IBM Cloud Object Storage System
3.16.8 September Maintenance

Release Notes

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

Contents

Support information v

Chapter 1. New Features and Improvements in ClevOS 3.16.8 1

Chapter 2. New Features and Improvements in ClevOS 3.16.7 2

Chapter 3. New Features and Improvements in ClevOS 3.16.6 3

Chapter 4. New Features and Improvements in ClevOS 3.16.5 4

Chapter 5. New Features and Improvements in ClevOS 3.16.4 5

Chapter 6. New Features and Improvements in ClevOS 3.16.3 6

Chapter 7. New Features and Improvements in ClevOS 3.16.2 7

Chapter 8. New Features and Improvements in ClevOS 3.16.1 8

Chapter 9. New Features and Improvements in ClevOS 3.16.0 9

Chapter 10. Interface Modifications 10

Chapter 11. Resolved Issues 11

Resolved issues in 3.16.8 September Maintenance 11
Resolved issues in 3.16.8 11
Resolved issues in 3.16.7 September Maintenance 11
Resolved issues in 3.16.7 August Maintenance 11
Resolved issues in 3.16.7 12
Resolved issues in 3.16.6 July Maintenance 12
Resolved issues in 3.16.6 13
Resolved issues in 3.16.5 April Maintenance 13
Resolved issues in 3.16.5 14
Resolved issues in 3.16.4 March Maintenance 14
Resolved issues in 3.16.4 14
Resolved issues in 3.16.3 February Maintenance 14
Resolved issues in 3.16.3 15
Resolved issues in 3.16.2 15
Resolved issues in 3.16.1 November Maintenance 15
Resolved issues in 3.16.1 15
Resolved issues in 3.16.0 August Maintenance 16
Resolved issues in 3.16.0 June Maintenance 16
Resolved issues in 3.16.0 February Maintenance 16
Resolved issues in 3.16.0 January Maintenance 17
Resolved issues in 3.16.0 December Maintenance 17
Resolved issues in 3.16.0 November Maintenance 17
Resolved issues in 3.16.0 17

Chapter 12. Product Alert Notifications 18

Chapter 13. Known issues....20
Upgrading and Installation....21
Container....21
Alerting and Reporting....21
System Behavior....22
Storage Pools....22
Data Evacuation....22
System Configuration....22
Deleting objects....22
Manager Web Interface....23
Vaults....23
Vault Mirrors....23
Vault migration....23

Chapter 14. Supported Hardware Platforms....24
IBM Cloud Object Storage Appliances....24
Hewlett Packard Enterprise....24
Seagate....25
Cisco....25
Dell....25
Lenovo....26
Quanta Cloud Technology (QCT)....26

Chapter 15. Incompatible Hardware and Firmware with ClevOS....27
Broadcom....27
Hewlett Packard....27
IBM Cloud Object Storage Appliances....27
Seagate....28
Supermicro....28

Notices....29
Trademarks....30

Support information

Technical support contacts.

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

Chapter 1. New Features and Improvements in ClevOS 3.16.8

There are no new features in this release.

Chapter 2. New Features and Improvements in ClevOS 3.16.7

There are no new features for this release.

Chapter 3. New Features and Improvements in ClevOS 3.16.6

Multiple Manager Devices for High Availability [Active-Active] (1661)

A maximum of two IBM COS Manager™ devices may run simultaneously within the system, providing continued visibility into system operation and provisioning capabilities if a Manager device fails. When both Manager devices are running, configuration changes can be performed concurrently, and events can be observed on either Manager device.

Systemic disk failure detection and handling (1705)

The IBM COS Manager™ provides drive Annual Replacement Rate (ARR) information for all storage pool sets, and alerts you if the ARR exceeds a specified threshold.

Chapter 4. New Features and Improvements in ClevOS 3.16.5

There are no new features in this release.

Chapter 5. New Features and Improvements in ClevOS 3.16.4

Trusted Software Installer (785)

The Trusted Software Installer (Software Signature Verification) feature was first introduced in ClevOS™ 3.15.3.38 and enforces that only IBM signed upgrade files can be used as part of the upgrade procedure. The enforcement of this feature is disabled by default, but can be enabled in the IBM Cloud Object Storage Manager™ UI.

Beginning with ClevOS 3.16.4.30 or LTSR ClevOS 3.16.0.82, the root CA used for verifying the upgrade files is rotated. Prior ClevOS releases do not include the trust anchors associated with the newly rotated root CA or its corresponding CRL. This means that all software packages signed with the previous signing certificate are unable to be verified after March 23, 2022 12:00:00 2022 GMT. As a result, anyone upgrading to ClevOS 3.16.4.30 (or newer) or LTSR ClevOS 3.16.0.82 (or newer), and anyone who is upgrading to any release after March 23, 2022 12:00:00 GMT, sees the **`Signature Verification Status: Failed`** warning in the IBM Cloud Object Storage Manager™ UI upgrade page.

On most systems, the message **`Signature Verification Status: Failed`** displays during the next ClevOS upgrade. In this case, the warning does not indicate that the upgrade file is compromised. It is simply the result of the previous ClevOS signing certificate expiring. If the Software Signature Verification feature was never enabled on the system, operators can ignore the warning and proceed as usual with the upgrade.

However, if the IBM Cloud Object Storage System™ has the Software Signature Verification feature enabled, a workaround is required before upgrading to ClevOS 3.16.4.30 (or newer) or LTSR ClevOS 3.16.0.82 (or newer). Also, after March 23, 2022 12:00:00 GMT, when the previous signing certificate expires, systems with the Software Signature Verification feature enabled can only upgrade to ClevOS 3.16.4.30 (and newer) or LTSR ClevOS 3.16.0.82 (or newer).

Basic Authentication for Device API (1796)

Basic Authentication is now supported in the Device Level API.

Chapter 6. New Features and Improvements in ClevOS 3.16.3

There are no new features in this release.

Chapter 7. New Features and Improvements in ClevOS 3.16.2

There are no new features in this release.

Chapter 8. New Features and Improvements in ClevOS 3.16.1

There are no new features in the October Maintenance release.

Chapter 9. New Features and Improvements in ClevOS 3.16.0

Expiration Lifecycles for Versioned Objects and Incomplete Multipart Uploads in Container Mode (1697)

The ClevOS system currently allows users to easily manage stale data by configuring expiration lifecycle on a bucket. This system only supported regular (non-versioned) objects in the past, disallowing users from enabling expiration on versioning-enabled container vaults (and vice versa). This feature extends object expiration to include versioned objects and incomplete multipart uploads. Users with versioned buckets and work flows that create incomplete MPUs can now take advantage of expiration lifecycle to manage their usage.

Add new channel for external management services (1786)

A new channel was created to support a new subnet/VLAN configuration to access external services.

Chapter 10. Interface Modifications

API updates for ClevOS 3.16.7:

- COS-80887, Fixed handling of multiple header fields with the same name for AWS signature authentication. Previously only the first header field was used in signature calculation.
- COS-88662, New error alert added for 500 errors caused by a failure on a remote store. Previously this type of 500 error would show up as uncategorized, but now generates a more specific root caused alert in the event console, as well as in the **`error_ root_cause`** field in the access log as **`REMOTE_STORE_FAILURE`**.

API updates for ClevOS 3.16.6:

- COS-90696, Beginning in the ClevOS 3.16.6.75 release, Device level APIs require the use of GCM mode in TLS cipher suites. Update client-side TLS cipher suite to support GCM mode.

API updates for ClevOS 3.16.4 have been referenced in the following documentation:

- REST API Developer Guide

  COS-86003, Basic Authentication is now supported in the Device Level API as part of F1796 (update to Edit System Device Level API Configuration). Added new parameter **`authenticated`**.

API updates for ClevOS 3.16.3 have been referenced in the following documentation:

- REST API Developer Guide

  You can enable or disable IP addresses and network types independent of each other using the resource configuration API (**`configureExtendedCOSAPISettings.adm`**). The existing property firewall rules are split in two separate properties - firewall rules for IP addresses and firewall rules for network types.

Chapter 11. Resolved Issues

Resolved issues in 3.16.8 September Maintenance

Table 1. Resolved issues	
Issue	**Description**
COS-82433	An issue was resolved where the Accesser® Appliance requests graph would fail to load if there were more than 200 unique combinations of resource/request/response for a selected time frame.

Resolved issues in 3.16.8

Table 2. Resolved issues	
Issue	**Description**
COS-90447	Resolved an issue where Slicestor® Devices would erroneously report a data drive multiple times when unable to accurately retrieve vendor attributes from the drive.
COS-89434	Improved the handling of the **`InterSocketAddress`** string in logs such as `Access.log` and `report.log`..
COS-88826	Resolved an issue where the storage service on Slicestor® Devices crashed and restarted in scenarios where index operations became hung.
COS-72024	Zone Slice Storage now checks if storage is available before performing writes and deletes.
COS-60397	To avoid an out of memory condition on Accesser® Devices, **`S3 POST Object`** requests will allow only 1000 form fields to be set in the body of the request. If this limit or the maximum size of a field is exceeded, the request will fail with a 400 HTTP status code indicating a bad request.
COS-36651	Resolved an issue where all data drives on a Slicestor® Device will transition to an offline state if an OS-only reinstall is performed and the Slicestor® Device is then registered with a new Manager Appliance.

Resolved issues in 3.16.7 September Maintenance

Table 3. Resolved issues	
Issue	**Description**
COS-91751	Resolved an issue that prevented device upgrades from utilizing neighbor devices to retrieve upgrade artifacts to reduce the load on the IBM COS Manager™ device.

Resolved issues in 3.16.7 August Maintenance

Table 4. Resolved issues	
Issue	**Description**
	Nothing to report.

Resolved issues in 3.16.7

Table 5. Resolved issues	
Issue	**Description**
COS-88662	New error alert added for 500 errors caused by a failure on a remote store. Previously this type of 500 error would show up as uncategorized, but now generates a more specific root caused alert in the event console, as well as in the **`error_ root_cause`** field in the access log as **`REMOTE_STORE_FAILURE`**.
COS-80887	Fixed handling of multiple header fields with the same name for AWS signature authentication. Previously only the first header field was used in signature calculation.
COS-28142	Resolved an issue handling list requests on a bad drive.

Resolved issues in 3.16.6 July Maintenance

Table 6. Resolved issues	
Issue	**Description**
COS-90617	Resolved an issue that was preventing the expiration of non-current versioned objects when the objects were written using encryption (SSEC, KeyProtect or HPCS).
COS-88517	Resolved an issue that would prevent slice revisions from being cleaned up in certain failure scenarios, which could lead to write errors.
COS-88402	The S3, Simple Object, Resource Configuration, and Service APIs provided by Accesser® Appliances will no longer allow the use of null characters in HTTP URLs. Requests that include null characters in the URL will now respond with a 400 status code indicating a bad request. If objects have previously been written using the S3 API and included a null character in the object name, contact IBM customer support for assistance with recovery of those objects.
COS-86762	Resolved an issue when a reallocation completed on a dsNet with more than 2500 devices while using container mode, the maximum number of connections to the Slicestor® Devices in the storage pools storing the service vault could be exceeded, potentially resulting in requests to Accesser® Appliances failing with HTTP status code 500 errors.
COS-86296	Resolved an issue where the following API requests were not properly checking if the requester was the bucket owner, which allowed requests to be serviced despite the requester having invalid permissions: • PUT Bucket Logging • PUT Bucket Request Payment • GET Bucket Request Payment • GET Fanout • LIST Fanout These API requests return HTTP status code 403 (access denied) if the requester is not the bucket owner.
COS-83520	Resolved an issue where the requester's storage account was missing from the access logs when requests were signed using AWS signatures and resulted in an HTTP status code 403. due to either an inactive user account or a container that is owned by an inactive account.

Table 6. Resolved issues (continued)	
Issue	**Description**
COS-81932	Resolved an issue where the bucket metadata and storage account bucket listing APIs were returning different bucket creation times.

Resolved issues in 3.16.6

Table 7. Resolved issues	
Issue	**Description**
COS-88517	Resolved an issue that would prevent slice revisions from being cleaned up in certain failure scenarios, which could lead to write errors.
COS-88402	The S3, Simple Object, Resource Configuration, and Service APIs provided by Accesser® Appliances will no longer allow the use of null characters in HTTP URLs. Requests that include null characters in the URL will now respond with a 400 status code indicating a bad request. If objects have previously been written using the S3 API and included a null character in the object name, contact IBM customer support for assistance with recovery of those objects.
COS-86762	Resolved an issue when a reallocation completed on a dsNet with more than 2500 devices while using container mode, the maximum number of connections to the Slicestor® Devices in the storage pools storing the service vault could be exceeded, potentially resulting in requests to Accesser® Appliances failing with HTTP status code 500 errors.
COS-86296	Resolved an issue where the following API requests were not properly checking if the requester was the bucket owner, which allowed requests to be serviced despite the requester having invalid permissions: • PUT Bucket Logging • PUT Bucket Request Payment • GET Bucket Request Payment • GET Fanout • LIST Fanout These API requests return HTTP status code 403 (access denied) if the requester is not the bucket owner.
COS-83520	Resolved an issue where the requester's storage account was missing from the access logs when requests were signed using AWS signatures and resulted in an HTTP status code 403. due to either an inactive user account or a container that is owned by an inactive account.
COS-81932	Resolved an issue where the bucket metadata and storage account bucket listing APIs were returning different bucket creation times.

Resolved issues in 3.16.5 April Maintenance

Table 8. Resolved issues	
Issue	**Description**
	Nothing to report.

Resolved issues in 3.16.5

Table 9. Resolved issues	
Issue	**Description**
	Nothing to report.

Resolved issues in 3.16.4 March Maintenance

Table 10. Resolved issues	
Issue	**Description**
COS-88282	Resolved an issue that resulted in upgrade failures on Slicestor® Devices where disks were removed.

Resolved issues in 3.16.4

Table 11. Resolved issues	
Issue	**Description**
COS-55305	Resolved an issue to reduce impact of reconciling logical usage after an unclean shutdown.
COS-82035	Resolved an issue to reduce impact of infrequently removing old references to bin files.
COS-82036	An advanced config parameter is added to allow an administrator to change the threshold for when old references to bin files are infrequently removed.
COS-85688	Resolved an issue where object write times could increase through the duration of an upgrade when upgrading from a release prior to 3.15.0 to a release 3.15.0 or newer. This problem was more likely to manifest on systems running higher workloads that were closer to maximum system throughput.
COS-86006	Fixed an issue that could cause the name index entries for a versioned object to become inconsistent after a crash or a failed write if the current version of that object is a delete marker.

Resolved issues in 3.16.3 February Maintenance

Table 12. Resolved issues	
Issue	**Description**
COS-85492	Resolved an issue on Slicestor® Devices where upgrades were taking longer than expected due to slow shutdown times. The shutdown time would increase with the number of Accesser® Appliances, the number of vaults, and the amount of time the Slicestor device had been running.
COS-85688	Resolved an issue where object write times could increase through the duration of an upgrade when upgrading from a ClevOS release prior to 3.15.0 to a ClevOS release 3.15.0 or newer. This problem was more likely to manifest on systems running higher workloads that were closer to the maximum system throughput.

Resolved issues in 3.16.3

Table 13. Resolved issues	
Issue	**Description**
COS-81272	Resolved an issue to fix unexpected 503 errors due to memory pressure on accesser devices.
COS-82035	Resolved an issue to reduce impact of infrequently removing old references to bin files.

Resolved issues in 3.16.2

Table 14. Resolved issues	
Issue	**Description**
COS-82454	Resolved an issue with creation of overlapping entries between the S3 Virtual Host Suffix and the Static Website Virtual Host Suffix.
COS-84458	Resolved an issue with ZSS Write Pointer Recovery.
COS-85388	Resolved an issue in which a Docker Accesser did not bring up dsnet-core.
COS-85468	Resolved an issue in which upgrading IBM Slicestor devices with a large number of disks may encounter an Out-of-Memory exception.
COS-85520	Resolved an issue in which device certificates with wildcard DNS SAN entries were causing an unexpected exception.

Resolved issues in 3.16.1 November Maintenance

Table 15. Resolved issues	
Issue	**Description**
COS-17176	An Advanced Configuration parameter is added to allow an administrator to set an alert threshold for network interface speeds. This is useful for preventing erroneous alerts for degraded network interface speeds when intentionally running at a rate less than the network interface's maximum speed. For more information on how to utilize this configuration parameter, contact IBM Support.
COS-85038	Resolved an issue where intent (storage type 4) slices were not cleaned up when one or more stores in a stripe were down, potentially leading to intent storage limit errors
COS-84483	Resolved an issue with SNMP Alert Forwarding which leads to permit exhaustion and prevents the device from reporting status to the IBM Cloud Object Storage Manager™.
COS-84521	An issue was resolved in which some Manager to device communication was prevented when external device certificates were used.

Resolved issues in 3.16.1

Table 16. Resolved issues	
Issue	**Description**
COS-84521	An issue was resolved in which some Manager to device communication was prevented when external device certificates were used.

Resolved issues in 3.16.0 August Maintenance

Table 17. Resolved issues	
Issue	**Description**
COS-90617	An issue was resolved which was preventing the expiration of non-current versioned objects when the objects were written using Server Side Encryption with Customer-Provided Keys (SSE-C).

Resolved issues in 3.16.0 June Maintenance

Table 18. Resolved issues	
Issue	**Description**
COS-89985	Improved the Zone Slice Storage full disk recovery tool which would sometimes fail in certain drive states.
COS-89984	Resolved an issue with the Zone Slice Storage manual compaction tool where it would fail to make progress and run indefinitely.
COS-89636	Resolved an issue where the service would crash on Slicestor® Devices in the presence of malformed disk identifiers.
COS-87845	Improved the visibility check used to prevent corrupt object created by PUT request that failed with a 500 error.
COS-82441	Resolved an issue on some models of Lenovo-based Slicestor® Devices, for which OS RAID arrays may erroneously report degraded/optimal after upgrade to affected releases.
COS-17176	An advanced configuration parameter has been added to allow an administrator to set an alert threshold for network interface speeds. This is useful for preventing erroneous alerts for degraded network interface speeds when intentionally running at a rate less than the network interface's maximum speed. For more information on how to utilize this configuration parameter, contact IBM Support.

Resolved issues in 3.16.0 February Maintenance

Table 19. Resolved issues	
Issue	**Description**
COS-55305	Resolved an issue to reduce impact of reconciling logical usage after an unclean shutdown.
COS-82035	Resolved an issue to reduce impact of infrequently removing old references to bin files.
COS-82036	An advanced config parameter is added to allow an administrator to change the threshold when old references to bin files are infrequently removed.
COS-85224	Resolved an issue that resulted in false errors being reported in the device logs.
COS-85688	Resolved an issue where object write times could increase through the duration of an upgrade when upgrading from a release prior to ClevOS release 3.15.0 to a release 3.15.0 or newer. This problem was more likely to manifest on systems running higher workloads that were closer to maximum system throughput.

Table 19. Resolved issues (continued)	
Issue	**Description**
COS-86006	Fixed an issue that could cause the name index entries for a versioned object to become inconsistent after a crash or a failed write if the current version of that object is a delete marker.
COS-87107	Resolved an issue where in a vault mode systems, upgrading Accesser® Appliances before Slicestor® Devices, to a ClevOS release 3.16.0 or higher, was causing 500 errors.

Resolved issues in 3.16.0 January Maintenance

Table 20. Resolved issues	
Issue	**Description**
	Nothing to report.

Resolved issues in 3.16.0 December Maintenance

Table 21. Resolved issues	
Issue	**Description**
	Nothing to report.

Resolved issues in 3.16.0 November Maintenance

Table 22. Resolved issues	
Issue	**Description**
COS-84483	Resolved an issue with SNMP Alert Forwarding which leads to permit exhaustion and prevents the device from reporting status to the IBM Cloud Object Storage Manager™.
COS-84521	An issue was resolved in which some Manager to device communication was prevented when external device certificates were used.
COS-85038	Resolved an issue where intent (storage type 4) slices were not cleaned up when one or more stores in a stripe were down, potentially leading to intent storage limit errors

Resolved issues in 3.16.0

Table 23. Resolved issues	
Issue	**Description**
	Nothing to report.

Chapter 12. Product Alert Notifications

IBM® clients with an IBM ID may sign up to receive product alert notifications that contain important information that may impact the use of the IBM Cloud Object Storage System™. In order to receive these notifications, clients need to subscribe to the "IBM Cloud Object Storage System™" product in MyNotifications. The table below represents the alert notifications that are applicable while running this latest version of ClevOS™ at the time of this release note publication. For any questions regarding the content of these product notifications, contact IBM Support.

Table 24. Product Alert Notifications for the IBM Cloud® Object Storage System

Alert Notification Title	Impacted ClevOS™ Releases	Alert Notification Published Date
Device level API's required TLS cipher suite updated in ClevOS 3.16.6.75	3.16.6.75 and future releases	July 13, 2022
Slicestor® disk model WUH721818AL4200 firmware issue	All ClevOS releases	Apr 29, 2022
Software Signature Verification issue impacting ClevOS™ upgrades	3.15 and 3.16	Feb 18, 2022
Format updated in API response for multipart copy.	3.15.8.97 and future releases	Dec 2, 2021
IBM Cloud Object Storage On-Premise Adopts Continuous Delivery Software Support Lifecycle.	3.16.0	Oct 29, 2021
Performance implications of non-homogenous COS storage pool expansions	All ClevOS releases	Jun 30, 2021
API changes related to S3 Object Versioning	3.15.7 and future releases	Apr 19, 2021
Issue with adding multiple drives in a IBM COS Slicestor® appliance	All ClevOS releases	Jul 20, 2020
A firmware issue can cause IBM COS Gen2 HW nodes to fail to boot up	ClevOS independent	Jun 18, 2020
Java™ version incompatibility preventing IPMI access	ClevOS independent	Mar 12, 2018
IPMI Configured via nut Command Does Not Persist on Device Restart	ClevOS independent	Jun 27, 2017
Drive-managed Shingled Magnetic Recording (SMR) drives are not approved and should not be used with named-object protocol workloads	ClevOS independent	Mar 16, 2017

Table 24. Product Alert Notifications for the IBM Cloud® Object Storage System (continued)		
Alert Notification Title	**Impacted ClevOS™ Releases**	**Alert Notification Published Date**
IBM COS Slicestor® 2584 Fails to Attach Drives	ClevOS independent	Feb 2, 2017

Chapter 13. Known issues

Table 25. Known issues

Issue	Failing Condition	Disposition
COS-58128	DLM cannot process more than 16 hot-swap events at once.	This issue will be fixed in a future release.
COS-50579	There is a known issue where slice data being reallocated from one Slicestor device to another would not be appropriately removed from the source Slicestor device if the reallocation process was erroneously marked as complete."	This issue still exists in 3.14.3 because the change was reverted in the latest fix.
COS-11201	In the Event Console of the Manager User Interface, the event details section for failing disk migration events contains a parameter that is called Migration Progress. However, it is not clear what this value represents.	This value corresponds to the percentage of failing disk migration that is complete.
COS-11355	Replacing a failed drive with another failed drive results in an inconsistent view on the Manager User Interface. On the Monitor Device page, in the "Summary of device health" section, both the replaced failed drive and the new failed drive are shown. The "Drive Information and Actions" view of the drive layout shows the replaced failed drive. On the Maintenance page, the FRU report contains the replaced failed drive.	Perform another replacement of the failed drive with a good drive.
COS-13575	The "stop migration" operation for failing disk migration on the Manager User Interface (UI) can take ~20 seconds to complete after being initiated by the user. The button continues to be enabled during this time. This issue exists for dispose and reset disk operations as well.	Do not hit the button again until the operation completes. If the drive stays in the same state for more than 20 seconds, perform a refresh of the page. If the drive continues to stay in this state, follow the recommended action that is provided in the Manager Administration Guide under disk lifecycle management.
COS-10031	When resuming a drive in the DIAGNOSTIC state from the Manager User Interface, it can take ~20 seconds to complete. The resume button is not disabled during this time.	Do not hit the resume button until the operation completes. If the drive stays in the DIAGNOSTIC state for more than 20 seconds, perform a refresh of the page. If the drive continues to stay in this state, follow the recommended action that is provided in the Manager Administration Guide under disk lifecycle management.

Table 25. Known issues (continued)		
Issue	**Failing Condition**	**Disposition**
COS-10445	When using the storage command from the localadmin shell on a Slicestor® device, it is possible to resume all drives that are currently in the DIAGNOSTIC state. However, in some cases , this process can take too long, which will cause the command to return an error code -15 due to a timeout.	Despite the error, the resume process is continuing in the background. The storage list command can be used to monitor the progress of resume process.
COS-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-23962	Vault quotas are static and do not update when storage pool capacities change. If a system expansion, set replacement, or set removal is performed on the storage pool, vault quotas for any vaults on that pool will not update to consider the new capacity.	The user-defined vault quotas work as expected. However, they cannot be consistent with the current storage pool capacity. For example, a vault quota can be higher than total storage pool capacity after a set removal.

Upgrading and Installation

Table 26. Upgrading and Installation		
Issue	**Failing Condition**	**Disposition**
	Nothing to report.	

Container

Table 27. Container		
Issue	**Failing Condition**	**Disposition**
COS-15401	If a user attempts to create a management vault by using "manual configuration" (accessed through the Configure Management Vault page) based on an existing vault template, management vault creation fails with the following message: "Cannot create a management vault from this template. It is deployed to access pools with standard vaults"	Use the "automatic configuration" available on the Configure Management Vault page.

Alerting and Reporting

Table 28. Alerting and reporting		
Issue	**Failing Condition**	**Disposition**
	Nothing to report.	

System Behavior

Table 29. System behavior

Issue	Failing Condition	Disposition
	Nothing to report.	

Storage Pools

Table 30. Storage pools

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

Data Evacuation

Table 31. Data evacuation

Issue	Failing Condition	Disposition
	Nothing to report.	

System Configuration

Table 32. System configuration

Issue	Failing Condition	Disposition
	Nothing to report.	

Deleting objects

Table 33. Deleting objects

Issue	Failing Condition	Disposition
	Nothing to report.	

Manager Web Interface

Table 34. Manager Web Interface

Issue	Failing Condition	Disposition
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 that is 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 appears. When the network comes back, reload the page, at which point an internal server error page appears in some scenarios.	Log out of the internal server error page and log back into the manager, which will take you through one time setup again.

Vaults

Table 35. Vaults

Issue	Failing Condition	Disposition
	Nothing to report.	

Vault Mirrors

Table 36. Vault mirrors

Issue	Failing Condition	Disposition
	Nothing to report.	

Vault migration

Table 37. Vault migration

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

Chapter 14. Supported Hardware Platforms

IBM Cloud Object Storage Appliances

Table 38. 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® 3110	4958/4957	A10	3.14.4
IBM COS Manager™ 3105	3401/3403	M01	3.8.1
IBM COS Manager™ 3110	4958/4957	M10	3.14.4
IBM COS Slicestor® 2212	3401/3403	S00	3.8.1
IBM COS Slicestor® 2448	3401/3403	S01	3.8.1
IBM COS Slicestor®3448	3401/3403	S02	3.8.3
IBM COS Slicestor®2584 (AP-TL-1)	3401/3403	S03	3.8.1
IBM COS Slicestor®2584 (AP-LS-1)	3401/3403	S03	3.13.1
IBM COS Slicestor®2212A	3401/3403	S10	3.10.0
IBM COS Slicestor®12	4958/4957	C10/J10	3.14.4
IBM COS Slicestor®53	4958/4957	C10/J11	3.14.4
IBM COS Slicestor®106	4958/4957	C10/J12	3.14.4
IBM COS Slicestor®92IBM Cloud Object Storage System™	4958/4957	C10/J15	3.15.5

Note: □ Requires RPQ

Hewlett Packard Enterprise

Table 39. Minimum Version of ClevOS Compatible with Hewlett Packard Enterprise Hardware

Appliance	Model	Minimum ClevOS
Manager Appliance	DL360P Gen8	3.2.1
Manager Appliance	DL360 Gen9	3.5.0
Manager Appliance	DL380 Gen9	3.5.0
Manager Appliance	DL360 Gen10	3.14.0
Accesser® Device	DL360P Gen8	3.2.1
Accesser® Device	DL360 Gen9	3.5.0
Accesser® Device	DL360 Gen10	3.14.0
Accesser® Device	DL380 Gen9	3.5.0

Table 39. Minimum Version of ClevOS Compatible with Hewlett Packard Enterprise Hardware (continued)		
Appliance	**Model**	**Minimum ClevOS**
Slicestor® Device	SL4540 Gen8	2.9.0
Slicestor® Device	DL380 Gen9	3.5.0
Slicestor® Device	Apollo 4200 Gen9	3.6.0
Slicestor® Device	Apollo 4200 Gen10	3.14.10
Slicestor® Device	Apollo 4510 Gen9	3.6.0
Slicestor® Device	Apollo 4510 Gen10	3.14.0
Slicestor® Device	Apollo 4530 Gen9	3.6.0

Seagate

Table 40. Minimum Version of ClevOS Compatible with Seagate Hardware		
Appliance	**Model**	**Minimum ClevOS**
Seagate OneStor®	AP-2584 1 AP-TL-1	3.4.2
Seagate Exos®	AP 5U84-Laguna Seca	3.15.0

Cisco

Table 41. Minimum Version of ClevOS Compatible with Cisco Hardware		
Appliance	**Model**	**Minimum ClevOS**
Cisco Slicestor® Device	UCS C3260	3.7.4
Cisco Slicestor® Device	UCS S3260 (Single Node)	3.12.0
Cisco Slicestor® Device	UCS S3260 (Dual Node)	3.12.0
Cisco Slicestor® Device	UCS S3260 M5 (56 drive configuration)	3.13.1
Cisco Slicestor® Device	UCS S3260 M5 (60 drive configuration)	3.14.3
Cisco Manager Appliance	UCS C220 M4	3.12.0
Cisco Accesser® Device	UCS C220 M4	3.12.0
Cisco Manager Appliance	UCS C220 M5	3.13.6
Cisco Accesser® Device	UCS C220 M5	3.13.6
Cisco Slicestor® Device	UCS C240	3.13.6

Dell

Table 42. Minimum Version of ClevOS Compatible with Dell Hardware		
Appliance	**Model**	**Minimum ClevOS**
Dell Slicestor® Device	DSS 7000	3.10.1

Table 42. Minimum Version of ClevOS Compatible with Dell Hardware (continued)		
Appliance	**Model**	**Minimum ClevOS**
Dell Slicestor® Device	R740xd w/ HDD Support	3.14.1
Dell Slicestor® Device	R740xd w/ NVMe Support	3.14.2
Dell Slicestor® Device	R740xd2	3.14.9

Lenovo

Table 43. Minimum Version of ClevOS Compatible with Lenovo Hardware		
Appliance	**Model**	**Minimum ClevOS**
Lenovo Manager Appliance	X3550 M5	3.10.1
Lenovo Accesser® Device	X3550 M5	3.10.1
Lenovo Manager Appliance	X3650 M5	3.10.1
Lenovo Manager Appliance	SR630	3.13.6
Lenovo Accesser® Device	SR630	3.13.6
Lenovo Slicestor® Device	SR650	3.13.6

Quanta Cloud Technology (QCT)

Table 44. Minimum Version of ClevOS Compatible with QCT Hardware		
Appliance	**Model**	**Minimum ClevOS**
QCT Manager Appliance	QuantaGrid D51PH-1ULH	3.13.4
QCT Accesser® Device	QuantaGrid D51PH-1ULH	3.13.4
QCT Slicestor® Device	QuantaGrid D51PH-1ULH	3.13.4

Chapter 15. Incompatible Hardware and Firmware with ClevOS

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

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

Broadcom

Table 45. Broadcom Hardware and Firmware Incompatibility with ClevOS

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

Hewlett Packard

Table 46. HP Hardware and Firmware Incompatibility with ClevOS

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

IBM Cloud Object Storage Appliances

Table 47. IBM COS Hardware and Firmware Incompatibility with ClevOS

Type	Model	Firmware affected
USM	IBM COS Slicestor®2584 (AP-TL-1) 3401/3403 S03	4.1.7
BMC	A3105, A4105, M3105, S2212A, S2448	1.0.125362, 1.0.135362
BMC	A10,C10,M10	< .97
CPLD	A10,C10,M10	< 1818

Table 48. IBM COS Drive Feature Hardware and Firmware Incompatibility with ClevOS

Model Affected	Feature	Capacity	Part manufacturer/model	Firmware affected
J15	AL4D	18TB	WD/WUH721818AL4200	J6Y2

Note: 18TB drives of model WUH721818AL4200 running J6Y2 firmware may be quarantined at elevated rates and require a device power cycle to resume. This issue is resolved in firmware version J6Y3.

Seagate

Table 49. Seagate Hardware and Firmware Incompatibility with ClevOS

Type	Model	Firmware affected
HDD	Seagate ST1000NM0033-9ZM173	SN04

Supermicro

Table 50. Supermicro Hardware and Firmware Incompatibility with ClevOS

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

Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

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

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

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

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

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

US

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

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

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

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

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

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

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

COPYRIGHT LICENSE:

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

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

Trademarks

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

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

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

Printed in USA