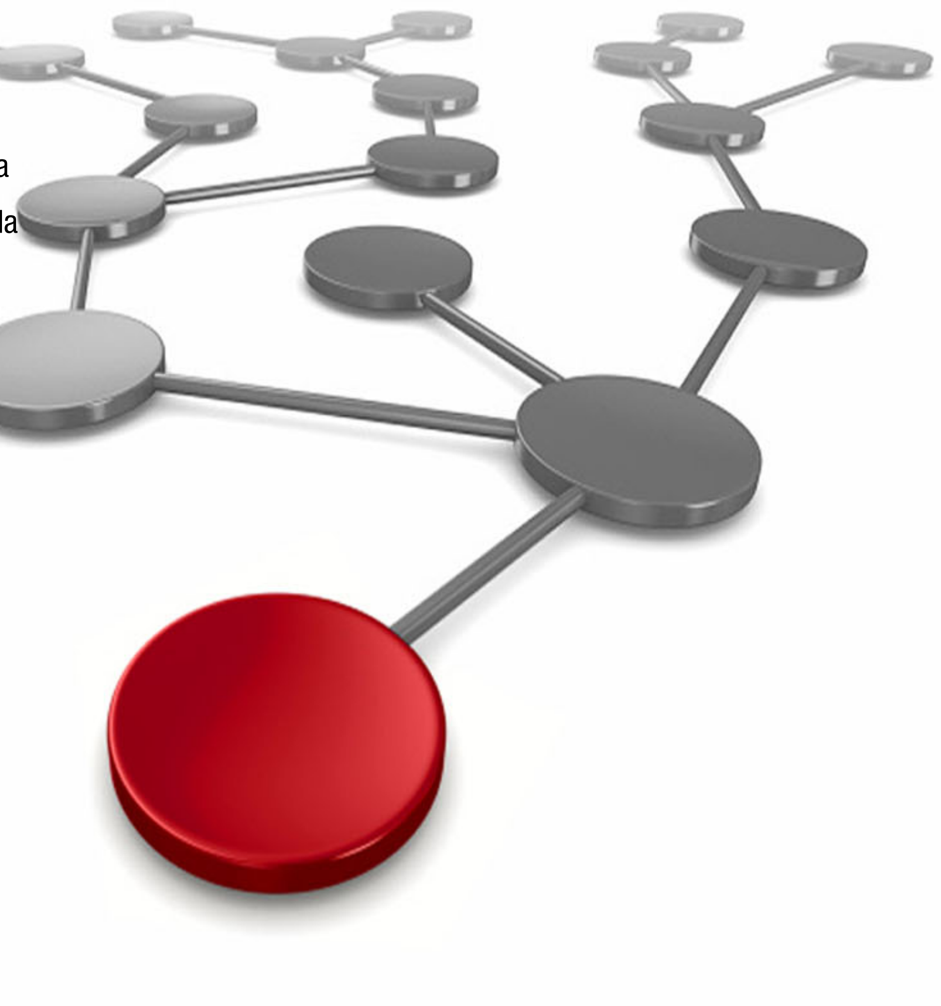
Redbooks
ibm.com/redbooks

IBM TS7700 R5.2.2 Cloud Storage Tier Guide

Yuki Asakura
Ole Asmussen
Nielson ’Nino’ de Carvalho
Larry Coyne
Derek Erdmann
Monica Falcone
Rin Fujiwara
Nobuhiko Furuya
Lourie Goodall
Joe Hew
Kousei Kawamura
Tony Makepeace
Erich Moraga
Stefan Neff
Tomoaki Ogino
Alberto Barajas Ortiz
Aderson Pacini
Trinidad Armando Rangel Ruiz
Michael Scott
Joe Swingler
Taisei Takai
Nao Takemura
Takahiro Tsuda
Chen Zhu



Cloud

Storage

IBM
Redpaper

IBM Redbooks

IBM TS7700 R5.2.2 Cloud Storage Tier Guide

July 2022

REDP-5573-02

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

Third Edition (July 2022)

This edition applies to Version 5, Release 2, Modification 2 of the IBM TS7700.

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®
FlashCopy®
Global Technology Services®
IBM®
IBM Cloud®
IBM Services®
IBM Spectrum®
IBM Z®
Parallel Sysplex®
POWER8®
POWER9™
Redbooks®
Redbooks (logo) ®
Slicestor®
System z®
WebSphere®
z/OS®
z/VM®

The following terms are trademarks of other companies:

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

The registered trademark Linux® is used pursuant to a sublicense from the Linux Foundation, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis.

Microsoft, 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 25 years of virtual tape experience, the IBM® TS7700 (IBM TS7760 and TS7770) now can store virtual tape volumes in object storage. This IBM® Redpaper™ publication helps you set up and configure the cloud object storage support for IBM Cloud® Object Storage or Amazon Simple Storage Service (Amazon S3).

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

In this 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 publication 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.

Authors

This paper was produced by a team of specialists from around the world.

Yuki Asakura is a software development engineer in Japan at IBM Tokyo Laboratory. He has been in charge of developing IBM TS7700 since he joined IBM in 2018. He is responsible for developing and supporting TS7700 software components that are related to hierarchical storage management for disk, tape and cloud storage, data transfer functions, and Grid functions.

Ole Asmussen is a Product Field Engineer for IBM Storage based in Hamburg, Germany. He has supported IBM Tape for over 20 years, working in various support level and supporting all IBM Tape products (3494, 3584, TS7700, and ProtecTier). He joined IBM as a Customer Service Representative in 1999 and was responsible for different accounts in Germany. In 2001, he joined the Support Center in Mainz, Germany.

Nielson ’Nino’ de Carvalho is a Level 2 certified IT specialist at IBM Lab Services in South Africa. He has over 10 years experience of IBM mainframe computing as a customer and with IBM. Nino has extensive technical experience implementing and supporting clients on a broad range of IBM products. His areas of expertise Include IBM Z and LinuxONE hardware, zOS and z/VM®, high-end disk, and tape solutions, including IBM FICON® connectivity.

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.

Derek Erdmann is a Data Facility Storage Management Subsystem (DFSMS) Software Technical Support Engineer who specializes in the Object Access Method (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 enhance the quality of the DFSMS product set.

Monica Falcone is an IT Management Consultant for IBM Systems European Storage Competence Center. She is responsible for the design and elaboration of complex high-end storage solutions to fit market requirements, and covering the promotions of new products and new functions. As a high-end tape expert, she provides technical support to the IBM sales team and advises IBM customers and IBM Business Partners about obtaining the best result for their needs. Monica holds a university diploma in computer science from the Frankfurt University of Applied Science in Frankfurt am Mainz, Germany. She joined IBM in 2002 and has worked in several IBM units and areas in different roles.

Rin Fujiwara works in the technical support team for DFSMS and high-end tape products in Japan. She has 15 years experience with IBM Z as a subject matter expert. Rin has supported DFSMS and TS7700 for 5 years.

Nobuhiko Furuya retired from IBM Japan at the end of October 2019, started his own company, V-SOL Inc., and continues to work with IBM and clients on TS7700 and DFSMS implementations. He has over 36 years experience in IBM and 1 year in V-SOL for IBM Z and the storage area.

Lourie Goodall is a Senior Technical Staff Member (STSM) with IBM Systems and Technology Group, which is based out of the IBM laboratory in Tucson, Arizona. She is an Architect for the IBM TS7700 Virtualization Engine. Lourie has worked in mainframe back-end tape and virtual tape storage for over 18 years and has authored or co-authored hundreds of design documents and numerous technical papers. Lourie was one of the original developers of the second generation of VTS: the TS7700.

Joe Hew works in the Tucson, Arizona product field engineering group, supporting the IBM TS7700. With many years in the 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).

Kousei Kawamura is a software engineer in Tokyo, Japan. He joined IBM Japan in 2012, and worked on software development of TS7700 hierarchical storage manager (HSM) component for 4 years. From 2013, he started to work as TS7700 domain manager (HDM) software developer as well. In 2016, Kousei moved from the HSM development team to work as a software developer of TS7700 Grid component.

Tony Makepeace is a IBM Brand Specialist working in the UK and Ireland. He has more than 37 years of experience in project management, installation, technical support, and pre-sales for mainframe systems. He spent the past 21 years working at IBM as a Tape specialist with particular focus on TS7700.

Erich Moraga works out of Dallas/Fort Worth, Texas as a subject matter expert in the IBM TS7700 Product Field Engineering group. He joined IBM in 1999 as an e-business consultant, transitioned to Windows application support, followed by IBM Z support as a National Duty manager. After he joined the support team for IBM Power Systems hardware he earned numerous awards and an Eminence & Excellence award. In 2012 he moved to IBM TS7600 PFE where he received four awards with a promotion in 2015. Erich continues to be recognized with more awards for his customer support of the TS7700.

Stefan Neff is an IBM Leading Technical Sales Professional for IBM DRI Solutions, especially Mainframe Tape, within the IBM Germany Systems Technical Sales organization. Stefan has more than 20 years of experience in backup and archive solutions and holds a Master Degree in Electrical Engineering and Computer Science from the University of Mainz-Bingen, Germany. He also focuses on IBM Tape Encryption solutions, IBM Spectrum® Protect backup solutions and IBM Spectrum Archive EE solutions. He is a Level 2 IBM Master Certified IT Specialist and an IBM High-End-Tape Certified Specialist. Stefan is the chairman of the German Technical Focus Group “DRI & Tape.” He holds storage virtualization patents and is an IBM 2nd plateau inventor.

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 SME 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 with the TS7700 Development effort in the Product Test area (focused on Functional Verification aspects), where he has served as a Team Lead for the last 8 years.

Aderson Pacini works in the Tape Support Group in the IBM Brazil Hardware Resolution Center. He is responsible for providing second-level support for tape products in Brazil. Aderson has extensive experience servicing a broad range of IBM products. He has installed, implemented, and supported all of the IBM Tape Virtualization Servers, from the IBM VTS B16 to the IBM TS7700 Virtualization Engine. Aderson joined IBM in 1976 as a Service Representative, and his entire career has been in IBM Services®.

Trinidad Armando Rangel Ruiz is a Computer Engineer from the Universidad Tecnologica de Guadalajara, graduated in 2009, the same year he joined IBM. For IBM, he started as a Storage Technical Consultant with the Guadalajara Development Lab (GDL) Executive Briefing Center. Trinidad is a Top Gun for SystemX and Enterprise Storage and has worked on the TS7700 since 2016. Currently, he is the TS7700 Field Support Test (FST) team lead.

Michael Scott is a Senior DFSMS Technical Support Engineer for the IBM Systems, Client Enablement, and Systems Assurance team. He has 23 years of experience in DFSMS technical support. He holds a Masters in Business Administration degree and a Bachelor of Sciences degree in Mathematics. Michael has 14 patents for the computer sciences field, and he is a DFSMS Technical Advocate.

Joe Swingler is a lead architect for IBM TS7700 Virtualization Engine. Joe joined IBM in 1999 and started with the virtual tape subsystem team. He began working with ESCON and Fibre Channel connection (IBM 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 based on the IBM z/OS® platform. He has more than 25 years of experience in technical support for planning and installing mainframe tape products. He is working as a Client Technical Specialist and is involved with most of the TS7700 related projects in Japan.

Nao Takemura is a member of IBM Systems Lab Services in Tokyo, Japan. He joined IBM Japan in 2007 and worked as a technical specialist of compilers and assembler on z/OS, supporting the customers to upgrade their compilers. He works as a technical specialist of TS7700, and supports the customers with TS7700 planning and configuration, implementation, and migration.

Takahiro Tsuda is a software development engineer in Japan at the IBM Tokyo Laboratory. He has worked as a IBM TS7700 Virtualization Engine microcode developer since he joined IBM in 2007. He is responsible for developing and supporting TS7700 software components and functions that are related to HSM between disk and tape storage and data transfer between networks.

Chen Zhu is a Consulting System Service Representative at the IBM Global Technology Services® (GTS) in Shanghai, China. He joined IBM in 1998 to support and maintain IBM Z products for clients throughout China. Chen has been working in the Technical Support Group (TSG) providing second-level support to IBM Z clients since 2005. His areas of expertise include IBM Z hardware, IBM Parallel Sysplex®, IBM Tape Library, and FICON connectivity.

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

Erika Dawson
Jeff Fields
Katsuyoshi Katori
Kohichi Masuda
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 by 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:

  ibm.com/redbooks

- Send your comments in an email:

  redbooks@us.ibm.com

- Mail your comments:

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

Stay connected to IBM Redbooks

- 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 that were 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 TS7700 R5.2.2 Cloud Storage Tier Guide
as created or updated on October 6, 2022.

October 2022, Third Edition (minor update)

This revision includes the following update:

Updated 7.3, “Creating a custom vault” on page 41 to clarify that the TS7700 does not support the object retention features at this time.

July 2022, Third Edition

This revision includes the following new and changed information. The updates are based on new functions and changes for IBM TS7700 R5.2.2.

New and changed information highlights

- Added minor release level updates
- Updated GUI information in Chapter 7, “Setting up an IBM Cloud Object Storage object store” on page 37, and Chapter 8, “Setting up Amazon Web Services cloud object storage” on page 55.
- Added update for BMR Cloud Content support in 12.2, “Bulk Volume Information Retrieval example” on page 118

Mach 2021, Second Edition

This revision includes the following new and changed information. The updates are based on new functions and changes for IBM TS7700 R5.1.

New and changed information highlights

- Added Chapter 17, “Cloud Storage Tier export, recovery, and testing” on page 167 to describe the new Cloud Export function.
- The ability for any TS7700C cluster to immediately access data in the cloud once put there by any peer is referred to as *Grid Awareness* (see Chapter 4, “Introducing the IBM TS7700 Cloud Storage Tier” on page 17).
- Highlighted the following topics in Chapter 3, “IBM z/OS and object stores” on page 13:
  - z/OS Object Access Method (OAM) Cloud Support

  - IBM DS8000® Transparent Cloud Tiering (TCT)
  - DFSMShsm migration
  - DFSMSdss Full Volume Dump
- In addition to IBM Cloud Object Storage private and Amazon Simple Storage Service (S3), TS7700 at code level R5.0 or higher supports IBM Cloud Object Storage public and RSTOR as a cloud storage service. For more information, see Chapter 5, “IBM TS7700C planning considerations” on page 25.
- New cloud configuration examples are included in Chapter 10, “Configuration examples” on page 89.
- New Library Request cloud storage command descriptions were added to Chapter 16, “Library Request Commands for use with Cloud Storage Tier” on page 149.

March 2020, First Edition

This revision includes the following new and changed information.

Changed information

Updated Chapter 13, “Migration and upgrade considerations” on page 127 with information about migrating data from an existing TS7700C to a TS7700C in the grid configuration by using ghost copies.

> **Note:** This publication (R5.0) has a new book number. Its predecessor is *IBM TS7760 R4.2 Cloud Storage Tier Guide*, REDP-5514.

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 6

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, which means that 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.

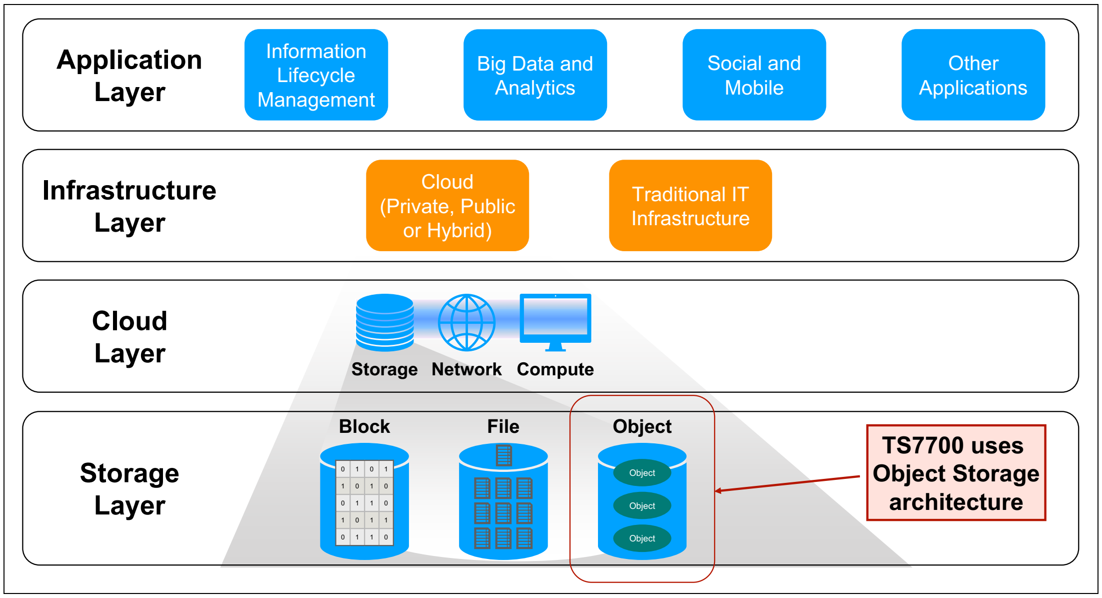
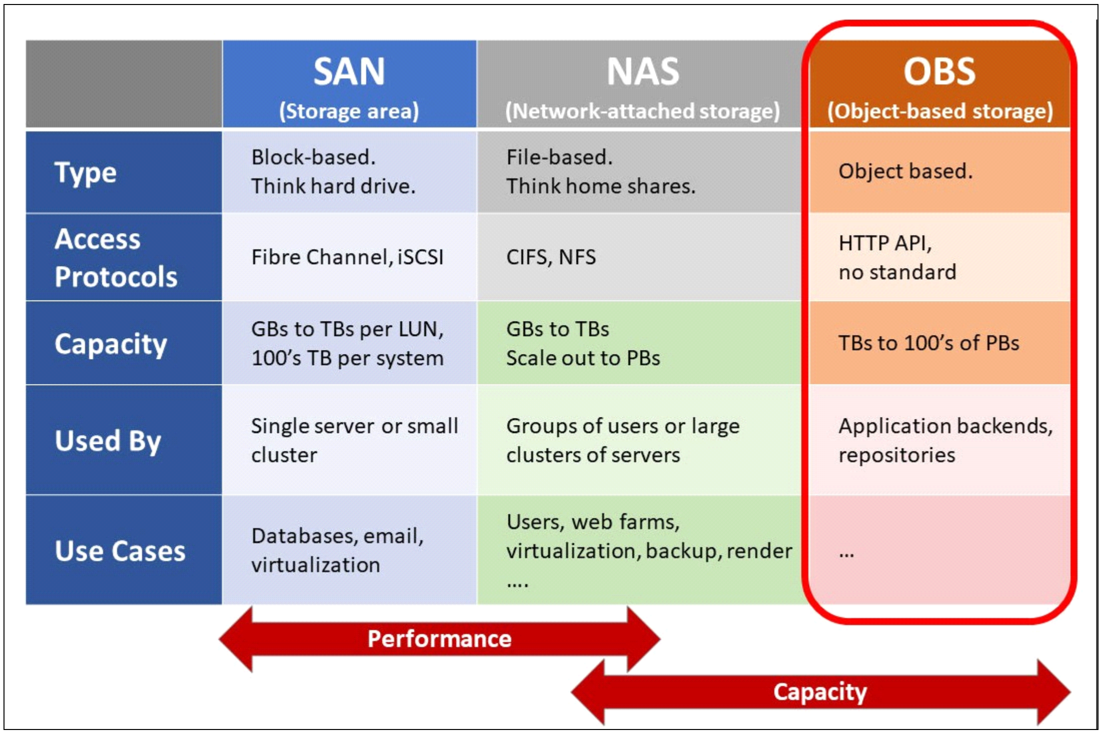


Figure 1-1 Transparent Cloud Tiering in the context of the cloud

The different storage types are compared from a network perspective in Figure 1-2 (storage area network (SAN) for block, network-attached storage (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:

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

1.2.1 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 or private network. 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 provider’s 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 regarding performance and often are assumed to be more secure.

1.2.2 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 realize all 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.

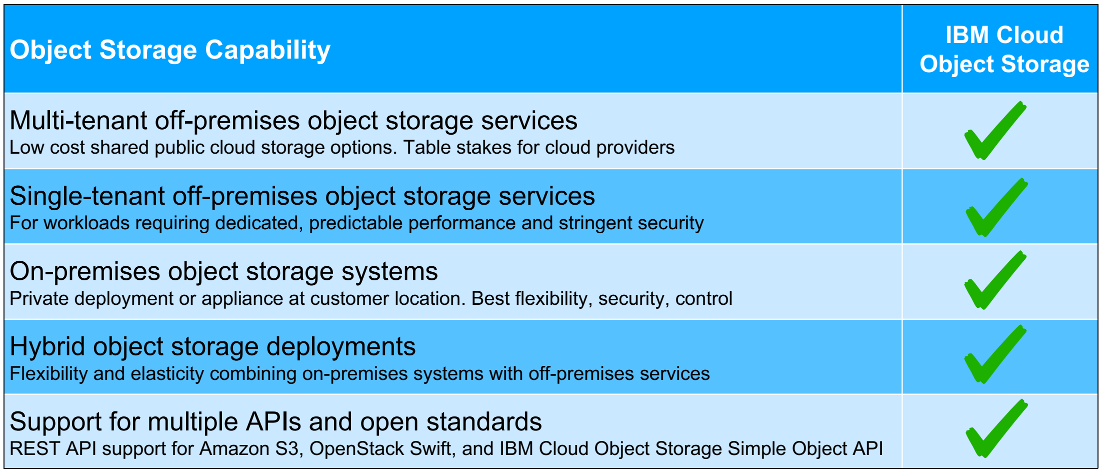
1.2.3 Hybrid cloud

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.

1.2.4 IBM Cloud Object Storage

IBM Cloud Object Storage 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 provide 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 colocate 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 the objects within that container by using tunable read, create, and delete access rights.

- Objects

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

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

  Many object store technologies also combine multi-part objects to form a single large object that easily exceeds 5 GB. This capability allows parts to be uploaded in smaller pieces but still represent all parts as a single object. The fact that it was uploaded by using many parts is forgotten after all the parts are combined. In such a case, a reverse direction multi-part read must be used to access these large objects. The sizes of the parts can differ from the original creation if the part size does not exceed the limits of the object store.

For most object sizes that are greater than 100 MB, the system performs multi-part reads. By using multi-part reads, the system can benefit from parallel part recalls which provide greater recall efficiency and support large objects. Although this processing is often contained within the client interface and hidden from the user application, it can be helpful to know that 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/*”
```

This example lists 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, “TS7700 object name format” on page 118.

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.

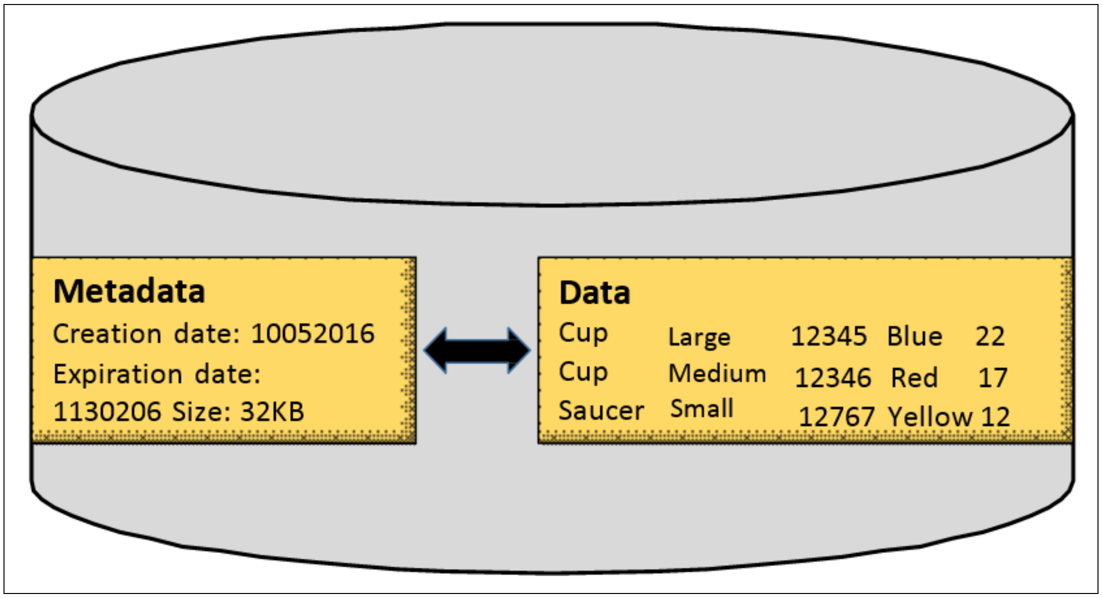


Figure 1-4 Data and metadata differences

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 about how different object stores provide resiliency through redundancy and geographical distance.

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 parity parts. By using parity techniques, 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 Cloud Object Storage 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 depends 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 that is stored, 1.7 units of available vault capacity is used. With the three site model, an entire region and a few 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 (RPO) if enough parts are written before the write returns.

Numerous IBM 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: Systems Edition*, REDP-5537
- 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 that are installed at each location where access of the IBM Cloud Object Storage data is required, or a location must have access to a remote Accesser node. For example, if two of the three regions have host presence, those two regions require Accesser 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. If no local Accesser nodes exist, a remote site's Accesser node can be used if network connectivity exists between the locations.

More information about IBM Cloud Object Storage, see IBM Documentation.

2.3 Amazon Simple Storage Service

Similar to IBM Cloud Object Storage Public, Amazon Simple Storage Service (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 (CRR) where buckets (*containers*) 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) depends 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.

2.4 RSTOR

Similar to IBM Cloud Object Storage Public, RSTOR 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, RSTOR offers multi-region replication options for objects. Objects that are contained within a bucket can be configured to replicate to *n* different regions.

The distance between the two or more regions is determined by the resiliency requirements of the organization. The two or more regions can span countries, continents, or even oceans if needed. The replication provides asynchronous consistency per region replica.

For more information about RSTOR, see RSTOR.

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” on page 14
- 3.2, “Tape Cloud Connector for z/OS” on page 14
- 3.3, “Advanced Archive for DFSMShsm” on page 14
- 3.4, “z/OS Object Access Method Cloud Support” on page 15
- 3.5, “DS8000 Transparent Cloud Tiering” on page 15
- 3.6, “TS7700 Cloud Storage Tier” on page 16
- 3.7, “Transparent Cloud Tiering” on page 16

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, this chapter focuses 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 at the time of writing.

3.2 Tape Cloud Connector for z/OS

With IBM Cloud Tape Connector for z/OS, you can 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 direct access storage device 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 direct access storage device before being offloaded to an object store through a gateway device. Any access of the tape from that point forward requires that it is recalled back into direct access storage device 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 Data Facility Storage Management Subsystem (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 Simple Storage Service (S3) cloud environments.

This offering provides direct IBM Z to cloud connectivity and is independent of the direct access storage device or tape technology that is used by the organization.

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

For more information, see this website.

3.4 z/OS Object Access Method Cloud Support

With APAR OA55700 (z/OS V2R3 and later), Object Access Method (OAM) can store and manage the primary copy of an OAM object on cloud storage through public, private, or hybrid cloud infrastructures that support the S3 API. Through SMS policies, an OAM object can be stored directly to the cloud or can migrate to the cloud based on the access requirements of the data. Also, you can recall an OAM object that is stored in the cloud back to the disk level of the OAM storage hierarchy. OAM managed backup copies continue to be supported for removable media, which are typically virtual or physical tape. Transparent to OAM, the IBM TS7700 can migrate OAM object data, including OAM managed backup copies to the cloud.

For more information, see the client documentation for APAR OA55700 and the z/OS DFSMS Planning, Installation, and Storage Administration Guide for Object Support.

3.5 DS8000 Transparent Cloud Tiering

The IBM DS8000 system, in combination with DFSMS, can tier data that is stored within the DS8000 to object store devices. The DS8000 system supports targeting different object store technologies, including the TS7700. When targeting a TS7700, the DS8000 system essentially becomes a user of the TS7700 Grid and offloads data directly to the TS7700 through TCP/IP, which eliminates the need to move the data through the IBM Fibre Channel connection (FICON) storage area network (SAN).

3.5.1 DFSMShsm migration

DFSMShsm can migrate data sets that are stored within the DS8000 system to object storage devices, including direct offload to a TS7700. Like how DFSMShsm supports ML2 (which often implies tape), DFSMShsm supports migration-level cloud (MLC).

By modifying existing or new migration policies, DFSMShsm can request that the DS8000 system migrate a data set from the DS8000 system directly to a chosen object store through TCP/IP. No data movement through the host occurs, and the data set’s granular management eliminates the need for DFSMShsm recycle processing and other hierarchical storage management (HSM) inefficiencies, which save CPU cycles on the host.

3.5.2 DFSMSdss Full Volume Dump

DFSMSdss can dump entire count key data (CKD) volumes within the DS8000 system to object store devices, including the TS7700. By modifying existing job control language (JCL), DFSMSdss can request that the DS8000 system dump a z/OS or Linux on IBM System z® volume to a chosen object store through TCP/IP connectivity. When dumping a volume, most of the CPU time is spent in data movement, and using Transparent Cloud Tiering (TCT) to dump volumes saves CPU cycles on the host.

For more information, see *IBM DS8000 and Transparent Cloud Tiering (DS8000 Release 9.2)*, SG24-8381.

3.6 TS7700 Cloud Storage Tier

The IBM TS7700 supports the ability to have logical volumes (LVOLs) tier to object stores, much as it supported tiering to physical tape since the 1990s. Through partitions and policy management, LVOLs 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 least recently used (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. In addition, the object store can support point-in-time (PiT) backups for disaster recovery (DR) and safeguarded recovery. This paper focuses on the TS7700 Cloud Storage Tier offering.

3.7 Transparent Cloud Tiering

Although 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 IBM TS7700 Cloud Storage Tier

In this chapter, we describe the TS7700 (TS7760 and TS7770) Cloud Storage Tier and its components.

4.1 Overview

Building on 25 years of virtual tape experience, the TS7700 can store virtual tape volumes in an object store. The TS7700 has always supported offloading to physical tape.

Offloading 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 offload to object storage.

Because object storage is cloud-based and accessible from different regions, the TS7700 Cloud Storage Tier support enables the cloud to be an extension of the grid. A high-level overview of TS7700 Cloud Storage Tier support is shown in Figure 4-1.

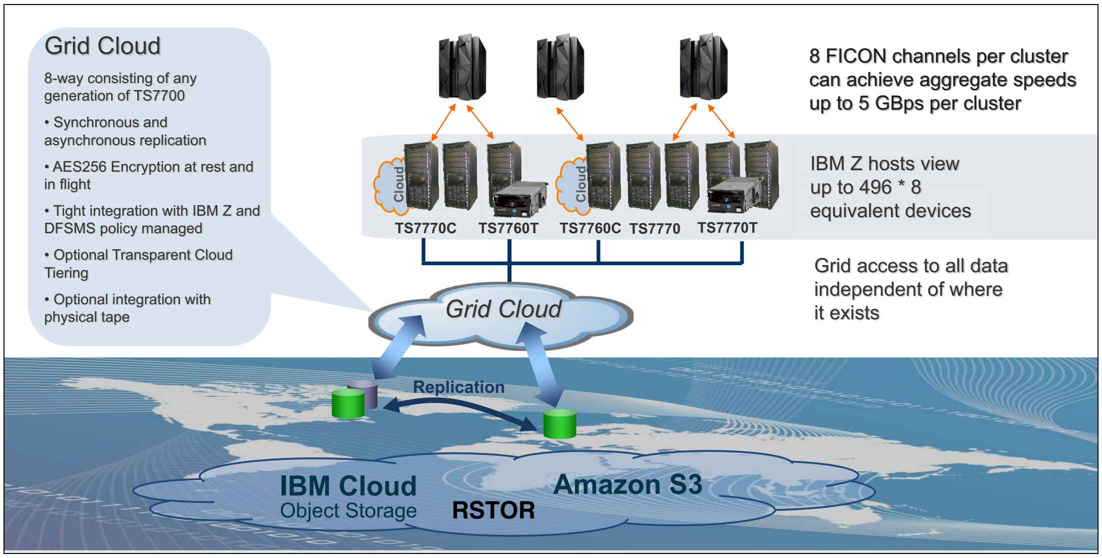

Grid Cloud
8-way consisting of any generation of TS7700
• Synchronous and asynchronous replication
• AES256 Encryption at rest and in flight
• Tight integration with IBM Z and DFSMS policy managed
• Optional Transparent Cloud Tiering
• Optional integration with physical tape
8 FICON channels per cluster can achieve aggregate speeds up to 5 GBps per cluster
IBM Z hosts view up to 496 * 8 equivalent devices
Grid access to all data independent of where it exists
Cloud
Cloud
TS7770C
TS7760T
TS7760C
TS7770
TS7770T
Grid Cloud
Replication
IBM Cloud
Object Storage
RSTOR
Amazon S3

Figure 4-1 High-level overview of TS7700 Cloud Storage Tier support

4.1.1 Cloud Storage Tier enabled cluster

A Cloud Storage Tier enabled cluster, or TS7700C, can be a member of any grid if the peer cluster code levels are compatible. Peers can be other TS7700C clusters, TS7700T clusters, or disk-only TS7700D clusters. By using Management Class (MC) policies, virtual volumes are replicated among peers in the grid. Those peers with Cloud Storage Tier support optionally can offload to an object store or have access to data in an object store if another peer has already offloaded a copy.

After one TS7700C cluster offloads a logical volume (LVOL), other TS7700C clusters in the same grid are made aware of the cloud copy. This process occurs immediately after the premigration from one TS7700C completes. If another TS7700C that also contains a replicated grid copy attempts to premigrate the same volume to the cloud, it skips the premigration process because it is aware of the copy that was put there by another TS7700C peer. Then, either cluster can recall the LVOL from the cloud if needed. In addition, any TS7700C cluster can also access the copy in the cloud, even if the TS7700C cluster has not received or is not configured to receive a grid copy of the LVOL. This ability for any TS7700C cluster to immediately access data in the cloud once put there by any peer is referred to as *Grid Awareness*, and it is an enhancement that was added in the R5.1 release.

If SYNC or RUN copy mode is selected and two or more TS7700C clusters attempt to premigrate the same volume concurrently, there is a small chance that two or more objects can be created for the same volume. Having two or more independent copies of the same volume in the object store is a supported outcome and does not prevent the grid from accessing data in the cloud. The two copies of a specific LVOL remain in the cloud until the LVOL is modified or expires.

LVOLs offload in their entirety to the object store. If the only available LVOL copy in the grid is within an object store, one of the TS7700C clusters can recall it into the disk cache. After the entire volume is in the disk cache, the content is accessible by using existing grid techniques, such as remote mounts.

For those LVOLs that premigrate to the cloud, a Cloud Export or TS7700 database backup can also be stored in the cloud, which provides a point-in-time (PiT) recovery point for disaster and safeguarded recovery. Cloud Export and Cloud Export Recovery are enhancements that are added in the R5.1 release. For more information, see Chapter 17, “Cloud Storage Tier export, recovery, and testing” on page 167.

Because a LVOL must be recalled entirely when the only copy exists in the cloud, choosing LVOL sizes that are smaller can provide faster time to access when only a subset of the content in the LVOL is required.

A high-level overview of how a TS7700C cluster can use an object store as a tier of storage is shown in Figure 4-2.

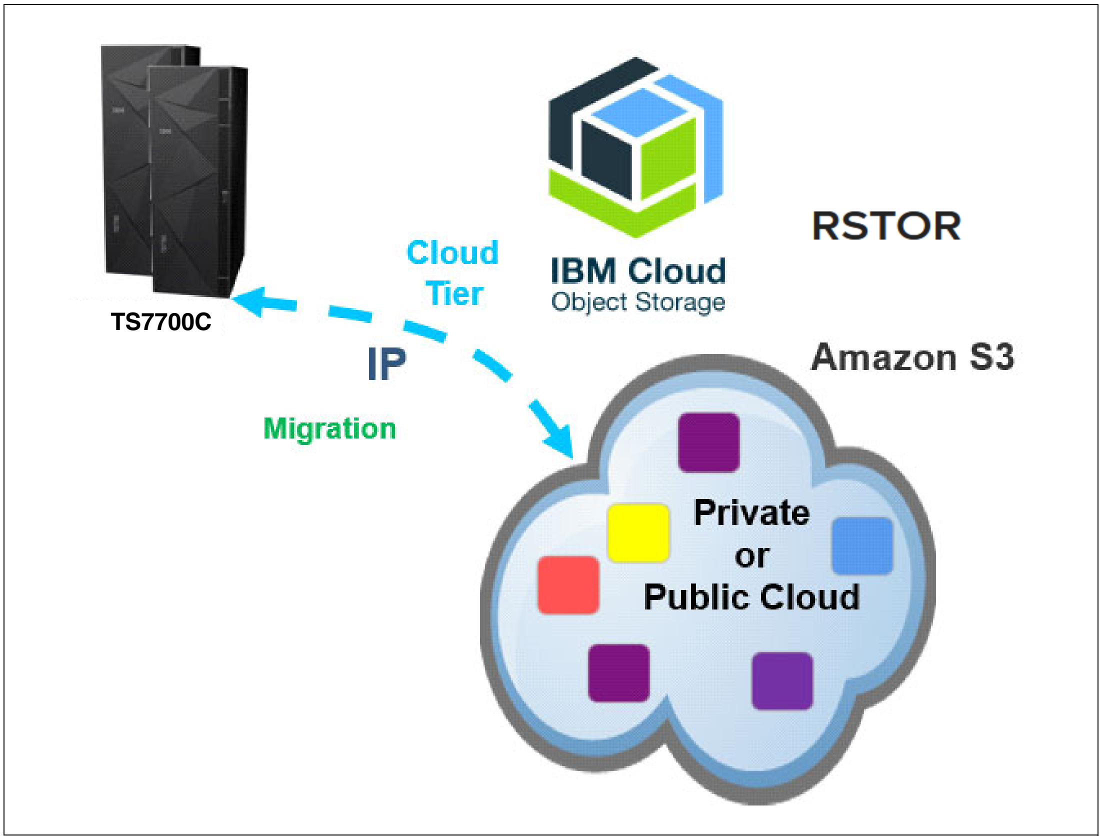


Figure 4-2 High-level overview of how an object store can be a storage tier behind the TS7700 cluster

Similar to TS7700 Tape Attach, the TS7700C includes disk cache partitions that are available to manage the disk cache footprint of the TS7700C. 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.

TS7700C disk cache partition support works much the same as TS7700T, as shown in Figure 4-3.

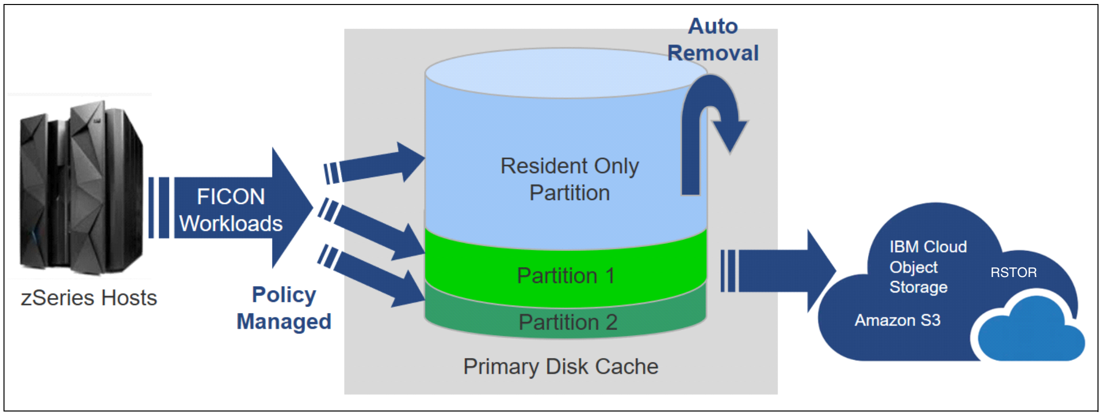


Figure 4-3 Partition support for the TS7700C

LVOLs that target any partition other than the residency-only partition are queued for premigration to an object store immediately after being closed. The policy that is assigned to the LVOL and how much space is available in the partition determines if and when the LVOL is removed from disk cache after the premigration completes. As with the TS7700T system, the copy in disk cache is removed, which makes the cloud instance the only available copy in that cluster. A recall of the LVOL 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 TS7700C 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 Accesser nodes that are used for connectivity to the IBM Cloud Object Storage vault.

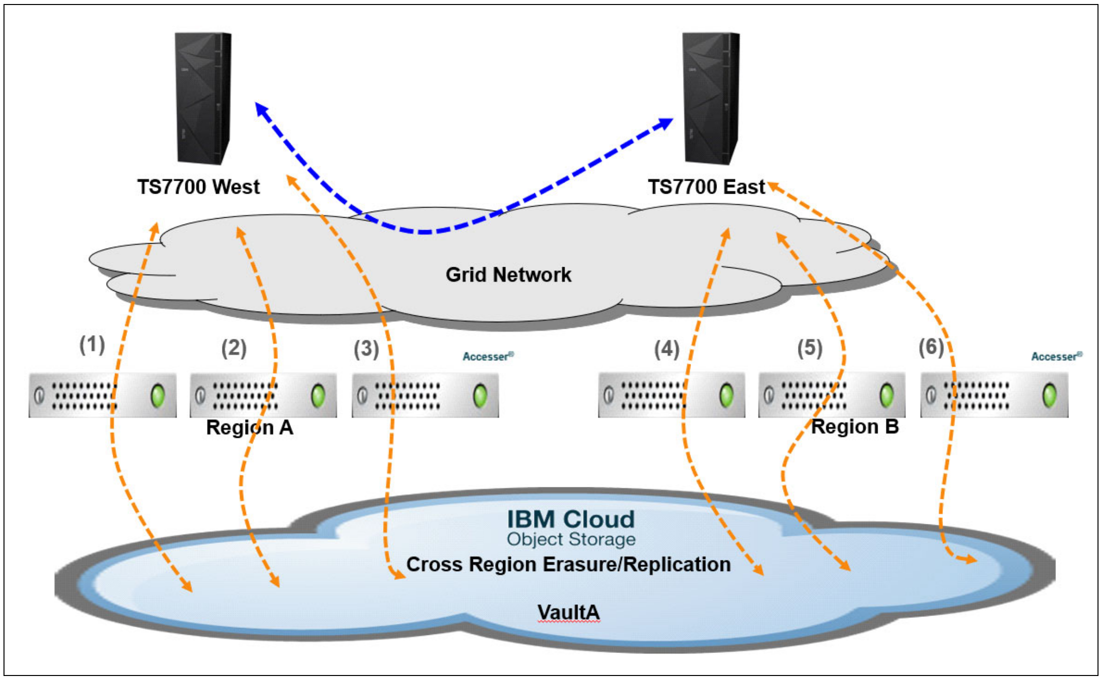


Figure 4-4 Two region access to an IBM Cloud Object Storage

Another sample of a cross region replication configuration for Amazon Simple Storage Service (S3) is shown in Figure 4-5.

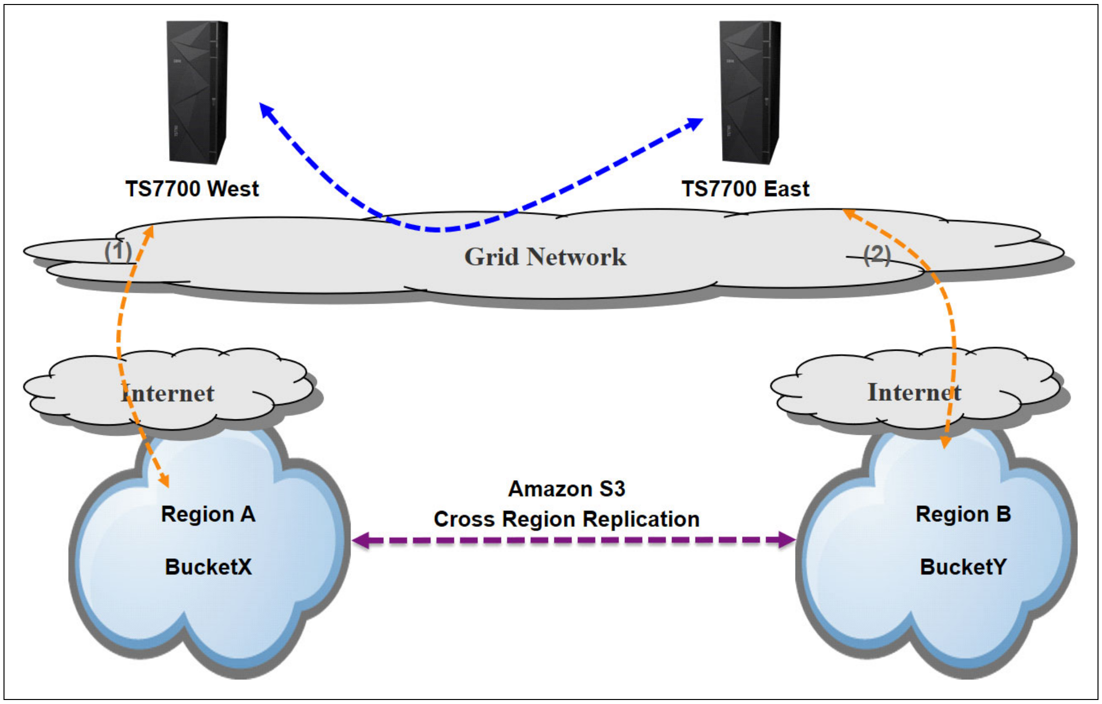


Figure 4-5 Cross Regional Amazon S3 configuration

Like grids where TS7700 disk-only clusters are mixed with TS7700T clusters, the TS7700C cluster can be mixed within the same grid of other TS7700D and TS7700T clusters. At the time of writing, a particular cluster cannot be both Tape Attach and support Cloud Storage Tier concurrently; 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 TS7700C clusters as they did with TS7700T clusters. An example of a Hybrid grid where TS7700, TS7700C, and TS7700T clusters exist is shown in Figure 4-6. By using auto-removal policies, data can migrate toward the clusters with deep capacity through physical tape or cloud storage tier support.

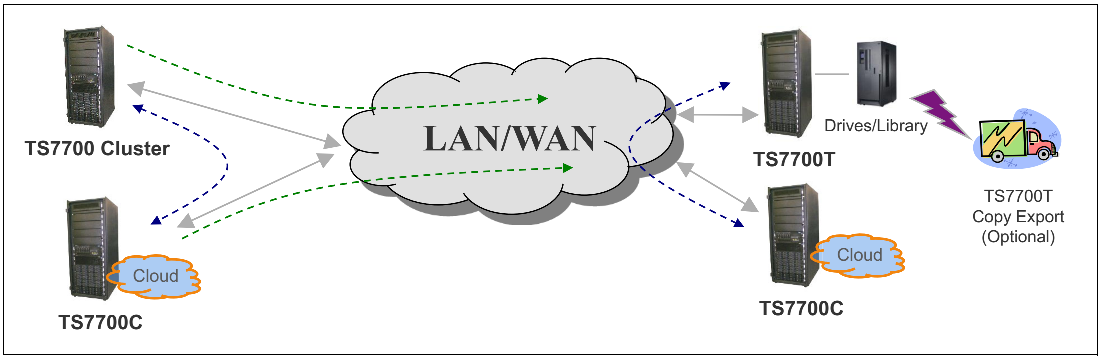


Figure 4-6 Hybrid grid configuration with TS7700C, TS7700T, and TS7700 clusters

4.1.2 TS7700C cloud pools

Cloud pools are used by the TS7700C to separate 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 LVOLs that are assigned to the particular cloud pool are in the same object store container or mirrored containers. A LVOL can target only one cloud pool within a grid, so the cloud pool definition within each TS7700C cluster must reference the same object store container or mirrored containers. As of R5.2.2, up to 256 cloud pools can be defined.

4.1.3 TS7700C accounts

Accounts are used by the TS7700C 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 TS7700C cluster can authenticate with object stores to store data for a specific cloud pool. Each TS7700C cluster can use a different account per cloud pool to provide flexibility when different accounts are used per region or use case.

4.1.4 TS7700C containers

Containers are used by the TS7700C 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.

TS7700C container URLs

URLs are required before vaults or buckets can be accessed. After one or more TS7700C containers are defined, one or more URLs can be assigned to that container. The URLs provide the address that the TS7700C uses to communicate with the vault or bucket endpoint in the object store. For IBM Cloud Object Storage, this URL can be one or more IP addresses that are associated with Accesser nodes, network load balancers, or NGINX proxy servers.

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 TS7700C 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 TS7700C cluster. However, which clusters use which URLs can be unique, so a cluster association with each cluster and its assigned URLs must be made. An example is when each region uses a different set of Accesser nodes and each one has their own unique URLs.

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.

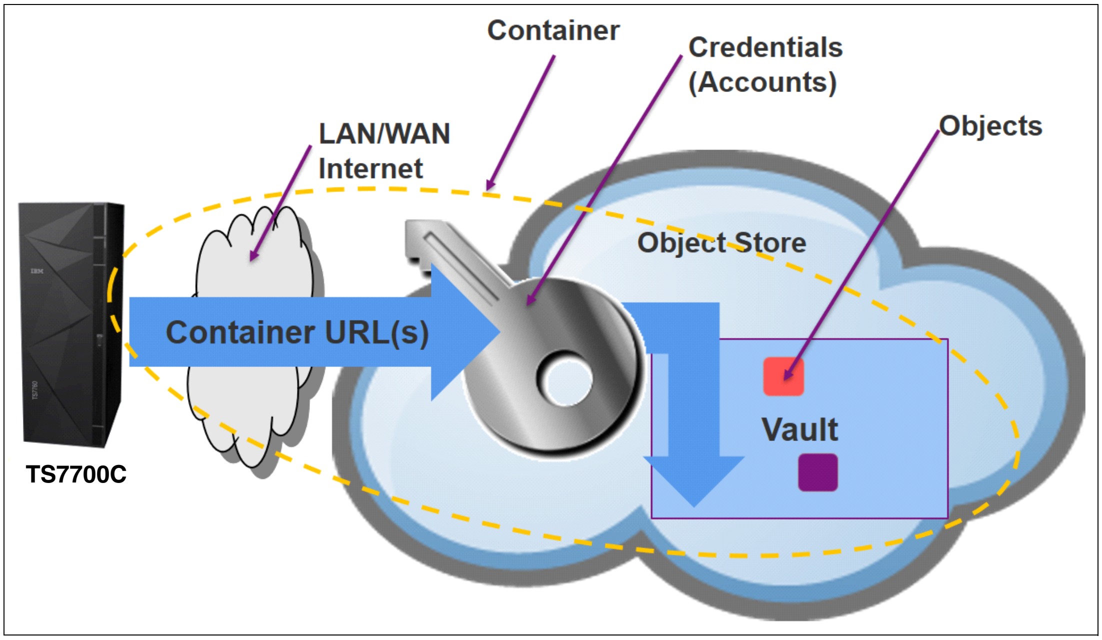


Figure 4-7 Overview of URLs, accounts, and containers

4.1.5 Container replication

In this section, we describe how the TS7700C 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 nodes to be used from an IBM Cloud Object Storage setup. With container URL definitions, each region can access a different set of URLs or Accesser nodes so that the most efficient local connection into the object store is used.

When vault mirroring or cross-region replication (CRR) 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 TS7700C attempts to premigrate LVOLs to a container where a copy exists, the TS7700C always checks whether the volume 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” is available at the alternative location. This check is most important in cases where eventual consistency occurs for multi-region replication.

5

IBM TS7700C planning considerations

In this chapter, we describe planning considerations for the TS7700C.

5.1 Overview

Beginning with release level 4.2, the TS7760 supports the Cloud Storage Tier feature for stand-alone and grid configurations. Release level 5.0 with the TS7770 continues that support. In this Redpaper publication, *TS7700* is used to include both TS7770 and TS7760. 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 R4.2 or higher before the TS7760 can be cloud-enabled. A TS7770 is at code level R5.0 level or higher.
- The Cloud Storage Tier feature, which is Feature Code (FC) 5278, can be enabled on a TS7700 non-concurrently.
- A total of 64 GB total physical memory is required before FC 4278 can be installed. Another 32 GB of memory (FC 3466) is a co-requisite to enabling Cloud Storage Tier support.
- The cloud enablement feature can be ordered (FC 5278) so that a TS7700 can be upgraded to attach to a cloud storage tier if it does not have tape that is attached. Cloud enablement and the tape attach feature are mutually exclusive. A TS7700 cannot be connected to a cloud storage tier and physical backend tape. However, a hybrid grid can be created with a TS7700T and TS7700C present.
- The TS7700 at code level R4.2 supports only IBM Cloud Object Storage private configurations with a fixed IP addressable endpoint on port 80 (for http) or 443 (for https) and public Amazon Simple Storage Service (S3) cloud object storage that is addressable through 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. In addition to IBM Cloud Object Storage private and Amazon S3, TS7700 at code level R5.0 or later supports IBM Cloud Object Storage public and RSTOR as cloud storage services.
- A TS7700 can be a TS7700C or TS7700T. The tape attach and cloud storage tier are currently mutually exclusive in the 4.2 release or higher.
- Any cloud hardware (IBM Cloud Object Storage), 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 IBM TS7700C” on page 117.
- A cloud container is accessible by way of a URL, which includes a hostname (for Amazon S3) or IP address (for IBM Cloud Object Storage). A hostname is resolved to an IP address by a Domain Name System (DNS). A TS7700 DNS IP address must be specified if a cloud URL includes a hostname, and the hostname 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 (MI) network must have a configurable DNS server capable of converting `*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.

5.1.1 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 FC 5278 installed and enabled is listed in the rightmost 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 Clusters	Existing Clusters	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.

5.1.2 Postinstallation 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 that 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 (LVOL) from CP0 to a CPx disk cache partition at code level R4.2, premigration to the cloud does not occur if the volume's Storage Group (SG) assignment did not previously assign it a cloud pool rank when the LVOL was last mounted. A mount or dismount is required to trigger a premigratoin to the cloud. Therefore, it is ideal that all LVOLs that are created in any cluster in a grid always assign a pool rank in anticipation of future `PARTRFSH` commands. At code level R5.0 or later, a mount or dismount is not needed because `PARTRFSH` can be used with the `MMOUNT` option to move a LVOL from CP0 to a CPx and assign a cloud pool rank. For more information, see Chapter 13, "Migration and upgrade considerations" on page 127.
- When `COPYRFSH` is used to copy a LVOL to a TS7700C cluster CPx disk cache partition at code level R4.2, premigration to the cloud does not occur if the volume's SG assignment did not previously assign it a cloud pool rank when the volume was last mounted by a host. A mount or dismount is required to trigger a premigratoin to the cloud. Therefore, it is ideal that all LVOLs that are created in any cluster in a grid always assign a pool rank in anticipation of future `COPYRFSH` commands. At code level R5.0 or later, a mount or dismount is not needed because `PARTRFSH` can be used with the `MMOUNT` option to move a LVOL from CP0 to a CPx and assign a cloud pool rank. Make sure that a cloud pool rank is assigned to a LVOL before running `COPYRFSH` commands. For more information, see Chapter 13, "Migration and upgrade considerations" on page 127.

6

SSL certificate

When a secure HTTPS connection is used to access a connected object store, SSL certificates are required to set up 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 (CA) 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 provide an identity signature that helps any client to certify that 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 CA that signed the certificate. The authority that signed the certificate is referred to as the 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 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 TS7700 is the client in this case and must trust the server (for example, IBM Cloud Object Storage) and the certificates it provides.

The TS7700 Management Interface (MI) 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 Cloud Object Storage Private) requires 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 Simple Storage Service (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 Storage

In this section, we describe how to set up your IBM Cloud Object Storage 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 window, 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 window, click **Add CA**. In the Add External CA window, follow the steps as described at this IBM Documentation web page.

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

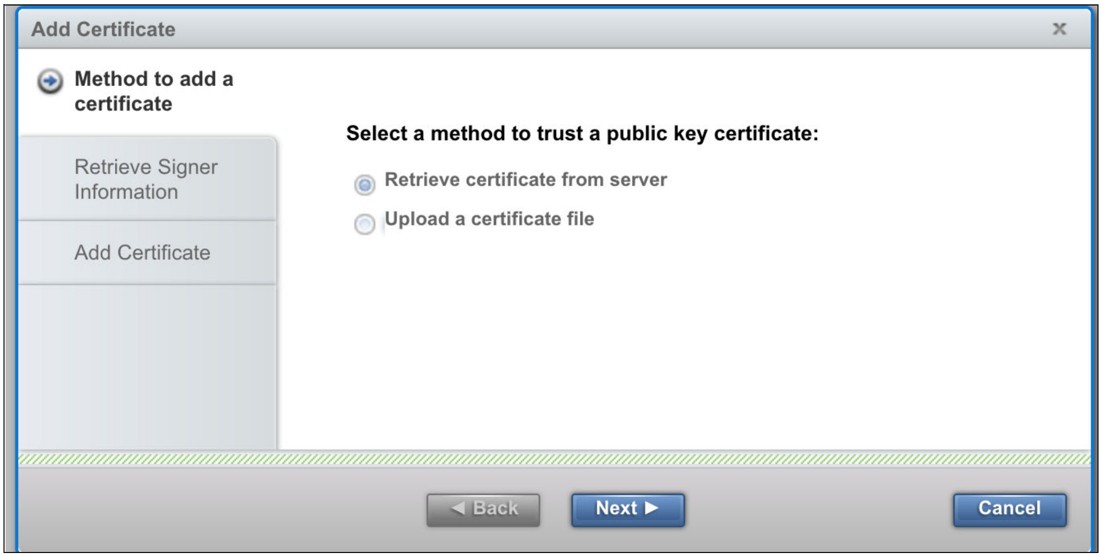
After an SSL certificate CA is set up on your IBM Cloud Object Storage, you must update the TS7700 to trust the CA that is used by the IBM Cloud Object Storage device. Which CA type is used determines which method is used to update the TS7700.

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 IBM Cloud Object Storage setup can expire sooner than the CA manually uploaded.

To automatically retrieve an IBM Cloud Object Storage CA, complete the following steps:

1. Select **Access** → **SSL Certificates** using TS7700 MI.
2. On the SSL Certificates window, click **New Certificate**.
3. On the Add Certificate window, select **Retrieve Certificate from server**, as shown in Figure 6-1.

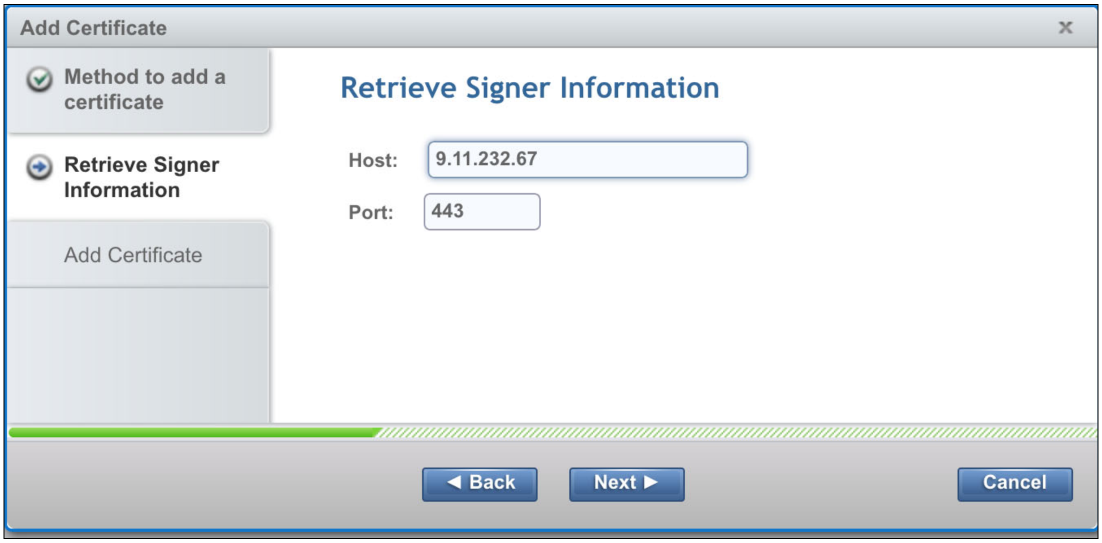

Select a method to trust a public key certificate:

● Retrieve certificate from server

○ Upload a certificate file

Figure 6-1 Retrieving SSL certificate (Step 1)

4. Then, enter the IP address of your IBM Cloud Object Storage Accesser node and click **Next**, as shown in Figure 6-2.



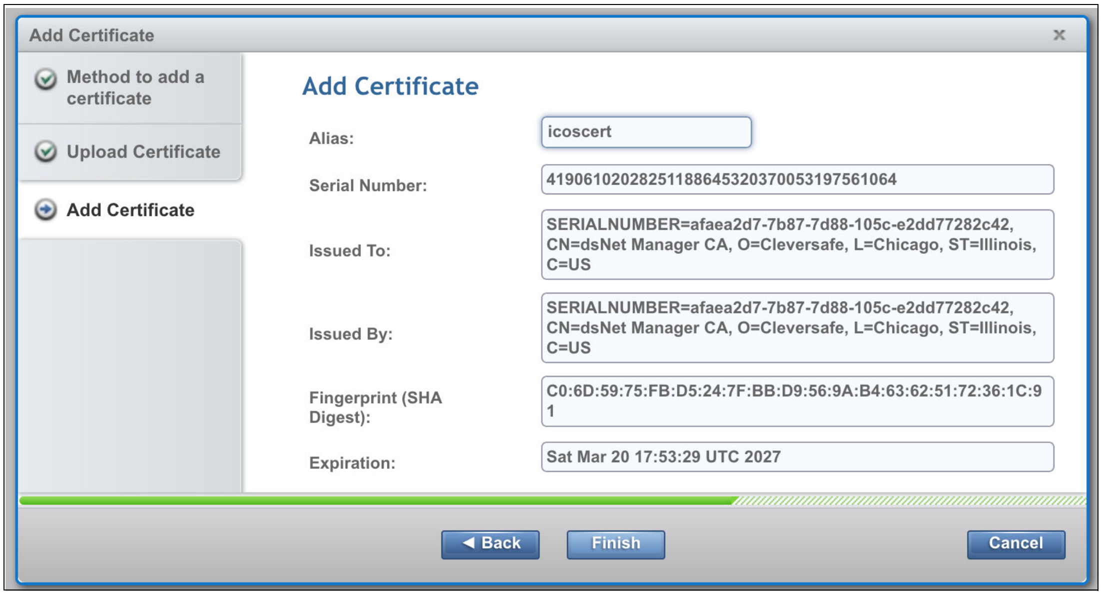
Retrieve Signer Information

Host: 9.11.232.67

Port: 443

Figure 6-2 Retrieving SSL certificate (Step 2)

5. Enter an alias of your internal SSL certificate (for example, `icoscert`) and click **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.



Add Certificate

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)

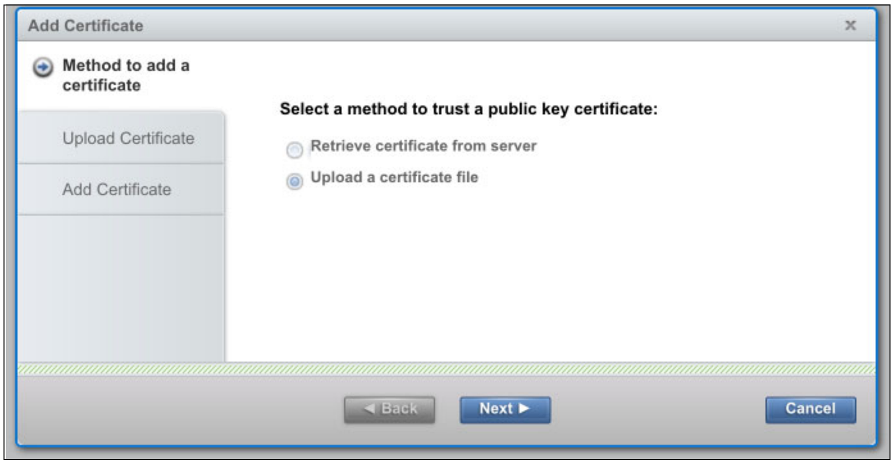
When manually uploading the trust of CA through a text file, select the Security menu in IBM Cloud Object Storage Manager and click **certificate authority** in the **System Fingerprint** field. Copy all the text that is displayed in your web browser, including “`-----BEGIN CERTIFICATE-----`” and “`-----END 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 Contents of the .pem file

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

MIIF1DCCA7ygAwIBAgIQH4bSWUjefmHgSojBqPd86DANBgkqhkiG9w0BAQ0FADCB
kTELMAkGA1UEBhMCVVMxETAPBgNVBAgMCElsbGlub2lzMRAwDgYDVQQHDAdDaGlj

…

IuSo89i55ct0+RL97GEgpQpfVIYgdefK3DNyA+IKgyS7nOntwoRjQ5MXgCWZUeNr
LjFOnrBSux8=
-----END CERTIFICATE-----
```

Next, you must upload the certificate file to the TS7700 by using MI. Complete the following steps:

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



Add Certificate

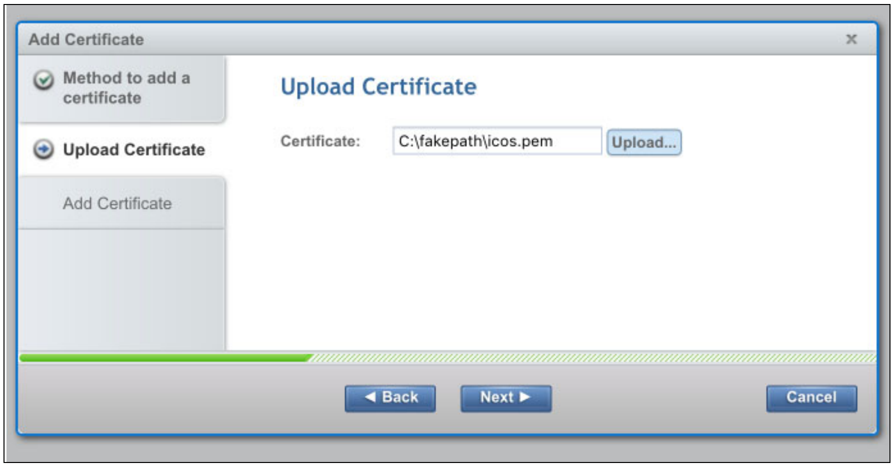
Select a method to trust a public key certificate:

○ Retrieve certificate from server

● Upload a certificate file

Figure 6-4 Selecting the Upload certificate file option

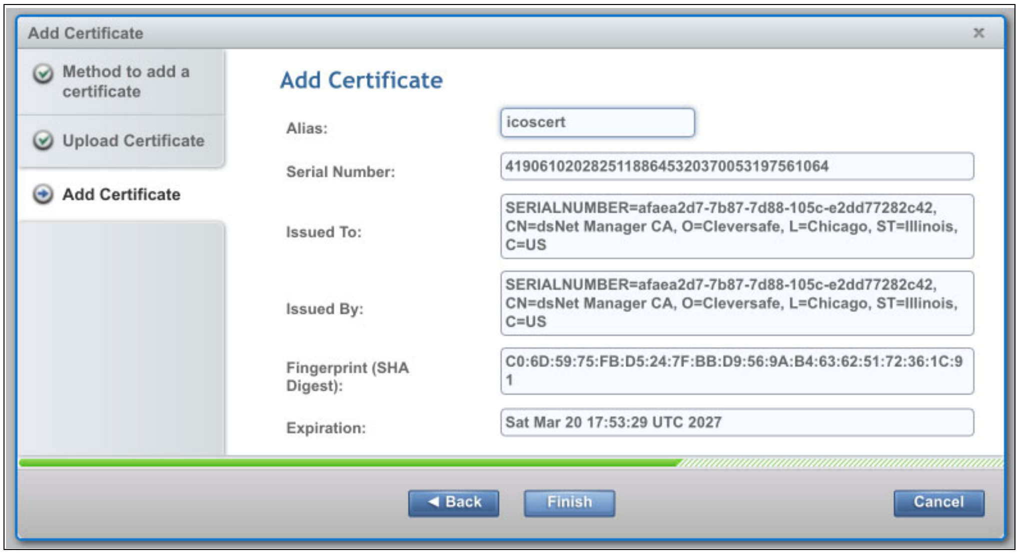
4. Click **Upload**, select your SSL certificate file (for example, `icos.pem`), and then, click **Next**, as shown in Figure 6-5.



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** (see 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.



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 6-6 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 IBM TS7700 for Cloud Storage Tier” on page 73.

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:

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 username plus password:
  - Access key ID
  - Secret access key

IBM Cloud Object Storage is presented as on-premises or off-premises (public) offering types. For the TS7700 at code level R4.2, on-premises IBM Cloud Object Storage is supported. IBM Cloud Object Storage off-premises (public) is supported by a Request for Price Quotation (RPQ).

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 uses 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 (MI) 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 IBM 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 that the storage pools were prepared in advance to allocate vaults for using TS7700 storage made 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 be used only 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 7.3, “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.

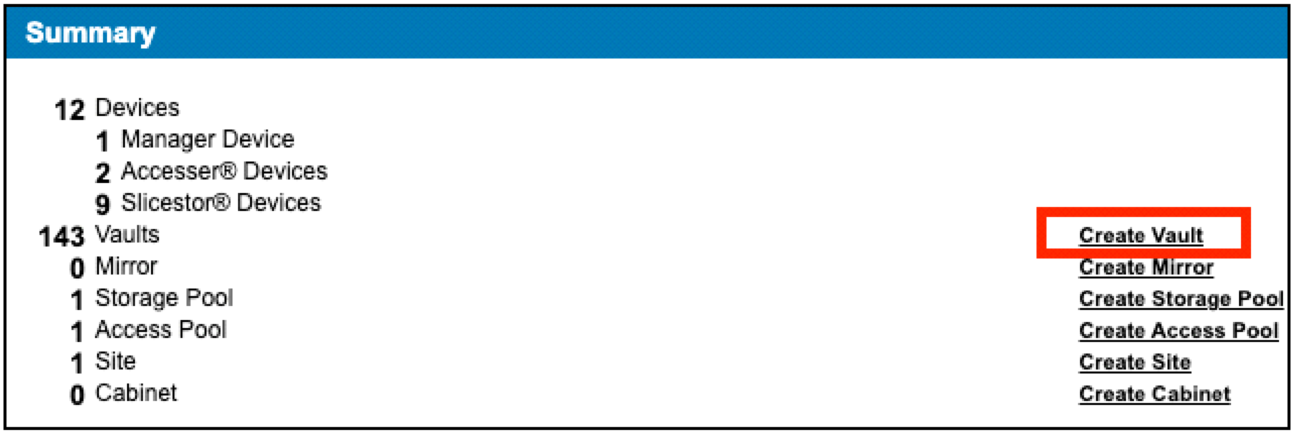
Vaults can be created by using the following methods:

- 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 IBM Cloud Object Storage Manager website of the corresponding on-premises IBM Cloud Object Storage. Select the **Configure** tab, click **Create Vault** in the Summary section (see Figure 7-1).

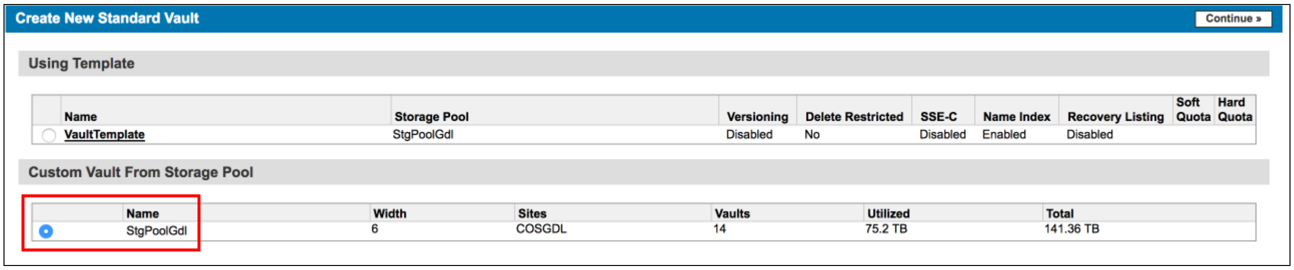


Summary

12 Devices		
1 Manager Device		
2 Accesser® Devices		
9 Slicestor® Devices		
143 Vaults		Create Vault
0 Mirror		Create Mirror
1 Storage Pool		Create Storage Pool
1 Access Pool		Create Access Pool
1 Site		Create Site
0 Cabinet		Create Cabinet

Figure 7-1 Create Vault option in the Configure window

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**.



Create New Standard Vault

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

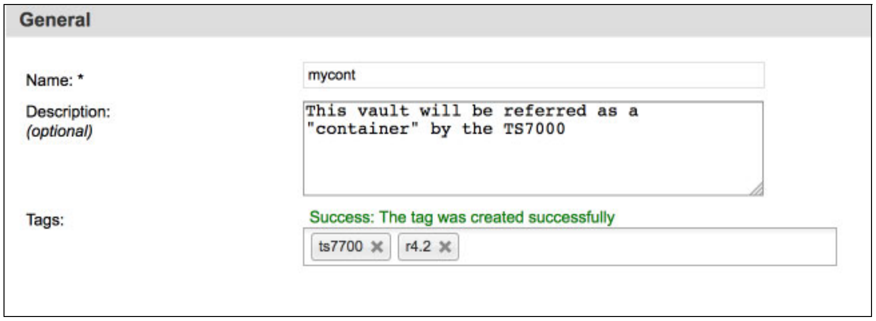
3. In the General section (see Figure 7-3), the following settings are available:

   – 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

ts7700 ✕ r4.2 ✕

Figure 7-3 Creating standard vault

   – The following options can be available in this window, 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 Simple Storage Service (S3) GET Service Extended and S3 GET Bucket Location APIs, are populated with the value set for region.
     - Storage Class (SC): 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 SC.

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.

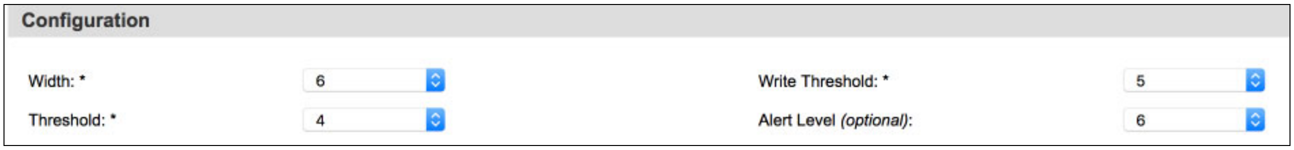
   – Threshold: The minimum number of slices that must be available to perform a read:

     - 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

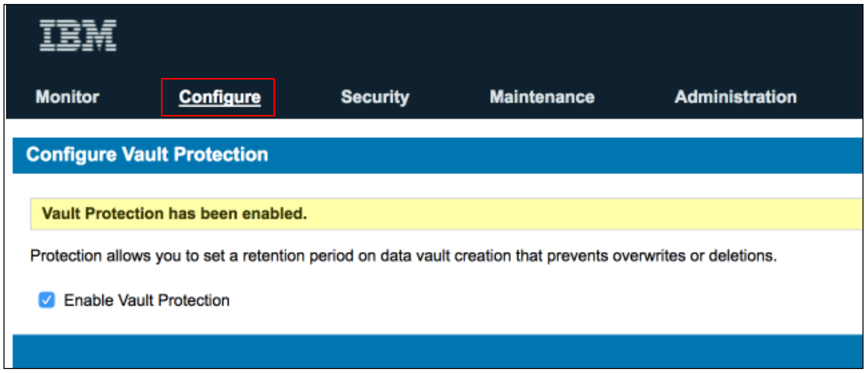
Write Threshold: * 5

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 an 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

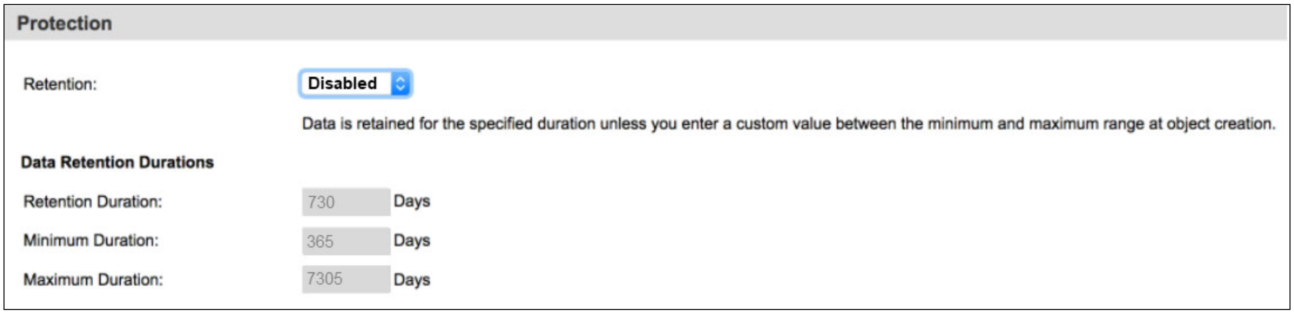
Figure 7-5 Enabling vault protection for the IBM Cloud Object Storage system

When a vault is created, the *Protection* section (see Figure 7-6 on page 45) displays only if the Vault Protection Configuration options were 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:** The TS7700 does not support retention enablement at this time. The retention descriptions below are for educational purposes only.

- Retention: This option is *not* supported for TS7700 at this time, and should be set to “disabled” (see Figure 7-6 on page 45). 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: Disabled

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

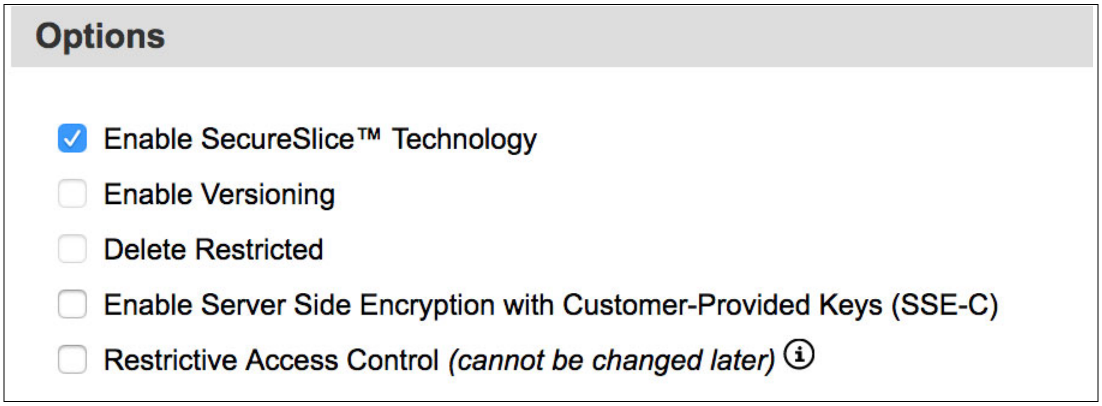
Retention Duration: 730 Days

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), complete the following fields.



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

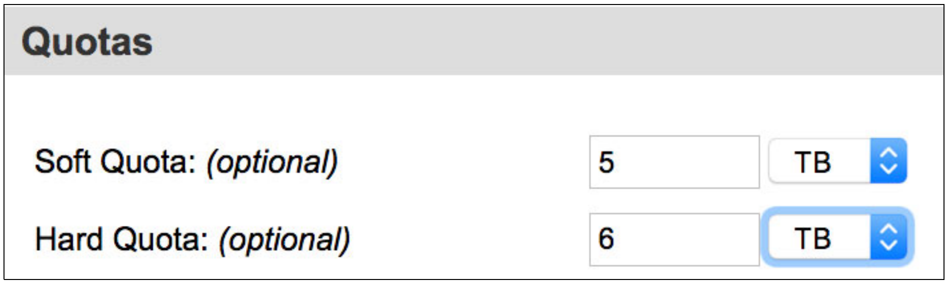
- Enable SecureSlice Technology: This optional setting provides extra encryption benefits that are combined with dispersal. This option is selected by default for new vaults. The feature can be deactivated, although it is not recommended. If it is cleared, a warning message appears, and a confirmation 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 object stores, 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).

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.

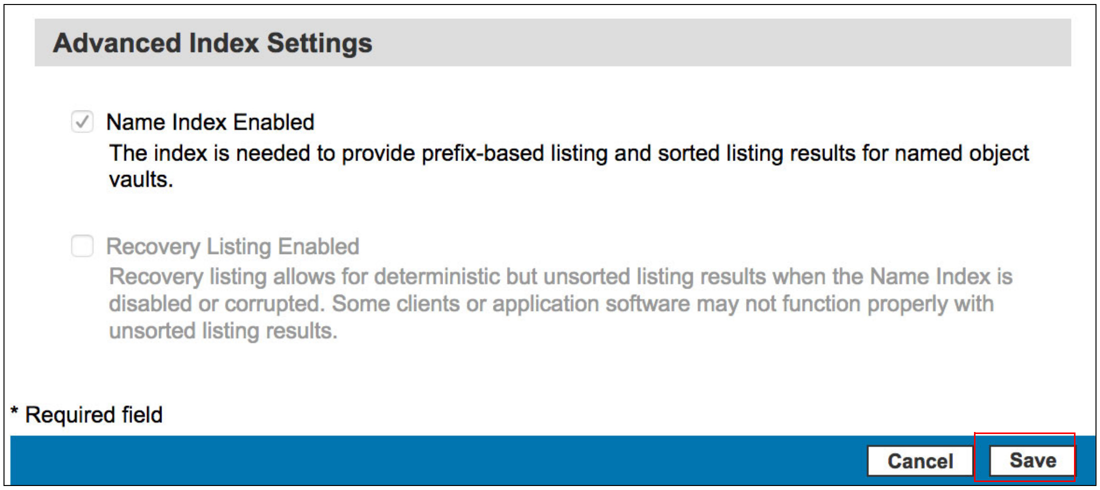

Quotas

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 on page 47), 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.

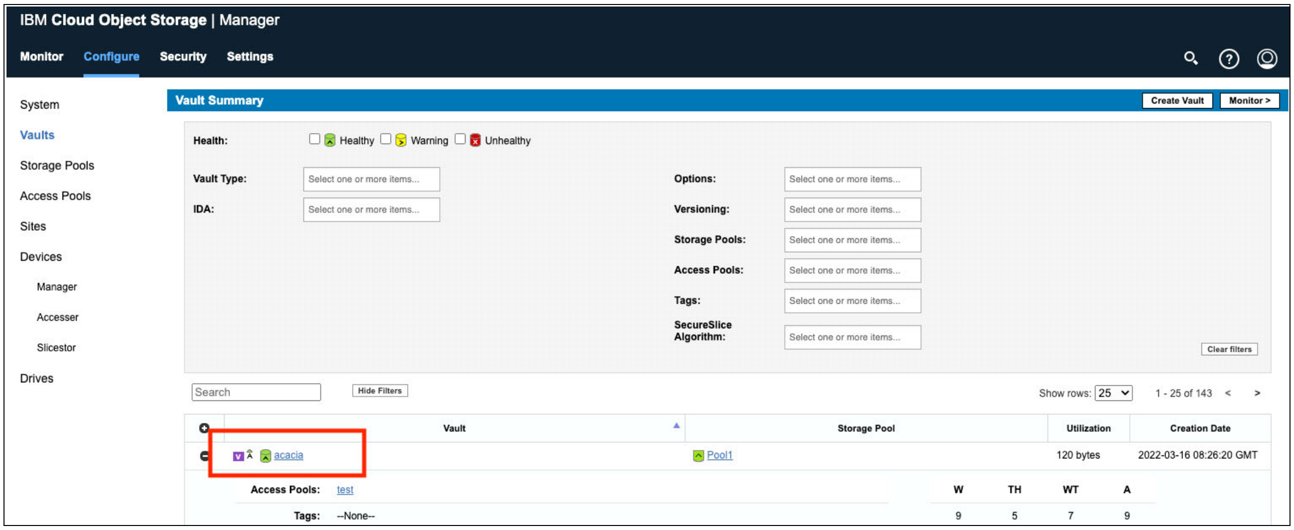
□ Recovery Listing Enabled
Recovery listing allows for deterministic but unsorted listing results when the Name Index is disabled or corrupted. Some clients or application software may not function properly with unsorted listing results.

* 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.



Health: □ Healthy □ Warning □ Unhealthy

Vault Type:	Select one or more items...	Options:	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...
		Tags:	Select one or more items...
		SecureSlice Algorithm:	Select one or more items...

Show rows: 25 1 - 25 of 143 < >

Vault	Storage Pool	Utilization	Creation Date
acacia	Pool1	120 bytes	2022-03-16 08:26:20 GMT

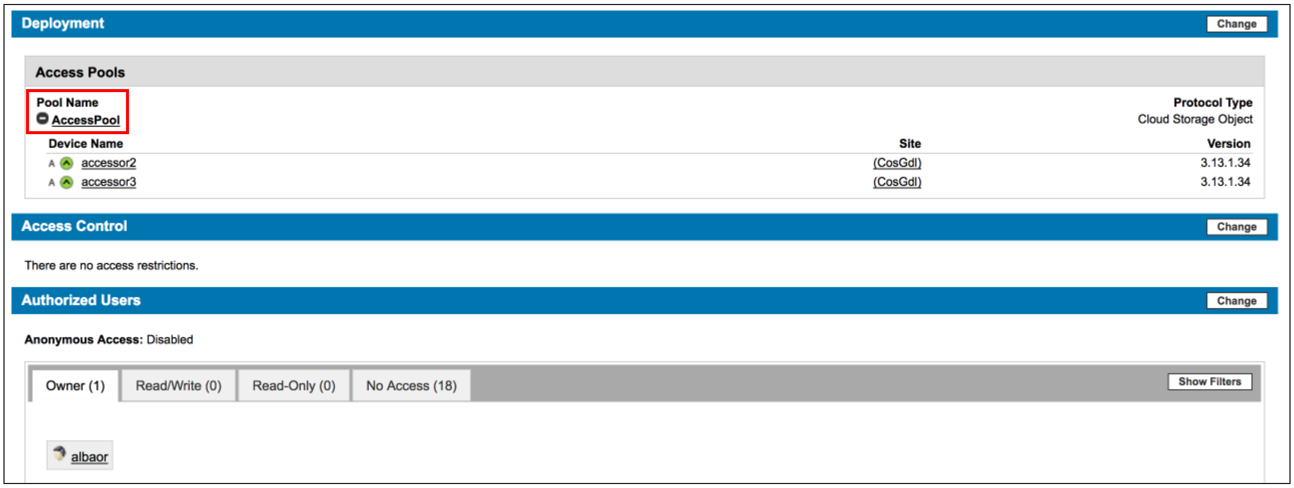
Access Pools: test
Tags: --None--

W	TH	WT	A
9	5	7	9

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

Access Pools

Pool Name	Protocol Type
AccessPool	Cloud Storage Object

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

Access Control

There are no access restrictions.

Authorized Users

Anonymous Access: Disabled

albaor

Figure 7-11 Adjusting other vault properties

7.4 Using vault templates

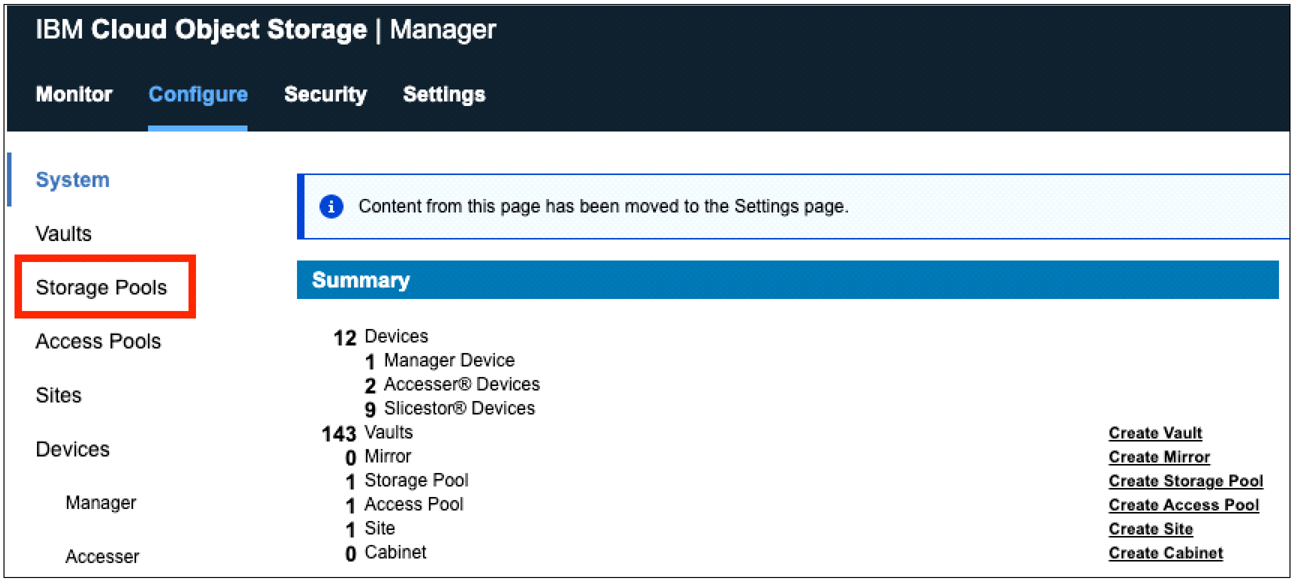
An alternative approach to vault creation is based on the use of vault templates. These templates allow a user to create multiple vaults with the same parameters quickly and enable common vault configurations to be used across multiple users.

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 IBM Cloud Object Storage Manager website of the corresponding on-premises IBM Cloud Object Storage. Click the **Configure** tab (see Figure 7-12) and then, click the **Storage Pools** navigation menu.



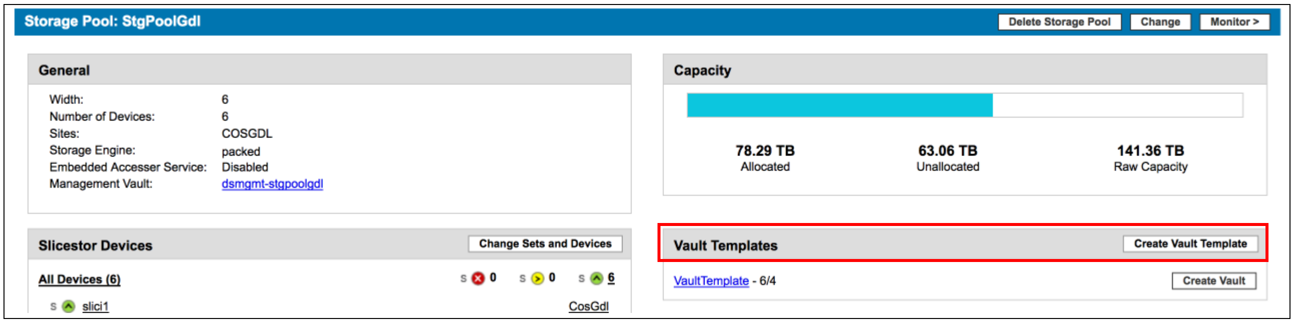
Content from this page has been moved to the Settings page.

Summary

12 Devices
1 Manager Device
2 Accesser® Devices
9 Slicestor® Devices
143 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.



Storage Pool: StgPoolGdl

General

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

Capacity

78.29 TB	63.06 TB	141.36 TB
Allocated	Unallocated	Raw Capacity

Slicestor Devices

All Devices (6) S 0 S 0 S 6

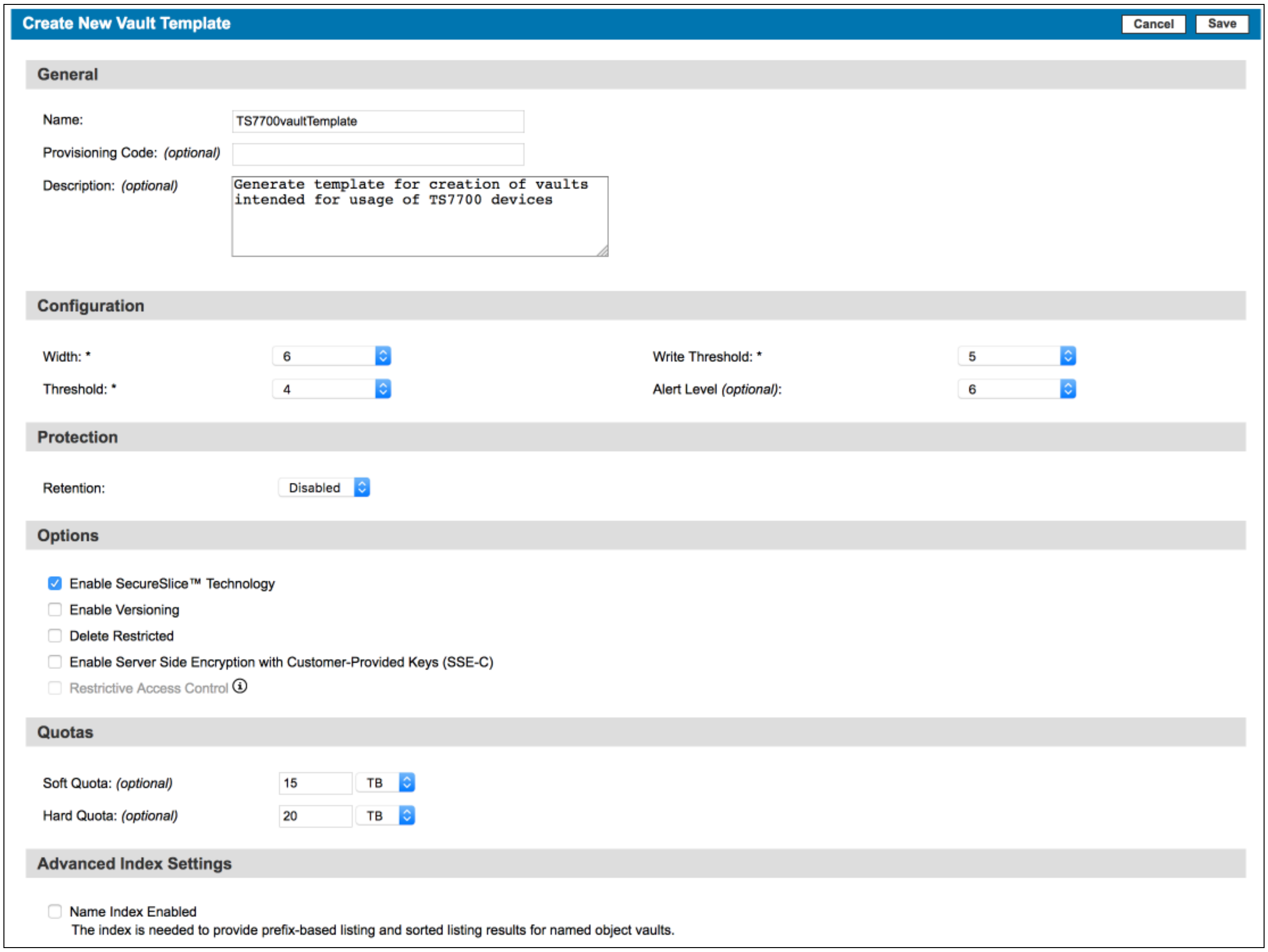
S slici1 CosGdl

Vault Templates

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 IBM Cloud Object Storage creation of a custom vault procedure.



Create New Vault Template

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.

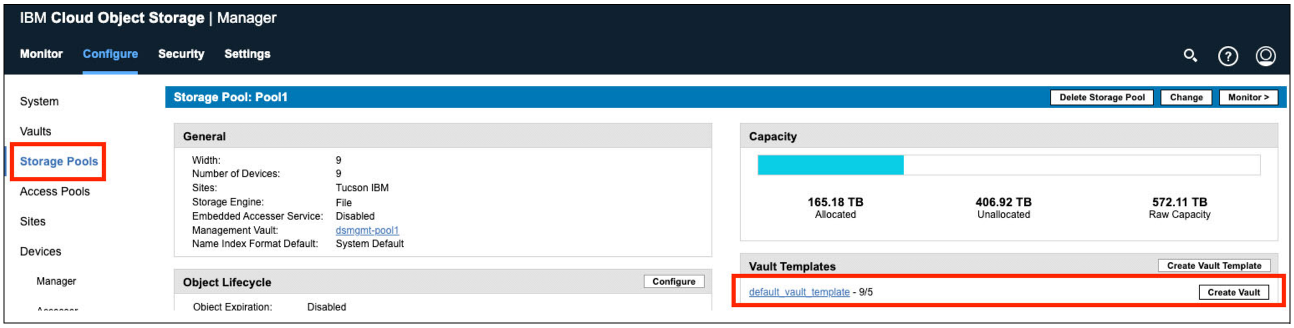
Figure 7-14 Configuring settings for a new vault template

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 IBM Cloud Object Storage Manager website of the corresponding on-premises IBM Cloud Object Storage. Click the **Configure** tab and then, click the **Storage Pools** navigation menu. Available options are listed under the Vault Templates section of that page (see Figure 7-15).



Storage Pool: Pool1

General

Width:	9
Number of Devices:	9
Sites:	Tucson IBM
Storage Engine:	File
Embedded Accesser Service:	Disabled
Management Vault:	dsmgmt-pool1
Name Index Format Default:	System Default

Object Lifecycle

Object Expiration:	Disabled

Capacity

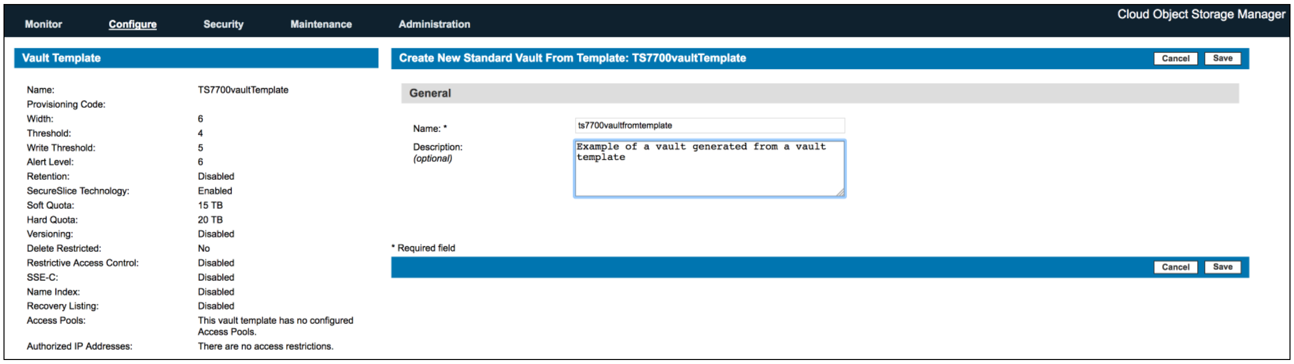
165.18 TB	406.92 TB	572.11 TB
Allocated	Unallocated	Raw Capacity

Vault Templates

default_vault_template - 9/5

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

2. Click **Create Vault** next to the template to be used. 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

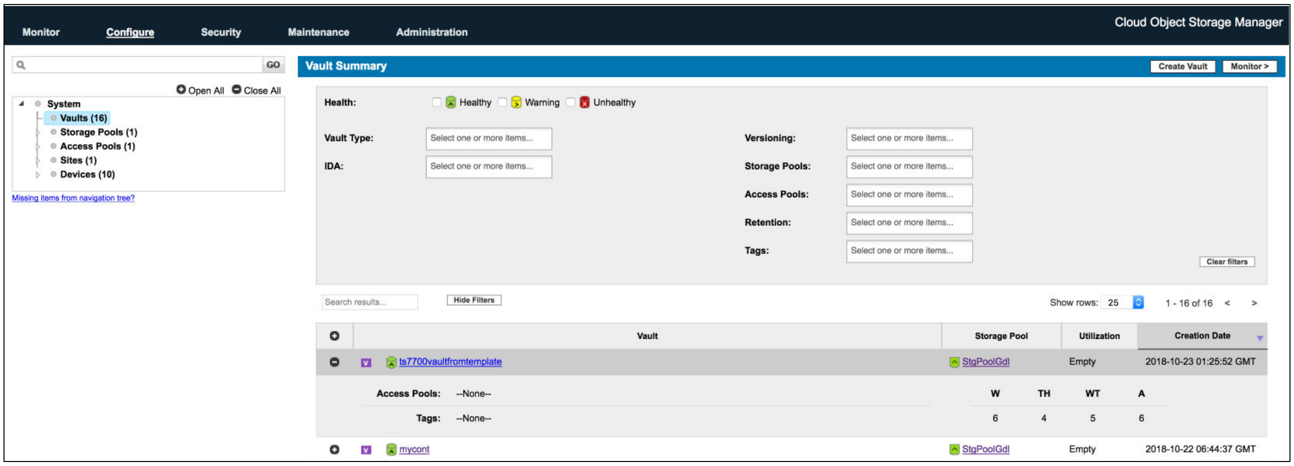
General

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).



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 - 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

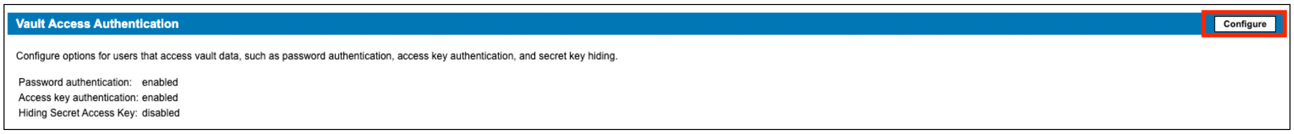
Figure 7-17   Displaying available vaults

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 IBM Cloud Object Storage Manager website of the corresponding on-premises IBM Cloud Object Storage. Click **Security** → **Access Authentication** (see Figure 7-18).

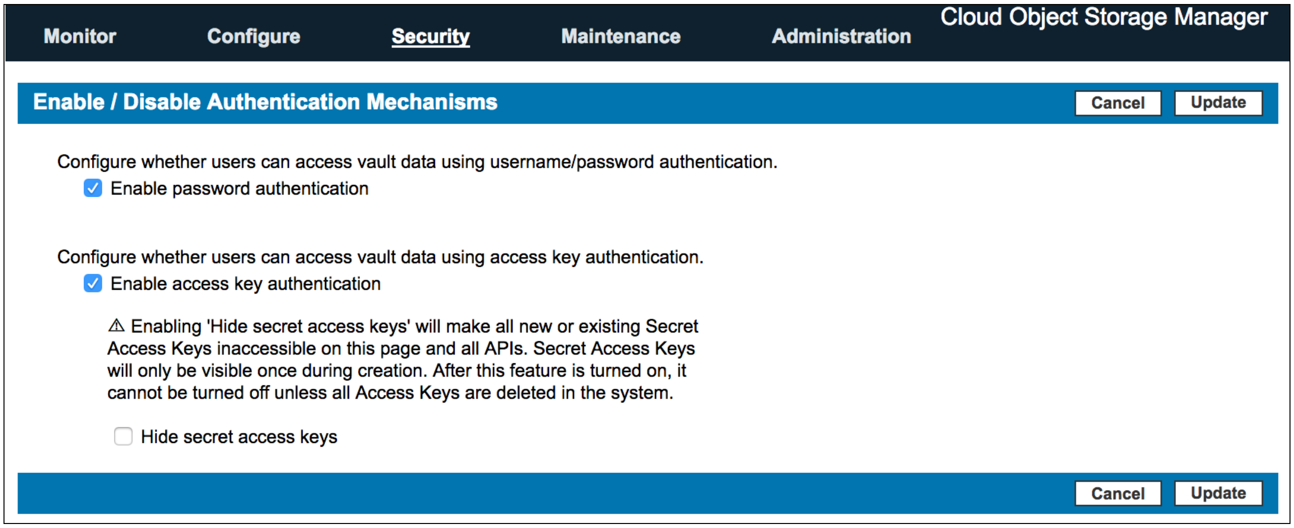


Configure options for users that access vault data, such as password authentication, access key authentication, and secret key hiding.

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

Figure 7-18   Checking the 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.



Enable / Disable Authentication Mechanisms

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

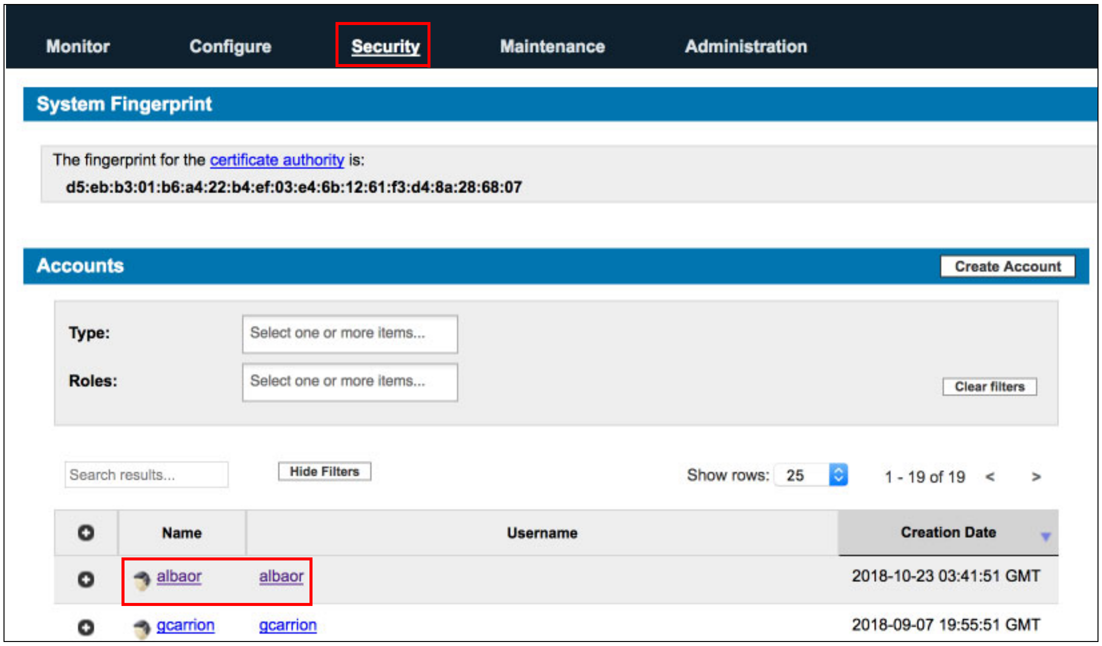
⚠ Enabling 'Hide secret access keys' will make all new or existing Secret Access Keys inaccessible on this page and all APIs. Secret Access Keys will only be visible once during creation. After this feature is turned on, it cannot be turned off unless all Access Keys are deleted in the system.

□ 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).



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...

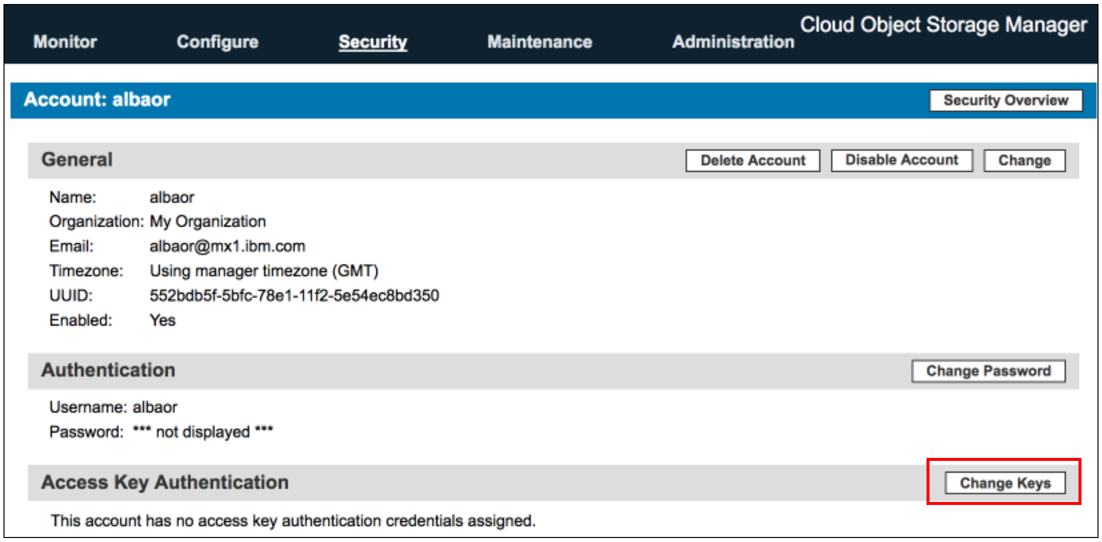
Roles: Select one or more items...

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

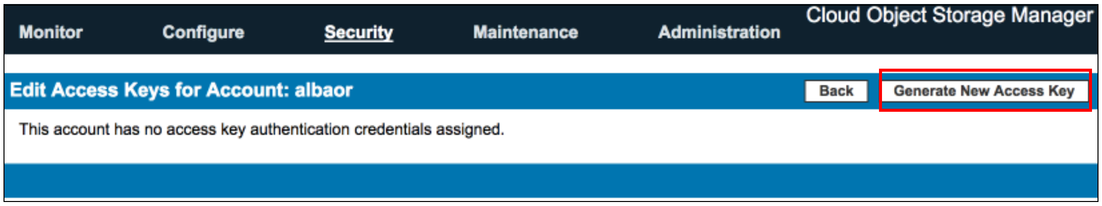
Username: albaor
Password: *** not displayed ***

Access Key Authentication

This account has no access key authentication credentials assigned.

Figure 7-21 Changing access keys for the 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).

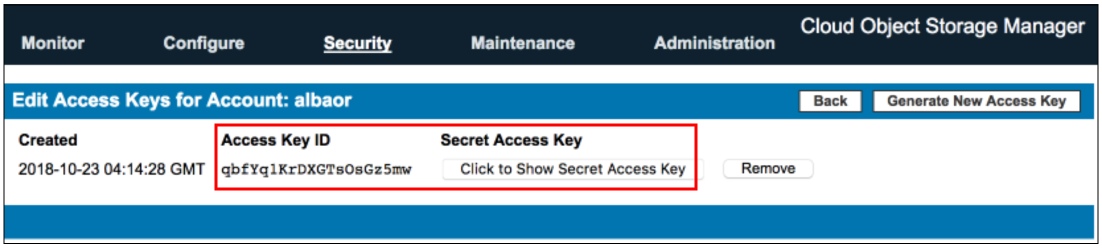


Edit Access Keys for Account: albaor

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 Amazon Web Services 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 (identity) and credentials from a root account by using the AWS console” on page 56
- 8.3, “Amazon S3 buckets” on page 61
- 8.4, “Cross-region replication” on page 67
- 8.5, “Setting up TS7700C tape devices with Amazon S3 Cross Region Replication” on page 70

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 “username” 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 Cloud Object Storage, 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 as a guide only. 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 (identity) 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 IAM user. AWS IAM is a web service that helps you securely control access to AWS resources and services.

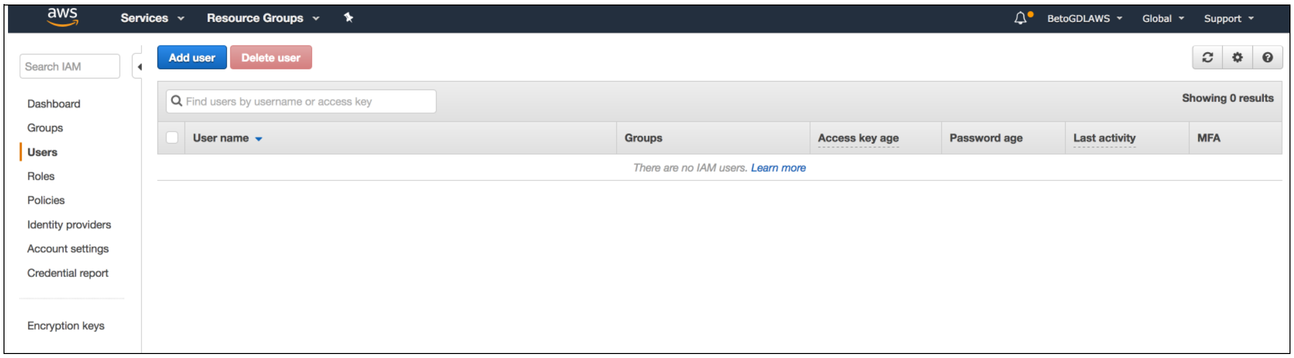
IAM is used to control who is authenticated (signed in) and authorized (has permissions) to use resources. When you first create an AWS account, you begin with a single sign-in identity that has complete access to all AWS services and resources in the account. This identity is called the AWS account 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 AWS web page.

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 windows that are used to create users, see this web page.

Complete the following steps to create IAM users:

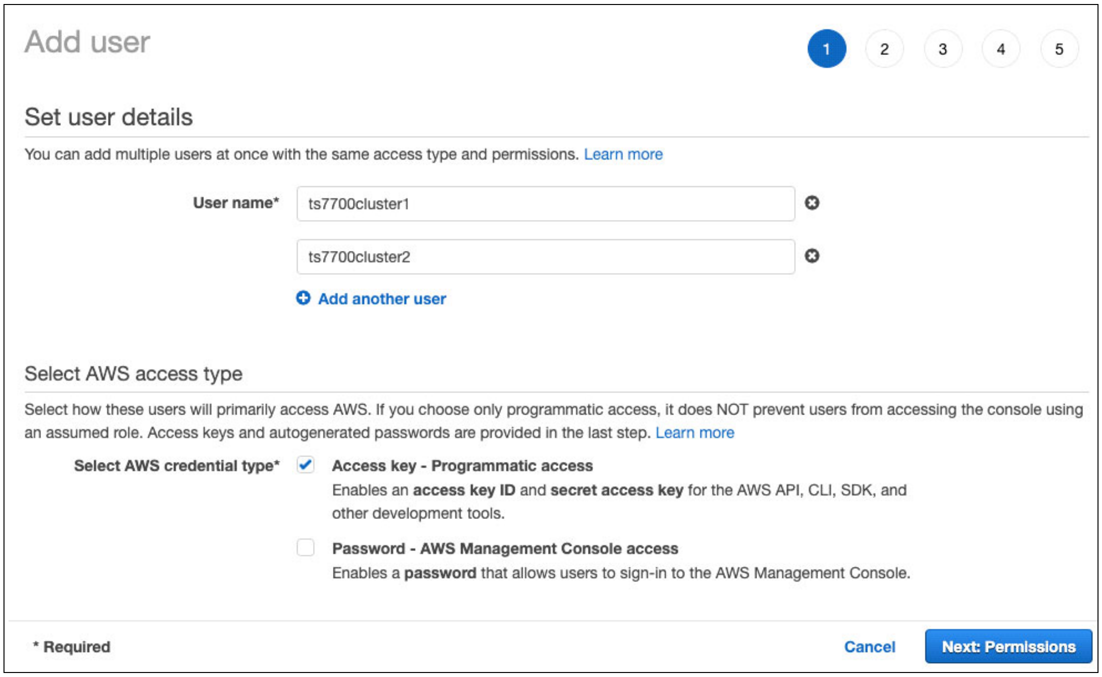
1. Sign in to the AWS Management Console and open the IAM console.
2. In the navigation pane, click **Users** and then, click **Add users** (see Figure 8-1). For TS7700, a minimum of one IAM user available per grid is required. Depending on your management style of the account resources, you might want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



There are no IAM users. Learn more

Figure 8-1 AWS Management Console: IAM console Users window

3. Enter a valid username 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 usernames. You can add up to 10 users at a time.



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 primarily access AWS. If you choose only programmatic access, it does NOT prevent users from accessing the console using an assumed role. Access keys and autogenerated passwords are provided in the last step. Learn more

Select AWS credential type*

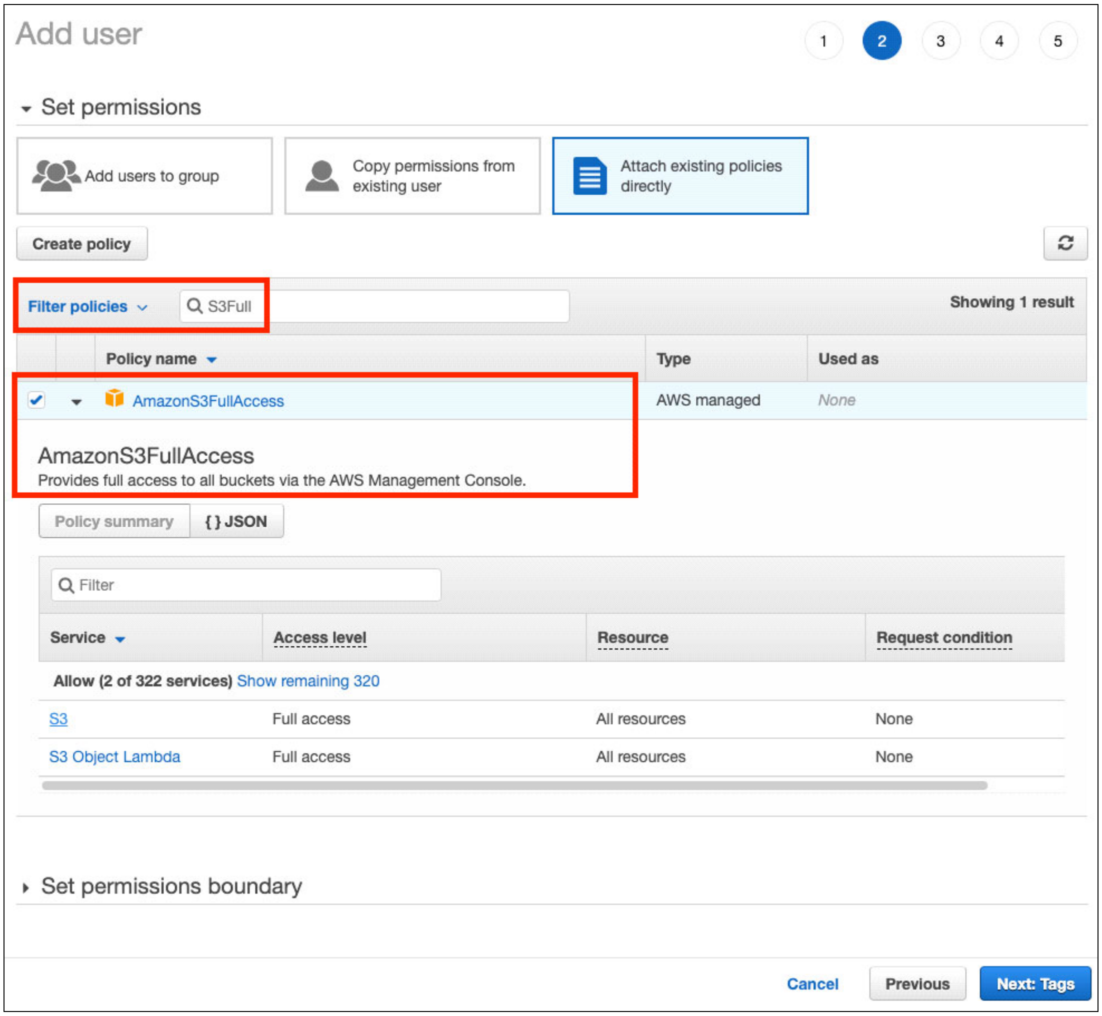
☑ Access key - Programmatic access
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

☐ Password - 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 **Access key - Programmatic access** option (as shown in Figure 8-2 on page 57) 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 (see 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: S3Full

Showing 1 result

		Policy name	Type	Used as
☑	▾	AmazonS3FullAccess	AWS managed	None

AmazonS3FullAccess
Provides full access to all buckets via the AWS Management Console.

Policy summary | { } JSON

Filter

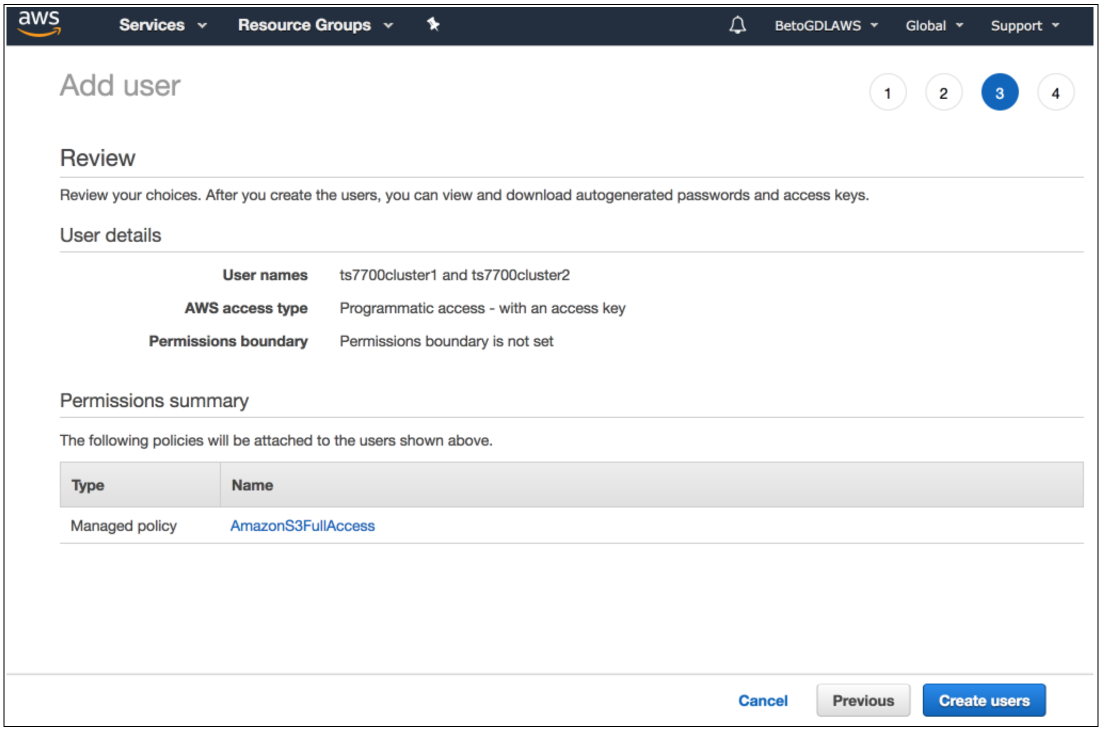
Service	Access level	Resource	Request condition
Allow (2 of 322 services) Show remaining 320			
S3	Full access	All resources	None
S3 Object Lambda	Full access	All resources	None

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 at this AWS web page).

6. Click **Next: Tags** and add a tag if needed. And then 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

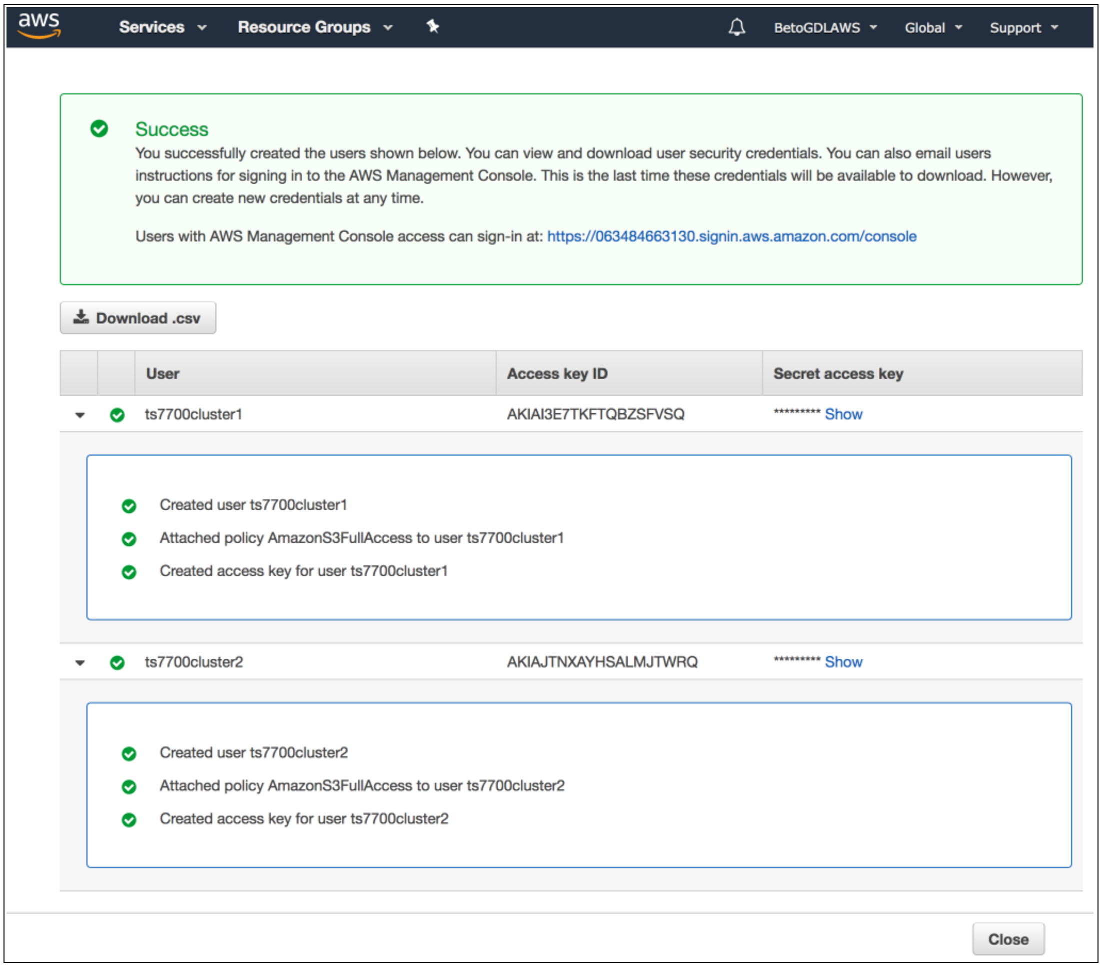
Permissions summary

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
ts7700cluster2	AKIAJTNXAYHSALMJTWRQ	********* Show

Created user ts7700cluster1

Attached policy AmazonS3FullAccess to user ts7700cluster1

Created access key for user ts7700cluster1

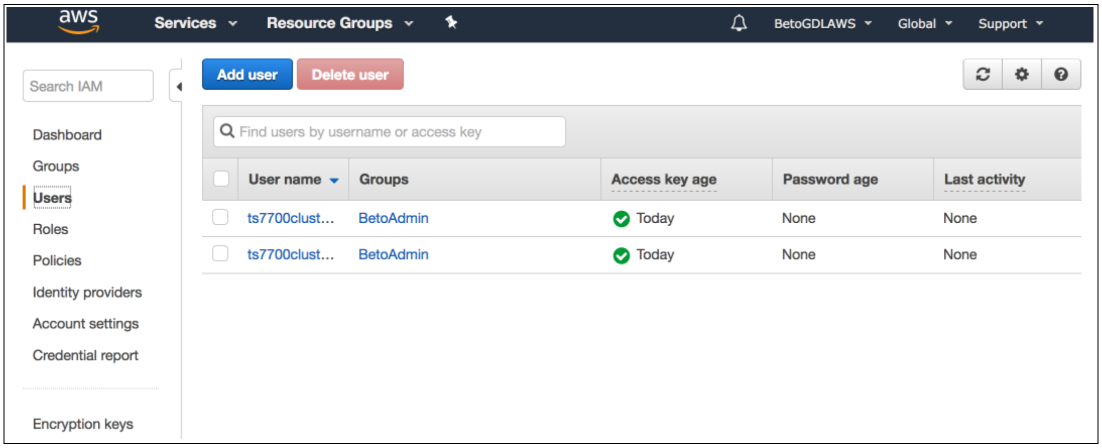
Created user ts7700cluster2

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 window 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 window under the root account

8.3 Amazon S3 buckets

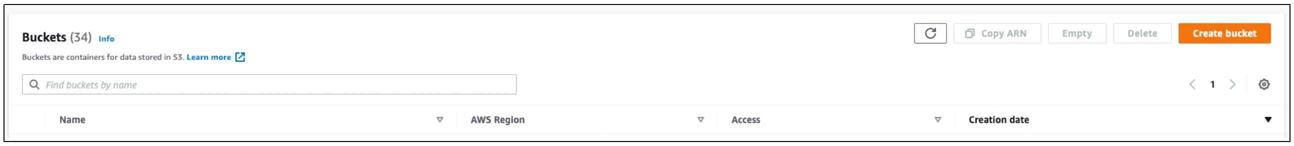
Before the TS7700 can upload data to Amazon S3 by way of the cloud storage tier, at least one bucket in an AWS Region must be created in advance to store the virtual volumes. Buckets feature configuration properties, including their geographical region, that can access the objects in the bucket, whether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



Buckets are containers for data stored in S3. Learn more

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 63. 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.

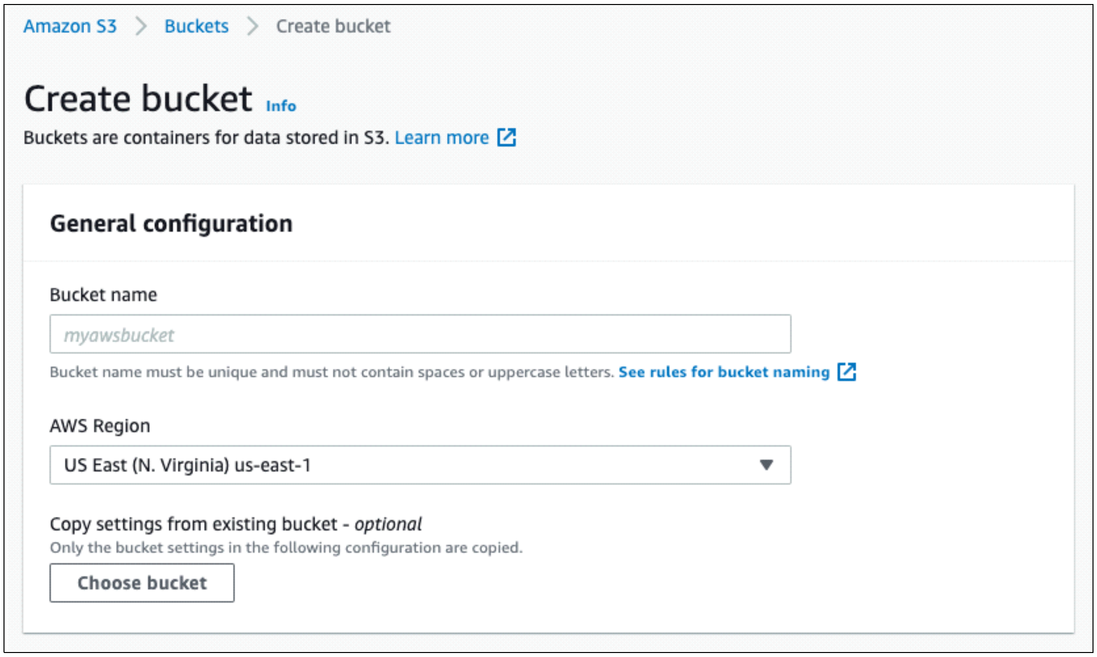
   – For Region, choose the AWS Region where you want the bucket to be stored. Select a Region close to the associated TS7700 to minimize latency and costs, or to address regulatory requirements.

     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).

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 the bucket whose settings you want to copy (see Figure 8-8).



Amazon S3 > Buckets > Create bucket

Create bucket Info

Buckets are containers for data stored in S3. Learn more

General configuration

Bucket name

myawsbucket

Bucket name must be unique and must not contain spaces or uppercase letters. See rules for bucket naming

AWS Region

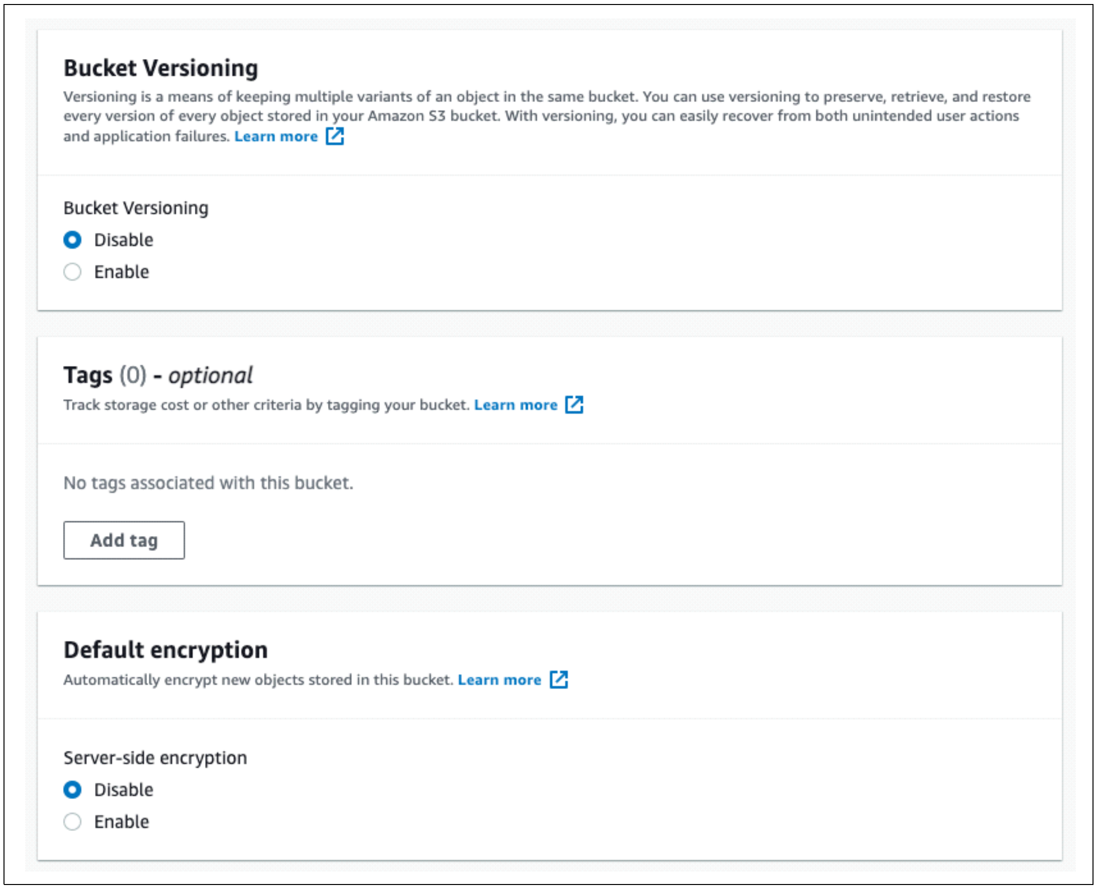
US East (N. Virginia) us-east-1

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

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

3. Set the bucket’s properties to configure the following fields (see Figure 8-9). These properties can be modified after the bucket is created:



Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more

Bucket Versioning

● Disable

○ Enable

Tags (0) - *optional*

Track storage cost or other criteria by tagging your bucket. Learn more

No tags associated with this bucket.

Add tag

Default encryption

Automatically encrypt new objects stored in this bucket. Learn more

Server-side encryption

● Disable

○ Enable

Figure 8-9 Setting the bucket properties

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

  AWS S3 object store manages object versioning for same name objects and TS7700 does not have a method to delete such objects retained within the AWS S3 object store. Therefore, a lifecycle policy must be created by your AWS Admin to automatically delete older versions after some time passes.

  However, TS7700 creates a unique object name for each Logical Volume Version, which differs from the versioning of AWS S3 object store.

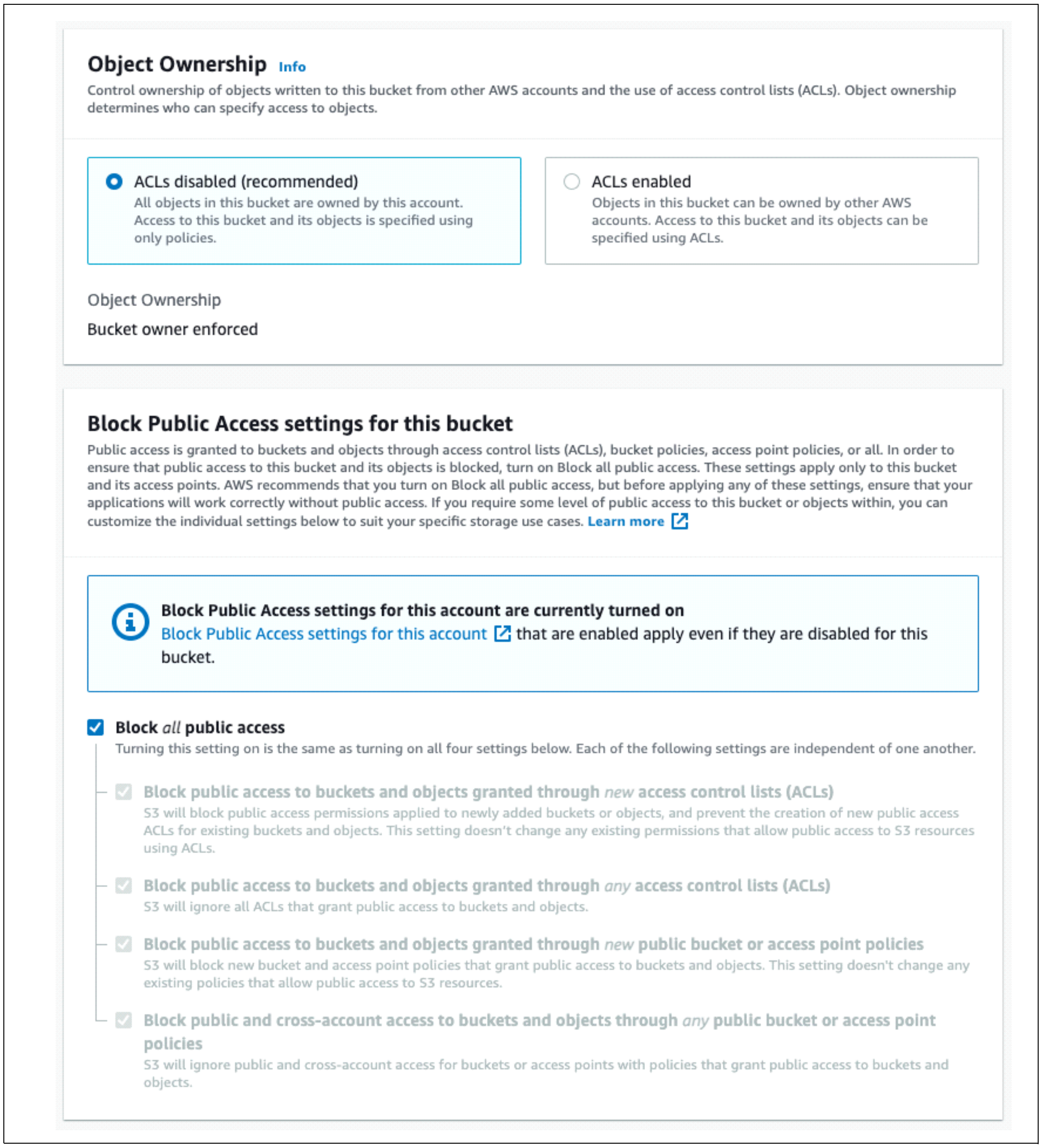
  For more information about TS7700 versioning, see 17.2, “Logical Volume Version Retention in the cloud” on page 170.

- 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.
- 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.

4. Set the Object Ownership option (as shown in Figure 8-10 on page 66) to manage the permissions that are set on the bucket that you are creating.

   Although the owning root account always includes full access permissions to created buckets, it is a best practice to create IAM user accounts and provide access for a specific bucket to specific IAM users, as described in 8.2, “Generating an IAM user (identity) 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 TS7700 tape devices.



Object Ownership Info

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

● ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

○ ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

Object Ownership
Bucket owner enforced

Block Public Access settings for this bucket

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more

Block Public Access settings for this account are currently turned on
Block Public Access settings for this account that are enabled apply even if they are disabled for this bucket.

☑ **Block *all* public access**
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- ☑ **Block public access to buckets and objects granted through *new* access control lists (ACLs)**
  S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- ☑ **Block public access to buckets and objects granted through *any* access control lists (ACLs)**
  S3 will ignore all ACLs that grant public access to buckets and objects.
- ☑ **Block public access to buckets and objects granted through *new* public bucket or access point policies**
  S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- ☑ **Block public and cross-account access to buckets and objects through *any* public bucket or access point policies**
  S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

Figure 8-10 Setting permissions for buckets

> **Warning:** Select the **Block all public access** option. Public access means that *anyone* can access the objects that are in the bucket.

5. When you are done configuring, click **Create bucket** then the bucket is created.

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 CRR can be owned by the same AWS account or by different accounts.

CRR 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 CRR rule to an S3 bucket, see this AWS web page.

8.4.1 Requirements for CRR

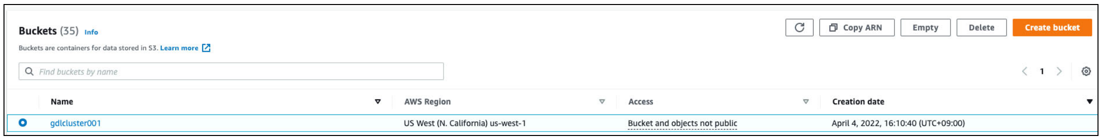
CRR includes the following requirements:

- 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 clean up older versions.
- Amazon S3 includes 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 Access Control List (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 Amazon Web Services. Click the entry that corresponds to the target “source” bucket (as shown in Figure 8-11) to open its bucket window.



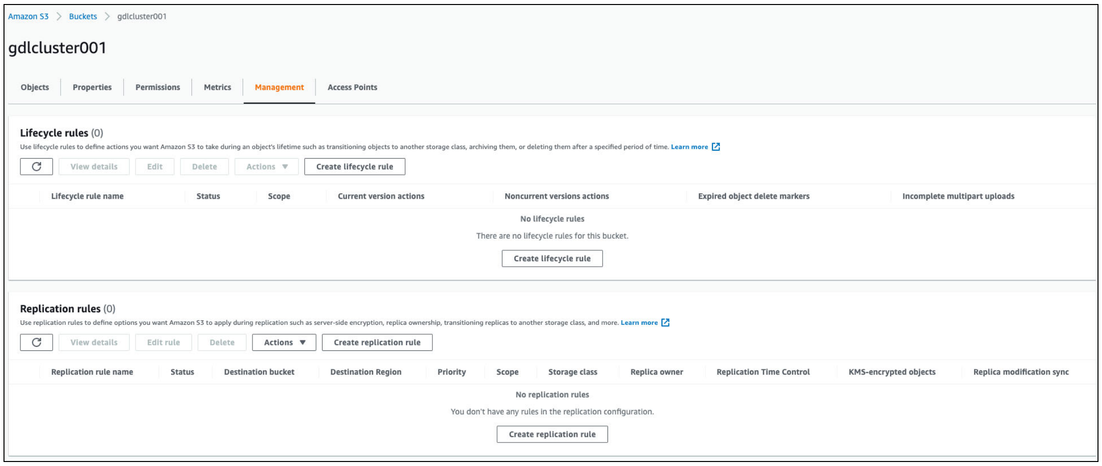
Buckets (35) Info

Buckets are containers for data stored in S3. Learn more

	Name	AWS Region	Access	Creation date
●	gdlcluster001	US West (N. California) us-west-1	Bucket and objects not public	April 4, 2022, 16:10:40 (UTC+09:00)

Figure 8-11 Selecting a target source bucket for CRR

2. In the bucket window, open the Management section (see Figure 8-12).



gdlcluster001

Lifecycle rules (0)

Use lifecycle rules to define actions you want Amazon S3 to take during an object's lifetime such as transitioning objects to another storage class, archiving them, or deleting them after a specified period of time.

Lifecycle rule name	Status	Scope	Current version actions	Noncurrent versions actions	Expired object delete markers	Incomplete multipart uploads

No lifecycle rules

There are no lifecycle rules for this bucket.

Replication rules (0)

Use replication rules to define options you want Amazon S3 to apply during replication such as server-side encryption, replica ownership, transitioning replicas to another storage class, and more.

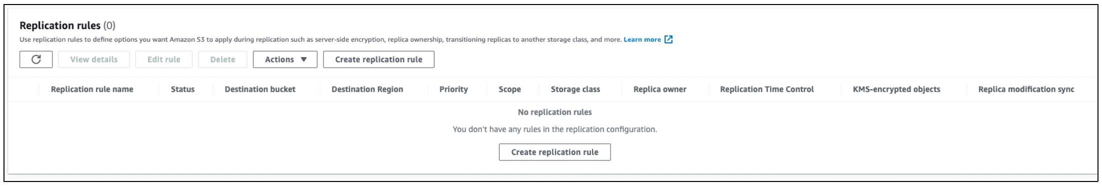
Replication rule name	Status	Destination bucket	Destination Region	Priority	Scope	Storage class	Replica owner	Replication Time Control	KMS-encrypted objects	Replica modification sync

No replication rules

You don't have any rules in the replication configuration.

Figure 8-12 Selecting the Replication configuration window

3. In the Replication rules section, click **Create replication rule** (see Figure 8-13).



Replication rules (0)

Use replication rules to define options you want Amazon S3 to apply during replication such as server-side encryption, replica ownership, transitioning replicas to another storage class, and more.

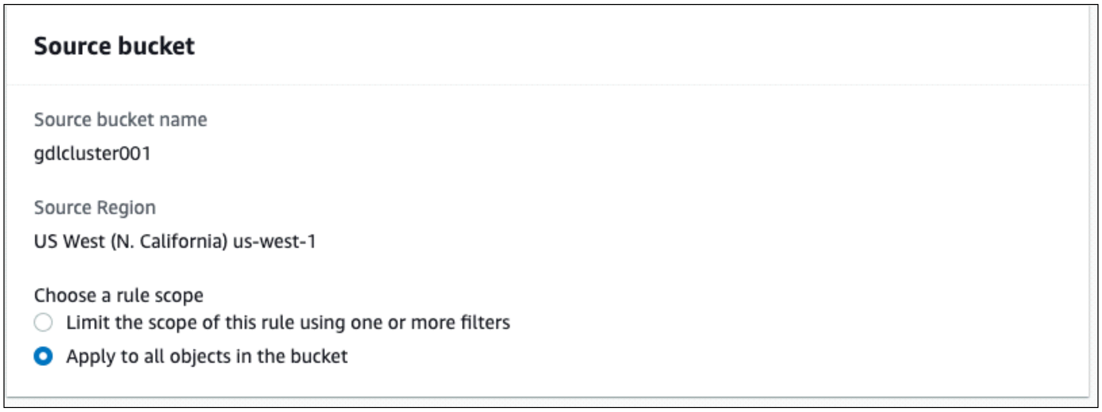
Replication rule name	Status	Destination bucket	Destination Region	Priority	Scope	Storage class	Replica owner	Replication Time Control	KMS-encrypted objects	Replica modification sync

No replication rules

You don't have any rules in the replication configuration.

Figure 8-13 Adding a CRR rule

4. Amazon S3 allows different settings for different use cases; however, for the TS7700 cloud object storage tier, you must select the **Apply to all objects in the bucket** option, as shown in Figure 8-14. Do *not* select the **Replicate objects encrypted with AWS KMS** option (TS7700 support for this option is to be supported in a future release).



Source bucket

Source bucket name
gdlcluster001

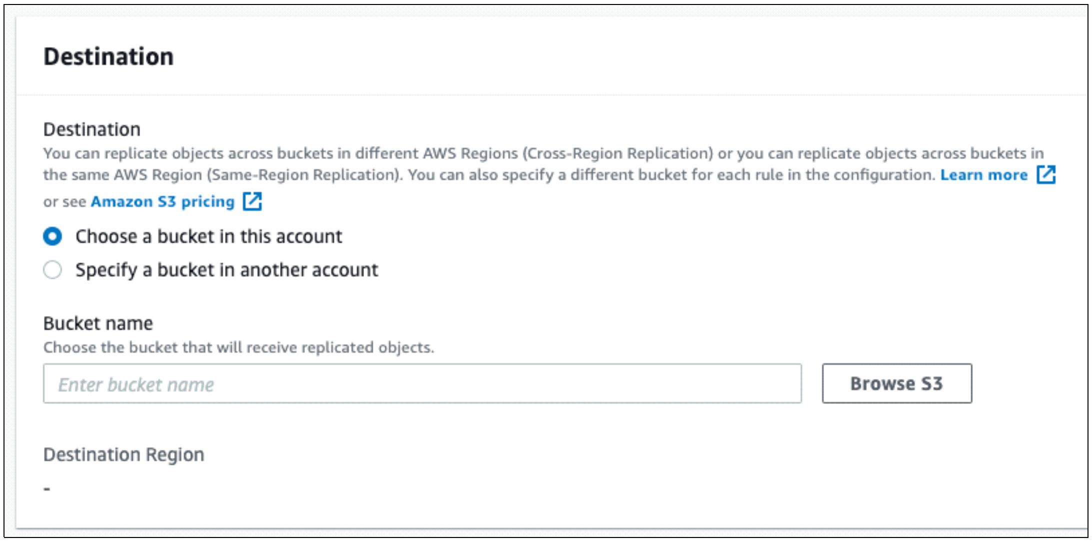
Source Region
US West (N. California) us-west-1

Choose a rule scope
○ Limit the scope of this rule using one or more filters
● Apply to all objects in the bucket

Figure 8-14 Creating a replication rule for CRR

5. Select the Destination bucket, as shown in Figure 8-15. Here, you must select a bucket that is in a region that is different from the Source bucket region.

> **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 AWS web page) and the name of the candidate destination bucket.



Destination

Destination

You can replicate objects across buckets in different AWS Regions (Cross-Region Replication) or you can replicate objects across buckets in the same AWS Region (Same-Region Replication). You can also specify a different bucket for each rule in the configuration. Learn more

or see Amazon S3 pricing

● Choose a bucket in this account

○ Specify a bucket in another account

Bucket name

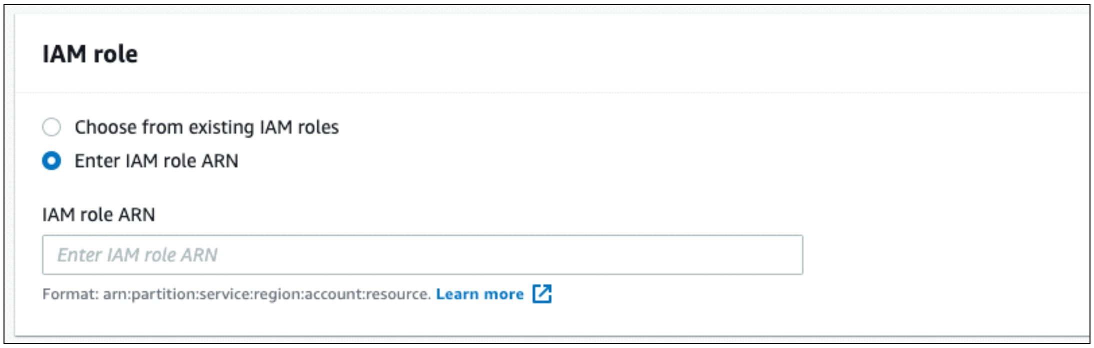
Choose the bucket that will receive replicated objects.

Destination Region

-

Figure 8-15 Selecting a destination bucket

6. Set up an AWS IAM role that Amazon S3 can assume to perform CRR of objects on your behalf. The following options are available, as shown in Figure 8-16:
   - It is highly recommended that you choose **Create new role** to have Amazon S3 create an IAM role for you.
   - 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

○ Choose from existing IAM roles

● Enter IAM role ARN

IAM role ARN

Enter IAM role ARN

Format: arn:partition:service:region:account:resource. Learn more

Figure 8-16 Determining an IAM role and rule name

7. Click **Save** to complete the process (click **Previous** to make any changes). Your new rule should be listed in the source bucket window.

8.5 Setting up TS7700C tape devices 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.

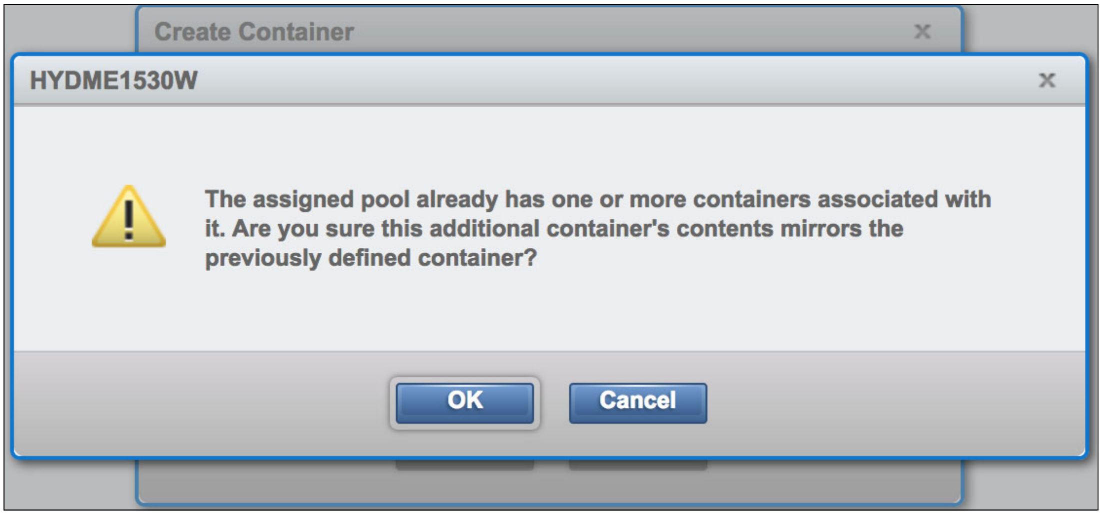
> **Note:** Each region can share an AWS IAM account or they can use unique AWS IAM accounts, depending on how the buckets and the cross region replication were configured.

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 disaster recovery (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 62.

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 9.2.2, “Cloud tier settings” on page 77.

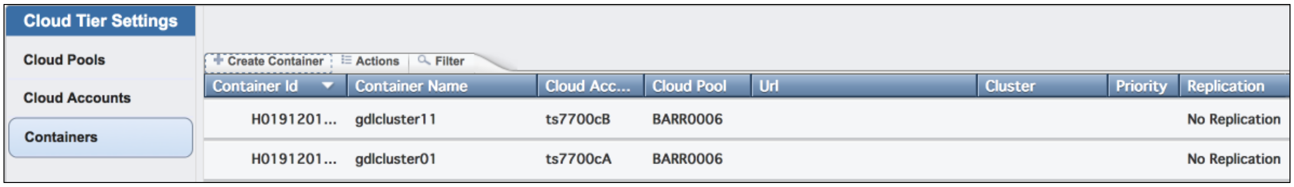
When the second container is created on TS7700, the warning message that is shown in Figure 8-17 is displayed. Because your two buckets are mirrored with AWS CRR, you can click **OK** to proceed.



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 8-17 Warning message on container creation

After the containers are created on the TS7700, two containers are listed in the Container Management Interface (MI) window, as shown in Figure 8-18.



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 8-18 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 window. 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 9.2.2, “Cloud tier settings” on page 77.

After a Cloud URL is created for each container, open the Container window on the MI 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 9.2.8, “Directing virtual volumes to the Cloud Storage Tier” on page 84.

9

Configuring IBM TS7700 for Cloud Storage Tier

In this chapter, we describe how to configure TS7700 for Cloud Storage Tier.

This chapter includes the following topics:

9.1 Prerequisites

The following tasks must be completed on the TS7700 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 TS7700 memory)
   - FC 4278: Cloud Enablement
   - FC 4275: 1 TB Active Premigration Queue (1 - 10 instances)
   - FC 5279: 5 TB Active Premigration Queue (0 - 10 instances)

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

2. If an existing TS7700 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 Chapter 5, "IBM TS7700C planning considerations" on page 25 through Chapter 8, "Setting up Amazon Web Services cloud object storage" on page 55.
4. Configure Cloud Tier Settings by using the TS7700 Management Interface (MI), 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:

     i. 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, Amazon Simple Storage Service (S3), or RSTOR), where virtual volumes belonging to the cloud pool can reside.

     Note: At the time of writing, RSTOR requires a SCORE (Request for Price Quotation (RPQ)). This process explains the setup and cloud attachment.

     ii. Define one or more URLs and assigned certificates for a given cloud container.

     iii. Associate a TS7700 cluster to one or more cloud URLs so that a cluster is aware of which URLs to use to access a given container.
5. Setup and assign one or more TS7700 Data Facility Storage Management Subsystem (DFSMS) constructs so that logical volumes (LVOLs) can use the new Cloud Storage Tier. Consider the following points:
   - Storage Class (SC) must be defined to offload LVOLs that are intended for an object store to a target CPx partition (not CP0).
   - Storage Groups (SGs) must be configured on *all* clusters in the grid so that newly created volumes can target a particular cloud pool rank.

9.1.1 Restrictions

Consider the following restrictions:

- At code level R4.2, the TS7700 supports only connecting to the following cloud object store services by using the S3 protocol:
  - IBM Cloud Object Storage as an on-premises 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).
- At code level R5.0, the TS7700 supports IBM Cloud Object Storage public and RSTOR. To attach RSTOR as a cloud tier, a SCORE must be submitted.
- Enabling a TS7700 for Cloud Storage Tier is supported for only TS7700s that are running code level R4.2 or higher.
- A single TS7700 can be a TS7700C or TS7700T. As of this writing, Tape attach and Cloud Storage Tier are mutually exclusive in the same cluster. TS7700C, TS7700T, and other TS7700 models can coexist in the same grid.
- A TS7700C can be a stand-alone cluster or in a grid with any TS7700 model type that is supported by the 4.2 or later release, such as the following model types:
  - IBM POWER7 processor-based TS7740, TS7720, and TS7720T
  - IBM POWER8® processor-based TS7760 and TS7760T
  - IBM POWER9™ processor-based TS7770 and TS7770T

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 TS7700 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 (minimum 1 FC required, extra FC 5274s are 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 window of the TS7700 MI. More steps, which are documented in "Cloud tier settings" on page 77, are needed afterward to complete the cloud-attachment configuration.
- FC 5274: 1 TB Active Premigration Queue (at least one is required). This concurrent procedure installs the corresponding Key License by using the TS7700 MI.
- FC 5279: 5 TB Active Premigration Queue (Optional after 10 FC 5274s are installed). This concurrent procedure installs the corresponding Key License by using the TS7700 MI.
- FC 3466: Adding 32 GB physical RAM memory to the TS7700 Server. This procedure is non-concurrent, so a maintenance window that requires the intervention of IBM service qualified personnel is necessary. 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.

9.2.1 Cloud Storage Tier MES

After the required FCs 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 alternative I/O drawers). If the TS7700C 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 (whether it is IBM Cloud Object Storage, Amazon S3, or RSTOR) 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 that 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 MI. 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.
- If the Amazon S3 is selected for use with Cloud Storage Tier, a Domain Name System (DNS) server must be set up by using the TS7700 MI in the Cluster Network Settings page under the Cluster Settings window. The DNS server that is on the MI network must also convert *amazonaws.com nameserver-based addresses. Without a properly set up 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 127.
- 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 TS7700. For more information about how to manage data after the MES is complete, see Chapter 13, “Migration and upgrade considerations” on page 127.

9.2.2 Cloud tier settings

After the Cloud Storage Tier feature is enabled, the TS7700 MI (see Figure 9-1) 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.

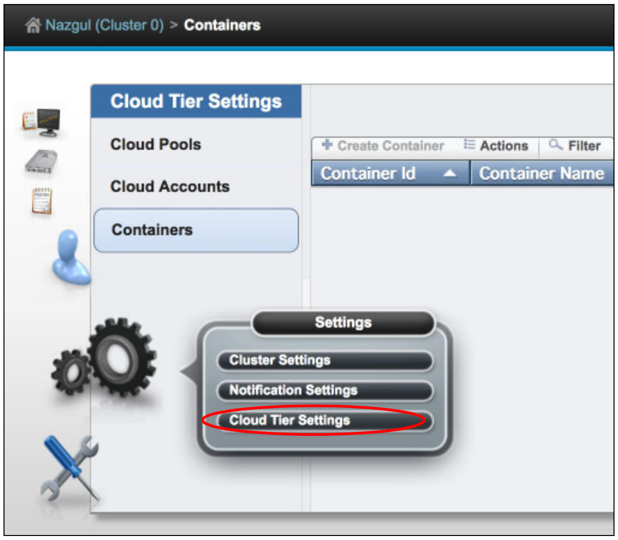
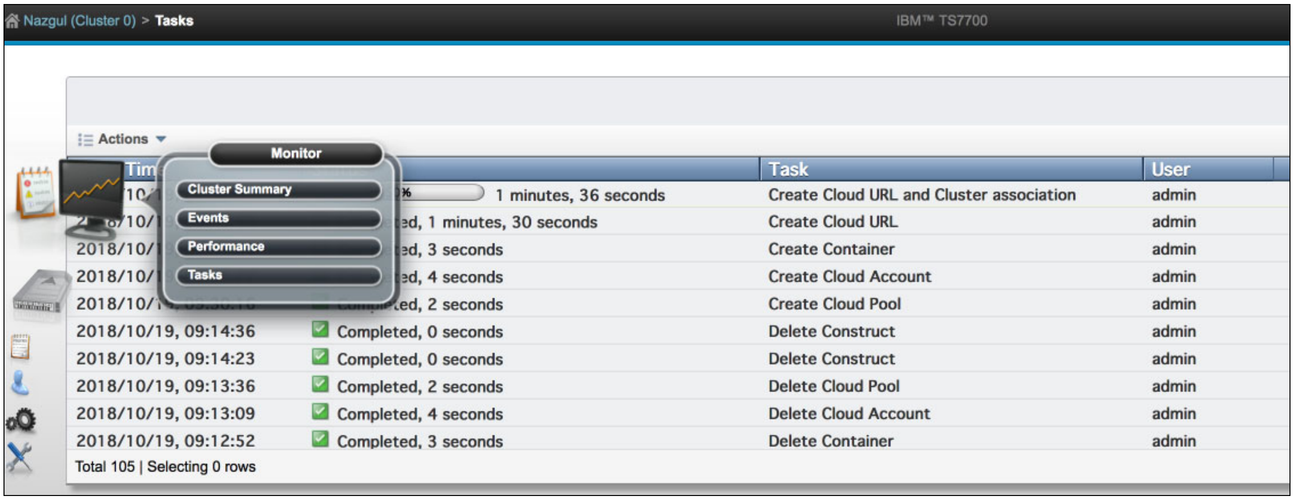


Figure 9-1 Accessing the Cloud Tier Settings window

All changes that are made within the Cloud Tier Settings window 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 MI. Figure 9-2 shows the task option being selected.

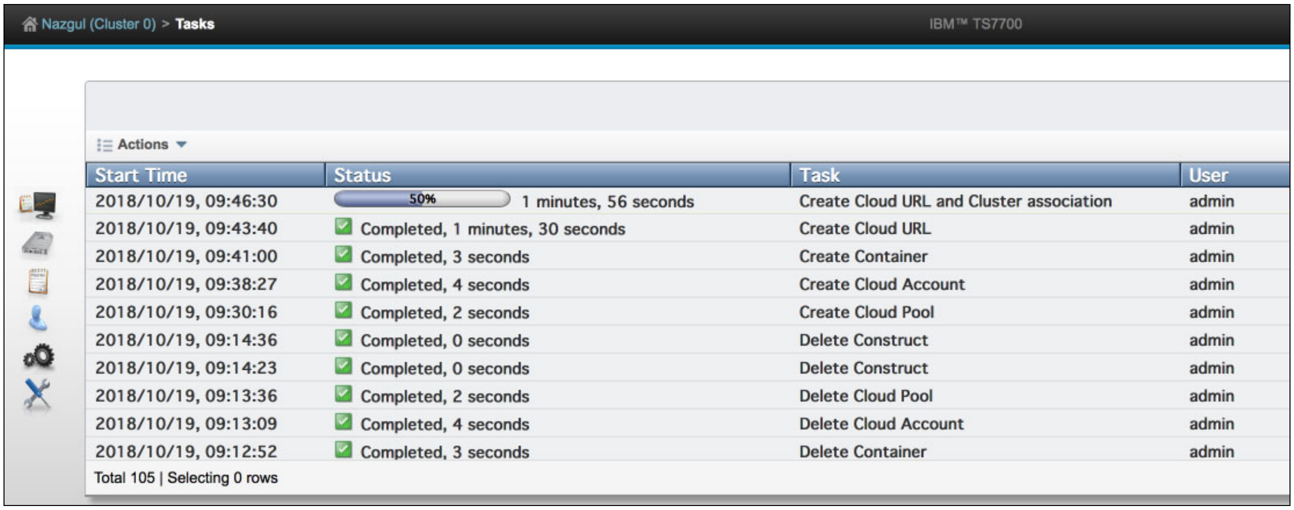


Tim		Task	User
10/	% 1 minutes, 36 seconds	Create Cloud URL and Cluster association	admin
/10/	ed, 1 minutes, 30 seconds	Create Cloud URL	admin
2018/10/	ed, 3 seconds	Create Container	admin
2018/10/	ed, 4 seconds	Create Cloud Account	admin
2018/10/	ted, 2 seconds	Create Cloud Pool	admin
2018/10/19, 09:14:36	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 window

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

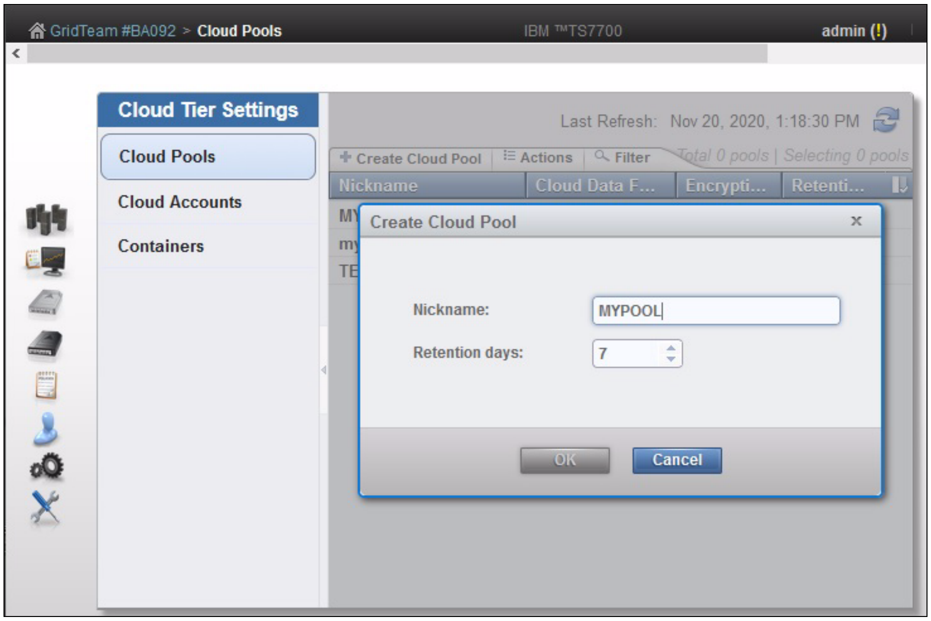
Figure 9-3 Example cloud setting task in progress

9.2.3 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 colocated 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 code level R5.0, up to 256 cloud pools per grid domain are supported. The following fields (see Figure 9-4) must be defined:

- Nickname: The 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 windows and displayed in summary windows, LIBRARY REQUEST outputs, and Bulk Volume Information Retrieval (BVIR) reports.
- Retention days: The user-specified number of days for how long the old premigrated volume in the cloud is retained. Supports 1 - 99999999 days. If 0 is specified, the volume is not retained in the cloud. The old version of a volume is retained after it is premigrated to the cloud.



Nickname: MYPOOL

Retention days: 7

Figure 9-4 Creating a cloud pool

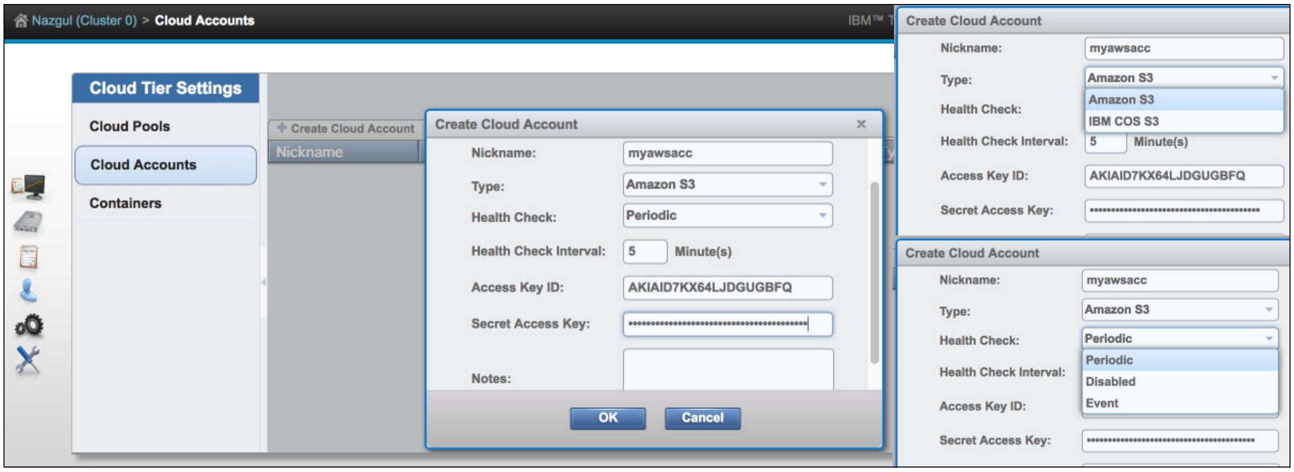
9.2.4 Cloud accounts

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 on page 80), 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 windows and displayed in summary windows, LIBRARY REQUEST outputs, and BVIR reports.

- Type: The object store service that is used. As of Release 5.2.2, the following options are available:
  - Amazon S3
  - IBM Cloud Object Storage
- Health Check: This field determines whether 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 are attempted. In addition, no health checks occur after error events are detected during normal operations.
  - Event (default): The TS7700 attempts to communicate with the object store only 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:

Figure 9-5 Creating cloud accounts

9.2.5 Containers

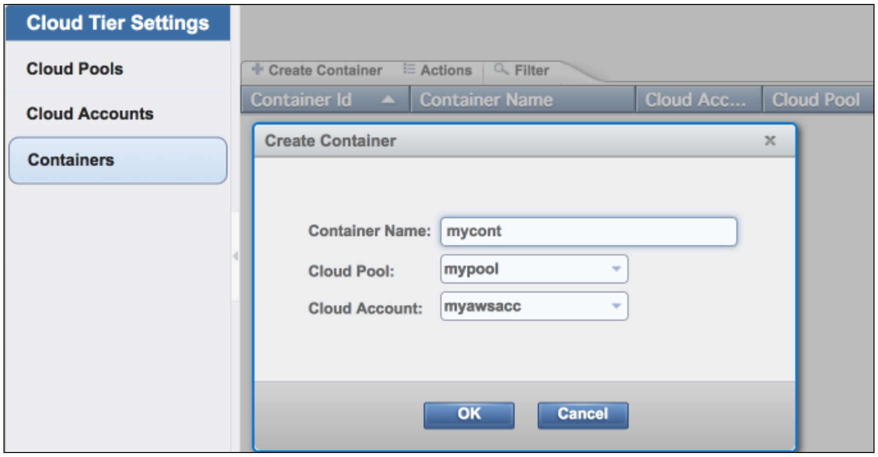
Containers are used to describe an object store vault or bucket. The container must be linked to a cloud pool, cloud account, and one or more URLs that are used to access the vault or bucket.

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 must be defined (see Figure 9-6):

- 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 are used. The cloud account must be created previously.



Container Name: mycont

Cloud Pool: mypool

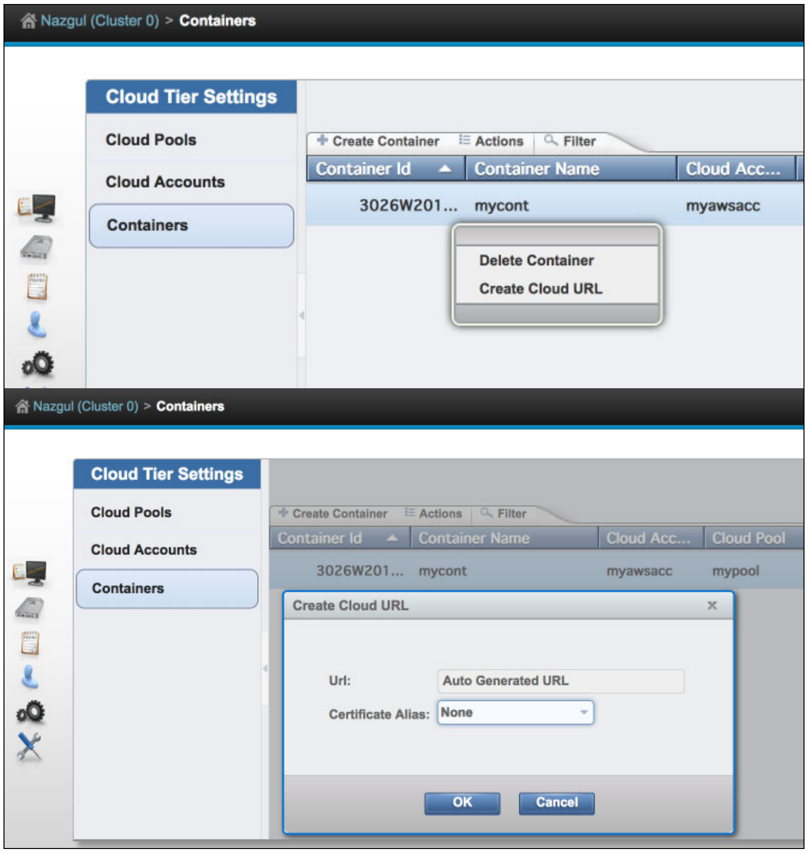
Cloud Account: myawsacc

Figure 9-6 Creating a cloud container

9.2.6 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 that is associated with the container. For example, if an IBM Cloud Object Storage three-site configuration has six total Accesser nodes 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:



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

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

- URL: This URL is the fully qualified http or https URL that is associated with the target bucket or vault. As of code level R5, only IBM Cloud Object Storage object stores and RSTOR (SCORE required) 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.

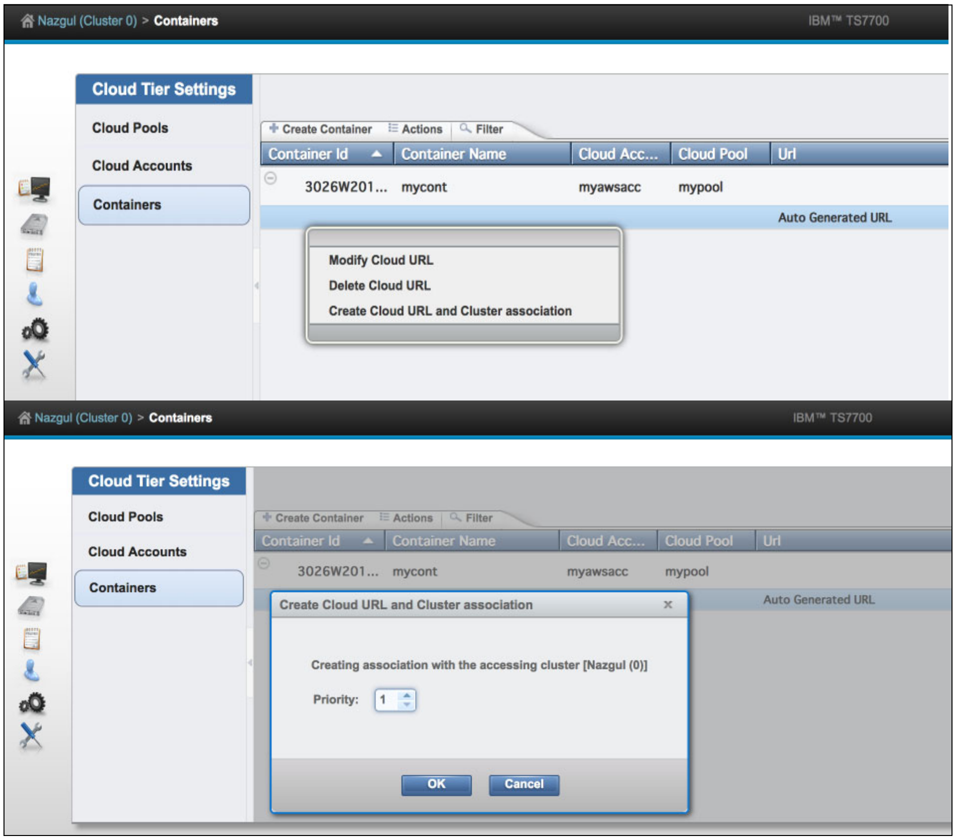
9.2.7 Associating URL values to specific TS7700 clusters

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 has different Accesser nodes and 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 R5.0, this action must be started from the MI of the TS7700 to be associated with the URL. Therefore, if a user creates three URLs by using a specific cluster's MI, the user must still log in to each cluster's MI, access the container's window, and set up the URL cluster association for that specific cluster.

After the user is logged in to 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 window opens where the user is prompted set a priority level for the association that is being created. As of the R5.0 code level, only priority "1" is valid, as shown in Figure 9-8.



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

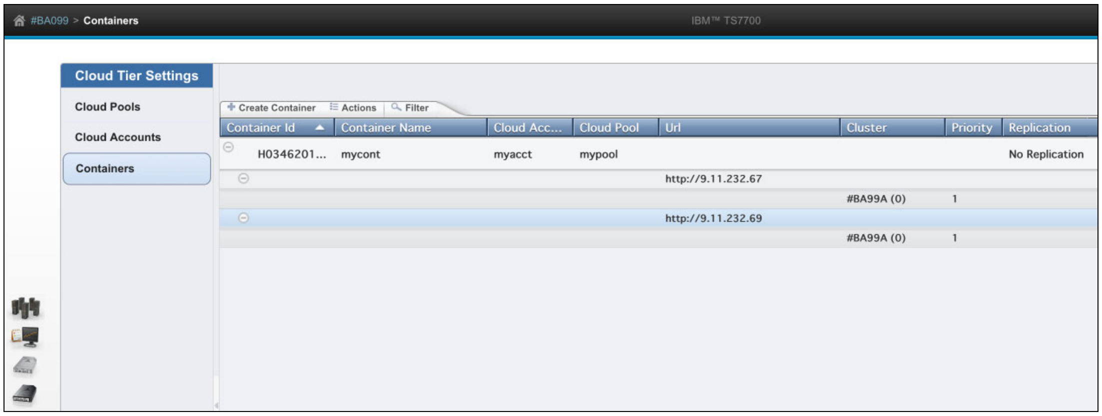
Create Cloud URL and Cluster association

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

Priority: 1

Figure 9-8 Creating a 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 cluster in the grid that will use that URL (see Figure 9-9).

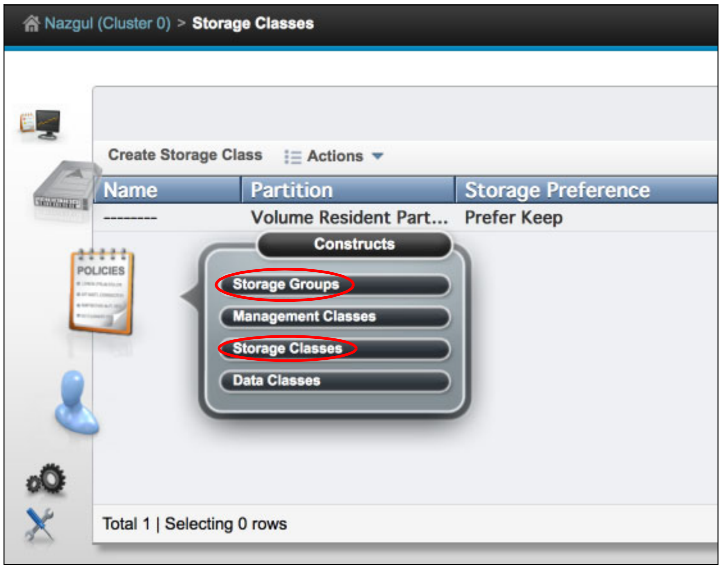


Container Id	Container Name	Cloud Acc...	Cloud Pool	Url	Cluster	Priority	Replication
H0346201...	mycont	myacct	mypool				No Replication
				http://9.11.232.67			
					#BA99A (0)	1	
				http://9.11.232.69			
					#BA99A (0)	1	

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

9.2.8 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 LVOLs to a connected object store. SC is used to direct which disk partition the LVOL is in and Storage Group (SG) 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

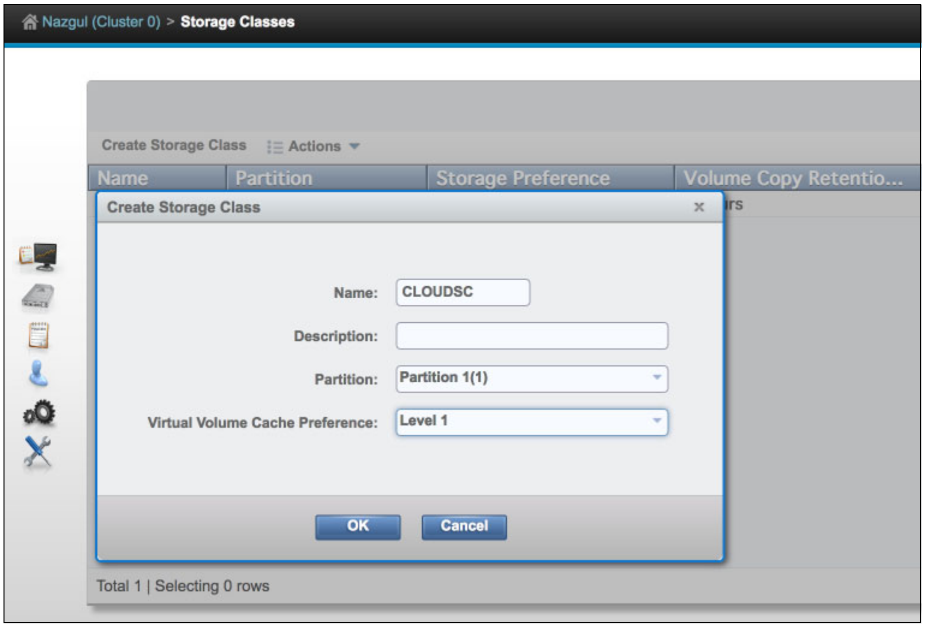
Figure 9-10 Constructs that are related to Cloud Storage Tier

How to configure these two constructs is described next.

9.2.9 Storage classes

SCs 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 after they are copied to the Cloud Storage Tier. The following values (see Figure 9-11) are available:
  - Use Initial Access Response Time (IART): Volumes are removed according to the IART of the running IBM Z application that created the LVOL.
  - 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)

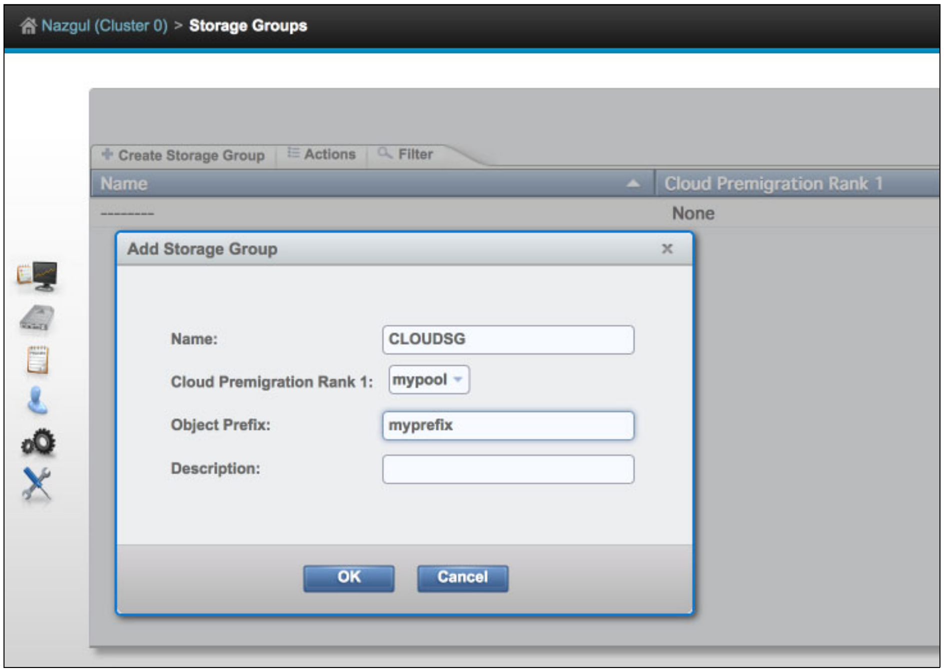
Virtual Volume Cache Preference: Level 1

Total 1 | Selecting 0 rows

Figure 9-11 Defining storage classes for cache partition assignment

9.2.10 Storage Groups

SGs 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) are applicable:



Name: CLOUDSG

Cloud Premigration Rank 1: mypool

Object Prefix: myprefix

Description:

Figure 9-12 Defining storage groups for Cloud Storage Tier

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

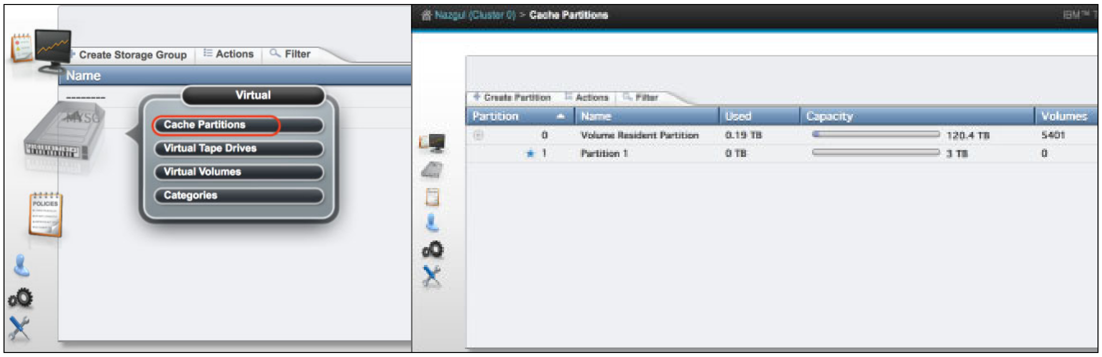
> **Note:** SGs always assign a Cloud Premigration Rank, even if the data is on non-cloud attached clusters only or are in CP0 resident-only partitions. If the LVOL is to ever copy to a newly configured cloud-attached cluster through COPYRFSH or the LVOL is moved from CP0 to CPx by the PARTRFSH, it does 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 SCs 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 LVOL in the cloud object store. The TS7700 includes its own metadata in the name, but this meta-data is the left most portion of the object name that allows a user to separate objects by workload.

For more information about the object naming convention, see 12.1, “TS7700 object name format” on page 118.

9.2.11 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 SG 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 move content from or to a cloud repository) by modifying or assigning new constructs (SC and SG 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 this IBM Support web page.

10

Configuration examples

This chapter shows some configuration examples of TS7700 with IBM Cloud Object Storage and Amazon Simple Storage Service (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” on page 90
- 10.2, “Two-way grid cluster with one cloud pool, account, and container with IBM Cloud Object Storage” on page 95
- 10.3, “Two-way grid with one cloud pool for an Amazon S3 cross-region replication set of buckets that are accessed by using different credentials” on page 98
- 10.4, “Four-way grid with one cloud pool, two accounts, and one container using IBM Cloud Object Storage” on page 101
- 10.5, “Four-way clusters (one TS7700C in each location) with one cloud pool, two accounts, and one container that uses IBM Cloud Object Storage” on page 105

10.1 Stand-alone cluster

This section shows the simplest configurations that use a stand-alone cluster with IBM Cloud Object Storage or Amazon S3.

10.1.1 Stand-alone cluster with IBM Cloud Object Storage

In this section, we describe the process to configure a stand-alone cluster with IBM Cloud Object Storage. Before you start setting up the Cloud Storage Tier on your TS7700, ensure that IBM Cloud Object Storage is set up in your environment. For more information about setting up your IBM Cloud Object Storage, see Chapter 7, “Setting up an IBM Cloud Object Storage object store” on page 37.

Figure 10-1 shows a stand-alone cluster that is connected to IBM Cloud Object Storage with three Accesser nodes. The Cloud Storage Tier is defined so that the TS7700 off loads volumes to the cloud pool MYPOOL. MYPOOL points to an IBM Cloud Object Storage 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, as shown in Figure 10-1. Although a load-balancer can be used between TS7700 and Accesser nodes, we assume in this example that TS7700 directly connects to the three Accesser nodes by using their unique IP address.

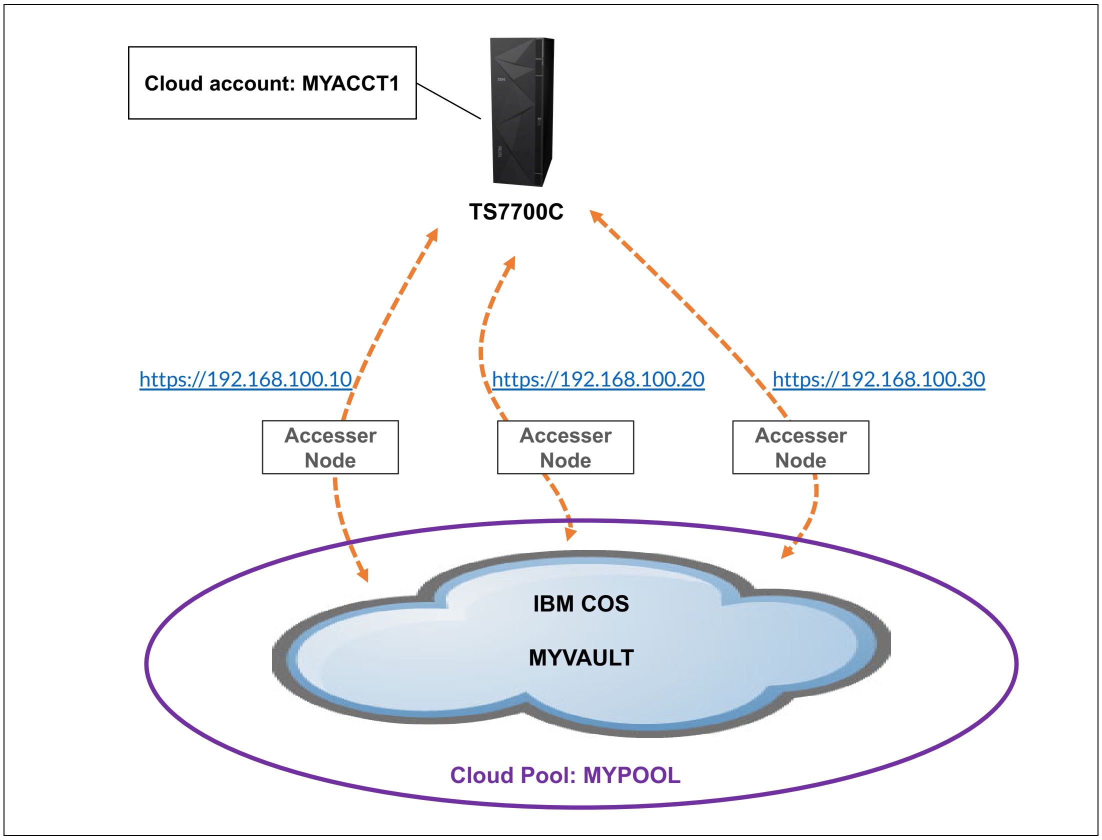


Figure 10-1 Stand-alone cluster with IBM Cloud Object Storage

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 (LVOLs) 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 IBM Cloud Object Storage. 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 IBM Cloud Object Storage admin).
7. Click **OK**.

Creating a container

Complete the following steps:

1. Verify that a vault (for example, MYVAULT) is created in IBM Cloud Object Storage.
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

Complete the following steps:

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 Amazon Web Services 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.

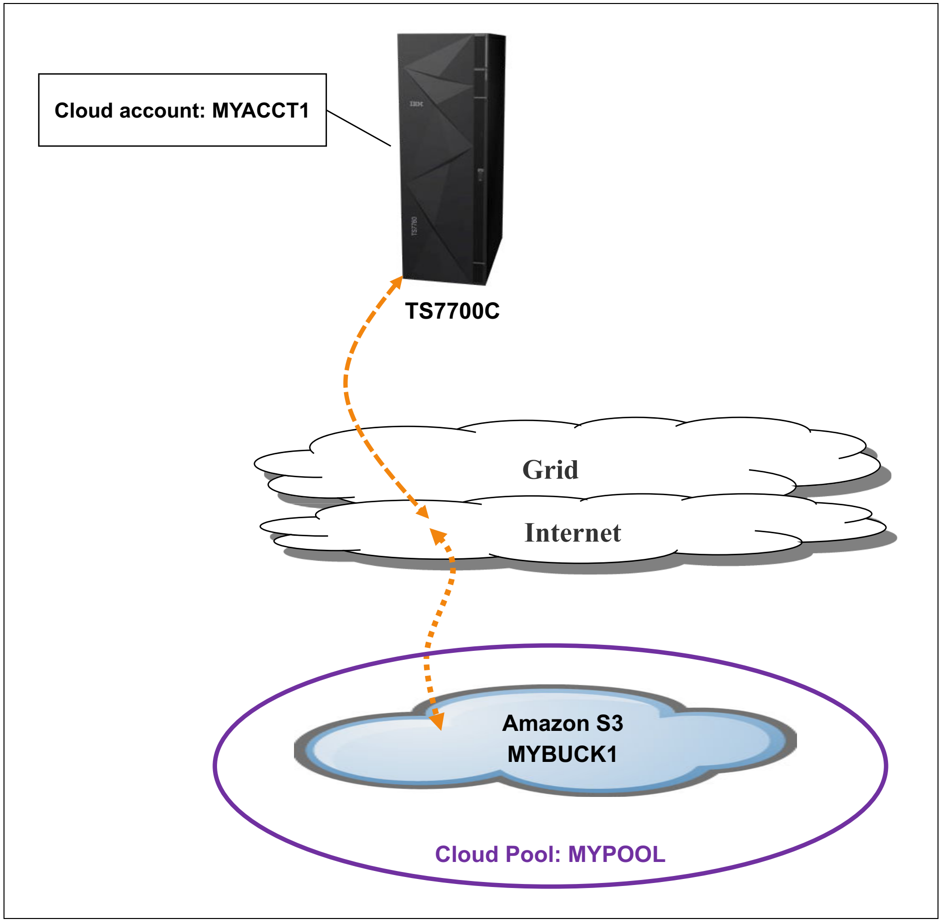


Figure 10-2 Stand-alone cluster with Amazon S3

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 LVOLs 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 step in this process is described next.

Creating a cloud pool

Complete the following steps:

1. Go to **Settings** → **Cloud Tier Settings** on the 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 cluster with one cloud pool, account, and container with IBM Cloud Object Storage

This section describes a two-way Grid TS7700C cluster with one cloud pool/account/container that uses IBM Cloud Object Storage. Before setting up the Cloud Storage Tier, IBM Cloud Object Storage must be set up in your environment. For more information about setting up your IBM Cloud Object Storage, see Chapter 7, “Setting up an IBM Cloud Object Storage object store” on page 37.

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

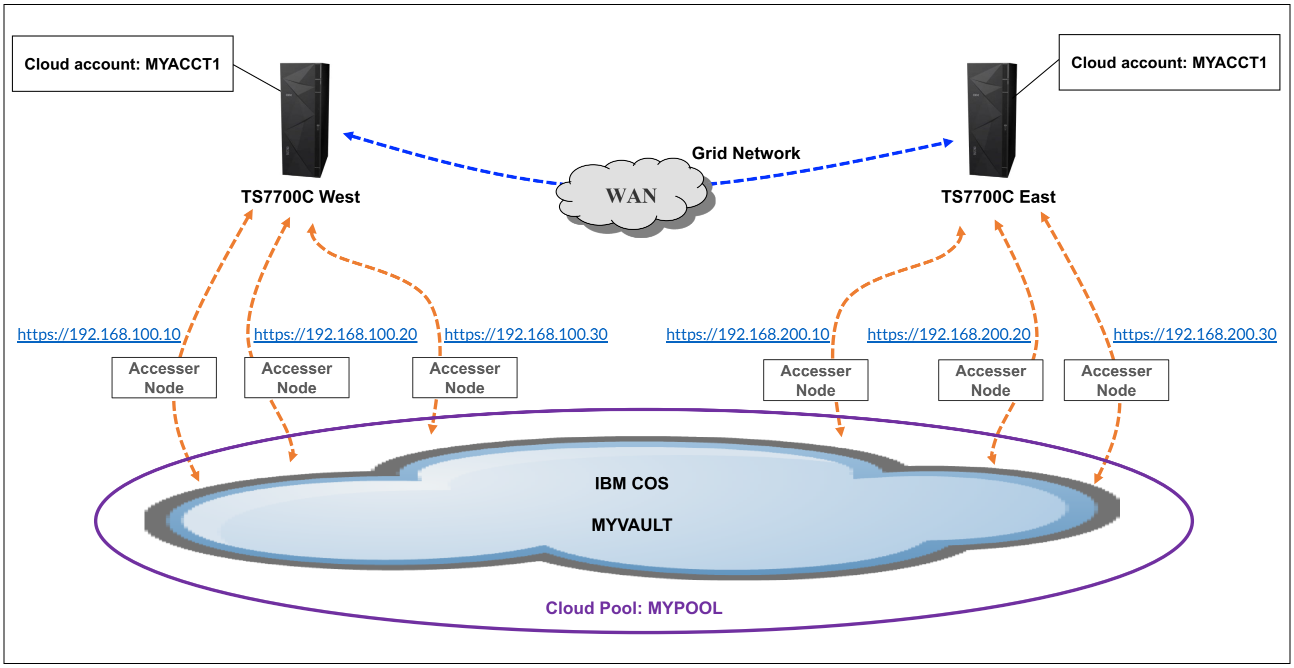


Figure 10-3 Two-way TS7700C clusters with one cloud account/pool/container using IBM Cloud Object Storage

Because six total Accesser nodes 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 Accesser nodes. However, we assume in this example that the TS7700 directly connects to the three Accesser 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 LVOLs 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 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 IBM Cloud Object Storage 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 IBM Cloud Object Storage.
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** → C**loud 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 IBM Cloud Object Storage vault.

10.3 Two-way grid with one cloud pool for an Amazon S3 cross-region replication set of buckets that are 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 Amazon Web Services cloud object storage” on page 55.

Figure 10-4 on page 99 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.

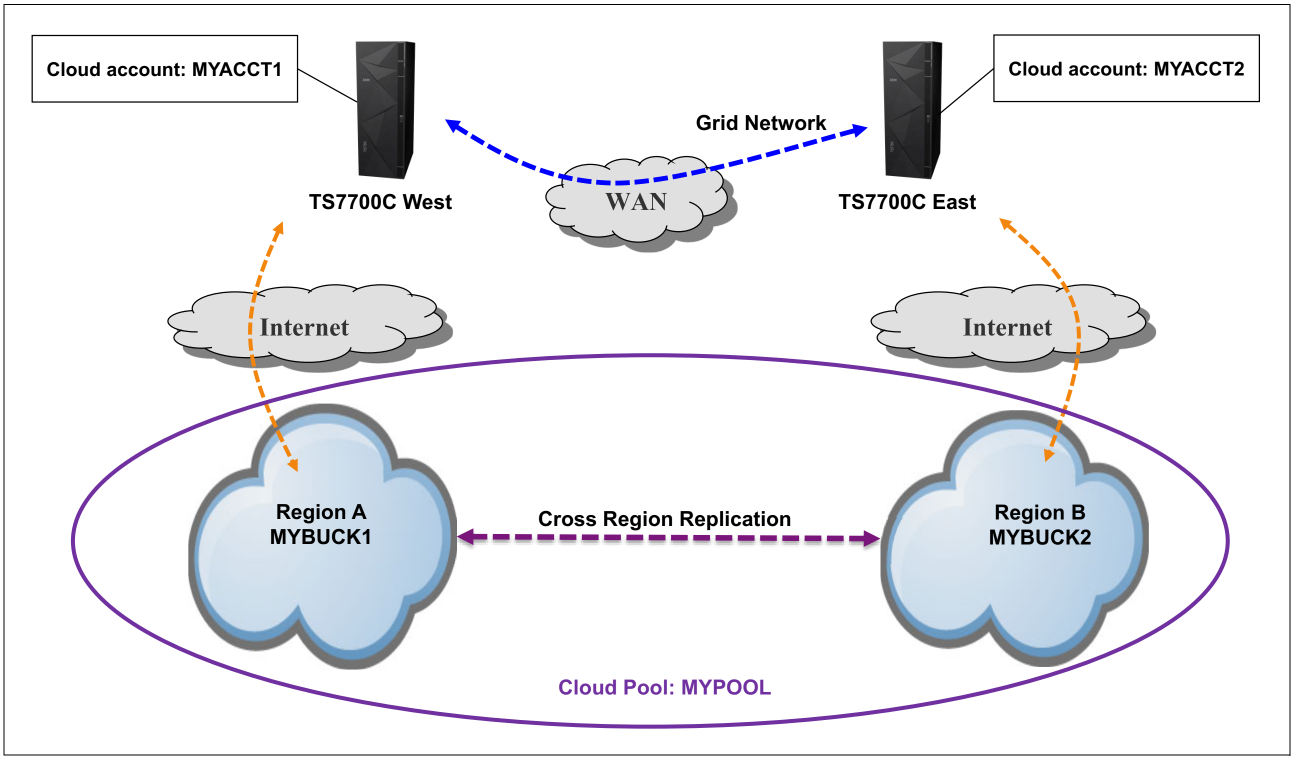


Figure 10-4 Two-way TS7700C clusters with one cloud pool, two accounts, and two containers using Amazon S3

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 step 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 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 CRR 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 IBM Cloud Object Storage

This section provides an example of a 4-way, 2-region TS7700C Grid with one cloud pool, two accounts (one per region), and one container that uses IBM Cloud Object Storage. Before setting up the Cloud Storage Tier, your IBM Cloud Object Storage must be set up in your environment. For more information about setting up your IBM Cloud Object Storage, see Chapter 8, “Setting up Amazon Web Services cloud object storage” on page 55.

Figure 10-5 shows a 4-way, 2-region TS7700C Grid and all four clusters are connected to the same cloud pool MYPOOL.

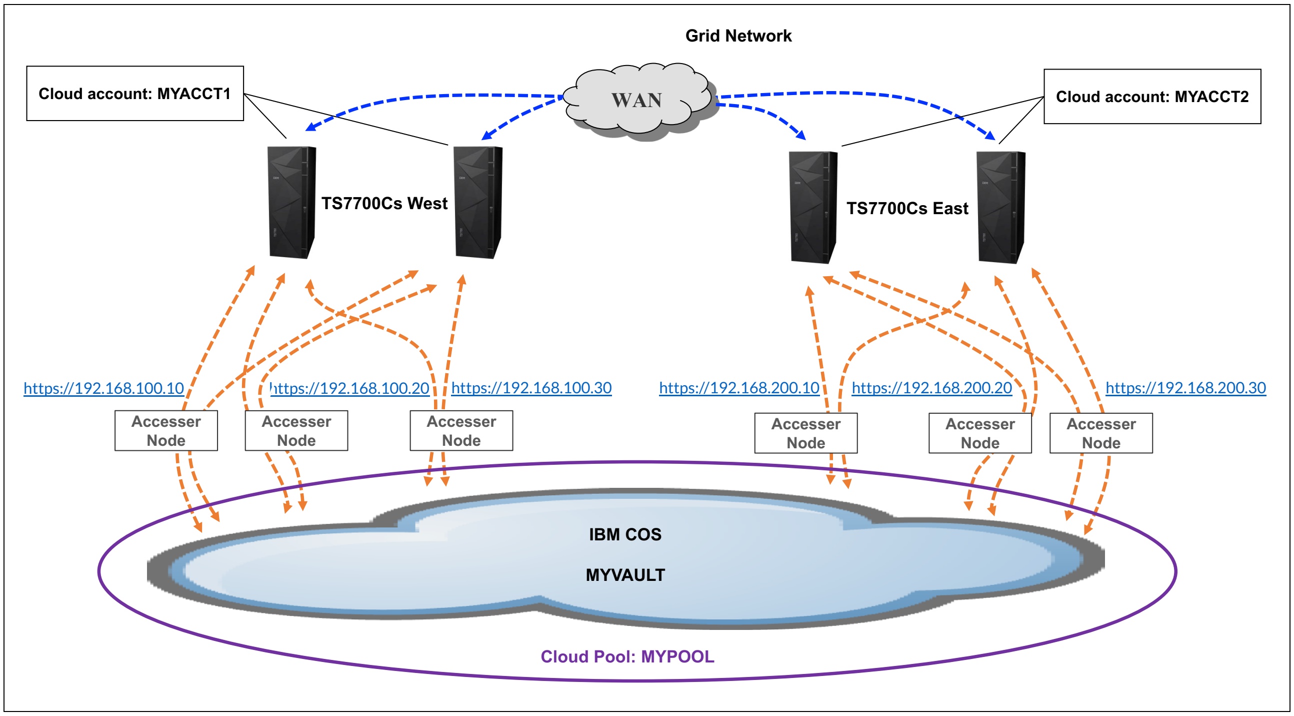


Figure 10-5 Four-way TS7700C clusters with one cloud pool/two accounts/one container using IBM Cloud Object Storage

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 Accesser nodes.

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 IBM Cloud Object Storage in West and East by using IBM Cloud Object Storage 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 LVOLs 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 IBM Cloud Object Storage, 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 about 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 step in this process is described next.

Creating a cloud pool

Complete the following steps:

1. On any of the four clusters, click **Settings** → C**loud Tier Settings** on the 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 IBM Cloud Object Storage 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 IBM Cloud Object Storage.
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 Accesser 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 that uses IBM Cloud Object Storage

This section shows how to set up a 4-way, 2-region grid where only one cluster in each region connects to an IBM Cloud Object Storage object store. One cloud pool, two accounts, and one container are available for a single vault inside an IBM Cloud Object Storage. Before setting up the Cloud Storage Tier, your IBM Cloud Object Storage must be set up in your environment. For more information about setting up your IBM Cloud Object Storage, see Chapter 7, “Setting up an IBM Cloud Object Storage object store” on page 37.

Figure 10-6 shows a 4-way, 2-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 (SG) values configured correctly to use the Cloud Storage Tier.

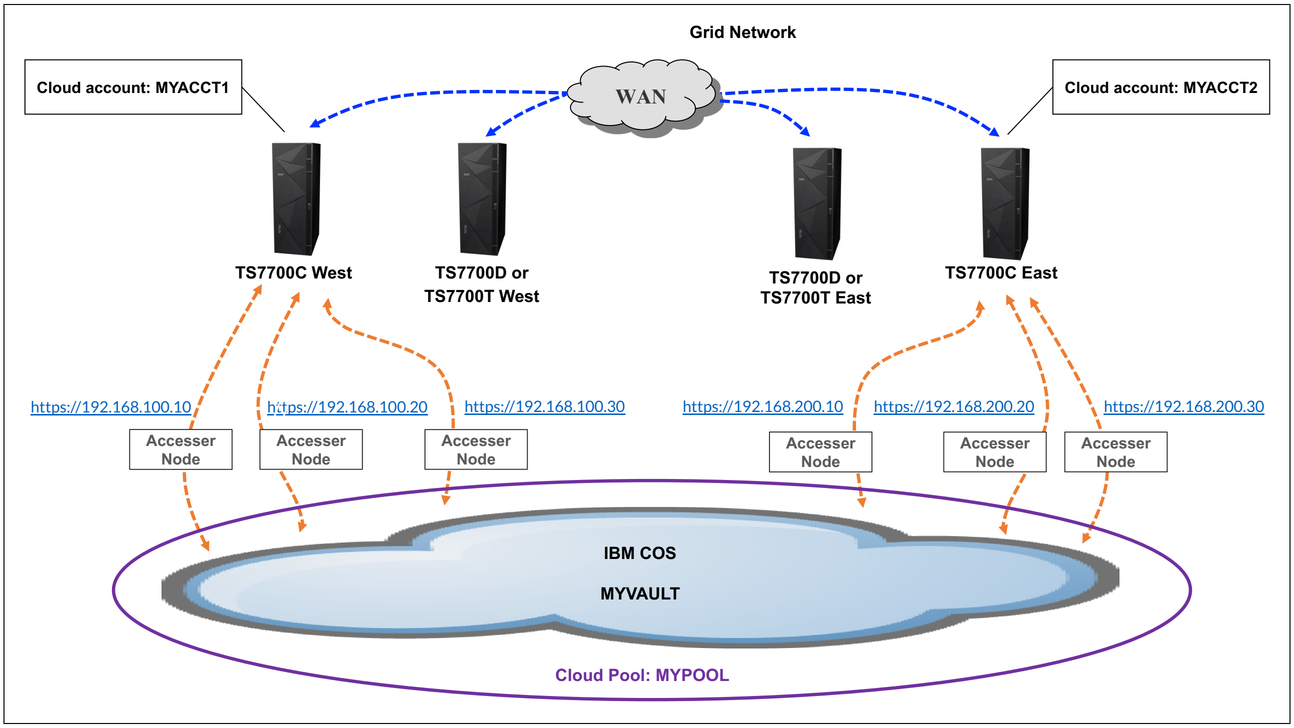


Figure 10-6 Four-way clusters

For example, you must create an SG that also points to MYPOOL on non-TS7700C clusters and assign the SG 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 an SG 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, 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 Accesser):

- `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 TS7700C cluster.

Creating a cloud pool

Complete the following steps:

1. On either TS7700C cluster, go to **Settings** → **Cloud Tier Settings** on the 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 IBM Cloud Object Storage 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) by 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 IBM Cloud Object Storage.
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 TS7700C 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 Accesser 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.

10.6 Stand-alone cluster with multiple cloud pools with IBM Cloud Object Storage and Amazon S3

This section shows how to set up multiple cloud pools with IBM Cloud Object Storage and Amazon S3. One cloud account and two vaults are available inside IBM Cloud Object Storage, and one cloud account and one bucket are available inside Amazon S3. Before setting up the Cloud Storage Tier, IBM Cloud Object Storage and Amazon S3 must be set up in your environment. For more information about setting up IBM Cloud Object Storage and Amazon S3, see Chapter 7, “Setting up an IBM Cloud Object Storage object store” on page 37 and Chapter 8, “Setting up Amazon Web Services cloud object storage” on page 55.

Figure 10-7 shows a stand-alone TS7700C with three cloud pools (MYPOOL1, MYPOOL2, and MYPOOL3), two cloud pools with two vaults (MYVAULT1 and MYVAULT2) inside IBM Cloud Object Storage, and one cloud pool with one bucket (MYBUCK) in Amazon S3. The same IBM Cloud Object Storage account (COSACCT) is used to access two vaults in IBM Cloud Object Storage, and the Amazon S3 account (AWSACCT) is used to access a bucket. To premigrate volumes to three different cloud pools, you must create three different SG constructs, and each of them points to its own cloud pool.

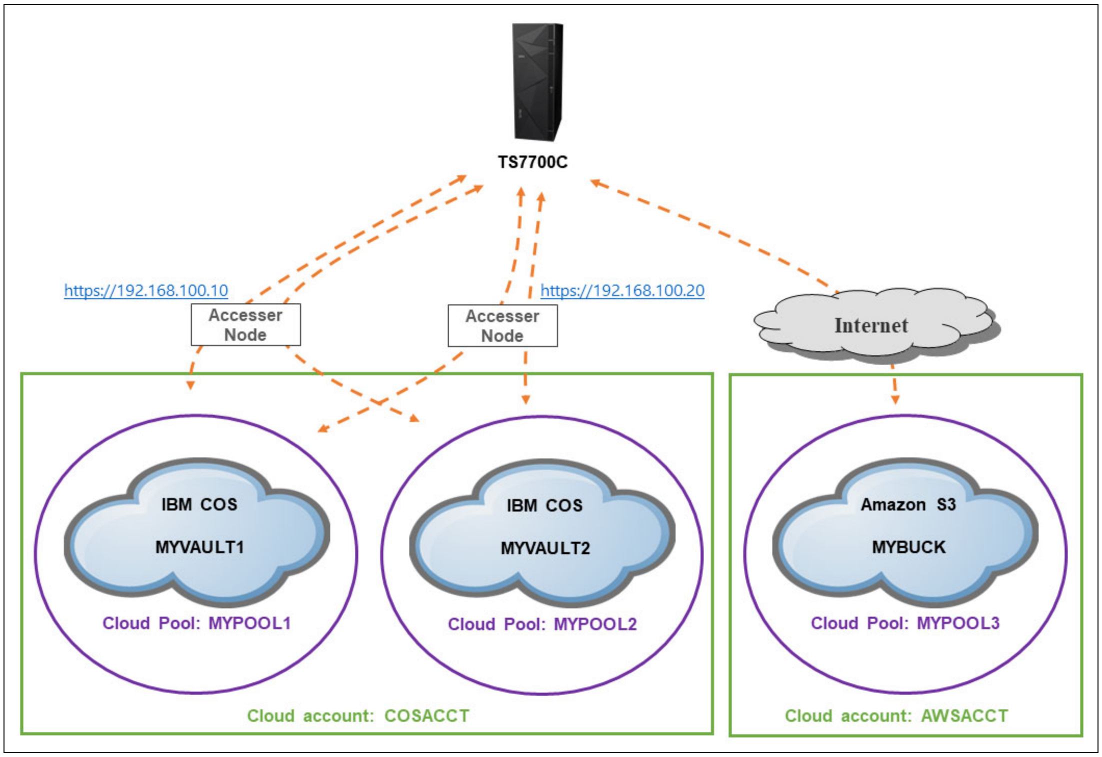


Figure 10-7 Multiple cloud pools

To set up this configuration, complete the following steps:

1. Create three cloud pools: MYPOOL1, MYPOOL2, and MYPOOL3.

   A cloud pool defines a group of common LVOLs that are collocated within the object store. In this example, one group of logical tape volumes is offloaded to MYPOOL1 inside IBM Cloud Object Storage, another group of LVOLs is offloaded to MYPOOL2 inside IBM Cloud Object Storage, and another group of LVOLs is offloaded to MYPOOL3 inside Amazon S3.

2. Create two accounts: COSACCT and AWSACCT.

   This step is needed to configure the credentials that are needed by the TS7700C to access IBM Cloud Object Storage and Amazon S3.

3. Create three containers: MYVAULT1, MYVAULT2, and MYBUCK.

   This step informs TS7700C about which vault and bucket it uses to offload a volume. The container must be assigned to the cloud pool, and you must select a cloud account to access the vault. The container name must be in sync with a vault in IBM Cloud Object Storage or a bucket in Amazon S3. In this example, two vaults in IBM Cloud Object Storage must be named: MYVAULT1, which is assigned to MYPOOL1, and MYVAULT2, which is assigned to MYPOOL2. The bucket in Amazon S3 must be named MYBUCK, which is assigned to MYPOOL3.

4. Create the following URLs for IBM Cloud Object Storage and Amazon S3:

   – `https://192.168.100.10` (for IBM Cloud Object Storage)
   – `https://192.168.100.20` (for IBM Cloud Object Storage)
   – Auto-generated URL (for Amazon S3)

5. Create the cloud URL and cluster associations.

   This step informs the cluster about which cloud URLs that were created in step 4 that it uses to access the vault. Three cloud URLs (`https://192.168.100.10, https://192.168.100.20`, and an auto-generated URL) must be associated with the cluster.

Each step of this process is described in more detail next.

Creating cloud pools

Complete the following steps:

1. On the TS7700C cluster, select **Settings** → **Cloud Tier Settings** on the MI and select **Cloud Pools**.
2. Click **Create Cloud Pool.**
3. Enter MYPOOL1 as the cloud pool's nickname.
4. Select **Standard Format** as the **Cloud Data Format**.
5. Click **OK**.
6. On the TS7700C cluster, create two more cloud pools (MYPOOL2 and MYPOOL3) by repeating steps 1 - 5.

Creating cloud accounts

Complete the following steps:

1. On the TS7700C cluster, select **Settings** → **Cloud Tier Settings** on the MI and select **Cloud Accounts**.
2. Click C**reate Cloud Account**.
3. Enter **COSACCT** 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 IBM Cloud Object Storage Admin) of your cloud account that is used in the West region and click **OK**.
7. On the TS7700C cluster, create another cloud account (AWSACCT) by using the **Access Key ID** and **Secret Access Key** pair that is used to access the bucket in Amazon S3. Make sure that **Amazon S3** is selected as the account type.

Creating containers

Complete the following steps:

1. Ensure that your vaults (MYVAULT1 and MYVAULT2) are created in IBM Cloud Object Storage.
2. On the TS7700C cluster, select **Settings** → **Cloud Tier Settings** on the MI and select **Containers**.
3. Click **Create Container**.
4. Enter MYVAULT1 as the container name.
5. Select **MYPOOL1** as the cloud pool.
6. Select **COSACCT** as the cloud account.
7. Click **OK**.
8. Create another container as MYVAULT2 and select **MYPOOL2** as the cloud pool and use COSACCT as the cloud account.
9. Create another container as MUBUCK and select **MYPOOL3** as the cloud pool and use **AWSACCT** as the cloud account.

When this process is completed, three containers are available: two for IBM Cloud Object Storage and one for Amazon S3.

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 the TS7700C cluster, select **Settings** → **Cloud Tier Settings** on the MI and select **Containers**.
3. Right-click the **MYVAULT1** container that is associated with COSACCT 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 **MYVAULT1** container and create another cloud URL for `https://192.168.100.20`.
9. Right-click the **MYVAULT2** container and create two cloud URLs for `https://192.168.100.10` and `https://192.168.100.20`
10. Right-click the **MYBUCK** container and select **Create Cloud URL** for the auto-generated URL.

When this process is complete, two URLs are defined under each of the two containers in IBM Cloud Object Storage (MYVAULT1 and MYVAULT2) and one URL is defined under a container in Amazon S3 (MYBUCK).

Creating a cloud URL and cluster associations

Complete the following steps:

1. On the TS7700C cluster, select **Settings** → **Cloud Tier Settings** in its MI window and select **Containers**.
2. Expand the Cloud URL that is assigned to MYVAULT1.
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 URL (`https://192.168.100.20`).
6. Expand the Cloud URL that is assigned to MYVAULT2, right-click the two Cloud URLs (`https://192.168.100.10` and `https://192.168.100.20`) that are assigned to MYVAULT2, and create **Cloud URL and Cluster associations**.
7. Expand the Cloud URL that is assigned to MYBUCK, right-click the **Cloud URL** (auto-generated URL) that is assigned to MYBUCK, and select **Create Cloud URL and Cluster association**.

When this process is complete, the TS7700C cluster is associated with three Cloud Pools: two Cloud Pools inside IBM Cloud Object Storage and one Cloud Pool in Amazon S3.

11

Disaster recovery principles

The description 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”, in *IBM TS7700 Release 5.2.2 Guide*, SG24-8464. It also adds considerations about DR when Cloud Storage Tier is attached to a TS7700 grid.

This chapter includes the following topics:

- 11.1, “Tier to cloud considerations” on page 114
- 11.2, “Cloud-based disaster recovery” on page 114
- 11.3, “Required data for restoring the host environment” on page 114
- 11.4, “Volume sizing” on page 115
- 11.5, “Recovery time objectives” on page 115
- 11.6, “Production activity and bandwidth” on page 115
- 11.7, “Redundancy in the cloud” on page 115
- 11.8, “Cost of object store retrieval” on page 115

11.1 Tier to cloud considerations

With the introduction of a new cloud storage tier, your production cluster and DR cluster can be TS7700Cs where both clusters are connected to the same cloud object store. In R5.0 or earlier releases, the data that is sent by the production cluster to the cloud object store was not automatically accessed by the DR cluster unless the copy policy on the production cluster allowed a copy to be sent to the DR cluster and that copy was completed.

TS7700 R5.1 introduced the Grid Awareness function. This function eliminates this requirement so that the DR cluster that is attached to the same cloud object storage as the production cluster can access the object data without needing a copy of the object on its tape volume cache (TVC).

An important aspect of Grid Awareness with the TS7700C is that immediate and automatic access to object stores in the cloud is available only to cloud-attached clusters (TS7700C drive) with R5.1 code level or later.

11.2 Cloud-based disaster recovery

The Cloud Storage tier provides more options for DR that you can use to continue with your existing DR process, and it adds an extra storage tier to the solution.

Cloud Export and Recovery is an optional function for customers that is similar to the Copy Export function. You use cloud object storage instead of physical tapes to export your data and restore it in a new empty TS7700C. It has the benefit of a reduced recovery point objective (RPO) and recovery time objective (RTO) after the copies are immediately available in the cloud versus being physically shipped and reinserted in the target cluster. It also reduces constraints regarding the number of physical drives that are available during recalls.

TS7700C drives that are configured in a grid can use cloud storage as a target location and skip the data transfer by using grid links to the other cloud-attached peers. Other TS7700C drives in the grid may have immediate access to the copy on the cloud if they have access to the container. Other non-cloud attached clusters that might be part of the grid still need a copy of the data through the grid links.

11.3 Required data for restoring the host environment

Volumes that contain data that is required to restore the host environment, such as direct access storage device 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 direct access storage device 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, hierarchical storage management (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 (LVOL) sizes might be preferred.

11.5 Recovery time objectives

When a TS7700C is part of the DR 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 (RTOs). 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 IBM 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 TS7700 object name format

This section describes the object name format. The name is long because we envision many use cases of merges, joins, sharing, importing, exporting, and so on, with the requirement that the object should never collide with any other TS7700 in the world. When looking in the object store, the objects that are created by the TS7700 take the following form:

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

PREFIX User-provided prefix in the Storage Group (SG)

XXXX 16-bit hexadecimal random value for object store hashing performance

COMPLIB Five-digit composite library ID of the grid that created the object

DISTLIB Five-digit distributed library ID of the cluster that created the object

SERIAL Five-character serial number of the cluster that created the object

VOLSER Six-character volume serial number that is being saved as an object

INSERT Token Insert Level

DATA Token Data Level

DATETIME YYYYMMDDHHMMSS Coordinated Universal Time time of when the object was created

Object names are shown in the following examples:

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

12.2 Bulk Volume Information Retrieval example

Bulk Volume Information Retrieval (BVIR) **`CLOUD VOLUME MAP`** can produce active logical volume (LVOL) 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.

With the `ALL` option, all versions of the LVOLs that are retained in the cloud are listed by the Volume Version Retention function that was introduced in R5.1.

BVIR CLOUD CONTENT is supported since R5.2.x to get a list of objects in the cloud for a specific cloud pool.

BVIR **`CLOUD BACKUP LIST`** returns a list of all cloud backups of the Cloud Export function that was introduced in R5.1. The output is the same format as the backup information in the `EXPORT STATUS` file.

For more information, see Chapter 17, “Cloud Storage Tier export, recovery, and testing” on page 167.

12.2.1 Sample output

Example 12-1 shows the BVIR **CLOUD VOLUME MAP ALL** output. The sample includes six LVOL records. Each record is 900 bytes.

Example 12-1 BVIR CLOUD VOLUME MAP ALL sample output

```
VTS BULK VOLUME DATA REQUEST
CLOUD VOLUME MAP ALL 0
09/17/2020 23:33:59 VERSION 10
S/N: HDCB0  LIB ID: D0030

VOLSER INSERT_VERSION       DATA_LEVEL           SYSPLEX_NAME SYSTEM_NAME
A00088 58                   101                  ISTC         ISTC
A00090 58                   102                  ISTC         ISTC
A00092 58                   101                  ISTC         ISTC
A00094 58                   101                  ISTC         ISTC
A00605 58                   101                  ISTC         ISTC
A00605 58                   102                  ISTC         ISTC

PROGRAM_NAME FILE_SIZE            CLOUD_ACCOUNT_ID    CLOUD_ACCOUNT_NICKNAME
IEBGENER     20628                HDCB020200727045456 ICOS1ACC
IEBGENER     20628                HDCB020200727045456 ICOS1ACC
IEBGENER     20628                HDCB020200727045456 ICOS1ACC
IEBGENER     20628                HDCB020200727045456 ICOS1ACC
IEBGENER     20628                HDCB020200727045456 ICOS1ACC
IEBGENER     40660                HDCB020200727045456 ICOS1ACC

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                 1             2020-09-17-14.47.23.000000
1                 0             1970-01-01-00.00.00.000000

PREMIGRATED_TIME           INITIATOR CLOUD_POOL          CLOUD_POOL_NAME
2020-08-06-16.22.58.000000 0         HDCB020200806151252 ICOS2POL
2020-08-08-18.29.45.000000 0         HDCB020200727045135 ICOS1POL
2020-08-11-03.02.45.000000 1         HDCB020200727045135 ICOS1POL
```

```
2020-08-11-03.02.45.000000 1         HDCB020200727045135 ICOS1POL
2020-09-17-14.26.16.000000 0         HDCB020200806151252 ICOS2POL
2020-09-17-14.47.25.000000 0         HDCB020200806151252 ICOS2POL

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                 12544           12544          0
1                 5376            5376           0

OBJECT_NAME
OBJPREF2/3f0a/C0003/D0030/HDCB0/A00088/58/101/20200806162257
OJBPREF1/24fd/C0003/D0030/HDCB0/A00090/58/102/20200808182944
OJBPREF1/71dc/C0003/D0031/HDCC0/A00092/58/101/20200811024856
OJBPREF1/204b/C0003/D0031/HDCC0/A00094/58/101/20200811024900
OBJPREF2/5748/C0003/D0030/HDCB0/A00605/58/101/20200917142614
OBJPREF2/4f88/C0003/D0030/HDCB0/A00605/58/102/20200917144723

CONTAINER_NAME
ts7700-vault02
ts7700-vault01
ts7700-vault01
ts7700-vault01
ts7700-vault02
ts7700-vault02
```

12.2.2 Sample job control language

Example 12-2 shows a job control language (JCL) sample to run BVIR **CLOUD VOLUME MAP ALL**.

Example 12-2 BVIR CLOUD VOLUME MAP ALL JCL sample

```
//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 ALL
/*
//SYSUT2    DD DSN=BVIR.CLOUD.VOLUME.MAP,DISP=(,KEEP),UNIT=GRIDLIB3,
//          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 TS7700 90 Day, 1 week, and 24 Hour Performance Evaluation Spreadsheets that are available at this IBM Support web page were not changed in R4.2. You can use these tools with the latest version, even if your TS7700 configuration includes cloud-attached clusters.

For more information about updates, see this IBM Support web page.

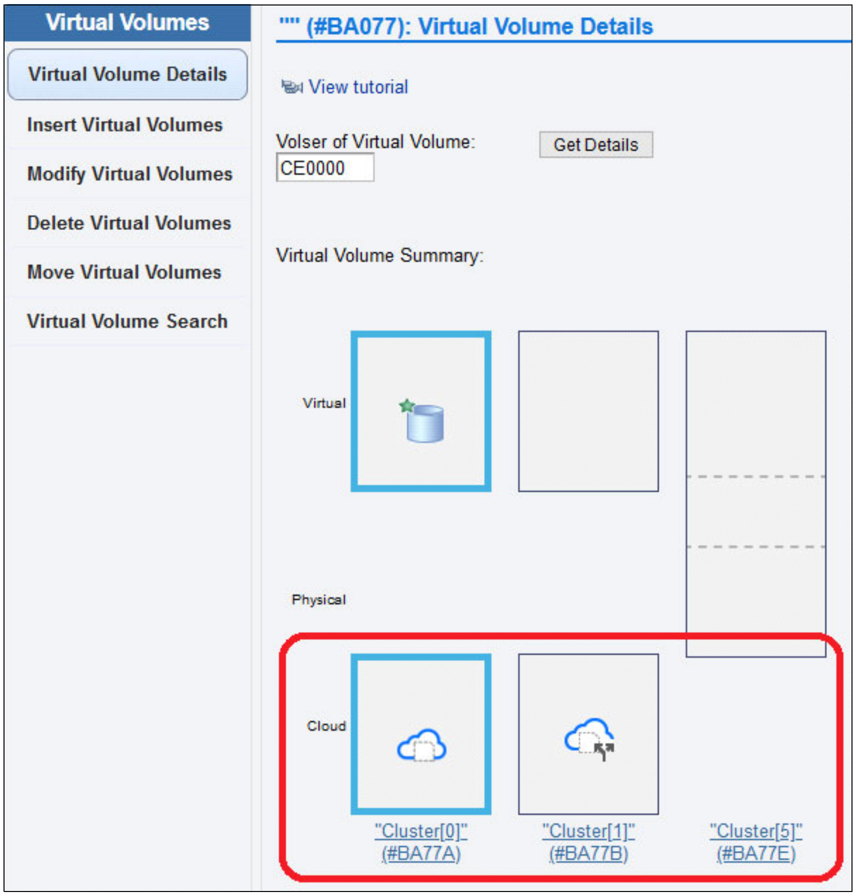
Until a future enhancement is made available, cloud-related statistics are reported within physical tape that is attached to a cluster's related fields. Cache hit, cache miss, premig, migrated, partition, or any other field that is related to Tape Attach also applies to cloud.

12.4 Management Interface windows

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

12.4.1 Virtual volumes details

You can display virtual volume details, including cloud-related information, as shown in Figure 12-1, Figure 12-2 on page 122, and Figure 12-3 on page 122.



"" (#BA077): Virtual Volume Details

Volser of Virtual Volume: CE0000

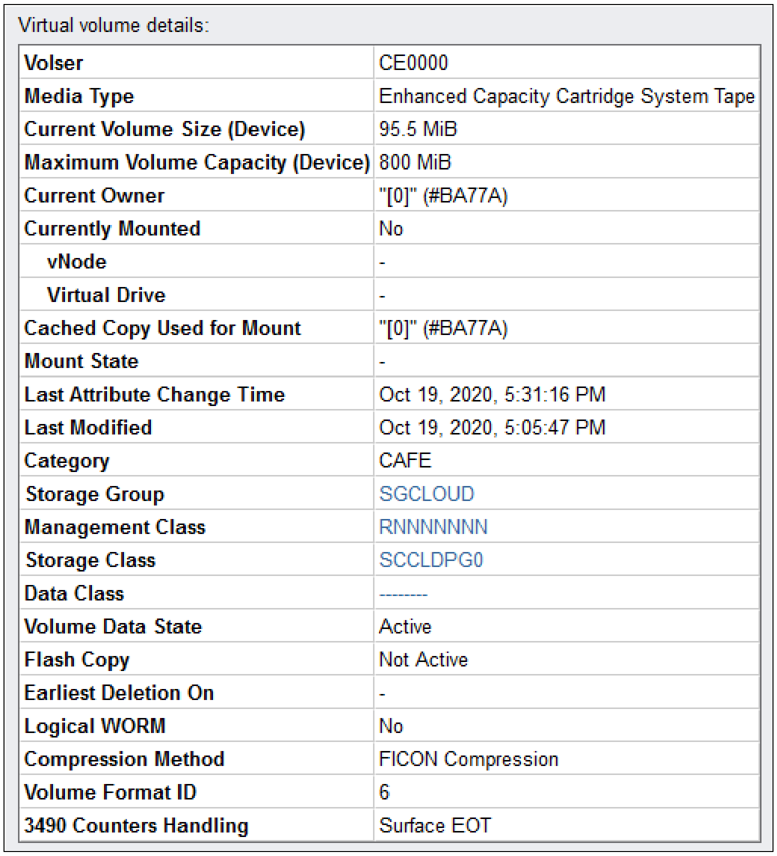
Virtual Volume Summary:

"Cluster[0]" (#BA77A)

"Cluster[1]" (#BA77B)

"Cluster[5]" (#BA77E)

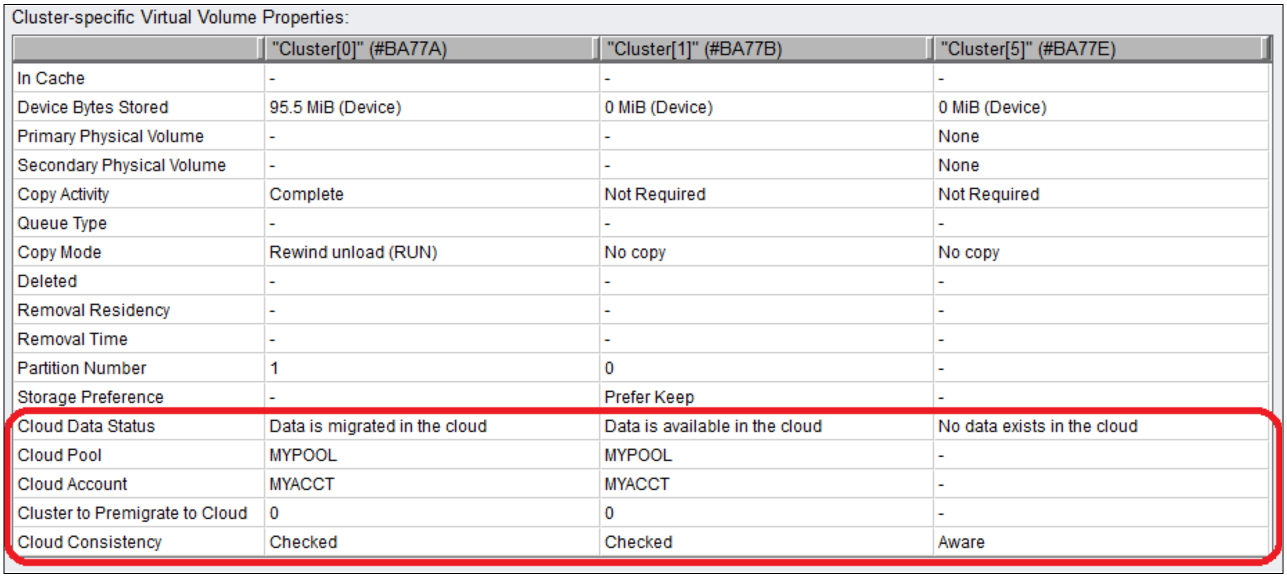
Figure 12-1 Virtual Volume Details: Part 1



Virtual volume details:

Volser	CE0000
Media Type	Enhanced Capacity Cartridge System Tape
Current Volume Size (Device)	95.5 MiB
Maximum Volume Capacity (Device)	800 MiB
Current Owner	"[0]" (#BA77A)
Currently Mounted	No
vNode	-
Virtual Drive	-
Cached Copy Used for Mount	"[0]" (#BA77A)
Mount State	-
Last Attribute Change Time	Oct 19, 2020, 5:31:16 PM
Last Modified	Oct 19, 2020, 5:05:47 PM
Category	CAFE
Storage Group	SGCLOUD
Management Class	RNNNNNNN
Storage Class	SCCLDPG0
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



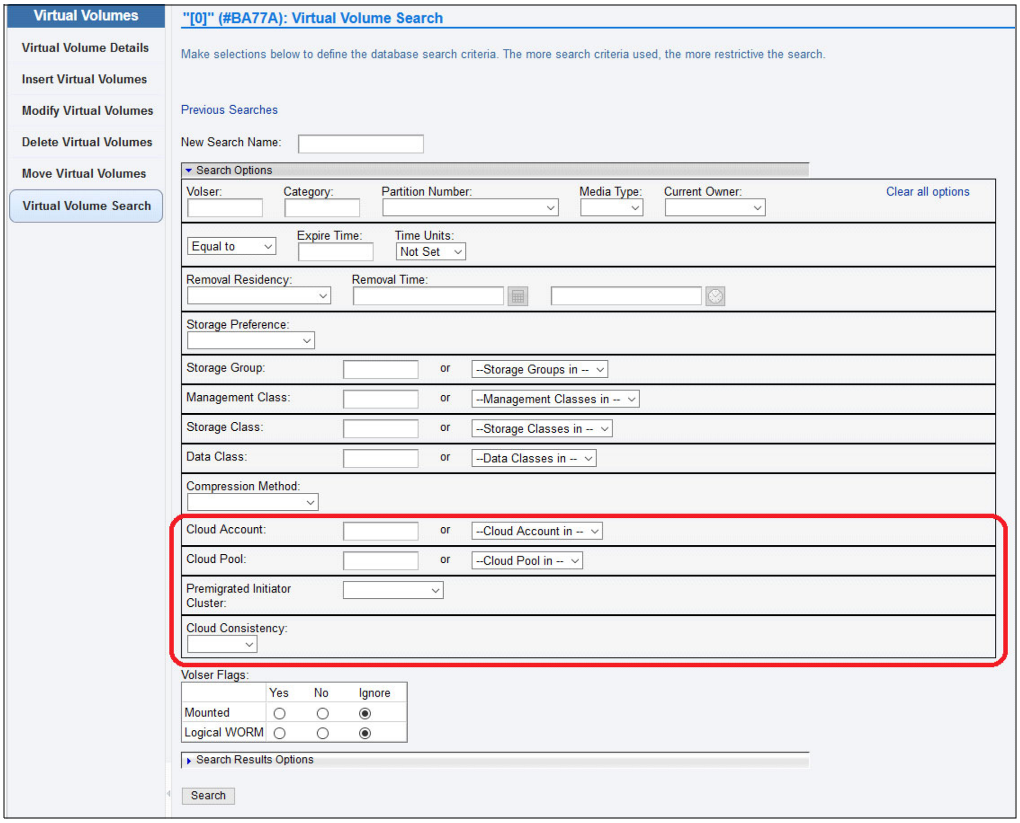
Cluster-specific Virtual Volume Properties:

	"Cluster[0]" (#BA77A)	"Cluster[1]" (#BA77B)	"Cluster[5]" (#BA77E)
In Cache	-	-	-
Device Bytes Stored	95.5 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	-
Storage Preference	-	Prefer Keep	-
Cloud Data Status	Data is migrated in the cloud	Data is available in the cloud	No data exists in the cloud
Cloud Pool	MYPOOL	MYPOOL	-
Cloud Account	MYACCT	MYACCT	-
Cluster to Premigrate to Cloud	0	0	-
Cloud Consistency	Checked	Checked	Aware

Figure 12-3 Virtual Volume Details: Part 3

12.4.2 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]" (#BA77A): Virtual Volume Search

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

Previous Searches

New Search Name:

▾ Search Options

Volser: | Category: | Partition Number: | Media Type: | Current Owner: | Clear all options

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 --Cloud Account in --

Cloud Pool: or --Cloud Pool in --

Premigrated Initiator Cluster:

Cloud Consistency:

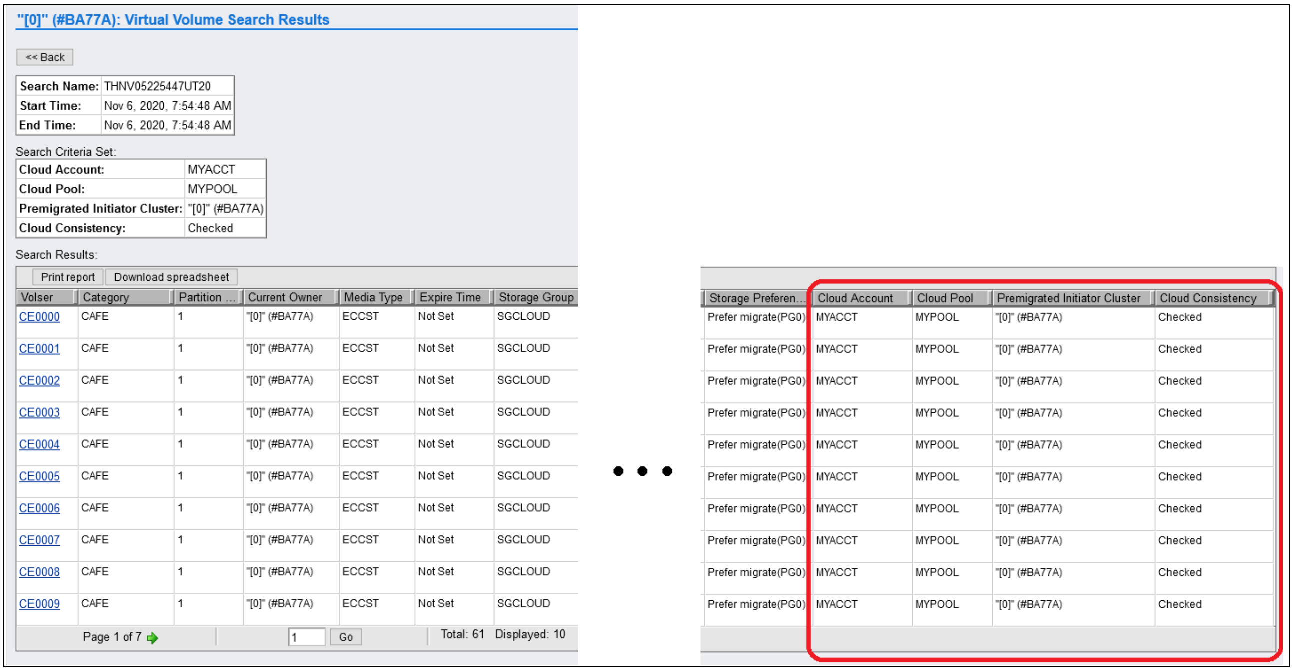
Volser Flags:

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

▸ Search Results Options

Search

Figure 12-4 Specifying filters to search virtual volumes



"[0]" (#BA77A): Virtual Volume Search Results

<< Back

Search Name:	THNV05225447UT20
Start Time:	Nov 6, 2020, 7:54:48 AM
End Time:	Nov 6, 2020, 7:54:48 AM

Search Criteria Set:

Cloud Account:	MYACCT
Cloud Pool:	MYPOOL
Premigrated Initiator Cluster:	"[0]" (#BA77A)
Cloud Consistency:	Checked

Search Results:

Print report | Download spreadsheet

Volser	Category	Partition ...	Current Owner	Media Type	Expire Time	Storage Group	Storage Preferen...	Cloud Account	Cloud Pool	Premigrated Initiator Cluster	Cloud Consistency
CE0000	CAFE	1	"[0]" (#BA77A)	ECCST	Not Set	SGCLOUD	Prefer migrate(PG0)	MYACCT	MYPOOL	"[0]" (#BA77A)	Checked
CE0001	CAFE	1	"[0]" (#BA77A)	ECCST	Not Set	SGCLOUD	Prefer migrate(PG0)	MYACCT	MYPOOL	"[0]" (#BA77A)	Checked
CE0002	CAFE	1	"[0]" (#BA77A)	ECCST	Not Set	SGCLOUD	Prefer migrate(PG0)	MYACCT	MYPOOL	"[0]" (#BA77A)	Checked
CE0003	CAFE	1	"[0]" (#BA77A)	ECCST	Not Set	SGCLOUD	Prefer migrate(PG0)	MYACCT	MYPOOL	"[0]" (#BA77A)	Checked
CE0004	CAFE	1	"[0]" (#BA77A)	ECCST	Not Set	SGCLOUD	Prefer migrate(PG0)	MYACCT	MYPOOL	"[0]" (#BA77A)	Checked
CE0005	CAFE	1	"[0]" (#BA77A)	ECCST	Not Set	SGCLOUD	Prefer migrate(PG0)	MYACCT	MYPOOL	"[0]" (#BA77A)	Checked
CE0006	CAFE	1	"[0]" (#BA77A)	ECCST	Not Set	SGCLOUD	Prefer migrate(PG0)	MYACCT	MYPOOL	"[0]" (#BA77A)	Checked
CE0007	CAFE	1	"[0]" (#BA77A)	ECCST	Not Set	SGCLOUD	Prefer migrate(PG0)	MYACCT	MYPOOL	"[0]" (#BA77A)	Checked
CE0008	CAFE	1	"[0]" (#BA77A)	ECCST	Not Set	SGCLOUD	Prefer migrate(PG0)	MYACCT	MYPOOL	"[0]" (#BA77A)	Checked
CE0009	CAFE	1	"[0]" (#BA77A)	ECCST	Not Set	SGCLOUD	Prefer migrate(PG0)	MYACCT	MYPOOL	"[0]" (#BA77A)	Checked

Page 1 of 7 | 1 Go | Total: 61 Displayed: 10

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 LVOL.

12.5.1 LI REQ STATUS command with GRLNKACT parameter

The **LI REQ STATUS GRLNKACT** command response is enhanced to include information about grid link activity to the cloud. In response to this request, the grid provides point-in-time (PiT) details about all of the grid link activity for all configured clusters in the grid. If any of the clusters are cloud-attached, the cloud activity across the links also is provided as CLD_REC and CLD_SEND. Before R5.0, the values for the cloud activity include the activity for Grid to Grid Migration (GGM). At R5.0 or later, Cloud, GGM, and DS8K object storage activities are provided separately as CLD_REC and CLD_SND, GGM_REC and GGM_SND, and OBJ_REC and OBJ_SND. The information is summed as 15-second intervals, and the next interval starting after the command is received and returned to the issuer.

For more information about the **GRLNKACT** parameter, see 16.2.8, "LI REQ STATUS command with GRLNKACT parameter" on page 161.

12.5.2 The LI REQ LVOL command with the 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 output for the current version of **INFO** 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 LVOL within the object store.

For more information about the **INFO** parameter, see 16.2.2, "LIBRARY REQUEST,composite_library,LVOL,volser,INFO" on page 151.

12.5.3 The LI REQ LVOL command with the CLDINFO parameter

This command provides the LVOL status of the cloud (that is, object data). It indicates whether the LVOL is premigrated to the cloud, and in which clusters in the grid the data is accessible from.

For more information about the **CLDINFO** parameter, see 16.2.4, "LIBRARY REQUEST,composite_library,LVOL,volser,CLDINFO" on page 153.

12.5.4 The LI REQ LVOL command with the CLDVERS parameter

The command is supported as the Volume Version Retention function since R5.1. This command provides the list of LVOL versions that are stored on the cloud (that is, object data).

For more information about the **CLDVERS** parameter, see 16.2.5, "LIBRARY REQUEST,distributed_library,LVOL,volser,CLDVERS,page_index" on page 153.

12.5.5 The LI REQ CLDBKUP command with the SHOW parameter

The command is supported as the Cloud Export function since R5.1. This command provides the list of all the pool backups that were created on the cloud.

For more information about the CLDBKUP parameter, see 16.2.7, “LIBRARY REQUEST,distributed_library,CLDBKUP,SHOW,page_index” on page 160.

12.5.6 Cloud-related operator messages

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

For the table of message IDs and descriptions, see 16.2.9, “Cloud-related operator messages” on page 163.

12.6 Capacity monitoring cloud storage

The capacity of your object store must be monitored. The TS7700C can surface an alert when the threshold is set for free space within the object store. Although you cannot determine exact space usage within the object store, you can monitor it by using the function within the object storage. This section describes capacity monitoring for cloud object storage.

12.6.1 Alerts for a space shortage within the object storage

You can set low and high alert levels for the amount of data that is stored in object storage since R5.1 by running the following commands:

```
LI REQ CLDSET,USEHIGH,<cloud pool nickname>,<number of terabytes>
LI REQ CLDSET,USELOW,<cloud pool nickname>,<number of terabytes>
```

An alert (operator intervention) is surfaced when the cloud usage exceeds the level for more than 5 minutes. The alert of **USEHIGH** repeats every 15 minutes. When the cloud usage falls below that level, another message that states that the condition is cleared is output.

When “0” is set, the alert is turned off. The default value is “0”. You can see low and high alert levels for each cloud pool by running the following command:

```
LI REQ CLDSET, USESHOW, <index>
```

Output is pagerized, that is, 128 cloud pools per page. The third keyword is the page index to show. The list is sorted by cloud pool ID.

12.6.2 Capacity monitoring on IBM Cloud Object Storage on-premises

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

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

For more information, see this IBM Documentation web page.

12.6.3 Capacity monitoring on AWS S3

Unlike an IBM Cloud Object Storage on-premises system, AWS Simple Storage Service (S3) provides unlimited capacity. However, it is still a best practice to monitor capacity usage, the amount of data that is transferred for recalls (not for premigration), the number of recall requests, and any CRR (if enabled) because all 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.

12.6.4 Capacity monitoring on IBM Cloud Object Storage public

Capacity monitoring is required to prevent the cloud object storage from becoming full on IBM Cloud Object Storage public.

You can use IBM Cloud Object Storage public with NGINX as the reverse proxy server, which is supported on TS7700C at R4.2 PGA2 or later with a SCORE request.

IBM Cloud Object Storage public provides the web-based console for a capacity utilization. For more information, see Getting started with IBM Cloud Storage.

12.6.5 Capacity monitoring on RSTOR

Capacity monitoring is required to prevent the cloud object storage from becoming full on RSTOR.

You can use RSTOR with NGINX as the reverse proxy server, which is supported on TS7700C at R4.2 PGA2 or later with a SCORE request.

RSTOR provides the web GUI for managing capacity utilization.

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

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 TS7700D or TS7700T to TS7700C in the Grid configuration
- Migrating data from an existing TS7700C to a TS7700C in the grid configuration by using ghost copies

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

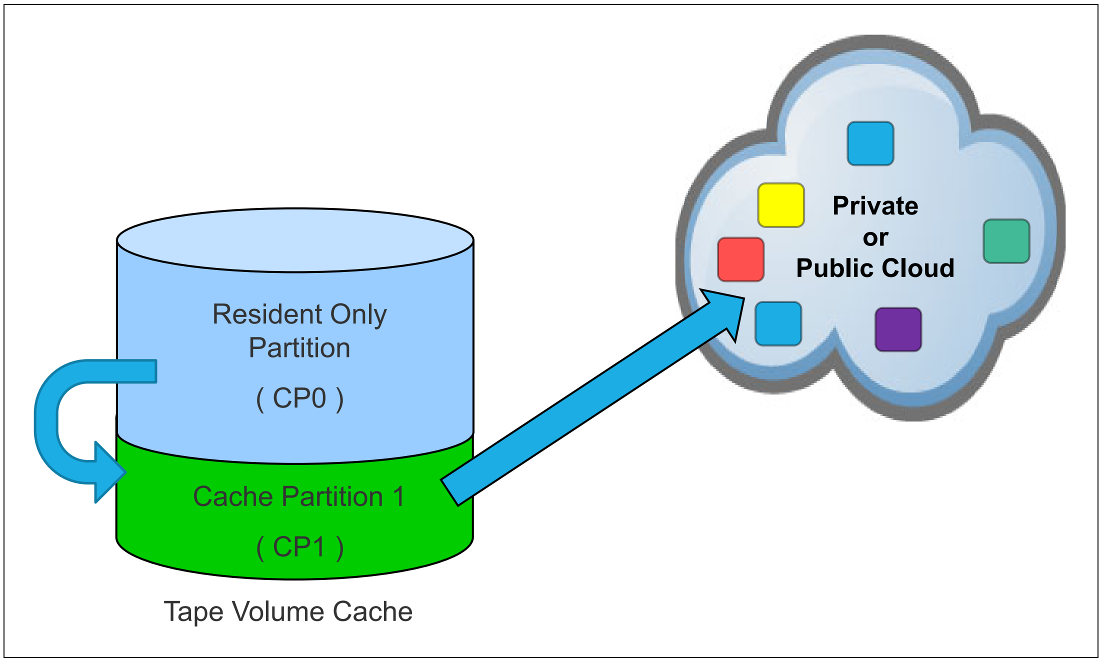


Figure 13-1 Partition Assignment change

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

With SC, you can 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 SC is also used to assign the migration preference group, which 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

With SG, you can determine the cloud pool that the volumes migrate to within the cloud.

> **Note:** You must specify the same cloud pool for a specific SG 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 SG 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. The primary action is a host-started mount/demount of a logical volume (LVOL). You can use the **PARTRFSH MMOUNT** command (which stands for *Mimic MOUNT*) to accept the new cloud pool assignment and new partition CPx location. To run the **PARTRFSH MMOUNT**, run the following command:

```
LIBRARY REQUEST,distributed_library,PARTRFSH,volser,MMOUNT
```

This command is useful when a TS7700 is upgraded to be attached to the cloud. After the new partition is defined by the SG and SC, you can use the command to update all the VOLSERs with the new construct so that the volume is pre-migrated to the cloud object store. Therefore, a mount/demount operation is not needed for the new constructs to be applied to the existing VOLSERs.

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

For more information about TAPETOOLs, see this web page.

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

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 TS7700D or TS7700T to TS7700C in the grid configuration through replication

To migrate data to the cloud through a cloud attached peer, you must first replicate volumes from a TS7700D or TS7700T cluster to a TS7700C cluster, and second target a CPx partition in the TS7700C cluster (see Figure 13-2).

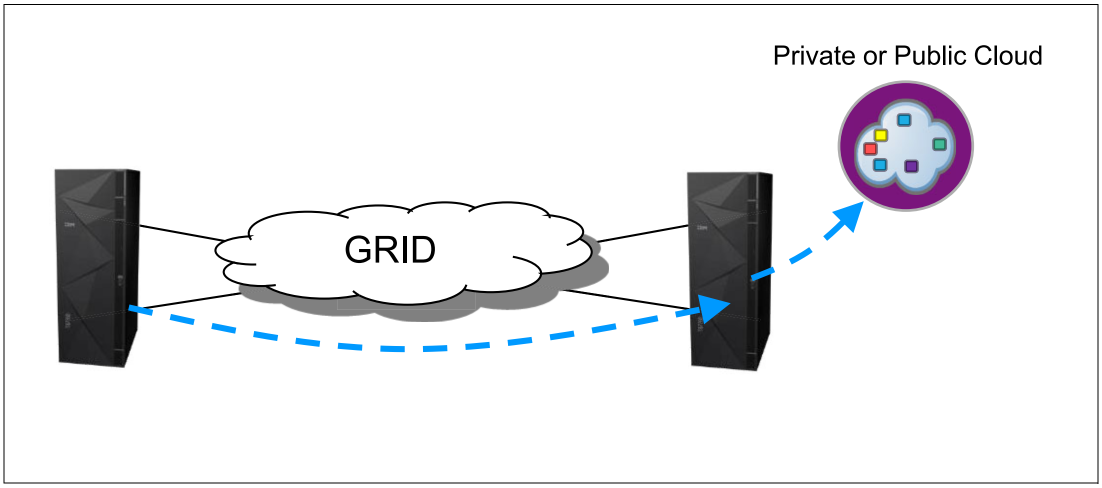


Figure 13-2 Copying the volumes to TS7700C

Complete the following steps to migrate volumes from a TS7700D or TS7700T cluster to a TS7700C cluster:

1. Change the assigned Management Class (MC) at one or more clusters to specify a copy consistency point for the TS7700C cluster.
2. Change the assigned SC in the TS7700C cluster to specify a CPx partition that is used at the target TS7700C cluster.
3. Change the assigned SG 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 MC, SC, or SG 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 MC 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

  With SC, you can 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 SC 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 (LRU) 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

  With SG, you can determine to which cloud pool the volume migrates.

> **Note:** You must specify the same cloud pool for an SG 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 SC 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 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 SG 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

The following list has some actions and checks that must be considered:

- If the LVOL has no cloud pool that is assigned or a CPx assignment, you must assign a cloud pool and a cache partition first.
- Construct changes do not automatically apply to volumes without an action first taking place, so after assigning a new construct to the volume, you have two ways to make it accept the new policy:
  - Mount / Demount
  - Mimic a mount by running the following command:

    ```
    “LIBRARY REQUEST,distributed_library,PARTRFSH,volser,MMOUNT”
    ```

If the LVOL’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.

After that, the **COPYRFSH CLDGHOST** command can be used to migrate the volume to the cloud through the new TS7700C cluster. Issue the following command to run the **COPYRFSH CLDGHOST**:

```
LIBRARY REQUEST,distributed_library,COPYRFSH,volser,CLDGHOST
```

For more information about this scenario, see page 223 of *TS7700 Library Request Command V5.22*.

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 SC that is the 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.

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.

13.1.3 Migrating data from TS7700C to TS7700C in the grid configuration by using ghost copies

To migrate data from an existing TS7700C to a newly joined TS7700C cluster in the grid configuration, you can skip replication of LVOLs through a grid link but make the new cluster aware of the LVOLs if they are already premigrated to the cloud from the existing TS7700C. (see Figure 13-3).

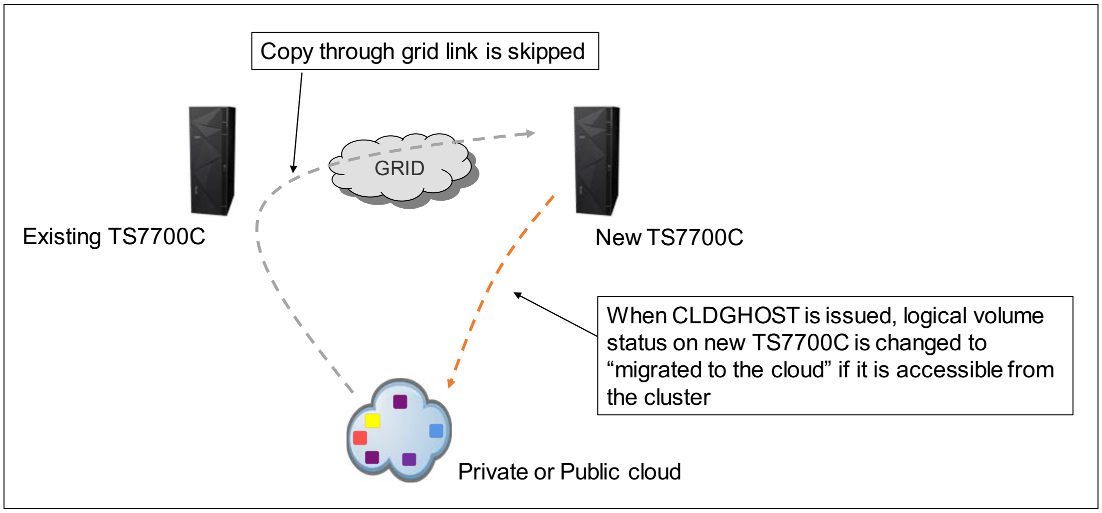

Copy through grid link is skipped
GRID
Existing TS7700C
New TS7700C
When CLDGHOST is issued, logical volume status on new TS7700C is changed to “migrated to the cloud” if it is accessible from the cluster
Private or Public cloud

Figure 13-3 Ghost copy to new TS7700C

This process is called *ghost copy* and can be done by using the **COPYRFSH CLDGHOST** command (which stands for *CLouD GHOST*).

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

1. Change the assigned MC at one or more clusters to specify a copy consistency point for the TS7700C cluster.
2. Change the assigned SC in the TS7700C cluster to specify a CPx partition that is used at the new TS7700C cluster.
3. Change the assigned SG in the new TS7700C cluster to specify the cloud pool assigned in the existing TS7700C clusters.
4. (Optional) Apply the MC, SC, or SG if a construct name change is required.
5. With R5.1 and later, the ghost copy is automatic for all cloud-attached clusters in the grid, and all clusters have access to the data. But, if you still want the cluster to have a valid copy mode and still view its copy as “migrated in the cloud”, then the **COPYRFSH CLDGHOST** command can be used to update the local cluster's copy policy and skip the copy because a volume exists in the cloud.

After all these steps are complete, the new TS7700C cluster is aware of the volumes in the cloud. The volume status on the new TS7700C becomes migrated and can be recalled from the cloud.

Constructs settings

To migrate the volumes from existing TS7700C clusters to a new TS7700C cluster, you must assign constructs to the volumes. The following constructs must be set to migrate to the new TS7700C cluster:

- Management Class

  The MC 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 new TS7700C. The TS7700C copy is in addition to any peer copies or other TS7700C clusters that also receive a copy.

- Storage Class

  With SC, you can 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 SC is also used to determine the migration preference group, whether the TS7700C attempts to retain the volume in disk cache by using an LRU algorithm, or whether it is flushed from disk cache when a copy to the cloud completes. Regardless of this preference, the volume status on the new TS7700C cluster will be changed as migrated after a ghost copy.

- Storage Group

  With SG, you can determine to which cloud pool the volume migrates.

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 MI Modify Virtual Volume window, you can assign new constructs to a volume. This function is primarily intended for non z/OS systems, and it cannot reflect any change to host system (include z/OS). Because SG 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.

If a cloud pool and the CPx partition are assigned to the LVOL on the new TS7700C cluster, the **COPYRFSH CLDGHOST** command can be used to run a ghost copy and make the new TS7700C cluster update the cloud data status to “migrated in the cloud”. To run a ghost copy, run the following command:

```
LIBRARY REQUEST,distributed_library,COPYRFSH,volser,CLDGHOST
```

After a ghost copy completes, the cloud data status is updated to `data is migrated in the cloud`.

The volume is recalled from the cloud to an existing TS7700C cluster, and a normal grid copy replicates the volume to the new TS7700C in one of the following three cases:

- **COPYRFSH** command is issued without the `CLDGHOST` keyword.
- The new TS7700C cluster is not connected to the cloud.
- The CP0 partition is assigned to the LVOL on the new TS7700C cluster.

For more information, see page 239 of *TS7700 Library Request Command V5.22*.

13.2 Upgrading a TS7700 to TS7700C

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

13.2.1 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, “IBM TS7700C planning considerations” on page 25 and Chapter 9, “Configuring IBM TS7700 for Cloud Storage Tier” on page 73.

13.2.2 Cache partitions

In addition to introducing a cloud tier and the cloud tier configuration windows, 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 13-4).

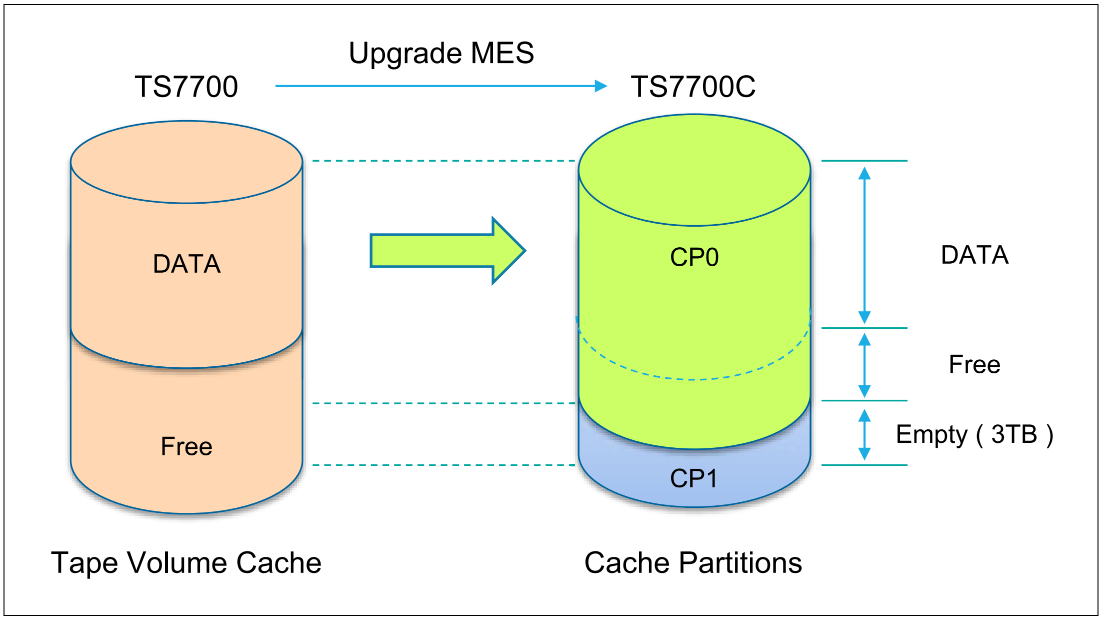


Figure 13-4 Cache partitions

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

13.2.3 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 IBM TS7700 for Cloud Storage Tier” on page 73.

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 128.

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” on page 138
- 14.2, “Domain Name System and JSON settings for AWS S3” on page 138
- 14.3, “Cloud service problems” on page 140
- 14.4, “Cloud or Grid network failures” on page 142
- 14.5, “Events that are cloud-related” on page 143

14.1 Network firewall problems

A TS7700C 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 Cloud Object Storage on-premises, AWS Simple Storage Service (S3), IBM Cloud Object Storage public, or RSTOR. If you are using a standard HTTP connection to IBM Cloud Object Storage on-premises, port 80 must be open.

14.2 Domain Name System and JSON settings for AWS S3

In this section, we describe the Domain Name System (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 Cloud Object Storage on-premises. For AWS S3, the TS7700C requires a DNS server to resolve the AWS hostnames 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, Management Interface (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 TS7700C must set up internal routing and firewall tables to communicate with all possible AWS addresses. The TS7700C 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 TS7700C 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 TS7700C 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 TS7700C firmware and can be outdated. Therefore, the TS7700C 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 TS7700C 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 that 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.

TS7700C can access AWS S3 Object Storage through the GRID network, which must be connected to the internet.

Figure 14-1 shows connections between TS7700C, DNS server in the Customer network, and AWS.

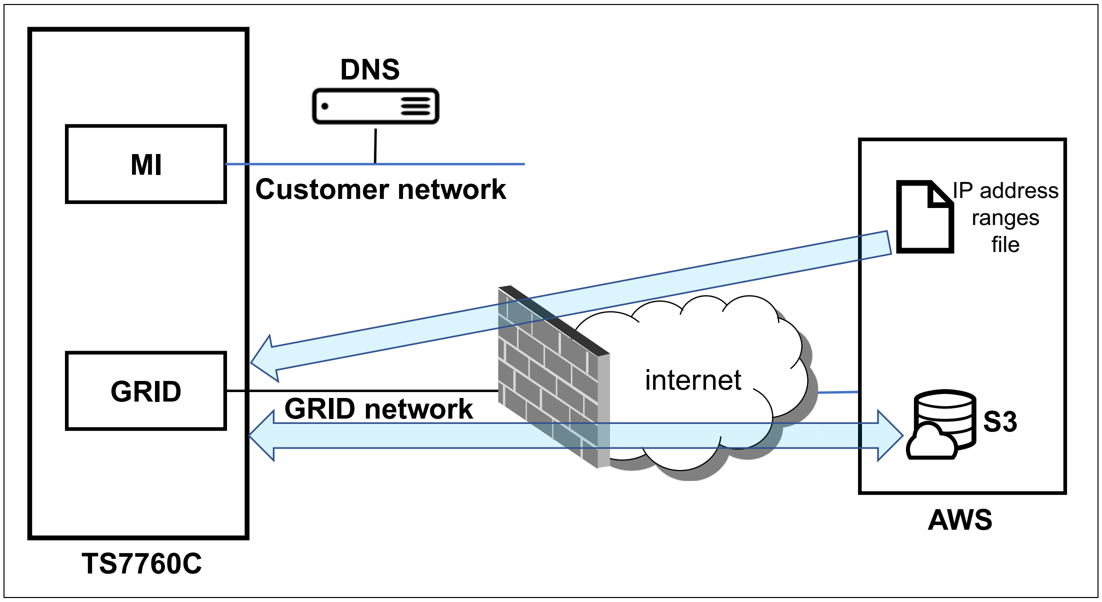


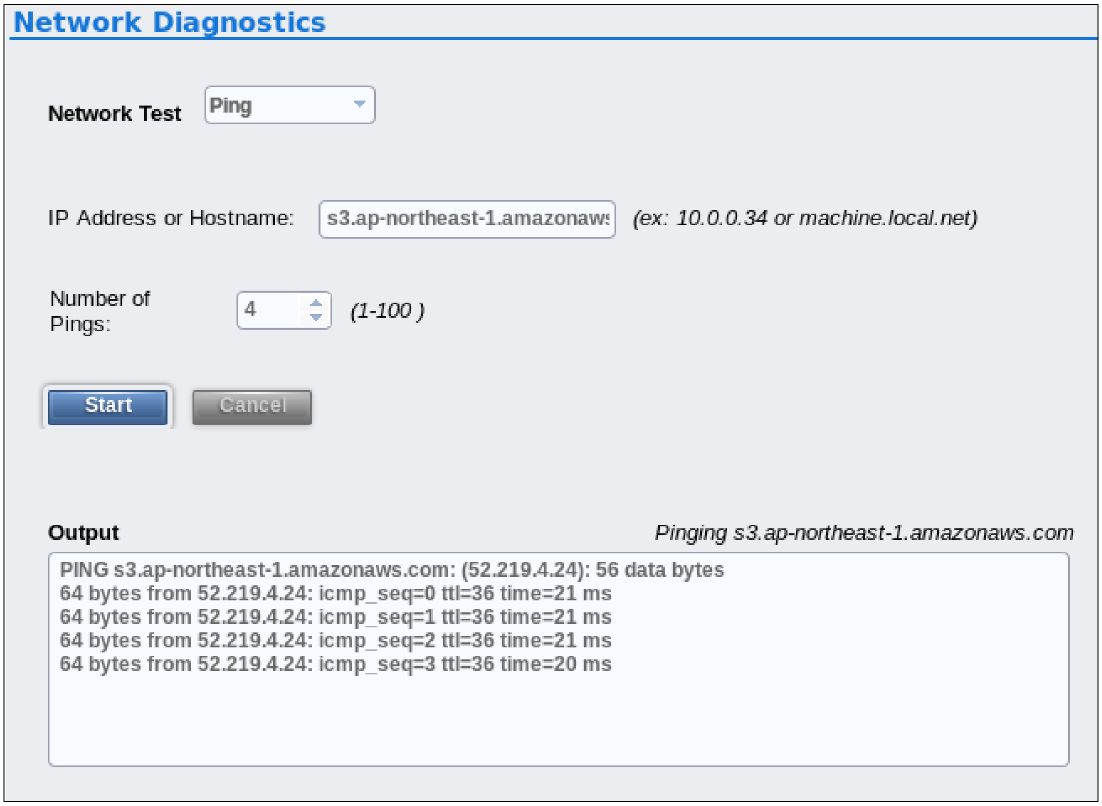
Figure 14-1   TS7700C and AWS network communication

To check the communications from the TS7700C to the AWS object storage 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)

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 a AWS S3 hostname 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 Cloud SSL certificate expired

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

14.3.2 Cloud credential expired 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 Object Storage is receiving heavy requests from other devices

If your Object Storage is shared by the TS7700C 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 Grid network is receiving heavy replication throughput

Because your Object Storage is shared by the TS7700C 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 Object store is 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. You must monitor usage of your object storage. Since R5.1, it is a best practice that you set alert levels to monitor your object store's usage capacity for the TS7700C to ensure that a full condition is not reached.

To set the alert for usage, see 12.6, “Capacity monitoring cloud storage” on page 125.

14.3.6 Time difference between TS7700C and Object Storage is greater than 10 minutes

The time on the TS7700C and the cloud object storage must be synchronized. If the time difference between the TS7700C and IBM Cloud Object Storage on-premises is greater than 10 minutes, a health monitor detects the error and issues the event OP0866. Use time servers within your TS7700C and IBM Cloud Object Storage on-premises 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 TS7700C 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 TS7700C to an object store failed, migration to the cloud is suspended for that specific TS7700C 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 TS7700C 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 TS7700C cluster fails because of a network issue, yet a second TS7700C cluster is successful.

After the network reconnects to the cloud and the TS7700C 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 done asynchronously by using an eject request of a logical volume (LVOL). 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 5,000 LVOL deletes per hour per TS7700 as described in the **LI REQ SETTING DELEXP** count setting. After the LVOL is deleted from within the TS7700C, the object is marked pending deletion in the TS7700C 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 LVOL 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 LVOL eject is completed, any object instance in an object store that is associated with the ejected LVOL 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 LVOL can be reinserted during this period, if needed.

14.4.5 LI REQ CLDINFO command

LVOL 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 that are cloud-related

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 IBM TS7700C" on page 117.

15

Performance considerations

This chapter describes performance considerations regarding TS7700 cloud attach and includes the following topics:

- 15.1, “Generalizing a grid configuration by using units of work” on page 146
- 15.2, “Cloud attach-specific performance considerations” on page 148

15.1 Generalizing a grid configuration by using units of work

The TS7700 performance behavior, including cloud object storage 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 (cluster 0 (CL0)) and a TS7700T (cluster 1 (CL1)). It is an example of a near worse case scenario in which all data is replicated and premigrated to tape and cloud.

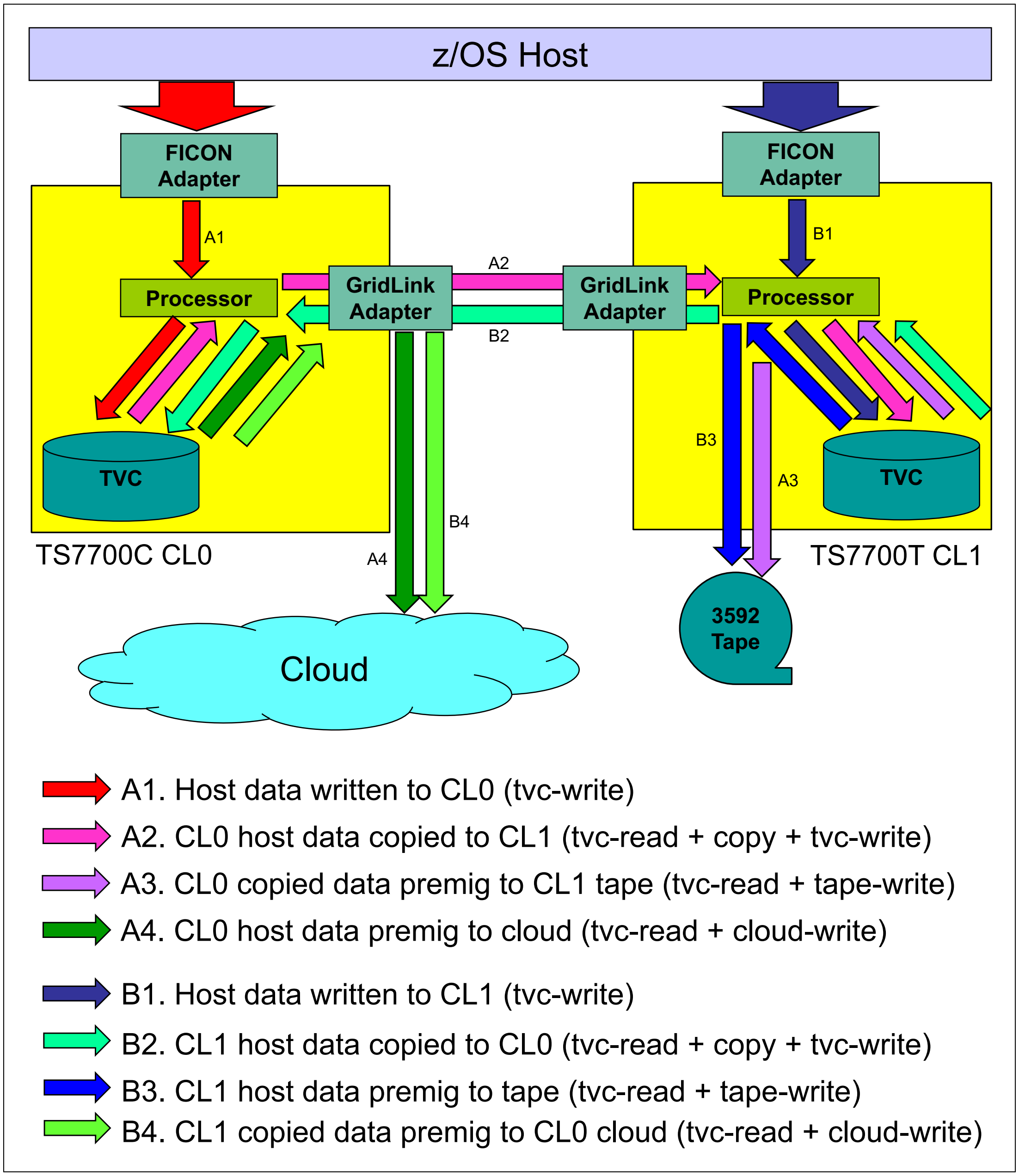

z/OS Host
FICON Adapter
A1
Processor
GridLink Adapter
A2
B2
GridLink Adapter
FICON Adapter
B1
Processor
TVC
TS7700C CL0
A4
B4
B3
A3
TVC
TS7700T CL1
3592 Tape
Cloud
A1. Host data written to CL0 (tvc-write)
A2. CL0 host data copied to CL1 (tvc-read + copy + tvc-write)
A3. CL0 copied data premig to CL1 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 tape volume cache (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 on page 146 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 on page 146:

- Each cluster receives its own 300 MBps decompressed from its connected hosts.
- All logical volumes (LVOLs) include RUN or Deferred copy mode with a zero deferred copy throttling (DCT).
- All LVOLs are premigrated to cloud on CL0 and 3592 tape on CL1.
- The data compression ratio is 3:1.
- None to minimal LVOLs 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 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-premises cloud stores. Maximum throughput to 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.

Feature Code (FC) 5274 (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 recovery point objective (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 Release 5.1 enhanced Cloud Storage Tier with grid awareness

With this support, any clusters that do not have a valid copy can access the cloud copy when the cluster that has a valid copy is not available. So, if you do not need to copy the LVOLs into cache and accessing the cloud copy is sufficient to achieve data access redundancy, then you do not need to replicate the volumes to other clusters. As a result, you can reduce the required grid network bandwidth.

15.2.3 Logical volume size

If network bandwidth is limited, premigration to a cloud and recall from a cloud for a LVOL requires longer times when compared to 3592 tape drives. For example, a 25 GB LVOL requires almost 40 minutes if only 100 Mbps bandwidth is available. It is a best practice that smaller volume sizes be used for workloads that require frequent recalls so that mount completion and access to data can occur sooner.

15.2.4 Premigrate and recall timeouts

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 that support the Cloud Storage Tier function.

This chapter includes the following topics:

16.1 Cloud Storage Tier host considerations

With R4.2, the TS7700 now can store logical volumes (LVOLs) on an attached Cloud Storage Tier. Although no host support is needed to use this Cloud Storage Tier function, applying OA55481 to each attached z/OS host is recommended. This APAR includes the following enhancements:

- Two messages:

  ```
  CBR3736E Cloud object store degraded in library library-name
  CBR3737I Cloud object store no longer degraded in library library-name
  ```

  The `CBR3736E` message is 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 is written to the host console because the **`D SMS,LIBRARY(`*`libname`*`)`** command was 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 that is configured to a cloud object store, it also includes the “Cloud object store configured” information.
- The `CBR1140I` message is written to the host console because 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 LVOL is in the cloud object store.

16.2 LI REQ support for Cloud Storage Tier

The following commands are available to support the Cloud Storage Tier function:

- `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`*`,LVOL,volser,CLDVERS,page_index`
- `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`
- `LIBRARY REQUEST,`*`distributed_library`*`,CLDSET,PFRCCPGO`
- `LIBRARY REQUEST,`*`distributed_library`*`,CLDSET,PFRCCTDL`
- `LIBRARY REQUEST,`*`distributed_library`*`,CLDSET,PFRCCTRY`
- `LIBRARY REQUEST,`*`distributed_library`*`,CLDSET,USEHIGH`
- `LIBRARY REQUEST,`*`distributed_library`*`,CLDSET,USELOW`
- `LIBRARY REQUEST,`*`distributed_library`*`,CLDSET,USESHOW,page_index`
- `LIBRARY REQUEST,`*`distributed_library`*`,CLDVR,RESERVE/DESTCAT/DESTVOL`

- LIBRARY REQUEST,*distributed_library*,CLDBKUP,SHOW,page_index
- LIBRARY REQUEST,*distributed_library*,STATUS,GRLNKACT

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 *TS7700 Library Request Command V5.22*.

16.2.1 LIBRARY REQUEST,distributed_library,CLDVR,RESERVE/DESTCAT/DESTVOL

For more information about CLDVR documentation, see the *IBM TS7700 Cloud Storage Tier Export, Recovery, and Testing Guide.*

16.2.2 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 **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 LVOL 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 the INFO 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 parameter **INFO**, no cloud-related information is displayed. Instead, a warning message is displayed that indicates the third keyword **INFO** is required to get LVOL information with the format, as shown in Example 16-2.

Example 16-2 LI REQ LVOL command sample output without the INFO 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
```

16.2.3 LIBRARY REQUEST,composite_library,LVOL,volser,INFO,FLASH

Starting with R4.2, the **`LIBRARY REQUEST,composite_library,LVOL,volser,FLASH`** command is replaced by a 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 has not received any new enhancements.

16.2.4 LIBRARY REQUEST,composite_library,LVOL,volser,CLDINFO

This command outputs the LVOL status on a cloud, that is, object data. It indicates whether the LVOL is premigrated to the cloud and from which clusters in the grid the data is accessible.

Starting with R5.1, LVOL versioning in the cloud is supported. If all the clusters in the domain are R5.1 level or later, the response lines include the volume version information, as shown in Example 16-3.

Example 16-3 LI REQ LVOL command result sample with the CLDINFO parameter

```
LOGICAL VOLUME CLOUD INFORMATION V2.0
 LOGICAL VOLUME:               Z99999
----------------------------------------------------------------------
  LIBRARY ST RK     POOL/ ACCOUNT/CL   CNT    SIZE(MiB)
 Lipizzan  M  1 MYPOOL01/MYACCT01/2     12        61250
              2 MYPOOL02/MYACCT02/2     40       700000
              3 MYPOOL03/MYACCT01/2     99      1000000
              4 MYPOOL04/MYACCT02/2     10      1800000
 Arabian  - NO DATA IS PREMIGRATED TO CLOUD
      Oak  M  1 MYPOOL01/MYACCT01/0     12        61250
 Palomino  - NO DATA IS PREMIGRATED TO CLOUD
```

16.2.5 LIBRARY REQUEST,distributed_library,LVOL,volser,CLDVERS,page_index

Starting with R5.1, LVOL versioning in the cloud is supported. The **`LIBRARY REQUEST,distributed_library,LVOL,volser,CLDVERS,page_index`** command shows the list of volume versions that are retained in the cloud. The list is separated into pages that are made up of seven records per page. Only one page can be displayed at a time, and the page index can be specified by a third keyword. The response lines are formatted as shown in Example 16-4.

Example 16-4 LI REQ LVOL command result sample with the CLDVERS parameter

```
LOGICAL VOLUME CLOUD VERSION INFORMATION V1.0
 LOGICAL VOLUME: ZCLD00 STATUS: NORMAL
----------------------------------------------------------------------
  0: myverylong40charactersgprefixname0123456/7683/BA030/BA87A/3957T/
     Z00000/10700000000000000000/10200000000000000000/20191007212440
  IV,DL,SZ: 0000000000000000278,0000000000000000150,1208
  PL,ACT  : MYPOOL,MYACCT
  D,P-TIME: 2020-05-14 01:59:21, 2020-05-14 01:57:08
----------------------------------------------------------------------
```

```
  1:    lipizzan/41c6/BA092/BA92C/CF55V/ZCLD00/278/147/20200509004039
  IV,DL,SZ: 0000000000000000278,0000000000000000147,1208
  PL,ACT  : MYPOOL,MYACCT
  D,P-TIME: 2020-05-09 01:01:10, 2020-05-09 00:43:08
----------------------------------------------------------------------
  2:    lipizzan/41be/BA092/BA92A/35B30/ZCLD00/278/145/20200509003102
  IV,DL,SZ: 0000000000000000278,0000000000000000145,1208
  PL,ACT  : MYPOOL,MYACCT
  D,P-TIME: 2020-05-09 00:34:48, 2020-05-09 00:31:03
----------------------------------------------------------------------
  3:    lipizzan/43fb/BA092/BA92A/35B30/ZCLD00/278/144/20200509001658
  IV,DL,SZ: 0000000000000000278,0000000000000000144,1208
  PL,ACT  : MYPOOL,MYACCT
  D,P-TIME: 2020-05-09 00:30:57, 2020-05-09 00:16:59
----------------------------------------------------------------------
  4:    lipizzan/41c6/BA092/BA92A/35B30/ZCLD00/278/143/20200509001331
  IV,DL,SZ: 0000000000000000278,0000000000000000143,1208
  PL,ACT  : MYPOOL,MYACCT
  D,P-TIME: 2020-05-09 00:16:40, 2020-05-09 00:13:32
----------------------------------------------------------------------
  5:    lipizzan/41c6/BA092/BA92C/CF55V/ZCLD00/278/142/20200508054359
  IV,DL,SZ: 0000000000000000278,0000000000000000142,820358
  PL,ACT  : MYPOOL,MYACCT
  D,P-TIME: 2020-05-09 00:13:28, 2020-05-08 05:44:01
----------------------------------------------------------------------
  6:    lipizzan/0f30/BA092/BA92C/CF55V/ZCLD00/278/139/20200507090256
  IV,DL,SZ: 0000000000000000278,0000000000000000139,1208
  PL,ACT  : MYPOOL,MYACCT
  D,P-TIME: 2020-05-07 09:38:13, 2020-05-07 09:02:57
----------------------------------------------------------------------
 8 MORE VERSIONS EXIST...
```

16.2.6 LIBRARY REQUEST,*distributed_library*,CLDSET(,keyword,*value*)

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 (DR) 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 running 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 TS7700C. The high- or low-priority mode of cloud premigration is described in the **CLDPRIOR** section.
  - Issued by running 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 GB) 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 running 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 Feature Code (FC) 5274 (1 TB Active Premigration Queue) x 10 plus FC 5279 (5 TB Active Premigration Queue) FCs are installed, the total size of the active premigration queue is 15 TB. Then, up to 15 * 1000 = 15000 GB 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 LVOL 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 LVOL recall task is available.

    Issued by running 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 running 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.
  - 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 running 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 Management Interface (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 one event is 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 running 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 one event is 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 LVOL from the cloud.
  - Issued by running 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 running 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`.
- **PFRCCPGO**: Ghost Copy Enablement during PG0 Replication:
  - Enables or disables the ghost copy when the local cluster is trying to replicate volumes to be assigned as PG0 from a remote cluster.
  - Issued by running the following command:

    `LIBRARY REQUEST,distributed_library,CLDSET,PFRCCPGO,ENABLE/DISABLE`

  - When it is set to `DISABLED`, normal grid copy instead of ghost copy is performed unless another trigger condition is met.
  - The default is `ENABLED`.
- **PFRCCTDL**: Ghost Copy Enablement during Time Delayed Replication:
  - Enables or disables the ghost copy when the local cluster is trying time-delayed replication of a volume from a remote cluster.
  - Issued by running the following command:

    `LIBRARY REQUEST,distributed_library,CLDSET,PFRCCTDL,ENABLE/DISABLE`

  - When it is set to `DISABLED`, normal grid copy instead of ghost copy is performed unless another trigger condition is met.
  - The default is `ENABLED`.
- **PFRCCTRY**: Number of Copy Attempts before Ghost Copy:
  - Sets the maximum number of normal grid copy retries to be run before applying a ghost copy.
  - Issued by running the following command:

    ```
    LIBRARY REQUEST,distributed_library,CLDSET,PFRCCTRY,value
    ```

  - When a specified number of normal grid copies of a LVOL fail in a row, then a ghost copy is applied.
  - When the value is set to `0`, the local cluster does not try ghost copy and continues to run a normal grid copy.
  - The default value is `0`.
- **USEHIGH**: High Warning Level of Amount of Data Stored in the Cloud:
  - Set the high warning level for the amount of data in terabytes that is stored in a cloud to which the cloud nickname points.
  - Issued by running the following command:

    ```
    LIBRARY REQUEST,distributed_library,CLDSET,USEHIGH,cloud_nickname,value
    ```

  - When the cloud usage exceeds the **USEHIGH** value for more than 5 minutes, an event message, `The amount of data stored in the cloud pool crossed USEHIGH value`, is created. The message repeats every 15 minutes.
  - When the cloud usage falls below **USEHIGH**, another event message, `The amount of data stored in the cloud pool is below USEHIGH value`, is created.
  - When the value is set to `0`, no event message is surfaced.
  - The default value is `0`.
- **USELOW**: Low Warning Level of Amount of Data Stored in the Cloud:
  - Set the low warning level for the amount of data in terabytes that is stored in a cloud to which the cloud nickname points.
  - Issued by running the following command:

    ```
    LIBRARY REQUEST,distributed_library,CLDSET,USELOW,cloud_nickname,value
    ```

  - When the cloud usage exceeds the **USELOW** value for more than 5 minutes, an event message, `The amount of data stored in the cloud pool crossed USELOW value`, is created.
  - When the cloud usage falls below **USELOW**, another event message, `The amount of data stored in the cloud pool is below USELOW value`, is created.
  - When the value is set to `0`, no event message is surfaced.
  - The default value is `0`.
- **USESHOW**: Show Low and High Warning Levels of Amount of Data Stored in the Cloud:
  - Shows the list of **USEHIGH** and **USELOW** settings for all the cloud pools.
  - Issued by running the following command:

    ```
    LIBRARY REQUEST,distributed_library,CLDSET,USESHOW,page_index
    ```

– The list is separated into pages that are made up of 141 records that use three columns each. Only one page can be displayed at a time, and the page index can be specified by a third keyword.

The response lines of a **USESHOW** request are formatted as shown in Example 16-5.

Example 16-5 CLDSET,USESHOW response format

```
CLDSET USESHOW V1.0
POOLNAME  UHIGH   ULOW  POOLNAME  UHIGH   ULOW  POOLNAME  UHIGH   ULOW
----------------------  ----------------------  ----------------------
 MYPOOL0      0      0   MYPOOL1      0      0   MYPOOL2    200     10
 MYPOOL3      0      0   MYPOOL4    200     10   MYPOOL5    200     10
-    0 more cloud pool usage settings exist
```

- **CLDSET** Default Response

  The response lines to a **CLDSET** request are formatted as shown in Example 16-6 when a valid setting is provided. Entering the **CLDSET** keyword without any other keywords provides this response as well.

Example 16-6 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
```

16.2.7 LIBRARY REQUEST,distributed_library,CLDBKUP,SHOW,page_index

Starting with R5.1, a cloud pool database backup function is supported. The **LIBRARY REQUEST,distributed_library,CLDBKUP,SHOW,page_index** command shows the list of cloud pool database backups that were created on the cloud. The list is separated into pages that are made up of 49 records per page. Only one page can be displayed at a time, and the page index can be specified by a third keyword. Example 16-7 shows a sample output of this command.

Example 16-7 LI REQ CLDBKUP SHOW command result sample

```
CLDBKUP SHOW V1.0
 POOLNAME BACKUPID BACKUPNAME                           DESCRIPTION
 MYPOOL01 10000001 S1234.C25B1.B25B1.20200121123456.001 DESCRIPT001
 MYPOOL01 10000002 S1234.C25B1.B25B1.20200121123457.002 DESCRIPT002
 MYPOOL01 10000003 S1234.C25B1.B25B1.20200121123458.003 DESCRIPT003
 [...]
 MYPOOL01 10000048 S1234.C25B1.B25B1.20200121123458.048 DESCRIPT048
 MYPOOL01 10000049 S1234.C25B1.B25B1.20200121123458.049 DESCRIPT049
 128 MORE BACKUPS EXIST...
```

16.2.8 LI REQ STATUS command with GRLNKACT parameter

The **`LI REQ STATUS GRLNKACT`** command response was enhanced to include information about the grid link activity of Grid to Grid Migration (GGM) and DS8000 Transparent Cloud Tiering (TCT). In response to this request, the grid provides point-in-time (PiT) 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 then 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 IBM WebSphere® message communication) and RFA (grid cluster-cluster data (file) transfer). Starting with R5.1, the total established TCP connections that are used for GGM and DS8000 TCT are shown.

  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).

  – The `MQ` column shows the total sum of the connections that are used for IBM MQ.

  – The `RFA` column shows the total sum of the connections that are used for RFA.

  – The `CLD` column shows the total sum of the connections that are used for cloud. Before the R5.1 code level, this sum might also include the sums for GGM activity with another copy source/target grid (if it is configured and used). For R5.1 and later, the sum for GGM is reported in the GGM column (see Example 16-8 on page 162).

  – The `GGM` column shows the total sum of the connections that are used for GGM.

  – The `OBJ` column shows the total sum of the connections that are used for DS8000 TCT.

- `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 the Grid Interface buffer. The counts are summed for IBM MQ, RFA, cloud, GGM, and DS8000 TCT usage. This view can also report each Grid Interface in a format that is like the view of the 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 that is related for IBM MQ. If the value is non-0, it must indicate that network activity exists for IBM MQ activity.

  – `GFA_REC/GFA_SND` shows the same counts that are related to GFA.

  – `CLD_REC/CLD_SND` shows the same counts that are related for cloud. Before the R5.1 code level, this figure also can include the information for GGM activity as it is shown in the GRID LINK ESTABLISHED SOCKET CONNECTIONS. For R5.1 and later, the counts for GGM are separated to `GGM_REC/GGM_SND` columns, as shown in Example 16-8 on page 162.

  - GGM_REC/GGM_SND shows the same counts that are related for GGM.
  - OBJ_REC/OBJ_SND shows the same counts that are related to DS8000 TCT.
- 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:

  - The Cx columns refer to the cluster ID.
  - The GRD_TOT column shows the total throughput of the remote clusters (Cx) in the grid.
  - The CLD column shows the throughput against the cloud if CLD is configured and used.
  - The GGM column shows the throughput of the GGM copy with the remote grid.
  - The OBJ column shows the throughput of DS8000 TCT.
  - The TOT column shows the sum of GRD_TOT, CLD, GGM, and OBJ.

  Before the R5.1 code level, GGM activity can be added to CLD or TOT, as shown in “GRID LINK ESTABLISHED SOCKET CONNECTIONS” on page 161. For R5.1 and later, the GGM activity is reported in the GGM column.
- 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 nonzero, the corresponding VOLSERs are provided after the ACTIVE EXPORT VOLUME COUNT.
  - ACTIVE IMPORT VOLUME COUNT provides the total number of the active import (recall) volumes. If it is nonzero, the corresponding VOLSERs are provided after the ACTIVE IMPORT VOLUME COUNT.

Example 16-8 shows the cloud-related grid link activity in the CLD column in the output from the **GRLNKACT** parameter.

Example 16-8 GRLNKACT parameter shows the cloud-related grid link activity in the CLD column

```
GRLNKACT STATUS V1.0
CLUSTER INDEX:  1 LINK COUNT:  4 Time: Thu Nov  5 07:39:24 CUT 2020
GRID LINK ESTABLISHED SOCKET CONNECTIONS------------------------------
LN INTF IP               C0  C1  C2  C3  C4  C5  C6  C7  MQ  RFA  CLD
L0 en0  10.30.1.21       108 0   0   0   0   0   0   0   108 0    0
L1 en8  10.31.1.21       0   0   0   0   0   0   0   0   0   0    0
L2 en1  10.32.1.21       0   0   0   0   0   0   0   0   0   0    0
L3 en9  10.33.1.21       0   0   0   0   0   0   0   0   0   0    0
LN INTF IP               GGM  OBJ
L0 en0  10.30.1.21       0    0
L1 en8  10.31.1.21       0    0
L2 en1  10.32.1.21       0    1
L3 en9  10.33.1.21       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  0     0     0        444      0        0        0        0
L1  0     0     0        0        0        0        0        0
```

```
L2  0     11    0        0        0        0        0        0
L3  0     0     0        0        0        0        0        0
TOT 1     11    -        -        -        -        -        -
LN  GGM_REC  GGM_SND  OBJ_REC  OBJ_SND
L0  0        0        0        0
L1  0        0        0        0
L2  0        0        11661    0
L3  0        0        0        0
GRID LINK THROUGHPUT ESTIMATES-MBps-----------------------------------
DIR C0   C2   C3   C4   C5   C6   C7   GRD_TOT CLD  GGM  OBJ  TOT
Tx  0    0    0    0    0    0    0    0       0    0    0    0
Rx  0    0    0    0    0    0    0    0       0    0    11   11
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
```

16.2.9 Cloud-related operator messages

Cloud-related operator messages are listed in Table 16-1. You can monitor them on the z/OS host as they are surfaced through the `CBR3750I` message.

Table 16-1 Cloud-related operator messages

ID	Description
OP0830	TCT daemon died.
OP0831	TCT 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 TCT node is down.
OP0840	SSL handshake exception for a cloud provider: {0}. cloud account ({1}), container ({2}), url ({3}).

ID	Description
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 (SC) {0} is set to off load to cloud storage, but the Storage Group (SG) {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.
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 TCT.
OP0869	Resource address file not found for TCT.
OP0870	Database corrupted for TCT.

ID	Description
OP0871	LKM down for TCT.
OP0872	Access forbidden for a cloud account: cloud account ({0}).
OP0873	Access denied for a cloud account: ({0}).
OP0874	File system corrupted for TCT.
OP0875	Directory error for TCT.
OP0876	Key manager error for TCT.
OP0877	Container pair root directory not found for TCT.
OP0878	Container exists: {0}. cloud account ({1}), container ({2}), url ({3}).
OP0879	RKM down for TCT: {0}. cloud account ({1}), container ({2}), url ({3}).
OP0880	RKM down for TCT: {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	TCT container {0} inaccessible by url {1} for unexpected reason: {2}, failure detail: {3}.
MDE8186	The TCT daemon died.
MDEB080	The TCT configuration during online processing failed. A call home is started if this setting is enabled.

17

Cloud Storage Tier export, recovery, and testing

The new IBM TS7700 Cloud Export suite of features include Cloud Export, Cloud Export Recovery, and Cloud Export Recovery Testing, which you can use to back up a snapshot of your tape data into the cloud and recover it from the cloud to an empty stand-alone TS7700 cluster. In addition, you can perform a recovery test that does not update any production data, but simulates a Cloud Recovery in an encapsulated test environment.

There are several scenarios where Cloud Export is a good choice to back up relevant data that must be recovered after such events as a cyberattack or internal fraud.

One extra key function that is introduced with the new suite is *Logical Volume (LVOL) Version Retention and Restore* in/from the cloud.

This chapter provides an introduction to the Cloud Export suite, including how it works and giving you with an overview of the use cases where the IBM TS7700 Cloud Export features are the appropriate solution.

> **Note:** For more information, see the *IBM TS7700 Cloud Storage Tier Export, Recovery, and Testing Guide*.

This chapter includes the following topics:

17.1 Introducing the IBM TS7700 Cloud Export suite of features

The IBM TS7700 Cloud Export features can take a point-in-time (PiT) backup of your data that is stored in the cloud by taking a snapshot of your TS7700C database and storing it in the cloud. This task is done by using the Cloud Export function. One or more cloud pools can be targeted for the export/backup operation.

The PiT backup can be used later to restore damaged or lost data or build a new TS7700C database. The restore is performed to an empty and stand-alone TS7700C. If you created several backups, you can choose which one that you want to recover by using the Cloud Export Recovery function.

With Cloud Export Recovery Testing, you can perform a recovery in a test-only mode in parallel with your daily production operation without affecting it. A temporary test pool in the cloud is created to perform the write and update operations while the read operations are performed to the production cloud pool.

Another new feature of the suite is the Logical Volume Version Retention in the cloud function. This feature tracks changes that are made to the objects that are written into the cloud depending on the retention period that is specified for the cloud pool. The feature determines when a Cloud Export backup should be deleted.

In addition to the IBM TS7700 Release 5.1 functions, new Library Requests Commands are implemented to manage the Cloud Export backups and the versions of the LVOLs in the cloud.

The IBM TS7700 Cloud Export suite provides a function that is similar to the Copy Export to physical tape function, but the suite targets an object store in the cloud without needing to consider any special physical tape handling.

Figure 17-1 shows an overview of the IBM TS7700 Cloud Export suite components. We review the export, restore, and volume retention version in the Cloud Functions in detail in this chapter.

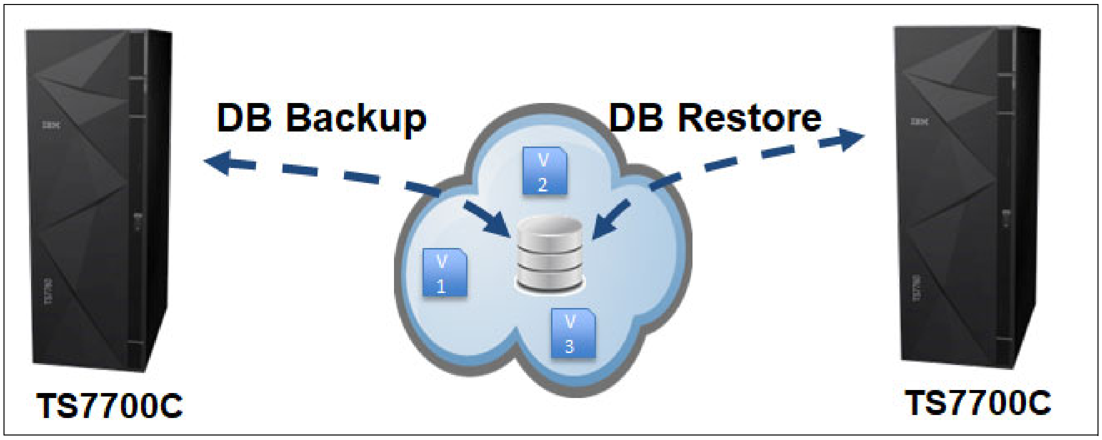


Figure 17-1 IBM TS7700 Cloud Export suite overview

17.1.1 Use cases

This section describes use cases where Cloud Export should be considered.

Disaster recovery

You can use an offsite cloud as an alternative to using the “tape on a truck” method for disaster recovery (DR). If your DR policy includes Copy Export backups on physical tape that are shipped to a DR site, you can now choose to use the Cloud Export instead. This new method reduces complexity and avoids any native tape transport to the DR site. Copy Export improves the underlining recovery time objective (RTO) and recovery point objective (RPO) by reducing the overall backup creation and recovery time.

If needed, you can consider extra cloud targets for a Cloud Export backup, for example, to a third site with a greater distance to your primary or secondary site. This use case might improve recovery time compared to a Copy Export to native tape approach.

The Cloud Export Recovery Testing feature makes it easy to perform regular DR tests to prove that the established policy meets the requirements that are related to data availability and business continuity.

Safeguarded copy and air gap

You can perform periodically Cloud Export backups to the cloud. By using these created PiT snapshots, you can recover to a specific consistent point, like IBM DS8000 Safeguarded Copy.

Depending on the cloud pool version retention policies that you define, the PiT snapshot can be retained for days, weeks, months, or longer. If there is an accidental or malicious action, you can restore the PiT snapshot of your environment that represents your TS7700C before the event. Then, this environment can be used to restore and recover those volumes that were corrupted or lost.

You can choose different cloud targets either on-premises or off-premises. An off-premises target provides more protection for your business data.

Legal holds

You might have internal or external regulatory needs to freeze one or more workloads in time. This task can be accomplished by freezing return-to-scratch processing or making copies of such protected data.

By using the Cloud Export feature in combination with the established Cloud Pool version retention policies, you can achieve the same outcome in an easy to manage way.

Test environment

You can create a pseudo-production environment to test major changes in a production-like environment. The Cloud Export Recovery feature in test mode combined with a primary disk PiT snapshot that was created with, for example, IBM Safeguarded Copy or IBM FlashCopy® can easily create this test environment.

Workload transfer

There are various reasons that you might need to transfer a workload from one grid to another one. One major reason is transferring a workload between independent clients. Interconnecting these clients through replication techniques might be insecure. Therefore, a safer approach like the Cloud Export feature is needed.

You can use Cloud Export to put a copy of the workload into a shared cloud. After the workload in inside the cloud, you can give the receiving party access to the cloud and use Cloud Export Recovery to restore the workload in a stand-alone TS7700C. The workload can be merged into an existing grid or used as a tape copy source to migrate the new workload into the target client grid.

17.1.2 Configuration requirements

You can run the IBM TS7700 Cloud Export suite on any TS7760 VEC or TS7770 VED if the following items are true:

- All the concerned clusters are running TS7700 microcode level R8.51.xx or higher.
- The cluster must be a TS7700C cluster with Feature Code (FC) 5278 Cloud Storage Tier enabled.

For more information about how to implement your cloud target, see Chapter 7, “Setting up an IBM Cloud Object Storage object store” on page 37 and Chapter 8, “Setting up Amazon Web Services cloud object storage” on page 55.

The configuration of the TS7700C and the cloud pools is described in Chapter 9, “Configuring IBM TS7700 for Cloud Storage Tier” on page 73. With TS7700 R8.51.xx, you can define up to 256 different cloud pools targeting different cloud providers.

For your IBM Z host, there are no specific requirements that relate to the new suite.

17.2 Logical Volume Version Retention in the cloud

IBM TS7700 Release 5.1 introduced a function that you can use to retain older versions of LVOLs in a cloud storage vault. This function is implemented by setting a retention days value that is greater than 0 on a cloud pool. You can modify the retention value whenever needed and this change is retroactive, so the value is valid for all objects in that cloud storage vault from the PiT when you performed the update.

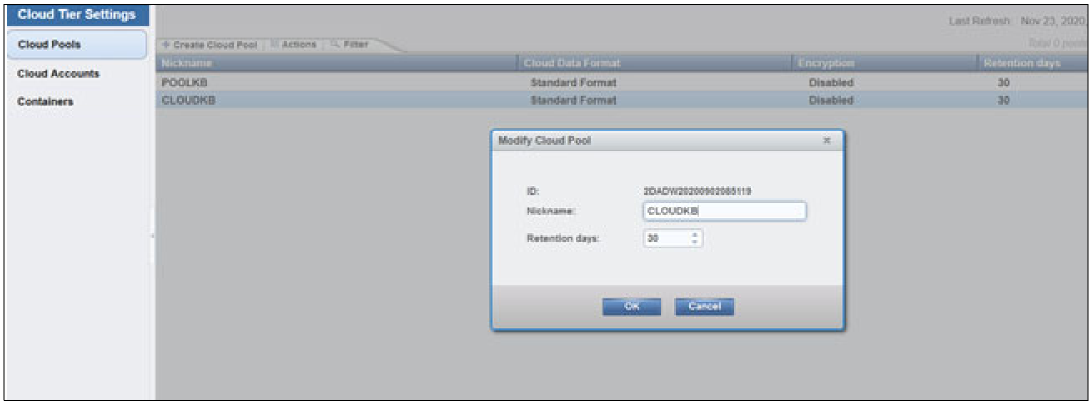
When an LVOL auto-expires, ejects, or is reused or modified, the version in the cloud before the event can be retained. The TS7700C continues to retain one or more prior versions of the LVOL in the cloud for the number of days that is specified in the cloud pool retention setting. Therefore, any one of these prior versions may be used as a restore point without worrying about normal or unexpected changes to data. This function is a critical step in maintaining a PiT recovery by using a cloud vault because the vault is constantly updated with new versions. Only by using prior version retention can you restore your data to a consistent PiT from one that corresponds to the Cloud Export backup that you want to restore.

The TS7700C tracks all previous versions of an LVOL that exist within the configured cloud pool volume version retention period. Previous versions outside of the configured retention period are automatically deleted within the storage vault.

Setting retention days

The value is set by using the IBM TS7700 Management Interface (MI) by selecting **Cloud Tier Settings** → **Cloud Pools**. In the Cloud Pools window, you find all defined cloud pools, and you can define more cloud pools. One of the options for the cloud pool is **Retention days**. You can set this option to 0 - 999999, where 0 means no version tracking. The value 999999 is the maximum value.

Figure 17-2 shows an example of the **Retention days** field in the IBM TS7700 MI.



Nickname	Cloud Data Format	Encryption	Retention days
POOLKB	Standard Format	Disabled	30
CLOUDKB	Standard Format	Disabled	30

Modify Cloud Pool

ID: 2DADW20200902085119

Nickname: CLOUDKB

Retention days: 30

Figure 17-2 Setting the Retention days field in the TS7700 MI

To check the available versions of a specific LVOL you issue the following `LIBRARY REQUEST` command:

```
LI REQ,<distributed library name>,LVOL,<VOLSER>,CLDVERS
```

The result lists all available versions of the specified LVOL, including the active version. The LVOL that is indicated in index `0` is always the current, active data, and `1` - *n* are previous versions of the LVOL.

Example 17-1 shows two outputs of the request (see the bold text) for the same VOLSER:

- The first time the request was issued, only the active LVOL was present. This information is shown in index `0` and version `101` with the timestamp `20201208134700`. The record is the only one that is present, and no older version of the LVOL existed when the command was run.
- The second request after the LVOL was modified shows index `0` and version `102`, which is the updated LVOL with the timestamp `20201209112422`. Index `1` in that case now has the timestamp before the update happened and still shows version `101`. In addition, you see the cloud pool `CLOUDKB`, which the LVOL belongs to, and the cloud provider name `ICOSKB`.

Example 17-1 Available LVOL versions

```
LI REQ,D0001,LVOL,A01102,CLDVERS
CBR1020I Processing LIBRARY command: REQ,D0001,LVOL,A01102,CLDVERS.
CBR1280I Library D0001 request. 195
Keywords: LVOL,A01102,CLDVERS
----------------------------------------------------------------------
LOGICAL VOLUME CLOUD VERSION INFORMATION V1.0
 LOGICAL VOLUME: A01102 STATUS: NORMAL
----------------------------------------------------------------------
  0: SGG5/41c6/00186/D0001/2DADW/A01102/10518/101/20201208134700
  IV,DL,SZ: 0000000000000010518,0000000000000000101,755103497
  PL,ACT  : CLOUDKB,ICOSKB
  D,P-TIME: 1970-01-01 00:00:00, 2020-12-08 13:49:22
----------------------------------------------------------------------

LI REQ,D0001,LVOL,A01102,CLDVERS
CBR1020I Processing LIBRARY command: REQ,D0001,LVOL,A01102,CLDVERS.
CBR1280I Library D0001 request. 240
Keywords: LVOL,A01102,CLDVERS
----------------------------------------------------------------------
LOGICAL VOLUME CLOUD VERSION INFORMATION V1.0
 LOGICAL VOLUME: A01102 STATUS: NORMAL
----------------------------------------------------------------------
  0: SGG5/634c/00186/D0001/2DADW/A01102/10518/102/20201209112422
  IV,DL,SZ: 0000000000000010518,0000000000000000102,830594524
  PL,ACT  : CLOUDKB,ICOSKB
  D,P-TIME: 1970-01-01 00:00:00, 2020-12-09 11:24:40
----------------------------------------------------------------------
  1: SGG5/41c6/00186/D0001/2DADW/A01102/10518/101/20201208134700
  IV,DL,SZ: 0000000000000010518,0000000000000000101,755103497
  PL,ACT  : CLOUDKB,ICOSKB
  D,P-TIME: 2020-12-09 11:19:16, 2020-12-08 13:49:22
```

17.3 Logical Volume Version Restore from the cloud

IBM TS7700 Release R5.1 PGA1 introduced the Logical Volume Version Restore function. With this function, users can restore older volume versions that were retained in the cloud and can access the contents of those versions.

Contrary to Cloud Export Recovery, Volume Version Restore does not require any special export operation to the cloud beforehand. Multiple volume versions that were premigrated to the cloud are retained for the duration of the preconfigured retention period.

Users can choose any retained version of a logical volume as a restore source, even if a newer version of the volume was corrupted or maliciously or accidentally modified, or if an older version of the volume was maliciously or accidentally deleted.

Overview of Volume Version Restore

Volume Version Restore is performed by remapping the version to be restored (restore source version) as the latest data of another scratch volume that a user specified as restore destination (restore destination volume). After the restore process completes, users can access the restored version data by mounting the restore destination volume.

During the Volume Version Restore procedure, no data movement occurs. The procedure completes by modifying the TS7700 database only. The data that is retained in the cloud also is not touched, so the data attributes of the restore source version, such as Logical WORM and compression states, is taken to the restore destination volume.

Other volume attributes are retained from the restore destination volume. Depending on the partition or copy mode that is assigned to the destination scratch volume, recall or grid copy is performed to follow the new volume attribute (if necessary) after the restore completed.

This feature benefits users by eliminating the following operational costs that are required for any data movement:

- Time to move volume version data from the cloud storage to TS7700
- Associated expense to read the version data out of the cloud storage
- Physical resources, such as memory, CPU, and disk utilization

Automatic Header/Trailer Update on Recall

Logical volumes that were created in the TS7700 by IBM Z contain header and trailer information that was put there by the TS7700 and IBM Z. Some of these headers and trailers reference the volume serial or VOLSER. During a volume version restore procedure, the database about restore destination volume points to the instance of restore source version in the cloud that still contains the previous volume's VOLSER information within its volume header and trailers.

If the volume is recalled into a TS7700C disk cache, the TS7700C automatically updates these internal headers and trailers during the recall procedure. By deferring the header and trailer updates, the volumes that are being restored only must be accessed if a recall is requested and the source version remains immutable in the object store.

Deferring header and trailer updates also allows many volumes to be restored quickly because no cloud access is required until the volume is accessed for host or copy activity. If the new volume is modified, the new modified version is a candidate to premigrate to the cloud and the previous instance is then retained again if the cloud pool has a retention policy configured.

Figure 17-3 shows an overview of Volume Version Restore and Automatic Header/Trailer Update on Recall.

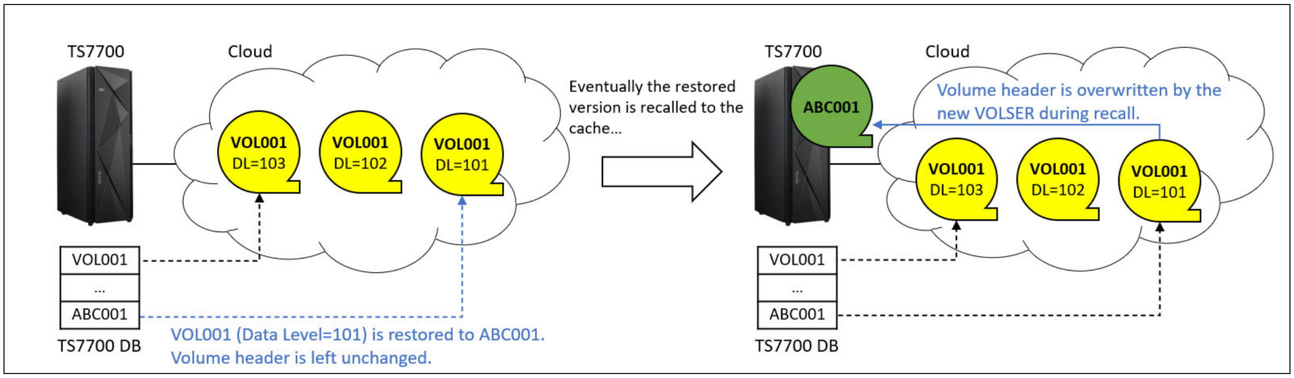

TS7700
Cloud
VOL001 DL=103
VOL001 DL=102
VOL001 DL=101
VOL001
...
ABC001
TS7700 DB
VOL001 (Data Level=101) is restored to ABC001.
Volume header is left unchanged.
Eventually the restored version is recalled to the cache...
TS7700
Cloud
ABC001
Volume header is overwritten by the new VOLSER during recall.
VOL001 DL=103
VOL001 DL=102
VOL001 DL=101
VOL001
...
ABC001
TS7700 DB

Figure 17-3 Volume Version Restore Procedure and Automatic Header/Trailer Update on Recall

17.4 Performing a Cloud Export

Cloud Export works like Copy Export, but instead of writing the tape data to physical tape, it writes to the defined cloud target. One more difference is that Cloud Export does not create a new copy of the tape data but only a snapshot, which it sends to the TS7700C database of the cluster to which you perform Cloud Export. Therefore, the LVOL that the backup references must be present in the cloud when the snapshot is created, which means the premigration process must be completed.

When you run Cloud Export, the TS7700C waits for all clusters in the entire grid that have volumes queued for premigration (targeting the relevant pools) to finish the premigrations before fulfilling the request. After all premigrations of the relevant pools are complete, the database PiT backup is completed and stored in the cloud.

17.4.1 Creating an export volume

The Cloud Export operation starts when the **LIBRARY EXPORT** command is issued, same as for Copy Export to tape. The Export Volume contains the information that is needed and created while running Cloud Export. For this purpose, a volume is created that contains the following information:

- The EXPORT LIST file contains instructions that creates a list of candidate volumes to include in the PiT backup of the cloud pool or pools that are specified in the **EXPPOOLS** parameter. The instructions also define **DBPOOLS**, where the database snapshot should be stored, which might be the same cloud pools that are specified in **EXPPOOLS** or to one or more other cloud pools outside the **EXPPOOLS**. EXPORT LIST version 04 is required for Cloud Export commands.
- The RESERVED file contains only a header that identifies it as the reserve file. This file is required to run the command.
- The EXPORT STATUS file returns information about the export operation. The TS7700C uses it to return details about the database backup that was taken and a list of all LVOLs that were exported to the defined cloud target. The database backup information can be variable length with a minimum of 200-characters per line if only one cloud pool is specified and a maximum of 7594-characters per line if 256 cloud pools are specified. EXPORT STATUS version 01 is required for Cloud Export results.

You must create the LVOL and ensure that it contains these files before initiating the **LIBRARY EXPORT** command. If any of these three files are missing, the command fails. Records that written in these files must be in a readable format, so they should not be compressed or encrypted. To prevent compression, specify TRTCH=NOCOMP in the job control language (JCL) code that creates this LVOL, and check the compression setting of the corresponding Data Class (DC). The encryption parameter is set in the TS7700 MI for the cloud pool. The parameter is disabled by default.

Note: There must be enough space on the LVOL that you choose for the **LIBRARY EXPORT** command to hold all the details about the LVOLs that are exported to the cloud. If there is not enough space on the volume, the TS7700 stops writing to the EXPORT STATUS file when it hits LEOT, and it adds a closing warning message that indicates the export was successful but the status file data was truncated due to the LEOT. This message also is sent in an operator message (Event Code OP0919) to the host, and an event is posted on the TS7700 MI. Using 25 GB logical tapes can help prevent running out of space.

EXPORT LIST creation parameters

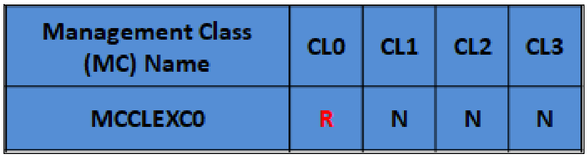
More and updated parameters are required to create the `EXPORT LIST` for the Cloud Export and the Copy Export:

- **`EXPORT LIST 04`**: Set to `04` if you perform a Copy Export. Set to `03` if you use IBM TS7700 microcode before R5.1.
- **`OPTYPE (CLOUD|TAPE)`**: Defines the export option to be performed, which is **`CLOUD`** for Cloud Export and **`TAPE`** for Copy Export.
- **`EXPORT PARAMETERS PHYSICAL POOL TO EXPORT 09`**: Only needed for Copy Export to tape. If you specify **`OPTYPE CLOUD`**, this parameter is ignored. Usually, you specify which tape pool should be backed up.
- **`OPTIONS1,COPY,LMTDBPVL`**: Needed for Copy Export to tape. It is ignored if **`OPTYPE CLOUD`** is specified.
- **`EXPPOOLS cloudpool1 cloudpool2... cloudpool256`**: This parameter defines the cloud pool or pools on which you want to perform a Cloud Export. You can specify one or more cloud pools. Specifying * includes all available cloud pools.
- **`DBPOOLS *|cloudpool...cloudpooln`**: This parameter defines the cloud pool or pools where the database snapshot will be stored. The pool or pools might be in the same cloud vaults to which the Cloud Export is performed or different cloud vaults. If a * is specified or if the field is left blank, the same cloud pools that are listed under **`EXPPOOLS`** are used.
- **`DESC mynote`**: You can specify a description that is related to the specific Cloud Export you create to distinguish it from other ones. The maximum size for this field is 12 characters.

Defining the constructs for Export Volume

The LVOL (described in 17.4.1, “Creating an export volume” on page 174) that is used for Cloud Export should not be stored in the same cloud pools that you are going to back up. To manage this task, you must define the following constructs in your IBM Z host and on the TS7700C cluster where the scratch volume is being requested:

- Specify a Storage Group (SG) that points to a cloud pool that is different from the ones that you are going to back up.
- Implement a Management Class (MC) to ensure that the LVOL is written in to only the TS7700C cluster to which you send the scratch volume request. Figure 17-4 shows an example about how the MC would look like if you assume a 4-way-grid where you want to target cluster 0 (CL0). So, CL1 - CL3 will have a **`NOCOPY`** policy where CL0 is set to `DEFERRED` or `RUN`.



Management Class (MC) Name	CL0	CL1	CL2	CL3
MCCLEXC0	R	N	N	N

Figure 17-4 Export Volume MC definition

- Define a DC that has not enabled compression.
- Your ACS Routines and your JCL should point out the specific SG, MC, and DC that you created to handle the Export Volume.

Creating the Export Volume

Now, you are ready to run the JCL that creates the EXPORT LIST, RESERVED, and EXPORT STATUS files.

Example 17-2 shows (see bolded text) what an Export Volume creation JOB looks like. It consists of three steps:

- STEP1 allocates the LVOL and writes EXPORT LIST.
- STEP2 creates the RESERVED file, which contains the header as described and accepted from the **LIBRARY EXPORT** command.
- STEP3 creates the EXPORT STATUS file.

The example prepares the list of volumes for the cloud pools MYCLOUD1 and MYCLOUD2. The corresponding TS7700 database snapshot for MYCLOUD1 and MYCLOUD2 will be stored in both pools due to the usage of the wildcard for **DBPOOLS**.

Example 17-2 JCL for Export Volume creation

```
//CPYEXCL JOB (DE0A047,DEASTO),RMM,MSGCLASS=H,CLASS=A,NOTIFY=&SYSUID,
//             REGION=0M
/*JOBPARM S=ANY
//********************************************************************************
//* CREATE COPY EXPORT TO THE CLOUD EXPORT LIST VOLUME
//* REMARKS: DO NOT USE COMPACTION & CONSIDER ENOUGH SIZE FOR LVOL
//********************************************************************************
//********************************************************************************
//* FILE 1: EXPORT LIST
//********************************************************************************
//STEP1 EXEC PGM=IEBGENER
//SYSPRINT DD SYSOUT=*
//SYSIN DD DUMMY
//SYSUT2 DD DSN=MYEXP.CLEXP.EXPLIST.D201126,
// UNIT=3390,DISP=(NEW,KEEP),LABEL=(1,SL),
// VOL=(,RETAIN),
// DCB=(RECFM=FB,BLKSIZE=80,LRECL=80,TRTCH=NOCOMP)
//SYSUT1 DD *
EXPORT LIST 04
OPTYPE CLOUD
EXPORT PARAMETERS PHYSICAL POOL TO EXPORT:09
OPTIONS1,COPY,EJECT,LMTDBPVL
EXPPOOLS MYCLOUD1 MYCLOUD2
DBPOOLS *
DESC DEMOCLOUDEXP
/*
//****************************************
//* FILE 2: RESERVED FILE
//****************************************
//STEP2 EXEC PGM=IEBGENER,COND=(4,LT)
//SYSPRINT DD SYSOUT=*
//SYSIN DD DUMMY
//SYSUT2 DD DSN=MYEXP.CLEXP.RESERVED.D201126,
// UNIT=3390,DISP=(NEW,KEEP),LABEL=(2,SL),
// VOL=(,RETAIN,REF=*.STEP1.SYSUT2),
// DCB=*.STEP1.SYSUT2
//SYSUT1 DD *
RESERVED FILE
/*
//****************************************
//* FILE 3: EXPORT STATUS FILE
//****************************************
```

```
//STEP3 EXEC PGM=IEBGENER,COND=(4,LT)
//SYSPRINT DD SYSOUT=*
//SYSIN DD DUMMY
//SYSUT2 DD DSN=MYEXP.CLEXP.EXPSTATS.D201125,
// UNIT=3390,DISP=(NEW,CATLG),LABEL=(3,SL),
// VOL=(,,REF=*.STEP1.SYSUT2),
// DCB=*.STEP1.SYSUT2
//SYSUT1 DD *
EXPORT STATUS 01
/*
```

After a successful job completion, a new VOLSER will be written that now contains the three export files. This VOLSER is used when you run the **LIBRARY EXPORT** command.
Example 17-3 shows the job output extract where you can find the VOLSER, which in this case is `VOLS=A03448`, that is created by the job (see bolded text).

Example 17-3 Job output extract to find the VOLSER

```
$HASP373 CPYEXCL  STARTED - INIT 1    - CLASS A        - SYS PE2
IEF403I CPYEXCL - STARTED - TIME=10.25.25
IEF233A M 2500,PRIVAT,SL,CPYEXCL,STEP1,MYEXP.CLEXP.EXPLIST.D201125
IEC705I TAPE ON 2500,A03448,SL,COMP,CPYEXCL,STEP1, MYEXP.CLEXP.EXPLIST.D201125,
IEC205I SYSUT2,CPYEXCL,STEP1,FILESEQ=1, COMPLETE VOLUME LIST,  535
DSN= MYEXP.CLEXP.EXPLIST.D201125,VOLS=A03448,TOTALBLOCKS=7
```

Running Cloud Export

After you create the Export Volume, you can run the **LIBRARY EXPORT** command, and the TS7700 performs the following steps:

1. Verifies the `EXPORT LIST` format and content, and obtains the starting time.
2. Monitors the premigration queue on all TS7700C clusters in the grid for all defined cloud pools to be exported as of the determined starting time.
3. After all the volumes are premigrated, initiates a database backup.
4. Generates the list of volumes that are premigrated to the cloud for the Cloud Export pools that are specified and writes it to the `EXPORT STATUS` file.
5. Generates the database backup information and writes it to the `EXPORT STATUS` file.
6. Exports the database backup to all cloud vaults that are specified in **DBPOOLS** and a list of all valid backups to all cloud vaults.

To start the run, start SDSF from your TSO session on your IBM Z host, as shown in Example 17-4, and run the Cloud Export command (see bolded text):

```
LIBRARY EXPORT <volser>
```

The <volser> entry is the Export Volume that you created.

Example 17-4 Running the LIBRARY EXPORT command

```
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
   Display  Filter  View  Print  Options  Search  Help
 -------------------------------------------------------------------------
 SDSF DA PE2      MZPEVS2  PAG  0  CPU/L     1/  0      LINE 1-7 (7)
 COMMAND INPUT ===> /LIBRARY EXPORT A03448                   SCROLL ===> CSR
 NP   JOBNAME  StepName ProcStep JobID    Owner    C Pos DP Real Paging    SIO
      CONSOLE  CONSOLE                               NS  FF 5287   0.00   0.00
```

During the run of the Cloud Export, status messages are sent to the IBM Z host system log to indicate which steps are running. Example 17-5 shows how each step is documented, and provides a clear and comprehensive understanding of the status of the operation. Two types of information that you can gather are the cloud container ID and the number of LVOLs and corresponding megabytes for which the PiT backup was performed (marked in italic in the example).

> **Note:** For more information, see the *IBM TS7700 Cloud Storage Tier Export, Recovery, and Testing Guide.*

Example 17-5 Library Export command execution messages

```
LIBRARY EXPORT A03448
CBR1000I OAM EXPORT command execution scheduled.
CBR3750I Message from library D0001: E0000 EXPORT OPERATION STARTED 164
FOR EXPORT LIST VOLUME A03448. Severity impact: INFORMATION.
CBR3750I Message from library D0001: E1030 COPYING LOGICAL EXPORT
VOLUMES FROM CACHE TO CLOUD. Severity impact: INFORMATION.
CBR3750I Message from library D0001: E1031 COPYING TO CLOUD CLOUDKB 166
(ID:2DADW20200902085119), CL/CNT/LASTVOL, 0/0/-, 1/0/-, 2/0/-, 3/0/-,
4/0/-, 5/0/-, 6/0/-, 7/0/-. Severity impact: INFORMATION.
CBR3750I Message from library D0001: E1039 COPIED LOGICAL EXPORT VOLUMES
 FROM CACHE TO CLOUD. Severity impact: INFORMATION.
CBR3750I Message from library D0001: E1040 CREATING CLOUD VOLUME MAP
REPORT FILE. Severity impact: INFORMATION.
CBR3750I Message from library D0001: E1049 CREATED CLOUD VOLUME MAP
REPORT FILE. Severity impact: INFORMATION.
CBR3750I Message from library D0001: E1100 CLOUD EXPORT PROCESSING
STARTED. Severity impact: INFORMATION.
CBR3750I Message from library D0001: E1110 DB BACKUP PROCESSING STARTED.
 Severity impact: INFORMATION.
CBR3750I Message from library D0001: E1119 DB BACKUP PROCESSING
COMPLETED. Severity impact: INFORMATION.
CBR3750I Message from library D0001: E1120 EXPORTING DB BACKUP TO CLOUD
POOLS. Severity impact: INFORMATION.
CBR3750I Message from library D0001: E1129 EXPORTED DB BACKUP TO CLOUD
POOLS. Severity impact: INFORMATION.
CBR3750I Message from library D0001: E1199 CLOUD EXPORT PROCESSING
COMPLETED. Severity impact: INFORMATION.
CBR3750I Message from library D0001: E1070 WRITING DB BACKUP INFO TO
STATUS FILE. Severity impact: INFORMATION.
CBR3750I Message from library D0001: E1079 WROTE DB BACKUP INFO TO
STATUS FILE. Severity impact: INFORMATION.
CBR3750I Message from library D0001: E1060 WRITING CLOUD VOLUME MAP TO
STATUS FILE. Severity impact: INFORMATION.
CBR3750I Message from library D0001: E1069 WROTE CLOUD VOLUME MAP TO
STATUS FILE. Severity impact: INFORMATION.
CBR3750I Message from library D0001: E0005 ALL EXPORT PROCESSING 180
COMPLETED FOR EXPORT LIST VOLUME A03448. Severity impact: INFORMATION.
CBR3855I Export operation for logical list volume A03448 in library 181
HYDRAG completed successfully.  Requested:  0  Exportable:  0
Exported:  351  Stacked volumes:  0  MBytes Exported:  251051  MBytes
Moved:  0
```

You can query your available backups by running the **LIBRARY REQUEST** command as shown in the following example:

```
LI REQ,<distributed library name>,CLDBKUP,SHOW,<page index>
```

Example 17-6 shows how the output of the command looks (see bolded text). The output shows one available PiT database snapshot (`BACKUPNAME`) that is stored twice: One with `BACKUP ID = 1` on cloud pool `POOLKB`, and the second one with `BACKUP ID = 2` on cloud pool `CLOUDKB`.

Example 17-6 Available Cloud Export backups in the cloud

```
LI REQ,D0001,CLDBKUP,SHOW
CBR1020I Processing LIBRARY command: REQ,D0001,CLDBKUP,SHOW.
CBR1280I Library D0001 request. 198
Keywords: CLDBKUP,SHOW
-------------------------------------------------------------------
CLDBKUP SHOW V1.0
 POOLNAME BACKUPID BACKUPNAME                           DESCRIPTION
 POOLKB          1 2DADW.00186.D0001.20201209104511.001 DEMOCLEXP
 CLOUDKB         2 2DADW.00186.D0001.20201209104511.001 DEMOCLEXP
```

More backup considerations outside the TS7700

When designing a backup solution and scope to maintain business continuity, you must consider what data should be included in this backup to resume business operations and maintain data integrity. To do so, complete the following steps:

1. Define which data must be part of the backup in addition to the tape data. If we look into the tape environment, the following data should be considered:
   - The Tape Management System (TMS) control data set.
   - The IBM Data Facility Storage Management Subsystem (DFSMS) and IBM DFSMShsm data.
   - The Tape Configuration Database (TCDB).
2. Define what data must be part of the PiT backup in addition to the tape data, which is in the scope of the Cloud Export. This backup can be performed in any of the following ways:
   - As one more component of Cloud Export.
   - Using one of the other available TS7700 functions like Copy Export.
   - Outside the TS7700. For example, an IBM DS8000 Safeguarded Copy volume-based backup or an IBM DS8000 Transparent Cloud Tiering (TCT) Full Volume Dump.

17.5 Performing Cloud Export Recovery

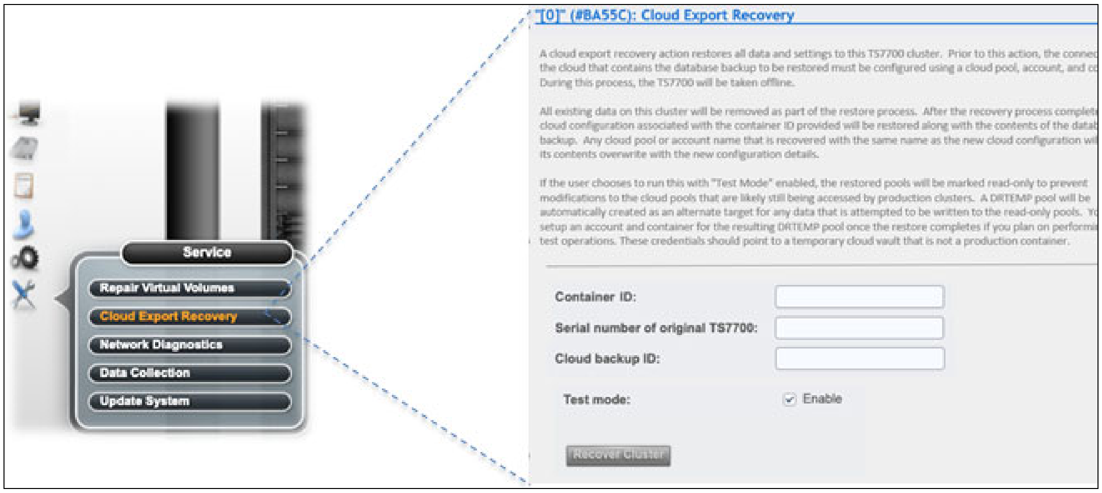
The Cloud Export Recovery can be performed only on an empty stand-alone TS7700C cluster, which must be defined as cluster 0 (CL0) and configured as cloud-attached by using the same definitions as the source TS7700C. The same cloud pools and cloud credentials must be defined to connect to the same cloud targets as the source cluster. This situation is also true for a security configuration that uses internal security or LDAP. In addition, the microcode levels on the target cluster must be the same or later as on the source cluster.

To perform the recovery, the following source cluster information must be available because it is required during the recovery to identify which backup needs to be recovered:

- Cloud Export `BACKUP_ID`: This ID was returned in the `EXPORT STATUS` file in the Export Volume after the Cloud Export was performed. In addition, it can be obtained if the **`LIBRARY REQUEST`** command **`LI REQ,<distributed library name>,CLDBKUP,SHOW,<index page>`** is issued or the Bulk Volume Information Retrieval (BVIR) report `CLOUD BACKUP` list is retrieved.
- Serial number (S/N) of the source cluster that created the Cloud Export backup.
- Cloud Container ID: The container ID of the target vault where the database snapshot was stored. It can be found in the Container pane of TS7700 MI under the Cloud Tier Settings window.

Cloud Export Recovery is started by selecting the Service icon in the TS7700 MI, and then clicking **Cloud Export Recovery**, as shown in Figure 17-5 on page 180. This option is visible in the **Service** menu only if the TS7700C is a stand-alone system and the user was given permission to access that page.

> **Note:** If the cluster is not empty when you issue the recovery, you are asked to confirm the deletion of the cluster data, which is the first step to be performed before the recovery itself is run.



"[0]" (#BA55C): Cloud Export Recovery

A cloud export recovery action restores all data and settings to this TS7700 cluster. Prior to this action, the connec the cloud that contains the database backup to be restored must be configured using a cloud pool, account, and co During this process, the TS7700 will be taken offline.

All existing data on this cluster will be removed as part of the restore process. After the recovery process complete cloud configuration associated with the container ID provided will be restored along with the contents of the datab backup. Any cloud pool or account name that is recovered with the same name as the new cloud configuration wil its contents overwrite with the new configuration details.

If the user chooses to run this with "Test Mode" enabled, the restored pools will be marked read-only to prevent modifications to the cloud pools that are likely still being accessed by production clusters. A DRTEMP pool will be automatically created as an alternate target for any data that is attempted to be written to the read-only pools. Yo setup an account and container for the resulting DRTEMP pool once the restore completes if you plan on performi test operations. These credentials should point to a temporary cloud vault that is not a production container.

Container ID:

Serial number of original TS7700:

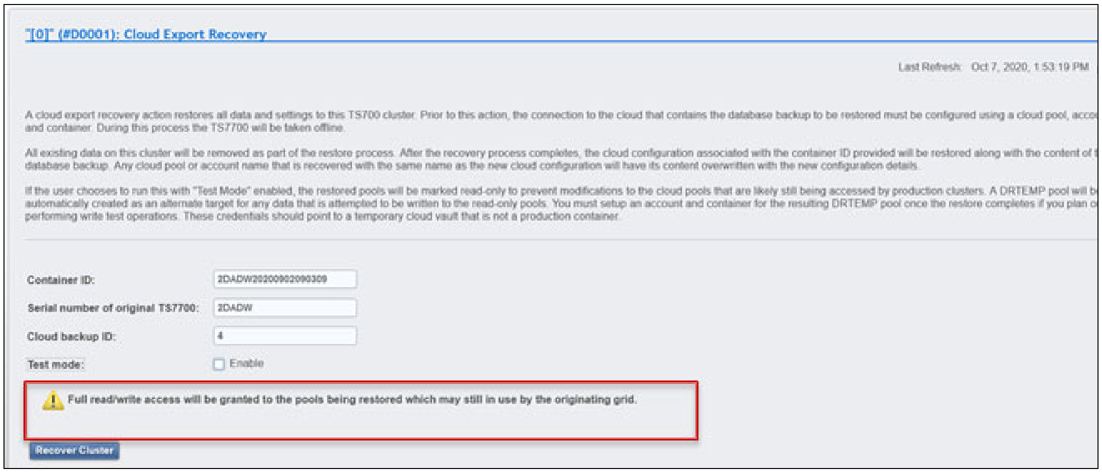
Cloud backup ID:

Test mode: ☑ Enable

Recover Cluster

Figure 17-5 TS7700 MI Cloud Export Recovery

Within the window, complete the **Container ID, Serial number of the original/source TS7700**, and the **Cloud backup ID** fields. If this situation is a real DR, clear the **Enable** checkbox for **Test mode** (selected by default), as shown in Figure 17-6. When you press **Recover Cluster**, the recovery starts, and status messages appear and inform you about which steps are being performed.



"[0]" (#D0001): Cloud Export Recovery

Last Refresh: Oct 7, 2020, 1:53:19 PM

A cloud export recovery action restores all data and settings to this TS700 cluster. Prior to this action, the connection to the cloud that contains the database backup to be restored must be configured using a cloud pool, acco and container. During this process the TS7700 will be taken offline.

All existing data on this cluster will be removed as part of the restore process. After the recovery process completes, the cloud configuration associated with the container ID provided will be restored along with the content of t database backup. Any cloud pool or account name that is recovered with the same name as the new cloud configuration will have its content overwritten with the new configuration details.

If the user chooses to run this with "Test Mode" enabled, the restored pools will be marked read-only to prevent modifications to the cloud pools that are likely still being accessed by production clusters. A DRTEMP pool will b automatically created as an alternate target for any data that is attempted to be written to the read-only pools. You must setup an account and container for the resulting DRTEMP pool once the restore completes if you plan o performing write test operations. These credentials should point to a temporary cloud vault that is not a production container.

Container ID: 2DADW20200902090309

Serial number of original TS7700: 2DADW

Cloud backup ID: 4

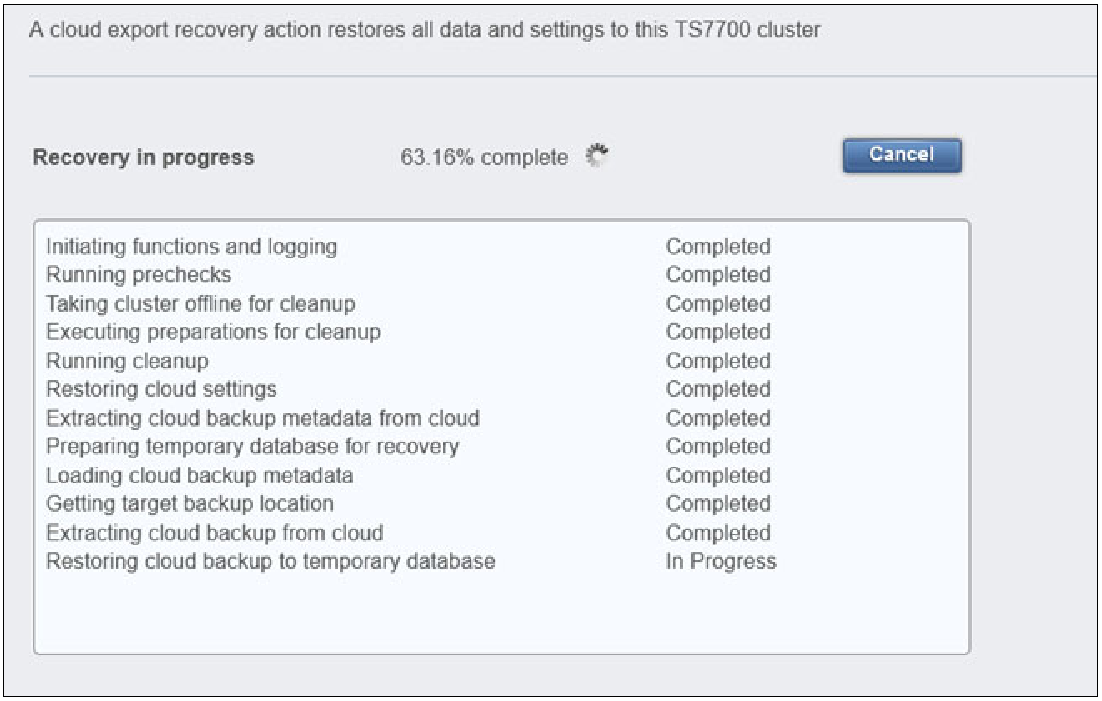
Test mode: □ Enable

⚠ Full read/write access will be granted to the pools being restored which may still in use by the originating grid.

Figure 17-6 Entering the required recovery information

> **Note:** During the recovery, the TS7700C cluster must be taken offline to clean up and replace the database. During offline processing, the MI restarts, which cause a temporary loss in connectivity, so any users that are logged in to the MI are logged off and must log in again.

After the cluster is back up, the TS7700 MI reconnects and you can continue to monitor the process. Figure 17-7 shows the messages that are displayed during the recovery.



A cloud export recovery action restores all data and settings to this TS7700 cluster

Recovery in progress 63.16% complete

```
Initiating functions and logging               Completed
Running prechecks                              Completed
Taking cluster offline for cleanup             Completed
Executing preparations for cleanup             Completed
Running cleanup                                Completed
Restoring cloud settings                       Completed
Extracting cloud backup metadata from cloud    Completed
Preparing temporary database for recovery      Completed
Loading cloud backup metadata                  Completed
Getting target backup location                 Completed
Extracting cloud backup from cloud             Completed
Restoring cloud backup to temporary database   In Progress
```

Figure 17-7 Recovery status messages

If Cloud Export Recovery failed, the status window indicates in which step the process failed. The TS7700 completes the following actions after a failed restore:

- Fully cleans up any database work that started.
- Restores the cloud credentials that are associated with the Container ID that were entered by the user at the start.
- Sends out an operator message to the attached IBM Z host.
- Brings the cluster back online.

After a successful completion, the “Recovery in progress complete” status shows 100%. If it fails, it states which steps failed. The status message window remains open until you choose to close it by clicking **Close Status**.

Now, you should review the cluster settings to verify that everything is defined as required for this new stand-alone cluster, including the TS7700 storage management constructs, the cloud target definition, the security settings including the Dual Control, the cache partition, and the pool definition.

More considerations outside the TS7700 Cloud Export Recovery

As described in 17.5, “Performing Cloud Export Recovery” on page 180, consider the data outside the TS7700. After the TS7700 recovers and full access is available, perform the following actions as needed:

- Recover the TMS catalog that matches the TS7700 PiT backup.
- Recover the TCDB that was taken in the same PiT.

- Review your IBM Z host HCD definitions and update them if needed by using the `COMPOSITE LIBRARY ID` of the recovered TS7700C.
- Recover or update the DFSMS and DFSMShsm environment. In this case, you must update the Library Definition in DFSMS by using the `COMPOSITE` and `DISTRIBUTED LIBRARY ID` of the recovered TS7700C.

17.6 Cloud Export Recovery Test Mode

Performing Cloud Export Recovery in Test Mode requires the same configuration steps that are used for Cloud Export Recovery, but this time you enable the **`TEST MODE`**. Leave the **Enable** option selected in the TS7700 MI recovery dialog, as shown in Figure 17-5 on page 180. The recovery in TEST MODE is also performed on an empty stand-alone TS770C cluster.

When the recovery is done, you can start working with the TS7700C cluster without affecting your production cloud pools. When running the recovery in TEST MODE, a temporary cloud pool that is named DRTEMP is created automatically for this purpose, which must be configured by using a cloud target that is different from the production cloud target. This task is done by going to the TS7700 MI and opening the Cloud Tier Settings window, where the cloud account and the target container for the DRTEMP pool are defined. If needed, you can define and configure more temporary cloud pools that are not in the same vault or cloud target as your production cloud environment.

All the recovered cloud pools are set to read-only on the test cluster, and every operation targeting those read-only pools are redirected to the DRTEMP cloud pool instead.

By following these steps, you can easily perform a DR test without modifying your live production environment. When the DR test is complete, you can clean up the DR environment, including the DRTEMP pool.

The read, update, and write workflow is shown in Figure 17-8.

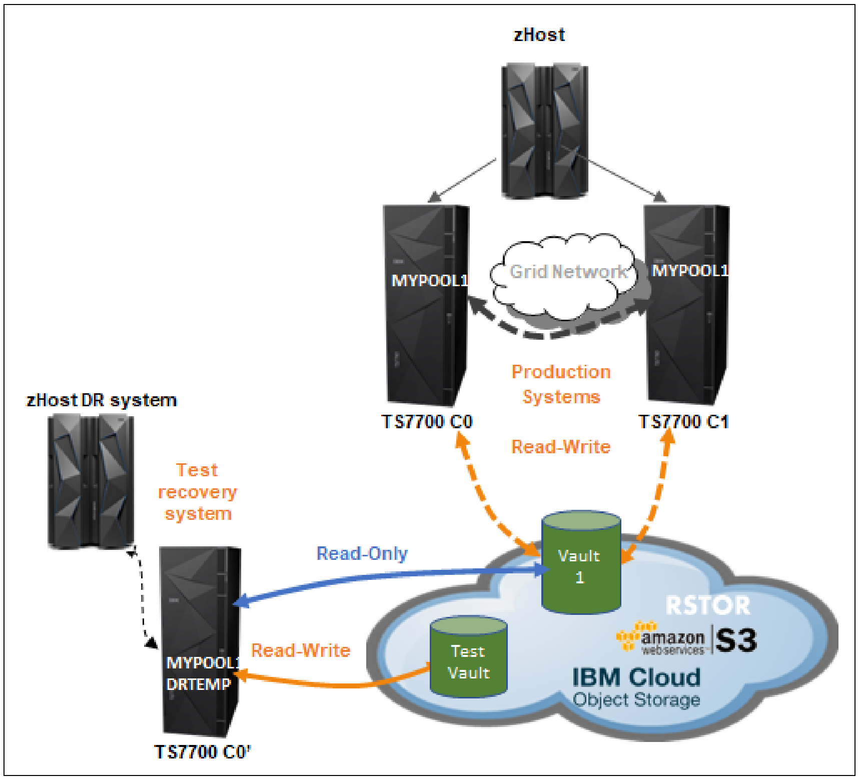


Figure 17-8   Cloud Export Recovery Test Mode workflow

In this workflow example, Vault1 is the production cloud pool, and during Cloud Export Recovery in Test Mode, this object store is fully accessible to the production TS7700C clusters C0 and C1 for read and write operations. At the same time, Vault1 is in read-only mode for the test recovery TS7700C cluster C0’, and all writes and updates are sent to the temporary cloud pool Test Vault that is configured for the DRTEMP cloud pool. The TS7700C cluster C0’ is connected to an IBM Z DR host system, so the whole test is done within an encapsulated environment. Only Vault1 is accessible from both the production and the test environment. Testing is performed without any impact to the ongoing production workflow. When the test is complete, the DRTEMP pool Test Vault can be deleted, and the test cluster C0’ is disconnected from the cloud target.

17.7 TS7700 Cloud Export suite of feature-related updates

This chapter describes the Library Request Commands and TS7700 BVIR reports that were introduced with IBM TS7700 Release 5.1 PGA1 or later for the management and monitoring of the Cloud Export suite of features.

17.7.1 Library Request Commands update summary

IBM TS7700 Release 5.1 PGA1 introduced Library Request commands that are used for Logical Volume Version Restore from the cloud.

Note: For more information, see the IBM TS7700 Cloud Storage Tier Export, Recovery, and Testing Guide.

17.7.2 TS7700 Bulk Volume Information Retrieval updates

IBM TS7700 Release 5.2 introduced the following BVIR report:

`CLOUD CONTENT <cloud pool nickname> (<number>)`: Reports the list of objects in the specified cloud pool. The list contains up to 4 million objects. To get the list of the remaining objects, specify a number as the 4th keyword to tell TS7700 the list page index to show

Note: For more information, see TS7700 Bulk Volume Information Retrieval Version R5.22.

17.8 Putting together all of the functions

Figure 17-9 puts together all the functions of the TS7700 Cloud Export suite.

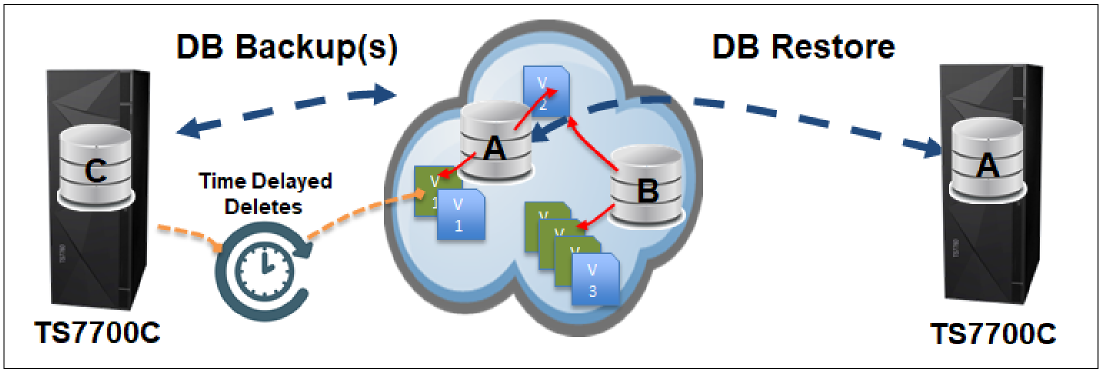


Figure 17-9 TS7700 Cloud Export functions

Periodically, you can create Cloud Export PiT backups to the cloud and set the retention period for those backups as required as `0` - `999999`. If the retention period is set to a value greater than `0`, the TS7700C retains the previous versions of the LVOLs that are assigned to this cloud pool for the number of days that are specified. You can choose to recover one of the created backups into an empty stand-alone cluster either in test mode or to rebuild a production environment (due to a failure) to maintain business continuity.

With the newly defined **`LIBRARY REQUEST`** commands, you can manage the cloud backups and LVOL versions. In addition, new TS7700 BVIR reports were introduced to collect all the required information behind the TS7700 Cloud Export suite.

Related publications

The publications that are listed in this section are considered suitable for a more detailed description of the topics that are covered in this paper.

IBM Redbooks

The following IBM Redbooks publications provide more information about the topic in this document. Note that some publications referenced in this list might be available in softcopy only:

- *IBM DS8000 and Transparent Cloud Tiering (DS8000 Release 9.2)*, SG24-8381
- *IBM TS7700 Release 5.2.2 Guide*, SG24-8464
- *IBM TS7700 Series DS8000 Object Store User's Guide Version 2.0*, REDP-5583

You can search for, view, and download these documents and other Redbooks, Redpapers, web docs, drafts, and other materials, at the following website:

ibm.com/redbooks

Online resources

The following websites are also relevant as further information sources:

- IBM Documentation - IBM TS7700 5.2.2:

  https://www.ibm.com/docs/en/ts7700-virtual-tape/5.2.2

- *TS7700 Cloud Storage Tier Export Recovery and Testing Guide*:

  https://www.ibm.com/support/pages/node/6355825

- *TS7700 Library Request Command V5.1b*:

  https://www.ibm.com/support/pages/node/6355035

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

REDP-5573-02

ISBN 0738460664

Printed in U.S.A.