IBM Cloud Object Storage System
Version 3.14.5 July Maintenance Release

Release Notes

This edition applies to IBM Cloud Object Storage System™ and is valid until replaced by new editions.

Contents

Support information

For more information on the product or help with troubleshooting, contact IBM Support at IBMCloudStorageSupport@us.ibm.com or visit the Directory of worldwide contacts.

Chapter 1. New Features and Improvements in ClevOS 3.14.5

IBM Log Server Integration (1423)

This feature adds new capability that facilitates upload of dump logs to the IBM Log Server, which replaces the existing IBM Log Server. Through this added functionality, the UI interface for log configuration allows users to configure two log-server endpoints as noted below:

- IBM Log Server that requires IBM log server host name, transfer ID and password. Transfer ID and password can be set up using the customer support portal IBM Support
- Log Destination, a custom or other internal configuration, which can be an SFTP or HTTP server

This benefits users who can choose between the configured log-server endpoints to upload logs using the UI interface for Collect Logs Now. An option to the above is to enter the IBM log-server end-point data on the UI interface for Collect Logs Now, and upload logs to the IBM log server while doing so without configuring server endpoints.

Drive Dashboard and Bulk Resume (1184)

This feature introduces a new Manager UI focused on drive management, which supports monitoring and issuing bulk-resume actions. Benefits include the ability to:

- View all drives in the system, including their properties, such as drive state, firmware, model, and association to a storage pool or set
- Sort tables and filters to easily locate drives of interest
- Aggregate drive information for a given storage pool or set through new graphs
- Issue resume actions to several drives at once by users who have the following roles: super user, system administrator, or operator

Note: This feature is only compatible with devices 3.13.4 or higher.

Chapter 2. New Features and Improvements in ClevOS 3.14.4

IBM® Branded Cloud Object Storage (COS) Hardware Refresh (1275)

Cloud Object Storage System™ Gen2 hardware is both an extension and an enhancement of the present Cloud hardware. It is an extension as it provides the same functionality using the same Cloud Object Storage software and can co-exist with the existing generation. Clients can intermix past and present generations of hardware in the same storage pool and cluster, even at the set level.

The Cloud Object Storage architecture does not change in the Gen2 hardware as the storage system is provided by a Manager, Accesser®, and a Slicestor® function. The Manager and Accesser appliance are very much consistent with the present Manager and Accesser appliance.

A key difference in Gen2 will be in how the storage layer is architected. In the present generation, the storage layer is provided by storage servers, meaning that the performance components and the storage components in the storage layer are in the same physical box and therefore must be installed, grown, and expanded together. In Gen2, the storage layer will be divided into two separate components, a controller node that contains the performance components and a disk enclosure that contains the storage components.

In both the present generation and in Gen2, the storage layer is called the Slicestor function, and the functional components, component names, and system management remains exactly the same. This ensures that the same version of Cloud Object Storage software is used across both the present generation and Gen2.

The Manager appliance, the Accesser appliance, and the Controller Node appliance are all based on the exact same 1U server. The appliance configuration is determined based on the function performed by the server:

The Manager (Model M10) appliance supports the following configuration:
- 1 x Intel Xeon Silver 4110 CPU
- 96 GB RAM
- 2 x 960 GB OS/Boot drives – SSD
- 1 x Broadcom MegaRAID 9361-4i controller set in RAID 1 managing the OS/Boot Drives
- 2 x 10 GbE ports
- 2 x Redundant power supplies

The Accesser (Model A10) appliance supports the following configuration:
- 1 x Intel Xeon Gold 6126 CPU
- 192 GB RAM
- 2 x 480 GB OS/Boot drives – SSD – Managed by integrated motherboard control with SW RAID
- 2 x 10 GB Ethernet ports
- 2 x Redundant power supplies

The Controller Node (Model C10) appliance supports the following configuration:
- 1 x Intel Xeon Silver 4110 CPU
- 96 GB RAM • 2 x 480 GB OS/Boot drives – SSD – Managed by integrated motherboard control with SW RAID
- 1 x Broadcom 9305-16e in HBA Mode used to manage the HDDs in the disk enclosures

- 2 x 10 GB Ethernet ports
- 2 x Redundant power supplies

Table 1. Disc enclosures (models J10, J11 and J12

Size	Small	Medium	Large
JBOD total rack space	2U	4U	4U
Slicestor total rack space	3U	5U	5U
Capacity enclosures (rack space/disks)	2U/12	4U/53	4U/106
Drive sizes (TB)	4, 8, 12	4, 8, 12	4, 8, 12
Node raw capacity (min/max TB)	48/144	212/636	424/1270

When a Controller Node and a disk enclosure are combined, they function as and are referred to as a Slicestor appliance, just like the storage appliance is used today. Gen2 hardware brings about a set of improvements, capabilities, and consolidations to Cloud Object Storage, while doing so at a reduced hardware cost and with increased hardware performance.

Changed Interfaces:
- Manager Application User Interface
- Manager Daemon Device Application Programming Interface
- Manager Application REST Application Programming Interface
- Manager Application Report CSV/Email Output
- Syslog
- SNMP Traps
- Manager Application Call Home Email Bodies.

Email Bodies of "Call Home" Emails

The Call Home Email functionality has been updated. If an incident has a chassis ID parameter, the chassis serial associated with the chassis ID will be used as the "Vender Serial Number" in the body of the email. If a serial cannot be found, then the serial associated with the hardware profile will be used (matching existing behavior).

Open Incident Upgrade Behavior

Any open Fan/Voltage/PSU incidents will automatically close temporarily upon upgrade. The closing event will have text similar to: "Incident closed automatically due to change in software version <version>".

The Device API ("breaking" / non-backwards compatible change made)

The Device API has been updated. Both the state and statistic endpoints of the Device API have been altered.
- The "state" endpoint

  Fan, voltage, and PSU JSON maps are moved within an enclosing "chassis" map where the key is the associated chassis ID. The Device API Developer Guide has been updated to reflect these changes. This is a "breaking" / non-backwards compatible change.
- The "statistic" endpoint

  The output of the "extract chassis components" System Advanced Configuration setting (also known as "compatibility mode") for "fan", "voltage", and "psu" maps have been updated. Each key is now prepended with "<chassis-id>." As an example: assume "Fan 1" is in chassis with ID "main", the key

would now be "main.Fan 1". The Device API Developer Guide was not updated to reflect these changes given compatibility mode is not referenced in that document.

Fan Graphs on the Monitor Device Page

Fan stat data series names will now be of the form "<chassis id> <fan-name>". The Manager Administration Guide has been updated to reflect this change. Chassis serial is not included on these graphs.

Old Fan Data on the Monitor Device Page

Old fan statistical data will remain on graphs.

Device Health Summary widget on the Monitor Device Page

The monitor device health summary lists failed fans and PSUs by name. The output was updated to be prepended with the failed fan/PSU's chassis id. For example, "Fan 1" may be listed as "Main Fan 1" if the chassis id was "main". The first letter of the chassis id is purposely capitalized to be consistent with the fan graph series names. Chassis serial is not included in the updates to this monitor device health summary widget.

The Manager Event Console and SNMP Traps

Users of the event console (via the UI/API) and SNMP traps will see chassis ID added to "drive reset", "psu failed", "psu ok", "fan speed error", "fan speed ok", "voltage error", and "voltage ok" events.

The Failed FRU Report Columns

The chassis ID/chassis serial of fans/PSUs was added to the FRU report. This includes JSON/XML/CSV/Email/UI views. The JSON/XML views will display the value provided by platform (even null and empty strings). The other views will render null and empty strings as "N/A". Non-empty blank strings will be rendered as non-empty blanks strings in all views. Note that chassis ID/chassis serial is not provided by devices in mainline (pre merge of this feature) so null/"N/A" will be rendered until those devices are updated to the build with this feature.

The Failed FRU Report Performance

The FRU report now looks up the chassis serial for each FRU using chassis ID provided by the management daemon. This lookup has impacted the FRU report generation performance negatively. Users may notice longer load times for the FRU report when systems have large numbers of devices.

Chapter 3. New Features and Improvements in ClevOS 3.14.3

Container IP allow/disallow (948)
Container mode bucket quota and bucket configuration service API (1342)

These features extend the Service API with the capability of performing bucket-level operations and setting quota and IP whitelisting and blacklisting in Container Mode such that a user with Manager credential, and Service User role, would be able to configure a bucket on behalf of their clients for both on premise, and public cloud. See Container Mode Guide for more information.

The bucket IP whitelisting in container mode extends the bucket IP enforcement capability to proxy client connections for on-prem deployments in both standard vault mode and container mode.

Access Control Consistency (1395)

The system provides a consistent Bucket Read Access Control that specifically addresses standard vault and container level read permission behavior. Previously, containers and standard vaults within the same system had inconsistent Bucket Read Access Control behavior. In some cases, a Bucket Read Access Control grants "read and listing" and in other cases just "listing."

New systems default Bucket Read Access Control to "read and listing." This protects existing operators from unexpected changes. If an operator wants to use listing only, it is recommended that listing is enabled prior to any vaults being created on the system. Otherwise, some objects may become inaccessible when the change is made. The object owner needs to explicitly add object access controls to fix this issue.

During upgrades, the initial value for Bucket Read Access Control are decided based on the following rules:

1. If the system has only container vaults (not migrated from standard vaults) and management vaults, listing is used.
2. Otherwise, "read and listing" are used.

A new checkbox has been added to the Configure Container Mode UI page (Configure Container Mode API). If checked, bucket level requests (for example, PUT bucket, DELETE bucket, ...) received using the Cloud Object Storage API are rejected. Instead, the Service API must be used to send bucket level requests. This should be enabled when operators want to force clients to use operator portals to execute bucket level requests.

Immutable Object Storage in 2 site/mirrored COS systems (1393)

This release enhances the existing protected mirror functionality to improve system availability during an outage or network partition. Vaults in a protected mirror are no longer designated as primary/secondary, instead writes can complete to either vault in a mirror and are synced. The protected mirror functionality is available only after all the devices in the system are upgraded to 3.14.3. Please refer to our third-party assessment letter from Cohasset Associates that speaks to the two site deployment ability to meet the requirements of SEC 17a-4(f).

Documentation to reference:

- Feature Description Document for Retention Vaults and Protected Mirrors
- IBM COS API Reference Guide
- Manager REST API Guide

- Manager Administration Guide
- Vault Mirror Guide

Interface Changes:

- In the manager REST API, the create mirror/mirror template APIs no longer support the protection state parameter; Instead the mirror type parameter is required

Vault Deletion Authorization (1406)

This feature provides an added layer of security against inadvertent or malicious deletion of data. If enabled, the Vault Deletion Authorization feature prevents a single storage system administrator from being able to delete vaults through the Manager UI and Manager REST API. In order for a vault to be deleted, two users with the System Administrator role must approve the deletion of the vault. Vault Deletion Authorization is disabled by default, and can be enabled by users with the Security Officer role.

Custom HTTPS Certificate Chain for Storage Pools with Embedded Accesser Service enabled. (1427)

This feature allows users of the Embedded Accesser Service to configure a single HTTPS certificate chain for the HTTPS interface running across all of the Slicestor devices in a storage pool. The certificate can be shared across all the devices (rather than requiring a unique certificate for each device), greatly lowering cost and maintenance effort.

Drive Dashboard and Bulk Resume (1184)

This feature introduces a new Manager UI focused on drive management, which supports monitoring and issuing bulk-resume actions. Benefits include the ability to:

- View all drives in the system, including their properties, such as drive state, firmware, model, and association to a storage pool or set
- Sort tables and filters to easily locate drives of interest
- Aggregate drive information for a given storage pool or set through new graphs
- Issue resume actions to several drives at once by users who have the following roles: super user, system administrator, or operator

Note: This feature is only compatible with devices 3.13.4 or higher.

Chapter 4. New Features and Improvements in ClevOS 3.14.2

Device Role-based Access (1286)

This feature adds local and LDAP account authentication to the device console login within a system. Permissions can be assigned to accounts by the Security Officer on the Security tab in the Manager Web Interface for Manager devices, all other devices, specified sites, and regions. User commands through the device console such as device configuration changes and local files accessed are recorded in audit logs and are linked back to their local account or LDAP username. These audit logs are stored in the Management Vault for archival purposes.

Login permissions include

- root access
- read only
- read/write
- no access

Manager UI Global Header and Navigation Changes (1172)

This feature introduces several changes to improve UI scalability and ease of use.

- The navigation tree has been replaced with a more scalable navigation menu
- New summary pages have been provided for access pools and sites
- Search has moved to the header
- Added icon-based menus in the header for help, user profile, and log out

NVMe support for ClevOS devices (1297)

This feature adds support for NVME block devices. Examples include NVME SSD drives and can be used for the operating system or data drive(s). This makes certification as a Slicestor device possible for servers using NVME rather than HDD to store Slice data. It is possible to create a storage pool or change a given storage pool's state such that it contains a mix of NVMe and non-NVMe devices. This state is strongly discouraged but not blocked by the Manager application. With this release, the Dell 740xd NVME server is certified as a Slicestor device.

The troubleshooting console still allows for users to call **`cat /proc/scsi/scsi`** on NVMe devices; the response does not include information related to NVMe drives. There are no plans to enhance the troubleshooting console to include the ability to grab NVMe drive information.

The Drive Report CSV export had one of its column headings changed from "SCSI Name" to "Device Name".

The Storage Pool Capacity and Disk Report export had one of its column headings changed from "SCSI Name" to "Device Name".

Deprecation:

- The **`SCSIName`** event parameter is now a deprecated event parameter in favor of the new **`deviceName`** event parameter.
- The **`csTrapSCSIName`** is now a deprecated MIB OBJECT-TYPE in favor of the new **`csTrapDeviceName`** MIB OBJECT-TYPE.

Customer facing API endpoints that have changed:

`CLEVERSAFE-TRAP-MIB.txt`

- The **csTrapDeviceName** OBJECT-TYPE was added, deprecating the **csTrapSCSIName** OBJECT-TYPE.
- The **csTrapDeviceName** OBJECT-TYPE was appended to notifications that contain **csTrapSCSIName**.
- The descriptions of **csTrapDriveName** and **csTrapDriveID** where modified.

`/manager/api/{format}/1.0/eventConsole.adm`

- The event parameter **DeviceName** was added, deprecating **SCSIName**.
- Events that send the **SCSIName** parameter will now also send the **deviceName** parameter.

Drive Report:

- CSV Export – The column heading "SCSI Name" was changed to "Device Name."
- JSON/XML view – The key "deviceName" was added. Its value is duplicate to that of "scsiName."

Note: Do not confuse the word "Device" with respect to the "Device Name" column and the "Device Serial #" columns. The former refers to the drive name and the later refers to the drive's device's serial number.

Storage Pool Capacity and Disk Report:

- CSV Export — The column heading "SCSI Name" was changed to "Device Name."
- JSON/XML view – The key "deviceName" was added. Its value is duplicate to that of "scsi."

Support Infiniband Hardware in 3rd Party Servers (1313)

This feature supports the Mellanox ConnectX-5 family of InfiniBand single and dual port cards that utilize the IPoIB protocol. Note the ConnectX-5 family of cards has not been sufficiently tested in Ethernet mode. InfiniBand ports can also have their transition modes set while setting the mtu, which is demonstrated in the following examples:

- port <PORTNAME> mtu connected/65520
- port <PORTNAME> mtu datagram/2044

Chapter 5. New Features and Improvements in ClevOS 3.14.1

Immutable Object Storage (1269)

Object Retention is supported for both Vault and Container Modes. In Vault Mode, you can create retention vaults or protected mirrors with immutable object storage policies and objects that are stored in these retention vaults or protected mirrors have an immutable object storage policy.

For Container Mode, you can create container vaults to allow object retention. When Retention is enabled for a container vault, you can create containers with an immutable object storage policy. Objects that are stored in these protected containers also have an immutable object storage policy.

Objects that are contained within retention vaults or protected containers cannot be deleted or modified until the immutable object storage policy allows for the deletion or overwrite. There are various ways to protect vaults or containers using the IBM Cloud Object Storage System to meet the needs of customers that have strict retention requirements from regulatory entities (such as the Security and Exchange Commission), or customers that might have organizational retention requirements, including finite retention, indefinite retention, permanent retention, and legal holds.

Before you upgrade to the 3.14.1 release, and to find more information on this feature, refer to the documentation listed in the reference table.

New Functionality

- Support for Immutable Object Storage in Container Mode
- Support for Permanent Retention
- System Level Configuration of Retention settings:
  - System Minimum Duration
  - System Maximum Duration
  - System Default Retention duration
  - Allow Permanent Retention
- Allows either Content MD-5 ***or*** V4 content signing for Write Operations
  - Previous releases required Content MD-5 even if V4 content signature was included
- S3 API updates to support permanent retention
  - Added flag for protection operations at bucket level to denote state of permanent retention
  - Updates to error codes and error messages
  - New error codes and error messages
  - Support of -2 for Object Retention-Period
    - -2 denotes permanent retention of object
- Access Log Updates
  - Additional failure messages included
  - New parameter added for bucket protection information to denote state of permanent retention
- Container Vault
  - Flag added to Container Vault Configuration to enable protection support
    - A protection policy can be added to a container only if the associated container vault is enabled for protection.
    - Enabling Protection for a container vault does not mean that all containers within that container vault must have protection that is enabled.

- Listing of buckets in a container that uses the service API shows that the protection is enabled/disabled

References to documentation that supports this feature:

Name	Location
Feature Description Document (discusses all features that are related to immutable object storage)	https://www.ibm.com/support/knowledgecenter/STXNRM
Manager Administration Guide	https://www.ibm.com/support/knowledgecenter/STXNRM
REST API Guide	https://www.ibm.com/support/knowledgecenter/STXNRM
COS API	https://www.ibm.com/support/knowledgecenter/STXNRM

Query number of parts with an MPU object (1176)

This feature provides support for the "part-number" query string for HEAD and GET requests for objects, which were uploaded using Multipart Upload (MPU). It supports querying the number of parts that are associated with an object that have been uploaded using MPU. This enables clients to parallelize large object reads by fetching the component parts in parallel. Additionally, this allows objects written using MPU to be copied while preserving the part boundaries of the original object thus preserving the duplicating etag for this object.

1. The part number query parameter can be provided for GET or HEAD requests.
   a. For a non-MPU object, a request to read part number 1 should be interpreted as a ranged read request for the entire object.
   b. For an MPU object, a request to read a part number should be interpreted as a ranged read request for the byte range that is associated with the requested part.
2. Part numbers must be between 1 and 10,000 (inclusive). Any request outside of this range will result in an HTTP 400 error. If a request is made for a part number that is beyond the range of the object, the response will be an HTTP 416 - Requested Range not satisfiable.
3. All ranged read responses must include the Content-Range header consistent with a ranged read response.

Vault Scalability: Support for Slicestor Devices with Large Drive Counts (1219 B)

This feature now supports a maximum of 1500 vaults for systems containing Slicestor devices with large drive counts, for example, those with 60 drives and 96 GB of physical memory. In previous releases, systems with such devices were limited to 1000 vaults.

The actual number of vaults that a system can support will vary based on the following:

- Number of drives within deployed Slicestor devices
- Physical memory present in Slicestor devices
- Manager hardware configuration
- Total number of devices within the system

Additional changes can be required to the Manager and Slicestor device configuration to leverage this feature. Please contact Customer Support if greater than 1000 vault support is required.

Support 9-wide Concentrated Dispersal Mode Device set (1372)

This feature now supports concentrated dispersal mode for a 9-wide storage pool. Unlike concentrated dispersal mode for 3-6 wide device sets, a 9-wide device set will not operate in concentrated dispersal mode by default, since a 9-wide device set is supported as one side of a mirror in standard dispersal mode. Please contact IBM customer support to enable a 9-wide device set in concentrated dispersal mode.

Chapter 6. New Features and Improvements in ClevOS 3.14.0

Indefinite Retention and Event-based Retention capability support (1247)

This feature update is now supporting the following items:

1. The ability to extend retention of an object from the current time using a new header (extend-retention-from-current-time). Refer to COS API documentation.
2. Interpretation of bucket max:

   Previous Releases: The total retention period (initial retention period + all subsequent retention extensions) applied to an object cannot exceed the bucket maximum.

   Current Release: The retention period being applied to an object in any single request cannot result in the expiration date of that object exceeding the bucket maximum + current time (i.e. cannot extend object beyond bucket maximum from current time)
3. This feature also provides users with the ability to write an object into a bucket with a retention period of -1. This value is used as a placeholder for a user to provide a finite retention period at a later time, through a POST ?extendRetention request. While the retention period of the object is set to -1, the object cannot be deleted or modified. Retention Period of -1 can only be set on the object metadata and can only be configured via an object write operation.
4. The ability for an application to store an object in the IBM Cloud Object Storage System with an indefinite retention period and then allow the object retention to be changed to a finite value. Third party applications can implement Event-based Retention through the use of the indefinite retention API.

Note: See supporting documentation in the Retention Vaults and Protected Mirrors FDD and COS API Guide.

Chapter 7. Interface Modifications

API updates for the 3.14.5 release have been referenced in the following documentation:

- REST API Developer Guide
  - NEW section added under Device Management>Bulk drive resume action
    New request parameters: **deviceUuid** and **driveUuid**
    New response parameters: **deviceStatus**, **driveResults**, **driveUuid**and **driveStatus**

API updates for the 3.14.4 release have been referenced in the following documentation:

- REST API Developer Guide
  - Updated section on Reports>Failed field replaceable unit report>Response>JSON response example
    Added new parameters **chassisID** and **chassisSerial**for 1275 hardware feature
  - Updated section on Reports>Field replaceable unit report>Response>Parameters
    Added new parameters **chassisID** and **chassisSerial** for 1275 hardware feature

API updates for the 3.14.3 release have been referenced in the following documentation:

- REST API Developer Guide
  - NEW section added under Vault Management>Vault deletion authorization
  - Updated section on Vault Management>Delete a vault
    New request parameter: action
  - NEW section added under Access Pool Management>Edit storage pool HTTPS certificate chain
    New request parameters: **privateKeyPem** and **certificatePem**
  - Revised section heading under Administration>Edit the system TLS Configuration to say Edit the system Network Transport Layer Configuration
    Updated request parameter description for parm **clientToAccesserConnectionMode**
  - NEW section added under Access Pool Management>Edit storage pool HTTPS certificate chain
    New request parameters: **privateKeyPem** and **certificatePem**

API updates for the 3.14.2 release have been referenced in the following documentation:

- REST API Developer Guide

API updates for the 3.14.1 release have been referenced in the following documentation:

- CSO API Developer Guide
  - Error Codes
  - Add protection to a bucket
    MinimumRetention, DefaultRetention, MaximumRetention, EnablePermanentRetention
  - List the protection configuration for a bucket
    EnablePermanentRetention
  - Upload a protected object
    Retention-Period, Retention-Expiration-Date
  - Upload a protected object using HTML webforms
    Retention-Period, Retention-Expiration-Date
  - Get the headers of a protected object
    Retention-Expiration-Date
  - Download a protected object

Retention-Period, Retention-Expiration-Date

- Copy a protected object or copy an object to a protected bucket

  Retention-Period

- Extend the retention period of a protected object

  Additional-Retention-Period, New-Retention-Period, New-Retention-Expiration-Date, Extend-Retention-From-Current-Time

- List legal holds on a protected object

  RetentionExpirationDate

- Upload a part for a protected object
- Complete a multipart upload for protected objects

  Retention-Period, Retention-Expiration-Date (edited)

- REST API Developer Guide
  - Updated section on Mirror Management>Create a Mirror

    New Request parameters: permanentRetentionEnabled and defaultPermanentRetentionDurationEnabled

    Revised Request parameters: minimumRetentionPeriod, maximumRetentionPeriod and defaultRetentionPeriod
  - Updated section on Mirror Management>Create a Mirror Template

    New Request parameters: permanentRetentionEnabled and defaultPermanentRetentionDurationEnabled

    Revised Request parameters: minimumRetentionPeriod, maximumRetentionPeriod and defaultRetentionPeriod
  - Updated section on Mirror Management>Edit a Mirror

    New Request parameters: permanentRetentionEnabled and defaultPermanentRetentionDurationEnabled

    Revised Request parameters: minimumRetentionPeriod, maximumRetentionPeriod and defaultRetentionPeriod
  - Updated section on Mirror Management>Edit a Mirror Template

    New Request parameters: permanentRetentionEnabled and defaultPermanentRetentionDurationEnabled

    Revised Request parameters: minimumRetentionPeriod, maximumRetentionPeriod and defaultRetentionPeriod
  - Updated section on Vault Management>Create a Vault

    New Request parameters: permanentRetentionEnabled and defaultPermanentRetentionDurationEnabled

    Revised Request parameters: minimumRetentionPeriod, maximumRetentionPeriod and defaultRetentionPeriod
  - Updated section on Vault Management>Create a Vault Template

    New Request parameters: permanentRetentionEnabled and defaultPermanentRetentionDurationEnabled

    Revised Request parameters: minimumRetentionPeriod, maximumRetentionPeriod and defaultRetentionPeriod
  - Updated section on Vault Management>Edit a Vault

    New Request parameters: permanentRetentionEnabled and defaultPermanentRetentionDurationEnabled

    Revised Request parameters: minimumRetentionPeriod, maximumRetentionPeriod and defaultRetentionPeriod
  - Updated section on Vault Management>Edit a Vault Template

New Request parameters: permanentRetentionEnabled and defaultPermanentRetentionDurationEnabled

Revised Request parameters: minimumRetentionPeriod, maximumRetentionPeriod and defaultRetentionPeriod

– NEW section added for Configure Vault Protection

New Request parameters: vaultProtectionEnabled, systemMinRetentionPeriod, systemMaxRetentionPeriod, systemDefaultRetentionPeriod and systemPermRetentionEnabled

API updates for the 3.14.0 release have been referenced in the following documentation:

- CSO API Developer Guide
  – Updated section on API reference>Operations on objects

New valid value of -1 for the Retention-Period header, which indicates indefinite retention:

- Requests
- Upload a protected object
- Upload a protected object using webforms
- Get an object's protection configuration
- Copy a protected object
- Complete a multipart upload for protected objects
- Responses
- Download a protect object

New header Extend-Retention-From-Current-Time:

- Requests
- Extend retention period of a protected object

- REST API Developer Guide
  – Added new section on Administration>Add notification service configuration
  – Added new section on Administration>Edit notification service configuration
  – Added new section on Administration>Delete notification service configuration
  – Added new section on Administration>Edit notification service configuration assignment
  – Updated section on Vault Management>Create a vault

New Request parameters: notificationServiceTopicOverride and notificationServiceConfigurationId

  – Updated section on Vault Management>Create a vault template

New Request parameters: notificationServiceTopicOverride and notificationServiceConfigurationId

  – Updated section on Vault Management>Edit a vault

New Request parameters: notificationServiceTopicOverride and notificationServiceConfigurationId

  – Updated section on Vault Management>Edit a vault template

New Request parameters: notificationServiceTopicOverride and notificationServiceConfigurationId

API updates for the 3.13 release have been referenced in the following documentation:

Feature Limitations:

COS-31712: If a user uses **`createVault`** and specifies retention periods, but does not specify the **`protectionState`** or the **`protectionState`** is specified as disabled' the user should expect a reject where as in previous releases of the software, the retention periods would have simply been ignored.

COS-34240: Changed **`retention-legal-hold-count`** header to lower-case for consistency with other retention header responses.

- CSO API Developer Guide

- Mirror-Destination header for GET /bucket, GET /bucket?acl, GET /bucket?cors, GET /bucket?uploads, GET /object, HEAD /object, GET /object?legalhold
- Maximum number of days for retention periods settings is 36159 days
- Value for the "Status" parameter is now "Retention" (it was "Compliance" before)
- New methods:

  POST /object (Specify retention periods and add a single legal hold to a protect object with webforms)

  POST /object?extendRetention (Extend the retention period of a protected object)

- Device API Guide
  - Updated section on Device API Reference>State

    New raid section added

    State -> raid

    Updated JSON and Response Parameters Table to include:

    - New Response parameter: raidStatus

    - New Response parameter: arrayHealth
  - Updated section on Device API Reference>Statistic

    Updated JSON and Response Parameters Table to include:

    - New Response parameter: applianceLayout

    - New Response parameter: applianceType

    New Response section: capabilities -> {monitoring, visualization and other capabilities available on the device - see Device API guide for details}

    New Response section chassis -> [discrete enclosure units that describes hardware entity information - see Device API guide for details]

    New Response section driveThresholds -> { total, warning and error thresholds by drive usage type - see Device API guide for details}

    New Response section raid -> arrayHealth parameter
- REST API Developer Guide
  - Updated section on Mirror Management>Create a Mirror

    New Request parameters: protectionState, minimumRetentionPeriod, maximumRetentionPeriod, defaultRetentionPeriod, and restrictiveAccessControlEnabled
  - Updated section on Mirror Management>Create a Mirror Template

    New Request parameters: protectionState, minimumRetentionPeriod, maximumRetentionPeriod, defaultRetentionPeriod, and restrictiveAccessControlEnabled
  - Updated section on Mirror Management>Edit a Mirror

    New Request parameters: protectionState, minimumRetentionPeriod, maximumRetentionPeriod, and defaultRetentionPeriod
  - Updated section on Mirror Management>Edit a Mirror Template

    New Request parameters: protectionState, minimumRetentionPeriod, maximumRetentionPeriod, defaultRetentionPeriod, and restrictiveAccessControlEnabled
  - Updated section on Vault Management>Create a Vault

    New Request parameter: restrictiveAccessControlEnabled
  - Updated section on Vault Management>Create a Vault Template

    New Request parameter: restrictiveAccessControlEnabled
  - Updated section on Vault Management>Edit a Vault Template

    New Request parameter: restrictiveAccessControlEnabled
  - NEW section added for Upgrade System Software
  - Updated section on Reports>Disk drive and device report>Response

Updated JSON
New Response parameter: chassisId
New Response parameter: enclosureId
New Response parameter: slotId

- Updated section on Reports>Failed field replaceable unit report>Response
  Updated JSON
  New Response parameter: chassisId
  New Response parameter: enclosureId
  New Response parameter: slotId
- Updated section on Reports>Firmware report>Response
  Updated JSON
  New Response parameter: chassisId
  New Response parameter: enclosureId
  New Response parameter: slotId
- Updated section on Reports>Storage pool capacity and disk report>Response
  Updated JSON
  New Response parameter: chassisId
  New Response parameter: enclosureId
  New Response parameter: slotId
- Updated section on Administration>View system configuration>Response
  Updated JSON
  New Response parameter: driveTotalCount
- Updated section on Device management>Device drive bay nut enclosure action
  Updated description
  Updated HTTP
  Updated Curl
  Response>New Response parameter: chassisId
  Response>New Response parameter: enclosureId
  Response>New Response parameter: slotId

API Changes 3.14.5

COS-53036: API URLs / parameters related to notification service functionality has changed such that the word "configuration" is no longer present. Old audit action codes were not migrated to remove the word "configuration."

COS-56456: Changed the status code returned for conditions where a bandwidth or operation rate limit is exceeded from HTTP status code 503 to HTTP status code 429.

COS-56281: Device API for Notification Service: Field has a typo for notification blob "**`notificationService`**" and Fields lack description..

API Changes 3.14.4

COS-53785: Fixed an issue where a HEAD request with a ranged read header would ignore the requested range and return the content length of the entire object.

COS-55935: Fixed an issue where a HEAD request for a portions of an object via a part number query would ignore the part information and return the content length of the entire object.

API Changes 3.14.3

COS-49565: Update Manager Data Model and REST API for mirrorType

API Changes 3.14.2

API Changes 3.14.1

COS-48002 : S3 Extended API now supports query parameter of ‘extended’ in addition to ‘pagination’ which was previously supported.

COS-42959: The AWS V4 content-sha256 is not always verified when present, and change an error message.

On-prem Vault mode WORM change in behavior:

- For a PUT protection request, either the content-md5 of the request body xml must be provided, or if using a V4 signature, the provided x-amz-content-sha256 must contain the actual hash instead of "UNSIGNED_PAYLOAD".

(The current on-prem vault mode protection does not require content verification (content-md5 or sha256) on the put protection request)

Change in behavior for regular requests with regard to content-sha256 verification:

- If using a V4 signature with a multipart upload PUT part, and the provided x-amz-content-sha256 contains the actual hash instead of "UNSIGNED_PAYLOAD", then that hash will be validated against the payload.
- If using content-md5 with a multipart upload PUT part or a write extent PATCH request, and the content-md5 is valid, but does not match the calculated payload hash, then the error code will be "BadDigest" now instead of "InvalidDigest".

API Changes 3.14.0

COS-42241: Release Note for CSAFE-9996

The 'settings' object in the viewSystem.adm method has been modified. The attributes accessPoolProtocolType, accessServicePorts, certificateExpirationNotificationDays have been removed.

Note: Removed content for the above attributes from the code in View System Configuration>Response>JSON Response Example .

API Changes 3.13.5

COS-42414: DOC UPDATES related to CSAFE-37117

In 3.13.5, code updates to support URL encoding for List Responses is available.

The below feature flag is used currently to disable the feature.

s3.listing-encoding-enabled = false

Once enabled the results for certain response elements will be URL encoded and users need to make corresponding updates if they are using the encoding-type in the requests.

For all the below operations, we now support a method to encode certain response elements using URL encoding in the response being sent. This is in compliance with AWS S3 API Version 2006-03-01. 1.

1. GET BUCKET (List Objects) Version 1

   When the Get Bucket list v1 request includes encoding-type element and when the method is set to URL, the response will URL encode the elements - Delimiter, Marker, Prefix, NextMarker and Key.
2. GET BUCKET (List Objects) Version 2

   When the Get Bucket list v2 request includes encoding-type element and when the method is set to URL, the response will URL encode the elements - Delimiter, Prefix, ContinuationToken, Key and StartAfter.
3. GET BUCKET Object Versions

   When the GET Bucket Object versions request includes encoding-type element and when the method is set to URL, the response will URL encode the elements - Delimiter, Prefix, Key, KeyMarker and NextKeyMarker.
4. LIST MULTIPART Uploads

   When the LIST Multipart Uploads request includes encoding-type element and when the method is set to URL, the response will URL encode the elements - Delimiter, Prefix, Key, KeyMarker and NextKeyMarker.
5. LIST PARTS

   When the LIST Parts request includes encoding-type element and when the method is set to URL, the response will URL encode the elements - Key Please refer to AWS S3 API reference for detailed notes for the above requests

Note: Please refer to AWS S3 API reference for detailed notes for the above requests.

API Changes 3.13.4

COS-33549: Device API

State API

When a device is upgraded, any existing disabled drive bay power control states in the openExternalEvents object are removed from the State API.

Statistic API

- Several hardware components such as chassis, enclosure, voltage sensors, fan sensors, power supply sensors, and drive configurations are reported in a new format.
- The voltage, fan, and power supply statistics are reported as properties of a **chassis**object instead of the root of the JSON output. However, statistics in the old format are available for backwards compatibility through the advanced configuration settings of the Manager application. For more information on this advanced configuration setting, contact IBM Customer Support.
- For voltage statistics, **maximum_voltage** and **minimum_voltage** readings are removed. Instead, a **status** property is added. The status can be OK, DISABLED, CRITICAL, UNKNOWN, or NOT_PRESENT.
- For fan statistics, **maximum_speed** and **minimum_speed** readings are removed. Instead, a **status** property is added. The status can be OK, DISABLED, CRITICAL, UNKNOWN, or NOT_PRESENT.
- For CPU temperature statistics, **maximum_temperature** has been removed. Instead, a **status** property is reported. The status can be OK, DISABLED, CRITICAL, UNKNOWN, or NOT_PRESENT.
- Drives now report specific usage types. Valid drive usage types are data, os, osSpare, database, and unknown.
- Drives have a new format for reporting bay identifier. It uses the three new identifiers (**chassis_id**, **enclosure_id** and **slot_id**) and concatenates them together to create the drive bay identifier.
- The enclosure object for listing drive bays with power control capability is no longer available in the root of the JSON by default. The drive bay power control statistics can now be found in **chassis[].enclosure[].slots[].phy**.The legacy enclosure object is available for backwards compatibility

through the advanced configuration settings of the Manager application. For more information on this advanced configuration setting, contact IBM Customer Support.

- PCI addresses have been removed from network interface sections in device statistic API.

API Changes 3.13.3

Information on the Get Bucket V2 APIs can be found the COS API guide.

Chapter 8. Resolved Issues

Resolved issues in 3.14.5 July Maintenance Release

Table 2. Resolved issues

Issue	Description
COS-57359	Resolved an issue where a reboot of IBM Cloud™ Object Storage Slicestor12, Slicestor53 or Slicestor106 models, the network connectivity is lost and services can not be restarted. On IBM Slicestor 2584 appliances, the serial number is unavailable after a reboot. Recovery of this issue previously required the enclosures to be power cycled. As this issue has been addressed, this is no longer required.

Resolved issues in 3.14.5

Table 3. Resolved issues

Issue	Description
COS-54415	When using Internet Explorer, the data are cached on first load for the following pages: access pool summary, site summary, and drives. The server now sends cache-control headers for those pages' requests.
COS-27974	Fixed an issue where there is Mismatched Diagnostic reason for file system issues on Manager device summary and open incident.
COS-47041	Fixed an issue where Stale entry of the replaced drive persists after failing disk migration was going on that drive, which was eventually replaced.
COS-52236	Fixed an issue where Notification Service incidents do not open when expected.
COS-54475	Fixed an issue where change in HDD model name results in duplicate drive entries.
COS-52443	Fixed an issue where DLM reports duplicate drives with ONLINE/ONLINE state - None Model Name.
COS-43509	Event message for virtual drives have been updated to display disk status.
COS-49906	Unexpected feature interaction leads to user being forced to enter a notification service topic when they should not be forced to do so.
COS-46315	UI elements related to notification service functionality is now hidden when notification service feature is not in use.
COS-52039	Vault summary report columns related to notification service properties are defective. Changed column headings. Added missing "configured topic" to row.
COS-50955	User must supply name when editing a notification service. If the value is not provided, the old previous value is used.
COS-49529	Altered behavior such that the TLS certificate property of notification services is not required.

Resolved issues in 3.14.4

Table 4. Resolved issues

Issue	Description
COS-49593	Fixed an issue where a race condition may cause on-heap resource permits to accumulate on an Accesser device and never be released, resulting in HTTP 503 errors.

Table 4. Resolved issues (continued)

Issue	Description
COS-48342	The Device API (/statistics) reports system load averages with a 100x multiplier in the "loadX" key in the API, which differs from typical output found from "uptime" or "top." This is required for legacy reasons.
COS-48308	When using the DMS or vault proxy features with the system in a mixed version scenario, a background service in the manager may upgrade vault formats prematurely. If this occurs, 500s would occur during writes from the upgraded source vault to the destination vault (DMS), or during reads to the upgraded proxy vault.
COS-53463	In releases after 3.14.1 and prior to this release, for some scenarios, the core software process does not shut down during upgrade within the configured timeout. In these cases, the manager application does not automatically stop the core software process. This issue has now been resolved. For releases without this fix, the workaround is to manually force stop the device by clicking the "Force Quit" button.
COS-48947	Today, we return a status code 507 when a user tries to create more containers in a storage account than is allowed. By comparison, AWS returns a HTTP 400® - TooManyBuckets error: TooManyBuckets You have attempted to create more buckets than allowed. 400 Bad Request Client We should evaluate whether it would be appropriate to change our behavior to match this expectation. A 4xx class "client error" status code seems more appropriate than a 5xx class "server error" status code.
COS-53785	Fixed an issue where a HEAD request with a ranged read header would ignore the requested range and return the content length of the entire object.
COS-55935	Fixed an issue where a HEAD request for a portions of an object via a part number query would ignore the part information and return the content length of the entire object.
COS-50845	In the Manager UI, a new section has been added under the Administration tab in the System Properties Configuration section called Slicestor Storage Engine. This functionality allows a user to set the default storage engine globally. This storage engine is applied to Slicestor devices during approval. Once set, the storage engine cannot be updated without a device reimage. A user can override the default storage engine by selecting the desired storage engine from the drop down available in the device approval section on the Home and top-level Configure pages.
COS-40727	In the Manager UI, the Allocated usage displayed on the Site, System, Storage Pool, and Slicestor Device pages has been updated. In prior ClevOS versions, the Allocated usage represented only the user (vault) data, but starting in ClevOS 3.14.4, the Allocated usage also includes the reserved file system data. In addition, the Manager UI will show an increase in Capacity to account for this change. The Unallocated usage will remain the same. Also, another change introduced in the Manager UI is to display the Reclaimable space on the Slicestor Device page. This usage represents data on disk that has been marked for deletion and is available to be compacted at some point in the future. The COS system has logic in place to determine when this data should be compacted.

Resolved issues in 3.14.3 June Maintenance Release

Table 5. Resolved issues

Issue	Description
COS-56191	Resolved an issue where incorrect drive model data would result in a drive being shown twice in the drive list. As part of this change, any prior state associated with the invalid drive model data is corrected.

Resolved issues in 3.14.3 May Maintenance Release

Table 6. Resolved issues

Issue	Description
COS-52911	Fixed an issue where size enforcement was not being performed properly when performing a multipart upload part upload by copying a part from an existing object.

Resolved issues in 3.14.3 April Maintenance Release

Table 7. Resolved issues

Issue	Description
COS-52590	Resolved an issue with slices being incorrectly processed during reallocation operations.
COS-50168	A STARTTLS option has been added to the "New Configuration" section of the SMTP Configuration page in the Manager. When configured, the Manager follows the STARTTLS protocol, which initiates a secure connection before authenticating to the mail server.

Resolved issues in 3.14.3 March Maintenance Release

Table 8. Resolved issues

Issue	Description
COS-46163	Fixed an issue where malformed requests with aws-chunked Content Encoding may encounter an exception during processing, causing the core process on the accesser appliance to restart.

Resolved issues in 3.14.3

Table 9. Resolved issues

Issue	Description
COS-39184	After triggering a storage pool expansion, set replacement or set removal, the audit indicating "The storage was modified. The size was changed from size1 to size2" can show incorrect size values.

Resolved issues in 3.14.2 February Maintenance Release

Table 10. Resolved issues

Issue	Description
COS-47620	Fixed an issue where Accesser devices may leak a small amount of memory when processing requests via HTTPS, leading to an out of memory condition and core process restart.

Resolved issues in 3.14.2

Table 11. Resolved issues

Issue	Description
COS-46326	In previous releases the default connection count for all connections between ClevOS devices was 1, and this was only increased when a network latency of greater than 20ms was detected. 3.14.2 has changed the default behavior to always use 8 connections no matter what the detected latency is. This new default is a configuration which was already being manually applied to many customer systems to fix various performance problems. The main impact of this change is that client connections will now allow 8 times more outstanding messages to a server before it begins to queue to that server. In addition, the change allows more parallelism for TLS processing. For these reasons this configuration often fixes situations where requests were responded to with error code 503 unnecessarily.
COS-46740	Deletion of a retention-enabled vault is only allowed if the manager can verify the vault is empty. In prior releases, the check to determine whether the vault is empty would fail if the Access Pool had a customer-supplied certificate chain configured. As a result, the manager would not allow the deletion of a retention-enabled vault, even when empty. This issue has now been resolved.
COS-41545	As part of System NTP Configuration, entering a comma separated list of NTP servers in the External NTP Servers field saves the comma as part of the NTP Server. The NTP server plus comma is rejected as an NTP server, resulting in it not being listed in ntpq -pn output and not taking effect. This issue impacts both the Manager REST API and UI.
COS-47362	In prior releases, incidents did not include severity information in email alerts. Severity and cleared information are now available in the Subject of the email alert. Examples: Subject: [dsnet-alert] Incident updated with critical event for storage pool SP1 Subject: [dsnet-alert] Incident closed with cleared event for storage pool SP1
COS-48911	In prior releases, email alerts did not include the Access Pool name as part of the Subject. This issue has now been resolved. Example: Subject: [dsnet-alert] Incident opened with critical event for access pool AP1
COS-44824	In prior releases, the Event Console Manager REST API with the streamTypes parameter set to openIncidentsCurrentState may fail with a 500 HTTP response. This issue has now been resolved.

Resolved issues in 3.14.1 February Maintenance Release

Table 12. Resolved issues

Issue	Description
COS-47620	Fixed an issue where Accesser devices may leak a small amount of memory when processing requests via HTTPS, leading to an out of memory condition and core process restart.
COS-50675	Resolved an issue where certain mid-stream IO errors that are encountered while using HTTPS were being incorrectly reported as a HTTP 500 error code.
COS-48112	Resolved an issue where slice reallocation between Slicestor devices may be erroneously marked as complete if the storage service was shutdown during the reallocation process.

Resolved issues in 3.14.1 January Maintenance Release

Table 13. Resolved issues

Issue	Description
COS-48885	In Release 3.13.4 and subsequent releases prior to this release, the Manager UI can report incorrect BGP load balancing router status, inconsistent with the load balancing router status provided by an Accesser device. This issue has now been resolved.
COS-48298	Resolved an issue that would cause various system processes to hang. This could result in components of the system silently becoming inoperative. It is recommended that all affected systems be upgraded.
COS-46718	Resolved an issue where services in the drive monitoring subsystem on Slicestor devices were slow to start. This resulted in errors that prevented the drive monitoring subsystem from initializing properly, which in turn prevented drives from being brought online.
COS-46799	Resolved an issue where Slicestor devices were erroneously detecting USB drives and attempting to process them as data drives. This resulted in existing drives sometimes being reported in invalid states and/or an inability to detect drive removals or insertions.

Resolved issues in 3.14.1 December Maintenance Release

Table 14. Resolved issues

Issue	Description
COS-48002	S3 Extended API now supports query parameter of 'extended' in addition to 'pagination' which was previously supported.

Resolved issues in 3.14.1

Table 15. Resolved issues

Issue	Description
COS-41430	If a device doesn't respond to a manager's "Force Kill" request during an upgrade, the manager will no longer initiate upgrades on devices that are waiting in the upgrade queue. The manager will also be unable to remove devices from the upgrade queue. This issue is resolved in this release.
COS-45556	BMC Status Missing from Statistic API. This issue is resolved in this release.
COS-43901	Resolved an issue where Put-Copy request between two different compliance enabled Mirror causes 500 Error.
COS-45018	Resolved an issue where Presigned URL for PUT object and POST(form) returns 403 SignatureDoesNotMatch

Resolved issues in 3.14.0

Table 16. Resolved issues

Issue	Description
COS-41430	If a device doesn't respond to a manager's "Force Kill" request during an upgrade, the manager no longer initiate upgrades on devices that are waiting in the upgrade queue. The manager is unable to remove devices from the upgrade queue. This issue has now been resolved.
COS-12691	Instability has been observed when running two 40 Gbit links in LACP mode.

Table 16. Resolved issues (continued)

Issue	Description
COS-12983	Virtual devices running ClevOS within VMware may experience a kernel panic when migrating the virtual machine to a new server using VMware (R) vMotion (tm).
COS-16114	On systems with RAM roughly equal to or greater than the size of the OS drive, a kernel panic may result in the system being in an unusable state.
COS-41035	In 3.13.4 with a mixed release system containing devices on a lower release compared to the Manager, when a drive is failed from the UI, the Monitor Device page displays an incomplete message "diskFailSuccess."
COS-1749	After recovering from an unresponsive IPMI controller, the open incident in the Manager event console sometimes fails to clear. The open incident is misleading, but has no impact on the system operation.

Chapter 9. Known issues

Table 17. Known issues

Issue	Failing Condition	Disposition
COS-50579	There is a known issue where slice data being reallocated from one Slicestor device to another would not be appropriately removed from the source Slicestor device if the reallocation process was erroneously marked as complete."	This issue still exists in 3.14.3 because the change was reverted in the latest fix.
COS-11201	In the Event Console of the Manager User Interface, the event details section for failing disk migration events contains a parameter that is called Migration Progress. However, it is not clear what this value represents.	This value corresponds to the percentage of failing disk migration that is complete.
COS-11355	Replacing a failed drive with another failed drive results in an inconsistent view on the Manager User Interface. On the Monitor Device page, in the "Summary of device health" section, both the replaced failed drive and the new failed drive are shown. The "Drive Information and Actions" view of the drive layout shows the replaced failed drive. On the Maintenance page, the FRU report contains the replaced failed drive.	Perform another replacement of the failed drive with a good drive.
COS-13575	The "stop migration" operation for failing disk migration on the Manager User Interface (UI) can take ~20 seconds to complete after being initiated by the user. The button continues to be enabled during this time. This issue exists for dispose and reset disk operations as well.	Do not hit the button again until the operation completes. If the drive stays in the same state for more than 20 seconds, perform a refresh of the page. If the drive continues to stay in this state, follow the recommended action that is provided in the Manager Administration Guide under disk lifecycle management.
COS-10031	When resuming a drive in the DIAGNOSTIC state from the Manager User Interface, it can take ~20 seconds to complete. The resume button is not disabled during this time.	Do not hit the resume button until the operation completes. If the drive stays in the DIAGNOSTIC state for more than 20 seconds, perform a refresh of the page. If the drive continues to stay in this state, follow the recommended action that is provided in the Manager Administration Guide under disk lifecycle management.
COS-10445	When using the storage command from the localadmin shell on a Slicestor device, it is possible to resume all drives that are currently in the DIAGNOSTIC state. However, in some cases , this process can take too long, which will cause the command to return an error code -15 due to a timeout.	Despite the error, the resume process is continuing in the background. The storage list command can be used to monitor the progress of resume process.
COS-7488	When performing a storage pool set removal, it is possible that once the reallocation has finished for a source Slicestor device, it can show some small amount of data still present.	No action is required. Once the set removal has completed, all slices have been reallocated to the new storage pool. Any discrepancy in a Slicestor device's used space is generally a result of small inaccuracies that can occur during normal usage of the system.

Table 17. Known issues (continued)

Issue	Failing Condition	Disposition
COS-13504	When failing a quarantined drive, it is possible that after data has been migrated off the failing drive, the Manager event console will report that no data migration was attempted.	No action is required. Despite the event description, data migration will always be attempted unless the user specifically chooses to skip migration via the localadmin shell storage command.
COS-22921	When someone attempts to delete a bucket they first need to determine the assesser that can be used to issue the command. The S3 GET Bucket Location is one means to determine this. However, this command can not work at every access pool.	Enhancing the S3 GET Bucket Location as a corner case command that can work at any access pool will be addressed in a future release.
COS-22990	The S3 remote proxy implementation of vault proxy has a few limitations that are related to communicating with an Amazon S3 endpoint. The version of the AWS SDK used to communicate to Amazon defaults to using V2 instead of V4 authentication, causing authentication issues when communicating with certain AWS endpoints.	For further assistance in configuring a remote proxy for use with Amazon S3, contact IBM customer support.
COS-23025	SL 4U slicestor devices, LEDs are incorrectly set.	Recovery Action: The user can use MegaCLI/storcli commands to issue LED actions before performing disk replacements. This will be fixed in a future release.
COS-23962	Vault quotas are static and do not update when storage pool capacities change. If a system expansion, set replacement, or set removal is performed on the storage pool, vault quotas for any vaults on that pool will not update to consider the new capacity.	The user defined vault quotas work as expected. However, they can not be consistent with the current storage pool capacity. For example, a vault quota can be higher than total storage pool capacity after a set removal.
COS-22924	When you upgrade the Manager to ClevOS 3.10.1 or newer for the first time, you might not be able to log in immediately. The Manager application might need an extra 20 - 30 minutes to become available due to database schema changes introduced in ClevOS 3.10.1. On systems with large databases, particularly systems with considerable historical event content, the time can be longer.	Contact Customer Support if it takes longer than 30 minutes to successfully log in to the Manager. Do not attempt to restart the Manager while it is upgrading.
COS-26214	Lack of documentation highlighting dependencies of Hadoop-connector package with GA releases.	For legacy customers who are still using Hadoop connector for ClevOS software, please contact IBM customer support to install a new package compatible with latest build.
COS-27469	When performing a PUT-COPY operation, a request header is used to specify the source of the copy operation. If this header is specified, but with an empty value, the request is expected to fail with an HTTP 400 - Bad Request. Instead, the object is being successfully created but with empty content.	This will be fixed in a future release.
COS-29681	When using the Microsoft IE9 web browser, certain Manager user interface elements like the left navigation panel and the vault capacity bar charts on the Monitor Vault page can not appear.	Microsoft has ended support of IE9 and IE10. Users should upgrade to Microsoft IE11 or higher, or use an alternative browser, such as Firefox, Safari, or Chrome.

Table 17. Known issues (continued)

Issue	Failing Condition	Disposition
COS-40881	The Manager REST API Edit Authentication Mechanism does not correctly update the value of the Hiding Secret Access Key flag and returns a status code 200. The flag is visible on the Security tab of the Manager UI.	This issue is resolved in a subsequent release.

Upgrading and Installation

Table 18. Upgrading and Installation

Issue	Failing Condition	Disposition
COS-7126	When extracting of upgrade file fails when a device is upgrading the failure message "The Selected File cannot be extracted while upgrades are in progress" continue to show if upload is restarted.	Only one upgrade file can be uploaded to the manager at a time. If another file is uploaded during an upgrade, an error message appears until the page is reloaded.
COS-15372	When upgrading from ClevOS 3.8.x, 3.9.x, or 3.10.0 to 3.10.1 or later, all drives not used for Slicestor data (for example, OS drives) will be reported as newly discovered in the Manager event console.	No action is required.

Container

Table 19. Container

Issue	Failing Condition	Disposition
COS-1852	When attempting to write an object to a container that does not exist, the Accesser appliance returns an HTTP 404 response with an error message of NoSuchKey instead of the appropriate NoSuchBucket. This includes cases where the container name includes a "/".	Ensure that your vault or container is successfully created before attempting to write objects to it. If you receive an error message of NoSuchKey for an upload request, verify that the container you are addressing does exist.
COS-15401	If a user attempts to create a management vault using "manual configuration" (accessed through the Configure Management Vault page) based on an existing vault template, management vault creation fails with the following message: "Cannot create a management vault from this template. It is deployed to access pools with standard vaults"	Use the "automatic configuration" available on the Configure Management Vault page.
COS-15218	Container creation or deletion can sometimes result in 500 error responses when the requests are sent concurrently with other configuration requests to the same storage account.	Retrying the request that received a 500 is a suggested recovery action. It's best to retry the request when not doing other operations on the same storage account.

Alerting and Reporting

Table 20. Alerting and reporting

Issue	Failing Condition	Disposition
	Nothing to report.	

System Behavior

Table 21. System behavior

Issue	Failing Condition	Disposition
COS-2498	The usage of a disk is counted while the disk is offline. However, its capacity is not counted.	No action. Awareness of limitation. If necessary a restart of core would fix the usage values. Limit DLM events
COS-2128	In a GDG configuration with high request latency to the remote stores and low latency to local stores, an Accesser Appliance opens multiple connections to the remote stores and a single connection to local stores. Large bursts of IO can overwhelm the single local connection, resulting in elevated response times and operation latencies.	Using the System Advanced Configuration framework, the Accesser Appliance can be configured to open multiple connections to local stores, allowing it to better handle burst of IO activity. The parameter to configure appropriately is network.connection-profile. Please refer to section 3 of the Advanced System Configuration guide for more details.
COS-1920	Support for "encoding-type" header when performing xml-based listing requests is not currently provided.	This feature is not currently supported

Storage Pools

Table 22. Storage pools

Issue	Failing Condition	Disposition
COS-2642	On the *Monitor Storage Pool Page, the **Reallocation Progress** graph, which displays historical data, is inaccurate when a device is down or statistics are not collected for a window of time.	The **Data Reallocation** progress bar, available at the top of the *Monitor Storage Pool Page, is always accurate. This view reflects the status and should be used to monitor progress of the data reallocation activity.

Data Evacuation

Table 23. Data evacuation

Issue	Failing Condition	Disposition
	Nothing to report.	

System Configuration

Table 24. System configuration

Issue	Failing Condition	Disposition
	Nothing to report.	

Deleting objects

Table 25. Deleting objects

Issue	Failing Condition	Disposition
9444	If a system is 100% full, customers might encounter an HTTP 500 error if they attempt to delete objects larger than the embedded content threshold (<1MB S3, >4MB SOH for default segments size). This issue has existed since release 3.0. It occurs because deleting large objects causes an intermediate write that appears larger to a Slicestor® Node, causing that node to fail the request due to an insufficient space error.	Contact IBM Support. They must use a development-provided procedure to free up disk space.

Manager Web Interface

Table 26. Manager Web Interface

Issue	Failing Condition	Disposition
COS-13189	For drives that do not have a SCSI name, some Disk Lifecycle Management (DLM) actions, such as resume and fail, performed through the Manager User Interface (UI) will fail.	Use drive serial number to perform the action from the command line. Obtain drive serial number information by executing (see SERIAL column): # storage list Perform the operation based on the drive serial number (Z29010L5), for example: # storage fail Z29010L5
COS-10031	When resuming a drive in the DIAGNOSTIC state from the Manager User Interface, it may take ~20 seconds to complete. The resume button is not disabled during this time.	Do not hit the resume button until the operation completes. If the drive stays in the DIAGNOSTIC state for more than 20 seconds, perform a refresh of the page. If the drive continues to stay in this state, follow the recommended action provided in the Manager Administration Guide under disk lifecycle management.
COS-23764	Upon network failure while going through the one time setup process in the manager, a network error page will appear. When the network comes back, re-load the page, at which point an internal server error page will appear in some scenarios.	Log out from the internal server error page and log back into the manager, which will take you through one time setup again.

Vaults

Table 27. Vaults

Issue	Failing Condition	Disposition
	Nothing to report	

Vault Mirrors

Table 28. Vault mirrors

Issue	Failing Condition	Disposition
COS-7019	When performing IO against a vault mirror with synchronous writes disable, HEAD requests performed against a successfully written object may return an HTTP 404 response.	If an HTTP 404 is returned for a HEAD request for a recently written object, please retry your request.
COS-13370	Through the Manager User Interface (UI), after creating a mirror from a mirror template that has Authorized IP Addresses populated, the mirror does not contain the specified IPs.	Perform the following workaround. After the mirror is created, add the IPs using the Edit Mirror Access Control page.

Vault migration

Table 29. Vault migration

Issue	Failing Condition	Disposition
COS-12442	When a vault migration finishes the work contained in its TODO queue, it kicks off a process to calculate the exact count of the number of objects migrated as part of the migration. This process of calculating the exact size is performed by each device in the target pool, and can take a long time to complete for large migrations.	

Chapter 10. Supported Hardware Platforms

IBM Cloud Object Storage Appliances

Table 30. Minimum Version of ClevOS Compatible with Cleversafe Hardware Platforms

Appliance	Product	Minimum ClevOS
System Manager Appliance	M2100	≤2.7.0
System Manager Appliance	M2105	3.2.2
System Manager Appliance	M3100	2.7.0
IBM COS Accesser® Device	A2100	≤2.7.0
IBM COS Accesser® Device	A3100	≤2.7.0
IBM COS Slicestor® Device	S1440	≤2.7.0
IBM COS Slicestor® Device	S2104	3.2.1
IBM COS Slicestor® Device	S2212	3.2.1
IBM COS Slicestor® Device	S2440	3.0.1
IBM COS Slicestor® Device	S4100	3.1.0

Table 31. Minimum Version of ClevOS Compatible with IBM Hardware Platforms

Product Name	Machine Type (1Yr/3Yr Warranty)	Model	Minimum ClevOS
IBM COS Accesser® 3105	3401/3403	A00	3.8.1
IBM COS Accesser® 4105	3401/3403	A01	3.8.1
IBM COS Accesser® F5100	3401/3403	A02	3.8.3
IBM COS Accesser® T5100	3401/3403	A02	3.10.1⌂
IBM COS Accesser® 3110	4958/4957	A10	3.14.4
IBM COS Manager™ 2105	3401/3403	M00	3.8.1
IBM COS Manager™ 3105	3401/3403	M01	3.8.1
IBM COS Manager™ 3110	4958/4957	M10	3.14.4
IBM COS Slicestor® 2212	3401/3403	S00	3.8.1
IBM COS Slicestor® 2448	3401/3403	S01	3.8.1
IBM COS Slicestor®3448	3401/3403	S02	3.8.3
IBM COS Slicestor®2584 (AP-TL-1)	3401/3403	S03	3.8.1
IBM COS Slicestor®2584 (AP-LS-1)	3401/3403	S03	3.13.1
IBM COS Slicestor®2212A	3401/3403	S10	3.10.0
IBM COS Slicestor®12	4958/4957	C10/J10	3.14.4
IBM COS Slicestor®53	4958/4957	C10/J11	3.14.4
IBM COS Slicestor®106	4958/4957	C10/J12	3.14.4

Note: ⌂ Requires RPQ

Hewlett Packard Enterprise

Table 32. Minimum Version of ClevOS Compatible with Hewlett Packard Enterprise Hardware

Appliance	Model	Minimum ClevOS
Manager Appliance	DL360P Gen8	3.2.1
Manager Appliance	DL360 Gen9	3.5.0
Manager Appliance	DL380 Gen9	3.5.0
Accesser® Device	DL360P Gen8	3.2.1
Accesser® Device	DL360 Gen9	3.5.0
Accesser® Device	DL380 Gen9	3.5.0
Slicestor® Device	SL4540 Gen8	2.9.0
Slicestor® Device	DL380 Gen9	3.5.0
Slicestor® Device	Apollo 4200 Gen9	3.6.0
Slicestor® Device	Apollo 4510 Gen9	3.6.0
Slicestor® Device	Apollo 4510 Gen10	3.14.0
Slicestor® Device	Apollo 4530 Gen9	3.6.0

Seagate

Table 33. Minimum Version of ClevOS Compatible with Seagate Hardware

Appliance	Model	Minimum ClevOS
Seagate OneStor®	AP-2584 1 AP-TL-1	3.4.2

Cisco

Table 34. Minimum Version of ClevOS Compatible with Cisco Hardware

Appliance	Model	Minimum ClevOS
Cisco Slicestor® Device	UCS C3260	3.7.4
Cisco Slicestor® Device	UCS S3260 (Single Node)	3.12.0
Cisco Slicestor® Device	UCS S3260 (Dual Node)	3.12.0
Cisco Slicestor® Device	UCS S3260 M5 (56 drive configuration)	3.13.1
Cisco Slicestor® Device	UCS S3260 M5 (60 drive configuration)	3.13.4
Cisco Manager Appliance	UCS C220 M4	3.12.0
Cisco Accesser® Device	UCS C220 M4	3.12.0
Cisco Manager Appliance	UCS C220 M5	3.13.6
Cisco Accesser® Device	UCS C220 M5	3.13.6
Cisco Slicestor® Device	UCS C240	3.13.6

Dell

Table 35. Minimum Version of ClevOS Compatible with Dell Hardware

Appliance	Model	Minimum ClevOS
Dell Slicestor® Device	DSS 7000	3.10.1
Dell Slicestor® Device	R740xd w/ HDD Support	3.14.1
Dell Slicestor® Device	R740xd w/ NVMe Support	3.14.2

Lenovo

Table 36. Minimum Version of ClevOS Compatible with Lenovo Hardware

Appliance	Model	Minimum ClevOS
Lenovo Manager Appliance	X3550 M5	3.10.1
Lenovo Accesser® Device	X3550 M5	3.10.1
Lenovo Manager Appliance	X3650 M5	3.10.1
Lenovo Manager Appliance	SR630	3.13.6
Lenovo Accesser® Device	SR630	3.13.6
Lenovo Slicestor® Device	SR650	3.13.6

Quanta Cloud Technology (QCT)

Table 37. Minimum Version of ClevOS Compatible with QCT Hardware

Appliance	Model	Minimum ClevOS
QCT Manager Appliance	QuantaGrid D51PH-1ULH	3.13.4
QCT Accesser® Device	QuantaGrid D51PH-1ULH	3.13.4
QCT Slicestor® Device	QuantaGrid D51PH-1ULH	3.13.4

Chapter 11. Incompatible Hardware and Firmware with ClevOS

The hardware components running firmware revisions listed below are incompatible with ClevOS due to the possibility of unexpected behavior.

Note: If you have any hardware on this list running the firmware revisions listed, please contact L3 support immediately to create an upgrade plan. You can determine your firmware revisions using the Firmware Report that is found under the Maintenance menu.

Broadcom

Table 38. Broadcom Hardware and Firmware Incompatibility with ClevOS

Type	Model	Firmware affected
RAID Controller	Broadcom MegaRAID 9361-8i	4.650.00-6121

Hewlett Packard

Table 39. HP Hardware and Firmware Incompatibility with ClevOS

Type	Model	Firmware affected
RAID Controller	HP-SL4540 Smart Array	6.64
iLO	HPE SL4540 Gen 8	2.30

IBM Cloud Object Storage Appliances

Table 40. IBM COS Hardware and Firmware Incompatibility with ClevOS

Type	Model	Firmware affected
USM	IBM COS Slicestor®2584 (AP-TL-1) 3401/3403 S03	4.1.7

Seagate

Table 41. Seagate Hardware and Firmware Incompatibility with ClevOS

Type	Model	Firmware affected
HDD	Seagate ST1000NM0033-9ZM173	SN04

Supermicro

Table 42. Supermicro Hardware and Firmware Incompatibility with ClevOS

Type	Model	Firmware affected
BMC	Supermicro SSG-6048R-E1CR60N	3.60

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
Armonk, NY 10504-1785
U.S.A.

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

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

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.

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

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

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

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

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary.

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.

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

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

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

COPYRIGHT LICENSE:

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

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

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at Copyright and trademark information at www.ibm.com/legal/copytrade.shtml.

Accesser®, Cleversafe®, ClevOS™, Dispersed Storage®, dsNet®, IBM Cloud Object Storage Accesser®, IBM Cloud Object Storage Dedicated™, IBM Cloud Object Storage Insight™, IBM Cloud Object Storage Manager™, IBM Cloud Object Storage Slicestor®, IBM Cloud Object Storage Standard™, IBM Cloud Object Storage System™, IBM Cloud Object Storage Vault™, SecureSlice™, and Slicestor® are trademarks or registered trademarks of Cleversafe, an IBM Company and/or International Business Machines Corp.

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

Printed in USA