IBM Cloud Object Storage System

Version 3.12.0 April 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 3.12.0

Compliance Enabled Vault (CEV) [77]

CEV capability can be enabled only after all devices are upgraded to 3.12. Please refer to our third-party assessment letter from Cohasset Associates that speaks to this features' ability to meet the requirements of SEC 17a-4(f).

The CEV Feature introduces mechanisms whereby objects that are stored in IBM COS Vaults can have associated protection configuration, and these protected objects cannot be deleted until the protection configuration allows for the deletion.

The Protection level can be defined for a vault and can have one of two settings: Vaults with the protection level set to compliance are defined as Compliance Enabled Vaults (CEV) and objects that are stored in a CEV have a protection configuration that determine when such an object can be deleted.

IBM COS as the archive storage element is responsible for the following:

- Enforcing Data Retention
- Enforcing Security Boundaries
- Support auditing capability through the access logs on devices. It is the user's responsibility to archive the access logs for future use.

Note: Protection functionality is configurable in the Cloud Object Storage (COS) Manager UI, COS REST API, or S3 API.

NOT Supported for CEV:

- Range-Writes are prevented
- Object Replication/ Vault Mirroring
- Vault Migration
- Proxy support - Not supported for Compliance Enabled Vaults in this release, but it is supported for standard vaults
- Compliance Vault migration is not supported
- POST Object for CEV

Supported Functionality

- Vault protection

  o Specify Retention Durations on vault: Min, Max, and Retention Durations.

  o If Retention Settings are not specified at the time of compliance vault creation, default values are used to create the compliance vault.

  o S3 API Extensions to specify per-object retention periods and Legal Holds. If Retention period is not specified during object creation, default retention period of the target compliance vault is used for the object.

  o Allows Compliance Enabled Vaults to contain objects that can have a retention period of "0." That is, the object does not have a retention period, but legal holds can still be applied to it.
- Applying Protected Object Retention

  o Prohibits deletes and overwrites for a specified amount of time after object creation.

  o No privileged deletions of protected objects or vaults.

  o Objects cannot be deleted even if the retention period expires if there are one or more legal holds on the object.

- Protection S3 extensions
  - o Ability to add/remove/list legal holds
  - o Ability to specify per object retention time or expiration date
- Protected vault deletion by using S3 or COS Manager UI or COS REST API(vault must be empty)

Compliance Vault Properties:

Vault Creation

- Several Methods
  - Using the Manager UI
  - Can be created by using Compliance Vault Templates at Manager UI
  - Can be created by using Compliance Vault Templates and S3 PUT Bucket. A compliance template cannot be selected to be the default template.
  - Can be created by using REST API
- Settings include Status, Minimum Duration, Maximum Duration, and Retention Duration.
  - These parameters are used to validate/store objects that are stored in the Compliance Vault.
- Indexing must be enabled and Versioning must be disabled for compliance vault.

Note: Default values for parameters are found in the CSO API Guide in the section covering Create a New Protected Vault.

Vault Modification

- Change to the Retention period settings for a Compliance Vault is only applied to new objects placed in that vault. An existing vault with objects cannot be changed to retention period settings.
- PUT Bucket extension added to support modification by using S3 API.
- It is required that the vault be deployed to an Accesser device before updating the retention settings on the vault.

Vault Deletion

- Compliance Vaults can be deleted only when empty of objects.
- It is required that the vault be deployed to an Accesser device and has an associated user account that allows listing to allow the vault deletion to proceed.

Note: A locked vault cannot be deleted until the vault is deployed to an Access Pool upgraded to 3.12.0.

Vault Listing

- A GET Bucket on a Compliance Vault (with the query parameter=?protection) returns configured Protection Settings for that vault.

Object Compliance Properties:

Objection Creation

- PUT Object
  - Request Headers added to allow for specifying a per object retention time and a single legal hold.
  - Retention Time can be provided as a duration or an expiration date.
  - If a retention time is not specified in the PUT request, and the object is placed in a Compliance Vault, the Default Retention Time that is configured for the vault is given to the object.

Object Modification

The following modifications are allowed on a protected object:

- Addition/deletion of legal holds on the object by authorized users
- Object ACLs

Object Deletion

- Objects in a Compliance Vault can be deleted only after the retention period for the object has expired and there are no Legal Holds on the object.
- A new return code ‘Unavailable for Legal Reasons (451)’ has been added to indicate delete failures due to object being under Protection.

Object Listing

- GET Object
- Response Headers added to return Retention Period, Legal Hold Count, Retention Period Expiration Date.

  Retention period and Expiration date are provided, irrespective of which value was used to create the object or if the vault default settings were used at object creation.
- GET Object legal hold.
- Subresource added to return Retention Period, Retention Period Expiration Date, and all Legal Holds in place for the object.

PUT COPY

- Request Headers added to allow for specifying a per object retention time and a single legal hold.
- Retention Time can be provided as a duration or an expiration date.
- If a retention time is not specified in the PUT request, and the object is placed in a Compliance Vault, the Default Retention Time that is configured for the vault is given to the object.
- Retention Directive Added to allow for copy of existing retention period and legal holds.

Data Security

- Administrative Access needs to be carefully controlled as Root Users have the ability to override the software protections that are built in to safeguard CEV objects and CEV vaults.
- Before creating protected vaults on a system, it is recommended that at least three external NTP servers should be configured for the system.
- Anonymous access is not supported for Protected Vault/Object Writes and Deletes.
- Content MD-5 is required for Object Upload operations to ensure that proper content is being uploaded.
- AWS V4 Authentication is required for all Protected Write/Delete operations. It is recommended that the AWS V4 Signature including content checksum in the signature.

Limitations

- SOH and SWIFT interfaces are not supported on protected vaults. Protection must not be enabled on existing vaults that contain objects that are written by using either one of these interfaces. Enabling Protection on these vaults render the SOH and SWIFT objects inaccessible.
- Objects can be placed into Protected Vaults with associated SSE-C Keys. Such an object is encrypted using the SSE-C key and is protected by using the retention headers provided during the Object Write request, or by using the vault defaults in the case where retention headers were not provided. However, once written, all attempts to modify or delete the object while its retention period has not expired, or while it still has an active legal hold will fail. Thus the SSE-C key that is associated with an object under protection cannot be modified to a new key (Key Rotation) until the retention time for the object has expired, and all legal holds for the object are deleted.

Supported Interfaces

Only S3 is supported for operations on Protected Vaults/Objects.

Documentation

IBM COS Compliance Enabled Vault API Extensions

- CSO API Reference Guide
- Manager REST API Guide
- Manager Administration Guide

Concentrated Dispersal (CD) [99]

This release features Concentrated Dispersal, which allows for smaller deployments. Device Sets can be created with as few as three Slicestor Appliances. The feature automatically activates when a Device Set is created with 3-6 Slicestor Appliances. When active, configurations for Vault Information Dispersal Algorithms (IDA) are preselected, and have IDA Widths that are some multiple of the number of Slicestor Appliances. The result is it enables more reliable and efficient deployments across a reduced number of devices that can support usable system configurations with as few as 80 TB of capacity.

Support retrieval of region code and billing class separately [1141]

This feature adds Region and Storage Class fields that are configurable from the Manager at the vault level only applicable to container vaults. The purpose of Region and Storage Class are as follows:

- Region, can be used as an indicator of where the contents of this container vault (objects and containers reside). The LocationConstraint element that is shown for container(s) associated to this vault in the S3 GET Service Extended and S3 GET Bucket Location are populated with the value set for region. If the region field is not set, the LocationConstraint element is populated with the container vault's provisioning code.
- Storage Class, can be used as a classification that is assigned to all objects stored within this container vault. The header x-amz-storage-class shown in the S3 GET/HEAD Object and the StorageClass element in the response body of the S3 GET Bucket are populated with the value set for storage class. If the storage class field is not set, all objects within the container vault have a storage class of STANDARD.

Cisco UCS S3260 M4 & C220 M4 - Long-term Support [1087]

The Cisco UCS C220 M4 is certified to provide either Manager or Accesser[1] functionality in an IBM COS system. The UCS C220 is a 1U unit with eight drive slots, only HDD1 and HDD2 are used in the situation.

The Cisco S3260 M4 is certified to provide Slicestor functionality in an IBM COS system. The UCS S3260 is a 4U unit with 56 top loading drive slots. IBM COS does not support the optional four bay disk expander at the back of the chassis. IBM supports this server in either Single Node or Dual Node Configuration.

Chapter 2. Interface Modifications

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.

Chapter 3. Resolved Issues

Resolved issues in 3.12.0 April Maintenance Release

Table 1. Resolved issues

Issue	Description
COS-36653	Fixed an issue where certain errors encountered during listing may be ignored, resulting in successful listing responses that omit ranges of results that should have been included in the output.
COS-31475	Resolved an issue that was preventing hard drive Advanced Power Management functionality from being disabled on Slicestor device data drives.
COS-27605	Resolved an issue where upon upgrade of certain Slicestor appliances, data drives could erroneously transition to a diagnostic or offline state, preventing them from being used by the device.
COS-34886	Fixed an issue where requests being sent via 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-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-31864	Fixed a race condition where slices maybe erroneously removed during an overwrite operation. This has been observed to impact the name index, which by nature is updated frequently. In this situation, write, delete, or listing requests to the impacted location of the index will fail and return HTTP status code 500.

Resolved issues in 3.12.0 December Maintenance Release

Table 2. Resolved issues

Issue	Description
COS-29189	OneStor Platform Laguna Seca (3584) devices do not report appliance information after upgrade.
COS-28665	Resolved an issue where the dlm process was erroneously reported as not running when a device was under extreme workload and stress.

Resolved issues in 3.12.0

Table 3. Resolved issues

Issue	Description
COS-25110	Status 503 responses not showing in Manager UI Accesser Requests chart
COS-26125	Device is potentially in an inconsistent state ERROR CODE 5
COS-26059	Invalid Directory Structure Exception results in Fatal Error
COS-26125	Handle Error code 5 during upgrade.
COS-25294	Manager indicates that the OS drive is OFFLINE after reimaging.
COS-27033	If a Vault's Alert Level is not set, the manager fails to send certain traps. Specifically, Storage Pool health alerts for that Vault's configuration are impacted.
COS-14435	Incorrect response code during vault deletion.

Table 3. Resolved issues (continued)

Issue	Description
COS-13862	Drive Capacity calculation updates.
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.
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.
COS-27474	Fixed an issue where 500 error is seen during upgrade.
COS-25294	During OS only image , drive state handling at the manager has been fixed in this release.
COS-25139	Some Accesser Request information has been captured in the Device API Guide. Additional attributes will be provided in a follow-on release. Refer to the document for details.
COS-27145	The Event Report Manager REST API has been updated to provide a detailed error response with a 422 status code, instead of incorrectly throwing an exception with 500 status code, when a user provides multiple stream types that reference the same stream data type.

Chapter 4. Known issues

Table 4. 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 4. 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-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-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-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.
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.

Table 4. Known issues (continued)

Issue	Failing Condition	Disposition
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-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.	Please Contact IBM Customer Support for assistance to expedite the recovery of the destroyed slices.

Upgrading and Installation

Table 5. 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.
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.

Container

Table 6. 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.

Table 6. Container (continued)

Issue	Failing Condition	Disposition
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 7. 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 8. 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.

Table 8. System behavior (continued)

Issue	Failing Condition	Disposition
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 9. 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.

Data Evacuation

Table 10. Data evacuation

Issue	Failing Condition	Disposition
	Nothing to report.	

System Configuration

Table 11. System configuration

Issue	Failing Condition	Disposition
	Nothing to report.	

Deleting objects

Table 12. 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 13. 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 14. Vaults

Issue	Failing Condition	Disposition
	Nothing to report	

Vault Mirrors

Table 15. 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.

Table 15. Vault mirrors (continued)

Issue	Failing Condition	Disposition
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 16. 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 17. 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 18. 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
Accesser Device	A2100	≤2.7.0
Accesser Device	A3100	≤2.7.0
Accesser Device	S1440	≤2.7.0
Accesser Device	S2104	3.2.1
Accesser Device	S2212	3.2.1
Accesser Device	S2440	3.0.1
Accesser Device	S4100	3.1.0

Table 19. 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 20. 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 20. 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 21. 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 22. 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

Dell

Table 23. Minimum Version of ClevOS Compatible with Dell Hardware

Appliance	Model	Minimum ClevOS
Dell Slicestor® Device	DSS 7000	3.10.1

Lenovo

Table 24. 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