IBM Cloud Object Storage System
Version 3.13.6

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 3.13.6

Support>1000 Number of Vaults (1219)

This feature now supports a maximum of 1500 vaults within a system that was limited to 1000 vaults in earlier releases. 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 may be required to the Manager and Slicestor device configuration to leverage this feature. Please contact Customer Support for details.

NTP Configuration for Protected Vaults (1298)

If the system has Vault Protection enabled or contains protected vaults or protected mirrors, then only accounts with the Super User role can configure NTP.

Concentrated Dispersal (CD) Support for Mirrors (1265)

Creating a mirror with CD as the seed vault was not allowed, but this restriction is removed now with this feature. CD mode support is extended for protected mirrors as well so now a user can create protected mirrors with CD vaults.

Chapter 2. New Features and Improvements in ClevOS 3.13.5

This release has various defect fixes.

Chapter 3. New Features and Improvements in ClevOS 3.13.4

Manager Integration into Appliance API [917]

The goal of this feature is to improve the underlying mechanisms used by our devices to report their health and status. The result is simplification of the hardware qualification process because hardware qualification has been decoupled from the manager application.

Behavioral Changes

- Bay numbering changes
  - Support a more general classification of disk drive location identification, the single field "bay" has been converted to a chassis, enclosure, and slot triplet. The bay field is still available for compatibility purposes. The unique location of a disk drive is the combination of chassis, enclosure, and slot. The bay is reported for the format "<chassis>:<enclosure>:<slot>".
- Device diagrams have been made consistent across hardware models.
  - Diagrams with views from the top of the device are all oriented in the same direction (front is to the bottom).
  - Diagrams with front and rear views of the device are consistently labeled with those views.

  Upgrade
- When upgrading HPE ProLiant / HPE Apollo devices, the fan speed data from before the upgrade was reported in "RPM" values artificially. Post-upgrade, the units for these fans are reported in their native unit, "Percent."

  This change in units results in errant behavior when looking at fan speed graphs with a timeframe from before and after upgrade.
- RAID events close/reopen upon upgrade of device.
  - Addresses field issues that are reported where some RAID events may not close properly after their reboots.
- Foreign/Unusable drive events close and re-open upon upgrade of a device because they rely on bay information and the format of the bay that has changed.
- After upgrade to this release, for the hard drive temperature graph found on the Monitor Device page, historical data will not be present for RAID drives. This issue does not arise for subsequent upgrades.

  API
- Multi-node devices "Node"/"Node Location" fields are only available from the manager REST API and GUI reports. These fields have been deprecated and removed from the device statistic API content output and replaced with the more general "enclosure" field within the "chassis" entity.
- All hardware information in the device statistic API is available under a single subtree. For more specific information, refer to the device statistic section in the device API guide.
- PCI addresses have been removed from network interface sections in the device statistic API.
- State information is also included for RAID drives.
- RAID drives under-drive use an identifier that is concatenated using UUID and the bay.
- Drives have a usage classification system to expand on the DLM NO_STORAGE field. Different device classes report different usages, but it is easier to identify different drives and why they may not be used for storing slice data.

  Firmware
- Some devices that did not report their network device firmware versions now support firmware reporting.

Interface Modifications

There have been a number of API changes that are documented in several sections in the Manager REST API Guide, and are detailed in the section within these release notes on Interface Modifications.

Included in the section on Interface Modifications is a list of device API changes.

COS Knowledge Center [1089]

The IBM Knowledge Center delivers IBM's technical content to our users, which is accessible online or packaged as a help system in a product UI. This feature created a public COS Knowledge Center at https://www.ibm.com/support/knowledgecenter/STXNRM for the on-premises documentation, and the creation of an embedded KC in the Manager UI. Prior to this feature, the COS documentation for the on-premises solution was only accessible through the product UI. The embedded KC replaces the current contextual help and Help Index.

- Knowledge Center is the one-stop-shop for all IBM documentation (3200+ products)
- A user can easily find IBM content from Google or internal IBM searches
- Search KC for product documentation, TechNotes, and DeveloperWorks articles
- Easily switch between product release versions with drop-down menu
- Content in KC can be updated separately from product builds, so a user always has the most up-to-date information
- Discover services/products through offers and Marketplace links in the UI
- Responsive mobile experience
- Thoughtful, accessible UI for best reading experience

Localadmin password recovery via Manager UI/API [1148]

This enhancement was made to enable a user to change their device password. The following highlight the changes made for this release:

- The SSH Key Configuration API has been renamed from *systemSshKeyConfiguration* to *securitySshKeyConfiguration*, and the section containing the original information in the Manager REST API Guide has been moved from the **Administration** chapter to the **Account management** chapter. See the Interface Modifications section in these Release Notes for more detail.

  Note: The existing (*systemSshKeyConfiguration*) API is still found in the Manager and is valid for backwards compatibility, but is planned to be removed in a future release.
- Introduced a new API called *securitySshConfiguration* to enable a user to change their device password without having to meet the current password requirement. A user can access the UI from the **Device SSH Authentication** that is found on the security page.
- Moved the SSH key configuration in Manager UI from the administration section to the security section, and found under the **Device SSH Authentication** section.

Chapter 4. New Features and Improvements in ClevOS 3.13.3

Support for GET Bucket V2 Listing [1145]

ClevOS has supported GET Bucket V1 listing(List Objects) with no change in the terms of APIs and is supported in an "as-is" condition. This release includes support for GET Bucket V2 listing(List Objects) and enables IBM Cloud Object Storage (COS) to have functional parity with AWS. This feature supports the return of some or all(up to 1,000) objects in a bucket. The request parameters are used as a selection to return a subset of the objects in a bucket. To use this operation, the user must have permissions to read/list objects in the bucket.

Request Parameter differences in list objects

1. The list-type parameter that is used to differentiate if the object listing is being done that uses Version1 or Version2.
   a. list-type=2 to be used specifically to initiate a Version2 listing
   b. default or if no list-type parameter is used will trigger Version1 listing
2. The continuation-token is used when a S3 response is truncated (IsTruncated response element is true). A NextContinuationToken element is included in the response, which the user can use in the continuation-token parameter in the next request to list subsequent set of objects. This parameter is only supported in Version2 listing.
3. The fetch-owner parameter is a new parameter that is added to the V2 Listing request, which is used to determine whether the Owner information is to be included in the response. By default, the fetch-owner parameter is false, meaning the Owner information is NOT included in the V2 listing response. Unlike V1 listing response that includes the Owner information by default.
4. The start-after parameter is a new parameter added to the V2 Listing request and is very similar to the "marker" parameter in the V1 Listing request. The start-after parameter is considered valid and is used in the first request ONLY, at which point the API returns key names after the specified object key in the start-after. If the start-after parameter is used by the user in subsequent requests (response was truncated and used along with continuation-token), the parameter is ignored.

   Note: In this case when the start-after parameter is included with continuation-token, the response will NOT include the start-after element.

Response Parameter differences for listing

1. The Marker and NextMarker response elements are only included if the object listing is V1. V2 Bucket Listing Response doesn't include these elements.
2. The ContinuationToken is only included in the response if the listing request is of list-type=2 and the request includes the ContinuationToken.
3. The NextContinuationToken is only included in the response if the listing request is of list-type=2 and the response was truncated (IsTruncation = true). User can use the value from the NextContinuationToken element and included it in the subsequent request under "continuation-token" query parameter.
4. The StartAfter parameter is a new parameter added to the V2 Listing request and included in the response to the first listing request for the request WITHOUT continuation-token. If the start-after parameter is used by the user in subsequent requests (response was truncated and used along with continuation-token), the parameter is ignored, and the response does NOT include the start-after element.

5. Owner element was always returned to the user in V1 listing response, if it exists. However, in V2 the response to include the Owner element is governed by the inclusion of "fetch-owner" parameter with value set to "true." The fetch-owner parameter is defaulted to false, so no Owner element is included in the V2 listing response.
6. KeyCount represents the number of keys that are included in the response. Value is always less than or equal to the MaxKeys.

Note: The Continuation Token is an opaque value that is returned by IBM COS to the clients.

Comprehensive phone home and automatic trouble ticket generation [1227]

This feature allows an administrator to configure an IBM COS system to open problem report tickets automatically with IBM Customer Support. A ticket will be created for every incident opened against blue-washed IBM hardware devices.

Chapter 5. New Features and Improvements in ClevOS 3.13.1

Retention of PII - GDPR [1224]

This feature is offered with the IBM Cloud Object Storage (COS) Manager for redacting Personally Identifiable Information (PII) from access logs that are stored on the system indefinitely, or for logs exported from the system. Additionally, the Manager provides a setting that can be used to guarantee that logs on the filesystem of Accesser appliances are deleted within a reasonable amount of time. These options prevent the indefinite retention of PII on the IBM COS System.

Chapter 6. Interface Modifications

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
- 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 updates for the 3.12 release have been referenced in the following documentation:

- CSO API Developer Guide
  - NEW section added for Compliance Enabled Vaults

- REST API Developer Guide
  - Updated section on Access Pool Management>Create an access pool Request parameters
  - Updated section on Storage Pool Management>Edit a storage pool Request parameters
  - Updated section on Administration>Configure Accesser API Request parameters
  - Added new section to Vault Management View a concentrated dispersal vault IDAs

API Changes 3.12

Only S3 is supported for operations on Protected Vaults/Objects and includes the following changes:
- Create Vault - 4 new parameters are added to the existing API: status and retention durations
- Edit Vault - 4 new parameters are added to the existing API: status, and retention durations
- Create Vault template - 4 new parameters are added to the existing API: status and retention durations
- Edit Vault Template - 4 new parameters are added to the existing API: status and retention durations
- Configure Vault Protection - new api to enable the feature.

COS-26638: In prior releases, the Storage Pool Capacity and Disk Report Manager REST API provided duplicate entries for any disk within a storage pool that is not in a “good” (pre-3.10.1) or “online” (3.10.1 or later) state. This issue has now been resolved.

COS-26512: The Compliance Report has been renamed to System Usage and Configuration Summary Report. The corresponding REST API endpoints have been updated to reflect this, as have any REST API fields that specify the Compliance Report.

Support retrieval of region code and billing class separately [1141]. APIs modified for this feature:
- Create Vault - Two parameters, region and storageClass are added to the request.
- Edit Vault - Two parameters, region and storageClass are added to the request.
- Create Vault From Template - Two parameters, region and storageClass are added to the request.

API Changes 3.13.3

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

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 3.13.5

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.

Chapter 7. Resolved Issues

Resolved issues in 3.13.6 Maintenance Release

Table 1. Resolved issues

Issue	Description
COS-39102	In prior releases, and when using Email Alert Rule Configuration in the Manager UI, notifications were not being sent when “Disk Events” was selected in the event category section. This issue has now been resolved.
COS-39511	In previous releases the “Past Disks” section of the disk usage graph found on the Monitor Device page of the Manager UI always used to display SCSI names. In the current release, this section shows the drive bay name if present, otherwise it will display the SCSI name. (edited)
COS-43036	Starting with release 3.13.4, the SNMP TRAP MIB document was missing traps related to BGP load balancing. This issue has now been addressed.
COS-43539	Fixed an issue where a malformed x-amz-credential header may encounter an exception during processing, causing the core process on the accesser appliance to restart.
COS-41421	Heavy multi-delete load will cause requests to return 503 status codes. This issue is fixed in this release.
COS-5202	The accuracy of the timing information within the “stat” access log field has been improved when errors are encountered.

Resolved issues in 3.13.5 September Maintenance Release

Table 2. Resolved issues

Issue	Description
COS-40989	Due to the need to provide more robust, manager backup file recovery, changes were introduced in 3.13.2 that increased the manager backup time by 4X (compared to pre-3.13.2) for systems with large DBs (> 20 GB), for example, those that have a substantial amount of historical statistics. In this release, optimizations have been introduced that reduce the manager backup time to 1.5X relative to pre-3.13.2 systems, while still greatly improving backup file recovery.
COS-37403	When upgrading storage pools to 3.12.4, Accesser devices may experience 500s while attempting to interact with their management vault because of “Unsupported vault type: object, format:” errors. This error will delay the upload of stats and access logs to the management vault. This issue has now been resolved.
COS-38134	In earlier releases, customers using web browsers with language settings other than English would have seen time zone abbreviations rendered using that language rather than English. The software will now ignore any language preference specified by the browser and always render time zone abbreviations using the common English syntax.
COS-42062	In prior releases, but subsequent to 3.13.4, after initiating a “Dispose” operation from the Manager UI, the Event Console indicates drive bay as ‘unknown.’ Once the operation completes, the next event shows the drive bay information correctly. This issue has now been resolved.
COS-41086	Manager restore may fail if management vault functionality was disabled prior to taking a backup. This issue has now been resolved.

Resolved issues in 3.13.5 Maintenance Release

Table 3. Resolved issues

Issue	Description
COS-41146	Increased the enforced limit for the maximum object size for a completed MPU from 5TB to 10TB to align with the maximum streaming object size.
COS-41088	In previous releases, in the Manager Automatic Report Emailing configuration, the initial setup of "Automatic Reporting Schedule" was ignored after clicking "Update." As a result, the Manager would not send scheduled reports via email. This issue has now been resolved.
COS-39142	In previous releases, when a vault is added/deleted from the system, gaps may occur in all vault usage graphs. Also, vault level incidents, storage pool level incidents, access pool level incidents, and storage pool state changes may be delayed by 60 seconds. This issue has now been resolved.
COS-40878	In previous releases, for systems with devices on an earlier release compared to the Manager, on the Monitor Device page of the Manager UI, the drive diagram displayed "object Object" as the reason for a drive in the Diagnostic state. This issue has now been resolved.
COS-40877	editAuthenticationMechanism API returns a 500 HTTP status code. This is now fixed to throw an appropriate error message to the user.
COS-36320	In prior releases but after 3.12.0, on occasion, after successful completion of a Manager restore operation, the UI displayed a connection refused error message. This issue has now been resolved.
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." The drive failure and migration of data is performed successfully. The messaging is improved in this release.
COS-30632	Device level API is not returning drive health value. This issue is fixed in this release.
COS-41776	The following access log entries are secondary entries that represent an internal operation and do not directly produce a response. As of this release, they no longer contain the response_length field: REST.COPY.OBJECT_GET, REST.COPY.PART_GET, BATCH.DELETE.OBJECT, REST.POST.OBJECT_RESTORE_GET .
COS-35148	Fixed an issue where “\r” is not included in the S3 listing response for objects that have “\r” in their name and is thereby causing Object deletion to fail when using output of listing for deletion.
COS-19350	When SNMP is enabled, each device exposes a sysObjectID (OID 1.3.6.1.2.1.1.2) attribute, which is used to uniquely identify a device on the network. In previous releases, this attribute was populated with a general purpose value (.1.3.6.1.4.1.8072.3.2.10) which was insufficient to determine whether a network device was an IBM COS device or determine what type of device it was (e.g. Slicestor device). This release addresses that limitation by introducing an IBM COS specific identifier for each appliance type. Each appliance will report the following values when querying the sysObjectID.0 attribute. Accesser device .1.3.6.1.4.1.28129.1.5.1 Manager device .1.3.6.1.4.1.28129.1.5.2 Slicestor device .1.3.6.1.4.1.28129.1.5.3

Resolved issues in 3.13.4 August Maintenance Release

Table 4. Resolved issues

Issue	Description
COS-42123	Removed the “Call Home” feature from the Manager UI for general availability use. It will be re-introduced in a future ClevOS release once the field trial phase has completed.

Table 4. Resolved issues (continued)

Issue	Description
COS-42159	Fixed an issue where attempts to add/remove legal holds or extend retention periods for protected objects which were written in previous releases (prior to 3.13.4) would fail with a HTTP 451 error.
COS-41549	Fixed an issue where listing operations occasionally ran into a hung task.

Resolved issues in 3.13.4 July Maintenance Release

Table 5. Resolved issues

Issue	Description
COS-40750	POST.CREDENTIALS operation failed with "Duplicate Content-Length" error.
COS-35118	Requests with a Transfer-Encoding: Chunked header fail with a 400: Bad Request error.
COS-37433	Fixed an issue where an S3 request to list the objects in the vault or container may encounter an HTTP 500 error when performing listings over a portion of the container namespace that is undergoing a heavy delete load.
COS-36238	Updated the behavior of the system to ignore the presence of the 'ibm-service-instance-id' header for operations for which this header is not required. Previously this would result in requests failing with a 403 response.
COS-36603	In previous releases, in a system with a service vault and a combination of standard and container vaults, new vaults created from a vault template in the Manager UI could be standard vaults when they should be container vaults. This issue has now been addressed.
COS-36470	In previous releases, on the Monitor Device page in the Manager UI, drive diagrams for storage device models IBM Cloud Object Storage 2584 and HPDM displayed empty bays as disabled, with no option to enable those bays. This issue has been corrected, allowing users to enable empty bays through the UI.
COS-34480	Prior to 3.13.2, in situations with a large number of vaults being created/deleted, the manager daemon on a device can run out of memory. This issue has now been resolved.
COS-36320	In prior releases but after 3.12.0, on occasion, after successful completion of a Manager restore operation, the UI displayed a connection refused error message. This issue has now been resolved.
COS-39634	Delete a container and re-create using the same container name was failing. This issue is addressed in this release.

Resolved issues in 3.13.4

Table 6. Resolved issues

Issue	Description
COS-35713	Improved handling on the accesser of slices that are queued and waiting to be sent to slow stores. We are now more efficient in ensuring that cancellation is effective in reclaiming resources and is appropriately targeting writes to stores that are slow or have large queues.
COS-38588	Error code for HTTP status code 507 should be reported properly.
COS-6803	For Slicestor® devices with multiple OS drives, degradation of OS drives does not affect the device's health on the Monitor device page.
COS-6490	If a manager appliance is imaged with a degraded RAID array, no event is presented to the user in the event console. In some cases this can cause no warnings to be shown about a potential problem.

Table 6. Resolved issues (continued)

Issue	Description
COS-15642	When upgrading devices that contain logical RAID drives, the Manager event console will show a drive offline event immediately followed by a drive online event for each physical drive that is part of a logical RAID drive.
COS-40438	PUT Object COPY fails with 400 if the object name contains '?'

Resolved issues in 3.13.3 June Maintenance Release

Table 7. Resolved issues

Issue	Description
COS-39537	Fixed an issue where object names with non-ASCII characters would not display properly in listing responses.

Resolved issues in 3.13.3

Table 8. Resolved issues

Issue	Description
COS-34106	The 's3-multi-delete' access log entry type has been removed. The information contained in this entry is redundant to the information contained in the access log entry for the originating request and the individual access log entries of request_type 'BATCH.DELETE.OBJECT' that are generated for the result of each individual delete action in a multi-delete request.
COS-35670	Enhanced the access log content to include the midstream_error field in cases where a PUT request fails mid-operation due to a client disconnect or server idle disconnect.

Resolved issues in 3.13.2

Table 9. Resolved issues

Issue	Description
COS-34106	The 's3-multi-delete' access log entry type has been removed. The information contained in this entry is redundant to the information contained in the access log entry for the originating request and the individual access log entries of request_type 'BATCH.DELETE.OBJECT' that are generated for the result of each individual delete action in a multi-delete request.
COS-35670	Enhanced the access log content to include the midstream_error field in cases where a PUT request fails mid-operation due to a client disconnect or server idle disconnect.
COS-33497	As a side effect-of a previous change in 3.9.1, additional content was added to the log content for s3 multi-delete results in the access log.

Resolved issues in 3.13.1 April Maintenance Release

Table 10. Resolved issues

Issue	Description
COS-31032	For the SL4540 hardware platforms, the popup dialog in the drive layout on the Monitor Device page of the Manager User Interface (UI) does not display the enclosure and bay information for a drive.

Table 10. Resolved issues (continued)

Issue	Description
COS-34419	For all appliances, the temperature readings are reversed for the current and maximum CPU temperatures in the Platform MIB: CLEVERSAFE-PLATFORM-MIB::csPfCPUTempNow.1 = Gauge32: 90 CLEVERSAFE-PLATFORM-MIB::csPfCPUTempMax.1 = Gauge32: 34
COS-33012	Corrected a typo in the field name of the 'control_throttle.writers_available_permits' report log entry.
COS-34104	The exported CSV content for the Failed FRU Report, available through the Maintenance page on the Manager User Interface (UI), does not capture failed virtual disks.
COS-35731	Added support for the CacheControl header across all APIs. The value of this header will now be stored in the object's metadata and returned in the result of a subsequent GET or HEAD on the object.
COS-36788	Fixed an issue where a low-probability race condition may result in an exception being encountered during listing, causing a restart of the core process on the Accesser appliance.
COS-37297	Fixed an issue where delimiter listing request was taking excessive time to complete.

Resolved issues in 3.13.1

Table 11. Resolved issues

Issue	Description
COS-33012	Corrected a typo in the field name of the 'control_throttle.writers_available_permits' report log entry.
COS-33565	Resolved an issue where SNMP traps are not generated for the following events: rebuilder agent/mirror synching hung, data reallocation paused/halted, token expiration failing to refresh.
COS-33565	In releases prior to 3.13.1, SNMP traps were not generated for the following events: • rebuilder agent/mirror synching hung • data reallocation paused/halted • token expiration failing to refresh
CSO-34104	The exported CSV content for the Failed FRU Report, available through the Maintenance page on the Manager User Interface (UI), does not capture failed virtual disks.

Resolved issues in 3.13.0

Table 12. Resolved issues

Issue	Description
COS-28326	The maximum supported fanout copy count has been decreased from 10,000 to 1,000.
COS-31032	For the SL4540 hardware platforms, the popup dialog in the drive layout on the Monitor Device page of the Manager User Interface (UI) does not display the enclosure and bay information for a drive. This issue has been fixed in this release

Resolved issues in 3.12.4 July Maintenance Release

Table 13. Resolved issues

Issue	Description
41510	Delete markers for versioned objects should not expect encryption keys. This issue is addressed in this release.

Resolved issues in 3.12.4 June Maintenance Release

Table 14. Resolved issues

Issue	Description
14450	Indexes that cannot be read will return zero for size in DMS metrics collection.
COS-39150	For storage pools that have a high number of vaults (>100), there is degradation in the performance of the scanning process used to determine what needs to be scanned to find data that may need to be rebuilt. As a result, this may slow the rate of scanning and rebuilding across the drives within a storage pool. Exposure to this issue is limited to ClevOS™ 3.12.4.72 and 3.13.3.59 releases. This issue is addressed in this release. If the system configuration meets the above conditions, the IBM COS support team should be contacted to assess any potential impact.
COS-39320	Fixed an issue where an HTTP 503 response from a remote endpoint with vault proxy configured would result in a HTTP 500 error response being returned.
COS-39045	In earlier releases, and on the Monitor Device page in the Manager UI, the Apollo 4510 (HP ProLiant XL450 Gen 9 Server) drive diagram was incorrectly rendered. This issue has been addressed.
COS-37403	When management vaults aren't deployed to Accesser pools, an unsupported vault type error 13 can be seen during upgrade from 3.12 to 3.13 releases. This issue is addressed in this release.

Resolved issues in 3.12.4 May Maintenance Release

Table 15. Resolved issues

Issue	Description
COS-37407	Vault deletion is not picking up increased reserved scheduler permit configuration changes.
COS-37563	A slow memory leak was introduced in 3.12.2 which affects very stable systems that don't drop connections to external devices very often. The leak is only present under certain race conditions and when heavily impacted by the leak, the core process will perform garbage collection more often than it otherwise would. Race conditions in the code were fixed so as to not leak old regions.
COS-38383	Fixed an issue where heavy rebuild delete activity may cause rebuilder to report that it is not making progress.
COS-37557	Clients observed a bunch of client disconnects due to request timeouts, for some of the stores. The root cause was that the scanning rate did not remain stable during the entire scanning cycle, and we observed huge spikes in it, especially at the beginning of the cycle. This resulted in a large number of listing requests, and affected the IO.
COS-39105	Fixed an issue where the Slicestore device may enter a potentially inconsistent state upon upgrading from a pre-3.12.x release to a post-3.12.x release.
COS-38405	Fixed an issue where conditional request headers (such as If-Modified-Since), were not properly returning a 304 - Not Modified response where the provided timestamp matches the existing object timestamp.

Resolved issues in 3.12.4 April Maintenance Release

Table 16. Resolved issues

Issue	Description
COS-32649	Fixed an issue with the manager application not starting up properly when certain fields of a multi-node device are not set properly.
COS-33227	In a multi-stripe system, the namespace boundaries between stripes are calculated in such a way that the boundaries between stripes is not the same for each pillar. This means that there are ranges of the namespace that may be entirely within the stripe for one index in a pillar, but spans stripes for another index. When doing reverse rebuild listing where a range crosses a stripe boundary, the client will select the wrong device to send the request to, resulting in a empty listing result.
COS-32383	Fixed an issue where a timing issue or race condition where, upon first establishing a connection between accesser and slicestore devices following a new device registration, OS drive replacement, or device certificate update, the accesser device may not be able to authenticate to the slicestore device.
COS-32492	Fixed an issue where a core process restart may be triggered due to a race condition that may exist while performing reallocation.

Resolved issues in 3.12.4 March Maintenance Release

Table 17. Resolved issues

Issue	Description
COS-34232	Resolved an issue that might result in inconsistent revisions of slices for an index node being persisted under heavy load. Affects any environment that uses the distributed index, including the name index, data migration services, globally prioritized rebuilder, and multi part uploads. Inconsistent slices are more likely to produce availability or reliability issues in configurations where the difference between width, and write threshold, is larger than the difference between write threshold and threshold.
COS-34143	Resolved an issue that was causing increased memory pressure on Slicestor devices when heavy slice listing operations were being performed. This was particularly prominent when utilizing Vault Mirrors or Data Migration Services, but could also be seen in heavy rebuild scenarios on storage pool sets with a large number of Slicestor devices.
COS-35277	Resolved an issue with Slicestors going into inconsistent state after upgrade.
COS-15399	Following an accesser OS drive replacement, a new device certificate must be generated for this device, and a whitelist containing this certificate information must be distributed to the other devices in the system which this device will attempt to communicate with.
COS-32383	Upon first establishing a connection between Accesser and Slicestor devices following a new device registration, OS drive replacement, or device certificate update, the Accesser device might not be able to authenticate to the Slicestor device due to a timing issue or race condition.
COS-34886	Requests sent through the SOH API that also include CORS headers ("Origin" and "Host") encounter an exception and cause the core process on the Accesser device to restart.

Resolved issues in 3.12.4

Table 18. Resolved issues

Issue	Description
COS-32649	Fixed an issue with manager startup handling of chassis ID in multi node chassis.

Resolved issues in 3.12.3

Table 19. Resolved issues

Issue	Description
COS-31605	In previous releases, when using Concentrated Dispersal with an older version of Firefox (before version 47), any creation of mirrored vaults can fail. This issue is resolved; however, users should upgrade to the latest version of Firefox.
COS-30962	In the Device Statistic API, service state and uptime metrics were unnecessarily included in the output, and have been removed.
COS-31470	In previous releases, if a set replacement or set removal was performed before initiating a device replacement activity, the set numbering displayed on pages that are associated with the device replacement flow is incorrect. This issue has been resolved.
COS-31449	Addressed an issue that is related to deletion of vault alias during migration.
COS-30097	500 Errors for GET.SERVICE request while PUT.VAULT is in process.
COS-2753	Locality settings with high stress causes disks to be quarantined because of timeouts with reason code 5.

Resolved issues in 3.12.2 January Maintenance Release

Table 20. Resolved issues

Issue	Description
COS-27973	Addressed an issue where Slicestors are exhibiting high cpu usage and causing dlm process to be restarted.
COS-30612	Addressed an issue where the server returns a 403 when a bucket is created through S3 and using the HMAC account/keys.
COS-30999	Fixed an issue with Manager returning internal error when the devices are approved in bulk.
COS-31227	Fixed an issue when adding a device on a storage pool with missing Slicestors.
COS-31482	Robust handling of Accesser stability in an error scenario.

Resolved issues in 3.12.2

Table 21. Resolved issues

Issue	Description
COS-28338	Updated access control permissions enforcement for Compliance Enabled Vault API extensions. PUT/GET legal holds require WRITE_ACL/READ_ACL permission and PUT/GET Bucket Protection operations now bucket owner permission after this fix.
COS-28629	In certain conditions, Execution of the storagectl commands (list, list all, info, and history) through the manager troubleshooting console will timeout, particularly when a significant amount of information is present, resulting in the following message to be displayed on the user interface: “The command is taking too long to execute .” This issue is fixed in this release.
COS-27795	Logging updates for token refresh failures.
COS-28787	In earlier releases, when operating in container mode with a service vault, the Create Vault link for each vault template on the “Template Management” page of the Manager user interface did not initiate the “Create Vault” process. This issue has now been resolved.
COS-28790	In release 3.10.2 and after, the CSV content associated with the Vault Summary Report on the Manager user interface did not contain the SSE-C column. The issue has been resolved in this release.
COS-28572	Fixed an issue where Manager complains about 2 drives missing for Lenovo System x3650.

Table 21. Resolved issues (continued)

Issue	Description
COS-29667	Fixed an issue with COS access logs reporting storage_account_id .
COS-22881	When performing a form-based upload using a POST request, if the client disconnects from the Accesser device before completing the request, the error is incorrectly logged as an HTTP 500 error and generates an event in the Manager UI event console.
COS-28179	Who to contact in the event of a scenario causing a large number of destroyed data-slices, such as multiple Slicestore reimage, site destruction, site reimage, or large scale long time scale outage.

Chapter 8. Known issues

Table 22. Known issues

Issue	Failing Condition	Disposition
COS-12691	Instability has been observed when running two 40 Gbit links in LACP mode.	Do not use LACP aggregated links with 40 Gbit Intel Network cards.
COS-11201	In the Event Console of the Manager User Interface, the event details section for failing disk migration events contains a parameter 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) may 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 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 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-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).	Should this occur when migrating a VMware virtual device using vMotion, a cold migration should be used instead such that the virtual machine is offline during the migration.
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. In some cases however, this process may 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-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.	Contact IBM® customer support to help correct the situation.

Table 22. Known issues (continued)

Issue	Failing Condition	Disposition
COS-7488	When performing a storage pool set removal, it is possible that once the reallocation has finished for an source Slicestor device, it may show some small amount of data still present.	No action is required. Once the set removal has completed, all slices will 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 may occur during normal usage of the system.
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 may 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 related to communicating with an Amazon S3 endpoint. The version of the AWS SDK used to communicate to Amazon will default 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 will work as expected. However, they may not be consistent with the current storage pool capacity. For example, a vault quota may 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 a HTTP 400 - Bad Request. Instead, the object is being successfully created but with empty content.	This will be fixed in a future release.

Table 22. Known issues (continued)

Issue	Failing Condition	Disposition
COS-29681	When using the Microsoft IE9 web browser, certain Manager user interface elements like the left navigation tree and the vault capacity bar charts on the Monitor Vault page may 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.
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" may show incorrect size values.	The audit message will be corrected in a subsequent release.
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."	The drive failure and migration of data is performed successfully. The drive failure and migration of data is performed successfully. The messaging will be improved in a subsequent release.
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 will be resolved in a subsequent release.
COS-41309	Cloud DVR use cases are not recommended with this release.	Contact IBM Customer Support for additional assistance.

Upgrading and Installation

Table 23. 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 (e.g. OS drives) will be reported as newly discovered in the Manager event console.	No action is required.

Container

Table 24. 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 will fail 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.

Table 24. Container (continued)

Issue	Failing Condition	Disposition
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 25. Alerting and reporting

Issue	Failing Condition	Disposition
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.	Contact IBM Customer Support to confirm and correct the false incident.

System Behavior

Table 26. 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 will open 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 27. 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 28. Data evacuation

Issue	Failing Condition	Disposition
	Nothing to report.	

System Configuration

Table 29. System configuration

Issue	Failing Condition	Disposition
	Nothing to report.	

Deleting objects

Table 30. 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 31. 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.

Table 31. Manager Web Interface (continued)

Issue	Failing Condition	Disposition
COS-41545	As part of System NTP Configuration in the Manager UI, 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.	Enter a space separated list of NTP servers in the External NTP Servers field.

Vaults

Table 32. Vaults

Issue	Failing Condition	Disposition
	Nothing to report	

Vault Mirrors

Table 33. 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 34. 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 9. Supported Hardware Platforms

IBM Cloud Object Storage Appliances

Table 35. 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 36. 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 Manager™ 2105	3401/3403	M00	3.8.1
IBM COS Manager™ 3105	3401/3403	M01	3.8.1
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

Note: ⌂ Requires RPQ

Hewlett Packard

Table 37. Minimum Version of ClevOS Compatible with Hewlett Packard 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

Table 37. Minimum Version of ClevOS Compatible with Hewlett Packard Hardware (continued)

Appliance	Model	Minimum ClevOS
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	3.6.0
Slicestor® Device	Apollo 4510	3.6.0
Slicestor® Device	Apollo 4530	3.6.0

Seagate

Table 38. 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 39. 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 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 40. Minimum Version of ClevOS Compatible with Dell Hardware

Appliance	Model	Minimum ClevOS
Dell Slicestor® Device	DSS 7000	3.10.1
Dell Slicestor® Device	R740xd	3.13.4

Lenovo

Table 41. Minimum Version of ClevOS Compatible with Lenovo Hardware

Appliance	Model	Minimum ClevOS
Lenovo Manager Appliance	X3550 M5	3.10.1

Table 41. Minimum Version of ClevOS Compatible with Lenovo Hardware (continued)

Appliance	Model	Minimum ClevOS
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 42. 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 10. 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 43. Broadcom Hardware and Firmware Incompatibility with ClevOS

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

Hewlett Packard

Table 44. HP Hardware and Firmware Incompatibility with ClevOS

Type	Model	Firmware affected
RAID Controller	HP-SL4540 Smart Array	6.64

IBM Cloud Object Storage Appliances

Table 45. 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 46. Seagate Hardware and Firmware Incompatibility with ClevOS

Type	Model	Firmware affected
HDD	Seagate ST1000NM0033-9ZM173	SN04

Supermicro

Table 47. 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