IBM Cloud Object Storage System™
Version 3.8.3

Release Notes

COSRN_3800-20160516L

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

Contents

Support information

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

Chapter 1. New Features and Improvements

New Features and Improvements in ClevOS 3.8.3 February Maintenance

PSS Manual Compaction Throttle

A set of System Advanced Configuration properties have been added to provide extra mechanisms of control for the compaction process that is used in storage pools utilizing Packed Slice Storage (PSS). The compaction process is used to reclaim unused space on an individual disk of a Slicestor® device, such as when object deletion is performed. By default, when the compaction process is triggered, it runs as fast as the disk allows to ensure that all available space is made available as quickly as possible. In some cases of heavy object delete workflows, the compaction process consumes such a high percentage of the overall disk bandwidth that client object I/O is negatively impaired. The newly introduced System Advanced Configuration properties allow the administrator to specify the maximum rate at which PSS compaction is allowed to run on each disk of a Slicestor device. For more information on how to use these properties, contact IBM® Customer Support.

Interface Modifications

A new response parameter for the List Vaults method has been added that provides an estimate of the vault object count. Look in the IBM Manager REST API Guide for more information.

New Features and Improvements in ClevOS 3.8.3

Native File Access

This new feature is designed to provide a Network Attached Storage (NAS) interface to the IBM Cloud Object Storage System™.

The user is able to create multiple NAS volumes (File Systems), each with storage backed by the system. The feature exposes user-defined Network File System server (NFS version 3) exports, which you can mount and interact with as you would expect from a typical NFS server. File metadata is managed and maintained by a clustered database solution, and file data is stored in the system. The system is scalable linearly as nodes are added.

Note: Additional IBM hardware is required to support this functionality (IBM COS Accesser F5100 (3401-A02, 3403-A02).

Hardware

This release introduces support for the following hardware:

- Accesser F5100 is the hardware component of the new Native File Access capability. A minimum of 3 Accesser F5100s are required, 6 in the case of multiple site deployments with a requirement to maintain file access to IBM COS with any one site offline.
- Slicestor 3448 Appliance is a 4U Slicestor that can be populated with 16, 32 or 48 data drives and uses the same chassis as the Slicestor 2448. The Slicestor 3448 uses a faster CPU and more memory to offer higher performance than the Slicestor 2448.

Note: Refer to the Appliance Manuals for Additional Information.

Performance

Selective Events, a performance optimization feature, yielded very significant improvements in small file (40%) and medium file (10%) write performance in Accesser® appliance bounded conditions (PSS, S3, Index On).

New Features and Improvements in ClevOS 3.8.2

Restricted Visibility to AWS Secret Keys in Manager GUI / REST API [877]

To enhance management of AWS Secret Access Keys, a new feature has been added to restrict visibility of these keys. This feature can be turned on through the "Enable/Disable Authentication Mechanisms" section of the Security tab on the Manager User Interface or through the Manager REST API. Once enabled, existing Secret Access Keys will no longer be accessible. Newly created Access Keys will allow Secret Access Keys to be visible one-time only. The feature cannot be disabled unless all Access Keys are deleted from the system. For additional information, please see the Manager Administration Guide and the Manager REST API Guide.

New Features and Improvements in ClevOS 3.8.1

Enhanced TLS ciphers and Key Exchange [854]

This release has an **updated list of default-enabled cipher suites**. The next section has a detailed description of this feature introduced in the 3.8.0 release.

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA

Forward Audit Messages Sylog [14177]

An enhancement has been provided to forward audit messages generated on the Manager device over Syslog. This capability is available in the Syslog section of the Alert Forwarding Configuration page (select "Configure Alert Forwarding" on the Administration tab). To enable, check the "Forward Audit Messages Over Syslog" box.

Note:
When using an Appliance Docker Container, administrators should avoid the use of *localhost* as a hostname for both the container instance (if using `--net=bridge` when invoking the container) and the host machine (irrespective of container configuration). See the *Appliance Container Administration Guide* for more information regarding configuring the hostname of the container.

New Features and Improvements in ClevOS 3.8.0

Click Through license [858]

This release introduces a "click through license" feature, which contains new End User License Agreement (EULA) content. It is expected that every customer accepts this newly documented EULA with IBM. The

feature will require a customer to view and accept the license agreements via the Manager user interface, before they are allowed to use the 3.8.0 version of ClevOS software in two scenarios: 1) during a new software installation process and 2) upgrade to the 3.8.0 release. During 3.6.X/3.7.X to 3.8.0 upgrade, a manager upgrade will be allowed, but the customer must accept the license agreements before they upgrade devices. For 3.8.0 to subsequent release upgrades (subject to N-2 constraints), the license agreements need to be accepted before the manager can be upgraded.

Mirror Template [394]

The mirror template feature introduces a capability similar to vault templates, but is separate and distinct. Functionality is provided to create, edit, and delete mirror templates. Two vaults will need to be taken into account. Similar to vault templates, the mirror template needs to address associations with a storage pool.

Update Virtual Machine Compatibility [438]

This feature upgrades the Virtual Hardware Compatibility matrix for VMs running on a VMware platform. Virtual Hardware provides common sets of hardware/resources available for VMs; each revision/version includes bug fixes, performance improvement, and a resource limit increase. This feature iteration upgrades the VMware Virtual Hardware version from 7(vmx-07) to 10(vmx-10). After the Virtual Hardware version is upgraded to 10, all ClevOS appliances, as a VM, will require VMware vSphere version 5.5 or higher to run successfully. In the case where a ClevOS VM is required to run in a version of VMware vSphere older than 5.5, you must contact IBM Support to make the ClevOS VM compatible with an older version of VMware.

Locked Vault [490]

This feature introduces support for a private vault using an account that has very limited visibility. This account only has vault provisioner privileges. CreateVaultFromTemplate API is used to create vaults by the external application using a certificate issued by the Manager. The external application has to register the CSR with the Manager before it can start interacting with the Manager using the API.

Version History Report [679]

The Manager now provides an API to collect software version history records for all devices in the system. Devices can be filtered by ID, type, storage pool, and storage pool group. Version history records for devices can be filtered by software version as well as start and end timestamps.

Data Migration Service [353]

The Data Migration Service allows for vault level data migration. Objects are copied from a source vault to a target vault. Objects on the source vault are not deleted. The vault proxy feature enables seamless access to objects on both source and destination during migration.

Embedded Accesser [593]

This release introduces support for Embedded Accesser, which provides Accesser functionality on the Slicestor appliance. This feature provides customers an opportunity to save on capital expenses by using one physical appliance for both Accesser and Slicestor functionality. However, before deploying this feature careful consideration needs to be given to the Slicestor hardware and the workload presented to the servers and the load balancing between the available Slicestor appliances.

Presumptuous Writes [694]

The Presumptuous (skip read before write) feature can lower average latency and increase max system operations per second for small object writes over named object interfaces (S3, Swift, WOS) when the

fraction of writes that are overwrites is low. By default, when data is written to an Accesser over a named object interface, the Accesser tries to read the object from Slicestors to check for an existing revision, then will proceed with the write, commit, and finalize steps. The Accesser can optimistically skip the read operation, and try to write a new object. If no object existed with the object's name, the operation will succeed and one round trip to the Slicestors will be saved. However, if an object with the same name did exist, then the Accesser will roll back the operation, and then proceed with the normal read, write, commit, and finalize steps, resulting in lower performance due to the extra round trip of the initial write. To gain the benefit of this feature while not degrading performance when overwrites are common, Accessers will only skip the read before writing to a vault when the historical average fraction of writes that are overwrites for the vault is below a threshold (0.2 by default). This historical average for the vaults is kept with a exponentially weighted moving average so that the average responds to changing write behavior over time.

Settings for this feature can be applied through system advanced configuration for Accessers or Slicestors with embedded Accesser services.

Enhanced TLS ciphers and Key Exchange [854]

This release introduces several security enhancements for clients connecting to the system Accesser over HTTPS. Encryption and key agreement algorithms considered weak by modern standards have been removed from the default set of enabled algorithms. These algorithms include RC4 encryption and Diffie-Hellman key agreement. In addition, support for Elliptic Curve based key agreement and server preference ordering has been added. Note that these enhancements have the potential to prevent clients using old SSL implementations from communicating with the Accesser over HTTPS. If your applications are still using these older cipher suites, contact IBM Support.

The full list of default-enabled cipher suites and their preference order is:

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256

Manager Enhancements

1. This enhancement lists Vault Templates in the viewSystem API response. This capability is currently supported in the UI, however it was not currently supported via the Manager REST API. The View System API response now includes information on Vault Templates.
2. For systems configured to use SFTP as the transfer protocol for Manager backup files, a security update has been provided. This enables integration support with a wider range of customer-managed SFTP servers, specifically those which are configured to disable the use of SHA-1 and instead exclusively enable only algorithms from the SHA-2 family.
3. A new field has been added to the View System API called storagePoolGroups (a storage pool group corresponds to a storage pool on the Manager user interface). The introduction of this field, coupled with filtering support in the Manager REST API, allows a user to more easily associate vaults with storage pools. See the Manager REST API documentation for details.

Chapter 2. Resolved Issues

Resolved issues in 3.8.3 June Maintenance Release

Table 1. Resolved issues

Issue	Description
COS-16555/14194	Delete operations for legacy SOH content can expose a race condition in the Accesser device's segment cache. This race condition can lead to an under-reporting of the size of the cache, leading to memory pressure and high GC's. This release introduces a fix for this condition.
COS-11741	After the manager prevents an N+3 or greater upgrade to the IBM COS system, this release allows a user to load the correct upgrade file and upgrade the devices to a software version consistent with the manager.
COS-9458	Idle Slicestor devices that are part of a storage pool utilizing the File Slice Storage engine would intermittently show events in the Manager event console that the device is not properly reporting status. Modifications were made to reduce the memory pressure being seen to avoid periods of unresponsive behavior.

Resolved issues in 3.8.3 April Maintenance Release

Table 2. Resolved issues

Issue	Description
COS-13569	DMS is not completing due to a negative number returned by stats.
COS-13820	Manager backup fails due to mysql killed by OOM.
COS-13242	CPU bounded High Latency observed in level-db results that is due to high concentration of delete markers.

Resolved issues in 3.8.3 March Maintenance Release

Table 3. Resolved issues

Issue	Description
COS-12285	Mirror template vault width selection at the manager for storage pools of width greater than 10.
COS-8028	Seagate - AP-2584 - Failed with timeout after Upgrade from 3.7 to 3.8.
COS-11595	IBM 2584 , mpt2sas not all Drives are attached after reboot.
COS-12288-9829	Handling of the Prioritization Filter

Resolved issues in 3.8.3 February Maintenance Release

Table 4. Resolved issues

Issue	Description
COS-7397	The dsnet-core process crashed after completing failing disk migration.

Resolved issues in 3.8.3 January Maintenance Release

Table 5. Resolved issues

Issue	Description
COS-8723	When performing concurrent delete operations on the same object, it is possible for listing requests which contain this object name to result in an HTTP 500 error. Introduced a software fix that prevents the error from occurring when this state is encountered.
COS-8208	When a system expansion is in progress and a vault is deleted, it is possible that a subset of the system reported statistics will stop being reported. In particular, the statistics for incoming and outgoing reallocation will stop reporting for the destination and source Slicestor devices respectively. Resolved an internal error that was causing all statistics to become unavailable when reallocation encountered a deleted vault.
COS-9343	S3 put copy holds onto write permit forever when source not found.
COS-8332	REST API call for Storage Pool Capacity and Disk ReportExport returns a 500 error.
COS-9480	PUT failures observed in the vault, when trying to overwrite a tombstone.
COS-8831	Addressed an issue where sustained IO failures would cause many vault failure events to be generated and sent to the Manager. Under heavy load conditions, this may cause Accesser appliances to become unresponsive. This fix introduces throttling for events, such that only one event will be generated per vault every 5 minutes. The event console on the System Manager UI may group common events together based on the request type. As a consequence of fewer events being reported, if the affected IO pattern consists of multiple requests types, then this may result in multiple groupings for each request type for the duration of the outage.

Resolved issues in 3.8.3 December Maintenance Release

Table 6. Resolved issues

Issue	Description
COS-7357	GET requests on objects uploaded as AWS chunked were including "Content-Encoding: aws-chunked" in the response headers, even though per the Amazon S3 reference for AWSv4, "S3 will store the resulting object without the aws-chunked encoding. Therefore, when you retrieve the object it will not be aws-chunked encoded."

Resolved issues in 3.8.3

Table 7. Resolved issues

Issue	Description
14811	Resolved an issue in the Manager user interface, when creating email alerts with Chrome on a MacOS, the scroll bars for filter event sources and event categories may not show up.
COS-2974	Under certain circumstances, not receiving a response from a disk read (the disk hangs for a given request) may hang parts of the core process. This may prevent other functions from completing like reallocation and orderly process shutdown.
COS-7255	Certain workload conditions that involve reading content through NFI may result in OOM issues on the filer process.
COS-4944	Intermittent Ranged reads were being observed for a slow client due to End of Stream exceptions.
COS-2657	File Server is a new device type that was added in this release. If Log Collection is being used, and if you want the File Server to be included, mark the checkbox for FileServer Devices in the log collection configuration on the manager . Similarly if Device Level API is being used, and if you want the File Server to be included, mark the checkbox for FileServer Devices in the Device Level Api Configuration on the manager .

Table 7. Resolved issues (continued)

Issue	Description
COS-1555	Previously, the drive report API failed for the following platforms: 'SSG-4UDPV3-2C0-CC075', 'SSG-4UDPV3-2C1-CC075', 'SSG-4UDPV3-2C2-CC075', 'SSG-4UDPV3-2C3-CC075', 'X9DRD-7LN4F', 'SYC-CDE465-CI025', 'HP ProLiant XL450 Gen9 Server'. Now, this API works as expected.
COS-6317	Intermittent 403 responses due to signature mismatch. Code was changed to force dsnet to wait, while trying to read, and until an EOS is received. This makes sure that everything is read before the system advances.
COS-6078	During heavy load, especially in the presence of conflicts or contention, the Accesser Appliance can encounter extremely long GCs, which cause the Accesser Appliance to become unresponsive. This release introduces a fix for this issue.
COS-6989	If a request contained a header with a value that contains multiple adjacent whitespace characters, the signature validation algorithm does not properly trim intermediate whitespace characters, which causes signature mismatches and ultimately HTTP 403 errors for AWS V4 signed requests. The signature calculation algorithm has been updated to properly handle intermediate whitespace characters.
COS-6139	When performing write-delete-overwrite workflows, it is possible to get into a state where an individual object cannot be updated, and PUT requests fail with a HTTP 500 error. The fix for this issue is to maintain a cache of recently encountered revisions that can be used to differentiate between internal states which lead to the update failures.

Resolved issues in 3.8.2 October Maintenance Release

Table 8. Resolved issues

Issue	Description
COS-2402	In previous releases, on the Monitor Storage Pool page, if devices experience communication issues, in certain scenarios, the expanded list of devices that are associated with a given problematic device is not viewable. The issue has been resolved in this release.
COS-3097	In prior releases, SNMP traps 205 (connection OK) and 206 (connection Idle) are erroneously sent when the LDAP connection state changes between OK and Idle. In this release, trap notifications that are related to these state changes are no longer sent.
COS-1418	Resolved an issue where memory was being unnecessarily allocated for performing disk write operations, which was not being reclaimed.
COS-2918	Before this release, the drive report API failed for the following platforms: 'SSG-4UDPV3-2C0-CC075', 'SSG-4UDPV3-2C1-CC075', 'SSG-4UDPV3-2C2-CC075', 'SSG-4UDPV3-2C3-CC075', 'X9DRD-7LN4F', 'SYC-CDE465-CI025', 'HP ProLiant XL450 Gen9 Server'. Now, this API works as expected.
COS-2939	In previous releases, the Slicestor 2448 appliance drive bay names were being reported incorrectly. For example, drive bay A1 was being reported as drive bay B1 and vice versa. The issue has been resolved by adjusting the drive bay names in ClevOS to match the hardware cabling.
COS-2015	This release addresses an issue where a change in behavior on Mellanox network interface may cause unreliable network interface naming. This can manifest as network interfaces coming after boot with different names than were configured which can cause outages. This affects HP SL4540, Seagate Onestor, IBM 2584 appliances.
COS-2807	In prior releases, when a user submits a request using AWS V4 authentication and one of the request query parameters contains a tilde character, the request will be rejected with a 403 Invalid Signature error. The signature verification algorithm has been updated to match the documented AWS v4 specification.

Resolved issues in 3.8.2

Table 9. Resolved issues

Issue	Description
14838	Fixed an issue where Accesser Appliances configured with an External CA may cause client I/O to become blocked while performing a lookup of the CRL from the remote distribution point. In cases where this remote distribution point was not accessible, I/O would be blocked until a 30 second disconnect timeout was reached.
14825	Fixed an issue where signature validation would fail when using AWS Authentication Signature Version 4 with unsigned payloads.
14810	To address security concerns prior to authentication, the login screen for the Manager user interface no longer displays the ClevOS version in the footer. All other pages will continue to display this information as before.

Resolved issues in 3.8.1

Table 10. Resolved issues

Issue	Description
14177	An enhancement has been made in Syslog section in Alert Forwarding Configuration page which allows to forward Audit messages generated from manager device over Syslog that can be enabled by checking, Forward Audit Messages Over Syslog (Audit messages are generated on Manager device only)
14415	On the Disk Drive and Device Report, certain columns (Cabinet, Slot, Chassis ID, Node Location and Node Count) were previously displayed only for systems to which they were applicable (systems utilizing cabinets or multi-node servers). In an effort to maintain consistency and backward compatibility, these columns will now always be displayed in this report.
14464	Erroneous column Drive Size on the Disk Drive and Device Report has been replaced with the new column Drive Capacity, which is accurately reporting capacity of the Disk Drive.
14579	Resolved an issue where a lock was preventing more than one thread from processing slice fanout operations during reads and writes..This had the potential to result in very slow failing disk migration, disk rebalancing, rebuild, and reallocation operations on slice fanout objects.
14688	Resolved an issue where a race condition was causing network requests to be lost or duplicated when a client was disconnected. Such requests would not complete until the system-core process was restarted, which had the potential to prevent the rebuild process from making progress.
14695	An issue has been fixed where a request that was rejected with a HTTP 503 response would record the response entry in the http log, but not the access log.
14708	An issue has been fixed where requests that were authenticated using either AWS SigV4 would not properly accept either the 'Date' header or 'X-Amz-Date' header for specifying date information for the signed request.
14579	Resolved an issue where a lock was preventing more than one thread from processing slice fanout operations during reads and writes..This had the potential to result in very slow failing disk migration, disk rebalancing, rebuild, and reallocation operations on slice fanout objects.
13897	While error code 3 may occur for a number of reasons, one particular scenario can occur when an internal error prevents the post-upgrade data integrity checks from proceeding. This error is not harmful or indicative of data corruption but rather an inability to execute the integrity checks used aspart of the upgrade orchestration process. The device will service I/O operations in the normal manner while in the inconsistent state but additional upgrades will be blocked until the condition is cleared.

Table 10. Resolved issues (continued)

Issue	Description
14374	The timestamps for the events in the rectangular view directly below a performance graph are off by 1 hour compared to the corresponding timestamp displayed in the main Event Console. The timestamps in the main Event Console are correct. Adjust the timestamp for any events in the rectangular view by 1 hour.
14441	The incoming connection count alert thresholds are currently set at substantially lower values than the maximum allowable connection count. As a result, incidents such as the one below can be misleading: "The incoming connection count of 1995 is close to the maximum of 20000. Please contact IBM Customer Support.". There is no service impact with this alert, unless 20,000 connections are exceeded. Contact Customer Support to change the alert thresholds on the system and help monitor the number of incoming connections.
12640	On some HP Gen9 Slicestor® Device platforms, drives may be offlined bythe disk controller, resulting in hung tasks. Those hung tasks arereported on the manager and the device will be offlined. The user must power cycle the device to clear the condition. This issue is fixed in this release.
13536	It has been observed that when performing read IO while the system is below threshold, system memory may be consumed and never released. If this condition persists, all available memory may be consumed, leading to HTTP 503 errors. This issue is fixed in this release.
14804	Fixed an issue where the core process on an Accessor Appliance may spontaneously restart during periods of network variability when performing IO operations on a vault with a width of 32 or greater.

Chapter 3. Known issues

Table 11. Known issues

Issue	Failing Condition	Disposition
14274	For client workloads that involve multipart upload on vaults deployed on file storage based storage pools, the multipart transaction index is used to determine whether or not a particular upload id exists in the system. Upon upgrading to this release, multipart index operations will use the index delegation feature by default.	This can lead to the situations where the index cache state on the Accesser appliance is out of sync with the state of the index on the dsnet, which may lead to multipart part uploads erroneously failing with the error message NoSuchUploadId. If this scenario is observed, please contact IBM support for further guidance.
14777	Versioning state watcher returns before new state is found in the registry	When performing a CSO API request to enable versioning on a vault, the request may return successfully to the caller before this change has taken effect on all nodes. To avoid issues associated with this please wait 60 seconds after changing the versioning state of a vault to ensure that the change has taken effect across all devices before proceeding.
14714	When performing heavy write IO to an empty vault, with index enabled and index delegation enabled, the index insertion operations on the index will take priority over asynchronous split operations, possibly causing the nodes in the index to become large.	The user can avoid this issue by pre-filling the vault with objects. If this condition persists, this can lead to increased latencies and IO failures. Contact IBM Support to confirm scenario.
14783	Problem Under certain circumstances, Slicestor® Device devices using MegaRAID SAS disk controllers may not immediately detect the removal or replacement of a drive.	A replacement drive should not be added until 90 seconds after the original drive is removed to allow the kernel time to finalize the removal of the device.
14591	Kernel panic detected on devices utilizing Avago MegaRAID SAS controllers..	Contact IBM Support to confirm scenario.
14639	An issue has been seen where client listing operations, or ongoing Data Migration activities, in the presence of a failed drive can cause listing operations to queue up in memory. Over time, this can cause significant memory to be consumed, leading to out of memory conditions and a core process crash.	Contact IBM Support to confirm scenario.
14770	On the Edit Access Pool page within the Manager user interface, when access device or vault deployment changes are made and the "Update" button is selected on the lower action bar, a popup confirmation dialog appears outside the view of the web browser window.	The issue can be bypassed entirely by selecting the "Update" button on the upper action bar within the Edit Access Pool page. Otherwise, scroll down to see the confirmation dialogue.
14581	Device with quarantined drives are not included in the Communication error widget.	In the Manager user interface, the "Communication Issues" view that appears on the Monitor Access Pool and Monitor Storage Pool pages, this view does not include devices in the warning (yellow) state.
14828	When using the AWS .NET SDK to create a vault, the SDK client uses an improper xml schema when performing the put bucket request, causing the request to fail with a HTTP 400 error.	As a workaround, clients can create vaults using an SDK for a different language, or create the vault by means of the Manager UI or REST API.

Table 11. Known issues (continued)

Issue	Failing Condition	Disposition
COS-2104	When issuing a PUT Bucket request for a vault or container that already exists, and a query parameter is provided with the request, the Accesser appliance will incorrectly return a HTTP 400 response code instead of a HTTP 409 response code.	Please retry the operation with query parameters omitted.
COS-4095	The passwordAuthenticationEnabled parameter of the Edit Authentication Mechanism Manager REST API will not take effect when it is the only parameter used in the API. However, if the accessKeyAuthenticationEnabled parameter is used in conjunction with passwordAuthenticationEnabled, the passwordAuthenticationEnabled parameter will work properly.	Contact IBM Support for additional assistance.
COS-2824	Locked vaults reporting zero usage can be deleted from the UI/API. For name index enabled locked vaults, even after deleting all objects, vault still report some data due to left over root index node on the vault. In this scenario, user is still allowed to delete locked vault based on the following checks: if reported usage on vault is less than 1MB then a recovery listing is done to get the accurate object count on the vault, only when the count is zero the user is allowed to delete the locked vault.	Contact IBM Support for additional assistance.
COS-2983	Nut activation would fail and roll back if no global or local ssh keys were set .	Upgrade to latest build, add global keys via the manager web client, or add keys manually in the nut shell .
COS-2498	The usage of a disk is counted while the disk is offline. However it's capacity is not counted.	No action. Awareness of limitation. If absolutely necessary a restart of core would fix the usage values. Limit dlm events
COS-5562	The troubleshooting console may incorrectly filter devices when selecting a storage pool, access pool, or site with an ID >= 10, resulting in a larger number of devices than expected.	Select devices individually or select multiple filters for storage pool, access pool, or site to limit the results.
COS-5473	The Storage Pool Capacity and Disk Report API output shows the wrong value (always zero) for percentageOfFreeSpace in the All Sets section.	Contact IBM Support for additional assistance.

Upgrading

Table 12. Upgrading

Issue	Failing Condition	Disposition
	Nothing to report.	

Alerting and Reporting

Table 13. Alerting and reporting

Issue	Failing Condition	Disposition
7598	In the following scenario, a drive is quarantined, pulled, permanently removed, disposed, Slicestor® Node powered down, drive replaced, and Slicestor® Node powered back up. The following incident appears and will remain in the Open Incident view of the Manager Web Interface: .Open Incident for Removed and Replaced Drive ==== Disk in drive bay X with S/N Y is a previously removed disk ==== **`Disk in drive bay X with S/N Y is a previously removed disk`** endif::[]	Contact IBM Support to close the incident.
7714	The Storage Pool Capacity and Used graph on the Monitor storage pool page will show a temporary drop in the capacity at times, particularly during upgrade. When upgrading, this is caused by timing issues between the polling of values and when the node values stabilize.	Once node upgrades complete, the capacity returns to normal. The capacity drops can be correlated with upgrade events in the Event Console for nodes in the storage pool.
11739	After recovering from an unresponsive IPMI controller, the open incident in the Manager event console sometimes fails to clear. The open incident is misleading, but has no impact on the system operation.	Contact IBM Support to confirm and correct the false incident.
12450	If a previously failed disk is reinserted into a Slicestor® Device and the system-core process is running, it generates an incident on the Manager indicating that a previously failed disk was reinserted. Normally, when said disk finally gets replaced, this incident clears. However, if this disk is replaced when the device is powered off or when, for any reason, the system-core process is not running, this incident will not get cleared but remain open forever.	If this situation occurs, contact IBM Support for assistance in manually clearing the incident.
14438	When viewing the Message Acknowledge Time graph with Firefox, a portion of the legend appears outside of the graph area.	There is no functional impact. To address this issue, use Safari or Chrome.

System Behavior

Table 14. System behavior

Issue	Failing Condition	Disposition
10659	Some drive-related SNMP traps may not appear immediately. If these events occur during early boot of the appliance or while critical system processes are down, there will be a delay in the delivery of these SNMP traps.	Once the appliance is fully up and running, the SNMP traps will be delivered as expected.
14296	Under conditions where an unresponsive or zombie Slicestor® Device is present in the system, performing multiple large object uploads in parallel may cause uploads to hang. This is caused by a resource starvation issue, in which the outstanding write requests to the zombie store cannot be canceled, and the associated resources freed, until the large object upload completes.	This issue is mitigated on IBM Cloud Object Storage Accesser® appliances with larger amounts of memory available. As a workaround, ensure that any potential zombie or unresponsive Slicestor® Devices are dealt with promptly.

Table 14. System behavior (continued)

Issue	Failing Condition	Disposition
14396	When performing multipart upload requests, especially in cases where multiple parts are uploaded in parallel, it is possible to observe degraded performance and metadata contention when the number of parts per multipart transaction grows large.	To mitigate the impact of this scenario, it is recommended that customers adjust the size of their parts such that an entire multipart upload does not exceed 1,000 parts.
14383	It has been observed that for ZTDG Accesser Appliances there are instances where the system time is not properly reported to the application layer, causing negative values to be reported in the stat entry in the device's access log.	This does not affect the proper operation of the system and will be addressed in a future release.
14425	Drive failure LEDs are not functional on HP Gen9 appliances.	This issue will be resolved in a future ClevOS release.

Storage Pools

Table 15. Storage pools

Issue	Failing Condition	Disposition
12355	On the *Monitor Storage Pool Page, the **Reallocation Progress** graph, which displays historical data, will be 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 current status and should be used to monitor progress of the data reallocation activity.

Security

Table 16. Security

Issue	Failing Condition	Disposition
AES-GCM ciphers (F854)	Performance of the native Java™ 8 implementation of AES-GCM ciphers is extremely poor and these ciphers have been defaulted to off in this release. Users should not enable these ciphers unless they are prepared to accept the poor performance that will result from their use.	A future ClevOS release will address the AES-GCM performance issue.
12058	The Diffie-Hellman (DH) algorithm used in HTTPS communication to/from the manager appliance is less secure than previously believed due to the possibility of logjam attacks.	No immediate change is required for the Manager application. To mitigate the risk of such attacks, support for export-strength cipher suites has been disabled, and Elliptic-curve Diffie-Hellman (ECDHE) key exchange has been adopted. A future ClevOS release will address the generation of strong and unique DH groups, as well as parameter configuration.
14436	When using AWSv2 authentication via the CSO API, if the user provides an access key id that is either null or an empty string, the system will respond with an HTTP 500 instead of the desired HTTP 403 response code.	Incorrect response code can be ignored.

Data Evacuation

Table 17. Data evacuation

Issue	Failing Condition	Disposition
13774	It has been observed that after data evacuation completes, the total evacuation bytes in the event console message indicating X out of Y evacuated isn't always byte-accurate.	Look at the destination Slicestor® Devices to see how much data is actually stored on it.
14465	If data evacuation is paused and then resumed, the progress bar in the Manager UI does not increase until evacuation is completed.	Data evacuation progress can be monitored by observing the allocated device capacity on the destination device. The data evacuation progress bar will be corrected in a future ClevOS release.

System Configuration

Table 18. System configuration

Issue	Failing Condition	Disposition
11405	On certain classes of drives (desktop), it has been observed that the drives can transition to a read-only state when quarantined. If this occurs, a subsequent attempt to fail the drive and migrate its slices to adjacent drives will be unsuccessful. Under normal circumstances this is not a major concern since the slices from that drive will be rebuilt. However, on some systems that are experiencing higher than usual rates of drive failure, this may cause reliability concerns.	If a drive quarantines immediately after being resumed, please call IBM support to verify whether it is safe to try to fail the drive and migrate its slices. IBM support will check the state of the drive and also assess the health of the system to confirm that the potential loss of slices from that drive will not impact data reliability.
13738	Because data is reallocated between Slicestor® Devices during system expansion, it is preferred that the new Slicestor® Devices are physically located in the same sites as the existing sets. If this is not possible, slices that need to be reallocated may need to cross WAN links between sites. This can result in a slower reallocation rate and a longer reallocation phase. Additionally, the higher latency that typically exists when traversing these links can result in a greater request latency for requests that the source store must proxy.	If this situation arises, contact Customer Support to discuss the proposed system expansion. We will work with you to ensure that the new set of devices is provisioned in such a way that the inter-site traffic is minimized.

Deleting objects

Table 19. Deleting objects

Issue	Failing Condition	Disposition
9444	If a system is 100% full, customers may encounter an HTTP 500 error if they attempt to delete objects larger than the embedded content threshold (<1MB S3, >4MB SOH for default segments size). This issue has existed since release 3.0. It occurs because deleting large objects causes an intermediate write that appears larger to a Slicestor® Node, causing that node to fail the request due to an insufficient space error.	Contact IBM Support. They must use a development-provided procedure to free up disk space.

Manager Web Interface

Table 20. Manager Web Interface

Issue	Failing Condition	Disposition
10648	On the edit cabinet page, when unassigned nodes exist, it is not possible to move nodes to the bottom of the cabinet because the page does not scroll automatically.	Change the zoom so that all the cabinet slots are visible and then move the node to the desired slot.

Vaults

Table 21. Vaults

Issue	Failing Condition	Disposition
13533	The IBM Cloud Object Storage System™ CSO API does not enforce that new vaults created through the PUT Bucket API method be created with a naming convention compliant with the Amazon S3 bucket naming restrictions.	Refer to the *Manager Administration Guide* - Create Vaults section for the required naming convention for vaults.

Vault mirrors

Table 22. Vault mirrors

Issue	Failing Condition	Disposition
10788	If an extreme network bandwidth imbalance exists between two sites in a mirrored vault configuration, and total load on the system exceeds the capacity of the slower site, traffic to both sites may experience a "sawtooth" pattern with alternating periods of high and low throughput. Additionally, pending writes to the slower site will prevent writes to the faster site from proceeding. This occurs even if synchronous write is disabled.	During normal operation, disabling synchronous write allows requests to return to a user as soon as the fastest site returns. Reducing average throughput demand over time to be lower than the throughput capacity of the slower site will remove the "sawtooth" I/O pattern and will allow bursts of I/O to occur at the speed of the fastest site.
12854	When performing writes of small objects to a vault mirror, and synchronous writes are disabled, it is possible to queue a large number of operations in the Accesser® Node memory. Â If this condition persists, it is possible for the Accesser® Node to run out of memory.	To mitigate this issue from occurring, customers should ensure that they are not uploading objects at a rate greater than the slower site can handle.

Vault migration

Table 23. Vault migration

Issue	Failing Condition	Disposition
14403	When a vault is configured with an internal proxy configuration, there is an inconsistency in the way the client-accesser vs. accesser Slicestor® Device throughput is represented.	All inbound and outbound traffic is included in the client-accesser graph, but only the traffic to the backing vault is included in the accesser- Slicestor® Device throughput graph

Table 23. Vault migration (continued)

Issue	Failing Condition	Disposition
14450	In cases where the target vault of an active vault migration goes below threshold or becomes unavailable, the migration progress bar displayed in the manager may erroneously jump to 100% completed. In this condition, the migration will still be active, and any un-migrated objects will still be migrated.	The migration completion event in the manager will only trigger once the migration has fully completed, irrespective of the status reported in the progress bar. Therefore the completion of a migration should be judged by the migration completion event in the manager.
14484	When performing a vault migration, it has been observed that it is possible for the migration activity to halt and not make any progress.	There is no workaround or mitigation identified for this issue at this time. If you are performing a vault migration and progress has halted, contact IBM support.

Installation

Table 24. Installation

Issue	Failing Condition	Disposition
9465	When installing ClevOS using a physical or virtual CD drive, the appliance may reboot or hang while booting.	Use a USB storage device to perform the installation.

Native File

Table 25. Native File

Issue	Description
COS-7255	Certain workload conditions that involve reading content through NFI may result in OOM issues on the filer process.
COS-4269	Filesystem directories may become unresponsive if a large number of files are stored in a single directory (50,000+) or files are frequently deleted and added.
COS-5896	File Accesser devices only support hardware Accesser devices. Docker Accesser installations are not supported.
COS-5454	Under heavy load conditions where the File Accesser or Accesser devices become overloaded, the client may receive "Remote I/O Error" messages.
COS-6872	The File Accesser device REST Endpoint does not support SSL Connections (HTTPS), only HTTP is supported.
COS-6851	Using Filesystem or Share names with capital letters may prevent some S3 clients from accessing content properly using the File Accesser device REST API.
COS-6805	File Accesser devices configured within a single IBM COS installation can support a maximum of 100,000 shares and filesystems across all devices.
COS-6895	The File Accesser device REST API endpoint does not support authentication requests using query parameters (AWS V2 style authentication).
COS-6305	If multiple File Accesser devices in a File Server Pool are down only one of them displays the "Not Actively Participating" message in the Manager UI.
COS-2655	Manager UI shows incorrect capacity of drives of File Accesser devices. Instead of reporting the individual drive capacity, aggregate capacity is displayed.
COS-7349	Filename character set conversion between Windows-1252 and UTF-8 does not handle extended ASCII characters properly and will result in filenames with extended ASCII characters represented by "?" for files written by Windows and read by Linux (or vice versa). Standard ASCII conversion works properly. This only applies when the "character set" setting of a share is modified from the default utf-8 encoding.

Chapter 4. Supported Hardware Platforms

IBM Cloud Object Storage Appliances

Table 26. Minimum Version of ClevOS Compatible with Listed Hardware Platforms

Appliance	Model	Minimum ClevOS
IBM Cloud Object Storage Manager™ Appliance	M2100	≤2.7.0
IBM Cloud Object Storage Manager™ Appliance	M2105	3.2.2
IBM Cloud Object Storage Manager™ Appliance	M3100	2.7.0
IBM Cloud Object Storage Manager™ Appliance	M3105	3.7.2
IBM Cloud Object Storage Accesser® Device	A2100	≤2.7.0
IBM Cloud Object Storage Accesser® Device	A3100	≤2.7.0
IBM Cloud Object Storage Accesser® Device	A3105	3.7.2
IBM Cloud Object Storage Accesser® Device	A4105	3.7.2
IBM Cloud Object Storage Accesser® Device	AF5100	3.8.3
IBM Cloud Object Storage Slicestor® Device	S1440	≤2.7.0
IBM Cloud Object Storage Slicestor® Device	S2104	3.2.1
IBM Cloud Object Storage Slicestor® Device	S2212	3.2.1
IBM Cloud Object Storage Slicestor® Device	S2440	3.0.1
IBM Cloud Object Storage Slicestor® Device	S2448	3.7.2
IBM Cloud Object Storage Slicestor® Device	S4100	3.1.0
IBM Cloud Object Storage Slicestor®Device	S3448	3.8.3
IBM Cloud Object Storage Slicestor®Device	S2584	3.8.1

Hewlett Packard

Table 27. Minimum Version of ClevOS Compatible with Hewlett Packard Hardware

Appliance	Model	Minimum ClevOS
Manager Appliance	DL360P Gen8	3.2.1
Manager Appliance	DL360 Gen9	3.5.0
Manager Appliance	DL380 Gen9	3.5.0
Accesser® Device	DL360P Gen8	3.2.1
Accesser® Device	DL360 Gen9	3.5.0
Accesser® Device	DL380 Gen9	3.5.0
Slicestor® Device	SL4540 Gen8	2.9.0
Slicestor® Device	DL380 Gen9	3.5.0
Slicestor® Device	Apollo 4200	3.6.0
Slicestor® Device	Apollo 4510	3.6.0
Slicestor® Device	Apollo 4530	3.6.0

Seagate

Table 28. Minimum Version of ClevOS Compatible with Seagate Hardware

Appliance	Model	Minimum ClevOS
Seagate OneStor®	AP-2584 1 AP-TL-1	3.4.2

Cisco

Table 29. Minimum Version of ClevOS Compatible with Cisco Hardware

Appliance	Model	Minimum ClevOS
Cisco Slicestor® Device	UCS C3260	3.7.4

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