IBM i
1.2

IBM Cloud Storage Solutions for i
User's Guide

Note

Before using this information and the product it supports, read the information in “Notices” on page 47.

This edition applies to version 1, release 2, modification 0 of IBM® Cloud Storage Solutions for i (product number 5733-ICC) and to all subsequent releases and modifications until otherwise indicated in new editions. This version does not run on all reduced instruction set computer (RISC) models nor does it run on CISC models.

This document may contain references to Licensed Internal Code. Licensed Internal Code is Machine Code and is licensed to you under the terms of the IBM License Agreement for Machine Code.

Contents

Chapter 1. IBM Cloud Storage Solutions for i V1.2.0 User's Guide

IBM Cloud Storage Solutions for i V1.2.0 User's Guide

Summary of changes

Changes made to IBM Cloud Storage Solutions for IBM i V1.2.0.

February 2021

"Cloud Storage Solutions system requirements" on page 3 is updated to say that both **HOSTNAME** and **DMNNAME** must be correctly configured before Cloud Storage Solutions is installed.

June 2020

Google Cloud Storage is added as a supported cloud service provider.

November 2017

Cloud Storage Solutions Advanced Edition

Cloud Storage Solutions is now available in an Advanced Edition. The Advanced Edition includes file compression and at rest file encryption. The basic edition includes features in previous releases, plus SSL transfer encryption, and a job monitor that tracks file transfers.

Cloud Storage Solutions Advanced Edition is available to everyone for 70 days after installation. After 60 days you will be prompted with warnings that Advanced Edition features will expire, and that you can upgrade to the Advanced Edition at any time. After 70 days you will only have basic edition features.

Compression, encryption, and SSL

You can configure Cloud Storage Solutions to compress files before copying them to the cloud to improve transfer performance with very large files. You can configure Cloud Storage Solutions to encrypt files before copying them to the cloud, so that they are encrypted while "at rest" in the cloud. And you can configure Cloud Storage Solutions to encrypt files while the files are being transferred to and from the cloud.

Compression and "at rest" encryption are available with the Cloud Storage Solutions Advanced Edition. Transfer encryption is available with all editions.

Job monitor

The job monitor tracks file transfers to maintain accurate information in the Cloud Storage Solutions database and send that information to the Cloud Storage Solutions exit point. It includes two jobs, QICCJOBMON and QICCEXTPRC, that must always be running in the Cloud Storage Solutions subsystem (QICCSBS).

PDF file for IBM Cloud Storage Solutions for i V1.2.0 User's Guide

You can view and print a PDF file of this information.

To view or download the PDF version of this document, select IBM Cloud Storage Solutions for i V1.2.0 User's Guide.

Saving PDF files

To save a PDF on your workstation for viewing or printing:

1. Right-click the PDF link in your browser.
2. Click the option that saves the PDF locally.
3. Navigate to the directory in which you want to save the PDF.
4. Click **Save**.

Downloading Adobe Reader

You need Adobe Reader installed on your system to view or print these PDFs. You can download a free copy from the Adobe Web site (https://get.adobe.com/reader/).

IBM Cloud Storage Solutions for i

IBM Cloud Storage Solutions for i is the IBM solution for storing IBM i files in the cloud.

You can use Cloud Storage Solutions to copy files securely to and from the cloud, eliminating the need for tape drives, tape cartridges, and courier services for off-site storage.

To use Cloud Storage Solutions you must obtain cloud server space. You can obtain space by creating an account with a third-party cloud service provider. Or you can obtain space by configuring your own server to use the File Transfer Protocol (FTP) and act as a cloud server.

After you obtain cloud server space, you can create a Cloud Storage Solutions resource to represent that space. For example, a resource can represent an account with a cloud provider or an FTP-enabled server. You can then use the resource to copy files between the IBM i computer and the cloud space represented by the resource.

To work with resources and files directly, you can use the Cloud Storage Solutions native IBM i interface. To program your applications to work with resources and files you can use the Cloud Storage Solutions APIs.

Cloud Storage Solutions passes cloud file transfer information to a registered IBM i exit point. To have your applications receive that information, you can register the applications as exit programs and associate them with the Cloud Storage Solutions exit point.

You can use Backup, Recovery, and Media Services (BRMS) for i5/OS with Cloud Storage Solutions to transfer virtual save media to and from the cloud. For more information on using Cloud Storage Solutions with BRMS, see the Using Cloud Storage Solutions for i with BRMS wiki page.

Service updates and support information

Service updates and support information for this product, including software fix packs, PTFs, frequently asked questions (FAQs), technical notes, troubleshooting information, and downloads, are available from the web.

To find service updates and support information, see the following website:

https://www-947.ibm.com/support/entry/portal/support?lnk=msdTS-supo-usen

Product documentation and updates

IBM Cloud Storage Solutions for i information is available on the web. You can receive updates to Cloud Storage Solutions information automatically by registering with the IBM My Notifications service.

Information on the web

You can access Cloud Storage Solutions documentation in the IBM i 7.1, 7.2 and 7.3 sections of the IBM Knowledge Center:

http://www.ibm.com/support/knowledgecenter

Receiving documentation updates automatically

To automatically receive emails that notify you when new technote documents are released, when existing product documentation is updated, and when new product documentation is available, you can register with the IBM My Notifications service. You can customize the service so that you receive information about only those IBM products that you specify.

To register with the My Notifications service:

1. Go to http://www.ibm.com/support/mysupport
2. Enter your IBM ID and password, or create one by clicking **Create an IBM id**.
3. When the My Notifications page is displayed, click **Subscribe** to select those products that you want to receive information updates about.
4. Click **Continue** to specify the types of updates that you want to receive.
5. Click **Submit** to save your profile.

Accessibility features

Accessibility features help users who have a disability, such as restricted mobility or limited vision, to use information technology products successfully.

The following list includes the major accessibility features in this product:

- Keyboard-only operation
- Interfaces that are commonly used by screen readers
- Keys that are discernible by touch but do not activate just by touching them
- Industry-standard devices for ports and connectors
- The attachment of alternative input and output devices

Also see the IBM® Human Ability and Accessibility Center for more information about the commitment that IBM has to accessibility.

Cloud Storage Solutions system requirements

Before you install Cloud Storage Solutions, you must meet the following software requirements.

Prerequisites

Ensure that both **HOSTNAME** and **DMNNAME** are correctly configured before Cloud Storage Solutions is installed.

PTFs

Install the following IBM PTFs on the appropriate IBM i version for product 5770SS1:

- IBM i version 7.1.0: PTF number SI65711
- IBM i version 7.2.0: PTF number SI65710
- IBM i version 7.3.0: PTF number SI65678

Cloud Storage Solutions administration

Administering Cloud Storage Solutions involves meeting the system requirements; obtaining cloud storage space; deciding which license you need and then installing it; and preparing to encrypt files. See the administration notes for warnings and best practices.

Obtaining cloud storage space

To use Cloud Storage Solutions you must obtain cloud server space. You can create an object storage account with a third-party cloud service provider, or you can use your own computer as a cloud server by configuring it to use the File Transfer Protocol (FTP).

Using third-party cloud providers

When you create an object storage account with a cloud service provider, they send you the location of your cloud server space and the credentials needed to access that space. For information on creating accounts, see any of the following supported cloud providers:

- AWS S3: https://aws.amazon.com
- IBM Cloud Object Storage: https://www.ibm.com/cloud-computing/products/storage/object-storage/cloud/

Using your own cloud server

You can also use any IBM i, Linux, or AIX computer with FTP installed as the cloud server. In this scenario, you must install FTP on both the target computer and the host IBM i computer so that the two computers can communicate. For information on installing FTP on IBM i, see the IBM Knowledge Center topic Installing TCP/IP. For information on installing FTP on Linux or AIX see the documentation for those operating systems.

Licensing Cloud Storage Solutions

You can use Cloud Storage Solutions for a 70-day trial period. After that you must purchase a license.

About this task

With the Cloud Storage Solutions license you can install one instance of Cloud Storage Solutions on one partition.

The Cloud Storage Solutions Advanced Edition includes file compression and at rest file encryption. The basic edition includes features that were in all previous releases, plus SSL transfer encryption, and the job monitor.

Cloud Storage Solutions Advanced Edition is available to everyone during the 70-day trial period. After 60 days you will be prompted with warnings that Advanced Edition features will expire, and that you can upgrade to the Advanced Edition at any time. After 70 days you will only have basic features.

When you purchase the product, IBM sends you license information, including the license key. If you are upgrading the product, installing the new key overrides the previous key. You cannot uninstall license keys. For more information on IBM i license keys, see the topic Software license keys.

Procedure

Take the following steps to install the Cloud Storage Solutions license:

1. Log in to the IBM i computer as a user with *ALLOBJ authority.
2. To prompt the **Work with License Information** command, type the following command and press Enter:

```
WRKLICINF
```

3. Type 1 in the **Opt** field of the following row:

Product	License Term	Feature	Description
5733ICC	V1R2M0	5101	Cloud Storage

4. If you purchased the Advanced Edition, type 1 in the **Opt** field of the following row:

Product	License Term	Feature	Description
5733ICC	V1R2M0	5102	Advanced

5. Press Enter.
6. In the **Add License Key Information** panel, enter the required license information provided by IBM, and press Enter.

Cloud Storage Solutions administration notes

Before administering Cloud Storage Solutions, read the following warnings and best practices.

After upgrade, re-enter existing resource user IDs and passwords
In Cloud Storage Solutions version 1.2, the encryption of resource user names and passwords has been enhanced. If you upgrade from version 1.1 to version 1.2, after you upgrade you must edit each existing resource and re-enter the user ID and password. If you do not re-enter this information you cannot copy file using the resource.

Do not cancel the QICCJOBMON and QICCEXTPRC jobs

The QICCJOBMON and QICCEXTPRC jobs must always be running in the Cloud Storage Solutions subsystem (QICCSBS). They are critical to maintaining and publishing accurate Cloud Storage Solutions data. The QICCJOBMON (job monitor) job monitors file transfers and maintains accurate information in the database. The QICCEXTPRC (exit processor) job sends database information to the Cloud Storage Solutions exit point.

These jobs start when the QICCSBS subsystem starts and end in an orderly way when that subsystem stops.

Small TCP/IP buffers and high network traffic on an IBM i computer affect FTP transfer speeds
If your FTP file copies are slow, check the TCP/IP send and receive buffer sizes on the host IBM i computer using the CHGTCPA command. These default buffer sizes are both 65535, but they can be changed by a system administrator to manage network traffic to and from the computer. Small buffers or high network traffic affect transfer speeds to and from FTP cloud resources.

Cloud Storage Solutions Security

Cloud Storage Solutions encryption

To keep your data secure, you can use Secure Sockets Layer (SSL) to encrypt files while they are transferred to and from the cloud. You can also use Advanced Encryption Standard (AES) symmetric encryption to encrypt files before they are copied to the cloud, so that they remain encrypted while "at rest" in the cloud.

Configuring Cloud Storage Solutions file transfer encryption

You can configure Cloud Storage Solutions to use Secure Socket Layer (SSL) to encrypt files while those files are being transferred to and from the cloud.

Before you begin

- This task includes steps for creating a *SYSTEM certificate keystore. This keystore may have already been created. If so, you will require its password. Ask your IBM i administrator for that information.

- To encrypt the files, you must download the correct certificate authorities from your cloud provider. To download the certificate authorities, you must enter your cloud storage Uniform Resource Identifier (URI) in a browser. When you create an account with a third-party cloud provider, the provider sends you this storage URI. You must make sure that the URI that you enter to download the certificate authorities is your actual storage location URI. If it is not, you will download the wrong certificate authorities and resource actions will fail.

  When you enter the URI in a browser, some provider sites automatically redirect you to a different page. If you are redirected, you must edit the URI to match your storage URI. Also, S3 resources are automatically generated. For example, when you create an S3 resource you provide the URI https://s3.amazonaws.com. But your actual bucket location might be https://companyA-west.s3.amazonaws.com/companyA-west, or something similar. You must make sure you enter the correct S3 URI.
- You must know any policies within your enterprise that dictate SSL options you must use, such as SSL protocol, SSL cipher, and SSL signature algorithm.

About this task

To configure Cloud Storage Solutions for SSL encryption, you must download certificate authorities from the resource URI that you received from the cloud provider when you created the account. You can then use the IBM i Digital Certificate Manager (DCM) to create a *SYSTEM certificate keystore, add the certificate authorities to the keystore, and then associate the certificate authorities with the Cloud Storage Solutions application.

After you configure SSL, you must create or change resources that use the account and include the https protocol in their resource URIs. Files copied to the cloud using that resource are then encrypted while they are being copied, and decrypted when they reach the cloud computer. When you copy files from the cloud back to a host IBM i computer using the same resource, the files are encrypted while copied and then decrypted on the IBM i using the same key that encrypted them.

To encrypt files while they are "at rest" on the cloud computer, see “Configuring Cloud Storage Solutions file at rest encryption” on page 8.

SSL encryption is available with the Cloud Storage Solutions basic edition.

For general information on using SSL on IBM i, see the IBM i Security Sockets Layer Guide.

Procedure

Take the following steps to configure SSL encryption:

1. Create a *SYSTEM certificate keystore:
   a) Log into IBM Navigator for i as a user with authority to use the Digital Certificate Manager.
   b) In the navigation pane, click **Internet Configurations**.
   c) Click **Digital Certificate Manager**.
   d) Click **Create New Certificate Store**.
   e) Select ***SYSTEM**, and then click **Continue**.

      Note : If the only option is **Other System Certificate Store**, a *SYSTEM certificate store already exists. Click **Cancel** and proceed to Step 2.
   f) Select **No - Do not create a certificate in the certificate store**.
   g) Enter a password for the certificate keystore, enter it again to confirm it, and then click **Continue**.
   h) Click **OK**. Do not log out.
2. Download the certificate authorities from the resource URI location. For example, in Chrome browsers on Microsoft Windows take the following steps:
   a) In a browser, enter the resource URI. (If the site displays an "Unauthorized" page, continue.)

      Make sure the cloud provider web site does not redirect you to another page. If so, edit the URI to exactly match your resource URI.

b) Click the browser Customize and control icon.

c) Select **More tools** > **Developer tools**.

d) Click the **Security** tab, and then click **View Certificate**.

e) In the Certificate dialog, click the Details tab.

f) Click **Copy to File**.

g) In the Certificate Export Wizard, click **Next**.

h) Select the **Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)** format, and then select **Include all certificates in the certification path if possible**.

Regardless of your browser, you must make sure that all certificate authorities in the certificate path are downloaded.

i) Click **Browse** to specify a file name and local location, then save the file.

j) Copy the certificate file to any directory on the IBM i computer.

3. Import the certificate into the *SYSTEM keystore:

a) In IBM Navigator for i, open the Digital Certificate Manager.

b) In the navigation pane, click **Select a Certificate Store**.

c) Select ***SYSTEM**, and then click **Continue**.

d) In the **Certificate store password** field, enter the *SYSTEM keystore password you created in Step 1, and then click **Continue**. The navigation pane displays tasks that you can perform with the *SYSTEM keystore.

e) In the navigation pane, click **Manage Certificates** > **Import certificate**.

f) Select **Certificate Authority (CA)** as the type of certificate to import, and then click **Continue**.

g) Enter the path and file name of the certificate file that you copied to the IBM i computer in Step 2, and then click **Continue**.

h) Enter a label for the certificate, and then click **Continue**. The certificate is imported into the *SYSTEM keystore. Click **OK**. Do not log out of the Digital Certificate Manager.

4. Add Cloud Storage Solutions to the list of client applications:

a) In the Digital Certificate Manager navigation pane, click **Manage Applications** > **Add applications**.

b) Select **Client**, and then click **Continue**.

c) In the Add application page, in the **Application ID** field, type `IBM_QICC`.

d) Select **Application description** and in the field type `IBM Cloud Storage Solutions for i`.

e) In the **Define the CA trust** list field, select **No**.

f) Select any SSL values that match your enterprise policies, such as the SSL protocol, SSL cipher, or SSL signature algorithm.

g) Click **Add**, then click **OK**.

5. Add the certificate authorities to the Cloud Storage Solutions trust list:

a) In the Digital Certificate Manager navigation pane, click **Manage Applications** > **Define CA trust list**.

b) Select **Client**, and then click **Continue**.

c) Select **IBM Cloud Storage Solutions for i**, and then click **Define CA Trust List**.

d) Select all of the certificate authorities that you imported in Step 3, and then click **OK**.

What to do next

To enable SSL in a resource, create or change the resource and specify the https protocol in the resource URI.

Configuring Cloud Storage Solutions file at rest encryption

You can configure Cloud Storage Solutions to make sure files are encrypted while they are "at rest" in the cloud, and are decrypted when they are copied back from the cloud.

About this task

Cloud Storage Solutions encrypts at rest files using the Advanced Encryption Standard (AES) symmetric encryption algorithm with a 128-bit key length. To encrypt files, you must create a keystore file. Then you create a key with a label and add the key to the keystore file.

After you create the keystore file and key, you can create or change a resource and provide keystore and key information. Then files copied to the cloud using that resource are encrypted before they are copied, and remain encrypted while at rest in the cloud. When you copy encrypted files from the cloud back to a host IBM i computer using the same resource, the files are decrypted using the same key that encrypted them.

To encrypt files as they are copied to and from the cloud using SSL, see “Configuring Cloud Storage Solutions file transfer encryption” on page 5. If SSL and at rest encryption are both enabled, the files are double-encrypted while they are copied.

If your cloud provider has their own at rest encryption, it is recommended that you use their encryption.

At rest encryption is available with the Cloud Storage Solutions Advanced Edition.

For more information on creating keystore files and labeled keys on IBM i, see the topic Managing cryptographic keystore files in the IBM Knowledge Center. For comprehensive IBM i security information, see the IBM System i Security: Protecting i5/OS Data with Encryption redbook.

Procedure

Take the following steps to configure at rest encryption:

1. Log into IBM Navigator for i.
2. In the navigation pane, click **Security** > **All Tasks** > **Cryptographic Services Key Management** > **Manage Master Keys**.
3. Select **1**, and then in the **Select Action** drop down, select **Load Part**.
4. In the Load Master Key Part dialog, type a passphrase and then click **OK**.
5. In the Manage Mast Keys dialog, select **1** again, and in the **Select Action** drop down, select **Set**.

   In the **1** row, the **Type** column value is **Set** and the **Current Key Verification Value** column contains a long alphanumeric value.
6. Click Close.
7. In the navigation pane, click **Security** > **All Tasks** > **Cryptographic Services Key Management** > **Manage Keystores**.
8. Click **Create New Keystore**, then type keystore details and click **OK**. In the Manage Keystores dialog you should see the new keystore listed.
9. Select the new keystore and click **Actions** > **Open keystore**.
10. Click **New Key Record**, type a label for the new key, and then click **Next**.
11. In the Functions not allowed dialog, do not select any functions. Click **Next**.
12. In the Key type dialog, select AES, and then click **Next**.
13. In the Key value generation dialog, select **Generate automatically**, and then click **Next**.
14. In the **AES key size (in bits)** field, type 128, and then click **Next**.
15. In the Summary dialog, make sure your selections are accurate. Click **Back** to make changes, or click **Finish**.

What to do next

To enable at rest encryption in a resource, create or change the resource and specify the required keystore, library, and key label information.

Working with resources in Cloud Storage Solutions

Use Cloud Storage Solutions commands to create, change, and display resources. A resource defines a cloud server location and the credentials needed to access that location.

The cloud service provider or FTP server administrator must provide the location and credential information for the resource. Cloud Storage Solutions supports several cloud service providers, including Amazon Simple Storage Service (Amazon S3), Google Cloud Storage, and IBM Cloud Object Storage.

To create and use resources, you can use Cloud Storage Solutions commands or the Cloud Storage Solutions API to copy files between IFS directories on the IBM i computer and the cloud server. You cannot work with files in the /QSYS.LIB file system.

Creating AWS S3, IBM Cloud Object Storage, or Google Cloud Storage resources

Use the **CRTS3RICC** command to create a Cloud Storage Solutions AWS S3 or IBM Cloud Object Storage resource. A resource defines a cloud server location and the credentials needed to access that location. After you create a resource, you can copy files between IFS directories and the cloud server location.

Before you begin

You must obtain storage space on an AWS S3 or IBM Cloud Object Storage cloud server. See "Obtaining cloud storage space" on page 4 for information.

You must decide on a unique resource name. The name can have a maximum of 10 characters, and must be unique among Cloud Storage Solutions resources. Resource names are IBM i basic names that must adhere to the *NAME type restrictions. Every basic name can begin with the characters A-Z, $, #, or @ and can be followed by up to nine characters. The remaining characters can include the same characters as the first but can also include numbers 0-9, underscores (_), and periods (.). Lowercase letters are changed to uppercase letters by the system. For more information, and information on names in quoted form, see the topic *Names (*NAME)* in the IBM Knowledge Center.

If you have Cloud Storage Solutions Advanced Edition, you can specify that Cloud Storage Solutions encrypt files at rest in the cloud when they are copied there using this resource. To specify a resource for at rest encryption, you must obtain the keystore file name and library, and the key label, from the administrator who created them on the IBM i computer. For more information on encryption, see "Cloud Storage Solutions encryption" on page 5.

Obtain the following information from the cloud service provider:

- The name of a user who is authorized to access the cloud server location.
- The authorization key required to access the cloud server location.
- The name of the resource bucket. A bucket is a directory in the cloud server location that acts as a root directory. When you copy files to the cloud they are placed below the specified bucket directory. You must create the bucket directory before you can copy files to it. Bucket names are case-sensitive; when specifying the name you must use the correct case.
- The Uniform Resource Identifier (URI) of the storage location. For AWS S3 resources this is always `s3.amazonaws.com`. For IBM Cloud Object Storage resources, ask the account owner. Or if the storage location is configured inside your enterprise network, ask your administrator. If you enable at rest encryption, include the https:// protocol at the beginning of the URI, for example `https://s3.amazonaws.com`. For Google Cloud Storage, this is always `storage.googleapis.com`.

About this task

If you have Cloud Storage Solutions Advanced Edition, you can specify that Cloud Storage Solutions compress files before copying them to the cloud, and then decompress the files after copying them from the cloud. You can enable compression when you create or change the resource.

You cannot use Cloud Storage Solutions to work with files in the /QSYS.LIB file system. This command is not threadsafe.

Procedure

1. On the IBM i command line, type **CRTS3RICC** and press F4.
2. Complete the following required fields, and press Enter:

Field	Action
Resource name	Type a unique resource name that is a maximum of 10 characters and follows the *NAME restrictions for an IBM i basic name.
Resource description	Type a description that is a maximum of 50 characters.
Access key id	Type the name of the authorized user.
Secret access key	Type the authorization key.
Use compression	Type *YES to compress files before they are copied to the cloud. Compression is available with Advanced Edition.
Use encryption	Type *YES and press Enter, then provide values in sub-fields. Encryption is available with Advanced Edition.
Keystore file	A subfield of the **Use encryption** field. Type the name of the keystore file.
Library	A subfield of the **Keystore file** field. Type the name of the library that contains the keystore file.
Key label	A subfield of the **Use encryption** field. Type the name of the key label.
Bucket	Type the name of the bucket directory, using the correct case. You must create this directory before you can copy files to it.
Resource URI	Type one of the following resource URIs: • For AWS S3 resources type: `s3.amazonaws.com` • For IBM Cloud Object Storage resources, ask the account owner or your administrator. • For Google Cloud Storage, `storage.googleapis.com`. If you have enabled at rest encryption, include the secure protocol https:// at the beginning of the URI.
Full qualified IFS Dir name	[This parameter is not currently implemented.] Optional. To display, press F10 and page down. Type the fully-qualified path location of the

Field	Action
	directory to associate with the resource. After you copy files from this directory to the cloud server, the files in both locations are kept in sync. The default value is *NONE.

What to do next

To copy files to the resource, see "Copying files to the cloud" on page 19.

Changing AWS S3. IBM Cloud Object Storage, or Google Cloud Storage resources

Use the **CHGS3RICC** command to change an AWS S3 or IBM Cloud Object Storage resource. A resource defines an AWS S3 or IBM Cloud Object Storage cloud server location and the credentials needed to access that location. Change a resource to use different credentials to access the same bucket, or to specify a different bucket.

Before you begin

If you have Cloud Storage Solutions Advanced Edition, you can specify that Cloud Storage Solutions encrypt files at rest in the cloud when they are copied there using this resource. To specify a resource for at rest encryption, you must obtain the keystore file name and library, and the key label, from the administrator who created them on the IBM i computer. For more information on encryption, see "Cloud Storage Solutions encryption" on page 5.

About this task

If you have Cloud Storage Solutions Advanced Edition, you can specify that Cloud Storage Solutions compress files before copying them to the cloud, and then decompress the files after copying them from the cloud. You can enable compression when you create or change the resource.

You cannot change the resource name with this command. This command is not threadsafe.

Procedure

1. On the IBM i command line, type **CHGS3RICC** and press F4.
2. In the **Resource name** field, type the name of the resource, and press Enter.
   If you do not know the resource name, press F4 to display a list of resources.
3. Edit one or more of the following fields, and press Enter:

Field	Action
Resource description	Change the description.
Access key id	Change the name of the authorized user. For security reasons, the default value is *SAME. To keep the original name, do not change the *SAME value.
Secret access key	Change the authorization key. For security reasons, the default value is *SAME. To keep the original key, do not change the *SAME value.
Bucket	Change the bucket name, using the correct case. This does not change the name of the bucket on the cloud server. It changes which bucket the resource will access.

Field	Action
Use compression	Type *YES to compress files before they are copied to the cloud. Compression is available with Advanced Edition.
Use encryption	Type *YES and press Enter, then provide values in subfields. Encryption is available with Advanced Edition.
Keystore file	A subfield of the **Use encryption** field. Type the name of the keystore file.
Library	A subfield of the **Keystore file** field. Type the name of the library that contains the keystore file.
Key label	A subfield of the **Use encryption** field. Type the name of the key label.
Resource URI	Change the resource URI. For AWS S3 resources the URI must be `s3.amazonaws.com`. For Google Cloud Storage, `storage.googleapis.com`. You can change IBM Cloud Object Storage URIs. If you have enabled at rest encryption, include the secure protocol https:// at the beginning of the URI.
Full qualified IFS Dir name	[This parameter is not currently implemented.] Optional. To display, press F10 and page down. Change the fully-qualified path location of the directory to associate with the resource. After you copy files from this directory to the resource, Cloud Storage Solutions keeps the files in both locations synchronized. Type *NONE to remove the current data and set the value to *NONE.

Displaying AWS S3, IBM Cloud Object Storage, or Google Cloud Storage resources

Use the **DSPS3RICC** command to display an AWS S3 or IBM Cloud Object Storage resource. A resource defines an AWS S3 or IBM Cloud Object Storage cloud server location and the credentials needed to access that location.

About this task

For security reasons, the **DSPS3RICC** command does not display the **Access key id** and **Secret access key** fields. This command is not threadsafe.

Procedure

1. From the IBM i command line, type **DSPS3RICC** and press F4.
2. In the **Resource name** field, type the name of the resource, and press Enter.
   If you do not know the resource name, press F4 to display a list of resources.

Creating FTP resources

Use the **CRTFPRICC** command to create an FTP resource. After you create the resource, you can copy files between IFS directories and the resource.

Before you begin

Choose a unique resource name that is a maximum of 10 characters. Resource names must be unique among all providers and transfer types. A resource name is an IBM i basic name that must adhere to the *NAME type restrictions. Every basic name can begin with the characters A-Z, $, #, or @ and can be followed by up to nine characters. The remaining characters can include the same characters as the first but can also include numbers 0-9, underscores (_), and periods (.). Lowercase letters are changed to uppercase letters by the system. For more information, and information on names in quoted form, see the topic *Names (*NAME)* in the IBM Knowledge Center.

If you have Cloud Storage Solutions Advanced Edition, you can specify that Cloud Storage Solutions encrypt files at rest in the cloud when they are copied there using this resource. To specify a resource for at rest encryption, you must obtain the keystore file name and library, and the key label, from the administrator who created them on the IBM i computer. For more information on encryption, see "Cloud Storage Solutions encryption" on page 5.

Obtain the following information from the server administrator:

- The ID and password of a user who is authorized to log into the FTP server, and who has access to the root directory.
- The root directory on the FTP server. When you copy files to the cloud they are placed below the specified root directory. You must create the root directory before you can copy files to it. FTP root directory names are not case-sensitive on the IBM i system; `/home/backups` and `/HOME/Backups` are the same path.
- The resource Uniform Resource Identifier (URI) of the FTP server including the fully-qualified name of computer that hosts the FTP server, for example, `myserver.enterprise.com`. The protocol (ftp://) is optional unless you enable at rest encryption, then include the ftps:// protocol at the beginning of the URI, for example:

  ```
  ftps://myserver.enterprise.com
  ```

  If the FTP port is 21 it is optional. The port number must be included if a value other than 21 is in use. For example:

  ```
  ftps://myserver.enterprise.com
  ftps://myserver.enterprise.com:23
  ```

About this task

If you have Cloud Storage Solutions Advanced Edition, you can specify that Cloud Storage Solutions compress files before copying them to the cloud, and then decompress the files after copying them from the cloud. You can enable compression when you create or change the resource.

FTP resources can target Linux, AIX, or IBM i computers. You cannot use Cloud Storage Solutions to work with files in the /QSYS.LIB file system. This command is not threadsafe.

Procedure

1. From the IBM i command line, type **CRTFPRICC**, and press F4.
2. Complete the following required fields, and press Enter:

Field	Action
Resource name	Type a unique resource name that is a maximum of 10 characters and follows the *NAME restrictions for an IBM i basic name.
Resource description	Type a description that is a maximum of 50 characters.
Login ID	Type the log in ID of the authorized user.
Login password	The password of the authorized user.
Use compression	Type *YES to compress files before they are copied to the cloud. Compression is available with Advanced Edition.
Use encryption	Type *YES and press Enter, then provide values in subfields. Encryption is available with Advanced Edition.
Keystore file	A subfield of the **Use encryption** field. Type the name of the keystore file.
Library	A subfield of the **Keystore file** field. Type the name of the library that contains the keystore file.
Key label	A subfield of the **Use encryption** field. Type the name of the key label.
Root directory	Type the root directory, for example `/home/backups`. The directory path must start with a slash (/). It is case-sensitive for Linux and AIX, and not case-sensitive for IBM i unless the target is on the /QOpenSys file system. You must create this directory before you can copy files to it.
Resource URI	Type the resource URI including the fully-qualified name of the FTP server. If you enabled at rest encryption, include the secure protocol ftps:// at the beginning of the URI. If you did not enable at rest encryption, the protocol is optional. If the port number is not the default of 21 you must include it, for example: `ftps://myserver.enterprise.com:23`.
Full qualified IFS Dir name	[This parameter is not currently implemented.] Optional. To display, press F10 and page down. Type the fully-qualified path location of the directory to associate with the resource. After you copy files from this directory to the resource, Cloud Storage Solutions keeps the files in both locations synchronized. The default value is `*NONE`.

What to do next

To copy files to the resource, see “Copying files to the cloud” on page 19.

Changing FTP resources

Use the **CHGFPRICC** command to edit the parameters of an FTP resource.

Before you begin

If you have Cloud Storage Solutions Advanced Edition, you can specify that Cloud Storage Solutions encrypt files at rest in the cloud when they are copied there using this resource. To specify a resource for at rest encryption, you must obtain the keystore file name and library, and the key label, from the administrator who created them on the IBM i computer. For more information on encryption, see “Cloud Storage Solutions encryption” on page 5.

Obtain new resource information from the server administrator.

About this task

If you have Cloud Storage Solutions Advanced Edition, you can specify that Cloud Storage Solutions compress files before copying them to the cloud, and then decompress the files after copying them from the cloud. You can enable compression when you create or change the resource.

You cannot use this command to change the resource name. This command is not threadsafe.

Procedure

1. From the IBM i command line, type **CHGFPRICC**, and press F4.
2. In the **Resource name** field, type the name of the resource, and press Enter.
   If you do not know the resource name, press F4 to display a list of resources.
3. Edit one or more of the following fields, and press Enter:

Field	Description
Resource description	Edit the description.
Login ID	Change the name of the authorized user. For security reasons, the default value is *SAME. To keep the original value, leave the *SAME value in the field.
Login Password	Change the login password. For security reasons, the default value is *SAME. To keep the original value, leave the *SAME value in the field.
Use compression	Type *YES to compress files before they are copied to the cloud. Compression is available with Advanced Edition.
Use encryption	Type *YES and press Enter, then provide values in subfields. Encryption is available with Advanced Edition.
Keystore file	A subfield of the **Use encryption** field. Type the name of the keystore file.
Library	A subfield of the **Keystore file** field. Type the name of the library that contains the keystore file.
Key label	A subfield of the **Use encryption** field. Type the name of the key label.
Root directory	Change the root directory. The directory path must start with a slash (/) and is not case-sensitive.

Field	Description
Resource URI	Change the resource URI. Include the fully-qualified name of the FTP server. If you enabled at rest encryption, include the secure protocol ftps:// at the beginning of the URI. If you did not enable at rest encryption, the protocol is optional. If the port number is not the default of 21 you must include it, for example: `ftps://myserver.enterprise.com:23`.
Full qualified IFS Dir name	[This parameter is not currently implemented.] Optional. To display, press F10 and page down. Type the fully-qualified path location of the directory to associate with the resource. After you copy files from this directory to the resource, Cloud Storage Solutions keeps the files in both locations synchronized. Type `*NONE` to remove the current data and set the value to `*NONE`.

Displaying FTP resources

Use the **DSPFPRICC** command to display an FTP resource.

About this task

For security reasons, the **DSPFPRICC** command does not display the **Login ID** and **Login Password** fields. This command is not threadsafe.

Procedure

1. From the IBM i command line, type **DSPFPRICC**, and press F4.
2. In the **Resource name** field, type the name of the resource, and press Enter.
   If you do not know the resource name, press F4 to display a list of resources.

Deleting resources

Use the **DLTRSCICC** command to delete a resource. After you delete a resource, you cannot copy files between the IFS and the resource.

About this task

This command is not threadsafe.

Procedure

1. From the IBM i command line, type **DLTRSCICC**, and press F4.
2. In the **Resource name** field, type the name of the resource, and press Enter.
   If you do not know the resource name, press F4 to display a list of resources.
3. In the **Delete ICC Resource** panel, press Enter. The resource is deleted.

Working with resources

Use the **WRKCFGICC** command to create, change, delete, and display resources.

About this task

This command is not threadsafe.

Procedure

1. From the IBM i command line, type **WRKCFGICC**, and press F4.
2. In the **Resource name** field, type the name of the resource, and press Enter.

   If you do not know the resource name, or you want to work with multiple resources, leave the value *ALL and press Enter to display all resources. To find a resource using a wild card, type the first few characters of a resource name followed by an asterisk (*), and then press Enter.
3. Perform one of the following steps:
   - To create a new resource, type 1 in the **Opt** column of the first row. Type the resource name in the **Resource Name** column using a maximum of 10 characters. Type the resource type in the **Type** column, and press Enter. Complete the resource by following steps in the appropriate topic: "Creating FTP resources" on page 13, or "Creating AWS S3, IBM Cloud Object Storage, or Google Cloud Storage resources" on page 9.
   - To work with an existing resource, type one of the options from the following table in the **Opt** column beside the resource, and press Enter:

Option	Action
2	Change a resource. You can change everything except the resource name. For information see "Changing FTP resources" on page 15.
4	Delete a resource. To delete multiple resources, type 4 beside each resource. After you delete a resource, you cannot copy files between the two locations.
5	Display a resource. View the information that defines the resource.

Working with status

When you copy or delete files, the operations are run in jobs. You can use the **WRKSTSICC** command to view the status of those jobs, and end them if necessary.

About this task

When you copy files to or from the cloud, the operation is run asynchronously, meaning in its own batch job instead of in the same job as the command. When you copy files asynchronously, you do not have to wait a long time for large files to finish copying before running other commands. Also, you can use the IBM i facilities to work with asynchronous jobs, for example by scheduling when the jobs run. Before you view jobs, you can specify a **Job type** filter that can display only synchronous or only asynchronous jobs. For information on copying files, see Copy file to cloud (CPYTOCLD) and Copy file from cloud (CPYFRMCLD).

This command is not threadsafe.

Procedure

1. From the IBM i command line, type **WRKSTSICC**, and press F4.
2. Enter values in the following fields to filter the list of jobs to display, and then press Enter:

   Note : To see the possible values for a field, position the cursor in the field and press F4.

Field	Action
Resource type	Type the resource type of the jobs to display. To display jobs of all resource types, type *ALL.

Field	Action
Status	Type one of the following values to specify the status of transfer jobs to display: • *ALL - Jobs of any status • *ACTIVE - Jobs that are currently running (default) • *WAITING - Jobs in the job queue • *FAILED - Jobs that failed • *SUCCESSFUL - Jobs that completed successfully • *ENDED - Jobs that failed or completed successfully • *NOTENDED - Jobs that are waiting or active
Job type	Type one of the following values to specify the type of jobs to display: • *ALL - Jobs run synchronously and asynchronously (default) • *ASYNC - Jobs run asynchronously • *SYNC - Jobs run synchronously
Age in days	Type the maximum age of the jobs to display, in days. For example, leaving the default value of 7 means the command displays jobs that were run seven days old or younger.
Operation	Type one of the following values to specify the operation of the jobs to display: • *ALL - All operations (default) • *FRMCLD - Copy file from cloud operations • *TOCLD - Copy file to cloud operations • *COPY - All copy operations to and from the cloud • *DELETE - Delete from cloud operations
Job name	Type a job name to display that job. Leave the *ALL value to display jobs of any name. You can add an asterisk after a set of characters to search for names that begin with those characters, for example specify L00000006* to find jobs whose names start with L00000006.
Job user	Type a user name to display jobs run by that user. Leave the *ALL value to display jobs run by all users.
Position to	Leave the *LAST value to display the bottom of the job list, with the newest jobs. Type *FIRST to display the top of the job list, with the oldest jobs. After you display the list you can page up or down to scroll through the list.

The resulting list has the following columns:

Column	Content
Opt	An option field to take actions on jobs.
File name/Time	Two combined columns: The path and name of the file being copied or deleted, and the date and

Column	Content
	time that the job was started. The path and file name are truncated if too long for the display.
Name	The name of the job.
User	The user who started the job.
Number	The job number.
Status	The current job status, for example **Active** means that the job is running.
Oper	The operation being run, for example **TOCLD** is a copy to cloud operation.
Graphic% / Complete%	Two combined columns: **Graphic %** is a graphic representation of how much of the operation is complete. Each asterisk represents 10 percent of the operation, and the appended number represents units in the current 10 percent. For example, the following value represents 95% completion, with the 9 asterisks equal to 90 percent, plus 5: `*********5` **Complete %** is a numeric representation of how much of the operation is complete, for example 95 means the operation is 95 percent complete.

3. Optional: To end jobs, type 4 in the **Opt** column beside the jobs and press Enter.
4. Optional: Press F17 to change the filter choices.

Working with files in Cloud Storage Solutions

Use commands to copy files to and from a cloud resource, and to delete files from the cloud.

Copying files to the cloud

Use the **CPYTOCLD** command to copy files from the IFS to a cloud resource.

Before you begin

- You must create a cloud resource.
- You must have IBM i Read (*R) authority on the file that you will copy, and Execute (*X) authority on all directories in the path leading to the file. For example, if you will copy the file `/home/user/jdoe/file.txt`, you must have Execute authority on the `home`, `user`, and `jdoe` directories, and Read authority on `file.txt`. For information on authorities, see *Planning integrated file system security* in the IBM Knowledge Center.

About this task

You cannot use Cloud Storage Solutions to work with files in the /QSYS.LIB file system.

The size of files that you can copy to a resource is determined by the cloud service provider.

When you copy files to or from the cloud, the operation is run asynchronously, meaning in its own batch job instead of in the same job as the command. When you copy files asynchronously, you do not have to wait a long time for large files to finish copying before running other commands. Also, you can use the IBM

i facilities to work with asynchronous jobs, for example by scheduling when the jobs run. In the **Submit to batch** field, you can specify instead that the copy operation be run in the same job as the command.

This command is not threadsafe.

Procedure

1. From the IBM i command line, type **CPYTOCLD**, and press F4.
2. Complete the following required fields, and press Enter:

Field	Action
Resource name	Type the name of an existing resource.
Submit to batch	Type *NO to run the copy operation in the same job as the command. Leave the *YES value to run the copy operation in its own job.
Local file name	Type the IFS path and the name of the file to copy, for example: `/home/user/jdoe/file.txt` The path must begin with a forward slash (/) and is not case-sensitive.
Cloud file name	Type a path and name for the cloud copy of the file, for example: `dir1/dir2/file.txt` If the path does not exist, it is created. When you specify this path, do not include the container, bucket, or root directory that is defined in the resource. Cloud Storage Solutions combines that directory with this path to create the full path in the cloud. The container, bucket, or root directory that is defined in the resource must exist before you copy files to the cloud. When overwriting an existing file, in most cases the directory and file name are case-sensitive. If you overwrite a file on an IBM i FTP computer, the directory and file name are not case-sensitive unless they are on the /QOpensys file system.

Copying files from the cloud

Use the **CPYFRMCLD** command to copy files from a cloud resource to the IFS.

Before you begin

You must have Execute (*X) authority on all directories in the path that you will copy the file to, and Write (*W) authority on the last directory in the path. If the file was copied before and exists in the path, the user must have Write access to it. For example, to copy `file.txt` to `/home/user/jdoe`, you must have Execute authority on the `home`, `user`, and `jdoe` directories, and Write authority on `jdoe`. If `file.txt` is already there, you must have Write authority on it. For information on authorities, see *Planning integrated file system security* in the IBM Knowledge Center.

About this task

You cannot use Cloud Storage Solutions to work with files in the /QSYS.LIB file system.

If you copy a file from an FTP cloud server to the IBM i computer, and that file was not originally copied to the FTP server using Cloud Storage Solutions, Cloud Storage Solutions assigns the file a coded character set identifier (CCSID) of 65535. A CCSID of 65535 means the operating system treats the file as binary data and it is unreadable in an editor.

If you copy a file from an Amazon S3 or IBM Cloud Object Storage cloud server to the IBM i computer, and that file was not originally copied to the cloud server using Cloud Storage Solutions, Cloud Storage Solutions reads the data and from it assigns the file a coded character set identifier (CCSID) of either 1208 (UTF-8) if it is text, or 65535 if it is binary.

If the CCSID of the downloaded file is not correct, you can change it. For information, see the topic *Changing the Coded Character Set Identifier (CCSID)* in the IBM Knowledge Center.

When you copy files to or from the cloud, the operation is run asynchronously, meaning in its own batch job instead of in the same job as the command. When you copy files asynchronously, you do not have to wait a long time for large files to finish copying before running other commands. Also, you can use the IBM i facilities to work with asynchronous jobs, for example by scheduling when the jobs run. In the **Submit to batch** field, you can specify instead that the copy operation be run in the same job as the command.

This command is not threadsafe.

Procedure

1. From the IBM i command line, type **CPYFRMCLD**, and press F4.
2. Complete the following required fields, and press Enter:

Field	Action
Resource name	Type the name of the resource that contains the file.
Submit to batch	Type *NO to run the copy operation in the same job as the command. Leave the *YES value to run the copy operation in its own job.
Cloud file name	Type the cloud path and the name of the file to be copied, for example: `dir1/dir2/file.txt` Do not include the container or bucket defined in the resource. The cloud file name path is appended to those directories to construct the full path for the cloud copy of the file. In most cases the directory and file name are case-sensitive. The directory and file name are not case-sensitive with IBM i FTP resources unless they are on the /QOpensys file system.
Local file name	Type the IFS path and file name of the file being copied, for example: `/home/user/jdoe/file.txt` The path must begin with a forward slash (/). Path and file names are not case-sensitive. If the path directories do not exist locally, they are created.

Field	Action
	You can type a local file name that is different from the cloud file name.

Deleting files from the cloud

Use the **DLTCLDF** command to delete files from a cloud resource.

Before you begin

Before you can delete a file from the cloud, you must know the name of the resource that contains the file, and the path and name of the file in the resource.

About this task

This command is not threadsafe.

Procedure

1. From the IBM i command line, type **DLTCLDF**, and press F4.
2. In the **Resource** field, type the name of the resource that contains the file.
3. In the **Cloud file name** field, type a resource path and the name of the file to delete, and press Enter.

   In most instances the path and file names are case-sensitive. However, if you are deleting a file from an IBM i FTP computer, and from a file system other than the /QOpenSys system, the path and file names are not case-sensitive.

Cloud Storage Solutions APIs

Use the Cloud Storage Solutions APIs to work with resources and files.

Cloud Storage Solutions Resource APIs

You can use the Resource APIs to create, update, get, and delete resource information. You can also get a list of resources, and get the information necessary to recreate all of your resources if your system experiences a catastrophic failure.

New APIs for creating, updating, and getting resources were introduced in Cloud Storage Solutions version 1.2. The version 1.1 APIs for those actions are deprecated. Applications developed to work with version 1.2 and later should use the new APIs.

The new resource APIs are generic instead of being cloud provider-specific. For example, to create an AWS S3, or FTP resource you call the same create resource API. To specify the type of resource to create, you provide a parameter with a resource information format.

A resource information format is an 8-character identifier for a structure that defines type-specific resource information. For example, to create an AWS S3 resource you would call the same API and specify a format of QICC0310, which identifies a structure that contains AWS S3-specific information.

If your applications were developed to use the version 1.1 create, update, and get resource APIs, it is recommended that you rewrite your code to use the new APIs. If you do not want to use the new compression and encryption features introduced in version 1.2, you can specify new formats that are provided for backward compatibility and do not contain parameters for those features. In those formats, compression and encryption are set to their default state of disabled. To use compression and encryption you must use the new formats with those parameters.

You can also continue to use the old APIs, which are deprecated but still supported and documented.

In addition to formats for creating, updating, and getting resources, there are formats for getting and updating the basic information that every resource contains: ID, type, name, description, and IBM i directory location.

Create Resource API

Use the `Qicc_create_resource` API to create Cloud Storage Solutions resources.

Required Parameter Group:			
1	Resource information format	Input	Char(8)
2	Size of resource information parameter	Input	Binary(4)
3	Resource information	Input	Char(*)
4	Error code	I/O	Char(*)
Threadsafe: No			

Required Parameter Group

Resource information format
INPUT; CHAR(8)

An 8-character identifier indicating the format of the resource information. The format defines the context and cloud provider for the resource you are acting on. Provide one of the following formats:

Format	Description
QICC0200	Format for FTP resource information. Use this format if you do not want to use compression and encryption.
QICC0210	Format for FTP resource information. Includes fields to enable compression and encryption.
QICC0300	Format for S3 resource information. Use this format if you do not want to use compression and encryption.
QICC0310	Format for S3 resource information. Includes fields to enable compression and encryption.

Size of resource information parameter
INPUT; BINARY(4)

The size of the resource information parameter.

Resource information
INPUT; CHAR(*)

The resource information. The format specified in the **`Resource information format`** parameter determines the resource information that is provided in this parameter.

Error code
I/O; CHAR(*)

The error code information structure in the ERRC0100 format. For information, see the *Error code parameter* topic in the IBM Knowledge Center.

Update Resource API

Use the `Qicc_update_resource` API to update Cloud Storage Solutions resources.

Required Parameter Group:			
1	Resource information format	Input	Char(8)
2	Size of resource information parameter	Input	Binary(4)
3	Resource information	Input	Char(*)

Required Parameter Group:			
4	Error code	I/O	Char(*)
Threadsafe: No			

Required Parameter Group

Resource information format
INPUT; CHAR(8)

An 8-character identifier indicating the format of the resource information. The format defines the context and cloud provider for the resource you are acting on. Provide one of the following formats:

Format	Description
QICC0000	Format for base resource information. Use this format if you do not want to use compression and encryption.
QICC0010	Format for base resource information. Includes fields to enable compression and encryption.
QICC0200	Format for FTP resource information. Use this format if you do not want to use compression and encryption.
QICC0210	Format for FTP resource information. Includes fields to enable compression and encryption.
QICC0300	Format for S3 resource information. Use this format if you do not want to use compression and encryption.
QICC0310	Format for S3 resource information. Includes fields to enable compression and encryption.

Size of resource information parameter
INPUT; BINARY(4)

The size of the resource information parameter.

Resource information
INPUT; CHAR(*)

The resource information. The format specified in the **`Resource information format`** parameter determines the resource information that is provided in this parameter.

Error code
I/O; CHAR(*)

The error code information structure in the ERRC0100 format. For information, see the *Error code parameter* topic in the IBM Knowledge Center.

Get Resource API

Use the `Qicc_get_resource_info` API to get Cloud Storage Solutions resources.

Required Parameter Group:			
1	Resource name	Input	Char(10)
2	Resource information format	Input	Char(8)
3	Size of resource information parameter	Input	Binary(4)
4	Resource information	Input	Char(*)
5	Resource information bytes supplied	Input	Binary(4)

Required Parameter Group:			
6	Error code	I/O	Char(*)
Threadsafe: No			

Required Parameter Group

Resource name
INPUT; CHAR(10)

The name of resource to get.

Resource information format
INPUT; CHAR(8)

An 8-character identifier indicating the format of the resource information. The format defines the context and cloud provider for the resource you are acting on. Provide one of the following formats:

Format	Description
QICC0000	Format for base resource information. Use this format if you do not want to use compression and encryption.
QICC0010	Format for base resource information. Includes fields to enable compression and encryption.
QICC0200	Format for FTP resource information. Use this format if you do not want to use compression and encryption.
QICC0210	Format for FTP resource information. Includes fields to enable compression and encryption.
QICC0300	Format for S3 resource information. Use this format if you do not want to use compression and encryption.
QICC0310	Format for S3 resource information. Includes fields to enable compression and encryption.

Size of resource information parameter
INPUT; BINARY(4)

The size of the resource information parameter.

Resource information
INPUT; CHAR(*)

The resource information. The format specified in the **Resource information format** parameter determines the resource information that is provided in this parameter.

Resource information bytes supplied
INPUT; BINARY(4)

The number of bytes in the resource information parameter value.

Error code
I/O; CHAR(*)

The error code information structure in the ERRC0100 format. For information, see the *Error code parameter* topic in the IBM Knowledge Center.

Delete Resource API

Use the `Qicc_delete_resource` API delete a resource.

Required Parameter Group:			
1	Resource name	Input	Char(10)
2	Error code	I/O	Char(*)
Threadsafe: No			

Required Parameter Group

Resource name
INPUT; CHAR(10)

Specify the unique name of the resource. The name is between 1 and 10 characters long and must be left-justified and padded with spaces.

Error code
I/O; CHAR(*)

The error code information structure in the ERRC0100 format. For information, see the *Error code parameter* topic in the IBM Knowledge Center.

Get Resource List API

Use the `Qicc_get_resource_list` API to return a list of the names of existing resources.

Required Parameter Group:			
1	Resource name	Input	Char(10)
2	Resource list	I/O	Char(28)
3	Result buffer	Output	Char(*)
4	Error code	I/O	Char(*)
Threadsafe: No			

Required Parameter Group

Resource name
INPUT; CHAR(10)

Resource name in UTF-8 (30 bytes) or UTF-16 (20 bytes) to specify the resource name. Can be a simple name, a generic name, or *ALL (must be upper case). A simple name will return at most one name. A generic name includes the first few letters of a set of similarly named resources followed by an asterisk, acting as a wild card. Entering generic name returns resources that start with the characters before the asterisk.

Resource list
Input; CHAR(28)

The specified buffer sizes and CCSID values, and the returned list content. See the *Get resource list format* section of this topic for a description of the format.

Result buffer
OUTPUT; CHAR(*)

Buffer provided to hold result. Can be a null pointer if the **`Buffer provided`** field in the Get resource list format is zero. Allows an initial call to determine the length of the buffer needed.

Error code
I/O; CHAR(*)

The error code information structure in the ERRC0100 format. For information, see the *Error code parameter* topic in the IBM Knowledge Center.

Get Resource List format

Table 1. Get resource list format

Offset		Use	Type	Field
Dec	**Hex**			
0	0	INPUT	Binary(4)	Buffer provided
4	4	INPUT	Binary(4)	Input CCSID
8	8	INPUT	Binary(4)	Output CCSID
12	C	OUTPUT	Binary(4)	Buffer available
16	10	OUTPUT	Binary(4)	Name length
20	14	OUTPUT	Binary(4)	Returned names
24	18	OUTPUT	Binary(4)	Available names

Fields

Buffer provided
The length of buffer provided in the **Result buffer** parameter, in bytes.

Input CCSID
The CCSID of the **Resource name** parameter. Must be 1200 or 1208.

Output CCSID
The CCSID of the **Result buffer** parameter. Must be 1200 or 1208.

Buffer available
The size of buffer needed to hold the names that match the value specified in the **Resource name** parameter, and that use the CCSID specified in the **Output CCSID** field.

Name length
The length of each name (in bytes) in the **Result buffer** parameter. If the **Output CCSID** field is 1200, the **Name length** value is 20. If the **Output CCSID** field is 1208, the **Name length** value is 30.

Returned names
A count of names returned in the **Result buffer** parameter.

Available names
The total number of names matching the name specified in the **Resource name** parameter.

Get Restore Command API

Use the `Qicc_get_cl_command` API to return the information necessary to recreate all of your resources. If you store the information in a safe location, you can later use it to recreate the resources if something catastrophic happens to your system.

To get resource information, you provide the name of the resource, and the function returns (as a string) the full IBM i Control Language (CL) command required to recreate that resource.

Required Parameter Group:			
1	Resource name	Input	Char(10)
2	Control Language command	Output	Char(1024)
3	Error code	I/O	Char(*)

Required Parameter Group:
Threadsafe: No

Required Parameter Group

Resource name
INPUT; CHAR(10)

Specify the unique name of the resource. The name is between 1 and 10 characters long and must be left-justified and padded with spaces.

Control Language command
OUTPUT; CHAR(1024)

The full Control Language (CL) command required to recreate the resource, as a string.

Error code
I/O; CHAR(*)

The error code information structure in the ERRC0100 format. For information, see the *Error code parameter* topic in the IBM Knowledge Center.

Resource information formats

To create, update, or get Cloud resources using the APIs, you must provide resource information in one of the available resource information formats. There are base formats that you can use to update or get information from any resource. You can use the remaining formats to create, update, or get information from specific resource types.

Base resource information formats

You can use the base resource information formats when calling the update resource and get resource APIs if you do not need to update or get type-specific information. (To create resources, you must use one of the type-specific formats.)

There are two base formats that contain information common to resources of every type: The QICC0000 format does not include the compression and encryption parameters introduced in Cloud Storage Solutions version 1.2. It is intended for backward compatibility with applications that were built to use the version 1.1 APIs. QICC0010 includes compression and encryption parameters.

If you are updating a resource, you must provide a name in the **resource_name** field to identify the resource to update. Then in fields that you want to update, provide new values. In fields that you do not want to update, provide the current value or the value *SAME. You cannot update a resource ID.

If you are getting a resource, provide no format values. The format returns all of the information for the resource specified in the get API.

The QICC0000 and QICC0010 formats contain the following resource information:

Offset		Type	Field
Dec	Hex		
0	0	INT	resource_id
4	4	INT	resource_type
8	8	CHAR(10)	resource_name
18	12	CHAR(100)	resource_desc
108	6C	CHAR(1024)	directory_name (not currently supported)
1132	46C	CHAR	compress_data (QICC0010 only)

Offset		Type	Field
Dec	Hex		
1133	46D	CHAR	encrypt_data (QICC0010 only)
1134	46E	CHAR(20)	keystore (QICC0010 only)
1154	482	CHAR(32)	keylabel (QICC0010 only)

Fields

resource_id
The unique ID that is assigned to the resource by Cloud Storage Solutions when the resource is created. You cannot update resource IDs.

resource_type
The cloud service provider. The following are possible values:

- 0: AWSS3, Google Cloud Storage, and IBM Cloud Object Storage
- 4: FTP

resource_name
The unique resource name. Names are a maximum of ten characters, and are IBM i basic names that must adhere to the *NAME type restrictions. Every basic name can begin with the characters A-Z, $, #, or @ and can be followed by up to nine characters. The remaining characters can include the same characters as the first but can also include numbers 0-9, underscores (_), and periods (.). Lowercase letters are changed to uppercase letters by the system. Basic names used in IBM-supplied commands can be no longer than 10 characters. However, in your own commands you can define parameters of type *NAME (specified on the TYPE parameter of the PARM or ELEM statements) with up to 256 characters. For more information, and information on names in quoted form, see the topic *Names (*NAME)* in the IBM Knowledge Center.

resource_desc
The resource description. Passed in values must have a CCSID of 1200 (UTF16); returned values have a CCSID of 1200 (UTF16). Values can include uppercase and lowercase letters.

directory_name
The name of the IFS directory to keep synchronized with the resource. Passed in values must have a CCSID of 1200 (UTF16); returned values have a CCSID of 1200 (UTF16). Values can include uppercase and lowercase letters. [This field is not currently supported.]

compress_data
Switch enabling or disabling file compression. A value of 0 means compression is disabled; a value of 1 means compression is enabled. This field is only available in QICC0200 and QICC0300 formats.

encrypt_data
Switch enabling or disabling file encryption. A value of 0 means encryption is disabled; a value of 1 means encryption is enabled. When enabled, Cloud Storage Solutions uses the Advanced Encryption Standard (AES) encryption algorithm to encrypt files before they are copied to the cloud. The files remain encrypted "at rest" in the cloud, and are decrypted when copied back to the host IBM i computer. This field is only available in QICC0200 and QICC0300 formats.

keystore
The name of the keystore file that contains the certificates that Cloud Storage Solutions should use to "at rest" encrypt files the cloud using the resource. This field is only available in QICC0200 and QICC0300 formats.

keylabel
The label of the certificate that Cloud Storage Solutions should use to "at rest" encrypt files using the resource. This certificate must be in the keystore file specified in the keystore field. This field is only available in QICC0200 and QICC0300 formats. Values can include uppercase and lowercase letters.

FTP resource information formats

You can use these formats to specify FTP resource information when calling the create, update, and get resource APIs.

There are two formats that contain FTP resource information: The QICC0200 format does not include compression and encryption parameters that were introduced in Cloud Storage Solutions version 1.2. It is intended for backward compatibility with applications that were built to use the version 1.1 APIs. QICC0210 includes compression and encryption parameters.

If you are creating a resource, you must provide all field values except **resource_id**. The resource ID is created by Cloud Storage Solutions when you create the resource.

If you are updating a resource, you must provide a name in the **resource_name** field to identify the resource to update. Then in fields that you want to update, provide new values. In fields that you do not want to update, provide the current value or the value *SAME. You cannot update a resource ID.

If you are getting a resource, provide no format values. The format returns all of the information for the resource specified in the get API.

The QICC0200 and QICC0210 formats contain the following resource information:

Offset		Type	Field
Dec	Hex		
0	0	INT	resource_id
4	4	INT	resource_type
8	8	CHAR(10)	resource_name
18	12	CHAR(100)	resource_desc
108	6C	CHAR(1024)	directory_name
1132	46C	CHAR(2046)	resource_uri
3178	C6A	CHAR(510)	container_name
3688	E68	CHAR(256)	auth_user
3944	F68	CHAR(512)	auth_pwd
4456	1168	CHAR	compress_data (QICC0210 only)
4457	1169	CHAR	encrypt_data (QICC0210 only)
4458	116A	CHAR(20)	keystore (QICC0210 only)
4478	117E	CHAR(32)	keylabel (QICC0210 only)

Fields

resource_id
The unique ID that is assigned to the resource by Cloud Storage Solutions when the resource is created. You cannot update resource IDs.

resource_type
The cloud service provider. The following are possible values:

- 0: AWSS3, Google Cloud Storage, and IBM Cloud Object Storage
- 4: FTP

resource_name
The unique resource name. Names are a maximum of ten characters, and are IBM i basic names that must adhere to the *NAME type restrictions. Every basic name can begin with the characters A-Z, $, #, or @ and can be followed by up to nine characters. The remaining characters can include the same

characters as the first but can also include numbers 0-9, underscores (_), and periods (.). Lowercase letters are changed to uppercase letters by the system. Basic names used in IBM-supplied commands can be no longer than 10 characters. However, in your own commands you can define parameters of type *NAME (specified on the TYPE parameter of the PARM or ELEM statements) with up to 256 characters. For more information, and information on names in quoted form, see the topic *Names (*NAME)* in the IBM Knowledge Center.

resource_desc
The resource description. Passed in values must have a CCSID of 1200 (UTF16); returned values have a CCSID of 1200 (UTF16). Values can include uppercase and lowercase letters.

directory_name
The name of the IFS directory to keep synchronized with the resource. Passed in values must have a CCSID of 1200 (UTF16); returned values have a CCSID of 1200 (UTF16). Values can include uppercase and lowercase letters. [This field is not currently supported.]

resource_uri
The Uniform Resource Identifier (URI) of the storage location. Include the fully-qualified name of computer that hosts the FTP server, for example, `myserver.enterprise.com`. If the port number of the FTP server computer is not the default port number of 21 then you must include the port, for example, `myserver.enterprise.com:23`. Passed in values must have a CCSID of 1200 (UTF16); returned values have a CCSID of 1200 (UTF16). Values can include uppercase and lowercase letters.

container_name
The server root directory. The directory must begin with a forward slash (/), and it must exist before you can copy files to it. Root directory names are not case sensitive for FTP resources created for IBM i computers. The root directory name is case sensitive when using FTP for non-IBM i computers. Passed in values must have a CCSID of 1200 (UTF16); returned values have a CCSID of 1200 (UTF16). Values can include uppercase and lowercase letters.

auth_user
The ID of a user who can log into the FTP server. Passed in values must have a CCSID of 1200 (UTF16); returned values have a CCSID of 1200 (UTF16). Values can include uppercase and lowercase letters.

auth_pwd
The password of the user specified in **`auth_user`**. Passed in values must have a CCSID of 1200 (UTF16); returned values have a CCSID of 1200 (UTF16). Values can include uppercase and lowercase letters.

compress_data
Switch enabling or disabling file compression. A value of 0 means compression is disabled; a value of 1 means compression is enabled. This field is only available in QICC0200 and QICC0300 formats.

encrypt_data
Switch enabling or disabling file encryption. A value of 0 means encryption is disabled; a value of 1 means encryption is enabled. When enabled, Cloud Storage Solutions uses the Advanced Encryption Standard (AES) encryption algorithm to encrypt files before they are copied to the cloud. The files remain encrypted "at rest" in the cloud, and are decrypted when copied back to the host IBM i computer. This field is only available in QICC0200 and QICC0300 formats.

keystore
The name of the keystore file that contains the certificates that Cloud Storage Solutions should use to "at rest" encrypt files the cloud using the resource. This field is only available in QICC0200 and QICC0300 formats.

keylabel
The label of the certificate that Cloud Storage Solutions should use to "at rest" encrypt files using the resource. This certificate must be in the keystore file specified in the keystore field. This field is only available in QICC0200 and QICC0300 formats. Values can include uppercase and lowercase letters.

S3 or IBM Cloud Object Storage resource information formats

You can use these formats to specify S3 or IBM Cloud Object Storage resource information when calling the create, update, and get resource APIs.

There are two formats that contain S3 and IBM Cloud Object Storage resource information: The QICC0300 format does not include compression and encryption parameters that were introduced in Cloud Storage Solutions version 1.2. It is intended for backward compatibility with applications that were built to use the version 1.1 APIs. QICC0310 includes compression and encryption parameters.

If you are creating a resource, you must provide all field values except **resource_id**. The resource ID is created by Cloud Storage Solutions when you create the resource.

If you are updating a resource, you must provide a name in the **resource_name** field to identify the resource to update. Then in fields that you want to update, provide new values. In fields that you do not want to update, provide the current value or the value *SAME. You cannot update a resource ID.

If you are getting a resource, provide no format values. The format returns all of the information for the resource specified in the get API.

The QICC0300 and QICC0310 formats contain the following resource information:

Offset		Type	Field
Dec	Hex		
0	0	INT	resource_id
4	4	INT	resource_type
8	8	CHAR(10)	resource_name
18	12	CHAR(100)	resource_desc
108	6C	CHAR(1024)	directory_name
1132	46C	CHAR(2046)	resource_uri
3178	C6A	CHAR(126)	bucket_name
3304	CE8	CHAR(40)	key_id
3344	D10	CHAR(80)	secret_key
3424	D60	CHAR	compress_data (QICC0310 only)
3425	D61	CHAR	encrypt_data (QICC0310 only)
3426	D62	CHAR(20)	keystore (QICC0310 only)
3446	D76	CHAR(32)	keylabel (QICC0310 only)

Fields

resource_id
The unique ID that is assigned to the resource by Cloud Storage Solutions when the resource is created. You cannot update resource IDs.

resource_type
The cloud service provider. The following are possible values:

- 0: AWSS3, Google Cloud Storage, and IBM Cloud Object Storage
- 4: FTP

resource_name
The unique resource name. Names are a maximum of ten characters, and are IBM i basic names that must adhere to the *NAME type restrictions. Every basic name can begin with the characters A-Z, $, #, or @ and can be followed by up to nine characters. The remaining characters can include the same

characters as the first but can also include numbers 0-9, underscores (_), and periods (.). Lowercase letters are changed to uppercase letters by the system. Basic names used in IBM-supplied commands can be no longer than 10 characters. However, in your own commands you can define parameters of type *NAME (specified on the TYPE parameter of the PARM or ELEM statements) with up to 256 characters. For more information, and information on names in quoted form, see the topic *Names (*NAME)* in the IBM Knowledge Center.

resource_desc
The resource description. Passed in values must have a CCSID of 1200 (UTF16); returned values have a CCSID of 1200 (UTF16). Values can include uppercase and lowercase letters.

directory_name
The name of the IFS directory to keep synchronized with the resource. Passed in values must have a CCSID of 1200 (UTF16); returned values have a CCSID of 1200 (UTF16). Values can include uppercase and lowercase letters. [This field is not currently supported.]

resource_uri
The Uniform Resource Identifier (URI) of the bucket. Passed in values must have a CCSID of 1200 (UTF16); returned values have a CCSID of 1200 (UTF16). Values can include uppercase and lowercase letters.

bucket_name
The name of the bucket, which is the root directory location on the cloud server. This directory must exist before you can copy files to it. Bucket names are case-sensitive; when specifying the name you must use the correct case. Passed in values must have a CCSID of 1200 (UTF16); returned values have a CCSID of 1200 (UTF16). Values can include uppercase and lowercase letters.

key_id
The name of a user authorized to access the bucket. Passed in values must have a CCSID of 1200 (UTF16); returned values have a CCSID of 1200 (UTF16). Values can include uppercase and lowercase letters.

secret_key
The authorization key required to access the bucket. Passed in values must have a CCSID of 1200 (UTF16); returned values have a CCSID of 1200 (UTF16). Values can include uppercase and lowercase letters.

compress_data
Switch enabling or disabling file compression. A value of 0 means compression is disabled; a value of 1 means compression is enabled. This field is only available in QICC0200 and QICC0300 formats.

encrypt_data
Switch enabling or disabling file encryption. A value of 0 means encryption is disabled; a value of 1 means encryption is enabled. When enabled, Cloud Storage Solutions uses the Advanced Encryption Standard (AES) encryption algorithm to encrypt files before they are copied to the cloud. The files remain encrypted "at rest" in the cloud, and are decrypted when copied back to the host IBM i computer. This field is only available in QICC0200 and QICC0300 formats.

keystore
The name of the keystore file that contains the certificates that Cloud Storage Solutions should use to "at rest" encrypt files the cloud using the resource. This field is only available in QICC0200 and QICC0300 formats.

keylabel
The label of the certificate that Cloud Storage Solutions should use to "at rest" encrypt files using the resource. This certificate must be in the keystore file specified in the keystore field. This field is only available in QICC0200 and QICC0300 formats. Values can include uppercase and lowercase letters.

Resource APIs (Deprecated)

The create, update, and get resource APIs in this section are deprecated, however they are still supported for applications that were developed to use them.

New applications should use the create, update, and get Cloud Storage Solutions resources in the current resource APIs.

Create AWS S3, Google Cloud Storage, or IBM Cloud Object Storage Resource API (Deprecated)

Use the `Qicc_create_AWSS3_resource` API to create an AWS S3 or IBM Cloud Object Storage resource.

Required Parameter Group:			
1	Resource information	Input	AWS S3 resource structure
2	Error code	I/O	Error code information structure
Threadsafe: No			

Required Parameter Group

resource_info
INPUT; AWS S3 resource structure

Provide the information required to create the resource. For the format of the structure, see "Qicc AWS S3 Resource Info structure (Deprecated)" on page 37.

Error code
I/O; Error code information structure

The error code information structure in the ERRC0100 format. For information, see the *Error code parameter* topic in the IBM Knowledge Center.

Change AWS S3, Google Cloud Storage, or IBM Cloud Object Storage Resource API (Deprecated)

Use the `Qicc_update_AWSS3_resource` API to edit the parameters of an AWS S3 or IBM Cloud Object Storage resource.

Required Parameter Group:			
1	Resource information	Input	S3 resource structure
2	Error code	I/O	Error code information structure
Threadsafe: No			

Required Parameter Group

Resource information
INPUT; S3 resource structure

Provide the information required to change the resource. For the format of the structure, see "Qicc AWS S3 Resource Info structure (Deprecated)" on page 37.

Error code
I/O; Error code information structure

The error code information structure in the ERRC0100 format. For information, see the *Error code parameter* topic in the IBM Knowledge Center.

Get AWS S3, Google Cloud Storage, or IBM Cloud Object Storage Resource Information API (Deprecated)

Use the `Qicc_get_AWSS3_resource_info` API to get information on an AWS S3 or IBM Cloud Object Storage resource.

Required Parameter Group:			
1	Resource name	Input	Char(10)
2	Resource information	Output	S3 resource structure
3	Error code	I/O	Error code structure
Threadsafe: No			

Required Parameter Group

Resource name
INPUT; CHAR(10)

Specify the unique name of the resource. The name is between 1 and 10 characters long and must be left-justified and padded with spaces.

Resource information
OUTPUT; S3 resource structure

Returned information on the cloud resource specified in the **`Resource name`** parameter. For the format of the structure, see "Qicc AWS S3 Resource Info structure (Deprecated)" on page 37.

Error code
I/O; Error code structure

The error code information structure in the ERRC0100 format. For information, see the *Error code parameter* topic in the IBM Knowledge Center.

Create FTP Resource API (Deprecated)

Use the `Qicc_create_ftp_resource` API to create an FTP resource.

Required Parameter Group:			
1	Resource information	Input	FTP resource structure
2	Error code	I/O	Error code structure
Threadsafe: No			

Required Parameter Group

resource_info
INPUT; FTP resource structure

Provide the information required to create the resource. For the format of the structure, see Qicc FTP Resource Info structure.

Error code
I/O; Error code structure

The error code information structure in the ERRC0100 format. For information, see the *Error code parameter* topic in the IBM Knowledge Center.

Change FTP Resource API (Deprecated)

Use the `Qicc_update_ftp_resource` API to edit the parameters of an FTP resource.

Required Parameter Group:		
1 Resource information	Input	FTP resource structure
2 Error code	I/O	Error code structure
Threadsafe: No		

Required Parameter Group

Resource information
INPUT; FTP resource structure

Provide the information required to create the resource. For the format of the structure, see Qicc FTP Resource Info structure.

Error code
I/O; Error code structure

The error code information structure in the ERRC0100 format. For information, see the *Error code parameter* topic in the IBM Knowledge Center.

Cloud Storage Solutions resource structures (Deprecated)

Use the Cloud Storage Solutions resource structures to pass resource information in the API.

Structures

Qicc Base Resource Info

Qicc S3 Resource Info

Qicc FTP Resource Info

Qicc Base Resource Info structure (Deprecated)
The Qicc Base Resource Info structure contains information common to all resource types.

Fields

in **`resource_id`**: byte [4]

out **`resource_type`**: byte [4]

out **`resource_name`**: char [10]

out **`resource_desc`**: char [50]

out **`directory_name`**: char [1024] [This field is not currently supported.]

Field descriptions

resource_id
The unique ID that is assigned to the resource by Cloud Storage Solutions when the resource is created.

resource_type
The cloud service provider. Values:

- 0: AWSS3 and IBM Cloud Object Storage
- 4: FTP

resource_name
The unique resource name. Names are a maximum of ten characters, and are IBM i basic names that must adhere to the *NAME type restrictions. Every basic name can begin with the characters A-Z, $, #, or @ and can be followed by up to nine characters. The remaining characters can include the same characters as the first but can also include numbers 0-9, underscores (_), and periods (.). Lowercase letters are changed to uppercase letters by the system. Basic names used in IBM-supplied commands can be no longer than 10 characters. However, in your own commands you can define parameters of type *NAME (specified on the TYPE parameter of the PARM or ELEM statements) with up to 256 characters. For more information, and information on names in quoted form, see the topic *Names (*NAME)* in the IBM Knowledge Center.

resource_desc
The resource description.

directory_name
The name of the IFS directory to keep synchronized with the resource. [This field is not currently supported.]

Qicc AWS S3 Resource Info structure (Deprecated)
The APIs to get, create, and change AWS S3, Google Cloud Storage, and IBM Cloud Object Storage resources use the Qicc AWS S3 Resource Info structure. Both resources use the AWS S3 protocol.

Fields

I/O **Qicc_AWSS3_Resource_Info_t**: Qicc Base Resource Info structure

I/O **resource_uri**: char [2046]

I/O **bucket_name**: char [126]

I/O **key_id**: char [40]

I/O **secret_key**: char [80]

Field descriptions

Qicc_AWSS3_Resource_Info_t
The Qicc Base Resource Info structure. See “Qicc Base Resource Info structure (Deprecated)” on page 36.

resource_uri
The Uniform Resource Identifier (URI) of the bucket.

bucket_name
The name of the bucket, which is the root directory location on the cloud server. This directory must exist before you can copy files to it. Bucket names are case-sensitive; when specifying the name you must use the correct case.

key_id
The name of a user authorized to access the bucket.

secret_key
The authorization key required to access the bucket.

Qicc FTP Resource Info structure (Deprecated)
The create and change FTP resource APIs use the Qicc FTP Resource Info structure.

Fields

I/O **resource_info_fields**: Qicc Base Resource Info structure

I/O **resource_uri**: char [2046]

I/O **container_name**: char [510]

I/O **auth_user**: char [256]

I/O **auth_pwd**: char [512]

Field descriptions

resource_info_fields
The Qicc Base Resource Info structure. See "Qicc Base Resource Info structure (Deprecated)" on page 36.

resource_uri
The Uniform Resource Identifier (URI) of the storage location. Include the fully-qualified name of computer that hosts the FTP server, for example, `myserver.enterprise.com`. If the port number of the FTP server computer is not the default port number of 21 then you must include the port, for example, `myserver.enterprise.com:23`.

container_name
The server root directory. The directory must begin with a forward slash (/), and it must exist before you can copy files to it. Root directory names are not case sensitive for FTP resources created for IBM i computers. The root directory name is case sensitive when using FTP for non-IBM i computers.

auth_user
The ID of a user who can log into the FTP server.

auth_pwd
The password of the user specified in **auth_user**.

Cloud Storage Solutions File APIs

Use the Cloud Storage Solutions API to work with files and the cloud.

Copy File to Cloud API

Use the `Qicc_copy_file_to_cloud` API to copy a file from the IFS to the cloud. If the file exists it is updated. If the file does not exist it is created.

You cannot use Cloud Storage Solutions to work with files in the /QSYS.LIB file system.

The size of files that you can copy to a resource is determined by the cloud service provider.

Required Parameter Group:			
1	Resource name	Input	Char(10)
2	IFS file name	Input	Path name structure
3	Cloud file name	Input	Path name structure
4	User data	Input	Char(52)
5	Asynchronous flag	Input	Byte(4)
6	Handle	Output	Byte(4)
7	Error code	I/O	Error code structure
Threadsafe: No			

Required Parameter Group

Resource name
INPUT; CHAR(10)

Specify the unique name of the resource. The name is between 1 and 10 characters long and must be left-justified and padded with spaces.

IFS file name
INPUT; Path name structure

The path and name of the file to copy to the cloud. In C++ programs, this is the Qlg_Path_Name_T structure. The path must begin with a forward slash (/). You must have Read (*R) authority on the file, and Execute (*X) authority on all directories in the path leading to the file. For example, to copy `/home/user/jdoe/file.txt`, you must have Execute authority on the `home`, `user`, and `jdoe` directories, and Read authority on `file.txt`. For information on authorities, see *Planning integrated file system security* in the IBM Knowledge Center. For information on the path name structure, see *Path name format* in the IBM Knowledge Center.

Cloud file name
INPUT; Path name structure

The path and name that the file should have in the cloud. In C++ programs, this is the Qlg_Path_Name_T structure. Do not include the container or bucket node specified in the resource. If the path directories do not exist, they are created. With most resources, if you are overwriting an existing file, the directory and file names are case-sensitive. For example if you had already copied the file example above, and then specified `dir1/dir2/FILE.txt`, Cloud Storage Solutions would create a second file named `FILE.txt` next to the original `file.txt`. FTP resources are not case-sensitive when copying to an IFS directory on an IBM i computer. For information on the path name structure, see *Path name format* in the IBM Knowledge Center.

User data
INPUT; CHAR(52)

Data provided by the caller and passed to the exit programs to help the caller identify which upload completed.

Asynchronous flag
INPUT; BYTE(4)

Specifies whether the copy operation is run in the same job as the command, or run asynchronously in its own separate batch job. When you copy files asynchronously, you do not have to wait for large files to finish copying before running other commands, which can take a long time. You can also use the IBM i facilities to work with asynchronous jobs, for example by scheduling when the job runs.

If zero, the function will wait for the copy to finish before returning to the caller. If non-zero, the function will initiate the copy and return without waiting for the copy to finish.

Handle
OUTPUT; BYTE(4)

An ID that uniquely identifies this file transfer. It will be passed to exit programs that are registered with the Cloud Connect exit point to uniquely identify which file transfer completed.

Error code
I/O; Error code structure

The error code information structure in the ERRC0100 format. For information, see the *Error code parameter* topic in the IBM Knowledge Center.

Copy Cloud to File API

Use the `Qicc_copy_cloud_to_file` API to copy a file from the cloud to the IFS. If the file exists it is updated. If the file does not exist it is created.

You cannot use Cloud Storage Solutions to work with files in the /QSYS.LIB file system.

If you copy a file from an FTP cloud server to the IBM i computer, and that file was not originally copied to the FTP server using Cloud Storage Solutions, Cloud Storage Solutions assigns the file a coded character set identifier (CCSID) of 65535. A CCSID of 65535 means the operating system treats the file as binary data and it is unreadable in an editor.

If you copy a file from an Amazon S3 or IBM Cloud Object Storage cloud server to the IBM i computer, and that file was not originally copied to the cloud server using Cloud Storage Solutions, Cloud Storage Solutions reads the data and from it assigns the file a coded character set identifier (CCSID) of either 1208 (UTF-8) if it is text, or 65535 if it is binary.

If the CCSID of the downloaded file is not correct, you can change it. See the topic *Changing the Coded Character Set Identifier (CCSID)* in the IBM Knowledge Center.

Required Parameter Group:			
1	Resource name	Input	Char(10)
2	Cloud file name	Input	Path name structure
3	IFS file name	Input	Path name structure
4	User data	Input	Char(52)
5	Asynchronous flag	Input	Byte(4)
6	Handle	Output	Byte(4)
7	Error code	I/O	Error code structure
Threadsafe: No			

Required Parameter Group

Resource name
INPUT; CHAR(10)

Specify the unique name of the resource. The name is between 1 and 10 characters long and must be left-justified and padded with spaces.

Cloud file name
INPUT; Path name structure

The path and name of the file in the cloud, for example: `dir1/dir2/file.txt`. In C++ programs, this is the Qlg_Path_Name_T structure. Do not include the container, bucket, or root directory that is defined in the resource. With most resources the directory and file names are case-sensitive. FTP resources are not case-sensitive when copying to an IFS directory on an IBM i computer. For information on the path name structure, see *Path name format* in the IBM Knowledge Center.

IFS file name
INPUT; Path name structure

An IFS path and name for the file to be copied from the cloud. In C++ programs, this is the Qlg_Path_Name_T structure. The path must begin with a forward slash (/). If the directories do not exist, they are created. The user copying the file must have Execute (*X) authority on all directories in the path, and Write (*W) authority on the last directory in the path. If the file was copied before and exists in the path, the user must have Write access to it. For example, to copy `file.txt` to `/home/user/jdoe`, you must have Execute authority on the `home`, `user`, and `jdoe` directories, and Write authority on `jdoe`. If `file.txt` is already there, you must have Write authority on it. For information on authorities, see *Planning integrated file system security* in the IBM Knowledge Center. For information on the path name structure, see *Path name format* in the IBM Knowledge Center.

User data
INPUT; CHAR(52)

Data provided by the caller and passed to the exit programs to help the caller identify which file copy completed.

Asynchronous flag
INPUT; BYTE(4)

Specifies whether the copy operation is run in the same job as the command, or run asynchronously in its own separate batch job. When you copy files asynchronously, you do not have to wait for large files to finish copying before running other commands, which can take a long time. You can also use the IBM i facilities to work with asynchronous jobs, for example by scheduling when the job runs.

If zero, the function will wait for the copy to finish before returning to the caller. If non-zero, the function will initiate the copy and return without waiting for the copy to finish.

Handle
OUTPUT; BYTE(4)

An ID that uniquely identifies this file transfer. It will be passed to exit programs that are registered with the Cloud Connect exit point to uniquely identify which file transfer completed.

Error code
I/O; Error code structure

The error code information structure in the ERRC0100 format. For information, see the *Error code parameter* topic in the IBM Knowledge Center.

Delete File from Cloud API

Use the `Qicc_delete_file_from_cloud` API to delete a file from the cloud.

Required Parameter Group:			
1	Resource name	Input	Char(10)
2	Cloud file name	Input	Path name structure
3	Error code	I/O	Error code structure
Threadsafe: No			

Required Parameter Group

Resource name
INPUT; CHAR(10)

Specify the unique name of the resource. The name is between 1 and 10 characters long and must be left-justified and padded with spaces.

Cloud file name
INPUT; Path name structure

The path and name of the file in the cloud. In C++ programs this is the Qlg_Path_Name_T structure. Do not include the container or bucket node that is defined in the resource. With most resources the directory and file names are case-sensitive. FTP resources are not case-sensitive when copying to an IFS directory on an IBM i computer. For more information, see *Path name format* in the IBM Knowledge Center.

Error code
I/O; Error code structure

The error code information structure in the ERRC0100 format. For information, see the *Error code parameter* topic in the IBM Knowledge Center.

List Files in Cloud API

Use the `Qicc_list_files_in_cloud` API to list the files in a cloud resource. You can use this API to verify that particular files are in the cloud.

Required Parameter Group:			
1	Resource name	Input	Char(10)
2	Cloud file name	Input	Char(**)
3	Handle	I/O	Byte(4)
4	File list	Output	Char(**)
5	Error code	I/O	Error code structure
Threadsafe: No			

Required Parameter Group

Resource name
INPUT; CHAR(10)

This is the unique name of the resource. The name is between 1 and 10 characters long and must be left-justified and padded with spaces.

Cloud file name
INPUT; CHAR(**)

This is optional. You can specify characters and a wildcard to return files that are stored in the resource, for example you can specify A* to return files that start with A. If not specified, all files are returned.

Handle
I/O; BYTE(4)

An ID that uniquely identifies the list, and the location in the list, that the function is working with. Set this value to 0 (zero) for the first function call. When the function returns it sets the handle value. Pass this handle back in on subsequent calls to this function.

File list
OUTPUT; CHAR(**)

The first file name in the list that matches the pattern defined in the **`Cloud file name`** parameter. Call the function repeatedly to get all names in the list; each call returns the next name in the list. When every name in the list has been returned, the value is empty.

Error code
I/O; Error code structure

The error code information structure in the ERRC0100 format. For information, see the *Error code parameter* topic in the IBM Knowledge Center.

Get Cloud Transfer State API

Use the `Qicc_get_cloud_transfer_state` API to get the state of a particular file transfer to or from the cloud.

Required Parameter Group:			
1	Handle	Output	Byte(4)
2	Error code	I/O	Error code structure
Threadsafe: No			

Required Parameter Group

Handle
OUTPUT; BYTE(4)

An ID that uniquely identifies this file transfer. It is returned by the "Copy File to Cloud API" on page 38 and "Copy Cloud to File API" on page 39. It will be passed to the exit point to uniquely identify which file transfer completed.

Error code
I/O; Error code structure

The error code information structure in the ERRC0100 format. For information, see the *Error code parameter* topic in the IBM Knowledge Center.

Cloud Storage Solutions exit point structures

To have Cloud Storage Solutions call your programs and pass in data after it transfers files to and from the cloud, you can register exit programs with the Cloud Storage Solutions QIBM_QICC_XFER_CLS exit point. When called, your exit programs must also pass a parameter to Cloud Storage Solutions specifying the success or failure of the call.

For general information about exit points and exit programs, including examples of exit programs, see the IBM Knowledge Center.

The Cloud Storage Solutions exit point uses the CLS00100 format, and is not threadsafe. The exit point is registered with the IBM i registration facility when Cloud Storage Solutions is installed, and deregistered when Cloud Storage Solutions is uninstalled.

When Cloud Storage Solutions calls an exit program it passes in two parameters. The first specifies whether the file was uploaded or downloaded; the second specifies information about the transfer. Each exit program that Cloud Storage Solutions calls returns a parameter that represents the success or failure of the call. All three parameters contain byte stream values that represents fields in a structure.

Structures

Qicc Exit Description

Qicc Exit Operation

Qicc Exit Control Value

Qicc Exit Description structure

The Qicc Exit Description structure contains the length of the structure byte stream and the type of operation being described.

Fields

- in exit_description_len (offset 0x00): byte [4]
- in operation (offset 0x04): byte [4]

Field descriptions

exit_description_len
The length of the Qicc Exit Description structure byte stream. The value is 4 bytes. In the byte stream, the value in hexadecimal format is 0x00000004.

operation
The type of operation being described: 0 means a file upload, 1 means a file download. In the byte stream, the value in hexadecimal format is 0x00 or 0x01.

Qicc Exit Operation structure

The Qicc Exit Operation structure contains information on the operation.

Fields

- in operation_info_len (offset 0x00): byte [4]
- in control_value_len (offset 0x04): int [4]
- in handle (offset 0x08): byte [4]
- in cloud_resource_name (offset 0x0C): char [10]
- in reserved (offset 0x16): byte [2]
- in cloud_service_name (offset 0x18): char [20]

- in cloud_resource_uri (offset 0x2C): char [1024]
- in operation (offset 0x42C): byte [4]
- in transfer_state (offset 0x430): byte [4]
- in transfer_error_code (offset 0x434): byte [4]
- in exit_user_data (offset 0x438): char [52]
- in async (offset 0x46C): byte [4]
- in cloud_path_name (offset 0x470): Qlg_Path_Name_T

For information on the Qlg_Path_Name_T structure, see *Path name format* in the IBM Knowledge Center.

Field descriptions

operation_info_len
The length of the Qicc Exit Operation structure byte stream. The value will be 1168 plus the cloud_path_name length.

control_value_len
The length of the Qicc Exit Control Value structure byte stream. The value is an integer of 4 bytes. In the byte stream, the value in hexadecimal format is 0x00000004.

handle
An ID that uniquely identifies a file transfer.

cloud_resource_name
The unique name of the cloud resource involved in the operation.

cloud_service_name
The unique name of the cloud service that provides the resource involved in the operation.

cloud_resource_uri
The Uniform Resource Identifier (URI) of the resource involved in the operation.

operation
The type of operation: 0 means a file upload, 1 means a file download. In the byte stream, the value in hexadecimal format is 0x00000000 or 0x00000001.

transfer_state
The file transfer status, with one of the following values:

- 0: Success
- 1: Failure
- 2: Failure (retriable error)

In the byte stream, the value in hexadecimal format is 0x00000000, 0x00000001, or 0x00000002.

transfer_error_code
The reason for a failed transfer, with one of the following values:

- 0000: No error
- 0001: Warning that the downloaded file was given a default value
- 0002: No connection to the server
- 0003: Communication error between the client and server
- 0004: Invalid password
- 0005: Invalid user
- 0006: Lost connection
- 0007: Connection timed out
- 0008: Ran out of storage
- 0009: Transfer canceled
- 0010: Maximum retires exceeded

- 0011: Data error
- 0012: Authority problem with the Cloud server
- 0013: Local file could not be opened, read, or written (io error)
- 0014: Cloud file not found
- 0015: Local file not found
- 0016: Internal program error

In the byte stream, an example of the value 0001 in hexadecimal format is 0x00000001.

exit_user_data
The user who called the cloud upload or download API. The information is passed to Cloud Storage Solutions by the program that called the upload or download API. This data can be used to identify a particular invocation of the API.

async
Indicates whether the operation should occur synchronously or asynchronously.

cloud_path_name
The path in the cloud that the file was uploaded to or downloaded from. The value uses the Qlg_Path_Name_T path name format. See *Path name format* in the IBM Knowledge Center.

Qicc Exit Control Value structure

Your program uses the Qicc Exit Control Value structure to specify whether it succeeded or failed in receiving parameters from the Cloud Storage Solutions programs.

Fields

out process_return_code (offset 0x00): byte [4]

Field descriptions

process_return_code

Your exit program returns an integer of four bytes that specify whether it succeeded or failed in receiving parameters from the Cloud Storage Solutions programs: 0 means success; 1 means failure.

The Qicc Exit Control Value structure is an integer of 4 bytes. In the byte stream, the value in hexadecimal format is 0x00000001.

Example:

In the following example, the Qicc Exit Control Value byte stream (in hexadecimal format) is 4 bytes long and represents a successful call from the Cloud Storage Solutions programs:

```
0x00000000
```

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs.

© Copyright IBM Corp. _enter the year or years_.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Programming interface information

This User's Guide publication documents intended Programming Interfaces that allow the customer to write programs to obtain the services of IBM Cloud Storage Solutions for i.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be

trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Linux® is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java™ and all Java-based trademarks and logos are trademarks of Oracle, Inc. in the United States, other countries, or both.

Other product and service names might be trademarks of IBM or other companies.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions:

Applicability: These terms and conditions are in addition to any terms of use for the IBM website.

Personal use: You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use: You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights: Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Privacy policy considerations

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user, or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM’s Privacy Policy at http://www.ibm.com/privacy and IBM’s Online Privacy Statement at http://

www.ibm.com/privacy/details the section entitled “Cookies, Web Beacons and Other Technologies” and the “IBM Software Products and Software-as-a-Service Privacy Statement” at http://www.ibm.com/software/info/product-privacy.

Index

Product Number: 5733-ICC