IBM Cloud Object Storage System
Version 3.10.2 August 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 3.10.2

S3 SSE - C (Server Side Encryption with Customer Keys) [391]

The Server Side Encryption with Customer Provided Keys (SSE-C) feature add support for API headers to the existing S3 storage API that give customers the abilities to use their own keys to encrypt objects server side over https. This feature enables IBM-COS to manage the encryption/decryption of objects without the customer having to do so prior to storing/retrieving the objects. IBM-COS will use the customer provided key to apply AES-256 encryption to the data and the customer key is removed from memory. The customer is responsible for all stages of key lifecycle management and for any key rotation scenarios. This can be accomplished with functionality offered in this feature where the customer needs to use GET and PUT operations or copy operation with new keys. This feature is agnostic of whether the system is in container or vault modes.

Refer to the Manager REST API and Cloud Storage Object API developer guide for further details.

Note:

- IBM-COS will reject any SSE-C requests made over HTTP.
- The ETag in the response for an SSE-C request is NOT the MD5 of the object data stored.
- Customer is responsible for maintaining a mapping between the key that is used to encrypt each object and the corresponding object name or id. IBM-COS does not store the key that is provided in SSE-C requests.
- Customer is responsible all aspects of key storage on the client side including key rotation.
- If the key is lost, GET operations for an SSE-C operation fail without the customer key and the stored object is lost.

Supported:

- PUT, GET, and HEAD operations with SSE-C headers.
- POST
- Object PUT-COPY
- Corresponding Response headers with SSE-C specific fields.
- Encryption / Decryption of objects for the above supported operations.
- Manager UI changes to support enablement SSE-C on vault(s).
- Error handling of missing and malformed SSE-C header(s).
- Encryption / Decryption of user attributes that are provided with requests.
- Multi-part Upload
- Vault Proxy
- Pre-signed URLs
- Versioning

Not Supported:

- Vault Mirroring
- Vault Migration

SSE-C impacted APIs:

- createVault
- editVault
- createVaultTemplate

- editVaultTemplate

Each of the above to introduce the 'ssecEnabled' flag to enable/disable the property.

- viewSystem
- viewSystemConfiguration

Each serialized vault object now has a 'ssecEnabled' flag.

Object Overwrite Information Added to Access Log [1091]

This feature introduces the fields previous_last_modified and previous_object_length into the access log for container mode only when an object's content is overwritten. previous_last_modified represents the last time the object's content was modified prior to the current request. previous_object_length represents the object's content length prior to the current request.

Add Per Vault TB days in dsNet Manager UI, API & Reports[716]

This feature introduces a new report to provide vault usage metrics in TB days for a given date range for each vault. The report includes all the vaults (standard, service, container, and management) on the system irrespective of the vault purpose. Vault usage metrics can be used for billing purposes. Refer to the Manager REST API and Cloud Storage Object API developer guide for further details.

A new API method vaultUsageReport.adm has been added .

An existing API method organizationPoolUsageReport.adm has been updated to modify the input property "scheduleMonthly" to "month."

Customer Provided Certificates for Access Pools[1064]

This feature allows customers to configure a single certificate chain for use on the HTTPS service across all devices in an Access Pool, rather than requiring a unique certificate to be installed on each Accesser device. This greatly reduces the cost and maintenance effort that is associated with purchasing certificates from a third-party certificate authority, especially for larger-sized Access Pools. This new certificate is only used for external user-facing HTTPS, not for internal device-to-device communication. If new devices are brought online and added to the Access Pool, they are automatically configured to use the same certificate chain as the existing devices.

The existing Manager REST API methods Create Access Pool and Edit Access Pool have been updated to include input parameters for "privateKeyPem" and "certificatePem." See the Manager REST API Guide for more details.

Chapter 2. Interface Modifications

API updates for the 3.10.2 release have been referenced in the following documentation:

- Manager REST API
  - Updated Account Management Chapter
  - Updated Cabinet Management Chapter
  - Updated Device Management Chapter
  - Updated Access Pool Management Chapter
  - Updated Storage Pool Management Chapter
  - Updated SMC Pool Management Chapter
  - Updated Mirror Management Chapter
  - Updated Vault Management Chapter
  - Updated Organization Management Chapter
  - Updated Reports Chapter
  - Updated Administration Chapter
- CSO API Developer Guide- Combined sections 3 and 4.
  - Merged sections 3 and 4 into one titled REST API Reference

API Changes 3.10.2

COS-22694: In previous releases, if you attempt to perform a multipart upload and upload a part while specifying customer user metadata attributes, the request will succeed but the user metadata headers will be ignored. Instead the request should be rejected with a 400 - Bad Request error indicating that metadata cannot be specified in this context. This fix has been incorporated into the current release.

COS-23644: In previous releases, if you attempt a request signed with AWS Signature Version 4 containing a header with an empty value, the request fails with a 403 Forbidden error.

Starting with 3.10.2, when validating requests signed with AWS Signature Version 4, an empty string value for headers with empty values is used rather than failing the request due to a missing header.

COS-23687: In previous releases, AWS Signature Version 4 Chunked Upload requests that also use Transfer-Encoding: chunked and do not provide a Content-Length header fail with a 403: Forbidden error.

Starting with 3.10.2, the accesser no longer requires a Content-Length header if a AWS Signature Version 4 Chunked Upload request is sent with Transfer-Encoding: chunked.

Vault Migration: The containerMode key was removed from the View System and View System Configuration API responses. Any scripts leveraging this key will have to be updated. In the View System and View System Configuration API responses, the vaultPurpose associated with each vault within the system can have one of the following values: standard, management, service, container. The presence of a vaultPurpose set to service or container indicates the system can support container vaults.

Chapter 3. Resolved Issues

Resolved issues in 3.10.2 August Maintenance Release

Table 1. Resolved issues

Issue	Description
COS-41510	Fixed an issue when using SSE-C on a versioning enabled vault where the deletion of an encrypted object, followed by a subsequent read, would result in a HTTP 400 error instead of the appropriate HTTP 404 response.

Resolved issues in 3.10.2 June Maintenance Release

Table 2. Resolved issues

Issue	Description
COS-35983	Resolved an issue on Slicestor devices where the DLM service may crash due to excessive memory use when resetting failing drives.
COS-38222	Resolved an issue on Slicestor devices that was causing intermittent hangs in subsystems that perform drive listing request.
COS-33211	Resolved an issue where dsnet-core crashes due to sanity check failure on disk in migration.
COS-38183	Resolved an issue where Post upgrade, a single Slicestor is in Inconsistent State, with core not running due to a DSD.
COS-36186	Resolved an issue where all Drives in DIAG state after clean shutdown of the DLM process.
COS-23413	Resolved an issue where Slicestor appliance is reporting 2 drives with the same SN in the same bay slot with different states.

Resolved issues in 3.10.2 April Maintenance Release

Table 3. Resolved issues

Issue	Description
COS-34886	Fixed an issue where requests being sent using the SOH API that also included CORS headers ('Origin' and 'Host') were encountering an exception and causing the core process on the accesser device to restart.
COS-29973	Resolved an issue with Slicestor devices where an upgrade would potentially fail due to inconsistencies on the data drive filesystems.
COS-28616	Resolved an issue with Slicestor devices where an upgrade would potentially fail due to bad handling of data drives that had been removed and reinserted into the device sometime in the past.
COS-32465	Resolved an issue with Slicestor devices where an upgrade would potentially fail due to data drives not being correctly recognized during device startup.
COS-34323	Resolved an issue with Slicestor devices where an upgrade would potentially fail due to data drives being erroneously quarantined due to race conditions when initializing multiple drives.

Resolved issues in 3.10.2 February Maintenance Release

Table 4. Resolved issues

Issue	Description
COS-27605	Resolved an issue where an upgrade of certain Slicestor appliances, data drives could erroneously transition to a diagnostic or offline state, which prevented them from being used by the device.
COS-28356	Resolved several issues that were causing temporary Slicestor device service outages due to increased memory pressure.
COS-28341	Resolved several issues where multiple hard drives in Slicestor devices were being reported in the same drive bay, which in some cases would cause service outage on the Slicestor.
COS-25718	Resolved several issues that were causing temporary service outages and upgrade failures due to process crashes.
COS-31475	Resolved an issue that was preventing hard drive Advanced Power Management functionality from being disabled on Slicestor device data drives.
COS-28665	Resolved an issue where the dlm process was erroneously reported as not running when a device was under extreme workload and stress.
COS-25365	Resolved an issue where upon removal of a Slicestor device data drive, the drive was still being reported as present with an invalid drive bay number.
COS-29673	Resolved an issue where an upgrade of a Slicestor device could fail due to slow initialization of data drives.
COS-31236	Resolved several issues that were preventing Slicestor appliance data drives from being properly handled when quarantined, failed, or removed.

Resolved issues in 3.10.2 December Maintenance Release

Table 5. Resolved issues

Issue	Description
COS-28665	Manager UI shows dlm process is frequently bouncing on multiple Slicestors.

Resolved issues in 3.10.2 November Maintenance Release

Table 6. Resolved issues

Issue	Description
COS-28097	In releases 3.10.0 and later, for the Apollo 4510 (1-node configuration), if bays greater than 60 are used, the Manager disk diagram on the Monitor Device page will display incorrectly. This issue is now resolved.
COS-28454	Cancellable calculation defect with Storage Deployed with Missing IBM COS Slicestor®.

Resolved issues in 3.10.2 October Maintenance Release

Table 7. Resolved issues

Issue	Description
COS-26682	Performing a fanout delete all operation during compaction causes data to be written to incorrect offset within the bucket file, which could then manifest as dropped bin files.
COS-28042	Fixed an issue with Accesser dsnet-core process restarting, due to a NoSuchElementException caused when listing with delimiter returns an entry that matches the name of a deleted object.

Table 7. Resolved issues (continued)

Issue	Description
COS-27960	Fixed an issue with decryption of encrypted object as part of upload part copy.

Resolved issues in 3.10.2 September Maintenance Release

Table 8. Resolved issues

Issue	Description
COS-23832	Selective debug logging is now enabled by default at a selection rate of 0.001 (i.e. 1/1000 requests).
COS-24639	API call fails "Internal Server Error" on editAccountAccessKey.adm.
COS-24169	GARP request is not issued when switching over physical interface in active/standby bond configuration.
COS-14745	Addressed issue with deletes and rebuilder work flow.
COS-23478	Appliance API fails to retrieve disk controller information due to unexpected format.
COS-24651	Core process startup issue when appliance library returns integers for bays.
COS-25230	HeadersNotSigned error when X-Amz-Content-SHA256 is not signed.
COS-25510	If a multipart Complete Upload and Abort Upload request are submitted concurrently for the same upload ID, it is possible for both requests to succeed, leaving the completed object in an inconsistent state. Subsequent GET requests on the complete object may return HTTP 500 errors.
COS-24768	Device API statistics call taking too long to return.
COS-25581	Slicestors coming up into INCONSISTENT_STATE after upgrade.
COS-25472	If an Abort Multipart Upload request is submitted while an Upload Part request is in flight, the Upload Part request may fail with a HTTP 500 error.
COS-25390	Incompatible controller types when mirroring between vaults on different formats causing 500 Error
COS-26114	The handling of a PUT Object Copy operation for directive due to customer provided keys.

Resolved issues in 3.10.2

Table 9. Resolved issues

Issue	Description
22467	When a Slicestor device has a slow or impaired disk, IO operations to that store can become queued. Index delegation requests can also be queued, causing elevated request latencies for end-user operations.
18646	It was observed that under heavy IO, elevated message acknowledgment times can be seen between an Accesser device and the Slicestor devices that are associated with an individual stripe. Intent operations can now be distributed to multiple stripes.
23078	Index split operations are performed in the background to maintain proper balance in the index structure. Update operations as part of a split could be improperly sequenced, such that failures might leave the index in an internally inconsistent state. This might result in 500 errors for insert, removal, or listing operations for this portion of the index. The fix ensures proper sequencing of the internal updates such that failed updates will always result in a consistent internal structure.

Table 9. Resolved issues (continued)

Issue	Description
22694	If you attempt to perform a multipart upload and upload a part while specifying customer user metadata attributes, the request succeeds but the user metadata headers are ignored. Instead, the request should be rejected with a 400 - Bad Request error indicating that metadata cannot be specified in this context.
COS-16642	Manager REST API and CSV output changes were made due to renaming of the header from 'suspendReason' to 'reason' and 'Suspend Reason' to 'Reason', respectively. These changes impact the contents of the Storage Pool Capacity and Disk Report and the Disk Drive and Device Report.
COS-14360	Strict enforcement of the maximum object size has been added to the product. The maximum object size that can be uploaded is 5TB. Upload requests for objects greater than this size will be rejected. Chunked-encoding uploads are no longer supported, and an explicit Content-Length header is required for all upload requests.
COS-16461	The System Advanced Configuration page in the Manager User Interface (UI) includes an "Existing Detailed Configuration Rules" section which lists existing advanced configuration settings on individual devices, storage pools, or access pools. However, File Server Pools and SMC Pool configuration settings do not appear in this section.
COS-22305	When using the List Vaults API with a hard quota for a vault and a merged storage pool, the quota is enforced at too low of a number, resulting in "over quota" errors being generated incorrectly. This does not impact soft quotas or expand storage pool functionality.
COS-14232	When performing large volumes of delete requests or deletes of large objects, either through individual delete requests or multi-delete operations, it is possible to consume large amounts of memory resources performing the background deletion operations, leading to resource exhaustion and 503 errors.
COS-23644	If a request signed with AWS Signature Version 4 contains a header with an empty value, the request will fail with a 403 Forbidden error.
COS-17217	Restart time for dsnet-core has been optimized.
COS-23687	AWS Signature Version 4 Chunked Upload requests that also use Transfer-Encoding: chunked and do not provide a Content-Length header fail with a 403: Forbidden error.

Chapter 4. Known issues

Table 10. Known issues

Issue	Failing Condition	Disposition
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.	Repair the OS drive or contact IBM® Customer Support for more information.
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-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.	A core process restart of the Slicestore reporting the authorization error. This will be addressed in a future release.
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.

Table 10. Known issues (continued)

Issue	Failing Condition	Disposition
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.
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-23406	If a client disconnects during the processing of a PUT request, a 200 response code might be logged to the status field of the HTTP access.log entry.	This only impacts the status code written to access.log. Avoid premature client disconnect during PUT operations.
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.	This will be addressed in a future release.
COS-16723	If a request is authenticated through AWS Signature V4, but a required header (for example, Host header) is missing, the Accesser device attempts to perform the requested operation anonymously instead of immediately failing the request with a 403 error.	Ensure that all authentication requests are properly formed. This will be addressed in a future release.
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-22963	When a slicestore device is unavailable, the core software on the accesser will cache this error state for a period of time, and will periodically attempt to connect to the store to determine if it has come back online. During these periodic connection attempts, other IO operations such as delegated index operations can be queued to this store, causing delays in request processing until the connection timeout is reached.	This will be addressed in a future release.
COS-23443	After performing a device replacement, the map of devices used to delegate index operations is not automatically updated to include the new device. As a result, index delegation operations will continue to be attempted to the old device (and will fast-fail), and the new device will not receive any delegated index operations.	This will be addressed in a future release.

Table 10. Known issues (continued)

Issue	Failing Condition	Disposition
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-23603	When a vault has both index disabled and recovery listing disabled, all attempts to perform listing requests will fail with an error. During the processing of these requests, a small amount of internal resources are leaked for each request. If many listing requests are performed in this configuration, it can lead to an out of memory condition and a core process restart.	This will be fixed in a future release.
COS-24148	Starting with release 3.10.1, a change was made to enable selective debug logging at a low rate by default. Selective logging rate will take precedence over selection frequency unless it is explicitly overridden to a selection rate of 0.0.	If a specific selection frequency is desired, the selection rate must be explicitly set to 0.0 to override the default selection rate in order for the selected frequency to take effect. Solution: This will be addressed in a future release.

Upgrading and Installation

Table 11. 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.
627	When installing ClevOS using a physical or virtual CD drive, the appliance might reboot or hang while booting.	Use a USB storage device to perform the installation.
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.
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.	No action is necessary. These events are simply representative of a transition phase of the RAID drives during the startup sequence and will be removed in a future release.
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 IBM 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.

Table 11. Upgrading and Installation (continued)

Issue	Failing Condition	Disposition
COS-9465	When installing ClevOS using a physical or virtual CD drive, the appliance might reboot or hang while booting.	Use a USB storage device to perform the installation.
COS-22994	In a system with a Manager device on release 3.10.1 or greater, and containing SMC devices, any Slicestor devices or Accesser devices on a release lower than 3.10.1 will not be able to communicate with the Manager.	Upgrade any Slicestor devices or Accesser devices on a release lower than 3.10.1 to the same release as the Manager.

Container

Table 12. 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-5390	The product does not currently support guaranteed delivery of access log or usage log entries to an end consumer.	Contact IBM Customer Support for more information.
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.
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 13. Alerting and reporting

Issue	Failing Condition	Disposition
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.
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.	Repair the RAID array by replacing the failing drive.

System Behavior

Table 14. System behavior

Issue	Failing Condition	Disposition
COS-5539	If a storage account is deleted and re-created with the same name, usage updates that are associated with the previous account might be applied to the new account.	Preventive Action: Always create accounts with unique IDs. Solution: Accounts will have an extra UUID to uniquely identify accounts, and usage updates will only be applied when the UUID matches the expected value. This change will be made in a future release.
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
2753	Under certain circumstances involving a combination of high concurrency (100 s to 1000 s of threads) and large object uploads (GB and larger), it is possible that multiple Slicestor appliances might experience disks being quarantined due to IO timeouts simultaneously.	This is a direct consequence of the workload being too high for the system and is likely to occur under certain test conditions but is much less likely to occur in a production environment. If this occurs, resume the disks and resume IO but reduce the workload on the system.
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 15. Storage pools

Issue	Failing Condition	Disposition
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.
COS-16664	For the "Storage Pool Capacity and Disk Report" accessed through the Maintenance tab of the Manager User Interface (UI), sorting for drive category columns do not work with the Safari browser.	Use an alternative browser, such as Chrome or Firefox.

Data Evacuation

Table 16. Data evacuation

Issue	Failing Condition	Disposition
	Nothing to report.	

System Configuration

Table 17. System configuration

Issue	Failing Condition	Disposition
	Nothing to report.	

Deleting objects

Table 18. 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 19. 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 20. Vaults

Issue	Failing Condition	Disposition
	Nothing to report	

Vault Mirrors

Table 21. Vault mirrors

Issue	Failing Condition	Disposition
10788	If an extreme network bandwidth imbalance exists between two sites in a mirrored vault configuration, and total load on the system exceeds the capacity of the slower site, traffic to both sites might experience a "sawtooth" pattern with alternating periods of high and low throughput. Additionally, pending writes to the slower site prevent writes to the faster site from proceeding. This occurs even if synchronous write is disabled.	During normal operation, disabling synchronous write allows requests to return to a user as soon as the fastest site returns. Reducing average throughput demand over time to be lower than the throughput capacity of the slower site will remove the "sawtooth" IO pattern and will allow bursts of IO to occur at the speed of the fastest site.
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 22. Vault migration

Issue	Failing Condition	Disposition
14450	In cases where the target vault of an active vault migration goes below threshold or becomes unavailable, the migration progress bar displayed in the manager might erroneously jump to 100% completed. In this condition, the migration will still be active, and any unmigrated objects will still be migrated.	The migration completion event in the manager will only trigger once the migration has fully completed, irrespective of the status reported in the progress bar. Therefore, the completion of a migration should be judged by the migration completion event in the manager.
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.	

Native File

Table 23. Native File

Issue	Failing Condition	Disposition
COS-5896	File Accesser devices only support hardware Accesser devices. Docker Accesser installations are not supported.	Deploy F5100 devices for use only with physical Accesser devices.
COS-6851	Using Filesystem or Share names with capital letters might prevent some S3 clients from accessing content properly by using the File Accesser device REST API.	Create Filesystems and Shares by using only lower case letters or avoid use of S3 clients that force lowercase referencing of bucket names.
COS-7497	When performing large file writes in excess of 1TB through the NFS gateway appliance, the write operation will fail to complete and return an error.	Avoid writing files in excess of 1TB, and break up large files into multiple smaller files.
COS-7898	An abrupt shutdown of a File Accesser device can cause issues with the storage database (Cassandra) upon restart.	Contact IBM Customer Support and run "nodetool repair" on the effected device. Use a graceful shutdown of a File Accesser device whenever possible.
COS-10195	Extended Characters in filename do not convert properly between windows and linux clients.	Do not set character encoding from default (UTF-8). Transformations may not work properly.
COS-7783	In process I/O may fail in the event of any File Accesser device going off line if that File Accesser is receiving a metadata update at the time of the outage.	Resend of failed data write.

Chapter 5. Supported Hardware Platforms

IBM Cloud Object Storage Appliances

Table 24. 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 25. 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	3401/3403	S03	3.8.1
IBM COS Slicestor®2212A	3401/3403	S10	3.10.0

Note: ⌂ Requires RPQ

Hewlett Packard

Table 26. 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
Accesser® Device	DL360P Gen8	3.2.1

Table 26. Minimum Version of ClevOS Compatible with Hewlett Packard Hardware (continued)

Appliance	Model	Minimum ClevOS
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 27. 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 28. Minimum Version of ClevOS Compatible with Cisco Hardware

Appliance	Model	Minimum ClevOS
Cisco Slicestor® Device	UCS C3260	3.7.4

Dell

Table 29. Minimum Version of ClevOS Compatible with Dell Hardware

Appliance	Model	Minimum ClevOS
Dell Slicestor® Device	DSS 7000	3.10.1

Lenovo

Table 30. 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

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