**************DEPRECATED**************

This document has been deprecated and should no longer be used. Reference the DFSMS Object Access Method Planning, Installation, and Storage Administration Guide for Object Support and the DFSMSdfp Diagnosis publications for the latest information on OAM's Cloud as a Tier support.

************** DEPRECATED **************

Installation Guide
OAM Cloud as a Tier
V2R3 and above

Document Name:	OAM-Cloud-Installation-Guide.docx
Document Owner:	Peter Sobik (pssobik@us.ibm.com) Albert Dennes (aedennes@us.ibm.com)
Version:	V1.8

Version	Date	Change Description	Revision Tag
1.0	05/11/2020	Initial version	None - this version replaces any earlier versions
1.1	07/28/2020	Added more detail in reference to coexistence installation	**Green**
1.2	07/30/2020	Removed reference to GDKOPPOP in section 3.1	None
1.3	8/27/2020	Updated CDA sample file names in section 2.4 and panel screenshots in chapter 3	Blue
1.4	9/28/2020	Fixed a reference to the OAM home directory. Added OAM RACF validation examples. Added CDA panel warning description.	Orange
1.5	10/15/2020	Added IBM Crypto Express card to list of requirements and ICSF master key requirement.	Purple
1.6	1/26/2020	Removed text to clarify that container names are always folded to lower case by CDA.	None

1.7	02/04/2021	Added additional diagnostic data, including OSREQ reason codes	Red
1.8	01/26/2022	***Deprecated***	None – no updates were made to content. Only added the deprecation statement to the front of the document to indicate this document should no longer be used.

Table of Contents

1 Overview

This installation guide consists of three sections. The first section covers security and user setup. The second section details the steps required to setup and configure the new Cloud Data Access (CDA) component. The third section discusses how to enable Cloud as a Tier support within OAM to leverage the capabilities provided by CDA to store and manage primary copies of OAM objects in the cloud.

1.1 Software Requirements

The following is a list of required software components that must be active in order to utilize this support:

- UNIX System Services (USS)
- Integrated Cryptographic Service Facility (ICSF) with an AES Master Key defined as AES SHA256
- Resource Access Control Facility (RACF) or equivalent security product

1.2 Hardware Requirements

The following is a list of required hardware components that must be installed in order to utilize this support:

- IBM Crypto Express card

1.3 Full support APARs

The following is a list of V2R3 and V2R4 APARs required to enable this support:

- OA55700 - OAM
- OA55713 - ISMF
- OA55714 - Naviquest
- OA55715 - SMS (for SMS, their V2R4 support is built into the base release)
- OA56304 - CDA
- OA56476 - OCE
- OA56478 - BAM
- OA59547 - HFS

In addition, if running in an OAMplex with z/OS V2R2, OAM coexistence APAR OA55701 is needed along with SMS APAR OA55715. For SMS, their full support is the same as their coexistence.

When the new Cloud Data Access (CDA) component of DFSMS is installed, the following GDK directory and files are automatically created with permissions 755:

/usr/lpp/dfsms/gdk/ 755

/usr/lpp/dfsms/gdk/providers/ 755 (with the 1st release of CDA, this directory is created and left empty)

/usr/lpp/dfsms/gdk/samples/ 755

/usr/lpp/dfsms/gdk/samples/providers/ 755

An IPL is required after all APARs are applied to complete installation.

1.4 Co-existence APARs for PLEX environments

If running in an OAMplex environment and/or a SYSPLEX environment that shares an SCDS, the following co-existence behavior must be adhered to before utilizing the full support…

V2R2 systems
- OA55701 (OAM) and OA55715 (SMS) must be applied.

V2R3 systems
- No coexistence available, full support only... OA55700 (OAM) must be applied. The OAM APAR should bring in all other dependencies. See section 1.2 for more details.

Note: For systems in a SYSPLEX that are not using OAM but are sharing an SCDS with other system(s) using OAM's cloud support… the non-OAM systems must apply OA55715 (SMS) for SCDS compatibility.

V2R4 systems
- Coexistence for OAM and SMS already available in base release. No further action needed for 2.4.

Note: OA55715 (SMS) co-existence is the same as their full support.

An IPL is required after all co-existence APARs are applied to complete installation.

1.5 Cloud Storage Provider Considerations

This guide will not discuss setup related to the cloud storage provider. At a minimum, it is expected that at least one bucket and set of S3 authorization keys have been created and proper authority has been granted to allow access to the bucket utilizing those keys. A valid endpoint, port, and region name will also be required. Also note if the cloud storage provider has an SSL/TLS version and/or cipher requirement.

2 Security Setup

2.1 Create the OAM home directory

1. Create a home directory for the OAM user.

```
mkdir OAM_home_dir_name
```

2. Create subdirectories for Cloud Data Access configuration files.

```
mkdir /OAM_home_dir_name/gdk
mkdir /OAM_home_dir_name/gdk/providers
```

Note: Recommended owner, group and permissions for these directories and files will be set in Section 2.5.

2.2 Create RACF OAM User and Group

RACF (or equivalent) user and group IDs for OAM must be created and configured. If these steps have already been completed from a prior OAM file system level setup, **ensure that the existing OAM user id's FILEPROCMAX and PROCUSERMAX settings are 50** if utilizing 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 OAM address spaces, the FILEPROCMAX and PROCUSERMAX settings should be **50 (or 25) multiplied** by the number of OAM's sharing the user id.

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

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

```
ADDGROUP oamgrp OMVS(GID(gid))
```

2. Create a user ID for OAM with a unique UID and assign it to the group above. A **setting of 50 per OAM address space** is recommend for both FILEPROCMAX and PROCUSERMAX if the OAM file system level is being utilized in conjunction with the cloud level, **otherwise a setting of 25 per OAM address space**, if utilizing just the cloud support. A home directory is required to store Cloud Data Access (CDA) configuration files

```
ADDUSER oam DFLTGRP(oamgrp) OWNER(oamgrp) NAME('OAM Address Space')
NOPASSWORD OMVS(UID(uid) FILEPROCMAX(fff) PROCUSERMAX(ppp)
HOME(OAM_home_dir_name))
```

3. Associate the OAM started task with the OAM group.

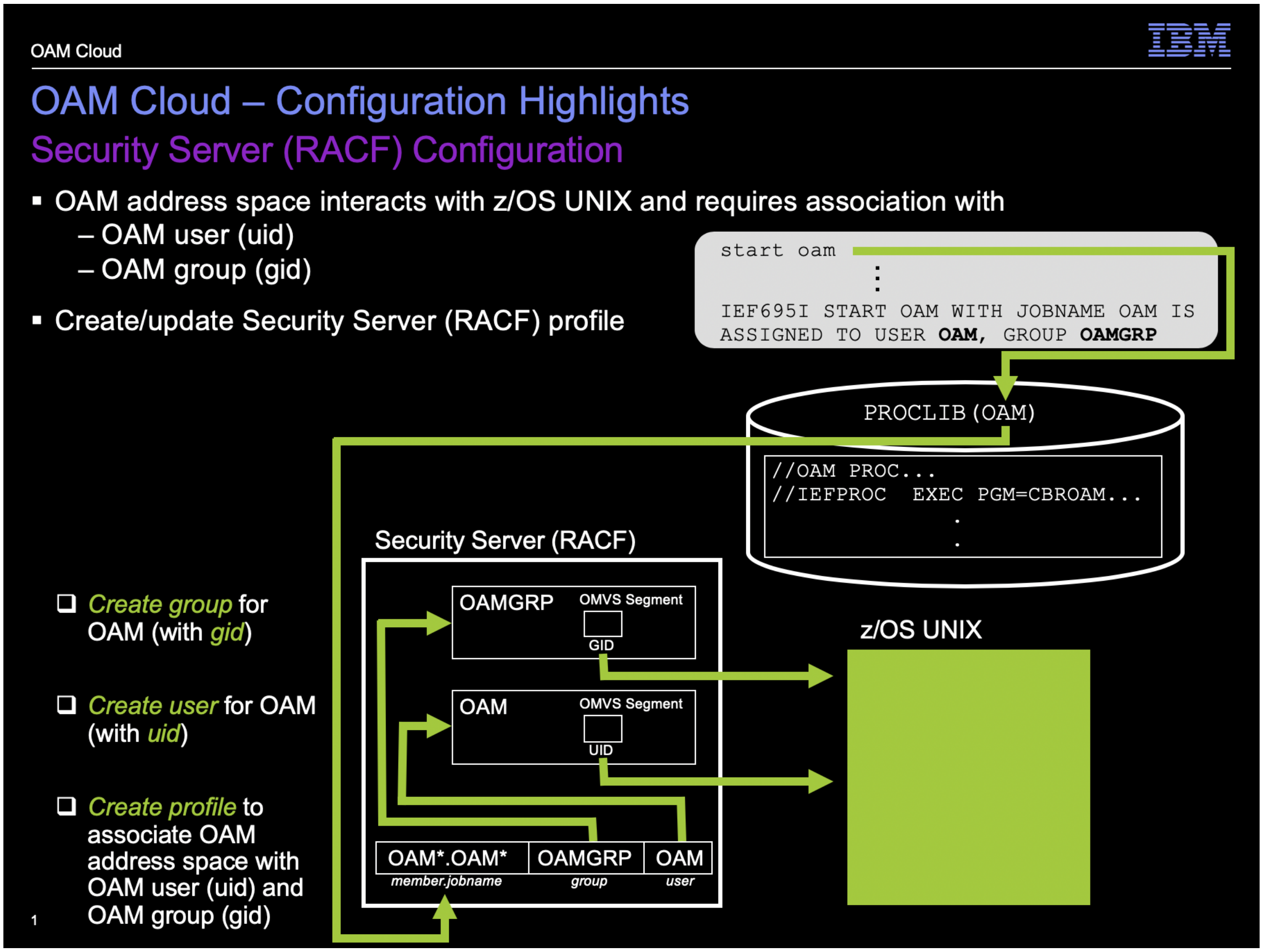
```
RDEFINE STARTED OAM*.OAM* STDATA(USER(=MEMBER) GROUP(oamgrp))
```

4. Refresh the RACF (or equivalent) profile.

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

See the 'Security configuration for the file system' section in the *DFSMS Object Access Method Planning, Installation, and Storage Administration Guide for Object Support* book for more information.

The diagram below details OAM’s interaction with the RACF (or equivalent) user id and group:



OAM Cloud

OAM Cloud – Configuration Highlights

Security Server (RACF) Configuration

- OAM address space interacts with z/OS UNIX and requires association with
  - OAM user (uid)
  - OAM group (gid)
- Create/update Security Server (RACF) profile

```
start oam
   :
IEF695I START OAM WITH JOBNAME OAM IS
ASSIGNED TO USER OAM, GROUP OAMGRP
```

PROCLIB (OAM)

```
//OAM PROC...
//IEFPROC   EXEC PGM=CBROAM...
                .
                .
```

Security Server (RACF)

OAM*.OAM*	OAMGRP	OAM
member.jobname	group	user

❑ *Create group* for OAM (with *gid*)

❑ *Create user* for OAM (with *uid*)

❑ *Create profile* to associate OAM address space with OAM user (uid) and OAM group (gid)

1

To validate that the RACF user id and group for OAM have been correctly associated with the OAM address space, check the following message in the system log during OAM initialization:

```
IEF695I START OAM      WITH JOBNAME OAM      IS ASSIGNED TO USER oam, GROUP
oamgrp
```

To validate the OAM RACF user id UNIX setup, issue the following TSO command:

LISTUSER *oam* OMVS

Example Output:

```
USER=oam NAME=oam                   OWNER=user   CREATED=18.337
 DEFAULT-GROUP=OAMGRP   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= OAM_home_dir_name
CPUTIMEMAX= NONE
ASSIZEMAX= NONE
FILEPROCMAX= 00000050
PROCUSERMAX= 00000050
THREADSMAX= NONE
MMAPAREAMAX= NONE
```

2.3 Create the RACF OAM administrator group

A RACF group for OAM administrators should be created with a unique GID. For example:

```
ADDGROUP oamadmin OMVS(GID(gid))
```

Add appropriate users to this group. This includes:

1. A system administrator who will be responsible for maintaining the Cloud Data Access configuration file in the /*OAM_home_dir_name*/gdk directory. See Section 3.2 for more details.

2. A storage administrator who will be responsible for updating the Cloud Data Access provider definition files located in /*OAM_home_dir_name*/gdk/providers. See Section 3.3 for more details.

3. A security (or storage) administrator will be responsible for adding cloud provider access keys utilizing the Cloud Data Access ISPF panels. See Section 3.4 for more details.

The use of a separate OAM administrator group is strongly recommended to prevent unauthorized users from accessing OAM file system objects.

2.4 Copy Cloud Data Access Configuration Files

Copy the provided sample JSON files to the OAM home directory:

1. /usr/lpp/dfsms/gdk/samples/gdkconfig.json should be copied to /*OAM_home_dir_name*/gdk/config.json
2. /usr/lpp/dfsms/gdk/samples/gdkkeyf.json should be copied to /*OAM_home_dir_name*/gdk/gdkkeyf.json
3. /usr/lpp/dfsms/gdk/samples/providers/IBMCOS.json should be copied to /*OAM_home_dir_name*/gdk/providers/IBMCOS.json

   Note: A sample cloud provider definition file for Amazon S3 is also provided under the name AWSS3.json.

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

2.5 Secure the OAM Home Directory

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

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

```
chmod -R 770 /OAM_home_dir_name
```

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

```
chgrp -R oamadmin /OAM_home_dir_name
```

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

```
chown -R oam /OAM_home_dir_name
```

2.6 Configure the CSFKEYS general resource class

The CSFKEYS RACF (or equivalent) general resource class must be configured to allow CDA to utilize 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 OAM 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 OAM user id must have READ access to the new CSFKEYS profile for resources beginning with GDK.
6. The security administrator who will be entering cloud provider keys must have READ and WRITE access to the new CSFKEYS profile for resources beginning with GDK.OAM. See Section 3.4 for more details.

2.7 Add SSL certificates

All required cloud provider SSL certificates must be added to RACF (or equivalent). The OAM 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.

3 Cloud Data Access Setup

3.1 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

A RACF (or equivalent) profile should be created to ensure only authorized users have access to these members.

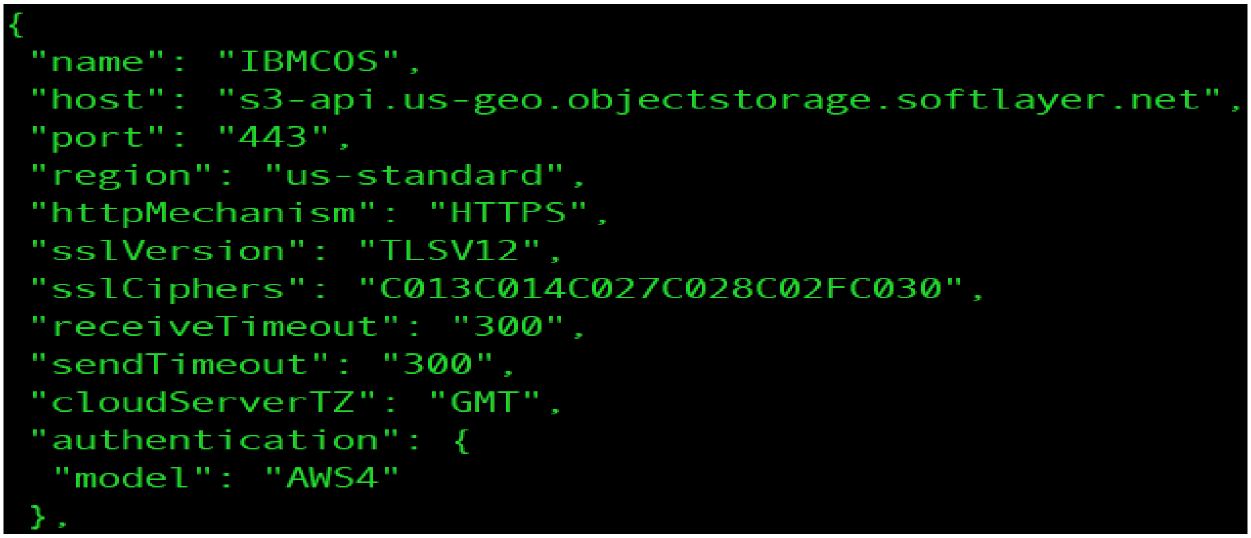
3.2 Alter Configuration File

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

It is recommended to leave the “log-level” setting at its default value “NONE”. If it becomes necessary, OAM or CDA support may request that this value be changed to assist with problem diagnosis.

3.3 Alter Cloud Provider Definition File

The cloud provider definition file IBMCOS.json contains fields and values which describe settings and supported operations related to the cloud storage provider. There can be multiple provider definition files which can 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). The following keys and values are described in detail below:



```
{
 "name": "IBMCOS",
 "host": "s3-api.us-geo.objectstorage.softlayer.net",
 "port": "443",
 "region": "us-standard",
 "httpMechanism": "HTTPS",
 "sslVersion": "TLSV12",
 "sslCiphers": "C013C014C027C028C02FC030",
 "receiveTimeout": "300",
 "sendTimeout": "300",
 "cloudServerTZ": "GMT",
 "authentication": {
  "model": "AWS4"
 },
```

- **name** - Required. The name of the cloud provider which will be utilized by the cloud key entry panel and OAM. Must match the filename.
- **host** - Required. The endpoint URL for the cloud provider
- **port** - Required. The endpoint URL port number.
- **region** - Required for “AWS4” authentication models. The name of the region name to be used.
- **httpMechanism** - Required. **Only HTTPS is supported**.
- **sslVersion** - Optional. Valid values are “TLSV12”, “TLSV11”, “TLSV10”, and “SSLV3”. It is recommended to set the highest version supported by the cloud storage provider. If no key pair is specified, SSL will be used but no security version will be sent on requests.
- **sslCiphers** - Optional. A string value that represents the specification of the cipher suites to be used by SSL. The recommendation is to remove this key pair unless a specific cipher suite is required by the cloud storage provider.
- **receiveTimeout** - Optional. The number of seconds an open SSL socket will wait for incoming requests. Default value is 300.
- **sendTimeout** - Optional. The number of seconds an open SSL socket will wait for outgoing requests. Default value is 300.
- **cloudServerTZ** - Optional. Valid value is a time zone abbreviation plus optional offset. For example, “UTC” or “EST+2”. This time zone is used when generating timestamps for cloud requests and should match the cloud provider. Default value is “GMT”.
- **authentication** - Required. Set to “AWS4” to utilize the S3 API.

All other entries under the “supportedOperations” key should not be altered.

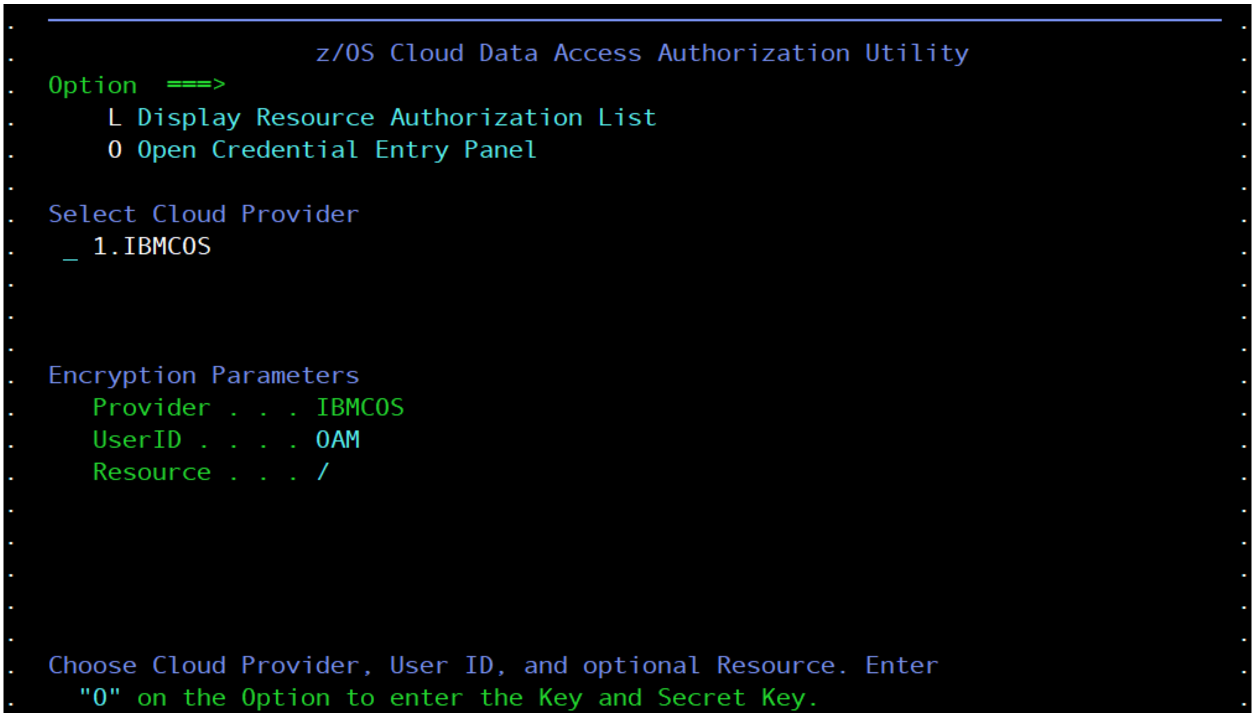
3.4 Add Cloud Provider Keys

Prior to starting this step, ensure that the security (or storage) administrator who will be entering the cloud provider keys has sufficient authority to write to the gdkkeyf.json file (/*OAM_home_dir_name*/gdk/gdkkeyf.json) and the CSFKEYS profile for resources beginning with GDK. See Section 2.5 and Section 2.6 for more details.

From the TSO command line, issue the following command:

```
EX ‘SYS1.SAXREXEC(GDKAUTHP)’
```

This will start a CDA panel where the S3 key pair will be encrypted and saved.

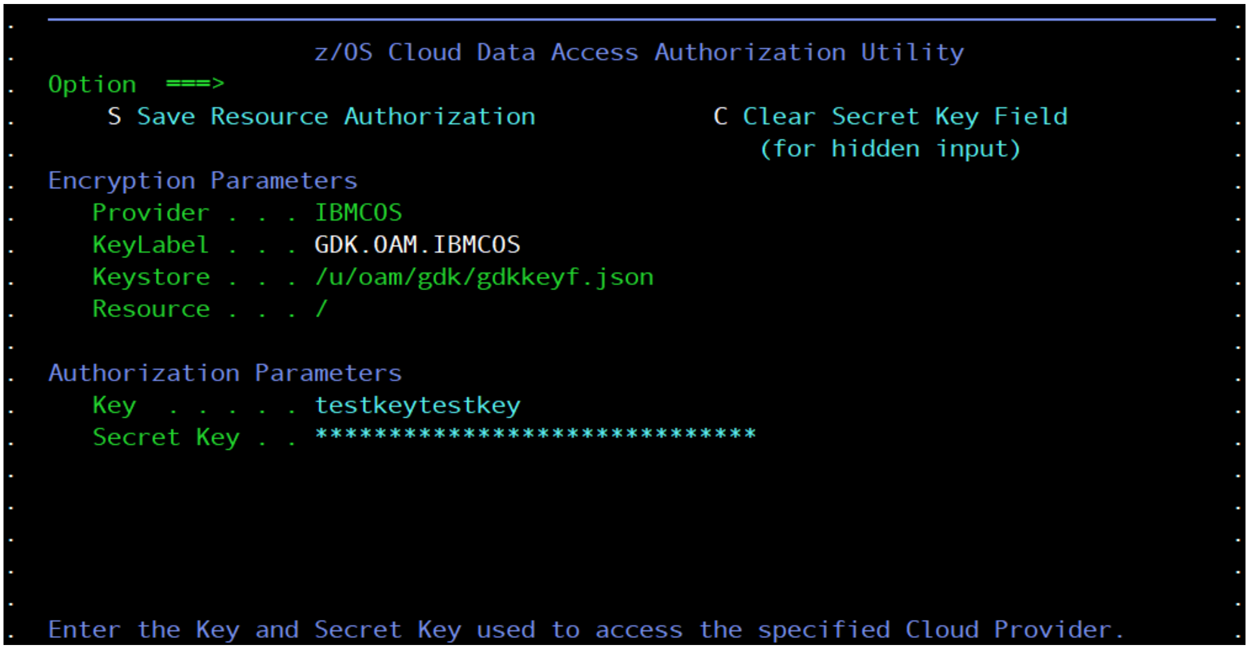


```
                      z/OS Cloud Data Access Authorization Utility
Option  ===>
    L Display Resource Authorization List
    O Open Credential Entry Panel

Select Cloud Provider
 _ 1.IBMCOS



Encryption Parameters
   Provider . . . IBMCOS
   UserID . . . . OAM
   Resource . . . /





Choose Cloud Provider, User ID, and optional Resource. Enter
  "O" on the Option to enter the Key and Secret Key.
```

1. Select the cloud provider associated with the key pair being added by entering the associated number under the “Select Cloud Provider” heading.
2. Enter the RACF (or equivalent) user id associated with OAM 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, simply enter a ‘/’ to indicate that this key pair is valid for any bucket associated with this cloud provider.

   Both specific and generic keys can be added and CDA will attempt to utilize specific keys tied to buckets before utilizing the generic key for the provider.

   Note: Only 1 generic key is used per provider. If a second is entered, it will overwrite the first.
4. Press Enter to save the values.
5. Enter an ‘O’ on the top Option line to continue to the next panel.



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

Authorization Parameters
   Key  . . . . . testkeytestkey
   Secret Key . . ******************************





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

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 hit.

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 may receive the following warning messages:

```
ERROR: getpwnam() error: EDC5121I Invalid argument.
ERROR: getpwnam() error: EDC5129I No such file or directory.
```

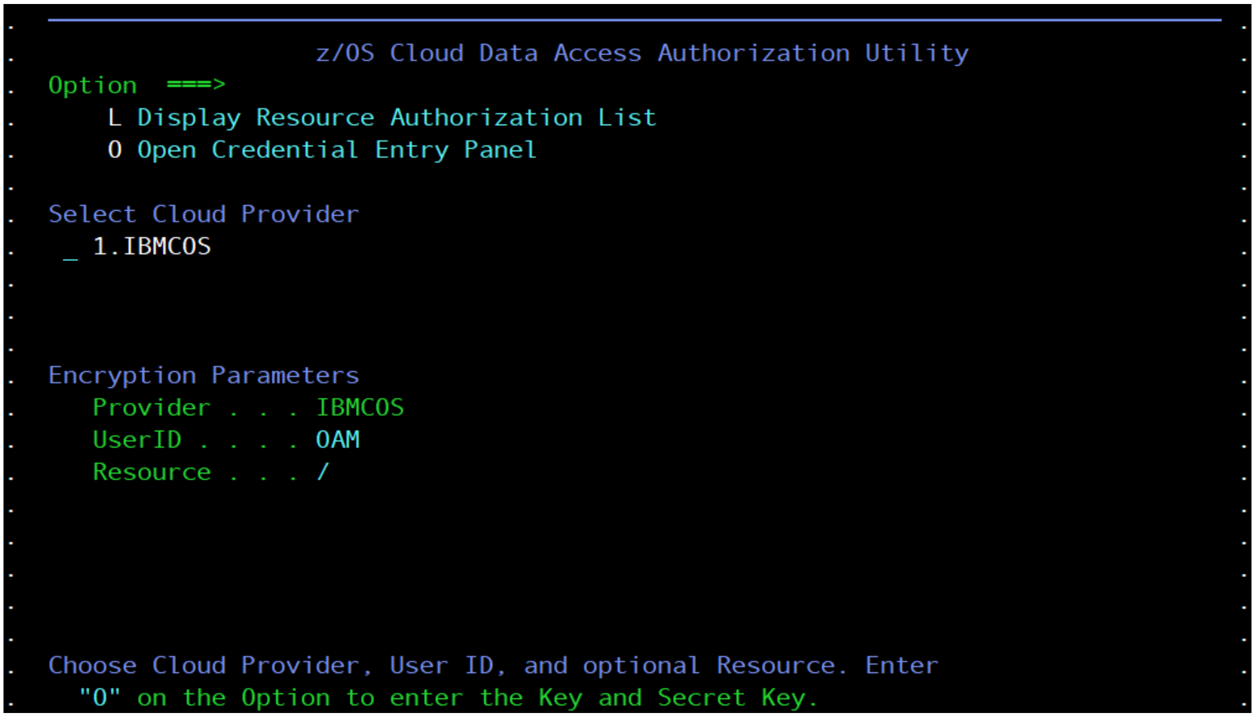
This behavior is expected because the UserID field has not yet been populated. Once the user id created in Section 2.2 has been specified here at least one time, the warning messages will no longer be displayed.

3.5 Delete Cloud Provider Keys (Optional)

From the TSO command line, issue the following command:

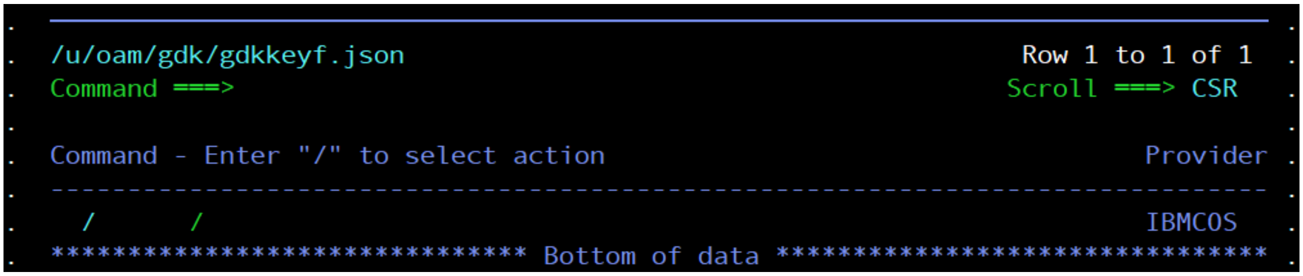
```
EX ‘SYS1.SAXREXEC(GDKAUTHP)’
```

This will start a CDA panel where the S3 key pair can be deleted.



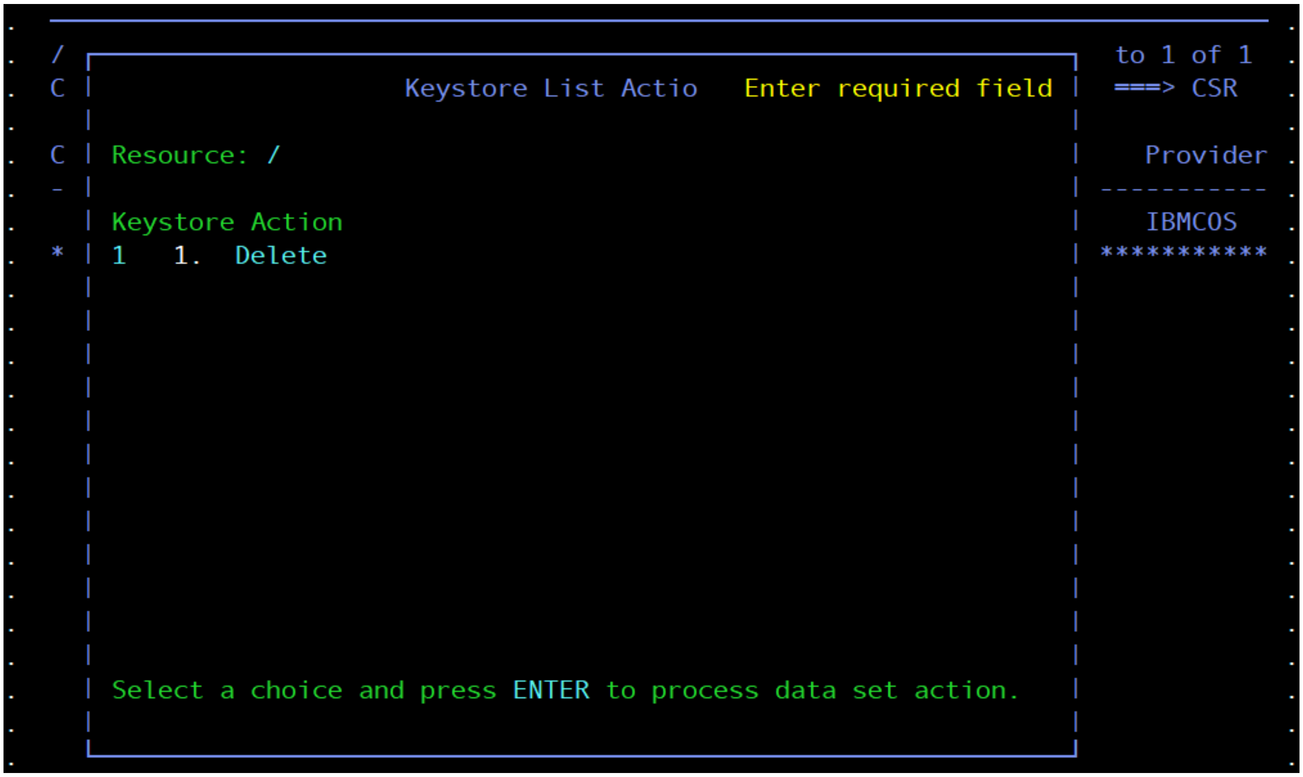
```
                    z/OS Cloud Data Access Authorization Utility
Option  ===>
    L Display Resource Authorization List
    O Open Credential Entry Panel

Select Cloud Provider
 _ 1.IBMCOS



Encryption Parameters
   Provider . . . IBMCOS
   UserID . . . . OAM
   Resource . . . /





Choose Cloud Provider, User ID, and optional Resource. Enter
  "O" on the Option to enter the Key and Secret Key.
```

1. Select the cloud provider associated with the key pair being removed by entering the associated number under the “Select Cloud Provider” heading.
2. Enter the RACF (or equivalent) user id associated with OAM into the UserID field under the “Encryption Parameters” section.
3. Enter an ‘L’ on the top Option line.



```
/u/oam/gdk/gdkkeyf.json                                   Row 1 to 1 of 1
Command ===>                                              Scroll ===> CSR

Command - Enter "/" to select action                            Provider
------------------------------------------------------------------------
  /      /                                                     IBMCOS
****************************** Bottom of data ********************************
```

4. Enter a '/' next to the key to be removed.



```
/ ┌──────────────────────────────────────────────────────────────┐  to 1 of 1
C |                  Keystore List Actio   Enter required field |  ===> CSR
  |                                                              |
C | Resource: /                                                  |   Provider
- |                                                              |  -----------
  | Keystore Action                                              |   IBMCOS
* | 1   1.  Delete                                               |  ***********
  |                                                              |
  |                                                              |
  |                                                              |
  |                                                              |
  |                                                              |
  |                                                              |
  |                                                              |
  |                                                              |
  |                                                              |
  |                                                              |
  |                                                              |
  |                                                              |
  | Select a choice and press ENTER to process data set action.  |
  |                                                              |
  └──────────────────────────────────────────────────────────────┘
```

5. Enter a '1' to confirm the delete action.

3.6 Backup Cloud Data Access Files

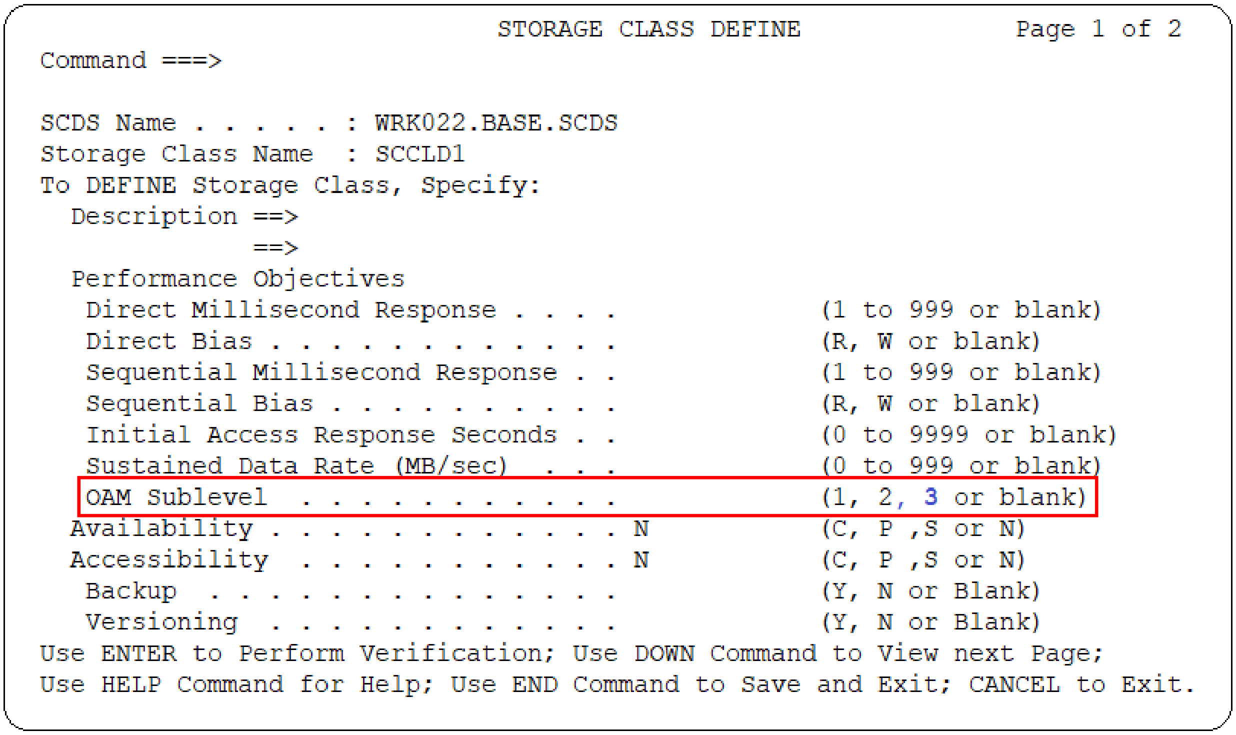
Once Cloud Data Access (CDA) has been configured, it is strongly recommended that an OAM administrator make a backup of all the files contained within the /*OAM_home_dir_name*/gdk directory.

4 OAM Setup

Note: More detail for each section below can be found in the OAM-Cloud-Support-Externals.docx document.

4.1 Define a Cloud Storage Class

Create or alter an existing Storage Class (and ACS routines if necessary) that will be used by OAM to direct objects to the cloud level in the OAM storage hierarchy. Set a new value of 3 in the “OAM Sublevel” field in conjunction with an Initial Access Response Seconds (IARS) value of 0 to direct objects utilizing this storage class to the cloud level.



```
                              STORAGE CLASS DEFINE             Page 1 of 2
Command ===>

SCDS Name . . . . . : WRK022.BASE.SCDS
Storage Class Name  : SCCLD1
To DEFINE Storage Class, Specify:
  Description ==>
              ==>
  Performance Objectives
   Direct Millisecond Response . . . .                 (1 to 999 or blank)
   Direct Bias . . . . . . . . . . . .                 (R, W or blank)
   Sequential Millisecond Response . .                 (1 to 999 or blank)
   Sequential Bias . . . . . . . . . .                 (R, W or blank)
   Initial Access Response Seconds . .                 (0 to 9999 or blank)
   Sustained Data Rate (MB/sec)  . . .                 (0 to 999 or blank)
   OAM Sublevel  . . . . . . . . . . .                 (1, 2, 3 or blank)
  Availability . . . . . . . . . . . . N               (C, P ,S or N)
  Accessibility  . . . . . . . . . . . N               (C, P ,S or N)
   Backup  . . . . . . . . . . . . . .                 (Y, N or Blank)
   Versioning  . . . . . . . . . . . .                 (Y, N or Blank)
Use ENTER to Perform Verification; Use DOWN Command to View next Page;
Use HELP Command for Help; Use END Command to Save and Exit; CANCEL to Exit.
```

4.2 Perform DB2 Updates

A new sample job, CBRSMCID, has been provided in SAMPLIB to assist in the creation and updating of required cloud level DB2 tables. Before running this job, ensure that the existing DB2 CBROAM storage group has an OCFSDTSP tablespace and FSDELETE table defined (File Storage Delete Table). If it does not, the sample job CBRSMR1D must be updated and executed before running CBRSMCID.

The first step of CBRSMCID will create a new OCCLDTSP tablespace and CLOUDID table. The second step will update the existing FSDELETE table with a new column.

After the updates have been completed, the DB2 bind jobs CBRPBIND and CBRABIND will both need to be run. Updated versions of these are also provided in SAMPLIB as a new package, CBRKCMC, has been added to both jobs.

In summary, the DB2 migration steps are as follows:

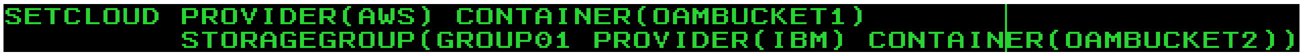
1. If necessary, update and run CBRSMR1D to create the FSDELETE table.
2. Update and run CBRSMCID to create the CLOUDID table and update the FSDELETE table.
3. Update and run the updated CBRPBIND.
4. Update and run the updated CBRABIND.

4.3 Create a SETCLOUD Statement in CBROAMxx PARMLIB

A new SETCLOUD statement has been added to configure the cloud level in the OAM storage hierarchy. Each object storage group intending to utilize the cloud level must specify a SETCLOUD statement to provide the cloud provider name and container name. Global values can be set and are used for all storage groups, but these will not override the specific storage group settings.

Note: The maximum length of a single SETCLOUD statement is 4096 characters. When specifying a large number of STORAGEGROUPs with lengthy container names, it might be necessary to use several different SETCLOUD statements.

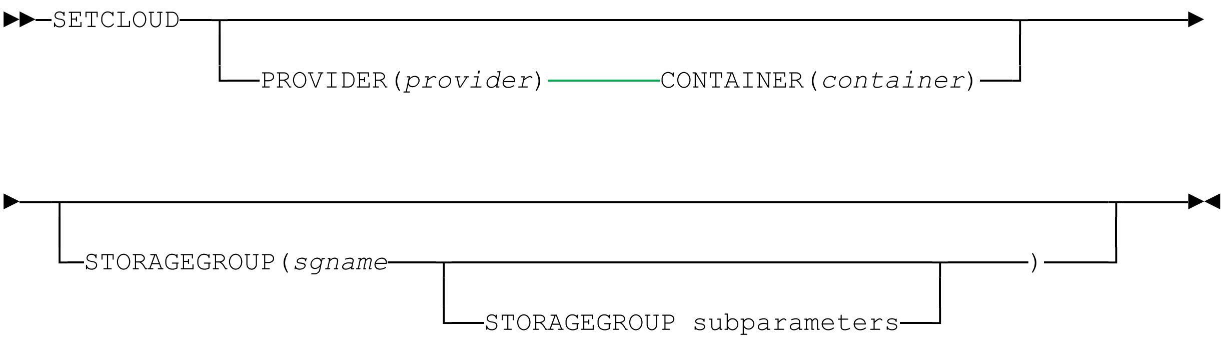
Example PARMLIB statement:



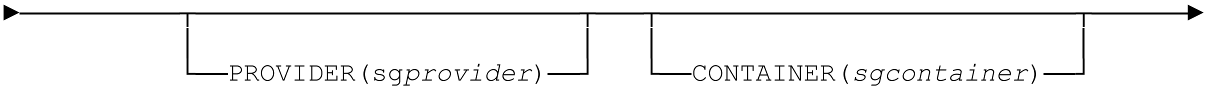
```
SETCLOUD  PROVIDER(AWS) CONTAINER(OAMBUCKET1)
          STORAGEGROUP(GROUP01 PROVIDER(IBM) CONTAINER(OAMBUCKET2))
```

This example would set a global provider for all storage groups to be AWS using a container value of OAMBUCKET1. The subsequent storage group setting would overwrite the global provider value with IBM and the container value OAMBUCKET2 only for storage group GROUP01.

The syntax for the SETCLOUD statement is as follows:



STORAGEGROUP subparameters



SETCLOUD Keyword Definitions

PROVIDER(*provider*)

Specifies the global provider name to be used for all storage groups for which there is no provider specified. *provider* must be 1 to 20 characters in length and must match the name defined in a Cloud Data Access (CDA) cloud provider definition file. Valid characters in the provider name are upper case alphabetic, numeric, @, #, and $. PROVIDER is required if CONTAINER is specified at the global level; otherwise it is optional. There is no default value.

CONTAINER(*container*)

Specifies the global container (or bucket) name to be used for all storage groups for which there is no container specified. The value for *container*:

- must be from 3 to 63 characters in length
- can only contain characters A-Z, a-z, 0-9, '.' (period), and '-' (hyphen)
- is case insensitive

Note: The cloud provider might have additional restrictions on the container name, but only the above are validated on the SETCLOUD statement. Refer to information from the cloud provider for the restrictions on the container (or bucket) name. If upper case letters are specified for this keyword, Cloud Data Access will convert the uppercase letters to lower case.

CONTAINER is required if PROVIDER is specified at the global level; otherwise it is optional. There is no default value.

STORAGEGROUP(*sgname*)

Specifies the name of an Object storage group which is in the active configuration, and which was previously defined using ISMF. This parameter on the SETCLOUD statement provides additional information beyond what was specified using ISMF for the Object storage group to which it pertains.

PROVIDER(*sgprovider*)

Specifies the desired cloud provider name. *sgprovider* must be from 1 to 20 characters in length and must match the name defined in a Cloud Data Access (CDA) cloud provider definition file. Valid characters in the provider name are upper case alphabetic, numeric, @, #, and $.

There is no default value.

If this keyword is not specified for a given storage group, the provider for that storage group is set using the PROVIDER set at the global level. PROVIDER is required if CONTAINER is specified for this storage group and PROVIDER is not specified at the global level.

CONTAINER(*sgcontainer*)

Specifies the name of the container in which the objects for this storage group are stored. If this keyword is not specified for a given storage group, the container for that storage group is set using the value set at the global level. The value for *sgcontainer*:

- must be from 3 to 63 characters in length
- can only contain characters A-Z, a-z, 0-9, '.' (period), and '-' (hyphen)

Note: The cloud provider might have additional restrictions on the container name, but only the above are validated on the SETCLOUD statement. Refer to information from the cloud provider for the restrictions on the container (or bucket) name. If upper case letters are specified, Cloud Data Access will convert the uppercase letters to lower case.

If this keyword is not specified for a given storage group, the container for that storage group is set using the CONTAINER set at the global level. CONTAINER is required if PROVIDER is specified for this storage group and CONTAINER is not specified at the global level.

5 Diagnostic Aids

5.1 General Information

To aid in diagnosing cloud request errors, OAM has added new OSREQ and OAM macro reason codes. These new codes will also percolate Cloud Data Access (CDA) and z/OS Web Enablement Toolkit reason codes. The new codes may be returned on OSREQ function calls as well as displayed in the system log through new message CBR6530I.

CBR6530I will be issued (if the diagnostic message threshold has not been reached) whenever an error has occurred while processing a cloud object request. This message provides additional diagnostic information that has been percolated from the service in the stack that encountered the error. These services include OAM, z/OS Web Enablement Toolkit, Cloud Data Access (CDA), and the cloud storage provider.

> Note: CBR6530I may not be issued if the threshold for diagnostic messages has been met. In this case, please refer to the OAM Cloud Tier Externals document, section 3.0.5.1 on Starting and Stopping Diagnostic Messages.

CBR6530I provides the following diagnostic information:

1. OAM cloud function failure (write, read, delete), Collection name, Object name, Cloud ID and OAM reason code.
2. For a LE Preinitialization failure, the failing PIPI function name and *PIPI-return-code* are displayed.
3. For a CDA service failure, the return code *CDA-return-code* provided by CDA is displayed. Additionally, if the CDA return code denotes that the error was a web toolkit failure or a bad response from the cloud provider, a second status area will be displayed after the CDA return code area.
4. For a web toolkit failure, the return code *toolkit-return-code*, the reason code *toolkit-reason-code*, the service ID *toolkit-service-ID*, and one or more lines (up to 70 characters each) of diagnostic messages *toolkit-diagnostic-message* will be shown.
5. If a bad HTTP response code is received from the cloud provider, the cloud provider status code *cloud provider-status-code* and one or more lines (up to 70 characters each) of cloud provider status messages *cloud-provider-status-message* will be shown.

5.2 OSREQ and OAM Macro Return and Reason Codes

The following OSREQ reason codes are added for return code 12 (X'0C'):

69 – yy zz	Cloud Data Access detected failure. Look up the Cloud Data Access reason code. yy zz is the CDA reason code.
6A – yy zz	Web Toolkit detected failure. Look up the Web Toolkit reason code. yy zz is the Web Toolkit reason code.
6B – yy zz	Cloud Provider detected failure. Look up the Cloud Provider reason code. yy zz is the Cloud Provider Reason Code

The following OAM macro reason codes are added for return code 8 (X'08'):
X'05A0' CBRCLD.BUFLEN INVALID OR MISSING
X'05A1' CBRCLD.BUFLEN IS LESS THAN CBRCLD.LENGTH
X'05A2' CBRCLD.BUFTOKEN AND CBRCLD.BUFFADDR BOTH MISSING
X'05A3' CBRCLD.BUFTOKEN AND CBRCLD.BUFFADDR BOTH PRESENT

X'05A4' CBRCLD.COLNAME IS INVALID OR MISSING
X'05A5' CBRCLD.CLOUDID IS MISSING ON A DELETE
X'05A6' CBRCLD.CLOUDID IS MISSING ON A READ
X'05A7' CBRCLD.CLOUDID IS PRESENT ON A WRITE
X'05A8' CBRCLD.CLINSTID IS MISSING ON A DELETE
X'05A9' CBRCLD.CLINSTID IS MISSING ON A READ
X'05AA' CBRCLD.CLINSTID IS PRESENT ON A WRITE
X'05AB' CBRCLD.OBJNAME IS INVALID OR MISSING
X'05AC' CBRCLD.OSREQ IS INVALID OR MISSING
X'05AD' CBRCLD PARM BLOCK ADDRESS IS ZERO
X'05AE' CBRCLD PARM BLOCK EYECATCHER IS INVALID
X'05AF' CBRCLD CLOUD REQUEST IS UNKNOWN
X'05B0' CBRCLD.GROUP IS INVALID OR MISSING
X'05B1' CBRCLD.SYSNAME IS INVALID OR MISSING
X'05B2' CBRCLD.WTDPTR IS PRESENT ON A DELETE
X'05B3' CBRCLD.WTDPTR IS MISSING ON A READ
X'05B4' CBRCLD.WTDPTR IS MISSING ON A WRITE
X'05B5' CBRCLD.CONNTOKN IS MISSING
. . .
X’0713’ No storage groups are cloud enabled
X’0714’ No cloud ID specified for cloud read or delete
X’0715’ Invalid cloud id for cloud read
. . .
X’0B30’ Cloud streaming send exit failure from CDA
X’0B31’ Cloud streaming receive exit failure from CDA
X’0B32’ Cloud ID row not found in DB2
X’0B33’ Internal error from CDA
X’0B34’ Error from the web tool kit
X’0B35’ Error from the cloud provider

The following OAM macro reason codes are added for return code 12 (X'0C'):

X’0B83’ Read of an object from the cloud failed. Access Backup is active for cloud errors; for OSREQ requests a read may be attempted for the backup copy of the object.

X’0B84’ LCS cloud tasks not operational

X’0B85’ PROVIDER or CONTAINER not defined for the object storage group

The following OAM macro reason codes are added for return code 16 (X'10'):
X’0C04’ Abend caused by bad CBRCLDP parameter list

. . .

X'0D90' File system/Cloud driver unable to MVS LOAD LE CELQPIPI/CEEPIPI
X'0D91' File system/Cloud driver unable to start LE CELQPIPI/CEEPIPI
X'0D92' File system/Cloud driver unable to end LE CELQPIPI/CEEPIPI
X'0D93' File system/Cloud driver unable to invoke LE CELQPIPI/CEEPIPI

. . .

X’0DB0’ Cloud ID CAF error from DB2
X’0DB1’ Cloud ID SQL error from DB2
X’0DB2’ Cloud processing internal logic error

The following OAM macro reason codes are updated:
X'0712' Missing instance id on a file system or cloud read or delete request

X'0B82' Object to be deleted from file system or cloud could not be added to file storage delete table

5.3 Cloud error information

OAM interacts with the cloud provider through Cloud Data Access (CDA) services when reading, writing, or deleting objects in the cloud level. CDA returns information about various errors to OAM including errors detected during processing within CDA itself (such as a configuration error), errors that occur while attempting to contact the cloud provider, or errors reported by the cloud provider.

5.4 Cloud Data Access Return Codes

0	Success
100	Unable to read the keyfile
101	Unable to write the keyfile
102	Unable to parse the keyfile
103	Keyfile was likely modified manually in an incorrect manner
104	Keyfile does not contain the user-specified cloud provider
105	Keyfile has no matching resource match for the given cloud provider
106	Keyfile could not be updated due to severe error
107	Keyfile resource could not be deleted due to severe error
108	Keyfile resource could not be added due to severe error
109	No credentials found for a given cloud resource
110	The provider specification file could not be opened
111	The provider specification file could not be parsed
112	The requested feature is not supported
113	The provided buffer is too small for the requested data
114	Invalid authorization parameters
115	Unable to open local file
116	Error applying the authorization calculations
117	The GDKKEYAD service was unable to generate a symmetric key
118	Keyfile doesn't have any entries specified for the current user
119	Decrypted key resulted in invalid data
120	Invalid return code provided for text translation
121	No associated text for specified return code
122	ICSF error occurred
123	httpMethod is not HTTPS
799	Unexpected error
800	Connection to the cloud provider could not be established
801	Web toolkit returned a bad return code

850	XML parser returned a bad return code
900	Requested object/resource could not be found (HTTP 404)
901	Denied access (HTTP 403)
902	The requested cloud provider operation is not supported
903	Response is not what was expected
904	Request failed (bad HTTP response code)