on designated DFSMShsm hosts.

Related reading: For more information about the ONLYIF command, see ***z/OS DFSMShsm Storage Administration***, chapter 56 “ONLYIF command”.

Chapter 75. Using the AUDIT command

Using the enhanced audit command to audit DFSMShsm control information

Using the AUDIT MEDIACONTROLS(CLOUD) command

Errors detected when using AUDIT MEDIACONTROLS for cloud storage

<Update the existing section “For migrated data set images”. Add a bullet as below: >

- If there is a data set record in the MCDS:
  - ...
  - If both MCDF_CLD_CDA_TCT and MCDF_CLD_DIRECT flags are ON, AUDIT reports *ERR 231 with the data set name.

Summary of errors detected by the enhanced AUDIT commands

<Update Table 72 with new or changed error codes highlighted.>

Error Number	ABARS	CPCTL	DSCTL (BACKUP)	DSCTL (MIG)	DSCTL	MEDCTL (SDSP)	MEDCTL	VOLCTL (BACKUP)	VOLCTL (MIG)	VOLCTL (RECOV)
:										
*ERR 204		D								
*ERR 205		D								
*ERR 206							D			
*ERR 207							C			
*ERR 208							C			
*ERR 209							D			
*ERR 210							C			
*ERR 211							C			
*ERR 215		D					D			
*ERR 216							C			
*ERR 217		D					D			
*ERR 218		D					D			
*ERR 219		D					D			
*ERR 220							D			

***ERR 221**							D			
***ERR 222**							D			
***ERR 230**							D			
***ERR 231**							**D**			

Error codes (*ERR) and diagnosis

<Update Table 76. “Error codes used in AUDIT reports” with *ERR 231. Add a new item in the ERR 215 description.>

Description	**AUDIT Repair Action**	**Troubleshooting Hints**
***ERR 215 THE DGN RECORD** *DGNkey* **IS FOR A CLOUD DUMP BUT CONTAINS INVALID VALUES**		
Invalid values might include: 1. Cloud dump flag DGNF_CLOUD is 0. 2. DGNCOPY# is greater than maximum number of allowed in a dump generation. 3. DGNNVSN is not 0. 4. DGN_CLOUD_NAME_LEN and DGN_CLOUD_NAME are inconsistent. 5. DGN TCT compression ratio is invalid. 6. Dump class name in DGNDCL is incorrect. 7. Container name in DGN record is incorrect. 8. More than one DGN cloud provider type indicators are set to 1. For example, both DGNF_CLD_CDA_TCT and DGNF_CLD_CDA_DIRECT flags are set to 1.		command to identify invalid values and then use FIXCDS G *dgnkey* PATCH offset command to change the fields with expected values. Or contact IBM support.
:		
***ERR 231 THE MCD RECORD *MCDkey* IS FOR A CLOUD MIGRATION COPY BUT CONTAINS INVALID VALUES**		
More than one MCD cloud provider type indicators are set to 1. For example, both MCDF_CLD_CDA_TCT and MCDF_CLD_DIRECT are both ON.		Use the FIXCDS D *mcdkey* DISPLAY *offset* command to identify invalid values and then use FIXCDS D mcdkey PATCH offset command to change the field with expected values. Or contact IBM support.

Chapter 77. Using the QUERY command

<Add the following QUERY NETWORK output messages for TS7700 TAPE-OBJECT cloud:>

NETWORK

- ARC0101I QUERY NETWORK COMMAND STARTING ON HOST=*host*
- ARC1590I CLOUD *cloud_name* ENDPOINTS AND STATISTICS
- ARC1591I ENDPOINT=*endpoint*, PORT=*port*, PREFERENCE=PREFERRED|BACKUP, STATUS=GOOD|BAD|UNKNOWN. ACTIVE CONNECTIONS=*number_of_active_connections*
- ARC0101I QUERY NETWORK COMMAND COMPLETED ON HOST=*host*

SETSYS

<Update the existing QUERY SETSYS output message ARC0340I as shown below:>

- ...
- ARC0340I COMPACTION OPTIONS ARE: TAPEMIGRATION=[YES | NO], DASDMIGRATION=[YES| NO], TAPEBACKUP=[YES | NO], DASDBACKUP=[YES | NO], TAPEHARDWARECOMPACT=[YES| NO], ZCOMPRESS OPTIONS ARE: TAPEMIGRATE=[YES|NO], DASDMIGRATE=[YES|NO], TAPEBACKUP=[YES|NO], DASDBACKUP=[YES|NO], **CLOUDMIGRATE[YES|NO]**

z/OS DFSMShsm Data Areas (GC14-7504)

The following DFSMShsm control data set structures and internal control blocks will be updated. New or changed fields are highlighted in bold purple.

DGN – Dump generation record

<Update the existing chapters 13 and 14. “Chapter 14 DGN – Cloud definition” content should be part of Chapter 13 – Dump Generation Record. Delete Chapter 14 and update chapter 13 as shown below. Moved and new fields added by OA66198 are highlighted in bold.>

```
-------------------------------------------------------------------------------------------------
      Offsets
 Actual    FIXCDS    Type      Len     Name                 Description
 -------------------------------------------------------------------------------------------------
   :
  65(41)    1(1)    1... ....         DGNF_RESUMING        Used by FRB DUMPONLY processing, while
                                                            processing.
                    .1.. ....         DGNF_COPYPOOL        When set to 1, DGN is for copy pool volume.
                    ..1. ....         DGNF_ZCOMP           When set to 1, zEDC compression is requested
                                                            for this volume.
                    ...x xxxx         *                    Reserved


   :
 192(C0)  128(80) FIXED         4    DGNFBID              File block ID where copy starts on volser
```

```
                                                    DGNDVSN(1). Only valid when DGNFLSEQ is
                                                    greater than or equal to two.
196(C4)  132(84) CHARACTER   16   *                 Reserved.
212(D4)  148(94) CHARACTER  244   DGNVLIST          Volume list.
212(D4)  148(94) FIXED        4   DGNNVSN           Number of dump volume serial numbers
                                                    that contain part of this dump copy.


The following volume list, within the DGNDCPYS array, contains 40 entries. Each entry consists
of the following field:

216(D8)  152(98) CHARACTER  6(40) DGNDVSN          A 40-element array consisting of 6-byte fields.
                                                    It contains the volume serial numbers that
                                                    contain part of this dump copy. Volumes are
                                                    recorded in the volume sequence order of
                                                    the dump copy when the dump copy was created.


The following cloud information exists when DGNF_CLOUD is set to 1 indicating the dump copy resides
in cloud object storage.

 212(D4)  148(94) STRUCTURE  244   DGN_DUMP_TARGET     DGN dump target

 212(D4)  148(94) FIXED        4   *                  Reserved

 216(D8)  152(98) STRUCTURE  120   DGN_CLOUD_INFO     DGN cloud information exists if the dump

                                                      Copy exists in the cloud object storage.

 216(D8)  152(98) FIXED        2   DGN_CLOUD_NAME_LEN  Length of cloud network connection name
 218(DA)  154(9A) CHARACTER   30   DGN_CLOUD_NAME      cloud network connection name
 248(F8)  184(B8) CHARACTER   44   DGN_CONTAINER_NAME  Name of Container
 292(124) 228(E4) FIXED        4   DGN_OBJ_NUMBER      Number of objects stored (not including
                                                      multi-part objects)
 296(128) 232(E8) CHARACTER   44   DGN_PBJPFX_NAME     Cloud object prefix name. Dump copy ds name
 340(154) 276(114) BITSTRING   2   DGN_CLD_FLAGS       Cloud flags
                  1... ....        DGNF_CLD_COMP       When set to 1, dump copy data is TCT compressed
                                                      compressed.
                  .1.. ....        DGNF_CLD_ENCRYPT    When set to 1, dump copy data is TCT encrypted
                  ..1. ....        DGNF_CLD_CDA_TCT    When set to 1, data was moved by CDA TCT
                  ...1 ....        DGNF_CLD_CDA_DIRECT When set to 1, data was moved by CDA DIRECT
                  .... xxxx        *                   Reserved
 342(156) 278(116) FIXED       1   DGN_CLD_COMP_PRCNT  Percent of space saved by TCT compression.
                                                      Valid when DGNF_CLD_COMP=ON
 343(157) 279(117) CHARACTER 113   *                  Reserved

 ------------------------------------------------------------------------------------------
```

FSR – Function statistical record

<Update the FSR structure as highlighted below in bold:>

```
------------------------------------------------------------------------------------------
    Offsets
Decimal (Hex) Type       Len  Name               Description
------------------------------------------------------------------------------------------
  :

 298 (12A)    BITSTRING    1  FSRFLG6            More flags.
              1... ....       FSRFMB             When set to 1, FSRBYTR and FSRBYTW are in Mbytes
              .1.. ....       FSRFXPLC           When set to 1, indicates that the data set being
                                                 expired is from Cloud storage.
              ..1. ....       FSRUNIXF           When set to 1, the record is for a UNIX file
```

```
                                                 and name area is after FSRTAPE information.
              ...1 ....       FSRF_COMP          When set to 1, indicates the data set was
                                                 already compressed prior to DFSMShsm migration.
                                                 FSR_USER_DATASIZE and FSR_COMP_DATASIZE are valid.
|             .... 1...       FSRF_ZEDC          When set to 1, indicates the data set was
|                                                 compressed by zEDC or by CDA compression with
|                                                 zEDC during migration.
|                                                 FSR_ZEDC_COMPRESS_PRCNT holds the percentage
|                                                 of compression for DASD or TAPE migration.
|             .... .x..       *                  Reserved
              .... ..1.       FSRF_CLD_COMP      When set to 1, data was TCT compressed.
              .... ...1       FSRF_CLD_ENCRYPT   When set to 1, data was TCT encrypted.
  299 (12B)   BITSTRING    1  FSRFLG7            More flags.
              1... ....       FSRF_CLOUD         When set to 1, record is for TCT full volume
                                                 dump or restore (cloud).
|             .1.. ....       FSRF_CLD_CDA_TCT   When set to 1, record is for a CDA TCT
|                                                 cloud provider.
|             ..1. ....       FSRF_CLD_CDA_DIRECT When set to 1, record is for a CDA DIRECT
|                                                 Cloud provider.
|             ...x xxxx       *                  Reserved.
  :
 ---------------------------------------------------------------------------------------------
```

FSR2 – Function statistical record for RMM reporting

<Update the FSR2 structure as highlighted below in bold:>

```
 ---------------------------------------------------------------------------------------------
     Offsets
 Decimal (Hex) Type       Len  Name               Description
 ---------------------------------------------------------------------------------------------
   :
  382 (17E)    BITSTRING    1  FSR2FLG6           More flags.
               1... ....       FSR2FMB            When set to 1, FSRBYTR and FSRBYTW are in
                                                  Megabytes.
               .1.. ....       FSR2FXPLC          When set to 1, expired data set is from
                                                  cloud storage.
               ..1. ....       FSR2UNIX           When set to 1, record is for a UNIX file.
               ...1 ....       FSR2F_COMP         When set to 1, indicates the data set was
                                                  already compressed prior to DFSMShsm migration.
                                                  FSR2_USER_DATASIZE and FSR2_COMP_DATASIZE
                                                  are valid.
|              .... 1...       FSR2F_ZEDC         When set to 1, indicates the data set was
|                                                  compressed by zEDC or by CDA compression with
|                                                  zEDC during migration.
|                                                  FSR2_ZEDC_COMPRESS_PRCNT holds the percentage
|                                                  of compression for DASD or TAPE migration.
|              .... .x..       *                  Reserved
               .... ..1.       FSR2F_CLD_COMP     When set to 1, data was TCT compressed.
               .... ...1       FSR2F_CLD_ENCRYPT  When set to 1, data was TCT encrypted.
  383 (17F)    FIXED        1  FSR2FLG7           More flags.
               1... ....       FSR2F_CLOUD        When set to 1, record is for TCT full volume
                                                  dump or restore (cloud).
|               .1.. ....       FSR2F_CLD_CDA_TCT  When set to 1, record is for a CDA TCT
|                                                  Cloud provider.
|               ..1. ....       FSR2F_CLD_CDA_DIRECT When set to 1, record is for a CDA DIRECT
|                                                 Cloud provider.
|               ...x xxxx       *                  Reserved
  :
 ---------------------------------------------------------------------------------------------
```

MCA – Migration control data set alias entry record

<Update the MCA structure as highlighted below in bold:>

```
-------------------------------------------------------------------------------------------------
     Offsets
Actual    FIXCDS    Type      Len    Name                 Description
-------------------------------------------------------------------------------------------------
  :
 497(1F1) 433(1B1) CHARACTER   3   MCD_MCDX_KEY_SUFFIX Last three bytes of the MCDX key when

  66(42)    2(2)   CHARACTER   2   *                   Reserved.
  66(42)    2(2)   BITSTRING   1   *                   This byte contains the following flags:
                   1... ....       MCAFRETV            When set to 1, this is a 'Retained' MCA
                                                       record and MCA_RETAINED_DATA structure
                                                       is valid.
  67(43)    3(3)   CHARACTER   1   *                   Reserved.
  68(44)    4(4)   CHARACTER  44   MCAINTNM            Migration control data set alias entry
                                                       record key, which is the name of the
                                                       user data set.
| 112(70)   48(30)  CHARACTER   0   MCAEND              End of core MCA record
  112(70)   48(30)  STRUCTURE 180   MCA_RETAINED_DATA   'Retained' MCA information Valid only
                                                       if MCAFRETV = ON
  112(70)   48(30)  STRUCTURE 128   MCA_RETAINED_CLOUD  Cloud related info of migration copy.
  112(70)   48(30)  FIXED       2   MCA_RETAINED_CLOUD_NAME_LENGTH
                                                       Length of cloud name
  114(72)   50(32)  CHARACTER  30   MCA_RETAINED_CLOUD_NAME
                                                       Name of cloud migration copy is on
  144(90)   80(50)  CHARACTER  44   MCA_RETAINED_CONTAINER_NAME
                                                       Container name migration copy is stored in
  188(BC)  124(7C)  FIXED       4   MCA_RETAINED_OBJ_NUMBER
                                                       Cloud object number

| 192(C0) 128(80)   BITSTRING   1   MCA_RETAINED_CLOUD_FLAGS
|                                                      Flags propagated from MCD
|                   1... ....       MCAF_RETAINED_CLOUD_CDA_TCT
|                                                      When set to 1, data was moved by CDA TCT
|                   .1.. ....       MCAF_RETAINED_CLOUD_CDA_DIRECT
|                                                      When set to 1, data was moved by CDA DIRECT
|                   ..xx xxxx       *                   Reserved

| 193(C1)  129(81)  CHARACTER  47   *                   Reserved
  240(F0)  176(B0)  STRUCTURE   8   MCA_RETAINED_REMIGRATE_TD
                                                       Timestamp of data set remigration to cloud
  240(F0)  176(B0)  CHARACTER   4   MCA_RETAINED_REMIGRATE_TIME
                                                       TOD in microseconds
  244(F4)  180(B4)  CHARACTER   4   MCA_RETAINED_REMIGRATE_DATE
                                                       Date of remigrate, '0CYYDDDS' hexadecimal
  248(F8)  184(B8)  CHARACTER  44   MCA_RETAINED_NEXT@  Key of next oldest 'Retained MCA record,
                                                       or all 0x00 if oldest 'Retained' MCA record
-------------------------------------------------------------------------------------------------
```

MCD – Migration control data set data set record

<Update the MCD structure as highlighted below in bold:>

```
-------------------------------------------------------------------------------------------------
     Offsets
Actual    FIXCDS    Type      Len    Name                 Description
-------------------------------------------------------------------------------------------------
  :
```

```
  497(1F1) 433(1B1) CHARACTER   3   MCD_MCDX_KEY_SUFFIX Last three bytes of the MCDX key when
                                                       its key was compressed. Valid when
                                                       MCDF_MCDX_KCONV is set on.
  500(1F4) 436(1B4) FIXED       1   MCD_CLD_COMP_PRCNT  Percent of space saved by TCT compression
                                                       During migration. Valid when MCDF_CLD_COMP=1.
  501(1F5) 437(1B5) BITSTRING   1   MCDFLGS5            This byte contains the following flags:
                    1... ....       MCDF_CLD_ENCRYPT    When set to 1, data set was TCT encrypted
                                                        during migration.
                    .1.. ....       MCDFRMVR            When set to 1, 'Retained' MCA records exist
                                                        that are associated to this MCD record.
                                                        MCDX_RETAINED_MCA_LNKLST is valid to
                                                        reference.
|                   ..1. ....       MCDF_CLD_CDA_TCT    When set to 1, data was moved by CDA TCT
|                   ...1 ....       MCDF_CLD_CDA_DIRECT When set to 1, data was moved by CDA DIRECT
|                   .... xxxx       *                   Reserved
| 502(209) 438(1B6) CHARACTER  18   *.                  Reserved
  520(208) 456(1C8) CHARACTER   0   MCDEND              End of record.

 ------------------------------------------------------------------------------------------------
```

MCVT – Management Communication Vector Table

<Update the MCVT structure as highlighted below in bold:>

```
--------------------------------------------------------------------------------------------------
    Offsets
 Decimal (Hex) Type       Len  Name                 Description
 ------------------------------------------------------------------------------------------------
   :
  661 (295)    BITSTRING    1  *                    This byte contains the following flags:
               1... ....       MCVTFITW            When set to 1, the dynamic allocation option
                                                   for input tape volumes is to wait for a unit
                                                   to become available. When set to 0, the option
                                                   is NOWAIT.
               .1.. ....       MCVTFOTW            When set to 1, the dynamic allocation option
                                                   for output tape volumes is to wait for a unit
                                                   to become available. When set to 0, the option
                                                   is NOWAIT.
               ..1. ....       MCVTFYTW            When set to 1, the dynamic allocation option for
                                                   input and output tape volumes during recycle
                                                   processing is to wait for a unit to become available.
                                                   When set to 0, the option is NOWAIT.
|              ...1 ....       MCVTF_CLOUD_CDAAPI  When set to 1, CDA API capability is available.
               .... 1...       MCVTF_AUXHOST_ABARS_MSG
                                                   When set to 1, ABARS message already issued
               .... .1..       MCVTF_ZCOMPBT       When set to 1, zEDC compression when backup to tape.
               .... ..1.       MCVTF_ZCOMPMT       When set to 1, zEDC compression when migration to tape.
               .... ...1       MCVTF_CLOUD_PSWD_SET  When set to 1, at least one Cloud password is set.
 662 (296)     BITSTRING    1  *
               1... ....       MCVTFRDK            When set to 1, check whether automatic primary
                                                   Space management should be restarted.
               .1.. ....       MCVTFRDI            When set to 1, automatic primary space management
                                                   Is being restarted from the point of interruption.
                                                   It is not started from the beginning.
               ..1. ....       MCVTFQSP            When set to 1, the migration control task is being
                                                   dispatched to check the space on a volume. This
                                                   is done as a result of a QUERY SPACE command.
               ...1 ....       MCVTF_DISABLE_DVC   When set to 1, allow users to disable the dynamic
                                                   Volume change function during DFSMShsm startup.
                                                   This bit is not part of PSM start/restart control
                                                   flags.
                .... 1...      MCVTF_ZCOMPMC       When set to 1, CDA compression using zEDC
```

```
                                                  when migrating to CDA DIRECT cloud provider.
                .... .xxx      *                  Reserved.
   :
   :
1492 (5D4)      CHARACTER    4  MCVT_TRACEFLG       Trace flags
                1... ....       MCVTF_TRTTOC       When set to 1, enable TTOC debug traces
                .1.. ....       MCVTF_AUDE45       When set to 1, enable AUDIT ERR45.
                ..1. ....       MCVTF_TVT_NSA      When set to 1, tasks wait during TVT rebuild
                ...1 ....       MCVTF_MCBR_IS      When set to 1, allow MCBR insert date time
                .... 1..        MCVTF_CAT_RSTOR_VS When set to 1, enable cataloging of a single-volume
                                                   VSAM data set restored from dump
                .... ..1..      MCVTF_WEBTKDBG     When set to 1, enable Web Toolkit Verbose messages
                .... ..1.       MCVTF_WEBTKDBGU    When set to 1, enable items that are normally
                                                   redacted to be logged
|               .... ...1       MCVTF_CDAS3DBG     When set to 1, enable debug PDA traces in HSM CDA
|                                                   processing
   :
```

```
 The MCLOUD extension (MCLOUDX) contains global control block information about Cloud servers that
 are defined to DFSMShsm with passwords provisioned from z/OS CDA (SETSYS CLOUD CDACREDS). This
 extension supports up to 255 different cloud servers. Each cloud provider name is further defined
 to have specific cloud properties for each DFSMShsm function supporting cloud. It supports up to
 8 functions. Currently supports: Slot 1 is Migration. Slot 2 is Dump.

   0 (0)        STRUCTURE       *                  MCLOUDX
   :
  55 (37)       BITSTRING    4  MCLDX_FLAGS Flags
|               1... ....       MCLDXF_VALID       When set to 1, the cloud entry is valid.
|               .1.. ....       MCLDXF_PW_CDA      When set to 1, the password is from CDA.
|               ..x. ....       *                  Reserved
|               ...1 ....       MCLDXF_CDATAPE     When set to 1, the entry describes a TAPE-OBJECT
|                                                   cloud defined with a CDA provider file.
|               .... 1...       MCLDXF_CDA_TCT     When set to 1, the entry describes a CDA TCT
|                                                   cloud provider
|               .... .1..       MCLDXF_CDA_DIRECT  When set to 1, the entry describes a CDA DIRECT
|                                                   cloud provider
|               .... ..1.       MCLDXF_CDAPROV     When set to 1, CDAPROVIDER was specified on
|                                                   the SETSYS CLOUD command
|               .... ...1       MCLDXF_SMSPROV     When set to 1, SMSPROVIDER was specified on
|                                                   the SETSYS CLOUD command
   :
```

MWE – Management Work Element

<Update the MCVT structure as highlighted below in bold:>

```
-------------------------------------------------------------------------------------------------
     Offsets
 Decimal (Hex) Type         Len  Name                Description
 -----------------------------------------------------------------------------------------------
   :
| 263 (107)    BITSTRING     1  MWEFLG9             More MWE flags.
   :
| 264 (108)    BITSTRING     1  MWEFLG12            More MWE flags. This field is kept in sync
|                                                   with the first byte of MCLDX_FLAGS for
|                                                   cloud operations.
|              xxx. ....        *                  Reserved for CDA cloud processing
|              ...1 ....        MWEF_CDA_TAPEOBJ   When set to 1, migration target is
|                                                   CDA TAPE-OBJECT cloud
|              .... 1...        MWEF_CDA_TCT       When set to 1, migration target is
|                                                   CDA TCT cloud
|              .... .1..        MWEF_CDA_DIRECT    When set to 1, migration target is
|                                                   CDA DIRECT cloud
```

```
|              .... ..1.       MWEF_CDAPROV        When set to 1, associated cloud is
|                                                  defined with SETSYS CDAPROVIDER
|              .... ...1       MWEF_SMSPROV        When set to 1, associated cloud is
|                                                  defined with SETSYS SMSPROVIDER
| 265 (109)    CHARACTER    1  *                   Reserved
   :
-------------------------------------------------------------------------------------------
```

UTILP – DFSMShsm data collection interface

<Update the UTILP structure as highlighted below in bold:>

```
-------------------------------------------------------------------------------------------
     Offsets
 Decimal (Hex) Type       Len  Name                 Description
 -------------------------------------------------------------------------------------------
   :
  216  (D8)    STRUCTURE   80  UM_CLD_INFO          MCD extension for CLOUD info
  216  (D8)    SIGNED       2  UM_CLOUD_NAME_LENGTH CLOUD name length
  218  (DA)    CHARACTER   30  UM_CLOUD_NAME       CLOUD name
  248  (F8)    CHARACTER   44  UM_CONTAINER_NAME   CLOUD container name
  292 (124)    SIGNED       4  UM_OBJ_NUMBER       Number of objects stored
  296 (128)    FIXED        1  UM_CLD_COMP_PERCENT Percent of space saved by TCT compression.
                                                   Valid when UM_CLD_COMP=ON
| 297 (129)    BITSTRING    1  UMFLAG5             Information flag #5
|              1... ....       UM_CDA_TCT         When ON, data was moved with CDA TCT
|              .1.. ....       UM_CDA_DIRECT      When ON, data was moved with CDA DIRECT
|              ..1. ....       UM_CDA_ZEDC        When ON, CDA compression was requested
|                                                  During migration to DIRECT cloud connection
|              ...x xxxx       *                  Reserved
| 298 (12A)    CHARACTER   30  *                   Reserved space
  328 (148)    CHARACTER   96  UMENCRYPTA
  328 (148)    CHARACTER    2  UMENCRPT
  330 (14A)    FIXED       64  UMENCRPL
  394 (18A)    CHARACTER   30  UMENCRPR
  424 (1A8)    CHARACTER    0  UMMDSIE             END OF DCUMCDS
-------------------------------------------------------------------------------------------
```

XC – Cloud provider record

<Update the XC structure as highlighted below in bold:>

```
-------------------------------------------------------------------------------------------
      Offsets
 Actual    FIXCDS   Type      Len    Name                Description
 -------------------------------------------------------------------------------------------
   :
   68(44)    4(4)   BITSTRING  4     XCPR_FLAGS Flags
|                   1... ....        XCPRF_VALID         When set to 1, the record is valid.
|                   .1.. ....        XCPRF_CDA_PW        When set to 1, the password is from z/OS CDA.
|                   ..1. ....        XCPRF_PW_WTO        When set to 1, the password is from WTOR.
|                   ...1 ....        XCPRF_CDA_TAPE      When set to 1, the record describes a TAPE-OBJECT
|                                                         cloud defined with a CDA provider file.
|                   .... 1...        XCPRF_CDA_TCT       When set to 1, the record describes a CDA TCT
|                                                         cloud provider.
|                   .... .1..        XCPRF_CDA_DIRECT    When set to 1, the record describes a CDA
|                                                         DIRECT cloud provider.
|                   .... ..1.        XCPRF_CDAPROV       When set to 1, CDAPROVIDER was specified on
```

```
|                                                    the SETSYS CLOUD command
|                  .... ...1       XCPRF_SMSPROV     When set to 1, SMSPROVIDER was specified on
|                                                    the SETSYS CLOUD command

|The following CCREDS password information exists when XCPRF_PW_WTO is set to 1.

   72(48)    8(8)    STRUCTURE 80    XCPR_CLDPW          Encrypted password area.
   :

|The following CDACREDS password information exists when XCPRF_PW_WTO is set to 1.

   72(48)    8(8)    STRUCTURE 80    XCPR_CLDPW_CDA      Encrypted password area.
   :
   :
```

---

z/OS DFSMShsm Diagnosis (GC52-1387)

Chapter 8. Diagnosing from return codes and reason codes

Return code processing

<Update Table 3 with new and changed entries for OA66198 as described below:>

Table 3. Entries that pass error codes to ARCERP

Error Code	Process Level	Description of Problem
ARCAUDCS		
4nn	Debug	Parameter list is not valid.
ARCCDDSS		
68	Debug	Unknown DFSMSdss error. Return code 68. Reason code 9999.
76	Snap	ABEND occurred in the LINK macro while loading DFSMSdss.
400	Debug	Parameter list is not valid.
ARCCLSRV		
16	Debug	z/OS client web enablement toolkit encountered an internal error during cloud operations.
400	Debug	Invalid macro ID.
401	Debug	No function specified.
402	Debug	More than one function specified.
403	Debug	Check password input bad.
404	Debug	Invalid object name (Delete object function).
405	Debug	Invalid input for Retrieve Object.

406	Debug	Invalid input for List Prefix.
407	Debug	No ZWEBP pointer passed in continuous mode.
408	Debug	Count object request with blank object or container name.
409	Debug	List object request with blank object or container name.
ARCCMDSS		
68	Debug	Unknown DFSMSdss error. Return code 69/ Reason code 9999.
76	Snap	ABEND occurred in the LINK macro while loading DFSMSdss.
4nn	Snap	Parameter list is not valid.
ARCCMUIM		
400 - 403	Abend	Addressability to EIDB or MDSSP cloud not be established.
404 – 411	Debug	Parameter list is not valid.
EIOPTION	Abend	ARCCMUIM returned an invalid option or return code to DFSMSdss.
ARCCPSEM		
12	Debug	The SETSYS EMERGENCY or SETSYS NOEMERGENCY command was issued on a host and secondary host promotion was not able to notify other hosts in the sysplex of the status change because the associated control blocks were not available. Try to issue the command again.
16	Snap	JGCB state is unknown.
ARCCRDSS		
69	Debug	Unknown DFSMSdss error. Return code 69. Reason code 9999.
69	Abend	DFSMSdss ABEND occurred. Return code 69. Reason code 9990.
76	Abend	ABEND occurred in the LINK macro while loading DFSMSdss.
4nn	Debug	Parameter list is not valid.
ARCCRUIM		
400 – 402	Abend	Addressability to EIDB or RDSSP cloud not be established.
403 – 417	Debug	Parameter list is not valid.
EIOPTION	Abend	ARCCRUIM returned an invalid option or return code to DFSMSdss.
ARCDVCLN		
400 – 404	Debug	Parameter list is not valid.
410	Abend	Invalid dump volume record (DGN).

900	Debug	The dump volume processing ends abnormally.
ARCFRVOL		
4nn	Debug	Parameter list is invalid.
98	Debug	Volume count in DGN record is invalid.
Return code from READ	Abend	Read of a DGN record failed.
Return code from READ	Debug	Read for update of a DGN record failed
ARCGRVOL		
70	Debug	System error occurred determining DS8000 cloud capability.
71	Debug	Serialization error during cloud resource checking.
99	Debug	Invalid DFSMSdss ASID number.
4nn	Debug	Parameter list is invalid.
ARCINIT		
GETMAIN return code	Abend	Error obtaining storage for DFSMShsm control blocks.
HSM SVC return code	Snap	HSM SVC error initializing DFSMShsm.
ARCMCSQC		
400	Snap	Invalid MTCB index.
401	Snap	Invalid post code.
ARCMDSN		
409	Log	Incorrect combination of DS1RECAL and DS1IND08 flags in the format 1 DSCB.
498	Debug	Invalid date of the last successful class transition.
ARCMDSUV		
nn	Debug	See the return codes for MIGRATION functions for ACR12nn error message table in *z/OS MVS System Messages, Vol 2 (ARC-ASA)* for more information.
69	Snap	SYNC error.
100	Debug	Dequeue error.
401	Debug	Invalid completion code.
ARCMLECD		
400	Debug	Invalid task ID.
401	Debug	Invalid MTCB ID.
402	Debug	No RCB provided.
403	Debug	RCB contains invalid information
ARCMVDS		
nn	Debug	If nnn is greater than or equal to 100 and less than 200, subtract 100 from nnn and see message ARC12nnI for an explanation of the failing condition. Note that the leading zero in nnn is not used in the message identifier. If nnn is greater

		than or equal to 9nn, an abnormal end occurred when the return code was set to nn. See message ARC0003I for more information about the abnormal end. If the return code is greater than 0, see message ARC12nnI for the reason for the abnormal end.
69	Snap	SYNC error.
4nn	Debug	Parameter list is not valid.
ARCRSTR		
nn	Debug	If nnn is greater than or equal to 9nn, an abnormal end occurred when the return code was set to nn. See message ARC0003I for more information about the abnormal end. If the return code is greater than 0, see message ARC11nnI for the reason for the error.
nn	Fatal	GETMAIN failed.
499	Debug	Invalid date of the last successful class transition.
ARCZLE		
4nn	Debug	Parameter list is not valid.

Chapter 9. Using patches for problem determination

Increasing the amount of PDA tracing performed

<Update Table 4, Conditional PDA Trace Points, with MCVTF_CDAS3DBG information:>

Trace Point	Offset	Initial Setting
:		
Thread checking and reservation during transparent cloud tiering processing	.MCVT.+24F	`BITS(...0....)` Inactive. MCVTF_CLOUD_TRACE - When set to 1, enable additional thread checking traces during TCT processing.
Expanded CDA processing tracing	.MCVT.+5D4	`BITS(.......0)` inactive. MCVTF_CDAS3DBG - When set to 1, enable additional traces during CDA cloud provider processing

<Add the following new section after the existing “Requesting suppressed verbose output with the z/OS Client Web enablement Toolkit” section: >

Requesting DEBUG log-level with z/OS Cloud Data Access

DFSMShsm uses DFSMSdfp Cloud Data Access (CDA) APIs to perform cloud operations such as validating CDA cloud provider file, listing cloud objects, and deleting a cloud object. CDA allows callers to request log-level DEBUG output to help diagnose errors. The same patch requesting "verbose output with the z/OS Client Web Enablement Toolkit" also affects the CDA log-level setting. This PATCH command causes both DFSMShsm and DFSMSdss to request the CDA DEBUG logging. When this option is enabled, DFSMShsm specifies DEBUG(CLMSG(DTL)) parameter to DFSMSdss for cloud operations.

The following PATCH command causes the CDA log-level DEBUG to be requested:

```
PATCH .ARCCVT.+5D4 BITS(.....1..)
```

The following PATCH command stops the CDA DEBUG logging.

```
PATCH .ARCCVT.+5D4 BITS(.....0..)
```

Diagnosing errors when accessing the cloud

Using cloud defined in SMS configuration

<exiting text>

Using cloud defined in CDA provider files

CDA credentials are used for various cloud operations. If a denied access response (HTTP 403) is received during SETSYS CLOUD command processing, it might be caused by incorrect CDA credentials. For example:

```
SETSYS CLOUD(NAME(IBMCOS) CDAPROVIDER)
```

```
ARC0300I **OPER** ISSUED===>SETSYS CLOUD(NAME(IBMCOS) CDAPROV)
ARC1594I Z/OS CLOUD DATA ACCESS ENCOUNTERED AN ERROR
ARC1594I (CONT.) WHILE PERFORMING GDKLIST  SERVICE, RETURN CODE=901
ARC1594I (CONT.) RETURN CODE TRANSLATION=Denied access (HTTP 403)
ARC1594I (CONT.) FOR CLOUD IBMCOS
ARC1594I (CONT.) CONTAINER /
ARC0100I SETSYS COMMAND COMPLETED - CLOUD(NAME(IBMCOS...
```

Related reading: See *z/OS DFSMShsm Diagnosis* for other errors and messages that might be issued.

z/OS DFSMS Access Method Services Commands (SC23-6846)

Appendix F. Interpreting DCOLLECT Output

DCOLLECT Output Record Structure

MIGRATED DATA SET INFORMATION (RECORD TYPE “M”)

Summary of changes:

- Add bit UM_CDA_TCT at offset 321 (X’141’)
- Add bit UM_CDA_DIRECT at offset 321 (X’141’)
- Add bit UM_CDA_ZEDC at offset 321 (X’141’)
- Changed reserved space at offset 322 with a length of 30 bytes

Add changes in the following mapping for Migrated data set information (record type “M”):

Offset	Type	Length	Name	Description
24(18)	STRUCTURE	328	UMMDSI	MIGRATED DATA SET INFORMATION (DEFINED ON DCUDATA)
24(18)	CHARACTER	44	UMDSNAM	DATA SET NAME
:				
238(EE)	BITSTRING	1	UMFLAG3	Information flag #3
	1...		UMEMPTY	ON, IF DATA SET WAS EMPTY AT THE TIME OF MIGRATION
	.1..		UM_CA_RECLAIM_ELIG	ON, IF THE VSAM KSDS DATA SET WAS ELIGIBLE FOR CA RECLAIM PROCESSING WHEN MIGRATED
	..1.		UMZFS	ON - VSAM LINEAR data set for ZFS usage
	...1		UMENCRDP	ON, WHEN THE DATA SET ENCRYPTION INFORMATION INUMENCRYPTA IS PRESENT IN THIS MIGRATION RECORD
	.... 1...		UM_BSON	ON, if BSON VSAMDB data set
	.... .1..		UM_JSON	ON, if JSON VSAMDB data set
	.... ..1.		UM_CLD_COMP	ON, data is TCT compressed
	1		UM_CLD_ENCRYPT	ON, data is TCT encrypted
239(EF)	BITSTRING	1	UMFLAG4	Information flag #4
	1...		UMALLSP_FMB	Mbyte flag for UMALLSP
	.1..		UMUSESP_FMB	Mbyte flag for UMUSESP

	..1.		UMRECSP_FMB	Mbyte flag for UMRECSP
	...1		UMDSIZE_FMB	Mbyte flag for UMDSIZE
	.... 1...		UM_FMB	If ON, the following variables: - UM_USER_DATASIZE - UM_COMP_DATASIZE are in megabytes
	XXX		*	Reserved
240(F0)	STRUCTURE		UM_CLD_INFO	MCD extension for CLOUD info
240(F0)	SIGNED	2	UM_CLOUD_NAME_LENGTH	CLOUD name length
242(F2)	CHARACTER	30	UM_CLOUD_NAME	CLOUD name
272(110)	CHARACTER	44	UM_CONTAINER_NAME	CLOUD container name
316(13C)	SIGNED	4	UM_OBJ_NUMBER	Number of objects stored
320(140)	FIXED	1	UM_CLD_COMP_PERCENT	Percent of space saved by TCT compression. Valid when UM_CLD_COMP=ON
321(141)	**BITSTRING**	**1**	**UMFLAG5**	**Information flag #5**
	1...		**UM_CDA_TCT**	**If ON, data was moved with CDA TCT.**
	.1..		**UM_CDA_DIRECT**	**If ON, data was moved with CDA DIRECT.**
	..1.		**UM_CDA_ZEDC**	**If ON, CDA compression was requested during migration to DIRECT cloud connection**
	...X XXXX		*****	**Reserved**
322(142)	**CHARACTER**	**30**	*	RESERVED SPACE
352(160)	CHARACTER	96	UMENCRYPTA	
352(160)	FIXED	2	UMENCRPT	Data set encryption type '0100'x – AES-256 XTS protected key 'FFFF'x – Data set is not encrypted
354(162)	CHARACTER	64	UMENCRPL	Data set encryption key label when created All 'FF'X key label indicates that the data set is not encrypted
418(1A2)	CHARACTER	30	EMENCRPR	Data set encryption reserved
448(1C0)	CHARACTER	0	UMMDSIE	END OF DCUMCDS

DCOLLECT Output Record Descriptions

Migrated data set record field

Add the following fields after UMEMPTY:

UM_CLD_COMP

Indicates, when the flag is set to 1, that this data is TCT compressed.

UM_CLD_ENCRYPT

Indicates, when the flag is set to 1, that this data is TCT encrypted.

UM_CLD_INFO

This structure defines the cloud information that was used for this data set at the time it was migrated.

UM_CLD_COMP_PERCENT

Contains percent of space saved by TCT compression. This field is valid only when UM_CLD_COMP flag is set to 1.

UM_CDA_TCT

Indicates, when the flag is set to 1, that this data was moved with CDA TCT.

UM_CDA_DIRECT

Indicates, when the flag is set to 1, that this data was moved with CDA DIRECT.

UM_CDA_ZEDC

Indicates, when the flag is set to 1, that CDA compression was requested during migration to DIRECT cloud connection.

z/OS MVS System Messages, Volume 2 (ARC-ASA) – SA38-0669

This section describes the messages changed and added by this enhancement. The changes are highlighted in purple.

ARC0103I (changed)

Add the missing insert ‘parameter’ to the message text. Add new parameters to the existing ARC0103I message description. Delete the second and third sentences about specific parameters in the first paragraph; the text belongs to the listed parameter description. The changes are highlighted in purple.

ARC0103I INVALID SETSYS PARAMETER *parameter*

Explanation

A SETSYS command was issued to establish or change the current setting of a parameter. The indicated parameter is invalid.

~~An ABARS or CSALIMITS parameter may have been specified for a host started with HOSTMODE=AUX.~~

~~When starting a DFSMShsm Filemode Host (HOSTTYPE=FILE), the plex name of PLEX0 may not be specified. Choose a different plex name for this Filemode host.~~

The parameters indicated in this message are:

...

CDAPROVIDER

When CDAPROVIDER was specified and the cloud provider (XC) MCDS record was not supported, the SETSYS command processing was terminated.

When CDAPROVIDER was specified with REMOVECREDENTIALS or REFRESH, the CDAPROVIDER option was ignored. SETSYS command processing continues.

CDACREDENTIALS

CDACREDENTIALS was specified with CDAPROVIDER. The CDACREDENTIALS parameter was ignored. DFSMShsm does not store credentials for CDA cloud providers. SETSYS CLOUD command processing continues.

CLOUDCREDENTIALS

CLOUDCREDENTIALS was specified with CDAPROVIDER. The CLOUDCREDENTIALS parameter was ignored. DFSMShsm does not store credentials for CDA cloud providers. SETSYS CLOUD command processing continues.

CLOUD(NAME)

Required subparameter *cloud_name* was not specified in the NAME(*cloudname*) parameter or was specified incorrectly. SETSYS command processing was terminated.

...

PLEXNAME

The name of the HSMplex can only be specified in the parmlib. An attempt was made to name the sysplex after start-up.

When starting a DFSMShsm Filemode Host (HOSTTYPE=FILE), the plex name of PLEX0 may not be specified. Choose a different plex name for this Filemode host.

...

SMSPROVIDER

When SMSPROVIDER was specified and the cloud provider (XC) MCDS record was not supported, the SETSYS command processing was terminated.

When SMSPROVIDER was specified with REMOVECREDENTIALS or REFRESH, the SMSPROVIDER option was ignored. SETSYS command processing continues.

When SMSPROVIDER was specified without the required CLOUDCREDENTIALS or CDACREDENTIALS parameter, the SETSYS command processing is terminated.

...

Programmer response

...

CDAPROVIDER

If the SETSYS command was terminated, verify the cloud provider (XC) MCDS record support has been enabled.

For information on enabling XC record support, see *z/OS DFSMShsm Implementation and Customization Guide*, Chapter 17 Tuning DFSMShsm, “Allowing CLOUD CDACREDCREDENTIALS and full volume dump restore using object storage” section.

CDACREDENTIALS

None.

CLOUDCREDENTIALS

None.

CLOUD(NAME)

Specify a valid *cloud_name* in the NAME(*cloud_name*) parameter and reissue the command.

...

SMSPROVIDER

If the SETSYS command was terminated, verify the following:

- Cloud provider (XC) MCDS record support has been enabled.
- Specify SMSPROVIDER with the required CLOUDCREDENTIALS or CDACREDENTIALS parameter and reissue the command.

For information on enabling XC record support, see *z/OS DFSMShsm Implementation and Customization Guide*, Chapter 17 Tuning DFSMShsm, “Allowing CLOUD CDACREDCREDENTIALS and full volume dump restore using object storage” section.

...

ARC0340I (changed)

Update ARC0340I message text and explanation with the new CLOUDMIGRTATE(NO | YES) information. The new text of “CLOUDMIGRATE=[YES | NO]” is added to the end of the existing message text.

ARC0340I COMPACTION OPTIONS ARE: TAPEMIGRATION=[YES | NO], DASDMIGRATION=[YES | NO], TAPEBACKUP=[YES | NO], DASDBACKUP=[YES | NO], TAPEHARDWARECOMPACT=[YES | NO], ZCOMPRESS OPTIONS ARE: TAPEMIGRATE=[YES | NO], DASDMIGRATE=[YES | NO], TAPEBACKUP=[YES | NO], DASDBACKUP=[YES | NO], CLOUDMIGRATE=[YES | NO]

Explanation

:

For ZCOMPESS options:

If CLOUDMIGRATE=YES, CDA compression using zEDC Services can be used for data when it is migrated to a DIRECT cloud connection.

If CLOUDMIGRATE=NO, CDA compression is not used for data when it is migrated to a DIRECT cloud connection.

If DASDMIGRATE=YES, zEDC Services can be used for data when it is migrated to a DASD migration level 1 or level 2 volume.

If DASDMIGRATE=NO, zEDC Service are not used for data when it is migrated to a DASD migration level 1 or level 2 volume.

If DASDBACKUP=YES, zEDC Services can be used for data when it is backed up to a DASD backup volume.

:

ARC0752I (changed)

ARC0752I CANNOT {RECOVER | RESTORE} VOLUME *volser*, {BACKUP | DUMP} NOT AVAILABLE, REASON=*reascode*

Add reason code 74 and 75 to explanation and programmer response. Delete the last sentence "*Reissue the DDELETE command specifying the required parameters"* In explanation.

Explanation

74

The current cloud provider properties are incompatible with the properties used at the time the dump copy was created. The volume cannot be restored.

75

The volume cannot be recovered from cloud object store because the cloud provider defined at the time the volume was dumped is no longer known to DFSMShsm. See preceding message ARC1598I for more information.

Programmer response

- For reason code 74, recreate or update the cloud provider definition with properties used at the time the dump copy was created and retry the recover from dump command.
- For reason code 75, define to DFSMShsm the cloud provider with properties used at the time the volume was dumped. Issue the SETSYS CLOUD command to define the cloud provider to DFSMShsm and retry the recall command.

ARC1179I (changed)

ARC1179I ERROR RECALLING DATA SET OR DELETING DATA SET

Add reason code 14 and 15 to explanation and programmer response.

Explanation

14

The data set cannot be recalled from cloud object store because the current cloud provider properties are incompatible with the properties used at the time the data set was migrated.

15

The data set cannot be recalled from cloud object store because the cloud provider defined at the time the data set was migrated is no longer known to DFSMShsm. See preceding message ARC1598I for more information.

Programmer response

14

Recreate or update the cloud provider definition with properties used at the time the data set was migrated and retry the recall command.

15

Define to DFSMShsm the cloud provider with properties used at the time the data set was migrated. Issue the SETSYS CLOUD command to define the cloud provider to DFSMShsm and retry the recall command.

ARC1208I (changed)

ARC1208I ERROR ALLOCATING MIGRATION COPY

Add reason code 18 to explanation and programmer response.

Explanation

18

Create container operation encountered an error.

Programmer response

8, 16, 18, 20

Contact the storage administrator or system programmer to correct the problem and retry the operation.

ARC1570I (new)

ARC1570I Z/OS LANGUAGE ENVIRONMENT SERVICE ENCOUNTERED AN ERROR WHILE CALLING THE CDA SERVICE *gdk_api* [OPERATION NAME *operation_name*] [FOR CLOUD *cloud_name*] [CONTAINER *container_name*] [OBJECT *object_name*]

Explanation

This message is followed by ARC1599I. It indicates that there was a failure while using the z/OS Language Environment service CEEPIPI to call a CDA API. The call to the CDA API has not yet happened when this error occurred.

gdk_api

Name of the CDA callable service.

operation_name

Name of the operation for which GDKGEN was invoked.

cloud_name

Name of the Cloud provider being accessed at the time of the error

container_name

The container being accessed at the time of the error

object_name

The object name being accessed at the time of the error.

System Action

The current request fails. DFSMShsm processing continues.

Programmer Response

None.

Storage Administrator Response:

Report the problem to IBM support.

Source

DFSMShsm

ARC1594I (new)

ARC1594I Z/OS CLOUD DATA ACCESS ENCOUNTERED AN ERROR
WHILE PERFORMING *cda_api* SERVICE, RETURN CODE=*cda_rc*
[RETURN CODE TRANSLATION=*rc_text*]
[FOR CLOUD *cloud_name*]
[CONTAINER *container_name*]
[OBJECT *object_name*]
[OPERATION NAME *op_name*]
[HTTP RESPONSE CODE=*http_code*]
[HWTHRQST RETURN CODE=*hwth_code*]
[HWTHRQST DIAG REASON CODE=*diag_reason*]
[HWTHRQST DIAG DESCRIPTION *diagarea*]

Explanation

An error occurred while performing the identified Cloud Data Access service *cda_api.* The CDA return code is *cda_rc*. The message may be followed by one or more pieces of the additional information below:

rc_text

The CDA service return code (*cda_rc*) text translation.

cloud_name

The cloud name that was being accessed at the time of error.

container_name

The container name that was being processed at the time of error.

object_name

The object name that was being processed at the time of error.

op_name

The identified service was GDKGEN, this field identifies the operation that was requested.

http_code

The service performed the operation and resulted in this HTTP response code error. The value is a converted 4-character decimal number.

hwth_code

CDA invoked the z/OS Client Web Enablement Toolkit HWTHRQST service. The service returned this error. The value is a converted 8-character hexadecimal number.

diag_reason

The first 4-bytes of the z/OS Web Enablement Toolkit diag area that contains the diag reason code. The value is a converted 8-character hexadecimal number.

diagarea

This is the z/OS Client Web Enablement Toolkit HWTHRQST service DiagArea.

System action

The cloud operation failed. DFSMShsm processing continues.

Programmer response

Refer to the identified z/OS Cloud Data Access callable service and associated return code in *z/OS MVS Programming: Callable Services for High-Level Languages* to identify the failing reason.

If HWTHRQST areas are provided, refer to the z/OS client web enablement toolkit in *z/OS MVS Programming: Callable Services for High-Level Languages* to identify the reason for the error.

Source

DFSMShsm

ARC1595I (new)

ARC1595I UNEXPECTED ERROR IN CDA PROVIDER FILE FOR CLOUD *cloud_name*, REASON=*reascode*

Explanation

While performing validation of a CDA provider file, DFSMShsm received an unexpected error. If '****' is displayed in *cloud_name*, the expected CDA provider file was not found.

Reascode

	Meaning
20	Specified key value for tctType was invalid. Accepted values are TAPE-OBJECT and TCT.

System action

The cloud operation failed. DFSMShsm processing continues.

Programmer response

Take the action for the received reason code.

Reascode

	Action
20	Ensure the CDA provider file for the specified CLOUD contain valid tctType information. Correct the error and rerun the DFSMShsm function. The accepted values are TAPE-OBJECT and TCT.

Source

DFSMShsm

ARC1596I (new)

ARC1596I SETSYS CLOUD FAILED FOR CLOUD *cloud_name*, RETURN CODE=*retcode*

Explanation

The SETSYS CLOUD command encountered an error.

Retcode

	Meaning
4	The specified CDA cloud provider name does not exist or is not found.

8

An existing cloud of the same name had been defined to DFSMShsm with the CLOUDCREDENTIALS parameter associated with an SMS network connection construct. The encrypted CCREDS password is stored by DFSMShsm.

Transition to CDAPROVIDER to use CDA provider configuration is not supported because the existing SMS cloud definition with associated credentials is still needed to recall data sets or restore volumes from the designated cloud object store.

10

An existing cloud of the same name had been defined to DFSMShsm with the CDACREDENTIALS parameter associated with an SMS network connection construct. The encrypted CDACREDS password is stored by DFSMShsm.

Transition to CDAPROVIDER to use CDA provider configuration is not supported because the existing SMS cloud definition with associated credentials is still needed to recall data sets or restore volumes from the designated cloud object store.

12

An existing cloud of the same name had been defined with a CDA provider configuration.

Transition to CLOUDCREDENTIALS associated with an SMS network connection construct is not supported because the existing CDA provider configuration with associated credentials is still needed to recall data sets or restore volumes from the designated cloud object store.

14

An existing cloud of the same name had been defined with a CDA provider file.

Transition to CDACREDENTIALS associated with an SMS network connection construct is not supported because the existing CDA provider configuration with associated credentials is still needed to recall data sets or restore volumes from the designated cloud object store.

System action

The SETSYS CLOUD operation failed. DFSMShsm processing continues.

Programmer response

Review and resolve the cause of the error and reissue the command.

Retcode

Action

4

Ensure the CDA provider definition file name matches the cloud name configured in your infrastructure. If a valid provider file exists, ensure it resides in the directory for DFSMShsm use. If the CDA provider file describes a TS7700 TAPE-OBJECT store, ensure the TAPE-OBJECT multiple endpoints functionality has been enabled.

For more information, see *z/OS DFSMShsm Implementation and Customization Guide*, section ‘CDA configuration for cloud storage’.

8, 10

Specify a new cloud name for the CDA provider file. If the existing cloud definition is not needed for any recall or restore operation, REMOVE the existing definition from the HSMPLEX, then resubmit the SETSYS CLOUD CDAPROVIDER command.

For information on removing a cloud definition in an HSMPLEX, see *z/OS DFSMShsm Storage Administration*.

12, 14

Specify a new cloud name for the SMS network connection construct. If the existing cloud definition is not needed for any recall or restore operation, REMOVE the existing definition from the HSMPLEX, then resubmit the SETSYS CLOUD CDAPROVIDER command.

For information on removing a cloud definition in an HSMPLEX, see *z/OS DFSMShsm Storage Administration*.

Source

DFSMShsm

ARC1597I (new)

ARC1597I CLOUD PROVIDER *cloud_name* INFORMATION OBTAINED FROM {CDA | SMS} SPECIFIES {TAPE-OBJECT | SWIFT | TCT | DIRECT}

Explanation

DFSMShsm SETSYS CLOUD processing obtained cloud provider information from the designated CDA or SMS configuration.

CDA indicates a valid, non-empty CDA provider file with the specified *cloud_name* was found. The provider file requests TS7700 TAPE-OBJECT, TCT, or DIRECT cloud connection be used.

SMS indicates an SMS network connection with the specified *cloud_name* was found. The network connection construct specifies TS7700 TAPE-OBJECT, SWIFT, or TCT provider protocol be use.

When '******' is displayed, DFSMShsm was unable to determine the requested cloud provider protocol.

System action

DFSMShsm processing continues.

Programmer response

None.

Source

DFSMShsm

ARC1598I (new)

ARC1598I CLOUD NAME *cloud_name* IS NOT DEFINED TO DFSMSHSM

Explanation

During recall from cloud, if the *cloud_name* entry is not found in DFSMShsm records, recall will fail with message ARC1179I. Message ARC1598I precedes ARC1179I.

System action

Recall fails.

Programmer response

Ensure the cloud provider where the migration copy resides is defined to DFSMShsm then reissue the RECALL command.

Source

DFSMShsm

ARC1599I (new)

A RC1599I Z/OS LANGUAGE ENVIRONMENT SERVICE CEEPIPI FAILED TO PERFORM THE FUNCTION=*operation*, RC=*retcode, error_text*

Explanation

DFSMShsm has encountered problems while invoking the CEEPIPI service.

This message may be followed by another message such as ARC1594I that indicates the type of CDA service or cloud operation being performed under Language Environment.

operation

The CEEPIPI operation that failed. The following are the possible operations.

- INIT_SUB
- CALL_SUB
- LE_TERM
- ADD_ENTRY
- UNKNOWN – DFSMShsm could not determine the operation.

retcode

Return code from CEEPIPI.

error_text

Description of the *retcode*.

System action

DFSMShsm processing continues.

Programmer response

Refer to the *z/OS Language Environment Programming Guide* for the return code and description.

Source

DFSMShsm

ARC1605I (changed)

Add new reason code 39 to the existing ARC1605I message description as shown below:

ARC1605I COMMAND HAD PARSE ERROR

Explanation

The TSO IKJPARS routine was called to check the syntax of a DFSMShsm request and encountered an error. Message ARC1001I precedes this message giving the operation entered, the reason-code, and the parse return code.

The values for reason-code are:

39

A SETSYS CLOUD command received a syntax error after the command was successfully parsed. If message ARC0103I was issued, it contains the specific invalid parameter.

Programmer Response

...

If reason-code is , 8, 16, 28, 36, 37, 38, 39, 40, 42, 44, 50 or 51, correct the problem and retry the command. If reason-code is 12, 20, or 24, DFSMShsm encountered a logical error. Notify the storage administrator or the system programmer.

...