IBM Cloud Object Storage System
3.15.7 August Maintenance

Release Notes

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

Contents

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 3.15.7

S3 Versioning (657)

ClevOS 3.15.7 introduces S3 Object Versioning support when operating this feature in container mode. As part of this release update, changes were made to align more closely with the S3 Object Versioning API. The following API changes tied to container mode also apply to clients that use Object Versioning with Vault mode:

- **`PUT-COPY`** metadata update operations now create a new Object Version if versioning is configured on the bucket. Previously, this operation would have only modified the metadata for the most current version.
- When a **`versionID`** query parameter is given for a request that does not support the parameter (ex: object uploads), an **`InvalidArgument`** error with HTTP Status code of 400 is returned rather than being ignored.
- **`GET`**, **`PUT`**, and **`DELETE`** Object Tagging requests are no longer supported for delete markers. A **`MethodNotAllowed`** error with HTTP status code of 405 is now returned.

This feature also introduces new behaviors that apply when operating in container mode. Clients that use Vault mode Object Versioning, and who are considering moving to Container mode, must be aware of the following differences in behavior:

- Maximum of 1000 versions per object history is removed. Users can create an unlimited number of versions for each object.
- Not all previous versions are preserved when an object is overwritten after versioning is suspended in Container mode. An object written when versioning is **`disabled`** or **`suspended`** that has a **`versionID`** of null, and only a single null version can exist. If a null version exists when the versioning state is toggled from **`enabled`** to **`suspended`**, the Vault mode of operation preserves all pre-existing versions during the subsequent overwrite by assigning the existing null version a new **`versionID`**. In the Container mode of operation, the existing null version is overwritten in this scenario. Customers must be aware that the Container mode of operation differs from Vault mode in this behavior.

Add TLS Endpoint to Device API (1686)

Device Level API now supports HTTPS in addition to the existing HTTP capability.

Separate Certificates for Manager UI and Internal Device Communication (1222)

Separate certificates for web UI/API HTTPS access are enabled instead of the default Manager internal certificates. As part of this feature, there is a format change to the Apache access log.

Chapter 2. New Features and Improvements in ClevOS 3.15.6

Multi-Set Deployment and Reallocation (900)

This feature introduces multiple sets that can be deployed to a storage pool before starting data reallocation.

Chapter 3. New Features and Improvements in ClevOS 3.15.5

This release includes support for a new hardware appliance, ongoing fixes and improvements, and support for the disk lifecycle management.

Chapter 4. New Features and Improvements in ClevOS 3.15.4

Storage account portal for Service API operations (1646)

You can create and delete storage accounts, credentials, and containers using the IBM® Manager UI and IBM REST API. A **Storage Account Portal** is now available through the **Configure Container Mode** page in the IBM Manager UI that allows a user to manage storage accounts, credentials, and containers. A new role, **`Storage Account Administrator`**, is added which is required to access the Storage Account Portal UI and the IBM REST API. This role, alone, only allows access to the **`Storage Account Portal`** interface. Also, new REST APIs are provided to perform the following operations:

- create storage accounts
- edit storage accounts
- delete storage accounts
- list storage accounts
- lookup storage accounts
- create credentials
- delete credentials
- list credentials
- lookup credentials
- create containers
- delete containers
- list containers
- lookup containers

See the *IBM Manager Administration Guide* and the *IBM REST API Development* guide for details.

Per Bucket, Per User Usage Metrics for IBM COS System (1641)

This feature adds a section to the Storage Account Portal (1646) that allows you to export daily historic usage for a container or storage account on the system. An Admin user can generate a report of the following:

- Current storage usage by container.
- Aggregated storage usage over a specified period of time by storage account.
- Daily historical usage over a specified date range by container.

These reports provide usage in units of bytes and objects for current usage and in units of byte-hours and object-hours for aggregated or historical usage. The report can be exported in the CSV, JSON, and XML formats.

This feature is enabled by default in systems upgraded to ClevOS 3.15.4, but usage must be updated for a container or storage account to begin tracking historic usage.

If the existing export options aren't sufficient, the Service API has been extended to allow custom historic usage queries. For specifics, see: *IBM Container Mode Service API - Bucket Management Guide*..

Chapter 5. New Features and Improvements in ClevOS 3.15.3

Trusted Software Installer (785)

`Software Signature Verification` is a new feature that enforces only IBM signed Upgrade files can be used as part of the upgrade procedure. Validity of the signature is verified by both the IBM COS Manager™ upon upload and by each device as it upgrades. Upgrades fail if the signature is not valid.

Object Tagging (1640)

Key-value pairs can now be added to object metadata for data classification in the form of **Object Tags**. Tags can be written, retrieved and removed through **`PUT, GET, DELETE Object Tag`** operations. Tags are useful for organizing data. Metadata search tools can specify object retrieval through the use of tags. Future enhancements to this feature allow for tag based operations, such as **lifecycle expiration**, to select for objects by tags. For more details, refer to the **Object Tagging** feature description document.

Code signing (1631)

This feature provides the capability to verify the delivered ClevOS release files have not been corrupted or modified since they were created. This is of importance where customer security requirements demand this level of checking. Use of this feature is optional, in that no software installation or upgrade is blocked by not performing the validation checks procedure provided here.

Code signing applies a certificate-based digital signature to files to both verify the author's identity (IBM), and to ensure the contents have not been tampered with or corrupted between the time it was signed by the author and received by the user. The process employs the use of a cryptographic hash to validate software authenticity and integrity, e.g. if the hash used to sign the application matches the hash on a downloaded application, the code integrity is intact.

Note: Any validation operation provided in this feature is optional. There is no operational requirement for the customer to validate digital signatures before installing or upgrading.

A zip file is included with each new release forward. This file, matching the pattern ‘clevos-<release>*_signatures.zip contains:

- One cryptographic hash file for each release file to be checked. For example, a file named clevos-<release>-manager-usbiso.iso.sig would contain the cryptographic hash for the corresponding release file clevos-<release>-manager-usbiso.iso.
- Materials for validation:
  - public_key.pem
  - certificate.pem
  - chain.pem

```
unzip clevos-<release>*_signatures.zip
```

For any file (<FILE)> to be validated against its cryptographic hash, execute:

```
openssl dgst -sha256 -verify public_key.pem \
-signature <FILE>.sig <FILE>
```

This is a pass/fail operation. Failure status indicates the file is not trustworthy and customer support should be contacted.

Additionally, the customer may optionally validate that the public key is present in the certificate and the certificate is still valid. The following command provides a guarantee by the Public Certificate Authority (Digicert), that the private-public keypair used to generate the signatures is actually owned by IBM.

```
# Show the certificate details; particularly:
# * It is signed by IBM and the root CA
# * Its Modulus and Exponent
```

openssl x509 -text -in certificate.pem-noout

```
# Sample output:
#. Issuer: … <CN=DigiCert SHA2 Assured ID Code Signing CA> …
#. :
#. Subject: … <CN=International Business Machines Corporation> …
#. :
# Modulus:
# 00:e2:45:27:25:e9:a3:1f:c2:37:27:ac:4c:89:86:
# ae:32:d5:2a:84:69:3b:01:cb:54:34:b0:b3:1b:6d: .......
#. :
# Exponent: 65537 (0x10001)
```

```
# Show the public key details:
#
```

openssl rsa -noout -text -inform PEM -in public_key.pem-pubin

```
# Sample output:
#. :
# Modulus:
# 00:e2:45:27:25:e9:a3:1f:c2:37:27:ac:4c:89:86:
# ae:32:d5:2a:84:69:3b:01:cb:54:34:b0:b3:1b:6d: .......
#. :
# Exponent: 65537 (0x10001)
```

Compare the above exponent/modulus data outputs of the public key and the certificate to confirm that the public key is indeed the one within the certificate.

Can also check the IBM public certificate validity:

```
# Check if the cert is still valid:
```

**openssl ocsp -no_nonce -issuer chain.pem **

**-cert certificate.pem -VAfile chain.pem **

-text -url **http://ocsp.digicert.com** -respout ocsptest

If the certificate is valid, the output will be:

```
Response verify OK
```

Note: This output goes to stderr; the command status return value does not indicate validity.

Chapter 6. New Features and Improvements in ClevOS 3.15.2

API support to restrict endpoint access and block anonymous access (1603)

This feature supports the **`PublicAccessBlock`** capabilities of S3 with support for **`BlockPublicAcls`** and **`IgnorePublicAcls`**.

Consolidation and reorganization of Manager configuration elements (1461)

The **Maintenance** and **Administration** tabs have been replaced with a **Settings** tab. The configuration options on the **Configure** tab are now present in the **Settings** tab. There are new categories that group similar configuration options together. A new Status column shows the configuration state of settings, providing an at-a-glance view.

A new **Search** box in the **Settings** tab allows you to find any configuration option quickly. Start typing a search phrase, and the drop down list will give matching configurations. Enter a phrase, and press enter to see the search results that match the Configuration titles and the Descriptions. The search phrase is highlighted for quick identification.

The **Tags** page is now only available by directly accessing the URL `http://{Manager IP}/manager/listTags.adm`.

In summary, the new **Settings** tab provides usability improvements by allowing quick access to all configuration options on one page. The search box makes it even easier to find a configuration option across the categories.

Chapter 7. New Features and Improvements in ClevOS 3.15.1

Static Website Hosting (1341)

The Static Website Hosting feature allows you to provide a low-cost, highly reliable solution to deliver the content in the COS bucket on a web page. Static Website Hosting allows a COS bucket to be configured to store static websites which deliver HTML, JavaScript, images, video, and other files to users of the website. Static Website Hosting does not support any server-side application code, such as PHP or ASP.NET. Static Website Hosting allows the data in the COS bucket to be served using a simple HTTP server. Static websites are typically used in cases where the website requires minimal to no server administration, websites which have few authors and require infrequent updates, and websites which need to automatically scale for an intermittent increase in traffic.

The Static Website Hosting feature allows you to configure a Website Configuration Policy for a COS bucket. Website configuration policy for a COS bucket can only be configured by the bucket owner. A website configuration policy for a COS bucket can be configured with index and error objects. The static web server appends the index object name when a request ends in / and returns the error object when there are errors. Optionally the website configuration can be used globally to redirect all requests to the website endpoint. A Website Configuration Policy is used to provide granular control over redirects by providing the routing rules as part of the policy.

The Static Website Hosting feature is supported in both Vault and Container mode systems. Operators may enable the Static Website Hosting feature through the IBM COS Manager for specific vaults. Operators may use the IBM COS Manager interface or IBM COS REST API commands to enable the feature for specific vaults. Enabling of the feature on vaults is NOT supported via the IBM COS Manager provisioning API. After the Static Website Hosting feature is enabled on specific vaults, you may add website policies for those vaults (or containers on those vaults) to use the feature and to define the website configuration policy.

To access a bucket as a Static Website, the client addresses the bucket via virtual host addressing, using a virtual host suffix specifically setup for the Static Website Hosting feature, known as the Static Website Virtual Host Suffix. Operators should configure the Static Website Virtual Host Suffix using the IBM COS Manager interface or by using IBM COS REST API commands for the access pools which will handle the Static Website requests. If the Static Website Virtual Host Suffix is `static-website.example.com`, then to access a COS bucket named `bucketname`, the client would use `http://bucketname.static-website.example.com/`. The `bucketname` must be DNS-compliant for the website to work. Operators should configure their DNS servers to perform proper routing of static website virtual host style addresses to the appropriate IBM Accesser® node or Load Balancer IP address. In the above example, the DNS servers should be configured so that all traffic towards `*.static-website.example.com` will have to be routed towards the IBM Accesser or the Load Balancer.

Allow Concentrated Dispersal mode container vaults (1645)

Container vaults are now supported in Concentrated Dispersal mode.

Container Mode Support of Manager and Accesser Appliance Docker Containers (1644)

Container mode is now supported on IBM COS docker containers. Refer to the Appliance Docker Container Guide documentation for more details.

Chapter 8. New Features and Improvements in ClevOS 3.15.0

Upgrade Performance and Scalability Enhancements (1012)

This feature for Upgrade Performance and Scalability Enhancements provides upgrade page load time and usability improvements for systems with > 3K devices. The upgrade page is now separated into two pages.

- The top-level UI upgrade page (**`upgrade.adm`**) displays storage and access pools, with the ability to display devices on a new page instead of everything being displayed on one page. With this change, the upgrade state is presented at different degrees of granularity: system, storage pool, or set.
- The new page displays individual device information for a storage pool set, an access pool or devices not belonging to any pool. This second page appears similar to previous versions of the Manager.

Zone Slice Storage (213D)

Zone Slice Storage (ZSS) is a new method for Slicestor® devices to store slices on disk. Traditionally, with Packed Storage, the Slicestor device manages a fixed number of files and stores data for many slices in each file. The concepts around a file and file system have been removed and replaced with a new solution that manages all data placement on the storage medium.

- ZSS is enabled at the storage pool level and can only be enabled on a new storage pool when completed before the creation of vaults for that pool.
- Any existing storage pool can be expanded with a new ZSS set.
- ZSS outperforms older designs in most user observable cases and demonstrates much better resiliency to power outages and other system conditions.
- ZSS enables the use of Host Managed Shingled Magnetic Recording (SMR) hard drives. SMR enables higher capacity than conventional Perpendicular Magnetic Recording (PMR) hard drives.

See the Zone Slice Storage feature description for more information.

Attention: Embedded accesser device users only, see the section on Performance Considerations in the Embedded Accesser Appliance Service Guide.

Advanced Configuration Parameters for Storage Sets (1654)

The IBM COS system currently allows a user to apply advanced configuration parameters at the **`global`**, **`storage pool`**, or **`device`** levels. This feature adds functionality in the Manager User Interface and associated REST API to update advanced configuration parameters at the set level on a **`storage pool`**.

Chapter 9. Interface Modifications

API updates for ClevOS 3.15.7 have been referenced in the following documentation:

- REST API Developer Guide
- Cloud Storage Object (CSO) API 2.5 Developer Guide

API updates for ClevOS 3.15.1 have been referenced in the following documentation:

- Container Mode Service API Guide
- CSO API 2.5 Developer Guide
  - COS-71196, hard quota support for buckets was originally added as part of F1342 (update to Service API). In the course of development for F1616, the following fix was added. First, it was found that the response when the hard quota is exceeded was using vault mode terminology. As part of the fix, the **<Code>** and **<Message>** fields were updated to the output below.

```
 <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Error>
     <Code>BucketQuotaExceeded</Code>
     <Message>The specified bucket hard quota has been exceeded.</Message>
     <Resource>/container/test</Resource>
     <RequestId>00000000-0000-0000-0000-000000000000</RequestId>
     <httpStatusCode>507</httpStatusCode>
</Error>
```

API updates for ClevOS 3.15.0 have been referenced in the following documentation:

- REST API Developer Guide

API changes for ClevOS 3.14.13 have been referenced in the following documentation:

- *Cloud Storage Object API 2.5 Development* guide (COS-76460/COS-76461)
  - PUT ACL for an Object in the Versioning Enabled bucket, with a non-existent version returned a 404 error code. However no information was included in the error code, message, and field. New behavior is updated to include the following fields as part of the response:

    Error code: `NoSuchVersion`

    Error message: `The specified version does not exist.`

    Extra fields: `<Key>object_name</Key><VersionId>requested_version_id</VersionId>`
  - PUT/GET ACL for an Object with `VersionId` which has a delete marker returned a 404 error code. New behavior is updated to return a 405 error code with the below fields as part of the response.

    Error code: `MethodNotAllowed`

    Error message: `The specified method is not allowed against this resource.`

    Extra fields: `<Method>method</Method><ResourceType>DeleteMarker</ResourceType>`
- *Cloud Storage Object API 2.5 Development* guide (COS-73284)

  New behavior is updated to include the header `x-amz-version-id` in the response for a PUT object for a version enabled bucket only when the versioning mode is ENABLED. Previously, the `x-amz-`

version-id header was included with a value of “null” in the PUT Object response when the versioning mode was SUSPENDED. This behavior is updated and the x-amz-version-id header is not included in the response.

New behavior is updated to include header x-amz-delete-marker with a value of “true” to be returned for GET/HEAD/DELETE object operations only when the object has a delete marker.

– GET/HEAD for an Object in the Versioning Enabled bucket, with a non-existent version returned a 404 error code. However no information was included in the Error code, message and field. New behavior is updated to include the following fields as part of the response.

  Error code: NoSuchVersion

  Error message: The specified version does not exist.

  Extra fields: <Key>object_name</Key><VersionId>requested_version_id</VersionId>

– GET/HEAD for an Object with VersionId which has a delete marker returned a 404 error code. New behavior is updated to return a 405 with the below fields as part of the response.

  Error code: MethodNotAllowed

  Error message: The specified method is not allowed against this resource.

  Extra fields: <Method>method</Method><ResourceType>DeleteMarker</ResourceType>

– GET/HEAD for an Object in the Versioning Suspended bucket using the versionid=null returned a 404 error code. New behavior is updated to return the object if present and return a 200 error.

Chapter 10. Resolved Issues

Resolved issues in 3.15.7 August Maintenance

Table 1. Resolved issues	
Issue	**Description**
COS-82437	Resolved an issue in which container initialization resulted in multiple instances of MySQL running.

Resolved issues in 3.15.7 July Maintenance

Table 2. Resolved issues	
Issue	**Description**
COS-81995	Resolved an issue where slices were not reported in listing operations after an unclean shutdown of Slicestor® Devices.
COS-82376	Improved memory handling of object metadata to reduce CPU utilization spikes on Accesser® Devices under some workloads.

Resolved issues in 3.15.7 June Maintenance

Table 3. Resolved issues	
Issue	**Description**
COS-81854	Support for Conditional Request Headers on Key Protect enabled buckets not operating properly. Clients performing requests on Key Protect buckets that included Conditional Request Headers (as defined by RFC 7232) were receiving 400 Bad Request responses . The list of affected requests are: • PUT object • POST object form based upload • POST initiate multipart upload • PUT object copy • DELETE object. **Note:** With this fix, clients now performing these types of requests will be able to fully utilize Conditional Request Headers.

Resolved issues in 3.15.7

Table 4. Resolved issues	
Issue	**Description**
COS-79332	Temporary loss of drive connectivity during dump-log on systems with J10, J11, J12, and J15 enclosures.

Table 4. Resolved issues (continued)	
Issue	**Description**
COS-79399	Drives larger than 16 TB were prevented from initializing on Slicestor devices when using the packed or file storage engines.
COS-77652	Resolved an issue where there was the potential for the dsnet-core process on a Slicestor appliance to restart upon incorrect detection of permit leak.
COS-81422	Resolved an issue with the Manager's container initializing sequence that caused the Manager application to not start.

Resolved issues in 3.15.6 May Maintenance

Table 5. Resolved issues	
Issue	**Description**
COS-77652	Resolved an issue where there was the potential for the dsnet-core process on a Slicestor appliance to restart upon incorrect detection of permit leak .

Resolved issues in 3.15.6 April Maintenance

Table 6. Resolved issues	
Issue	**Description**
COS-80254	Resolved an issue where upgrades may fail if using custom HTTPS certificates for access pools or storage pools.

Resolved issues in 3.15.6 March Maintenance

Table 7. Resolved issues	
Issue	**Description**
COS-79399	Resolved an issue that would prevent drives larger than 16 TB from initializing on Slicestor devices when using the packed or file storage engines.

Resolved issues in 3.15.6

Table 8. Resolved issues	
Issue	**Description**
COS-72810	GET/HEAD for an Object in the **Versioning Enabled** bucket, with an invalid version would return a 404. New behavior has been updated to return a 400 with the below fields as part of the response: • Error code: InvalidArgument • Error message: Invalid version id specified • Extra fields: <ArgumentName>versionId</ ArgumentName><ArgumentValue>malformed_version_id</ArgumentValue>
COS-78441	POST.OBJECT request was rejected with 403 because duplicate entries were specified in the Policy.

Table 8. Resolved issues (continued)	
Issue	**Description**
COS-78443	Excessive ZSS startup / shutdown time due to journal with 74 zones due to a non-optimal journal capture policy.
COS-78428	Compaction stops in ZSS leading to **`InsufficientStorageException`** across multiple disks on multiple servers.
COS-78177	Resolved an issue with a Radisys appliance logging when there is non-existent serial port.
COS-78762	Core may hang indefinitely during clean shutdown while reallocation is running.
COS-79241	Suspended multipart overwrite deletes previous version data.

Resolved issues in 3.15.5

Table 9. Resolved issues	
Issue	**Description**
COS-77447	Change the status code from 507 to 422 when bucket or vault quota is exceeded. Currently, an HTTP 507 response code is used for a vault or bucket quota violation. Instead, a 422: "Unprocessable Entity" error is returned. This short description of this error is `The request was well-formed but was unable to be followed due to semantic errors.`
COS-77122	Resolved an issue with applying certificate on the IBM COS Manager™.
COS-76944	Resolved DLM issue memory handling due to cgroup.

Resolved issues in 3.15.4 February Maintenance

Table 10. Resolved issues	
Issue	**Description**
COS-78552	Resolved an issue where GET and HEAD requests may have failed with HTTP Status Code 500 during the ClevOS upgrade of Accesser® Appliances.
COS-78315	Resolved an issue where ACL was not set in a scenario of a pre-signed URL PUT request.

Resolved issues in 3.15.4

Table 11. Resolved issues	
Issue	**Description**
COS-75232	Added explicit boolean flag in access logs to define whether an operation was on an embedded content object or not.
COS-76460	Method not allowed on **`delete marker fail`** with a 404.
COS-72822	**`Deleting an Object`** with a **`VersionId`** returns an **`x-amz-delete-marker`** response header.
COS-73284	No Error Message for **`GET object version`** (which got deleted).

Resolved issues in 3.15.3 December Maintenance

Table 12. Resolved issues

Issue	Description
COS-73183	Adding a Generic Device from the Edit Cabinet page was failing. The issue is now resolved.
COS-77152	In prior releases, for Slicestor devices with more than 48 drives and high traffic volume, it is possible for the disk management shut down timer, which monitors the time expected to quiesce the drives, to expire even though the shut down process is still actively making progress. The timer expiration may cause in-flight disk management database operations to be lost. In very rare cases, when disk management restarts, the database may not completely recover. This could lead to drives reporting an inconsistent state. In order to avoid this situation, the command below must be run on each Slicestor device to increase the timer from 2 minutes to 4 minutes, allowing sufficient time for disk management to complete its shutdown. • storagectl configure engine.main.stop_timeout 240 This command must be executed once per Slicestor device prior to an upgrade. The setting will persist across reboots and subsequent upgrades. In this release, the default has been changed from 2 minutes to 4 minutes. For systems being upgraded to a release with this change, the command above must be run on all Slicestor devices prior to upgrade. However, subsequent upgrades and new installations do not require this command to be executed. For any questions, please contact IBM Customer Support.

Resolved issues in 3.15.1 October Maintenance

Table 13. Resolved issues

Issue	Description
COS-75266	In prior releases of the Concentrated Dispersal (CD) feature (3.12 and later), the re-calculation of weights for CD sets was not being performed properly. The Manager will now re-calculate weights for CD sets if the storage pool is expanded or a set is removed/replaced. Furthermore, the Manager will notify the operator a CD set can be resized if usable capacity has changed. This behavior was previously suppressed for CD sets and was only available to standard storage pool sets.
COS-75788	Resolved an issue that prevented manual tuning of request scheduling on Slicestor appliances.
COS-76394	Resolved an issue where sequential named writes may see a performance degradation with named index feature enabled sequential.

Resolved issues in 3.15.1 September Maintenance

Table 14. Resolved issues

Issue	Description
COS-75370	Resolved an intermittent issue where a Slicestor device would occasionally experience hung I/O operations under heavy load, which would result in the storage service being shutdown.

Resolved issues in 3.15.1

Table 15. Resolved issues

Issue	Description
COS-71105	In previous releases, hard quota was not being enforced for POST object requests. Starting from 3.15.1, check against the hard quota has now been added and will be enforced for POST object requests going forward.

Resolved issues in 3.15.0

Table 16. Resolved issues

Issue	Description
COS-70873	Resolved an issue to prevent network saturation under certain conditions.
COS-63621	Resolved an issue where a DLM crash could have caused corruption of configuration database

Chapter 11. 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 17. Product Alert Notifications for the IBM Cloud® Object Storage System

Alert Notification Title	Impacted ClevOS Releases	Alert Notification Published Date
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
IBM COS Slicestor® 2584 Fails to Attach Drives	ClevOS independent	Feb 2, 2017

Chapter 12. Known issues

Table 18. 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-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.

Table 18. Known issues (continued)

Issue	Failing Condition	Disposition
COS-7488	When performing a storage pool set removal, it is possible that once the reallocation has finished for a source Slicestor device, it can show some small amount of data still present.	No action is required. Once the set removal has completed, all slices have been reallocated to the new storage pool. Any discrepancy in a Slicestor device's used space is generally a result of small inaccuracies that can occur during normal usage of the system.
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-22990	The S3 remote proxy implementation of vault proxy has a few limitations that are related to communicating with an Amazon S3 endpoint. The version of the AWS SDK used to communicate to Amazon defaults to using V2 instead of V4 authentication, causing authentication issues when communicating with certain AWS endpoints.	For further assistance in configuring a remote proxy for use with Amazon S3, contact IBM customer support.
COS-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.
COS-29681	When using the Microsoft IE9 web browser, certain Manager user interface elements like the left navigation panel and the vault capacity bar charts on the Monitor Vault page cannot appear.	Microsoft has ended support of IE9 and IE10. Users should upgrade to Microsoft IE11 or higher, or use an alternative browser, such as Firefox, Safari, or Chrome.
COS-64358	If an Accesser device restarts during a cycle , a small number of object deletions may be delayed up to 72 hours.	This issue will be fixed in a future release.

Upgrading and Installation

Table 19. Upgrading and Installation

Issue	Failing Condition	Disposition
	Nothing to report	

Container

Table 20. Container

Issue	Failing Condition	Disposition
COS-1852	When attempting to write an object to a container that does not exist, the Accesser appliance returns an HTTP 404 response with an error message of NoSuchKey instead of the appropriate NoSuchBucket. This includes cases where the container name includes a "/".	Ensure that your vault or container is successfully created before attempting to write objects to it. If you receive an error message of NoSuchKey for an upload request, verify that the container you are addressing does exist.
COS-15401	If a user attempts to create a management vault 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 21. Alerting and reporting

Issue	Failing Condition	Disposition
	Nothing to report.	

System Behavior

Table 22. System behavior

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

Storage Pools

Table 23. 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 24. Data evacuation

Issue	Failing Condition	Disposition
	Nothing to report.	

System Configuration

Table 25. System configuration

Issue	Failing Condition	Disposition
	Nothing to report.	

Deleting objects

Table 26. Deleting objects

Issue	Failing Condition	Disposition
	Nothing to report.	

Manager Web Interface

Table 27. 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.

Table 27. Manager Web Interface (continued)		
Issue	**Failing Condition**	**Disposition**
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 28. Vaults		
Issue	**Failing Condition**	**Disposition**
	Nothing to report	

Vault Mirrors

Table 29. Vault mirrors		
Issue	**Failing Condition**	**Disposition**
COS-7019	When performing IO against a vault mirror with synchronous writes disable, HEAD requests performed against a successfully written object may return an HTTP 404 response.	If an HTTP 404 is returned for a HEAD request for a recently written object, please retry your request.

Vault migration

Table 30. 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 13. Supported Hardware Platforms

IBM Cloud Object Storage Appliances

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

Product Name	Machine Type (1Yr/3Yr Warranty)	Model	Minimum ClevOS
IBM COS Accesser® 3105	3401/3403	A00	3.8.1
IBM COS Accesser® 4105	3401/3403	A01	3.8.1
IBM COS Accesser® 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 32. Minimum Version of ClevOS Compatible with Hewlett Packard Enterprise Hardware

Appliance	Model	Minimum ClevOS
Manager Appliance	DL360P Gen8	3.2.1
Manager Appliance	DL360 Gen9	3.5.0
Manager Appliance	DL380 Gen9	3.5.0
Accesser® Device	DL360P Gen8	3.2.1
Accesser® Device	DL360 Gen9	3.5.0
Accesser® Device	DL380 Gen9	3.5.0
Slicestor® Device	SL4540 Gen8	2.9.0
Slicestor® Device	DL380 Gen9	3.5.0

Table 32. Minimum Version of ClevOS Compatible with Hewlett Packard Enterprise Hardware (continued)		
Appliance	**Model**	**Minimum ClevOS**
Slicestor® Device	Apollo 4200 Gen9	3.6.0
Slicestor® Device	Apollo 4510 Gen9	3.6.0
Slicestor® Device	Apollo 4510 Gen10	3.14.0
Slicestor® Device	Apollo 4530 Gen9	3.6.0

Seagate

Table 33. Minimum Version of ClevOS Compatible with Seagate Hardware		
Appliance	**Model**	**Minimum ClevOS**
Seagate OneStor®	AP-2584 1 AP-TL-1	3.4.2
Seagate Exos®	AP 5U84-Laguna Seca	3.15.0

Cisco

Table 34. Minimum Version of ClevOS Compatible with Cisco Hardware		
Appliance	**Model**	**Minimum ClevOS**
Cisco Slicestor® Device	UCS C3260	3.7.4
Cisco Slicestor® Device	UCS S3260 (Single Node)	3.12.0
Cisco Slicestor® Device	UCS S3260 (Dual Node)	3.12.0
Cisco Slicestor® Device	UCS S3260 M5 (56 drive configuration)	3.13.1
Cisco Slicestor® Device	UCS S3260 M5 (60 drive configuration)	3.14.3
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 35. Minimum Version of ClevOS Compatible with Dell Hardware		
Appliance	**Model**	**Minimum ClevOS**
Dell Slicestor® Device	DSS 7000	3.10.1
Dell Slicestor® Device	R740xd w/ HDD Support	3.14.1
Dell Slicestor® Device	R740xd w/ NVMe Support	3.14.2

Lenovo

Table 36. Minimum Version of ClevOS Compatible with Lenovo Hardware

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

Quanta Cloud Technology (QCT)

Table 37. Minimum Version of ClevOS Compatible with QCT Hardware

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

Chapter 14. Incompatible Hardware and Firmware with ClevOS

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

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

Broadcom

Table 38. Broadcom Hardware and Firmware Incompatibility with ClevOS

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

Hewlett Packard

Table 39. HP Hardware and Firmware Incompatibility with ClevOS

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

IBM Cloud Object Storage Appliances

Table 40. IBM COS Hardware and Firmware Incompatibility with ClevOS

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

Seagate

Table 41. Seagate Hardware and Firmware Incompatibility with ClevOS

Type	Model	Firmware affected
HDD	Seagate ST1000NM0033-9ZM173	SN04

Supermicro

Table 42. Supermicro Hardware and Firmware Incompatibility with ClevOS

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

Notices

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

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

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

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

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

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

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

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

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

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

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

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

US

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

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

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

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

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

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

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

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

COPYRIGHT LICENSE:

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

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

Trademarks

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

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

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

Printed in USA