Redbooks
ibm.com/redbooks

IBM TS7760 R4.2 Cloud Storage Tier Guide

Sosuke Matsui

Derek Erdmann

Nobuhiko Furuya

Rin Fujiwara

Joe Hew

Tomoaki Ogino

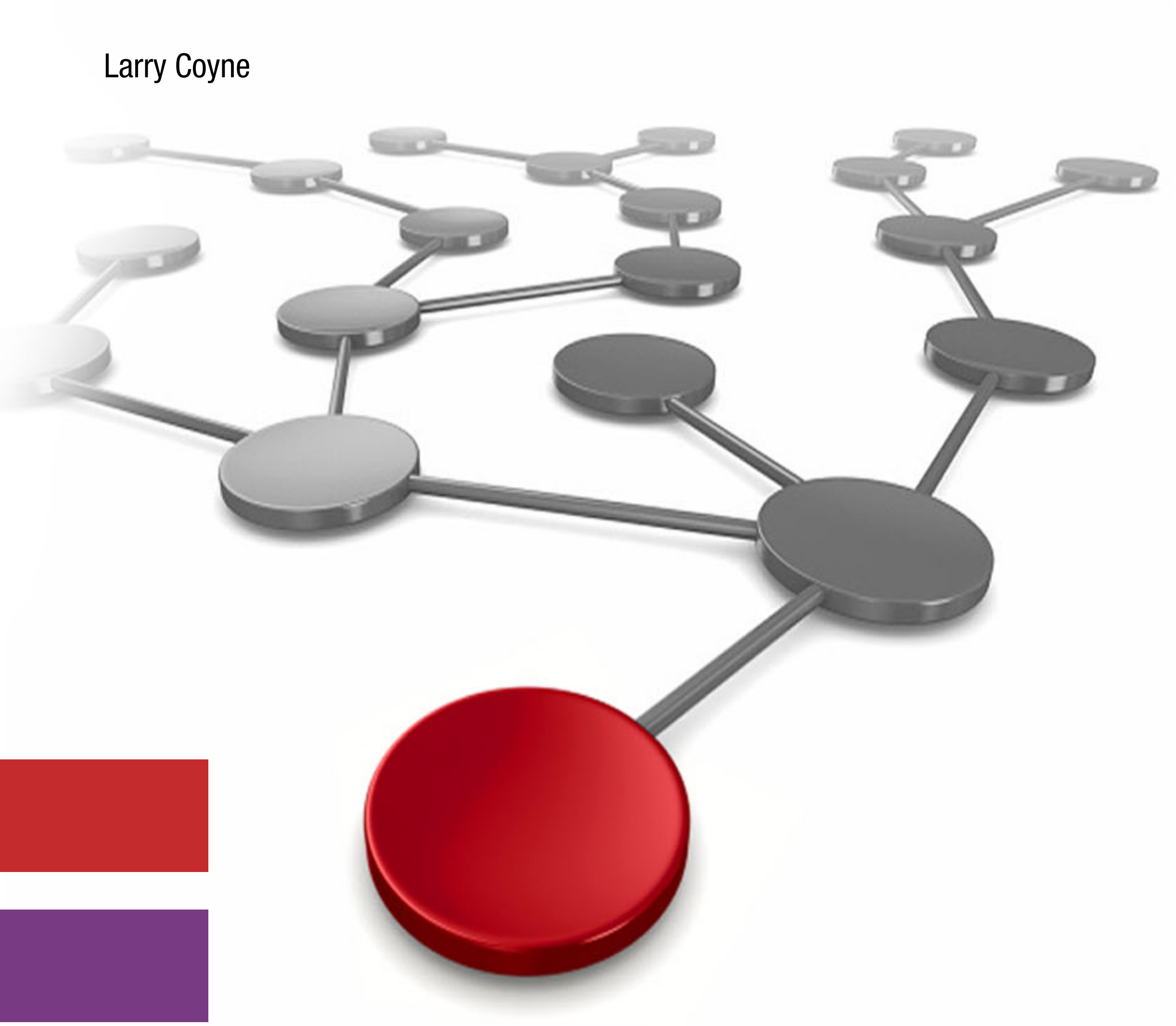
Alberto Barajas Ortiz

Michael Scott

Joe Swingler

Taisei Takai

Larry Coyne



Cloud

Storage

IBM

Redpaper

IBM Redbooks

IBM TS7760 R4.2 Cloud Storage Tier Guide

May 2019

REDP-5514-00

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

First Edition (May 2019)

This edition applies to Version 4, Release 2, Modification 0 of the IBM TS7700.

This document was created or updated on June 7, 2019.

Contents

Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

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, MD-NC119, Armonk, NY 10504-1785, US

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 jurisdictions 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 websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

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

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

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.

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

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 actual people or business enterprises 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.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation, 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 http://www.ibm.com/legal/copytrade.shtml

The following terms are trademarks or registered trademarks of International Business Machines Corporation, and might also be trademarks or registered trademarks in other countries.

Accesser®
DS8000®
FICON®
IBM®
IBM Cloud™
IBM Z®
Redbooks®
Redpaper™
Redbooks (logo) ®
Slicestor®
z/OS®

The following terms are trademarks of other companies:

SoftLayer, are trademarks or registered trademarks of SoftLayer, Inc., an IBM Company.

Windows, 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.

Other company, product, or service names may be trademarks or service marks of others.

Preface

Building on over 20 years of virtual tape experience, the TS7760 now supports the ability to store virtual tape volumes in an object store. This IBM Redpaper publication helps you set up and configure the new cloud object storage support for IBM Cloud Object Storage (COS) or Amazon Simple Storage Service (Amazon S3).

The TS7700 supported off loading to physical tape for over two decades. Off loading to physical tape behind a TS7700 is used by hundreds of organizations around the world. By using the same hierarchical storage techniques, the TS7700 can also off load to object storage. Because object storage is cloud-based and accessible from different regions, the TS7760 Cloud Storage Tier support essentially allows the cloud to be an extension of the grid.

In this IBM Redpaper publication, we provide a brief overview of cloud technology with an emphasis on Object Storage. Object Storage is used by a broad set of technologies, including those technologies that are exclusive to IBM Z®. The aim of this publication is to provide a basic understanding of cloud, Object Storage, and different ways it can be integrated into your environment.

This Redpaper is intended for system architects and storage administrators with TS7700 experience who want to add the support of a Cloud Storage Tier to their TS7700 solution.

Note: As of this writing, the TS7760C supports the ability to offload to on-premise cloud with IBM Cloud Object Storage and public cloud with Amazon S3.

Authors

This paper was produced by a team of specialists from around the world working at the Tokyo Development Laboratory.

Sosuke Matsui is a software development engineer in Tokyo, Japan. He joined IBM Japan in 2009, and worked on the development and testing of asynchronous replication of IBM Scale Out Network Attached Storage for 5 years. Currently, he is responsible for the development and testing of TS7700 Cloud Storage Tier component. He is a member of the Association for Computing and Machinery (ACM) and Information Processing Society of Japan (IPSJ).

Derek Erdmann is a DFSMS Software Technical Support Engineer who specializes in the OAM product area, where he has been the Team Lead for 4 years. He graduated from Northern Illinois University in 2009 with a Master’s degree in Computer Science with an emphasis in Enterprise Computing. He has spent the last 7 years with IBM working with customers and developers to enhanced the quality of the DFSMS product set.

Nobuhiko Furuya is a Level 2 certified IT specialist in Japan. His 35 years with IBM have been with IBM z Systems®. His area of expertise is mainframe storage systems, such as DFSMS and high-end tape products (mainly TS7700) and acts as an SME for these areas.

Rin Fujiwara is an advisory IT specialist in Japan. She has 15 years of experience in the IBM Z area. She has spent the last 5 years as a Subject Matter Expert in the areas of DFSMS and high-end tape products, working with customers and field engineers in project phases of post-sales and pre-sales.

Joe Hew works in the Tucson, Arizona product field engineering group, supporting the IBM TS7700. With many years in the information technology (IT) field, Joe has worked in system-level test on various products, such as storage controllers, tape libraries, adapters, Serial Storage Architecture (SSA), and storage area networks (SANs). Joe is a Microsoft Certified Professional and a Certified Level 2 Fibre Channel Practitioner (awarded by the Storage Networking Industry Association).

Tomoaki Ogino is a Level 1 certified IT specialist at IBM Japan. He has 30 years of experience in IBM Z® and worked at IBM for 28 years in the field directly with customers. He is a Subject Matter Expert in the areas of DFSMS and high-end tape products and supporting post-sales and pre-sales for 2 years.

Alberto Barajas Ortiz graduated from the Technological Institute of Superior Studies of Monterrey (MEXICO) in 2016 with a Master's degree in Administration of Information Technology, and he is a PMI-certified Project Management Professional. He has worked for IBM since 2001. During the last 13 years, he has been collaborating to the TS7700 Development effort in the Product Test area (mainly focused in Functional Verification aspects), where he has served as a Team Lead for the last 8 years.

Michael Scott is a Senior Data Facility Storage Management Subsystem (DFSMS) Technical Support Engineer in the IBM Systems, Client Enablement, and Systems Assurance team. He has 16 years of experience in DFSMS technical support. He holds a Master's in Business Administration and a Bachelor of Sciences in Mathematics. Michael has six patents that were issued in the computer sciences field, and is a DFSMS Technical Advocate. Currently, he is the team lead for the DFSMS technical support education program.

Joe Swingler is a STSM and Master Inventor with IBM's Systems Group, based out of the IBM laboratory in Tucson, Arizona, USA. He is currently a lead architect for IBM's TS7700 Virtualization Engine. Joe joined IBM in 1999 and started with the virtual tape subsystem team. He began working with ESCON and FICON channel virtualization and eventually became the lead architect of the TS7700 Grid design. Joe has since become a lead architect of TS7700 and has owned the design of many features, including the TS7700 Cloud Storage Tier support. Joe holds a BSEE from Arizona State University.

Taisei Takai is a Level 2 Certified Technical Specialist in IBM Japan. His area of expertise is storage mainly based on the z/OS platform. He has more than 25 years of experience in technical support for planning and installing mainframe tape products. He is currently working as a Client Technical Specialist and is involved with most of the TS7700 related projects in Japan.

Larry Coyne is a Project Leader at the IBM International Technical Support Organization, Tucson, Arizona, center. He has over 35 years of IBM experience, with 23 years in IBM storage software management. He holds degrees in Software Engineering from the University of Texas at El Paso and Project Management from George Washington University. His areas of expertise include client relationship management, quality assurance, development management, and support management for IBM storage management software.

Thanks to the following people for their contributions to this project:

Erika Dawson
Michael Engelbrecht
Kohichi Masuda
Takeshi Nohta
Katsuyoshi Katori
Takahiro Tsuda
IBM Systems

Now you can become a published author, too!

Here's an opportunity to spotlight your skills, grow your career, and become a published author—all at the same time! Join an IBM Redbooks residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

We want our papers to be as helpful as possible. Send us your comments about this paper or other IBM Redbooks publications in one of the following ways:

- Use the online **Contact us** review Redbooks form found at:

  ibm.com/redbooks

- Send your comments in an email to:

  redbooks@us.ibm.com

- Mail your comments to:

  IBM Corporation, IBM Redbooks
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400

Stay connected to IBM Redbooks

- Find us on Facebook:

  http://www.facebook.com/IBMRedbooks

- Follow us on Twitter:

  http://twitter.com/ibmredbooks

- Look for us on LinkedIn:

  http://www.linkedin.com/groups?home=&gid=2130806

- Explore new Redbooks publications, residencies, and workshops with the IBM Redbooks weekly newsletter:

  https://www.redbooks.ibm.com/Redbooks.nsf/subscribe?OpenForm

- Stay current on recent Redbooks publications with RSS Feeds:

  http://www.redbooks.ibm.com/rss.html

Summary of changes

This section describes the technical changes made in this edition of the paper and in previous editions. This edition might also include minor corrections and editorial changes that are not identified.

Summary of Changes
for IBM TS7760 R4.2 Cloud Storage Tier Guide
as created or updated on June 12, 2019.

June 2019, First Edition minor udpates

This revision includes the following new and changed information.

Changed information

- Updated Cloud Premigration Rank 1 in "Storage groups" on page 89
- Updated default of "CPMCNTH: Cloud Premigration Count High:" on page 150
- Updated default of "CPMCNTL: Cloud Premigration Count Low:" on page 150
- Updated Chapter 8, "Setting up an AWS Cloud Object Storage" on page 55 with AWS S3 screen capture figures
- Added Appendix 12.1, "TS7760 object name format" on page 116

1

Cloud overview

In this chapter, we provide high-level overview of basic cloud concepts. This overview helps you to better understand the role Object Storage plays in the cloud hierarchy.

This chapter includes the following topics:

- 1.1, “What defines a cloud?” on page 2
- 1.2, “Cloud storage and public, private, and hybrid models” on page 4
- 1.3, “Object Storage hierarchy” on page 5

1.1 What defines a cloud?

The cloud is a combination of one or more different solutions, components, and services. It can consist of different layers, including but not limited to the following layers:

- Application Layer: This layer is where applications can be hosted and run, and can use pre-coded software APIs that you can integrate to create applications.
- Infrastructure Layer: This layer is where entire systems can be hosted. An Infrastructure Layer can be composed of a mix of cloud and traditional infrastructures that are interconnected.

  This layer is composed of three main classes of components:

  - Compute Layer: This layer is where computations and resident applications run. Think of this layer as virtual server instances that are running on physical hardware.
  - Storage Layer: This layer is where persistent data is stored, which can include everything from temporary storage to indefinitely retained content.
  - Network Layer: This layer provides an interconnect between all of the different layers and communications into and out of the cloud.

Within the Storage Layer, the following storage types often exist:

- **Block Storage:** This storage type allows virtual server instances and physical servers to use traditional block type storage, which can be used to create file systems (temporary or long-term).
- **File Storage:** This storage type allows virtual server instances and physical servers to store files into pre-existing file systems, which are usually persistent across application instances.
- **Object Storage:** This storage type allows applications that are running inside or outside of the cloud to store binary blobs of unstructured data persistently. These blobs or objects can be accessed from a global namespace (worldwide), which makes it attractive for distributed technologies.

  Object stores can have different internal tiers and often provide the most attractive cost point for storing data. Data that is stored in an object store is persistent and often retained by applications for long durations. Objects are immutable, meaning you can create them and then delete them, but you cannot modify them.

The different layers and where Object Storage exists in a cloud is shown in Figure 1-1 on page 3.

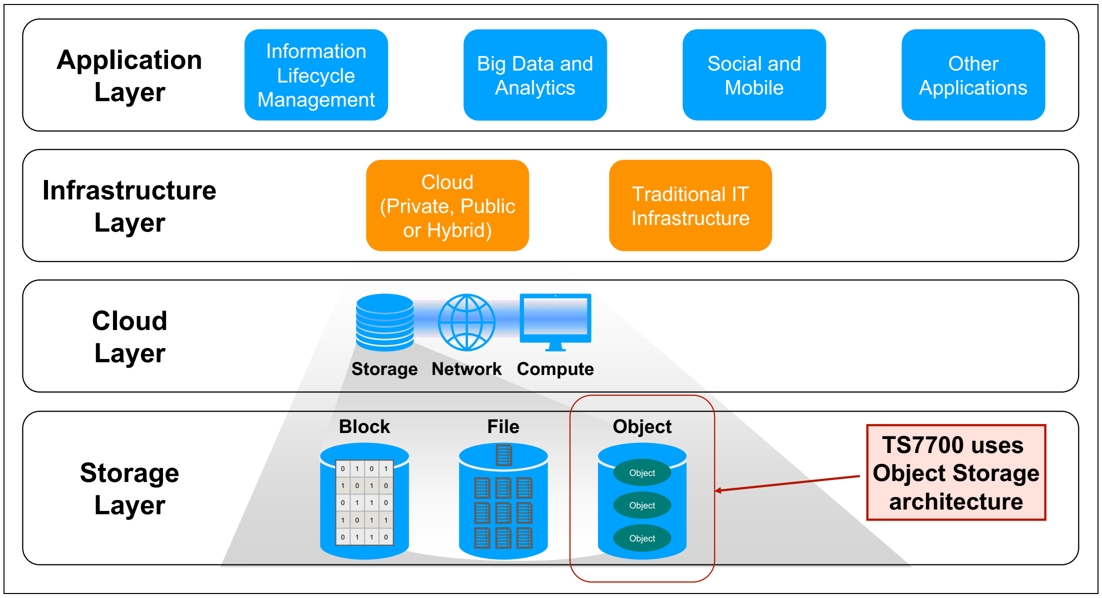
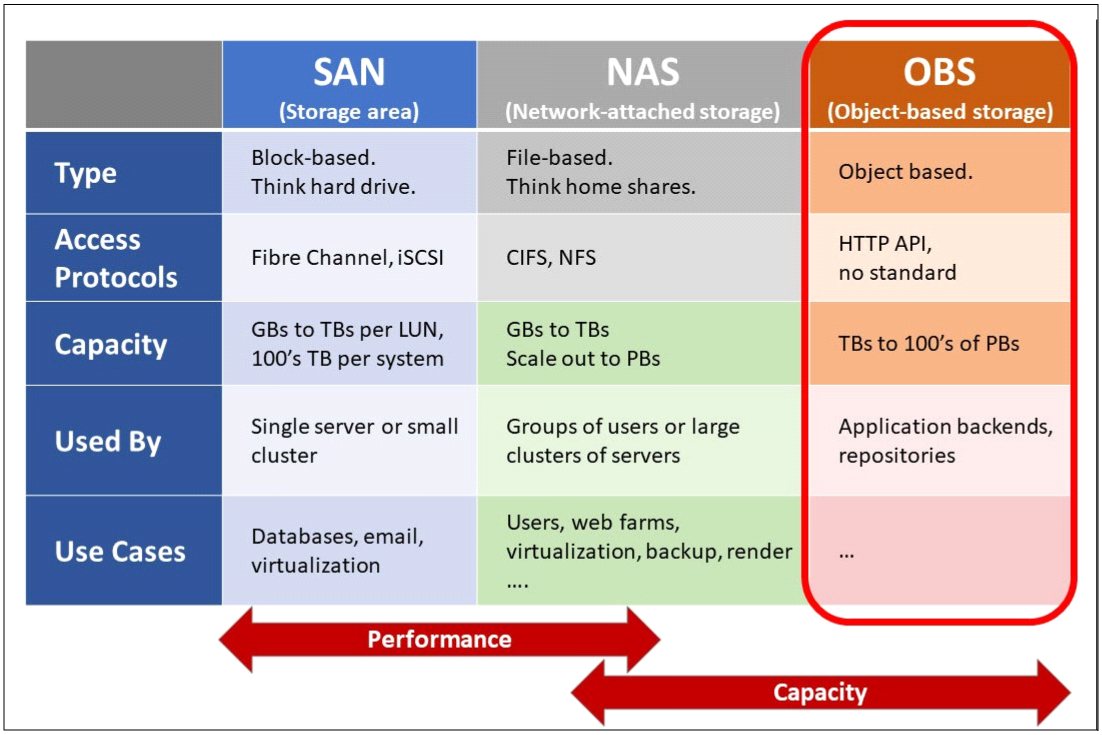


Figure 1-1   TCT in the context of the Cloud

The different storage types are compared from a network perspective in Figure 1-2 (SAN for block, NAS for file, and OBS for Object Storage).



	SAN (Storage area)	NAS (Network-attached storage)	OBS (Object-based storage)
Type	Block-based. Think hard drive.	File-based. Think home shares.	Object based.
Access Protocols	Fibre Channel, iSCSI	CIFS, NFS	HTTP API, no standard
Capacity	GBs to TBs per LUN, 100's TB per system	GBs to TBs Scale out to PBs	TBs to 100's of PBs
Used By	Single server or small cluster	Groups of users or large clusters of servers	Application backends, repositories
Use Cases	Databases, email, virtualization	Users, web farms, virtualization, backup, render ….	…

Figure 1-2   Types of storage

Object stores use a RESTful API in which all interactions with the object store occur through HTTP(S) requests. This process greatly simplifies the ability to integrate technologies with object stores and can allow the access to be global, assuming the HTTP(S) namespace is global. Overall, object stores are excellent storage targets for cold or archive data, which is likely to be retained for longer periods and rarely accessed.

Demand for Object Storage grew significantly over the last few years. The demand is so high that stand-alone object stores that are independent of the other cloud components now exist. Private, dedicated, onsite object store solutions often are installed within an organization's owned or leased facilities, as described next.

1.2 Cloud storage and public, private, and hybrid models

Cloud delivery models refer to how a cloud solution is used by an organization, where the data is located, and who operates the cloud solution. Several delivery models are available that can deliver the needed capabilities in a cloud solution.

The following cloud delivery models are available:

- Public
- Private
- Hybrid

These delivery models can be integrated with traditional IT systems and other clouds. They are divided into the following categories:

- On-premise: Consists of a private cloud infrastructure at your organization's location.
- Off-premise: Consists of a cloud infrastructure that is hosted in a cloud service provider's location.

Public cloud

A *public cloud* is a solution in which the cloud infrastructure is available to the general public or a large industry group over the internet. The infrastructure is not owned by the user, but by an organization that provides cloud services. Services can be provided at no cost, as a subscription, or as a pay-as-you-go model.

Another delivery model option is available that is known as *community cloud*, or *multi-tenant cloud*, which often consists of a public cloud that is shared among multiple organizations to lower costs. For ease of understanding, this publication treats this delivery model as part of the public cloud category.

Direct Link or *Direct Attach* are terms that refer to an organization's ability to have one or more dedicated links into a public cloud providers infrastructure. These owned or leased lines provide access to the public cloud solution without the use of the internet. They tend to be more reliable with regards to performance and often are assumed to be more secure.

Private cloud

A *private cloud* is a solution in which the infrastructure is provisioned for the exclusive use of a single organization. The organization often acts as a cloud service provider to internal business units that realizes all of the benefits of a cloud without having to provision their own infrastructure. By consolidating and centralizing services into a cloud, the organization benefits from centralized service management and economies of scale.

A private cloud provides an organization with some advantages over a public cloud. The organization gains greater control over the resources that make up the cloud. In addition, private clouds are ideal when the type of work that is being done is not practical for a public cloud because of network latency, security, or regulatory concerns.

A private cloud can be owned, managed, and operated by the organization, a third party, or a combination of the two. The private cloud infrastructure is provisioned on the organization's premises, but it can also be hosted in a data center that is owned by a third party.

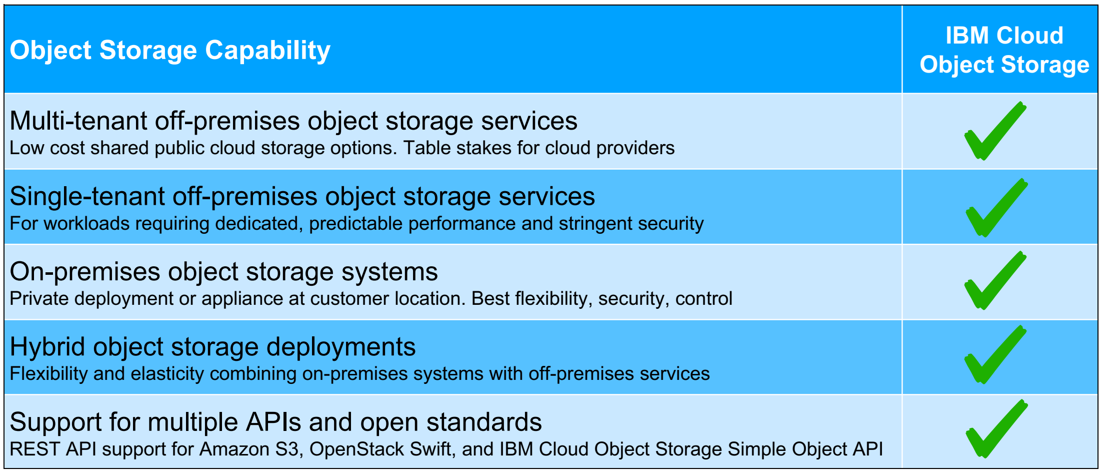
Hybrid cloud

As the name implies, a *hybrid cloud* is a combination of various cloud types (public, private, and community). Each cloud in the hybrid mix remains a unique entity, but is bound to the mix by technology that enables data and application portability.

The hybrid approach allows a business to use the scalability and cost-effectiveness of a public cloud without making available applications and data beyond the corporate intranet. A well-constructed hybrid cloud can service secure, mission-critical processes, such as receiving customer payments (a private cloud service) and secondary processes, such as employee payroll processing (a public cloud service).

IBM Cloud Object Storage

IBM Cloud™ Object Storage (COS) offers all these delivery model options. Each option with its capabilities is shown in Figure 1-3.



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

Figure 1-3 IBM Cloud Object Storage capabilities

For more information about the IBM Cloud Object Storage service offering, see *Cloud Object Storage as a Service: IBM Cloud Object Storage from Theory to Practice - For developers, IT architects and IT specialists*, SG24-8385, or see the IBM Cloud Object Storage web page.

For more information about other IBM Cloud Storage solutions, see *IBM Private, Public, and Hybrid Cloud Storage Solutions*, REDP-4873, or see the IBM Cloud web page.

1.3 Object Storage hierarchy

Data that is written to an object store is organized into a hierarchy. The hierarchy consists of accounts, containers, and objects. Objects are in containers (also known as *vaults* or *buckets*) and accessible through the credentials of an account.

1.3.1 Storage cloud hierarchy

The storage cloud hierarchy consists of the following entities:

- Account

  An account is the top level of the hierarchy and is created by the service provider, but owned by the consumer. Accounts can also be referred to as *projects* or *tenants* and provide a namespace for the containers.

  An account includes an owner that is associated with it, and the owner of the account has full access to all of the containers and objects within the account. One or more accounts can be defined to access one or more containers, which provides a wide range of options for access to objects in an object store.

- Containers

  Containers (also known as *vaults* or *buckets*) are similar to folders in Windows or UNIX, and provide an area to collocate stored objects. Rules can be configured for containers that provide features, such as container-to-container synchronization, quotas, retention compliance, availability requirements, and object versioning.

  One main difference between traditional folders and containers is that containers cannot be nested. That is, no support is available for creating a container within another container. However, object names can have directory-like delimiters within their names, which provide a further level of organization.

  Container names can be up to 256 characters and must be unique within the namespace of the object store. If the object store is in a public cloud, the container name often is unique to all container names in the world for that public cloud service.

  Objects within a container are protected by using read and write Access Control Lists (ACLs). No security mechanism is available to protect an individual object within a container. After a user is granted access to a container, that user can access all of the objects within that container.

- Objects

  Objects are the blobs of data that are within an object store. Objects are limited in size, such as 5 GB, so larger objects are often broken up and stored by using multiple segment objects.

  After all of the segment objects are stored, a manifest object is created to piece all of the segments together. When a large object is retrieved, the manifest object is supplied and the Object Storage service concatenates all of the segments and returns them to the requester.

  For most sizes that are greater than 100 MB, the system performs multi-part uploads. By creating multiple parts, the system parallel recall and greater recall efficiency is achieved. Although all of this processing is often contained within the client interface and hidden from the user application, it can be helpful to know it is occurring.

  Object keys or names can use delimiters to help group objects, as with subdirectories in a file system. For example, an object name might feature the following format:

  ```
  mybackup/2018/email/20180203bak
  ```

  If indexing services are enabled on the target container, administrator tools and graphical interfaces for the object store can often be used to list objects by using search criteria that considers the delimiters, as shown in the following example:

  ```
  search: “*/*/email/*” which will list all email backups for any year
  ```

The objects can also have a defined individual expiration date. The expiration dates can be set when an object is stored and modified by updating the object's metadata, but only if the user application supports setting expiration dates.

For more information about the object naming convention, see 12.1, "TS7760 object name format" on page 116.

1.3.2 Metadata

In addition to the objects, default metadata and expanded metadata can be associated with each object. Viewing metadata can help learn basic information about an object and store custom information by the user. For example, metadata for an object might contain information, such as creation date, expiration date, and size.

The difference between data and metadata is shown in Figure 1-4.

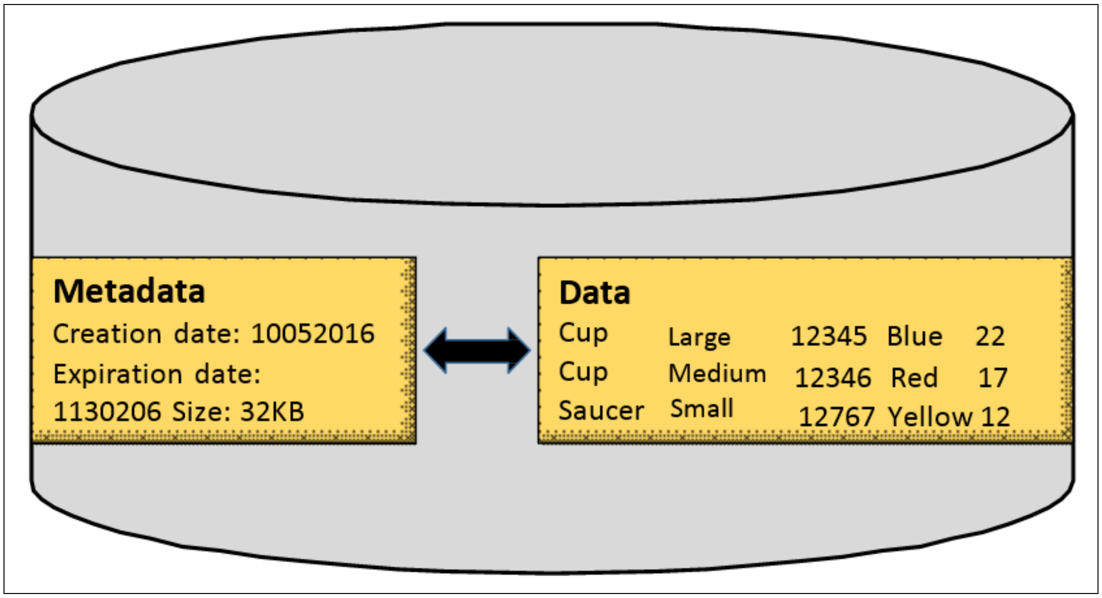


Figure 1-4 Data and metadata differences

An example of a data file that contains a list of dinnerware items, which is the data that the user stored, is shown in Figure 1-4. The metadata is then stored separately to retain information about the object.

2

Container resiliency

In this chapter, we describe basic concepts of how different object stores provide resiliency through redundancy and geographical distance.

> **Note:** As of this writing, the TS7760C supports the ability to offload to on-premise cloud with IBM Cloud Object Storage and public cloud with Amazon S3.

This chapter includes the following topics:

2.1 IBM Cloud Object Storage public

IBM Cloud Object Storage Public features different options for resiliency. By using the IBM Cloud Object Storage erasure coding function, data that is written into the object store is spread across multiple nodes by using more parity parts. By using parity techniques, which are similar to Reed-Solomon, data can be read from the IBM Cloud Object Storage nodes if a minimum number of nodes are available. That minimum is determined by the requirements that were configured during the vault creation process.

For example, what is the minimum number of nodes required to read back data and how many other parity nodes should be used per write? If all configured nodes are within one IBM COS public region that is closest to the organization's lab, the performance is highest and the latency is the lowest, but the resiliency is limited only to that region. If geo cross regional resiliency is required, certain IBM Cloud Object Storage public regions support cross regional node distribution further spreading parts across two or more geographical regions. Whether it is two regions or three regions is dependent on what cross regional options are available and the resiliency requirements of the organization.

Three geo regions provide the most resiliency with an erasure parity overhead of 1.7. Therefore, for every one unit of data stored, 1.7 units of available vault capacity is used. With the three site model, an entire region and a small number of other nodes can be lost without losing data.

A minimum write threshold can be configured so that any write can provide a zero recovery point objective if enough parts are written before the write returns.

Numerous Accesser® nodes exist per region, which makes the access to your data highly available.

For more information about IBM Cloud Object Storage public and its regions and resiliency, see these resources:

- *IBM Cloud Object Storage Concepts and Architecture: An Under-the-Hood Guide for IBM Cloud Object Storage*, REDP-5435
- IBM Cloud Object Storage web page
- Global locations and resiliency options for IBM Cloud Object Storage web page

2.2 IBM Cloud Object Storage On-premise

IBM Cloud Object Storage On-premise is similar to IBM Cloud Object Storage Public, in that the erasure coding technique is used to distribute parts of data and parity across multiple nodes. If the private organization's nodes all exist within one region or site, the resiliency is site-wide or regional.

If a two geo region mode is used, it requires a 100% mirror of the two regions with erasure among the nodes within each region. The mirroring among the two regions is asynchronous or often referred to as eventual consistency. It requires over a 2x capacity increase to accommodate a region loss because 100% of your data must replicate to each region, plus perform erasure coding among the nodes in each region.

The three region model is ideal allowing the traditional 1.7 factor increase in capacity to sustain a complete region loss. However, the three region model does have the highest latency, which can affect performance.

Unlike the public version of IBM Cloud Object Storage where many Accesser nodes are part of the architecture and hidden from the user, a private IBM Cloud Object Storage setup needs physical Accesser nodes installed at each location where access of the IBM Cloud Object Storage data is required. For example, if two of the three regions have host presence, those two regions require Accessers to access the data in the IBM Cloud Object Storage. Assuming three Accesser nodes per host enabled region, the three nodes provide scaling for throughput and more availability at each region.

More information about IBM Cloud Object Storage, see IBM Knowledge Center.

2.3 Amazon S3

Similar to IBM Cloud Object Storage Public, Amazon S3 features regions in which a high level of availability exists within that region, but a loss of that region can result in a data loss event. Therefore, if resiliency beyond one region is required, Amazon S3 offers cross-region replication where buckets that are defined in different regions can mirror each other.

The distance between the two regions is determined by the resiliency requirements of the organization. The two regions can span countries, continents, and even oceans, if needed. The two regions require that a unique bucket is defined in each region, so which region is accessed for data (original or copy) is dependent on which bucket is referenced. The bucket-to-bucket replication provides eventual consistency or is asynchronous.

For more information about Amazon S3, see this Amazon web page.

3

IBM z/OS and object stores

In this chapter, we describe different methods in which z/OS® users can use cloud object storage.

This chapter includes the following topics:

3.1 Overview

As explained in Chapter 1, “Cloud overview” on page 1, object stores are excellent target devices for cold or archive data. Content that often must be retained for longer periods and rarely accessed is a good candidate for object storage. Although thousands (if not millions) of devices in the world support the use of object stores, we focus on z/OS use cases.

Today, a few options are available for enabling the use of object stores under z/OS. Although some overlap exists between these options, each option includes some unique features.

The goal of this chapter is to highlight the differences between these offerings. We do not suggest which option is best for you. Because different options are always being added, this chapter is current as of this writing.

3.2 Tape Cloud Connector for z/OS

IBM Cloud Tape Connector for z/OS allows you to easily copy and move mainframe data to private, hybrid, or public Cloud storage. This feature offers improved security, flexibility, and economies of scale for archive or backup and recovery. IBM Cloud Tape Connector for z/OS processes and moves your data without the need for more hardware gateway devices. It uses zIIP processors to minimize CPU cost of data movement.

This offering provides IBM Z to cloud connectivity and is independent of the DASD or Tape technology that is used by the organization.

By emulating virtual tape devices, applications or utilities that can write to tape can use Tape Cloud Connector for z/OS. When content is copied or written to such an emulated tape, it is initially stored in DASD before being offloaded to an object store through a gateway device. Any access of the tape from that point forward requires that it be recalled back into DASD as a virtual tape device.

3.3 Advanced Archive for DFSMShsm

IBM Advanced Archive for DFSMShsm creates an archive tier for backing up inactive mainframe data that is managed by DFSMShsm. The added, lower-impact management tier uses less CPU resources to improve DFSMShsm efficiency and adds cloud storage to virtual and physical tape media options.

IBM Advanced Archive for DFSMShsm preserves DFSMS policies to properly back up data and manage retention. When applications or users recall data that is stored in a cloud, it is returned to DFSMShsm control and made available. IBM Advanced Archive for DFSMShsm supports IBM Cloud Object Storage, IBM SoftLayer®, and Amazon S3 cloud environments.

This offering provides direct IBM Z to cloud connectivity and is independent of the DASD or Tape technology used by the organization.

When a dataset is archived to the cloud, DFSMShsm surrenders awareness of the dataset after it is successfully stored in an object store. If this dataset is accessed, the advanced archive technology recalls the dataset back into DASD and again makes DFSMShsm aware of its presence.

For more information, see this website.

3.4 z/OS Object Access Method (OAM) Cloud Support

IBM intends to deliver a new cloud tier to OAM's existing storage hierarchy which will provide the ability to store and manage primary copies of OAM objects on cloud storage, via public or private cloud infrastructures supporting the Amazon S3 API, and the ability to recall an object stored in the cloud to the disk level of the storage hierarchy. OAM managed backup copies will continue to be supported as they are today to removable media, typically virtual or physical tape.

For more information see this website `this website`.

3.5 DS8000 Transparent Cloud Tiering

The IBM DS8000®, in combination with DFSMShsm, supports the ability to have datasets that are stored within the DS8000 be migrated to object store devices. Similar to how DFSMShsm supports ML2 (which often implies tape), DFSMShsm supports migration level cloud or MLC where the C stands for Cloud.

By modifying existing or new migration policies, DFSMShsm can request the DS8000 migrate a dataset from the DS8000 directly to a chosen object store through TCP/IP connectivity. No data movement through the host occurs and the dataset granular management eliminates the need for DFSMShsm recycle processing and other HSM inefficiencies, which saves CPU cycles on the host.

The DS8000 supports targeting different object store technologies and having the dataset objects migrate to the TS7700. The DS8000 essentially becomes a user of the TS7700 Grid and offloads datasets directly to the TS7700 through TCP/IP, which eliminates the need to migrate the dataset through the FICON® SAN.

For more information, see *IBM DS8880 and z/OS DFSMS: Transparent Cloud Tiering*, SG24-8381.

3.6 TS7700 Cloud Storage Tier

The IBM TS7700 supports the ability to have logical volumes tier to object stores, much as it has supported tiering to physical tape since the 1990s. Through partitions and policy management, logical volumes in their entirety can be premigrated to an object store and then eventually migrated or removed from TS7700 disk cache that is based on policy and LRU algorithms. This feature provides a tier of cold storage behind the TS7700, which improves the cost of ownership and redundancy of data within the TS7700. This IBM Redpaper publication is focused on this particular offering.

3.7 Transparent Cloud Tiering

Although Transparent Cloud Tiering (TCT) is not a stand-alone product, it is important to understand what it is because it is mentioned frequently within the IBM portfolio.

TCT is an internal IBM software offering that enables numerous IBM products to use object storage. Instead of each product creating its own interface to many different object store vendors, TCT provides a common interface for IBM products to use across different object stores. This feature enables solutions, such as the DS8000 and TS7700, to have a much more consistent and simplified means of using object stores from different vendors that often can have variances in support and protocols.

4

Introducing the TS7760 Cloud Storage Tier

In this chapter, we describe the TS7760 Cloud Storage Tier and its components.

4.1 Overview

Building on over 20 years of virtual tape experience, the TS7760 now supports the ability to store virtual tape volumes in an object store. The TS7700 supported offloading to physical tape for over two decades.

Offloading to physical tape behind a TS7700 is utilized by hundreds of organizations around the world. By using the same hierarchical storage techniques, the TS7700 can also offload to object storage.

Because object storage is cloud-based and accessible from different regions, the TS7760 Cloud Storage Tier support allows the cloud to be an extension of the grid. A high-level overview of TS7760 Cloud Storage Tier support is shown in Figure 4-1.

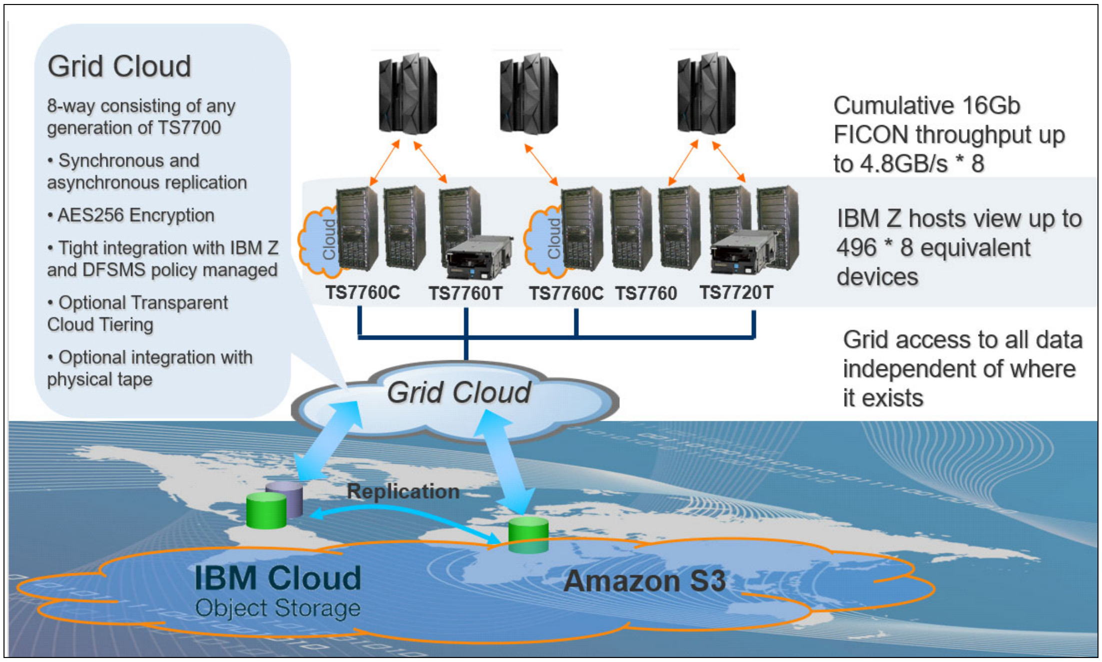

Grid Cloud
8-way consisting of any generation of TS7700
• Synchronous and asynchronous replication
• AES256 Encryption
• Tight integration with IBM Z and DFSMS policy managed
• Optional Transparent Cloud Tiering
• Optional integration with physical tape
Cumulative 16Gb FICON throughput up to 4.8GB/s * 8
IBM Z hosts view up to 496 * 8 equivalent devices
Cloud
Cloud
TS7760C
TS7760T
TS7760C
TS7760
TS7720T
Grid access to all data independent of where it exists
Grid Cloud
Replication
IBM Cloud
Object Storage
Amazon S3

Figure 4-1 High level overview of TS7760 Cloud Storage Tier support

4.1.1 Cloud Storage Tier enabled cluster

A Cloud Storage Tier enabled cluster, or TS7760C, can be a member of any grid if the peer cluster code levels are compatible. Peers can be other TS7760C clusters, TS7700T clusters, or disk only TS7700 clusters. By using management class policies, virtual volumes are replicated among peers in the grid. Those peers with Cloud Storage Tier support then can offload to an object store.

After one TS7760C cluster offloads a logical volume, other peers that attempt to offload the same logical volume detect that the volume exists in the object store and can skip the premigration phase. Either cluster can then recall the logical volume from the cloud, if needed.

Logical volumes offload in their entirety to the object store. If the only available logical volume copy in the grid is within an object store, one of the TS7760C clusters who migrated that volume previously can recall it into disk cache. After the entire volume is present in disk cache, the content is accessible by using the existing grid techniques.

Because a volume must be recalled entirely, choosing logical volume sizes that are smaller can provide faster time to access when the entire content of the logical tape is not being accessed.

Note: As of this writing, the TS7760C supports the ability to offload to on-premise cloud with IBM Cloud Object Storage and public cloud with Amazon S3.

A high-level view of how a TS7760C can use an object store as a tier of storage is shown in Figure 4-2.

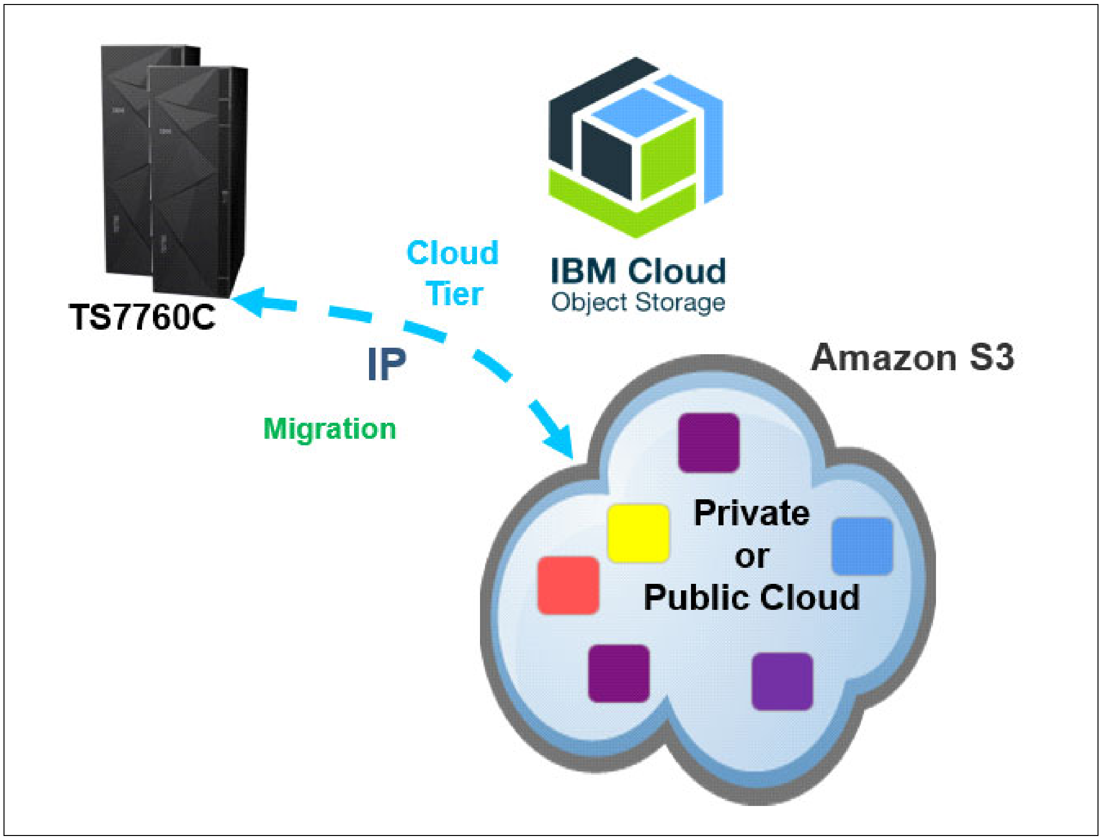


Figure 4-2 High level overview of how an object store can be a storage tier behind the TS7760

Similar to TS7760 Tape Attach, the TS7760C includes disk cache partitions that are available to manage the disk cache footprint of the TS7760C. Workloads that benefit from larger disk cache footprints can use a large disk cache partition; workloads that do not require as much disk cache residency can target smaller partitions.

TS7760C disk cache partition support works much the same as TS7760T, as shown in Figure 4-3.

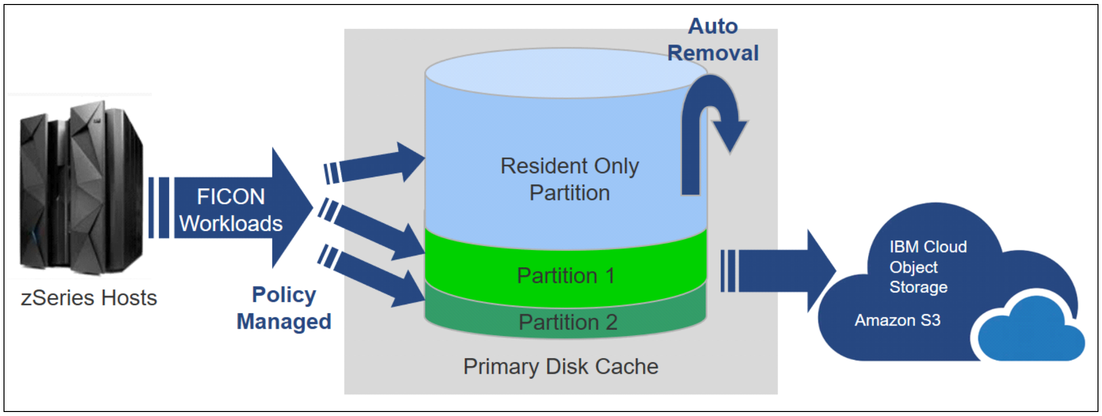


Figure 4-3 Partition support for the TS7760C

Logical volumes that target any partition other than the residency-only partition premigrate to an object store immediately. The policy that is assigned to the logical volume and how much space is available in the partition determines if and when the logical volume is removed from disk cache after the premigration. That is, as with the TS7760T, the copy in disk cache is removed, which makes the cloud instance the only available copy in that cluster. A recall of the logical volume from the object store into the disk cache is required if that cluster was chosen for the tape volume cache (TVC) or a copy source.

By using the TS7700 grid network (same physical link), the TS7760C can communicate with regional and multi-region object store configurations. For example, a two site configuration is shown in Figure 4-4 in which each site has three Accessers that are used for connectivity to the IBM Cloud Object Storage vault.

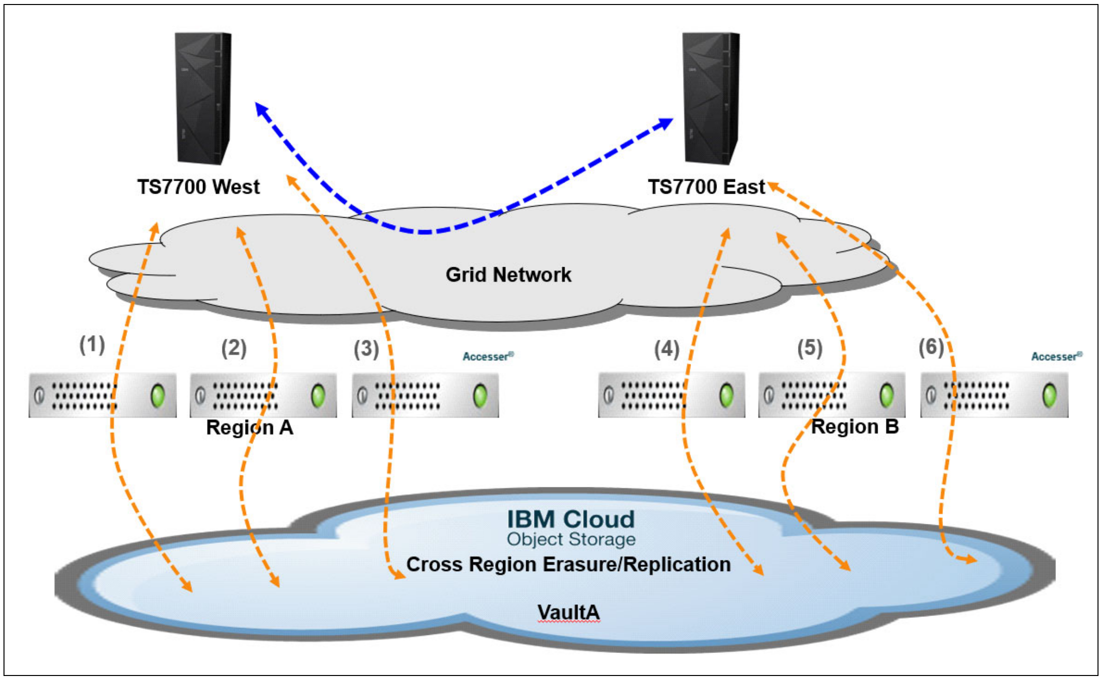


Figure 4-4 Two region access to an IBM Cloud Object Store

Another sample of a cross region replication configuration for Amazon S3 is shown in Figure 4-5.

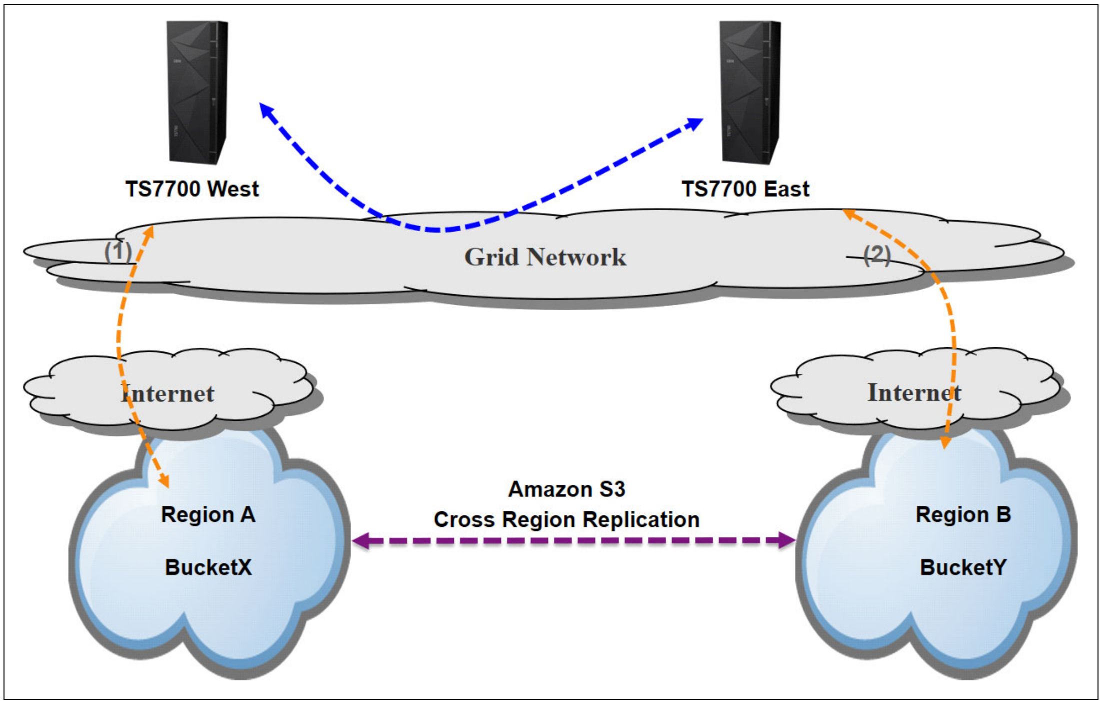


Figure 4-5 Cross Regional Amazon S3 configuration

Similar to TS7700 disk-only that is mixed with TS7760T clusters, the TS7760C can be mixed within the same grid. At the time of this writing, a particular cluster cannot be both Tape Attach and support Cloud Storage Tier at the same time; therefore, the two features are mutually exclusive.

However, Cloud Storage Tier clusters can be mixed in a grid with disk-only and Tape Attach clusters. Hybrid grid concepts apply with TS7760C clusters as they did with TS7700T clusters. An example of a Hybrid grid where TS7760, TS7760C, and TS7760T clusters exist is shown in Figure 4-6. By using auto-removal policies, data can migrate towards the clusters with deep capacity through physical tape or cloud storage tier support.

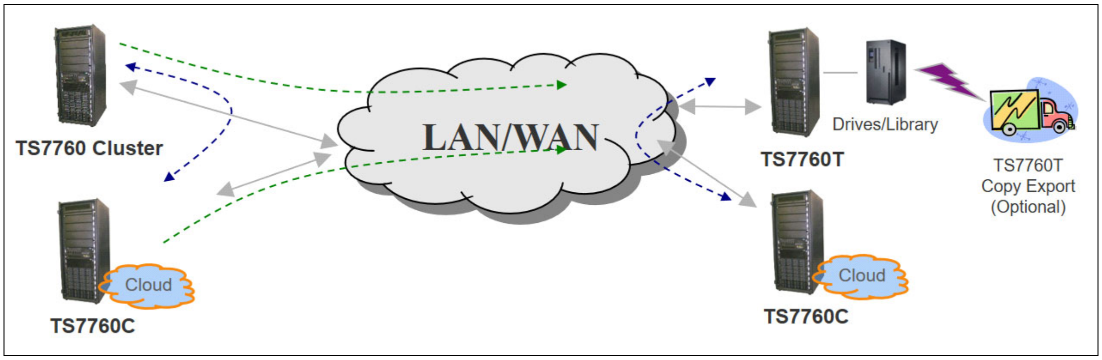


Figure 4-6 Hybrid grid configuration with TS7760C, TS7760T, and TS7760 clusters

4.1.2 TS7760C cloud pools

Cloud pools are used by the TS7760C to segregate data in the cloud. A user can define a grid-scope cloud pool as a method to separate data by type, by user or tenant or even by object store target. Through policy management, workloads are assigned to a particular cloud pool so all logical volumes that are assigned to the particular cloud pool are in the same object store container or mirrored container. As of this writing, only one cloud pool per grid is supported. Future enhancements will support up to 128 cloud pools.

4.1.3 TS7760C accounts

Accounts are used by the TS7760C to authenticate with a particular object store. A user can define up to 128 grid-scope accounts, which contain information, such as user key and a secret key or password. By using accounts, the TS7760C can authenticate with object stores to store data for a specific cloud pool.

4.1.4 TS7760C containers

Containers are used by the TS7760C to store and retrieve data in an object store. A user defines a container for a specific vault or bucket in the object store. The container is then tied to a cloud pool and account.

Data that is associated with the assigned cloud pool uses the provided account information to authenticate with the assigned vault or bucket. More than one container can be defined because each region of the grid can access a different bucket or require different user credentials to authenticate with the object store. Up to 128 grid-scope containers can be defined.

TS7760C container URLs

URLs are required before vaults or buckets can be accessed. After one or more TS7760C containers are defined, one or more URLs can be assigned to that container. The URLs provide the address of how the TS7760C can communicate with the vault or bucket in the object store. For IBM Cloud Object Storage, this URL can be one or more IP addresses that are associated with Accessers or network load balancers.

For Amazon S3, a single URL is generated by using the bucket name that is provided in the container definition. After a container has one or more URLs assigned to it, one or more TS7760C clusters in the grid must be associated with the URLs. That is, the URLs that are provided are grid-scope and can be used by any TS7760C cluster. However, which clusters use which URLs can be unique; therefore, a cluster association with each cluster and its assigned URLs must be made.

A high-level overview of how URLs are used to connect to a vault in an object store by using credentials that are assigned in an account is shown in Figure 4-7. The container definition ties them together.

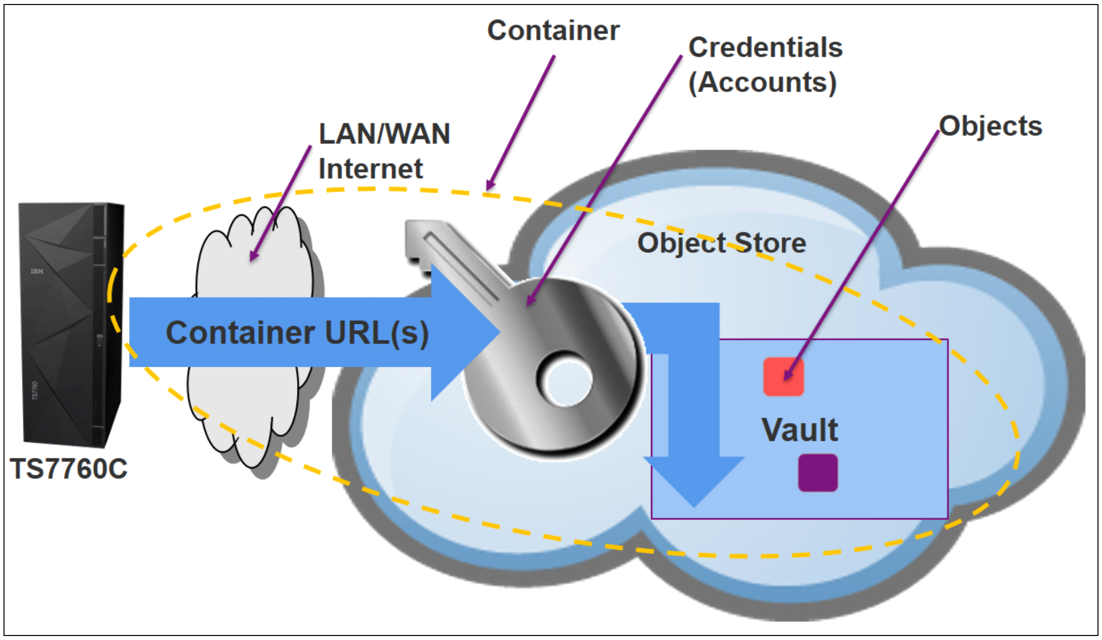


Figure 4-7 Overview of URLs, accounts, and containers

4.1.5 Container Replication

In this section, we describe how the TS7760C works with different object store resiliency use cases. As described in Chapter 2, “Container resiliency” on page 9, there are different methods of which object stores can be resilient.

For availability purposes, the TS7700 supports multiple URLs for a specific container, which allows one or more Accesser to be used from an IBM Cloud Object Storage setup. With container URL definitions, each region can access a different set of URLs or Accessers so that the local most efficient connection into the object store is used.

When vault mirroring or cross-region replication is enabled, two containers can be defined at each region that are tied to the same cloud pool. This way, each region can use its own container definition, set of URLs, and credentials to access the same content in the cloud pool.

When the TS7760C attempts to premigrate logical volumes to a mirrored bucket, the TS7760C always checks if the mirror copy exists before skipping the premigration. This extra audit provides another layer of security by not removing grid replicated volumes from disk cache unless the “copy in the cloud” truly is available at the alternative location.

5

TS7760C planning considerations

In this chapter, we describe planning considerations for the TS7760C.

5.1 Overview

Beginning with release level 4.2, the TS7760 supports the Cloud Storage Tier feature for stand-alone and grid configurations. Consider the following points regarding the TS7700 Cloud Storage Tier function:

- If the TS7760 is part of a grid, the entire grid must be at code level 4.2 or higher before the TS7760 can be cloud enabled.
- The Cloud Storage Tier feature, which is feature code (FC) 5278, can be enabled on a TS7760 non-concurrently.
- A total of 64 GB total physical memory is required before FC4278 can be installed. Another 32 GB of memory (FC3466) is a co-requisite to enabling Cloud Storage Tier support.
- The cloud enablement feature can be ordered (FC 5278) so a TS7760 can be upgraded to attach to a cloud storage tier, if it does not have tape attached. Cloud enablement and the tape attach feature are mutually exclusive. A TS7760 cannot be connected to a cloud storage tier and physical backend tape. However, a hybrid grid can be created with a TS7760T and TS7760C present.
- The TS7700 supports only IBM COS private configurations with a fixed IP addressable endpoint on port 80 (for http) or 443 (for https) and public Amazon S3 cloud object storage that are addressable by way of the public internet accessible bucket-based domain name (for example, `http://bucket.s3.amazonaws.com`). Make sure port 80 (for http) or port 443 (for https) is opened on the destination side in the Grid network.
- A TS7760 can be a TS7760C or TS7760T. Tape attach and cloud storage tier are currently mutually exclusive in the 4.2 release.
- Any cloud hardware (IBM COS), accounts, and containers (vaults or buckets) should be configured and setup before the TS7700 Cloud Storage Tier feature is configured.
- The TS7700 cannot monitor the available capacity of an attached object store. Therefore, the TS7700 user *must* monitor the available capacity. For more information, See Chapter 12, “Monitoring the TS7700C” on page 115.
- A cloud container is accessible by way of a URL, which includes a host name (for Amazon S3) or Internet Protocol (IP) address (for IBM Cloud Object Storage). A host name is resolved to an IP address by a Domain Name System (DNS). A TS7700’s DNS IP address must be specified if a cloud URL includes a host name, and the host name must be translatable by the specified DNS server.
- A minimum of 1 TB of active premigration queue is required (FC 5274). Up to 10 FC 5274 can be installed and after this amount, up to 10 increments of 5 TB active premigration queue can be installed (FC 5279).
- The configured clock time on the TS7700 and the cloud endpoint device must be synchronized. If the time difference between the TS7700 and cloud endpoint is greater than 10 minutes, authentication fails when you configure or use the cloud storage tier.
- The TS7700 connection to an object store uses the TS7700 grid network. Therefore, the same physical network that is used for grid replication must be used for object store connectivity. Your network team must be able to configure the grid network so that it can route properly to any targeted object stores. If the connected object store is AWS S3, the internet must be accessible from the grid network for outbound communications on port 80 or 443.
- If Amazon S3 cloud object storage is to be used, the TS7700 management interface network must have a configurable DNS server capable of translating `*amazonaws.com` addresses into IP addresses.

- Port 80 (for http) or port 443 (for https) must be opened within the grid network for the TS7700 to communicate with the object store.
- Although no IBM Z host software support is required to use the TS7700 Cloud Storage Tier support, APAR OA55481 does add support for new cloud-related SMS displays.
- In a stand alone configuration, the TS7700C grid network adapters are used exclusively to communicate with the attached object store.
- At the time of this writing, the TS7700C does not support retention enabled vaults.

Cluster join grid merge considerations

Some considerations must be considered when join or merge events occur with one or more clusters supporting cloud object tier. Different cluster join and grid merge scenarios are listed in Table 5-1. Whether they can be supported when one or more clusters have FC5278 installed and enabled is listed in the right-most column.

> **Note:** If you intend on joining a cloud enabled cluster to a grid, that cluster must not have any configured cloud settings.

Table 5-1 TS7700 4.2 GA support for joins and merges

Type	Joining/Merging Cluster(s)	Existing Cluster(s)	4.2 GA Supported
Join	Not Cloud Enabled	Not Cloud Enabled	Yes
Join	Cloud Enabled	Not Cloud Enabled	Yes[a]
Join	Not Cloud Enabled	Cloud Enabled	Yes
Join	Cloud Enabled	Cloud Enabled	Yes[a]
Merge	Not Cloud Enabled	Not Cloud Enabled	Yes
Merge	Cloud Enabled	Not Cloud Enabled	Yes
Merge	Not Cloud Enabled	Cloud Enabled	Yes
Merge	Cloud Enabled	Cloud Enabled	Yes[b]

[a] Only supported if the joining cluster does not have any configured cloud pools, cloud accounts, containers or URLs.

[b] Only supported if the resulting grid contains no more than one cloud pool and no more than 256 items for each of the following components: cloud accounts, containers, cloud URLs and cluster associations.

Post installation for grid

Because object store and grid replication traffic share the grid network links, running into a false-positive link imbalance issue greatly increases. That is, the TS7700 can falsely believe an issue exists with one or more links because of throughput differences on the links.

Having IBM service adjust the TS7700 internal NTC threshold value away from its default 60% can help reduce the following false warnings:

- When **PARTRFSH** is used to move a logical volume from CP0 to a CPx disk cache partition, premigration to the cloud does not occur if the volume's storage group assignment did not previously assign it a cloud pool rank when the logical volume was last mounted. A mount or demount is required to trigger a premigratoin to the cloud. Therefore, it is ideal that all logical volumes that are created in any cluster in a grid always assign a pool rank in anticipation of future **PARTRFSH** commands. For more information, see Chapter 13, "Migration and upgrade considerations" on page 125.
- When **COPYRFSH** is used to copy a logical volume to a TS7760C cluster CPx disk cache partition, premigration to the cloud does not occur if the volume's storage group assignment did not previously assign it a cloud pool rank when the volume was last mounted by a host. A mount or demount is required to trigger a premigratoin to the cloud. Therefore, it is ideal that all logical volumes that are created in any cluster in a grid always assign a pool rank in anticipation of future **COPYRFSH** commands. For more information, see Chapter 13, "Migration and upgrade considerations" on page 125.

6

SSL certificate

When a secure HTTPS connection is used to access a connected object store, SSL certificates are required to setup the secure connection. To ensure the data that is exchanged between the TS7700 and the cloud provider is encrypted, we recommend the use of a secure http connection (https) for accessing the cloud storage.

This chapter provides a brief explanation of certificate authority types and how to configure the TS7700 to trust these certificates.

This chapter includes the following topics:

6.1 Overview

When an SSL connection is established, one or more certificates are used to secure the connection. The certificates provide a method to encrypt the connection and provides an identity signature that helps any client to certify the server or object store is valid. This identity can be verified through the SSL authority signature that is within the certificate.

The signature can be self-signed by the server device, signed by an organization's internal authority, or publicly signed by a third party public authority. Independent of how it is signed, a client must trust the authority, which requires the client have a corresponding trust entry that is associated with the certificate authority that signed the certificate. The authority that signed the certificate is referred to as the *certificate authority* (CA).

Self-signed certificates are generally signed by the server device and then distributed by all exchanges from that point forward. That is, the server device acts as the CA.

After some duration, such as before the certificate expires, a newly self-signed certificate might need to be generated and used from that point forward. By using the same self-signed certificate for a duration of time, client devices' trust authority lists must be updated only periodically for that server's internal CA.

However, because each server acts as its own CA and generates its own signature, each client must be updated to trust every server's internal CA within the organization. A server can also create its own root-like CA in which all self-signed certificates that are generated by that server from that point forward are signed by the same internal CA. In this case, new certificates can be periodically created by that server, yet the clients do not need a trust authority update because they are all signed by the same previously trusted CA for that server.

Internally signed certificates are signed by a centralized authority within the organization. For example, it might be an organization's own internal root CA, or an assigned CA, acting as authority for all devices within the organization. This method provides a centralized level of control for all devices within an organization. That is, server devices that are not signed by the organization's root CA, or cannot provide a chain of trust to the root CA, cannot be trusted.

In addition, clients must create only a trust entry, or a chain of trust entry, for the organization's root CA because all certificates that are used by any server are signed by the same CA. This trust entry results in fewer certificate trust updates across numerous devices. After a client's trust list includes the organization's CA, or a chain of trust to the root CA, new certificates can be generated for existing and new devices without the need to update the client's trust list.

Last, publicly signed certificates are fee-based certificates that are signed by a well-known publicly trusted CA. Client devices have a list of trusts for public CAs; therefore, if the server provides a publicly signed certificate or a chain of certificates that leads to a publicly signed certificate, the client can trust that the server is who it states it is.

Client devices do not need to be manually updated to trust publicly signed CAs because the CA is well-known and trusted. Publicly signed certificates often are associated with broad domain names (for example, `*ibm.com`) and therefore, often are used by publicly addressable object stores only.

For all cases where a non-public CA is used to sign a certificate, the trusted CA list of the TS7700 must be updated. The TS700 is the client in this case and must trust the server (for example, IBM COS) and the certificates it provides.

The TS7700 management interface can be used to upload a trust of CA or manually download it from a server device. Once within the TS7700, the trusted CA can be assigned to URL connections to selected object stores that are providing the TS7700 permission to trust those connections.

In most use cases, any private object store (for example, IBM COS Private) require a trust CA update in the TS7700. A public object store (for example, `*amazonaws.com`) most likely does not require a trust update unless you configured your AWS S3 account to use your organization's own internal CA signed certificates.

In the following sections, we describe how to upload a trust CA into the TS7700 and associate it with connections to a particular object store that uses non-public CAs.

6.2 IBM Cloud Object Store

In this section, we describe how to set up your IBM Cloud Object Store and TS7700 to use a self-signed certificate or an external organization-signed certificate.

6.2.1 Self-signed CA inside your IBM Cloud Object Storage

A self-signed certificate can be generated by using IBM Cloud Object Storage Manager. When an IBM Cloud Object Storage system is initially configured, it automatically generates a self-signing CA that is used to generate certificates for all its addressable nodes. You can choose to have the IBM Cloud Object Storage generate a new CA at any time.

To have an IBM Cloud Object Storage generate a new self-signing CA, select the Administration menu and click the Configure in Certificate Authority Configuration field. In the Certificate Authority Configuration panel, click **Edit** in the Internal CA field and click **Generate new CA**.

All client devices that use this IBM Cloud Object Storage device need their trusted CA list updated to communicate with this IBM Cloud Object Storage device after a CA is generated. Therefore, generating a new CA should be done only under agreement from all users of the IBM Cloud Object Storage device.

6.2.2 Internal organization CA inside your IBM Cloud Object Storage

An internal organization's CA, or chain of trust to its CA, can be added to IBM Cloud Object Storage by using IBM Cloud Object Storage Manager. Although this CA is internal to the organization, the IBM Cloud Object Storage device views it as external; therefore, it must be updated to use the organization's CA.

To add the CA into your IBM Cloud Object Storage set up, select the Administration menu and click Configure in Certificate Authority Configuration field. In the Certificate Authority Configuration panel, click **Add CA**. In the Add External CA panel, follow the steps as described in IBM Knowledge Center.

All client devices that use this IBM Cloud Object Storage device might need their trusted CA list updated if they are not configured to trust the organization's CA. Therefore, having the IBM Cloud Object Storage changed to use a new external CA should be done only under agreement from all users of the IBM Cloud Object Storage device.

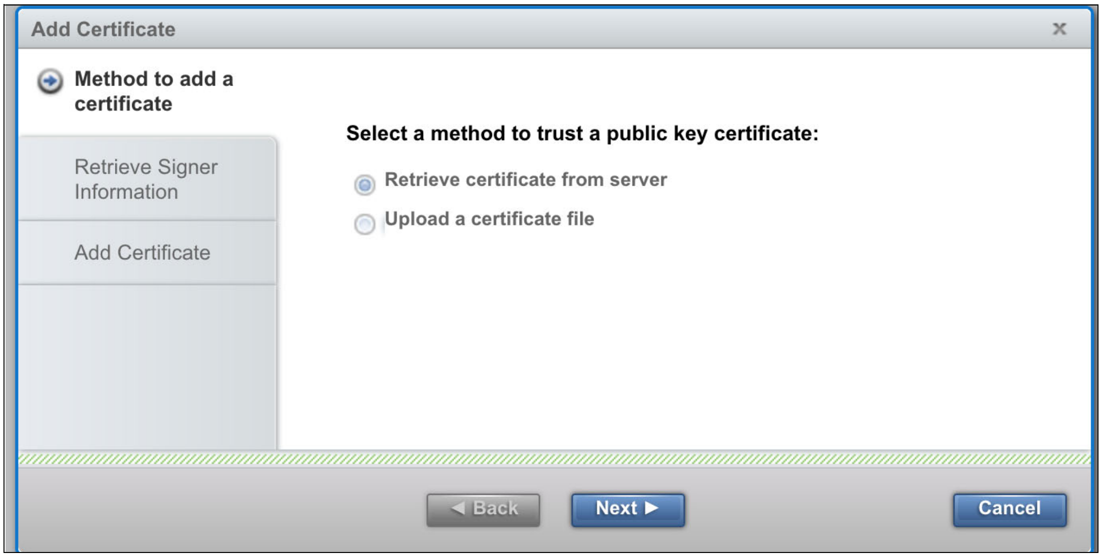
6.2.3 Updating the TS7700 CA trust list

After a SSL certificate CA is set up on your IBM Cloud Object Storage, you must update the TS7700 to trust the CA that is used by the IBM Cloud Object Storage device. Which CA type is used determines which method is used to update the TS7700.

Self-signed IBM Cloud Object Storage CA

For self-signed IBM Cloud Object Storage CAs, you must get a copy of the IBM Cloud Object Storage-generated public trust CA from your IBM Cloud Object Storage device and upload it into the TS7700. By uploading this CA, the TS7700 trusts the certificates that are signed by that particular IBM Cloud Object Storage internal CA. You can have the TS7700 automatically retrieve the trust of CA from the IBM Cloud Object Storage set up, or you can manually upload by using a text file. The manual upload method is recommended, because the CA automatically retrieved from an ICOS setup can expire sooner than the CA manually uploaded.

To automatically retrieve an ICOS CA, select **Access** →**SSL Certificates** using TS7700 Management Interface (MI). On the SSL Certificates panel, press **New Certificate**. On the Add Certificate panel, select **Retrieve Certificate** from server as shown in Figure 6-1.


Add Certificate

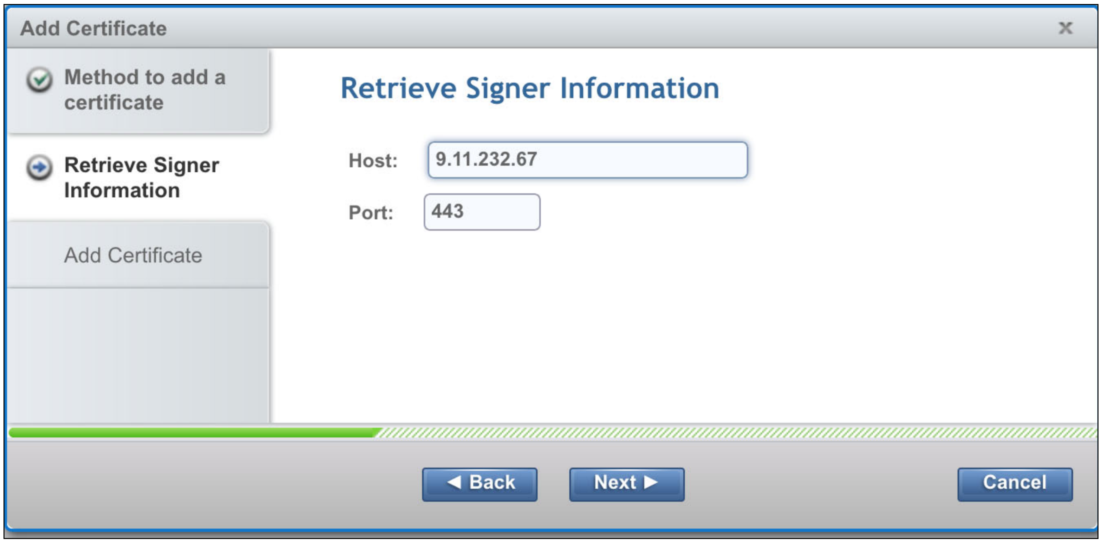
Select a method to trust a public key certificate:

● Retrieve certificate from server

○ Upload a certificate file

Figure 6-1 Retrieving SSL certificate (Step 1)

Then, enter the IP address of your IBM Cloud Object Storage (ICOS) accesser node and press Next as shown in Figure 6-2.

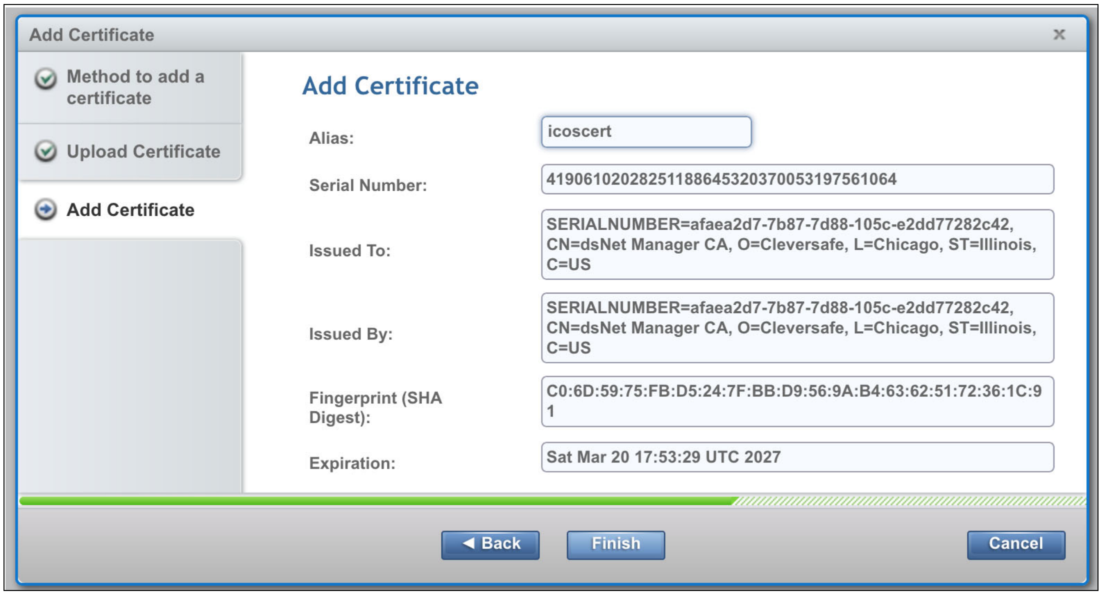

Add Certificate
Method to add a certificate
Retrieve Signer Information
Add Certificate
Retrieve Signer Information
◀ Back
Next ▶
Cancel

Host: 9.11.232.67

Port: 443

Figure 6-2 Retrieving SSL certificate (Step 2)

Enter an alias of your internal SSL certificate (e.g. icoscert) and press Finish as shown in Figure 6-3. The alias is used later when assigning different URLs to this specific CA, so choose a simple alias name that is memorable.



Alias: icoscert

Serial Number: 41906102028251188645320370053197561064

Issued To: SERIALNUMBER=afaea2d7-7b87-7d88-105c-e2dd77282c42, CN=dsNet Manager CA, O=Cleversafe, L=Chicago, ST=Illinois, C=US

Issued By: SERIALNUMBER=afaea2d7-7b87-7d88-105c-e2dd77282c42, CN=dsNet Manager CA, O=Cleversafe, L=Chicago, ST=Illinois, C=US

Fingerprint (SHA Digest): C0:6D:59:75:FB:D5:24:7F:BB:D9:56:9A:B4:63:62:51:72:36:1C:91

Expiration: Sat Mar 20 17:53:29 UTC 2027

Figure 6-3 Retrieving SSL certificate (step 3)

When manually uploading the trust of CA through a text file, select the Security menu in IBM Cloud Object Storage Manager and click **certificate authority** in the **System Fingerprint** field. Copy all the text that is displayed in your web browser, including “`-----BEGIN CERTIFICATE-----`” and “`-----END CERTIFICATE-----`”. Paste the text into a simple text editor, and save it as a text file (for example, `icos.pem`), as shown in Example 6-1.

Example 6-1 Content of .pem file

```
-----BEGIN CERTIFICATE-----

MIIF1DCCA7ygAwIBAgIQH4bSWUjefmHgSojBqPd86DANBgkqhkiG9w0BAQ0FADCB
```

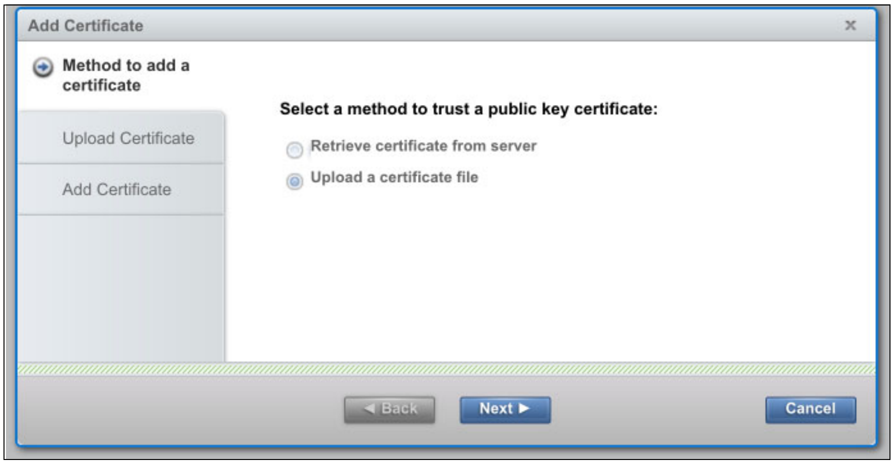
```
kTELMAkGA1UEBhMCVVMxETAPBgNVBAgMCElsbGlub2lzMRAwDgYDVQQHDAdDaGlj

…

IuSo89i55ct0+RL97GEgpQpfVIYgdefK3DNyA+IKgyS7n0ntwoRjQ5MXgCWZUeNr
LjF0nrBSux8=
-----END CERTIFICATE-----
```

Next, you must upload the certificate file to the TS7700 using Management Interface (MI). Complete the following steps.

1. Select **Access** →**SSL certificates**.
2. In the SSL Certificates panel, click **New Certificate**.
3. In the Add Certificate panel, select **Upload certificate file** and click **Next**, as shown in Figure 6-4.



Add Certificate

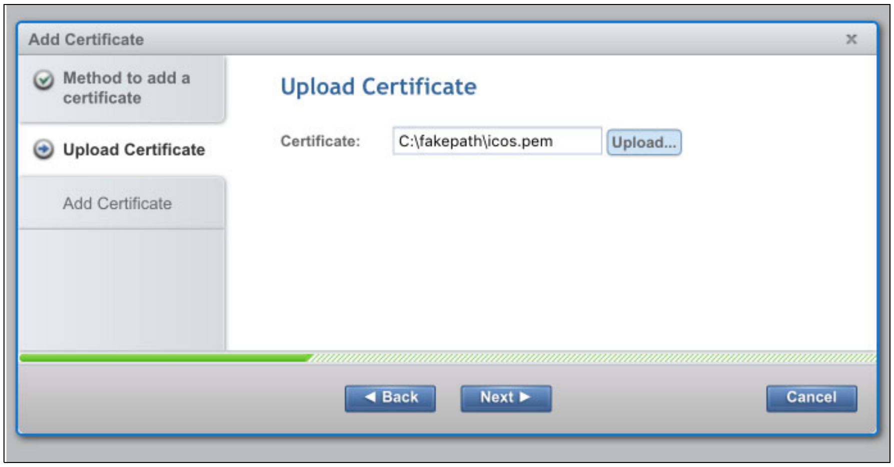
Select a method to trust a public key certificate:

○ Retrieve certificate from server

● Upload a certificate file

Figure 6-4 Selecting the Upload certificate file option

4. Click **Upload**, select your SSL certificate file (for example, `icos.pem`), and then, click **Next**, as shown in Figure 6-5.



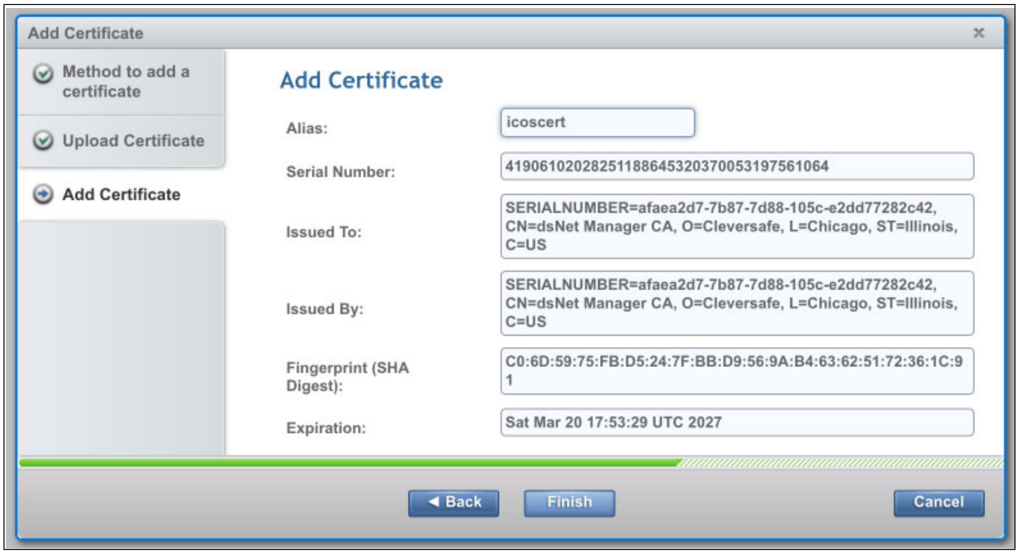
Add Certificate

Upload Certificate

Certificate: C:\fakepath\icos.pem

Figure 6-5 Certificate upload progress

5. Enter an alias of your internal SSL certificate (for example, `icoscert`) and click **Finish**, as shown in Figure 6-6. Because the alias is used later when assigning different URLs to this specific CA, choose a simple alias name that is easy to remember.



Add Certificate

Alias: icoscert

Serial Number: 419061020282511886453203700531975610 64

Issued To: SERIALNUMBER=afaea2d7-7b87-7d88-105c-e2dd77282c42, CN=dsNet Manager CA, O=Cleversafe, L=Chicago, ST=Illinois, C=US

Issued By: SERIALNUMBER=afaea2d7-7b87-7d88-105c-e2dd77282c42, CN=dsNet Manager CA, O=Cleversafe, L=Chicago, ST=Illinois, C=US

Fingerprint (SHA Digest): C0:6D:59:75:FB:D5:24:7F:BB:D9:56:9A:B4:63:62:51:72:36:1C:91

Expiration: Sat Mar 20 17:53:29 UTC 2027

Figure 6-6 Finishing the upload process

You can now use the https protocol for newly created URLs and assign this CA to the URLs by using the chosen alias. For more information about assigning the URLs, see Chapter 9, “Configuring TS7700 for cloud storage tier” on page 77.

Internally-signed organization’s CA

For internally-signed CAs that are used by your organization, the chain of trust CA must be uploaded into your TS7700 at least once. The method that is used is similar to the self-signed method that is described in “Self-signed IBM Cloud Object Storage CA” on page 32, but the certificate file, its contents, or the server address must be obtained by the organization’s CA administrator. The `*.der` (binary) or `*.pem` (text) type certificate types can be upload into the TS7700.

6.3 Amazon S3

Because all **amazonaws.com* accessible buckets use a public signed CA, you do not need to update the TS7700’s CA for Amazon S3 connections. When you configure the cloud storage tier and create a cloud URL, select **None** as a certificate alias. TS7700 always uses https protocol when connecting to an Amazon S3 bucket, even if no SSL certificate is provided.

7

Setting up an IBM Cloud Object Storage Object Store

IBM Cloud Object Storage is a highly scalable cloud storage service that is designed for high durability, resiliency, and security. The TS7700 can be enabled to use IBM Cloud Object Storage as a Cloud Storage Tier.

This chapter explains how to set up your IBM Cloud Object Storage so that it can be used by the IBM TS7700C and includes the following topics:

- “TS7700 interaction with IBM Cloud Object Storage” on page 38
- “Creating an IBM Cloud Object Storage vault” on page 40
- “Creating a custom vault” on page 41
- “Using vault templates” on page 47
- “Granting access key authentication” on page 51

7.1 TS7700 interaction with IBM Cloud Object Storage

A TS7700 that is enabled to use Cloud Storage Tier must connect to a previously installed cloud object store. For the IBM Cloud Object Storage case, the user must obtain the following elements to complete the TS7700 configuration process:

- The URL of the IBM Cloud Object Storage system in the form of a web address, which includes the indication of the access web protocol (http or https) and the numeric static IP address that is associated to the service (for example, https://192.168.100.210).
- The name of the vault to be used to store TS7700 virtual volumes. The vault is referred to by the TS7700 as a *cloud container*.
- Authentication credentials. An account should be created in the IBM Cloud Object Storage system that owns storage resources to be used by the TS7700. To access such resources, the TS7700 uses the Access Management (IAM) method, which requires the following credentials to be supplied instead of the traditional user name plus password:
  - Access key ID
  - Secret access key

IBM Cloud Object Storage is presented in on-premises or off-premises (public) offering types. For the TS7700 at R4.2 code level, only on-premise IBM Cloud Object Storage is supported.

This chapter describes the following basic management procedures for the IBM Cloud Object Storage system, which are related to TS7700 requirements:

- Creating a IBM Cloud Object Storage vault (as a custom vault or originating from a template) and configuring its corresponding properties.
- Generating IAM authentication credentials to access the vault.

IBM Cloud Object Storage is a dispersed storage mechanism that use a cluster of storages nodes to store pieces of the data across the available nodes. IBM Cloud Object Storage uses an Information Dispersal Algorithm (IDA) to divide files into unrecognizable slices that are then distributed to the storage nodes. No single node contains all of the data, which makes it safe and less susceptible to data breaches while also needing only a subset of the storage nodes to be available to fully retrieve stored data. This ability to reassemble all the data from a subset of the chunks dramatically increases the tolerance to node and disk failures (IBM, 2017).

The IBM Cloud Object Storage architecture is composed of the following three functional components:

- IBM Cloud Object Storage Manager: This component provides an out-of-band management interface that is used for administrative tasks, such as system configuration, storage provisioning, and monitoring the health and performance of the system.
- IBM Cloud Object Storage Accesser: This component imports and reads data, encrypts and encodes data on import, and decrypts and decodes data on read. It is a stateless component that presents the storage interfaces to the client applications and transforms data by using an IDA.
- IBM Cloud Object Storage Slicestor®: This node is primarily responsible for storage of the data slices. It receives data from the Accesser on import and returns data to the Accesser as required by reads.

Consider the following key concepts for IBM Cloud Object Storage:

- Device sets

  IBM Cloud Object Storage uses the concept of device sets to group Slicestor devices. Each device set consists of the “width” number of Slicestor devices. Device sets can be spread across one or multiple data centers and regions.

- Storage pool

  A set of one or more device sets. Storage pools can be spread across one or multiple data centers and regions as they consist of one or many device sets

- Vaults

  Logical storage containers for data objects that are contained in a storage pool.

- Width

  The width of a vault or storage pool is the number of Slicestor devices that the data is striped across for a vault or storage pool. For example, a storage pool that has 30 storage devices is a 30-wide storage pool. As the storage pool grows, device sets of 30 more devices are added; however, the width of the storage pool remains at 30. The maximum vault width can be set to a value up to the size of the storage pool in which is it contained.

- Vault Threshold

  The threshold of an IBM Cloud Object Storage system is the number of devices that must be available for the data to be transparently readable to the user. For example, a 30-wide vault system with a threshold of 18 means that any 18 of the devices must be up for the data to be readable. Conversely, 12 of the 30 devices can be down or unavailable without affecting data accessibility.

The TS7700 interacts with IBM Cloud Object Storage through the credential records in IBM Cloud Object Storage to grant access to VAULTs. It is out of the scope of this document to describe the procedure to install and configure the IBM Cloud Object Storage offering. For the topics that are covered here, it is assumed that the IBM Cloud Object Storage is fully available and storage pools were prepared in advance to allocate vaults for usage of TS770 storage of virtual volumes.

A storage pool is defined by a logical grouping of Slicestor devices that are used to store vault data. A vault is initially created on a storage pool and can be expanded by using an existing storage pool or by creating a storage pool.

Note: A Slicestor device can be assigned to one storage pool only. Likewise, a storage pool can be created from unassigned devices only. After it is created, a storage pool cannot be expanded; however, more pools can be created and merged to expand a vault.

7.2 Creating an IBM Cloud Object Storage vault

A vault is created inside of a storage pool. Consider the following rules:

- Storage pools must be defined before vault creation. If pools are not defined, vault creation is redirected to the Create Storage Pool page.
- Multiple vaults can be created on a storage pool.
- Each pool can only be used by a single vault type.

The following types of vaults can be created:

- Management vaults retain statistics data that is generated within the system.
- Standard vaults are used to store user data. This type of vault must be paired to a TS7700 cloud container.
- Container vaults are used when the system is in container mode. Containers are created in container vaults. User data is stored within containers.
- Service vaults are needed when the system is operating in container mode. The service vault is used internally by the system to store container metadata, storage accounts, and access keys.

A system can contain a limited number of vaults. Standard and container vaults count against this limit, but management and service vaults do not. The maximum number of vaults is limited to 1000 by default. When the limit is reached, standard vault creation requests are rejected.

Standard vaults can be created after the system is set up and a storage pool is available. To use Standard vaults, the system must be operating in vault mode.

Note: As part of the planning phase, a determination must be made about the vault width and threshold (for more information about these settings, see “Creating a custom vault” on page 41). These decisions affect the availability, resiliency, performance, and storage capacity of the vault. These settings should be used to adjust the characteristics of each vault as wanted for the specific application.

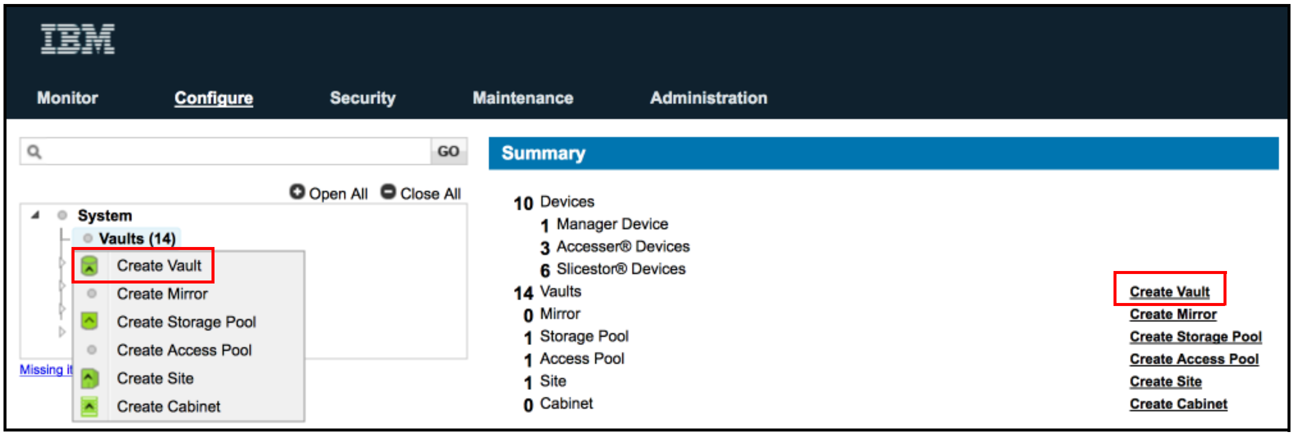
Vaults can be created by using the following methods:

- Customizing a configuration
- Using a vault template

7.3 Creating a custom vault

The TS7700 requires a vault to be used as a container. Complete the following steps:

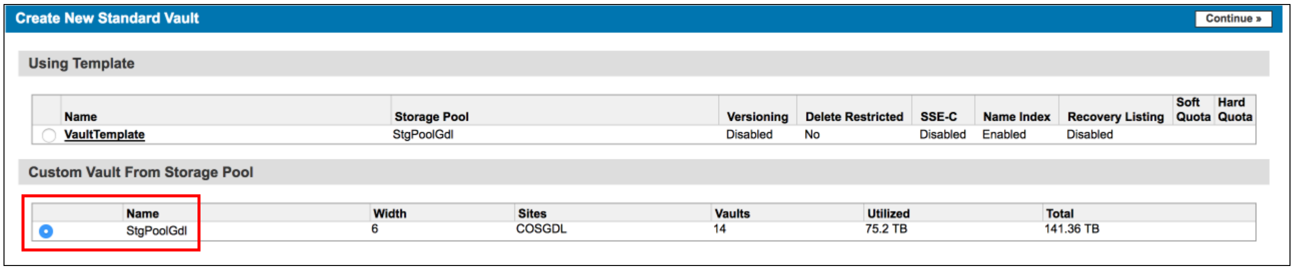
1. Open the Cloud Object Storage Manager web site of the corresponding on-premises IBM Cloud Object Storage. Select the **Configure** tab, click **Create Vault** in the Summary section, or right-click any item in the navigation tree (see Figure 7-1).



10 Devices
1 Manager Device
3 Accesser® Devices
6 Slicestor® Devices
14 Vaults
0 Mirror
1 Storage Pool
1 Access Pool
1 Site
0 Cabinet

Figure 7-1 Create Vault option in the Configure panel

2. If storage pools were created in advance, the Create New Standard Vault page opens (storage vaults are inside storage pools). Select **Custom Vault From Storage pool** (see Figure 7-2) for the target pool and then, click **Continue**.



Using Template

	Name	Storage Pool	Versioning	Delete Restricted	SSE-C	Name Index	Recovery Listing	Soft Quota	Hard Quota
○	VaultTemplate	StgPoolGdl	Disabled	No	Disabled	Enabled	Disabled		

Custom Vault From Storage Pool

	Name	Width	Sites	Vaults	Utilized	Total
●	StgPoolGdl	6	COSGDL	14	75.2 TB	141.36 TB

Figure 7-2 Selecting a method to create a new standard vault

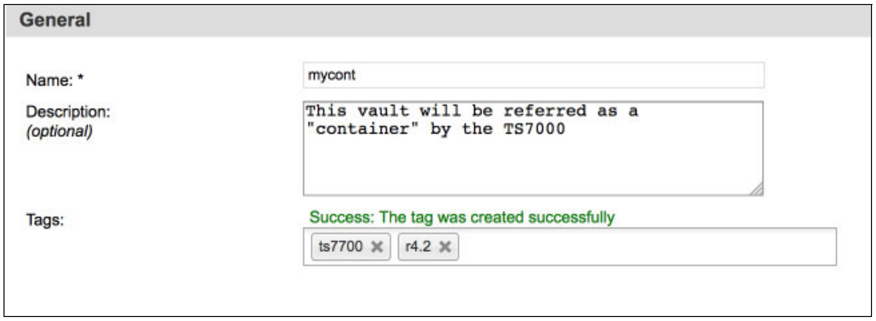
3. In the General section (see Figure 7-3 on page 42), the following settings are available:

   – Name: Each vault must be uniquely named. The IBM Cloud Object Storage Manager use this name for all references to this vault. Consider the following rules:

     - Container names must be 3 - 63 characters long.
     - Container names must not contain uppercase characters, underscores, or periods (“.”).

   – Description: Optional free-form description of the vault.

   – Tags: Optional labels can be created and or assigned to a vault before the vault is created.



General

Name: * mycont

Description: *(optional)*

```
This vault will be referred as a
"container" by the TS7000
```

Tags:

Success: The tag was created successfully

Figure 7-3 Creating standard vault

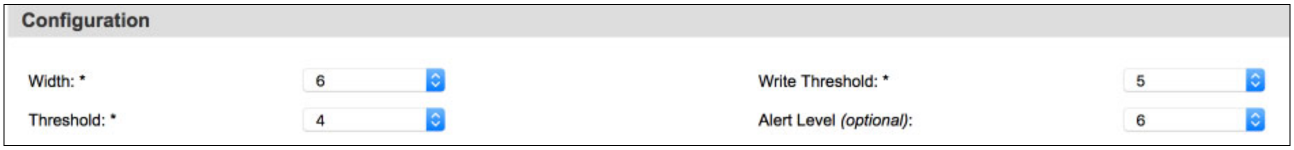
- The following options can be available in this panel, depending on the configuration of the IBM Cloud Object Storage or the IBM Cloud Object Storage storage pool where the vault is stored:
  - Provisioning code: During the container creation process, specify a unique provisioning code to indicate in which container vault the container should be created. The default value is the vault name, after it is entered. The value often is the `locationConstraint` or `region`. If the provisioning code is not set, containers can be created in this new container vault if it is configured as the default container vault for an access pool.
  - Region (Optional): A region can be provided to indicate where the contents of this vault is stored. The `locationConstraint` parameter, which is shown for containers that are associated with this vault in the S3 GET Service Extended and S3 GET Bucket Location APIs, are populated with the value set for region.
  - Storage class: This setting is optional setting, is used for the IBM Cloud Object Storage, and differs from the construct policy type that is used for the TS7700. It is provided to assign a classification to all objects that are stored within this vault. The `header x-amz-storage-class` is shown in the S3 GET/HEAD Object and the StorageClass in the response body of the S3 GET Bucket are populated with the value set for storage class.

4. Several options are displayed in the Configuration section. When the width of the pool for this vault is greater than 6, complete the following fields:
   - Width: The width of the vault corresponds to the number of slices into which all data in the vault is split. Vault width must be a factor of the storage pool width. The Manager Web Interface allows any vault width that is greater than or equal to 6 and less than or equal to 60.
   - Threshold: The minimum number of slices that must be available to perform a read:
     - Pre-defined, supported thresholds are presented when the drop-down list is clicked. The vault threshold (which is always less than the width) determines the reliability of the vault. If the set of available Slicestor devices is such that the number of slices falls below this threshold, the vault content cannot be read, and the vault appears as red in the Monitor application.
     - The Manager Web Interface allows any value between 1 and Vault Width, inclusive.
     - If the vault is on a storage pool that spans multiple sites, the Manager Web Interface warns the user if the selected threshold is high enough such that a single site outage affects read and write availability.

– Write threshold: The Manager Web Interface allows any value if the following conditions are met:

  - Write Threshold > Threshold (Write Threshold = Threshold is allowed if Threshold = Vault Width or if Vault Width < 6).
  - Write Threshold <= Vault Width.
  - Write Threshold + Threshold) > Vault Width.
  - Write Threshold defaults to Threshold + 2, if that is within the allowed range. Otherwise, the selected Write Threshold is the halfway point between the minimum allowed Write Threshold and Vault Width, rounded up. This value is selected by default in the Write Threshold drop-down when Threshold is selected. This value is also used as the Write Threshold when a vault is created through the Manager REST API and a Write Threshold is not specified.
  - If the vault is on a storage pool that spans multiple sites, the Manager Web Interface warns the user if the selected write threshold is high enough such that a single site outage affects write availability.

– Alert level: Optional setting. If the set of available Slicestor devices is such that the number of slices is between the write threshold and the alert level exclusive, the vault icon is yellow in the Monitor application. In this case, the vault is still fully functional (see Figure 7-4).



Configuration

Width: * 6

Threshold: * 4

Write Threshold: * 5

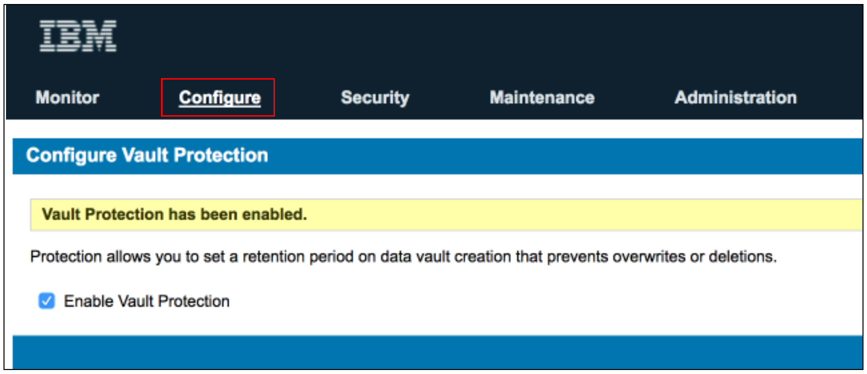
Alert Level *(optional)*: 6

Figure 7-4 Create new standard vault (Configuration section)

– When the width of the pool for the vault is 7, you also should be able to select a vault optimization to create a Concentrated Dispersal vault. This option is available only if the parent storage pool also was configured for Concentrated Dispersal. In this mode, each Slicestor device can be responsible for multiple slices of a object that is stored in the system instead of only one (when you choose a vault optimization, it cannot be changed later). Consider the following settings:

  - Storage efficiency: Width value of 7. This setting provides more usable capacity with reasonable performance.
  - Performance: Width value of 3 - 6 (better performance with less usable capacity).

5. Select a protection setting for the vault to be created (if applicable), as shown in Figure 7-5.



Configure Vault Protection

Vault Protection has been enabled.

Protection allows you to set a retention period on data vault creation that prevents overwrites or deletions.

☑ Enable Vault Protection

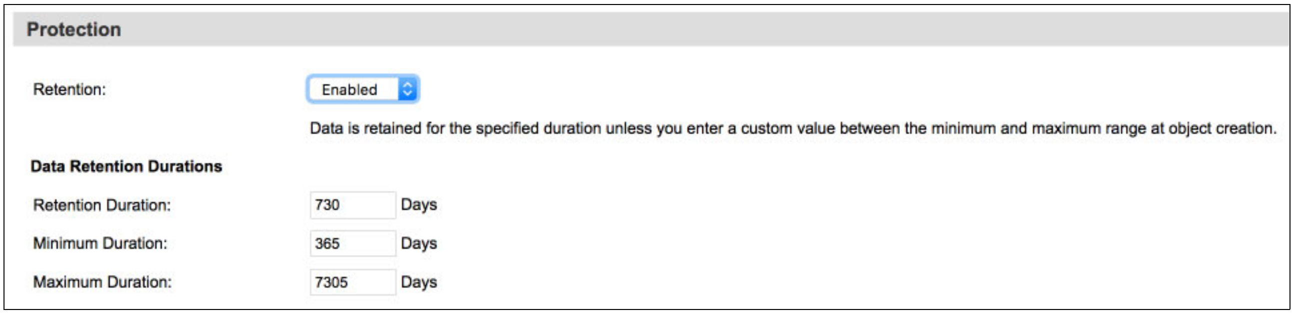
Figure 7-5 Enabling vault protection for the IBM Cloud Object Storage system

When a vault is created, the *Protection* section (see Figure 7-6) displays only if the Vault Protection Configuration options was enabled from the Configure tab. It allows objects that are stored in vaults to include associated deletion protection, where protected objects cannot be deleted until the associated data retention duration expires, and all legal holds associated with the object are removed. Consider the following settings:

- Disabled: The vault to be created does not include a protection `levelRetention` set; therefore, the remaining fields are *not* shown.

  > **Note:** This option is selected for TS7700 that is running R4.2.

- Retention: This option is *not* supported for TS7700 machines at R4.2 code level (see Figure 7-6). This option means that data is retained for a default duration of time unless you specify a custom duration. After you create the vault, you can modify the retention time settings, but you cannot change the protection level. In the Data Retention Durations section, specify the following values or accept the default values:
  - Default Duration: The default retention period (in days) for an object in this vault. The minimum supported value is 0 days, and the maximum is 36159 days. The default value is 730 days.
  - Minimum Duration: The minimum retention period (in days) for an object in this vault. The minimum supported value is 0 days, and the maximum is 36159 days. The default value is 365 days.
  - Maximum Duration: The maximum retention period (in days) for an object in this vault. The minimum supported value is 0 days, and the maximum is 36159 days. The default value is 7305 days.



Protection

Retention: Enabled

Data is retained for the specified duration unless you enter a custom value between the minimum and maximum range at object creation.

Data Retention Durations

Retention Duration: 730 Days

Minimum Duration: 365 Days

Maximum Duration: 7305 Days

Figure 7-6 Create new standard vault ("Protection" section)

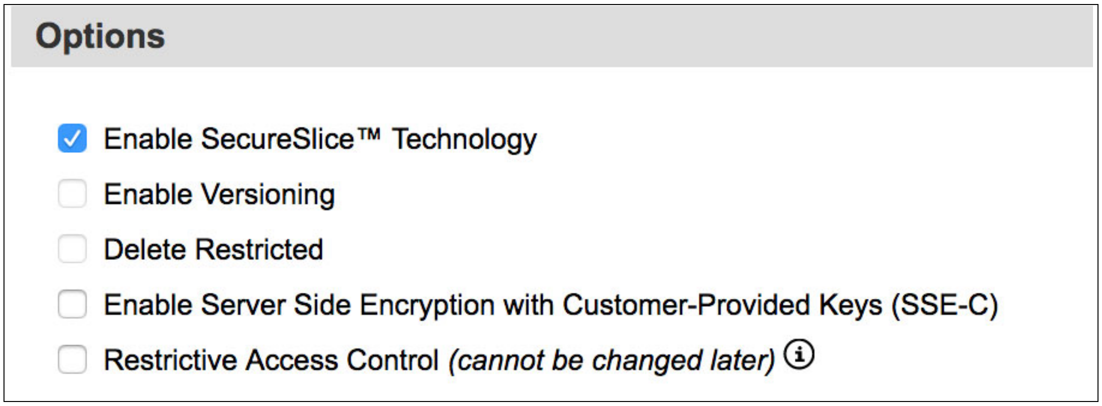
6. In the Options section (see Figure 7-7 on page 45), complete the following fields:
   - Enable SecureSlice Technology: This optional setting provides extra encryption benefits that are combined with dispersal. This option is selected by default for new vaults. The feature can be deactivated, although it is not recommended. If it is cleared, a warning message appears, and a confirmation is needed before proceeding. After the vault is created, the SecureSlice option cannot be modified.
   - Enable Versioning: Do not check this option for TS7700 vaults. It enables versioning on the vault and the TS7700 does not support a method to expire previously deleted objects. Therefore, to prevent the vault from expanding in capacity indefinitely, do not enable versioning.
   - Delete Restricted: Because TS7700 needs full access to stores objects do *not* use this feature, which allows Security Officers to restrict vault access permissions such that users with write access to the vault are not able to delete objects from the vault.

Also, object versioning is enabled in parallel to this feature, which is not fully supported by the TS7700.

– Enable Server-Side Encryption with Customer-Provided Keys (SSE-C): Do *not* select this option when vaults are created that are intended for TS7700 (support pending to be implemented). In IBM Cloud Object Storage, all stored objects are encrypted by default by using randomly generated keys and an all-or-nothing-transform.

  The default encryption model provides at-rest security, and this feature allows some workloads to possess the encryption keys that are used. Requests to read or write objects or their metadata send the required encryption information (customer-managed keys) as headers in HTTP requests.

– Restrictive Access Control: This setting restricts reads, metadata writes, and access control to only the owner of the object on protected vaults (this setting cannot be modified after the vault is created).



Options

☑ Enable SecureSlice™ Technology

☐ Enable Versioning

☐ Delete Restricted

☐ Enable Server Side Encryption with Customer-Provided Keys (SSE-C)

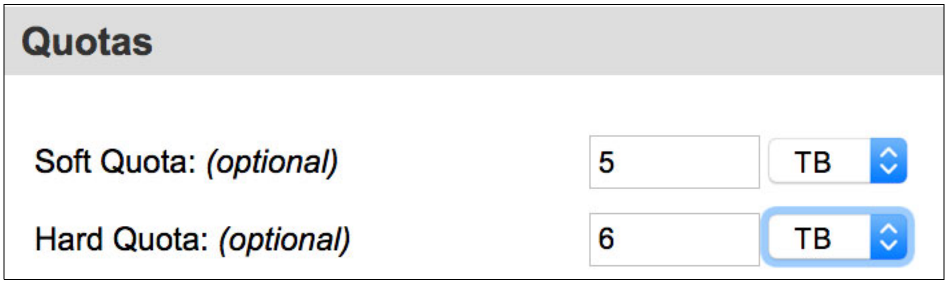
☐ Restrictive Access Control *(cannot be changed later)* ⓘ

Figure 7-7 Creating standard vault

7. In the Quotas section (see Figure 7-8), complete the following optional fields, if needed:

   – Soft Quota: A notification is sent to the Event Console if the soft quota setting is exceeded. It does not cause restrictions to usage. Setting the quota higher than the total space available in one or more storage pools that are associated with this vault has no effect.

   – Hard Quota: The Accesser device (or application) does not permit the user to exceed the hard quota value for this vault. A notification is also sent to the Event Console if the hard quota setting is exceeded. Setting the quota higher than the total space available in one or more storage pools that are associated with this vault has no effect.



Quotas

Soft Quota: *(optional)* 5 TB

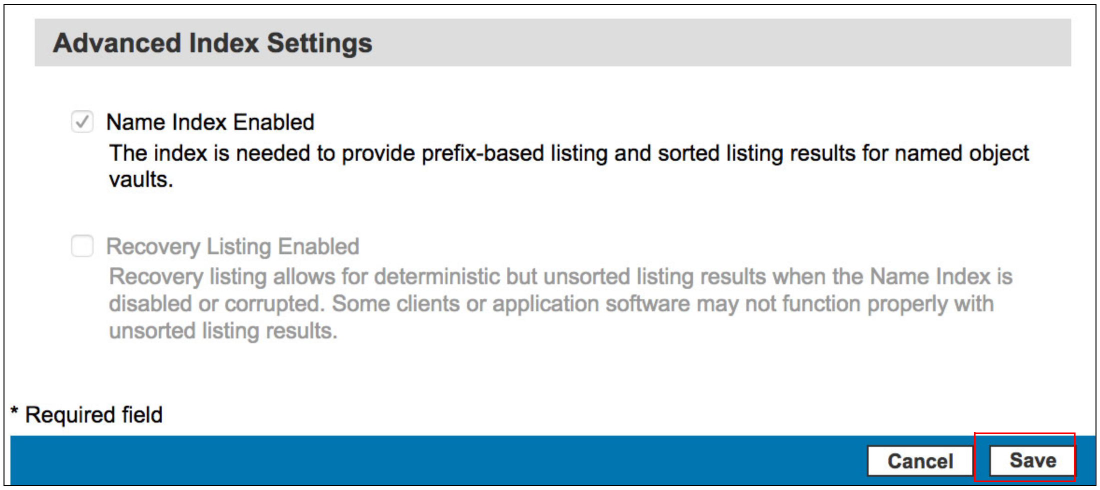
Hard Quota: *(optional)* 6 TB

Figure 7-8 Create new standard vault ("Quotas" section)

8. In the Advanced Index Settings section (see Figure 7-9), the Name Index Enabled is selected by default for Standard vaults and you can enable Recovery Listing. Consider the following options:

   – Name Index Enabled: This option is enabled by default to allow a user to list the contents of a vault in lexicographical order based on the object’s name or key. The Name Index is updated whenever objects are added or removed from a vault. The Name Index must be enabled to provide prefix-based listing and sorted listing results for named object vaults. To accommodate TS7700 future cloud salvage recovery procedures, it is highly recommended that this option is enabled.

   – Recovery Listing Enabled: This option enables limited listing capability, even when the contents of a vault are not indexed. When enabled, Recovery Listing lists the `SourceNames` of the metadata headers. Recovery Listing is slower than the Name Index listing and the results are not sorted. Recovery Listing can be used to list the contents of a vault for which Name Index is corrupted or not enabled. If Name Index Enabled is not used, this option is required at a minimum for TS7700 use.



Advanced Index Settings

☑ Name Index Enabled
The index is needed to provide prefix-based listing and sorted listing results for named object vaults.

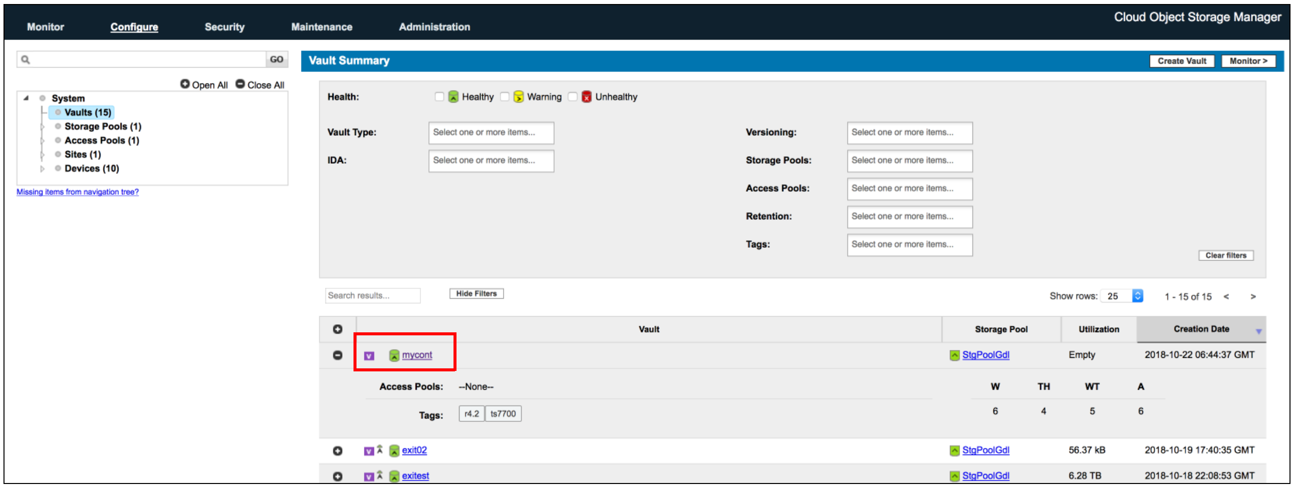
☐ Recovery Listing Enabled
Recovery listing allows for deterministic but unsorted listing results when the Name Index is disabled or corrupted. Some clients or application software may not function properly with unsorted listing results.

* Required field

Figure 7-9 Creating standard vault

9. Click **Save**.

   The new vault is shown in the Vault Summary page, as shown in Figure 7-10.



Vault Summary

Health: ☐ Healthy ☐ Warning ☐ Unhealthy

Vault Type: Select one or more items...

IDA: Select one or more items...

Versioning: Select one or more items...

Storage Pools: Select one or more items...

Access Pools: Select one or more items...

Retention: Select one or more items...

Tags: Select one or more items...

Show rows: 25 1 - 15 of 15

	Vault	Storage Pool	Utilization	Creation Date
⊖	mycont	StgPoolGdl	Empty	2018-10-22 06:44:37 GMT
⊕	exit02	StgPoolGdl	56.37 kB	2018-10-19 17:40:35 GMT
⊕	exitest	StgPoolGdl	6.28 TB	2018-10-18 22:08:53 GMT

Access Pools: --None--

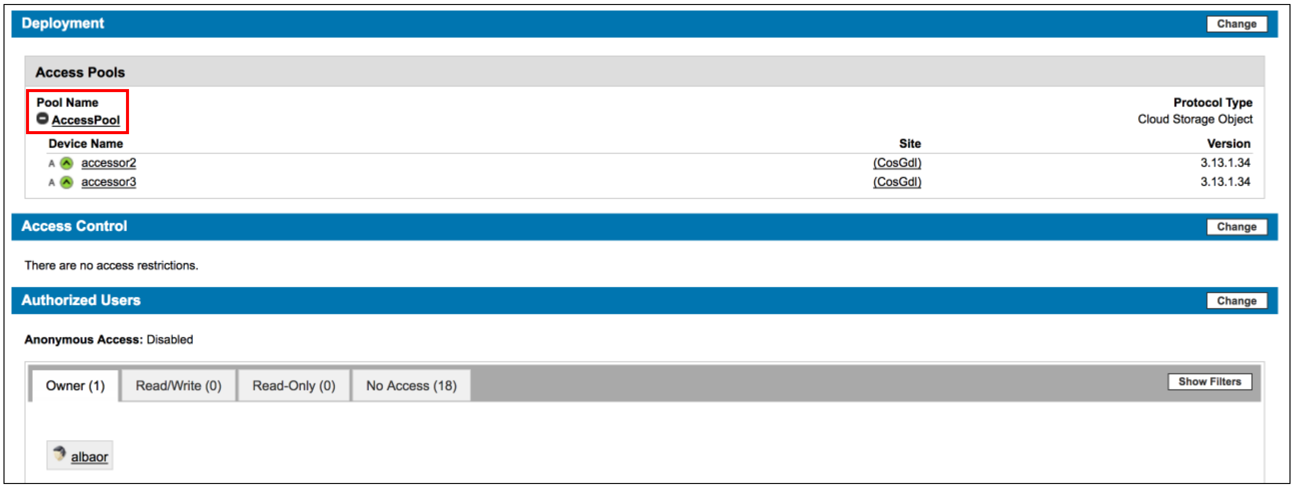
Tags: r4.2 ts7700

W	TH	WT	A
6	4	5	6

Figure 7-10 Showing Vault Summary

10.Click the vault and adjust the following properties as needed (see Figure 7-11):

- Deployment: A vault must be deployed to be visible by an Accesser pool. Available Access Pools are shown, and their view can be expanded to show their assigned devices. Click **Change** to open the Deployment menu. The Accesser registry update (and Vault availability) can take up to 5 minutes.
- Access control: For added data security, the Vault access can be restricted to specific IP addresses.
- Authorized users: Access permissions must be granted for each object vault. Extend proper authorization for TS7700 cloud accounts that must access created vaults.



Deployment Change

Access Pools

Pool Name AccessPool

Protocol Type Cloud Storage Object

Device Name	Site	Version
A accessor2	(CosGdl)	3.13.1.34
A accessor3	(CosGdl)	3.13.1.34

Access Control Change

There are no access restrictions.

Authorized Users Change

Anonymous Access: Disabled

albaor

Figure 7-11 Adjusting other vault properties

7.4 Using vault templates

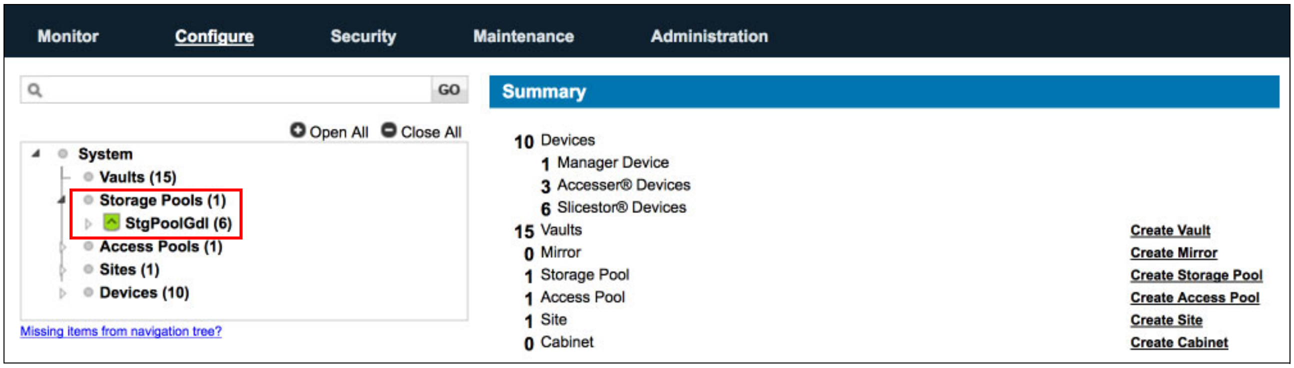
An alternative approach to vault creation is based on the use of vault templates. These templates allow a user to create multiple vaults with the same parameters quickly and enable common vault configurations to be used across multiple users.

Your IBM Cloud Object Storage administrator might create a vault template on your behalf, which makes the process of creating TS7700-based vaults much easier. A vault template is created on a storage pool and can then be used when a vault is created. All parameters that are set in the vault template apply to the vault.

7.4.1 Creating vault templates

Complete the following steps to create a vault template:

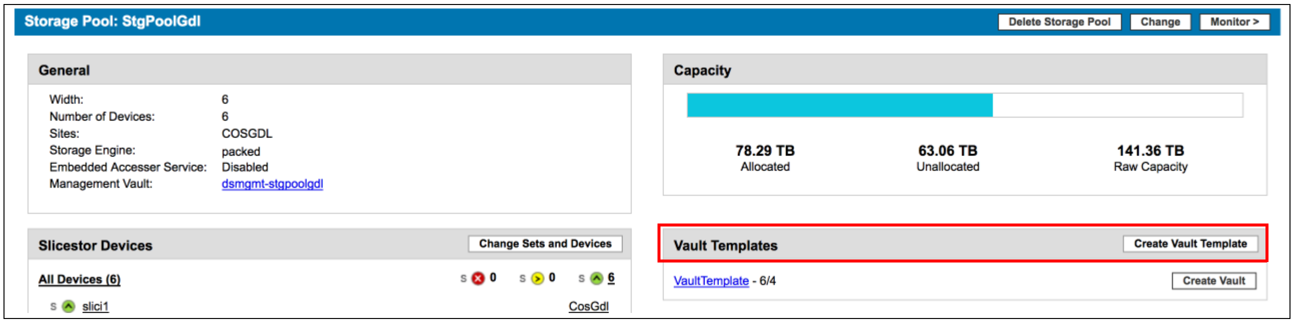
1. Open the Cloud Object Storage Manager web site of the corresponding on-premises IBM Cloud Object Storage. Click the **Configure** tab (see Figure 7-12) and then, click the storage pool for which you want to create a vault template.



10 Devices
1 Manager Device
3 Accesser® Devices
6 Slicestor® Devices
15 Vaults
0 Mirror
1 Storage Pool
1 Access Pool
1 Site
0 Cabinet

Figure 7-12 Selecting a storage pool to create a vault template

2. In the Vault Templates section, click **Create Vault Template**, as shown in Figure 7-13.



Width: 6
Number of Devices: 6
Sites: COSGDL
Storage Engine: packed
Embedded Accesser Service: Disabled
Management Vault: dsmgmt-stgpoolgdl

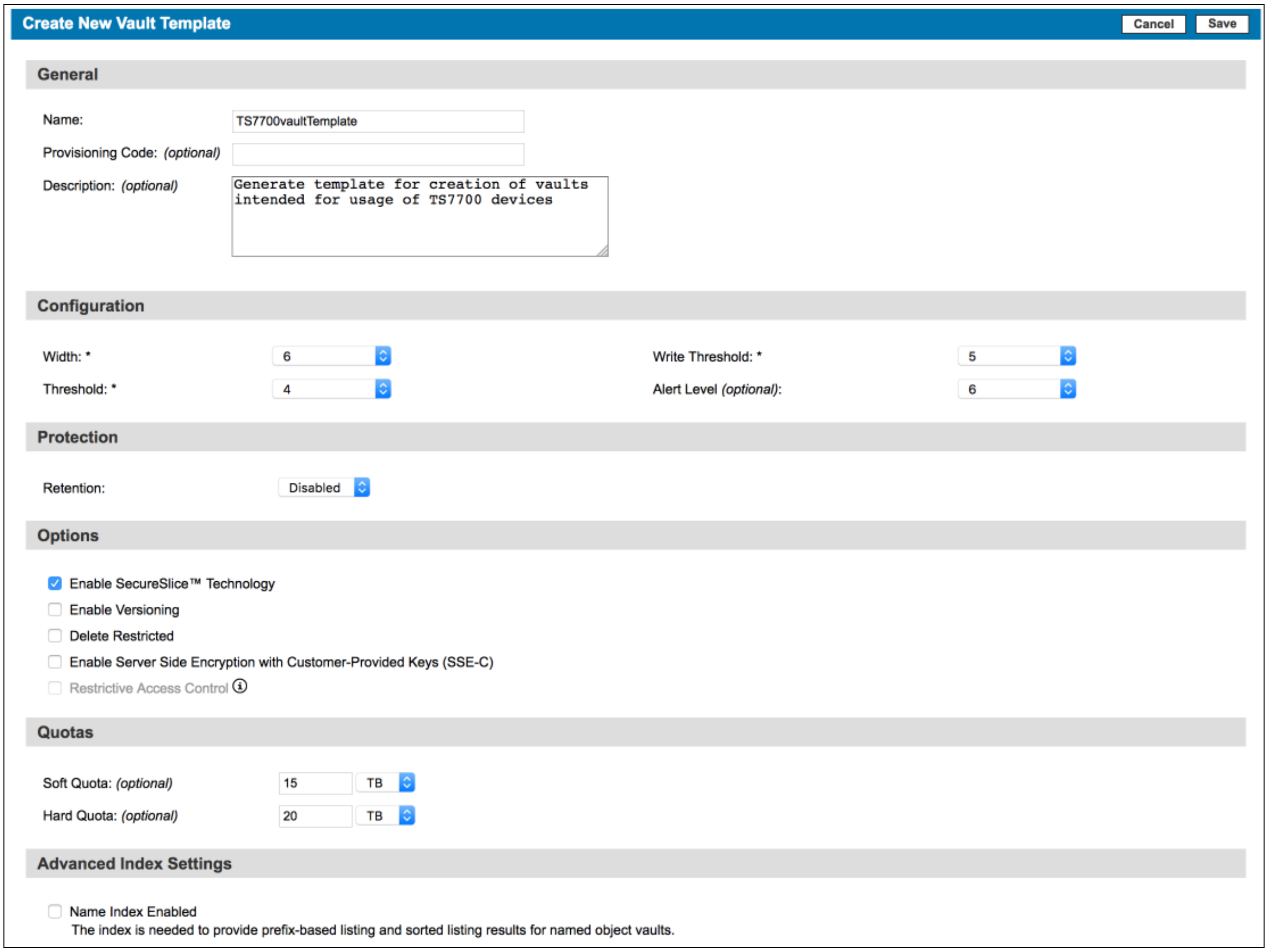
78.29 TB Allocated
63.06 TB Unallocated
141.36 TB Raw Capacity

All Devices (6) S 0 S 0 S 6
S slici1 CosGdl

VaultTemplate - 6/4

Figure 7-13 Creating a vault template from a storage pool

3. Configure the template according to the target use case (see Figure 7-14). The allowed values of fields to fill for vault templates are the same as those fields that are described in the Cloud Object Storage creation of a custom vault procedure.



General

Name: TS7700vaultTemplate

Provisioning Code: *(optional)*

Description: *(optional)* Generate template for creation of vaults intended for usage of TS7700 devices

Configuration

Width: * 6

Threshold: * 4

Write Threshold: * 5

Alert Level *(optional)*: 6

Protection

Retention: Disabled

Options

☑ Enable SecureSlice™ Technology

□ Enable Versioning

□ Delete Restricted

□ Enable Server Side Encryption with Customer-Provided Keys (SSE-C)

□ Restrictive Access Control ⓘ

Quotas

Soft Quota: *(optional)* 15 TB

Hard Quota: *(optional)* 20 TB

Advanced Index Settings

□ Name Index Enabled

The index is needed to provide prefix-based listing and sorted listing results for named object vaults.

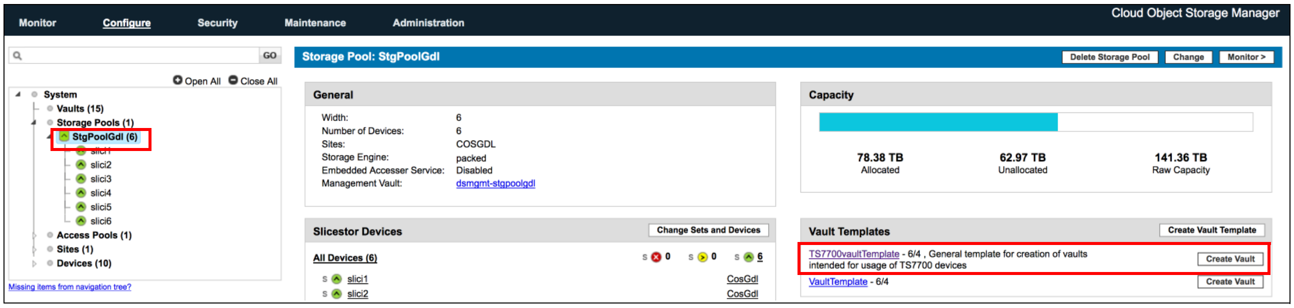
Figure 7-14 Configuring settings for a new vault template

4. When complete, click **Save**.

7.4.2 Creating a vault by using a template

Complete the following steps to create a vault by using a template:

1. Open the Cloud Object Storage Manager web site of the corresponding on-premises IBM Cloud Object Storage. Click the **Configure** tab and then, click the storage pool for which you want to create a vault. Available options are listed under the Vault Templates section of that page (see Figure 7-15 on page 50).



- System
  - Vaults (15)
  - Storage Pools (1)
    - StgPoolGdl (6)
      - slici1
      - slici2
      - slici3
      - slici4
      - slici5
      - slici6
  - Access Pools (1)
  - Sites (1)
  - Devices (10)

Storage Pool: StgPoolGdl

General

Width:	6
Number of Devices:	6
Sites:	COSGDL
Storage Engine:	packed
Embedded Accesser Service:	Disabled
Management Vault:	dsmgmt-stgpoolgdl

Capacity

78.38 TB	62.97 TB	141.36 TB
Allocated	Unallocated	Raw Capacity

Slicestor Devices

All Devices (6) s 0 s 0 s 6

s slici1	CosGdl
s slici2	CosGdl

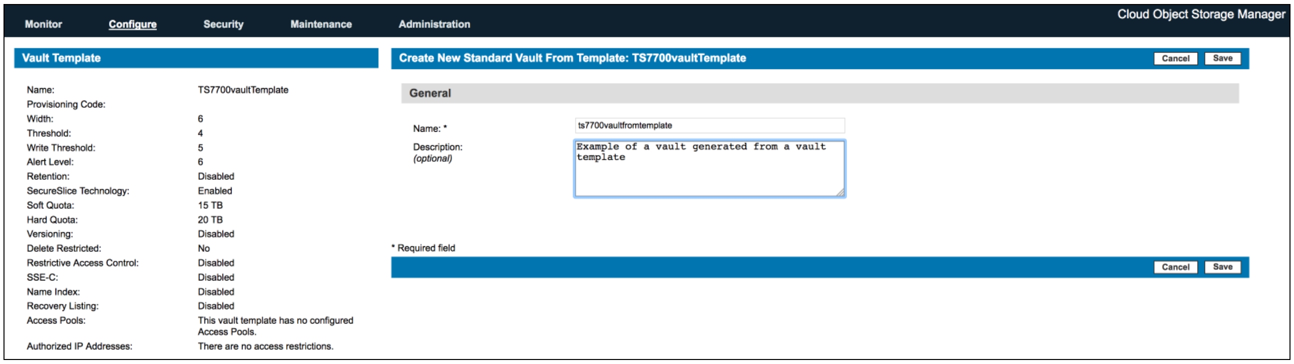
Vault Templates

TS7700vaultTemplate - 6/4 , General template for creation of vaults intended for usage of TS7700 devices

VaultTemplate - 6/4

Figure 7-15 Locating vault templates available to a storage pool

2. Click **Create Vault** next to the template to be used. At this point, the new vault needs a unique name assigned to it. The newly created vault inherits the SecureSlice state (enabled or disabled) from the Vault Template. It cannot be changed for the vault after it is created (see Figure 7-16).



Vault Template

Name:	TS7700vaultTemplate
Provisioning Code:	
Width:	6
Threshold:	4
Write Threshold:	5
Alert Level:	6
Retention:	Disabled
SecureSlice Technology:	Enabled
Soft Quota:	15 TB
Hard Quota:	20 TB
Versioning:	Disabled
Delete Restricted:	No
Restrictive Access Control:	Disabled
SSE-C:	Disabled
Name Index:	Disabled
Recovery Listing:	Disabled
Access Pools:	This vault template has no configured Access Pools.
Authorized IP Addresses:	There are no access restrictions.

Create New Standard Vault From Template: TS7700vaultTemplate

General

Name: * ts7700vaultfromtemplate

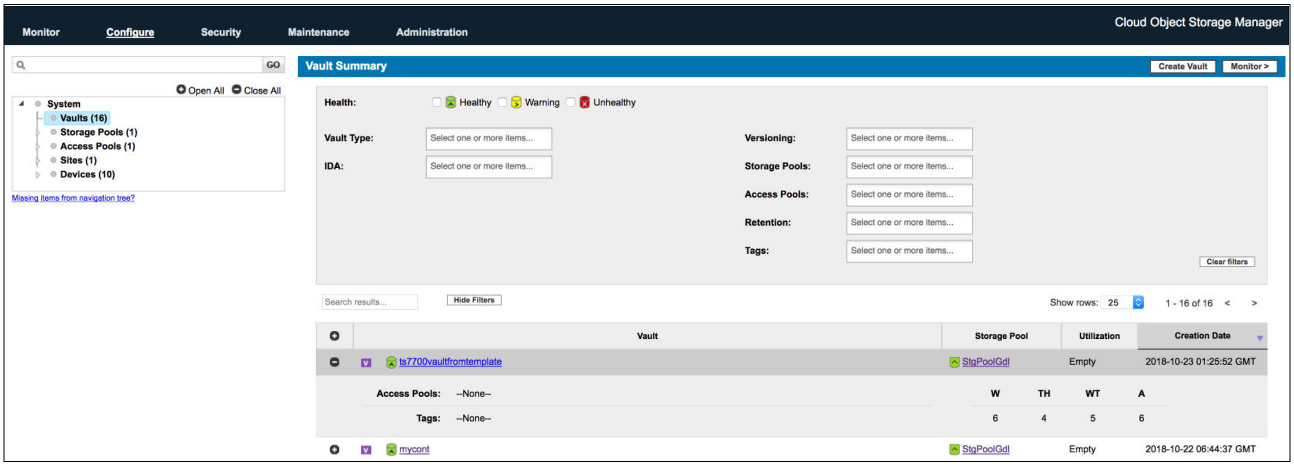
Description: *(optional)*

```
Example of a vault generated from a vault
template
```

* Required field

Figure 7-16 Creating a vault by using a template

3. Click **Save**, and your new vault is available for immediate use (see Figure 7-17.



- System
  - Vaults (16)
  - Storage Pools (1)
  - Access Pools (1)
  - Sites (1)
  - Devices (10)

Vault Summary

Health: □ Healthy □ Warning □ Unhealthy

Vault Type:	Select one or more items...	Versioning:	Select one or more items...
IDA:	Select one or more items...	Storage Pools:	Select one or more items...
		Access Pools:	Select one or more items...
		Retention:	Select one or more items...
		Tags:	Select one or more items...

Search results...

Show rows: 25 1 - 16 of 16 < >

Vault	Storage Pool	Utilization	Creation Date
ts7700vaultfromtemplate	StgPoolGdl	Empty	2018-10-23 01:25:52 GMT
mycont	StgPoolGdl	Empty	2018-10-22 06:44:37 GMT

Access Pools: --None--

Tags: --None--

W	TH	WT	A
6	4	5	6

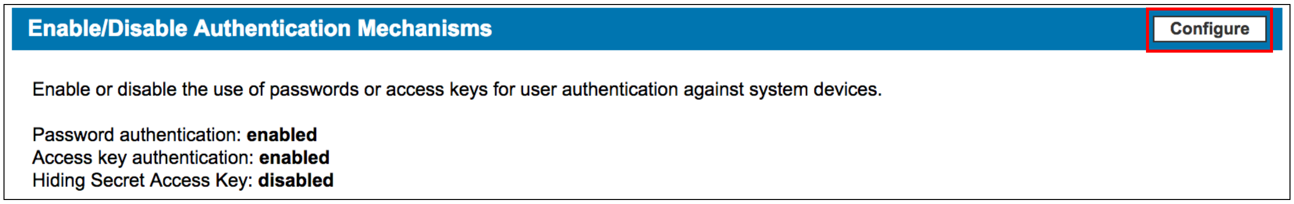
Figure 7-17 Displaying available vaults

7.5 Granting access key authentication

Access Key Authentication enables the generation of AWS-style credentials for user accounts. These credentials can be used to perform AWS authentication for S3 requests. As of release 4.2, this method must be used to be compatible with the TS7700.

Complete the following steps:

1. Open the Cloud Object Storage Manager web site of the corresponding on-premises IBM Cloud Object Storage. Click **Security** →**Enable/Disable Authentication Mechanisms** (see Figure 7-18).

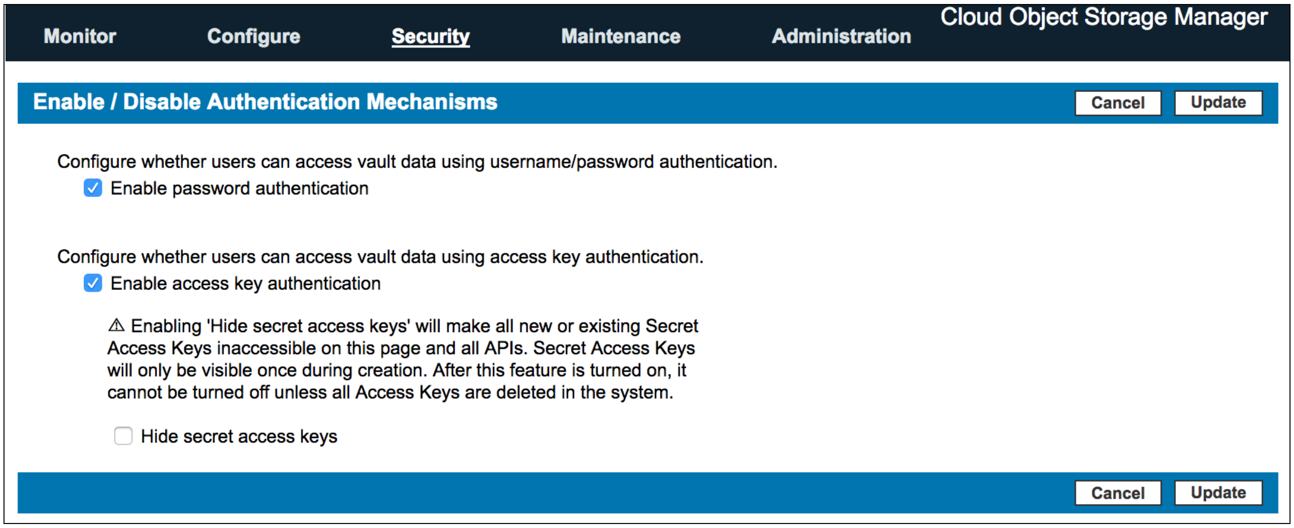


Enable or disable the use of passwords or access keys for user authentication against system devices.

Password authentication: **enabled**
Access key authentication: **enabled**
Hiding Secret Access Key: **disabled**

Figure 7-18 Checking configuration of authentication mechanisms

2. Enable Access Key by clicking **Configure** (see Figure 7-19). The target user account must exist or be created in advance. Accounts that are created while Access Key Authentication is enabled (which is the required authentication method for TS7700 access) no longer require a username and password to be set (but remains as a valid option). Be careful if the Hide secret access keys option is selected because keys are shown during creation time only (they cannot be recovered later); therefore, so copy them to a safe location.


Monitor
Configure
Security
Maintenance
Administration
Cloud Object Storage Manager
Enable / Disable Authentication Mechanisms
Cancel
Update

Configure whether users can access vault data using username/password authentication.

☑ Enable password authentication

Configure whether users can access vault data using access key authentication.

☑ Enable access key authentication

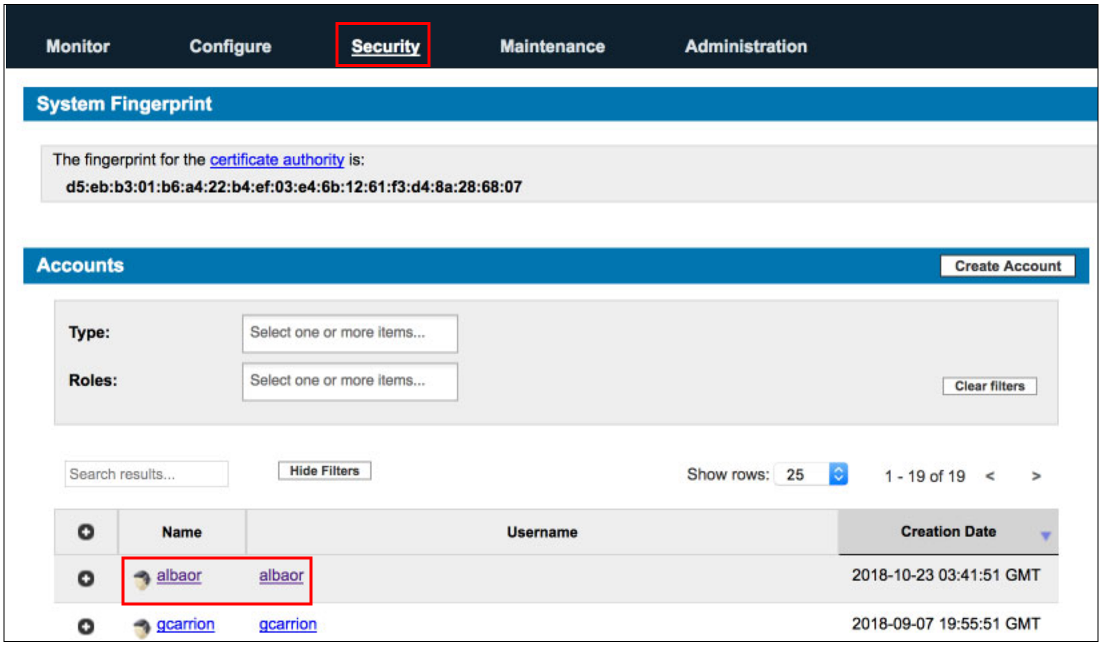
⚠ Enabling 'Hide secret access keys' will make all new or existing Secret Access Keys inaccessible on this page and all APIs. Secret Access Keys will only be visible once during creation. After this feature is turned on, it cannot be turned off unless all Access Keys are deleted in the system.

☐ Hide secret access keys

Figure 7-19 Enabling or disabling authentication mechanisms

3. Complete the following steps to set up Access Key Authentication:

   a. Select the target account by clicking **Security** →**Account Name** (see Figure 7-20 on page 52).



System Fingerprint

The fingerprint for the certificate authority is:
d5:eb:b3:01:b6:a4:22:b4:ef:03:e4:6b:12:61:f3:d4:8a:28:68:07

Accounts

Type: Select one or more items...
Roles: Select one or more items...

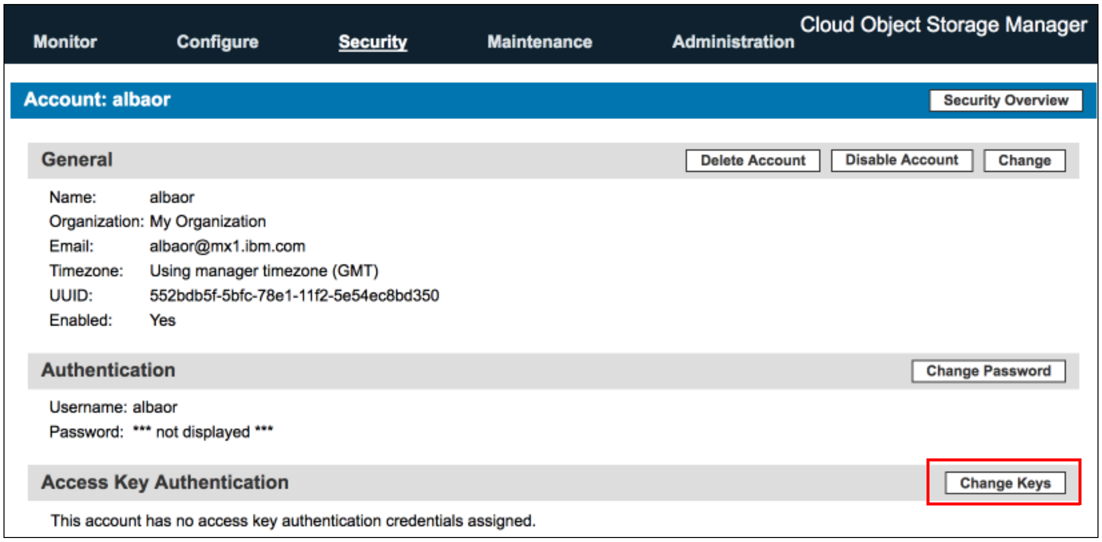
Search results...

Show rows: 25   1 - 19 of 19 < >

	Name	Username	Creation Date
⊕	albaor	albaor	2018-10-23 03:41:51 GMT
⊕	gcarrion	gcarrion	2018-09-07 19:55:51 GMT

Figure 7-20   Displaying IBM Cloud Object Storage user accounts

b. Create access keys for the target account. Select **Change Keys** to create access keys, as shown in Figure 7-21.



Account: albaor

General

Name: albaor
Organization: My Organization
Email: albaor@mx1.ibm.com
Timezone: Using manager timezone (GMT)
UUID: 552bdb5f-5bfc-78e1-11f2-5e54ec8bd350
Enabled: Yes

Authentication

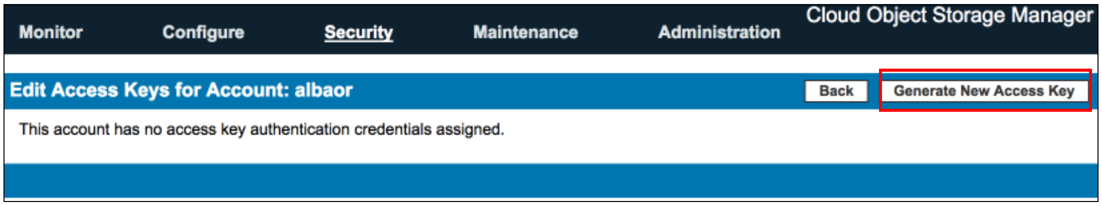
Username: albaor
Password: *** not displayed ***

Access Key Authentication

This account has no access key authentication credentials assigned.

Figure 7-21   Changing access keys for selected user

c. Click **Generate New Access Key** to create corresponding credentials. A maximum of 10 different access keys can be created (see Figure 7-22).

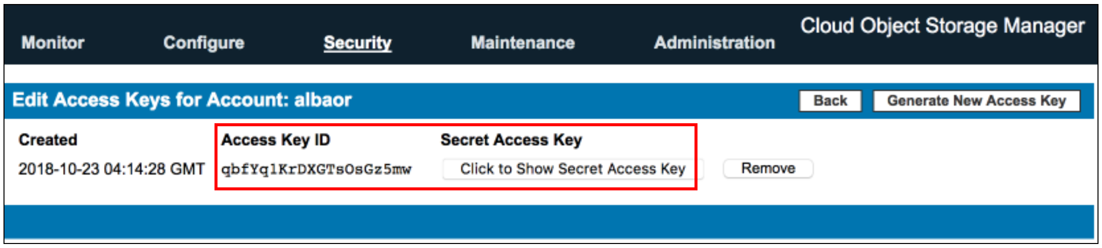


Edit Access Keys for Account: albaor

This account has no access key authentication credentials assigned.

Figure 7-22   Generating new access keys

Generated Access Key ID and Secret Access Key are required when Cloud Account access is configured in the TS7700 (see Figure 7-23).



Edit Access Keys for Account: albaor

Created	Access Key ID	Secret Access Key
2018-10-23 04:14:28 GMT	qbfYqlKrDXGTsOsGz5mw	Click to Show Secret Access Key

Figure 7-23 Displaying access keys

8

Setting up an AWS Cloud Object Storage

Amazon Simple Storage Service (Amazon S3) is a cloud computing web service that is offered by Amazon Web Services (AWS), which manages data within an AWS cloud object storage. The basic storage units of Amazon S3 are objects that are organized into buckets that are owned by AWS accounts, which are identified within each bucket by a unique user-assigned key.

This chapter describes how to set up AWS S3 for the IBM TS7700C and includes the following topics:

- 8.1, “TS7700 interaction with Amazon S3” on page 56
- 8.2, “Generating an IAM user and credentials from a root account by using the AWS console” on page 56
- 8.3, “Amazon S3 buckets” on page 62
- 8.4, “Cross-region replication” on page 67
- 8.5, “Setting up TS7700Cs with Amazon S3 Cross Region Replication” on page 75

8.1 TS7700 interaction with Amazon S3

A TS7700 that is enabled to use Cloud Storage Tier must connect to a previously installed cloud object storage. If Amazon S3 is used for this purpose, the user obtains the following elements to complete the TS7700 configuration:

- Authentication credentials: An account must be created in the AWS Web Services Cloud Platform, which owns storage resources to be used by the TS7700. To access such resources, the authentication method to be used by TS7700 is the Identity and Access Management (IAM) method, which requires the following credentials to be supplied instead of the traditional “user name” plus “password”:
  - Access key ID
  - Secret access key
- Name of the Amazon S3 *bucket* to be used by TS7700 to store virtual volumes as file objects into it. The bucket is then referred by the TS7700 as a *cloud container*. If cross region replication is used, two bucket names (one from each region) must be obtained.

Note: Unlike the case of IBM COS, the user does not need to provide a URL to connect to Amazon S3 because URLs for this public service are known in advance.

This chapter describes the following basic management procedures for the resources that are assigned in the Amazon S3 environment, which are related to TS7700 requirements:

- Generating IAM users and authentication credentials
- Creating an Amazon S3 bucket and configuring corresponding properties
- Configuring Cross Region Replication

Disclaimer: This chapter is provided only as a guide. Work with your AWS administrator to ensure that your AWS configurations are set up based on the requirements of your organization.

8.2 Generating an IAM user and credentials from a root account by using the AWS console

The TS7700 Cloud Storage Tier can use Amazon S3 buckets by associating them with its own TS7700 cloud containers. However, first we must be authenticated to the Amazon S3 services as an Identity and Access Management (IAM) user. AWS IAM is a web service that helps you securely control access to AWS resources and services.

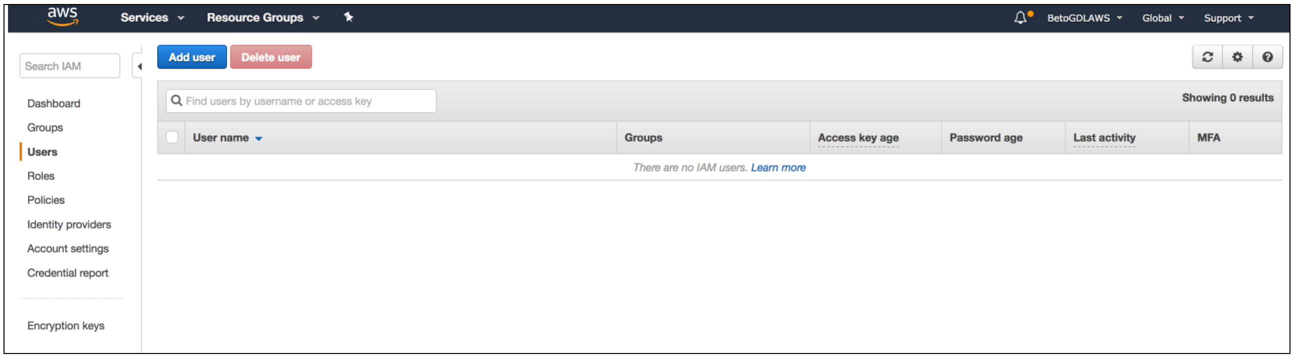
IAM is used to control who is authenticated (signed in) and authorized (has permissions) to use resources. When you first create an AWS account, you begin with a single sign-in identity that has complete access to all AWS services and resources in the account. This identity is called the AWS account root user and is accessed by signing in with the email address and password that was used to create the account in the AWS portal. For more information, see this website.

AWS strongly recommends to *not* use the root user for your everyday tasks, even the administrative tasks. Instead, adhere to the best practice of using the root user to create only your first IAM user. Then, securely lock away the root user credentials and use them to perform only a few account and service management tasks.

> **Note:** For more information about the IAM Console panels that are used to create users, see this web page.

Complete the following steps to create IAM users:

1. Sign in to the AWS Management Console and open the IAM console.
2. In the navigation pane, click **Users** and then, click **Add user** (as shown in Figure 8-1). For TS7700, a minimum of one IAM user available per grid is required. Depending on your management style of the account resources, you might want to set different users to segregate different workload types or locations.

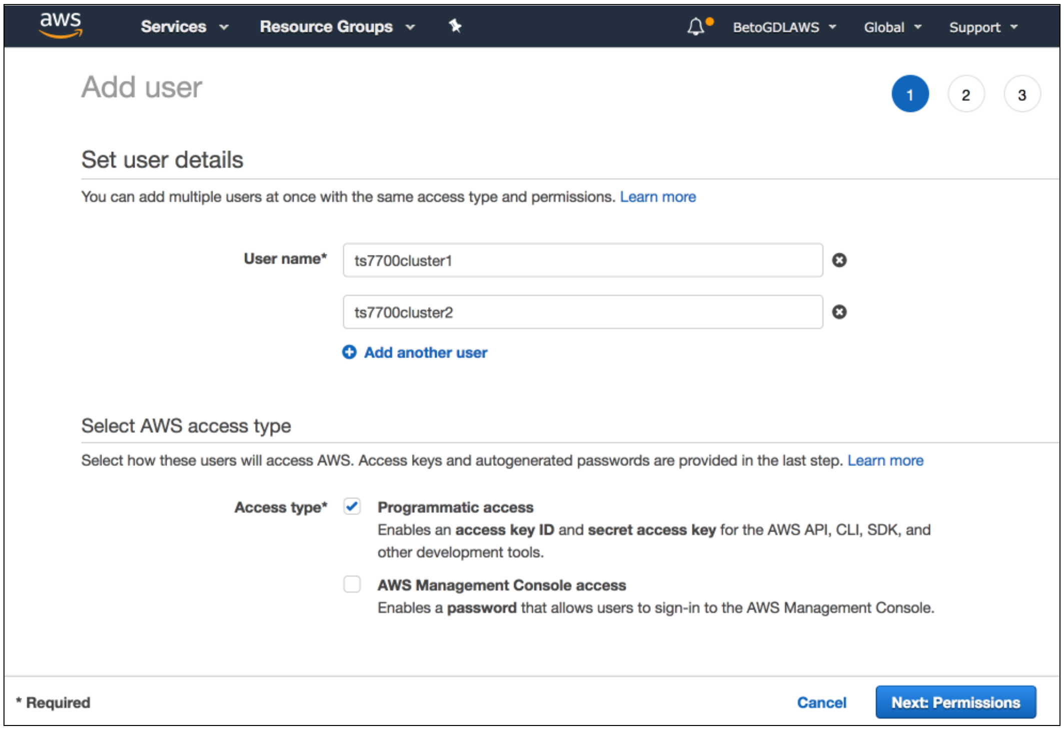


	User name	Groups	Access key age	Password age	Last activity	MFA

There are no IAM users. Learn more

Figure 8-1 AWS Management Console - IAM console Users panel

3. Enter a valid user name for the new user (see Figure 8-2). This sign-in name is for AWS. If you want to add other users, click **Add another user** for each user and enter their user names. You can add up to 10 users at a time.



Add user

Set user details

You can add multiple users at once with the same access type and permissions. Learn more

User name* ts7700cluster1

ts7700cluster2

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. Learn more

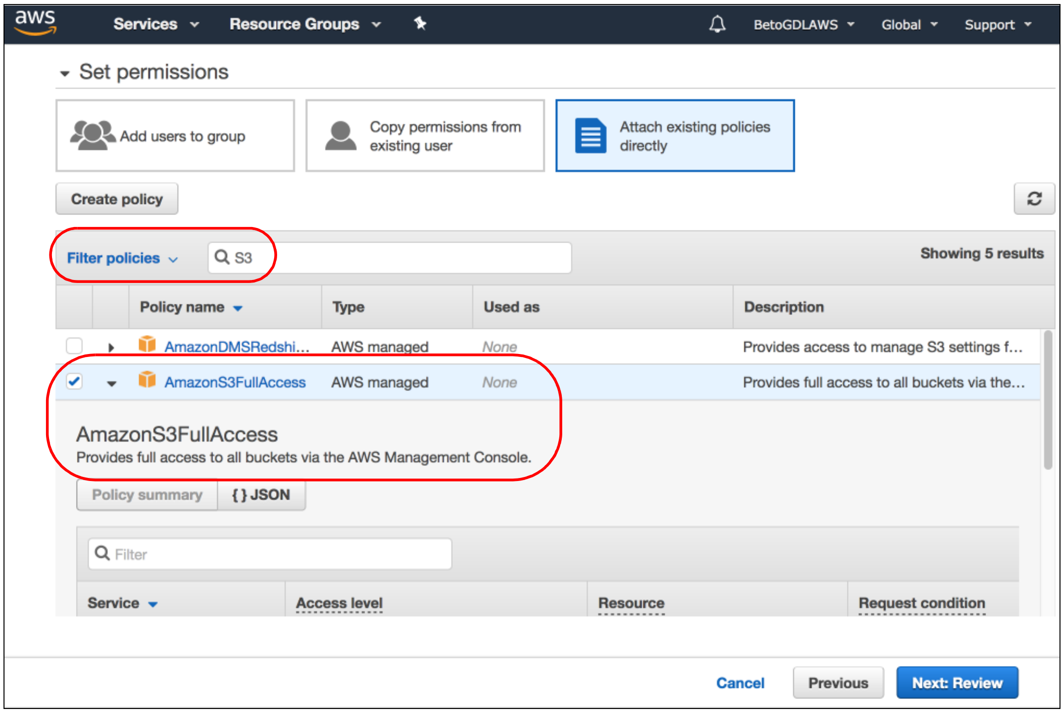
Access type* ☑ **Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

□ **AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

* Required

Figure 8-2 Adding new users under a root account

4. Select the **Programmatic access** option (as shown in Figure 8-2) as the type of access for this set of users. This selection enables the IAM authentication mode, which is required for TS7700 cloud account definitions. Then, click **Next: Permissions**.
5. On the Set permissions page (as shown in Figure 8-3) we show how to set permissions by attaching existing policies to users directly. The following permission options are available:
   - Add user to group
   - Copy permissions from existing user
   - Attach existing policies to user directly



Filter policies: S3 — Showing 5 results

		Policy name	Type	Used as	Description
□	▸	AmazonDMSRedshi...	AWS managed	None	Provides access to manage S3 settings f...
☑	▾	AmazonS3FullAccess	AWS managed	None	Provides full access to all buckets via the...

AmazonS3FullAccess

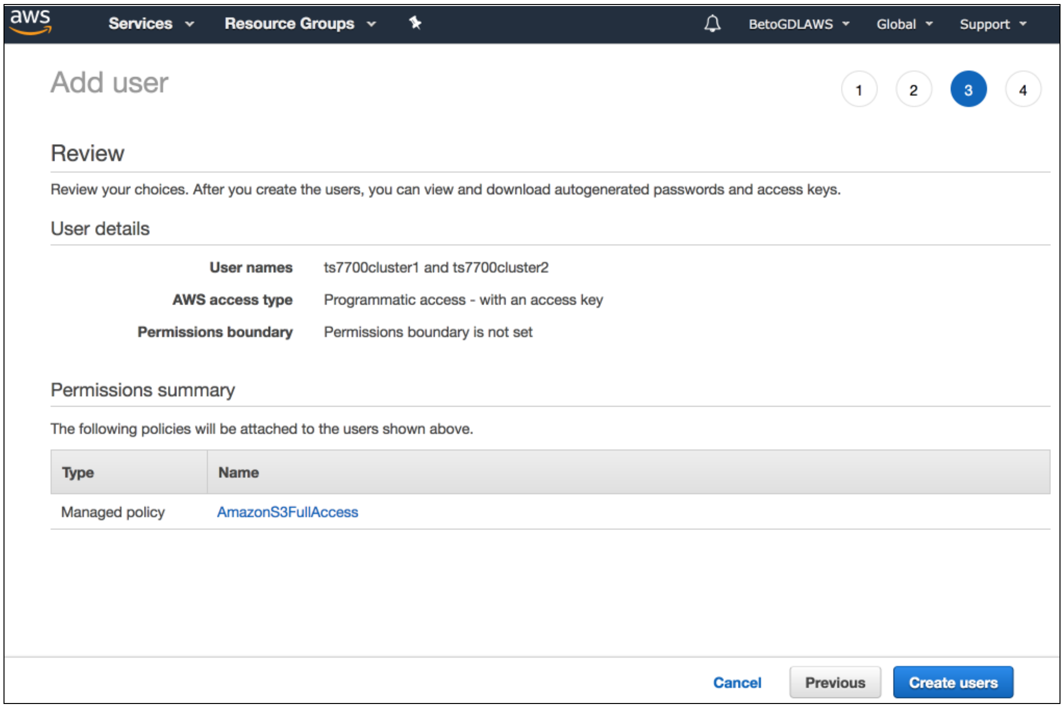
Provides full access to all buckets via the AWS Management Console.

Figure 8-3 Setting permissions for new IAM users

Whatever method is chosen to attach permissions to the new users, the TS7700 cloud accounts require full access to the S3 buckets that they use for storage of virtual volumes.

TS7700 must read, write, and delete objects in those buckets whenever needed. You can create your own fully customized permission policies by clicking **Create policies** (that is, you might want to limit access for specific IAM users to use only specific buckets, as described here).

6. Click **Next: Review** to see all of your selections, as shown in Figure 8-4. Click **Create users** when you are ready to proceed.



Add user

Review

Review your choices. After you create the users, you can view and download autogenerated passwords and access keys.

User details

User names	ts7700cluster1 and ts7700cluster2
AWS access type	Programmatic access - with an access key
Permissions boundary	Permissions boundary is not set

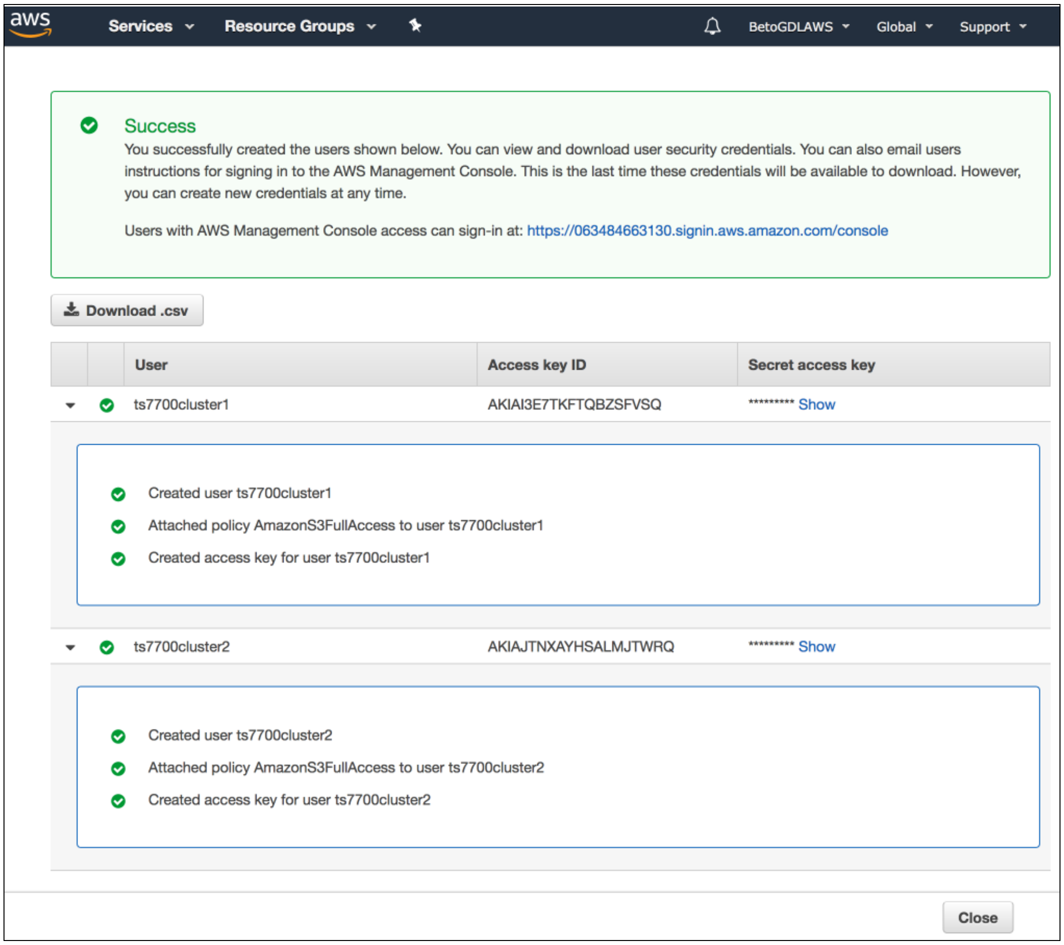
Permissions summary

The following policies will be attached to the users shown above.

Type	Name
Managed policy	AmazonS3FullAccess

Figure 8-4 Reviewing options for new users

7. After the users are created, a confirmation window opens. In this window, you can view the users' access keys (access key IDs and secret access keys) by clicking **Show** next to each access key that you want to see. Save the access keys by clicking **Download.csv** and then, save the file to a safe location, as shown in Figure 8-5.



Success

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: https://063484663130.signin.aws.amazon.com/console

User	Access key ID	Secret access key
ts7700cluster1	AKIAI3E7TKFTQBZSFVSQ	********* Show

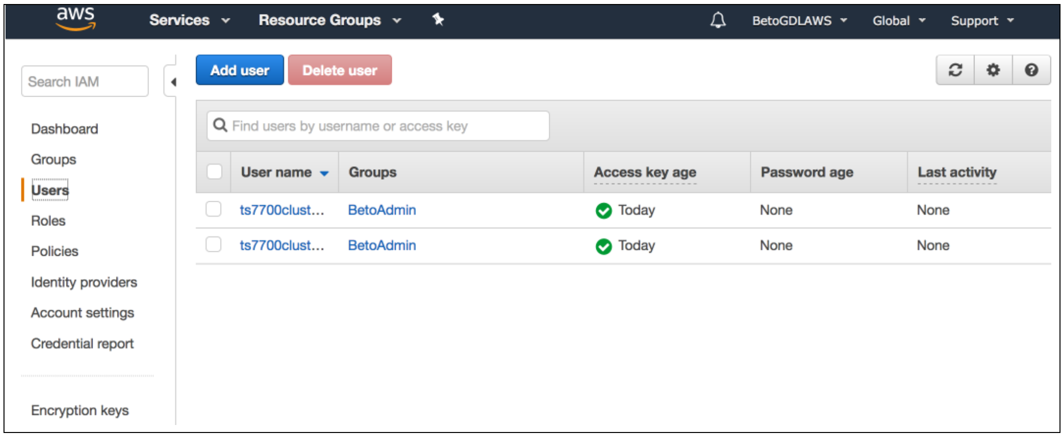
- Created user ts7700cluster1
- Attached policy AmazonS3FullAccess to user ts7700cluster1
- Created access key for user ts7700cluster1

User	Access key ID	Secret access key
ts7700cluster2	AKIAJTNXAYHSALMJTWRQ	********* Show

- Created user ts7700cluster2
- Attached policy AmazonS3FullAccess to user ts7700cluster2
- Created access key for user ts7700cluster2

Figure 8-5 Credentials for new IAM users

8. After clicking **Close** in the confirmation window, the Users panel is displayed, in which you confirm that your new users are now included in the list of registered users, as shown in Figure 8-6.



	User name	Groups	Access key age	Password age	Last activity
□	ts7700clust...	BetoAdmin	✓ Today	None	None
□	ts7700clust...	BetoAdmin	✓ Today	None	None

Figure 8-6 New users shown in the Users panel under the root account

8.3 Amazon S3 buckets

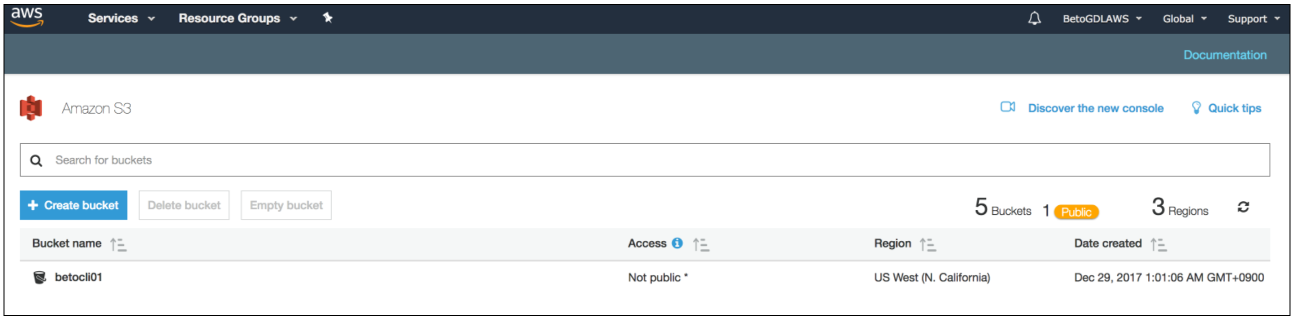
Before the TS7700 can upload data to Amazon S3 by way of the cloud storage tier, at least one bucket in an AWS Region must be created in advance to store the virtual volumes. Buckets feature configuration properties, including their geographical region, that can access the objects in the bucket, whether they replicate to another region bucket or other metadata properties.

Note: For more information about creating S3 buckets, see this web page.

8.3.1 Creating an S3 bucket

Complete the following steps to create an S3 bucket:

1. Sign in to the AWS Management Console. Open the Amazon S3 console and click **Create bucket**, as shown in Figure 8-7.



Bucket name	Access	Region	Date created
betocli01	Not public *	US West (N. California)	Dec 29, 2017 1:01:06 AM GMT+0900

Figure 8-7 Amazon S3 console

2. On the Name and region page, enter a name for your bucket and choose the AWS Region in which you want the bucket to be stored, as shown in Figure 8-8 on page 64. Complete the following fields on this page:

   – For Bucket name, enter a unique name for your new bucket. Use the following naming guidelines for compatibility with TS7700 container naming conventions:

     - The bucket name can be 3 - 63 characters long, and can contain only lowercase characters, numbers, and dashes.
     - Each label in the bucket name must start with a lowercase letter or number.
     - The bucket name cannot contain underscores or end with a dash.
     - The bucket name cannot be formatted as an IP address (for example, 198.51.100.24).
     - The name must be unique across all bucket names in Amazon S3 across all regions and all S3 users in the world.
     - The name must not contain uppercase characters or periods (“.”).
     - The name of the bucket cannot be changed after it is created.

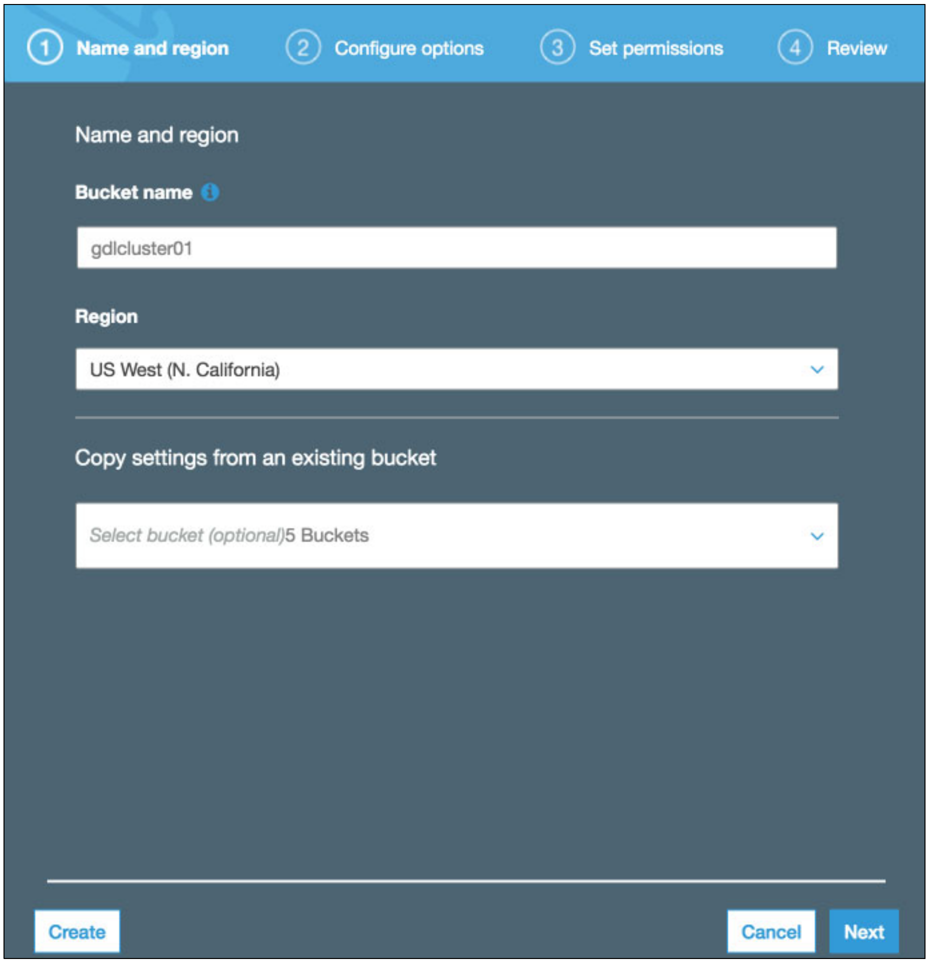
   – For Region, choose the AWS Region where you want the bucket to be stored. Select a Region close to the associated TS7700 to minimize latency and costs, or to address regulatory requirements.

     Objects that are stored in a Region never leave that Region unless you specifically transfer them to another Region manually or through cross region replication. In addition, the Amazon S3 bucket must be created in an AWS Region that is supported by the TS7700 (see Table 8-1 on page 63).

Table 8-1 AWS regions supported by TS7700

Region Name	Region
US West (N. California)	us-west-1
US West (Oregon)	us-west-2
Asia Pacific (Mumbai)	ap-south-1
Asia Pacific (Seoul)	ap-northeast-2
Asia Pacific (Singapore)	ap-southeast-1
Asia Pacific (Sydney)	ap-southeast-2
Asia Pacific (Tokyo)	ap-northeast-1
EU (Frankfurt)	eu-central-1
EU (Ireland)	eu-west-1
South America (São Paulo)	sa-east-1

– (Optional) You can copy the attributes of an existing bucket when a bucket is created. This method can be helpful when multiple buckets must be created. To copy the attributes of an existing bucket when a bucket is created, choose **Copy settings from an existing bucket** and then, choose the bucket whose settings you want to copy and click **Create**. The bucket properties versioning, tags, and logging are copied.



Name and region

Bucket name: gdlcluster01

Region: US West (N. California)

Copy settings from an existing bucket

Select bucket (optional)5 Buckets

Figure 8-8 Creating an S3 bucket: Adding name and selecting AWS region

3. If you did not copy settings from another bucket, click **Next** to show the Properties options page (as shown in Figure 8-9 on page 65) to configure the following fields (which can be modified after the bucket is created):

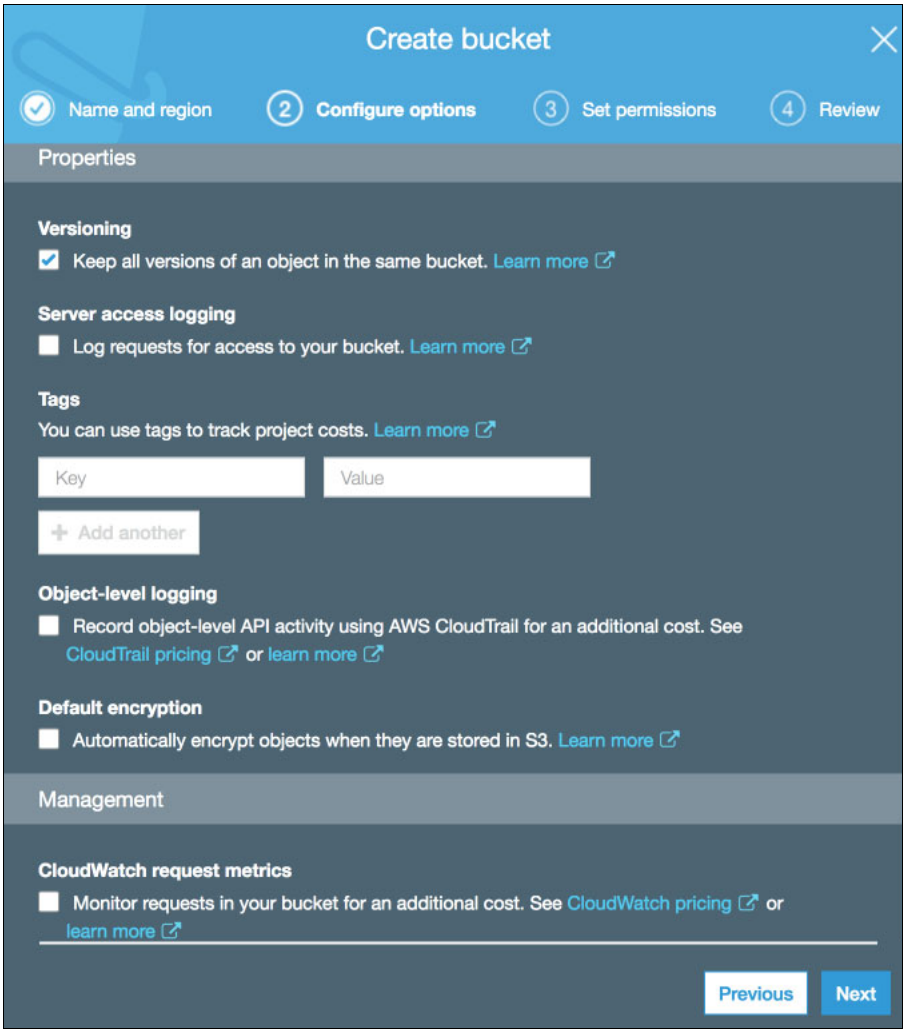
   – Versioning: If you want to enable object versioning for the bucket Select the **Keep all versions of an object in the same bucket.** If you are using cross regional replication, versions must be enabled. Otherwise, versions are optional assuming you understand the following limitation.

     - The TS7700 at 4.2 does not have a method to delete older versions retained within the AWS S3 object store. Therefore, a life cycle policy should be created by your AWS Admin to automatically delete older versions after some time period has passed.

   – Server access logging: Select **Log requests for access to your bucket** to enable server access logging on the bucket, which enables the logging of detailed records for the requests that are made to your bucket. This option is not specific to TS7700 operations and is configured based on needs of the user.

   – Tags: You can use cost allocation bucket tags to annotate billing for your use of a bucket. Each tag is a key-value pair that represents a label that you assign to a bucket. To add a tag, enter a Key and a Value. Choose **Add another** to add another tag. This option is not specific to TS7700 operations and is configured based on needs of the user.

- Object-level logging: Select this option if you want to record object-level API activity by using AWS CloudTrail for an extra cost. This option is not specific to TS7700 operations and should be configured based on needs of the user.
- Default encryption: AWS allows you to enable default encryption for a bucket so that all objects are encrypted when they are stored within it. However, the TS7700 has not yet implemented functions to manage client provided keys for the encryption process against S3. Therefore, enable default encryption only when encryption is required by your organization. Keep in mind that data in flight between the TS7700 and AWS S3 is always encrypted through the TLS HTTPS connection. Enabling encryption here ensures that data at rest within AWS S3 is encrypted as well.
- CloudWatch request metrics: Select this option if you want to monitor requests in your bucket (extra costs might apply). This option is not specific to TS7700 operations and is configured based on the needs of the user.



Create bucket

Name and region | 2 Configure options | 3 Set permissions | 4 Review

Properties

Versioning

☑ Keep all versions of an object in the same bucket. Learn more

Server access logging

□ Log requests for access to your bucket. Learn more

Tags

You can use tags to track project costs. Learn more

Key | Value

Object-level logging

□ Record object-level API activity using AWS CloudTrail for an additional cost. See CloudTrail pricing or learn more

Default encryption

□ Automatically encrypt objects when they are stored in S3. Learn more

Management

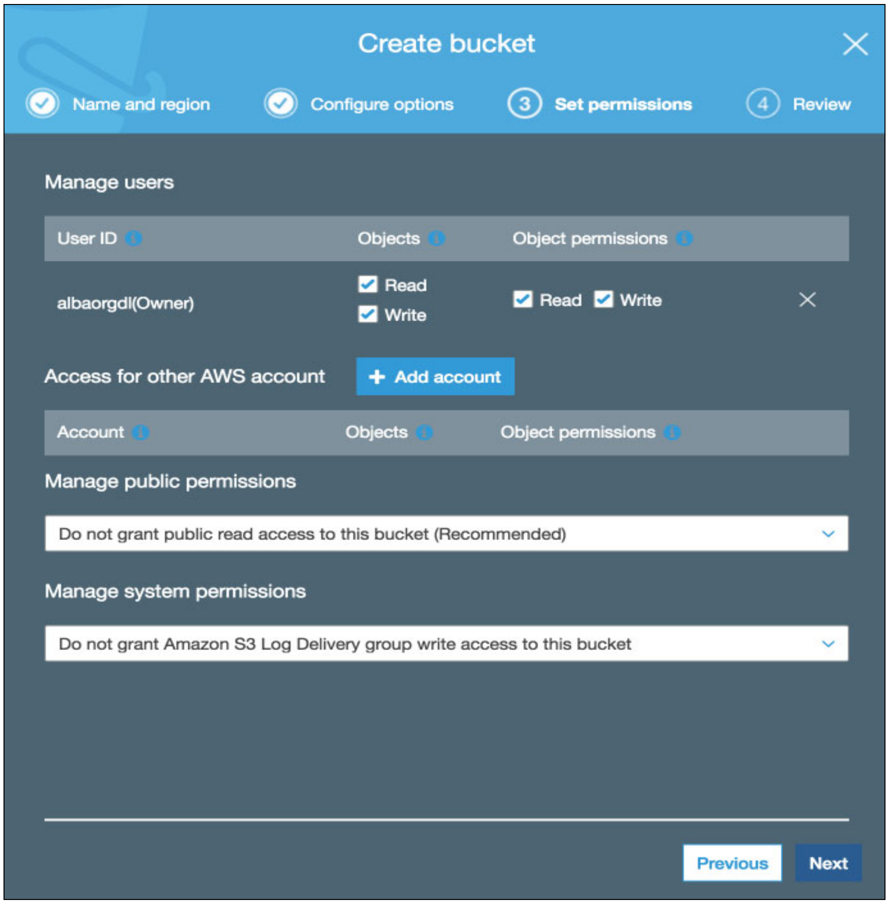
CloudWatch request metrics

□ Monitor requests in your bucket for an additional cost. See CloudWatch pricing or learn more

Figure 8-9 Setting bucket properties

4. Click **Next** to show the Set permissions page (as shown in Figure 8-10 on page 66) to manage the permissions that are set on the bucket that you are creating. The owning root account always includes full access permissions to created buckets, but it is a best practice to create IAM user accounts and provide access for a particular bucket to specific IAM users, (as described in “Generating an IAM user and credentials from a root account by using the AWS console” on page 56). For example, you might create an IAM user for

each TS7700 grid, region, or cluster. This feature enables you to be more flexible about which TS7700s can access which buckets and easily provide a method to change access rules for one or more TS7700s.



Manage users

User ID	Objects	Object permissions
albaorgdl(Owner)	☑ Read ☑ Write	☑ Read ☑ Write

Access for other AWS account

Account	Objects	Object permissions

Manage public permissions

Do not grant public read access to this bucket (Recommended)

Manage system permissions

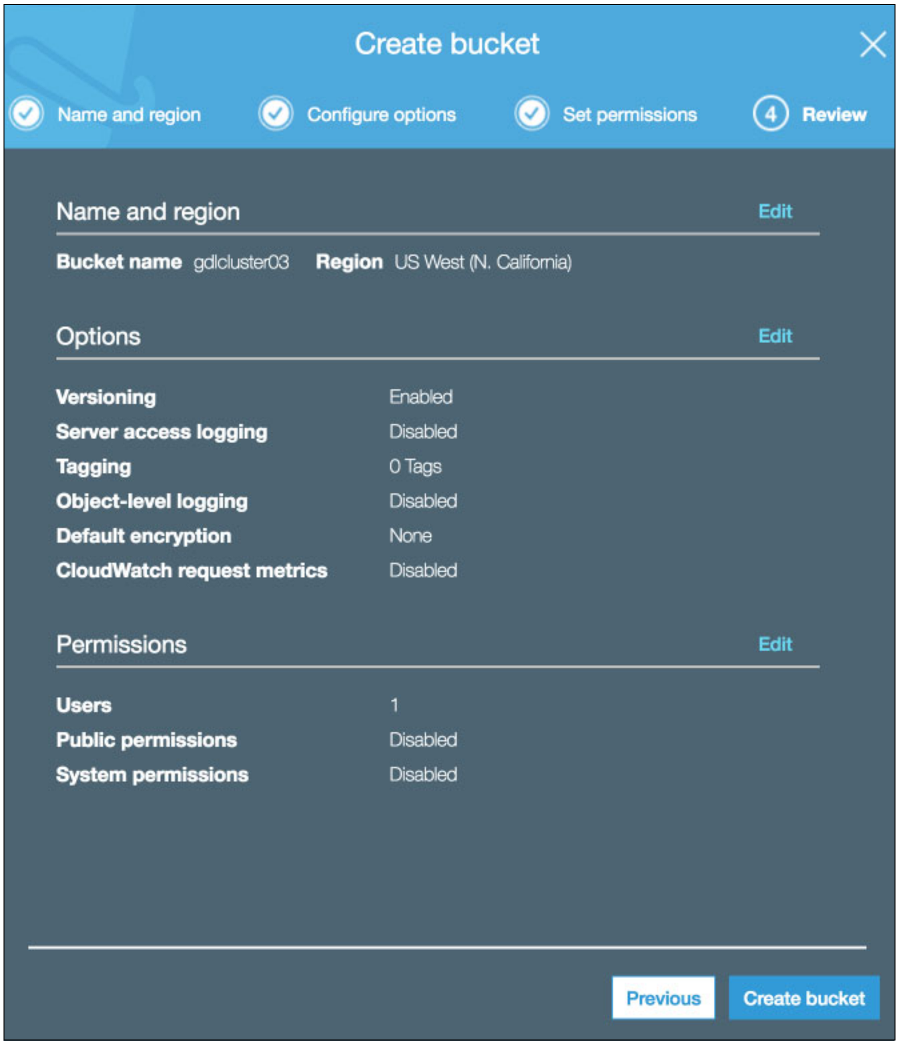
Do not grant Amazon S3 Log Delivery group write access to this bucket

Figure 8-10 Setting permissions for buckets

Click **Add account** to grant access to other AWS accounts (that is, if you want to have multiple TS7700 accounts belonging to different parent root accounts that share buckets), which must be identified by *canonical ID*. Canonical ID is a long string that is implemented by AWS primarily to be used for programmatic cross-account accesses (you can obtain the canonical ID of a root account by performing the procedures that are described at this web page.

> **Warning:** Do *not* grant public read access to the bucket that you are creating. Granting public read access permissions means that *anyone* can access the objects that are in the bucket.

5. When you are done configuring permissions on the bucket, click **Next** to show the Review page (as shown in Figure 8-11) so you can verify the configured settings. If you want to change something, click **Previous** to return and change the wanted settings. If the current settings are correct, click **Create bucket**.



Name and region

Bucket name gdlcluster03 **Region** US West (N. California)

Options

Versioning	Enabled
Server access logging	Disabled
Tagging	0 Tags
Object-level logging	Disabled
Default encryption	None
CloudWatch request metrics	Disabled

Permissions

Users	1
Public permissions	Disabled
System permissions	Disabled

Figure 8-11 Review configured bucket setting

8.4 Cross-region replication

Amazon S3 offers Cross-region replication (CRR) as another service to enable the automatic asynchronous copying of objects across buckets in different AWS Regions. Buckets that are configured for cross-region replication can be owned by the same AWS account or by different accounts.

Cross-region replication is enabled at bucket-level granularity, which means that you must apply the replication rule to the source and target bucket. In a bidirectional configuration, each bucket within each region acts as a source and a destination. For a minimum configuration, you are required to have the following information:

- The destination bucket, where you want Amazon S3 to replicate objects.
- An AWS IAM role that Amazon S3 can assume to replicate objects on your behalf.

Note: For more information about adding a Cross-Region Replication (CCR) rule to an S3 bucket, see this web page.

8.4.1 Requirements for CRR

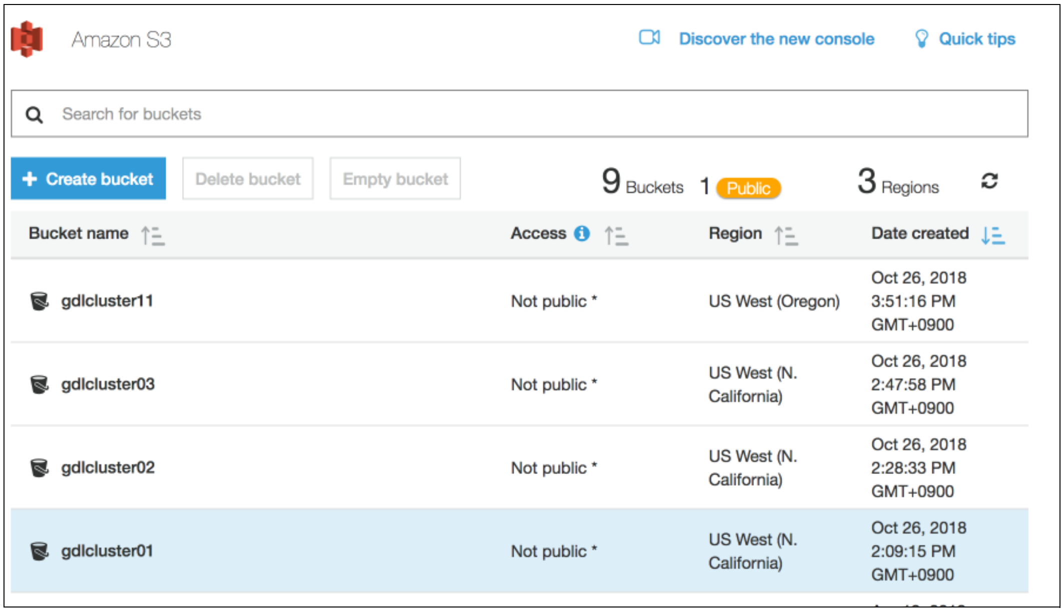
CRR includes the following requirements:

- Source and destination buckets include versioning that is enabled.
- The source and destination buckets are in different AWS Regions. Because the TS7700 does not support the ability to clean up previously deleted or overwritten versions of objects, a lifecycle policy must be configured on source and destination buckets within AWS to automatically cleanup older versions.
- Amazon S3 include permissions to replicate objects from the source bucket to the destination bucket on your behalf.
- If the owner of the source bucket does not own the objects in the bucket, the object owner grants the bucket owner READ and READ_ACP permissions with the object ACL.
- Any preexisting content within a bucket is not automatically replicated after CRR is enabled. Only objects that are created from that point forward are replicated.

8.4.2 Setting up S3 buckets for CRR

Complete the following steps:

1. Sign in to the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3. Click the entry that corresponds to the target "source" bucket (as shown in Figure 8-12) to open its bucket panel.



Bucket name	Access	Region	Date created
gdlcluster11	Not public *	US West (Oregon)	Oct 26, 2018 3:51:16 PM GMT+0900
gdlcluster03	Not public *	US West (N. California)	Oct 26, 2018 2:47:58 PM GMT+0900
gdlcluster02	Not public *	US West (N. California)	Oct 26, 2018 2:28:33 PM GMT+0900
gdlcluster01	Not public *	US West (N. California)	Oct 26, 2018 2:09:15 PM GMT+0900

Figure 8-12 Selecting target source bucket for CRR

2. In the bucket panel, open the Management section. Click **Replication** to open the corresponding panel (see Figure 8-13).

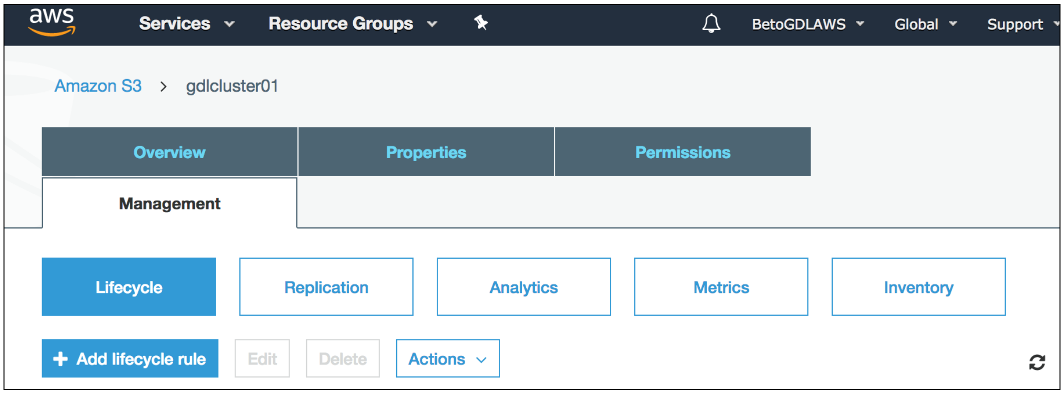


Figure 8-13 Selecting the Replication configuration page

3. In the Replication panel, click **Add rule** (see Figure 8-14).

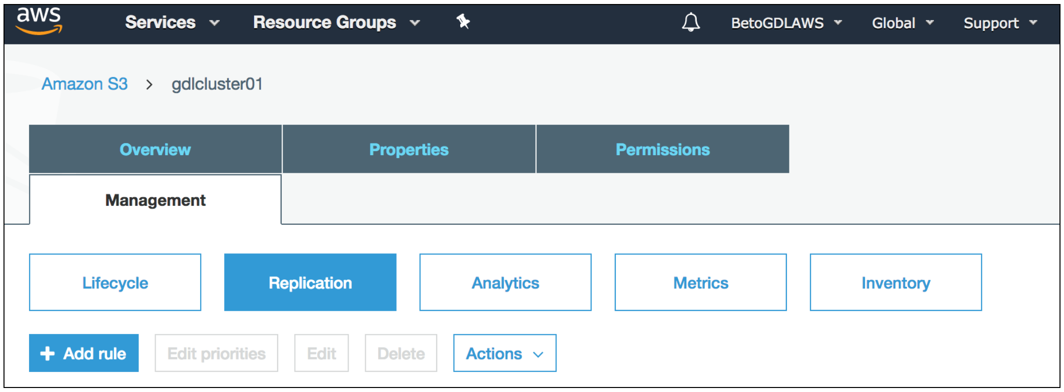
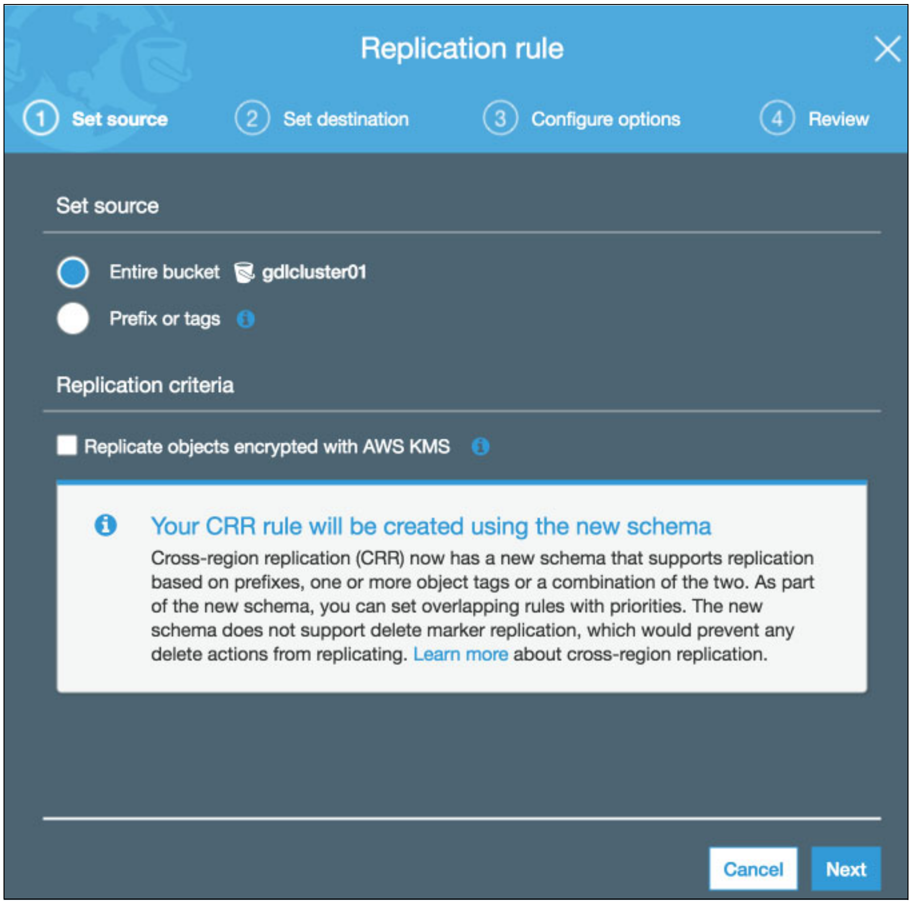


Figure 8-14 Adding CRR rule

Amazon S3 allows different settings for different use cases; however, for the TS7700 cloud Object Storage tier, you must select the **Entire bucket** option, as shown in Figure 8-15. Do *not* select the **Replicate objects encrypted with AWS KMS** option (TS7700 support for this option will be supported in a future release).



Set source

● Entire bucket gdlcluster01

○ Prefix or tags

Replication criteria

□ Replicate objects encrypted with AWS KMS

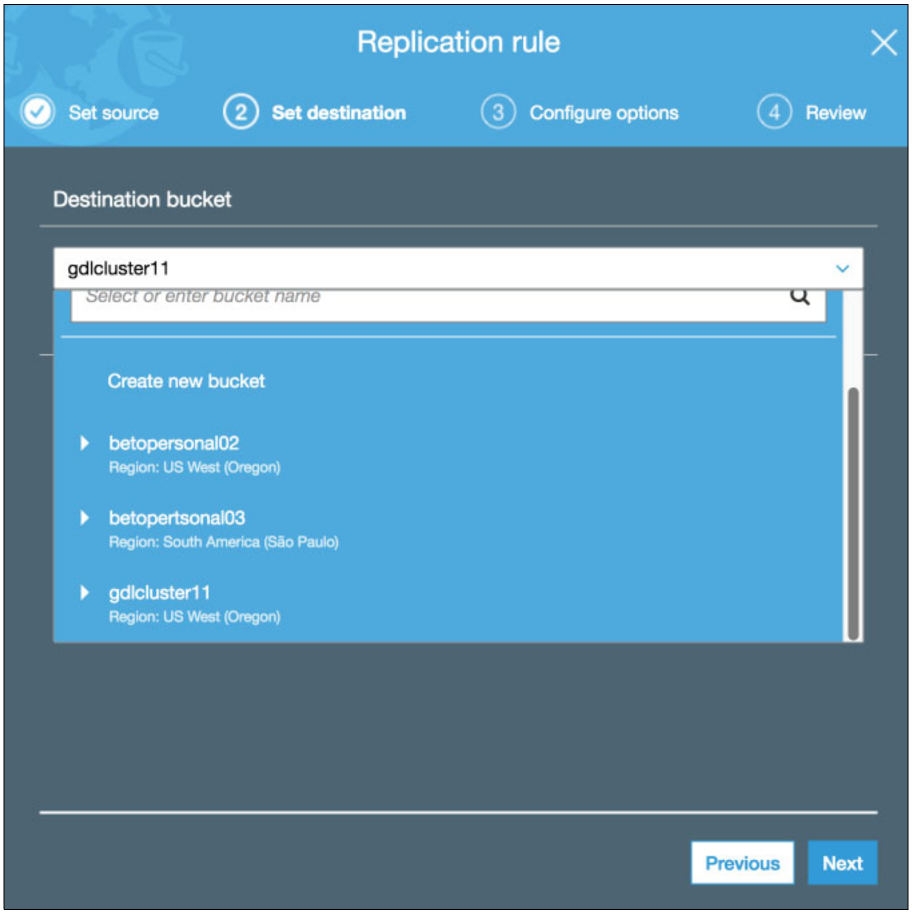
Your CRR rule will be created using the new schema

Cross-region replication (CRR) now has a new schema that supports replication based on prefixes, one or more object tags or a combination of the two. As part of the new schema, you can set overlapping rules with priorities. The new schema does not support delete marker replication, which would prevent any delete actions from replicating. Learn more about cross-region replication.

Figure 8-15 Creating a replication rule for CRR

4. Select the Destination bucket, as shown in Figure 8-16. Here, you must select a bucket that is in a region that is different from the Source bucket region. You select the Change object ownership to destination bucket owner option only if the candidate destination bucket corresponds to a different AWS account.

> **Note:** You can select a bucket that belongs to the local AWS root account, or to a different AWS account, in which case you must supply the corresponding AWS account ID (12 characters, which can be obtained by following the steps at this web page) and the name of the candidate destination bucket.



Replication rule

Set source · 2 Set destination · 3 Configure options · 4 Review

Destination bucket

gdlcluster11

Select or enter bucket name

Create new bucket

betopersonal02
Region: US West (Oregon)

betopertsonal03
Region: South America (São Paulo)

gdlcluster11
Region: US West (Oregon)

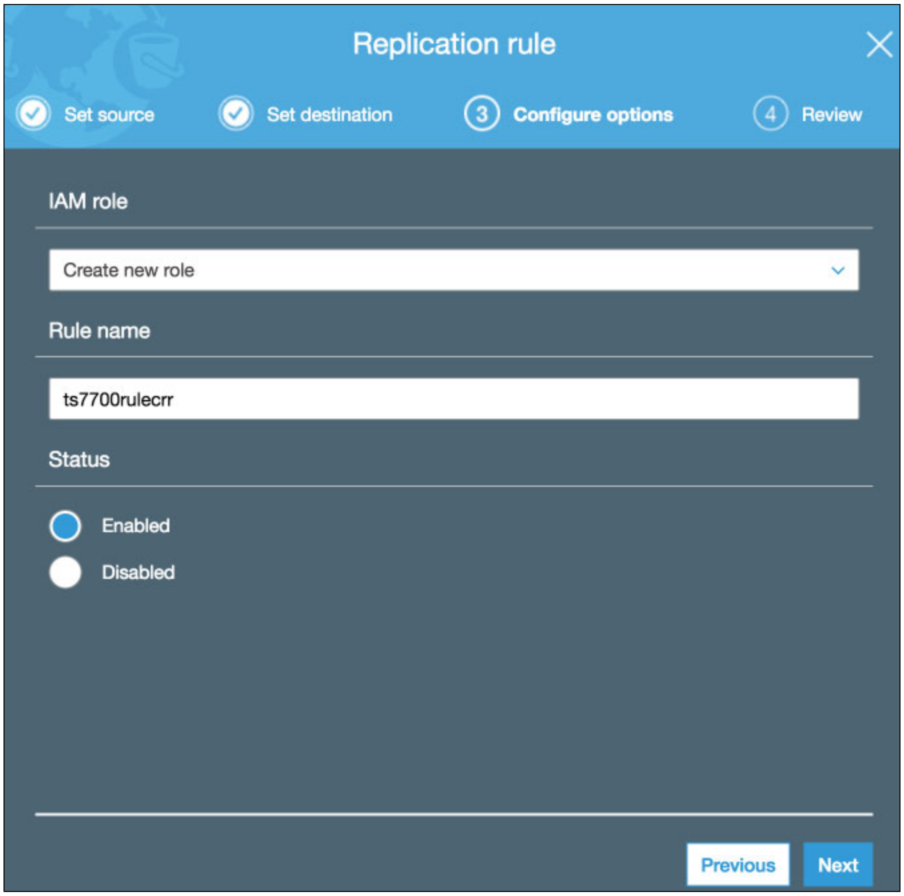
Figure 8-16 Selecting a "Destination" bucket

5. Click **Next** to proceed to set up an AWS Identity and Access Management (IAM) role that Amazon S3 can assume to perform cross-region replication of objects on your behalf. The following options are available, as shown in Figure 8-17:

   – It is highly recommended that you choose **Create new role** to have Amazon S3 create an IAM role for you. When you save the rule, a new policy is generated for the IAM role that matches the source and destination buckets that you choose. The name of the generated role is based on the bucket names and uses the following naming convention:

     ```
     replication_role_for_source-bucket_to_destination-bucket
     ```

   – You can choose to use an existing IAM role. If you do, you must choose a role that grants Amazon S3 the necessary permissions for replication. Replication fails if this role does not grant Amazon S3 sufficient permissions to follow your replication rule.



IAM role: Create new role

Rule name: ts7700rulecrr

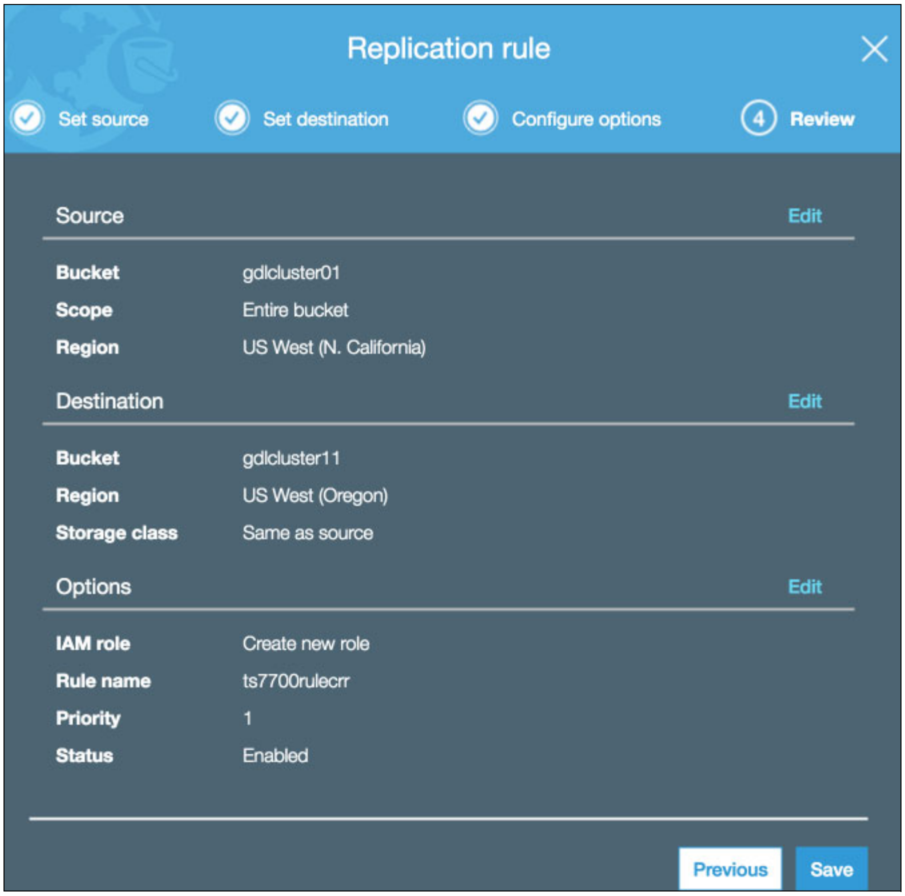
Status:

● Enabled

○ Disabled

Figure 8-17 Determining IAM role and rule name

6. Click **Next** to display the configured options for your review, as shown in Figure 8-18. If the options are configured correctly, click **Save** to complete the process (click **Previous** to make any changes).



Source

Bucket	gdlcluster01
Scope	Entire bucket
Region	US West (N. California)

Destination

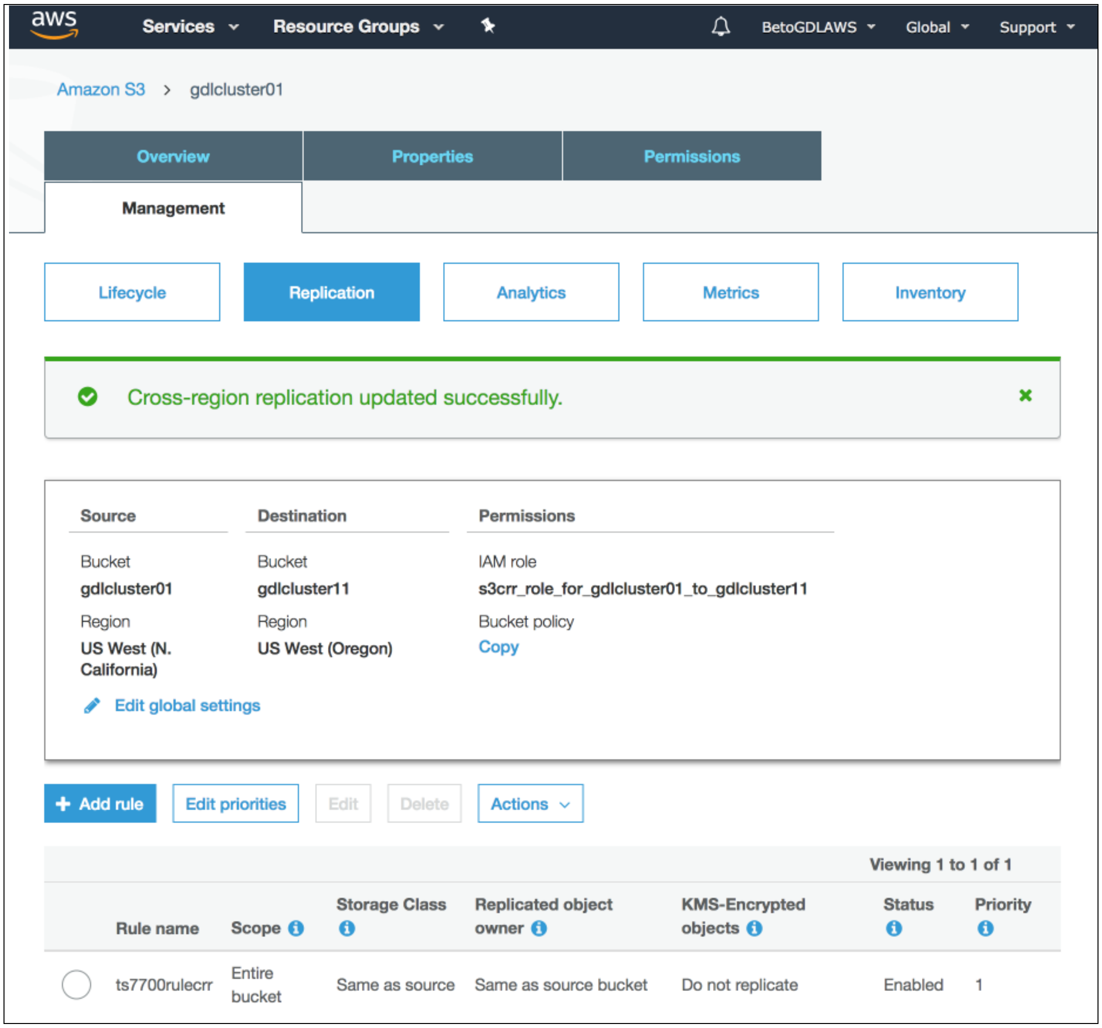
Bucket	gdlcluster11
Region	US West (Oregon)
Storage class	Same as source

Options

IAM role	Create new role
Rule name	ts7700rulecrr
Priority	1
Status	Enabled

Figure 8-18 Reviewing CRR rule

Your new rule should be listed in the source bucket panel, as shown in Figure 8-19.



Cross-region replication updated successfully.

Source	Destination	Permissions
Bucket	Bucket	IAM role
gdlcluster01	gdlcluster11	s3crr_role_for_gdlcluster01_to_gdlcluster11
Region	Region	Bucket policy
US West (N. California)	US West (Oregon)	Copy

Viewing 1 to 1 of 1

	Rule name	Scope	Storage Class	Replicated object owner	KMS-Encrypted objects	Status	Priority
○	ts7700rulecrr	Entire bucket	Same as source	Same as source bucket	Do not replicate	Enabled	1

Figure 8-19 Available replication rules

8.5 Setting up TS7700Cs with Amazon S3 Cross Region Replication

If your cloud Object Storage is Amazon S3 and you have two clusters in different locations in the same Grid, you might want to set up Amazon Cross Region Replication for faster access to the cloud and multi-region-level redundancy.

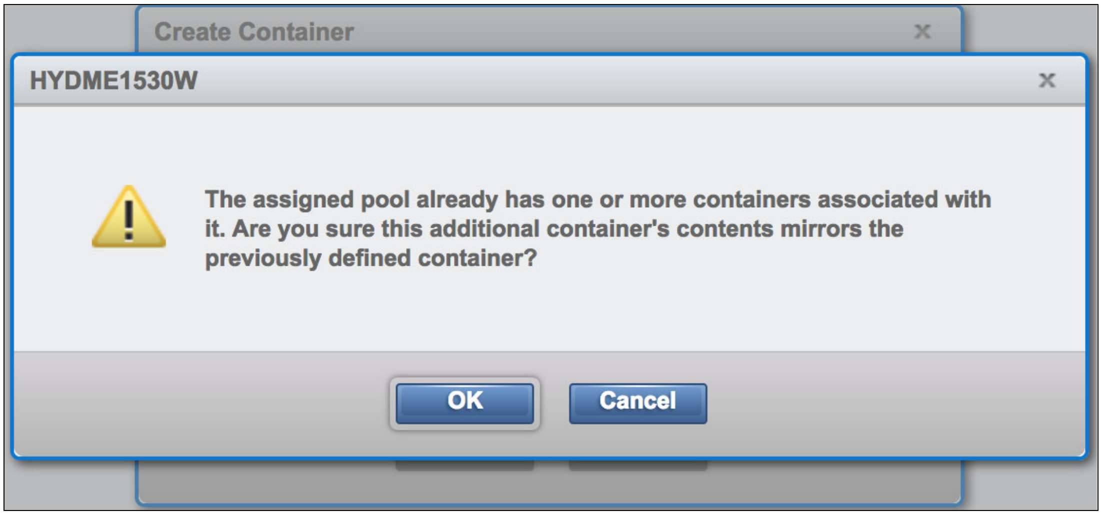
> **Note:** Each region can share an AWS IAM account or they can use unique AWS IAM accounts, depending on how the buckets and the cross region replication were configured.

When setting up Cross Region Replication, consider selecting the nearest regions to the TS7700C clusters that communicate most often with the AWS S3 bucket. For example, if a four-way configuration exists with two clusters nearest to AWS Region A and two DR clusters nearest to AWS Region B, a bucket in AWS Region A and in AWS Region B should be configured and setup for cross region replication bi-directionally.

> **Note:** As of release 4.2, the TS7700 supports only AWS regions, as listed in Table 8-1 on page 63.

After the pair of S3 buckets that are linked by CRR are created, two TS7700 cloud containers must be created on TS7700C to connect to them (one container for each region). To create containers in the TS7700, follow the steps that are described in “Cloud tier settings” on page 80.

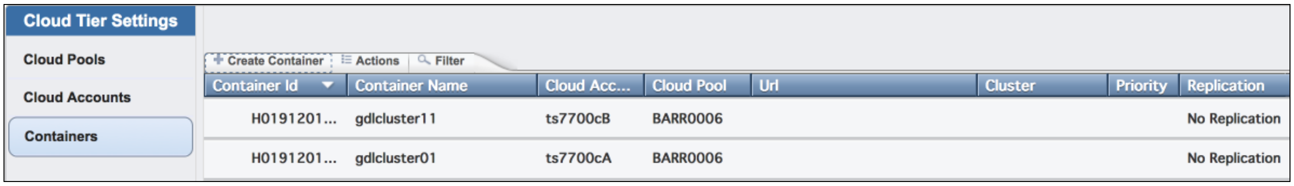
When the second container is created on TS7700, the warning message that is shown in Figure 8-20 is displayed. Because your two buckets are mirrored with AWS Cross-region replication, you can click **OK** to proceed.



The assigned pool already has one or more containers associated with it. Are you sure this additional container's contents mirrors the previously defined container?

Figure 8-20 Warning message on container creation

After the containers are created on the TS7700, two containers are listed in the Container MI panel, as shown in Figure 8-21.



Container Id	Container Name	Cloud Acc...	Cloud Pool	Url	Cluster	Priority	Replication
H0191201...	gdlcluster11	ts7700cB	BARR0006				No Replication
H0191201...	gdlcluster01	ts7700cA	BARR0006				No Replication

Figure 8-21 Containers for a pair of Amazon S3 buckets (CRR)

> **Note:** When you create containers for a pair of Amazon S3 buckets on TS7700, you might see “No Replication” in the Replication column that is in the Container panel. This message is a TS7700 reporting error and will be fixed in a future release.

Next, a Cloud URL must be created for each container. To create a Cloud URL, follow the steps that are described in “Cloud tier settings” on page 80.

After a Cloud URL is created for each container, open the Container panel on the Management Interface of the cluster you want to use the Cloud URL. Right-click the Cloud URL you want to assign to that cluster and select **Create Cloud URL and Cluster association**. Using the four way grid configuration example, you associate two clusters with one region container and the other two containers with the other region container.

You are now ready to start sending data to the TS7700 Cloud Storage Tier and both regions include access to the mirrored buckets and all content within them.

For more information about how to use corresponding data management policies, see “Directing virtual volumes to the cloud storage tier” on page 88.

9

Configuring TS7700 for cloud storage tier

In this chapter, we describe how to configure TS7700 for cloud storage tier.

The following topics are included:

9.1 Prerequisites

The TS7700 requires the following tasks be completed before the cloud storage tier feature can be used:

1. Install the following required Feature Codes (FCs):
   - FC 3466: 32 Gb Memory Upgrade (64 Gb total TS7760 memory)
   - FC 4278: Cloud Enablement
   - FC 4275: 1 TB Active Premigration Queue (1 to 10 instances)
   - FC 5279: 5 TB Active Premigration Queue (0 to 10 instances)

   Note: FC 3466 and FC 4278 are non-concurrent if not previously activated.

2. If an existing TS7760 is used, perform the non-concurrent cloud storage tier Miscellaneous Equipment Specification (MES), which is used to identify procedures that are intended to modify capabilities of the product for machines that are in the field, which can be an addition, improvement, removal, or any combination of these options.
3. Previously configure your object store, vaults, credentials, and certificates as described in chapters 5 through 8.
4. Configure Cloud Tier Settings by using the TS7700 Management Interface, which requires setting up the following groups of settings:
   - Cloud pool: Assign a name for the group of virtual volumes in the TS7700 that is intended to be stored in the cloud pool.
   - Cloud account: Information about the target cloud object store to be used (type and authentication credentials).
   - Cloud container, which includes the following components:
     1. One or more TS7700 cloud containers with names matching the correct location name (vault or bucket) in the selected cloud object store (IBM Cloud Object Storage or Amazon S3) where virtual volumes belonging to the cloud pool can reside.
     2. Define one or more URLs and assigned certificates for a given cloud container.
     3. Associate a TS7700 cluster to one or more cloud URLs so that a cluster is aware of which URLs to utilize to access a given container.
5. Setup and assign one or more TS7700 DFSMS constructs so that logical volumes can use the new cloud storage tier. Consider the following points:
   - Storage class must be defined to have logical volumes intended for object store offload to target a CPx partition and not CP0.
   - Storage groups must be configured on *all* clusters in the grid to have newly created volumes target a particular cloud pool rank.

9.1.1 Restrictions

Consider the following restrictions:

- At the Release 4.2 code level, the TS7700 supports only connecting to the following cloud object store services by using the Simple Storage Service (S3) protocol:
  - IBM Cloud Object Storage as an on-premise private facility with a fixed IP addressable endpoint on port 80 or 442 (for example, https:\\192.168.0.120).

  - Amazon S3, which is the storage service that is provided by the Amazon Web Services Cloud Platform. It is addressable by way of a public domain name (for example, http://bucket.s3.amazonaws.com)
- Enabling a TS7700 for cloud storage tier is supported for only TS7760s that are running code level Release 4.2 or higher.
- A single TS7760 can be a TS7760C or TS7760T. Tape attach and cloud storage tier are currently mutually exclusive in the same cluster in the 4.2 release. TS7760C, TS7760T, and other TS7700 models can coexist in the same grid.
- A TS7760C can be a stand alone cluster or in a grid with any TS7700 model type that is supported by the 4.2 release. This means model types including Power7 based TS7740, TS7720, and TS7720T, Power8 based TS7760, and TS7760T.

9.2 Feature codes for cloud storage tier

The following FCs are required for implementing the TS7700 cloud storage tier:

- FC 3466 (32 GB memory upgrade): Installs 32 GB of memory to reach a total of 64 GB of physical RAM memory in the TS7700 server.
- FC 5278 (Cloud Enablement): Enables the TS7760 to store and retrieve objects from cloud-based storage.
- FC 5274 (enable 1 TB Active Premigration Queue): Allows the process of copying data from the main cache storage subsystem to the tape or cloud storage tier, which is known as *premigration*. This FC controls the amount of data that is allowed into the premigration queue before the TS7700 starts slowing down workloads that are coming from the inbound host processing or copies (which is known as *throttling*). A minimum of 1 FC instance is required.

The following optional FCs are available:

- FC 5274: Enables 1 TB Active Premigration Queue (another FC beyond the first FC is optional up to a maximum of 10 features).
- FC 5279: Enables 5 TB Active Premigration Queue (maximum of 10 features). Before installing any instance of this FC, the maximum 10 FC 5472 features must be installed. If all 10 5279 features are also installed, the premigration queue becomes unbound.

Installing cloud storage tier FCs are available for machines that are in the field. The following FCs are available:

- FC 5278: Cloud enablement. Installing the FC is a concurrent procedure, but must later be activated as part of an MES procedure, which is nonconcurrent. The license is entered by using the License New Feature License action on the Feature Licenses page, which is included in the Settings panel of the TS7700 Management Interface. More steps, which are documented in “Cloud tier settings” on page 80, are needed afterwards to complete the cloud-attachment configuration.
- FC 5274/5279: Enable 1/5TB Active Premigration Queue. This concurrent procedure installs the corresponding Key License by using the TS7700 Management Interface.
- FC 3466: Adding 32 GB physical RAM memory to the TS7700 server. This procedure is non-concurrent, a maintenance window is necessary that requires the intervention of IBM service qualified personnel. Host transactions are not possible while the installation occurs. It is best to schedule the installation of more memory at the same time as the FC 5278 MES Enablement procedure, which is also nonconcurrent.

Cloud storage tier MES

After the required Feature Codes are installed, the cloud storage tier nonconcurrent MES can be performed, which requires IBM service qualified personnel to perform. The MES procedure is not documented in this Redpaper, but the following considerations apply:

- The Cloud storage tier feature uses the Grid network ports (slot C1 of Primary and Alternate I/O drawers). If the TS7760C is a stand-alone cluster, grid ports must be connected to the network. Therefore, they require assigned IP addresses as though they were members of a grid. Each physical port (up to four) must have an assigned fix IP address.
- The selected cloud storage tier repository must be reachable (roundtable) from the grid connections. Therefore, your local network team likely must be involved in advance.
- The time on the TS7700 and the selected cloud storage repository (be it IBM Cloud Object Storage or Amazon S3) must be synchronized. If the time difference between them is greater than 10 minutes, different types of failures can affect daily operations. For this reason, it is recommended to use a Network Time Protocol (NTP) service to ensure proper system synchronization is in place. The TS7700 must have the address of the selected NTP server configured.This address is reachable by using the network segment that is assigned to the TS7700 Management Interface. If IBM Cloud Object Storage is used, it is recommended that it also use an NTP server to stay synchronized relative to the UTC-based time of the TS7700's.
- If the Amazon S3 is selected for use with cloud storage tier, a DNS server must be set up by using the TS7700 Management Interface in the Cluster Network Settings page under the Cluster Settings panel. The DNS server that is on the Management Interface network must also translate *amazonaws.com nameserver-based addresses. Without a properly setup DNS server, the TS7700 cannot communicate with *amazonaws.com-based object stores.
- If HTTPS is used to communicate with IBM Cloud Object Storage, a certificate must be configured. For more information, see Chapter 6, "SSL certificate" on page 29.
- After the MES completes and the cluster is put online, disk partitioning is enabled and a single CP1 partition of 3 TB is created. If any data is in the cluster, it is located within the CP0 resident only partition. For more information about how to manage data after the MES is complete, see Chapter 13, "Migration and upgrade considerations" on page 125.
- After the MES completes and is put online, data that is within an object store that is connected to the same grid is not immediately accessible by the newly MES based TS7760. For more information about how to manage data after the MES is complete, see Chapter 13, "Migration and upgrade considerations" on page 125.

Cloud tier settings

After the cloud storage tier feature is enabled, the TS7700 Management Interface (see Figure 9-1 on page 81) provides a new Cloud Settings option after it is online. The following Grid Scope Object Store required connectivity settings can be configured here:

- Cloud Pools: Where a policy-based pool can be defined (similar to physical volume pools on a TS7700T).
- Cloud Accounts: Where user credentials and target object store type is defined.
- Containers: Where containers, vaults, buckets, and their associated URLs and certificates (if applicable) are defined.

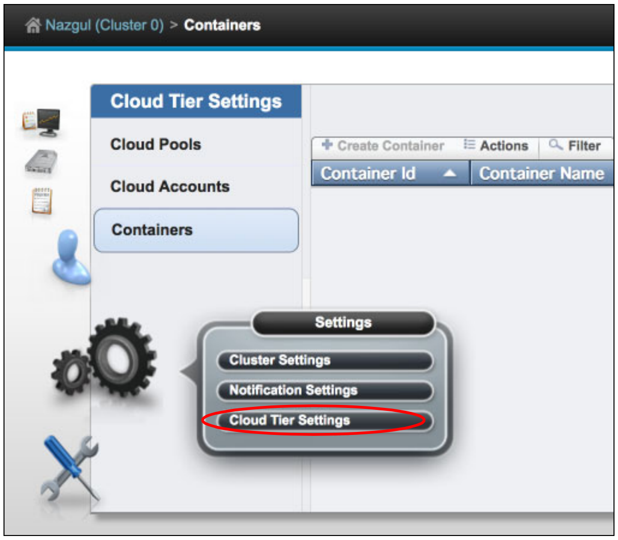
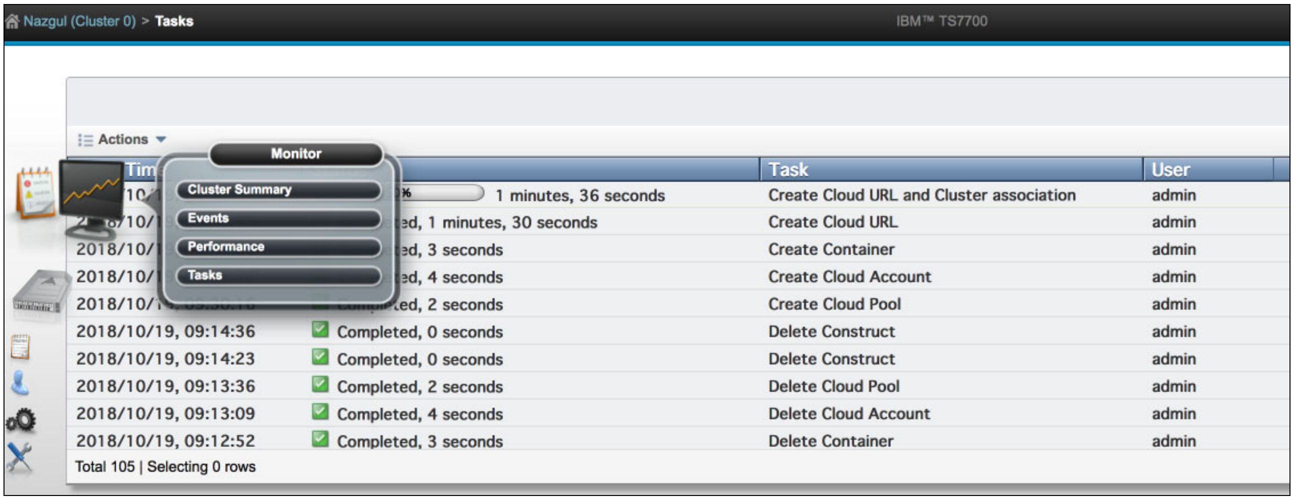


Figure 9-1 Accessing "Cloud Tier Settings" page

All changes that are made within the Cloud Tier Settings panel are asynchronous operations. Therefore, a change request states only that the request was successfully submitted and the status of the request must be viewed on the Tasks page of the Management Interface. Figure 9-2 shows the task option being selected.

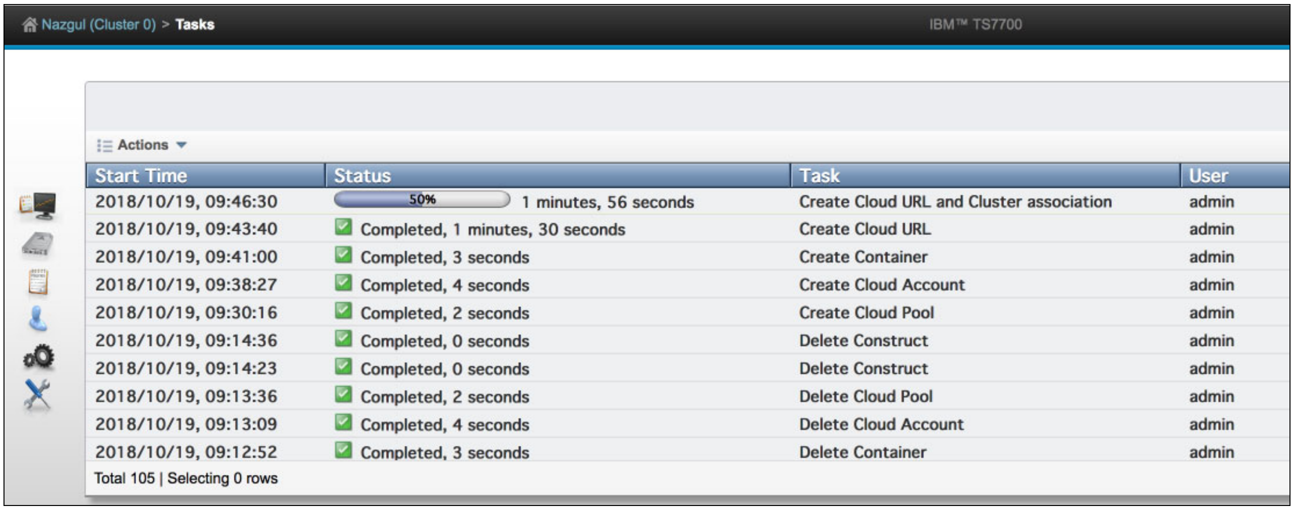


Tim		Task	User
10/1	% 1 minutes, 36 seconds	Create Cloud URL and Cluster association	admin
2 8/10/1	ed, 1 minutes, 30 seconds	Create Cloud URL	admin
2018/10/1	ed, 3 seconds	Create Container	admin
2018/10/1	ed, 4 seconds	Create Cloud Account	admin
2018/10/1	ted, 2 seconds	Create Cloud Pool	admin
2018/10/19, 09:14:36	✓ Completed, 0 seconds	Delete Construct	admin
2018/10/19, 09:14:23	✓ Completed, 0 seconds	Delete Construct	admin
2018/10/19, 09:13:36	✓ Completed, 2 seconds	Delete Cloud Pool	admin
2018/10/19, 09:13:09	✓ Completed, 4 seconds	Delete Cloud Account	admin
2018/10/19, 09:12:52	✓ Completed, 3 seconds	Delete Container	admin

Total 105 | Selecting 0 rows

Figure 9-2 Accessing the "Tasks" monitoring page

Figure 9-3. shows an example of a cloud configuration task in progress.



Start Time	Status	Task	User
2018/10/19, 09:46:30	50% 1 minutes, 56 seconds	Create Cloud URL and Cluster association	admin
2018/10/19, 09:43:40	✓ Completed, 1 minutes, 30 seconds	Create Cloud URL	admin
2018/10/19, 09:41:00	✓ Completed, 3 seconds	Create Container	admin
2018/10/19, 09:38:27	✓ Completed, 4 seconds	Create Cloud Account	admin
2018/10/19, 09:30:16	✓ Completed, 2 seconds	Create Cloud Pool	admin
2018/10/19, 09:14:36	✓ Completed, 0 seconds	Delete Construct	admin
2018/10/19, 09:14:23	✓ Completed, 0 seconds	Delete Construct	admin
2018/10/19, 09:13:36	✓ Completed, 2 seconds	Delete Cloud Pool	admin
2018/10/19, 09:13:09	✓ Completed, 4 seconds	Delete Cloud Account	admin
2018/10/19, 09:12:52	✓ Completed, 3 seconds	Delete Container	admin

Total 105 | Selecting 0 rows

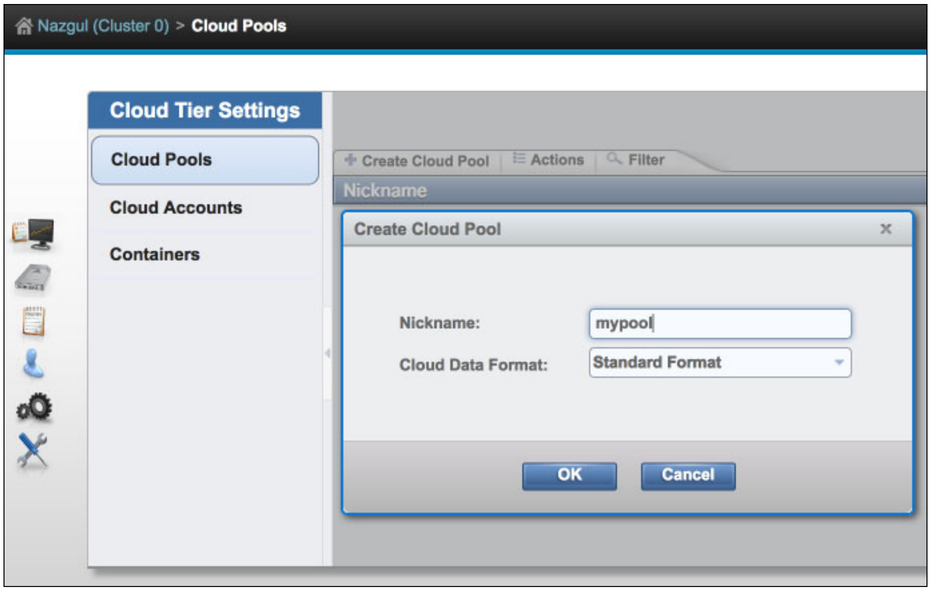
Figure 9-3 Example cloud setting task in progress

Cloud pools

All virtual tape volumes that are stored in an object store must be contained within a cloud pool. A TS7700 cloud pool serves as a grouping entity for virtual volumes that are intended to be stored in a cloud object store.

A cloud pool is a co-located collection of virtual volumes in the cloud. DFSMS policy management is then used to determine which cloud pool a virtual tape volume should be stored within. In the Release 4.2 code level, only one cloud pool per grid domain is supported. The following fields (see Figure 9-4 on page 83) must be defined:

- Nickname: User-provided name for the pool. Choose a name (up to eight characters) that easily identifies the pool. This nickname is used to reference the pool in other cloud setting panels and displayed in summary panels, LIBRARY REQUEST outputs, and Bulk Volume Information Request (BVIR) reports.
- Cloud Data Format: Used for future function enhancements (only Standard Format is supported for Release 4.2).



Nickname: mypool
Cloud Data Format: Standard Format

Figure 9-4 Creating cloud pool

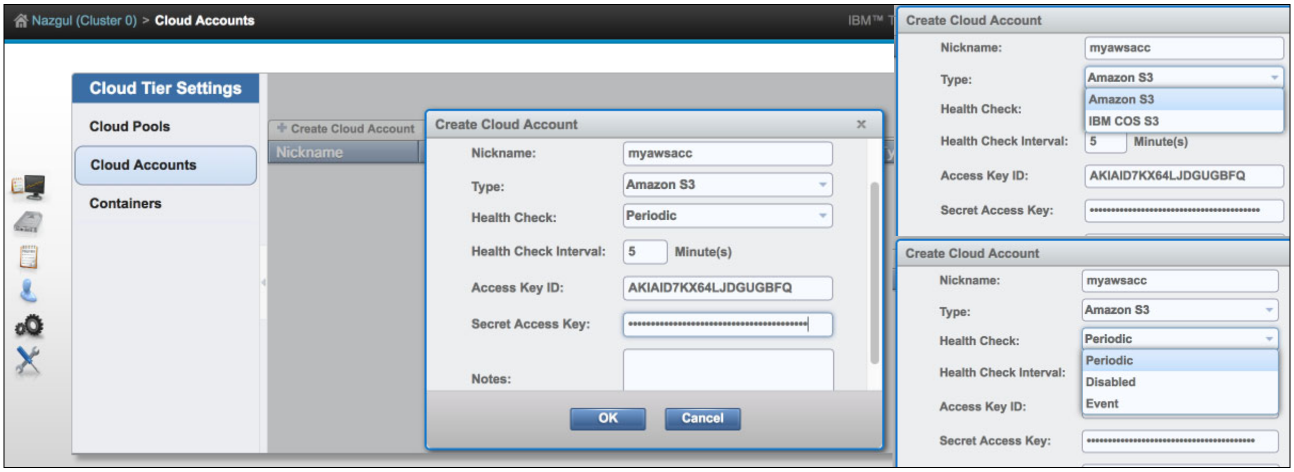
Cloud accounts

A cloud account describes an object store type, the user credentials that are needed to authenticate with the object store, and other settings related to the account. At least one cloud account must be defined before virtual tape volumes can be premigrated to an object store. Two or more can be defined if different credentials are required for different entry points into the object store. For example (see Figure 9-5), each region or cluster can use different credentials when accessing an object store. In most cases, only one account must be defined. The following settings are associated with a cloud account:

- **Nickname:** User-provided name for the account. Choose a name (up to eight characters) that easily identifies the account. This nickname is to reference the account in other cloud setting panels and displayed in summary panels, LIBRARY REQUEST outputs, and Bulk Volume Information Request (BVIR) reports.
- **Type:** The object store service to be used. As of Release 4.2, the following options are available:
  - Amazon S3
  - IBM Cloud Object Storage
- **Health Check:** This field determines if and when the TS7700 checks the availability of the object store that is associated with this account. If an issue is detected, the TS7700 enters the operations degraded state and an operator intervention message is posted. The TS7700 automatically exits the operations degraded state when health check passes. The following options are available:
  - **Periodic:** The TS7700 periodically attempts to communicate with the object store. How often is determined by the Health Check Interval setting (in minutes, default of 5). In addition to the periodic checks, the TS7700 attempts to communicate with the object store if any error event is detected during normal operations. The error event check can include storing one or more temporary objects in the object store followed by their deletion.
  - **Disabled (not recommended):** No periodic health checks is attempted. In addition, no health checks occur after error events are detected during normal operations.

  - **Event (default):** The TS7700 only attempts to communicate with the object store after any error event is detected during normal operations. The error event check can include storing one or more temporary objects in the object store followed by their deletion.

- **Cloud object store access keys:** These keys are the security credentials that are provided by the cloud service administration to access the object store that is associated with this account. The following fields are required (see Figure 9-5):
  - Access Key ID
  - Secret Access Key: This field is stored internally within the TS7700 by using AES256 encryption



Create Cloud Account

Nickname: myawsacc

Type: Amazon S3

Health Check: Periodic

Health Check Interval: 5 Minute(s)

Access Key ID: AKIAID7KX64LJDGUGBFQ

Secret Access Key: ••

Notes:

Create Cloud Account

Nickname: myawsacc

Type: Amazon S3

Amazon S3

IBM COS S3

Health Check:

Health Check Interval: 5 Minute(s)

Access Key ID: AKIAID7KX64LJDGUGBFQ

Secret Access Key: ••

Create Cloud Account

Nickname: myawsacc

Type: Amazon S3

Health Check: Periodic

Periodic

Disabled

Event

Health Check Interval:

Access Key ID:

Secret Access Key: ••

Figure 9-5 Creating cloud accounts

Containers

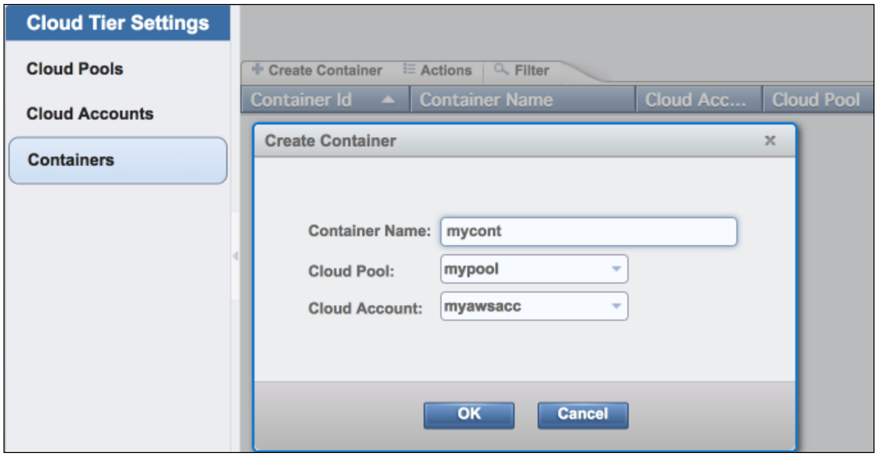
Containers are used to describe an object store vault or bucket. It must be linked to a cloud pool, cloud account, and finally one or more URLs that are used to access the vault or bucket.

If you are attaching to an IBM Cloud Object Storage, the container describes a vault. If you are attaching to Amazon S3, the container describes a bucket.

More than one container can be defined in a TS7700 grid if any of the container’s attributes vary by cluster. For example, if the URLs or credentials that are used are unique per location, two or more container definitions must be created. Or, you might need to define two containers when a form of object store mirroring is used (for example, Amazon S3 cross region replication) because each region’s vault or bucket has a unique name.

The following fields (see Figure 9-6) must be defined:

- Container Name: This name is the name of the vault or bucket within the object store. This name is *not* a nickname. The vault or bucket must be created in advance in the target cloud object store by the object store administrator.
- Cloud Pool: This pool is the cloud pool that is associated with this container. Any virtual volume that references the selected cloud pool can use this container when the object store is accessed. The cloud pool must be created previously.
- Cloud Account: This account is the cloud account that is associated with this container. When the vault or bucket that is defined by this container is accessed, the selected cloud account and credentials is used. The cloud account must be created previously.



Container Name: mycont

Cloud Pool: mypool

Cloud Account: myawsacc

Figure 9-6 Creating cloud container

Defining URL values for containers

After a cloud container is successfully created, the user must define one or more URL values that are used to connect to the bucket or vault associated with the container. For example, if an IBM Cloud Object Storage three-site configuration has six total Accessers that one or more TS7700s use as access points into the IBM Cloud Object Storage, six total URLs must be defined for the container.

For Amazon S3 configurations, at least one URL per container must be defined. Figure 9-7 shows how to define this URL, the user must right-click the container name entry, which shows the Create Cloud URL option to open a new window in which the following fields must be completed:

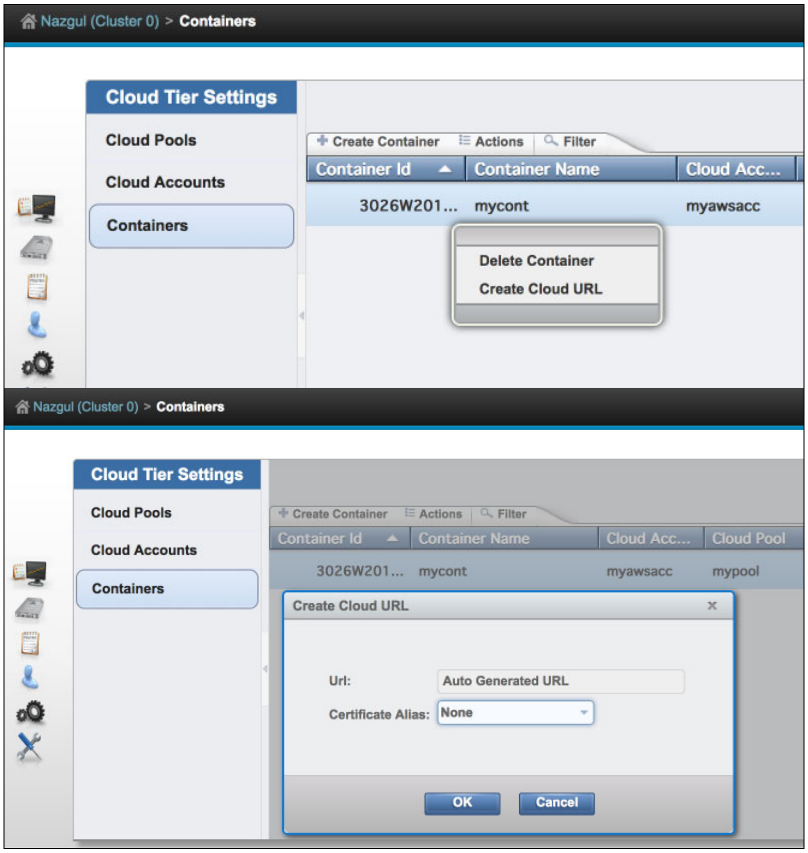
- URL: This URL is the fully qualified http or https URL that is associated with the target bucket or vault. As of the R4.2 release, only IBM Cloud Object Storage object stores require a URL.

  Amazon S3-based containers auto-fill the URL field based on the bucket name that is provided when the container was defined. For IBM Cloud Object Storage setups, the entered value must be a fixed IP address (for example, HTTPS://192.168.200.10) and is often associated with an IBM Cloud Object Storage Accesser or a connected load balancer.

  The entered address must be accessible through the TS7700 Grid network. If more than one Accesser or load balancer IP exists, each one must be created individually by using the same right-click method on the container definition.

- Certificate Alias: This field allows the user to define which optional certificate trusted authority entry is used when a secure connection is created by using the defined URL. This issue is applicable only to URL values that start with HTTPS (versus HTTP).

  This field must be completed if the connected object store uses a non-public certificate authority (CA), which often applies to all IBM Cloud Object Storage private configurations. The chosen alias is associated with a previously configured certificate. For more information about SSL certificates and how to preconfigure them in the TS7700, see Chapter 6, “SSL certificate” on page 29.



Container Id	Container Name	Cloud Acc...	Cloud Pool
3026W201...	mycont	myawsacc	mypool

Url: Auto Generated URL

Certificate Alias: None

Figure 9-7 Creating a cloud URL

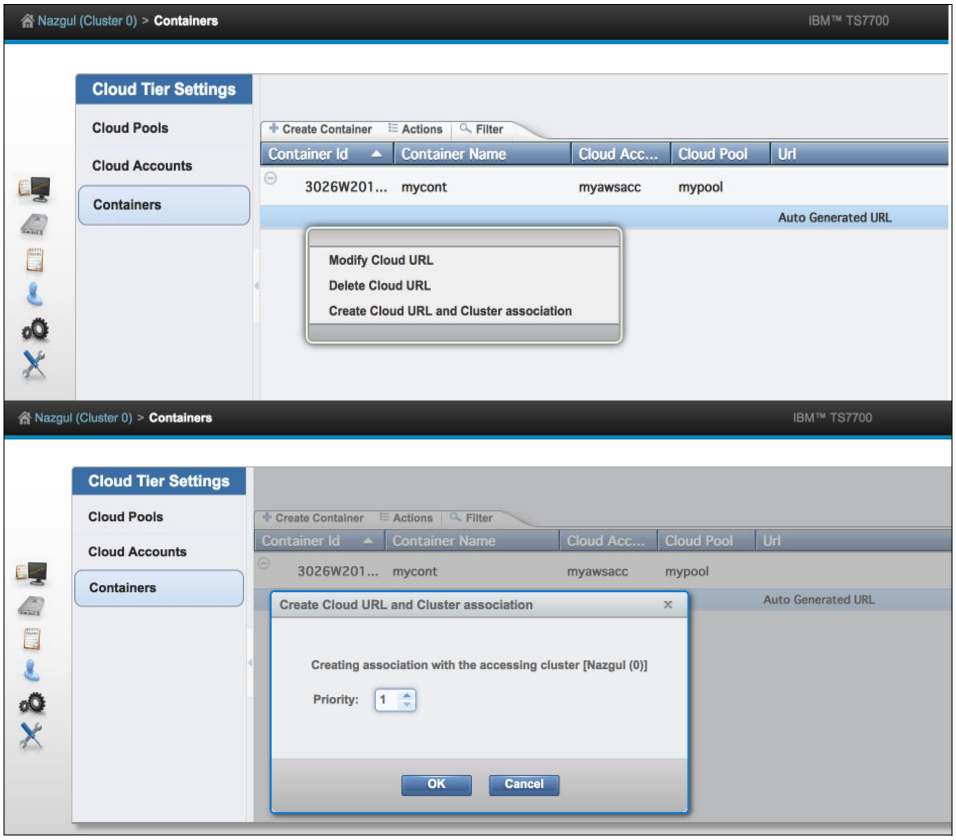
Associating URL values to specific TS7700 clusters

After one or more URL values are defined for a specific container definition, the user must inform which cluster or clusters can use the URL. For example, each region in an IBM Cloud Object Storage private configuration have different Accessers and therefore different URL values that are based on region.

One or more clusters can use some of the defined Accesser URL values while another set of clusters use a different set of Accesser URL values. By setting up a cluster URL associating, the TS7700 uses the correct URL values within its region.

As of R4.2, this action must be started from the Management Interface of the TS7700 to be associated with the URL. Therefore, if a user creates three URLs by using a specific cluster's Management Interface, the user must still log into each cluster's Management Interface, access the Container's panel, and set up the URL cluster associating for that specific cluster.

After the user is logged into the specific cluster that must be associated with one or more URLs, right-click the URL entry to show the Create Cloud URL and Cluster association option. A panel is displayed in which the user is prompted set a priority level for the association that is being created. As of R4.2, only priority "1" is valid. See Figure 9-8.



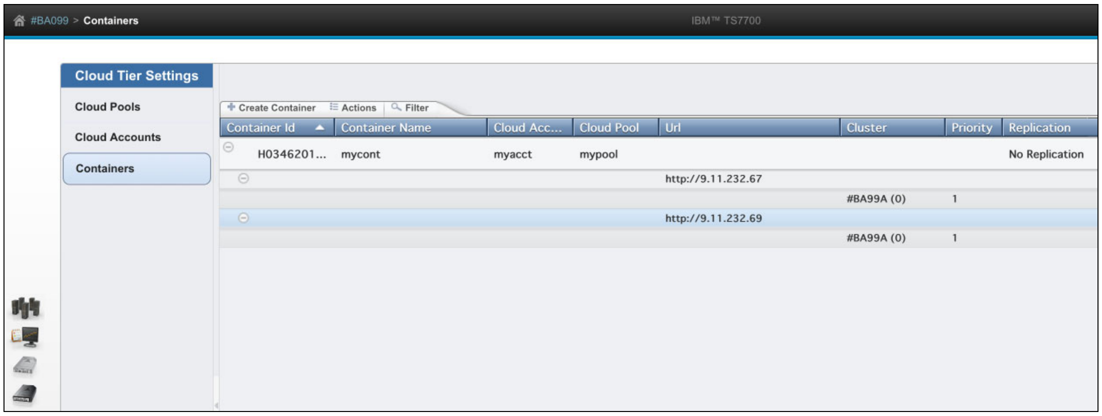
Container Id	Container Name	Cloud Acc...	Cloud Pool	Url
3026W201...	mycont	myawsacc	mypool	
				Auto Generated URL

Creating association with the accessing cluster [Nazgul (0)]

Priority: 1

Figure 9-8 Creating cloud URL and cluster association

Only containers with URLs that are assigned to a specific cluster can be accessed by that cluster. This way, each cluster can access data in a pool by way of different containers, accounts, and URLs. The process must be completed for each defined URL and for each cluster in the grid which will use that URL (see Figure 9-9).

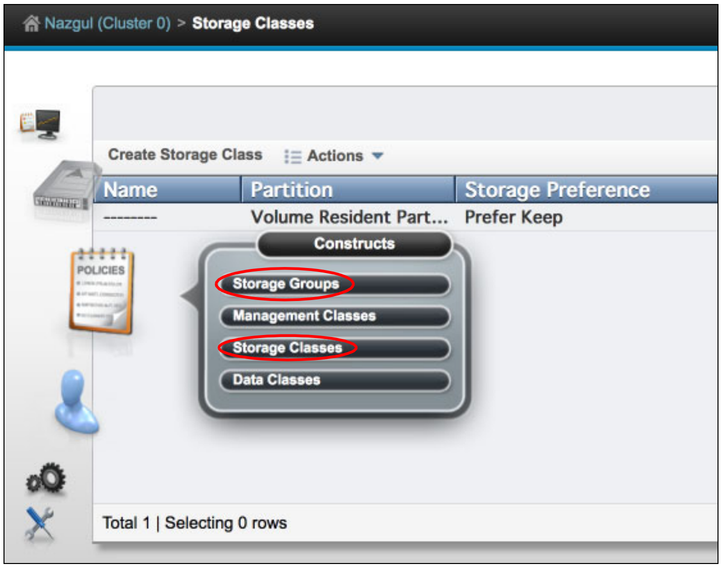


Container Id	Container Name	Cloud Acc...	Cloud Pool	Url	Cluster	Priority	Replication
H0346201...	mycont	myacct	mypool				No Replication
				http://9.11.232.67			
					#BA99A (0)	1	
				http://9.11.232.69			
					#BA99A (0)	1	

Figure 9-9 Container completely configured with a single URL and cluster association

Directing virtual volumes to the cloud storage tier

After a defined container is available, one or more URLs are defined, and the proper cluster associations are set up, you can use the policy management support of the TS7700 to direct virtual volumes to the cloud storage tier. Two constructs must be updated to properly direct logical volumes to a connected object store. Storage Class is used to direct which disk partition the logical volume is in and Storage Group is used to determine which cloud pool the data should be tiered (see Figure 9-10).



Name	Partition	Storage Preference
--------	Volume Resident Part...	Prefer Keep

Total 1 | Selecting 0 rows

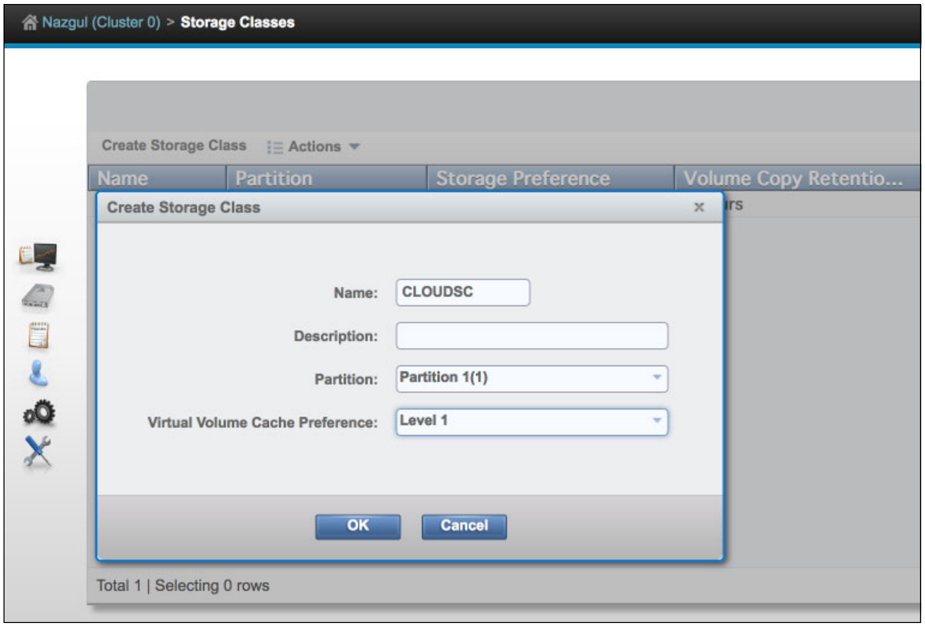
Figure 9-10 Constructs related to cloud storage tier

How to configure these two constructs is described next.

Storage classes

Storage classes (SC) are used to determine which cache partition a virtual volume targets. Consider the following points:

- Only virtual volumes that are targeting a partition other than CP0 support premigration to an object store.
- Similar to a tape attached cluster, a disk cache migration preference must be selected for virtual volumes that are associated to the SC. This configuration determines how soon volumes are removed from disk cache following their copy to the cloud storage tier. The following values (See Figure 9-11 on page 89) are available:
  - Use IART: Volumes are removed according to the Initial Access Response Time (IART) of the running IBM Z application that created the logical volume.
  - Level 0: Volumes are removed from the disk cache when they are copied to tape or cloud and any replication tasks to peers completed.
  - Level 1: Copied volumes remain in disk cache until more space is required in which a least recently used (LRU) algorithm is used to determine which Level 1 volumes should be removed to free up space.



Create Storage Class

Name: CLOUDSC

Description:

Partition: Partition 1(1)

Virtual Volume Cache Preference: Level 1

Figure 9-11 Defining storage classes for cache partition assignment

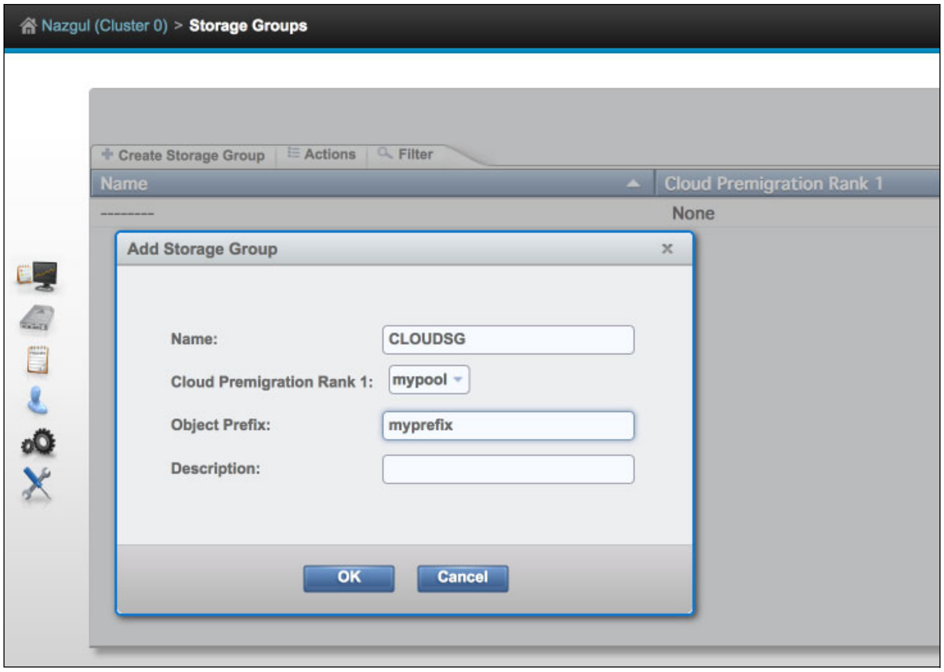
Storage groups

Storage groups (SG) are used to determine to which cloud pool a volume that is contained in a disk cache partition is copied. All clusters in the grid domain (even those clusters there are not configured for cloud storage tier), must agree on which cloud pool a particular SG uses. The following fields (Figure 9-12 on page 90) are applicable:

- Cloud Premigration Rank 1: This field represents the name of the cloud pool that receives copies of the virtual volumes. If a logical volume's assigned SG has no Cloud Premigration Rank configured but the Storage Class states the logical volume must be in a CPx partition then one of the following will occur:
  - If there is no cloud pool configured on the TS7700, the TS7700 instead stores the volume within CP0 and posts message (G0079).
  - If there is a cloud pool configured on the TS7700, the TS7700 assigns the configured cloud pool to the volume and posts message (G0078).

  > **Note:** Storage Groups always assign a Cloud Premigration Rank, even if the data is on non-cloud attached clusters only or are in CP0 resident-only partitions. If the logical volume is to ever copy to a newly configured cloud-attached cluster through COPYRFSH or the logical volume is moved from CP0 to CPx by the PARTRFSH, it does not premigrate to the cloud if the SG was not configured with a Cloud Premigration Rank when the volume was last mounted.
  >
  > Therefore, it is a recommended practice to always select a cloud premigration rank for storage classes and to ensure that all SGs in all clusters in the same grid agree on which Cloud Premigration Rank pool must be used.

- Object Prefix: This field allows the user to assign a prefix string on the key name or object name that is used to store the logical volume in the cloud object store. The TS7700 includes its own meta-data in the name, but this meta-data is the left most portion of the object name that allows a user to segregate objects by workload. For more information about the object naming convention, see 12.1, "TS7760 object name format" on page 116.



Name	Cloud Premigration Rank 1
--------	None

Name: CLOUDSG

Cloud Premigration Rank 1: mypool

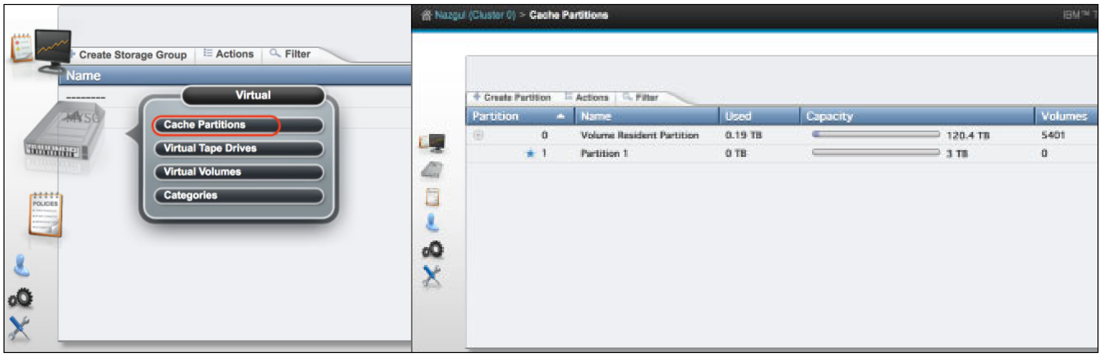
Object Prefix: myprefix

Description:

Figure 9-12 Defining storage groups for cloud storage tier

Cache partitions for cloud storage tier

TS7700 uses a non-resident cache partition (which is similar to partitions that are used for tape storage) for cloud storage as a method to manage disk cache footprint. Which CPx partition is used does not have a direct association to a particular cloud object store. Only which Storage Group is used determines which cloud pool receives the data. See Figure 9-13.



Partition	Name	Used	Capacity	Volumes
0	Volume Resident Partition	0.19 TB	120.4 TB	5401
★ 1	Partition 1	0 TB	3 TB	0

Figure 9-13 Cache partitions

Machines that are configured for cloud storage tier can still use the resident-only partition CP0 for disk-only storage. Data can be moved later between different partitions (and therefore move content from or to a cloud repository) by modifying or assigning new constructs (Storage Class and Storage group with configurations that are associated to have data in the Cloud Storage Tier), followed by mount or demount sequences or by using the **`LI REQ PARTRFSH`** command. For more information, see *IBM TS7700 Series z/OS Host Command Line Request User's Guide*, WP101091.

10

Configuration examples

This chapter shows some configuration examples of TS7700 with IBM Cloud Object Storage (ICOS) and Amazon S3. The examples show how to set up cloud pools, accounts, containers, and URLs for each configuration.

This chapter includes the following topics:

10.1 Stand-alone cluster

This section shows the simplest configurations that use a stand-alone cluster with ICOS or Amazon S3.

10.1.1 Stand-alone cluster with ICOS

In this section, we describe the process to configure a stand-alone cluster with ICOS. Before you start setting up the cloud storage tier on your TS7700, ensure that ICOS is set up in your environment. For more information about setting up your ICOS, see Chapter 8, “Setting up an AWS Cloud Object Storage” on page 55.

Figure 10-1 shows a stand-alone cluster that is connected to ICOS with three accessor nodes. The cloud storage tier is defined so that the TS7700 off loads volumes to the cloud pool MYPOOL. MYPOOL points to an ICOS vault MYVAULT, and TS7700 uses a cloud account MYACCT1 to access the vault.

Three IP addresses (`https://192.168.100.10`, `https://192.168.100.20`, and `https://192.168.100.30`) are available to access the vault. Although a load-balancer can be used between TS7700 and accessor nodes, we assume in this example that TS7700 directly connects to the three accessor nodes by using their unique IP address.

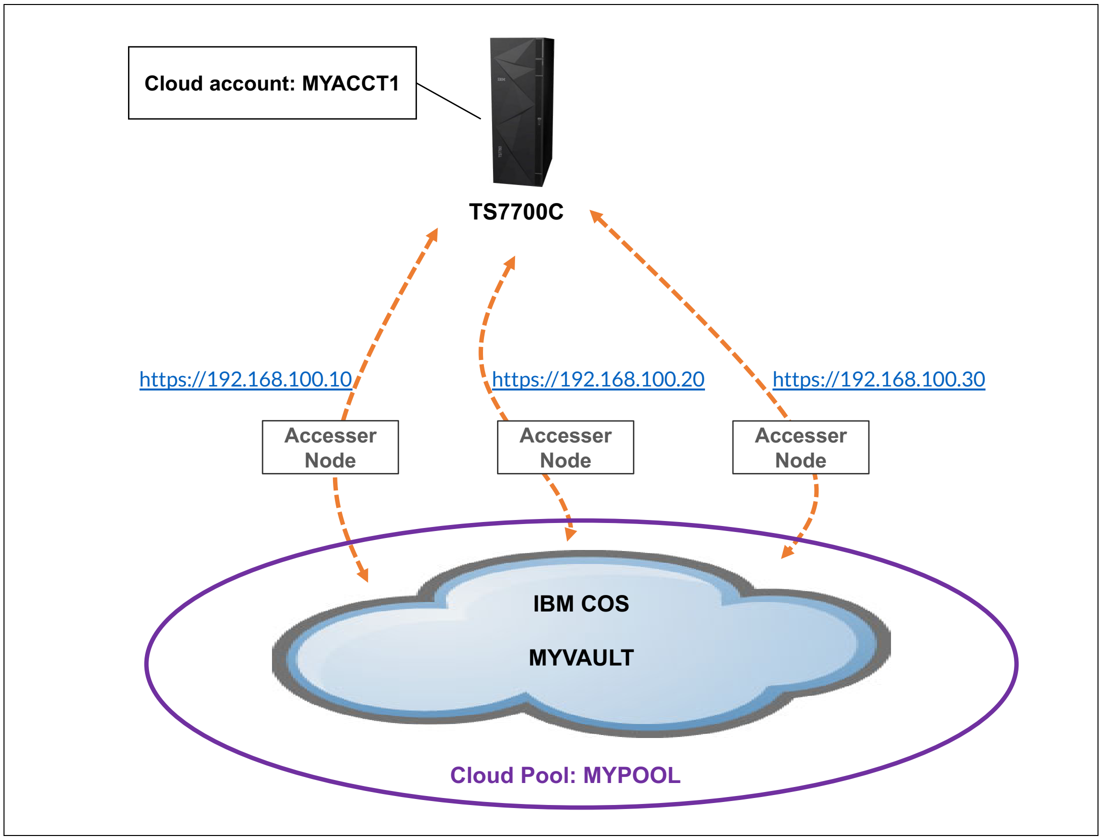


Figure 10-1 Stand-alone cluster with ICOS

The following process is used to set up such a configuration on the TS7700:

1. Create a cloud pool MYPOOL.

   A cloud pool defines a group of common logical volumes that are collocated within the object store.

2. Create a cloud account MYACCT1.

   This step is needed to configure the access credentials that are needed by the TS7700 to access the object store.

3. Create a container MYVAULT.

   This step informs the TS7700 which vault it uses to off load a volume. A container must be assigned to a cloud pool. You also must select a cloud account to use to access the vault. In this example, MYVAULT is the target of volumes that are assigned to MYPOOL, and MYACCT1 is used to access MYVAULT. The container name must be the same name as the vault on ICOS. In this example, a container is named as MYVAULT.

4. Create three cloud URLs (`https://192.168.100.10`, `https://192.168.100.20`, and `https://192.168.100.30`).

   This step informs the TS7700 which URLs can be used to access the vault.

5. Create a cloud URL and cluster association for each URL.

   This step informs a specific cluster which URLs it uses from the previous step. Although only one cluster exists in this example, the cluster association must still be completed.

Each of these steps in this process is described next.

Creating a cloud pool

Complete the following steps:

1. Go to **Settings** →**Cloud Tier** Settings on the Management Interface (MI) and select **Cloud Pools**.
2. Click **Create Cloud Pool**.
3. Enter `MYPOOL` as the cloud pool's nickname
4. Select **Standard Format** as Cloud Data Format
5. Click **OK**.

Creating a cloud account

Complete the following steps:

1. Go to **Settings** →**Cloud Tier Settings** on your MI and select **Cloud Accounts**.
2. Click **Create Cloud Account**.
3. Enter `MYACCT1` as a cloud account's nickname.
4. Select **IBM COS S3** as the account type.
5. Select a health check method (Periodic is recommended).
6. Enter your Access Key ID and Secret Access Key of your cloud account (which is provided to you by your ICOS admin).
7. Click **OK**.

Creating a container

Complete the following steps:

1. Verify that a vault (for example, MYVAULT) is created in ICOS.
2. Go to **Settings** →**Cloud Tier Settings** on your MI and select **Containers**.
3. Click **Create Container**.
4. Enter `MYVAULT` as a container name.
5. Select **MYPOOL** as the cloud pool.
6. Select **MYACCT1** as the cloud account.
7. Click **OK**.

Creating cloud URLs

1. Verify that an SSL certificate is uploaded to your TS7700.

   For more information about uploading an SSL certificate, see Chapter 6, “SSL certificate” on page 29. If your cloud URL does not use the secure https protocol, you do not need to upload an SSL certificate.

2. Go to **Settings** →**Cloud Tier Settings** on your MI and select **Containers**.
3. Right-click the **MYVAULT** container and select **Create Cloud URL**.
4. Enter `https://192.168.100.10` as a URL.
5. Select the SSL certificate alias that you uploaded.
6. Click **OK**.
7. If you use the non-secured http protocol, enter `http://192.168.100.10` as a URL instead and leave the certificate alias blank.
8. After you create the first URL, right-click the **MYVAULT** container again and create a second and third cloud URL by using the same process for `https://192.168.100.20` and `https://192.168.100.30`.

Creating cloud URL and cluster associations

Complete the following steps:

1. Go to **Settings** →**Cloud Tier Settings** on MI and select **Containers**.
2. Expand the container to show the Cloud URLs you created.
3. Right-click one of the Cloud URLs, and select **Create Cloud URL and Cluster association**.
4. Set `1` as a priority and click **OK**.
5. Create an association for each Cloud URL that you created so that each URL can be used by this cluster.

10.1.2 Stand-alone cluster with Amazon S3

In this section, the process that is used to configure a stand-alone TS7700C cluster with Amazon S3 is described. An Amazon Web Service (AWS) account must be created before a stand-alone cluster can be set up with Amazon S3. For more information about setting up an AWS account, see Chapter 8, “Setting up an AWS Cloud Object Storage” on page 55.

Figure 10-2 shows a stand-alone cluster that is connected to Amazon S3. The cloud storage tier is defined so that TS7700C off loads logical tape volumes to the cloud pool MYPOOL. MYPOOL points to AWS bucket MYBUCK1, and TS7700C uses a cloud account MYACCT1 to access the vault.

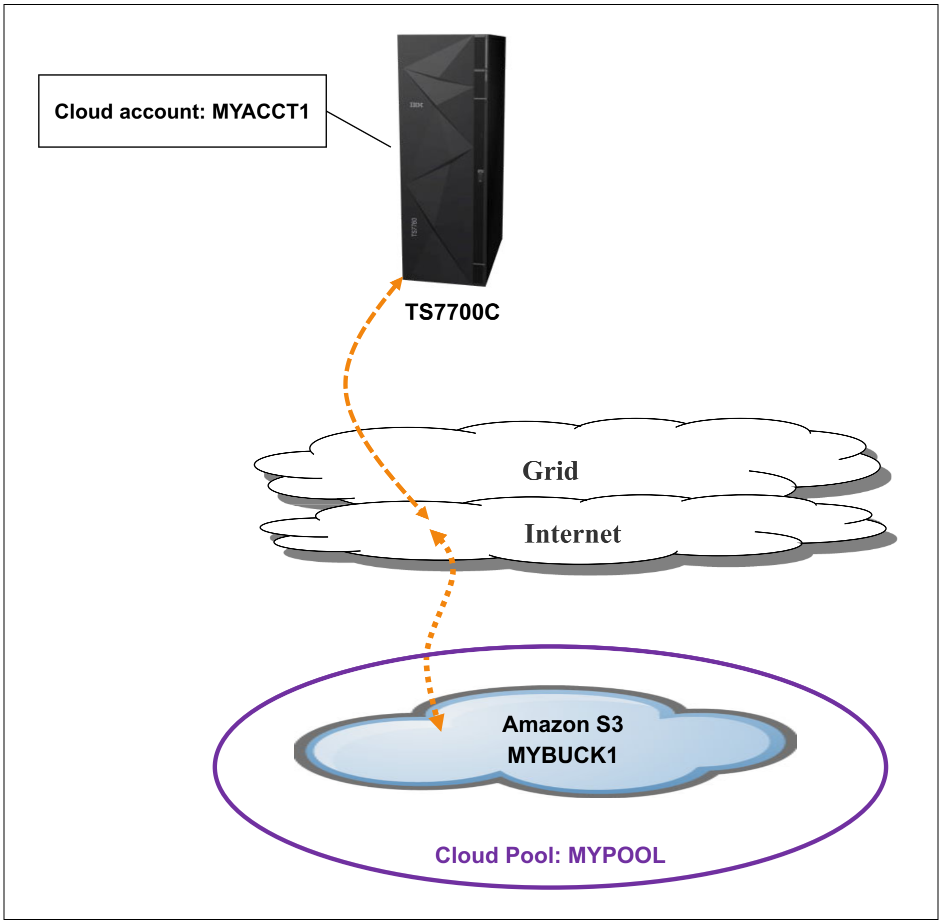


Figure 10-2 Stand-alone cluster with Amazon S3

The following process is used to set up such a configuration:

1. Create a cloud pool MYPOOL.

   A cloud pool defines a group of common logical volumes that are collocated within the object store.

2. Create a cloud account MYACCT1.

   In this step, the access credentials that are needed by the TS7700 to access the object store are configured.

3. Create a container MYBUCK1.

   In this step, the TS7700 is informed of which AWS bucket it uses to off load logical tape volumes. A container must be assigned to a cloud pool. You must select a cloud account to use to access the AWS bucket. In this example, MYBUCK1 is the target of volumes that are assigned to MYPOOL. MYACCT1 is used to access MYBUCK1. The container name must be the same name as the AWS bucket in Amazon S3. In this example, a container is named MYBUCK1.

4. Create a cloud URL.

   Often, the TS7700 is informed of which URL to use to access the bucket in this step. However, but you do not need to provide an Amazon S3 URL. Instead, the TS7700 automatically generates the URL by using the bucket name.

5. Create a cloud URL and cluster association for the previously created URL.

   In this step, a specific cluster is informed that it can use the URL created in the previous step. Although only one cluster exists in this example, the cluster association must still be completed.

Each of these steps in this process is described next.

Creating a cloud pool

Complete the following steps:

1. Go to **Settings** →**Cloud Tier Settings** on the Management Interface (MI) and select **Cloud Pools**.
2. Click **Create Cloud Pool**.
3. Enter `MYPOOL` as the cloud pool's nickname.
4. Select **Standard Format** as the Cloud Data Format.
5. Click **OK**.

Creating a cloud account

Complete the following steps:

1. Go to **Settings** →**Cloud Tier Settings** on MI and select **Cloud Accounts**.
2. Click **Create Cloud Account**.
3. Enter `MYACCT1` as the cloud account's nickname.
4. Select **Amazon S3** as the account type.
5. Select a health check method (Periodic is recommended).
6. Enter your AWS S3 Access Key ID and Secret Access Key of your cloud account.
7. Click **OK**.

Creating a container

Complete the following steps:

1. Verify that a bucket MYBUCK1 is created in Amazon S3.
2. Go to **Settings** →**Cloud Tier Settings** on your MI and select **Containers**.
3. Click **Create Container**.
4. Enter `MYBUCK1` as the container name.
5. Select **MYPOOL** as the cloud pool.
6. Select **MYACCT1** as the cloud account.
7. Click **OK**.

Creating a cloud URL

Complete the following steps:

1. Go to **Settings** →**Cloud Tier Settings** on MI and select **Containers**.
2. Right-click the **MYBUCK1** container and select **Create Cloud URL**.
3. Click **OK** on the Create Cloud URL window.

Creating a cloud URL and cluster association

Complete the following steps:

1. Go to **Settings** →**Cloud Tier Settings** on MI and select **Containers**.
2. Expand the container **MYBUCK1** so that it displays the Cloud RUL you created.
3. Right-click the Cloud URL and select **Create Cloud URL and Cluster association**.
4. Set 1 as a priority.
5. Click **OK**.

10.2 Two-way grid with one cloud pool, account, and container with ICOS

This section describes a two-way Grid TS7700C cluster with one cloud pool/account/container that uses ICOS. Before setting up the cloud storage tier, ICOS must be set up in your environment. For more information about setting up your ICOS, see Chapter 8, “Setting up an AWS Cloud Object Storage” on page 55.

Figure 10-3 shows the two-way Grid with one cloud pool/account/container that uses ICOS. In this example, we assume that the ICOS configuration has three accessor nodes in each region and the contents that is in the single vault is made redundant through ICOS’s erasure coding. The cloud storage tier is defined so that the TS7700C off loads logical volumes to the cloud pool MYPOOL. MYPOOL points to an ICOS vault MYVAULT, and the two TS7700Cs in West and East use a cloud account MYACCT1 to access the vault.

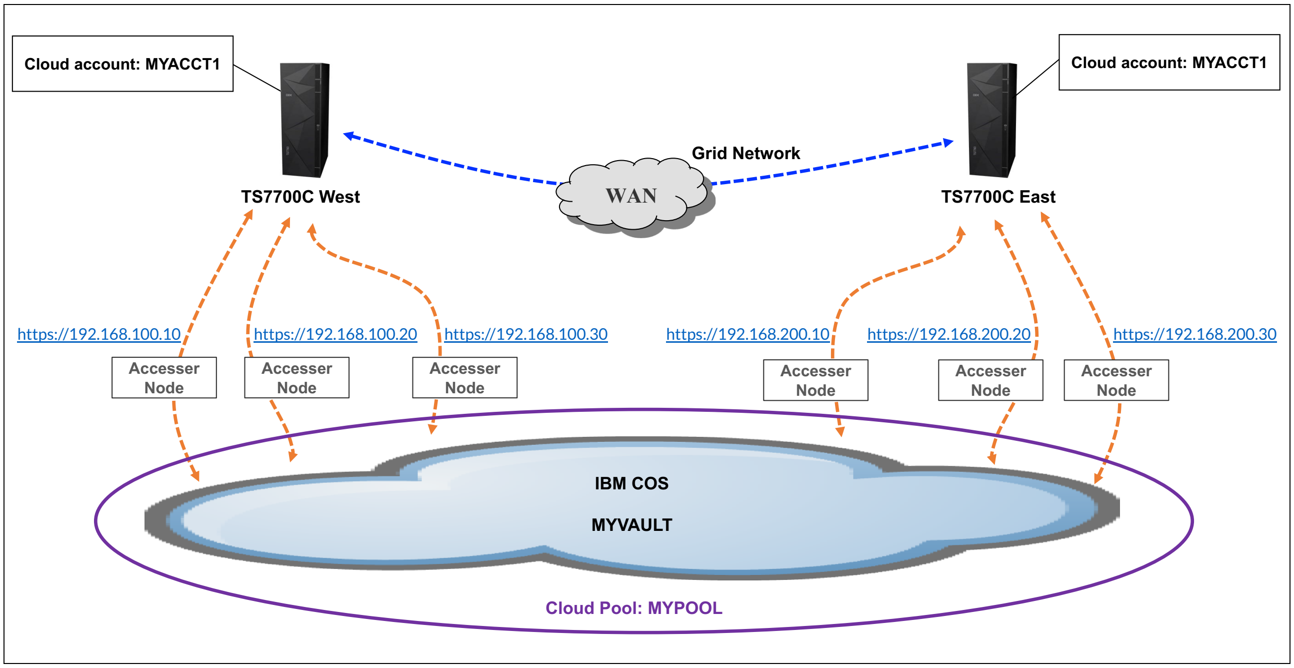


Figure 10-3 Two-way TS7700C clusters with one cloud account/pool/container using ICOS

Because six total accessors are used, six unique cloud URLs are available to access the vault. Each of the six URLs must be assigned to the MYVAULT container.

Three IP addresses (`https://192.168.100.10`, `https://192.168.100.20`, and `https://192.168.100.30`) must be associated with TS7700C West. Three cloud URLs (`https://192.168.200.10`, `https://192.168.200.20`, `https://192.168.200.30`) must be associated with TS7700C East.

A load-balancer can be used between the TS7700 and accessor nodes. However, we assume in this example that the TS7700 directly connects to the three accessor nodes by using their unique IP addresses.

The following process is used to set up such a configuration. The first four steps must be completed only once per grid by using either of the clusters. Step five requires a unique step per cluster:

1. Create a cloud pool MYPOOL.

   A cloud pool defines a group of common logical volumes that are collocated within the object store.

2. Create a cloud account MYACCT1.

   In this step, the access credentials that are needed by the TS7700 to access the object store are configured.

3. Create a container MYVAULT.

   In this step, TS7700C is informed which vault it uses to off load a volume. The container must be assigned to the cloud pool, and you must select a cloud account to use to access the vault. The container name must be in sync with a bucket in Amazon S3. In this example, a container must be named as MYVAULT, which is assigned to MYPOOL, and MYACCT1 is used to access MYVAULT.

4. Create six cloud URLs (`https://192.168.100.10`, `https://192.168.100.20`, `https://192.168.100.30`, `https://192.168.200.10`, `https://192.168.200.20`, and `https://192.168.200.30`).

   In this step, the TS7700 is informed which URLs can be used to access the vault.

5. Create a cloud URL and cluster association for each URL.

   In this step, a specific cluster is informed which URLs it uses from the previous step. Although all URLs are assigned to the same container, which cluster can use those URLs must be defined. This step must be completed on the cluster where the association is to be assigned. In this example, you need to assign three cloud URLs (`https://192.168.100.10`, `https://192.168.100.20`, and `https://192.168.100.30`) to TS7700 West and the other three cloud URLs (`https://192.168.200.10`, `https://192.168.200.20`, and `https://192.168.200.30`) to TS7700 East.

Each of these steps in this process is described next.

Creating a cloud pool

Complete the following steps:

1. In either cluster, go to **Settings** →**Cloud Tier Settings** on the Management Interface (MI) and select **Cloud Pools**.
2. Click **Create Cloud Pool**.
3. Enter `MYPOOL` as the cloud pools nickname.
4. Select **Standard Format** as the Cloud Data Format.
5. Click **OK**.

Creating a cloud account

Complete the following steps:

1. In either cluster, go to **Settings** →**Cloud Tier Settings** on your MI and select **Cloud Accounts**.
2. Click **Create Cloud Account**.
3. Enter `MYACCT1` as the cloud account's nickname.
4. Select **IBM COS S3** as the account type.
5. Select a health check method (Periodic is recommended).
6. Enter your Access Key ID and Secret Access Key (provided by your ICOS Admin) of your vault's cloud account.
7. Click **OK**.

Creating a container

Complete the following steps:

1. Verify that your vault (for example, MYVAULT) is created in ICOS.
2. In either cluster, go to **Settings** →**Cloud Tier Settings** on your MI and select **Containers**.
3. Click **Create Container**.
4. Enter `MYVAULT` as the container name.
5. Select **MYPOOL** as the cloud pool.
6. Select **MYACCT1** as the cloud account.
7. Click **OK**.

Creating a cloud URL

Complete the following steps:

1. Verify that an SSL certificate is uploaded in your TS7700 grid.

   For more information about uploading an SSL certificate, see Chapter 6, "SSL certificate" on page 29. If your cloud URL does not use the secure https protocol, you do not need to upload an SSL certificate.
2. In either cluster, go to **Settings** →**Cloud Tier Settings** on your MI and select **Containers**.
3. Right-click the **MYVAULT** container and select **Create Cloud URL**.
4. Enter `https://192.168.100.10` as the URL.
5. Select the alias for the SSL certificate that you uploaded.
6. Click **OK**.
7. If you use the non-secure http protocol, enter `http://192.168.100.10` as the URL instead and leave the certificate field blank.
8. After completed, right-click the **MYVAULT** container again and create cloud URLs for the remaining URLs (`https://192.168.100.20`, `https://192.168.100.30`, `https://192.168.200.10`, `https://192.168.200.20`, and `https://192.168.200.30`). Because all six URLs are associated with the same vault, all six can be created under the same container.

Creating a cloud URL and cluster association

Complete the following steps:

1. On the TS7700C West cluster, go to **Settings →Cloud Tier Settings** on its MI and select **Containers**.
2. Expand the Cloud URLs you created.
3. Right-click **https://192.168.100.10**, and select **Create Cloud URL and Cluster association**.
4. Set `1` as a priority and click **OK**.

   The TS7700C West cluster is informed that it can use that URL to access the ICSO vault. Create an association for the other two URLs (`https://192.168.100.20` and `https://192.168.100.30`) on TS7700C West so it has three URLs it can use to access the vault.
5. Log out of the TS7700C West MI and log in to the MI of the TS7700C East cluster and repeat the steps for its three URLs (`https://192.168.200.10`, `https://192.168.200.20`, and `https://192.168.200.30`).

After this process is completed, each cluster in each region now is aware of which of the six URLs it uses to access the ICOS vault.

10.3 Two-way grid with one cloud pool for an Amazon S3 Cross Region Replication set of buckets accessed by using different credentials

This section shows a two-way TS7700C cluster Grid with one cloud pool, two accounts (one for each AWS Region), and two containers (one for each region bucket) that use Amazon S3. Two Amazon Web Service accounts must be created before setting up the TS7700C clusters with Amazon S3. For more information about setting up the AWS accounts, see Chapter 8, “Setting up an AWS Cloud Object Storage” on page 55.

Figure 10-4 on page 101 shows a two-way TS7700C cluster Grid with one cloud pool, two accounts, and two containers that use Amazon S3. The two TS7700C clusters shares a cloud pool MYPOOL because all data is synchronized between regions. This configuration is achieved through AWS S3 Cross Region Replication, which requires each region to have a unique bucket name (for example, MYBUCK1 and MYBUCK2).

The contents in the buckets are synchronized by using Amazon Cross Region Replication. Because each bucket can have different access credentials, this example uses two cloud accounts (MYACCT1 and MYACCT2) to connect to each region’s unique bucket. Although they can use the same account, this example assumes that two different accounts are used.

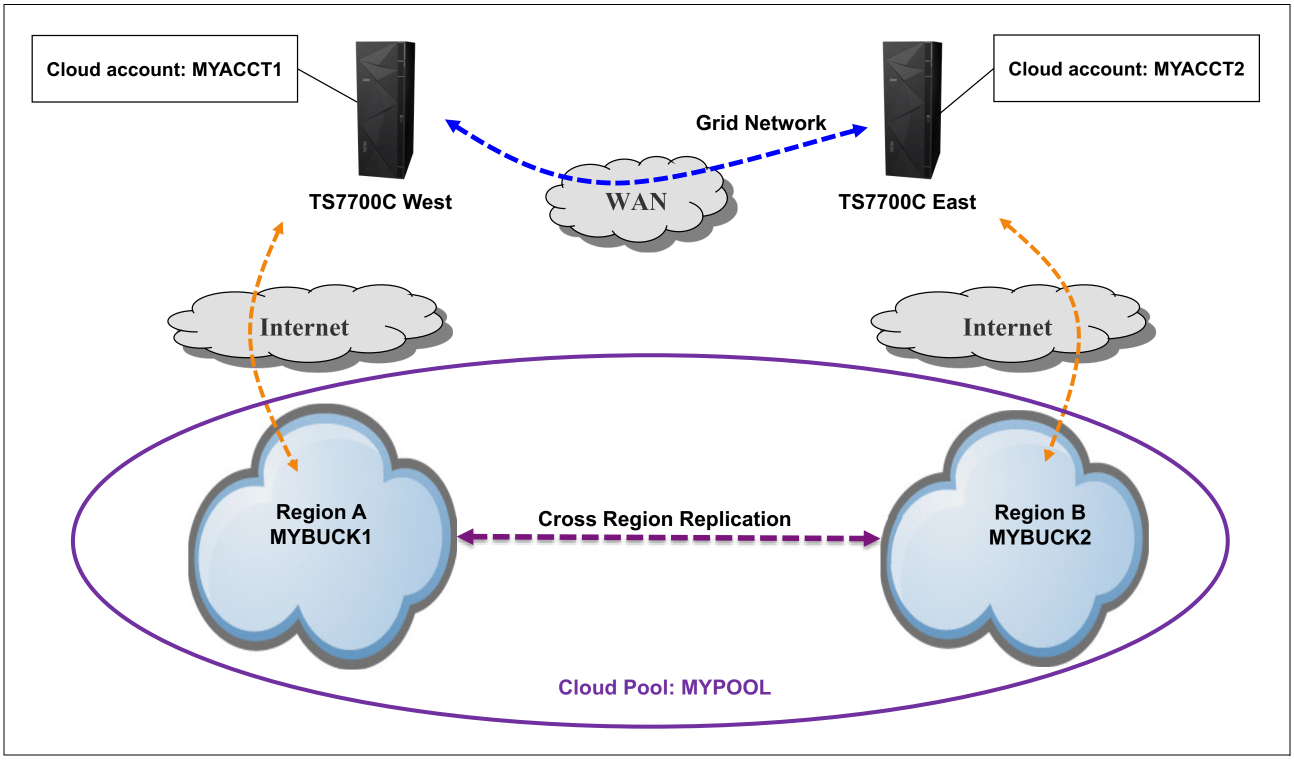


Figure 10-4 Two-way TS7700C clusters with one cloud pool, two accounts, and two containers using Amazon S3

The following process is used to set up such a configuration. The first four steps must be completed only once per grid by using either cluster. Step five requires a unique step per cluster:

1. Create a cloud pool that is named MYPOOL.

   In this example, a cloud pool represents a pair of containers where logical tape volumes are offloaded. The TS7700C West offloads to MYBUCK1, the TS7700C East cluster offloads to MYBUCK2.

   The contents in MYBUCK1 and MYBUCK2 must be replicated bi-directionally by using Amazon Cross Region Replication so that anything that is put into either bucket is accessible from the other bucket as one cross-regional pool.

2. Create two accounts (MYACCT1 and MYACCT2).

   This step is needed to configure the credentials that are needed by the TS7700 to access the object store.

3. Create two containers (MYBUCK1 and MYBUCK2).

   In this step, both TS7700C clusters or informed which buckets are associated with MYPOOL. The containers (MYBUCK1 and MYBUCK2) must be assigned to the cloud pool (MYPOOL). You also must select the appropriate cloud account for each container (MYACCT1 for MYBUCK1 and MYACCT2 for MYBUCK2). Before containers are created on either TS7700C, you must set up Amazon Cross Region Replication bi-directionally between MYBUCK1 and MYBUCK2.

4. Create a cloud URL under each container.

   Normally, the TS7700 is informed of which URL to use to access the buckets, but you do not need to provide an Amazon S3 URL. Instead, the TS7700 automatically generates the URL by using the bucket name under which you are creating the URL.

5. Create a cloud URL and cluster association for the previously created URLs.

   In this step, each of the two clusters is informed of which URL that was created in the previous step is used to access a bucket. You must associate the TS7700 West cluster to the cloud URL that is assigned to MYBUCK1 and associate TS7700 East to the Cloud URL that is assigned to MYBUCK2.

Each of these steps in this process is described next.

Creating a cloud pool

Complete the following steps:

1. On either cluster, go to **Settings** → **Cloud Tier Settings** on the Management Interface (MI) and select **Cloud Pools**.
2. Click **Create Cloud Pool**.
3. Enter `MYPOOL` as the cloud pool's nickname.
4. Select **Standard Format** as the Cloud Data Format.
5. Click **OK**.

Creating cloud accounts

Complete the following steps:

1. On either cluster, go to **Settings** → **Cloud Tier Settings** on your MI and select **Cloud Accounts**.
2. Click **Create Cloud Account**.
3. Enter `MYACCT1` as the cloud account's nickname.
4. Select **Amazon S3** as the account type.
5. Select a health check method (Periodic is recommended).
6. Enter your AWS S3 Access Key ID and Secret Access Key (which is provided by your AWS S3 Admin) of your cloud account that is used to access MYBUCK1 in the West region.
7. Click **OK**.
8. On either cluster, create a second cloud account (MYACC2) by using the Access Key ID and Secret Access Key pair that is used to access MYBUCK2 in the East region.

Creating containers

Complete the following steps:

1. Ensure that buckets MYBUCK1 and MYBUCK2 are created in Amazon S3 in each region and cross regional replication is enabled bi-directionally.
2. In either cluster, click **Settings** → **Cloud Tier Settings** on the MI and select **Containers**.
3. Click **Create Container**.
4. Enter `MYBUCK1` as the container name.
5. Select **MYPOOL** as the cloud pool
6. Select **MYACCT1** as the cloud account
7. Click **OK**.
8. On either cluster, repeat this process and create a second container for MYBUCK2 and use MYACCT2 as the cloud account.

Creating a cloud URL

Complete the following steps:

1. On either cluster, click **Settings** →**Cloud Tier Settings** on the MI and select **Containers**.
2. Right-click the **MYBUCK1** container and select **Create Cloud URL**.
3. In the Create Cloud URL window, click **OK**.
4. In the container window, create a cloud URL for MYBUCK2. This process can be completed on the same cluster.

Creating a cloud URL and cluster association

Complete the following steps:

1. On TS7700C West cluster, click **Settings** →**Cloud Tier Settings** on its MI and select **Containers**.
2. Expand the Cloud URL that you created for MYBUCK1.
3. Right-click the Cloud URL and select **Create Cloud URL and Cluster association**.
4. Set **1** as a priority.
5. Click **OK**.

   The TS7700C West cluster is informed that it must use that URL to access MYBUCK1.
6. Log out of the TS7700C West cluster.
7. Log in to the TS7700C East cluster's MI and create an association with the cloud URL that is assigned to MYBUCK2.

10.4 Four-way grid with one cloud pool, two accounts, and one container using ICOS

This section provides an example of a four-way two region TS7700C Grid with one cloud pool, two accounts (one per region), and one container using ICOS. Before setting up the cloud storage tier, your ICOS must be set up in your environment. For more information about setting up your ICOS, see Chapter 8, "Setting up an AWS Cloud Object Storage" on page 55.

Figure 10-5 on page 104 shows a four-way, two-region TS7700C Grid and all four clusters are connected to the same cloud pool MYPOOL. Two TS7700C clusters in the West region use one cloud account (MYACCT1) to access the cloud pool, and the other two TS7700C clusters in the East region use another cloud account (MYACCT2) to access the same cloud pool. MYVAULT is assigned to the cloud pool, and the following cloud URLs are available to be used to access the vault:

- `https://192.168.100.10`
- `https://192.168.100.20`
- `https://192.168.100.30`
- `https://192.168.200.10`
- `https://192.168.200.20`
- `https://192.168.200.30`)

Three URLs are used per region because each region includes three accessor nodes.

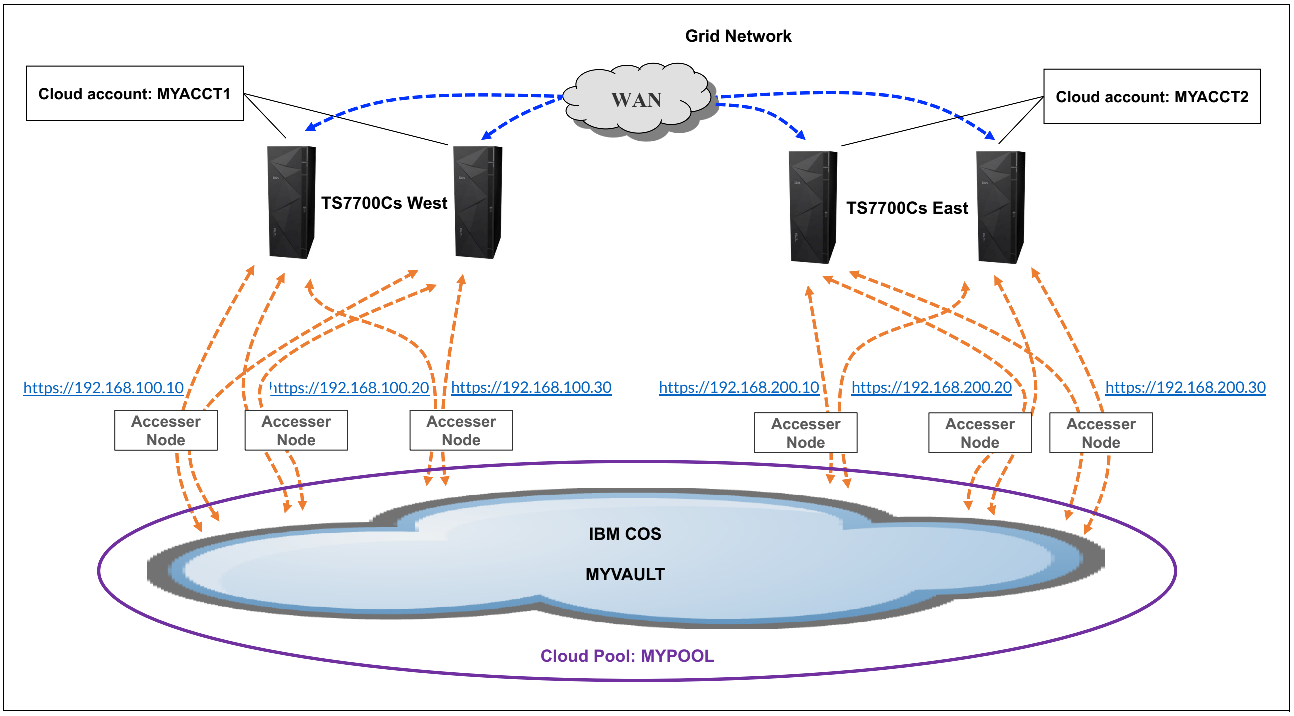


Figure 10-5 Four-way TS7700C clusters with one cloud pool/two accounts/one container using ICOS

Thee cloud URLs (`https://192.168.100.10`, `https://192.168.100.20`, and `https://192.168.100.30`) must be associated with the two TS7700Cs in the West region and other three cloud URLs (`https://192.168.200.10`, `https://192.168.200.20`, and `https://192.168.200.30`) must be associated with the two TS7700Cs in the East region.

The following process is used to set up such a configuration. The first four steps must be completed only once per grid by using any of the four clusters. Step five requires a unique step per cluster:

1. Create a cloud pool.

   A cloud pool defines a container where logical tape volumes are offloaded. In this example, logical tape volumes are offloaded to MYVAULT from all the TS7700C clusters that are in the grid. The contents of MYVAULT must be synchronized between ICOS in West and East by using ICOS's multi-sites erasure coding or 2-site replication.

2. Create two accounts MYACCT1 and MYACCT2.

   This step is needed to configure the credentials that are needed by the TS7700 to access the object store.

3. Create two containers with the same name (MYVAULT) because each region must use its own account.

   If both regions used the same account, only one container is needed. This step informs the TS7700C which vault and account it uses to offload logical volumes from either region. The containers must be assigned to the cloud pool, and you must select a cloud account to use to access each container.

   Before creating containers on the TS7700C, a vault, such as MYVAULT on ICOS, must be created with the correct read/write access from accounts MYACCT1 and MYACCT2.

4. Create the following cloud URLs:

   - `https://192.168.100.10`
   - `https://192.168.100.20`
   - `https://192.168.100.30`
   - `https://192.168.200.10`
   - `https://192.168.200.20`
   - `https://192.168.200.30`)

   This step informs the TS7700C which cloud URLs are available to access the vault.

5. Create cloud URL and cluster associations.

   This step informs each unique cluster which cloud URLs that were created in the previous step it uses to access the vault. Three cloud URLs (`https://192.168.100.10`, `https://192.168.100.20`, and `https://192.168.100.30`) must be associated with TS7700Cs in the West region. The other three cloud URLs (`https://192.168.200.10`, `https://192.168.200.20`, and `https://192.168.200.30`) must be associated with the TS7700Cs in East region.

Each of these steps in this process is described next.

Creating a cloud pool

Complete the following steps:

1. On any of the four clusters, click **Settings** →**Cloud Tier Settings** on the Management Interface (MI) and select **Cloud Pools**.
2. Click **Create Cloud Pool**.
3. Enter `MYPOOL` as the cloud pool’s nickname.
4. Select **Standard Format** as the Cloud Data Format.
5. Click **OK**.

Creating cloud accounts

Complete the following steps:

1. On any of the four clusters, click **Settings** →**Cloud Tier Settings** on your MI and select **Cloud Accounts**.
2. Click **Create Cloud Account**.
3. Enter `MYACCT1` as the cloud account’s nickname
4. Select **IBM COS S3** as the account type.
5. Select a health check method (Periodic is recommended).
6. Enter the Access Key ID and Secret Access Key (provided by your ICOS Admin) of the cloud account that is used in the West region.
7. Click **OK**.
8. Create another cloud account (MYACCT2) by using the Access Key ID and Secret Access Key pair that is used in the East region.

Creating containers

Complete the following steps:

1. Ensure a vault (for example, MYVAULT) is created in your ICOS.
2. On any of the four clusters, click **Settings** →**Cloud Tier Settings** on your MI and select **Containers**.

3. Click **Create Container**.
4. Enter `MYVAULT` as the container name.
5. Select **MYPOOL** as the cloud pool.
6. Select **MYACCT1** as the cloud account.
7. Click **OK**.
8. Create another container with the same name and select **MYPOOL** as the cloud pool and use **MYACCT2** as the cloud account.

When this process is completed, two containers are available: one for region West and one for region East.

Creating cloud URLs

Complete the following steps:

1. Ensure that an SSL certificate is uploaded to your TS7700 Grid.

   For more information about uploading an SSL certificate, see Chapter 6, “SSL certificate” on page 29. If your cloud URL does not use the secure https protocol, you do not need to upload an SSL certificate.
2. On any of the four clusters, click **Settings** →**Cloud Tier Settings** on the MI and select **Containers**.
3. Right-click the **MYVAULT** container that is associated with MYACCT1 and click **Create Cloud URL**.
4. Enter `https://192.168.100.10` as a URL.
5. Select the SSL certificate alias for the certificate that you uploaded.
6. Click **OK**.
7. If you use the non-secure http protocol, enter `http://192.168.100.10` as a URL instead and leave the certificate option blank.
8. Right-click the same container again and create a second cloud URL for `https://192.168.100.20` and then, a third URL for `https://192.168.100.30`.
9. Right-click the **MYVAULT** container that is associated with MYACCT2 and create three cloud URLs for `https://192.168.200.10`, `https://192.168.200.20`, and `https://192.168.200.30`.

When this process is completed, three URLs are defined under each of the two containers: three for region West and three for region East.

Creating cloud URL and cluster associations

Complete the following steps:

1. On both TS7700C clusters in the West region, click **Settings** →**Cloud Tier Settings** on their MI windows (you must log in to each one individually) and select **Containers.**
2. Expand the Cloud URLs you created for the West region.
3. Right-click **https://192.168.100.10** and select **Create Cloud URL and Cluster association**.
4. Set **1** as a priority and click **OK**.
5. Create an association for the other two West region URLs (`https://192.168.100.20` and `https://192.168.100.30`).

6. Repeat these steps for the two clusters in the East region by associating them both with the three accessor URLs for that region.
7. Log in to each one individually and set up an association with `https://192.168.200.10`, `https://192.168.200.20`, and `https://192.168.200.30`.

When this process is completed, both clusters in the East are associated with three of the URLs. Also, both clusters in the West are associated with the other three URLs.

10.5 Four-way clusters (one TS7700C in each location) with one cloud pool, two accounts, and one container using ICOS

This section shows how to set up a four-way two region grid where only one cluster in each region connects to an ICOS object store. One cloud pool, two accounts, and one container are available for a single vault inside an ICOS. Before setting up the cloud storage tier, your ICOS must be set up in your environment. For more information about setting up your ICOS, see Chapter 8, "Setting up an AWS Cloud Object Storage" on page 55.

Figure 10-6 on page 107 shows a four-way two region grid with one TS7700C in each region. In this example, cloud configuration settings are used only on the two TS7700C clusters, but the other two peer clusters must still have their Storage Group values configured correctly to use the cloud storage tier.

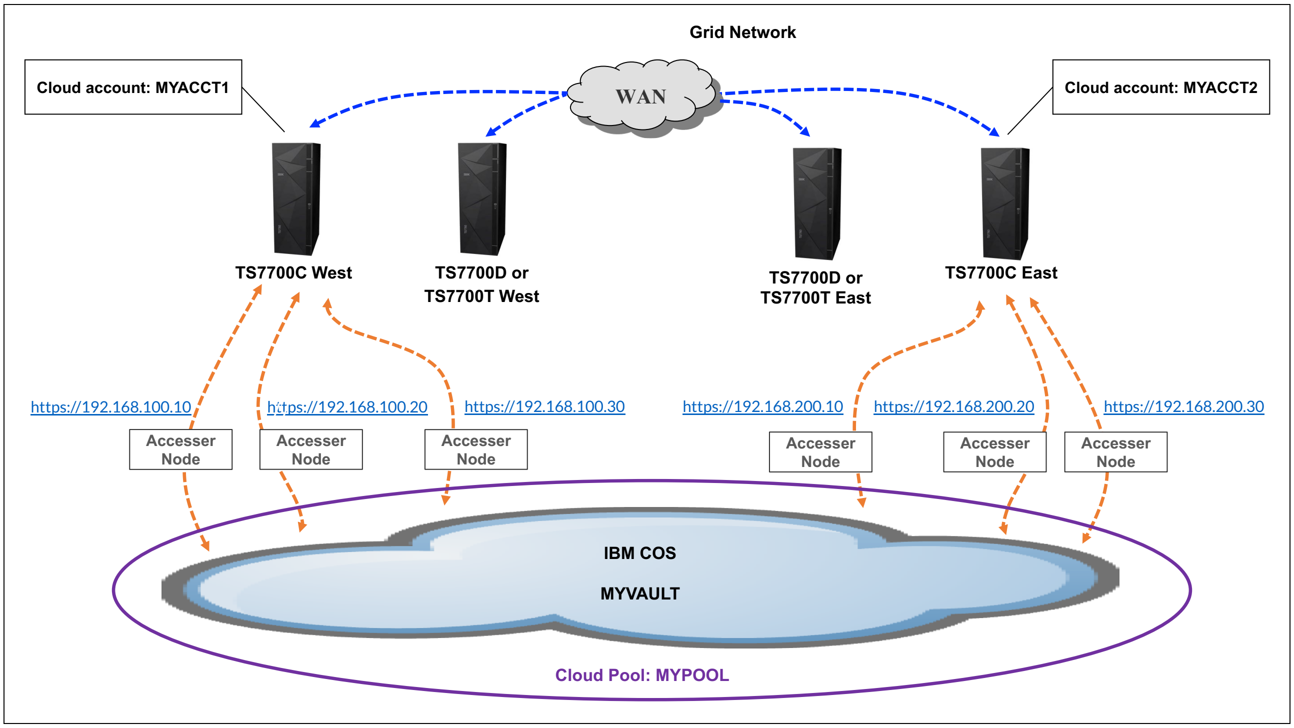


Figure 10-6 Four-way clusters

For example, you must create a Storage Group that also points to MYPOOL on non-TS7700C clusters and assign the Storage Group to logical tape volumes that ultimately end up in the cloud after replicating or remote mounting into a TS7700C cluster. If you do not create such a Storage Group on non-TS7700C clusters, any volume that is mounted by non-TS7700C clusters is not premigrated to MYPOOL on TS7700C clusters.

In Figure 10-6 on page 107, the two TS7700C clusters share a cloud pool (MYPOOL) to offload logical tape volumes to the cloud. The TS7700C cluster in the West region uses one cloud account (MYACCT1) to access the cloud pool, and the other TS7700C cluster in the East region uses another cloud account (MYACCT2) to access the same cloud pool.

MYVAULT is assigned to the cloud pool, and the following cloud URLs are used to access the vault (three URLs per region or one per available accessor):

- `https://192.168.100.10`
- `https://192.168.100.20`
- `https://192.168.100.30`
- `https://192.168.200.10`
- `https://192.168.200.20`
- `https://192.168.200.30`)

Thee cloud URLs (`https://192.168.100.10`, `https://192.168.100.20`, and `https://192.168.100.30`) must be associated with TS7700C in the West region. The other three cloud URLs (`https://192.168.200.10`, `https://192.168.200.20`, and `https://192.168.200.30`) must be associated with the TS7700C in the East region.

Each step of this process is described next. The first four steps must be completed once per grid by using either of the two TS7700C clusters. Step five requires a unique step per TS7760C cluster.

Creating a cloud pool

Complete the following steps:

1. On either TS7700C cluster, go to **Settings** →**Cloud Tier Settings** on the Management Interface (MI) and select **Cloud Pools**.
2. Click **Create Cloud Pool**.
3. Enter `MYPOOL` as the cloud pool's nickname.
4. Select **Standard Format** as the Cloud Data Format.
5. Click **OK**.

Creating a cloud account

Complete the following steps:

1. On either TS7700C cluster, click **Settings** →**Cloud Tier Settings** on MI and select **Cloud Accounts**.
2. Click **Create Cloud Account**.
3. Enter `MYACCT1` as the cloud account's nickname.
4. Select **IBM COS S3** as the account type.
5. Select a health check method (Periodic is recommended).
6. Enter the Access Key ID and Secret Access Key (provided by your ICOS Admin) of your cloud account that is used in the West region and click **OK**.
7. On either TS7700C cluster, create another cloud account (MYACCT2) using the Access Key ID and Secret Access Key pair that is used to access the vault from the East region.

Creating containers

Complete the following steps:

1. Ensure a vault (for example, MYVAULT) is created in your ICOS.
2. On either TS7700C cluster, click **Settings** →**Cloud Tier Settings** on the MI and select **Containers**.
3. Click **Create Container**.
4. Enter MYVAULT as the container name.
5. Select **MYPOOL** as the cloud pool.
6. Select **MYACCT1** as the cloud account.
7. Click **OK**.
8. Create another container with the same name and select **MYPOOL** as the cloud pool and use MYACCT2 as the cloud account.

When this process is completed, two containers are available: one for region West and one for region East.

Creating cloud URLs

Complete the following steps:

1. Ensure that an SSL certificate is uploaded to your TS7700 grid.

   For more information about uploading an SSL certificate, see Chapter 6, “SSL certificate” on page 29. If your cloud URL does not use the secure https protocol, you do not need to upload an SSL certificate.
2. On either TS7700C cluster, click **Settings** →**Cloud Tier Settings** on the MI and select **Containers**.
3. Right-click the **MYVAULT** container that is associated with MYACCT1 and select **Create Cloud URL**.
4. Enter `https://192.168.100.10` as a URL.
5. Select an SSL certificate alias for the certificate that you uploaded.
6. Click **OK**.
7. If you use the non-secure http protocol, enter `http://192.168.100.10` as a URL instead and leave the certificate alias blank.
8. Right-click the same container again and create the cloud URLs for `https://192.168.100.20` and then, a third time for `https://192.168.100.30`.
9. On either TS7760C cluster, right-click the **MYVAULT** container that is associated with MYACCT2 and create cloud URLs for `https://192.168.200.10`, `https://192.168.200.20`, and `https://192.168.200.30`.

When this process is completed, three URLs are defined under each of the two containers: three for region West and three for region East.

Creating cloud URL and cluster associations

Complete the following steps:

1. On the TS7700C cluster in the West region, click **Settings** →**Cloud Tier Settings** in its MI window (you must log in to this specific TS7700C cluster) and select **Containers**.
2. Expand the Cloud URLs you for the West region.

3. Right-click **https://192.168.100.10** and select **Create Cloud URL and Cluster association**.
4. Set **1** as a priority and click **OK**.
5. Create an association for the other two West region URLs (`https://192.168.100.20` and `https://192.168.100.30`).
6. Repeat these steps on the TS7700C cluster in the East region by associating it with the three accessor URLs for that region.
7. Log in to the TS7700C West cluster and set up an association with `https://192.168.200.10`, `https://192.168.200.20`, and `https://192.168.200.30`.

When this process is complete, the TS7700C cluster West cluster is associated with the three URLs for the West region. The other three URLs are associated with the TS7700C East region.

11

Disaster recovery principles

The discussion of TS7700C disaster recovery (DR) principles that is presented in this chapter is meant to supplement the information that is available in Chapter 5 Disaster Recovery of the IBM Redbooks publication *TS7700 Release 4.2 Guide*. It also adds considerations to disaster recovery when a Cloud Storage Tier is attached to a TS7700 Grid.

This chapter includes the following topics:

11.1 Tier to Cloud Considerations

With the introduction of a new cloud storage tier, your production cluster and DR cluster can be TS7760Cs where both clusters are connected to the same cloud object store. However, even if both are attached to the same cloud object store and the logical data for a production volume is in the cloud object store, the DR host (by way of the DR cluster) can access only that data if the copy policy on the production cluster sends a copy to the DR cluster and that copy completed replication to the DR cluster.

The DR cluster being attached to the same cloud object store as the production cluster does not allow it to access the data that is stored in the cloud object store by the production cluster. The best way to think about a cloud object store (as it relates to functionality from a DR perspective) is that it is synonymous with a tape-attached TS7700.

11.2 Cloud object store availability

An important aspect of data management with the TS7700C is that access to object stores in the cloud are available only to a cluster where the LVOL was resident in that cluster's TVC or replicated to that cluster across the grid.

In the case of replication, the timing of when the replication completes and the copy policies are selected is important. For example, copies on the deferred queue might not be complete at the point when a disaster occurs. Regardless of the presence of a copy of the data in the object store in the cloud, that copy becomes inaccessible from any cluster where the LVOL did not finish replication to that cluster.

If the data is critical, the copy policies must be set up with Run or (better yet) Sync on the DR cluster so that a copy of the LVOL is ensured to be placed in the DR cluster TVC. After that copy is replicated, the volume can then be migrated to object store in the cloud from either site and still be accessible from the DR cluster.

11.3 Required data for restoring the host environment

Volumes that contain data that is required to restore the host environment, such as DASD full volume backups of IPL required data, must be kept in resident partitions. Although backups of these volumes can be kept in the object store in the cloud, most current full volumes backups of the DASD pool normally are not good candidates to migrate to the object store in the cloud because of the recall time that is required to restore them.

Also, primary data (for example, HSM ML2 files), also cannot be good candidates to keep only in object stores on the cloud because the time that is required to recall such data can affect restoring the host to operational status.

11.4 Volume sizing

An important aspect of object store management is the consideration of multi-file volumes. When a volume is recalled from object stores, it must be recalled in its entirety. Even if only one file must be accessed, the entire logical tape volume must be recalled to the TVC.

Therefore, sizing volumes with multiple files is done carefully. Unless a volume contains files that all must be accessed, smaller logical volume sizes might be preferred.

11.5 Recovery time objectives

When a TS7700C is part of the disaster recovery plan, consider the amount of data in the object store in the cloud that is required to be recalled if a disaster occurs. The amount of data that is required and how quickly that data can be moved from the object store in the cloud back to the DR cluster factors heavily into the recovery time objectives. Any volumes that need to be immediately available to minimize the time it takes to return to operational status must be kept in resident partitions on the DR cluster.

11.6 Production activity and bandwidth

After the host system is recovered and normal operations resume, some data in the object store on the cloud might exist that must be recalled. The grid links are being shared between the object store access points and the other clusters in the grid. If the copy policies in the grid are replicating volumes between the remaining clusters while the object store recalls are ongoing, the potential for grid link degradation exists.

Consider the temporary use of copy policies that limit the number of copies being written across the grid links until all object store recalls are complete. Optionally, sizing can be done to ensure that bandwidth is available at the DR site to accommodate the object store retrieval from the cloud and the normal grid workload.

11.7 Redundancy in the cloud

Consideration must be made of the possibility of a failure that can affect the availability of the cloud. If the data that is stored in the cloud is critical to operations, you might want to replicate the cloud to multiple locations to reduce the chance that such an outage limits access to the data. For more information, see Chapter 2, “Container resiliency” on page 9.

11.8 Cost of object store retrieval

The policies of the cloud service provider dictate the costs that are associated with retrieving data from the object store in the cloud. The speed at which that data must be recalled and the amount of data is a factor in those costs. However, other factors can be important, such as the need for redundancy in the cloud and to where you are transferring the data.

12

Monitoring the TS7700C

In this chapter, we describe some of the tools that are available for monitoring your TS7700C activities.

This chapter includes the following topics:

12.1 TS7760 object name format

This section describes the object name format. The name is long as we envision many use cases of merges, joins, sharing, importing, exporting, etc. with the requirement that the object should never collide with any other TS7760 in the world. When looking in the object store, the objects created by the TS7760 will take the following form:

PREFIX/XXXX/COMPLIB/DISTLIB/SERIAL/VOLSER/INSERT/DATA/DATETIME

PREFIX	User provided prefix in Storage Group
XXXX	16 bit hexadecimal random value for object store hashing performance
COMPLIB	Five digit composite library ID of grid who created object
DISTLIB	Five digit distributed library ID of cluster who created object
SERIAL	Five character serial number of cluster who created object
VOLSER	Six character volume serial that is being saved as an object
INSERT	Token Insert Level
DATA	Token Data Level
DATETIME	YYYYMMDDHHMMSS UTC time of when object was created

Here are two examples of object names:

- GRD123/ba65/BA092/BA92A/H1233/CLD003/120/100/201710250526
- fossilman/0b31/BA099/BA99A/H9840/ZKM000/106/103/20180613102558

12.2 BVIR example

BVIR CLOUD VOLUME MAP can produce active logical volume lists that are premigrated to cloud. VOLSER, file size, object name, and so on, can be listed. You can get detailed cloud information for each volume by using this tool.

Sample output

Example 12-1 shows BVIR CLOUD VOLUME MAP output. The sample includes five logical volume records. Each record is 900 bytes.

Example 12-1 BVIR CLOUD VOLUME MAP sample output

```
VTS BULK VOLUME DATA REQUEST
CLOUD VOLUME MAP 0
09/07/2018 05:53:03 VERSION 01
S/N: H4022  LIB ID: D0020

VOLSER INSERT_VERSION      DATA_LEVEL          SYSPLEX_NAME SYSTEM_NAME
1E8675 84                  103                 IST7         IST7
1E8677 84                  103                 IST7         IST7
1K1662 91                  102                 IST7         IST7
1K1664 91                  102                 IST7         IST7
1K1666 91                  102                 IST7         IST7
1K1668 91                  102                 IST7         IST7
```

```
PROGRAM_NAME FILE_SIZE            CLOUD_ACCOUNT_ID    CLOUD_ACCOUNT_NICKNAME
GETPUT1B     3003008696           H40222018080306041 6 MKAC01
```

```
PROGRAM_NAME FILE_SIZE            CLOUD_ACCOUNT_ID    CLOUD_ACCOUNT_NICKNAME
GETPUT1B     3003008696           H402220180803060416 MKAC01
GETPUT1B     3003008696           H402220180803060416 MKAC01
GETPUT1B     3003008696           H402220180803060416 MKAC01
GETPUT1B     3003008696           H402220180803060416 MKAC01
GETPUT1B     3003008696           H402220180803060416 MKAC01
GETPUT1B     3003008696           H402220180803060416 MKAC01

ENCRYPTION_FLAG ENCRYPTION_KEY_LABEL1
0               NULL
0               NULL
0               NULL
0               NULL
0               NULL
0  NULL

ENCRYPTION_KEY_LABEL2
NULL
NULL
NULL
NULL
NULL
NULL

CLOUD_DATA_FORMAT DELETE_REASON DELETED_TIME
1                 0             1970-01-01-00.00.00.000000
1                 0             1970-01-01-00.00.00.000000
1                 0             1970-01-01-00.00.00.000000
1                 0             1970-01-01-00.00.00.000000
1                 0             1970-01-01-00.00.00.000000
1                 0             1970-01-01-00.00.00.000000

PREMIGRATED_TIME           INITIATOR CLOUD_POOL          CLOUD_POOL_NAME
2018-09-07-02.16.58.000000 0         H402220180803055327 MKPL01
2018-09-07-05.05.03.000000 0         H402220180803055327 MKPL01
2018-09-06-08.57.24.000000 0         H402220180803055327 MKPL01
2018-09-07-01.41.44.000000 0         H402220180803055327 MKPL01
2018-09-07-04.38.25.000000 0         H402220180803055327 MKPL01
2018-09-07-05.16.25.000000 0         H402220180803055327 MKPL01

CLOUD_PREMIG_RANK COMPOSITE_STATE CLUSTER0_STATE COMP_CLU_MASK_REQS_UPD
1                 5376            5376           0
1                 5376            5376           0
1                 5376            5376           0
1                 5376            5376           0
1                 5376            5376           0
1                 5376            5376           0

OBJECT_NAME
MKCL0/2751/C0002/D0020/H4022/1E8675/84/103/20180907020807
MKCL0/6da5/C0002/D0020/H4022/1E8677/84/103/20180907044011
MKCL0/004a/C0002/D0020/H4022/1K1662/91/102/20180906084903
MKCL0/5416/C0002/D0020/H4022/1K1664/91/102/20180907013319
MKCL0/027b/C0002/D0020/H4022/1K1666/91/102/20180907043007
MKCL0/308d/C0002/D0020/H4022/1K1668/91/102/20180907050801
```

```
CONTAINER_NAME
mkcn02
mkcn02
mkcn02
mkcn02
mkcn02
mkcn02
```

Sample JCL

Example 12-2 shows sample JCL to run BVIR CLOUD VOLUME MAP.

Example 12-2 BVIR CLOUD VOLUME MAP sample JCL

```
//VTSBVIR  JOB  MSGLEVEL=(1,1),MSGCLASS=X,CLASS=A,NOTIFY=&SYSUID,
//         REGION=0M
//STEP1     EXEC PGM=IEBGENER
//SYSPRINT  DD SYSOUT=*
//SYSUT1    DD *
VTS BULK VOLUME DATA REQUEST
CLOUD VOLUME MAP
/*
//SYSUT2    DD DSN=BVIR.CLOUD.VOLUME.MAP,DISP=(,KEEP),UNIT=GRIDLIB2,
//          LABEL=(1,SL),MGMTCLAS=MCRNN,
//          LRECL=80,BLKSIZE=80,TRTCH=NOCOMP
//SYSIN     DD DUMMY
/*
//STEP2     EXEC PGM=IEBGENER
//SYSPRINT  DD SYSOUT=*
//SYSUT1    DD DSN=BVIR.CLOUD.VOLUME.MAP,DISP=OLD,UNIT=3490,
//          VOL=(,,REF=*.STEP1.SYSUT2),LRECL=900,RECFM=F,BLKSIZE=900
//SYSUT2    DD DSN=BVIR.CLOUD.VOLUME.MAP.LIST,DISP=(,CATLG),
//          SPACE=(CYL,(10,10),RLSE)
//SYSIN     DD DUMMY
/*
```

12.3 VEHSTATS

This section describes the VEHSTATS statistics report to understand TS7700 performance.

VEHSTATS and the following TS7700 90 Day, 1 week, and 24 Hour Performance Evaluation Spreadsheets are not changed at R4.2 GA timing. You can use these tools at the latest version, even if your TS7700 configuration includes cloud attached clusters.

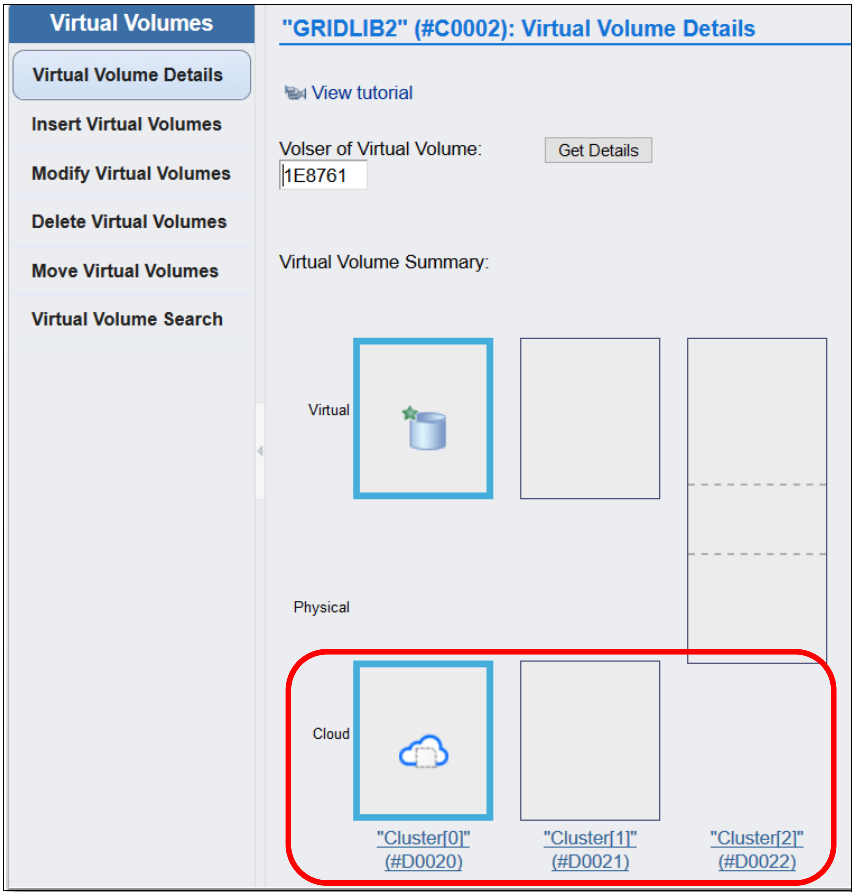
Until a future enhancement is made available, be aware that cloud-related statistics are reported within physical tape that is attached to a cluster’s related fields. Cache hit, cache miss, premig, migrated, partition, or any other field that is related to Tape Attach also applies to cloud.

12.4 MI windows

This section describes Management Interface (MI) windows that are related to cloud attach.

Virtual Volumes Details

You can display virtual volume details, including cloud-related information, as shown in Figure 12-1 on page 119, Figure 12-2 on page 120, and Figure 12-3 on page 120.

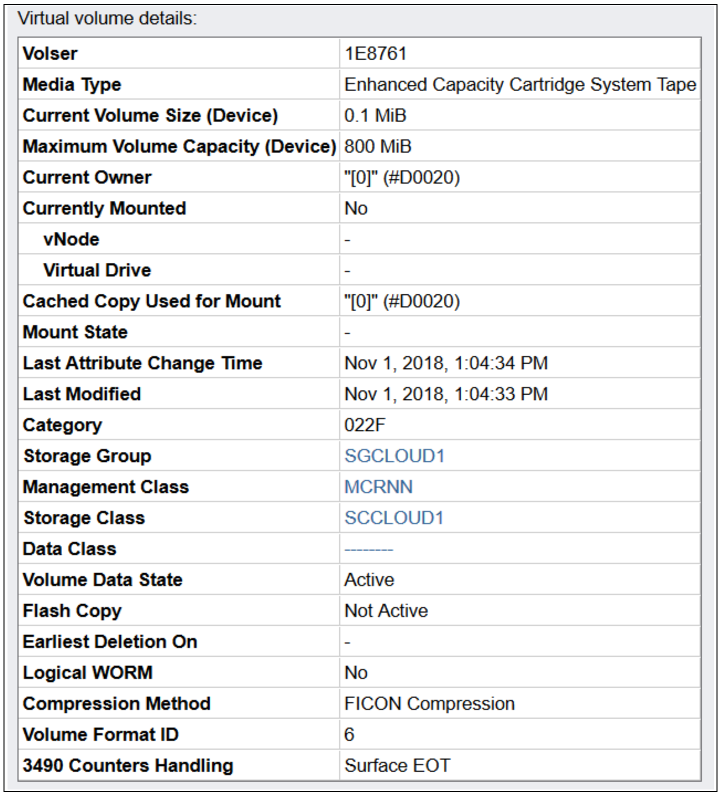


"GRIDLIB2" (#C0002): Virtual Volume Details

Volser of Virtual Volume: 1E8761

Virtual Volume Summary:

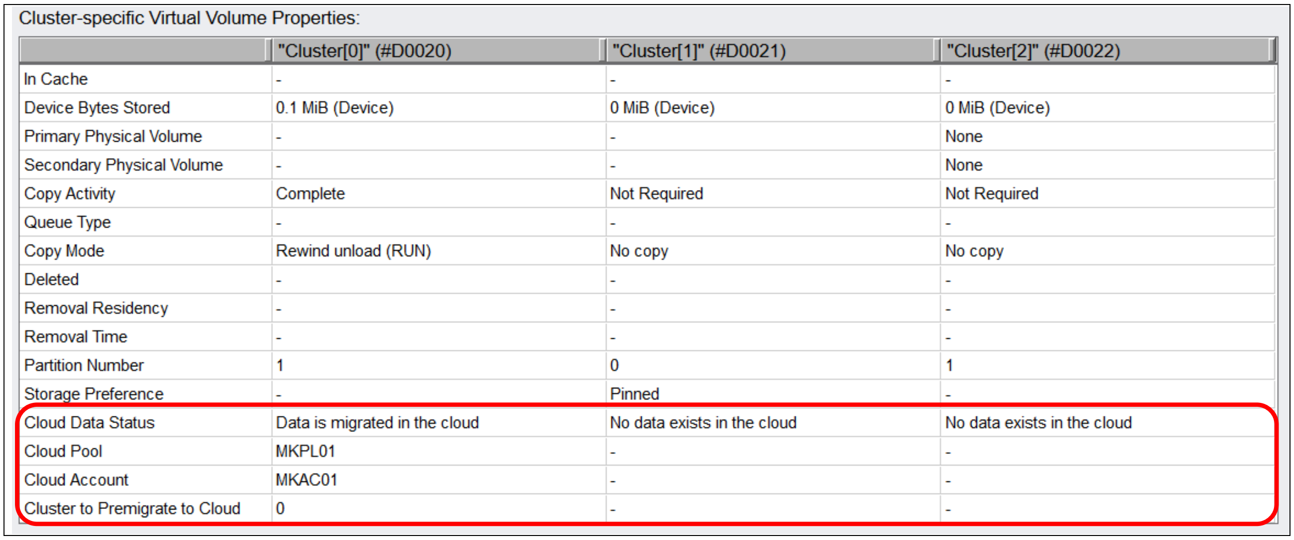
Figure 12-1 Virtual Volume Details, Part 1



Virtual volume details:

Volser	1E8761
Media Type	Enhanced Capacity Cartridge System Tape
Current Volume Size (Device)	0.1 MiB
Maximum Volume Capacity (Device)	800 MiB
Current Owner	"[0]" (#D0020)
Currently Mounted	No
vNode	-
Virtual Drive	-
Cached Copy Used for Mount	"[0]" (#D0020)
Mount State	-
Last Attribute Change Time	Nov 1, 2018, 1:04:34 PM
Last Modified	Nov 1, 2018, 1:04:33 PM
Category	022F
Storage Group	SGCLOUD1
Management Class	MCRNN
Storage Class	SCCLOUD1
Data Class	--------
Volume Data State	Active
Flash Copy	Not Active
Earliest Deletion On	-
Logical WORM	No
Compression Method	FICON Compression
Volume Format ID	6
3490 Counters Handling	Surface EOT

Figure 12-2 Virtual Volume Details, part 2



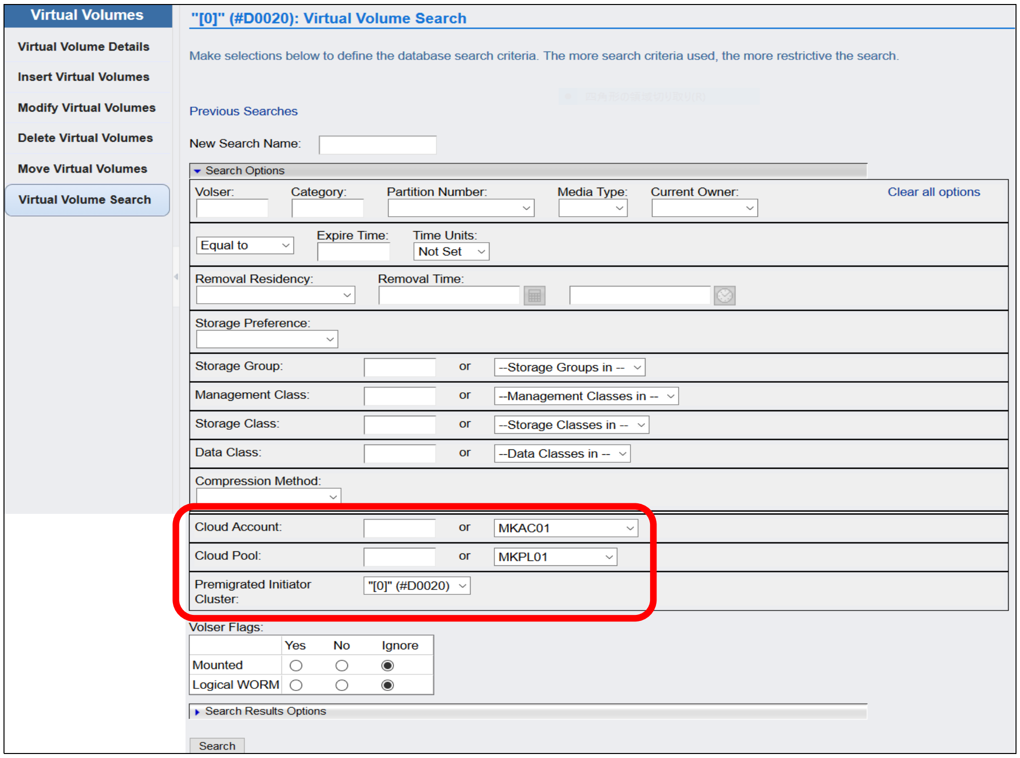
Cluster-specific Virtual Volume Properties:

	"Cluster[0]" (#D0020)	"Cluster[1]" (#D0021)	"Cluster[2]" (#D0022)
In Cache	-	-	-
Device Bytes Stored	0.1 MiB (Device)	0 MiB (Device)	0 MiB (Device)
Primary Physical Volume	-	-	None
Secondary Physical Volume	-	-	None
Copy Activity	Complete	Not Required	Not Required
Queue Type	-	-	-
Copy Mode	Rewind unload (RUN)	No copy	No copy
Deleted	-	-	-
Removal Residency	-	-	-
Removal Time	-	-	-
Partition Number	1	0	1
Storage Preference	-	Pinned	-
Cloud Data Status	Data is migrated in the cloud	No data exists in the cloud	No data exists in the cloud
Cloud Pool	MKPL01	-	-
Cloud Account	MKAC01	-	-
Cluster to Premigrate to Cloud	0	-	-

Figure 12-3 Virtual Volume Details, part 3

Virtual Volume Search

You can search virtual volumes by specifying filters, including cloud-related criteria, as shown in Figure 12-4 and Figure 12-5.



"[0]" (#D0020): Virtual Volume Search

Make selections below to define the database search criteria. The more search criteria used, the more restrictive the search.

New Search Name:

Volser: Category: Partition Number: Media Type: Current Owner:

Equal to | Expire Time: | Time Units: Not Set

Removal Residency: Removal Time:

Storage Preference:

Storage Group: or --Storage Groups in --

Management Class: or --Management Classes in --

Storage Class: or --Storage Classes in --

Data Class: or --Data Classes in --

Compression Method:

Cloud Account: or MKAC01

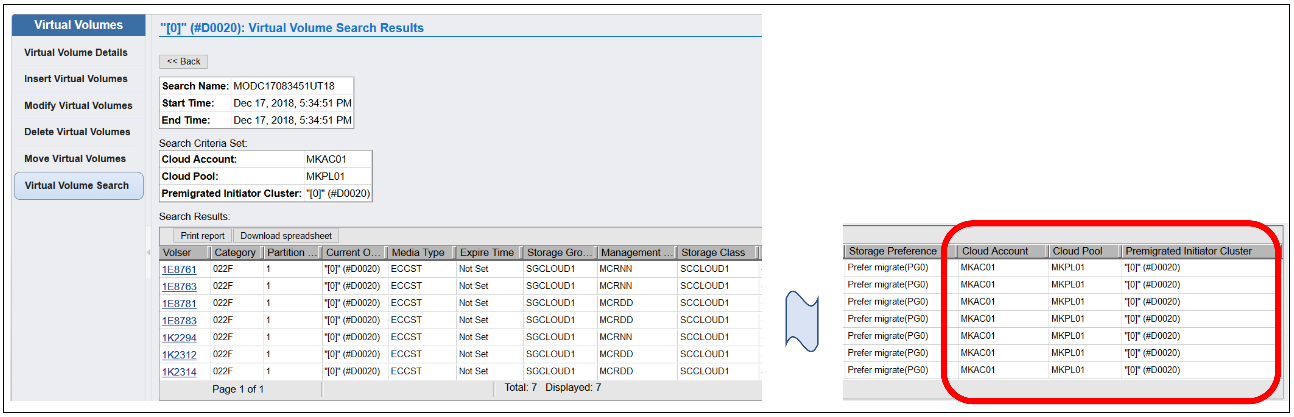
Cloud Pool: or MKPL01

Premigrated Initiator Cluster: "[0]" (#D0020)

Volser Flags:

	Yes	No	Ignore
Mounted	○	○	●
Logical WORM	○	○	●

Figure 12-4 Specifying filters to search virtual volumes



"[0]" (#D0020): Virtual Volume Search Results

Search Name:	MODC17083451UT18
Start Time:	Dec 17, 2018, 5:34:51 PM
End Time:	Dec 17, 2018, 5:34:51 PM

Search Criteria Set:

Cloud Account:	MKAC01
Cloud Pool:	MKPL01
Premigrated Initiator Cluster:	"[0]" (#D0020)

Search Results:

Volser	Category	Partition ...	Current O...	Media Type	Expire Time	Storage Gro...	Management ...	Storage Class	Storage Preference	Cloud Account	Cloud Pool	Premigrated Initiator Cluster
1E8761	022F	1	"[0]" (#D0020)	ECCST	Not Set	SGCLOUD1	MCRNN	SCCLOUD1	Prefer migrate(PG0)	MKAC01	MKPL01	"[0]" (#D0020)
1E8763	022F	1	"[0]" (#D0020)	ECCST	Not Set	SGCLOUD1	MCRNN	SCCLOUD1	Prefer migrate(PG0)	MKAC01	MKPL01	"[0]" (#D0020)
1E8781	022F	1	"[0]" (#D0020)	ECCST	Not Set	SGCLOUD1	MCRDD	SCCLOUD1	Prefer migrate(PG0)	MKAC01	MKPL01	"[0]" (#D0020)
1E8783	022F	1	"[0]" (#D0020)	ECCST	Not Set	SGCLOUD1	MCRDD	SCCLOUD1	Prefer migrate(PG0)	MKAC01	MKPL01	"[0]" (#D0020)
1K2294	022F	1	"[0]" (#D0020)	ECCST	Not Set	SGCLOUD1	MCRNN	SCCLOUD1	Prefer migrate(PG0)	MKAC01	MKPL01	"[0]" (#D0020)
1K2312	022F	1	"[0]" (#D0020)	ECCST	Not Set	SGCLOUD1	MCRDD	SCCLOUD1	Prefer migrate(PG0)	MKAC01	MKPL01	"[0]" (#D0020)
1K2314	022F	1	"[0]" (#D0020)	ECCST	Not Set	SGCLOUD1	MCRDD	SCCLOUD1	Prefer migrate(PG0)	MKAC01	MKPL01	"[0]" (#D0020)

Page 1 of 1 Total: 7 Displayed: 7

Figure 12-5 Search virtual volumes result sample

12.5 LI REQ commands

This section summarizes the LI REQ commands that are used to show cloud-related information for each logical volume.

LI REQ STATUS command with GRLNKACT parameter

The `LI REQ STATUS GRLNKACT` command response has been enhanced to include information about grid link activity to the cloud. In response to this request the grid will provide point in time details about all of the grid link activity for all configured clusters in the grid. If any of the clusters are cloud attached, cloud activity across the links will also be provided. The information is summed into 15 second intervals and the next interval starting after the command is received is returned to the issuer.

Refer to 16.2.5, “LI REQ STATUS command with GRLNKACT parameter” on page 154 for additional detail about the GRLNKACT parameter.

LI REQ LVOL command with new INFO parameter

The standard `LI REQ LOVL` command was enhanced to include more information. The `INFO` parameter must be included to receive the newer content.

The previous version continues to function, but it no longer is planned for improvement because it does include any space for future enhancements.

The new `INFO` version now includes cloud-related attributes. The `CD` field in the last section stands for “Cloud Data” and indicates the number of cloud copies that specific cluster is aware of that were successfully premigrated to an object store. Only when this value is one or higher can that cluster access the logical volume within the object store.

Refer to 16.2.1, “LIBRARY REQUEST,composite_library,LVOL,volser,INFO” on page 147 for additional detail about the INFO parameter.

LI REQ LVOL command with new CLDINFO parameter

This command provides the logical volume status on cloud (i.e. object data). It indicates if the logical volume is already premigrated to the cloud and in which clusters in the Grid the data is accessible from.

Refer to 16.2.2, “LIBRARY REQUEST,composite_library,LVOL,volser,CLDINFO” on page 148 for additional detail about the CLDINFO parameter.

Cloud-related operator messages

Cloud-related operator messages can be monitored on the z/OS host by filtering CBR3750I.

Refer to 16.2.6, “Cloud-related operator messages” on page 156 for the table of message IDs and descriptions.

12.6 Capacity monitoring cloud storage

The capacity of your object store must be monitored because the TS7700C cannot determine what free space is available within the object store. This section describes capacity monitoring for cloud Object Storage.

12.6.1 Capacity monitoring on IBM Cloud Object Storage

Capacity monitoring is required to prevent the cloud Object Storage from becoming full on IBM Cloud Object Storage on-premises system.

IBM Cloud Object Storage provides the monitor function for a capacity utilization on the Manager Web Interface through the IBM Cloud Object Storage management network.

For more information, see IBM Knowledge Center.

12.6.2 Capacity monitoring on AWS S3

Unlike IBM COS on-premises system, AWS S3 provides unlimited capacity. However, it is still advised to monitor capacity usage, the amount of data that is transferred for recalls (not for premigration), the number of recall requests, and any cross-regional replication (if enabled) because all of these factors can influence the cost of the object store storage.

AWS S3 provides usage details on its Billing and Cost Management console dashboard and the CloudWatch monitoring tool.

For more information about pricing and guides, see the AWS S3 home page.

13

Migration and upgrade considerations

This chapter describes the considerations for data migration and upgrading TS7700 to TS7700C.

This chapter includes the following topics:

- 13.1, “Data migration considerations” on page 126
- 13.2, “Upgrade existing TS7700 to TS7700C considerations” on page 130

13.1 Data migration considerations

This section describes specific considerations for migrating data to the cloud storage tier.

The following scenarios are described in this section:

- Migrating data from the Resident-Only partition (CP0) of a TS7700C cluster
- Migrating data from existing TS7700 in the Grid configuration

13.1.1 Migrating data from the Resident-Only partition

The TS7700C and TS7700T support cache partitions. Cache partitions consist of one resident-only-partition (CP0) and 1 - 7 cache partitions (CP1-CP7) or CPx partitions. All CPx partitions automatically migrate volumes to the cloud storage tier, but the CP0 partition does not include direct access to the cloud storage tier. Therefore, volumes that are in the CP0 partition do not automatically move to the cloud storage tier without intervention.

The process that is used to migrate volumes that are in CP0 to a cloud storage tier include the following overall steps:

1. Change the assigned storage class partition assignment to move volumes to CPx (see Figure 13-1).
2. Change the assigned storage group to specify a target cloud pool to migrate volumes to the cloud storage tier.
3. (Optional) Apply the storage class or storage group if a construct name change is required.
4. Migrate volumes to the cloud by assigning the new constructs.

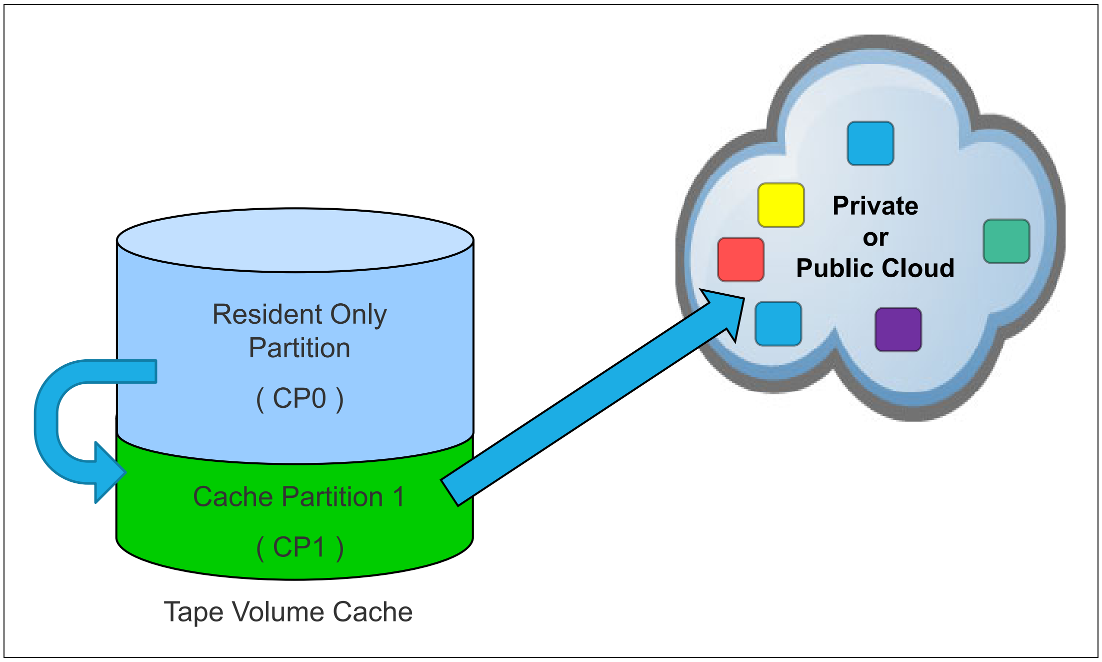


Figure 13-1 Partition Assignment change

Constructs settings

To migrate the volumes to the cloud storage tier, you must ensure that the assigned constructs for the volumes are set up correctly. This process can be done by modifying the assigned construct attributes or by creating one or more constructs and assigning these constructs to the volumes that must be migrated to the cloud.

Storage Class

Storage Class allows you to determine which cache partition the volume targets before migrating to the cloud. You must assign a cache partition CPx (CP1 - CP7) because volumes in the CP0 partition remain in disk cache and do not migrate to the cloud.

The Storage Class is also used to assign the migration preference group. This determines whether the TS7700C attempts to retain the volume in disk cache or whether it is flushed from disk cache when a copy to the cloud completes. This preference is accepted after the volume is moved into a CPx partition.

Storage Group

Storage Group allows you to determine the cloud pool that the volumes migrate to within the cloud.

Note: You must specify the same cloud pool for a specific Storage Group on all TS7700s in the grid configuration, even if the cluster is not cloud enabled.

Assigning the new constructs settings to a volume

You can apply new construct rules by using one of the following methods:

- Modify the constructs that are assigned to the volumes so that the new rules can apply from that point forward.
- Create constructs and use the `LMPOLICY` command to assign them to the volumes.

Note: By using the Management Interface (MI) Modify Virtual Volume window, you can assign new constructs to a volume. This function is primarily intended for non-z/OS system and it updates the constructs without informing any connected host (including z/OS). Because Storage Group is recorded in VOLCAT and DFSMSrmm CDS on z/OS, a best practice is to use the `LMPOLICY` command to update the constructs.

Existing volumes accepting new constructs

Construct changes do not automatically apply to volumes without an action first taking place. The primary action is a host-started mount/demount of a logical volume. If the logical volume's assigned cloud pool is already assigned when it was last mounted or created, the `PARTRFSH` command can be used to have the new partition CPx location be accepted.

In either case, the volume is moved to a CPx partition, premigrated to the storage cloud tier and then, migrated depending on the storage class-assigned preference group.

You can use the PRESTAGE tool in IBM Tape Tools to request mount/demount across a series of volumes. The PRESTAGE program from the TAPETOOL FTP site can be used to request mount/demount processing in an efficient way.

For more information about the TAPETOOLs, see this web page.

Note: Only mount/demount requests can update the SG `cloud pool` setting of a volume. The `PARTRFSH` command can change the partition assignment of a volume, but it cannot update the cloud pool assignment. If the intended use case is to retain data in CP0 until you determine it should be manually moved to the cloud by using `PARTRFSH`, ensure that your cloud pool is always assigned for all storage groups in the grid. That is, ensure that all storage group definitions across all data that might eventually end up in the cloud have a storage pool assigned, even if it is in a non-cloud TS7700 or a CP0 partition. This configuration allows a future move to CPx to accept the previously applied cloud pool.

Plan the movement carefully. All data that is moved from CP0 to a CPx partition is added immediately to the premigration queue. Moving too much data concurrently can fill up the premigration queue and can lead to host I/O throttling for any inbound host or copy workload also targeting CPx partitions.

13.1.2 Migrating data from TS7700 in the grid configuration through replication

To migrate data to the cloud through a cloud attached peer, you must first replicate volumes from a TS7700 or TS7700T cluster to a TS7700C cluster and second target a CPx partition in the TS7700C cluster (see Figure 13-2).

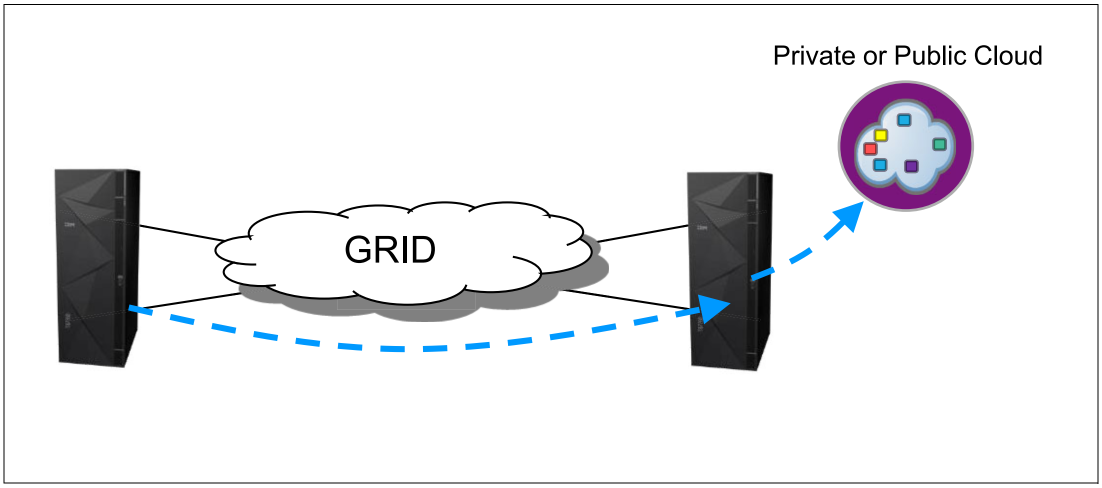


Figure 13-2 Copy the volumes to TS7700C

Complete the following steps to migrate volumes from a TS7700 or TS7700T cluster to a TS7700C cluster:

1. Change the assigned management class at one or more clusters to specify a copy consistency point for the TS7700C cluster.
2. Change the assigned storage class in the TS7700C cluster to specify a CPx partition that is used at the target TS7700C cluster.
3. Change the assigned storage group within all clusters in the grid to specify a cloud pool to migrate to for volumes targeting the TS7700C CPx partition.
4. (Optional) Apply the management class, storage class, or storage group if a construct name change is required.
5. Migrate volumes to the cloud by assigning the new constructs.

Constructs settings

To migrate the volumes to the cloud storage tier, you must assign constructs to the volumes. The following constructs must be set to migrate to the cloud:

- Management Class

  The Management Class determines the copy consistency point policy of the grid or which clusters receive a copy. You must specify a copy policy value that places a copy of the volume on the TS7700C. The TS7700C copy is in addition to any peer copies or other TS7700C clusters that also receive a copy.

- Storage Class

  Storage Class allows you to determine which cache partition the volume targets in the TS7700C cluster before migrating to the cloud. You must assign a cache partition CPx (CP1 through CP7) because volumes in the CP0 partition remain in disk cache and not migrate to the cloud.

  The Storage Class is also used to determine the migration preference group, whether the TS7700C attempts to retain the volume in disk cache by using a least recently used algorithm, or whether it is flushed from disk cache when a copy to the cloud completes. This preference is accepted after the volume is replicated into a CPx partition.

- Storage Group

  Storage Group allows you to determine to which cloud pool the volume migrates.

  > **Note:** You must specify the same cloud pool for a Storage Group on all TS7700s in the grid configuration, even if the cluster is not cloud enabled.
  >
  > Review the `LI REQ SETTING COPYFSC` value before completing this operation. If `DISABLED`, the storage class preference group that is defined within the TS7700C cluster is ignored.

Assigning the new constructs settings to a volume

You can apply new construct rules by using one of the following methods:

- Modify the constructs that are assigned to the volumes so that the new rules can apply from that point forward.
- Create constructs and use the z/OS `LMPOLICY` command to assign them to a set of volumes.

> **Note:** By using the management Interface (MI) Modify Virtual Volume window, you can assign new constructs to a volume. This function is primarily intended for non-z/OS system and it cannot reflect any change to host system (include z/OS). Because Storage Group is recorded in VOLCAT and DFSMSrmm CDS on z/OS, a best practice is to use LMPOLICY to update the constructs.

Existing volumes accepting the new constructs

Construct changes do not automatically apply to volumes without an action first taking place. The primary action is a host-started mount/demount of a logical volume.

If the logical volume’s assigned cloud pool is already assigned when it was last mounted or created, the `COPYRFSH` command can be used to have the new partition CPx location be accepted after the copy process completes.

In either case, the volume is replicated to the TS7700C cluster that is targeting the CPx partition, premigrated to the storage cloud tier, and then, migrated depending on the storage class that is assigned preference group.

You can use the PRESTAGE tool in IBM Tape Tools to request mount/demount across a series of volumes. The PRESTAGE program from the TAPETOOL FTP site can be used to request mount/demount processing in an efficient way.

For more information about the TAPETOOLs, see this web page.

Note: Only mount/demount request can update the SG `cloud pool` setting of a volume. The `COPYRFSH` command can change the replication assignment and target partition assignment of a volume, but it cannot update the cloud pool assignment. If the intended use case is to manually replicate data from one cluster to a TS7700C cluster after it is determined that it should be moved manually to the cloud by using `COPYRFSH`, ensure that your cloud pool is always assigned for all storage groups in the grid. That is, ensure that all storage group definitions across all data that might eventually end up in the cloud have a storage pool assigned, even if it is in a non-cloud TS7700 or if it is in a CP0 partition. This configuration allows a future move to CPx by `PARTRFSH` or `COPYRFSH` to accept the previously applied cloud pool.

Plan the movement carefully. All data that is moved from a peer cluster to the TS7700C CPx partition is added immediately to the premigration queue. Moving too much data concurrently might fill up the premigration queue and can lead to host I/O throttling for any inbound host or copy workload that also is targeting the TS7700C CPx partitions.

13.2 Upgrade existing TS7700 to TS7700C considerations

This section describes specific considerations for upgrading a TS7700 to a TS7700C.

Prerequisites and installation work

The prerequisites and installation work of updating cloud enable function are the same as for the initial installation. For more information, see Chapter 5, “TS7760C planning considerations” on page 25 and Chapter 9, “Configuring TS7700 for cloud storage tier” on page 77.

Cache partitions

In addition to introducing a cloud tier and the cloud tier configuration panels, the TS7700 to TS7700C upgrade process results in the TS7700C cluster having a predefined CPx partition that is 3 TB. This partition initially is empty because all data within the TS7700 cluster before the upgrade is allocated to the CP0 or resident-only partition. The initial size of the CPx partition can be changed and new CPx partitions can be defined after the upgrade is complete (see Figure 13-3).

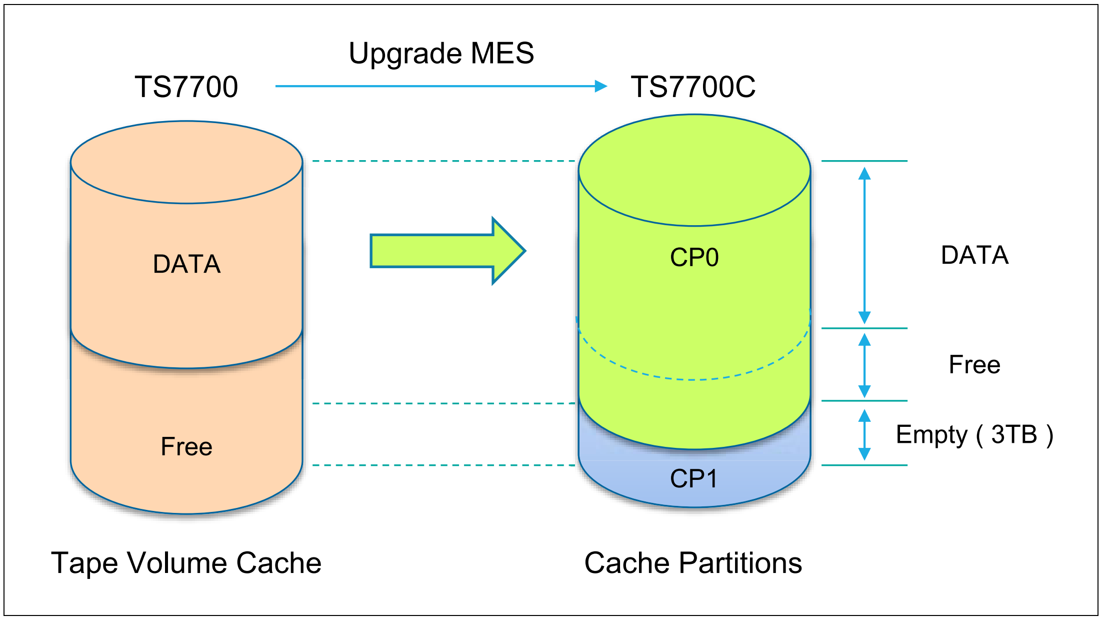


Figure 13-3 Cache Partitions

The CP1 size can be altered while the TS7700C is online. CPx partitions also can be created.

Cloud tier settings

After the cloud tier upgrade process is completed, you must configure the cloud tier settings. The settings are the same as for the initial setup. For more information, see Chapter 9, “Configuring TS7700 for cloud storage tier” on page 77.

After the cloud configuration is completed, you can move data within the CP0 partition to a CPx partition, as described in 13.1.1, “Migrating data from the Resident-Only partition” on page 126.

14

Troubleshooting

This chapter describes different troubleshooting concepts that you can use to help analyze potential problems that might occur while the storage cloud tier function is used in the TS7700C.

This chapter includes the following topics:

14.1 Network firewall problems

A TS7760C communicates with cloud Object Storage through the GRID network. Your grid network firewall must allow communications on port 443 when using a secure HTTPS connection to IBM COS or AWS S3. If you are using a standard HTTP connection to IBM COS, port 80 must be open.

14.2 DNS and JSON settings for AWS S3

In this section we describe the DNS server and AWS JSON file settings for AWS S3.

14.2.1 DNS Server

A DNS server is required when AWS S3 is used. It is not required for IBM COS. For AWS S3, the TS7760C requires a DNS server to resolve the AWS host names through the customer network. This DNS server must exist within the customer internal network, or the same network that is used for services, such as SNMP, ISKLM, MI, SYSLOG, and other customer provided services.

The DNS server resolves a URL, such as `https://mybucket.s3.amazonaws.com` into an IPv4 IP address. The TS7700C then routes the connection through the grid network to the DNS-provided IP address. Therefore, the DNS server must resolve AWS public addresses.

14.2.2 AWS JSON file

The TS7760C must set up internal routing and firewall tables to communicate with all possible AWS addresses. The TS7760C uses an AWS-provided JSON file that contains all possible IP addresses that are used by AWS services. During the first Create Cloud URL and Cluster Association operation on a cluster, the TS7760C attempts to download the latest AWS JSON file through the customer internal network.

If the DNS server is operational and the customer network is also attached to the internet, the latest JSON download is successful. If it is unsuccessful (which is likely), the TS7760C uses an internal JSON file to set up the routing and firewall tables to communicate over the grid network.

This initial JSON seed file is included in the TS7760C firmware and can be outdated. Therefore, the TS7760C attempts to download the latest version over the grid network after the JSON seed file is used.

Assuming the DNS server is set up correctly and the DNS provided AWS IP address for the JSON file is in the initial JSON seed table, the latest JSON file is downloaded through the grid network and used to update the routing tables and firewall. From this point forward, the TS7760C checks periodically and downloads a copy of the latest JSON file through the GRID network.

A rare chance exists that the persistent JSON seed file does not contain the IP address the DNS server provided for the JSON file location. IBM Support must be involved to help provide a later JSON file manually if this issue occurs.

TS7760C can access AWS S3 Object Storage through the GRID network, which must be connected to the internet.

Figure 14-1 shows connections between TS7760C, DNS server in the Customer network, and AWS.

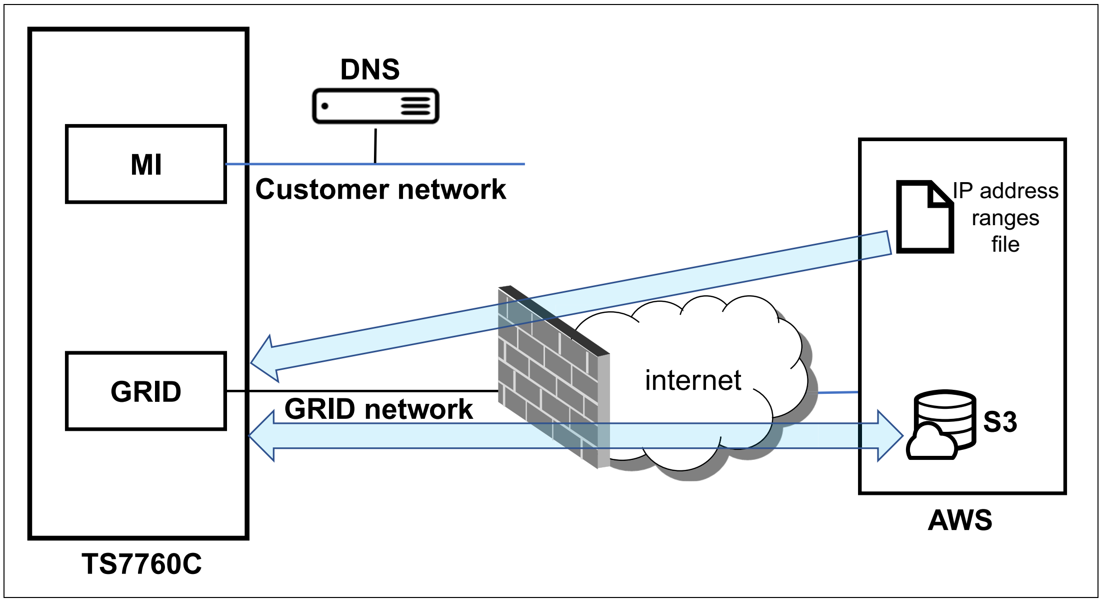


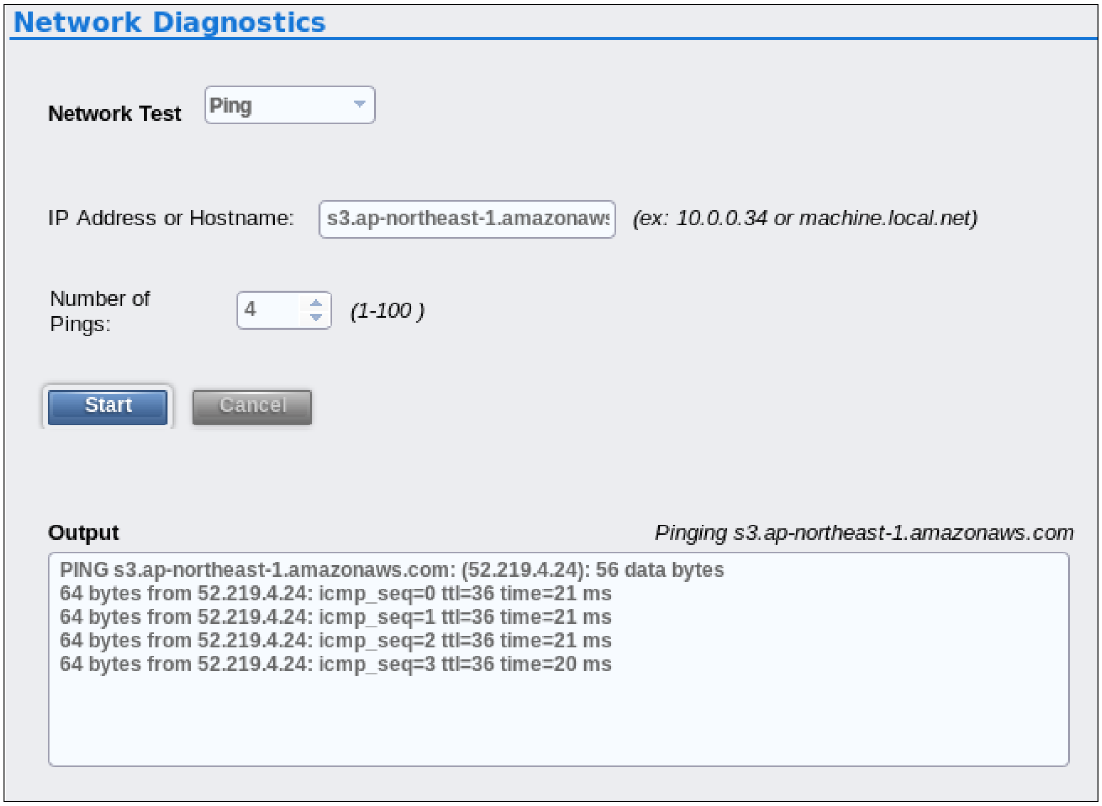
Figure 14-1 TS7760C and AWS network communication

To check the communications from the TS7760C to the AWS object store network, you can use the Network Test ping or trace route diagnostic function from the MI menu. Select **Service ICON →Network Diagnostic**.

The following example IP address is used:

```
s3.ap-northeast-1.amazonaws.com
```

A sample ping window is shown in Figure 14-2.



Network Test: Ping

IP Address or Hostname: s3.ap-northeast-1.amazonaws (ex: 10.0.0.34 or machine.local.net)

Number of Pings: 4 (1-100)

Output

Pinging s3.ap-northeast-1.amazonaws.com

```
PING s3.ap-northeast-1.amazonaws.com: (52.219.4.24): 56 data bytes
64 bytes from 52.219.4.24: icmp_seq=0 ttl=36 time=21 ms
64 bytes from 52.219.4.24: icmp_seq=1 ttl=36 time=21 ms
64 bytes from 52.219.4.24: icmp_seq=2 ttl=36 time=21 ms
64 bytes from 52.219.4.24: icmp_seq=3 ttl=36 time=20 ms
```

Figure 14-2 Ping to AWS S3's host name from Network Diagnostics

If the DNS server or JSON file setup was unsuccessful, the ping to such an external s3 based address fails.

14.3 Cloud service problems

This section describes problems that are related to a cloud Object Storage service.

14.3.1 Did your cloud SSL certificate expire?

When you use the HTTPS protocol with the IBM COS, a valid trust server certificate is required for SSL/TLS. If the certificate expired, you cannot access the IBM COS and the health monitor (if enabled for the Cloud Account) detects an error and issues the event OP0880.

14.3.2 Did your cloud credential expire or is no longer valid?

If your access key or the valid secret access key expired or is no longer valid, you cannot access the cloud and the health monitor (if enabled for the Cloud Account) detects an error and issues the event OP0838.

14.3.3 Is your Object Storage receiving heavy requests from other devices?

If your Object Storage is shared by the TS7760C with other devices, heavy requests for the Object Storage can affect performance.

Premigration throughput to the Object Storage is slower and the premigration-queue is longer. If it exceeds the premigration throttling threshold, host write throttling occurs and host write performance is affected and throttled down.

To monitor, you can use the MI to check health status on the Cluster Summary window and check throttling status on Monitor-Performance window.

In VEHSTATS, the premigration statistics and host write throttling statistics history are available for review. Those reports are the same as a TS7700 with tape drives attached.

You can also use the **LI REQ GRLNKACT** command to analyze 15-second periods of cloud throughput.

14.3.4 Is your grid network receiving heavy replication throughput?

Because your Object Storage is shared by the TS7760C with the grid network traffic, heavy replication and remote mount activity can slow the maximum performance to the object store.

You can also use the **LI REQ GRLNKACT** command to analyze 15-second periods of cloud throughput to see how the total network throughput is being shared among grid and cloud activity.

14.3.5 Is your object store full?

If your storage becomes full, you cannot add data to the object store. A health monitor detects the error and issues the event OP0882. It is recommended that you monitor your object store’s available capacity for the TS7760C to ensure that a full condition is not reached. Because the TS7760C cannot determine the object store’s available capacity, the monitoring must be done by using other methods.

14.3.6 Time difference between TS7760C and Object Storage is greater than 10 minutes

The time on the TS7760C and the cloud Object Storage must be synchronized. If the time difference between the TS7760C and IBM COS is greater than 10 minutes, a health monitor detects the error and issues the event OP0866. Use time servers within your TS7760C and IBM COS configuration to ensure that the times are synchronized.

14.4 Cloud or Grid network failures

This section describes failure warnings that can surface if the TS7760C cannot communicate with one or more provided object store URLs. Depending on the scope, the failure might lead to cloud access failure.

The following error messages are issued for various network-related failures:

```
CBR3750I Message from library GRIDCL20: OP0831 The Transparent Cloud
Tiering service is unreachable: MKAC01. cloud account (mkcn01),
container (auto-generated S3 URL), url (). Severity impact: SERIOUS.
CBR3762E Library GRIDCL20 intervention required.
CBR3786E VTS operations degraded in library GRIDCL20.
CBR3786E VTS operations degraded in library GRIDLIB2.
CBR3750I Message from library GRIDCL20: OP0728 Ping test to address
10.32.1.1 has an excessive packet loss. Has been in this condition for up to 10
minutes.. Severity impact: WARNING.
CBR3750I Message from library GRIDCL20: OP0541 The link to gateway IP
10.32.1.1 is degraded.. Severity impact: WARNING.
CBR3762E Library GRIDCL22 intervention required.
```

After the network issue is resolved, you see the following messages (they can be delayed by several minutes):

```
CBR3768I VTS operations in library GRIDCL20 no longer degraded.
CBR3768I VTS operations in library GRIDLIB2 no longer degraded.
```

14.4.1 Migration of volumes suspended

During a network failure where all available URLs on a TS7760C to an object store failed, migration to the cloud is suspended for that specific TS7760C cluster. After at least one URL connection reconnects, migration automatically resumes within a few minutes.

14.4.2 Recall of volumes suspended

When a job mounts a volume where the only available copy in the grid is within an object store and all TS7760C clusters include failed connections to the object store, recalling from the cloud is suspended and the following messages are issued:

```
CBR3750I Message from library GRIDCL20: OP0846 Mount of virtual volume
 1K1664 from the cloud pool MKPL01 failed. Severity impact: SERIOUS.
CBR3750I Message from library GRIDCL20: OP0831 The Transparent Cloud
Tiering service is unreachable: MKAC01. cloud account (mkcn01),
container (auto-generated S3 URL), url (). Severity impact: SERIOUS.
CBR3762E Library GRIDCL20 intervention required.
CBR4195I LACS retry possible for job COPYTEZ2: 801
IEE763I NAME= CBRLLACS CODE= 140394
CBR4000I LACS WAIT permanent error for drive 0E04.
CBR4171I Mount failed. LVOL=1K1664, LIB=GRIDLIB2, PVOL=??????, RSN=22.
```

```
IEE764I END OF CBR4195I   RELATED MESSAGES
007 CBR4196D Job COPYTEZ2, drive 0E04, volser 1K1664, error code
140394. Reply 'R' to retry or 'C' to cancel.
```

A subset of these messages might surface if a recall attempt at one TS7760C cluster fails because of a network issue yet a second TS7760C cluster is successful.

After the network reconnects to the cloud and the TS7760C warning state is cleared, retry the mount by replying R to the CBR4196D message if the condition resulted in a failed mount attempt.

14.4.3 Delete expire processing of volumes

Deleting an object from the cloud Object Storage is do0ne asynchronously by using an eject request of a logical volume. A volume becomes a candidate for delete-expire after all of the following conditions are met:

- The amount of time since the volume entered the scratch category is equal to or greater than the Expire Time.
- The amount of time since the volume’s record data was created or last modified is greater than 12 hours.
- At least 12 hours passed since the volume was migrated out of or recalled back into disk cache.

After these criteria are met, the delete expire process handles up to 2,000 logical volume deletes per hour per TS7700 as described in the **LI REQ SETTING DELEXP** count setting. After the logical volume is deleted from within the TS7760C, the object is marked pending deletion in the TS7760C DB and the background delete threads (as configured through **CLDSET**) requests deletions in the object store.

If the object store is unavailable, the deletions are suspended until it becomes available. The logical volume can be reused during this period, even if the previous volume instance is still marked for pending deletion

14.4.4 Logical volume eject processing

When a logical volume eject is completed, any object instance in an object store that is associated with the ejected logical volume is marked for pending deletion. The eject is viewed as successful after the object is marked for pending deletion.

Asynchronously, the number of delete tasks that are defined in **LI REQ CLDSET** are used to delete the objects in the cloud. Any network or communication with the object store defer these deletions until the network condition is resolved. A new instance of the logical volume can be reinserted during this period, if needed.

14.4.5 LI REQ CLDINFO command

Logical volume status on the cloud by using the **`LI REQ LVOL,<volser>, CLDINFO`** command is available, even if the TS7700 cannot connect to the Object Storage during a network failure.

14.5 Events related to a cloud

You can check events on the MI’s Events window or in the CBR3750I messages on the host console when issues occur.

For more information about events that are related to a cloud storage tier, see Chapter 12, “Monitoring the TS7700C” on page 115.

15

Performance considerations

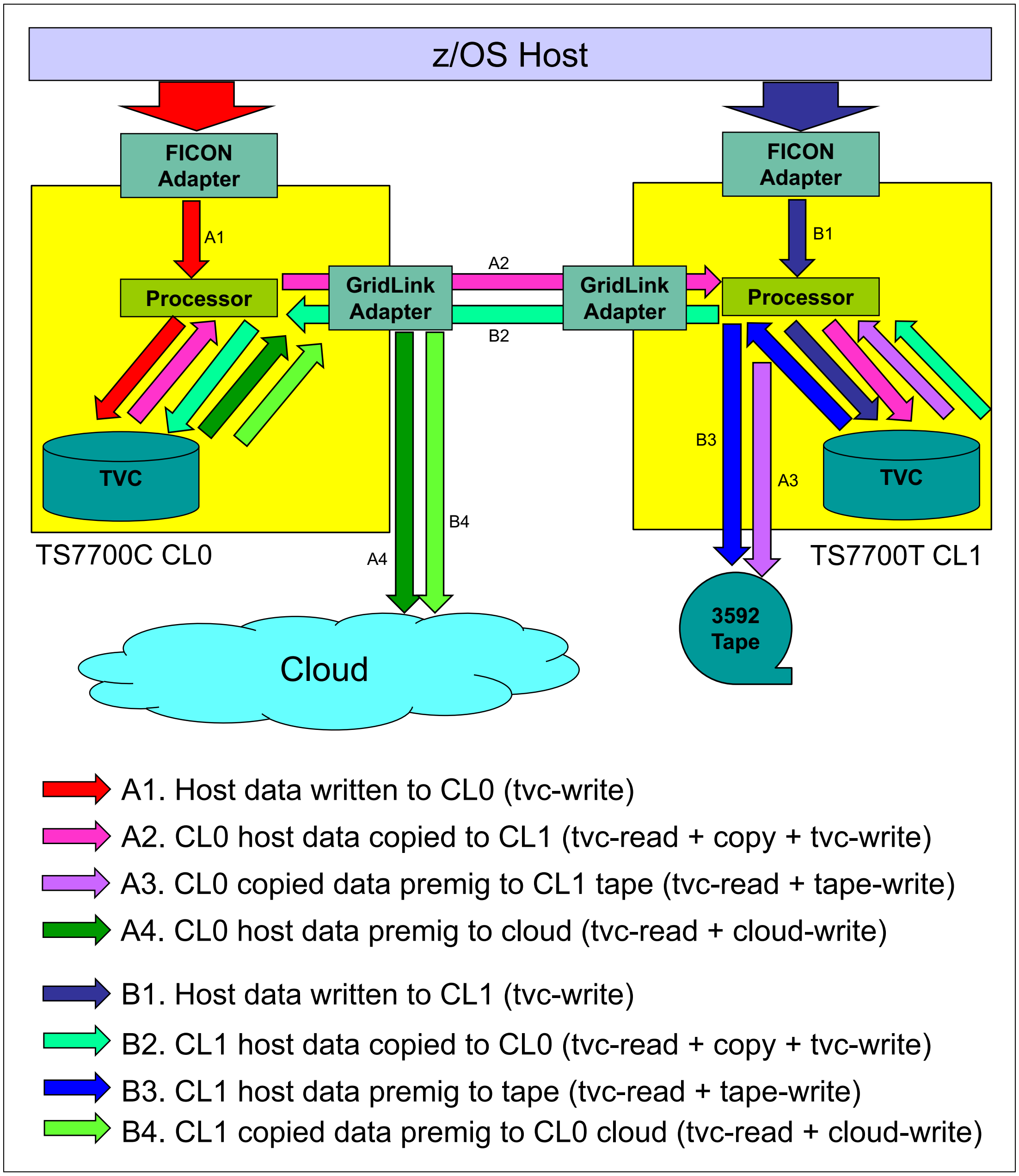
This chapter describes performance considerations regarding TS7700 cloud attach and includes the following topics:

- 15.1, “Generalizing a grid configuration using units of work” on page 142
- 15.2, “Cloud attach-specific performance considerations” on page 144

15.1 Generalizing a grid configuration using units of work

The TS7700 performance behavior, including cloud Object Store data, depends on the configuration. First, it is important to understand the data flow within a TS7700 grid.

Figure 15-1 shows a sample data flow in a two-cluster grid that consists of a TS7700C (CL0) and a TS7700T (CL1). It is an example of a near worse case scenario in which all data is replicated and premigrated to tape and cloud.



➡ A1. Host data written to CL0 (tvc-write)

➡ A2. CL0 host data copied to CL1 (tvc-read + copy + tvc-write)

➡ A3. CL0 copied data premig to CL1 tape (tvc-read + tape-write)

➡ A4. CL0 host data premig to cloud (tvc-read + cloud-write)

➡ B1. Host data written to CL1 (tvc-write)

➡ B2. CL1 host data copied to CL0 (tvc-read + copy + tvc-write)

➡ B3. CL1 host data premig to tape (tvc-read + tape-write)

➡ B4. CL1 copied data premig to CL0 cloud (tvc-read + cloud-write)

Figure 15-1 TTS7700 data flow sample in a two-cluster grid

The goal of this example is to inform you of how disk cache or TVC disk cache cumulative throughputs can be a factor in configuration's performance. In addition, total bandwidth on the grid links can be a factor in the configuration's throughputs. The example that is shown in Figure 15-1 attempts to break each activity to and from the disk TVC disk and each activity on the grid network as units of work.

This list describes the assumptions of the example in Figure 15-1:

- Each cluster receives its own 300 MBps uncompressed from its connected hosts.
- All logical volumes include RUN or Deferred copy mode with a zero DCT.
- All logical volumes are premigrated to cloud on CL0 and 3592 tape on CL1.
- The data compression ratio is 3:1.
- None to minimal logical volumes are read from the host in this example.

With a 300 MBps channel speed, the A1 and B1 units of work each are 100 MBps after compression. If all things are at equilibrium in a sustained state of operation, each arrow or unit of work must match the 100 MBps throughput.

CL0 includes five total arrows (TVC reads and writes) coming into or out of its TVC disk cache. Therefore, its disk cache must sustain a total of 500 MBps of raw compressed 1:1 mixed read/write throughput. CL1 also must sustain the same rate because it also has five units of work or arrows into and out of the disk cache.

If deferred copy throttling (DCT) is enabled, the replication component can be deferred allowing fewer units of work into and out of the TVC disk cache. Premigration to the cloud or tape might be delayed or skipped, which also reduces the total demand on disk cache throughput.

The most complex grid configurations can be generalized by using this basic unit of work concept. It can help determine whether disk cache is potentially a performance limiter.

By using the TS7700 performance white paper, you can determine the maximum mixed 1:1 throughput of your disk cache configuration that is based on how many physical drawers are installed. It can then be used to determine the expected maximum sustained states of operation of the solution. If remote copies to a third location are also occurring, those copies also add units of work to the TVC disk cache and grid network links.

For this same example, the total units of work on the CL0 grid network are four: one outbound for replication, one inbound for replication, and two for outbound cloud premigration. The cumulative read/write rate of the grid network at CL0 must be 400 MBps to sustain the worst case scenario in this example. Again, limiting replication or deferring or skipping premigration can reduce the workload on the links.

15.2 Cloud attach-specific performance considerations

This section describes the cloud attach-specific performance considerations.

15.2.1 Network bandwidth and premigration queue size

Network bandwidth to public cloud Object Stores is often limited when compared to private on premise cloud stores. Maximum throughput to an Object Store is also likely slower than the speed of which the TS7700 can write to 3592 physical tape drives.

Therefore, the premigration queue size can build up faster on a TS7700C cluster because it might have slower premigration speeds than similar TS7700T configurations. If the premigration backlog causes the sustained speed of operations to the TS7700C to be slower than expected (excessive throttling), consider adding premigration increments.

FC5274 (1 TB Active Premigration Queue) and FC5279 (5 TB Active Premigration Queue) are features that allow for an increase of premigration queue size.

If the grid remote write, replication, and cloud premigration activity exceeds the available bandwidth of the grid links, throttling or delays can occur. Therefore, it is ideal that the available grid network bandwidth can accommodate the expected throughputs of the configuration. Lower than needed bandwidth speeds can result in delayed RPO times, delayed premigration rates to the cloud, or lower than expected host rates when synchronous or RUN replication types are used.

15.2.2 Logical volume size

If network bandwidth is limited, premigration to a cloud and recall from a cloud for a logical volume requires longer times when compared to 3592 tape drives. For example, a 25 GB logical volume requires almost 40 minutes if only 100 Mbps bandwidth is available. It is recommended that smaller volume sizes be used for workloads that require frequent recalls so that mount completion and access to data can occur sooner.

15.2.3 Premigrate and recall time outs

You can customize premigrate and recall time out value by using the **LIBRARY REQUEST CLDSET** command. The timeout values are based on a 1 GB scaling factor, which allows you to choose a rate that accommodates all volume sizes.

You can also set the maximum concurrent tasks to premigrate and recall by using the **LIBRARY REQUEST CLDSET** command. If network bandwidth is narrow, you might need to set longer timeout values. If too many tasks are sharing the bandwidth, you can choose a smaller number of concurrent tasks so that each task receives a larger portion of the available bandwidth.

16

Library Request Commands for use with Cloud Storage Tier

This chapter describes APAR OA55481 and the LI REQ commands supporting the Cloud Storage Tier functionality that is introduced in R4.2.

This chapter includes the following topics:

16.1 Cloud Storage Tier host considerations

With R4.2, the TS7700 now can store logical volumes on an attached Cloud Storage Tier. Although no host support is needed to use this new Cloud Storage Tier functionality, applying OA55481 to each attached z/OS host is recommended. This APAR includes the following enhancements:

- Two new messages:

  ```
  CBR3736E Cloud object store degraded in library library-name
  CBR3737I Cloud object store no longer degraded in library library-name
  ```

  The CBR3736E message written to the host console for a distributed library, and for the composite library to which it belongs when the cloud object store enters the degraded state. The composite library stays in this state if at least one of its distributed libraries is in this state. It leaves this state when all of its distributed libraries are no longer in this state. The CBR3737I is surfaced when a distributed library or a composite library leaves this state.

- The CBR1110I message written to the host console as a result of the **D SMS,LIBRARY(*libname*)** command is updated to include the status line “Cloud object store configured” if the distributed library includes a configured cloud Object Store. If this command is issued against a composite library that has at least one distributed library configured to a cloud Object Store it will also include the “Cloud object store configured” information.
- The CBR1140I message is written to the host console as a result of the **D SMS,VOLUME(*volser*)** command was updated to include the status line “Cloud object store instance of volume exists” when at least one copy of the logical volume is in the cloud Object Store.

16.2 LI REQ support for Cloud Storage Tier

The following commands were created to support the Cloud Storage Tier functionality that introduced in R4.2:

- `LIBRARY REQUEST,composite_library,LVOL,volser,INFO`
- `LIBRARY REQUEST,composite_library,LVOL,volser,INFO,FLASH`
- `LIBRARY REQUEST,composite_library,LVOL,volser,CLDINFO`
- `LIBRARY REQUEST,distributed_library,CLDSET`
- `LIBRARY REQUEST,distributed_library,CLDSET,CPMCNTH,value`
- `LIBRARY REQUEST,distributed_library,CLDSET,CPMCNTL,value`
- `LIBRARY REQUEST,distributed_library,CLDSET,CLDPRIOR,value`
- `LIBRARY REQUEST,distributed_library,CLDSET,CRCCNT,value`
- `LIBRARY REQUEST,distributed_library,CLDSET,CDELCNT,value`
- `LIBRARY REQUEST,distributed_library,CLDSET,CPMTOUT,value`
- `LIBRARY REQUEST,distributed_library,CLDSET,CRCTOUT,value`
- `LIBRARY REQUEST,distributed_library,CLDSET,CDELTOUT,value`
- `LIBRARY REQUEST,distributed_library,CLDSET,CENABLMT,ALL,ENABLE/DISABLE`

This section provides an overview of these commands and describes the syntax, output, and keyword descriptions for each command. For more information about these options, see the white paper *TS7700 Library Request Command V4.2*, WP101091.

16.2.1 LIBRARY REQUEST,composite_library,LVOL,volser,INFO

Starting with R4.2, the **`LIBRARY REQUEST,composite_library,LVOL,volser`** command is replaced by the command with the following syntax:

```
LIBRARY REQUEST,composite_library,LVOL,volser,INFO
```

The standard **`LI REQ LVOL`** command was enhanced to include more information. The **`INFO`** parameter must be included to receive the newer content.

The previous version continues to function, but it no longer is planned for improvement because it does include any space for future enhancements.

The new **`INFO`** version now includes cloud-related attributes. The **`CD`** field in the last section stands for “Cloud Data” and indicates the number of cloud copies that specific cluster is aware of that were successfully premigrated to an object store. Only when this value is one or higher can that cluster access the logical volume within the object store.

Example 16-1 shows a sample output that uses the INFO parameter.

Example 16-1 LI REQ LVOL command sample output with INFO new parameter

```
LI REQ,GRIDLIB2,LVOL,1K1662,INFO
CBR1020I Processing LIBRARY command: REQ,GRIDLIB2,LVOL,1K1662,INFO.
CBR1280I Library GRIDLIB2 request. 804
Keywords: LVOL,1K1662,INFO
-------------------------------------------------------------------
LOGICAL VOLUME INFO V1 .0
 LOGICAL VOLUME               : 1K1662
 MEDIA, FMT, MAX(MB), CWRAP    : ECST, 6,  25000, N
 SIZE(MB) COMP, CHAN, RATIO    : 2863, 0, NA(FICON)
 CURRENT OWNER, TVC LIB        : cluster2, cluster0
 MOUNTED LIB/DV, MNT STATE     : -/-, -
 CACHE PREFERENCE, CATEGORY    : PG0, 022F (PRIVATE)
 LAST MOUNTED (UTC)            : 2018-09-11 00:23:20
 LAST MODIFIED LIB/DV, UTC(UTC): cluster0/000F, 2018-09-06 08:48:08
 KNOWN CPYS, REQ, REMOVED      : 1, 1, 0 (N)
 DEL EXP, WHEN (UTC)           : N, -
 HOT, FLASH COPY               : N, NOT ACTIVE
-------------------------------------------------------------------
  LIBRARY RQ CA P-PVOL S-PVOL CPS CPQ CPP RM CP CD
 cluster0  N  N ------ ------ CMP   - RUN  N  1  1
 cluster1  N  N ------ ------ NOR   - NOC  N  1  0
 cluster2  N  N ------ ------ NOR   - NOC  N  1  0
```

> **Note:** If you do not specify the new parameter **`INFO`**, no cloud-related information is displayed. Instead, a warning message is displayed that indicates the third keyword **`INFO`** is required to get logical volume information with the new format, as shown in Example 16-2.

Example 16-2 LI REQ LVOL command sample output without INFO new parameter

```
LI REQ,GRIDLIB2,LVOL,1K1662
CBR1020I Processing LIBRARY command: REQ,GRIDLIB2,LVOL,1K1662.
CBR1280I Library GRIDLIB2 request. 810
Keywords: LVOL,1K1662
-------------------------------------------------------------------
LOGICAL VOLUME INFORMATION V5 .1
```

```
 LOGICAL VOLUME:               1K1662
 MEDIA TYPE:                   ECST
 COMPRESSED SIZE (MB):         2863
 MAXIMUM VOLUME CAPACITY (MB): 25000
 CURRENT OWNER:                cluster2
 MOUNTED LIBRARY:
 MOUNTED VNODE:
 MOUNTED DEVICE:
 TVC LIBRARY:                  cluster0
 MOUNT STATE:
 CACHE PREFERENCE:             PG0
 CATEGORY:                     022F
 LAST MOUNTED (UTC):           2018-09-11 00:23:20
 LAST MODIFIED (UTC):          2018-09-06 08:48:08
 LAST MODIFIED VNODE:          000F
 LAST MODIFIED DEVICE:         000F
 TOTAL REQUIRED COPIES:        1
 KNOWN CONSISTENT COPIES:      1
 KNOWN REMOVED COPIES:         0
 IMMEDIATE-DEFERRED:           N
 DELETE EXPIRED:               N
 RECONCILIATION REQUIRED:      N
 LWORM VOLUME:                 N
 FLASH COPY:                   NOT ACTIVE
 FORMAT ID:                    6
 COMPRESSION METHOD:           FICON
 3490 COUNTERS HANDLING:       SURFACE EOT
----------------------------------------------------------------------
  LIBRARY  RQ CACHE PRI PVOL  SEC PVOL  COPY ST  COPY Q  COPY CP  REM
cluster0   N     N   ------    ------     CMPT       -      RUN    N
 cluster1   N     N   ------    ------  NOT REQ       -  NO COPY    N
 cluster2   N     N   ------    ------  NOT REQ       -  NO COPY    N
----------------------------------------------------------------------
  LIBRARY  CP
 cluster0   1
 cluster1   1
 cluster2   1
>>> THIS LI REQ IS NO LONGER MAINTAINED. PLEASE ADD 3RD KW 'INFO'
>>> TO GET LVOL INFORMATION
```

16.2.2 LIBRARY REQUEST,composite_library,LVOL,volser,CLDINFO

The use of this command provides the logical volume status on cloud; that is, object data. It indicates whether the logical volume is premigrated to the cloud and from which clusters in the grid the data is accessible. The response lines are formatted as shown in Example 16-3.

Example 16-3   LI REQ LVOL command result sample with new CLDINFO parameter

```
LI REQ,GRIDLIB2,LVOL,1K1662,CLDINFO
CBR1020I Processing LIBRARY command: REQ,GRIDLIB2,LVOL,1K1662,CLDINFO.
CBR1280I Library GRIDLIB2 request. 817
Keywords: LVOL,1K1662,CLDINFO
----------------------------------------------------------------------
LOGICAL VOLUME CLOUD INFORMATION V1 .0
```

```
 LOGICAL VOLUME:              1K1662
----------------------------------------------------------------------
  LIBRARY ST     POOL/ ACCOUNT/CL     POOL/ ACCOUNT/CL
 cluster0  M   MKPL01/  MKAC01/0
 cluster1  - NO DATA IS PREMIGRATED TO CLOUD
 cluster2  - NO DATA IS PREMIGRATED TO CLOUD
```

16.2.3 LIBRARY REQUEST,*composite_library*,LVOL,*volser*,INFO,FLASH

Starting with R4.2, the **LIBRARY REQUEST,composite_library,LVOL,volser,FLASH** command is replaced by the command with the following syntax:

LIBRARY REQUEST,*composite_library*,LVOL,*volser*,INFO,FLASH

The older **LIBRARY REQUEST,composite_library,LVOL,volser,FLASH** command continues to function, but does not receive any new enhancements.

16.2.4 LIBRARY REQUEST,*distributed_library*,CLDSET

The cloud attachment function was introduced as part of code release level R4.2. The LI REQ CLDSET options are introduced as part of this enhancement.

The LI REQ (keyword “CLDSET”) commands can help manage settings that are associated with cloud storage tier support. For example, it can be used to change the number of concurrent data premigration tasks to cloud. Also, it can temporarily enable or disable the data premigration, recall, and deletion to and from cloud.

The CLDSET request also provides information about many of the current cloud data workflow and management settings of the cluster and the ability to modify the settings. The CLDSET is applicable to TS7700C clusters only.

In the response of the CLDSET request, the cluster that is associated with the distributed library in the request modifies its settings based on the extra keywords that are specified. If no other keywords are specified, the request returns the current settings.

Note: All settings are persistent across machine restarts, service actions, or code updates. The settings are not carried forward as part of Disaster Recovery from Copy Exported tapes or the recovery of a system.

All requests are applicable to a TS7700C distributed library only. If the distributed library that is specified in the LI REQ command is not a TS7700C, the following error text is returned:

```
‘ONLY SUPPORTED IN CLOUD ENABLED TS7700 VIRTUALIZATION ENGINE’
```

If the composite library is specified, the following error text is returned:

```
‘REQUEST INVALID FOR COMPOSITE LIBRARY’
```

The following other keywords can be specified by using the **CLDSET** command, each controlling a different cloud-related function:

- CPMCNTH: Cloud Premigration Count High:
  - Sets the highest number of premigration tasks that the TS7700C starts in parallel when premigraton to the cloud is a priority; for example, when the CLDPRIOR threshold is crossed. The high or low priority mode of cloud premigration is described in the CLDPRIOR section.
  - Issued by using the following command:

    ```
    LIBRARY REQUEST,distributed_library,CLDSET,CPMCNTH,value
    ```

  - The default value is 40. The maximum value is 128, and the minimum value is 1.
  - A value lower than CPMCNTL cannot be set. If it is attempted, CPMCNTH automatically sets to the same value as CPMCNTL.
  - If the provided value is out of range (less than 1, or more than 128), the following error is returned:

    ```
    'AN ERROR OCCURED PROCESSING THE HOST REQUEST. RETURN CODE = 2'
    ```

- CPMCNTL: Cloud Premigration Count Low:
  - Sets the lowest number of premigration processes that the TS7700C starts in parallel when premigration to the cloud is not a priority; for example, when the CLDPRIOR threshold is not crossed. A nonzero value allows some premigration to the cloud to occur, even when it is not required, such as during the peak mode of operation of a TS7760C. The high or low priority mode of cloud premigration is described in the CLDPRIOR section.
  - Issued by using the following command:

    ```
    LIBRARY REQUEST,distributed_library,CLDSET,CPMCNTL,value
    ```

  - The default value is 0. The maximum value is 128 and the minimum value is 0.
  - A value higher than CPMCNTH cannot be set. If it is attempted, CPMCNTL automatically sets to the same value as CPMCNTH.
  - If the provided value is out of range (less than 0, or more than 128), the following error is returned:

    ```
    'AN ERROR OCCURED PROCESSING THE HOST REQUEST. RETURN CODE = 2'
    ```

- CLDPRIOR: Cloud Premigration Priority Threshold
  - Sets the threshold (in GBs) of unpremigrated data to cloud at which the TS7700C begins increasing the number of cloud premigration tasks that are allowed to compete with host I/O for cache and processor cycles. If the premigration queue is below this threshold, a number of tasks up to the value set for CPMCNTL are used for premigration to the cloud. If it is above this threshold, a number of tasks up to the value set for CPMCNTLH are used for premigration to the cloud.
  - Issued by using the following command:

    ```
    LIBRARY REQUEST,distributed_library,CLDSET,CLDPRIOR,value
    ```

  - The amount of cloud unpremigrated data must be above the value that is specified for 150 seconds before the other cloud premigration tasks are added. As the amount of data to premigrate to cloud continues to grow above this threshold setting, so do the number of enabled cloud premigration tasks until the maximum CPMCNTH task count is reached.

If the amount of cloud unpremigrated data falls below this threshold for at least 150 seconds, the number of cloud premigration tasks can be reduced depending on host I/O demand. If I/O host demand is high, the number of premigration tasks eventually is reduced to a minimum of CPMCNTL tasks.

  - The default value is 0, which results in an internal default value of the premigration queue size minus 400 GB. The maximum value can be set up to the total size of the active premigration queue. For example, if FC 5274 (1 TB Active Premigration Queue) x 10 plus FC 5279 (5 TB Active Premigration Queue) feature codes are installed, the total size of the active premigration queue is 15 TB. Then, up to 15 * 1000 = 15000 in GBs can be set.
  - A value higher than the total size of the active premigration queue (P) cannot be set. If it is attempted, CPMCNTL automatically sets to “P”.

- CRCCNT: Cloud Recall Count:
  - Sets the maximum number of logical volume recalls that the TS7700C starts in parallel at any time when a recall from the cloud must be done. If more recalls are required than the CRCCNT value, they are queued until a logical volume recall task is available.

    Issued by using the following command:

    ```
    LIBRARY REQUEST,distributed_library,CLDSET,CRCCNT,value
    ```

  - The default value is 20. The maximum value is 32 and the minimum value is 1.
  - If the provided value is out of range (less than 1, or more than 32), the following error is returned:

    ```
    ‘AN ERROR OCCURED PROCESSING THE HOST REQUEST. RETURN CODE = 2’
    ```

- CDELCNT: Cloud Delete Count
  - Sets the number of stale (unnecessary) data delete tasks that the TS7700C starts in parallel at any time when object data deletion in cloud must be done.
  - Issued by using the following command:

    ```
    LIBRARY REQUEST,distributed_library,CLDSET,CDELCNT,value
    ```

  - The default value is 0, which results in an internal default value of 5. The maximum value is 16 and the minimum value is 1. The maximum value is 16 and the minimum value is 1.
  - If the provided value is out of range (more than 16), the following error is returned:

    ```
    ‘AN ERROR OCCURED PROCESSING THE HOST REQUEST. RETURN CODE = 2’
    ```

- CPMTOUT: Cloud Premigration Timeout
  - Sets the timeout value, in seconds, to premigrate 1 GiB of data from the cluster to the cloud.
  - Issued by using the following command:

    ```
    LIBRARY REQUEST,distributed_library,CLDSET,CPMTOUT,value
    ```

  - For example, if a 6 GiB volume is premigrated, the premigration process waits up to six times this timeout value before it times out. The larger the CPMCNTH tasks value, the longer a premigration can take to complete because the bandwidth to the cloud is shared by up to CPMCNT tasks. Therefore, this value might need to be adjusted if the CPMCNTH value is modified. Similarly, CRCCNT and grid copy tasks counts can use grid link and cloud bandwidth; therefore, adjusting this timeout value might be needed if grid copies, recalls, and premigration are all occurring in parallel in higher numbers.

  - When a cloud premigration timeout occurs, an event is posted to MI, as shown in the following example:

    ```
    ‘Cloud pre-migration for virtual volume <volser> to cloud pool
    <cloud_pool_nickname > timed out with <timeout> seconds, where CPMTOUT is
    <CPMTOUT> and size of the virtual volume is <lvol size> GiB’

    (*) Given multiple cloud premigration timeouts can occur at a time, only 1
    event will be posted at a specific interval. New events can be posted every
    interval.
    ```

  - The default value is 1800 (seconds) (that is, 30 minutes per 1 GiB of data). The maximum value is 99999999 and the minimum value is 1.
  - A volume size is always rounded up to the nearest GiB value when determining the total timeout value for a volume. For example, a 25 GB maximum size volume containing only 13.2 GiB of data is timed as a 14 GiB volume, or 14 times the CPMTOUT value. A 4 GB maximum size volume that contains only 3 MiB of data is timed as a 1 GiB volume.
  - If the provided value is out of range (less than 1), the following error is returned:

    ```
    ‘AN ERROR OCCURED PROCESSING THE HOST REQUEST. RETURN CODE = 2’
    ```

- CRCTOUT: Cloud Recall Timeout
  - Sets the timeout value, in seconds, to recall 1 GiB of data from the cloud to the cluster.
  - Issued by using the following command:

    ```
    LIBRARY REQUEST,distributed_library,CLDSET,CRCTOUT,value
    ```

  - For example, if a 6 GiB volume is recalled, the recall process waits up to six times this timeout value before it times out. The larger the CRCCNT tasks value, the longer a recall can take to complete because the bandwidth from the cloud is shared by up to CRCCNT tasks. Therefore, this value might need to be adjusted if CRCCNT is modified. Similarly, CPMTOUT and grid copy tasks counts can use grid link and cloud bandwidth; therefore, adjusting this timeout value might be needed if grid copies, recalls, and premigration are all occurring in parallel in higher numbers.
  - When a cloud recall timeout occurs, an event is posted to MI, as shown in the following example:

    ```
    ‘Cloud recall for virtual volume <volser> from cloud pool
    <cloud_pool_nickname > timed out with <timeout> seconds, where CRCTOUT is
    <CPCTOUT> and size of the virtual volume is <lvol size> GiB’

    (*) Given multiple cloud recall timeouts can occur at a time, only 1 event
    will be posted at a specific interval. New events can be posted every
    interval.
    ```

  - The default value is 1800 (seconds) (that is, 30 minutes per 1 GiB of data). The maximum value is 42900 and the minimum value is 1.
  - A volume size is always rounded up to the nearest GiB value when determining the total timeout value for a volume. For example, a 25 GB maximum size volume that contains only 13.2 GiB of data is timed as a 14 GiB volume or 14 times the CRCTOUT value. A 4 GB maximum size volume that contains only 3 MiB of data is timed as a 1 GiB volume.
  - If the provided value is out of range (less than 0 or more than 42900), the following error is returned:

    ```
    ‘AN ERROR OCCURED PROCESSING THE HOST REQUEST. RETURN CODE = 2’
    ```

- CDELTOUT: Cloud Delete Timeout:
  - Sets the timeout value, in seconds, to delete one logical volume from the cloud.
  - Issued by using the following command

    ```
    LIBRARY REQUEST,distributed_library,CLDSET,CDELTOUT,value
    ```

  - This value is not dependent on volume size; therefore, all volume sizes are timed equally.
  - When a cloud object deletion timeout occurs, an event is posted to MI, as shown in the following example:

    ```
    'Deleting object <volser> from container < container_name> of cloud pool <
    cloud_pool_nickname> timed out with CDELTOUT (<CDELTOUT> seconds)'
    ```

  - The default value is 1800 (seconds) (that is, 30 minutes per 1 GiB of data). The maximum value is 42900 and the minimum value is 1.
  - If the provided value is out of range (less than 0 or more than 42900), the following error is returned:

    ```
    'AN ERROR OCCURED PROCESSING THE HOST REQUEST. RETURN CODE = 2'
    ```

- CENABLMT: Cloud Enablement:
  - Enables or disables the cloud data handling operations (cloud data premigration, recall, or delete) to or from the cluster.
  - Issued by using the following command:

    ```
    LIBRARY REQUEST,distributed_library,CLDSET,CENABLMT,ALL,ENABLE/DISABLE
    ```

  - When it is set to “DISABLED”, no new cloud data premigration, recall, or delete to or from the cluster occurs.
  - When DISABLED, the distributed library enters the operations degraded state for the cloud. The library exits this state when the value is set to ENABLED and no other issues are associated with the attached object store.
  - The default is “ENABLED”.
- CLDSET Default Response

  The response lines to a CLDSET request are formatted as shown in Example 16-4 when a valid setting is provided. Entering the CLDSET keyword without any other keywords provides this response as well.

Example 16-4 CLDSET response format

```
CLOUD SETTINGS V1 .0
 CPMCNTH  =       20    CPMCNTL  =        5
 CLDPRIOR =        0
 CRCCNT   =       20
 CDELCNT  =        1
 CPMTOUT  =     1800
 CRCTOUT  =     1800
 CDELTOUT =     3600
 -------------------------------------------------------------------
 CENABLMT Controls
   CLDPM    =   ENABLED
   CLDRCALL =   ENABLED
   CLDDEL   =   ENABLED
```

16.2.5 LI REQ STATUS command with GRLNKACT parameter

The `LI REQ STATUS GRLNKACT` command response was enhanced to include information about grid link activity to the cloud. In response to this request, the grid provides point-in-time details about all of the grid link activity for all configured clusters in the grid. If any of the clusters are cloud-attached, cloud activity across the links also is provided. The information is summed into 15-second intervals and the next interval starting after the command is received is returned to the issuer.

The report includes the following sections:

- **GRID LINK ESTABLISHED SOCKET CONNECTIONS**

  This view reports how many TCP sockets are established from each Grid interface on the local clusters to the peer cluster and cloud. It also provides the total established TCP connections, which are used for IBM MQ (Grid cluster-cluster WebSphere message communication) and RFA (Grid cluster-cluster data [file] transfer).

  Consider the following points:

  – The number of the socket connections are provided per each Grid interface (L0:Primary, L1:Alternate, L2:Primary2, and L3:Alternate2) with the resource name (enX) and IP addresses. Cx columns show the connections that are used for Grid communications with the peer cluster Cx (Cx means cluster ID x).

  – MQ column shows the total sum of the connections used for MQ.

  – RFA column shows the total sum of the connections used for RFA.

  – CLD column shows the total sum of the connections that are used for cloud. This sum might also include the sums for GGM (Grid to Grid Migration) activity with another copy source/target Grid if it is configured and used (a future release will separate cloud and GGM activity).

- **NET ACTIVITY**

  This view reports how much data (in MB) was sent or received on each Grid interface in the last 15-second interval. It also provides the current network request counts in Grid interface buffer. They are summated for MQ/RFA/Cloud usage. This view is also reported based on each Grid interface the same as the view of established socket connections. Consider the following points:

  – TxMBs shows the total transmitted network activity (in MBs) from the Grid interface in the last 15 seconds.

  – RxMBs shows the total received network activity (in MBs) into the Grid interface in the last 15 seconds.

  – MQ_REC/MQ_SND shows the current network request (receiving/sending) counts in each Grid network interface buffer related for MQ. If the value is non-0, it must indicate that network activity exists for MQ activity.

  – GFA_REC/GFA_SND: The same counts related for GFA.

  – CLD_REC/CLD_SND: The same counts that are related for cloud. This figure also can include the information for GGM (Grid to Grid Migration) activity as it is shown in the "**GRID LINK ESTABLISHED SOCKET CONNECTIONS**".

- **GRID LINK THROUGHPUT ESTIMATES**

  This view reports the estimated Grid link throughput estimation in the last 15-second interval. The values except with cloud are retrieved from TS7700 Statistical Data. Tx/Rx provide the transmitted network throughput to the remote target/received network throughput from the remote target. The unit is MBps.

Consider the following points:

- Cx columns refers to the cluster ID.
- GRD_TOT column shows the total throughput with the remote clusters (Cx) in the Grid.
- CLD column shows the throughput against the cloud if configured and used.
- TOT column shows the sum of GRD_TOT and CLD.

(*) GGM activity can be completed CLD or TOT as it is shown in the “**GRID LINK ESTABLISHED SOCKET CONNECTIONS**” on page 154.

- **GRID CLOUD TIER EXPORT AND IMPORT ACTIVITY**

  This view reports the current cloud data premigration (export) and recall (import) status. The active premigration and recall volumes to or from cloud are provided. Consider the following points:

  - ACTIVE EXPORT VOLUME COUNT provides the total number of the active export (premigration) volumes. If it is non-0, the corresponding volsers are provided below the `ACTIVE EXPORT VOLUME COUNT`.
  - ACTIVE IMPORT VOLUME COUNT provides the total number of the active import (recall) volumes. If it is non-0, the corresponding volsers are provided below the `ACTIVE IMPORT VOLUME COUNT`.

Example 16-5 shows the cloud-related grid link activity in the new CLD column in the output from the GRLNKACT parameter.

Example 16-5 GRLNKACT parameter shows cloud related grid link activity in CLD column

```
> SHOWING RESULTS FOR COMMANDS: STATUS,GRLNKACT
"GRLNKACT STATUS V1 .0                                                 "
"CLUSTER INDEX:  6 LINK COUNT:  2 TIME: THU FEB 21 20:28:55 CUT 2019   "
"GRID LINK ESTABLISHED SOCKET CONNECTIONS------------------------------"
"LN INTF IP               C0  C1  C2  C3  C4  C5  C6  C7  MQ  RFA  CLD "
"L0 EN10 10.11.150.23     0   134 113 0   0   0   0   115 362 0    26  "
"L1 EN4  10.11.151.23     0   0   0   0   0   0   0   0   0   0    14  "
"L2 -    -                0   0   0   0   0   0   0   0   0   0    0   "
"L3 -    -                0   0   0   0   0   0   0   0   0   0    0   "
"NET ACTIVITY -----TCP RECV/SEND ADAPTER BUFFER ACTIVITY BYTES---------"
"LN  TXMBS RXMBS MQ_REC   MQ_SND   GFA_REC  GFA_SND  CLD_REC  CLD_SND  "
"L0  13    0     0        888      0        0        0        0        "
"L1  22    0     0        0        0        0        0        1032081  "
"L2  0     0     0        0        0        0        0        0        "
"L3  0     0     0        0        0        0        0        0        "
"TOT 36    1     -        -        -        -        -        -        "
"GRID LINK THROUGHPUT ESTIMATES-MB/S-----------------------------------"
"DIR C0   C1   C2   C3   C4   C5   C6   C7   GRD_TOT CLD  TOT          "
"TX  0    0    0    0    0    0    0    0    0       36   36           "
"RX  0    0    0    0    0    0    0    0    0       0    0            "
"GRID CLOUD TIER EXPORT AND IMPORT ACTIVITY----------------------------"
"ACTIVE EXPORT VOLUME COUNT: 40                                        "
"CL0651 CL0671 CL0677 CL0679 CL0681 CL0683 CL0685 CL0687               "
"CL0689 CL0691 CL0693 CL0695 CL0697 CL0699 CL0701 CL0703               "
"CL0705 CL0707 CL0709 CL0711 CL0713 CL0715 CL0717 CL0719               "
"CL0721 CL0723 CL0725 CL0727 CL0729 CL0730 CL0731 CL0732               "
"CL0733 CL0735 CL0737 CL0739 CL0741 CL0743 CL0745 CL0749               "
"ACTIVE IMPORT VOLUME COUNT: 0                                         "
> EXECUTING COMMANDS: STATUS,GRLNKACT
```

16.2.6 Cloud-related operator messages

Cloud-related operator messages are listed in Table 16-1. You can monitor them on the z/OS host filtering CBR3750I.

Table 16-1 Cloud related operator messages

ID	Description
OP0830	Transparent Cloud Tiering daemon died.
OP0831	Transparent Cloud Tiering service is unreachable: {0}. cloud account ({1}), container ({2}), url ({3}).
OP0832	URL that is associated with container is invalid: {0}. cloud account ({1}), container ({2}), url ({3}).
OP0833	URL that is associated with container is malformed: {0}. cloud account ({1}), container ({2}), url ({3}).
OP0834	The URL associated with container is malformed: {0}. cloud account ({1}), container ({2}), url ({3}).
OP0835	Connect exception to Cloud Service Provider: {0}. cloud account ({1}), container ({2}), url ({3}).
OP0836	Socket timeout for a cloud connection: {0}. cloud account ({1}), container ({2}), url ({3}).
OP0837	Invalid cloud configuration: {0}. cloud account ({1}), container ({2}), url ({3}).
OP0838	Invalid credentials for cloud provider: {0}. cloud account ({1}), container ({2}), url ({3}).
OP0839	The network of Transparent cloud tiering node is down.
OP0840	SSL handshake exception for a cloud provider: {0}. cloud account ({1}), container ({2}), url ({3}).
OP0841	SSL handshake bad certificate exception for a cloud provider: {0}. cloud account ({1}), container ({2}), url ({3}).
OP0842	SSL handshake socket closed exception for a cloud provider.
OP0843	The TS7700 cannot communicate with the Cloud provider.
OP0844	Virtual volumes with Storage Class {0} is set to off load to cloud storage, but the storage group {1} does not have the cloud premigration rank set properly.
OP0845	Unable to write to Cloud Container {0}.
OP0846	Mount of virtual volume {0} from the cloud pool {1} failed.
OP0847	Cloud pre-migration for virtual volume {0} to cloud pool {1} timed out with {2} seconds, where CPMTOUT is {3} and size of the virtual volume is {4} GiB.
OP0848	Cloud recall for virtual volume {0} from cloud pool {1} timed out with {2} seconds, where CRCTOUT is {3} and size of the virtual volume is {4} GiB.
OP0849	Deleting object {0} from container {1} of cloud pool {2} timed out with CDELTOUT ({3} seconds).
OP0850	SSL handshake invalid path certificate exception for a cloud provider.
OP0851	SSL handshake failure exception for a cloud provider.

ID	Description
OP0852	SSL handshake unknown exception for a cloud provider.
OP0853	SSL peer unverified exception for a cloud provider.
OP0854	SSL protocol exception for a cloud provider.
OP0855	SSL exception for a cloud provider.
OP0856	SSL no cert exception for a cloud provider.
OP0857	SSL not trusted cert exception for a cloud provider.
OP0858	SSL invalid algorithm exception for a cloud provider.
OP0859	SSL invalid padding exception for a cloud provider.
OP0860	SSL unrecognized message for a cloud provider.
OP0861	Bad request for a cloud provider.
OP0862	Precondition failed for a cloud provider.
OP0863	Container creation failed: container ({0}).
OP0864	Cloud Bucket limit exceeded: container ({0}).
OP0865	Container does not exist: container ({0}).
OP0866	Time skew with a cloud provider.
OP0867	Cloud provider server error.
OP0868	Internal directory not found for Transparent Cloud Tiering.
OP0869	Resource address file not found for Transparent Cloud Tiering.
OP0870	Database corrupted for Transparent Cloud Tiering.
OP0871	LKM down for Transparent Cloud Tiering.
OP0872	Access forbidden for a cloud account: cloud account ({0}).
OP0873	Access denied for a cloud account: ({0}).
OP0874	File system corrupted for Transparent Cloud Tiering.
OP0875	Directory error for Transparent Cloud Tiering.
OP0876	Key manager error for Transparent Cloud Tiering.
OP0877	Container pair root directory not found for Transparent Cloud Tiering.
OP0878	Container exists: {0}. cloud account ({1}), container ({2}), url ({3}).
OP0879	RKM down for Transparent cloud tiering: {0}. cloud account ({1}), container ({2}), url ({3}).
OP0880	RKM down for Transparent cloud tiering: {0}. cloud account ({1}), container ({2}), url ({3}).
OP0881	SSL key exception for a cloud provider: {0}. cloud account ({1}), container ({2}), url ({3}).
OP0882	Transparent Cloud Tiering container {0} inaccessible by url {1} for unexpected reason: {2}, failure detail: {3}.

ID	Description
MDE8186	The Transparent Cloud Tiering daemon died.
MDEB080	The Transparent Cloud Tiering configuration during online processing failed. A call home is started if this setting is enabled.

Related publications

The publications that are listed in this section are considered particularly suitable for a more detailed discussion of the topics that are covered in this paper.

IBM Redbooks

The IBM Redbooks publication *IBM TS7700 Release 4.2 Guide*, SG24-8366, provides more information about the topic in this document. Note that this publication might be available in softcopy only.

You can search for, view, download or order this document and other Redbooks, Redpapers, Web Docs, draft, and other materials, at the following website:

ibm.com/redbooks

Online resources

The following websites are also relevant as further information sources:

- IBM Knowledge Center - IBM TS7700 Customer documentation 4.2.0:

  https://www.ibm.com/support/knowledgecenter/en/STFS69_4.2.0/hydra_c_ichome.html

- IBM TS7700 R4.2 delivers cloud storage tier support - IBM Announcement:

  https://www.ibm.com/common/ssi/ShowDoc.wss?docURL=/common/ssi/rep_ca/5/897/ENUS118-055/index.html&request_locale=en

- IBM White paper - TS7700 Library Request Command V4.2:

  http://www-03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP101091

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

REDP-5514-00

ISBN 0738457671

Printed in U.S.A.